Mathematische Logik 2: Vorlesungmitschrift

Erich Grädel

(Mitschrift von Theodor Teslia)

Inhaltsverzeichnis

1 Mengenlehre

„Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können.“
(David Hilbert, 1926)

1.1 Mengen und Klassen

Reine Mengen sind Kollektion an Objekten, die ebenfalls wieder Mengen sind, als Alternative lassen sich Mengen ausgehend von Urelementen definieren.
Wie führt die Mathematik Objekte ein?

- Explizite Konstruktion aus schon vorhandenen Objekten, bspw. Konstruktion der rationalen, reellen und komplexen Zahlen, ausgehend von den ganzen und natürlichen.
- Axiomatisches formulieren von gewünschten Eigenschaften der Objekte und betrachte alle Objekte, die die Eigenschaften erfüllen, bspw. Gruppen, Vektorräume, ...

Definition 1.1 (Mengen)
Intuitiv sind Mengen *Kollektionen von Objekten*, die selbst wieder Mengen sind.
$a \in b$: a ist ein Element in der Menge b.
$a \subseteq b$: Jedes Element von a ist auch in b.
Eine Konstruktive Definition von aller Menge könnte wie folgt aussehen:
$\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}$ *usw.* Problem: Wie sieht dieses *usw.* aus?

Mengen lassen sich auch als Bäume darstellen. Dies lässt sich in Abbildung 1 Beispielhaft für die Menge $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ erkennen.

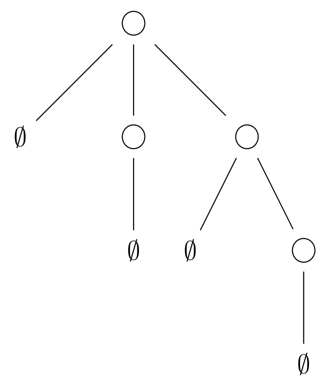

Abbildung 1: Darstellung der Menge $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ als Baum

Definition 1.2 (Hereditär endliche Mengen)
Die *hereditär endlichen Mengen* (HF) bilden eine Miniaturversion der Mengenlehre. Es gilt $\mathrm{HF}_0 \subset \mathrm{HF}_1 \subset \mathrm{HF}_2 \subset \dots$. Definiert sind diese Mengen induktiv als $\mathrm{HF}_0 \coloneqq \emptyset$ und $\mathrm{HF}_{n+1} \coloneqq \{x : x \subseteq \mathrm{HF}_n\}$, so dass HF_{n+1} die Potenzmenge von HF_n ist.

Eine Menge ist hereditär endlich, wenn sie Element einer Menge HF_n für ein n ist. Weiter wird $\mathrm{HF} \coloneqq \{x : x \in \mathrm{HF}_n \text{ für ein } n \in \mathbb{N}\}$ definiert. Dies wirft folgende Frage auf: Ist HF eine Menge?

Beispiel 1.1
Wir wollen nun die ersten HF-Mengen bilden:

- $\mathrm{HF}_0 = \emptyset$
- $\mathrm{HF}_1 = \{\emptyset\}$
- $\mathrm{HF}_2 = \{\emptyset, \{\emptyset\}\}$
- $\mathrm{HF}_3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

Es lässt sich erkennen, dass $\mathrm{HF}_n \subset \mathrm{HF}_{n+1}$ und $\mathrm{HF}_n \in \mathrm{HF}_{n+1}$ für ein beliebiges n. Auch ist es möglich zu folgern, dass HF_n endlich viele Elemente besitzt und jede Menge $a \in \mathrm{HF}_{n+1}$ die Gestalt $a = \{b_0, \dots, b_{k-1}\}$ mit $b_0, \dots, b_{k-1} \in \mathrm{HF}_n$. Außerdem gilt, dass HF nicht hereditär endlich ist.

Definition 1.3 (Natürliche Zahlen)
Eine *natürliche Zahl* n ist definiert als $[n] := \{[0], \dots, [n-1]\}$, wobei $[0] = \emptyset$ gilt. Die Menge der natürlichen Zahlen $\mathbb{N}$ lässt sich nun als $\mathbb{N} := \{[n] : n \text{ eine nat. Zahl}\} \notin \mathrm{HF}$ definieren.

Eine Folgerung ist $[n] \in \mathrm{HF}_{n+1} \setminus \mathrm{HF}_n$.

Axiomensysteme für die Mengenlehre

Das Modell der Mengenlehre besteht aus einer Kollektion $\mathcal{S}$ von Objekten, die wir Mengen nennen und einer Beziehung $\in$ zwischen diesen Objekten, so dass alle Axiome des Axiomensystems erfüllt werden.

Definition 1.4 (Extensionalitätsaxiom (Ext.))
Zwei Mengen sind gleich, genau dann, wenn sie die selben Elemente haben. In einer Formel aus der Prädikatenlogik mit Signatur $\{\in\}$ wäre dies $\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$.

Definition 1.5 (Konsistenz)
Die *Konsistenz* des Axiomensystems der Mengenlehre beschreibt, ob es ein Modell des Axiomensystems gibt oder ob dieses widersprüchlich ist. Es ist nicht möglich, die Konsistenz unseres Axiomensystems zu beweisen.

Definition 1.6 (Vollständigkeit)
Das Axiomensystem der Mengenlehre ist *Vollständig*, wenn alle Modelle „gleich “ sind, in dem Sinn, dass die gleichen Eigenschaften gelten. Es gibt kein vollständiges Axiomensystem für die Mengenlehre.

Nehmen wir an, dass $(\mathcal{S}, \in)$ ein beliebiges, aber festes Modell der Mengenlehre ist. Die Axiome sollen regeln, welche Kollektionen von Elementen aus $\mathcal{S}$ selbst wieder Elemente von $\mathcal{S}$, also Mengen sind. Dabei werden Kollektionen *Klassen* genannt und Klassen, die keine Mengen sind, werden als *echte Klassen* bezeichnet.

Definition 1.7 (Die naive Mengenlehre)
Das Axiomensystem der naiven Mengenlehre besitzt zwei Axiome. Zum einen das Extensionalitätsaxiom (siehe Definition 1.4) und das Axiomenschema der vollen Komprehension. Dieses besagt, dass sich für jede Formel $\psi(x)$ die Menge $\{x : \psi(x)\}$ bilden lässt: also für feste $\psi(x) \in \mathrm{FO}$ gilt $\exists z \forall z (x \in z \leftrightarrow \psi(x))$.

Satz 1.1 (Zermelo-Russel Paradoxon)
Die naive Mengenlehre ist inkonsistent.

Sei $\psi(x) \coloneqq x \notin x$. Nach dem Komprehensionsschema muss nun folgende Formel gelten: $\exists z \forall x (x \in z \leftrightarrow x \notin x)$, aus welcher die Menge $z = \{x : x \notin x\}$ folgt. Eine solche Menge kann aber nicht existieren, da sonst $z \in z \Leftrightarrow z \notin z$ gelten müsste. Es folgt, dass $\{x : x \notin x\}$ immer eine echte Klasse sein muss.

Definition 1.8 (Das Axiomensystem ZFC)
Das Axiomensystem ZFC (**Z**ermelo-**F**raenkel-**C**hoice) ist das meist-benutzte Axiomensystem. Es besitzt die folgenden Axiome:

- Das Extensionalitätsaxiom
- Das Aussonderungsaxiom: $\forall z \exists y \forall x (x \in y \leftrightarrow (x \in z \wedge \psi(x)))$. Dieses ist eine schwächere Version des Komprehensionsschemas, bei dem eine Menge aus einer bereits bestehenden Menge ausgewählt wird.
- Das Erzeugungsaxiom (Kreationsaxiom): Für jede Menge x ex. eine *Stufe* $s \in \mathcal{S}$ mit $x \in s$.
- Das Unendlichkeitsaxiom: Es gibt eine *Limesstufe* und damit eine unendliche Menge.
- Das Ersetzungsaxiom: Für jede Funktion $F : \mathcal{S} \to \mathcal{S}$ mit der Eigenschaft, dass $\mathrm{Def}(F)$ eine Menge ist, ist auch $\mathrm{Bild}(F)$ eine Menge.
- Das Auswahlaxiom: Auf jeder Menge ex. eine *Auswahlfunktion*

Definition 1.9 (Klassenoperatoren)
Seien A, B Klassen.

- $A \subseteq B$: Jede Menge aus A ist auch in B.
- $\bigcap A \coloneqq \{x : x \in y \text{ für alle } y \in A\}$
- $A \cap B \coloneqq \{x : x \in A \text{ und } x \in B\}$
- $A \setminus B \coloneqq \{x : x \in A \text{ aber } x \notin B\}$

Für eine Formel $\psi(x)$ kann $\{x : \psi(x)\}$ entweder eine Menge oder eine echte Klasse sein. Somit lässt sich das Aussonderungsaxiom umformulieren: Für jede Menge a und jede Klasse A ist $a \cap A$ eine Menge. Daraus folgt, dass auch $a \setminus A$ eine Menge sein muss, dass $\bigcap A$ eine Menge ist, falls A mindestens eine Menge enthält und, dass $\bigcap \emptyset = S$ keine Menge ist.

1.2 Stufen und Geschichten

Eine mögliche Methode zur Definition der gesamten Klasse aller Mengen ist es, die induktive Konstruktion der hereditär endlichen Mengen zu erweitern. So ist $\mathcal{S}$ dann die Vereinigung einer aufsteigenden Folge von Mengen S_α, welche wir die Stufen von $\mathcal{S}$ nennen. Es gilt $S_0 \coloneqq \emptyset$ und für die bereits definierte Stufe S_α setzen wir $S_{\alpha+1} \coloneqq \{x : x \in S_\alpha\}$.

Sobald eine unendliche Folge von solchen Stufen definiert wurde, lässt sich eine neue Stufe als Vereinigung aller bisherigen Stufen definieren.

So erhalten wir:

- $S_0 = \mathrm{HF}_0 = \emptyset$, $S_1 = \mathrm{HF}_1, \ldots, S_n = \mathrm{HF}_n$

- $S_\omega \coloneqq \bigcup_n S_n = \bigcup_n \mathrm{HF}_n = \mathrm{HF}$
- $S_{\omega+1} \coloneqq \{x : s \in S_\omega\}, \ldots$
- $S_{\omega+\omega} \coloneqq \{x : x \in S_{\omega+n}$ für ein $n\}$ *usw.*

Definition 1.10 (Die Akkumulation)
Sei A eine Klasse. Die *Akkumulation* von A ist $\mathrm{acc}(A) \coloneqq \{x : (\exists y \in A) x \in y \vee x \subset y\})$.

Da für eine Klasse A und ein Element $a \in A$ natürlich gilt, dass $a \subseteq a$, gilt auch $a \in \mathrm{acc}(A)$ und somit $A \subseteq \mathrm{acc}(A)$.

Definition 1.11 (Geschichten)
Eine *Geschichte* ist eine Klasse H, so dass für alle $a \in H$ gilt $\mathrm{acc}(a \cap H) = a$.

Die Stufe mit Geschichte H ist $S \coloneqq \mathrm{acc}(H)$.

Beispiel 1.2 (Beispiele zu Geschichten und Stufen)
Im Folgenden soll für einige Mengen ihre Akkumulation gezeigt werden und bewiesen, dass es sich bei diesen auch um Geschichten handelt.

- $\mathrm{acc}(\emptyset) = \emptyset$. $\emptyset$ ist eine Geschichte und die Stufe mit Geschichte $\emptyset$ ist $\emptyset$.
- $\{\emptyset\} = [1] = \mathrm{HF}_1 = \{\mathrm{HF}_0\}$: $\mathrm{acc}(\{\emptyset\}) = \{\emptyset\}$. $\{\emptyset\}$ ist auch eine Geschichte, denn für das einzige Element $\emptyset$ gilt $\mathrm{acc}(\emptyset \cap \{\emptyset\}) = \mathrm{acc}(\emptyset) = \emptyset$. Die Stufe mit Geschichte $\{\emptyset\}$ ist also $\{\emptyset\}$.
- $\{\emptyset, \{\emptyset\}\} = [2] = \mathrm{HF}_2 = \{\mathrm{HF}_0, \mathrm{HF}_1\}$: $\mathrm{acc}(\mathrm{HF}_2) = \mathrm{HF}_2$. HF_2 ist eine Geschichte, denn $\mathrm{acc}(\emptyset \cap \{\emptyset, \{\emptyset\}\}) = \mathrm{acc}(\emptyset) = \emptyset$ und $\mathrm{acc}(\{\emptyset\} \cap \{\emptyset, \{\emptyset\}\}) = \mathrm{acc}(\{\emptyset\}) = \{\emptyset\}$. Somit ist die Stufe mit Geschichte $\{\emptyset, \{\emptyset\}\}$ die Menge $\{\emptyset, \{\emptyset\}\}$.

Dies wirft die Frage auf, ob es eine Verallgemeinerung gibt. Demnach soll nun überprüft werden, ob $[n]$, HF_n oder $\mathrm{G}_n \coloneqq \{\mathrm{HF}_0, \ldots, \mathrm{HF}_{n-1}\}$ Geschichten sind, für beliebige $n \in \mathbb{N}$.

- $[n]$: Für $k < n$ müsste gelten, dass $\mathrm{acc}([n] \cap [k]) = \mathrm{acc}([k]) = [k]$. Aber $\mathrm{acc}([k])$ enthält alle Teilmengen von $[k-1]$, für $k = 4$ also alle Teilmengen von $\{[0], [1], [2]\}$, demnach auch $\{[0], [2]\}$. Es gilt aber, dass $\{[0], [2]\} \notin [k]$ und es folgt $\mathrm{acc}([k]) \neq [k]$. Für $n \geq 3$ ist n also keine Geschichte.
- HF_n: Dies gilt wieder nicht, denn $[n-1] \in \mathrm{HF}_n$ und $\mathrm{acc}([n-1] \cap \mathrm{HF}_n) = \mathrm{acc}([n-1]) \neq [n-1]$.
- G_n: Die Menge $\mathrm{G}_n \coloneqq \{\mathrm{HF}_0, \ldots, \mathrm{HF}_{n-1}\}$ ist aber eine Geschichte für beliebige $n \in \mathbb{N}$. Für $n = 0, 1, 2$ wurde dies schon in Beispiel 1.2 gezeigt. Sei dies für G_n bereits bewiesen, wir zeigen dies nun für $\mathrm{G}_{n+1} = \mathrm{G}_n \cup \{\mathrm{HF}_n\}$.

  G_{n+1} ist eine Geschichte, wenn für alle $k \leq n$ gilt: $\mathrm{acc}(\mathrm{HF}_k \cap \mathrm{G}_{n+1}) = \mathrm{HF}_k$. $\mathrm{HF}_k \cap \mathrm{G}_{n+1} = \{\mathrm{HF}_0, \ldots, \mathrm{HF}_{k-1}\} = \mathrm{G}_k$ und per Induktionsvoraussetzung gilt $\mathrm{acc}(\mathrm{G}_k) = \mathrm{HF}_k$.

Also ist G_{n+1} eine Geschichte. Die Stufe mit Geschichte G_{n+1} ist $\mathrm{acc}(\mathrm{G}_{n+1}) = \mathrm{acc}(\mathrm{G}_n \cup \{\mathrm{HF}_n\}) = \mathrm{acc}(\mathrm{G}_n) \cup \mathrm{HF}_n \cup \{x : x \subseteq \mathrm{HF}_n\} = \mathrm{HF}_n \cup \mathrm{HF}_n \cup \mathrm{HF}_{n+1} = \mathrm{HF}_{n+1}$.

Dies gibt die Idee für die Rückrichtung: Für jede Stufe S_α soll gelten, dass sie die Geschichte $H(S_\alpha) = \{S_\beta : \beta < \alpha\}$ hat.

Definition 1.12 (Minimales Element)
Eine Menge $m \in A$ ist ein *minimales Element* von A, wenn $m \cap A = \emptyset$, d.h. es gibt kein $a \in A$ mit $a \in m \in A$.

Definition 1.13 (Fundiertheit einer Menge)
Eine Menge a ist fundiert, wenn jede Menge b mit $a \in b$ ein minimales Element enthält. Der fundierte Teil von A ist $\mathrm{fd}(A) := \{x \in A : x \text{ ist fundiert}\}$.

Beispiel 1.3 (Beispiele für minimale Elemente und Fundiertheit)
$\emptyset$ ist offensichtlich fundiert.
$\{\emptyset\}$ ist ebenfalls fundiert. Sei $\{\emptyset\} \in b$. Wenn $\{\emptyset\} \cap b = \emptyset$ ist $\{\emptyset\}$ das minimale Element. Andernfalls ist $\{\emptyset\} \cap b = \{\emptyset\}$ und $\emptyset$ ist das minimale Element von b.

Satz 1.2
Wenn H eine Geschichte ist, dann enthält jede nicht-leere Teilmenge von H ein minimales Element.

Beweis. Es sei $a \in b \subseteq H$ und $c = \{\mathrm{fd}(x) : x \in a \cap b\} = \{y : y = \mathrm{fd}(x) \text{ für } x \in a \cap b\}$. Wenn $c = \emptyset$, dann ist $a \cap b = \emptyset$ und a ist das minimale Element von b. Sei $c \neq \emptyset$. Wir wollen zeigen, dass $c \subseteq \mathrm{fd}(a)$.

Lemma 1.2.1*:* Sei H eine Geschichte, mit $a, b \in H$ und $a \in b$. Dann muss $\mathrm{fd}(a) \in \mathrm{fd}(b)$ gelten.

Beweis. Ansonsten wäre $\mathrm{fd}(a) \in \mathrm{acc}(b \cap H) = b$, da $\mathrm{fd}(a) \subseteq a \in b \cap H$. Also gilt mit der Voraussetzung $\mathrm{fd}(a) \in b \backslash \mathrm{fd}(b)$. Demnach ex. eine Menge x mit $\mathrm{fd}(a) \in x$ ohne minimale Elemente. Speziell ist $\mathrm{fd}(a)$ kein minimales Element von x, d. h. $\mathrm{fd}(a) \cap x \neq \emptyset$. Sei $y \in \mathrm{fd}(a) \cap x$. Da $y \in \mathrm{fd}(a)$ ist y fundiert. Da $y \in x$ hat x ein minimales Element. Dies ist ein Widerspruch zu der Aussage, dass $\mathrm{fd}(a) \in b \setminus \mathrm{fd}(b)$, es muss also $\mathrm{fd}(a) \in \mathrm{fd}(b)$ gelten. □

Sei $y \in c$. Dann ist $y = \mathrm{fd}(x)$ für ein $x \in a \cap b$. Aus dem Lemma folgt, dass $y \in \mathrm{fd}(a)$. Also $c \subseteq \mathrm{fd}(a)$.

Wenn $y \in c \subseteq \mathrm{fd}(a)$, dann ist y fundiert und c hat ein minimales Element z. Nach der Definition von c ist dann $z = \mathrm{fd}(x)$ für ein $x \in a \cap b$.

Behauptung: x ist das minimale Element von b. Wenn nicht, dann existiert ein $u \in x \cap b$. Da $u \in x \in a \cap b \subseteq a \cap H$ und $a \in H$ ist auch u in $\mathrm{acc}(a \cap H) = a$. Also $u \in a \cap b$ und daher $\mathrm{fd}(u) \in c = \{\mathrm{fd}(x) : x \in a \cap b\}$. Aus dem Lemma folgt $\mathrm{fd}(u) \in \mathrm{fd}(x)$, da $u \in b \subseteq H$ und $x \in b \subseteq H$. Also $\mathrm{fd}(u) \in \mathrm{fd}(x) \cap c \neq \emptyset$. Also ist $z = \mathrm{fd}(x)$ nicht minimales Element von c. Dies ist ein Widerspruch. □

Satz 1.3
Sei H eine Geschichte. Jedes Element $a \in H$ ist eine Stufe mit Geschichte $H \cap a$.

Beweis. Da H eine Geschichte ist, gilt $a = \mathrm{acc}(H \cap a)$. Wenn $H \cap a$ eine Geschichte ist, dann ist a die zugehörige Stufe. Sei $b \in H \cap a$. Dann $b \subseteq a$, da $c \in b \in H \cap a \Rightarrow c \in \mathrm{acc}(H \cap a) = a$ und also $H \cap b = (H \cap a) \cap b$. Da $b \in H$ gilt, dass $b = \mathrm{acc}(H \cap b) = \mathrm{acc}((H \cap a) \cap b)$. Also ist $H \cap a$ eine Geschichte. □

Definition 1.14 (Transitive und Erbliche Klassen)
Eine Klasse ist

- *transitiv*, wenn für alle $a \in b \in A$ auch $a \in A$ gilt, also jedes Element von A ist auch Teilmenge von A.
- *erblich*, wenn für alle $a \subseteq b \in A$ auch $a \in A$ gilt.

Satz 1.4
Sei S eine Stufe mit Geschichte H. Dann gelten:

a) S ist erblich und transitiv.

b) $S = \{x : x \subseteq s \text{ für eine Stufe } s \in S\}$

c) $\mathrm{H}(S) := \{s \in S : s \text{ ist Stufe}\}$ ist eine Geschichte von S.

Beweis. a) Sei $b \in S = \mathrm{acc}(H)$, es ist zu zeigen, dass $a \in b \Rightarrow a \in S$ und $a \subseteq b \Rightarrow a \in S$. Sei $c = \{s \in H : b \in s \vee b \subseteq s\} \subseteq H$ Da $b \in \mathrm{acc}(H)$ ist $c \neq \emptyset$ und daher existiert ein $s \in c$ mit $s \cap c = \emptyset$. Nach Definition von c gilt $b \in s$ oder $b \subseteq s$.
Behauptung: $b \notin s$, da sonst $b \in s = \mathrm{acc}(H \cap s)$, also ex. $z \in H \cap s$ mit $b \subseteq z$ oder $b \in z$. Dann ist aber $z \in c \cap s \neq \emptyset$, also ein Widerspruch. Es muss also $b \subseteq s$ gelten.

- $a \in b \Rightarrow a \in b \subset s = \mathrm{acc}(H \cap s) \subseteq (H) = S \Rightarrow a \in S$
- $a \subseteq b \Rightarrow a \subseteq b \subseteq s \in H \Rightarrow a \in \mathrm{acc}(H) = S$

b)

$\supseteq$: $a \subseteq s \in S \overset{a)}{\Rightarrow} a \in S$.

$\subseteq$: Sei $a \in S = \mathrm{acc}(H)$. Es gilt $s \in H$ mit $a \in s$ oder $a \subseteq s$. Nach dem Satz 1.3 ist s eine Stufe mit Geschichte $H \cap s$ und daher erblich und transitiv (nach a)). Wenn $a \in s$, dann $a \subseteq s$. Also $a \subseteq s \in H \subseteq S$ und daher $a \in \{x : x \subseteq s \text{ für ein } s \in S\}$.

c) $\mathrm{acc}(\mathrm{H}(S)) = \{x : (\exists s \in \mathrm{H}(S)) x \in s \vee x \in s\} = \{x : (\exists s \in S) s \text{ ist Stufe}, x \subseteq s \in\} \overset{b)}{=} S$. $\mathrm{H}(S)$ ist also eine Geschichte. $\mathrm{H}(S) \cap s = \{s \in S \cap s : x \text{ Stufe}\} = \{x \in s : x \text{ Stufe}\}$. Dann $\mathrm{acc}(\mathrm{H}(S) \cap s) = \{y : (\exists s' \in s) s' \text{ ist Stufe}, y \subseteq s'\} \overset{b)}{=} S$ □

Aus diesen Sätzen folgt, dass für die Geschichte H einer Stufe S gilt, dass $H \subseteq H(S)$. Sei $a \in H$. Es folgt $a \in S = \mathrm{acc}(H)$ und a ist eine Stufe mit Geschichte $H \cap a$, also $a \in H(S)$,

Satz 1.5
Jede nicht-leere Klasse A von Stufen hat ein minimales Element $s_0(A)$.

Beweis. Sei $A \subset \{s : s \text{ ist eine Stufe}\}$, so dass kein $s \in s_0(A) \cap A$ existiert. Sei $s \in A$ und $x := s \cap A$. Wenn $x = \emptyset$, dass $s_0(A) = s$. Andernfalls ist $x \subseteq \{t \in s : t \text{ ist eine Stufe}\}$ eine nicht-leere Teilmenge einer Geschichte und hat daher ein minimales Element $m \in x$, so dass gilt $m \cap x = \emptyset$. Setze $s_0(A) = m$, es folgt $s_0(A) \cap A = \emptyset$. Wäre nämlich $t \in s_0(A) \cap A = m \cap A$, da $t \in m \in x \subset s$, also $t \in s$, da m transitiv ist, also $t \in x$. Es würde also ein $t \in m \cap x$ existieren. Widerspruch! □

Satz 1.6
Seien S, T Stufen, welche auch Mengen sind. Dann gilt entweder $S \in T$, $S = T$ oder $T \in S$.

Beweis. Wenn nicht, dann ist die Klasse $A := \{s : s \text{ ist Stufe und es gibt eine Stufe } t \text{ mit } s \notin t, s \neq t \text{ und } t \notin s\}$ nicht leer und enthält ein minimales Element $s_0 = s_0(A)$. Die Klasse $B := \{t : t \text{ is eine Stufe, so dass } s_0 \notin t, s_0 \neq t \text{ und } t \notin s_0\}$ muss dann ebenfalls ein minimales Element t_0 enthalten. Es gilt $\boxed{s_0 \notin t_0, s_0 \neq t_0 \text{ und } t_0 \notin s_0}$. Sei $s \in s_0$. Dann ist $s \neq t_0$, da sonst $t_0 \in s_0$. Zweitens ist $t_0 \notin s$, da sonst $t_0 \in s \notin s_0$ und damit $t_0 \in s_0$. Wenn auch noch $s \notin t_0$ gelten würde, dann wäre $s \in A$ im Widerspruch zur Minimalität von s_0. Also muss $s \in t_0$. Aber damit ist gezeigt, dass $s_0 \subseteq t_0$. Analog lässt sich zeigen, dass $t_0 \subseteq s_0$ sein muss. Also $s_0 = t_0$. Widerspruch! □

Aus dieser wichtigen Eigenschaft lassen sich einige Folgerungen feststellen. Seien S, T Stufen aus $\mathcal{S}$.

a) $S \notin S$

b) $S \subseteq T \Leftrightarrow S = T$ oder $S \in T$

c) $S \subseteq T$ oder $T \subset S$

d) $S \subsetneq T \Leftrightarrow S \in T$

Beweis. a) Wäre $S \in S$, wäre $A = \{s : s \text{ ist Stufe}, s \in s\}$ eine nicht-leere Klasse an Stufen, mit minimalem Element s_0, das heißt $s_0 \cap A = \emptyset$. Aber $s_0 \in A$, wonach $s_0 \in s_0$, was zur Folge hat, dass $s_0 \in s_0 \cap A \neq \emptyset$. Widerspruch!

b) „$\Leftarrow$“: Wenn $S = T$, dann ist offensichtlich $S \subseteq T$ und wenn $S \in T$, dann gilt wegen der Transitivität auch $S \subseteq T$.

„$\Rightarrow$ “: Wenn $S \neq T$ und $S \notin T$, dann muss $T \in S$ gelten, wenn nun aber $S \subseteq T$, dann ist $T \in S \subseteq T$, was ein Widerspruch zu Teil a) ist.

c) Wenn $S \not\subseteq T$, dann muss wegen b) $S \notin T$ und $S \neq T$ gelten. Also ist $T \in S$ und daher auch $T \subseteq S$.

d) $S \subsetneq T \Leftrightarrow S \subseteq T \wedge S \neq T \Rightarrow S \in T$ □

Statt $S \in T$, bzw. $S \subsetneq T$ schreibt man oft $S < T$. Die so erzeugte lineare Ordnung von Stufen bezeichnet man als *kumulative Hierarchie* und ist die durch $\in$ linear geordnete Kollektion aller Stufen.

Das *Kreationsaxiom* besagt, dass zu jeder Menge a eine Menge s existiert, welche eine Stufe ist, mit $a \in s$. Aus diesem folgt, dass es zu jeder Stufe s eine höhere Stufe t mit $s \in t$ gibt, welche ebenfalls eine Stufe ist. Es lässt sich dadurch auch erkennen, dass $\mathcal{S}$ die Vereinigung aller Stufen ist. Wenn wir zudem akzeptieren, dass $\emptyset$ eine Menge ist, also $\mathcal{S} \neq \emptyset$, dann folgt, dass $\mathrm{HF} \subseteq \mathcal{S}$ und, dass $\mathcal{S}$ selbst wieder eine Stufe mit der Geschichte $H(\mathcal{S}) = \{s : s \text{ ist eine Stufe}\}$ ist.

Definition 1.15 (Nachfolgerstufe)
Eine Stufe T ist die *Nachfolgerstufe* zur Stufe S, wenn $S \in T$ und keine Stufe T' existiert, mit $S \in T' \in T$.

Definition 1.16 (Limesstufe)
Eine Stufe $S \neq \emptyset$ ist eine *Limesstufe*, wenn sie keine Nachfolgerstufe ist.

Definition 1.17
Für jede Klasse A ist $S(A)$ die kleinste Stufe mit $A \subseteq S$. Dies ist wohldefiniert, da jede nicht-leere Klasse von Stufen ein minimales Element besitzt. Es gilt $S(s) = s$ für jede Stufe s.

Es gilt, dass HF_{n+1} die Nachfolgerstufe von HF_n ist.
Aus dem *Aussonderungsaxiom* lassen sich weitere praktische Eigenschaften folgern. Sei a eine Menge. Es lassen sich nun Elemente aussondern, so dass man die Mengen $\{a\}$, $\mathrm{acc}(a)$ und $\bigcup a := \{b : b \in x \text{ für ein } x \in a\}$ bilden kann.
Für eine Stufe s mit $a \in s \in \mathcal{S}$ gilt:

- $\{a\} = \{x \in s : x = a\}$
- $\{\mathrm{acc}(a)\} = \{x \in s : (\exists b \in a) x \in b \vee x \subseteq b\}$
- $\bigcup a = \{b \in s : (\exists x \in a) b \in x\}$

Lemma 1.2.2*:* Wenn $a \in b$, dann $S(a) \in S(b)$.

Beweis. Da $a \in b \subseteq S(b) = \mathrm{acc}(H(S(b)))$ ex. $s \in S(b)$ mit $a \in s$ (und durch die Transitivität $a \subseteq s$), also ist $S(a) \subseteq s$ und daher $S(a) \subseteq s \in S(b)$ und da $S(b)$ erblich ist, folgt $S(a) \in S(b)$. $\square$

Lemma 1.2.3*:* $\mathcal{S}$ ist die einzige Stufe, welche ein echte Klasse ist.

Beweis. Sei S eine Stufe, $S \neq \mathcal{S}$. Also ex. $a \in \mathcal{S} \setminus S$. Es folgt, dass $S(a) \notin S$, da sonst $a \subseteq S(a) \in S$ und daher $a \in S$. Für Stufen $T \supseteq S(a)$ gilt daher $T \notin H(\mathcal{S}) = \{s \in \mathcal{S} : s \text{ ist Stufe}\}$. Also $H(S) \subseteq \{T : T \text{ ist Stufe}, T \in S(a)\}$. Da $S(a)$ und $H(S(a))$ mengen sind, ist auch $H(S)$ eine Menge und damit auch $S = \mathrm{acc}(H(S))$. $\square$

Daraus lässt sich folgern, dass die folgenden Aussagen für eine Klasse A äquivalent sind:

1. A ist eine echte Klasse.
2. $S(A)$ ist eine echte Klasse.
3. $S(A) = \mathcal{S}$.

Beweis. 3. $\Rightarrow$ *1.*: Wenn A eine Menge ist, ist auch $S(A)$ eine Menge. Nach Kontraposition gilt die Folgerung.

1. $\Rightarrow$ *2.*: Wenn $S(A)$ eine Menge ist, ist auch $A = A \cap S(A)$ eine Menge. Nach Kontraposition gilt die Folgerung.

2. $\Rightarrow$ *3.*: Dies wurde in Lemma 1.2.3 bewiesen. $\square$

Satz 1.7
Für jede Menge a gilt $a \notin a$.

Beweis. Es gelte $a \in a$. Dann $a \in a \subseteq S(a)$. $S(a) = \{x : x \subseteq s \text{ für eine Stufe } s \in S(a)\}$, also existiert $s \in S(a)$ mit $a \subseteq s$. $S(a)$ ist aber die minimale Stufe, die a als Teilmenge enthält. Widerspruch! $\square$

Durch diesen Satz ist die Fundiertheit der Mengenlehre bewiesen.

Satz 1.8
Jede nicht-leere Klasse enthält ein minimales Element.

Beweis. Sei A eine nicht-leere Klasse. $B = \{S(b) : b \in A\}$ ist die nicht-leere Klasse der Stufen in A und hat ein minimales Element $s_0 = S(b_0)$. D.h. $S(b_0) \cap B = \emptyset$. Behauptung: b_0 ist das minimale Element von A. Andernfalls ex. $b_1 \in b_0 \cap A$. Da $b_1 \in b_0$ ist auch $S(b_1) \in S(b_0)$. Da $b_1 \in A$ folgt $S(b_1) \in b$. Also $S(b_1) \in S(b_0) \cap B \neq \emptyset$. Widerspruch! $\square$

Lemma 1.2.4*:* Set $S \in \mathcal{S}$ eine Stufe. Die Nachfolgerstufe von S ist $\mathcal{P}(S)$, wobei $\mathcal{P}$ die Potenzfunktion ist.

Beweis. Es gibt eine minimale Stufe T mit $S \in T$. Nun ist zu zeigen, dass $\mathcal{P}(S) = T$.

Aus $a \subseteq S \in T$ folgt wegen der Erblichkeit von T auch $a \in T$. Also $\mathcal{P}(S) \subseteq T$. Sei $s \in T$ eine Stufe. $S \notin s$, da T die Nachfolgerstufe von S ist. Also gilt $S = s$ oder $s \in S$ und $s \subseteq S$. Für alle Stufen s gilt $s \in T \Leftrightarrow s \subseteq S$. Nun gilt $T = \{x : x \subseteq s \text{ für eine Stufe } s \in T\} = \{x : x \subseteq s \text{ für eine Stufe } s \subseteq S\} = \{x : x \subseteq S\} = \mathcal{P}(S)$ $\square$

Satz 1.9
Sei $S \neq \emptyset$ eine Stufe. Nun sind äquivalent:

1. S ist eine Limesstufe.

2. $S = \bigcup H(S)$.

3. Für alle $a \in S$ ex. eine Stufe $t \in S$ mit $a \in t$.

4. Wenn $a \in S$, dann $\mathcal{P}(a) \in S$.

5. Wenn $a \in S$, dann $\{a\} \in S$.

Beweis.
- *1.* $\Rightarrow$ *2.*: Es gilt $S = \{x \subseteq s$ für eine Stufe $s \in S\}$ und $H(S) = \{s \in S :$ s ist eine Stufe$\}$. Wenn S eine Limesstufe ist, dann gilt für alle $s \in S$ auch $\mathcal{P}(s) \in S$. $\bigcup H(S) = \{x : x \in s$ für ein $s \in H(S)\} = \{x : x \in s$ für eine Stufe $s \in S\}$ und da S eine Limesstufe gilt, dass dies gleich zu $\{s : s \in \mathcal{P}(s)$ für eine Stufe $s \in S\} = \{x : x \subseteq$ s für eine Stufe $s \in S\} = S$ ist.

- *2.* $\Rightarrow$ *1.*: Sei $S = \mathcal{P}(()T)$ für eine Vorgängerstufe T mit $H(S) = H(T) \cup \{T\}$. $\bigcup H(S) =$ $\{x : x \in s \in S, s$ ist Stufe$\} = \{x : x \in T\} = T \neq S$. Widerspruch!

- *1.* $\Rightarrow$ *3.*: Da $S = \{s : x \subseteq s$ für eine Stufe $s \in S\}$ folgt für $a \in S$, dass eine Stufe s existiert mit $a \subset s$, also $a \in \mathcal{P}(()s) \in S$.

- *3.* $\Rightarrow$ *4.*: Für $a \in S$ ex. eine Stufe $t \in T$ mit $a \in t$. Sei nun $x \in \mathcal{P}(a)$. Aus $x \subseteq a \in t$ folgt $x \in t$, das heißt $\mathcal{P}(a) \in S = \{x : x \subseteq s$ für eine Stufe $s \in S\}$.

- *4.* $\Rightarrow$ *5.*: Wenn $a \in S$, dann $\{a\} \subseteq P(a) \in S$. Da S erblich ist, ist $\{a\} \in S$.

- *5.* $\Rightarrow$ *1.*: Wenn S keine Limesstufe ist, also $S = \mathcal{P}(T)$, dann $T \in S$ und nach *5.* $\{T\} \in S$. Da $S = \mathcal{P}(T)$ ist $\{T\} \subseteq T$, also $T \in T$. Widerspruch!

$\square$

Definition 1.18 (cut einer Klasse)
Der cut einer Klasse A ist die Menge $\mathrm{cut}(A) \coloneqq \{x \in A : S(x) \subseteq S(y)$ für alle $y \in A\}$. In Worten enthält $\mathrm{cut}(A)$ also die Elemente von A mit minimaler Stufe.

Es gilt $\mathrm{cut}(\emptyset) = \emptyset$ und $\mathrm{cut}(\{a\}) = \{a\}$. Für $a \in A$ ist $\mathrm{cut}(A) \subseteq S(a)$.

Satz 1.10
Eine Stufe ist eine Limesstufe, genau dann, wenn $\mathrm{cut}(a) \in S$ für alle $a \subseteq S$.

Beweis. $\Rightarrow$: Für $a = \emptyset$ ist $\mathrm{cut}(a) = \emptyset \in S$. Sei $x \in a \subseteq S$. Dann ex. ein $s \in S$ mit $x \in s$ und $x \subseteq s$, also $\mathrm{cut}(a) \subseteq s \in S$.
$\Leftarrow$: Sei $S = \emptyset$. Dann $\emptyset \subseteq S$, aber $\mathrm{cut}(\emptyset) = \emptyset \notin S$. Sei $S = \mathcal{P}(T)$ eine Nachfolgerstufe. Dann ist $T \in S$, also $\{T\} \subseteq S$, aber $\mathrm{cut}(\{T\}) = \{T\} \notin S$. Also muss S eine Limesstufe sein. $\square$

Nun wurden die ersten vier der sechs Axiome des Axiomensystems ZFC betrachtet. Das Aussonderungs-, Extensionalitäts-, Kreations- und Unendlichkeitsaxiom.

