GRUNDSTRUKTUREN

Skript zur Vorlesung 2024

Lorenz Halbeisen

ETH Zürich

Das Skript wurde im Frühling 2022 zur Vorlesung “Grundstrukturen” geschrieben und im Frühling 2024 überarbeitet. Bei dieser Gelegenheit möchte ich den Studierenden, insbesondere Herrn Roy Seitz, für die zahlreichen Kommentare und Verbesserungsvorschläge danken.

INHALTSVERZEICHNIS

0. TERME, FORMELN UND FORMALE BEWEISE

In diesem Kapitel wird die Syntax (auch Sprache genannt) der Logik erster Stufe definiert. Insbesondere werden wir definieren, was Terme und Formeln sind. Dafür brauchen wir zuerst ein sogenanntes *Alphabet*, d.h. ein Vorrat an Zeichen und Symbolen, aus dem wir Terme und Formeln bilden können.

DAS ALPHABET

Das Alphabet der Logik erster Stufe besteht aus folgenden Zeichen und Symbolen:

(a) **Variablen**: Zum Beispiel $x, y, v_0, v_1, \ldots$, von denen wir einen unendlichen Vorrat haben. Variablen stehen für Objekte, die wir untersuchen. Diese Objekte können zum Beispiel natürliche Zahlen sein (in der Zahlentheorie), oder auch Mengen (in der Mengenlehre), oder Vektoren (in der linearen Algebra), etc.

(b) **Logische Operatoren**: $\neg$ (*nicht*), $\wedge$ (*und*), $\vee$ (*oder*), $\rightarrow$ (*impliziert*).

(c) **Logische Quantoren**: $\exists$ (*Existenzquantor*) und $\forall$ (*Allquantor*), nach einem logischen Quantor steht *immer* eine Variable.

(d) **Gleichheitsrelation** $=$: Das Zeichen "$=$" steht für eine spezielle binäre Relation, nämlich für die Gleichheitsrelation.

(e) **Konstantensymbole**: Diese Symbole werden verwendet um spezielle Konstanten (in einer Theorie) zu bezeichnen. Konstantensymbole sind zum Beispiel 0 (in der Zahlentheorie), $\emptyset$ (in der Mengenlehre), etc.

(f) **Funktionssymbole**: Diese Symbole werden verwendet um spezielle Funktionen (in einer Theorie) zu bezeichnen. Funktionssymbole sind zum Beispiel $+$ (in der Zahlentheorie), $\sin$ (in der Analysis), etc. Zu jedem Funktionssymbol gehört eine *Stelligkeit*. Zum Beispiel ist $+$ ein 2-stelliges Funktionssymbol und $\sin$ ist ein 1-stelliges Funktionssymbol.

(g) **Relationssymbole**: Diese Symbole werden verwendet um spezielle Relationen (in einer Theorie) zu bezeichnen. Relationssymbole sind zum Beispiel $<$ (in der Zahlentheorie), $\in$ (in der Mengenlehre), etc. Zu jedem Relationssymbol gehört eine *Stelligkeit*. Zum Beispiel sind $<$ und $\in$ beides 2-stellige Relationssymbole.

Die Symbole (a)–(d) sind die **logischen Symbole**, diese Symbole haben wir immer. Die Symbole (e)–(g) sind die **nicht-logischen Symbole**, welche und wieviele dieser Symbole wir haben, hängt von der Theorie ab, die wir untersuchen. Die nicht-logischen Symbole einer Theorie bilden die **Signatur** (oder Sprache) der Theorie, diese wird mit $\mathscr{L}$ oder $\mathscr{L}_{\mathsf{T}}$ (für eine Theorie T) bezeichnet. Zum Beispiel ist $\mathscr{L}_{\mathsf{ZFC}} = \{\in\}$ die Signatur der Mengenlehre ZFC.

TERME

Mit den Zeichen des Alphabets können wir nun spezielle Zeichenketten oder Wörter bilden. In der Sprache der Logik erster Stufe heissen diese Zeichenketten *Terme*. Im Folgenden sei $\mathscr{L}$ eine beliebige Signatur.

Eine Zeichenkette ist ein **$\mathscr{L}$-Term**, oder einfach ein **Term**, falls die Zeichenkette durch endlich viele Anwendungen der folgenden Regeln entstanden ist.

(T0) Jede Variable ist ein $\mathscr{L}$-Term.
(T1) Jedes Konstantensymbol in $\mathscr{L}$ ist ein $\mathscr{L}$-Term.

(T2) Sind $\tau_1, \ldots, \tau_n$ bereits konstruierte $\mathscr{L}$-Terme und ist F ein n-stelliges Funktionssymbol in $\mathscr{L}$, dann ist $F\tau_1 \cdots \tau_n$ ein $\mathscr{L}$-Term.

Um die Regel (T2) zu definieren, haben wir Variablen für Terme gebraucht. Da nun Variablen aus unserem Alphabet selber Terme sind, haben wir neue Variablen τ_i, die nicht zu unserem Alphabet gehören, eingeführt.

FORMELN

Mit Termen (bzw. mit den Wörtern) und weitern Zeichen aus unserem Alphabet, können wir nun wieder spezielle Zeichenketten oder Sätze bilden. In der Sprache der Logik erster Stufe heissen diese Zeichenketten *Formeln*. Im Folgenden sei $\mathscr{L}$ eine beliebige Signatur.

Eine Zeichenkette ist eine **$\mathscr{L}$-Formel**, oder einfach eine **Formel**, falls die Zeichenkette durch endlich viele Anwendungen der folgenden Regeln entstanden ist.

(F0) Sind τ_1 und τ_2 $\mathscr{L}$-Terme, dann ist $= \tau_1\tau_2$ eine $\mathscr{L}$-Formel.
(F1) Sind $\tau_1, \ldots, \tau_n$ bereits konstruierte $\mathscr{L}$-Terme und ist R ein n-stelliges Relationssymbol in $\mathscr{L}$, dann ist $R\tau_1 \cdots \tau_n$ eine $\mathscr{L}$-Formel.
(F2) Ist φ eine bereits konstruierte $\mathscr{L}$-Formel, dann ist $\neg\varphi$ eine $\mathscr{L}$-Formel.
(F3) Sind φ und ψ bereits konstruierte $\mathscr{L}$-Formeln, dann sind $\wedge\varphi\psi$, $\vee\varphi\psi$, und $\rightarrow \varphi\psi$ ebenfalls $\mathscr{L}$-Formeln.
(F4) Ist φ eine bereits konstruierte $\mathscr{L}$-Formel und ν eine beliebige Variable, dann sind $\exists\nu\varphi$ und $\forall\nu\varphi$ ebenfalls $\mathscr{L}$-Formeln.

Um Formeln einfach lesbar zu machen verwenden wir üblicherweise die Infix-Notation mit Klammern anstelle der polnischen Notation. Zum Beispiel schreiben wir $\varphi \wedge \psi$ anstelle von $\wedge\varphi\psi$, $(\varphi \rightarrow \psi) \rightarrow \varphi$ anstelle von $\rightarrow\rightarrow \varphi\psi\varphi$, etc.

Weiter schreiben wir für binäre Relationssymbole R und binäre Funktionssymbole F meist xRy und xFy anstelle von Rxy bzw. Fxy. Zum Beispiel schreiben wir $x = y$ anstelle von $= xy$, und $x + y$ anstelle von $+xy$.

Ist eine Formel φ von der Form $\exists\nu\psi$ oder $\forall\nu\psi$ (für eine Variable ν und eine Formel ψ) und die Variable ν kommt in ψ vor, dann sagen wir, dass die Variable ν im Bereich eines logischen Quantors ist; die Variable wird dann durch den Quantor **gebunden**. Ist eine Variable ν in einer Formel ψ an einer gewissen Stelle nicht im Bereich eines Quantors (d.h. die Variable ist nicht gebunden), so kommt die Variable ν an der entsprechenden Stelle **frei** vor in ψ. Die Menge der Variablen, welche in einer Formel ψ frei vorkommen, wird mit $\mathrm{frei}(\psi)$ bezeichnet. Da eine Variable in einer Formel ψ an mehreren Stellen vorkommen kann, kann eine Variable sowohl frei wie auch gebunden in ψ vorkommen. Zum Beispiel kommt die Variable x in der Formel $\exists z(x = z) \wedge \forall x(x = y)$ sowohl frei wie auch gebunden vor. Durch Umbenennen der Variablen lässt sich aber erreichen, dass jede Variable in einer Formel entweder nur gebunden oder nur frei vorkommt.

Eine Formel φ ist ein **Satz**, falls φ keine freien Variablen enthält (d.h. $\mathrm{frei}(\varphi) = \emptyset$). Zum Beispiel ist $\forall x\forall y(x = y)$ ein Satz, aber $\forall x(x = y)$ ist nur eine Formel.

Manchmal ist es nützlich die freien Variablen in einer Formel explizit aufzulisten; wir schreiben $\varphi(x_1, \ldots, x_n)$ um anzuzeigen, dass die Variablen $x_1, \ldots, x_n$ frei in φ vorkommen.

Ist φ eine Formel, ν eine Variable und τ ein Term, dann ist $\varphi(\nu/\tau)$ diejenige Formel, die wir erhalten, wenn wir an jeder Stelle, an der die Variable ν in φ frei vorkommt, die Variable ν ersetzen durch den Term τ. Dieser Prozess, bei dem wir aus φ die Formel $\varphi(\nu/\tau)$ erhalten, heisst **Substitution**. Eine Substitution $\varphi(\nu/\tau)$ ist nur dann **zulässig**, wenn keine Variable im Term τ durch Quantoren von φ gebunden werden. Beachte, dass falls $x \notin \mathrm{frei}(\varphi)$ und x im

Term τ nicht vorkommt die Substitution $\varphi(x/\tau)$ zulässig ist. In diesem Fall ist die Formel φ identisch mit $\varphi(x/\tau)$, was wir durch $\varphi \equiv \varphi(x/\tau)$ ausdrücken — das Gleichheitszeichen "=" macht zwischen Formeln keinen Sinn.

Die Logischen Axiome

Bei der Definition von Formeln haben wir zwar Zeichen wie zum Beispiel "=" oder "$\wedge$" gebraucht, wir haben aber nicht festgelegt, was diese Zeichen später, wenn wir Formeln interpretieren werden, bedeuten sollen. Zum Beispiel möchten wir, dass die Formel $x = x$ "wahr" ist. Da es aber auf der syntaktischen Ebene keinen Wahrheitsbegriff gibt, können wir $x = x$ nicht einfach als "wahr" definieren. Wir können aber gewisse Formeltypen (oder Formelschemata), wie zum Beispiel $x = x$, auszeichnen. Die folgenden **logischen Axiome**, eigentlich *Axiomenschemata*, sind solche ausgezeichneten Formeltypen, welche den Gebrauch der logischen Operatoren und Quantoren sowie der Gleichheitsrelation regeln.

Sei $\mathscr{L}$ eine Signatur und seien φ, φ_1, φ_2, φ_3, und ψ beliebige $\mathscr{L}$-Formeln:

L_0: $\varphi \vee \neg\varphi$
L_1: $\varphi \to (\psi \to \varphi)$
L_2: $(\psi \to (\varphi_1 \to \varphi_2)) \to ((\psi \to \varphi_1) \to (\psi \to \varphi_2))$
L_3: $(\varphi \wedge \psi) \to \varphi$
L_4: $(\varphi \wedge \psi) \to \psi$
L_5: $\varphi \to (\psi \to (\psi \wedge \varphi))$
L_6: $\varphi \to (\varphi \vee \psi)$
L_7: $\psi \to (\varphi \vee \psi)$
L_8: $(\varphi_1 \to \varphi_3) \to ((\varphi_2 \to \varphi_3) \to ((\varphi_1 \vee \varphi_2) \to \varphi_3))$
L_9: $\neg\varphi \to (\varphi \to \psi)$

Sei τ ein $\mathscr{L}$-Term, ν eine Variable, und sei die Substitution $\varphi(\nu/\tau)$ zulässig:

L_{10}: $\forall\nu\varphi(\nu) \to \varphi(\tau)$
L_{11}: $\varphi(\tau) \to \exists\nu\varphi(\nu)$

Sei ψ eine Formel und sei ν eine Variable mit $\nu \notin \mathrm{frei}(\psi)$:

L_{12}: $\forall\nu(\psi \to \varphi(\nu)) \to (\psi \to \forall\nu\varphi(\nu))$,
L_{13}: $\forall\nu(\varphi(\nu) \to \psi) \to (\exists\nu\varphi(\nu) \to \psi)$.

Seien τ, $\tau_1, \ldots, \tau_n$, $\tau'_1, \ldots, \tau'_n$ $\mathscr{L}$-Terme, sei $R \in \mathscr{L}$ ein n-stelliges Relationssymbol und sei $F \in \mathscr{L}$ ein n-stelliges Funktionssymbol:

L_{14}: $\tau = \tau$
L_{15}: $(\tau_1 = \tau'_1 \wedge \cdots \wedge \tau_n = \tau'_n) \to (R(\tau_1, \ldots, \tau_n) \to R(\tau'_1, \ldots, \tau'_n))$
L_{16}: $(\tau_1 = \tau'_1 \wedge \cdots \wedge \tau_n = \tau'_n) \to (F(\tau_1, \ldots, \tau_n) = F(\tau'_1, \ldots, \tau'_n))$

Die logischen Axiome L_0–L_9 sind die Axiome der Aussagenlogik, welche den Gebrauch der logischen Operatoren regeln, die logischen Axiome L_{10}–L_{13} regeln den Gebrauch der logischen Quantoren, und die logischen Axiome L_{14}–L_{16} regeln den Gebrauch der Gleichheitsrelation.

Nicht-Logischen Axiome

Wenn wir eine konkrete Theorie haben, wie zum Beispiel die Zahlentheorie, so kommen zu den logischen Axiomen sogenannte **nicht-logische Axiome** hinzu, welche den Gebrauch (bzw. die Bedeutung) der nicht-logischen Symbole dieser Theorie regeln. Die nicht-logischen Axiome

einer Theorie sind ausgezeichnete Formeln (meistens Sätze) welche wir meist mit $\mathbf{\Phi}$ (bzw. T) bezeichnen.

FORMALE BEWEISE

Um aus gegebenen Formeln Schlüsse zu ziehen oder Aussagen über bestimmte Terme zu machen, brauchen wir sowohl Schlussregeln wie auch einen Algorithmus, der uns sagt, auf welche Formeln wir die Schlussregeln anwenden können.

Wir brauchen nur zwei **Schlussregeln**, nämlich

$$\text{Modus Ponens (MP):}\quad \frac{\varphi \to \psi,\ \varphi}{\psi} \qquad \text{und} \qquad \text{Verallgemeinerung } (\forall):\quad \frac{\varphi}{\forall \nu \varphi}\,.$$

Im ersten Fall sagen wir, dass die Formel ψ aus den Formeln $\varphi \to \psi$ und φ durch Modus Ponens, abgekürzt (MP), entstanden ist, und im zweiten Fall sagen wir, dass die Formel $\forall \nu \varphi$ (wobei ν für irgend eine Variable steht) aus der Formel φ durch Verallgemeinerung, abgekürzt ($\forall$) entstanden ist.

Mit den zwei Schlussregeln (MP) und ($\forall$) können wir nun formale Beweise definieren: Sei $\mathscr{L}$ eine Signatur (d.h. eine möglicherweise leere Menge von nicht-logischen Symbolen) und sei $\mathbf{\Phi}$ eine (möglicherweise leere) Menge von $\mathscr{L}$-Formeln. Eine $\mathscr{L}$-Formel ψ ist **beweisbar** aus $\mathbf{\Phi}$ (oder beweisbar in $\mathbf{\Phi}$), bezeichnet mit $\mathbf{\Phi} \vdash \psi$, falls es eine endliche Sequenz $\varphi_0, \ldots, \varphi_n$ von $\mathscr{L}$-Formeln gibt, sodass $\varphi_n \equiv \psi$ (d.h. die Formeln φ_n und ψ sind identisch), und für alle i mit $i \leq n$ sind wir in mindestens einem der folgenden Fälle:

- φ_i ist eine Instanziierung eines logischen Axioms
- φ_i ist eine Formel aus $\mathbf{\Phi}$
- es gibt $j, k < i$ sodass $\varphi_j \equiv \varphi_k \to \varphi_i$
- es gibt ein $j < i$, sodass $\varphi_i \equiv \forall \nu\, \varphi_j$ für eine Variable ν die in keiner Formel von $\mathbf{\Phi}$ frei vorkommt

Die Sequenz $\varphi_0, \ldots, \varphi_n$ ist dann ein **formaler Beweis** von ψ aus $\mathbf{\Phi}$.

Im Fall, wenn $\mathbf{\Phi}$ die leere Menge ist, schreiben wir einfach $\vdash \psi$. Ist eine Formel ψ nicht aus $\mathbf{\Phi}$ beweisbar (d.h. es gibt keinen formalen Beweis von ψ aus $\mathbf{\Phi}$), so schreiben wir $\mathbf{\Phi} \nvdash \psi$.

Formale Beweise, auch für sehr einfache Formeln, können recht lang und knifflig sein. Als Beispiel für einen formalen Beweis zeigen wir:

$$\vdash \varphi \to \varphi$$

φ_0:	$(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$	Instanziierung von L_2
φ_1:	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	Instanziierung von L_1
φ_2:	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	aus φ_0 und φ_1 mit (MP)
φ_3:	$\varphi \to (\varphi \to \varphi)$	Instanziierung von L_1
φ_4:	$\varphi \to \varphi$	aus φ_2 und φ_3 mit (MP)

Das folgende Theorem ist sehr nützlich um formale Beweise zu vereinfachen.

DEDUKTIONSTHEOREM (DT). *Ist $\mathbf{\Phi}$ eine Menge von Formeln und gilt $\mathbf{\Phi} + \psi \vdash \varphi$, so gilt auch $\mathbf{\Phi} \vdash \psi \to \varphi$; und umgekehrt, gilt $\mathbf{\Phi} \vdash \psi \to \varphi$, dann gilt auch $\mathbf{\Phi} + \psi \vdash \varphi$.*

Beweis. Mit (MP) folgt aus $\mathbf{\Phi} \vdash \psi \to \varphi$ direkt $\mathbf{\Phi} + \psi \vdash \varphi$. Für die andere Richtung nehmen wir an, dass $\mathbf{\Phi} + \psi \vdash \varphi$ gilt. Sei nun die Sequenz $\varphi_0, \ldots, \varphi_n$ mit $\varphi_n \equiv \varphi$ ein formaler Beweis von φ aus $\mathbf{\Phi} + \psi$. Für jedes $i \leq n$ ersetzen wir nun φ_i durch eine Sequenz von Formeln, welche mit $\psi \to \varphi_i$ endet. Dazu sei $i \leq n$ und wir nehmen an, dass $\mathbf{\Phi} \vdash \psi \to \varphi_j$ gilt für alle $j < i$.