Mit den ersten dreien ist es noch möglich, dass $\mathcal{S} = \emptyset$ oder $\mathcal{S} = \mathrm{HF}$ gilt. Durch dass Unendlichkeitsaxiom, welches die Existenz einer Limesstufe fordert ist dies nicht mehr möglich. Benutzt man diese vier Axiome lässt sich also aussagen, dass $S \neq \emptyset$, die Mengen HF_n für beliebige n existieren und HF eine Menge ist.
Der bisherige Aufbau von $\mathcal{S}$ sieht also wie folgt aus: $S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_\omega \subset S_{\omega+1} \subset S_{\omega+2} \subset \ldots$. Wobei S_ω die kleinste Limesstufe ist. Weiter gilt dann auch, dass $S_{\omega+n+1} = \mathcal{P}(S_{\omega+n})$.

Nun stellt sich aber die Frage, wie es weiter geht. Ist $S_{\omega+\omega} \coloneqq \{x : x \in S_{\omega+n}$ für ein $n)\}$ eine Menge? Seien nun also $(\mathcal{S}, \in)$ und $(\mathcal{S}', \in)$ zwei Modelle der vier Axiome mit den Stufen $(S_\alpha)_{\alpha<\kappa}$, $(S'_\alpha)_{\alpha<\lambda}$. Es lässt sich einsehen, dass $\kappa, \lambda \geq \omega + \omega$ gilt und, dass $S_n = S'_n = \mathrm{HF}_n$ für endliche n gelten muss.

1.3 Relationen und Funktionen

Sei (a, b) ein geordnetes Paar. Es ist bekannt, dass wenn $(a, b) = (a', b')$ gilt, auch $a = a'$ und $b = b'$ gelten muss.

Definition 1.19 (Geordnete Paare)
Seien a, b Mengen. Nun wird das geordnete Paar $(a, b) \coloneqq \{\{a\}, \{a, b\}\}$ definiert. Für Klassen A, B gilt $A \times B = \{(a, b) : a \in A, b \in B\}$

Lemma 1.3.1*:* Wenn $\{a, b\} = \{a, c\}$ gilt, muss $b = c$ folgen.

Beweis. $b \in \{a, b\} = \{a, c\}$. Also $b = a$ oder $b = c$. Wenn $b \neq c$, dann $b = a$ und $c \in \{a, c\} = \{a, b\} = \{a\}$. Also $c = a = b$. Widerspruch! □

Lemma 1.3.2*:* Wenn $(a, b) = (c, d)$ muss $a = c$ und $b = d$ folgen.

Beweis. $\{a\} \in \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, das heißt $\{a\} = \{c\}$ oder $\{a\} = \{c, d\}$. In beiden Fällen gilt aber $a = c$ und $\{a\} = \{c\}$. Nach Lemma 1.3.1 gilt wegen $\{a, b\} = \{c, d\}$ und $a = c$ auch $b = d$. □

Weiter lässt sich $\langle A, B\rangle \coloneqq (\{[0] \times A\}) \cup (\{[1]\} \times B)$ definieren.
Für Mengen $a_0, \ldots, a_n$ seien Tupel beliebiger Länge definiert als

$$\begin{aligned} () &\coloneqq \emptyset, \\ (a_0) &\coloneqq a_0 \text{ und} \\ (a_0, \ldots, a_n) &\coloneqq ((a_0, \ldots, a_{n-1}), a_n). \end{aligned}$$

Um diese einfacher definieren zu können bestimmen wir zudem

$$\begin{aligned} A^0 &\coloneqq \{()\}, \\ A^1 &\coloneqq A \text{ und} \\ A^{n+1} &\coloneqq A^n \times A. \end{aligned}$$

Nun ist eine n-stellige Relation eine Klasse $R \subseteq \mathcal{S}^n$. Wenn $R \subseteq A^n$ für eine Klasse A ist, dann sagen wir zu R, dass sie eine n-stellige Relation über A ist.

Definition 1.20 (Binäre Relation)
Eine *binäre Relation* R ist eine Relation, mit $R \subseteq A^2$.

Weiter ist $\mathrm{Def}(R) \coloneqq \{a : (a, b) \in R \text{ für ein } b\}$ und $\mathrm{Bild}(R) \coloneqq \{b : (a, b) \in R \text{ für ein } a\}$. Offensichtlich gilt $R \subseteq \mathrm{Def}(R) \times \mathrm{Bild}(R)$.

Definition 1.21 (Funktionale Relationen)
Eine binäre Relation ist funktional, wenn für alle $a \in \mathrm{Def}(R)$ genau ein $b \in \mathrm{Bild}(R)$ existiert so, dass $(a, b) \in R$. Die zugehörige Notation ist dann $R(a)$, wobei $R = \{(a, R(a)) : a \in \mathrm{Def}(R)\}$.

Definition 1.22 (Partielle und Totale Funktionen)
Eine *partielle Funktion* von A nach B ist eine funktionale Relation $F \subseteq A \times B$.
Eine *totale Funktion* von A nach B dagegen ist eine funktionale Relation $F \subseteq A \times B$ für die zusätzlich gilt, dass $\mathrm{Def}(F) = A$ und $\mathrm{Bild}(F) \subseteq B$. Die Notation hierfür ist dann $F : A \to B$.

Für eine Menge a und eine Klasse B schreibt man B^a für die Klasse aller Funktionen $f : a \to B$. Die Einschränkung einer Funktion $F : A \to B$ auf eine Teilklasse $C \subseteq A$ ist

$$F \upharpoonright C := F \cap (C \times B).$$

Das Bild von C unter F ist $F[C] := \mathrm{Bild}(F \upharpoonright C)$.

Die bereits bekannten Begriffe *injektiv*, *surjektiv* und *bijektiv* sind wie üblich definiert.

Lemma 1.3.3*:* Seien $A \subseteq B \subseteq C$ Mengen. Wenn eine injektive Funktion $f : C \to A$ existiert, dann gibt es auch eine injektive Funktion $g : C \to B$.

Beweis. Sei $Z := \bigcap\{X \subseteq C : C \setminus B \subseteq X, f[X] \subseteq X\}$. Es gilt $C \setminus B \subseteq Z$ und also $C \setminus Z \subseteq B$, $C \setminus Z = B \setminus Z$.
Weiter ist $f[Z] \subseteq Z$. Daraus folgt die Behauptung, dass die Funktion $g(x)$ mit

$$g(x) := \begin{cases} f(x) & \text{für } x \in Z \\ \mathrm{id} & \text{für } x \in C \setminus Z \end{cases}$$

eine bijektive Funktion von C nach B ist. Es gilt $g \upharpoonright Z = f \upharpoonright Z$ ist injektiv und $g[Z] \subseteq Z \cap B$ und $g \upharpoonright C \setminus Z = id_{C \setminus Z}$ ist bijektiv und $g[C \setminus Z] \subseteq B$.

Es bleibt zu zeigen, dass $g[Z] = f[Z] = Z \cap B$, denn dann ist $g[C] = g[Z] \cup g[C \setminus Z] = (Z \cap B) \cup B \setminus Z = B$, da $C \setminus Z = B \setminus Z$ und $g[C \setminus Z] = C \setminus Z$.

Angenommen es gibt $a \in (Z \cap B) \setminus f[Z]$. Da $a \in B$ gilt für $X := Z \setminus \{a\}$

- $C \setminus B \subseteq X$ (da $C \setminus B \subseteq Z$, $a \in B$)
- $f[X] \subseteq X$ (da $f[X] = f[Z \setminus \{a\}] \subseteq f[Z] \subseteq Z \setminus \{a\} = X$)

Also müsste $Z \subseteq X$ gelten. Widerspruch! □

Satz 1.11 (Cantor-Schröder-Bernstein)
Wenn es eine injektive Funktion $f : A \to B$ und eine andere injektive Funktion $g : B \to A$ existiert, dann gibt es auch eine bijektive Funktion $h : A \to B$.

Beweis. Die Funktion $g \circ f : A \to g[f[A]]$ ist bijektiv. Nach dem Lemma 1.3.3 muss dann auch eine weitere bijektive Funktion $p : A \to g[B]$ existieren. Der Zusammenhang lässt sich einfach in Abbildung 2 erkennen.

Nun ist $g^{-1} \upharpoonright g[B] : g[B] \to B$ ebenfalls bijektiv. Es lässt sich dann $h := g^{-1} \circ p : A \to B$ als bijektive Funktion von A nach B definieren. □

1.4 Ordinalzahlen

Es wurden bereits die Zahlen $0, 1, 2, \ldots, n, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega$ diskutiert, welche so genannte Ordinale darstellen. Mit diesen soll sich in diesem Kapitel genauer befasst werden.

Definition 1.23 (Graph)
Ein *Graph* ist ein Paar (A, R) so, dass $R \subseteq A \times A$ ein binäre Relation ist.

Definition 1.24 (Partielle Ordnungen)
Eine *partielle Ordnung* ist ein Graph $(A, <)$ so, dass $<$ irreflexiv und transitiv ist. Eine alternative Definition ist $(A, \leq)$, wobei $\leq$ reflexiv, transitiv und antisymmetrisch ist.

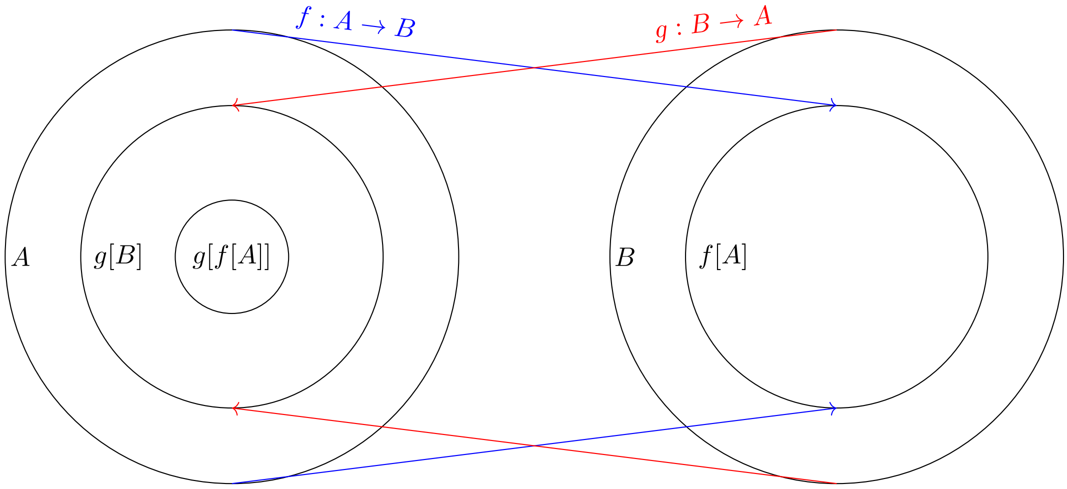

Abbildung 2: Grafik des Sachverhalts im Satz 1.11

Eine *lineare Ordnung* $(A, <)$ ist eine partielle Ordnung so, dass für alle $a, b \in A$ entweder $a < b$, $a = b$ oder $b < a$ gilt.

Ein Graph (A, R) ist *fundiert*, wenn jede nicht-leere Teilmenge $B \subseteq A$ ein Element $b \in B$ enthält so, dass $\{a \in B : (a, b) \in R\} = \emptyset$. Also: Eine partielle Ordnung ist fundiert, wenn jede nicht-leere Teilmenge $B \subseteq A$ ein $<$-minimales Element enthält.

Definition 1.25 (Wohlordnungen)
Eine *Wohlordnung* $(A, <)$ ist eine fundierte lineare Ordnung so, dass für jedes $a \in A$ die Klasse $\downarrow a \coloneqq \{b \in A : b < a\}$ eine Menge ist.

Definition 1.26 (Mengenähnlichkeit)
Eine Relation $R \subseteq A \times A$, bei der für ein beliebiges b die Klasse $\{a \in A : (a, b) \in R\}$ eine Menge ist wird auch als mengenähnlich bezeichnet.

Lemma 1.4.1*:* Sei $(A, <)$ eine fundierte, mengenähnliche, partielle Ordnung. Dann existiert in A keine unendliche absteigende Folge $(a_n)_{n\in\omega}$ mit $a_{n+1} < a_n$ für alle n, wobei ω die Menge der natürlichen Zahlen bezeichnet.

Bemerkung: $(a_n)_{n\in\omega}$, $f : \omega \to A$ mit $a_n \coloneqq f(n)$

Beweis. Wenn eine solche Folge existiert, dann ist $\{a_n : n \in \omega\} = f[\omega] \subseteq A$ eine nicht-leere Klasse ohne $<$-minimales Element. Da $f[w] \subseteq \{a_0\} \cup \downarrow a$ und A mengenähnlich ist, ist $f[w]$ eine Menge. Dies ist aber ein Widerspruch zur Fundiertheit. $\square$

Um zu zeigen, dass jedes Element einer fundierten, mengenähnlichen partiellen Ordnung $(A, <)$ eine Eigenschaft ψ erfüllt zeigt man, dass für jedes a, dass wenn ψ für alle $b < a$ gilt, dann auch für a.

Satz 1.12 (Induktionsprinzip)
Sei $(A, <)$ eine fundierte, mengenähnliche partielle Ordnung. Dann gilt

a) Jede nicht-leere Teilklasse hat ein $<$-minimales Element.

b) Sei $X \subseteq A$ so, dass für alle $a \in A$ gilt: Wenn $\downarrow a \subseteq X$, dann ist $a \in X$. Es folgt, dass $X = A$.

Beweis. a) Sei $B \subseteq A$, $a \in B$. Wegen der Mengenähnlichkeit ist $\downarrow a$ eine Menge und aus dem Aussonderungsaxiom folgt, dass auch $X := B \cap (\downarrow a \cup \{a\})$ eine nicht-leere Teil*menge* von A ist. Es folgt auch, dass X ein minimales Element b besitzt.

Behauptung: b ist auch das $<$-minimale Element von B. Andernfalls gibt es ein $c \in B$ mit $c < b \leq a$. Da $b \in X \subseteq B$ würde aber auch $c \in X$ folgen. Widerspruch!

b) Annahme: X sei wie gefordert, aber $X \neq A$. Also existiert ein $a \in A \setminus X$. Definiere $B :=\downarrow a \cup \{a\} \setminus \{X\}$. Dies ist eine nicht-leere Teilmenge und hat daher ein minimales Element b. Also ist $\downarrow b \subseteq A \setminus B \subseteq X$ und daher ist $b \in X$. Widerspruch!

□

Definition 1.27 (Ordinalzahlen)
Eine *Ordinalzahl* ist eine transitive Menge, welche durch $\in$ linear geordnet ist. Beispiele sind $[n]$ für beliebige n, ω, $\omega \cup \{\omega\}$. Die Klasse aller Ordinalzahlen ist On

Lemma 1.4.2*:* Ordinalzahlen sind wohlgeordnet durch $\in$.

Beweis. Sei $\beta \subseteq \alpha \in \mathrm{On}$ und $\beta \neq \emptyset$. Da β fundiert ist, existiert ein $\gamma \in \beta$ mit $\gamma \cap \beta = \emptyset$. Also ist γ kleinstes Element in β bezüglich. $\in$ □

Definition 1.28 (Anfangsstück)
Ein *Anfangsstück* einer Ordnung $(A, <)$ ist eine Teilmenge $I \subseteq A$ so, dass, wenn $a \in I$ und $b < a$, auch $b \in I$ ist.

Ein Anfangsstück von $\alpha \in \mathrm{On}$ ist also eine Teilmenge $\beta \subseteq \alpha$ so, dass $\delta \in \gamma \in \beta \Rightarrow \delta \in \beta$, also eine transitive Teilmenge von α.

Lemma 1.4.3*:* Sei $\alpha \in \mathrm{On}$. β ist ein echtes Anfangsstück von α, genau dann wen $\beta \in \alpha$

Beweis. $\Rightarrow$: Sei γ das kleinste Element von $\alpha \setminus \beta$. Es gilt $\beta = \gamma \in \alpha$, da für beliebige δ gilt, dass $\delta \in \gamma \Leftrightarrow (\delta \in \alpha \wedge \delta \notin \alpha \setminus \beta) \Leftrightarrow \delta \in \beta$

$\Leftarrow$: Sei $\beta \in \alpha$ und $\delta \in \gamma \in \beta$. Es gilt $\delta \in \beta$, da sonst $\delta = \beta$ oder $\beta \in \delta$. Widerspruch!

□

Satz 1.13 a) $(\mathrm{On}, \in)$ ist ein Wohlordnung

b) Wenn $\alpha \in \mathrm{On}$, dann ist $\alpha = \{\beta \in \mathrm{On} : \beta \in \alpha\} =\downarrow a$

c) On ist eine echte Klasse

Beweis. a) Zu zeigen ist, dass $\in$ eine lineare Ordnung ist. $\alpha \notin \alpha$ und $\alpha \in \beta, \beta \in \gamma \Rightarrow \alpha \in \gamma$ folgt direkt aus der Definition der Ordinalzahlen.

Seien nun $\alpha, \beta \in \mathrm{On}, \alpha \neq \beta$. Nun ist $x \in \alpha \cap \beta$ ein Anfangsstück von α und β. Aus $y \in z \in \alpha \cap \beta$ folgt wegen der Transitivität $y \in \alpha \cap \beta$. Nun muss $x = \alpha$ oder $x = \beta$ gelten. Sonst ist $x \in \alpha$ und $x \in \beta$, also $\alpha \cap \beta \in \alpha \cap \beta$. Widerspruch!

Wenn $x \in \alpha$, dann ist $x \in \beta$, also $\alpha \in \beta$, oder umgekehrt.

b) Dies folgt direkt aus *a)*

c) Wäre On eine Menge, wäre sie eine transitive, durch $\in$ linear geordnete Menge und müsste sich dadurch selbst enthalten. Widerspruch!

$\square$

Definition 1.29 (Nachfolgerordinal)
Für $\alpha \in \mathrm{On}$ ist $\alpha + 1 := \alpha \cup \{\alpha\}$ das *Nachfolgerordinal* von α.

Definition 1.30 (Limesordinal)
$\alpha \in \mathrm{On}$ ist ein *Limesordinal*, wenn $\alpha \neq \emptyset$ und α kein Nachfolgerordinal ist.

Da $(\mathrm{On}, \in)$, bzw. $(\mathrm{On}, <)$, eine Wohlordnung ist, existiert die transfinite Induktion über On. Das heißt: für jede Teilklasse $X \subseteq \mathrm{On}$ gilt: wenn für alle $\alpha \in \mathrm{On}$ gilt, dass für jedes $\beta < \alpha$ aus $\beta \in X$ folgt, dass $\alpha \in X$, dann ist $X = \mathrm{On}$.

Um zu zeigen, dass irgendeine Eigenschaft $\varphi(x)$ auf alle Ordinale zutrifft, also $X := \{\alpha \in \mathrm{On} : \varphi(x)\} = \mathrm{On}$ gibt es folgende Strategien.

1. Zeige, dass $\varphi(0)$ gilt. Zeige, dass wenn $\varphi(\alpha)$ auch $\varphi(\alpha+1)$ ist. Zeige für jedes Limesordinal λ, dass $\varphi(\lambda)$ gilt, wenn für alle $\alpha < \lambda$ auch $\varphi(\alpha)$ korrekt ist.

2. Betrachte eine beliebige Ordinalzahl α und nimm an, dass $\varphi(\beta)$ für alle $\beta < \alpha$ gilt. Zeige, dass dann $\varphi(\alpha)$ folgt.

1.4.1 Ordinale und Stufen

Zur Erinnerung: für jede Menge a ist $S(a)$ die kleinste Stufe mit $a \subseteq S(a)$ und aus $a \in b$ folgt $S(a) \in S(b)$.

Letzteres gilt natürlich auch für Ordinalzahlen. Wir wollen nun aber auch die Umkehrung betrachten. Wenn $\alpha \notin \beta$ ist, dann folgt $\alpha = \beta$ oder $\beta \in \alpha$, also $S(\alpha) = S(\beta)$ oder $S(\beta) \in S(\alpha)$. In beiden Fällen gilt $S(\alpha) \notin S(\beta)$. Es gilt also auch die Rückrichtung: $\alpha \in \beta \Leftrightarrow S(\alpha) \in S(\beta)$.

Satz 1.14
Die Funktion $F : \mathrm{On} \to H(\mathcal{S}), F(\alpha) := S(\alpha)$ ist ein Isomorphismus zwischen On und $H(\mathcal{S})$. Das heißt F ist bijektiv und $\beta < \alpha \Leftrightarrow F(\beta) \in F(\alpha)$.

Bemerkung: Mit $H(\mathcal{S})$ wird die Klasse aller Stufen, die Mengen sind, also aller Stufen außer $\mathcal{S}$ bezeichnet.

Beweis. Es ist bereits bekannt, dass F injektiv und ein starker Homomorphismus ist. Es bleibt die Surjektivität zu beweisen. Wenn dies nicht der Fall wäre, dann existiert eine minimale Stufe $S \in \mathcal{S}$ mit $S \notin \mathrm{Bild}(F)$.

Sei $X := \{\beta \in \mathrm{On} : S(\beta) \in S\}$. X ist ein echtes Anfangsstück von On, das heißt es gibt $\alpha \in \mathrm{On}$ so, dass $X = \downarrow \alpha = \alpha$. Demnach betrachten wir nun $S(\alpha)$ und wie sich dies zu S verhält.

- $S(\alpha) \in S$, dann ist $\alpha \in X = \alpha$. Widerspruch!

- $S(\alpha) = S$, dann ist $S \in \mathrm{Bild}(F)$. Widerspruch!

- $S \in S(\alpha)$, dann ist $S(\alpha)$ die kleinste Stufe so, dass $\alpha \subseteq S(\alpha)$, sodass $\beta \in S(\alpha)$ für alle $\beta \in \alpha$ gilt. Da aber $\beta \in S(\beta) \in S$ für alle $\beta \in \alpha$ ist, folgt $S(\alpha) \subseteq S$. Widerspruch!

$\square$

Definition 1.31
Für $\alpha \in \mathrm{On}$, setze $S_\alpha := S(\alpha)$. Dies sind dann die *Indizes der kumulativen Hierarchie.*

Es folgt, dass $S_0 \subset S_1 \subset \cdots \subset S_\omega \subset \cdots \subset S_\alpha \subset S_{\alpha+1} \subset \ldots$, $H(\mathcal{S}) = \{S_\alpha : \alpha \in \text{On}\}$ und $\mathcal{S} = \bigcup\{S_\alpha : \alpha \in \text{On}\}$.

Definition 1.32 (Rang einer Menge)
Der *Rang* einer Menge a ist das Ordinal $\rho(a) = \alpha$ mit $S(a) = S_\alpha$.

Für Ordinale α gilt $\rho(\alpha) = \alpha$. Eine Klasse X ist eine Menge genau dann, wenn $\{\rho(x) : x \in X\}$ durch eine Ordinalzahl beschränkt ist.

1.4.2 Der Rekursionssatz

Sei A eine Klasse und definiere $A^\infty \coloneqq \{f : f : \alpha \to A, \text{Fkt. für ein } \alpha \in \text{On}\}$. Dies lässt sich in Worten formulieren, als die Menge aller Folgen, welche in ihrer Länge durch ein Ordinal beschränkt sind.
Sei G nun eine partielle Funktion $G : \mathcal{S}^\infty \to \mathcal{S}$.

Lemma 1.4.4*:* Es gibt höchstens eine Funktion $f : \alpha \to \mathcal{S}$ so, dass f eine Menge ist und $f(\beta) = G(f \restriction \beta)$ für alle $\beta < \alpha$.

Bsp.: $f(17) = G(f \restriction \{0, \ldots, 16\})$.

Beweis. Nehmen wir an, dass f und f' die geforderte Eigenschaft erfüllen. Sei $X = \{\beta \in \alpha : f(\beta) = f'(\beta)\}$. Wenn $\beta < \alpha$ und $\beta \subseteq X$, dann $f \restriction \beta = f' \restriction \beta$, also $f(\beta) = G(f \restriction \beta) = G(f' \restriction \beta) = f'(\beta)$, also $\beta \in X$. Es folgt $X = \alpha$ und $f = f'$. □

Nun ist das Ziel zu zeigen, dass jede totale Funktion $G : \mathcal{S}^\infty \to \mathcal{S}$ auf eindeutige Weise eine Funktion $F : \text{On} \to \mathcal{S}$ definiert.
Für die Existenz wird aber ein zusätzliches Axiom benötigt:
Ersetzungsaxiom: Wenn $F : A \to S$ eine Funktion ist und $a \subseteq A$ eine Menge ist, dann ist auch $F[a]$ eine Menge. Oder in anderen Worten: Wenn F eine Funktion ist und $\text{Def}(F)$ eine Menge ist, dann ist auch $\text{Bild}(F)$ eine Menge.

Satz 1.15 (Rekursionssatz)
Zu jeder Funktion $G : \mathcal{S}^\infty \to \mathcal{S}$ gibt es genau eine Funktion $F : \text{On} \to \mathcal{S}$ so, dass $F(\alpha) = G(F \restriction \alpha)$ für alle $\alpha \in \text{On}$.

Beweis. Sei $\alpha \in \text{On}$. Wir wissen dass es höchstens eine Funktion $f_\alpha : \alpha \to \mathcal{S}$ mit $f_\alpha(\beta) = G(f\alpha \restriction \beta)$ für alle $\beta < \alpha$ gibt.
Die Existenz solch einer Funktion f_α soll nun per Induktion nach α geschehen so, dass für alle $\beta < \alpha$ gilt, dass $f_\beta = f_\alpha \restriction \beta$.

- $\alpha = 0$: Dann ist $f_\alpha = \emptyset$, die Bedingung gilt also.
- $\alpha + 1$: Dann lässt sich $f_{\alpha+1}$ als $f_{\alpha+1} \coloneqq f_\alpha \cup \{(\alpha, F(f_\alpha))\}$ definieren.
- α Limesordinal: Setze $X \coloneqq \{f_\beta : \beta < \alpha\}$. X ist eine Menge, denn X ist das Bild der Funktion $H : \alpha \to \mathcal{S}^\infty$ mit $H(\beta) = f_\beta$ für $\beta \in \alpha$.
  Nun ist $f_\alpha \coloneqq \bigcup X = \{(\gamma, f_\beta(\gamma), \gamma < \beta < \alpha)\}$. f_α ist tatsächlich eine Funktion von α nach $\mathcal{S}$: Für alle $\gamma < \alpha$ existiert ein β mit $\gamma < \beta < \alpha$ und damit ein Paar $(\gamma, f_\beta(\gamma)) \in f_\alpha$. Für $(\gamma, f_\beta(\gamma)), (\gamma, f_{\beta'}(\gamma)) \in f_\alpha$ so, dass $\beta < \beta'$ ist $f_\beta = f_{\beta'} \restriction \beta$, also $f_\beta(\gamma) = f_{\gamma'}(\gamma)$. Es folgt also $\text{Def}(f_\alpha) = \alpha$.

Setze $F = \bigcup\{f_\alpha : \alpha \to \mathcal{S} : \alpha \in \mathrm{On}\} = \{(\beta, f_\alpha(\beta)) : \beta < \alpha \in \mathrm{On}\}$, F ist eine Funktion mit $\mathrm{Def}(F) = \mathrm{On}$.
Für jedes $\beta \in \mathrm{On}$ ist $F(\beta) = f_\alpha(\beta)$ für ein (und damit alle!) α mit $\beta < \alpha$.
$F \restriction \beta = f_\alpha \restriction \beta$ für $\beta < \alpha$, $F(\beta) = f_\alpha(\beta) = G(f_\alpha \restriction \beta) = G(F \restriction \beta)$. $\square$

Damit ist der Rekursionssatz bewiesen. Nun sollen Anwendungen von diesem gezeigt werden.

Konstruktion von $F : \mathrm{On} \to A$: Sei $a \in A, s : A \to A, h : \mathcal{P}(A) \to A$. Nun lässt sich $G : A^\infty \to A$ definieren durch:

$$\begin{aligned} &G(\emptyset) := a, \\ &G(F \restriction \alpha + 1) := s(F(\alpha)), \\ &G(F \restriction \lambda) := h(F[\lambda]) \end{aligned}$$

für ein Limesordinal λ und Nachfolgerordinal α.
Mit dem Rekursionssatz folgt die Existenz und Eindeutigkeit der Funktion $F : \mathrm{On} \to A$ mit $F(\alpha) = G(F \restriction \alpha)$. Es gilt

$$\begin{aligned} &F(\emptyset) = a, \\ &F(\alpha + 1) = s(F(\alpha)), \\ &F(\lambda) = h(F[\lambda]). \end{aligned}$$

Addition von Ordinalzahlen: Es sollen nun Ausdrücke wie $\alpha + \beta$ definiert werden, für $\alpha, \beta \in \mathrm{On}$. $\alpha + \beta := F_\alpha : \mathrm{On} \to \mathrm{On}, \beta \mapsto \alpha + \beta$. Genauer lässt sich rekursiv definieren, dass

$$\begin{aligned} &\alpha + 0 := \alpha, \\ &\alpha + (\beta + 1) := (\alpha + \beta) + 1, \\ &\alpha + \lambda := \sup\{\alpha + \beta : \beta < \lambda\} \end{aligned}$$

für ein Limesordinal λ.
Bemerkung: Addition ist nicht kommutativ! Dies lässt sich leicht an einem Beispiel erkennen: $\omega + 1 = \omega \cup \{\omega\} \neq \omega$, aber $1 + \omega = \sup\{1 + n : n \in \omega\} = \omega$.

Eine andere interessante Beobachtung ist, dass sich Addition zweier Ordinalzahlen durch „Hintereinanderlegen“ zweier Wohlordnungen darstellen lässt. Für $\alpha + \beta$ lassen sich Strukturen $\mathfrak{A} = (A, <), \mathfrak{B} = (B, <)$ finden, wobei beide Strukturen Wohlordnungen sind. Das „Hintereinanderlegen“ lässt sich in Abbildung 3 erkennen. Da $\mathfrak{A}$ und $\mathfrak{B}$ beides Wohlordnungen sind, lässt sich leicht einsehen, dass dann auch $\mathfrak{A} + \mathfrak{B}$ eine Wohlordnung ist.

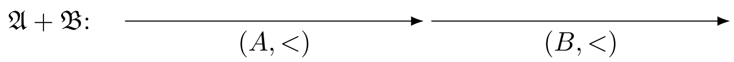

Abbildung 3: Darstellung von Addition durch „Hintereinanderlegen“ von Wohlordnungen

Multiplikation von Ordinalzahlen: Analog zur Addition kann man auch die Multiplikation definieren. Für $\alpha, \beta \in \mathrm{On}$ ist dafür definiert:

$$\begin{aligned} &\alpha \cdot 0 := 0 \\ &\alpha \cdot (\beta + 1) := \alpha \cdot \beta + \alpha \\ &\alpha \cdot \lambda := \sup\{\alpha \cdot \beta : \beta < \lambda\} \end{aligned}$$

für ein Limesordinal λ.

Und ebenso, wie Addition durch Wohlordnungen darstellbar ist, lässt sich Multiplikation mithilfe von zwei Wohlordnungen $\mathfrak{A} = (A, <)$ und $\mathfrak{B} = (B, <)$ bilden. Dabei gilt $\mathfrak{A} \cdot \mathfrak{B} := \mathfrak{C} = (A \times B, <_C)$ mit $(a, b) <_C (a', b')$ genau dann, wenn $b < b'$ oder $b = b' \wedge a < a'$. Graphisch dargestellt ist dies in Abbildung 4.

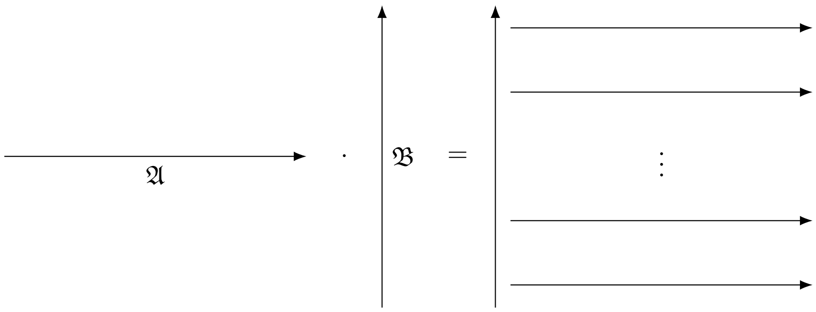

Abbildung 4: Graphische Darstellung von Multiplikation mithilfe von Wohlordnungen

Auch hier lässt es sich wieder feststellen, dass Multiplikation nicht kommutativ ist. Ein Beispiel hierfür ist $\omega \cdot 2 = \omega \cdot (1+1) = \omega + \omega = \sup\{\omega + n : n \in \omega\} > \omega + n$ für alle $n \in \omega$, aber $2 \cdot \omega = \sup\{2 \cdot n : n < \omega\} = \omega < \omega + 1$.

Also gilt im Allgemeinen auch **nicht** $(\alpha + \alpha') \cdot \beta = \alpha\beta + \alpha'\beta$, da beispielsweise $(1+1) \cdot \omega = 2 \cdot \omega = \omega \neq \omega + \omega = 1 \cdot \omega + 1 \cdot \omega$.

Potenzen von Ordinalzahlen: Zuletzt wird nun noch das Potenzieren von Ordinalzahlen definiert. Für $\alpha, \beta, \lambda \in \mathrm{On}$, α, β Nachfolgerordinale und λ ein Limesordinal sein nun definiert:

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

Satz 1.16 (Cantor-Normalform)
Jedes $\alpha \in \mathrm{On}$ hat eine eindeutige Darstellung $\alpha = \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k$ mit $k \in \omega, n_1, \ldots, n_k \in \omega \setminus \{0\}$ und $\alpha \geq \beta_1 > \beta_2 > \cdots > \beta_k \geq 0$.

Beweis. Dies soll per Induktion gezeigt werden. Für $\alpha = 0$ ist dies trivial, da dies die einzige Darstellung der 0 ist. Sei unsere Induktionsvoraussetzung nun also, dass alle Ordinale, die kleiner als α sind eine eindeutige Cantor-NF besitzen.
Sei γ das kleinste Ordinal so, dass $\omega^\gamma > \alpha$. γ muss ein Nachfolger sein, denn wäre es ein Limesordinal, dann wäre γ nicht das kleinste Ordinal mit der geforderten Eigenschaft.
Also ist $\gamma = \beta + 1$ und β ist das größte Ordinal mit $\omega^\beta \leq \alpha$. Also existieren Ordinale $n < \omega$ und γ so, dass $\alpha = \omega^\beta \cdot n + \gamma, \gamma < \omega^\beta \leq \alpha$.

Nach der Induktionsvoraussetzung hat γ eine eindeutige Cantor-Normalform und damit auch α. $\square$

Es lässt sich jedoch feststellen, dass die Cantor-NF nicht immer hilfreich ist. Sei beispielsweise $\omega_1 = \min\{\alpha \in \mathrm{On} : \text{ es gibt keine injektive Abb. } f : \alpha \to \omega\}$ das kleinste nicht abzählbare

Ordinal. Gesucht sei nun die Cantor-Normalform von ω_1.
$\omega_1 = \sup\{\alpha \in \mathrm{On} : \alpha \text{ ist abzählbar}\}$ ist ein Limesordinal. Betrachte nun $\omega^{\omega_1} = \sup\{\omega^\alpha : \alpha \text{ ist abzählbar}\}$. Es lässt sich feststellen, dass $\omega^{\omega_1} \leq \omega_1 \leq \omega^{\omega_1}$, also muss $\omega_1 = \omega^{\omega_1}$ sein.

Die Cantor-NF von ω_1 ist also ω^{ω_1}, was offensichtlicherweise nicht sonderlich hilfreich ist.

Satz 1.17 (Ordinale Normalform für Wohlordnungen)
Jede Wohlordnung $(a, <)$ über einer Menge a ist isomorph zu genau einer Ordinalzahl.

Beweis. Zu einer gegebenen Wohlordnung $(a, <)$ suchen wir ein $\alpha \in \mathrm{On}$ und eine bijektive Abbildung $f : \alpha \to a$ so, dass für $\gamma < \beta < \alpha$ auch $f(\gamma) < f(\beta)$ ist.

Definiere $F : \mathrm{On} \to a \cup \{a\}$ durch

$$F(\alpha) \coloneqq \begin{cases} \min\{a \setminus F[\alpha]\} & \text{wenn } F[\alpha] \subsetneq a \\ a & \text{sonst} \end{cases}$$

Behauptung: $a \in \mathrm{Bild}(F)$. Andernfalls wäre F eine injektive Abbildung von On nach a, dann wäre für $\beta < \alpha$ aber entweder $F(\alpha) \notin F[\alpha]$ oder $F(\beta) \in F[\alpha]$, also $F(a) \neq F(b)$. Das heißt, dass $F : \mathrm{On} \to \mathrm{Bild}(F)$ bijektiv ist und da $\mathrm{Bild}(F) \subseteq a$ eine Menge ist, müsste $F^{-1}[\mathrm{Bild}(F)] = \mathrm{On}$ nach dem Ersetzungsaxiom eine Menge sein. Widerspruch!

Sei α also die kleinste Ordinalzahl so, dass $F(\alpha) = a$. Dann ist $f = F \upharpoonright \alpha$ die gesuchte Bijektion:

- f ist Ordnungserhaltend und damit auch injektiv, da für $\gamma < \beta < \alpha$ folgt, dass $f[\gamma] \subsetneq f[\beta]$, da $f(\gamma) = \min\{a \setminus f[\gamma]\} < \min\{a \setminus f[\beta]\} = f(\beta)$.
- f ist surjektiv, da sonst ein kleinstes Element $b \in a \setminus f[\alpha]$ existieren würde. Dann wäre $F(\alpha) = b$ im Widerspruch zu $F(\alpha) = a$.

□

1.5 Das Auswahlaxiom (AC)

Definition 1.33 (Auswahlfunktionen)
Eine *Auswahlfunktion* auf einer Menge x ist eine Funktion $f : x \to \mathcal{S}$ so, dass $f(z) \in z$ für jedes nicht-leere $z \in x$.

Das Auswahlaxiom (AC) besagt, dass auf jeder Menge eine solche Auswahlfunktion existiert.

Es lässt sich sehen, dass wenn auf $\bigcup X$ eine Wohlordnung existiert, man eine Auswahlfunktion bilden kann, ohne das Auswahlaxiom nutzen zu müssen. Sei $z \in X, z \neq \emptyset$. Dann ist $f(z) = \min(z)$ eine Auswahlfunktion.

Dies ist die eine Richtung des Wohlordnungssatzes von Zermelo, welches auch aus dem AC folgt. Die andere Richtung soll nun ebenfalls gezeigt werden.

Satz 1.18 (Wohlordnungssatz von Zermelo)
Auf jeder Menge a existiert eine Wohlordnung.