- Ist φ_i ein logisches Axiom oder $\varphi_i \in \mathbf{\Phi}$, dann haben wir:

$\varphi_{i,0}$:	φ_i	$\varphi_i \in \mathbf{\Phi}$ oder φ_i ist ein logisches Axiom
$\varphi_{i,1}$:	$\varphi_i \to (\psi \to \varphi_i)$	Instanziierung von L_1
$\varphi_{i,2}$:	$\psi \to \varphi_i$	aus $\varphi_{i,1}$ und $\varphi_{i,0}$ mit (MP)

- Der Fall $\varphi_i \equiv \psi$ folgt direkt aus $\vdash \varphi_i \to \varphi_i$, was im obigen Beispiel gezeigt wurde.

- Falls φ_i aus φ_j und $\varphi_k \equiv (\varphi_j \to \varphi_i)$ durch Modus Ponens erhalten wurde, wobei $j, k < i$, dann haben wir:

$\varphi_{i,0}$:	$\psi \to \varphi_j$	weil $j < i$
$\varphi_{i,1}$:	$\psi \to (\varphi_j \to \varphi_i)$	weil $k < i$
$\varphi_{i,2}$:	$\varphi_{i,1} \to ((\psi \to \varphi_j) \to (\psi \to \varphi_i))$	Instanziierung von L_2
$\varphi_{i,3}$:	$(\psi \to \varphi_j) \to (\psi \to \varphi_i)$	aus $\varphi_{i,2}$ und $\varphi_{i,1}$ mit (MP)
$\varphi_{i,4}$:	$\psi \to \varphi_i$	aus $\varphi_{i,3}$ und $\varphi_{i,0}$ mit (MP)

- Falls φ_i aus φ_j durch Verallgemeinerung erhalten wurde, dann folgt die Behauptung aus:

$\varphi_{i,0}$:	$\psi \to \varphi_j$	weil $j < i$
$\varphi_{i,1}$:	$\forall\nu(\psi \to \varphi_j)$	aus $\varphi_{i,0}$ durch ($\forall$)
$\varphi_{i,2}$:	$\forall\nu(\psi \to \varphi_j) \to (\psi \to \varphi_i)$	Instanziierung von L_{12}
$\varphi_{i,3}$:	$\psi \to \varphi_i$	aus $\varphi_{i,2}$ und $\varphi_{i,1}$ mit (MP)

Somit haben wir gezeigt, dass $\mathbf{\Phi} \vdash \psi \to \varphi$ gilt. ⊣

Als Anwendung des DEDUKTIONSTHEOREMS zeigen wir, dass die Gleichheitsrelation "$=$" eine Äquivalenzrelation ist: Eine binäre Relation R ist eine **Äquivalenzrelation** falls R reflexiv, symmetrisch und transitiv ist.

reflexiv:	$\forall x(xRx)$
symmetrisch:	$\forall x \forall y(xRy \to yRx)$
transitiv:	$\forall x \forall y \forall z\big((xRy \wedge yRz) \to xRz\big)$

Wir zeigen nun, dass die binäre Relation "$=$" reflexiv und symmetrisch ist; dass "$=$" auch transitiv ist wird in Aufgabe 2 gezeigt.

"$=$" ist reflexiv:

φ_0:	$x = x$	Instanziierung von L_{14}
φ_1:	$\forall x(x = x)$	aus φ_0 mit ($\forall$)

"=" ist symmetrisch:
Wir zeigen zuerst $\{x = y\} \vdash y = x$, d.h. $\mathbf{\Phi} \vdash y = x$ für $\mathbf{\Phi}$ die Menge mit der einzigen Formel $x = y$.

φ_0:	$(x = y \wedge x = x) \to (x = x \to y = x)$	Instanziierung von L_{15}
φ_1:	$x = x$	Instanziierung von L_{14}
φ_2:	$x = y$	$x = y \in \mathbf{\Phi}$
φ_3:	$x = x \to (x = y \to (x = y \wedge x = x))$	Instanziierung von L_5
φ_4:	$x = y \to (x = y \wedge x = x)$	aus φ_3 und φ_1 mit (MP)
φ_5:	$x = y \wedge x = x$	aus φ_4 und φ_2 mit (MP)
φ_6:	$x = x \to y = x$	aus φ_0 und φ_5 mit (MP)
φ_7:	$y = x$	aus φ_6 und φ_1 mit (MP)

Somit haben wir $\{x = y\} \vdash y = x$. Mit dem DEDUKTIONSTHEOREM erhalten wir also

$$\vdash x = y \to y = x$$

und durch Verallgemeinerung erhalten wir schliesslich:

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

LOGISCHE ÄQUIVALENZ

Die Formel $\varphi \leftrightarrow \psi$ ist eine abgekürzte Schreibweise für $(\varphi \to \psi) \wedge (\psi \to \varphi)$, d.h. jede Formel, in welcher der binäre logische Operator $\leftrightarrow$ vorkommt, kann ersetzt werden durch eine Formel, in welcher $\leftrightarrow$ nicht mehr vorkommt. Wir sagen nun, dass zwei Formeln φ und ψ **logisch äquivalent** sind, in Zeichen $\varphi \Leftrightarrow \psi$, falls gilt:

$$\vdash \varphi \leftrightarrow \psi \quad \text{bzw.} \quad \vdash (\varphi \to \psi) \wedge (\psi \to \varphi)$$

Mit L_5 und (MP) gilt $\varphi \Leftrightarrow \psi$ genau dann wenn

$$\vdash \varphi \to \psi \quad \text{und} \quad \vdash \psi \to \varphi\,.$$

Der Beweis des folgenden Satzes benutzt "Metainduktion" über den Formelaufbau und ist relativ aufwendig.

SATZ ÜBER LOGISCHE ÄQUIVALENZ. *Sei φ eine Formel und sei α eine Teilformel von φ. Weiter sei ψ eine Formel, die aus φ dadurch entstanden ist, dass in φ ein- oder mehrmals α durch eine Formel β ersetzt wurde. Dann gilt:*

$$\textit{Ist} \;\; \alpha \Leftrightarrow \beta, \quad \textit{so ist auch} \;\; \varphi \Leftrightarrow \psi.$$

1. AXIOMENSYSTEME UND SEMI-FORMALE BEWEISE

In diesem Kapitel werden die Axiome einiger Theorien aufgelistet und es wird der Begriff eines *semi-formalen* Beweises eingeführt.

AXIOMENSYSTEME

Gruppentheorie GT**.** Die Signatur der Gruppentheorie ist $\mathscr{L}_{\mathsf{GT}} = \{\mathtt{e}, \circ\}$, wobei $\mathtt{e}$ ein Konstantensymbol und $\circ$ ein 2-stelliges Funktionssymbol ist.

Die Axiome der Gruppentheorie sind:

GT_0:	$\forall x \forall y \forall z \big(x \circ (y \circ z) = (x \circ y) \circ z\big)$	($\circ$ ist *assoziativ*)
GT_1:	$\forall x (\mathtt{e} \circ x = x)$	($\mathtt{e}$ ist *links-neutral*)
GT_2:	$\forall x \exists y (y \circ x = \mathtt{e})$	(jedes Element hat ein *links-Inverses*)

Strenggenommen sind die Erläuterungen in den Klammern nicht korrekt: Zum Beispiel kann das Funktionssymbol $\circ$ als *Symbol* nicht assoziativ sein. Erst, wenn das Funktions*symbol* $\circ$ in einem *Modell* $\mathbf{M}$ als 2-stellige *Funktion* $\circ^{\mathbf{M}} : A \times A \to A$ interpretiert wird, kann die Funktion $\circ^{\mathbf{M}}$ assoziativ sein, und das ist, was mit GT_0 gemeint ist.

Es sei nochmals erwähnt, dass es auf der syntaktischen (oder formalen) Ebene, auf der wir uns befinden, weder Konstanten, noch Funktionen oder Relationen gibt, sondern nur verschiedene, bedeutungslose Typen von Symbolen. Es gibt auch kein wahr und falsch, sondern nur syntaktisch korrekt geformte Terme und Formeln. Erst auf der semantischen Ebene, die im nächsten Kapitel behandelt wird, werden den Termen Objekte zugeordent, den Funktionssymbolen Funktionen, und den Relationssymbolen Relationen.

Ringtheorie RT**.** Die Signatur der Ringtheorie (für Ringe mit 1) ist $\mathscr{L}_{\mathsf{RT}} = \{\mathtt{0}, \mathtt{1}, +, \cdot\}$, wobei $\mathtt{0}$ und $\mathtt{1}$ Konstantensymbole sind und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Ringtheorie (für Ringe mit 1) sind:

RT_0:	$\forall x \forall y \forall z \big(x + (y + z) = (x + y) + z\big)$	($+$ ist *assoziativ*)
RT_1:	$\forall x \forall y (x + y = y + x)$	($+$ ist *kommutativ*)
RT_2:	$\forall x (\mathtt{0} + x = x)$	($\mathtt{0}$ ist *links-neutral* bzgl. $+$)
RT_3:	$\forall x \exists y (y + x = \mathtt{0})$	(*links-Inverse* bzgl. $+$)
RT_4:	$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	($\cdot$ ist *assoziativ*)
RT_5:	$\forall x (\mathtt{1} \cdot x = x \wedge x \cdot \mathtt{1} = x)$	($\mathtt{1}$ ist *neutral* bzgl. $\cdot$)
RT_6:	$\forall x \forall y \forall z \big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$	($\cdot$ ist *links-distributiv* über $+$)
RT_7:	$\forall x \forall y \forall z \big((x + y) \cdot z = (x \cdot z) + (y \cdot z)\big)$	($\cdot$ ist *rechts-distributiv* über $+$)

Lässt man RT_5 weg, so erhält man auf der semantischen Ebene Ringe ohne 1, und verlangt man zusätzlich RT_8: $\forall x \forall y (x \cdot y = y \cdot x)$, so erhält man auf der semantischen Ebene *kommutative Ringe* (mit bzw. ohne 1).

Da die Operation $+$ mit RT_1 kommutativ ist, ist $\mathtt{0}$ auch rechts-neutral (also neutral) bzgl. $+$ und jedes Element hat bzgl. $+$ ein rechts-Inverses (also ein Inverses).

Körpertheorie KT**.** Die Signatur der Körpertheorie ist $\mathscr{L}_{\mathsf{KT}} = \{\mathtt{0}, \mathtt{1}, +, \cdot\}$, wobei $\mathtt{0}$ und $\mathtt{1}$ Konstantensymbole sind und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Körpertheorie sind:

KT_0:	$\forall x \forall y \forall z \big(x + (y + z) = (x + y) + z\big)$	($+$ ist *assoziativ*)
KT_1:	$\forall x \forall y (x + y = y + x)$	($+$ ist *kommutativ*)
KT_2:	$\forall x (\mathtt{0} + x = x)$	($\mathtt{0}$ ist *link-neutral* bzgl. $+$)
KT_3:	$\forall x \exists y (y + x = \mathtt{0})$	(*links-Inverse* bzgl. $+$)
KT_4:	$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	($\cdot$ ist *assoziativ*)
KT_5:	$\forall x \forall y (x \cdot y = y \cdot x)$	($\cdot$ ist *kommutativ*)
KT_6:	$\forall x (\mathtt{1} \cdot x = x)$	($\mathtt{1}$ ist *link-neutral* bzgl. $\cdot$)
KT_7:	$\forall x \exists y (x \neq \mathtt{0} \to y \cdot x = \mathtt{1})$	(*links-Inverse* bzgl. $\cdot$ für $x \neq \mathtt{0}$)
KT_8:	$\forall x \forall y \forall z \big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$	($\cdot$ ist *links-distributiv* über $+$)
KT_9:	$\mathtt{0} \neq \mathtt{1}$	($\mathtt{0}$ ist verschieden von $\mathtt{1}$)

Da die Operationen $+$ und $\cdot$ mit KT_1 bzw. KT_5 kommutativ sind, sind links-neutrale Elemente auch rechts-neutral (also neutral), links-Inverse auch rechts-Inverse (also Inverse), und $\cdot$ ist auch *rechts-distributiv* über $+$.

Dichte Lineare Ordnungen DLO**.** Die Signatur der Theorie der dichten linearen Ordnungen ist $\mathscr{L}_{\mathsf{DLO}} = \{<\}$, wobei $<$ ein 2-stelliges Relationssymbol ist.

Die Axiome der Theorie der dichten linearen Ordnungen sind:

DLO_0:	$\forall x \neg (x < x)$	($<$ ist nicht *reflexiv*)
DLO_1:	$\forall x \forall y \forall z \big((x < y \wedge y < z) \to x < z\big)$	($<$ ist *transitiv*)
DLO_2:	$\forall x \forall y \big(x < y \vee x = y \vee y < x\big)$	($<$ definiert eine *lineare* Ordnung)
DLO_3:	$\forall x \forall y \exists z \big(x < y \to (x < z \wedge z < y)\big)$	($<$ definiert eine *dichte* Ordnung)
DLO_4:	$\forall x \exists y \exists z \big(y < x \wedge x < z\big)$	(keine grössten bzw. kleinsten Elemente)

Peano-Arithmetik PA**.** Die Signatur der Peano-Arithmetik ist $\mathscr{L}_{\mathsf{PA}} = \{\mathtt{0}, \mathtt{s}, +, \cdot\}$, wobei das Symbol $\mathtt{0}$ ein Konstantensymbol ist, $\mathtt{s}$ ein 1-stelliges Funktionssymbol ist, und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Peano-Arithmetik sind:

PA_0:	$\neg \exists x (\mathtt{s}x = \mathtt{0})$	($\mathtt{0}$ ist kein Nachfolger)
PA_1:	$\forall x \forall y (\mathtt{s}x = \mathtt{s}y \to x = y)$	($\mathtt{s}$ ist *injektiv*)
PA_2:	$\forall x (x + \mathtt{0} = x)$	(definiert $x + \mathtt{0}$)
PA_3:	$\forall x \forall y (x + \mathtt{s}y = \mathtt{s}(x + y))$	(definiert $x + \mathtt{s}y$)
PA_4:	$\forall x (x \cdot \mathtt{0} = \mathtt{0})$	(definiert $x \cdot \mathtt{0}$)
PA_5:	$\forall x \forall y (x \cdot \mathtt{s}y = (x \cdot y) + x)$	(definiert $x \cdot \mathtt{s}y$)

Sei φ eine $\mathscr{L}_{\mathsf{PA}}$-Formel und ν eine Variable mit $\nu \in \mathrm{frei}(\varphi)$:

PA_6: $\big(\varphi(\mathtt{0}) \wedge \forall \nu (\varphi(\nu) \to \varphi(\mathtt{s}\nu))\big) \to \forall \nu \varphi(\nu)$

Beachte, dass PA_6 (im Gegensatz zu den Axiomen PA_0–PA_5) nicht ein einzelnes Axiom ist, sondern ein Axiomenschema, denn für jede $\mathscr{L}_{\mathsf{PA}}$-Formel φ mit einer freien Variablen erhalten wir eine Form von PA_6. Das Axiomenschema PA_6 wird **Induktions-Axiom** genannt und wird

für Induktionsbeweise benutzt. Weil PA_6 ein Axiomenschema ist, besteht das Axiomensystem PA der Peano-Arithmetik aus unendlich vielen Axiomen.

SEMI-FORMALE BEWEISE

Wie schon erwähnt werden formale Beweise relativ schnell sehr lang. Das liegt daran, dass in einem formalen Beweis nicht nur die relevanten, theorieabhängigen Zusammenhänge vorkommen, welche durch die nicht-logischen Axiome gegeben sind, sondern auch alle inner-logischen Strukturen, welche aus den logischen Axiomen folgen. Wenn wir nun in einem formalen Beweis alle Schritte, bei denen wir mit logischen Axiomen gewisse Formeln umgeformt haben, weglassen, so beruhen die ausgeführten Schritte im Wesentlichen nur noch auf den nicht-logischen Axiomen. Wir nennen solche Beweise **semi-formale Beweise** (diese Definition ist naturgemäss ebenfalls semi-formal).

Als Beispiel für einen semi-formalen Beweis zeigen wir $\mathsf{PA} \vdash \mathtt{s0} + \mathtt{s0} = \mathtt{ss0}$ (vgl. mit Aufgabe 4):

$$\underbrace{\mathtt{s0} + \mathtt{s0}}_{=\mathtt{s0}+\mathtt{s(0)}} \overset{\mathsf{PA}_3}{=} \mathtt{s}(\underbrace{\mathtt{s0} + \mathtt{0}}_{=\mathtt{s0}}) \overset{\mathsf{PA}_2}{=} \mathtt{ss0}$$

Als Beispiel für einen semi-formalen Induktionsbeweis zeigen wir $\mathsf{PA} \vdash \forall x\big(\mathtt{ss0} \cdot x = x + x\big)$:

- Wir definieren: $\varphi(x) :\equiv \mathtt{ss0} \cdot x = x + x$
- $\mathsf{PA} \vdash \varphi(\mathtt{0})$: $\mathtt{ss0} \cdot \mathtt{0} \overset{\mathsf{PA}_4}{=} \mathtt{0} \overset{\mathsf{PA}_2}{=} \mathtt{0} + \mathtt{0}$
- $\mathsf{PA} \vdash \varphi(x) \to \varphi(\mathtt{s}x)$: Wir nehmen an, dass $\mathtt{ss0} \cdot x = x + x$ gilt, verwenden den bereits bewiesenen Satz $\mathtt{ss0} = \mathtt{s0} + \mathtt{s0}$, und verwenden implizit, dass $+$ assoziativ und kommutativ ist (siehe Aufgaben 6.(b) und 6.(d)).

$$\mathtt{ss0} \cdot \mathtt{s}x \overset{\mathsf{PA}_5}{=} (\underbrace{\mathtt{ss0} \cdot x}_{=x+x}) + \underbrace{\mathtt{ss0}}_{=\mathtt{s0}+\mathtt{s0}} =$$
$$(x + \mathtt{s0}) + (x + \mathtt{s0}) \overset{\mathsf{PA}_3}{=} \mathtt{s}(x + \mathtt{0}) + \mathtt{s}(x + \mathtt{0}) \overset{\mathsf{PA}_2}{=} \mathtt{s}x + \mathtt{s}x$$

- Wir haben somit $\mathsf{PA} \vdash \varphi(\mathtt{0})$ und $\mathsf{PA} \vdash \forall x\big(\varphi(x) \to \varphi(\mathtt{s}x)\big)$ gezeigt, und damit auch
$$\mathsf{PA} \vdash \varphi(\mathtt{0}) \wedge \forall x\big(\varphi(x) \to \varphi(\mathtt{s}x)\big)\,.$$
Mit dem Induktionsaxiom PA_6 erhalten wir dann schliesslich:
$$\mathsf{PA} \vdash \forall x\big(\mathtt{ss0} \cdot x = x + x\big)$$

2. MODELLE

SYNTAX UND SEMANTIK

Die mathematische Logik zerfällt in *Syntax* (Theorie der Beziehungen zwischen den Zeichen) und *Semantik* (Lehre der Bedeutung der Symbole, bzw. deren Interpretation). Im Vergleich zur Musik könnte man sagen, dass die Syntax (d.h. die formale Logik) der Partitur entspricht, welche Schwarz auf Weiss festhält, welche Noten gespielt werden sollen, während die Semantik der Umsetzung einer Partitur in hörbare Musik entspricht, welche sich zwar an die Partitur halten muss, in der Interpretation der Partitur aber frei ist. Obwohl die ganze Musik schon in der Partitur enthalten ist, so wird sie doch erst durch die Interpretation mit Leben erfüllt. Nehmen wir zum Beispiel als "Partitur" die Gruppenaxiome, so erhalten auch diese erst durch das betrachten konkreter Gruppen (d.h. erst durch die Interpretation) ihre Bedeutung. Bevor wir Terme und Formeln interpretieren und Modelle für axiomatische Theorien konstruieren, werden im Folgenden ein paar Parallelen zwischen der syntaktischen und der semantischen Ebene der Mathematik aufgezeigt.