Beweis. Aus einer Auswahlfunktion f auf $\mathcal{P}(a)$ können wir eine Wohlordnung auf a konstruieren. Sei $F : \mathrm{On} \to a \cup \{a\}$ mit

$$F(\alpha) = \begin{cases} f(a \setminus F[\alpha]) & \text{wenn } F[\alpha] \subsetneqq a \\ a & \text{sonst} \end{cases}$$

Wie im letzten Beweis gezeigt gibt es ein $\alpha \in \mathrm{On}$ mit $F(\alpha) = a$ und $F \restriction \alpha : \alpha \to a$ bijektiv. $F \restriction \alpha$ ist surjektiv, denn sonst ist $F(\alpha) \neq a$ und $F \restriction \alpha$ überträgt de Wohlordnung von α auf a.

Für $y, z \in a$ setze $y <_a z$ genau dann, wenn $(F \restriction \alpha)^{-1}(y) < (F \restriction \alpha)^{-1}(z)$. □

Ein weiteres, zum Auswahlaxiom äquivalentes Axiom ist das Lemma von Zorn (Kuratowski).

Definition 1.34 (Lemma von Zorn (Kuratowksi))
Wenn $(a, <)$ eine partielle Ordnung auf einer Menge a ist, in der jede linear geordnete Teilmenge $b \subseteq a$ eine obere Schranke $s_b \in a$ hat, dann besitzt die Menge ein maximales (bemerke: nicht größtes) Element m_a.

Satz 1.19
Aus den Axiomen von ZF und dem Auswahlaxiom lässt sich das Lemma von Zorn folgern.

Beweis. Sei f eine Auswahlfunktion auf $\mathcal{P}(a)$. Für jede Teilmenge $b \subseteq a$, welche durch $<$ linear geordnet ist, setze $y_b := \{x \in a : \forall u(u \in b \to u < x)\}$ als die Menge der *echten* oberen Schranken von b.

Definiere nun $F : \mathcal{P}(a) \to a \cup \{a\}$ durch

$$F(b) := \begin{cases} f(y_b) & \text{wenn } b \text{ durch } < \text{ linear geordnet ist und } y_b \neq \emptyset \\ a & \text{sonst} \end{cases}$$

Mithilfe des Rekursionssatzes lässt sich dann eine Funktion $G : \mathrm{On} \to a \cup \{a\}$ mit $\alpha \mapsto F(G[\alpha]) = F(\mathrm{Bild}(G \restriction \alpha))$ definieren.

$G[\alpha]$ ist eine linear geordnete Teilmenge von a und $G(\alpha)$ ist eine echte obere Schranke für $G[\alpha]$ außer dann, wenn $G[\alpha]$ keine echte obere Schranke besitzt, dann gilt $G(\alpha) = a$.

Wie in vorherigen Beweisen folgt, dass G den Wert a annehmen muss, da sonst G eine ordnungserhaltende Abbildung von On nach a wäre und On eine Menge sein würde.
Sei α also minimal mit $G(\alpha) = a$. $G[\alpha]$ ist nach Konstruktion eine linear geordnete Teilmenge von a ohne *echte* obere Schranke.
Sei m eine obere Schranke (und damit größtes Element) von $G[\alpha]$. Damit ist m maximales Element von (a, y). □

Satz 1.20
Aus den Axiomen von ZF und dem Lemma von Zorn folgt das Auswahlaxiom.

Beweis. Sei x eine beliebige Menge und $a := \{f | f : z \to \bigcup z : z \subseteq x$ und f ist eine Auswahlfunktion auf $z\}$. Es gilt $a \neq \emptyset$, da die leere Funktion in a ist und a ist durch $\subsetneq$ partiell geordnet.

Wir behaupten, dass jede linear geordnete Teilmenge $b \subseteq a$ eine obere Schranke $g_b \in a$ besitzt. Setze $g_b := \bigcup b \subseteq x \times \bigcup x$, so dass $g_b = \{(c, f(c)) : c \in z \subseteq x, f : z \to \bigcup z, f \in b\}$. Wenn $(c, f(c)), (c, f'(c)) \in g_b$ sind, dann ist $f, f' \in b$, aber es gilt $f \subseteq f'$ oder $f' \subseteq f$. Da f, f' Funktionen sind, folgt $f(c) = f'(c)$, g_b ist also eine wohldefinierte Funktion.

Für $c \in \mathrm{Def}(g_b)$ ist $g_b(c) = f(c) \in c$ für ein $f \in b$. Also ist g_b eine Auswahlfunktion, das heißt $g_b \in a$.

Schließlich ist g_b eine obere Schranke für b, also besitzt a nach dem Zornschen Lemma ein maximales Element $f \in a$.

Behauptung: f ist eine Auswahlfunktion auf x. Wenn nicht, dann ist f eine Auswahlfunktion auf einer echten Teilmenge $z \subsetneq x$ und es gibt ein nicht-leeres $y \in x \setminus z$. Für jedes $c \in y$ ist dann $f' := f \cup \{(y, c)\}$ eine Auswahlfunktion auf $z \cup \{y\} \subseteq x$ mit $f \subsetneq f'$. Widerspruch zur Maximalität von f. □

1.5.1 Folgerungen aus dem Auswahlaxiom

Satz 1.21
Jeder Vektorraum hat eine Basis.

Beweis. Sei V ein Vektorraum. Wenn $V = \{0\}$, dann ist $\emptyset$ eine Basis. Sei also $V \neq \{0\}$. Definiere $X \coloneqq \{B \subseteq V : B \text{ ist unabhängig}\}$ (zur Erinnerung: $B \subseteq V$ ist unabhängig, wenn kein Element $v \in B$ sich als endliche Linearkombination von anderen Elementen aus B schreiben lässt).
X ist nicht leer, da für $V \neq \{0\}, v \in V$ die Menge $\{v\}$ linear unabhängig ist.
Weiter folgt, dass $(X, \subsetneq)$ eine partielle Ordnung ist, in der jede Kette $K \subseteq X$ eine obere Schranke, nämlich $\bigcup K$ besitzt. Es gilt $\bigcup K \in X$, denn sonst lässt sich ein $v \in \bigcup K$ als endliche Linearkombination $v = \lambda_1 v_1 + \cdots + \lambda_k v_k$ schreiben. Aber dann existiert ein $B \in K$ mit $v, v_1, \ldots, v_m \in B$.

Nach dem Lemma von Zorn hat X also ein maximales Element $B_{\max}$. $B_{\max}$ ist unabhängig und jedes $v \in V$ lässt sich als Linearkombination $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$ schreiben. Sonst wäre $B_{\max} \bigcup \{v\}$ unabhängig, im Widerspruch zur Maximalität von $B_{\max}$. □

Eine weitere Folgerung des Auswahlaxioms ist der Satz von Banach-Tarski, welcher im folgenden Kapitel genauer betrachtet werden soll.

1.5.2 Der Satz von Banach-Tarski

Informell lässt sich der Satz wie folgt definieren: „Eine Kugel $B \subseteq \mathbb{R}^3$ kann in endlich viele Teile zerlegt werden, die dann via einfacher Isometrien zu zwei disjunkten Kopien von B zusammengesetzt werden können.“

Im Folgenden werden nun einige begriffe definiert:

Definition 1.35 (Isometrie)
Sei $A \subseteq \mathbb{R}^3$. Eine Funktion $\varphi : A \to \mathbb{R}^3$ ist eine *Isometrie*, wenn $\|\varphi(a) - \varphi(b)\| = \|a - b\|$ für alle $a, b \in A$.

Definition 1.36 (Kongruenz)
Zwei Mengen $A, B \subseteq \mathbb{R}^3$ sind *kongruent* ($A \cong B$), wenn eine Isometrie φ auf A existiert mit $\varphi(A) = B$.

Definition 1.37 (Zerlegungsäquivalenz)
A, B sind *Zerlegungsäquivalent* ($A \sim_z B$), wenn $n \in \mathbb{N}$ und Partitionen $A = A_1 \cup \cdots \cup A_n$, $B = B_1 \cup \cdots \cup B_n$ existieren, mit $A_i \cong B_i$ für alle $i \leq n$.

Es bleibt nun zu zeigen, dass $\sim_z$ eine Äquivalenzrelation ist. Reflexivität und Symmetrie ist leicht einsehbar, gezeigt werden muss nun also nur noch die Transitivität.

Sei $A \sim_z B$ und $B \sim_z C$. Es gibt also Partitionen

$$\begin{aligned}
&A = A_1 \cup \cdots \cup A_n, \\
&B = B_1 \cup \cdots \cup B_n \text{ mit} \\
&\varphi_i \text{ so, dass q} A_i \cong B_i, \forall i \leq n
\end{aligned}$$

und

$$\begin{aligned}
&B = B'_1 \cup \cdots \cup B'_m, \\
&C = C_1 \cup \cdots \cup C_m \text{ mit} \\
&\psi_i \text{ so, dass } B'_i \cong C_i, \forall i \leq m
\end{aligned}$$

Setze $B_{ij} \coloneqq B_i \cap B'_j, i \leq n, j \leq m$, wodurch wieder eine Partition von B gebildet wird. Weiter sei $A_{ij} \coloneqq \varphi_i^{-1}(B_{ij})$ und $C_{ij} \coloneqq \psi_j(B_{ij})$.

Dann ist $\psi_j \circ \varphi_i$ eine Isometrie von A_{ij} nach C_{ij} und A_{ij}, C_{ij} bilden Partitionen von A bzw. C, also ist $A \sim_z C$.

Weiter kann man folgende Eigenschaften der Relationen $\sim_z$ feststellen, welche hier aber nicht bewiesen werden sollen:

- Wenn $A \sim_z B$, dann existiert eine Bijektion $g : A \to B$ mit $C \sim_z g(C)$ für alle $C \subseteq A$
- Für Partitionen $A = A_1 \cup \cdots \cup A_n, B = B_1 \cup \cdots \cup B_n$ mit $A_i \sim_z B_i$ folgt $A \sim_z B$.
- Wir definieren $A \leq B :\Leftrightarrow \exists B' \subseteq B : A \sim_z B'$
- Wenn $A \leq B$ und $B \leq A$, dann ist $A \sim_z B$

Ein Vorbereitender Satz für den Satz von Banach-Tarski ist das Hausdorff-Paradoxon. Dieses beschreibt eine Paradoxe Zerlegung der $2-$Sphäre $S^2 = \{(x,y,z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$.

Satz 1.22 (Hausdorff-Paradoxon)
Es gibt Mengen $A, B, C, D \subseteq S^2$ mit

- A, B, C, D bilden eine Partition von S^2
- D ist abzählbar
- $A \cong B \cong C \cong (B \cup C)$

Beweis. Definiere

$$\psi \coloneqq \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

als eine Rotation um $\frac{2\pi}{3} = 120°$, um die z-Achse (die z-Achse ist die Achse, die nach „oben" geht). Es gilt $\psi^3 = 1 = \mathrm{id}_{\mathbb{R}^3}$.

Weiter sei

$$\varphi_\theta \coloneqq \begin{pmatrix} -\cos\theta & 0 & \sin\theta \\ 0 & -1 & 0 \\ \sin\theta & 0 & \cos\theta \end{pmatrix}$$

eine Rotation um $\pi = 180°$, um die Achse a_θ in der x-z-Ebene (die x-z-Ebene ist die Ebene parallel zur Tafel in der Vorlesung). Hier gilt dann $\varphi_\theta \cdot \varphi_\theta = 1$.

Die Gruppe $(G_\theta, \cdot)$ lässt sich nun durch reduzierte Wörter $g = g_1 \dots g_n$ über dem Alphabet $\Gamma = \{\psi, \psi^2, \varphi\}$ darstellen so, dass hintereinander stehende Zeichen, welche sich zu 1 kürzen nicht vorkommen. Die Darstellung ist also eindeutig.

Wir wollen θ so wählen, dass G_θ frei ist, das heißt, dass für jedes $g \in G_\theta$ genau eine Darstellung $g = g_1 \dots g_n$ durch ein reduziertes Wort existiert. Solche θ existieren.

Für $g = g_1 \dots g_n \in \Gamma^*$ sei $g(\theta)$ die Rotation die entsteht, wenn wir $\varphi = \varphi_\theta$ setzen. Und es sei $\theta_g \coloneqq \{\theta \in [0, 2\pi) : g(\theta) = 1\}$.

Lemma 1.5.1*:* Für jedes $g \in \Gamma^* \setminus \{\varepsilon\}$ ist θ_g endlich.

Mithilfe des Lemmas 1.5.1, welches hier nicht bewiesen werden soll, lässt sich folgern, dass $M = \bigcup_{g \in \Gamma^+, g \text{ red.}} \theta_g$ abzählbar ist und wir ein $\theta \in [0, 2\pi] \setminus M$ finden können. Dann ist $g(\theta) \neq 1$ für alle reduzierten $g \in \Gamma^+$ und also G_θ frei über $\{\psi, \psi^2, \varphi_\theta\}$. Fixiere ein solches θ und sei $\varphi \coloneqq \varphi_\theta$

sowie $D \coloneqq \{s \in S^2 : gx = x$ für ein $g \in G_\theta\}$. Jede nicht-triviale Rotation fixiert genau zwei Punkte von S^2, die Schnittpunkte mit der Rotationsachse, also ist D abzählbar

Sei $Q \coloneqq S^2 \setminus D$. Die Bahn von $x \in Q$ unter G_θ ist $G_\theta x = \{gx : g \in G_\theta\}$. Die Bahnen von G_θ auf Q bilden eine Partition. Mit dem Auswahlaxiom existiert also eine Auswahlfunktion auf der Menge dieser Bahnen und damit eine Menge R, welche aus jeder Bahn $G_\theta x$ für $x \in Q$ genau ein Element enthält. Damit ist $Q = \bigcup\{gR : g \in G_\theta\} = \{gr : g \in \Gamma^*, r \in R\}$.

Wir konstruieren die Zerlegung $Q = A\dot\cup B\dot\cup C$ induktiv gemäß der Länge von g. Wenn $|g| = 0$, d.h. $g = 1$ und $gr = r$, setzen wir $r \in A$, also ist $R \subseteq A$. Für $|g| = n + 1$, also ist $gr = h\tilde{g}r$ mit $h \in \{\psi, \psi^2, \varphi\}$, definieren wir die Zugehörigkeit von gr zu A, B, C gemäß der Tabelle 1.

$\tilde{g}h$	φ	ψ	ψ^2
A	B	B	C
B	A	C	A
C	A	A	B

Tabelle 1: Tabelle für die Zugehörigkeiten zu den Mengen für das Hausdorff-Paradoxon

Da jedes Element von Q eine eindeutige Darstellung $g \cdot r$ hat, ist damit die Partition $Q = \dot\cup B\dot{B}\dot{C}$ und damit $S^2 = A\dot\cup B\dot\cup C\dot\cup D$ definiert. Es bleibt zu zeigen, dass $A\cong B\cong C\cong B \cup C$ gilt. Wir behaupten, $\psi(A) = B$, $\psi^2(A) = C$ und $\varphi(A) = B \cup C$.

$\psi(A) \subseteq B$: Sei $A = g \cdot r \in A$.

- Falls $g = \varphi\tilde{g}$, ist $\psi(a) = \psi\varphi\tilde{g}r \in B$ gemäß der Tabelle 1.
- Falls $g = \psi\tilde{g}$, ist $\psi(a) = \psi^2\tilde{g}r$. Da $a = \psi\tilde{g}r \in A$, ist $\tilde{g}r \in C$ und daher $\psi^2 gr \in B$.
- Falls $g = \psi^2\tilde{g}$ gilt $\psi(a) = \tilde{g}r$. Da $a = \psi^2\tilde{g}r \in A$, ist $\tilde{g}r \in B$.

$B \subseteq \psi(A)$: Sei $b \in B$. Gemäß der Tabelle gilt einer der folgenden Fälle:

- Wenn $b = \varphi(a)$ für ein $a \in A$, setze $\tilde{a} = \psi^2(b) \in A$. Dann ist $\psi(\tilde{a}) = \psi\psi^2(b) = b$, also $b \in \psi(A)$.
- Für $b = \psi(a)$ für ein $a \in A$ ist nichts zu zeigen.
- Falls $b = \psi^2(c)$ für ein $c \in C$, setze $a = \psi(c) \in A$. Wir enthalten $\psi(a) = \psi^2(c) = b$, also $b \in \psi(A)$.

Analog kann $\psi^2(A) = C$ gezeigt werden.

$\varphi(A) \subseteq B \cup C$: Sei $a = g \cdot r \in A$.

- Für $g = \varphi\tilde{g}$ ist $\varphi(a) = \varphi\varphi\tilde{g}r$. Da $a = \varphi\tilde{g}r \in A$, ist $\tilde{g}r \in B \cup C$. Also $\varphi(a) \in B \cup C$.
- Wenn $g = \psi\tilde{g}$ oder $g = \psi^2\tilde{g}$, dann gilt $\varphi(a) = \varphi gr \in B \subseteq B \cup C$.

$B \cup C \subseteq \varphi(A)$: Sei $x \in B \cup C$. Folgende Fälle können auftreten

- Wenn $x = \varphi(a)$ für ein $a \in A$ ist nichts zu zeigen.
- Falls $x \in \psi(A) \cup \psi(B) \cup \psi^2(A) \cup \psi^2(C)$, setze $a = \varphi(x) \in A$. Dann erhalten wir $\varphi(a) = \varphi^2(x) = x$, also $x \in \varphi(A)$.

Also liefern φ, ψ und ψ^2 die gesuchten Isometrien. □

Wir nutzen nun das Hausdorff-Paradoxon aus, um eine paradoxe Zerlegung der Einheitskugel $U = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 \leq 1\}$ zu erhalten.

Satz 1.23 (Banach-Tarski-Paradoxon)
Für disjunkte Kopien U' von U gilt $U \sim_z U \dot\cup U'$.

Beweis. Sei $S = S^2$ die Oberfläche von U. Nach dem Satz von Hausdorff haben wir die Zerlegung $A \dot\cup B \dot\cup C \dot\cup D$ mit D abzählbar und den Kongruenzen $A \cong B \cong C \cong B \cup C$. Für $X \subseteq S^2$ sei $X^* := \{rx : x \in X, 0 < r \leq 1\} \subseteq U$.

Nun gilt $A^* \dot\cup B^* \dot\cup C^* \dot\cup D^* \dot\cup \{0\}$ ist eine Partition von U. Es folgt aus dem Hausdorff-Paradoxon, dass $A^* \sim_z B^* \cup C^*$ und $B^* \sim_z B^* \cup C^*$. Weiter ist $A^* \cup B^* \sim_z B^* \cup C^*$, da $A^* \cong C^*$. Analog gilt $A^* \cup B^* \sim_z A^* \cup B^* \cup C^*$, da $B^* \cong B^* \cup C^*$. Aus den letzten Feststellungen ergibt sich, dass $A^* \sim_z A^* \cup B^* \cup C^*$.

Sei nun $X := A^* \cup D^* \cup \{0\}$. Dann ist $X \sim_z U$, da, wie eben festgestellt, $A^* \sim_z A^* \cup B^* \cup C^*$ gilt.

Fixiere eine Rotation φ so, dass $\varphi(D) \cap D = \emptyset$. Dann ist $\varphi(D)^* \subsetneqq A^* \cup B^* \cup C^* \sim_z A^* \sim_z B^*$. Also existiert ein $M \subsetneq B^*$ mit $\varphi(D)^* \sim_z M$.

Wir wählen ein $p \in B^* \setminus M$ und setzen $Y := C^* \dot\cup M \cup \{p\}$. Dann ist $Y \sim_z U$, denn $C^* \sim_z A^* \cup B^* \cup C^*$, $M \sim_z D^*$ und $\{p\} \sim_z \{0\}$ und damit ist $Y = C^* \cup M \cup \{p\} \sim_z A^* \cup B^* \cup C^* \cup D^* \cup \{0\} = U$.

Daraus folgt ebenfalls, dass $Y \sim_z U'$. Da $X \cap Y = \emptyset$, ist $X \dot\cup \sim_z U \dot\cup U'$. Da außerdem $X \cup Y \subseteq U \subseteq U \cup U'$ erhalten wir auch $X \cup Y \sim_z U$. Also gilt $U \sim_z U \dot\cup U'$. □

1.6 Mächtigkeiten und Kardinalzahlen

Definition 1.38
Zwei Mengen x, y sind *gleichmächtig* ($x \sim y$) genau dann, wenn eine Bijektion $f : x \to y$ existiert. Wir sagen x ist höchstens so mächtig wie y ($x \preccurlyeq y$), wenn eine injektive Funktion $f : x \to y$ existiert.

Lemma 1.6.1*:* Ohne das Auswahlaxiom, also nur mit ZF, gelten folgende elementare Eigenschaften:

1. $\sim$ ist eine Äquivalenzrelation auf $\mathcal{S}$.
2. $x \sim y$ gilt genau dann, wenn $x \preccurlyeq y \land y \preccurlyeq x$ (nach Cantor-Schröder-Bernstein).
3. $\preccurlyeq$ ist reflexiv und transitiv. Wir nennen dies eine *Quasiordnung*.
4. Wenn $x \subseteq y$, dann ist $x \preccurlyeq y$.

Auf Basis von ZF ist das Auswahlaxiom äquivalent dazu, dass $\preccurlyeq$ eine totale Quasiordnung ist. Auch folgt mithilfe des Auswahlaxioms, dass für jedes x ein $\beta \in \mathrm{On}$ existiert, mit $x \sim \beta$.

Definition 1.39 (Kardinalität)
Die *Mächtigkeit* oder *Kardinalität* $|x|$ einer Menge x ist die kleinste Ordinalzahl α, die gleichmächtig zu x ist, also $x = \min\{\alpha \in \mathrm{On} : \alpha \sim x\}$.

Lemma 1.6.2*:* Es gilt

a) $x \sim y$ gdw. $|x| = |y|$.

b) $x \preccurlyeq y$ gdw. $|x| \leq |y|$.

Beweis. a): Der Beweis dient als Übung für den Leser. Als Hinweis: Es lässt sich einfach eine passende Bijektion finden, wodurch die Gleichheit klar ist.

b): $\Leftarrow$: Nach Definition existiert eine bijektive Abbildung $f : x \to |x|$. Nach Voraussetzung ist $|x| \leq |y|$ und von $|y|$ existiert eine Bijektion nach y. Also gibt es eine injektive Funktion von x nach y, also $x \preccurlyeq y$.

$\Rightarrow$: Nach Voraussetzung gibt es eine injektive Abbildung $f : x \to y$ und eine injektive Funktion $\hat{f} : |x| \to |y|$. Weiter folgt offensichtlicherweise, dass $\hat{f} : |x| \to f[|x|] \subseteq |y|$ eine Bijektion auf eine Teilmenge von $|y|$ ist.

Auch lässt sich erkennen, dass $f[|x|]$ isomorph zu einem $\beta \in \mathrm{On}$ ist, da $f[|x|]$ ebenfalls eine Wohlordnung ist. Also gibt es einen Isomorphismus $g : (\beta, <) \xrightarrow{\sim} (f[|x|], <) \subseteq (|y|, <) = (\alpha, <)$ für ein Ordinal α.

Nun bleibt zu zeigen, dass falls g ordnungserhaltend ist auch $\beta \leq \alpha$ gilt.

Voraussetzung: Dies wurde bereits für alle $\beta' < \beta$ gezeigt. Da $g : \beta \to \alpha$ für jedes $\beta' < \beta$ eine ordnungserhaltende Abbildung $g \restriction \beta' : \beta' \to g[\beta']$ induziert, also $\beta' \leq g[\beta'] < \alpha$. Aus der Definition von $\beta = \{\beta' : \beta' < \beta\} \subseteq\subseteq \{\beta' : \beta' < \alpha\} = \alpha$, also ist $\beta \leq \alpha$. □

Definition 1.40 (Kardinalzahlen)
Die Klasse aller *Kardinalzahlen* ist $\mathrm{Cn} := \{|x| : x \in \mathcal{S}\} = \{\alpha \in \mathrm{On} : |\alpha| = \alpha\}$

Es lässt sich feststellen, dass alle natürlichen Zahlen Kardinalzahlen sind, ebenso wie ω. Aber das Ordinal $\omega + 1 \notin \mathrm{Cn}$, da sich eine Bijektion von ω nach $\omega + 1$ definieren lässt, wodurch $\omega + 1$ die Kardinalität ω hat.

Definition 1.41 (Endlichkeit und Abzählbarkeit)
Eine Menge x ist *endlich*, falls $x \sim n$ für ein $n \in \omega$ gilt.
Eine Menge x ist *abzählbar*, falls $x \preccurlyeq \omega$.

Satz 1.24 (Cantor)
Für alle Mengen x gilt, dass $|x| < |\mathcal{P}(x)|$.

Beweis. Es soll gezeigt werden, dass es keine surjektive Abbildung $f : x \to \mathcal{P}(x)$ geben kann.

Sei $y = \{a \in x : a \notin f(a)\}$. Nun gilt $y \notin \mathrm{Bild}(f)$. Sonst gilt $y = f(b)$ für ein $b \in a$.

- Falls $b \in y$, dann gilt nach der Definition von y, dass $b \notin f(b)$, aber da $f(b) = y$ folgt dann $b \notin y$. Widerspruch!
- Falls $b \notin y$, dann lässt sich das obige Argument umkehren und genauso zu $b \in y$ führen, was auch hier wieder ein Widerspruch ist.

□

Damit folgt, dass zu jeder Kardinalzahl $\kappa \in \mathrm{Cn}$ ein $\kappa' \in \mathrm{Cn}$ existiert, mit $\kappa' > \kappa$.
Weil $C_n \subseteq \mathrm{On}$ gibt es ein kleinstes solches κ', wir nennen dieses dann κ^+.

Lemma 1.6.3*:* Sei κ eine Kardinalzahl und unendlich. Dann ist κ ein Limesordinal.

Beweis. Wir zeigen $\alpha \sim \alpha + 1$ für alle $\alpha \in \mathrm{On}$ mit $\alpha \geq \omega$.

Definiere eine bijektive Abbildung

$$f : \alpha + 1 \to \alpha, \beta \mapsto \begin{cases} \beta + 1 & \text{falls } \beta < \omega \\ \beta & \text{falls } \omega \leq \beta < \alpha \\ 0 & \text{falls } \beta = \alpha \end{cases}$$

Also kann $\alpha + 1$ keine Kardinalzahl sein, da es eine kleinere Ordinalzahl gibt, zu der $\alpha + 1$ bijektiv ist. □

Definition 1.42
Cn^∞ bezeichne $\mathrm{Cn} \setminus \omega$ (Bemerke: $\omega \in \mathrm{Cn}^\infty$).

Da $\mathrm{Cn}^\infty \subseteq \mathrm{On}$ und nach dem Satz von Cantor unbeschränkt ist, ist Cn^∞ (und damit auch Cn) eine echte Klasse.

Definition 1.43 (Nachfolger- und Limeskardinale)
Sei $\kappa \in \mathrm{Cn}^\infty$. Dann ist κ ein *Nachfolgerkardinal*, falls $\kappa = \lambda^+$ für ein $\lambda \in \mathrm{Cn}$.
Sonst heißt κ *Limesordinal*.

Beachte: Nachfolgerkardinale sind Limesordinale.

Definition 1.44
Wir definieren eine Funktion $\aleph : \mathrm{On} \to \mathrm{On}$ als $\aleph_0 := \omega$, $\aleph_{\alpha+1} := \aleph_\alpha^+$ und $\aleph_\lambda = \bigcup_{\alpha<\lambda} \aleph_\alpha$ für ein Limesordinal λ.

Man beachte, dass nicht $\aleph(\alpha)$ für ein Ordinal α geschrieben wird, sondern $\aleph_\alpha$.

Satz 1.25
Es gilt $\mathrm{Cn}^\infty = \{\aleph_\alpha : \alpha \in \mathrm{On}\}$

Beweis. $\supseteq$: Dies soll induktiv gezeigt werden. Der Induktionsanfang und der Schritt für Nachfolgerordinale ist klar.

Zu zeigen: Für Limesordinale λ ist $\aleph_\lambda \in \mathrm{Cn}^\infty$. Zuerst gilt nach der Übung $\aleph_\lambda \in \mathrm{On}$. Sei $\beta \in \aleph_\lambda$. Dann existiert ein $\alpha < \lambda$, mit $\beta \in \aleph_\alpha = |\aleph_\alpha| \subseteq |\aleph_\lambda|$. Also ist $\aleph_\lambda$ die nächste Kardinalzahl.

$\subseteq$: Der Basisfall ist klar, da $\omega = \aleph_0$. Sei $\kappa \in \mathrm{Cn}^\infty$ und $\kappa > \omega$.

Es existiert ein $\alpha \in \mathrm{On}$ mit $\aleph_\alpha \geq \kappa$ (sonst wäre Bild($\aleph$) beschränkt und damit eine Menge, aber $\aleph$ ist eine Bijektion von On nach Bild($\aleph$) und damit wäre On eine Menge. Widerspruch!).

Sei nun $\alpha = \min\{\beta \in \mathrm{On} : \aleph_\beta \geq \kappa\}$. Dann gilt $\kappa = \aleph_\alpha$, ansonsten wäre $\kappa < \aleph_\alpha$ und somit für alle $\beta < \alpha$ gilt $\aleph_\beta < \kappa < \aleph_\alpha$.

- Falls $\alpha = \beta+1$. Dann ist $\alpha_\alpha = \aleph_\beta^+$ die kleinste Kardinalzahl größer $\aleph_beta$. Widerspruch.
- Falls α ein Limesordinal ist, dann ist $\aleph_\alpha = \bigcup_{\beta<\alpha} \aleph_\beta \leq \kappa < \aleph_\alpha$.

□

1.6.1 Kardinalzahlarithmetik

Seien $\kappa, \lambda, \mu \in \mathrm{Cn}$. Dann seien

- $\kappa + \lambda = |\kappa \dot\cup \lambda| = |\kappa \times \{0\} \cup \lambda \times \{1\}|$.
- $\kappa \cdot \lambda = |\kappa \times \lambda|$.
- $\kappa^\lambda = |\kappa^\lambda| = |\{f | f : \lambda \to \kappa|\}$.

Weiter lässt sich feststellen, dass die für endliche Kardinale bekannten Eigenschaften, auch für alle Kardinale gelten. Diese werden hier nun beispielhaft aufgeführt.

1. $(\mathrm{Cn}, +, 0)$ bildet ein abelsches Monoid.

2. $(\mathrm{Cn} \setminus \{0\}, \cdot, 1)$ bildet ebenfalls ein abelsches Monoid.

3. Wenn $\kappa \leq \lambda$, dann ist $\kappa + \mu \leq \lambda + \mu$.

4. Es gilt $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

5. Für $\kappa \leq \lambda$ gilt $\kappa \cdot \mu \leq \lambda \cdot \mu$.

6. Für alle κ ist $0 \cdot \kappa = \kappa \cdot 0 = 0$.

7. Es gilt $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$ und $\kappa^{\lambda \cdot \mu} = (\kappa^\lambda)^\mu$.

8. $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$.

9. Es gelten $\kappa^0 = 1$, $\kappa^1 = \kappa$ und $0^\kappa = 0$ für $\kappa \neq 0$.

Satz 1.26 (Hessenberg, 1906)
Für $\lambda \in \mathrm{Cn}^\infty$ gilt $\lambda \cdot \lambda = \lambda$.

Um dies zu zeigen werden noch einige Zwischenschritte benötigt. Zuerst lässt sich erkennen, dass der Satz bewiesen ist, falls sich zeigen lässt, dass $\alpha \times \alpha \sim \alpha$ für alle $\alpha \geq \omega$ gilt, denn dann gilt $\lambda \cdot \lambda = |\lambda \times \lambda| = |\lambda| = \lambda$.

Wie entweder leicht einsehbar oder bereits bekannt, gilt $\omega \times \omega \sim \omega$, da sich sehr einfach eine Bijektion zwischen natürlichen Zahlen und Paaren von diesen finden lässt. Beispielsweise stellt die Abbildungsvorschrift $(i, j) \mapsto \frac{1}{2}(i + j)(i + j + 1) + j$ eine solche dar.

Nun wollen wir eine Wohlordnung $<^*$ auf $\mathrm{On} \times \mathrm{On}$ definieren. Für $\alpha, \alpha', \beta, \beta' \in \mathrm{On}$ gilt $(\alpha, \beta) <^* (\alpha', \beta')$ genau dann, wenn

- $\max\{\alpha, \beta\} < \max\{\alpha, \beta\}$ oder
- $\max\{\alpha, \beta\} = \max\{\alpha, \beta\}$ und $\alpha < \alpha'$ oder
- $\max\{\alpha, \beta\} = \max\{\alpha, \beta\}$ und $\alpha = \alpha'$ und $\beta < \beta'$.

Für ein $\gamma \in \mathrm{On}$ wird zusätzlich die Menge $S_\gamma := \{(\alpha, \beta) \in \mathrm{On}^2 : \max\{\alpha, \beta\} = \gamma\}$ definiert. Eine grafische Darstellung lässt sich in Abbildung 5 sehen. Die blau gezeichnete Linie stellt die Menge S_γ dar und das grüne Rechteck illustriert, welche Paare kleiner als ein gegebenes Paar (α, β) sind.

Lemma 1.6.4*:* $<^*$ ist eine Wohlordnung.

Beweis. Sei $A \subseteq \mathrm{On} \times \mathrm{On}$ nicht-leer. Setze $\delta := \{\delta' \in \mathrm{On} : A \cap S'_\delta \neq \emptyset\}$. Nun ist das Minimum von A das Paar (α_0, β_0) mit $\alpha_0 := \min\{\alpha \in \mathrm{On} : \exists\beta[(\alpha, \beta) \in A \cap S_\delta]\}$ und $\beta_0 := \min\{\beta \in \mathrm{On} : (\alpha_0, \beta) \in A \cap S_\delta\}$. □

Definition 1.45
Die Gödelsche Paarfunktion $G : \mathrm{On} \times \mathrm{On} \to \mathrm{On}$ ist definiert als $G(\alpha, \beta) = \mathrm{otp}(\{(\alpha', \beta') : (\alpha', \beta') <^* (\alpha, \beta)\}, <^*)$.

Hierbei bezeichnet $\mathrm{otp}(A, <)$ die Ordinalzahl α so, dass $(A, <) \cong (\alpha, <)$. Also ist $(\alpha, \beta) \downarrow^{<^*} \cong (G(\alpha, \beta), <)$.

Lemma 1.6.5*:* Es gilt $G(\alpha, \beta) = \{G(\alpha', \beta') : (\alpha', \beta') <^* (\alpha, \beta)\}$.

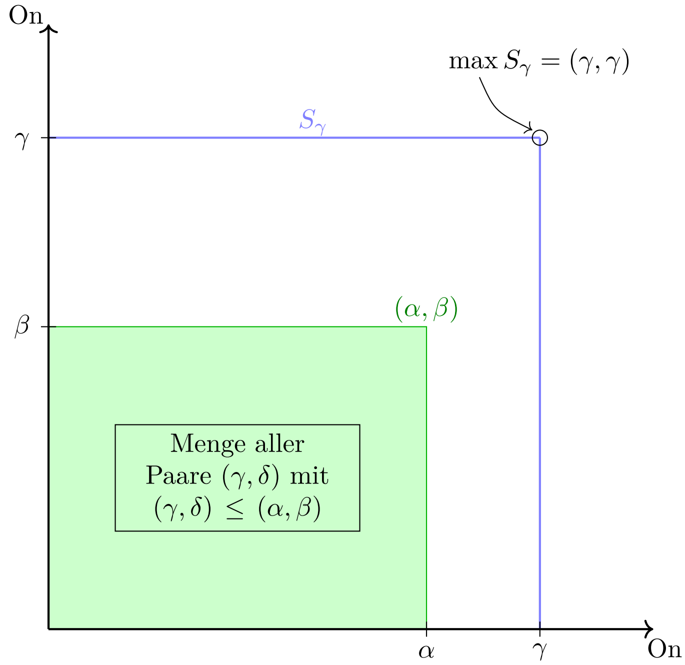

Abbildung 5: Die grafische Darstellung von $<^*$.

Der Beweis zum obigen Lemma lässt sich durch eine Graphik, welche den Isomorphismus von $((\alpha,\beta),<)$ nach $(G(\alpha,\beta),<)$ verdeutlicht.
Damit folgt dann, dass G ordnungserhaltend und injektiv ist.

Lemma 1.6.6*:* a) $G(\alpha,\beta) \geq \max\{\alpha,\beta\}$.

b) $G[\alpha\times\alpha] = G(0,\alpha)$. Insbesondere ist $\alpha \leq G[\alpha\times\alpha]$.

c) $G[\omega\times\omega] = \omega$.

Beweis. a): $G(\alpha,\beta) = (\{(\alpha',\beta') \in \mathrm{On} : (\alpha',\beta') <^* (\alpha,\beta)\}, <^*) \supseteq (\{(\gamma,0) : \gamma < \alpha\}, <^*) \cong (\alpha,<)$. Es folgt, dass $G(\alpha,\beta) \geq \beta$. Analog lässt sich dies für $G(\alpha,\beta) \supseteq \beta$ zeigen.

b): $\alpha\times\alpha = \{(\beta,\gamma) \in \mathrm{On}^2 : (\beta,\gamma) <^* (0,\alpha)\}$. Nach dem Lemma folgt $G[\alpha\times\alpha] = G(0,\alpha)$ und wegen a) ist $\alpha \leq G(0,\alpha) = G[\alpha\times\alpha]$.

c): Jedes $(m,n) \in \omega\times\omega$ hat nur endlich viele $<^*$-Vorgänger, also folgt $G(m,n) < \omega$. Demnach ist $G[\omega\times\omega] \leq \omega$. $G[\omega\times\omega] \geq \omega$ folgt aus b). Also muss $G[\omega\times\omega] = \omega$ gelten. Die Abbildung $G \restriction \omega\times\omega$ ist also eine Bijektion von $\omega\times\omega$ nach ω. □

Nachdem nun einige Hilfsaussagen gezeigt und diskutiert wurden können wir jetzt den Satz von Hessenberg beweisen. Zu Erinnerung: Wir müssen zeigen, dass, basierend auf ZFC, für alle Ordinale $\alpha \geq \omega$ gilt, dass $\alpha\times\alpha \sim \alpha$.

Beweis: Satz von Hessenberg. Wir wollen dies durch eine transfinite Induktion über α zeigen.
Induktionsanfang: $\alpha = \omega$: Dies folgt aus dem Teil c) des eben bewiesenen Lemmas.

Für $\alpha > \omega$ lassen sich zwei Fälle aufstellen.

- Falls ein $\beta < \alpha$ existiert mit $\beta \sim \alpha$, dann ist $\alpha \times \alpha \sim \beta \times \beta \overset{\mathrm{IV}}{\sim} \beta \sim \alpha$.
- Sonst ist α ein Limesordinal, da $\beta + 1 \sim \beta$ wäre. Mit b) des Lemmas folgt $G[\alpha \times \alpha] \geq \alpha$. Für einen Widerspruch nehmen wir $G[\alpha \times \alpha] > \alpha$ an.