Syntaktische Ebene	*Semantische Ebene*
Terme. Das sind Zeichenketten, welche nach den formalen Regeln (T0)–(T2) aufgebaut werden. Zum Beispiel ist das Konstantensymbol $\mathtt{e}$ der Gruppentheorie ein Term.	***Objekte***. Terme sind Namen für Objekte. Durch die Interpretation wird ein Term (Name) zu dem Objekt, welches er bezeichnet. Zum Beispiel wird das Konstantensymbol $\mathtt{e}$ durch die Interpretation zum Neutralelement e einer Gruppe, e ist also ein Objekt.
Formeln. Das sind Zeichenketten, welche nach den formalen Regeln (F0)–(F4) aufgebaut werden. Formeln sind weder wahr noch falsch; auf der syntaktischen Ebene gibt es keinen Wahrheitsbegriff!	***Aussagen***. Wird eine Formel interpretiert, so wird sie zu einer konkreten Aussage über bestimmte Objekte die entweder wahr oder falsch ist; und zwar unabhängig davon, ob wir ihren Wahrheitswert kennen.
Logische Axiome. Das sind Formeln, genauer Formelschemata, aus denen, mit Hilfe von Schlussregeln, weitere Formeln hergeleitet werden können.	***Tautologien***. Egal wie wir ein logisches Axiom interpretieren, die Aussage die wir erhalten ist immer wahr, eine sogenannte *Tautologie*. Die logischen Axiome sind so gewählt, dass aus ihnen alle Tautologien hergeleitet werden können.
Nicht-logische Axiome. Das sind Formeln (bzw. Formelschemata) welche nicht-logische Symbole enthalten, aus denen, mit Hilfe von Schlussregeln, weitere Formeln hergeleitet werden können. Zum Beispiel sind die Gruppenaxiome, welche die nicht-logischen Symbole $\mathtt{e}$ und $\circ$ enthalten, nicht-logische Axiome.	***Axiomensystem einer Theorie***. Das sind Axiome (d.h. Grundaussagen), welche am Anfang einer Theorie (z.B. Gruppentheorie) stehen. Die nicht-logischen Symbole werden dann in einem Modell der Theorie so interpretiert, dass alle Axiome wahr werden.

In der Mathematik sind wir nur in der formalen Logik auf der syntaktischen Ebene. Ansonsten arbeiten wir immer auf der semantischen Ebene. Selbst wenn wir zum Beispiel eine allgemeine Gruppe untersuchen, besteht diese Gruppe in unserer Vorstellung aus Elementen, also aus Objekten, wobei auf der Menge der Objekte eine konkrete binäre Operation (mit gewissen Eigenschaften) definiert ist. Sogar wenn wir mathematische Beweise führen, bleiben wir

auf der semantischen Ebene – wir können aber (wie wir später sehen werden) jeden richtigen mathematischen Beweis in einen formalen Beweis der syntaktischen Ebene übersetzen, dessen Korrektheit ein Computer überprüfen kann. Obwohl mathematische Theorien (wie z.B. die Gruppentheorie) üblicherweise auf nicht-logischen Axiomen beruhen, wird der Übergang von der syntaktischen Ebene der nicht-logischen Axiome (z.B. der Gruppenaxiome) auf die semantische Ebene (z.B. der konkreten Gruppen) im Allgemeinen nicht vollzogen. In der Gruppentheorie mag dies noch statthaft sein, denn wir können Modelle von endlichen Gruppen effektiv angeben. Wesentlich anders ist es aber bei der Mengenlehre oder der Peano-Arithmetik, denn es gibt kein umfassendes System, in welchem ein Modell der Mengenlehre oder der Peano-Arithmetik existiert.

STRUKTUREN, INTERPRETATIONEN, MODELLE

Sei $\mathscr{L}$ eine beliebige, aber festgelegte Signatur. Eine **$\mathscr{L}$-Struktur** $\mathbf{M}$ besteht aus einer nichtleeren Menge A, dem sogenannten **Bereich** von $\mathbf{M}$, zusammen mit einer Abbildung, welche jedem Konstantensymbol $c \in \mathscr{L}$ ein Element $c^{\mathbf{M}} \in A$ zuordnet, jedem n-stelligen Relationssymbol $R \in \mathscr{L}$ eine Menge von n-Tupeln $R^{\mathbf{M}} \subseteq A^n$ zuordnet, und jedem n-stelligen Funktionssymbol $F \in \mathscr{L}$ eine Funktion $F^{\mathbf{M}} : A^n \to A$ zuordnet.

Um auch Variablen zu interpretieren, definieren wir sogenannte Variablenbelegungen: Eine **Variablenbelegung j** in einer $\mathscr{L}$-Struktur $\mathbf{M}$ mit Bereich A, ist eine Abbildung, welche jeder Variablen ν ein Objekt $j(\nu) \in A$ zuordnet. Für eine Variable ν, ein Objekt $a \in A$ und eine Variablenbelegung j einer $\mathscr{L}$-Struktur $\mathbf{M}$ mit Bereich A, definieren wir zudem die Variablenbelegung $j\frac{a}{\nu}$ wie folgt:

$$j\tfrac{a}{\nu}(\nu') = \begin{cases} a & \text{falls } \nu' \equiv \nu, \\ j(\nu') & \text{sonst.} \end{cases}$$

Eine **$\mathscr{L}$-Interpretation** $\mathbf{I}$ ist ein Paar $(\mathbf{M}, j)$ das aus einer $\mathscr{L}$-Struktur $\mathbf{M}$ und einer Variablenbelegung j in $\mathbf{M}$ besteht.

Für eine Interpretation $\mathbf{I} = (\mathbf{M}, j)$ und ein Objekt $a \in A$ definieren wir:

$$\mathbf{I}\,\tfrac{a}{\nu} := \big(\mathbf{M}, j\tfrac{a}{\nu}\big)$$

Bezüglich einer $\mathscr{L}$-Interpretation $\mathbf{I} = (\mathbf{M}, j)$, wobei A der Bereich von $\mathbf{M}$ ist, ordnen wir jedem $\mathscr{L}$-Term τ ein Objekt $\mathbf{I}(\tau) \in A$ wie folgt zu:

- Für Variablen ν sei $\mathbf{I}(\nu) := j(\nu)$.
- Für Konstantensymbole $c \in \mathscr{L}$ sei $\mathbf{I}(c) := c^{\mathbf{M}}$.
- Für ein n-stelliges Funktionssymbol $F \in \mathscr{L}$ und $\mathscr{L}$-Terme $\tau_1, \ldots, \tau_n$, sei

$$\mathbf{I}\big(F\tau_1 \cdots \tau_n\big) := F^{\mathbf{M}}\big(\mathbf{I}(\tau_1), \ldots, \mathbf{I}(\tau_n)\big)\,.$$

Nun sind wir in der Lage, mit $\mathscr{L}$-Interpretationen auch Formeln zu interpretieren. Mehr noch, wir können sogar definieren, wann eine Formel φ bezüglich einer bestimmten Interpretation $\mathbf{I}$ wahr ist, bzw. wann eine Formel φ in $\mathbf{I}$ gilt – was wir mit $\mathbf{I} \models \varphi$ bezeichnen.

Ist φ eine Formel, so ist sie aus den Regeln (F0)–(F4) entstanden, d.h. φ ist von der Form $\tau_1 = \tau_2$, $R(\tau_1, \ldots, \tau_n)$, $\neg\psi$, $\psi_1 \wedge \psi_2$, $\psi_1 \vee \psi_2$, $\psi_1 \to \psi_2$, $\exists\nu\psi$ oder $\forall\nu\psi$. Wir definieren nun $\mathbf{I} \models \varphi$ wie folgt:

$$
\begin{aligned}
\mathbf{I} \models \tau_1 = \tau_2 \quad &\iff \quad \mathbf{I}(\tau_1) \text{ IST DASSELBE OBJEKT WIE } \mathbf{I}(\tau_2) \\
\mathbf{I} \models R(\tau_1, \ldots, \tau_n) \quad &\iff \quad \big(\mathbf{I}(\tau_1), \ldots, \mathbf{I}(\tau_n)\big) \text{ IST EIN ELEMENT DER MENGE } R^{\mathbf{M}} \\
\mathbf{I} \models \neg\psi \quad &\iff \quad \text{NICHT } \mathbf{I} \models \psi \\
\mathbf{I} \models \psi_1 \wedge \psi_2 \quad &\iff \quad \mathbf{I} \models \psi_1 \text{ UND } \mathbf{I} \models \psi_2 \\
\mathbf{I} \models \psi_1 \vee \psi_2 \quad &\iff \quad \mathbf{I} \models \psi_1 \text{ ODER } \mathbf{I} \models \psi_2 \\
\mathbf{I} \models \psi_1 \to \psi_2 \quad &\iff \quad \text{FALLS } \mathbf{I} \models \psi_1 \text{ DANN } \mathbf{I} \models \psi_2 \\
\mathbf{I} \models \exists\nu\psi \quad &\iff \quad \text{ES EXISTIERT EIN } a \text{ IN } A \text{ MIT } \mathbf{I}\tfrac{a}{\nu} \models \psi \\
\mathbf{I} \models \forall\nu\psi \quad &\iff \quad \text{FÜR ALLE } a \text{ IN } A \text{ GILT } \mathbf{I}\tfrac{a}{\nu} \models \psi
\end{aligned}
$$

Beachte, dass für jede $\mathscr{L}$-Interpretation $\mathbf{I}$ und für jede $\mathscr{L}$-Formel φ gilt:

$$\textit{entweder} \quad \mathbf{I} \models \varphi \quad \textit{oder} \quad \mathbf{I} \models \neg\varphi\,.$$

Mit anderen Worten, entweder ist eine Formel in einer Interpretation wahr, d.h. $\mathbf{I} \models \varphi$, oder die Formel ist nicht wahr bzw. falsch, d.h. $\mathbf{I} \not\models \varphi$, dann ist ihre Negation $\neg\varphi$ wahr, d.h. $\mathbf{I} \models \neg\varphi$

Sei nun $\mathscr{L}$ eine beliebige Signatur, φ eine $\mathscr{L}$-Formel und M eine $\mathscr{L}$-Struktur. Dann ist M **ein Modell von $\boldsymbol{\varphi}$**, in Zeichen $\mathrm{M} \models \varphi$, falls für *jede* Variablenbelegung j gilt: $(\mathbf{M}, j) \models \varphi$. Ist $\boldsymbol{\Phi}$ eine Menge von $\mathscr{L}$-Formeln, dann ist M **ein Modell von $\boldsymbol{\Phi}$**, in Zeichen $\mathrm{M} \models \boldsymbol{\Phi}$, falls für jede Formel $\varphi \in \boldsymbol{\Phi}$ gilt: $\mathrm{M} \models \varphi$.

Zum Beispiel sei $\mathscr{L} = \{\mathsf{c}, f\}$, wobei c ein Konstantensymbol und f ein 1-stelliges Funktionssymbol ist. Weiter sei $\boldsymbol{\Phi}$ die Menge, welche aus folgenden beiden $\mathscr{L}$-Sätzen besteht:

$$\underbrace{\forall x\big(x = \mathsf{c} \vee x = f(\mathsf{c})\big)}_{\varphi_1} \quad \text{und} \quad \underbrace{\exists x(x \neq \mathsf{c})}_{\varphi_2}$$

Wir konstruieren nun zwei Modelle $\mathbf{M}_1$ und $\mathbf{M}_2$ (bzw. zwei $\mathscr{L}$-Strukturen) mit demselben Bereich A, so dass $\mathbf{M}_1 \models \boldsymbol{\Phi}$ und $\mathbf{M}_2 \not\models \boldsymbol{\Phi}$: Zuerst wählen wir $A := \{0, 1\}$ und definieren

$$\mathsf{c}^{\mathbf{M}_1} := 0, \quad f^{\mathbf{M}_1}(0) := 1, \quad f^{\mathbf{M}_1}(1) := 0,$$

$$\mathsf{c}^{\mathbf{M}_2} := 0, \quad f^{\mathbf{M}_2}(0) := 0, \quad f^{\mathbf{M}_2}(1) := 1.$$

Es ist leicht zu zeigen, dass der Satz φ_2 in beiden Modellen gilt, wohingegen φ_1 nur im Modell $\mathbf{M}_1$ gilt. Insbesonder haben wir $\mathbf{M}_1 \models \varphi_1 \wedge \varphi_2$ und $\mathbf{M}_2 \models \neg\varphi_1 \wedge \varphi_2$.

DER KORREKTHEITSSATZ

Der Korrektheitssatz besagt, dass jeder Satz, welcher aus einer Menge T von Sätzen beweisbar ist, in jedem Modell von T wahr ist.

KORREKTHEITSSATZ. *Sei $\mathscr{L}$ eine Signatur, sei T eine Menge von $\mathscr{L}$-Sätzen, sei σ ein $\mathscr{L}$-Satz, der aus T beweisbar ist (d.h. $T \vdash \sigma$), und sei M ein beliebiges Modell von T (d.h. $\mathrm{M} \models T$). Dann gilt $\mathrm{M} \models \sigma$.*

Begründung. Sowohl die logischen Axiome als auch die Sätze aus T sind wahr in jedem Modell $\mathrm{M} \models \mathsf{T}$, und mit den Schlussregeln erhalten wir aus wahren Formeln immer wahre Formeln. Somit ist auch die letzte Formel σ eines formalen Beweises wahr in M, d.h. es gilt $\mathrm{M} \models \sigma$.
Folgerung.

- Ist σ ein Satz und gilt $\mathsf{T} \vdash \sigma$, dann gilt für jedes Modell $\mathrm{M} \models \mathsf{T}$, $\mathrm{M} \models \sigma$.

  Begründung. Hätten wir ein Model $\mathrm{M} \models \mathsf{T}$, in dem σ nicht gilt, so hätten wir $\mathrm{M} \models \neg\sigma$, was aber dem Korrektheitssatz widerspricht.

DER GÖDEL'SCHE VOLLSTÄNDIGKEITSSATZ

Eine Menge T von Sätzen heisst **konsistent** (oder **widerspruchsfrei**), falls es keine Formel φ gibt mit $\mathsf{T} \vdash \varphi \wedge \neg\varphi$. Ist T nicht konsistent so heisst T **inkonsistent**. Aus Aufgabe 0.(f) folgt, dass für eine inkonsistente Theorie T gilt: $\mathsf{T} \vdash \psi$ für jede Formel ψ.

Der Gödel'sche Vollständigkeitssatz besagt nun, dass jede konsistente Menge von Sätzen ein Modell besitzt. Etwas allgemeiner formuliert besagt der Gödel'sche Vollständigkeitssatz folgendes:

GÖDEL'SCHER VOLLSTÄNDIGKEITSSATZ. *Sei $\mathscr{L}$ eine Signatur, sei T eine Menge von $\mathscr{L}$-Sätzen, und sei σ ein $\mathscr{L}$-Satz mit $T \nvdash \sigma$ (d.h. T ist konsistent). Dann existiert ein Modell $\mathrm{M} \models T$ mit $\mathrm{M} \models \neg\sigma$.*

Folgerungen.

- Ist T eine konsistente Menge von Sätzen, so hat T ein Modell.

  Begründung. Ist T konsistent, so existiert ein Satz σ, der nicht aus T beweisbar ist, d.h. $\mathsf{T} \nvdash \sigma$, und somit existiert auch ein Model $\mathrm{M} \models \mathsf{T}$.

- Ist σ ein Satz und gilt für jedes Modell $\mathrm{M} \models \mathsf{T}$, $\mathrm{M} \models \sigma$, dann gilt $\mathsf{T} \vdash \sigma$.

  Begründung. Hätten wir $\mathsf{T} \nvdash \sigma$, so gäbe es ein Model $\mathrm{M} \models \mathsf{T}$ mit $\mathrm{M} \models \neg\sigma$.

- Ist σ ein Satz und gilt $\mathsf{T} \nvdash \sigma$ und $\mathsf{T} \nvdash \neg\sigma$, so existieren zwei Modelle $\mathrm{M}_1 \models \mathsf{T}$ und $\mathrm{M}_2 \models \mathsf{T}$ mit $\mathrm{M}_1 \models \neg\sigma$ und $\mathrm{M}_2 \models \sigma$.

  Begründung. Mit $\mathsf{T} \nvdash \sigma$ gibt es ein Modell $\mathrm{M}_1 \models \mathsf{T} + \neg\sigma$, und mit $\mathsf{T} \nvdash \neg\sigma$ gibt es ein Modell $\mathrm{M}_2 \models \mathsf{T} + \sigma$.

- Zusammen mit dem Korrektheitssatz erhalten wir schliesslich folgende Aussage:

  > *Ein Satz σ ist genau dann aus einer Menge von Sätzen T formal beweisbar, wenn σ in jedem Modell von T gilt.*

BEMERKUNGEN ZU MATHEMATISCHEN BEWEISEN

Um zu zeigen, dass ein Satz σ aus einem Axiomensystem T beweisbar ist, führen wir üblicherweise keine formalen Beweise, sondern benutzen den Gödel'schen Vollständigkeitssatz und zeigen, dass in jedem Modell von T der Satz σ gilt (d.h. wahr ist). Mit dem Gödel'schen Vollständigkeitssatz ist dann der Satz σ aus dem Axiomensystem T formal beweisbar. Dieses Vorgehen ist ein *mathematischer Beweis* von σ aus T.

Wenn wir zum Beispiel aus den Axiomen der Gruppentheorie GT einen Satz σ zeigen wollen, so gehen wir wie folgt vor: Wir nehmen irgend ein Modell von GT, also irgend eine Gruppe $(G, \mathsf{e}, \circ)$, und zeigen, dass der Satz σ in $(G, \mathsf{e}, \circ)$ gilt, d.h. $(G, \mathsf{e}, \circ) \models \sigma$.