  Wähle $(\beta, \gamma) \in \alpha \times \alpha$ mit $G(\beta, \gamma) = \alpha$. Setze $\delta := \max\{\beta, \gamma\} + 1$. Also ist $(\beta, \gamma) \in \delta \times \delta$ und $\alpha = G(\beta, \gamma) \in G[\delta \times \delta]$ und daher $\alpha \subseteq G[\delta \times \delta]$.

  Nun ist $\alpha \overset{(1)}{>} \delta \overset{(2)}{>} \omega$, weil (1) α ein Limesordinal ist und (2), weil $\alpha \notin G[\omega \times \omega]$.

  Nach der Induktionsvoraussetzung existieren die Bijektion $g : \delta \to \delta \times \delta$ und die Abbildung $h := G \circ g : \delta \to G[\delta \times \delta] \supseteq \alpha$.

  Die Umkehrabbildung $h^{-1} \restriction \alpha \to \delta$ ist nun aber eine injektive Abbildung von α in eine Teilmenge von δ. Es folgt $\alpha \sim \delta$, also müsste für α eigentlich der erste Fall gelten. Widerspruch!

Es gilt also $G[\alpha \times \alpha] = \alpha$ und damit ist $G \restriction \alpha \times \alpha$ eine Bijektion von $\alpha \times \alpha$ nach α. □

Es wurde nun also gezeigt, dass aus dem Wohlordnungssatz, daher auch dem Auswahlaxiom, die eben bewiesene Eigenschaft folgt. Die Umkehrung lässt sich aber auch zeigen.

Satz 1.27 (Tarski, 1924)
In ZF gilt: Die Aussage, dass $a \times a \sim a$ für alle unendlichen Mengen a gilt impliziert das Auswahlaxiom

Beweis. Sei a eine Menge und $\beta \in \mathrm{On}$ so, dass keine Surjektion von a nach β existiert. Nach Voraussetzung gilt $f : a \cup \beta \to (a \cup \beta) \times (a \cup \beta)$. Nun konstruieren wir eine Wohlordnung auf a.

Beobachtung: $\beta \times \{x\} \not\subseteq f[a]$, denn sonst ist $h : a \to \beta \times \{x\} \to \beta$ surjektiv. Widerspruch!

Also $S_b := \{\gamma \in \beta : f(\gamma) \in \beta \times \{b\}\} \neq \emptyset$.

Damit ist die Funktion $g : a \to \beta, x \mapsto \min S_x$. Dies ist injektiv und wohldefiniert, denn $S_c \cap S_d = \emptyset$ für $c \neq d \in a$ und g induziert eine Wohlordnung auf a durch:

$$b < c \text{ gdw. } g(n) < g(c).$$

Damit wurde eine Wohlordnung gefunden und der Satz von Tarski ist bewiesen. □

Aus dem Satz von Hessenberg lassen sich einige Eigenschaften folgern.
Für $\kappa \in \mathrm{Cn}$ und $\kappa \leq \lambda \in \mathrm{Cn}^\infty$ gilt

$$\kappa + \lambda = \kappa \cdot \lambda = \lambda.$$

Dies lässt sich daran sehen, dass

$$\lambda \leq \kappa + \lambda \leq \lambda + \lambda \leq 2 \cdot \lambda = \lambda$$

bzw.

$$\lambda \leq \kappa \cdot \lambda \leq \lambda \cdot \lambda = \lambda.$$

Weiter gilt für $n \geq 1$ und $\lambda \in \mathrm{Cn}^\infty$, dass $\lambda^n = \lambda$.

Satz 1.28 a) $|\mathcal{P}(x)| = 2^{|x|}$.

b) Wenn $2 \leq \kappa \leq \lambda$ mit $\kappa \in \mathrm{Cn}, \lambda \in \mathrm{Cn}^\infty$, dann ist $\kappa^\lambda = 2^\lambda$.

Beweis. a): $\mathcal{P}(x) \sim \{f : x \to 2\}$ und nach Definition ist $|\{f : x \to 2\}| = 2^{|x|}$.
b): $2^\lambda \leq \kappa^\lambda \leq (2^\lambda)^\lambda = 2^{\lambda \cdot \lambda} = 2^\lambda$. □

Durch weitere Überlegungen kann man feststellen, dass $|\mathbb{Q}| = |\omega \times \omega| = \omega$ und $|\mathbb{R}| = \omega^\omega = 2^\omega = |\mathcal{P}(\mathbb{N})|$. Und mit Hilfe von Satz 1.24 folgt, dass $|\mathbb{R}| \neq |\mathbb{Q}|$.

1.6.2 Die Kontinuumshypothese (CH)

Die Kontinuumshypothese (englisch: continuum hypothesis) besagt, dass $\omega^+ = 2^\omega$ oder anders ausgedrückt: $\aleph_1 = 2^{\aleph_0}$. Zusätzlich gibt es auch die verallgemeinerte Kontinuumshypothese (GCH), nach welche $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ für alle $\alpha \in \mathrm{On}$ gilt.

Es lässt sich aber zeigen, dass *CH unabhängig von* ZFC *ist.* Das heißt, es gilt sowohl ZFC $\not\models CH$, als auch ZFC $\not\models \neg CH$, wobei davon ausgegangen wird, dass ZFC konsistent ist und es somit überhaupt ein Modell von ZFC gibt.

Der Beweis dafür wurde von zwei Mathematikern geführt. Der erste Teil wurde von Kurt Gödel im Jahre 1938 bewiesen. Dafür hat er aus dem bekannten Stufenmodell $(S_\alpha)_{\alpha\in\mathrm{On}}$ eine konstruierbare Hierarchie $(L_\alpha)_{\alpha\in\mathrm{On}}$ erzeugt. Für diese gilt $L_0 \coloneqq \emptyset$, für Limesordinale λ ist $L_\lambda \coloneqq \bigcup_{\beta<\lambda} L_\beta$ und für $\alpha + 1$ ist $L_{\alpha+1} \coloneqq \{x \subseteq L_\alpha : \exists a_1, \ldots, a_n \exists\varphi(z, y_1, \ldots, y_n) : x = \{z \in L_\alpha : (L_\alpha, \in) \models \varphi(z, a_1, \ldots, a_n)\}\}$ die Menge aller Teilmengen, die sich mithilfe einer FO-Formel darstellen lassen.

Damit konnte Gödel folgern, dass $(L, \in) \models ZF$, $(L, \in) \models AC$ und $(L, \in) \models GCH$.
Den zweiten Teil konnte Paul Cohen im Jahre 1963 beweisen. Sein Endresultat war, dass $ZF \not\models AC$ und ZFC $\not\models CH$.
Daraus folgt also, dass mithilfe von ZFC nichts über die Korrektheit der Kontinuumshypothese aussagen lässt. ZFC ist also nicht vollständig. Zusätzlich nehmen die obigen Überlegungen die Konsistenz von ZFC an.

Trotz dieser Probleme mit ZFC wird dieses als „Standard“ Axiomensystem angenommen. Wie im nächsten Kapitel nämlich gezeigt werden wird, gilt für alle Axiomensysteme, welche genügend Aussagekraft haben, dass deren Konsistenz nicht gezeigt werden kann und sie nicht vollständig sein können.

2 Die Gödelschen Unvollständigkeitssätze

In diesem Kapitel sollen die Gödelschen Unvollständigkeitssätze behandelt werden. Durch diese wird einsehbar sein, dass die Unvollständigkeit von ZFC, wie sie im Kapitel zur Kontinuumshypothese festgestellt wurde, nicht behoben werden kann, egal wie das Axiomensystem der Mengenlehre gewählt wird.

2.1 Das Hilbertsche Programm

Unter dem Hilbertschen Programm versteht man die Bestrebungen des deutschen Mathematikers David Hilbert (1862 – 1943) zur Axiomatisierung der verschiedenen Zweige der Mathematik in der Prädikatenlogik erster Ordnung. Insbesondere sollte es möglich sein, mathematische Folgerungen auf syntaktische Ableitungen in einem formalen Kalkül zu reduzieren. Ebenso war das Ziel effektive Verfahren (heute auch Algorithmen genannt) zu konstruieren, um die Gültigkeit mathematischer Aussagen in einer Theorie zu entscheiden. Diese Teilergebnisse sollten dann im Beweis der Widerspruchsfreiheit der Mathematik gipfeln. All diese Vorhaben kommen einem mit dem heutigen Wissen sehr utopisch vor und so soll im weiteren Verlauf des Kapitels auch bewiesen werden, dass viele Teile des Programms nicht so aufgehen, wie es sich Hilbert gewünscht hätte.
Dennoch konnte einige Erfolge erzielt werden:

- Die Axiomatisierung wichtiger Teile der Mathematik durch geeignete Axiomensysteme konnte gezeigt werden
- Die Peano-Arithmetik stellt eine mögliche Axiomatisierung der bekannten Arithmetik in den natürlichen Zahlen dar
- Das Axiomensystem ZFC erlaubt eine Formalisierung der Mathematik innerhalb der Mengenlehre
- Der Begriff *Beweis* konnte durch formale Systeme wie das Hilbert-Frege-System, den Sequenzenkalkül und weiteren, präzisiert werden.
- Durch den Beweis des Vollständigkeitssatzes von Kurt Gödel in 1931, welcher aussagt, dass $\Phi \models \psi$ äquivalent ist zu $\Phi \vdash \psi$ (für $\Phi \subseteq \mathrm{FO}, \psi \in \mathrm{FO}$), konnte gezeigt werden, dass die gewünschte Reduktion von mathematischen auf syntaktische Folgerungen gültig ist.
- Zuletzt konnten algorithmische Verfahren gefunden werden, um die Erfüllbarkeit bzw. Gültigkeit von *Fragmenten* von FO zu entscheiden.

Jedoch haben fundamentale Resultate aus den 30er-Jahren das Hilbertsche Programm scheitern lassen:

1. Gödelscher Unvollständigkeitssatz Jede hinreichend reichhaltige, rekursiv axiomatisierbare Theorie ist unvollständig (bspw. bezieht sich dies auf PA und ZFC).

Satz von Church/Turing Die Erfüllbarkeit bzw. Gültigkeit von FO ist unentscheidbar.

2. Gödelscher Unvollständigkeitssatz Ist Φ ein entscheidbares, hinreichend starkes Axiomensystem, dann ist aus Φ die Widerspruchsfreiheit von Φ nicht beweisbar. Insbesondere gilt dies für $\Phi = \mathrm{ZFC}$.

2.2 Theorien

Definition 2.1 (Theorie)
Eine *Theorie* $T \subseteq \mathrm{FO}(\tau)$ ist eine erfüllbare Satzmenge, welche unter $\models$ abgeschlossen ist. Das heißt, wenn $T \models \psi$, dann ist bereits $\psi \in T$.

Im weiteren Verlauf wird die Notation $\Phi^{\models}$ für den Abschluss von Φ unter $\models$ verwendet. Aus dem Vollständigkeitssatz und der Definition der Theorie ergibt sich für eine Theorie $T = T^{\models} = T^{\vdash}$.

Definition 2.2 (Vollständigkeit)
Eine Theorie T ist *vollständig*, wenn für jeden Satz $\psi \in \mathrm{FO}(\tau)$ gilt: $\psi \in T$ oder $\neg\psi \in T$.

Definition 2.3 (Rekursive Axiomatisierbarkeit)
Eine Theorie T ist *rekursiv axiomatisierbar*, wenn eine entscheidbare Menge $\Phi \subseteq \mathrm{FO}$ existiert mit $\Phi^{\models} = T$.

Satz 2.1
Sei T eine vollständige Theorie. Dann sind äquivalent:

1. T ist rekursiv axiomatisierbar.
2. Es gibt ein rekursiv aufzählbares Axiomensystem Φ mit $T = \Phi^{\models}$.
3. T ist rekursiv aufzählbar.
4. T ist entscheidbar.

Bemerkung: Um *Rekursive Aufzählbarkeit* abzukürzen wird r.e. geschrieben, was für *recursively enumerable* steht.

Beweis. 1. ⇒ 2. Da 1. eine schwächere Aussage als 2. ist, welches 1. sogar impliziert, ist die Folgerung trivial.

2. ⇒ 3. Wenn Φ r.e. ist, dann ist dies auch die Menge aller endlichen $\Phi_0 \subseteq \Phi$. Sei M nun ein Algorithmus mit Haltemenge $L(M) = \Phi$. Um zu überprüfen, ob ein $\Phi_0 = \{\varphi_1, \ldots, \varphi_m\} \subseteq \Phi$ ist, soll M nacheinander auf $\varphi_1, \ldots, \varphi_m$ angewendet werden und halten, wenn M auf allen φ_i hält.

Indem man nun systematisch alle endlichen $\Phi_0 \subseteq \Phi$ und alle im Sequenzenkalkül ableitbaren Sequenzen $\Phi \Rightarrow \psi$ aufzählt, erhält man ein Aufzählungsverfahren für T.

3. ⇒ 4. T ist vollständig, also gilt $\psi \notin T$ genau dann, wenn $\neg\psi \in T$. Mit T ist also auch das Komplement von T in $\mathrm{FO}(\tau)$ r.e. Also ist T entscheidbar.

4. ⇒ 1. Wähle $\Phi = T$. Mit der Definition ergibt sich, dass T dann rekursiv aufzählbar ist. □

Wir betrachten nun die Struktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$. Die Theorie $\mathrm{TA} := \mathrm{Th}(\mathfrak{N}) = \{\psi : \mathfrak{N} \models \psi\}$ wird als echte Arithmetik (engl.: *true arithmetic*) bezeichnet. Offensichtlich ist TA vollständig. Das Axiomensystem der Peano-Arithmetik Φ_{PA} besteht aus folgenden Axiomen:

- $\forall x \neg(x + 1 = 0)$
- $\forall x \forall y (x + 1 = y + 1 \rightarrow x = y)$
- $\forall x (x + 0 = x)$
- $\forall x \forall y (x + (y + 1) = (x + y) + 1)$
- $\forall x (x \cdot 0 = 0)$

- $\forall x \forall y (x \cdot (y+1) = (x \cdot y) + x)$

und dem Axiomenschema der vollständigen Induktion:

$$\forall \overline{y}((\varphi(0,\overline{y}) \land \forall x(\varphi(x,\overline{y}) \to \varphi(x+1,\overline{y}))) \to \forall x \varphi(x,\overline{y}))$$

für jede Formel $\varphi(x,\overline{y}) \in \mathrm{FO}(\tau_{\mathrm{ar}})$.

Erlaubt man anstatt der Prädikatenlogik erster Ordnung auch die monadische Logik zweiter Stufe, lässt sich das Axiomenschema der vollständigen Induktion auch als allgemeines Induktionsaxiom formulieren:

$$\forall X((X(0) \land \forall x\,(X(x) \to X(x+1))) \to \forall x X(x)) \in MSO$$

In Φ_{PA} wird das Induktionsaxiom dagegen aber nur für definierbare Teilmengen gefordert. Die Peano Arithmetik $\mathrm{PA} := \Phi_{\mathrm{PA}}^{\models}$ ist rekursiv axiomatisiert und daher r.e.

Definition 2.4 (Repräsentative Axiomensysteme)
Ein Axiomensystem Φ ist *repräsentativ* (oder *erlaubt Kodierungen*), wenn man zu jeder Zahl $n \in \mathbb{N}$ einen Term t_n angeben kann (z.B. $t_n := \underbrace{1 + \cdots + 1}_{n\text{-mal}}$) so, dass gilt:

1. $\Phi \vdash \neg t_n = t_m$ (für $n \neq m$)
2. Für jede totale berechenbare Funktion $f : \mathbb{N}^k \to \mathbb{N}$ existiert eine Formel $\varphi_f(\overline{x}, y)$ so, dass für alle $n_1, \ldots, n_k$
   - $\Phi \vdash \exists! y \varphi_f(t_{n_1}, \ldots, t_{n_k}, y)$
   - Wenn $f(n1, \ldots, n_k) = m$, dann $\Phi \vdash \varphi_f(t_{n_1}, \ldots, t_{n_k}, t_m)$
   - Wenn $f(n_1, \ldots, n_k) \neq m$, dann $\Phi \vdash \neg\varphi_f(n_1, \ldots, n_k, m)$

Wenn Φ repräsentativ ist, dann wird auch jede entscheidbare Relation $R \subseteq \mathbb{N}^k$ durch eine Formel $\varphi_R(x_1, \ldots, x_k)$ dargestellt:

- $(n_1, \ldots, n_k) \in R \Rightarrow \Phi \vdash \varphi_R(t_{n_1}, \ldots, t_{n_k})$
- $(n_1, \ldots, n_k) \notin R \Rightarrow \Phi \vdash \neg\varphi_R(t_{n_1}, \ldots, t_{n_k}$

Insgesamt lässt sich feststellen, dass TA, PA und auch ZFC repräsentativ sind.

Definition 2.5
Wir definieren die Funktion $[\cdot,\cdot] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (x,y) \mapsto \frac{1}{2}(x+y)(x+y+1) + x$.

Lemma 2.2.1*:* Die Funktion $[\cdot,\cdot]$ ist bijektiv.

Beweis. Das Paar (x, y) erhält die Nummer

$$\left(\sum_{0 \leq n < x+y} n+1\right) + x = \left(\sum_{1 \leq n \leq x+y} n\right) + x = \frac{1}{2}(x+y)(x+y+1) + x = [x,y].$$

□

Weiter lässt sich dann festlegen, dass Tupel als $[a_1, \ldots, a_n] := [a_0, [a_1, \ldots, a_n]]$ definiert sind, für $n > 1$. Demnach lässt sich eine definierbare Bijektion $\mathbb{N}^k \to \mathbb{N}$ für ein festes, aber beliebiges k finden.

Satz 2.2 (Chinesischer Restsatz)
Seien $q_0, \ldots, q_{n-1}$ paarweise teilerfremd und $q \coloneqq \prod_{i<n} q_i$. Dann ist die Funktion

$$F : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q_0\mathbb{Z} \times \cdots \times \mathbb{Z}/q_{n-1}\mathbb{Z}, a \mapsto (a_0, \ldots, a_{n-1})$$

eine Bijektion.

Beweis. Seien $a, a' \in \mathbb{Z}/q\mathbb{Z}$ so, dass $a \equiv_{q_j} a'$ für alle $j < n$. Also wird $a - a'$ von allen q_j geteilt und daher, da die q_j teilerfremd sind, auch von dem Produkt q, also ist $a \equiv_q a'$. □

Lemma 2.2.2 (Gödelsches β-Lemma)*:* Es gibt eine totale berechenbare Funktion $\beta : \mathbb{N}^3 \to \mathbb{N}$ so, dass zu jeder endlichen Folge $(a_0, \ldots, a_{n-1})$ über $\mathbb{N}$ zwei Zahlen $a, b \in \mathbb{N}$ existieren, mit $\beta(a, b, j) = a_j$ für alle $j < n$.

Beweis. Setze $\beta(x, y, z) \coloneqq x \mod (1 + y(z + 1))$. β ist definierbar durch die Formel

$$\varphi_\beta(x, y, z, v) \coloneqq v < 1 + y(z + 1) \land \exists u(x = u + uy(z + 1) + v).$$

Es ist nun zu zeigen, dass sich für alle $a_0, \ldots, a_{n-1}$ zwei a, b angeben lassen so, dass $a \equiv a_j \mod (1 + b(j + 1))$ und $b \coloneqq m!$ für $m = \max\{n, a_0, \ldots, a_n - 1\}$.
Behauptung: Für $0 \leq i < j \leq n$ sind $1 + (i + 1) + b$ und $1 + (j + 1) + b$ teilerfremd.

Andernfalls ex. ein $p > 1$ mit $p|1 + (i + 1) + b$ und $p|1 + (j + 1) + b$. Es folgt, dass $p|(i - j)b$, aber $p \nmid b$ (sonst $p \nmid 1 + (i + 1) + b$), also $p|(i - j)$ und daher $p < n$. Dies ist aber unmöglich, da b von jeder Zahl, welche kleiner als n geteilt wird.

Nach dem chinesischen Restsatz existiert dann ein $a < \prod_{j=0}^{n-1}(1 + b(j + 1))$ mit $a \equiv a_j \mod (1 + b(j + 1))$ für alle $j < n$. □

Eine Folge $(a_0, \ldots, a_{n-1})$ über $\mathbb{N}$ kodieren wir nun durch $\langle a_0, \ldots, a_{n-1}\rangle \coloneqq [a, b, n]$ so, dass $\beta(a, b, i) = a_i$ für alle $i < n$, mit $b = (\max\{n, a_0, \ldots, a_{n-1}\})!$. Weiter ist die Länge solch einer Folge $\ln(\langle a_0, \ldots, a_{n-1}\rangle) \coloneqq n$ und $\pi_i(\langle a_0, \ldots, a_{n-1}) = a_i$.

Es lässt sich feststellen, dass $[\cdot, \cdot]$, β, ln und π in TA, PA und ZFC definierbar sind.

2.3 Kodierung von Turing Maschinen

Mit den Ergebnissen aus dem vorherigen Kapitel ist es nicht schwer Turing Maschinen zu kodieren und mithilfe dieser gewisse Widersprüche zu zeigen.

Eine Turing Maschine (kurz: TM) ist ein Tupel $M = (Q, \Sigma, \delta, q_0, F)$ und eine Konfiguration einer TM ist ein Tripel $c = [q, w, p]$, wobei $q < |Q|$, $w = (w_0, \ldots, w_{n-1}) \in \Sigma^*$ mit $w_i \leq |\Sigma|$, und $p \leq |w|$. Es soll zudem noch bemerkt werden, dass die Relation $\vdash_M$ die Nachfolgerrelation ist. $x \vdash_M y$ gilt also genau dann, wenn y in M eine gültige Nachfolgerkonfiguration ist.

Sei nun $\Phi \in \{\text{TA}, \Phi_{\text{PA}}, \text{ZFC}\}$ und M eine TM. Es gibt Formeln $\text{Konf}_M(x)$, $\text{Start}_m(x, y)$, $\text{End}_M(x, y)$ und $\text{Lauf}_M(x)$ mit

- $\Phi \vdash \text{Konf}_M(n)$ gdw. n kodiert eine gültige Konfiguration von M, also $n = [q, w, p]$.
- $\Phi \vdash \text{Start}_M(n, m)$ gdw. n kodiert die Inputkonfiguration von M auf m.
- $\Phi \vdash \text{End}_M(n, m)$ gdw. n kodiert eine Endkonfiguration von M mit Bandinschrift (Output) m.
- $\Phi \vdash \text{Lauf}_M(x)$ gdw. x beschreibt eine gültige Berechnung von M, d.h. eine Folge $x = \langle c_0, \ldots, c_n\rangle$ mit $\text{Konf}_M(c_i)$ und $c_i \vdash_M c_{i+1}$.

Mit diesen Formeln und des Erlaubens von Kodierungen von TA, Φ_{PA} und ZFC erhält man die Folgerung, welche zuerst von Tarski formuliert wurde:

$$\boxed{\text{TA ist unentscheidbar}}$$

Der Beweis lässt sich mithilfe des Halteproblems führen. Angenommen, TA wäre entscheidbar. Da TA vollständig ist, ließe sich mithilfe der obigen Formeln für beliebige TMs entscheiden, ob gegebene Läufe gültig sind. Mithilfe der Formeln würde man dann das Halteproblem lösen können. Nach Turing (1937) ist dies aber nicht möglich, weshalb TA nicht entscheidbar sein kann.

Die exakt gleiche Argumentation lässt sich auch auf PA und $\text{ZFC}^{\models}$ übertragen, weshalb diese ebenfalls nicht entscheidbar sein können.

Dies führt zum ersten Unvollständigkeitssatz von Gödel:

Satz 2.3 (1. Gödelscher Unvollständigkeitssatz) 1. Es gibt kein entscheidbares Axiomensystem für TA.

2. PA ist unvollständig

Beweis. *1.* ist zwar die gleiche Aussage wie die Folgerung Tarskis, Gödel hat dies aber über einen anderen Weg noch vor Turings Entdeckung der Unentscheidbarkeit des Halteproblems gezeigt, welchen wir und im Folgenden anschauen möchten.

2. ist durch einen Widerspruch mithilfe des ersten Teiles möglich. Wäre PA vollständig, dann wäre es ein Axiomensystem für TA. Nach *1.* wäre PA dann aber nicht entscheidbar, war entgegen der Definition von PA geht. Also muss PA unvollständig sein. □

2.4 Gödelisierung von Termen und Formeln

Wie im vorherigen Kapitel erwähnt hat Gödel einen anderen Weg für seine Unvollständigkeitssätze verwendet, unter anderem, weil Turing seinen Beweis erst einige Jahre nach Gödel veröffentlicht hat. In diesem Kapitel soll nun der Beweisweg von Gödel betrachtet werden.
Als Gödelisierung wird das Verfahren bezeichnet, den Termen und Formeln einer Logik eine eindeutige, natürliche Zahl zuzuordnen. Ein Term t wird zu einer natürlichen Zahl $\ulcorner t \urcorner \in \mathbb{N}$ und eine Formel φ wird zu der Zahl $\ulcorner \varphi \urcorner \in \mathbb{N}$. Für eine Formel $\theta(x)$ und $k \in \mathbb{N}$ schreibt man $\theta(k)$ für $\theta[x/\underbrace{1 + \cdots + 1}_{k\text{-mal}}]$, also das Ersetzen von jedem Vorkommen von x in θ durch einen Term, welcher zu k auswertet.

Satz 2.4 (Fixpunktsatz)
Φ erlaube Kodierungen. Zu jeder Formel $\psi(x) \in \text{FO}(+, \cdot, 0, 1)$ ex. ein Satz φ mit $\Phi \vdash \varphi \leftrightarrow \psi(\ulcorner \varphi \urcorner)$.

Der Fixpunktsatz lässt sich auch anders formulieren: Aus jeder Formel $\psi(x) \in \text{FO}(+, \cdot, 0, 1)$ wird eine Funktion $f_\psi, \varphi \mapsto \psi(\ulcorner \varphi \urcorner)$ gebildet. Jede solche Funktion hat einen bis auf Äquivalenz bestimmten Fixpunkt.

Beweis. Sei $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ die Funktion mit $f(\ulcorner \theta(x) \urcorner, k) := \ulcorner \theta(k) \urcorner$ und $f(n, k) = 0$, wenn n nicht die Gödelnummer einer Formel $\theta(x)$ ist.

Da f berechenbar ist, gibt es eine Formel $\alpha(x, y, z)$ mit $\Phi \vdash \alpha(n, k, m)$ gdw. $m = f(n, k)$. Für eine gegebene Formel $\psi(x)$ setze $\theta(x) := \forall z(\alpha(x, x, z) \to \psi(z))$ und $\varphi := \theta(\ulcorner \theta \urcorner)$. Dann gilt $f(\ulcorner \theta \urcorner, \ulcorner \theta \urcorner) = \ulcorner \varphi \urcorner$, also

$$\Phi \vdash \alpha(\ulcorner \theta \urcorner, \ulcorner \theta \urcorner, \ulcorner \varphi \urcorner) \tag{$*$}$$

Es bleibt zu zeigen, dass $\Phi \vdash \varphi \leftrightarrow \psi(\ulcorner \varphi \urcorner)$ gilt.

⇒: Man betrachte die Sequenz $\Phi \vdash (\varphi \wedge \alpha(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner, \ulcorner\varphi\urcorner)) \to \psi(\ulcorner\varphi\urcorner)$. Zur Erinnerung ist φ definiert als $\varphi := \forall z(f(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner) = z \to \psi(z))$. Falls nun also φ und $\alpha(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner, \ulcorner\varphi\urcorner)$ gilt, dann muss, wegen der Aussage von φ, auch $\psi(\ulcorner\varphi\urcorner)$ gelten.
Durch $(*)$ folgt dann $\Phi \vdash \varphi \to \psi(\ulcorner\varphi\urcorner)$

⇐: Es gilt $\Phi \vdash \exists! z\alpha(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner, z)$. Die Existenz folgt aus $(*)$ und die Eindeutigkeit, da α eine Funktion repräsentiert. Demnach ist dann

$$\Phi \vdash \forall z(\alpha(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner, z) \to z = \ulcorner\varphi\urcorner).$$

Mit der Definition von φ folgt dann

$$\Phi \vdash \psi(\ulcorner\varphi\urcorner) \to \underbrace{(\forall z(f(\ulcorner\theta\urcorner, \ulcorner\theta\urcorner) = z \to \psi(z)))}_{\varphi}$$

bzw. $\Phi \vdash \psi(\ulcorner\varphi\urcorner) \to \varphi$.

□

Satz 2.5
Sei $\mathfrak{A}$ eine Struktur deren Universum $\mathbb{N}$ umfasst so, dass $\mathrm{Th}(\mathfrak{A})$ Kodierungen erlaubt. Dann existiert keine Formel $\mathrm{True}_{\mathfrak{A}}(x)$ so, dass für alle ψ gilt: $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{A} \models \mathrm{True}_{\mathfrak{A}}(\ulcorner\psi\urcorner)$.

Beweis. Wir nehmen an $\mathrm{True}_{\mathfrak{A}}(x)$ existiert. Nach dem Fixpunktsatz existiert zu $\neg\,\mathrm{True}_{\mathfrak{A}}(x)$ ein Fixpunkt φ so, dass

$$\mathrm{Th}(\mathfrak{A}) \vdash \varphi \leftrightarrow \neg\,\mathrm{True}_{\mathfrak{A}}(\ulcorner\varphi\urcorner). \qquad (*)$$

Informell „behauptet“ φ, dass φ falsch ist. Nun folgt

$$\mathfrak{A} \models \varphi \overset{(*)}{\Longleftrightarrow} \mathfrak{A} \models \neg\,\mathrm{True}_{\mathfrak{A}}(\ulcorner\varphi\urcorner) \xLeftrightarrow{\text{Def. von True}_{\mathfrak{A}}} \mathfrak{A} \not\models \varphi.$$

Widerspruch! □

Die wahren Sätze von $\mathrm{Th}(\mathfrak{N})$ sind also nicht in $\mathrm{Th}(\mathfrak{N})$ repräsentierbar. Anders formuliert:
Sei T eine repräsentative und vollständige Theorie. Dann ist T nicht in T definierbar. Das heißt es gibt keine Formel $\mathrm{True}_T(x)$ mit

$$\psi \in T \Leftrightarrow \mathrm{True}_T(\ulcorner\psi\urcorner) \in T.$$

Damit folgt wieder der 1. Gödelsche Unvollständigkeitssatz (die genau Definition kann in Satz 2.3 gefunden werden):
Sei T rekursiv axiomatisierbar und repräsentativ. Dann ist T unvollständig. Sonst wäre T entscheidbar und da T repräsentativ ist, wäre die entscheidbare Menge $\{\ulcorner\psi\urcorner : \psi \in T\}$ in T definierbar.

Sei Φ entscheidbar und repräsentativ. Nun nehmen wir uns eine geeignete Kodierung von Ableitungen im Sequenzenkalkül und betrachten $B \subseteq \mathbb{N} \times \mathbb{N}$ mit

$$(n, m) \in B \text{ gdw. } n = \ulcorner\Phi_0 \Rightarrow \psi\urcorner \text{ gültige Sequenz}, \Phi_0 \subseteq \Phi \text{ endlich und } m = \ulcorner\psi\urcorner.$$

B ist entscheidbar, also existiert eine Formel $\mathrm{Beweis}_\Phi(x, y)$ so, dass $\Phi \vdash \mathrm{Beweis}_\Phi(n, m)$ gdw. $(n, m) \in B$. Weiter werden die Formeln $\mathrm{Abl}_\Phi(x) := \exists y\,\mathrm{Beweis}_\Phi(y, x)$ und $\mathrm{Wf}_\Phi := \neg\,\mathrm{Abl}_\Phi(\ulcorner\neg 0 = 0\urcorner)$ definiert. Dabei bezeichnet $\mathrm{Abl}_\Phi(x)$, dass es einen Beweis für x gibt und Wf_Φ drückt die Widerspruchsfreiheit von Φ aus.

Satz 2.6 (2. Gödelscher Unvollständigkeitssatz)
Ist $\Phi \supseteq \Phi_{\mathrm{PA}}$ entscheidbar und konsistent, dann ist $\Phi \nvdash \mathrm{Wf}_\Phi$.

Beweis. Nach dem Fixpunktsatz existiert ein Satz φ mit $\Phi \vdash \varphi \leftrightarrow \neg\,\mathrm{Abl}_\Phi(\ulcorner\varphi\urcorner)$. Ähnlich zum vorherigen Beweis „behauptet" φ seine eigene Unbeweisbarkeit. Nun ist $\Phi \nvdash \varphi$, da sonst eine Ableitung $\Phi_0 \Rightarrow \varphi$ mit endlichem $\Phi_0 \subseteq \Phi$ existiert und somit würde $\Phi \vdash \mathrm{Abl}_\Phi(\ulcorner\varphi\urcorner)$ folgen und damit $\Phi \vdash \neg\varphi$. Also ist $\mathrm{Wf}_\Phi \to \neg\,\mathrm{Abl}_\Phi(\ulcorner\varphi\urcorner)$.

Man kann diesen Beweis in $\Phi \supseteq \Phi_{\mathrm{PA}}$ nachvollziehen und zeigen, dass $\Phi \vdash \mathrm{Wf}_\Phi \to \neg\,\mathrm{Abl}_\Phi(\ulcorner\varphi\urcorner)$. Dies ist aber sehr schwer und technisch, weshalb dies nicht hier vorgeführt werden soll.
Wenn nun aber $\Phi \vdash \mathrm{Wf}_\Phi$ gelten würde, dann auch $\Phi \vdash \neg\,\mathrm{Abl}_\Phi(\ulcorner\varphi\urcorner)$ und damit $\Phi \vdash \varphi$. Widerspruch! □

Aus einem repräsentatives Axiomensystem lässt sich damit also nicht die Widerspruchsfreiheit von diesem folgern. Damit gilt also $\mathrm{ZFC} \nvdash \mathrm{Wf}_{\mathrm{ZFC}}$.

3 Modelltheorie

Nachdem in den letzten Teilen wichtige Konzepte der Mengenlehre und die Gödelschen Unvollständigkeitssätze vermittelt wurden, sollen werden hier nun zentrale Ideen der Modelltheorie gezeigt.

3.1 Erhaltungssätze (Charakterisierungssätze)

Ein wichtiges Ziel der Modelltheorie ist es, einen Zusammenhang zwischen Syntax und Semantik zu bilden. Allgemein lässt sich dies formalisieren: Eine Formel $\psi \in \mathrm{FO}$ hat eine semantische Eigenschaft P gdw. wenn ψ äquivalent zu einer Formel in einem Fragment $F_p \subseteq \mathrm{FO}$ ist.

Beispiele dafür sind der *Satz von Łos-Tarski* und *Satz von Benthem*.

Satz von Łoś-Tarski $\psi \in \mathrm{FO}$ ist erhaltend unter Substrukturen (d.h. wenn $\mathfrak{B} \models \psi$ und $\mathfrak{A} \subseteq \mathfrak{B}$, dann ist auch $\mathfrak{A} \models \psi$) gdw. ψ äquivalent ist zu einer universellen Formel $\forall \bar{x}(\varphi)$, wobei φ quantorenfrei ist.

Satz von van Benthem $\psi(x) \in \mathrm{FO}$ ist invariant unter Bisimulation (d.h. wenn $\mathcal{K} \models \psi(v)$ und $\mathcal{K}, v \sim \mathcal{K}', v'$, dann gilt auch $\mathcal{K}' \models \psi(v')$) gdw. $\psi(x)$ äquivalent zu einer Formel $\psi' \in \mathrm{ML}$ ist.

In beiden Fällen gilt, dass die Richtung von Syntax zur Semantik trivial ist. Beispielsweise ist die Bisimulations-Invarianz von zu einer Modallogischen Formel äquivalenten FO-Formel klar. Die Rückrichtung ist aber alles andere als offensichtlich und wird daher noch genauer in diesem Kapitel betrachtet.

Refresher zur Modallogik

Für eine Formel ψ gilt $\psi \in \mathrm{ML}$ (Modallogik), wenn ψ induktiv definiert ist, durch folgende Grammatik

$$\psi ::= P_i \mid \neg\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid \psi \rightarrow \psi \mid \Diamond\psi \mid \Box\psi.$$

Das Modell einer Modallogischen Formel ist eine Kripkestruktur $\mathcal{K} = (V, (P_i)_{i \in I}, (E_a)_{a \in A})$. Wobei V eine Menge an Knoten, E_a für jedes $a \in A$ eine zweistellige Kantenrelation und P_i für jedes $i \in I$ eine einstellige Relation ist, welche die Eigenschaften von Knoten darstellt.
Semantisch ist ML definiert als

- $\mathcal{K}, v \models P_i$ gdw. $v \in P_i$.
- Die Junktoren $\wedge, \vee, \rightarrow$ sind wie aus AL oder FO bekannt.
- $\mathcal{K}, v \models \Diamond\psi$ genau dann, wenn es ein $w \in vE := \{w : (v, w) \in E\}$ gibt, mit $\mathcal{K}, w \models \psi$.
- $\mathcal{K}, v \models \Box\psi$ genau dann, wenn für alle $w \in vE$ gibt, mit $\mathcal{K}, w \models \psi$.

Die Modallogik lässt sich in die Prädikatenlogik einbetten. Es gibt also eine Abbildung mit $\psi \mapsto \psi^*(x)$, welche wie folgt definiert ist:

- $P_i \mapsto P_i x$
- $\psi_1 \circ \psi_2 \mapsto \psi_1^*(x) \circ \psi_2^*(x)$ für $\circ \in \{\wedge, \vee, \rightarrow\}$
- $\Diamond\psi \mapsto \exists y(Exy \wedge \psi^*(y))$
- $\Box\psi \mapsto \forall y(Exy \rightarrow \psi^*(y))$

Das Bild dieser Abbildung wird als modales Fragment der Prädikatenlogik bezeichnet.
Eine Bisimulation zwischen zwei Kripkestrukturen $\mathcal{K} = (V, (P_i)_{i\in I}, E)$ und $\mathcal{K}' = (V', (P_i')_{i\in I}, E')$ ist eine Relation $Z \subseteq V \times V'$ so, dass für alle $(v, v') \in Z$ gilt:

- $v \in P_i \Leftrightarrow v' \in P_i'$
- Hin: Zu jedem Knoten $w \in vE$ existiert ein $w' \in v'E'$ so, dass $(w, w') \in Z$.
- Her: Zu jedem Knoten $w' \in v'E'$ existiert ein $w \in vE$ so, dass $(w, w') \in Z$,

Es lässt sich erkennen, dass ML Bisimulationsinvariant ist. Das heißt, wenn $\mathcal{K}, v \models \psi$ und $\mathcal{K}, v \sim \mathfrak{K}', v'$, dann ist auch $\mathcal{K}', v' \models \psi$.

Weiter mit Erhaltungssätzen

Definition 3.1 (Existenziell-positiv)
Eine FO-Formel ist *existenziell positiv* (Σ_1^+-Formel), wenn sie weder Allquantoren, noch Negationen oder Implikationen enthält, also aus Atomen mit $\wedge$, $\vee$ und $\exists$ aufgebaut ist.

Definition 3.2 (Existenzielle und universelle Formeln)
Eine FO-Formel ist existenziell (Σ_1-Formel), wenn sie die Form $\exists \bar{x}\varphi$ mit quantorenfreiem φ hat.
Eine FO-Formel ist universell (Π_1-Formel), wenn sie die Form $\forall \bar{x}\varphi$ mit quantorenfreiem φ hat.

Induktiv ist weiter definiert, dass eine Formel ψ eine Σ_{n+1}-Formel ist, wenn $\psi = \exists \bar{x}\varphi$ gilt und φ eine Π_n-Formel ist. Dual ist dies für Π_{n+1}-Formeln definiert. Eine Π_{n+1}-Formel ist von der Form $\forall \bar{x}\varphi$ für ein φ, welches eine Σ_n-Formel ist. Offensichtlich sind diese Formeln in Pränex-Normalform. Auch lässt sich erkennen, dass wenn φ eine Σ_n-Formel ist, $\neg\varphi$ eine Π_n-Formel wird.

Definition 3.3 (Abgeschlossenheit)
Eine Formel $\psi(x)$ ist abgeschlossen unter einer Abbildung $f : \mathfrak{A} \to \mathfrak{B}$, wenn für alle $\bar{a}$ aus $\mathfrak{A}$ gilt $\mathfrak{A} \models \psi(\bar{x}) \Rightarrow \mathfrak{B} \models \psi(f\bar{a})$.

Definition 3.4 (Homomorphismen)
Ein *Homomorphismus* h ist eine Abbildung von $\mathfrak{A}$ nach $\mathfrak{B}$, für welche gilt, wenn $\bar{a} \in R^{\mathfrak{A}}$, dann ist $(h\bar{a}) \in R^{\mathfrak{B}}$ für ein Relationssymbol R und analog für Funktionen.
Weiter ist ein *starker Homomorphismus* ein **injektiver** Homomorphismus h, für den gilt $\bar{a} \in R^{\mathfrak{A}}$ **gdw.** $(h\bar{a}) \in R^{\mathfrak{B}}$. Einen starken Homomorphismus nennt man auch eine *Einbettung.*

Lemma 3.1.1*:* Jede Σ_1^+-Formel bleibt unter Homomorphismen erhalten.

Beweis. Sei $h : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. Zunächst gilt für jeden Term $t(\bar{x})$:

$$h([\![t(\bar{a})]\!]^{\mathfrak{A}}) = [\![t(h\bar{a})]\!]^{\mathfrak{B}}, \tag{$*$}$$

denn:

- $t := x_i$: klar, da beide Seiten den Wert ha_i „erhalten“.
- $t := gt_1 \ldots t_k$: Dann ist

$$\begin{aligned} h[\![t(\bar{a})]\!]^{\mathfrak{A}} &= h(g^{\mathfrak{A}}([\![t_1(\bar{a})]\!]^{\mathfrak{A}}, \ldots, [\![t_k(\bar{a})]\!]^{\mathfrak{A}})) \\ &\overset{h \text{ Hom.}}{=} g^{\mathfrak{B}}(h[\![t_1(\bar{a})]\!]^{\mathfrak{A}}, \ldots, h[\![t_k(\bar{a})]\!]^{\mathfrak{A}}) \\ &\overset{\text{IV.}}{=} g^{\mathfrak{B}}([\![t_1(h\bar{a})]\!]^{\mathfrak{B}}, \ldots, [\![t_k(h\bar{a})]\!]^{\mathfrak{B}}) \\ &= [\![t(h\bar{a})]\!]^{\mathfrak{B}}. \end{aligned}$$

Durch eine Induktion über den Formelaufbau lässt sich dann diese Eigenschaft auch für Formeln ψ feststellen:

- $\psi := t_1(\bar{x}) = t_2(\bar{x})$:

$$\begin{aligned}\mathfrak{A} \models t_1(\bar{a}) = t_2(\bar{a}) &\Longleftrightarrow [\![t_1(\bar{a})]\!]^{\mathfrak{A}} = [\![t_2(\bar{a})]\!]^{\mathfrak{A}} \\ &\Longrightarrow h[\![t_1(\bar{a})]\!]^{\mathfrak{A}} = h[\![t_2(\bar{a})]\!]^{\mathfrak{A}} \qquad (\triangle) \\ &\overset{(*)}{\Longleftrightarrow} [\![t_1(h\bar{a})]\!]^{\mathfrak{B}} = [\![t_2(h\bar{a})]\!]^{\mathfrak{B}} \Leftrightarrow \mathfrak{B} \models t_1(h\bar{a}) = t_2(h\bar{a}).\end{aligned}$$

- $\psi := Rt_1(\bar{x}), \dots, t_k(\bar{x})$:

$$\begin{aligned}\mathfrak{A} \models Rt_1(\bar{a}), \dots, t_k(\bar{a}) &\Longleftrightarrow ([\![t_1(\bar{a})]\!]^{\mathfrak{A}}, \dots, [\![t_k(\bar{a})]\!]^{\mathfrak{A}}) \in R^{\mathfrak{A}} \\ &\overset{h \text{ Hom.}}{\Longrightarrow} (h[\![t_1(\bar{a})]\!]^{\mathfrak{A}}, \dots, h[\![t_k(\bar{a})]\!]^{\mathfrak{A}}) \in R^{\mathfrak{B}} \qquad (\bigcirc) \\ &\overset{(*)}{\Longleftrightarrow} ([\![t_1(h\bar{a})]\!]^{\mathfrak{B}}, \dots, [\![t_k(h\bar{a})]\!]^{\mathfrak{B}}) \in R^{\mathfrak{B}} \Leftrightarrow \mathfrak{B} \models Rt_1(h\bar{a}), \dots, t_k(h\bar{a}).\end{aligned}$$

- Die Fälle $\psi := \varphi \wedge \varphi'$ und $\psi := \varphi \vee \varphi'$ sind klar.
- $\psi := \exists y \varphi(\bar{x}, y)$:

$$\begin{aligned}\mathfrak{A} \models \exists y \varphi(\bar{a}, y) &\Longrightarrow \text{es ex. } b \text{ mit } \mathfrak{A} \models \varphi(\bar{a}, b) \\ &\overset{\text{IV}}{\Longrightarrow} \mathfrak{B} \models \varphi(h\bar{a}, hb) \Rightarrow \mathfrak{B} \models \exists y \varphi(h\bar{a}, y).\end{aligned}$$

□

Lemma 3.1.2*:* Σ_1-Formeln $\psi(\bar{x})$ bleiben unter Einbettung erhalten.

Beweis. Sei h eine Einbettung. Ohne Einschränkung lässt sich voraussetzen, dass $\psi(\bar{x})$ in Negations-NF ist. Nun lässt sich die Behauptung durch eine Induktion über den Formelaufbau wie oben zeigen:

- Für $\psi := t_1 = 2t_2$ oder $\psi := Rt_1, \dots, t_n$ lässt sich dies genauso wie oben zeigen.
- Da h injektiv ist, gilt die Folgerung $(\triangle)$ auch in die andere Richtung. Man erhält also eine Kette an Äquivalenzen. Dadurch lässt sich diese analog auf den hier beschriebenen Fall ψ anwenden.
- Falls $\psi := \neg Rt_1, \dots, t_n$ lässt sich das Argument wie im vorherigen Beweis verwenden. Die Folgerung von $(\bigcirc)$ wird aber eine Äquivalenz, da h ein starker Homomorphismus ist.
- Die Fälle $\psi := \varphi \wedge \varphi'$, $\psi := \varphi \vee \varphi'$ und $\exists y \varphi(\bar{x}, y)$ lassen sich genauso wie oben beweisen.

□

Lemma 3.1.3*:* Π_1-Formeln bleiben unter Substrukturen erhalten.

Beweis. Seien $\mathfrak{A}, \mathfrak{B}$ zwei Strukturen mit $\mathfrak{A} \subseteq \mathfrak{B}$ und $\psi(\bar{x})$ eine Π_1-Formel. Angenommen, es gilt $\mathfrak{A} \models \neg\psi(\bar{a})$ und $\mathfrak{B} \models \psi(\bar{a})$ für $\bar{a}$ aus A. Dann ist $\neg\psi(\bar{x})$ aber äquivalent zu einer Σ_1-Formel. Mit Lemma 3.1.1 folgt aber $\mathfrak{A} \models \neg\psi(\bar{a}) \Rightarrow \mathfrak{B} \models \neg\psi(\bar{a})$. Widerspruch! □

Definition 3.5
Eine Folge $(\mathfrak{A})_{i<\alpha}$ von τ-Strukturen ist eine *Kette*, wenn jeweils $\mathfrak{A}_i \subseteq \mathfrak{A}_j$ für $i < j$. Die Vereinigung $\bigcup_{i<\alpha} \mathfrak{A}_i$ einer solchen Kette ist die Struktur $\mathfrak{A}$ mit Universum $A = \bigcup_{i<\alpha} A_i$ und

- $\bar{a} \in R^{\mathfrak{A}}$ gdw. $\bar{a} \in R^{\mathfrak{A}_i}$ für ein $i < \alpha$ (und daher für alle $j < \alpha$ mit $\bar{a} \in A_j$).
- $f^{\mathfrak{A}}(\bar{a}) = b$ gdw. $f^{\mathfrak{A}_i}\bar{a} = b$ für ein (und dadurch alle) $i < \alpha$ mit $\bar{a} \in A_i$.

$\varphi(x)$ bleibt Erhalten unter Vereinigung von Ketten, wenn für jede Kette $(\mathfrak{A}_i)_{i<\alpha}$ mit $\bar{a} \in A_0$ und $\mathfrak{A}_i \models \varphi(\bar{a})$ für alle i, dann auch $\bigcup_{i<\alpha} \mathfrak{A}_i \models \varphi(\bar{a})$ gilt.
Dies sind nicht aber alle Formeln. Sei bspw. $\mathfrak{A}_i = (\{0, \ldots, i\}, <^{\mathbb{N}})$. Jedes $\mathfrak{A}_i$ hat ein maximales Element, aber $\bigcup \mathfrak{A}_i = (\mathbb{N}, <)$ nicht. Das heißt, es gibt Σ_2-Formeln, welche nicht unter Vereinigung von Ketten erhalten bleiben, in diesem Beispiel die Formel $\exists x \forall y (y \leq x)$.

Lemma 3.1.4*:* Π_2-Formeln bleiben erhalten unter Vereinigung von Ketten.

Beweis. Sei $(\mathfrak{A}_i)_{i<\alpha}$ eine Kette, $\mathfrak{A} := \bigcup_{i<\alpha} \mathfrak{A}_i$ und $\bar{a} \subseteq A_0$. Weiter sei $\forall \bar{y} \varphi(\bar{x}, \bar{y})$ eine Π_2-Formel (also $\varphi(\bar{x}, \bar{y})$ eine Σ_1-Formel) so, dass $\mathfrak{A}_i \models \forall \bar{y} \varphi(\bar{a}, \bar{y})$ für alle $i < \alpha$.

Nun ist zu zeigen, dass $\mathfrak{A} \models \forall \bar{y} \varphi(\bar{a}, \bar{y})$. Angenommen, es existiert ein $\bar{b} \subseteq \mathfrak{A}$ mit $\mathfrak{A} \models \neg\varphi(\bar{a}, \bar{b})$. Da $|\bar{b}|$ endlich ist, existiert ein $j < \alpha$ mit $\bar{b} \subseteq A_j$. Da $\neg\varphi$ äquivalent zu einer Π_1-Formel ist und $\mathfrak{A}_j \subseteq \mathfrak{A}$, folgt wegen Lemma 3.1.3, dass $\mathfrak{A}_j \models \neg\varphi(\bar{a}, \bar{b})$ im Widerspruch zu $\mathfrak{A}_j \models \forall \bar{y} \varphi(\bar{a}, \bar{y})$. □

Definition 3.6 (Expansion um Konstanten)
Sei $\mathfrak{A}$ eine τ-Struktur und $B \subseteq A$. Dann ist $\mathfrak{A}_B$ die Expansion von $\mathfrak{A}$ um je eine Konstante für b für jedes Element $b \in B$.

Definition 3.7 (Elementares Diagramm)
Ist T eine vollständige Theorie und $\mathfrak{A} \models T$, dann ist $T(B) := \mathrm{Th}(\mathfrak{A}_B)$. Im Fall $B = A$ nennen wir $T(A) := \mathrm{Th}(\mathfrak{A}_A)$ das *elementare Diagramm* von $\mathfrak{A}$.

Im Gegensatz dazu ist das Diagramm $D(\mathfrak{A})$ definiert durch

$$D(\mathfrak{A}) := \{\varphi(\bar{a}) \in T(A) : \varphi \text{ atomar oder negiert-atomar}\}.$$

Definition 3.8
$\mathfrak{A}$ ist eine *elementare Substruktur* von $\mathfrak{B}$ ($\mathfrak{A} \preccurlyeq \mathfrak{B}$), wenn $\mathfrak{A} \subseteq \mathfrak{B}$ und für jede Formel $\varphi(\bar{x}) \in \mathrm{FO}$ und alle $\bar{a}$ aus A gilt: $\mathfrak{A} \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{B} \models \varphi(\bar{a})$.

Dies soll durch zwei Beispiele genauer beleuchtet werden.

- $\mathfrak{A} = (\mathbb{Q}, <), \mathfrak{B} = (\mathbb{R}, <)$. Dann lässt sich leicht feststellen, dass $\mathfrak{A} \preccurlyeq \mathfrak{B}$.
- $\mathfrak{A} = (\mathbb{N} \setminus \{0\}, <), \mathfrak{B} = (\mathbb{N}, <)$. Es gilt $\mathfrak{A} \subseteq \mathfrak{B}$ und sogar $\mathfrak{A} \cong \mathfrak{B}$. Aber trotzdem ist $\mathfrak{A} \not\preccurlyeq \mathfrak{B}$. Sei $\varphi(x)$ in einer Struktur wahr, gdw. x das kleinste Element der Struktur ist. Dann ist $\mathfrak{A} \models \varphi(1)$, aber $\mathfrak{B} \not\models \varphi(1)$.

Satz 3.1 (Tarski-Vaught-Test)
Sei $\mathfrak{A} \subseteq \mathfrak{B}$. Nun sind äquivalent:

1. $\mathfrak{A} \preccurlyeq \mathfrak{B}$.
2. Für jede Formel $\varphi(\bar{x}, y)$ und alle $\bar{a}$ aus $\mathfrak{A}$ gilt: $\mathfrak{B} \models \exists y \varphi(\bar{a}, y) \Rightarrow \mathfrak{B} \models \varphi(\bar{a}, a')$ für ein $a' \in A$.

Beweis. 1. $\Rightarrow$ 2.: Sei $\mathfrak{A} \preccurlyeq \mathfrak{B}$ und $\mathfrak{B} \models \exists y \varphi(\bar{a}, y)$. Dann gilt $\mathfrak{A} \models \exists y \varphi(\bar{a}, y)$, das heißt $\mathfrak{A} \models \varphi(\bar{a}, a')$ für ein $a' \in A$. Da $\mathfrak{A} \preccurlyeq \mathfrak{B}$, folgt $\mathfrak{B} \models \varphi(\bar{a}, a')$.

2. $\Rightarrow$ 1.: Das Kriterium des Tests sei erfüllt. Nun ist zu zeigen, dass für jede Formel $\psi(\bar{x})$ und $\bar{a}$ aus $\mathfrak{A}$ gilt: $\mathfrak{A} \models \psi(\bar{a}) \Leftrightarrow \mathfrak{B} \models \psi(\bar{a})$. Dies soll wieder durch eine Induktion über den Formelaufbau passieren.

- Die atomaren Fälle $\psi \coloneqq x = y$ und $\psi \coloneqq R\bar{x}$, als auch die einfachen Induktionsschritte $\psi \coloneqq \neg\varphi$, $\psi \coloneqq \varphi \wedge \varphi'$ und $\psi \coloneqq \varphi \vee \varphi'$ sind klar.
- $\psi \coloneqq \exists y \varphi(\bar{a}, y)$:
  - $\mathfrak{A} \models \exists y \varphi(\bar{a}, y) \Rightarrow \mathfrak{A} \models \varphi(\bar{a}, a')$ für ein $a' \in A \overset{\text{IV}}{\Rightarrow} \mathfrak{B} \models \varphi(\bar{a}, a') \Rightarrow \mathfrak{B} \models \exists y \varphi(\bar{a}, y)$.
  - $\mathfrak{B} \models \exists y \varphi(\bar{a}, y) \overset{\text{Test}}{\Rightarrow} \mathfrak{B} \models \varphi(\bar{a}, a')$ für ein $a' \in A \overset{\text{IV}}{\Rightarrow} \mathfrak{A} \models \varphi(\bar{a}, a') \Rightarrow \mathfrak{A} \models \exists y \varphi(\bar{a}, y)$.

□

Definition 3.9 (Elementare Einbettung)
$f : \mathfrak{A} \to \mathfrak{B}$ ist eine *elementare Einbettung* ($f : \mathfrak{A} \preccurlyeq \mathfrak{B}$), wenn gilt: f ist eine Einbettung und für alle $\varphi(\bar{x}), \bar{a}$: $\mathfrak{A} \models \bar{a} \Leftrightarrow \mathfrak{B} \models \varphi(f\bar{a})$. Es ergibt sich dadurch folgendes Verhalten: $\mathfrak{A} \cong f[\mathfrak{A}] \preccurlyeq \mathfrak{B}$.

Definition 3.10 (Elementare Kette)
Eine Kette $(\mathfrak{A}_i)_{i \in \alpha}$ ist elementar, wenn $\mathfrak{A}_i \preccurlyeq \mathfrak{A}_j$ für $i \leq j$ gilt.

Satz 3.2
Für jede Kette elem. $(\mathfrak{A}_i)_{i \in \alpha}$ gilt $\mathfrak{A}_k \preccurlyeq \bigcup \mathfrak{A}_i$ für alle $k < \alpha$.

Beweis. ohne Beweis. □

Lemma 3.1.5*:* Sei $\mathfrak{A} \subseteq \mathfrak{B}$ und $\mathfrak{B}_A \models \mathrm{Th}(\mathfrak{A}_A) = T(A)$. Dann ist $\mathfrak{A} \preccurlyeq \mathfrak{B}$.

Zur Erinnerung: $T(A)$ ist das elementare Diagramm.

Beweis. Wenn $\mathfrak{A} \models \varphi(\bar{a})$, dann folgt $\varphi(\bar{a}) \in T(A)$ und da $\mathfrak{B}$ Modell von $T(A)$ ist, gilt $\mathfrak{B} \models \varphi(\bar{a})$.
Im Gegensatz ist mit den gleichen Argumenten, sowie der Vollständigkeit von $T(A)$ einsehbar, dass $\mathfrak{A} \not\models \varphi(\bar{a}) \Rightarrow \neg\varphi(\bar{a}) \in T(A) \Rightarrow \mathfrak{B} \not\models \varphi(\bar{a})$ gilt. □

Typen

Definition 3.11
Sei $\mathfrak{A}$ eine τ-Struktur, $B \subseteq A$ und $n \in \mathbb{N}$. Dann ist definiert:

1. Ein *n-Typ* von $\mathfrak{A}$ über B ist eine Menge p von Formeln $\varphi(x_0, \ldots, x_{n-1}) \in \mathrm{FO}(\tau \cup B)$ so, dass $p \cup \mathrm{Th}(\mathfrak{A}_B)$ erfüllbar ist.
2. $\mathrm{tp}_{\mathfrak{A}}(\bar{a}/B) \coloneqq \{\varphi(\bar{x}) \in \mathrm{FO}(\tau \cup B) : \mathfrak{A}_B \models \varphi(\bar{a})\}$.
3. $\mathfrak{A}$ *realisiert* den Typen p über B, wenn ein Tupel $\bar{a}$ aus $\mathfrak{A}$ existiert mit $p \subseteq \mathrm{tp}_{\mathfrak{A}}(\bar{a}/B)$.
4. Ein Typ p über B ist *vollständig*, wenn kein n-Typ q von $\mathfrak{A}$ über B existiert, mit $p \subsetneq q$.
5. Der *Stone-Raum* $S^n(B)$ ist die Menge der vollständigen n-Typen über B.

Zwei Beispiele sollen dies verdeutlichen.

Beispiel 3.1 1. Es sei $\mathfrak{A} = (\omega, s, 0)$, wobei $s(n) \coloneqq n + 1$ die Sukzessor-Funktion ist. Dann ist $S^1(\emptyset) \supseteq \{p_0, p_1, \ldots\} \cup \{p_\infty\}$, mit

- $p_n \coloneqq \mathrm{tp}(n/\emptyset) \models x = \underbrace{ss\cdots s}_{n\text{-mal}}0$ für ein $n \in \mathbb{N}$.
- $p_\infty \models \{x \neq \underbrace{ss\cdots s}_{n\text{-mal}}0 : n \in \omega\}$.

Es lässt sich feststellen, dass p_∞ nicht in $\mathfrak{A}$ realisiert ist. Die Menge $\{x \neq \underbrace{ss\cdots s}_{n\text{-mal}}0 : n \in \omega\} \cup \mathrm{Th}(\omega, s, 0)$ ist aber dennoch erfüllbar. Dies lässt sich mithilfe des Kompaktheitssatzes zeigen. Offensichtlich ist jede endliche Teilmenge erfüllbar, demnach also also auch die gesamte Menge.

2. Als zweites Beispiel soll $\mathfrak{A} = (\mathbb{Q}, <)$ für ein festes, aber beliebiges $A \subseteq \mathbb{Q}$ betrachtet werden. Nun gibt es für ein festes $a \in A$ folgende Typen:

   (a) $p \models x = a$.

   (a^+) $p \models x > b$ für alle $A \ni b \leq a$ und $p \models x < b$ für alle $A \ni b > a$. Die erste Folgerung besagt, dass x größer als alle $b \in A$ ist, welche kleiner-gleich a sind. Insbesondere ist x also größer als a. Die Zweite Formel besagt, dass x kleiner als das nächste $b \in A$ ist, welches größer als a ist. Wenn a' also die nach a nächste Zahl in A ist, ist $x \in (a, a')$. Bzw. *x ist direkt über a*.

   (a^-) Dieser Typ besagt, dass x *direkt unter* a ist und lässt sich analog zu (a^+) darstellen.

   Zusätzlich gibt es noch den Typen $(+\infty)$ mit $p \models x > a$ für alle $a \in A$, sowie den dazu analog definierten Typen $(-\infty)$.

   Falls $A = A_0 \dot\cup A_1$ gilt, A_0 kein größtes, A_1 kein kleinstes Element hat und $a_0 < a_1$ für beliebige $a_0 \in A_0, a_1 \in A_1$ gilt, dann existiert noch der Typ p mit $p \models x > a$ für $a \in A_0$ und $p \models x < a$ für $a \in A_1$.

Lemma 3.1.6*:* Sei $\mathfrak{A}$ eine τ-Struktur, $\mathfrak{B} \subseteq \mathfrak{A}$ und p ein n-Typ über B. Dann gibt es eine elementare Erweiterung $\mathfrak{C} \succcurlyeq \mathfrak{A}$ in der p realisiert ist.

Beweis. Sei $\Phi := p \cup \mathrm{Th}(\mathfrak{A}_A)$. Wenn $\mathfrak{C} \models \Phi$, dann ist $\mathfrak{C} \succcurlyeq \mathfrak{A}$ und es gibt $\bar{c}$ mit $\mathrm{tp}_{\mathfrak{C}}(\bar{c}/A) \supseteq p$. Es muss also gezeigt werden, dass Φ erfüllbar ist. Wegen des Kompaktheitssatzes reicht es zu zeigen, dass jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar ist. Sei also $\Phi_0 := \{\varphi_1, \ldots, \varphi_n\} \subseteq \Phi$.

In Φ_0 können nur endlich viele Konstanten aus B und nur endlich viele Konstanten aus $A \setminus B$ vorkommen. Es gilt also $\bigwedge \Phi_0 = \varphi_1 \wedge \cdots \wedge \varphi_n = \psi(\bar{x}, \bar{b}) \wedge \varphi(\bar{b}, \bar{c})$ mit $\bar{b} \subseteq B, \bar{c} \subseteq A \setminus B$. Die Formel $\psi(\bar{x}, \bar{b})$ entspricht somit den Formeln, die aus p und die Formel $\varphi(\bar{b}, \bar{c})$ denen, die aus $\mathrm{Th}(\mathfrak{A}_A)$ stammen. Es folgt also $\mathfrak{A} \models \varphi(\bar{b}, \bar{c})$ bzw. $\exists \bar{y} \varphi(\bar{b}, \bar{y}) \in \mathrm{Th}(\mathfrak{A}_B)$. Da p ein Typ über B ist, existiert ein Modell $\mathfrak{D}$ von $\psi(\bar{x}, \bar{b}) \wedge \exists \bar{y} \varphi(\bar{b}, \bar{y})$ so, dass also $\mathfrak{D}, \bar{e} \models \psi(\bar{e}, \bar{b}) \wedge \exists \bar{y} \varphi(\bar{b}, \bar{y})$. Wähle nun $\bar{d}$ so, dass $\mathfrak{D} \models \varphi(\bar{d}, \bar{b})$. $\mathfrak{D}$ ist dann ein Modell von Φ_0. Nach dem Kompaktheitssatz muss also auch ein Modell von Φ existieren. $\square$

Satz 3.3 (Amalgamationssatz)
Seien $\mathfrak{B}, \mathfrak{C}$ τ-Strukturen und $\bar{a} \subseteq B, \bar{c} \subseteq C$ Folgen von Elementen mit $(\mathfrak{B}, \bar{a}) \equiv (\mathfrak{C}, \bar{c})$. Dann gibt es eine elementare Erweiterung $\mathfrak{D} \succcurlyeq \mathfrak{B}$ und eine elementare Einbettung $f : \mathfrak{C} \preccurlyeq \mathfrak{D}$ mit $f(c_i) = a_i$ für alle i. Wenn $\langle \bar{a} \rangle_{\mathfrak{B}}$ die von $\bar{a}$ erzeugte Unterstruktur von $\mathfrak{B}$ ist, dann gibt es, da $(\mathfrak{B}, \bar{a}) \equiv (\mathfrak{C}, \bar{c})$, eine Einbettung $g : \langle \bar{a} \rangle_{\mathfrak{B}} \to \mathfrak{C}$ mit $g(\bar{a}) = \bar{c}$. Es ergibt sich ein Zusammenhang wie in Abbildung 6a.

Beweis. Sei $T := \mathrm{Th}(\mathfrak{B}_B) \cup \mathrm{Th}(\mathfrak{C}_C)$. Behauptung: T ist erfüllbar. Sei $T_0 \subseteq T$ endlich und $\varphi(\bar{a}, \bar{c}')$ die Konjunktion der Formeln aus $T_0 \cap \mathrm{Th}(\mathfrak{C}_C)$ mit $\bar{c}' \subseteq C \setminus \bar{a}$.

Wenn T_0 nicht erfüllbar wäre, dann würde $\mathrm{Th}(\mathfrak{B}_B) \models \neg\varphi(\bar{a}, \bar{c}')$ gelten. Da die Konstanten $\bar{c}'$ nicht in B vorkommen folgt $\mathrm{Th}(\mathfrak{B}_B) \models \forall \bar{y} \neg\varphi(\bar{a}, \bar{y})$. Auf Grund der elementaren Äquivalenz folgt aber aus $\mathfrak{B}, \bar{a} \models \forall \bar{y} \neg\varphi(\bar{a}, \bar{y})$, dass $\mathfrak{C}, \bar{a} \models \forall \bar{y} \neg\varphi(\bar{a}, \bar{y})$, was aber im Widerspruch zu $\varphi(\bar{a}, \bar{c}') \in \mathrm{Th}(\mathfrak{C}_C)$ steht. Also ist T_0 erfüllbar und nach dem Kompaktheitssatz ist auch T erfüllbar.

Sei $\mathfrak{D}^+ = (\mathfrak{D}, B^{\mathfrak{D}^+} \cup C^{\mathfrak{D}^+})$ mit $D^+ \models T$. Da $(\mathfrak{D}, B^{\mathfrak{D}^+}) \models \mathrm{Th}(\mathfrak{B}_B)$ kann man annehmen, dass $\mathfrak{D} \succcurlyeq \mathfrak{B}$ und $\bar{b}^{\mathfrak{D}^+} = \bar{b}$ für alle $\bar{b} \subseteq B$.

Setze $f(c) = c^{\mathfrak{D}^+}$ für alle $c \in C$. Da $(\mathfrak{D}, C^{\mathfrak{D}^+}) \models \mathrm{Th}(\mathfrak{C}_C)$ ist $f : C \to D$ eine elementare Einbettung. Schließlich ist $f(a) = a^{\mathfrak{D}^+} = a$ für alle a. □

Daraus ergeben sich auch einige Folgerung:

1. Sei $\mathfrak{B} \equiv \mathfrak{C}$. Dann existiert ein $\mathfrak{D} \succcurlyeq \mathfrak{B}$ mit elementarer Einbettung $f : \mathfrak{C} \preccurlyeq \mathfrak{D}$.
2. Wenn $\mathfrak{A} \preccurlyeq \mathfrak{B}$ und $\mathfrak{A} \preccurlyeq \mathfrak{C}$, dann gilt mit dem Amalgamationssatz ein $\mathfrak{D} \succcurlyeq \mathfrak{B}$ mit einer elementaren Einbettung $f : \mathfrak{C} \preccurlyeq \mathfrak{D}$. Setzt man nun $\mathfrak{C}' := f(\mathfrak{C})$, erhält man einen Zusammenhang wie in Abbildung 6b dargestellt.

(a)
$$\begin{tikzcd}
 & \mathfrak{D} & \\
\mathfrak{B} \arrow[ur, phantom, "\succcurlyeq"] & & \mathfrak{C} \arrow[ul, "f"'] \\
 & \langle\bar{a}\rangle_{\mathfrak{B}} \arrow[ul, phantom, "\preccurlyeq"] \arrow[ur, "g"'] &
\end{tikzcd}$$

(b)
$$\begin{tikzcd}
 & \mathfrak{D} & \\
\mathfrak{B} \arrow[ur, phantom, "\succcurlyeq"] & & \mathfrak{C}' \arrow[ul, phantom, "\preccurlyeq"] \\
 & \mathfrak{A} \arrow[ul, phantom, "\preccurlyeq"] \arrow[ur, phantom, "\succcurlyeq"] &
\end{tikzcd}$$

Abbildung 6: Darstellung des Amalgamationssatzes (a) und dessen Folgerung (b)

Satz 3.4
Zu jeder Struktur $\mathfrak{A}$ existiert eine elementare Erweiterung $\mathfrak{C}$ so, dass jeder Typ p über A in $\mathfrak{C}$ realisiert ist.

Beweis. Sei $(p_\alpha)_{\alpha<\kappa}$ die Aufzählung aller vollständigen Typen über A. Für jedes $\alpha < \kappa$ wählen wir eine elementare Erweiterung $\mathfrak{B}_\alpha \succcurlyeq \mathfrak{A}$ in der p_α realisiert ist. Konstruiere eine elementare Kette $(\mathfrak{C}_\alpha)_{\alpha<\kappa}$ wie folgt:

- $\mathfrak{C}_0 := \mathfrak{A}$.
- $\mathfrak{C}_\lambda := \bigcup_{\alpha<\lambda} C_\alpha$ für Limesordinale λ.
- $\mathfrak{C}_{\alpha+1}$ ist eine elementare Erweiterung von $\mathfrak{C}_\alpha$ mit der elementaren Einbettung $f : \mathfrak{B}_\alpha \preccurlyeq \mathfrak{C}_{\alpha+1}$ so, dass $f(a) = a$ für $a \in A$.

Setze $\mathfrak{C} := \bigcup\limits_{\alpha<\kappa} \mathfrak{C}_\alpha$. $\mathfrak{C}$ ist eine elementare Erweiterung aller C_α und damit auch von $\mathfrak{A}$ und realisiert jeden Typen über A. □

Satz 3.5
Seien $\mathfrak{B}, \mathfrak{C}$ τ-Strukturen und $\bar{a}$ ein Tupel aus B. Zusätzlich sei $f : \langle\bar{a}\rangle_{\mathfrak{B}} \to \mathfrak{C}$ so, dass $\mathfrak{C} \models \varphi(f\bar{a}) \Rightarrow \mathfrak{B} \models \varphi(\bar{a})$ für Σ_1-Formeln $\varphi(\bar{x})$ gilt. Dann existiert eine elementare Erweiterung $\mathfrak{D} \succcurlyeq \mathfrak{B}$ und eine Einbettung $g : \mathfrak{C} \to \mathfrak{D}$ mit $gf\bar{a} = \bar{a}$.

Beweis. Es lässt sich feststellen, dass f eine Einbettung sein muss. Da $\mathfrak{C} \models fa \neq a' \Rightarrow \mathfrak{B} \models a \neq a'$ gilt, muss f injektiv sein und betrachtet man $\mathfrak{C} \models \neg Rf\bar{x} \Rightarrow \mathfrak{B} \models \neg R\bar{a}$ lässt sich feststellen, dass f eine Einbettung ist.

Man nehme nun eine zu $\mathfrak{C}$ isomorphe Struktur $\mathfrak{C}'$ so, dass $f = \mathrm{id}_{\langle\bar{a}\rangle_{\mathfrak{B}}}$ und $B \cap C' = \langle\bar{a}\rangle_{\mathfrak{B}}$ ist. Sei $T = \mathrm{Th}(\mathfrak{B}_B) \cup D(\mathfrak{C}')$. Zur Erinnerung: $D(C')$ ist das atomare Diagramm von C', also die Menge aller atomaren und negiert-atomaren Formeln, die in C' erfüllt sind. Um zu zeigen, dass T erfüllbar ist, soll wieder der Kompaktheitssatz verwendet werden. Sei $T_0 \subseteq T$ also endlich und $\varphi(\bar{a}, \bar{c}')$ die Konjunktion der endlich vielen atomaren bzw. negiert-atomaren Formeln aus $T_0 \cap D(\mathfrak{C}')$ mit $c' \subseteq C' \setminus A$.

Wenn T_0 unerfüllbar wäre, dann würde $\mathrm{Th}(\mathfrak{B}_B) \models \neg\varphi(\bar{a}, \bar{c}')$ gelten. Also $\mathrm{Th}(\mathfrak{B}_B \models \forall\bar{y}\neg\varphi(\bar{a}, \bar{y})$. Daraus folgt $\mathfrak{B}, \bar{a} \models \neg\exists\bar{y}\varphi(\bar{a}, \bar{y})$ und mit der von f geforderten Eigenschaft $\mathfrak{C}', \bar{a} \models \neg\exists\bar{y}\varphi(\bar{a}, \bar{y})$. Dies ist aber ein Widerspruch zu $\varphi(\bar{a}, \bar{c}) \in D(\mathfrak{C}')$.

Der Rest des Beweises verläuft völlig analog zum Beweis des Amalgamationssatzes. □

Aus diesem Satz lässt sich folgern, dass für zwei τ-Strukturen $\mathfrak{B}$ und $\mathfrak{C}$, welche die Eigenschaft erfüllen, dass für beliebige Σ_1-Sätze φ gilt $\mathfrak{C} \models \varphi \Rightarrow \mathfrak{B} \models \varphi$, sich $\mathfrak{C}$ in eine elementare Erweiterung von $\mathfrak{B}$ einbetten lässt.

Definition 3.12
Für Φ sei $\Phi_\forall := \{\varphi \in \Pi_1 : \Phi \models \varphi\}$ und $\Phi_\exists := \{\varphi \in \Sigma_1 : \Phi \models \varphi\}$.

Satz 3.6
Sei $T \subseteq \mathrm{FO}(\tau)$ eine Theorie. Dann gilt $\mathfrak{A} \models T_\forall$ gdw. eine Erweiterung $\mathfrak{B} \supseteq \mathfrak{A}$ existiert, mit $\mathfrak{B} \models T$.

Beweis. $\Leftarrow$: $\mathfrak{B} \supseteq \mathfrak{A}$ mit $\mathfrak{B} \models T$ impliziert $\mathfrak{B} \models T_\forall$ und da Π_1-Formeln unter Substrukturen abgeschlossen sind und $\mathfrak{B} \supseteq \mathfrak{A}$ gilt, folgt $\mathfrak{A} \models T_\forall$.

$\Rightarrow$: Es gelte $\mathfrak{A} \models T_\forall$. Behauptung: es gibt ein Modell $\mathfrak{C}$ von $\mathrm{Th}(\mathfrak{A})_\exists \cup T$. Wenn nicht, dann gibt es eine endliche Teilmenge $\{\varphi_0, \dots, \varphi_{n-1}\} \subseteq \mathrm{Th}(\mathfrak{A})_\exists$, welche zusammen mit T unerfüllbar sind. D.h. $T \models \neg\varphi_0 \wedge \cdots \wedge \neg\varphi_{n-1} =: \psi \in \Pi_1$. Da also $\psi \in T_\forall$ folgt $\mathfrak{A} \models \psi$. Dies steht aber im Widerspruch zu $\mathfrak{A} \models \{\varphi_0, \dots, \varphi_{n-1}\}$. Es existiert also solch ein Modell $\mathfrak{C}$.

Für jeden Σ_1-Satz φ gilt: $\mathfrak{A} \models \varphi \Rightarrow \mathfrak{C} \models \varphi$. Also kann man $\mathfrak{A}$ in eine elementare Erweiterung von $\mathfrak{C}$ einbetten. Es gibt also eine Einbettung f so, dass $f(\mathfrak{A}) \subseteq \mathfrak{D}$ und $\mathfrak{D} \succcurlyeq \mathfrak{C}$ gilt. Es gilt $\mathfrak{D} \models T$. Also existiert ein $\mathfrak{B} \supseteq \mathfrak{A}$ mit $\mathfrak{B} \models T$. □

Satz 3.7 (Łoś-Tarski)
Sei $T \subseteq \mathrm{FO}(\tau)$ eine Theorie und $\Phi \subseteq \mathrm{FO}(\tau)$ eine Satzmenge. Dann sind äquivalent:

1. Wenn $\mathfrak{A}, \mathfrak{B} \models T, \mathfrak{A} \subseteq \mathfrak{B}$ und $\mathfrak{B} \models \Phi$, dann auch $\mathfrak{A} \models \Phi$ (Φ bleibt $\mod T$ unter Substrukturen erhalten).