Ist zum Beispiel $\sigma \equiv \forall x \forall y \big(y \circ x = \mathsf{e} \ \rightarrow \ x \circ y = \mathsf{e} \big)$, so nehmen wir irgend eine Gruppe $(G, \mathsf{e}, \circ)$ und irgend ein Element $x \in G$, und zeigen, dass jedes links-Inverse von x auch rechts-Inverses von x ist:

- Weil $(G, \mathsf{e}, \circ) \models \mathsf{GT}_2$, existiert zu jedem Element in G ein links-inverses Element. Sei nun $x \in G$, sei $\bar{x} \in G$ ein link-Inverses von x und sei $\bar{\bar{x}} \in G$ ein links-inverses von $\bar{x}$. In $(G, \mathsf{e}, \circ)$ gilt somit

$$\bar{\bar{x}} \circ \bar{x} = \mathsf{e} \quad \text{und} \quad \bar{x} \circ x = \mathsf{e}.$$

- Weil $(G, \mathsf{e}, \circ) \models \mathsf{GT}_1$, gilt in $(G, \mathsf{e}, \circ)$ auch

$$x \circ \bar{x} = \mathsf{e} \circ (x \circ \bar{x}) = (\bar{\bar{x}} \circ \bar{x}) \circ (x \circ \bar{x}).$$

- Weil $(G, \mathsf{e}, \circ) \models \mathsf{GT}_0$, gilt in $(G, \mathsf{e}, \circ)$ auch

$$(\bar{\bar{x}} \circ \bar{x}) \circ (x \circ \bar{x}) = \bar{\bar{x}} \circ \big(\bar{x} \circ (x \circ \bar{x}) \big) = \bar{\bar{x}} \circ \big((\bar{x} \circ x) \circ \bar{x} \big) = \bar{\bar{x}} \circ (\mathsf{e} \circ \bar{x}).$$

- Weil $(G, \mathsf{e}, \circ) \models \mathsf{GT}_1$, gilt in $(G, \mathsf{e}, \circ)$ auch

$$\bar{\bar{x}} \circ (\mathsf{e} \circ \bar{x}) = \bar{\bar{x}} \circ \bar{x} = \mathsf{e},$$

  und somit gilt $x \circ \bar{x} = \mathsf{e}$ in $(G, \mathsf{e}, \circ)$.

- Weil nun die Gruppe $(G, \mathsf{e}, \circ)$ und das Element $x \in G$ beliebig waren, gilt in jeder Gruppe $(G, \mathsf{e}, \circ) \models \mathsf{GT}$, das jedes links-inverse eines beliebigen Elements $x \in G$ auch rechts-inverses von x ist.

Beachte, dass wir in diesem mathematischen Beweis nur über die Wahrheit von Aussagen im Modell $(G, \mathsf{e}, \circ)$ argumentiert haben. Insbesondere haben wir die Axiome der Gruppentheorie – und implizit die logischen Axiome – nicht dazu benutzt, logische Schlüsse zu ziehen, sondern nur um zu zeigen, dass bestimmte Aussagen in $(G, \mathsf{e}, \circ)$ wahr sind.

Ein mathematischer Beweis benutzt also immer implizit den Gödel'schen Vollständigkeitssatz. Es ist natürlich auch möglich, dass ein gewisser Satz σ in machen Modellen einer Theorie T wahr und in anderen Modellen falsch ist. Seien zum Beispiel $\mathbf{M}_1$ und $\mathbf{M}_2$ zwei Modelle von T und sei σ ein Satz für den gilt $\mathbf{M}_1 \models \sigma$ und $\mathbf{M}_2 \not\models \sigma$, d.h. $\mathbf{M}_2 \models \neg\sigma$. Dann folgt aus dem Korrektheitssatz, dass gilt: $\mathsf{T} \nvdash \sigma$ und $\mathsf{T} \nvdash \neg\sigma$. Ein Satz σ, der aus einer Theorie T weder beweisbar noch widerlegbar ist, ist **unabhängig** von T. Für die Theorie GT ist zum Beispiel $\sigma \equiv \forall x \forall y (x \circ y = y \circ x)$ ein solcher Satz. Beachte, ist σ unabhängig von T, so ist sowohl $\mathsf{T} + \sigma$ wie auch $\mathsf{T} + \neg\sigma$ konsistent; insbesondere hat sowohl $\mathsf{T} + \sigma$ wie auch $\mathsf{T} + \neg\sigma$ ein Modell.

3. Die Axiome der Zermelo-Fraenkel'schen Mengenlehre

Die Signatur der Zermelo-Fraenkel'schen Mengenlehre ZF ist $\mathscr{L}_{\mathsf{ZF}} = \{\in\}$, wobei $\in$ ein 2-stelliges Relationssymbol ist. Anstelle von $\in yx$ schreiben wir $y \in x$ und sagen "y ist Element von x", und für $\neg(y \in x)$ schreiben wir $y \notin x$.

Das Axiomensystem von Zermelo

Im Jahr 1905 begann Ernst Zermelo die Mengenlehre zu axiomatisieren und publizierte 1908 sein erstes Axiomensystem, das aus folgenden sieben Axiomen bestand:

(a) *Axiom der Bestimmtheit*
besagt, dass eine Menge durch ihre Elemente bestimmt ist

(b) *Axiom der Elementarmengen*
besagt, dass es gewisse Mengen gibt, wie z.B. leere Menge oder Paarmenge

(c) *Axiom der Aussonderung*
besagt, dass aus Mengen gewisse Teilmengen ausgesondert werden können

(d) *Axiom der Potenzmenge*
besagt, dass zu jeder Menge die Menge ihrer Teilmengen existiert

(e) *Axiom der Vereinigung*
besagt, dass wir Mengen von Mengen vereinigen können

(f) *Axiom der Auswahl*
besagt, dass cartesische Produkte nicht-leerer Mengen nicht leer sind

(g) *Axiom des Unendlichen*
besagt, dass es eine Menge gibt, die nicht endlich ist.

Die Axiome (a) – (e) und Axiom (g) (d.h. alle Axiome ausser dem Auswahlaxiom), sind die Axiome $0-6$ der *Zermelo-Fraenkel'schen Mengenlehre*, welche im folgenden Abschnitt eingeführt werden.

Die Axiome $0-6$

0. Axiom der leeren Menge.

$$\exists x \forall z (z \notin x)$$

Das *Axiom der leeren Menge* besagt, dass eine Menge existiert, welche keine Elemente besitzt. Insbesondere existiert mindestens eine Menge, nämlich eine leere Menge.

1. Extensionalitätsaxiom.

$$\forall x \forall y \big(\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y \big)$$

Das *Extensionalitätsaxiom* besagt, dass zwei Mengen, welche dieselben Elemente besitzen, identisch sind. Die Umkehrung dieser Implikation folgt aus dem logischen Axiom L_{15}.

Aus dem Axiom der leeren Menge folgt mit dem Extensionalitätsaxiom, dass die **leere Menge** eindeutig ist; diese wird mit $\emptyset$ bezeichnet.

Wir definieren nun das binäre Relationssymbol $\subseteq$ für **Teilmenge** wie folgt:

$$y \subseteq x :\Longleftrightarrow \forall z (z \in y \rightarrow z \in x)$$

Beachte, dass $\emptyset \subseteq x$ für jede Menge x gilt. Weiter definieren wir das binäre Relationssymbol $\subsetneq$ für **echte Teilmenge** durch

$$y \subsetneq x :\Longleftrightarrow\ y \subseteq x \wedge y \neq x\,.$$

2. Paarmengenaxiom.

$$\forall x \forall y \exists u \forall z \big(z \in u \leftrightarrow (z = x \vee z = y)\big)$$

Das *Paarmengenaxiom* besagt, dass für alle Mengen x und y immer eine Menge u existiert, welche nur die Mengen x und y als Elemente besitzt. Für die Menge, welche nur x und y enthält, schreiben wir $\{x, y\}$. Beachte, dass aus dem Extensionalitätsaxiom die Gleichheit $\{x, y\} = \{y, x\}$ folgt, und dass für $x = y$ die Gleichheit $\{x, y\} = \{x\}$ gilt.

Mit dem Paarmengenaxiom können wir nun wie folgt auch **geordnete Paare** definieren:

$$\langle x, y\rangle := \big\{\{x\}, \{x, y\}\big\}$$

Es lässt sich einfach zeigen, dass gilt

$$\langle x, y\rangle = \langle x', y'\rangle \iff x = x' \wedge y = y',$$

und somit können wir das binäre Funktionssymbol $\langle\,\cdot\,,\,\cdot\,\rangle$ wie folgt definieren:

$$\langle x, y\rangle = u :\Longleftrightarrow\ \forall z\big(z \in u \leftrightarrow \big(z = \{x\} \vee z = \{x, y\}\big)\big)$$

Analog könnten wir auch geordnete Tripel, Quadrupel, etc., definieren, doch das wird einfacher, wenn wir mehr Axiome zur Verfügung haben.

3. Vereinigungsaxiom.

$$\forall x \exists u \forall z \big(z \in u \leftrightarrow \exists w(w \in x \wedge z \in w)\big)$$

Das *Vereinigungsaxiom* besagt, dass zu jeder Menge x eine Menge u existiert, welche alle Mengen enthält, welche Elemente von Elementen von x sind.

Mit dem Vereinigungsaxiom können wir die **unäre Vereinigungsfunktion** $\bigcup$ wie folgt definieren:

$$\bigcup x = u :\Longleftrightarrow\ \forall z\big(z \in u \leftrightarrow \exists w(w \in x \wedge z \in w)\big)$$

Zum Beispiel gilt $x = \bigcup\{x\}$. Mit Hilfe des Vereinigungsaxioms und des Paarmengenaxioms können wir die **binäre Vereinigungsfunktion** $\cup$ wie folgt definieren:

$$x \cup y := \bigcup\{x, y\}$$

Ebenfalls mit dem Vereinigungsaxiom und dem Paarmengenaxiom, und durch die Definition $x + 1 := x \cup \{x\}$, können wir zum Beispiel folgende Mengen bilden:

$$\begin{aligned} 0 &:= \emptyset \\ 1 &:= 0 + 1 = 0 \cup \{0\} = \{0\} \\ 2 &:= 1 + 1 = 1 \cup \{1\} = \{0, 1\} \\ 3 &:= 2 + 1 = 2 \cup \{2\} = \{0, 1, 2\} \end{aligned}$$

Allgemein können wir jede natürliche Zahl n identifizieren mit der Menge $\{0, \ldots, n-1\}$, wobei die leeren Menge $\emptyset$ der Zahl 0 entspricht. Diese Konstruktion führt zu folgender Definition: Eine Menge x heisst **induktiv**, falls

$$\forall y(y \in x \to (y \cup \{y\}) \in x).$$

Formal definieren wir ein 1-stelliges Relationssymbol ind wie folgt:

$$\mathrm{ind}(x) :\Longleftrightarrow\ \forall y\big(y \in x \to \big(y \cup \{y\}\big) \in x\big)$$

Einerseits ist die leere Menge $\emptyset$ induktiv, d.h. $\mathrm{ind}(\emptyset)$. Andererseits können wir aus den bisherigen Axiomen nicht beweisen, dass es auch nicht-leere induktive Mengen gibt – dies wird aber durch das nächste Axiom garantiert.

4. Unendlichkeitsaxiom.

$$\exists I\big(\emptyset \in I \wedge \mathrm{ind}(I)\big)$$

Das *Unendlichkeitsaxiom* besagt, dass es eine nicht-leere induktive Menge gibt, welche die leere Menge enthält. Jede der oben konstruierten Mengen $0, 1, 2, 3 \ldots$ (d.h. jede natürliche Zahl) gehört zu jeder induktiven Menge I welche $\emptyset$ enthält.

5. Aussonderungsaxiom (Axiomenschema). Für jede Formel $\varphi(z)$ mit der einzigen freien Variable z, ist der folgende Satz ein Axiom:

$$\forall x \exists y \forall z\big(z \in y \leftrightarrow \big(z \in x \wedge \varphi(z)\big)\big)$$

Das *Aussonderungsaxiom* besagt, dass zu jeder Formel $\varphi(z)$ und jeder Menge x eine Menge y existiert, so dass y genau diejenigen Elemente z von x enthält, für die $\varphi(z)$ gilt. Etwas informeller können wir das Aussonderungsaxiom (bzgl. φ) wie folgt ausdrücken: Für jede Menge x und jede Formel φ ist

$$\{z \in x : \varphi(z)\}$$

eine Menge. Beachte, dass uns das Aussonderungsaxiom nur erlaubt, aus bestehenden Mengen gewisse Elemente auszusondern und die "Kollektion" der ausgesonderten Elemente bildet dann eine Menge. Wir können aber im Allgemeinen keine Kollektionen von Mengen mit einer bestimmten Eigenschaft bilden, bzw. solche Kollektionen sind im Allgemeinen keine Mengen. Zum Beispiel ist für eine Menge x und $\varphi(z) \equiv z \notin z$, $\{z \in x : \varphi(z)\}$ eine Menge, aber die Kollektion $\{z : \varphi(z)\}$ ist *keine* Menge.

Mit dem Aussonderungsaxiom können wir nun auch Durchschnitt und Differenz von Mengen definieren: Seien x_0 und x_1 Mengen und sei $\varphi(z) :\equiv z \in x_0$ (x_0 ist ein Parameter von φ). Dann definieren wir das binäre Funktionssymbol $\cap$ für **Durchschnitt** wie folgt:

$$x_0 \cap x_1 = y :\Longleftrightarrow\ y = \{z \in x_1 : \varphi(z)\}$$

Um Formeln besser lesbar zu machen, definieren wir:

$$\exists x \in w\ \varphi(x) \ :\Longleftrightarrow\ \exists x\big(x \in w\ \wedge\ \varphi(x)\big)$$

$$\forall x \in w\ \varphi(x) \ :\Longleftrightarrow\ \forall x\big(x \in w \to \varphi(x)\big)$$

Analog zum Vereinigungssymbol $\bigcup$, und mit Hilfe von diesem, definieren wir mit der Formel $\varphi(u) :\equiv \forall z \in x\ (u \in z)$ das unäre Durchschnittssymbol $\bigcap$ durch

$$\bigcap x = y :\Longleftrightarrow\ y = \Big\{u \in \bigcup x : \varphi(u)\Big\}.$$

Beachte, dass die Gleichheit $x \cap y = \bigcap\{x, y\}$ gilt. Mit $\varphi(z) :\equiv z \notin y$ können wir das binäre Funktionssymbol $\setminus$ für **Mengendifferenz** definieren durch

$$x \setminus y = u :\Longleftrightarrow\ u = \{z \in x : \varphi(z)\}.$$

6. Potenzmengenaxiom.

$$\forall x \exists z \forall y (y \in z \leftrightarrow y \subseteq x)$$

Das *Potenzmengenaxiom* besagt, dass zu jeder Menge x eine Menge $\mathscr{P}(x)$ existiert, die sogenannte **Potenzmenge** von x, deren Elemente die Teilmengen von x sind. Weil mit dem Extensionalitätsaxiom die Potenzmenge von x eindeutig ist, können wir formal das 1-stellige Funktionssymbol $\mathscr{P}$ wie folgt definieren:

$$\mathscr{P}(x) = z :\Longleftrightarrow \forall y (y \in z \leftrightarrow y \subseteq x)$$

DEFINITIONEN UND KONSTRUKTIONEN AUS DEN AXIOMEN $0-6$

Die Menge ω. Als erstes definieren (bzw. konstruieren) wir mit den Axiomen $0-6$ die Menge ω als die kleinste induktive Menge, welche $\emptyset$ enthält: Mit dem Unendlichkeitsaxiom existiert eine induktive Menge I_0 welche $\emptyset$ enthält. Mit dem Potenzmengenaxiom bilden wir die Potenzmenge $\mathscr{P}(I_0)$ und mit dem Aussonderungsaxiom bilden wir dann zuerst die Menge aller $X \in \mathscr{P}(I_0)$, die induktiv sind und $\emptyset$ enthalten, und bilden dann den Durchschnitt all dieser Mengen X. Die Menge ω ist also wie folgt definiert:

$$\omega := \bigcap \big\{ X \in \mathscr{P}(I_0) : \emptyset \in X \wedge \mathrm{ind}(X) \big\}$$

Es ist nicht schwierig zu zeigen, dass der Durchschnitt induktiver Mengen, welche $\emptyset$ enthalten, wieder eine induktive Menge ist, welche $\emptyset$ enthält; und weil ω in jeder solchen Menge enthalten ist, ist ω tatsächlich die kleinste induktive Menge, die $\emptyset$ enthält.

Die Menge ω ist auch die kleinste Menge, welche die "Menge" $\mathbb{N}$ (im naiven Sinn) der natürlichen Zahlen $0, 1, 2, \ldots$ (wie wir sie oben definiert haben) enthält, d.h. "$\mathbb{N} \subseteq \omega$". Es sei hier erwähnt, dass aus dem *Gödel'schen Unvollständigkeitssatz* folgt, dass $\mathbb{N} = \omega$ nicht beweisbar ist – insbesondere ist die Existenz der Menge $\mathbb{N}$ formal nicht beweisbar. Da wir aber andererseits auch nicht "$\mathbb{N} \subsetneq \omega$" zeigen können, dürfen wir ohne Einschränkung annehmen, dass die Mengen $\mathbb{N}$ und ω identisch sind – insbesondere ist die Menge $\mathbb{N}$ aus den Axiomen der Mengenlehre konstruierbar.

Cartesische Produkte. Für beliebige Mengen A und B definieren wir das binäre Funktionssymbol $\times$ durch

$$A \times B := \big\{ \langle x, y \rangle : x \in A \wedge y \in B \big\}$$

wobei $\langle x, y \rangle = \big\{ \{x\}, \{x, y\} \big\}$ ist. Die Menge $A \times B$ heisst **cartesisches Produkt** von A und B. Beachte, dass das cartesische Produkt $A \times B$ von A und B eine Teilmenge der Menge $\mathscr{P}(\mathscr{P}(A \cup B))$ ist.

Funktionen. Mit Hilfe cartesischer Produkte können wir nun **Funktionen** $f : A \to B$, welche jedem Element der Menge A genau ein Element der Menge B zuordnen, als Teilmengen von $A \times B$ auffassen. Die Menge aller Funktionen $f : A \to B$, welche wir mit ${}^A B$ bezeichnen, ist definiert durch

$${}^A B := \big\{ f \subseteq A \times B : \forall x \in A \, \exists! y \in B \, \big(\langle x, y \rangle \in f \big) \big\}$$

wobei $\exists! y$ bedeutet, dass es genau ein y gibt, d.h. $\exists! y \varphi(y)$ ist eine abgekürzte Schreibweise für

$$\exists y \big(\varphi(y) \wedge \forall z (\varphi(z) \to z = y) \big).$$

Für Funktionen $f \in {}^A B$ schreiben wir üblicherweise $f : A \to B$ und für $\langle x, y \rangle \in f$ schreiben wir üblicherweise $f(x) = y$. Ist die Menge A ein cartesisches Produkt, zum Beispiel $A =$

$C_1 \times C_2$, so ist $f : A \to B$ eine 2-stellige Funktion. Wir können auch injektive, surjektive oder bijektive Funktionen definieren, zum Beispiel:

$$f \in {}^{A}B \text{ ist injektiv } \iff \forall x, x' \in A\, \forall y \in B\, \big((\langle x, y\rangle \in f \wedge \langle x', y\rangle \in f) \to x = x'\big)$$

Eine Menge A heisst **endlich**, falls eine Bijektion $f : n \to A$ existiert für ein $n \in \omega$. Beachte, dass diese Definition von "endlich" nur dann mit dem richtigen Endlichkeitsbegriff übereinstimmt, wenn $\mathbb{N} = \omega$. Eine Menge A heisst **abzählbar**, falls eine Surjektion $f : \omega \to A$ existiert, andernfalls heisst A **überabzählbar**. Beachte, dass insbesondere jede endliche Menge abzählbar ist.

THEOREM 3.1 (Cantor). *$\mathscr{P}(\omega)$ ist überabzählbar.*

Beweis. Sei $g : \omega \to \mathscr{P}(\omega)$ eine Funktion. Um zu zeigen, dass $\mathscr{P}(\omega)$ überabzählbar ist, genügt es zu zeigen, dass g nicht surjektiv ist. Das heisst wir müssen eine Menge $\Gamma \in \mathscr{P}(\omega)$ finden, sodass für alle $n \in \omega$ gilt $g(n) \neq \Gamma$. Sei

$$\Gamma := \big\{n \in \omega : n \notin g(n)\big\}.$$

Dann ist $\Gamma \subseteq \omega$, d. h. $\Gamma \in \mathscr{P}(\omega)$, und für $n_0 \in \omega$ mit $g(n_0) = \Gamma$ hätten wir

$$n_0 \in \Gamma \iff n_0 \notin g(n_0) \iff n_0 \notin \Gamma\,,$$

was offensichtlich ein Widerspruch ist. ⊣

Endliche cartesische Produkte und Relationen. Mit Hilfe von Funktionen können wir nun auch endliche cartesische Produkte definieren: Sei A eine Mengen und $n \in \omega$. Dann ist das n-fache cartesische Produkt der Menge A definiert als die Menge aller Funktionen $f : n \to A$, also

$$\underbrace{A \times \ldots \times A}_{n\text{-mal}} := {}^{n}A\,,$$

wobei anstelle von ${}^{n}A$ meist A^n geschrieben wird.

Mit Hilfe endlicher cartesischer Produkte können wir nun auch Relationen definieren: Für eine Menge A und ein $n \in \omega$, ist $R \subseteq A^n$ eine $\boldsymbol{n}$**-stellige Relation** auf A.

Zwei Beispiele für Ordnungsrelationen:

- Eine binäre Relation R auf A ist eine **lineare Ordnung** auf A, falls R transitiv ist und für alle Elemente $x, y \in A$ *Trichotomie* gilt (d.h. entweder xRy, oder $x = y$, oder yRx).
- Eine lineare Ordnung R auf A ist eine **Wohlordnung** auf A, falls jede nicht-leere Teilmenge $S \subseteq A$ ein R-minimales Element besitzt, d.h. es existiert ein $x_0 \in S$, sodass für alle $y \in S$ gilt $\neg yRx_0$. Beachte, dass, weil R eine lineare Ordnung ist, das R-minimale Element x_0 eindeutig ist. Falls eine Wohlordnung R auf der Menge A existiert, so sagen wir, dass A **wohlordenbar** ist.

Mit dem *Auswahlaxiom*, welches wir später behandeln, kann gezeigt werden, dass sich jede Menge wohlordnen lässt.

DIE AXIOME 7 & 8

Das nächste Axiom stammt von Abraham Fraenkel.

7. Ersetzungsaxiom (Axiomenschema). Um dieses Axiom zu formulieren, führen wir den Begriff der *Klassenfunktion* ein: Sei $\varphi(x, y)$ eine Formel mit $x, y \in \mathrm{frei}(\varphi)$, so dass gilt

$$\forall x\, \exists! y\, \varphi(x, y).$$

Dann ist das 1-stellige Funktionssymbol F, definiert durch

$$F(x) = y :\Longleftrightarrow\ \varphi(x, y),$$

eine **Klassenfunktion**. Das *Ersetzungsaxiom* besagt, dass für jede Klassenfunktion F und für jede Menge A, das Bild von A unter F eine Menge ist, d.h.

$$F[A] := \big\{F(x) : x \in A\big\}$$

ist eine Menge. Etwas kürzer ausgedrückt: *Bilder von Mengen unter Funktionen sind Mengen.*

Mit dem Ersetzungsaxiom können wir Mengen wie zum Beispiel

$$\big\{\mathscr{P}(x) : x \in \mathscr{P}(\omega)\big\}$$

bilden; setze $A = \mathscr{P}(\omega)$ und $F(x) := \mathscr{P}(x)$.

Das letzte Axiome ist zwar für die Mengenlehre wichtig, hat aber auf die allgemeine Mathematik keinen Einfluss.

8. Fundierungsaxiom.

$$\forall x \left(x \neq \emptyset \to \exists y\big(y \in x \wedge (y \cap x = \emptyset)\big)\right).$$

Das *Fundierungsaxiom* besagt, das jede Menge wohlfundiert ist, d.h. jede nicht-leere Menge x besitzt ein Element $y \in x$, sodass kein Element von y ein Element von x ist.

Mit dem Fundierungsaxiom erhalten wir, dass es keine unendlich absteigenden Sequenzen der Form

$$x_0 \ni x_1 \ni x_2 \ni \cdots$$

gibt, denn sonst würde die Menge $\{x_0, x_1, x_2, \ldots\}$ dem Fundierungsaxiom widersprechen. Insbesondere gibt es keine Menge x für die $x \in x$ gilt, und es gibt auch keine Zyklen wie zum Beispiel $x_0 \in x_1 \in \cdots \in x_n \in x_0$.

Das Axiomensystem, bestehend aus den Axiomen $0-6$ von Zermelo, dem Ersetzungsaxiom von Fraenkel, sowie dem Fundierungsaxiom, bildet die Axiome der **Zermelo–Fraenkel'schen Mengenlehre** und wird mit ZF bezeichnet.

4. KONSTRUKTION DER REELLEN ZAHLEN

Im Vorwort zu seiner Schrift *Stetigkeit und irrationale Zahlen* schreibt Richard Dedekind: *"Die Betrachtungen, welche den Gegenstand dieser kleinen Schrift bilden, stammen aus dem Herbst des Jahres 1858. Ich befand mich damals als Professor am eidgenössischen Polytechnikum zu Zürich zum ersten Male in der Lage, die Elemente der Differentialrechnung vortragen zu müssen, und fühlte dabei empfindlicher als jemals früher den Mangel einer wirklich wissenschaftlichen Begründung der Arithmetik.* [...] *Für mich war damals dies Gefühl der Unbefriedigung ein so überwältigendes, dass ich den festen Entschluß faßte, so lange nachzudenken, bis ich eine rein arithmetische und völlig strenge Begründung der Prinzipien der Infinitesimalanalysis gefunden haben würde.* [...] *Dies gelang mir am 24. November 1858."*

In diesem Kapitel werden wir (in der Mengenlehre) aus den rationalen Zahlen ein Modell der reellen Zahlen konstruieren, und zwar so, wie es auch Dedekind gemacht hat, nämlich mit *Dedekind'schen Schnitten.*

DIE AXIOME DER REELLEN ZAHLEN

Die Signatur des Axiomensystems R der reellen Zahlen ist $\mathscr{L}_{\mathsf{R}} = \{0, 1, +, \cdot, <\}$, wobei 0 und 1 Konstantensymbole sind, $+$ und $\cdot$ binäre Funktionssymbole sind und $<$ ein binäres Relationssymbol ist.

Die erste Gruppe des Axiomensystems R besteht aus den Körperaxiomen KT:

R_0:	$\forall x \forall y \forall z \big(x + (y + z) = (x + y) + z\big)$	($+$ ist *assoziativ*)
R_1:	$\forall x \forall y (x + y = y + x)$	($+$ ist *kommutativ*)
R_2:	$\forall x (0 + x = x)$	(0 ist *link-neutral* bzgl. $+$)
R_3:	$\forall x \exists y (y + x = 0)$	(*links-Inverse* bzgl. $+$)
R_4:	$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	($\cdot$ ist *assoziativ*)
R_5:	$\forall x \forall y (x \cdot y = y \cdot x)$	($\cdot$ ist *kommutativ*)
R_6:	$\forall x (1 \cdot x = x)$	(1 ist *link-neutral* bzgl. $\cdot$)
R_7:	$\forall x \exists y (x \neq 0 \to y \cdot x = 1)$	(*links-Inverse* bzgl. $\cdot$ für $x \neq 0$)
R_8:	$\forall x \forall y \forall z \big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$	($\cdot$ ist *links-distributiv* über $+$)
R_9:	$0 \neq 1$	

Die zweite Gruppe des Axiomensystems R besteht aus den Axiomen für dichte lineare Ordnungen DLO:

R_{10}:	$\forall x \neg (x < x)$	($<$ ist nicht *reflexiv*)
R_{11}:	$\forall x \forall y \forall z \big((x < y \wedge y < z) \to x < z\big)$	($<$ ist *transitiv*)
R_{12}:	$\forall x \forall y \big(x < y \vee x = y \vee y < x\big)$	($<$ definiert eine *lineare* Ordnung)
R_{13}:	$\forall x \forall y \exists z \big(x < y \to (x < z \wedge z < y)\big)$	($<$ definiert eine *dichte* Ordnung)
R_{14}:	$\forall x \exists y \exists z \big(y < x \wedge x < z\big)$	(keine grössten bzw. kleinsten Elemente)

Die dritte Gruppe des Axiomensystems R besteht aus zwei Axiomen, welche die Ordnungsstruktur mit den Rechenoperationen verbindet:

R_{15}: $\forall x \forall y \forall z \big(x < y \to x + z < y + z\big)$ (Kompatibilität von $<$ mit $+$)

R_{16}: $\forall x \forall y \big((0 < x \wedge 0 < y) \to 0 < x \cdot y\big)$ (Kompatibilität von $<$ mit $\cdot$)

Um das letzte Axiom, das **Vollständigkeitsaxiom** R_{17}, zu formulieren, müssen wir über Teilmengen von $\mathbb{R}$ sprechen. Insbesondere kann das Axiom R_{17} nur mit Hilfe der Mengenlehre – in der wir ein Modell der reellen Zahlen konstruieren – formuliert werden.

R_{17}: Jede nicht-leere nach oben beschränkte Teilmenge $X \subseteq \mathbb{R}$ hat ein *Supremum* in $\mathbb{R}$.

Etwas formaler ausgedrückt, mit der Definition $x \leq y :\Longleftrightarrow\ x < y \vee x = y$, heisst das:

$$\forall X \Big(\big(X \subseteq \mathbb{R} \wedge X \neq \emptyset \wedge \exists r\, \forall x \in X\, (x \leq r)\big) \to \exists s\, \big(\forall x \in X (x \leq s) \wedge \forall t\, \big(\forall x \in X (x \leq t) \to s \leq t\big)\big)\Big)$$

Dedekind'sche Schnitte

Wir konstruieren die reellen Zahlen aus den rationalen Zahlen $\mathbb{Q}$, welche ihrerseits aus $\mathbb{N}$ (bzw. ω) und $\mathbb{Z}$ konstruiert wurden. Das heisst wir gehen aus von einem Modell $\mathbb{Q} = (\mathbb{Q}, \mathtt{0}, \mathtt{1}, +, \cdot, <)$ der rationalen Zahlen, in dem die Axiome $\mathsf{R}_0 - \mathsf{R}_{16}$ gelten. Um weniger Fallunterscheidungen machen zu müssen, schränken wir uns auf die Konstruktion der positiven reellen Zahlen ein – die Konstruktion der negativen reellen Zahlen ist analog. Dafür definieren wir

$$\mathbb{Q}^+ := \{p \in \mathbb{Q} : p > 0\}\,.$$

Ein **Dedekind'scher Schnitt** ist eine Teilmenge $\alpha \subseteq \mathbb{Q}^+$ mit folgenden Eigenschaften:

(D0) $\alpha \neq \emptyset$ und $\alpha \neq \mathbb{Q}^+$.

(D1) Falls $p \in \alpha$ und $q \in \mathbb{Q}^+$ mit $q < p$, so folgt $q \in \alpha$ (α ist *nach unten abgeschlossen*).

(D2) Für jedes $p \in \alpha$ existiert ein $q \in \alpha$ mit $p < q$ (α enthält kein *maximales Element*).

Offensichtlich sind Dedekind'sche Schnitte nach oben beschränkt: Falls α ein Dedekind'scher Schnitt ist, so existiert wegen (D0) eine Zahl $p \in \mathbb{Q}^+ \setminus \alpha$. Damit ist aber p eine obere Schranke von α, denn wäre $q \in \alpha$ mit $q > p$, so wäre aufgrund von (D1) auch $p \in \alpha$, ein Widerspruch.

Ein Dedekind'scher Schnitt α teilt die positiven rationalen Zahlen in zwei disjunkte Stücke:

Wir definieren nun die *positiven reellen Zahlen* als Menge aller Dedekind'schen Schnitte:

$$\mathbb{R}^+ := \{\alpha \subseteq \mathbb{Q}^+ : \alpha \text{ ist ein Dedekindscher Schnitt}\}.$$

Die reellen Zahlen sollen aber die rationalen Zahlen erweitern; diese lassen sich jedoch in natürlicher Weise als Dedekind'sche Schnitte darstellen: Für positive rationale Zahlen $p \in \mathbb{Q}^+$ definieren wir

$$\alpha_p := \{q \in \mathbb{Q}^+ : q < p\}.$$

Dann ist α_p ein Dedekind'scher Schnitt. Um dies zu sehen, müssen wir (D0) – (D2) nachprüfen: (D0) ist offensichtlich. Für (D1) sei $q \in \alpha_p$ und $r \in \mathbb{Q}^+$ mit $r < q$. Da $q < p$, folgt auch $r < p$ und somit $r \in \alpha_p$. Für (D2) sei $q \in \alpha_p$. Somit gilt $q < p$ und für $r := \frac{p+q}{2}$ folgt $r \in \mathbb{Q}^+$, $q < r < p$ und $r \in \alpha_p$.

Für positive rationale Zahlen $p \in \mathbb{Q}^+$ identifizieren wir p mit α_p und erhalten so eine *Einbettung* $\mathbb{Q}^+ \hookrightarrow \mathbb{R}^+$ (ähnlich wie wir auch eine Einbettung $\mathbb{Z} \hookrightarrow \mathbb{Q}$ haben). Es gibt nun aber auch Dedekind'sche Schnitte, die eine "Lücke" in den rationalen Zahlen darstellen. Solche Lücken heissen *irrationale* Zahlen. Zum Beispiel stellt der Dedekind'sche Schnitt

$$\alpha := \{p \in \mathbb{Q}^+ : p^2 < 2\}$$

eine solche Lücke dar. Üblicherweise wird dies implizit mit der Eindeutigkeit der Primfaktorzerlegung der natürlichen Zahlen bewiesen, was wir aber erst später zeigen werden. Der folgende indirekte Beweis stammt aus Dedekinds Schrift *Stetigkeit und irrationale Zahlen*: Wir müssen zeigen, dass es keine rationale Zahl $\frac{p}{q}$ gibt mit $\frac{p^2}{q^2} = 2$. Für einen Widerspruch nehmen wir an, dass Zahlen $p, q \in \mathbb{N}$ existieren mit $\frac{p^2}{q^2} = 2$. Es gibt also positive Zahlen $p, q \in \mathbb{N}$ welche die Gleichung

$$p^2 - 2q^2 = 0$$

erfüllen, woraus $q < p$ und $p < 2q^2$ folgt. Wir dürfen annehmen, dass q die kleinste Zahl ist, welche die Eigenschaft besitzt, dass ihr Quadrat durch Multiplikation mit 2 eine Quadratzahl ist. Setzen wir $\bar{q} := p - q$ und $\bar{p} := 2q - p$, so folgt aus $q < p$ und $\frac{p}{q} < 2$, dass gilt $q < p < 2q$ und $0 < \bar{q} < q$. Mit der Voraussetzung $p^2 - 2q^2 = 0$ erhalten wir

$$\bar{p}^2 - 2\bar{q}^2 = 4q^2 - 4pq + p^2 - 2(p^2 - 2pq + q^2) = -p^2 + 2q^2 = 0$$

und weil $0 < \bar{q} < q$ ist, widerspricht dies der Minimalität von q.

Es stellt sich nun die Frage, wie sich Dedekind'sche Schnitte addieren und multiplizieren lassen. Die Antwort auf diese Frage ist sehr einfach: Man betrachtet einfach die Menge, die dadurch entsteht, dass man alle Elemente des einen Schnittes mit allen Elementen des anderen Schnittes addiert bzw. multipliziert.

Für Dedekind'sche Schnitte $\alpha, \beta \in \mathbb{R}^+$ definieren wir:

$$\alpha + \beta := \big\{p + q : p \in \alpha \wedge q \in \beta\big\}$$

$$\alpha \cdot \beta := \big\{p \cdot q : p \in \alpha \wedge q \in \beta\big\}$$

LEMMA 4.1. *Seien α, β Dedekind'sche Schnitte. Dann sind $\alpha + \beta$ und $\alpha \cdot \beta$ ebenfalls Dedekind'sche Schnitte.*

Beweis. Wir zeigen nur, dass $\alpha + \beta$ ein Dedekind'scher Schnitt ist; der Beweis, dass auch $\alpha \cdot \beta$ ein Dedekind'scher Schnitt ist, ist analog.

(D0) Da $\alpha, \beta \neq \emptyset$, gibt es $p \in \alpha$ und $q \in \beta$. Somit folgt $p + q \in \alpha + \beta$. Da $\alpha, \beta \neq \mathbb{Q}^+$, gibt es $r \in \mathbb{Q}^+ \setminus \alpha$ und $s \in \mathbb{Q}^+ \setminus \beta$. Für $p \in \alpha$ und $q \in \beta$ ist $p < r$ und $q < s$, also ist $p + q < r + s$, woraus folgt $r + s \notin \alpha + \beta$, d.h. $\alpha + \beta \neq \mathbb{Q}^+$.

(D1) Sei $r \in \alpha + \beta$ und $s \in \mathbb{Q}^+$ mit $s < r$. Es gibt $p \in \alpha, q \in \beta$ mit $r = p + q$. Also gilt $s < p + q$ und somit $s - q < p$. Ist $s \leq p, q$, so folgt aus (D1) für α und β, $s \in \alpha$ und $s \in \beta$. Insbesondere ist dann

$$s = \underbrace{\frac{s}{2}}_{\in\alpha} + \underbrace{\frac{s}{2}}_{\in\beta} \in \alpha + \beta$$

wie gewünscht. Sei nun $s \not\leq p, q$, und ohne Beschränkung der Allgemeinheit sei $s > q$. Aus (D1) für α und $s < p + q$ folgt $s - q < p$, also $s - q \in \alpha$. Somit ist

$$s = \underbrace{s - q}_{\in\alpha} + \underbrace{q}_{\in\beta} \in \alpha + \beta.$$

(D2) Sei $r = p + q \in \alpha + \beta$ mit $p \in \alpha$ und $q \in \beta$. Gemäss (D2) für α gibt es ein $p' \in \alpha$ mit $p < p'$. Somit ist $r = p + q < p' + q$ und $p' + q \in \alpha + \beta$.