2. Es gibt eine Satzmenge $\Psi \subseteq \Pi_1$, die nur aus Π_1-Sätzen besteht so, dass für jedes Modell von T gilt: $\mathfrak{A} \models \Phi \Leftrightarrow \mathfrak{A} \models \Psi$ (Auf Modellen von T ist Φ äquivalent zu einer Menge von universellen Sätzen).

Beweis. 2. $\Rightarrow$ *1.*: Diese Richtung lässt sich leicht mithilfe von Lemma 3.1.3 einsehen.

1. $\Rightarrow$ *2.*: Setze $\Psi := (T \cup \Phi)_\forall$ und sei $\mathfrak{A} \models T$. Nun gilt $\mathfrak{A} \models \Psi \overset{\text{Satz 3.6}}{\Longleftrightarrow}$ es ex. $\mathfrak{B} \supseteq \mathfrak{A}$ mit $\mathfrak{B} \models T \cup \Phi$. Mit *1.* folgt dann $\mathfrak{A} \models \Phi$. Also wenn $\mathfrak{A} \models \Phi$ dann auch $\mathfrak{A} \models \Psi$. □

Daraus lässt sich die in der Einleitung bereits geschilderte Aussage des Satzes folgern: $\varphi(\bar{x}) \in \mathrm{FO}(\tau)$ bleibt unter Substrukturen erhalten gdw. $\varphi(\bar{x})$ äquivalent zu einer Formel $\psi(\bar{x}) \in \Pi_1$ ist.

Beweis. Sei $\bar{c}$ ein Tupel von neuen Konstanten. Betrachte die Theorie $T := \{\eta \in \mathrm{FO}(\tau \cup \{\bar{c}\}) :\models \eta\}$ aller Tautologien über der Signatur $\tau \cup \{\bar{c}\}$. Wähle $\Phi = \{\varphi(\bar{c})\}$. Aus dem Satz von Łoś-Tarski folgt, dass $\varphi(\bar{c})$ äquivalent zu einer einer Menge von Ψ von universellen Sätzen ist, also $\Psi \models \varphi(\bar{c})$. Nach dem Kompaktheitssatz existiert eine endliche Teilmenge $\Psi_0 \subseteq \Psi$ so, dass $\Psi_0 \models \varphi(\bar{c})$. Setze $\psi(\bar{c}) := \bigwedge \Psi_0$. Nun ist $\psi(\bar{c}) \equiv \varphi(\bar{c})$, also $\psi(\bar{x}) \equiv \varphi(\bar{x})$. □

Definition 3.13 (κ-Saturiertheit)
Eine Struktur $\mathfrak{A}$ ist *κ-saturiert*, wenn jeder Typ von $\mathfrak{A}$ über B mit $|B| < \kappa$ in $\mathfrak{A}$ realisiert ist.

Satz 3.8
Jede Struktur $\mathfrak{A}$ besitzt eine ω-saturierte elementare Erweiterung $\mathfrak{B} \succcurlyeq \mathfrak{A}$.

Beweis. Wir definieren wieder eine Folge $(\mathfrak{B}_\alpha)_{\alpha<\omega}$ mit

- $\mathfrak{B}_0 := \mathfrak{A}$.
- $\mathfrak{B}_{\alpha+1} \succcurlyeq \mathfrak{B}_\alpha$ so, dass in $\mathfrak{B}_{\alpha+1}$ jeder Typ von $\mathfrak{B}_\alpha$ über eine endlichen Konstantenmenge realisiert ist.

Nun sei $\mathfrak{B} := \bigcup_{\alpha<\omega} \mathfrak{B}_\alpha$. Weiter sei p ein Typ in $\mathfrak{B}$ über einer endlichen Konstantenmenge $C \subseteq B$. Dann ist $C \subseteq B_\alpha$ für ein endliches α. Nach Konstruktion ist p dann in $\mathfrak{B}_{\alpha+1}$ und damit auch $\mathfrak{B}$ realisiert. $\square$

Definition 3.14 (Modales Fragment)
Wir definieren die Abbildung $f : \mathrm{ML} \to \mathrm{FO}$, welche ML-Formeln, in FO-Formeln übersetzt. Diese ist induktiv definiert als:

- $f(P_i) := P_i x$
- $f(\psi_1 \circ \psi_2) := \psi_1^*(x) \circ \psi_2^*(x)$ für $\circ \in \{\wedge, \vee, \to\}$
- $f(\Diamond\psi) := \exists y(Exy \wedge \psi^*(y))$
- $f(\Box\psi) := \forall y(Exy \to \psi^*(y))$

Das *Modale Fragment der Prädikatenlogik* $\mathrm{MF} \subseteq \mathrm{FO}$ ist definiert als $\mathrm{MF} := \{\psi^*(x) : \exists\psi \in \mathrm{ML}(f(\psi) = \psi^*(x))\}$.

Bevor wir nun den Satz von van Benthem beweisen wollen, benötigen wir ein weiteres Hilfslemma, welches eine wichtige Aussage über ML-äquivalente Kripkestrukturen trifft.

Lemma 3.1.7*:* Seien $\mathcal{K}, \mathcal{K}'$ ω-saturiert, mit $\mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'$. Dann ist $\mathcal{K}, v \sim \mathcal{K}', v'$.

Beweis. Sei $Z = \{(u, u') : \mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'\}$. Behauptung: Z ist eine Bisimulation.

Wenn $(u, u') \in Z$, dann ist $\mathcal{K}, u \models P_i \Leftrightarrow \mathcal{K}', u' \models P_i$, für alle $i \in I$.

Hin-Eigenschaft: Sei $(u, w) \in E_a$. Zu zeigen ist, dass es ein w' gibt, mit $(u', w') \in E'_a$ so, dass $(w, w') \in Z$. Wir definieren $p = \{E_a u' x\} \cup \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}, w)$, wobei $\mathrm{Th}_{\mathrm{MF}}(\mathcal{K}, w) := \{\varphi^*(x) \in \mathrm{MF} : \mathcal{K} \models \varphi^*(w)\}$ ist. p ist ein Typ von $\mathcal{K}'$ über $\{u'\}$. Wenn dies nicht der Fall wäre, dann würde ein endliches $\Phi_0 \subseteq \mathrm{Th}_{\mathrm{ML}}(\mathcal{K}, w)$ existieren so, dass $\mathcal{K}' \not\models E_a u' w' \wedge \bigwedge \Phi_0(w')$ für alle w', bzw.

$$\mathcal{K}' \models \forall y \left(E_a u' y \to \neg \bigwedge \Phi_0(y) \right).$$

Da wir aber $\mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$ vorausgesetzt haben, folgt

$$\mathcal{K} \models \forall y \left(E_a u y \to \neg \bigwedge \Phi_0(y) \right),$$

was aber im Widerspruch steht zu $\mathcal{K} \models E_a u w \wedge \bigwedge \Phi_0(w)$.

Also ist p realisiert in $\mathcal{K}'$, das heißt, es gibt ein w' mit $\mathcal{K}' \models p(w')$. Also ist $(u', w') \in E_a$ und $\mathcal{K}, w \equiv_{\mathrm{ML}} K', w'$. Das heißt $(w, w') \in Z$.

Die Her-Eigenschaft lässt sich völlig analog zeigen.

Z ist also eine Bisimulation. Es folgt $\mathcal{K}, v \sim \mathcal{K}', v'$. $\square$

Satz 3.9 (van Benthem)
Es sei $\tau = \{P_i : i \in I\} \cup \{E_a : a \in A\}$, wobei für alle $i \in I$, P_i ein einstelliges und für alle $a \in A$, E_a ein zweistelliges Relationssymbol ist.

Eine Formel $\psi(x) \in \mathrm{FO}(\tau)$ ist invariant unter Bisimulation gdw. $\psi(x)$ äquivalent ist, zu einer Formel $\varphi \in \mathrm{ML}$.

Beweis. $\Leftarrow$: Diese Richtung wurde bereits in MaLo 1 bewiesen.

$\Rightarrow$: Sei $\psi(x)$ invariant unter Bisimulation und $\Phi := \{\varphi(x) \in \mathrm{MF}(\tau) : \psi(x) \models \varphi(x)\}$ die Menge der modalen Folgerungen aus $\psi(x)$. Wir behaupten nun $\Phi \models \psi(x)$. Sobald wir dies gezeigt haben, folgt der Satz von van Benthem. Denn dann gibt es ein endliches $\Phi_0 \subseteq \Phi$ so, dass $\Phi_0 \models \psi(x)$. Setzt man dann $\varphi^*(x) := \bigwedge \Phi_0$ ist φ^* die Übersetzung einer modalen Formel φ. φ ist äquivalent zu $\psi(x)$.
Sei also $\mathcal{K}_0 \models \Phi(v_0)$. Zu zeigen ist, dass $K_0 \models \psi(v_0)$. Wir definieren $\Theta := \{\psi(x)\} \cup \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_0, v_0)$. Θ ist erfüllbar. Ansonsten existieren $\theta_0(x), \dots, \theta_{n-1}(x) \in \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_0, v_0)$ so, dass $\{\psi(x)\} \cup \{\theta_0(x), \dots, \theta_{n-1}(x)\}$ unerfüllbar ist. Also ist

$$\psi(x) \models \neg(\theta_0(x) \wedge \cdots \wedge \theta_{n-1}(x))$$

und damit $\neg(\theta_0(x) \wedge \cdots \wedge \theta_{n-1}(x)) \in \Phi$. Demnach dann

$$\mathcal{K}_0 \models \neg(\theta_0(v_0) \wedge \cdots \wedge \theta_{n-1}(v_0)).$$

Dies ist aber ein Widerspruch zu $\theta_0(x), \dots, \theta_{n-1}(x) \in \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_0, v_0)$.

Es gibt also ein Modell $\mathcal{K}_1, v_1$ von Θ. Seien $\mathcal{K}_0^+ \succcurlyeq \mathcal{K}_0, \mathcal{K}_1^+ \succcurlyeq \mathcal{K}_1$ ω-saturierte Erweiterungen von $\mathcal{K}_0$ bzw. $\mathcal{K}_1$. Weiter ist $\mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_0^+, v_0) = \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_0, v_0) = \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_1, v_1) = \mathrm{Th}_{\mathrm{MF}}(\mathcal{K}_1^+, v_1)$. Mithilfe von Lemma 3.1.7 lässt sich einsehen, dass aus $\mathcal{K}_0^+, v_0 \equiv_{\mathrm{ML}} \mathcal{K}_1^+, v_1$ folgt, dass $\mathcal{K}_0^+, v_0 \sim \mathcal{K}_1^+, v_1$ gilt. Da $\mathcal{K}_1, v_1 \preccurlyeq \mathcal{K}_1^+, v_1$ und $\mathcal{K}_1 \models \psi(v_1)$ folgt $\mathcal{K}_1^+ \models \psi(v_1)$. Wegen der Bisimulationsinvarianz von $\psi(x)$ gilt dann auch $\mathcal{K}_0^+ \models \psi(v_0)$ und da $\mathcal{K}_0, v_0 \preccurlyeq \mathcal{K}_0^+, v_0$ folgt $\mathcal{K}_0 \models \psi(v_0)$. Dies war zu zeigen. □

Mit diesem Satz lässt sich einsehen, dass die Modallogik ML äquivalent zu dem unter Bisimulation abgeschlossenen Fragment der Prädikatenlogik erster Stufe ist. Im Verlauf des Skriptes wird die weitere Modallogik L_μ eingeführt werden. Nun stellt sich die Frage, ob sich auch für diese eine Logik finden lässt, welches Bisimulationsinvariantes Fragment dieser Modallogik entspricht. Mit einem noch komplexeren Beweis als dem, für den Satz von van Benthem lässt sich zeigen, dass genau das für die Monadische Logik zweiter Stufe gilt.

Eine weitere Überlegung ist die, ob die beiden diskutierten Erhaltungssätze auch für endliche Strukturen gelten. Es lässt sich zeigen, dass dies für die meisten Sätze nicht gilt. Eine Ausnahme stellt hier jedoch der Satz von van Benthem dar. Dieser lässt sich auch für endliche Strukturen benutzen. In diesem Fall wird aber ein anderer Beweis benötigt, als wir hier verwendet haben. Beispielsweise wurde mithilfe von ω-saturierten Strukturen argumentiert. Diese sind nach Konstruktion im Allgemeinen nicht endlich Generell lässt sich auch sagen, dass sehr viel kombinatorischer argumentiert werden muss. Sätze wie den Kompaktsheitssatz kann man beispielsweise nicht anwenden. Über Erhaltungssätze soll nun aber genug gesagt sein.

Weiter soll die infinitäre Logik definiert und die aus MaLo 1 bekannten vollständige Ehrenfeucht-Fraïssé-Theorie hergeleitet werden.

3.2 Infintäre Logik und Ehrenfeucht-Fraïssé-Spiele

Definition 3.15
Sei τ eine Signatur und $\kappa \in \mathrm{Cn}^\infty$. Dann ist die infinitäre Logik $\mathrm{L}_{\kappa\omega}$ definiert als

- Jede atomare Formel $\varphi \in \mathrm{FO}(\tau)$ ist in $\mathrm{L}_{\kappa\omega}[\tau]$.
- Für $\varphi \in \mathrm{L}_{\kappa\omega}[\tau]$ sind $\neg\varphi$, $\exists x\varphi$, $\forall x\varphi \in \mathrm{L}_{\kappa\omega}[\tau]$.
- $\Phi \subseteq \mathrm{L}_{\kappa\omega}[\tau]$ sei eine Formel**menge** mit $|\Phi| < \kappa$. Dann sind auch $\bigvee \Phi$ und $\bigwedge \Phi$ Formeln aus $\mathrm{L}_{\kappa\omega}[\tau]$.

Zusammenfassend ist $\mathrm{L}_{\infty\omega}[\tau] \coloneqq \bigcup_{\kappa\in\mathrm{On}} \mathrm{L}_{\kappa\omega}[\tau]$ definiert.

Man kann schnell feststellen, dass $\mathrm{L}_{\omega\omega}[\tau] = \mathrm{FO}(\tau)$ ist.
Um dies besser zu verinnerlichen sollen einige Beispiele erläutert werden:

Beispiel 3.2
- $\varphi_{\text{fin}} \coloneqq \bigvee\{\neg\varphi_{\geq n} : n < \omega\} \in L_{\omega_1\omega}$, mit $\varphi_{\geq n} = \exists x_1 \cdots \exists x_n(\bigwedge_{1\leq i<j\leq n} x_i \leq x_j)$. Zuerst soll bemerkt werden, dass in diesem Kontext die Schreibweise ω_n für $\aleph_n$ verwendet wird. Des Weiteren gilt
$$\mathfrak{A} \models \varphi_{\text{fin}} \Leftrightarrow A \text{ endlich.}$$
- Sei p ein Typ über B mit $|B| < \kappa$. Dann definieren wir $\varphi(\bar{x}) = \bigwedge p$ und es gilt $\mathfrak{A} \models \exists\bar{x}\varphi(\bar{x})$, also ist p realisiert in $\mathfrak{A}$.

Satz 3.10
Der Kompaktheitssatz gilt nicht für $\mathrm{L}_{\kappa\omega}$, wenn $\kappa > \omega$.

Beweis. Sei $\varphi_{\text{fin}} \in \mathrm{L}_{\kappa\omega}$ für $\kappa > \omega$. Dann ist offensichtlich $\Phi = \{\varphi_{\text{fin}}\} \cup \{\varphi_{\geq n} : n \in \omega\}$ unerfüllbar, aber jede endliche Teilmenge ist erfüllbar. □

Definition 3.16 (Quantorenrang)
Der aus FO bekannte *Quantorenrang* soll nun auch für die infinitäre Logik $\mathrm{L}_{\kappa\omega}$ definiert werden. Für $\psi \in \mathrm{L}_{\kappa\omega}$ ist $\mathrm{qr}(\psi) \in \mathrm{On}$ definiert:

- ψ atomar: $\mathrm{qr}(\psi) = 0$
- $\mathrm{qr}(\neg\psi) = \mathrm{qr}(\psi)$
- $\mathrm{qr}(\exists x\psi(x)) = \mathrm{qr}(\forall x\psi(x)) = \mathrm{qr}(\psi) + 1$
- $\mathrm{qr}(\bigvee \Phi) = \mathrm{qr}(\bigwedge \Phi) \coloneqq \sup\{\mathrm{qr}(\varphi) : \varphi \in \Phi\}$

Auch hier sollen wieder Beispiele zum besseren Verständnis angegeben werden:

Beispiel 3.3
- $\mathrm{qr}(\varphi_{\text{fin}}) = \sup\{\mathrm{qr}(\varphi_{\geq n}) : n < \omega\} = \omega$.
- Sei $\varphi(x) \in L_{\omega_1\omega}(<)$ die Formel, die aussagt, dass x nur endlich viele Vorgänger besitzt. Dann ist $\mathrm{qr}(\varphi(x)) = \omega$ und $\mathrm{qr}(\forall x\varphi(x)) = \omega + 1$.

Definition 3.17 (Äquivalenzen)
Wir schreiben $\mathfrak{A} \equiv_\alpha \mathfrak{B}$, wenn für alle $\varphi \in \mathrm{L}_{\infty\omega}$ mit $\mathrm{qr}(\varphi) \leq \alpha$ gilt: $\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi$.
Analog sei $\mathfrak{A} \equiv_\infty \mathfrak{B}$, wenn für alle $\varphi \in \mathrm{L}_{\infty\omega}$ gilt $\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi$.

Definition 3.18 (Lokaler Isomorphismus)
Ein *lokaler Isomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$, für relationale Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ ist eine Abbildung p mit $\mathrm{Def}(p) \subseteq A, \mathit{Bild}(p) \subseteq B$ so, dass $p = \emptyset$ oder $p : \mathfrak{A}|_{\mathrm{Def}(p)} \xrightarrow{\sim} \mathfrak{B}|_{\mathit{Bild}(p)}$. p wird dann auch partieller Isomorphismus genannt.

$\mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ beschreibt die Menge aller lokalen Isomorphismen von $\mathfrak{A}$ nach $\mathfrak{B}$.

Um lokale Isomorphismen zu notieren werden zwei Notationen verwendet. Seien $\bar{a} = (a_1, a_2, \ldots, a_n)$ und $\bar{b} = (b_1, b_2, \ldots, b_n)$ so, dass $a_i \in A, b_i \in B$ für $1 \leq i \leq n$. Dann sind $p : \bar{a} \mapsto \bar{b}$ und $p = \{(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)\}$ zwei Notationen für den Isomorphismus p.

Spiele

Nun wollen wir Ehrenfeucht-Fraïssé-Spiele für infinitäre Logiken genauer betrachten.

Definition 3.19 (Ehrenfeucht-Fraïssé-Spiele)
Ein EF-*Spiel* $G_\alpha(\mathfrak{A}, \mathfrak{B})$ wird von zwei Spielern gespielt. Dem *Herausforderer (I)* und der *Duplikatorin (II)*.

Eine *Position* ist ein Tupel $(\beta, \mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$, mit $\beta \leq \alpha$, $\bar{a} \subseteq A$, $\bar{b} \subseteq B$ und $|\bar{a}| = |\bar{b}|$. Die Startposition ist das Tupel $(\alpha, \mathfrak{A}, \langle\rangle, \mathfrak{B}, \langle\rangle)$.

Des weiteren soll nun ein *Zug* von der Position $(\beta, \mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ aus beschrieben werden: I wählt ein $\gamma < \beta$ und ein $c \in A$ oder $d \in B$. Dann wählt II aus der jeweils anderen Struktur ein $d \in B$ oder $c \in A$. Die neue Position ist dann $(\gamma, \mathfrak{A}, \bar{a}c, \mathfrak{B}, \bar{b}d)$.

Wird eine Position $(\beta, \mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ erreicht so, dass $\bar{a} \mapsto \bar{b} \notin \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$, dann hat I gewonnen, andernfalls endet das Spiel in einer Position $(0, \mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ mit $\bar{a} \mapsto \bar{b} \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$. Dann hat II gewonnen.

Zur Vereinfachung sagen wir „I/II gewinnt $G_\alpha(\mathfrak{A}, \mathfrak{B})$" für „I/II hat eine Gewinnstrategie für $G_\alpha(\mathfrak{A}, \mathfrak{B})$".

Definition 3.20 (Unendliches EF-Spiel)
Zusätzlich zu dem Spiel $G_\alpha(\mathfrak{A}, \mathfrak{B})$ gibt es das Spiel $G_\infty(\mathfrak{A}, \mathfrak{B})$. Dieses verhält sich genauso wie das erstere, bloß wird die erste Komponente der Position weggelassen so, dass Partien unendlich lange dauern können. Unendliche Partien sind von II gewonnen.

Definition 3.21 (Hin- und Her-Eigenschaft)
Sei $I \subseteq \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ und $p \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$. Dann sagen wir p hat die *Hin- und Her-Eigenschaft (HHE)* bzgl. I, wenn gilt:

- Hin: $\forall a \in A \exists b \in B (p \cup \{(a, b)\} \in I)$
- Her: $\forall b \in B \exists a \in A (p \cup \{(a, b)\} \in I)$

Definition 3.22 (Hin- und Her-System)
Ein Hin- und Her-System $(I_\alpha(\mathfrak{A}, \mathfrak{B}))_{\alpha \in On}$ zu $\mathfrak{A}$ nach $\mathfrak{B}$ besteht aus der Folge von Mengen $I_\alpha(\mathfrak{A}, \mathfrak{B}) \subseteq \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$, welche wie folgt definiert ist:

- $I_0(\mathfrak{A}, \mathfrak{B}) := \{p \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B}) : p \text{ endlich}\}$
- $I_{\alpha+1} := \{p \in I_\alpha(\mathfrak{A}, \mathfrak{B}) : p \text{ hat die HHE bzgl. } I_\alpha(\mathfrak{A}, \mathfrak{B})\}$
- $I_\delta(\mathfrak{A}, \mathfrak{B}) := \bigcap_{\alpha < \delta} I_\alpha(\mathfrak{A}, \mathfrak{B})$ für ein Limesordinal δ.

Ein HHE-System ist also eine absteigende Kette der Form $I_0(\mathfrak{A}, \mathfrak{B}) \supseteq I_1(\mathfrak{A}, \mathfrak{B}) \supseteq \cdots \supseteq I_\alpha(\mathfrak{A}, \mathfrak{B}) \supseteq I_{\alpha+1}(\mathfrak{A}, \mathfrak{B}) \supseteq \cdots$. Auch lässt sich feststellen, dass es ein α gibt so, dass $I_\alpha(\mathfrak{A}, \mathfrak{B}) = I_{\alpha+1}(\mathfrak{A}, \mathfrak{B})$ Wir definieren dann $I_\infty := I_\alpha(\mathfrak{A}, \mathfrak{B})$. Weiter gilt für alle $p \in I_\alpha(\mathfrak{A}, \mathfrak{B})$ und $q \subseteq p$, dass auch $q \in I_\alpha(\mathfrak{A}, \mathfrak{B})$, woraus auch folgt, dass $I_\alpha(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$ genau dann ist, wenn $\emptyset \in I_\alpha(\mathfrak{A}, \mathfrak{B})$.

Definition 3.23
Um die Notation zu vereinfachen, führen wir folgende Schreibweisen ein:

- $\mathfrak{A} \cong_\alpha \mathfrak{B} :\Leftrightarrow I_\alpha(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$
- $\mathfrak{A} \cong_\infty \mathfrak{B} :\Leftrightarrow I_\infty(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$

Lemma 3.2.1*:* $\mathfrak{A} \cong_\infty \mathfrak{B}$ ist genau dann, wenn eine nicht leere Menge $I \subseteq \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ existiert so, dass jedes $p \in I$ die HHE bzgl. I besitzt.

Beweis. $\Rightarrow$: Setze $I = I_\infty(\mathfrak{A}, \mathfrak{B})$.

$\Leftarrow$: Sei $J := \{p \in I_0(\mathfrak{A}, \mathfrak{B}) : p \subseteq q$ für $q \in I\}$. Dann ist $J \neq \emptyset$ und $J \subseteq I_0(\mathfrak{A}, \mathfrak{B})$. Nun hat jedes $p \in J$ die HHE bzgl. I und somit bzgl. jedem $J' \supseteq J$. Daraus folgt direkt $J \subseteq I_\alpha(\mathfrak{A}, \mathfrak{B})$ für jedes Ordinal α. Also $J \subseteq I_\infty(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$. Also gilt $\mathfrak{A} \cong_\infty \mathfrak{B}$. □

Mithilfe von Beispielen sollen HHE-Systeme nun genauer erläutert werden.

Beispiel 3.4 a) Sei $\mathfrak{A} = (\mathbb{Z}, <)$ und $\mathfrak{B} = (\mathbb{Q}, <)$. Dann ist

- $I_0(\mathfrak{A}, \mathfrak{B}) = \{\bar{a} \mapsto \bar{b} : \bar{a}, \bar{b} \text{endlich}, a_i < a_k \Leftrightarrow b_i < b_k \, \forall i, k\}$
- $I_1(\mathfrak{A}, \mathfrak{B}) = \{\bar{a} \mapsto \bar{b} \in I_0(\mathfrak{A}, \mathfrak{B}) : |a_i - a_k| \geq 2 \text{ für } a_i \neq a_k\}$
- $I_2(\mathfrak{A}, \mathfrak{B}) = \{\emptyset\}$
- $I_3(\mathfrak{A}, \mathfrak{B}) = \emptyset$

b) Sei dagegen nun $\mathfrak{C} = (\mathbb{Q}, <)$ und $\mathfrak{D} = (\mathbb{R}, <)$. Dann ist

- $I_0(\mathfrak{C}, \mathfrak{D}) = I_0(\mathfrak{A}, \mathfrak{B})$
- $I_1(\mathfrak{C}, \mathfrak{D}) = I_0(\mathfrak{C}, \mathfrak{D}) = I_\infty(\mathfrak{C}, \mathfrak{D})$

Lemma 3.2.2*:* Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, $\bar{a}, \bar{b}$ Tupel aus A bzw. B und $\alpha \in On$. Dann gilt:
II gewinnt $G_\alpha(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ gdw. $\bar{a} \mapsto \bar{b} \in I_\alpha(\mathfrak{A}, \mathfrak{B})$.

Beweis. Dies soll durch eine Induktion bewiesen werden. $\alpha = 0$: II gewinnt $G_0(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b}) \Leftrightarrow \bar{a} \mapsto \bar{b} \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B}) \Leftrightarrow \bar{a} \mapsto \bar{b} \in I_0(\mathfrak{A}, \mathfrak{B})$.

$\alpha = \beta + 1$:

$$\begin{aligned}
&\text{II gewinnt } G_\alpha(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b}) \\
\Leftrightarrow &(\forall c \in A)(\exists d \in B)\text{II gewinnt } G_\beta(\mathfrak{A}, \bar{a}c, \mathfrak{B}, \bar{b}d) \wedge (\forall d \in B)(\exists c \in A)\text{II gewinnt } G_\beta(\mathfrak{A}, \bar{a}c, \mathfrak{B}, \bar{b}d) \\
\overset{\text{IV}}{\Leftrightarrow} &(\forall c \in A)(\exists d \in B)\bar{a}c \mapsto \bar{b}d \in I_\beta(\mathfrak{A}, \mathfrak{B}) \wedge (\forall d \in B)(\exists c \in A)\bar{a}c \mapsto \bar{b}d \in I_\beta(\mathfrak{A}, \mathfrak{B}) \\
\Leftrightarrow &\bar{a} \mapsto \bar{b} \text{ hat HHE bzgl. } I_\beta(\mathfrak{A}, \mathfrak{B}) \\
\Leftrightarrow &\bar{a} \mapsto \bar{b} \in I_\alpha(\mathfrak{A}, \mathfrak{B}).
\end{aligned}$$

α Limesordinal:

$$\begin{aligned}
&\text{II gewinnt } G_\alpha(\mathfrak{A}, \mathfrak{B}) \\
\Leftrightarrow &\text{II gewinnt } G_\beta(\mathfrak{A}, \mathfrak{B}) \forall \beta < \alpha \\
\overset{\text{IV}}{\Leftrightarrow} &\bar{a} \mapsto \bar{b} \in I_\beta(\mathfrak{A}, \mathfrak{B}) \forall \beta < \alpha \\
\Leftrightarrow &\bar{a} \mapsto \bar{b} \in I_\alpha(\mathfrak{A}, \mathfrak{B}).
\end{aligned}$$

□

Aus diesem Ergebnis lässt sich dann auch leicht folgern, dass $\mathfrak{A} \cong_\alpha \mathfrak{B}$ genau dann ist, wenn II $G_\alpha(\mathfrak{A}, \mathfrak{B})$ gewinnt.

Satz 3.11
Zu einer Struktur $\mathfrak{A}$, $\bar{a} \in A^n$, $\alpha \in On$ existiert, $\psi^\alpha_{\mathfrak{A},\bar{a}} \in \mathrm{L}_{\infty\omega}$ mit $\mathrm{qr}(\psi^\alpha_{\mathfrak{A},\bar{a}}) = \alpha$ und $\mathfrak{B} \models \psi^\alpha_{\mathfrak{A},\bar{a}}(\bar{b}) \Leftrightarrow \bar{a} \mapsto \bar{b} \in I_\alpha(\mathfrak{A}, \mathfrak{B})$.

Beweis.
- $\alpha = 0$: $\psi^0_{\mathfrak{A},\bar{a}}(\bar{x}) := \bigwedge\{\varphi(\bar{x}) : \varphi \text{ quantorenfrei}, \mathfrak{A} \models \varphi(\bar{a})\}$.

- $\alpha = \beta + 1$: $\psi^\alpha_{\mathfrak{A},\bar a} \coloneqq \bigwedge\{\exists y \psi^\beta_{\mathfrak{A},\bar a c}(\bar x, y) : c \in A\} \wedge \forall y \bigvee\{\psi^\beta_{\mathfrak{A},\bar a}(\bar x, y) : c \in A\}$.

  Es gilt $\mathrm{qr}(\psi^\alpha_{\mathfrak{A},\bar a}) = \mathrm{qr}(\psi^\beta_{\mathfrak{A},\bar a}(\bar x, y)) + 1 = \beta + 1 = \alpha$ und

$$\begin{aligned}
&\mathfrak{B} \models \psi^\alpha_{\mathfrak{A},\bar a}(\bar b)\\
\Leftrightarrow& \forall c \in A \exists d \in B(\mathfrak{B} \models \psi^\beta_{\mathfrak{A},\bar a c}(\bar b, d)) \text{ und } \forall d \in B \exists c \in A(\mathfrak{B} \models \psi^\beta_{\mathfrak{A},\bar a c}(\bar b, d))\\
\Leftrightarrow& \forall c \in A \exists d \in B(\bar a c \mapsto \bar b d \in I_\beta(\mathfrak{A}, \mathfrak{B})) \text{ und } \forall d \in B \exists c \in A(\bar a c \mapsto \bar b d \in I_\beta(\mathfrak{A}, \mathfrak{B}))\\
\Leftrightarrow& \bar a \mapsto \bar b \in I_\alpha(\mathfrak{A}, \mathfrak{B}).
\end{aligned}$$

- α Limesordinal: $\psi^\alpha_{\mathfrak{A},\bar a} \coloneqq \bigwedge\{\psi^\beta_{\mathfrak{A},\bar a}(\bar x)\beta < \alpha\}$

  Außerdem ist $\mathrm{qr}(\psi^\alpha_{\mathfrak{A},\bar a}(\bar x)) = \sup\{\psi^\beta_{\mathfrak{A},\bar a} : \beta < \alpha\} = \sup\{\beta : \beta < \alpha\} = \alpha$ und

$$\begin{aligned}
&\mathfrak{B} \models \psi^\alpha_{\mathfrak{A},\bar a}(\bar b)\\
\Leftrightarrow& \mathfrak{B} \models \psi^\beta_{\mathfrak{A},\bar a}(\bar b) \quad \forall \beta < \alpha\\
\Leftrightarrow& \bar a \mapsto \bar b \in I_\beta(\mathfrak{A}, \mathfrak{B}) \quad \forall \beta < \alpha\\
\Leftrightarrow& \bar a \mapsto \bar b \in I_\alpha(\mathfrak{A}, \mathfrak{B}).
\end{aligned}$$

□

Daraus folgt dann für endliche τ, $\alpha < \omega$ und $n \in \omega$

a) $\psi^\alpha_{\mathfrak{A},\bar a}(\bar x) \in \mathrm{FO}(\tau)$

b) Bis auf logische Äquivalenz gibt es *(bei festem τ, α und n, doch bel. $\mathfrak{A}$, $\bar a$)* nur endlich viele verschiedene Formeln $\psi^\alpha_{\mathfrak{A},\bar a}(\bar x)$.

Beweis. Sei $\alpha = 0$: Also gibt es zu endlichem τ und n nur endlich viele atomare τ-Formeln $\varphi(x_1, \dots, x_n)$ und damit auch nur endlich viele quantorenfreie Formeln.

Da a), b) für ein α gilt, folgt $\psi^{\alpha+1}_{\mathfrak{A},\bar a}(\bar x) \in \mathrm{FO}$, es folgt, dass es nur endlich viele Formeln gibt. □

Lemma 3.2.3*:* Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, $\bar a \in A^n$, $\bar b \in B^n$ und $\psi(\bar x) \in \mathrm{L}_{\infty\omega}[\tau]$ mit $\mathrm{qr}(\psi) \le \alpha$ so, dass $\mathfrak{A} \models \psi(\bar a)$ und $\mathfrak{B} \models \neg\psi(\bar b)$. Dann gewinnt I $G_\alpha(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$.

Beweis. Wir wollen dies durch eine Induktion über den Formelaufbau beweisen. Dafür nehmen wir ohne Beschränkung an, dass ψ in Negations-Normalform ist.

Sei ψ atomar oder negiert-atomar: Da $\mathfrak{A} \models \psi(\bar a)$ und $\mathfrak{B} \models \neg\psi(\bar b)$ ist $\bar a \mapsto \bar b \notin \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$, also gewinnt I $G_0(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$.

Sei $\psi = \bigwedge \Phi$: Also ex. $\varphi \in \Phi$ mit $\mathfrak{A} \models \varphi(\bar a)$ und $\mathfrak{B} \models \neg\varphi(\bar b)$. Da $\mathrm{qr}(\varphi) = \beta \le \alpha$ folgt nach IV, dass I das Spiel $G_\beta(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$ und damit auch $G_\alpha(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$.

$\psi = \bigvee \Phi$ ist genau analog.

Sei $\psi = \exists x\varphi$: Es gibt also ein $c \in A$ mit $\mathfrak{A} \models \varphi(\bar a, c)$ und für alle $b \in B$ gilt $\mathfrak{B} \models \neg\varphi(\bar b, d)$. Sei $\mathrm{qr}(\varphi) = \beta < \alpha$. Nach IV gewinnt dann I das Spiel $G_beta(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$. Also gewinnt I das Spiel $G_\alpha(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$ durch Wahl von c.

Sei $\psi = \forall x\varphi$: Es gibt also ein $d \in B$ mit $\mathfrak{B} \models \neg\varphi(\bar d)$, aber für alle $c \in A$ gilt $\mathfrak{A} \models \varphi(\bar a, c)$. I gewinnt $G_\alpha(\mathfrak{A}, \bar a, \mathfrak{B}, \bar b)$ durch Wahl von $d \in B$. □

Satz 3.12 (Ehrenfeucht, Fraïssé)
Es sind äquivalent:

a) 1. $\mathfrak{A} \equiv_\alpha \mathfrak{B}$

2. $\mathfrak{A} \cong_\alpha \mathfrak{B}$

3. II gewinnt $G_\alpha(\mathfrak{A}, \mathfrak{B})$

bzw.

b) 1. $\mathfrak{A} \equiv_\infty \mathfrak{B}$

2. $\mathfrak{A} \cong_\infty \mathfrak{B}$

3. II gewinnt $G_\infty(\mathfrak{A}, \mathfrak{B})$

Beweis. a): *2.* $\Leftrightarrow$ *3.*: Dies wurde bereits in Lemma 3.2.2 gezeigt.

3. $\Rightarrow$ *1.*: Sei $\mathfrak{A} \not\equiv_\alpha \mathfrak{B}$. Dann existiert ein $\psi \in \mathrm{L}_{\infty\omega}$ mit $\mathrm{qr}(\psi) = \alpha$, $\mathfrak{A} \models \psi$ und $\mathfrak{B} \models \neg\psi$. Also gewinnt I das Spiel $G_\alpha(\mathfrak{A}, \mathfrak{B})$.

1. $\Rightarrow$ *2.*: Betrachte $\psi^\alpha_\mathfrak{A}$. Da $\mathfrak{A} \models \psi^\alpha_\mathfrak{A}$, $\mathrm{qr}(\psi^\alpha_\mathfrak{A}) = \alpha$ und $\mathfrak{A} \equiv_\alpha \mathfrak{B}$ folgt $\mathfrak{B} \models \psi^\alpha_\mathfrak{A}$. Also $\emptyset \in I_\alpha(\mathfrak{A}, \mathfrak{B})$ bzw. $I_\alpha(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$ und es gilt $\mathfrak{A} \cong_\alpha \mathfrak{B}$.

b): *2.* $\Rightarrow$ *3.*: Sei $\bar{a} \mapsto \bar{b} \in I_\infty(\mathfrak{A}, \mathfrak{B})$. Wenn I ein $c \in A$ (oder $d \in B$) wählt, kann II ein $d \in B$ (oder $c \in A$) wählen so, dass $\bar{a}c \mapsto \bar{b}d \in I_\infty(\mathfrak{A}, \mathfrak{B})$. Auf diese Weise kann II unbegrenzt weiter spielen.

3. $\Rightarrow$ *1.*: Sei $\mathfrak{A}, \bar{a} \not\equiv_\alpha \mathfrak{B}, \bar{b}$. Also existiert ein $\psi(\bar{x}) \in \mathrm{L}_{\infty\omega}$ mit $\mathfrak{A} \models \psi(\bar{a})$ und $\mathfrak{B} \models \neg\psi(\bar{b})$. Sei $\alpha = \mathrm{qr}(\psi)$. Dann gewinnt I $G_\alpha(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ und damit auch $G_\infty(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$.

1. $\Rightarrow$ *2.*: Sei $\kappa > \max(|A|, |B|)$. Dann ist $I_\kappa(\mathfrak{A}, \mathfrak{B}) = I_\infty$, da $|I_0(\mathfrak{A}, \mathfrak{B})| < \kappa$. Wegen $\mathfrak{A}, \bar{a} \equiv_\infty \mathfrak{B}, \bar{b}$ folgt $\mathfrak{A}, \bar{a} \equiv_\kappa \mathfrak{B}, \bar{b}$ und damit $\bar{a} \mapsto \bar{b} \in I_\kappa(\mathfrak{A}, \mathfrak{B}) = I_\infty(\mathfrak{A}, \mathfrak{B})$ womit dann $\mathfrak{A}, \bar{a} \cong_\infty \mathfrak{B}, \bar{b}$ gilt. $\square$

Axiomatisierbarkeit von Wohlordnungen

Definition 3.24 (Die Klasse WO)
Die Klasse WO ist definiert als $\mathrm{WO} := \{(A, <) : (A, <) \text{ is eine Wohlordnung}\}$.

Es ist bekannt, dass Wohlordnungen nicht in FO axiomatisierbar sind. Betrachtet man beispielsweise die Strukturen $\mathfrak{A} = (\omega, <)$ und $\mathfrak{B} = (\omega, <) + (\mathbb{Z}, <)$ erkennt man, dass $\mathfrak{A} \equiv_\omega \mathfrak{B}$ gilt, obwohl $\mathfrak{A} \in \mathrm{WO}$ und $\mathfrak{B} \notin \mathrm{WO}$ ist.

Nach den eben getroffenen Erkenntnissen stellt sich nun die Frage: Reicht $\mathrm{L}_{\infty\omega}$ aus, um Wohlordnungen zu axiomatisieren?

Lemma 3.2.4*:* Für jede Ordinalzahl α existiert ein $\varphi_\alpha \in \mathrm{L}_{|\alpha|^+\omega}$ mit $\mathrm{qr}(\varphi_\alpha) = \alpha + 1$ so, dass $(A, <) \models \varphi_\alpha \Leftrightarrow (A, <) \cong (\alpha, <)$.

Beweis. Für $\alpha = 0$ lässt sich die Formel $\varphi_0 := \neg\exists x(x = x)$ aufstellen.

Sei nun also $\alpha > 0$. Dann ist

$$\varphi_\alpha := \forall x \bigvee_{\beta<\alpha} \varphi_\beta^{(x)} \wedge \bigwedge_{\beta<\alpha} \exists x \varphi_\beta^{(x)}.$$

Dabei ist $\varphi_\beta^{(x)}$ die Relativierung von φ_β auf $\{y : y < x\}$. Das heißt $\exists u\theta(u)$ wird durch $\exists u(u < x \wedge \theta(u))$ ersetzt, und analog für $\forall u\theta(u)$.

Nun gilt:

$$\begin{aligned}(A,<) \models \varphi_\alpha \Leftrightarrow & \forall a \in A \exists \beta < \alpha (\{b : b < a\}, <) \models \varphi_\beta \\ & \text{und } \forall \beta < \alpha \exists a \in A (\{b : b < a\}, <) \models \varphi_\beta \\ \Leftrightarrow & \forall a \in A \exists \beta < \alpha (\{b : b < a\}, <) \cong (\beta, <) \\ & \text{und } \forall \beta < \alpha \exists a \in A (\{b : b < a\}, <) \cong (\beta, <) \\ \Leftrightarrow & (A,<) \cong (\alpha, <)\end{aligned}$$

□

Eine Idee die man nun bekommen kann, um WO zu axiomatisieren wäre die Formel $\psi = \bigwedge\{\varphi_\alpha : \alpha \in \mathrm{On}\}$ zu benutzen. Dies ist aber nicht möglich, da sich $\{\varphi_\alpha : \alpha \in \mathrm{On}\}$ eine echte Klasse ist, welche in $\mathrm{L}_{\omega\omega}$ nicht wie eine Menge verwendet werden kann.

Satz 3.13
Zu jedem $\alpha \in \mathrm{On}$ existiert ein $\delta > \alpha$ so, dass $\underbrace{(\delta, <)}_{\in \mathrm{WO}} \equiv_\alpha \underbrace{(\delta, <) + (\mathbb{Z}, <) \cdot (\delta, <)}_{\notin \mathrm{WO}}$.

Beweis. Der Beweis kann im Vorlesungsskript nachgelesen werden. □

Satz 3.14
WO ist nicht $\mathrm{L}_{\infty\omega}$-axiomatisierbar.

Satz 3.15
Angenommen $\psi \in \mathrm{L}_{\infty\omega}$ axiomatisiere WO und $\alpha := \mathrm{qr}(\psi)$. Für ein geeignetes $\delta > \alpha$ gilt dann aber $\mathrm{WO} \ni (\delta, <) \models \psi$ und $\mathrm{WO} \not\ni (\delta, <) + (\mathbb{Z}, <) \cdot (\delta, <) \models \psi$. Widerspruch.

Satz 3.16
Seien $\mathfrak{A}, \mathfrak{B}$ Strukturen mit $\mathfrak{A} \cong_\infty \mathfrak{B}$ und A, B abzählbar. Dann ist $\mathfrak{A} \cong \mathfrak{B}$.

Beweis. Wähle Aufzählung $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ aller Elemente von $\mathfrak{A}$ bzw. $\mathfrak{B}$. Wir konstruieren nun eine Folge $(p_n)_{n\in\mathbb{N}}$ von lokalen Isomorphismen $p_n \in I_\infty(\mathfrak{A}, \mathfrak{B})$:

- $p_0 := \emptyset \in I_\infty(\mathfrak{A}, \mathfrak{B})$.
- Da p_n die HHE bzgl. $I_\infty(\mathfrak{A}, \mathfrak{B})$ besitzt, gibt es ein $b \in B$ so, dass $p_n \cup \{(a_n, b)\} \in I_\infty(\mathfrak{A}, \mathfrak{B})$ und es existiert ein $a \in A$ mit $p_n \cup \{(a, b_n)\} \in I_\infty(\mathfrak{A}, \mathfrak{B})$. Somit ist dann $p_{n+1} := p_n \cup \{(a_n, b)\} \cup \{(a, b_n)\}$.

Nun ist für alle $n < \omega$ $\{a_0, \dots, a_{n-1}\} \subseteq \mathrm{Def}(p_n)$ und $\{b_0, \dots, b_{n-1}\} \subseteq \mathrm{Bild}(p_n)$. Setzt man nun $p := \bigcup_{n\in\mathbb{N}} p_n$ erhält man einen lokalen Isomorphismus $p : A \to B$ von $\mathfrak{A}$ nach $\mathfrak{B}$ mit $\mathrm{Def}(p) = A$ und $\mathrm{Bild}(p) = B$, also einen Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$. □

Satz 3.17
Für ω-saturierte Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ gilt $\mathfrak{A} \equiv_\infty$ genau dann, wenn $\mathfrak{A} \equiv_\omega \mathfrak{B}$.

Beweis. $\Rightarrow$: Diese Richtung ist klar.
$\Leftarrow$: Sei $I := \{\bar{a} \mapsto \bar{b} : \mathrm{tp}_\mathfrak{A}(\bar{a}/\emptyset) = \mathrm{tp}_\mathfrak{B}(\bar{b}/\emptyset)\}$. Behauptung: I hat die HHE bzgl. I.

Hin: Sei $\bar{a} \mapsto \bar{b} \in I$ und $c \in A$. Setze $p = \mathrm{tp}_\mathfrak{A}(c/\bar{a})$ und sei q der Typ, der aus p entsteht, wenn $\bar{a}$ durch $\bar{b}$ ersetzt wird. Nun ist $p \cup \mathrm{Th}(\mathfrak{A}, \bar{a})$ erfüllbar und wegen $\mathfrak{A}, \bar{a} \equiv_\omega \mathfrak{B}, \bar{b}$ ist auch $q \cup \mathrm{Th}(\mathfrak{B}, \bar{b})$ erfüllbar. Da $\mathfrak{B}$ ω-saturiert ist, existiert $d \in B$ mit $\mathrm{tp}_\mathfrak{B}(d/\bar{b}) = q$. Dann ist $\mathrm{tp}_\mathfrak{A}(\bar{a}c/\emptyset) = \mathrm{tp}_\mathfrak{B}(\bar{b}d/\emptyset)$ und also $\bar{a}c \mapsto \bar{b}d \in I$.

Her: Dies lässt sich völlig analog zur Hinrichtung zeigen.
Es folgt $\mathfrak{A} \equiv_\infty \mathfrak{B}$. □

4 Fixpunktlogiken

In diesem Kapitel sollen die Fixpunktlogiken L_μ und LFP erläutert werden. Um diese besser verstehen zu können müssen aber zuerst einige Grundbegriffe aus der Fixpunkttheorie besprochen werden.

4.1 Algebraische Fixpunkttheorie

$(X, \leq)$ sei eine partielle Ordnung, also reflexiv, transitiv und antisymmetrisch (d.h. wenn $x \leq y$ und $y \leq x$, dann ist $x = y$).
Für $Y \subseteq X$ ist x Infimum von Y, wenn

1. $x \leq y$ für alle $y \in Y$ und
2. Wenn $x' \leq y$ für alle $y \in Y$, dann ist $x' \leq x$

Völlig analog ist x Supremum von Y, wenn

1. $y \leq x$ für alle $y \in Y$ und
2. Wenn $y \leq x'$ für alle $y \in Y$, dann ist $x \leq x'$

Definition 4.1 (Verband)
$(X, \leq)$ ist ein *Verband*, wenn $(X, \leq)$ eine partielle Ordnung ist so, dass für alle $x, y \in X$ die Menge $\{x, y\}$ ein Infimum $x \sqcap y$ und ein Supremum $x \sqcup y$ besitzt.

Definition 4.2 (Beschränkte und vollständige Verbände)
Um Verbände besser charakterisieren zu können sollen nun zwei wichtige Begriffe eingeführt werden:

- Ein Verband ist *beschränkt*, wenn er ein kleinstes Element $\bot$ und ein größtes Element $\top$ besitzt.
- Ein Verband ist *vollständig*, wenn jede Menge $Y \subseteq X$ ein Supremum $\sup Y = \bigsqcup Y$ und ein Infimum $\inf Y = \bigsqcap Y$ besitzt.

Wenn beispielsweise die Struktur $(X, \wedge, \vee)$ mit assoziativen, kommutativen, binären Funktionen $\vee$, $\wedge$ zusätzlich noch das Absorptionsgesetz $x \vee (x \wedge y) = x \wedge (x \vee y) = x$ erfüllt, dann ist $(X, \leq)$ ein Verband mit $x \leq y :\Leftrightarrow x \wedge y = x$. Wenn es dann zusätzlich neutrale Elemente gibt, ist $(X, \leq)$ beschränkt.

Definition 4.3 (Boolesche Algebra)
Eine *Boolesche Algebra* ist eine Struktur $(X, \wedge, \vee, \neg)$ so, dass

- $(X, \wedge, \vee)$ ein beschränkter Verband ist
- Die Distributionsgesetze $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ und $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ erfüllt werden
- $x \vee \neg x = \top$ und $x \wedge \neg x = \bot$ gilt

Einer der wohl wichtigsten Verbände ist die Mengenalgebra $(\mathcal{P}(A), \cap, \cup)$ für eine Menge A. Mit der Komplementoperation ist diese dann sogar eine Boolesche Algebra mit $\bot = \emptyset$ und $\top = A$.

Im folgenden sei $(X, \leq)$ immer ein vollständiger Verband.

Definition 4.4 (Operatoren)
Ein *Operator* ist eine Funktion $F : X \to X$. Einige weitere wichtige Begriffe sind:

- F ist *monoton*, wenn $x \leq y \Rightarrow F(x) \leq F(y)$ für alle $x, y \in Y$ gilt.
- F ist *inflationär*, wenn $x \leq F(x)$ für alle $x \in X$ gilt.
- F ist *deflationär*, wenn $F(x) \leq x$ für alle $x \in X$ gilt.
- x ist *Fixpunkt* von F, wenn $F(x) = x$.
- x ist *kleinster (größter) Fixpunkt*, wenn $x = F(x)$ und $x \leq y$ $(y \leq x)$ für alle Fixpunkte y von F gilt. Wir sagen dann $\mathrm{lfp}(F) = x$ $(\mathrm{gfp}(F) = x)$.

Satz 4.1 (Knaster, Tarski)
Sei F ein monotoner Operator auf einem vollständigen Verband $(X, \leq)$. Dann hat F einen kleinsten Fixpunkt $\mathrm{lfp}(F)$ und einen größten Fixpunkt $\mathrm{gfp}(F)$. Außerdem gilt $\mathrm{lfp}(F) = \bigsqcap\{x \in X : F(x) \leq x\}$ bzw. $\mathrm{gfp}(F) = \bigsqcup\{x \in X : x \leq F(x)\}$.

Beweis. Sei $\Phi := \{x \in X : F(x) \leq x\}$ und $y = \bigsqcap \Phi$. Für $x \in \Phi$ gilt $y \leq x$ und daher $F(y) \leq F(x)$, also ist $F(y) \leq \bigsqcap \Phi = y$. Andererseits gilt $y \leq F(y)$, denn wegen $F(y) \leq y$ gilt $F(F(y)) \leq F(y)$, also ist $F(y) \in \Phi$ und wegen $y = \bigsqcap \Phi$ folgt dann $F(y) = y$. Da $y \leq x$ für alle $x \in X$ mit $F(x) \leq x$, insbesondere also für alle Fixpunkte, ist, muss y der kleinste Fixpunkt von F sein.

Der Beweis für den größten Fixpunkt lässt sich völlig dual führen. □

Damit haben wir also eine konstruktive Methode, um einen Fixpunkt zu finden. Diese ist aber nicht sonderlich effizient, weshalb wir ein anderes, induktives Verfahren einführen wollen.

Sei $F : X \to X$ also ein Operator. Mithilfe von diesem wollen wir zwei Folgen $(X^\alpha)_{\alpha \in On}$ und $(Y^\alpha)_{\alpha \in On}$ definieren, welche uns induktiv Fixpunkte liefern sollen.

- $X^0 := \bot$ und $Y^0 := \top$
- $X^{\alpha+1} := F(X^\alpha)$ und $Y^{\alpha+1} := F(Y^\alpha)$
- Für ein Limesordinal λ: $X^\lambda := \bigsqcup\{X^\alpha : \alpha < \lambda\}$ und $Y^\lambda := \bigsqcap\{Y^\alpha : \alpha < \lambda\}$

Weiter nennen wir F induktiv, wenn $X^\beta \leq X^\alpha$ für $\beta < \alpha$ gilt und es lässt sich leicht feststellen, dass F bereits induktiv ist, falls F inflationär oder monoton ist.

Definition 4.5 (Abschlussordinale und induktive Fixpunkte)
Da X eine Menge ist, muss es ein Ordinal β geben so, dass $X^\beta = X^{\beta+1}$ und damit $X^\beta = X^\alpha$ für alle $\beta \leq \alpha$.

Das kleinste solche Ordinal β ist das *Abschlussordinal* $\mathrm{cl} \uparrow (F)$ und das zugehörige $X^\beta =: X^\infty$ ist der *induktive Fixpunkt* von F.

Lemma 4.1.1*:* Sei $X = (\mathcal{P}(A), \subseteq)$ eine Mengenalgebra und $F : \mathcal{P}(A) \to \mathcal{P}(A)$ induktiv. Dann ist $\mathrm{cl} \uparrow (F) < |A|^+$.

Zur Erinnerung: Für ein Kardinal $\kappa \in \mathrm{Cn}$ ist κ^+ das nächstgrößere Kardinal.

Beweis. Wenn nicht, dann ist $X^\beta < X^{\beta+1}$ für alle $\beta < |A|^+$, also existiert $a_\beta \in X^{\beta+1} \setminus X^\beta$ für alle $\beta < |A|^+$. Bildet man nun die Menge $\Phi = \{a_\beta : \beta < |A|^+\}$ ist leicht ersichtlich, dass $|\Phi| = |A|^+$, was einen Widerspruch zu $\Phi \subseteq A$ darstellt. □

Satz 4.2
Sei $F : X \to X$ monoton. Dann ist $\mathrm{lfp}(F) = X^\infty$.

Beweis. Offensichtlich ist $F(X^\infty) = X^\infty$, also ist $\mathrm{lfp}(F) \le X^\infty$ bereits klar. Für $X^\infty \le \mathrm{lfp}(F)$ ist nun folgendes zu zeigen:

Für alle $x \in X$ mit $F(x) \le x$ gilt $X^\alpha \le x$ für alle α. Sei also $F(x) \le x$.

- Im Fall $\alpha = 0$ ist $X^0 = \bot \le x$.
- Für $X^{\alpha+1}$ ist $X^{\alpha+1} = F(X^\alpha) \overset{\text{IV}}{\le} F(x) \le x$.
- Für ein Limesordinal λ ist $X^\lambda = \bigsqcup\{X^\alpha : \alpha < \lambda\}$. Da nach der Induktionsvoraussetzung $X^\alpha \le x$ für alle $\alpha < \lambda$, ist auch $X^\lambda \le x$.

□

Sei $X = (\mathcal{P}(a), \cup, \cap)$ eine Mengenalgebra und $\bar{x} := A \setminus x$ die Komplementoperation. Zu $F : \mathcal{P}(A) \to \mathcal{P}(A)$ definieren wir den dualen Operator $F^\star : \mathcal{P}(A) \to \mathcal{P}(A)$ durch $F^\star(x) := \overline{F(\bar{x})}$.

Satz 4.3
Sei $F : \mathcal{P}(A) \to \mathcal{P}(()A)$ monoton. Dann ist

a) $F^\star$ monoton

b) $\mathrm{lfp}(F) = \overline{\mathrm{gfp}(F^\star)}$

c) $\mathrm{gfp}(F) = \overline{\mathrm{lfp}(F^\star)}$

Beweis. a) Sei $x \subseteq y$. Dann ist $\bar{x} \supseteq \bar{y}$, also $F(\bar{x}) \supseteq F(\bar{y})$ (da F monoton) und damit ist $\overline{F(\bar{x})} \subseteq \overline{F(\bar{y})}$ bzw. $F^\star(x) \subseteq F^\star(y)$.

b) Sei $(x_\alpha)_{\alpha \in On}$ die lfp-Induktion von F und $(y^\star_\alpha)_{\alpha \in On}$ die gfp-Induktion von $F^\star$. Nun stellen wir die Behauptung $x_\alpha = \overline{y^\star_\alpha}$ für alle α, die wir durch eine Induktion beweisen wollen.

   - $x_0 = \emptyset = \bar{A} = \overline{y^\star_0}$
   - $x_{\alpha+1} = F(x_\alpha) \overset{\text{IV}}{=} F(\overline{y^\star_\alpha}) = \overline{F^\star(y^\star_\alpha)} = \overline{y^\star_{\alpha+1}}$
   - λ ein Limesordinal: $x_\lambda = \bigcup\{x_\alpha : \alpha < \lambda\} = \overline{\bigcap\{\bar{x_\alpha} : \alpha < \lambda\}} \overset{\text{IV}}{=} \overline{\bigcap\{y^\star_\alpha : \alpha < \lambda\}} = \overline{y^\star_\lambda}$

c) Dieser Fall ist dual zu Fall b) und lässt sich genauso beweisen.

□

4.2 Der modale μ-Kalkül

Bei der modalen Logik L_μ handelt es sich, informell ausgedrückt, um die Modallogik ML zusammen mit größten und kleinsten Fixpunkten.

Die Syntax lässt sich formal auf zwei Arten ausdrücken. Wir fixieren $(P_i)_{i \in I}$ als Menge an atomaren Aussagen, $A \ne \emptyset$ als nichtleere Menge an Aktionen und VAR als Menge von Fixpunkt-Variablen. Die erste Grammatik erlaubt das negieren beliebiger Formeln:

$$\psi := P_i \quad | \quad X \quad | \quad \psi \vee \psi \quad | \quad \psi \wedge \psi \quad | \quad \neg\psi \quad | \quad \langle a\rangle\psi \quad | \quad [a]\psi \quad | \quad \mu X.\psi \quad | \quad \nu X.\psi$$

wobei $i \in I$, $a \in A$, $X \in$ VAR und X nur positiv vorkommen darf.

Als alternative lässt sich auch folgende Grammatik nutzen, welche Formeln direkt in Negations-Normalform definiert, wodurch die Einschränkung der nicht-negierten Fixpunkt-Variablen wegfallen kann:

$$\psi := P_i \quad | \quad \neg P_i \quad | \quad X \quad | \quad \psi \vee \psi \quad | \quad \psi \wedge \psi \quad | \quad \langle a\rangle\psi \quad | \quad [a]\psi \quad | \quad \mu X.\psi \quad | \quad \nu X.\psi$$

Wie auch in der bisher bekannten Modallogik werden L_μ-Formeln auf Kripkestrukturen $\mathcal{K} = (V, (P_i)_{i\in I}, (E_a)_{a\in A})$ ausgewertet, wobei $P_i \subseteq V$ und $E_a \subseteq V \times V$ für beliebiges $i \in I$ und $a \in A$ gilt.

Die Semantik für die bereits bekannten Operatoren wie z.B. $\langle a\rangle\psi$ sind wie in ML, es muss also nur die Semantik für Fixpunkt-Variablen, $\mu X.\psi$ und $\nu X.\psi$ erläutert werden.

Um die weiteren Definitionen simpler zu halten werden Fixpunkt-Variablen nie frei sondern immer durch μ oder ν gebunden vorkommen. Im weiter folgenden wird uns dies nicht einschränken. Generell gilt also $\mathcal{K}, v \models \mu X.\psi :\Leftrightarrow v \in \mathrm{lfp}(F^\psi_\mathcal{K})$. Durch die Formel wird also ein Operator $F^\psi_\mathcal{K} : \mathcal{P}(V) \to \mathcal{P}(V)$ definiert, mit $U \mapsto F^\psi_\mathcal{K}(U) \coloneqq \{v \in V : K, v \models \psi[X/U]\}$. Jedes vorkommen von X in ψ wird also durch U ersetzt. Dadurch, dass X ausschließlich positiv vorkommt ist $F^\psi_\mathcal{K}$ monoton und es existieren kleinste und größte Fixpunkte.

Analog gilt $\mathcal{K}, v \models \nu X.\psi :\Leftrightarrow v \in \mathrm{gfp}(F^\psi_\mathcal{K})$.

Beispiel 4.1
Einige Beispiele sollen dies weiter erläutern:

1. Wir betrachten die Formel $\mu X.\psi$ mit $\psi = (P \vee \langle a\rangle X)$ mit der Kripkestruktur $\mathcal{K} = (V, P, E_a)$. Durch scharfes hinsehen erhält man den Operator

$$F^\psi : X \mapsto P \cup \{\text{es gibt Transition von } v \xrightarrow{a} X\}.$$

   Da in der Formel μ verwendet wird, ist die Frage nach dem kleinsten Fixpunkt des Operators. Im letzten Kapitel haben wir zwei Methoden kennengelernt: Zum Einen die Methode in Satz 4.1 und zum anderen die Fixpunkt-Induktion. Die Fixpunkt ist meistens einfacher auszuführen und wird deshalb auch eher verwendet.

   Aus der Definition ergibt sich $X^0 = \emptyset$. Weiter ist

   - $X^1 = \{v : v \models P \vee \langle a\rangle\emptyset\} = P$
   - $X^2 = P \cup \{v : v \xrightarrow{a} P\}$
   - $X^3 = P \cup \{v : v \xrightarrow{a} X^2\} = P \cup \{v : v \xrightarrow{a} P\} \cup \{v : v \xrightarrow{a} w \xrightarrow{a} P\}$
   - $X^n = \{v : v \xrightarrow[a]{<n} P\}$
   - $X^\infty = \mathrm{lfp}(F) = \{v : v \xrightarrow[a]{*} P\}$

   Die Formel drückt also aus, dass von v immer ein Knoten in P erreicht werden kann.

2. Sei $\psi \coloneqq \nu X.\Diamond 1 \wedge \Box X$ eine Formel, die auf Strukturen der Form $\mathcal{K} = (V, E)$ ausgewertet werden soll. Zu Erinnerung bedeutet $\Diamond 1$, dass es einen Nachfolgerknoten gibt. Wie im letzten Beispiel wird wieder die Fixpunkt-Iteration verwendet, nun aber für den größten Fixpunkt. Es gilt also $Y^0 = V$ und weiter:

   - $Y^1 = \{v : vE \neq \emptyset\}$
   - $Y^2 = \{v : vE \neq \emptyset \wedge vE \subseteq Y^1\}$
   - $Y^{n+1} = \{v : vE \neg\emptyset \wedge vE \subseteq Y^n\}$
     $= \{v : \text{kein Pfad von } v \text{ der Länge } \leq n \text{ erreicht einen Terminalknoten}\}$
   - $Y^\infty = \{v : \text{kein Pfad von } v \text{ erreicht einen Terminalknoten}\}$

3. Wir wollen nun einen Spielgraphen $\mathcal{K} = (V, E)$ und ein Spiel darauf betrachten. Es gibt die beiden Spieler 0 und 1. Diese ziehen abwechselnd entlang E, wobei der verliert, der nicht mehr ziehen kann. Es ergeben sich also zwei Mengen

$$W_i := \{w : \text{Spieler } i \text{ hat Gewinnstrategie von } w\}$$

für $i \in \{0, 1\}$. Es wird behauptet: $v \in W_0 \Leftrightarrow \mathcal{K}, v \models \mu X.\Diamond\Box X$. Um dies zu zeigen wird wieder eine Fixpunktinduktion, beginnend mit $X^0 = \emptyset$ durchgeführt:

- $X^1 = \{v : \mathcal{K}, v \models \Diamond\Box 0\} = \{v : \text{Sp. 0 kann von } v \text{ zu einem Terminalknoten ziehen}\}$
- $X^{n+1} = \{v : \mathcal{K}, v \models \Diamond\Box X^n\}$
  $= \{v : \text{Sp. 0 kann von } v \text{ zu einem } w \text{ ziehen so, dass alle Züge von Sp. 1 von } w \text{ aus in } X^n \text{ landen}\}$
  $\{v : \text{Sp. 0 kann von } v \text{ aus in } \leq n \text{ eigenen Zügen gewinnen}\}$
- $X^\infty = W_0$

Modifizieren wir das Spiel so, dass der Spielgraph die Form $\mathcal{K} = (V, V_0, V_1, E)$ hat, mit $V_0 \dot\cup V_1 = V$ und so, dass Spieler i zieht, wenn sich das Spiel auf einem Knoten in V_i „befindet“, dann lässt sich die eben gezeigte Eigenschaft formulieren mit

$$\psi = \mu X.(V_0 \wedge \Diamond X) \vee (V_1 \wedge \Box X)$$

und auf analoge Weise folgt auch dann $X^\infty = W_0$.

4. Wir betrachten wieder Kripkestrukturen der Form $\mathcal{K} = (V, E)$ und die Formel $\psi := \mu X.\Box X$. Behauptung:

$$\mathcal{K}, v \models \mu X.\Box X \Leftrightarrow \text{alle Pfade vom Graphen sind endlich (Fundiertheit).}$$

Es ergibt sich:

- $X^0 = \emptyset$
- $X^1 = \{v : vE = \emptyset\}$
- $X^n = \{v : \text{es gibt von } v \text{ aus keinen Pfad der Länge } n\}$
- $X^\omega = \bigcup_{n<\omega} X^n = \{v : \text{es gibt ein } n \text{ so, dass alle Pfade von } v \text{ Länge } < n \text{ haben}\}$

Es lässt sich erkennen, dass $X^\omega \neq X^\infty$. Man betrachte die Kripkestruktur, welche eine Wurzel v mit genau einem Nachfolgeknoten w besitzt. Von w geht für jedes $n \in \omega$ ein Pfad der Länge der n aus so, dass die Struktur nur endliche Pfade besitzt, aber unendlich verzweigt ist. Es lässt sich leicht sehen, dass X^1 alle äußersten Knoten der Pfade von w sind, X^2 die letzten beiden Knoten der Pfade mit Länge ≥ 2 von w ausgehend und der eine Knoten des Pfades der Länge 1 und so weiter. Die erste Menge, in der w vorkommen kann ist demnach X^ω, ansonsten wäre $w \in X^n$ für ein $n \in \omega$. Es gibt aber einen Pfad von w aus mit der Länge $n + 1$, der erste Knoten dieses Pfades ist also nicht in X^{n-1}, also kann w nicht in X^n sein. Die Wurzel v ist dann in $X^{\omega+1}$, was dadurch auch das Abschlussordinal ist.

Weiter soll $(A, <)$ eine lineare Ordnung sein. Wir betrachten $(A, <)$ als eine Kripkestruktur $\mathcal{K} = (A, E_<)$ mit $E_< = \{(a, b) : b < a\}$. Dann gilt

$$\mathcal{K}, a \models \mu X.\Box X \forall a \Leftrightarrow (A, <) \text{ ist WO.}$$

Im modalen μ-Kalkül lassen sich also Wohlordnungen ausdrücken.

5. Sei $\mathcal{K} = (V, P, E)$ endlich verzweigt. Wir wollen uns nun die Formel $\psi \coloneqq \nu X.\mu Y.\Diamond((P \wedge X) \vee Y)$ anschauen. Aufgrund der geschachtelten Fixpunktoperatoren müssen wir für jeden äußeren Fixpunkt-Iterationsschritt die innere Fixpunktiteration ausführen. Wir beginnen also mit $X^0 = V$. Dann ist

   - $Y^{00} = \emptyset$
   - $Y^{01} = \{v : \mathcal{K}, v \models \Diamond((P \wedge 1) \vee 0)\} = \{v : \mathcal{K}, v \models \Diamond P\} = \{v : v \xrightarrow{1} P\}$
   - $Y^{02} = \{v : \mathcal{K}, v \models \Diamond(P \vee Y^{01})\} = \{v : \xrightarrow[\geq 1]{\leq 2} P\}$
   - $Y^{0n} = \{v : v \xrightarrow[\geq 1]{\leq n} P\}$
   - $Y^{0\infty} = \{v : v \xrightarrow{+} P\}$

   und dann für $X^1 = Y^{0\infty} = \{v : v \xrightarrow{+} P\}$ folgt

   - $Y^{10} = \emptyset$
   - $Y^{11} = \{v : \mathcal{K}, v \models \Diamond((P \wedge \{v : v \xrightarrow{+} P\}) \vee 0)\} = \{v : v \xrightarrow{1} P \xrightarrow{+} P\}$
   - $Y^{1n} = \{v : \xrightarrow[\geq 1]{\leq n} P \xrightarrow{+} P\}$
   - $Y^{1\infty} = \{v : v \xrightarrow{+} P \xrightarrow{+} P\}$,

   also $X^2 = Y^{1\infty} = \{v : v \xrightarrow{+} P \xrightarrow{+} P\}$ und auf dem selben Weg erhält man $X^n = \{v :$ es ex. Pfad von v auf welchem Pmin. n mal vorkommt$\}$ und damit auch

   $$X^\infty = \bigcap_{n<\infty} X^n = \{v : \text{es ex. Pfad von } v \text{ auf welchem } P \text{ unendlich oft vorkommt}\}$$

Die Negationsnormalform

Wir wollen nun betrachten, wie sich die Negationsnormalform einer beliebigen L_μ-Formel bilden lässt. Wie bekannt gelten $\neg(\psi \wedge \varphi) \equiv \neg\psi \vee \neg\varphi$, $\neg(\psi \vee \varphi) \equiv \neg\psi \wedge \neg\varphi$, $\neg\langle a \rangle\psi \equiv [a]\neg\psi$ und $\neg[a]\psi \equiv \langle a \rangle\neg\psi$.

Es bleiben also noch die Fixpunktoperatoren. Es lässt sich feststellen, dass für diese gilt: $\neg\mu X.\psi \equiv \nu X.\neg\psi[X/\neg X]$ und $\neg\nu X.\psi \equiv \mu X.\neg\psi[X/\neg X]$. Wie anfangs gefordert lassen sich auf diese Weise keine Negationen von Fixpunkt-Variablen bilden. Es wird zwar jede Fixpunktvariable durch $\neg X$ ersetzt, durch die Negation der Formel selber wird dieses aber wieder zu X. Beispielsweise ist $\neg\mu X.\Box X \equiv \nu X.\Diamond X$.

Einbettung in andere Logiken

Ein interessanter Aspekt jeder Logik ist die Einbettung von dieser in andere Logiken und die Einbettung anderer Logiken in diese. Dies wollen wir nun für den modalen μ-Kalkül betrachten.

Offensichtlich lässt sich ML in L_μ einbetten. Da bereits ML $\leq$ FO $\leq$ MSO bekannt ist stellt sich die Frage, ob $\mathrm{L}_\mu \leq$ MSO gilt. Es ist klar, dass das ML-Fragment von L_μ mithilfe einer Funktion in MSO eingebettet werden kann so, dass folgender Zusammenhang entsteht $\psi \mapsto \psi^*(x)$. Wir müssen uns also Formeln mit Fixpunkt-Operatoren annehmen. Sei dafür $\psi \coloneqq \mu X.\varphi(X)$. Es lässt sich feststellen, dass die Formel $\psi^*(x) = \forall X((\forall y \varphi^*(X, y) \rightarrow Xy) \rightarrow Xx)$ äquivalent und eine MSO-Formel ist.

Genauer sagt $\psi^*(x)$ aus, dass x in allen Mengen X enthalten ist so, dass $F^\varphi(X) \subseteq X$. Mithilfe von Satz 4.1 folgt dann daraus, dass $x \in \text{lfp}(F^\varphi)$ ist.

Weiter lässt sich feststellen, dass L_μ das bisimulationsinvariante Fragment von MSO ist, so, wie ML dieses von FO ist. Dies wurde 1996 von Janin und Walukiewicz bewiesen, der Beweis ist aber über dem Niveau dieser Vorlesung, weshalb diese Eigenschaft nicht weiter behandelt werden soll.

Nun bilden wir aus ML die Logik ML^∞ auf die selbe Weise, wie wir aus FO die infinitäre Logik $L_{\infty\omega}$ gebildet haben. Genauer: Indem wir Kon- und Disjunktionen über Mengen beliebiger Kardinalität erlauben. Offensichtlich ist ML^∞ bisimulationsinvariant.

Satz 4.4
Sei $\kappa \in \text{Cn}$. Über der Klasse aller Kripkestrukturen der Kardinalität $< \kappa$ ist L_μ in ML^∞ einbettbar.

Beweis. Alle Operatoren, außer den Fixpunkt-Operatoren, lassen sich trivial einbetten. Wir brauchen also nur $\mu X.\psi$ zu behandeln. Dafür definieren wir, analog zur Fixpunkt-Induktion, eine induktiv definierte Folge:

- $\psi^0 := 0$
- $\psi^{\alpha+1} := \psi[X/\psi^\alpha]$
- Für Limesordinale λ: $\psi^\lambda := \bigvee\{\psi^\alpha : \alpha < \lambda\}$.

Sei $\mathcal{K}$ eine Kripkestruktur der Kardinalität $< \kappa$ und $X^0, X^1, \ldots$ die durch F^ψ definierte lfp-Induktion. Dann ergibt sich nach Konstruktion $\mathcal{K}, v \models \psi^\alpha \Leftrightarrow v \in X^\alpha$ und $v \in X^\infty = \text{lfp}(F^\psi) \Leftrightarrow v \in X^\alpha$ für ein $\alpha < \kappa^+$. Also gilt $\mu X.\psi \equiv \bigvee\{\psi^\alpha : \alpha < \kappa^+\} \in ML^\infty$ auf Kripkestrukturen der Kardinalität $< \kappa$. □

Daraus folgt, dass L_μ bisimulationsinvariant sein muss.

In MaLo 1 wurde bereits die Logik CTL eingeführt und es wurde gesehen, dass sich diese nicht in FO einbetten lässt. Dies ist aber in L_μ möglich. Zur Wiederholung soll nun die Syntax von CTL gezeigt werden:

$$\psi := P_i \quad | \quad \neg\psi \quad | \quad \psi \vee \psi \quad | \quad \psi \wedge \psi \quad | \quad EX\psi \quad | \quad AX\psi \quad | \quad E(\psi U \psi) \quad | \quad A(\psi U \psi)$$

Die ersten vier Formeln sind offensichtlich auch in L_μ darstellbar. Mit Erinnerung an die Semantik von CTL lässt sich zudem leicht sehen, dass $EX\psi \equiv \Diamond\psi$ und $AX\psi \equiv \Box\psi$ gelten. Es bleiben also nur noch die Until-Operatoren. Wir definieren also eine Funktion $()^* : CTL \to L_\mu, \varphi \mapsto \varphi^*$ mit $E(\psi U \varphi)^* := \mu X.\varphi^* \vee (\psi^* \wedge \Diamond X)$ und $A(\psi U \varphi)^* := \mu X.\varphi^* \vee (\psi^* \wedge \Box X)$. Diese beiden L_μ-Formeln bezeichnen wir als *alternationsfrei*.

Definition 4.6 (Der alternationsfreie μ-Kalkül)
Eine L_μ-Formel ist *alternationsfrei*, wenn in keiner Unterformel $\mu X.\varphi$ (bzw. $\nu X.\varphi$) eine ν-Variable (bzw. μ-Variable) frei vorkommt.

Ein Gegenbeispiel wäre $\nu X.\mu Y.(\Diamond(P \wedge X) \vee \psi)$. Die Unterformel $\mu Y.(\Diamond(P \wedge X) \vee \psi)$ ist nun eine $\mu X.\varphi$ Unterformel, in der aber die ν-Variable X vorkommt. Dieses Beispiel ist also nicht alternationsfrei.

Bei alternationsfreien Formeln muss man selbst bei mehreren Fixpunkt-Operatoren keine verschachtelte Fixpunkt-Iteration durchführen. Der Berechnungsaufwand wird also deutlich verringert. Es gilt aber leider folgender Satz:

Satz 4.5
Die Alternationshierachie von L_μ ist strikt.

Anders ausgedrückt besagt der Satz, dass mehr Alternationen von Fixpunkt-Operatoren zu einer größeren Ausdrucksstärke führen. Der dazugehörige Beweis ist aber nicht einfach und wird hier daher nicht geführt.

Neben CTL wollen wir nun eine andere Logik in L_μ einbetten. Diese ist die *Propositional Dynamic Logic* (PDL). In dieser gibt es zwei verschiedene Formeln: zum Einen gibt es Zustandsformeln, welche wir mit φ beschreiben und zum Anderen gibt es Programmformeln, welche wir π nennen. Die dazugehörigen Grammatiken sind:

$$\varphi \coloneqq P_i \quad | \quad \varphi \wedge \varphi \quad | \quad \varphi \vee \varphi \quad | \quad \neg\varphi \quad | \quad \langle\pi\rangle\varphi$$
$$\pi \coloneqq E \quad | \quad \varphi? \quad | \quad \pi \cup \pi \quad | \quad \pi;\pi \quad | \quad \pi^*$$

Für eine Kripkestruktur $\mathcal{K} = (V, E)$ ist $\pi^\mathcal{K} \subseteq V \times V$. Wir wollen nun die einzelnen Bausteine von Programmfunktionen definieren, da die Semantik der Zustandsformeln bereits aus ML bekannt ist.