⊣

In *Stetigkeit und irrationale Zahlen* schreibt Richard Dedekind: *"Ebenso wie die Addition lassen sich auch die übrigen Operationen der sogenannten Elementar-Arithmetik definieren, nämlich die Bildung der Differenzen, Produkte, Quotienten, Potenzen, Wurzeln, Logarithmen, und man gelangt auf diese Weise zu wirklichen Beweisen von Sätzen (wie z. B. $\sqrt{2}\cdot\sqrt{3} = \sqrt{6}$), welche meines Wissens bisher nie bewiesen sind."*

Als Beispiel für die Multiplikation zweier Dedekind'scher Schnitte beweisen wir nun die Gleichung $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$, d.h. für $\alpha = \{p \in \mathbb{Q}^+ : p^2 < 2\}$ und $\beta = \{q \in \mathbb{Q}^+ : q^2 < 3\}$ ist

$$\alpha \cdot \beta = \{r \in \mathbb{Q}^+ : r^2 < 6\}.$$

Beachte zuerst, dass für rationale Zahlen $\frac{s}{t} \in \alpha$ und $\frac{u}{v} \in \beta$ stets $\frac{s^2}{t^2} \cdot \frac{u^2}{v^2} < 6$ gilt. Sei nun $r \in \mathbb{Q}^+$ mit $r^2 < 6$. Wir müssen rationale Zahlen $\frac{s}{t} \in \alpha$ und $\frac{u}{v} \in \beta$ finden, sodass $r^2 < \frac{s^2}{t^2} \cdot \frac{u^2}{v^2}$. Sei $n \in \mathbb{N}$, sodass $6 - r^2 > \frac{1}{n}$, und sei $m \in \mathbb{N}$, sodass $m > 22n$. Dann ist

$$\tfrac{1}{n} > \tfrac{22}{m} > \tfrac{22-\frac{20}{m}}{m} = \tfrac{22m-20}{m^2} = \tfrac{10m+12m-20}{m^2}$$

und es gilt

$$\left(2 - \tfrac{4}{m}\right) \cdot \left(3 - \tfrac{5}{m}\right) = 6 - \tfrac{10m+12m-20}{m^2} > 6 - \tfrac{1}{n} > r^2.$$

Sei $k \in \mathbb{N}$ so, dass gilt $\left(\frac{k+1}{m}\right)^2 \geq 2 > \left(\frac{k}{m}\right)^2$, dann gilt

$$2 - \tfrac{k^2}{m^2} \leq \left(\tfrac{k+1}{m}\right)^2 - \left(\tfrac{k}{m}\right)^2 = \tfrac{2k+1}{m^2}$$

und weil $k < \frac{3m}{2}$ (denn $\frac{9}{4} > 2$), erhalten wir

$$2 - \tfrac{k^2}{m^2} < \tfrac{3m+1}{m^2} = \tfrac{m\left(3+\frac{1}{m}\right)}{m^2} < \tfrac{4}{m}.$$

Analog sei $l \in \mathbb{N}$ so, dass gilt $\left(\frac{l+1}{m}\right)^2 \geq 3 > \left(\frac{l}{m}\right)^2$, dann gilt wieder $3 - \frac{l^2}{m^2} \leq \frac{2l+1}{m^2}$ und weil $l < 2m$ (denn $4 > 3$), erhalten wir

$$3 - \tfrac{l^2}{m^2} < \tfrac{4m+1}{m^2} = \tfrac{m\left(4+\frac{1}{m}\right)}{m^2} < \tfrac{5}{m}.$$

Schliesslich sei $p := 2 - \frac{4}{m}$ und $q := 3 - \frac{5}{m}$. Dann ist

$$0 < p < \tfrac{k^2}{m^2} < 2 \quad \text{und} \quad 0 < q < \tfrac{l^2}{m^2} < 3.$$

Insbesondere ist $\frac{k}{m} \in \alpha$ und $\frac{l}{m} \in \beta$, und mit obiger Ungleichung gilt

$$r^2 < 6 - \tfrac{1}{n} < p \cdot q < \tfrac{l^2}{m^2} \cdot \tfrac{k^2}{m^2} < 6$$

womit $\frac{k}{m}$ und $\frac{l}{m}$ die gesuchten Zahlen sind.

Wir können analog die Konstruktion auch auf die negativen Zahlen ausweiten. Damit lässt sich leicht zeigen, dass die so konstruierten reellen Zahlen wie gewünscht die Körperaxiome erfüllen. Etwas formaler ausgedrückt haben wir das Modell $\mathbb{Q} = (\mathbb{Q}, 0, 1, +, \cdot)$ der rationalen Zahlen zu einem Modell $(\mathbb{R}, 0, 1, +, \cdot)$ erweitert. Was noch fehlt, ist die Ordnungsstruktur der reellen Zahlen und wir müssen auch zeigen, dass das Axiom R_{17} erfüllt ist.

Für Dedekind'sche Schnitte α und β definieren wir:

$$\alpha < \beta :\Longleftrightarrow \alpha \subsetneq \beta.$$

Weil $\mathbb{Q} \models \mathsf{DLO}$ folgt aus der Definition der Dedekind'schen Schnitte leicht, dass $<$ eine (strikte) lineare Ordnungsrelation ist, und weil $\mathbb{Q} \models \mathsf{DLO} + \mathsf{R}_{15} + \mathsf{R}_{16}$ gilt, folgt (wieder aus

der Definition der Dedekind'schen Schnitte), dass die Axiome $\mathsf{DLO} + \mathsf{R}_{15} + \mathsf{R}_{16}$ auch in $\mathbb{R} = (\mathbb{R}, 0, 1, +, \cdot, <)$ erfüllt sind. Es bleibt also nur noch $\mathbb{R} \models \mathsf{R}_{17}$ zu zeigen. Mit anderen Worten, wir müssen zeigen, dass in $\mathbb{R}$ jede nach oben beschränkte Menge ein Supremum besitzt:

THEOREM 4.2. *Die reellen Zahlen $\mathbb{R}$ sind vollständig, d.h. jede nicht-leere nach oben beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Supremum.*

Beweis. Wir beschränken uns auch hier der Einfachheit halber auf die positiven reellen Zahlen. Sei $X \neq \emptyset$ eine nach oben beschränkte Teilmenge von $\mathbb{R}^+$, d.h. die Elemente $\alpha \in X$ sind Dedekind'sche Schnitte der Form $\alpha \subseteq \mathbb{Q}^+$. Wir setzen

$$\beta := \bigcup_{\alpha \in X} \alpha = \big\{p \in \mathbb{Q}^+ : \exists \alpha \in X \ (p \in \alpha)\big\}.$$

Wir zeigen zuerst, dass β ein Dedekind'scher Schnitt ist.

(D0) Offensichtlich gilt $\beta \neq \emptyset$, da $X \neq \emptyset$. Wir zeigen noch, dass $\beta \neq \mathbb{Q}^+$. Da X nach oben beschränkt ist, gibt es eine rationale Zahl $q \in \mathbb{Q}^+$ mit $p < q$ für alle $p \in \beta$. Somit ist $q \in \mathbb{Q}^+ \setminus \beta$.

(D1) Sei $p \in \beta$ und $q \in \mathbb{Q}^+$ mit $q < p$. Dann gibt es ein $\alpha \in X$ mit $p \in \alpha$, und da α (D1) erfüllt, folgt $q \in \alpha \subseteq \beta$.

(D2) Sei $p \in \beta$. Dann gibt es ein $\alpha \in X$ mit $p \in \alpha$. Da α kein maximales Element besitzt, gibt es ein $q \in \alpha$ mit $p < q$. Da $\alpha \subseteq \beta$, folgt $q \in \beta$.

Somit ist also $\beta \in \mathbb{R}^+$. Da nun $\alpha \subseteq \beta$ (d.h. $\alpha \leq \beta$) für alle $\alpha \in X$, ist β eine obere Schranke von X. Es bleibt noch zu zeigen, dass β die kleinste obere Schranke von X ist. Sei $\gamma \in \mathbb{R}^+$ beliebig mit $\gamma < \beta$. Dann gibt es ein $p \in \beta \setminus \gamma$, und nach Definition von β existiert ein $\alpha \in X$ mit $p \in \alpha$. Daraus folgt $\gamma < \alpha$, und weil $\alpha \in X$, kann γ keine obere Schranke von X sein. Also ist β die kleinste obere Schranke von X. ⊣

Es stellt sich die Frage, ob es auch andere Modelle der reellen Zahlen gibt, oder ob zumindest alle Modelle der reellen Zahlen isomorph zueinander sind. Obwohl dies manchmal sogar "bewiesen" wird, ist die Aussage nicht ganz richtig. Genau genommen haben wir nämlich das Modell $\mathbb{R}$ in einem Modell von ZF konstruiert, d.h. die Menge $\mathbb{R}$ der reellen Zahlen ist nicht "absolut" sondern hängt vom zugrunde gelegten Modell von ZF ab, in dem $\mathbb{R}$ konstruiert wurde. Insbesondere hängt die Grösse der Menge $\mathbb{R}$ davon ab, wie gross die Menge $\mathscr{P}(\omega)$ im zugrunde gelegten Modell von ZF ist, was aber von ZF unabhängig ist, d.h. von ZF nicht entschieden wird.

INTERVALLSCHACHTELUNGEN

Die Vollständigkeit der reellen Zahlen ist von fundamentaler Bedeutung für die Grundlagen der Analysis. Zum Beispiel lassen sich damit der Satz von Bolzano-Weierstraß oder der Zwischenwertsatz beweisen.

Eine wichtige Folgerung aus der Vollständigkeit der reellen Zahlen ist der folgende Satz, für den wir zuerst den Begriff der *Intervallschachtelung* definieren: Eine **Intervallschachtelung** ist eine Folge $(I_n)_{n\in\mathbb{N}}$ von nicht-leeren abgeschlossenen Intervallen $I_n = [x_n, y_n]$ mit der Eigenschaft

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots$$

und $\lim\limits_{n\to\infty} (y_n - x_n) = 0$.

THEOREM 4.3. *Sei $((I_n)_{n\in\mathbb{N}}$ eine Intervallschachtelung mit $I_n = [x_n, y_n]$. Dann gibt es genau eine reelle Zahl x mit $x \in \bigcap\limits_{n\in\mathbb{N}} I_n$.*

Beweis. Aufgrund der Vollständigkeit von $\mathbb{R}$ gibt es Zahlen $x, y \in \mathbb{R}$ mit

$$x = \sup\{x_n \in \mathbb{R} : n \in \mathbb{N}\} \quad \text{und} \quad y = \inf\{y_n \in \mathbb{R} : n \in \mathbb{N}\}.$$

Somit gilt

$$x_0 \leq x_1 \leq x_2 \leq \cdots \leq x \leq y \leq \cdots \leq y_2 \leq y_1 \leq y_0$$

und somit $x, y \in \bigcap_{n\in\mathbb{N}} I_n$. Es bleibt zu zeigen, dass $x = y$. Wäre $x < y$, so wäre $\varepsilon := y - x > 0$. Nach Annahme gibt es aber ein $n \in \mathbb{N}$, sodass $y_n - x_n < \varepsilon$ und damit $y - x \leq y_n - x_n < \varepsilon$, was aber ein Widerspruch ist zur Definition von x und y. ⊣

Es sei erwähnt, dass sich mit Hilfe von Theorem 4.3 die reellen Zahlen auch als Äquivalenzklassen von *Cauchy-Folgen* konstruieren lassen.

5. DAS AUSWAHLAXIOM

1904 (und dann nochmals 1907) hat Ernst Zermelo bewiesen, dass sich jede Menge *wohlordnen* lässt. (Zur Erinnerung: Eine Wohlordnung auf einer Menge A ist eine lineare Ordnung $<$ bei der jede nicht-leere Menge $S \subseteq A$ bezüglich $<$ ein minimales Element hat.) Für die Beweise benutzte Zermelo beide Male ein nicht-konstruktives Prinzip, das sogenannte *Auswahlaxiom*.

9. Auswahlaxiom.

$$\forall \mathscr{F}\Big(\emptyset \notin \mathscr{F} \to \exists f\Big(f \in {}^{\mathscr{F}}\bigcup \mathscr{F} \wedge \forall x \in \mathscr{F}\big(f(x) \in x\big)\Big)\Big)$$

Das *Auswahlaxiom* besagt, das es für jede Familie $\mathscr{F}$ von nicht-leeren Mengen eine Funktion f gibt, die aus jeder Menge $x \in \mathscr{F}$ ein Element $f(x)$ auswählt. Etwas informeller heisst dies, dass jede Familie nicht-leerer Mengen eine Auswahlfunktion besitzt, oder noch etwas kürzer, cartesische Produkte nicht-leerer Mengen sind nicht leer.

Die Axiome ZF zusammen mit dem Auswahlaxiom AC (für *Axiom of Choice*) ist das Axiomensystem der **Mengenlehre** und wird mit ZFC bezeichnet.

ÄQUIVALENTE FORMULIERUNGEN DES AUSWAHLAXIOMS

In der Mathematik wird anstelle des Auswahlaxioms meist eine äquivalente Formulierung benutzt, wie zum Beispiel das *Kuratowski-Zorn Lemma* — manchmal auch bloss *Lemma von Zorn* genannt, obwohl Kuratowski dieses Lemma mehr als 10 Jahre vor Zorn bewiesen und publiziert hat.

Bevor wir nun zwei zum Auswahlaxiom äquivalente Auswahlprinzipien formulieren (und deren Äquivalenz zu AC beweisen), beweisen wir, ohne das Auswahlaxiom zu benutzen, ein Lemma. Dafür müssen wir aber zuerst die Begriff *Partialordnung*, *Kette* und *obere Schranke* einführen. Eine Menge P zusammen mit einer binäre Relation $\leq$ ist eine **Partialordnung**, falls die Relation $\leq$ reflexiv ($x \leq x$), anti-symmetrisch (aus $x \leq y$ und $y \leq x$ folgt $x = y$), und transitiv (aus $x \leq y$ und $y \leq z$ folgt $x \leq z$) ist. Eine Teilmenge $K \subseteq P$ einer Partialordnung $(P, \leq)$ ist eine **Kette**, falls K durch $\leq$ linear geordnet wird. Ist $A \subseteq P$ eine Teilmenge der Partialordnung $(P, \leq)$, so ist $q \in P$ eine **obere Schranke von A**, falls $x \leq q$ für alle $x \in A$.

LEMMA 5.1. *Sei $(P, \leq)$ eine nicht-leere Partialordnung. Falls eine Funktion $\mathrm{g} : \mathscr{P}(P) \to P$ existiert die jeder Kette $K \subseteq P$ eine obere Schranke $\mathrm{g}(K)$ zuordnet, und falls eine Funktion $f : P \to P$ existiert, sodass für alle $x \in P$ gilt $x \leq f(x)$, so existiert ein $p_0 \in P$ mit $p_0 = f(p_0)$.*

Beweis. Da jede wohlgeordnete Teilmenge von P eine Kette ist, genügt es das Lemma zu beweisen unter der Voraussetzung, dass jede wohlgeordnete Menge $W \subseteq P$ eine obere Schranke $\mathrm{g}(W)$ hat.

Ist $W \subseteq P$ eine durch "$<$" wohlgeordnete Menge und ist $x \in W$, dann sei

$$W_x := \big\{y \in W : y < x\big\}.$$

Eine Teilmenge A einer wohlgeordneten Menge W heisst **Anfangsabschnitt** von W, falls A mit jedem Element x auch alle y aus W enthält für die gilt $y < x$. Für jedes $x \in W$ ist W_x ein Anfangsabschnitt von W, und auch die ganze Menge W ist ein Anfangsabschnitt von W. Ist A ein Anfangsabschnitt von W, so schreiben wir $A \preccurlyeq W$. Es gilt sogar, dass jeder Anfangsabschnitt der wohlgeordneten Menge W entweder W selber ist, oder von der Form W_x (für ein $x \in W$) ist. Wenn nämlich ein Anfangsabschnitt $A \neq W$ ist und wenn $x_0 \in W$ das $<$-minimale Element ist welches nicht in A ist, so ist $A = W_{x_0}$.

Eine wohlgeordnete Menge $K \subseteq P$ ist eine **fg-Kette**, falls für alle $x \in K$ gilt

$$x = f(\mathrm{g}(K_x))\,.$$

Zum Beispiel ist, weil $\emptyset \subseteq P$ eine wohlgeordnete Menge ist, $\{f(\mathrm{g}(\emptyset))\}$ eine fg-Kette. Insbesondere haben alle f-Ketten dasselbe $<$-minimale Element $f(\mathrm{g}(\emptyset))$. Weiter ist jeder Anfangsabschnitt einer fg-Kette wieder eine fg-Kette.

Seien K und L zwei fg-Ketten. Wir zeigen:

$$K \not\preccurlyeq L \Rightarrow L \preccurlyeq K$$

Die Anfangsabschnitte von K sind die Abschnitte K_y (für $y \in K$) und K selbst. Da K durch die Relation "$<$" wohlgeordnet wird, werden die Anfangsabschnitte K_y durch "$\subsetneq$" wohlgeordnet, denn es gilt:

$$K_x \subsetneq K_y \iff x < y$$

Ist K nicht Anfangsabschnitt von L, so existiert ein $\subsetneq$-minimaler Anfangsabschnitt $A \preccurlyeq K$, sodass $A \not\preccurlyeq L$.

Hätte A kein $<$-maximales Element, so existiert zu jedem $x \in A$ ein $y \in A$ mit $x < y$ und wir hätten $A = \bigcup_{y\in A} A_y$. Weil nun $A \not\preccurlyeq L$ und A $\subsetneq$-minimal ist mit dieser Eigenschaft, ist für alle $y \in A$, $A_y \preccurlyeq L$ und somit ist auch $A = \bigcup_{y\in A} A_y \preccurlyeq L$, im Widerspruch zur Wahl von A.

Somit hat A ein $<$-maximales Element $y_0 \in A$ und $A = A_{y_0} \cup \{y_0\}$, wobei $A_{y_0} \preccurlyeq L$. Wäre nun $L \neq A_{y_0}$, so gäbe es ein $<$-minimales Element $z \in L$ das nicht zu A_{y_0} gehört für das gilt

$$A_{y_0} = L_z\,,$$

und weil K und L zwei fg-Ketten sind und $K_{y_0} = A_{y_0}$, erhalten wir:

$$y_0 = f(g(K_{y_0})) = f(g(L_z)) = z$$

Das heisst, $y_0 = z$ und aus $A = A_{y_0} \cup \{y_0\} = L_z \cup \{z\} \preccurlyeq L$ folgt $A \preccurlyeq L$, entgegen der Voraussetzung. Es bleibt also nur die Möglichkeit $L = A_{y_0} = K_{y_0}$, d. h. L ist ein Anfangsabschnitt von K.

Von zwei fg-Ketten ist also immer eine ein Anfangsabschnitt der anderen. Ist nun

$$U := \bigcup \big\{K \subseteq P : K \text{ ist eine } fg\text{-Kette}\big\}$$

die Vereinigung aller fg-Ketten, dann ist U ebenfalls eine fg-Kette die in keiner fg-Kette echt enthalten ist. Sei $q := \mathrm{g}(U)$ eine obere Schranke von U. Dann ist $q \in U$, denn sonst wäre, weil $f(q) \geq q$, U in der fg-Kette $U \cup \{f(q)\}$ echt enthalten. Daraus folgt, dass auch $p_0 := f(q)$ in U ist. Wäre nun $q \neq p_0$, so folgt aus der Definition von f und aus $f(q) = p_0$, dass gilt $q < p_0$. Dies ist jedoch ein Widerspruch zu $p_0 \in U$ und q obere Schranke von U. Somit ist $q = p_0$, woraus $f(p_0) = p_0$ folgt. ⊣

Die folgende Aussage ist wohl das bekannteste zu AC äquivalente Auswahlprinzip:

Kuratowski-Zorn Lemma KZL. Ist $(P, \leq)$ eine nicht-leere Partialordnung, sodass jede Kette $K \subseteq P$ eine obere Schranke hat, so hat P ein maximales Element.