- $(\varphi?)^\mathcal{K} = \{(v, v) : \mathcal{K}, v \models \varphi\}$
- $(\pi_1 \cup \pi_2)^\mathcal{K} = \pi_1^\mathcal{K} \cup \pi_2^\mathcal{K}$
- $(\pi_1; \pi_2)^\mathcal{K} = \pi_1^\mathcal{K} \circ \pi_2^\mathcal{K} = \{(v, w) : \exists z((v, z) \in \pi_1^\mathcal{K} \wedge (z, w) \in \pi_2^\mathcal{K})\}$
- $(\pi^*)^\mathcal{K} = \bigcup_{n\in\mathbb{N}}(\pi^\mathcal{K})^n$, wobei die Potenzierung induktiv durch $(\pi^\mathcal{K})^0 \coloneqq \{(v, v) : v \in V\}$ und $(\pi^\mathcal{K})^{n+1} \coloneqq (\pi^\mathcal{K})^n \circ \pi^\mathcal{K}$ definiert ist.

Satz 4.6
Zustandsformeln von PDL können in L_μ übersetzt werden.

Beweis. Die einzige Art an Formel, die betrachtet werden muss sind Formeln der Art $\langle\pi\rangle\varphi$. Abhängig von π definieren wir also eine Übersetzung $(\langle\pi\rangle\varphi)^*$:

- $\pi = E \rightsquigarrow \Diamond\varphi^*$
- $\pi = \psi? \rightsquigarrow \psi^* \wedge \varphi^*$
- $\pi = \pi_1 \cup \pi_2 \rightsquigarrow (\langle\pi_1\rangle\varphi)^* \vee (\langle\pi_2\rangle\varphi)^*$
- $\pi = \pi_1; \pi_2 \rightsquigarrow \langle\pi_1\rangle^*\langle\pi_2\rangle^*\varphi^*$
- $\pi = \pi_1^* \rightsquigarrow \mu X.\varphi \vee \langle\pi_1\rangle^* X$

□

Auswerten von Schaltkreisen

Wir wollen eine logische Schaltung mithilfe von Gattern logisch beschreiben. Dafür benutzen wir Strukturen wie $\mathfrak{C} = (V, E, \mathrm{OR}, \mathrm{AND}, 1, \ldots, I_1, I_0)$ oder $\mathfrak{C}' = (V, E, I_1, I_0, \mathrm{NAND})$. Dabei stellen V eine Menge an Knoten und E eine Menge an Kanten dar so, dass wir einen DAG (*Directed Acyclic graph*) erhalten. I_n, $n \in \{0, 1\}$ beschreibt welche Knoten „wahr“ sind und die einstelligen Relationen OR AND und NAND stellen dar, wie die Knoten ausgewertet werden sollen. Nun betrachten wir das Problem: $\mathfrak{C}, v \models \psi \Leftrightarrow \mathfrak{C}$ wertet v zu 1 aus und es stellt sich die Frage: Ist ψ in L_μ definierbar? Ein erster versuch ist

$$\psi \coloneqq \mu T.I_1 \vee (\mathrm{OR} \wedge \Diamond T) \vee (\mathrm{AND} \wedge \Box T).$$

Mit dieser Formel lässt sich aber keine Negation darstellen, da es während der Fixpunktiteration nicht bekannt ist, ob ein Knoten „falsch“ oder bloß noch nicht ausgewertet ist. Wir können also keine funktional vollständigen Schaltkreise bilden. Was benötigt wird, ist das parallele Ausführen mehrerer Fixpunktinduktionen so, dass wir eine Formel von der Form

$$\mu T, F \quad \begin{array}{l} T \leftarrow I_1 \vee \Diamond F \\ F \leftarrow I_0 \vee \Box T. \end{array}$$

Formal benötigen wir also einen Operator F, welcher mehrere Operatoren besitzt, also

$$F \begin{cases} F_1 : \mathcal{P}(B_1) \times \cdots \times \mathcal{P}(B_m) \to \mathcal{P}(B_1) \\ \vdots \\ F_m : \mathcal{P}(B_1) \times \cdots \times \mathcal{P}(B_m) \to \mathcal{P}(B_m) \end{cases}$$

Simultaner μ-Kalkül

Um solche Operatoren benutzen zu können führen wir den simultanen μ-Kalkül (S-L$_\mu$) ein. Seien $\psi_1(X_1, \ldots, X_m), \ldots, \psi_m(X_1, \ldots, X_m)$ Formeln, in welchen die X_i nur positiv auftreten. Dann sind $\left[\mu\bar{X}.(\psi_1, \ldots, \psi_m)\right]$ und $\left[\nu\bar{X}(\psi_1, \ldots, \psi_m)\right]$ Formeln von S-L$_\mu$.

Semantisch behandelt dieser Kalkül ebenfalls die schon bekannten Kripkestrukturen. Ein mehrdimensionaler Operator wie oben wird dann wie folgt implizit gebildet $F^\Psi = (F^{\psi_1}, \ldots, F^{\psi_m}) : \mathcal{P}(V) \times \cdots \times \mathcal{P}(V) \to \mathcal{P}(V) \times \cdots \times \mathcal{P}(V)$ und die einzelnen Operatoren werden wie bekannt interpretiert: $F^{\psi_i} : (X_1, \ldots, X_,) \mapsto \{v : (\mathcal{K}, \bar{X}), v \models \psi_1\}$. Aus bekannten Gründen hat F^Ψ dann einen kleinsten Fixpunkt $\mathrm{lfp}(F^\Psi) = (X_1^\infty, \ldots, X_m^\infty)$ und $\mathcal{K}, v \models \left[\mu\bar{X}(\psi_1, \ldots, \psi_m)\right]_i \Leftrightarrow v \in X_i^\infty$.

Satz 4.7
S-L$_\mu \equiv$ L$_\mu$.

Beweis. Der Beweis wird nur für $m = 2$ gezeigt und verwendet das Beki-Prinizip. Für höhere m lässt sich der Beweis aber einfach erweitern und erfordert bloß mehr Schreibarbeit.
Wir haben also zwei Operatoren $F : \mathcal{P}(B) \times \mathcal{P}(C) \to \mathcal{P}(B)$ und $G : \mathcal{P}(B) \times \mathcal{P}(C) \to \mathcal{P}(C)$. Zusammengefasst werden diese dann durch den Operator

$$(F, G) : \mathcal{P}(B) \times \mathcal{P}(C) \to \mathcal{P}(B) \times \mathcal{P}(C)$$

mit dem kleinsten Fixpunkt (F^∞, G^∞).

Für jedes $X \subseteq B$ sei nun $G_X : \mathcal{P}(C) \to \mathcal{P}(C), Y \mapsto G(X, Y)$ monoton und hat den kleinsten Fixpunkt $(G_X)^\infty \subseteq C$.

Lemma 4.2.1*:* Sei $E : \mathcal{P}(B) \to \mathcal{P}(B), X \mapsto F(X, \mathrm{lfp}(G_X))$. Dann ist E monoton mit dem kleinsten Fixpunkt $E^\infty = F^\infty$.

Beweis. Monotonie: Sei $X \subseteq X'$. Nun ist zu zeigen, dass $G_X^\alpha \subseteq G_{X'}^\alpha$ für alle α, also auch $G_X^\infty \subseteq G_{X'}^\alpha$, gilt.

- $\alpha = 0$: Dieser Fall ist klar.
- $G_X^{\alpha+1} = G_X(G_X^\alpha) = G(X, G_X^\alpha) \subseteq G(X', G_{X'}^\alpha) \subseteq G_{X'}^{\alpha+1}$
- α Limesordinal: Dieser Fall ist ebenfalls klar.

Also ist $E(X) = F(X, G_X^\infty) \subseteq F(X', G'^\infty_X) = E(X')$ und E ist monoton. Es bleibt zu zeigen, dass $E^\infty = F^\infty$.

Dafür soll zuerst gezeigt werden, dass $(G_{F^\infty})^\infty \subseteq G^\infty$. Es gilt $G_{F^\infty}(G^\infty) = G(F^\infty, G^\infty) = G^\infty$. G^∞ ist also ein Fixpunkt von G_{F^∞}. Da $(G_{F^\infty})^\infty$ der kleinste Fixpunkt ist, folgt die Behauptung.
Weiter ist $E(F^\infty) = F(F^\infty, (G_{F^\infty})^\infty) \subseteq F(F^\infty, G^\infty) = F^\infty$ und damit folgt $E^\infty = \bigcap\{X : E(X) \subseteq X\} \subseteq F^\infty$.

Nun muss gezeigt werden, dass für jedes α gilt $F^\alpha \subseteq E^\alpha$ und $G^\alpha \subseteq (G_{E^\alpha})^\infty$.

- $\alpha = 0$: Dieser Fall ist klar.
- $F^{\alpha+1} = F(F^\alpha, G^\alpha) \subseteq F(E^\infty, (G_{E^\alpha})^\infty) = E(E^\infty) = E^\infty$ und $G^{\alpha+1} = G(F^\alpha, G^\alpha) \subseteq G(E^\infty, (G_{E^\infty})^\infty) = G_{E^\infty}((G_{E^\infty})^\infty) = (G_{E^\infty})^\infty$
- α Limesordinal ist ebenfalls klar.

□

Damit können wir zwei Formeln aufstellen:

$$\mu X.Y.(\psi(X,Y), \varphi(X,Y))_1 = \mu X.\psi(X, \mu Y \varphi(X,Y))$$
$$\mu X.Y.(\psi(X,Y), \varphi(X,Y))_2 = \mu Y.\varphi(\mu X.\psi(X,Y), Y)$$

um den zweistelligen Operator (F,G) mit $F : (X,Y) \mapsto \{v : \mathcal{K}, v \models \psi(X,Y)\}$ und $G : (X,Y) \mapsto \{\mathcal{K}, v \models \varphi(X,Y)\}$ in einstellige Formeln aufzuteilen. Nun gilt

$$\mathcal{K}, v \models [\mu X.Y(\psi, \varphi)]_1 \Leftrightarrow v \in F^\infty.$$

Die Formel $\psi(X, \mu Y.\varphi(X,Y))$ definiert aber den Operator $E : X \mapsto F(X, (G_X)^\infty)$ mit $G_X : Y \mapsto G(X,Y)$. Also ist

$$\mathcal{K}, v \models \mu X.\psi(X, \mu Y.\varphi(X,Y)) \Leftrightarrow v \in E^\infty.$$

Mit dem Lemma folgt $E^\infty = F^\infty$, also ist die Formel $\psi(X, \mu Y.\varphi(X,Y))$ äquivalent zu $[\mu X.Y(\psi, \varphi)]_1$.
□

4.3 Least Fixed-Point Logic

Im vorherigen Kapitel haben wir uns weitgehend mit dem modalen μ-Kalkül beschäftigt, welcher die Modallogik ML um kleinste und größte Fixpunkte erweitert. In diesem Kapitel machen wir das gleiche mit FO. Doch warum reicht FO nicht aus?

1. FO besitzt keinen Iterationsmechanismus, weshalb Eigenschaften wie transitive Abgeschlossenheit nicht in FO darstellbar sind.
2. FO kann nur lokale Eigenschaften ausdrücken (mehr dazu in der Vorlesung Algorithmische Modelltheorie)
3. FO hat eine geringe Komplexität. Hält man $\mathfrak{A}$ fest und misst die Komplexität von $\mathfrak{A} \models \varphi$ bzgl. $|\varphi|$, ist die Komplexität in PSPACE.

   Beim Betrachten der Datenkomplexität hält man jedoch ψ fest und misst die Komplexität von $\mathfrak{A} \models \psi$ bzgl. $|\mathfrak{A}|$. Komplexitätstheoretisch ist dieses Problem in $\mathrm{AC}^0 \subseteq$ LOGSPACE. Ist ein Problem also nich in LOGSPACE lösbar, so lässt es sich auch nicht in FO ausdrücken.

Man möchte also eine Logik finden, in welche alle Probleme aus PTIME ausdrückbar sind. Dies führt uns zur Logik *Least Fixed Point* (LFP), welche FO um kleinste und größte Fixpunkte erweitert.

Wenn $\psi(T, \bar{x})$ eine Formel ist, in der T nur positiv auftritt und $|\bar{x}| = \text{Stelligkeit}(T)$ und $\bar{u}$ ein Tupel von Termen ist mit $|\bar{u}| = |\bar{x}|$, dann sind

$$[\text{lfp}\, T\bar{x}.\psi(T, \bar{x})]\,(\bar{u})$$

und

$$[\text{gfp}\, T\bar{x}.\psi(T, \bar{x})]\,(\bar{u})$$

Formeln in LFP.
Semantik: Sei $\mathfrak{A}$ eine Struktur, in der alle Relationen in ψ außer T und alle Variablen außer $\bar{x}$ interpretiert werden. Dann gilt

$$\mathfrak{A} \models \left[\begin{array}{c}\text{lfp}\\ \text{gfp}\end{array} T\bar{x}.\psi(T, \bar{x})\right](\bar{u}) \Leftrightarrow \bar{u}^{\mathfrak{A}} \in \begin{array}{c}\text{lfp}\\ \text{gfp}\end{array} \left(F_{\mathfrak{A}}^{\psi}\right).$$

Beispiel 4.2
Sei $G = (V, E)$ ein Graph und die LFP-Formel $\text{tc}(u, v)$ wie folgt definiert:

$$\text{tc}(u, v) \coloneqq [\text{lfp}\, Txy.Exy \vee \exists z(Exz \wedge Tzy)](u, v).$$

Dann sieht die Fixpunktinduktion folgendermaßen aus

- $T^0 = \emptyset$,
- $T^1 = E$,
- $T^i = \{(a, b) : \text{es gibt Pfad der Länge } \geq 1 \text{ und } \leq i \text{ von } a \text{ nach } b\}$
- $T^\infty = \{(a, b) : \text{es gibt Pfad der Länge } l \geq 1 \text{ von } a \text{ nach } b\}$

Insgesamt gilt also $G \models \text{tc}(u, v) \Leftrightarrow (u, v) \in \text{TC}(E)$.

Eine Interessante Beobachtung ist, dass sich Parameter eliminiert lassen. Wir können eine Formel

$$\varphi(u, v) \coloneqq [\text{lfp}\, Ty.Euy \vee \exists z(Exz \wedge Tzy)](v)$$

definieren, deren Fixpunktvariablen nur eine Stelligkeit von 1 haben, aber dennoch $\text{tc}(u, v) \equiv \varphi(u, v)$ gilt.

Wieder betrachten wir für beliebige $\mathfrak{A} = (A, \dots)$ mit $|A| = n \in \mathbb{N}$ und feste $[\text{lfp}\, T\bar{x}.\psi(T, \bar{x})]$ mit k-stelligem T die Komplexität von dem Problem

$$\text{Gilt } \mathfrak{A} \models [\text{lfp}\, T\bar{x}.\psi(T, \bar{x})](\bar{a})?$$

Wir stellen fest, dass $F_{\mathfrak{A}}^{\psi} : \mathcal{P}(A^k) \to \mathcal{P}(A^k)$ polynomiell berechenbar ist. Der i-te Induktionsschritt T^i der Fixpunktinduktion ist das also auch. Dann folgt, dass $\text{lfp}(F_{\mathfrak{A}}^{\psi}) = T^m$ für ein $m \leq n^k$. Informell können wir also schließen:

$$\text{LFP} \subseteq \text{PTIME}$$

Beispiel 4.3
Es sollen nun wieder Beispiele für LFP dargestellt werden.
Wir suchen eine Formel $\psi(x, y) \in \mathrm{LFP}$ so, dass für jede Kripkestruktur $\mathcal{K}$ gilt $\mathcal{K} \models \psi(v, w) \Leftrightarrow \mathcal{K}, v \sim \mathcal{K}, w \Leftrightarrow (v, w) \in Z_{\max}$. $Z_{\max}$ bezeichnet die maximale Bisimulation auf $\mathcal{K}$. Dafür definieren wir

$$\begin{aligned}\psi(x,y) \coloneqq [\mathrm{gfp}\, Zxy. &\bigwedge_{i \in I} P_i x \leftrightarrow P_i y \\ &\wedge \bigwedge_{a \in A} \forall x'(E_a x x' \to (\exists y(Eyy' \wedge Zx'y'))) \\ &\wedge \bigwedge_{a \in A} \forall y'(E_a y y' \to (\exists x(Exx' \wedge Zx'y')))](x, y).\end{aligned}$$

Die Fixpunktinduktion beginnt mit $Z^0 = V \times V$ und es gilt $Z^0 \supseteq Z^1 \supseteq \cdots \supseteq Z^i \supseteq Z^\infty = Z_{\max}$.

Nun wollen wir wieder Spiele kodieren. Wir haben einen Spielgraphen $G = (V, E, V_0, V_1)$ und möchten die Gewinnregion von Spieler 0 bestimmen. Dafür stellen wir folgenden Zusammenhang fest:

$$\begin{aligned}&\text{Sp. 0 gewinnt } G \text{ von } v \text{ aus} \\ \Leftrightarrow &G \models [\mathrm{lfp}\, Wx.(V_0 x \wedge \exists y(Exy \wedge Wy)) \vee (V_1 x \wedge \forall y(Exy \to Wy))](v).\end{aligned}$$

Weiter ist jede LFP-Formel über endlichen Strukturen durch quantorenfreie Interpretationen in diese Formel „übersetzbar".

Im letzten Kapitel haben wir festgestellt, dass sich der modale μ-Kalkül in die monadische Logik zweiter Ordnung übersetzten lässt. Hier wollen wir nun ein Verfahren einführen, welches LFP in SO einbettet:

$$[\mathrm{lfp}\, T\bar{x}.\psi(T, \bar{x})](\bar{y}) \rightsquigarrow \forall T((\forall \bar{x}(\psi(T, \bar{x}) \to T\bar{x})) \to T\bar{y}).$$

Dies reicht für die Einbettung aus, da gfp-Formeln nicht zwangsläufig benötigt werden. Dies folgt aus der Äquivalenz

$$\neg[\mathrm{lfp}\, T\bar{x}.\psi(T, \bar{x})] \equiv [\mathrm{gfp}\, T\bar{x}.\neg\psi[T/\neg T](T, \bar{x})].$$

Ähnlich dazuhaben wir festgestellt, dass $L_\mu \overset{(\kappa)}{\subseteq} \mathrm{ML}^\infty$ mit der Einschränkung gilt, dass die Strukturen eine durch κ beschränkte Größe besitzen. Analog wollen wir nun $\mathrm{LFP} \overset{(\kappa)}{\subseteq} \mathrm{L}_{\infty\omega}$ zeigen.
Sei $[\mathrm{lfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{x})$ eine LFP-Formel, für die wir eine äquivalente $\mathrm{L}_{\infty\omega}$ Formel finden wollen (für durch κ beschränkte Modelle). Dafür definieren wir erneut eine Folge $(\psi^\alpha(\bar{x}))_{\alpha < \kappa^+}$ mit

- $\psi^0(\bar{x}) \coloneqq \bar{x} \neq \bar{x}$
- $\psi^{\alpha+1}(\bar{x}) \coloneqq \psi[R\bar{u}/\psi^\alpha(\bar{u})](\bar{x})$
- $\psi^\lambda(\bar{x}) = \bigvee_{\alpha < \lambda} \psi^\alpha(\bar{x})$.

Dann ist für Strukturen $\mathfrak{A} = (A, \dots)$ mit $|A| \leq \kappa$

$$[\mathrm{lfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{x} \overset{(\kappa)}{\equiv} \bigvee_{\alpha < \kappa^+} \psi^\alpha(\bar{x}).$$

4.4 Inflationäre und Partielle Fixpunkte

Wir wollen nun zwei weitere Fixpunkt-Logiken einführen. Zum Einen die *Inflationary Fixed-Point Logic* (IFP) und zum Anderen die *Partial Fixed-Point Logic* (PFP). Man betrachte dafür zuerst den Operator $F^{\psi}_{\mathfrak{A}} : T \mapsto \{\bar{a} : (\mathfrak{A}, T) \models \psi(T, \bar{a})\}$, welcher implizit durch eine Formel $\psi(T, \bar{x})$ definiert wird. Setzt man voraus, dass T nur positiv in ψ vorkommt, dann ist $F^{\psi}_{\mathfrak{A}}$ für jede Struktur $\mathfrak{A}$ monoton. Was passiert aber, wenn man diese Bedingung weg lässt?

Zuerst fällt einem auf, dass Formeln $\psi(T, \bar{x})$ gibt, die immer monotone Operatoren definieren, auch wenn T negiert auftritt (bspw. wenn das negierte T in einer Unterformel vorkommt, die sowieso immer falsch ist). Warum wird dann also nicht bloß Monotonie statt Positivität gefordert? Dies liegt daran, dass Monotonie eine semantische und unentscheidbare Bedingung ist, die dann Auswirkungen auf die Syntax hat. Logiken sollten aber eine entscheidbare Syntax haben.

Sei also $\psi(T, \bar{x})$ so, dass T sowohl positiv, als auch negativ auftreten kann. $F^{\psi}_{\mathfrak{A}}$ ist im Allgemeinen weder monoton, noch inflationär. Aus $F^{\psi}_{\mathfrak{A}}$ lässt sich aber der inflationäre

$$G^{\psi}_{\mathfrak{A}} : T \mapsto T \cup F^{\psi}_{\mathfrak{A}}(T)$$

und dual der deflationäre Operator

$$H^{\psi}_{\mathfrak{A}} : T \mapsto T \cap F^{\psi}_{\mathfrak{A}}(T)$$

definieren.

Inflationäre Fixpunkt Logik

Dies führt uns zur Logik IFP. Zu $\psi(T, \bar{x})$ konstruieren wir neue Formeln $[\mathrm{ifp}\, T\bar{x}.\psi(T, \bar{x})](\bar{u})$, $[\mathrm{dfp}\, T\bar{x}.\psi(T, \bar{x})][\bar{u}]$.
Semantik: Auf $\mathfrak{A}$ definiert der Operator $\mathrm{G}^{\psi}_{\mathfrak{A}}$ die induktive Folge

- $T^0 = \emptyset$
- $T^{\alpha+1} = G^{\psi}_{A}(T^{\alpha}) = T^{\alpha} \cup F^{\psi}_{\mathfrak{A}}(T^{\alpha})$
- $T^{\lambda} = \bigcup_{\alpha<\lambda} T^{\alpha}$

mit dem induktiven Fixpunkt T^{∞}. Dann gilt

$$\mathfrak{A} \models [\mathrm{ifp}\, T\bar{x}.\psi(T, \bar{x})](\bar{a}) \Leftrightarrow \bar{a} \in T^{\infty}$$

und analog für dfp.
Falls T nur positiv in ψ auftritt, dann sind die lfp-Induktionen und die ifp-Induktionen gleich. Ebense gfp und dfp. Auch wird auf endlichen Strukturen der ifp-/dfp-Fixpunkt nach polynomiell vielen Stufen erreicht (bzgl. $|A|$). Also gilt LFP $\subseteq$ IFP $\subseteq$ PTIME.

Beispiel 4.4 (Der faule Ingenieur)
Sei $\varphi(x)$ eine Spezifikation, die von allen Zuständen eines Systems $\mathfrak{A}$ erfüllt sein soll. Da es a gibt, mit $\mathfrak{A} \models \varphi(a)$ lässt sich $\mathfrak{A}$ auf $\mathfrak{A}|_{\varphi}$ durch das $\{a \in A : \mathfrak{A} \models \varphi(a)\}$ induzierte Redukt eingrenzen. Durch das entfernen von Zuständen kann es aber sein, dass andere Zustände nicht mehr die Spezifikation erfüllen. Wir benötigen also eine Induktion. Sei $\mathfrak{A}^0 = \mathfrak{A}$, $\mathfrak{A}^{\beta+1} = \mathfrak{A}^{\beta}|_{\varphi}$ und $\mathfrak{A}^{\lambda} = \bigcap_{\beta<\lambda} \mathfrak{A}^{\beta}$. Diese Folge erreicht einen Fixpunkt $\mathfrak{A}^{\infty}$ mit $\mathfrak{A}^{\infty} \models \forall x \varphi(x)$.

Um diesen Vorgang zu formalisieren, definieren wir zuerst $\varphi|_Z$ als die Relativierung von φ durch eine neue Mengenvariable Z. Das heißt, man ersetzt Unterformeln $\exists y \alpha$ durch $\exists y(Zy \wedge \alpha)$ bzw. $\forall y \alpha$ durch $\forall y(Zy \rightarrow \alpha)$. So erhält man dann einen deflationären Operator

$$\mathrm{Op} : Z \mapsto \{a : \mathfrak{A}|_Z \models \varphi(a)\} = \{a : \mathfrak{A} \models Za \wedge \varphi|_Z(a)\}$$

und es folgt $\mathfrak{A}^\infty$ nicht leer $\Leftrightarrow \mathfrak{A} \models \exists x[\mathrm{dfp}\, Zx.\varphi|_Z(x)](x)$.

Satz 4.8 (Gurevich-Shelah, Kreutzer)
LFP $\equiv$ IFP.

Beweis. Der Beweis wird in der Vorlesung Algorithmische Modelltheorie geführt. □

Partielle Fixpunkt Logik

Nun kommen wir zur zweiten bereits erwähnten Logik: PFP. Wieder verwenden wir den Operator $F^\psi_\mathfrak{A}$ ohne die Positivitätsbedingung, aber nur auf endlichen Strukturen. Für $\psi(R, \bar{x})$ und dem Induktionsanfang $R^0 = \emptyset$ führt uns dies auf eine Folge R^0, R^1, R^2, ... Sei $n = |A|$ und $k =$ Stelligkeit(R). Dann erreicht man nach $m \leq 2^{n^k}$ Schritten eine Stufe R^m so, dass entweder $F^\psi_\mathfrak{A}(R^m) = R^m =: \mathrm{pfp}(F^\psi_\mathfrak{A})$ (siehe Abb. 7a) oder $F^\psi_\mathfrak{A}(R^m) = R^i$ für $i < m$ (siehe Abb. 7b).

(a) $\quad \emptyset \longrightarrow R^1 \longrightarrow \cdots \longrightarrow R^m \circlearrowleft$

(b) $\quad \emptyset \longrightarrow \cdots \longrightarrow R^i \longrightarrow \cdots \longrightarrow R^m$

Abbildung 7: Existenz eines Partiellen Fixpunktes (a) und das Fehlen davon (b)

Für $\psi(R, \bar{x})$ ist $[\mathrm{pfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{u})$ eine PFP-Formel. Die Semantik dazu ist:

$$\mathfrak{A} \models [\mathrm{pfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{a}) \Leftrightarrow \text{der Fixpunkt } \mathrm{pfp}(F^\psi_\mathfrak{A}) \text{ ex. und } \bar{a} \in \mathrm{pfp}(F^\psi_\mathfrak{A}).$$

Falls R nur positiv in $\psi(R, \bar{x})$ auftritt, dann ist $\mathrm{lfp}(F^\psi_\mathfrak{A}) = \mathrm{pfp}(F^\psi_\mathfrak{A})$, also gilt LFP $\equiv$ IFP $\subseteq$ PFP. Was noch unbekannt ist, ist ob PFP $\subseteq$ PTIME gilt. Dies liegt daran, dass es Beispiele gibt, in denen die pfp-Fixpunktinduktion erst nach 2^{n^k} den Fixpunkt erreicht.

Sei $(A, <)$ eine lineare Ordnung und

$$\psi(R, x) := (Rx \wedge \exists y(y < x \wedge \neg Ry)) \vee (\neg Rx \wedge \forall y(y < x \rightarrow Ry)) \vee \forall y Ry.$$

R^α definiert ein $0-1$-Wort der Länge n, also eine Zahl $m_\alpha < 2^n$ so, dass gilt $m_0 = 0$, $m_{\alpha+1} = m_\alpha + 1$. Es folgt $m_\alpha = \alpha$ für $\alpha \leq 2^n$ und $m_{2^n+1} = m_{2^m} = R^{2^n}$. Der Fixpunkt wird also erst nach exponentiell vielen Schritten erreicht.

Satz 4.9
PFP $\subseteq$ PSPACE

Beweis. Zu zeigen: Wenn für jedes $\mathfrak{A}$ $F^\psi_\mathfrak{A}$ mit polynomiellen Platz (bzgl. $|A|$) berechenbar ist, dann auch der partielle Fixpunkt.

Wir können aber nicht die gesamte Folge $R^0, R^1, \ldots$ berechnen und jeweils testen, ob $R^n = R^i$ für ein $i < n$, da dafür exponentiell viel Speicher gebraucht wird. Die Lösung ist dafür ist, jeweils die letzten beiden berechneten Stufen zu speichern und zu zählen, wie viele Stufen bereits berechnet wurden.

Sei $F^\psi_\mathfrak{A}$ also PSPACE-berechenbar, $n = |A|$ und $k =$ Stelligkeit(R). Frage: Gilt $\mathfrak{A} \models [\mathrm{pfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{a})$?.

Diese Frage soll von folgendem Algorithmus mit Polynomiellen Platzverbrauch gelöst werden:

$R \leftarrow \emptyset$
for $i = 0, \ldots, 2^{n^k}$ **do**

$R^* \leftarrow F^{\psi}_{\mathfrak{A}}(R)$
if $R^* = R$ **then**
  if $\bar{a} \in R^\star$ **then**
    return true
  else
    return false
  end if
else
  $R \leftarrow R^*$
end if
end for
return false

$\square$

Definition 4.7 (Infinitäre Logik mit beschränkter Variablenanzahl)
Wir definieren $\mathrm{L}^k_{\infty\omega} \coloneqq \{\psi \in \mathrm{L}_{\infty\omega} : \psi \text{ besitzt nur die Variablen } x_1, \dots, x_k\}$ und als Zusammenfassung $\mathrm{L}^\omega_{\infty\omega} \coloneqq \bigcup_{k<\omega} \mathrm{L}^k_{\infty\omega}$.

Satz 4.10
$\mathrm{LFP}, \mathrm{IFP}, \mathrm{PFP} \subseteq \mathrm{L}^\omega_{\infty\omega}$

Beweis. Sei $\psi(R, x_1, \dots, x_m) \in \mathrm{L}^\omega_{\infty\omega}$ eine Formel, welche die Variablen $x_1, \dots, x_m, y_1, \dots, y_l$ benutzt. Dann lässt sich jede Stufe R^α der lfp-Induktion durch eine Formel $\psi^\alpha(x_1, \dots, x_m) \in \mathrm{L}^{2m+l}_{\infty\omega}$ beschreiben. Dabei werden zusätzlich zu $x_1, \dots, x_m, y_1, \dots, y_l$ die Variablen $z_1, \dots, z_m$ verwendet.

Wir definieren $\psi^0(\bar{x}) = x_1 \neq x_1$ und

$$\psi^{\alpha+1} \coloneqq \psi[R\underbrace{u_1 \dots u_m}_{\bar{u}}/\exists \bar{z}(\bar{z} = \bar{u} \wedge \exists \bar{x}(\bar{x} = \bar{z} \wedge \psi^\alpha(\bar{x})))].$$

$\bar{u}$ ist dann ein Tupel von Variablen aus $x_1, \dots, x_m, y_1, \dots, y_l$ und in allen ψ^α kommen solche Variablen nur in R-Atomen vor. Es folgt $LFP \subseteq \mathrm{L}^\omega_{\infty\omega}$.

Für IFP ist dies analog, mit dem einzigen Unterschied, dass der Induktionsschritt als $\psi^{\alpha+1} :\!- \psi^\alpha \vee \psi[\dots]$ definiert werden muss.

Während wir aber bei LFP und IFP den Fixpunkt einfach als $\bigvee_{\alpha<\kappa^+} \psi^\alpha(\bar{x})$ definieren können, muss bei PFP das Abschlusskriterium explizit formuliert werden:

$$[\mathrm{pfp}\, R\bar{x}.\psi(R, \bar{x})](\bar{x}) \equiv \bigvee_{n<\omega} \forall \bar{x}((\psi^{n+1}(\bar{x}) \leftrightarrow \psi^n(\bar{x})) \wedge \psi^n(\bar{x})).$$

$\square$

Für $\mathrm{L}^k_{\infty\omega}$ lässt sich eine Abwandlung des EF-Spiels definieren. $\mathfrak{A}, \bar{a} \equiv^k \mathfrak{B}, \bar{b}$: für jede Formel $\psi(\bar{x}) \in \mathrm{L}^k_{\infty\omega}$ gilt $\mathfrak{A} \models \psi(\bar{a}) \Leftrightarrow \mathfrak{B} \models \psi(\bar{b})$. Dies führt und zu folgendem Spiel:

Definition 4.8 (k-pebble game)
Die Positionen sind Tupel $\bar{a} = (a_1, \dots, a_i)$ und $\bar{b} = (b_1, \cdots, b_i)$ mit $i \leq k$.

In einem Zug wählt I ein $j \leq k$ und ein Element $a'_j \in A$ oder $b'_j \in B$. II antwortet mit einem Element der anderen Struktur ($b'_j \in B$ oder $a'_j \in A$). Die neue Position ist dann $\bar{a}\frac{a'_j}{a_j}$, $\bar{b}\frac{b'_j}{b_j}$. Die neue Syntax bedeutet einfach, dass falls a_j in $\bar{a}$ vorhanden war, dieses durch a'_j ersetzt wird. Andernfalls wird a'_j zu $\bar{a}$ hinzugefügt.

I gewinnt, wenn $\bar{a} \mapsto \bar{b} \notin \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ und II gewinnt, wenn sie nie verliert.

Satz 4.11
II gewinnt das k-pebble game von $\mathfrak{A}, \bar{a}$, $\mathfrak{B}, \bar{b}$ aus gdw. $\mathfrak{A}, \bar{a} \equiv^k \mathfrak{B}, \bar{b}$

Der Beweis lässt sich einfach aus dem Satz von Ehrenfeucht-Fraïssé herleiten.

Können LFP, IFP, PFP **zählen?**

Wir definieren die Klassen

$$\text{EVEN} = \{A : |A| \text{ gerade}\}$$

und

$$\text{EVEN}_< = \{(A, <) : < \text{ lineare Ordnung auf } A, |A| \text{ gerade}\}.$$

Es gilt $\text{EVEN}_< \in \text{LFP}$:

$$\begin{aligned} \psi := ``< \text{ ist lin. Ord.''} \wedge \\ &\exists x(``x \text{ ist das kleinste Element''}) \wedge \\ &\exists y(``y \text{ ist das größte Element''}) \wedge \\ &\neg[\text{lfp}\, Gz : z = x \vee \exists u(Gu \wedge ``z \text{ is übernächstes Element nach } u''))](y) \end{aligned}$$

Die Fixpunktinduktion definiert dabei die Menge der geraden Elemente bzgl. $<$.

Satz 4.12
Es gilt aber $\text{EVEN} \notin \text{L}^{\omega}_{\infty\omega}$ (also $\notin$ LFP, IFP, PFP).

Beweis. Sei $\psi \in \text{L}^{k}_{\infty\omega}(\emptyset)$. Zu zeigen: Es gibt endliche Mengen A und B, wobei $|A|$ gerade und $|B|$ ungerade ist, aber $A \equiv^k B$.

Sei dafür $\bar{a} = (a_1, \ldots, a_k) \in A^k$ und $\bar{b} = (b_1, \ldots, b_k) \in B^k$. Dann ist $A, \bar{a} \equiv^k B, \bar{b}$ gdw. $\bar{a}$ und $\bar{b}$ den gleichen Gleichehitstype haben (also $a_i = a_j$ gdw. $b_i = b_j$ $\forall i, j \leq k$) und $|A|, |B| \geq k$. Dann gewinnt II das k-pebble game auf A, B und EVEN ist nicht in $\text{L}^{\omega}_{\infty\omega}$ definierbar. □

Ein anderer Beweisansatz ist der über das 0-1-Gesetz.

Satz 4.13 (0-1-Gesetz)
Für jeden Satz $\psi \in \text{L}^{\omega}_{\infty\omega}(\tau)$ konvergieren die Wahrscheinlichkeiten $\mu_n(\psi) = \Pr[\mathfrak{A} \models \psi : \mathfrak{A}$ eine τ-Struktur mit Universum $0, \ldots, n-1]$ entweder gegen 0 oder gegen 1, wenn $n \to \infty$.

Es gilt

$$\mu_n(\text{EVEN}) = \begin{cases} 0 & n \text{ ungerade} \\ 1 & n \text{ gerade,} \end{cases}$$

also gibt es keinen Grenzwert $\lim\limits_{n\to\infty} \mu_n(\text{EVEN})$. EVEN lässt sich also nicht $\text{L}^{\omega}_{\infty\omega}$ definieren.

Daran, dass $\text{EVEN}_<$ aber definierbar ist lässt sich erkennen, dass es geordnete Strukturen besser definierbar sind. Es ist tatsächlich so, dass es auf geordneten Strukturen einen sehr engen Zusammenhang zwischen Logik und Komplexität gibt. So gilt in diesem Fall LFP $\equiv$ IFP $\equiv$ PTIME und PFP $\equiv$ PSPACE.

Satz 4.14
Jede Eigenschaft geordneter endlicher Strukturen ist $\text{L}^{\omega}_{\infty\omega}$ definierbar.

Beweis. Wir zeigen dies für $\tau = \{E, <\}$, also geordnete Graphen. Sei dafür $\mathfrak{C}$ eine beliebiger Klasse endlicher, geordneter Graphen $G = (V, E, <)$.

Nun können wir eine Formel $\varphi_n(x) \in \text{L}^{2}_{\infty\omega}$ definieren die besagt, dass x das n-te Element der Struktur ist:

- $\varphi_0(x) \coloneqq \neg\exists y(y < x)$
- $\varphi_{n+1}(x) \coloneqq \exists y(y < x \wedge \varphi_n(y)) \wedge \forall y(y < x \to \bigvee_{m \leq n} \varphi_m(y))$, wobei $\varphi_n(y)$ die Formel Formel ist, in der alle x und y Vorkommen vertauscht wurden.

Für $G = (V, E^G, <)$ mit $V = \{v_1, \ldots, v_n\}$, $v_i < v_j \Leftrightarrow i < j$ definieren wir nun die Formel

$$\psi_G \coloneqq \forall x \forall y (Exz \leftrightarrow \bigvee_{(v_i,v_j) \in E^G} (\varphi_i(x) \wedge \varphi_j(z)) \wedge \exists x \varphi_n(x) \wedge \neg\exists x \varphi_{n+1}(x)) \in \mathrm{L}^3_{\infty\omega}\,.$$

Setze nun $\eta^{\mathfrak{C}} \coloneqq \bigvee\{\psi_G : G \in \mathfrak{C}\} \in \mathrm{L}^3_{\infty\omega}$. $\square$