Für das nächste Auswahlprinzip das zu AC äquivalent ist, brauchen wir den Begriff *endlichen Charakter*: Eine Familie $\mathscr{F}$ von Mengen hat **endlichen Charakter**, falls für jede Menge $x \in \mathscr{F}$ gilt, x ist in $\mathscr{F}$ genau dann, wenn jede endliche Teilmenge von x in $\mathscr{F}$ ist.

Teichmüller-Prinzip TP. Ist $\mathscr{F}$ eine nicht-leere Familie von Mengen mit endlichem Charakter, so hat $\mathscr{F}$ ein bezüglich $\subseteq$ maximales Element.

THEOREM 5.2. *Die folgenden Auswahlprinzipien sind äquivalent.*

(a) *Auswahlaxiom* AC

(b) *Kuratowski-Zorn Lemma* KZL

(c) *Teichmüller-Prinzip* TP

Beweis. AC $\Rightarrow$ KZL: Sei $(P, \leq)$ eine nicht-leere Partialordnung, sodass jede Kette eine obere Schranke hat. Mit AC wählen wir für jede Kette $K \subseteq P$ eine obere Schranke $S(K)$ und definieren für ein $q_0 \in P$ die Funktion $\mathrm{g} : \mathscr{P}(P) \to P$ durch

$$\mathrm{g}(X) := \begin{cases} S(X) & \text{falls } X \subseteq P \text{ eine Kette ist,} \\ q_0 & \text{sonst.} \end{cases}$$

Weiter definieren wir für jedes $x \in P$ die Menge

$$M_x := \begin{cases} \{x\} & \text{falls } x \text{ ein maximales Element von } P \text{ ist,} \\ \{y \in P : y > x\} & \text{sonst.} \end{cases}$$

Dann ist $\{M_x : x \in P\}$ eine Familie von nicht-leeren Mengen und mit AC können wir eine Funktion $f : P \to P$ definieren sodass für alle $x \in P$ gilt:

$$f(x) \in M_x$$

Weil $f(x) \geq x$ (für alle $x \in P$) und nach Voraussetzung jede Kette $K \subseteq P$ eine obere Schranke $g(K)$ hat, existiert mit Lemma 5.1 ein $p_0 \in P$ mit $f(p_0) = p_0$, d. h. P hat ein maximales Element.

KZL $\Rightarrow$ TP: Sei $\mathscr{F}$ eine nicht-leere Familie von Mengen mit endlichem Charakter. Dann ist $(\mathscr{F}, \subseteq)$ eine nicht-leere Partialordnung. Für jede Kette $K \subseteq \mathscr{F}$ sei $U_K := \bigcup K$. Weil $\mathscr{F}$ endlichen Charakter hat, gehört, für Ketten K, jede endliche Teilmenge von U_K zu $\mathscr{F}$, und damit gehört auch U_K zu $\mathscr{F}$ und ist eine obere Schranke der Kette K. Somit hat jede Kette in $\mathscr{F}$ eine obere Schranke, und mit KZL hat somit $\mathscr{F}$ ein bezüglich $\subseteq$ maximales Element.

TP $\Rightarrow$ AC: Sei $\mathscr{F}$ eine Familie von nicht-leeren Mengen. Wir müssen eine Auswahlfunktion für $\mathscr{F}$ finden. Dazu bilden wir die Menge

$$\mathscr{E} = \left\{ f \in {}^{\mathscr{G}}\bigcup \mathscr{G} : f \text{ ist eine Auswahlfunktion für eine Teilfamilie } \mathscr{G} \subseteq \mathscr{F} \right\}.$$

Eine Funktion $f : \mathscr{G} \to \bigcup \mathscr{G}$ ist eine Auswahlfunktion für $\mathscr{G}$ genau dann, wenn jede endliche Teilfunktion von f (d.h. $f|_{\mathscr{G}'}$ für endliche Teilmengen $\mathscr{G}' \subseteq \mathscr{G}$), eine Auswahlfunktion ist. Die Familie $\mathscr{E}$ hat somit endlichen Charakter und mit TP hat $\mathscr{E}$ ein maximales Element f_0. Weil f_0 maximal ist, muss gelten $\mathrm{dom}(f_0) = \mathscr{F}$ und somit ist f_0 eine Auswahlfunktion für $\mathscr{F}$. $\dashv$

6. KONSTRUKTION VON NICHTSTANDARD-MODELLEN

FILTER UND ULTRAFILTER

Sei S eine beliebige nicht-leere Menge. Eine Menge $\mathscr{F} \subseteq \mathscr{P}(S)$ heisst **Filter** über S, falls $\mathscr{F}$ die folgenden Eigenschaften hat:

- $S \in \mathscr{F}$ und $\emptyset \notin \mathscr{F}$
- $(x \in \mathscr{F} \wedge y \in \mathscr{F}) \to (x \cap y) \in \mathscr{F}$
- $(x \in \mathscr{F} \vee y \in \mathscr{F}) \to (x \cup y) \in \mathscr{F}$

Insbesondere gilt, dass $x \in \mathscr{F}$ und $x \subseteq y$ impliziert, dass auch $y \in \mathscr{F}$. Ein Filter über S ist somit eine Mengen von nicht-leeren Teilmengen von S welche abgeschlossen ist unter Obermengen und endlichen Durchschnitten. Zum Beispiel ist $\{S\}$ ein Filter über S.

Ein interessanteres Beispiel eines Filters über einer unendlichen Menge S ist der Filter

$$\mathscr{F} := \big\{x \subseteq S : S \setminus x \text{ ist endlich}\big\},$$

welcher der sogenannte *Fréchet-Filter* ist. Eine Menge $\mathscr{U} \subseteq \mathscr{P}(S)$ ist ein **Ultrafilter** über S, falls $\mathscr{U}$ ein Filter über S ist und für jede Menge $x \in \mathscr{P}(S)$ gilt: entweder $x \in \mathscr{U}$ oder $(S \setminus x) \in \mathscr{U}$. In anderen Worten ist $\mathscr{U}$ ein Ultrafilter, falls $\mathscr{U}$ in keinem Filter echt enthalten ist. Zum Beispiel ist für jedes $a \in S$, die Menge

$$\mathscr{U}_a := \big\{x \subseteq S : a \in x\big\}$$

ein Ultrafilter über S. Solche Ultrafilter heissen *triviale Ultrafilter*. Insbesondere ist jeder Ultrafilter über einer endlichen Menge trivial.

Es stellt sich die Frage, ob nicht-triviale Ultrafilter existieren, zum Beispiel Ultrafilter welche den Fréchet-Filter enthalten. Allgemein stellt sich die Frage, ob sich jeder Filter zu einem Ultrafilter erweitern lässt. Diese Frage wird vom Ultrafilter-Theorem beantwortet, welches mit dem Auswahlaxiom bewiesen werden kann – in ZF aber nicht beweisbar ist.

Ultrafilter-Theorem UFT. Ist $\mathscr{F} \subseteq \mathscr{P}(S)$ ein Filter über S, dann lässt sich $\mathscr{F}$ zu einem Ultrafilter erweitern.

ULTRAPRODUKTE UND ULTRAPOTENZEN

Sei $\mathscr{L}$ eine beliebige Signatur, sei I eine nicht-leere Menge, und für jedes $\iota \in I$ sei $\mathbf{M}_\iota$ eine $\mathscr{L}$-Struktur mit Bereich A_ι. Weiter sei $A := \bigtimes_{\iota \in I} A_\iota$ das cartesische Produkt der Mengen A_ι. Die Elemente aus A identifizieren wir mit Funktionen $f : I \to \bigcup_{\iota \in I} A_\iota$, wobei für jedes $\iota \in I$ gilt $f(\iota) \in A_\iota$. Schliesslich sei $\mathscr{U} \subseteq \mathscr{P}(I)$ ein Ultrafilter über I. Bezüglich $\mathscr{U}$ definieren wir die binäre Relation $\sim$ auf A durch

$$f \sim g \;:\Longleftrightarrow\; \big\{\iota \in I : f(\iota) = g(\iota)\big\} \in \mathscr{U}\,.$$

FAKTUM 6.1. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Wir müssen zeigen, dass $\sim$ reflexiv, symmetrisch und transitiv ist. Offensichtlich gilt für alle $f, g \in A$, $f \sim f$ und $f \sim g \leftrightarrow g \sim f$. Seien nun $f, g, h \in A$ mit $f \sim g$ und $g \sim h$. Weiter sei

$$x := \big\{\iota \in I : f(\iota) = g(\iota)\big\} \quad \text{und} \quad y := \big\{\iota \in I : g(\iota) = h(\iota)\big\}\,.$$

Dann sind $x, y \in \mathscr{U}$ und weil $\mathscr{U}$ ein Filter ist, ist auch $x \cap y$ und jede Obermenge von $x \cap y$ in $\mathscr{U}$. Damit ist

$$x \cap y \subseteq \big\{\iota \in I : f(\iota) = h(\iota)\big\} \in \mathscr{U}\,,$$

woraus $f \sim h$ folgt, was zu zeigen war. ⊣

Für $f \in A$ sei

$$[f] := \{g \in A : g \sim f\}$$

und sei

$$A^* := \big\{[f] : f \in A\big\}.$$

Wir konstruieren nun die $\mathscr{L}$-Struktur $\mathbf{M}^*$ mit dem Bereich A^* wie folgt:

- Für jedes Konstantensymbol $c \in \mathscr{L}$ sei $f_c \in A$ definiert durch

  $$f_c(\iota) := c^{\mathbf{M}_\iota} \quad \text{für alle } \iota \in I,$$

  und sei

  $$c^{\mathbf{M}^*} := [f_c].$$

- Für jedes n-stellige Funktionssymbol $F \in \mathscr{L}$ sei $F^{\mathbf{M}^*} : (A^*)^n \to A^*$, sodass

  $$F^{\mathbf{M}^*}\big([f_0], \dots, [f_{n-1}]\big) = [f] \iff \Big\{\iota \in I : F^{\mathbf{M}_\iota}\big(f_0(\iota), \dots, f_{n-1}(\iota)\big) = f(\iota)\Big\} \in \mathscr{U}.$$

- Für jedes n-stellige Relationssymbol $R \in \mathscr{L}$ sei $R^{\mathbf{M}^*} \subseteq (A^*)^n$, sodass

  $$\big\langle [f_0], \dots, [f_{n-1}]\big\rangle \in R^{\mathbf{M}^*} \iff \Big\{\iota \in I : \big\langle f_0(\iota), \dots, f_{n-1}(\iota)\big\rangle \in R^{\mathbf{M}_\iota}\Big\} \in \mathscr{U}.$$

FAKTUM 6.2. *Die Konstanten $c^{\mathbf{M}^*}$, die Funktionen $F^{\mathbf{M}^*}$, und die Relationen $R^{\mathbf{M}^*}$ sind wohldefiniert.*

Beweis. Wir zeigen nur, dass die Funktionen $F^{\mathbf{M}^*} : (A^*)^n \to A$ wohldefiniert sind, der Beweis für die Wohldefiniertheit von $c^{\mathbf{M}^*}$ und $R^{\mathbf{M}^*}$ ist ähnlich. Sei $F \in \mathscr{L}$ ein n-stelliges Funktionssymbol und seien $\langle f_0, \dots, f_{n-1}\rangle$ und $\langle g_0, \dots, g_{n-1}\rangle$ Elemente in A^n sodass für jedes $0 \leq i < n$ gilt

$$f_i \sim g_i \quad \text{beziehungsweise} \quad [f_i] = [g_i]\,.$$

Weiter definieren wir $f, g \in A$ durch

$$f(\iota) := F^{\mathbf{M}_\iota}\big(f_0(\iota), \dots, f_{n-1}(\iota)\big) \quad \text{und} \quad g(\iota) := F^{\mathbf{M}_\iota}\big(g_0(\iota), \dots, g_{n-1}(\iota)\big)\,.$$

Mit der Definition von $\sim$ und weil $\mathscr{U}$ ein Ultrafilter über I ist, haben wir

$$\big\{\iota \in I : f_0(\iota) = g_0(\iota) \wedge \dots \wedge f_{n-1}(\iota) = g_{n-1}(\iota)\big\} \in \mathscr{U},$$

und damit erhalten wir

$$\Big\{\iota \in I : F^{\mathbf{M}_\iota}\big(f_0(\iota), \dots, f_{n-1}(\iota)\big) = F^{\mathbf{M}_\iota}\big(g_0(\iota), \dots, g_{n-1}(\iota)\big)\Big\} \in \mathscr{U}.$$

Es gilt somit $\big\{\iota \in I : f(\iota) = g(\iota)\big\} \in \mathscr{U}$, woraus $[f] = [g]$ folgt, d. h.

$$F^{\mathbf{M}^*}\big([f_0], \dots, [f_{n-1}]\big) \;=\; F^{\mathbf{M}^*}\big([g_0], \dots, [g_{n-1}]\big)\,.$$

Damit hängt $F^{\mathbf{M}^*}$ nicht von der Wahl der Repräsentanten von $[f_i]$ ab. ⊣

Die $\mathscr{L}$-Struktur $\mathbf{M}^*$ mit Bereich A^* ist das **Ultraprodukt** der $\mathscr{L}$-Strukturen $\mathbf{M}_\iota$ ($\iota \in I$) bezüglich dem Ultrafilter $\mathscr{U}$ über I. Falls wir für alle $\iota \in I$ dieselbe $\mathscr{L}$-Struktur $\mathbf{M}$ haben, d. h. $\mathbf{M}_\iota = \mathbf{M}$ für alle $\iota \in I$, dann ist $\mathbf{M}^*$ die **Ultrapotenz** von $\mathbf{M}$ bezüglich $\mathscr{U}$.

Im nächsten Abschnitt zeigen wir, dass falls jede $\mathscr{L}$-Struktur $\mathbf{M}_\iota$ ein Modell der $\mathscr{L}$-Theorie T ist, auch das Ultraprodukt $\mathbf{M}^*$ ein Modell von T ist.

DER SATZ VON ŁOŚ

Sei wie oben $\mathscr{L}$ eine beliebige Signatur, sei I eine nicht-leere Menge, und für jedes $\iota \in I$ sei $\mathbf{M}_\iota$ eine $\mathscr{L}$-Struktur mit Bereich A_ι. Weiter sei $\mathscr{U}$ Ultrafilter über I und sei $\mathbf{M}^*$ das Ultraprodukt der $\mathscr{L}$-Strukturen $\mathbf{M}_\iota$ ($\iota \in I$) bezüglich $\mathscr{U}$. Mit dem folgenden Theorem können wir entscheiden, welche $\mathscr{L}$-Sätze im Modell $\mathbf{M}^*$ wahr sind.

THEOREM 6.3 (SATZ VON ŁOŚ). *Für jeden $\mathscr{L}$-Satz σ gilt:*

$$\mathbf{M}^* \models \sigma \quad \iff \quad \big\{\iota \in I : \mathbf{M}_\iota \models \sigma\big\} \in \mathscr{U}$$

Beweis. Mit den logischen Axiomen lässt sich zeigen, dass jeder $\mathscr{L}$-Satz σ logisch äquivalent ist zu einem $\mathscr{L}$-Satz σ' welcher nur $\neg$ und $\wedge$ als logische Operatoren und nur $\exists$ als Quantor enthält. Somit genügt es den SATZ VON ŁOŚ für $\mathscr{L}$-Sätze σ' zu beweisen. Der Beweis ist mit Induktion über der Anzahl der Symbole $\neg$, $\wedge$ und $\exists$ welche im $\mathscr{L}$-Satz σ' vorkommen.

Nach Konstruktion von $\mathbf{M}^*$ gilt der SATZ VON ŁOŚ für atomare $\mathscr{L}$-Sätze σ', d. h. für Sätze σ' die mit den Regeln (F0) und (F1) gebildet wurden.

Sei $\sigma' \equiv \neg\sigma_0$, wobei wir annehmen, dass der SATZ VON ŁOŚ für σ_0 bereits bewiesen wurde. Dann haben wir:

$$\begin{aligned}
\mathbf{M}^* \models \neg\sigma_0 \quad &\iff \quad \mathbf{M}^* \not\models \sigma_0 \\
&\iff \quad \big\{\iota \in I : \mathbf{M}_\iota \models \sigma_0\big\} \notin \mathscr{U} \\
&\iff \quad I \setminus \big\{\iota \in I : \mathbf{M}_\iota \models \sigma_0\big\} \in \mathscr{U} \\
&\iff \quad \big\{\iota \in I : \mathbf{M}_\iota \not\models \sigma_0\big\} \in \mathscr{U} \\
&\iff \quad \big\{\iota \in I : \mathbf{M}_\iota \models \neg\sigma_0\big\} \in \mathscr{U}
\end{aligned}$$

Sei nun $\sigma' \equiv \sigma_1 \wedge \sigma_2$, wobei wir annehmen, dass der SATZ VON ŁOŚ für σ_1 und σ_2 bereits bewiesen wurde. Dann haben wir:

$$\begin{aligned}
\mathbf{M}^* \models \sigma_1 \wedge \sigma_2 \quad &\iff \quad \mathbf{M}^* \models \sigma_1 \quad \text{UND} \quad \mathbf{M}^* \models \sigma_2 \\
&\iff \quad \underbrace{\big\{\iota \in I : \mathbf{M}_\iota \models \sigma_1\big\}}_{=:x_1} \in \mathscr{U} \text{ UND } \underbrace{\big\{\iota \in I : \mathbf{M}_\iota \models \sigma_2\big\}}_{=:x_2} \in \mathscr{U} \\
&\iff \quad x_1 \cap x_2 \in \mathscr{U} \\
&\iff \quad \big\{\iota \in I : \mathbf{M}_\iota \models \sigma_1 \wedge \sigma_2\big\} \in \mathscr{U}
\end{aligned}$$

Sei nun $\sigma' \equiv \exists\nu\sigma_0$ (für eine Variable ν), wobei wir annehmen, dass für ein $[g] \in A^*$ gilt

$$\mathbf{M}^* \tfrac{[g]}{\nu} \models \sigma_0(\nu) \iff \big\{\iota \in I : \mathbf{M}_\iota \tfrac{g(\iota)}{\nu} \models \sigma_0(\nu)\big\} \in \mathscr{U}.$$

Dann haben wir:

$$\begin{aligned}
\mathbf{M}^* \models \exists\nu\sigma_0 \quad &\iff \quad \text{ES EXISTIERT EIN } [g_0] \text{ IN } A^* \text{ MIT } \mathbf{M}^* \tfrac{[g_0]}{\nu} \models \sigma_0(\nu) \\
&\iff \quad \text{ES EXISTIERT EIN } [g_0] \text{ IN } A^* \text{ MIT } \underbrace{\big\{\iota \in I : \mathbf{M}_\iota \tfrac{g_0(\iota)}{\nu} \models \sigma_0(\nu)\big\}}_{=:x} \in \mathscr{U}
\end{aligned}$$

Weil $x \subseteq \big\{\iota \in I : \mathbf{M}_\iota \models \exists\nu\sigma_0\big\}$, folgt $\big\{\iota \in I : \mathbf{M}_\iota \models \exists\nu\sigma_0\big\} \in \mathscr{U}$, und wir erhalten

$$\mathbf{M}^* \models \exists\nu\sigma_0 \quad \implies \quad \big\{\iota \in I : \mathbf{M}_\iota \models \exists\nu\sigma_0\big\} \in \mathscr{U}.$$

Um die andere Richtung zu zeigen brauchen wir AC. Falls, für ein $\iota \in I$, $\mathbf{M}_\iota \models \exists\nu\sigma_0$, dann existiert ein $a_\iota \in A_\iota$, sodass $\mathbf{M}_\iota \frac{a_\iota}{\nu} \models \sigma_0(\nu)$, andernfalls sei a_ι irgend ein Element von A_ι. Für

die Funktion

$$\begin{array}{rccc} g_0: & I & \to & \bigcup A \\ & \iota & \mapsto & a_\iota \end{array}$$

gilt $\{\iota \in I : \mathbf{M}_\iota \models \exists \nu \sigma_0\} = \{\iota \in I : \mathbf{M}_\iota \frac{g_0(\iota)}{\nu} \models \sigma_0(\nu)\}$. Insbesondere haben wir

$$\{\iota \in I : \mathbf{M}_\iota \models \exists \nu \sigma_0\} \in \mathscr{U} \quad \Longrightarrow \quad \{\iota \in I : \mathbf{M}_\iota \frac{g_0(\iota)}{\nu} \models \sigma_0(\nu)\} \in \mathscr{U},$$

woraus folgt

$$\{\iota \in I : \mathbf{M}_\iota \models \exists \nu \sigma_0\} \in \mathscr{U} \quad \Longrightarrow \quad \mathbf{M}^* \models \exists \nu \sigma_0 .$$

Somit gilt:

$$\mathbf{M}^* \models \exists \nu \sigma_0 \Longleftrightarrow \{\iota \in I : \mathbf{M}_\iota \models \exists \nu \sigma_0\} \in \mathscr{U}$$

⊣

Ist zum Beispiel $I = \omega$ und für alle $n \in \omega$, $\mathbf{M}_n = \mathbb{N}$ (wobei $\mathbb{N}$ das Standardmodell der Peano-Arithmetik ist), so gelten in der Ultrapotenz $\mathbf{M}^*$ von $\mathbb{N}$ genau dieselben $\mathscr{L}_{\mathsf{PA}}$-Sätze wie im Modell $\mathbb{N}$. Insbesondere lassen sich die Modelle $\mathbb{N}$ und $\mathbf{M}^*$ durch die Sätze, die in ihnen gelten, nicht unterscheiden, obwohl das Modell $\mathbb{N}$ für nicht-triviale Ultrafilter $\mathscr{U}$ über ω überabzählbar ist.

7. EINFÜHRUNG IN DIE NICHTSTANDARD-ANALYSIS

Die Idee der Nichtstandard-Analysis ist, dass wir gleichzeitig mit zwei Modellen der reellen Zahlen arbeiten. Ein Modell, nennen wir es das *Grundmodell*, übernimmt die Rolle des Standardmodells $\mathbb{R}$, und das andere Modell, eine Ultrapotenz von $\mathbb{R}$ bezüglich einem nicht-trivialen Ultrafilter $\mathscr{U}$ über ω, welches wir mit $\mathbb{R}^*$ bezeichnen, ist aus der Sicht von $\mathbb{R}$ ein Nichtstandardmodell. In $\mathbb{R}^*$ sind dieselben Sätze wahr wie im Modell $\mathbb{R}$, d. h. die beiden Modelle sind elementar äquivalent. Wir stellen uns nun auf den Standpunkt, dass die eigentliche Analyse im Modell $\mathbb{R}^*$ stattfindet, aber — als Menschen die in $\mathbb{R}$ leben — können wir nur den Standardteil der reellen Zahlen in $\mathbb{R}^*$ "sehen". Auch wenn wir eine recht eingeschränkte Sicht von aus $\mathbb{R}$ auf die richtige Analysis haben, können wir aufgrund der Tatsache, dass die Modelle $\mathbb{R}$ und $\mathbb{R}^*$ elementar äquivalent sind, keinen Unterschied zwischen den beiden Modellen auf der formalen Ebene sehen, denn jeder Satz der in einem der Modelle wahr ist, ist auch im anderen Modell wahr. Um zum Beispiel ein Problem in $\mathbb{R}$ zu lösen, können wir unsere Berechnungen auch in $\mathbb{R}^*$ durchführen, wobei wir in $\mathbb{R}^*$ reelle Zahlen verwenden können, die es in $\mathbb{R}$ nicht gibt, und am Ende "projizieren" wir das Ergebnis einfach wieder auf $\mathbb{R}$.

Wir betrachten nun die Modelle $\mathbb{R}$ und $\mathbb{R}^*$ etwas genauer und legen auch die Notationen fest: Der Bereich von $\mathbb{R}$ wird mit $\mathbb{R}$ bezeichnet, mit den natürlichen Zahlen $\mathbb{N}$, und der Bereich von $\mathbb{R}^*$ wird mit $\mathbb{R}^*$ bezeichnet, mit den natürlichen Zahlen $\mathbb{N}^*$. Die Elemente aus $\mathbb{R}^*$ sind Äquivalenzklassen $[f]$ von Funktionen $f : \omega \to \mathbb{R}$. Für solche Äquivalenzklassen schreiben wir auch einfach r^*. Durch die Einbettung

$$\begin{array}{rcll} \mathbb{R} & \to & \mathbb{R}^* & \\ r & \mapsto & [c_r] & \text{wobei } c_r : \omega \to \{r\} \end{array}$$

erhalten wir, dass $\mathbb{R}$ eine Teilmenge ist von $\mathbb{R}^*$, und auch, dass $\mathbb{N}$ eine Teilmenge ist von $\mathbb{N}^*$. Ferner sehen wir, dass die Äquivalenzklasse $[d]$ für $d(n) := n$ (für alle $n \in \mathbb{N}$) ein Element aus $\mathbb{N}^*$ ist, welches grösser ist als alle Elemente aus $\mathbb{N}$. Für $N := [d]$ ist damit $N \in \mathbb{N}^* \setminus \mathbb{N}$. Andererseits ist die Äquivalenzklasse $\delta_0 := [d^{-1}]$ für $d^{-1}(n) := \frac{1}{n}$ (für alle $n \in \mathbb{N}$) ein Element aus $\bar{\mathbb{R}}$, für welches gilt $0 < \delta_0 < \frac{1}{n}$ (für alle $n \in \mathbb{N}$). Vom Standpunkt von $\mathbb{R}$ aus gesehen existiert δ_0 nicht, denn δ_0 wäre eine unendlich kleine reelle Zahl, eine sogenannte **Infinitesimalzahl** (d. h. eine reelle Zahl ungleich Null, deren Absolutwert kleiner ist als $\frac{1}{n}$ für jedes $n \in \mathbb{N}$). Wir sagen, dass $r^*, s^* \in \mathbb{R}^*$ **unendlich nahe** sind, bezeichnet mit $r^* \approx s^*$, wenn $r^* - s^*$ infinitesimal ist. Man beachte, dass $\approx$ eine Äquivalenzrelation auf $\mathbb{R}^*$ definiert.

Sei $\bar{\mathbb{R}}$ die Menge aller reellen Zahlen $r^* \in \mathbb{R}^*$, für die es $s_1, s_2 \in \mathbb{R}$ gibt mit $s_1 \leq r^* \leq s_2$. Offensichtlich ist $\mathbb{R} \subseteq \bar{\mathbb{R}} \subseteq \mathbb{R}^*$.

Die folgende Proposition besagt, dass die reellen Zahlen in $\bar{\mathbb{R}}$ genau die reellen Zahlen sind, die auf $\mathbb{R}$ "projiziert" werden können, d. h. die unendlich nahe bei einer reellen Zahl aus $\mathbb{R}$ liegen.

PROPOSITION 7.1. *Für jedes $r^* \in \bar{\mathbb{R}}$ existiert genau ein $r \in \mathbb{R}$, sodass $r^* \approx r$.*

Beweis. Die Eindeutigkeit ist offensichtlich, denn aus $r_1, r_2 \in \mathbb{R}$ mit $r^* \approx r_1$ und $r^* \approx r_2$ folgt aus der Transitivität, dass $r_1 \approx r_2$, und weil $r_1, r_2 \in \mathbb{R}$ folgt $r_1 - r_2 = 0$, also $r_1 = r_2$.

Um die Existenz zu zeigen gehen wir wie folgt vor: Sei $r^* = [f]$ für ein $f : \omega \to \mathbb{R}$ und seien $s, t \in \mathbb{R}$ so, dass $[c_s] \leq [f] \leq [c_t]$. Dann gilt

$$\big\{n \in \omega : s \leq f(n) \leq t\big\} \in \mathscr{U} .$$

Wir konstruieren nun die Sequenzen (s_n) und (t_n) in $\mathbb{R}$ wie folgt: Sei $s_0 := s$ und $t_0 := t$. Seien s_n und t_n bereits konstruiert mit

$$x_n := \big\{n \in \omega : s_n \leq f(n) \leq t_n\big\} \in \mathscr{U} \,,$$

Sei

$$y_n := \big\{n \in \omega : s_n \leq f(n) \leq \tfrac{s_n+t_n}{2}\big\} \qquad \text{und} \qquad z_n := \big\{n \in \omega : \tfrac{s_n+t_n}{2} < f(n) \leq t_n\big\} \,.$$

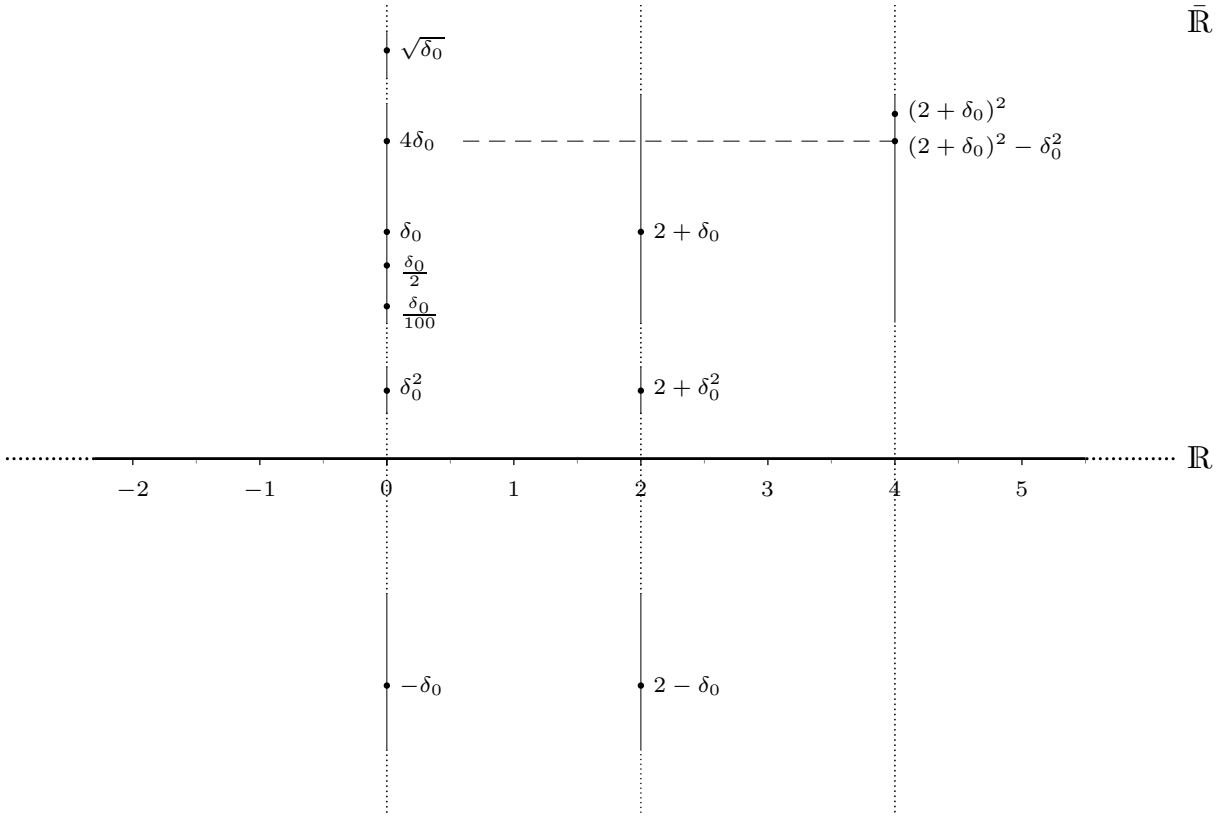
Weil $\mathscr{U}$ ein Ultrafilter ist haben wir entweder $y_n \in \mathscr{U}$ oder $(\omega \setminus y_n) \in \mathscr{U}$. Im ersten Fall, sei $s_{n+1} = s_n$ und $t_{n+1} = \frac{s_n+t_n}{2}$, im zweiten Fall sei $s_{n+1} = \frac{s_n+t_n}{2}$ und $t_{n+1} = t_{n+1}$. Beachte, dass $y_n \cup z_n = x_n$ und somit $x_n \cap (\omega \setminus y_n) = z_n$, sodass in beiden Fällen gilt

$$x_{n+1} := \big\{n \in \omega : s_{n+1} \leq f(n) \leq t_{n+1}\big\} \in \mathscr{U} \,.$$

Die Folge (s_n) ist monoton wachsend und die Folge (t_n) ist monoton fallend, wobei für alle $n \in \mathbb{N}$ gilt $[c_{s_n}] \leq [f] \leq [c_{t_n}]$. Weil nach Konstruktion, $\lim_{n\to\infty}(t_n - s_n) = 0$, ist das Supremum $r \in \mathbb{R}$ der Folge (s_n) gleich dem Infimum der Folge (t_n), und somit ist $r^* \approx r$. ⊣

Für $r^* \in \bar{\mathbb{R}}$ heisst die eindeutig bestimmte Zahl $r \in \mathbb{R}$, sodass $r \approx r^*$, der **Standardteil** von $r^* \in \bar{\mathbb{R}}$, bezeichnet mit $\mathrm{st}\,(r^*)$. Proposition 7.1 besagt, dass jede reelle Zahl $r^* \in \bar{\mathbb{R}}$ von der Form $r^* = [c_r] + [f_\delta]$ ist, wobei $r = \mathrm{st}\,(r^*)$ und für $f_\delta : \omega \to \mathbb{R}$ gilt $\lim_{n\to\infty} f_\delta(n) = 0$. Um die Notation zu vereinfachen schreiben wir für r^* bloss $r + \delta$ anstelle von $[c_r] + [f_\delta]$.

Sei zum Beispiel $N \in \mathbb{N}^* \setminus \mathbb{N}$ und $\delta_0 := \frac{1}{N}$. Dann ist der Standardteil von δ_0 gleich 0, d. h., für die Leute in $\mathbb{R}$ ist $\delta_0 \approx 0$. Weiter ist $2 + \delta_0 \approx 2$ bzw. $\mathrm{st}\,(2 + \delta_0) = 2$. Ferner ist $2 + \delta_0$ in $\bar{\mathbb{R}}$, aber $N = \frac{1}{\delta_0}$ ist nicht in $\bar{\mathbb{R}}$, weil es kein $s \in \mathbb{R}$ gibt, sodass $N \leq s$. Die Menge $\bar{\mathbb{R}}$, als eine Teilmenge von $\mathbb{R}^*$, ist linear geordnet durch $<^*_{\mathbb{R}}$. Beachte, dass $<^*_{\mathbb{R}}$ eingeschränkt auf $\mathbb{R}$ die lineare Ordnung auf $\mathbb{R}$ ist. Die folgende Figur veranschaulicht die Ordnungsstruktur von $\bar{\mathbb{R}}$.



Das folgende Resultat zeigt unter anderem, wie man in der Nichtstandard-Analysis ohne Limites bestimmte Integrale berechnen kann (Beweise finden sich in Ch. 4,5,6 von [Rob]*).

PROPOSITION 7.2.

(a) Sei $a \in \mathbb{R}$, sei f eine reelle Funktion welche stetig ist an der Stelle a, und sei $a^* \in \mathbb{R}^*$ mit $a^* \approx a$. Dann gilt:

$$f(a^*) \approx f(a)$$

(b) Sei $a \in \mathbb{R}$ und sei f eine reelle Funktion. Existiert ein $r \in \mathbb{R}$ sodass

$$\operatorname{st}\left(\frac{f(a+\delta)-f(a)}{\delta}\right) = r \quad \text{für alle } \delta \approx 0 \text{ mit } \delta \neq 0,$$

so ist f differenzierbar an der Stelle a und es gilt $f'(a) = r$.

(c) Sei $b \in \mathbb{R}$, sei f eine reelle Funktion welche stetig ist im Intervall $[0, b]$, und sei $N \in \mathbb{N}^* \setminus \mathbb{N}$. Dann gilt in $\mathbb{R}$:

$$\int_0^b f(x)\,dx \;=\; \operatorname{st}\left(\frac{b}{N}\sum_{k=0}^{N-1} f\left(\tfrac{kb}{N}\right)\right).$$

EIN BEISPIEL

$$\int_0^{2\pi} \ln(2-e^{ix})dx$$

Sei $N \in \mathbb{N}^* \setminus \mathbb{N}$. Mit Proposition 7.2.(c) gilt:

$$\int_0^{2\pi} \ln(2-e^{ix})dx = \operatorname{st}\left(\frac{2\pi}{N}\cdot\sum_{k=0}^{N_1}\ln\left(2-e^{2\pi ik/N}\right)\right) = \operatorname{st}\left(\frac{2\pi}{N}\cdot\ln\Big(\prod_{k=0}^{N_1}\left(2-e^{2\pi ik/N}\right)\Big)\right)$$

Sei nun $\xi := e^{2\pi i/N}$. Dann sind ξ^k für $k = 0, \ldots, N-1$ grad die N verschiedenen Nullstellen von $X^N - 1$. Das heisst,

$$X^N - 1 = (X-\xi^0)\cdot(X-\xi^1)\cdot(X-\xi^2)\cdot\ldots\cdot(X-\xi^{N-1}),$$

und somit ist

$$\prod_{k=0}^{N_1}\left(2-e^{2\pi ik/N}\right) = \prod_{k=0}^{N_1}\left(2-\xi^k\right) = 2^N - 1\,.$$

Weiter ist

$$\tfrac{2\pi}{N}\cdot\ln\left(2^{N-1}\right) < \tfrac{2\pi}{N}\cdot\ln\left(2^N-1\right) < \tfrac{2\pi}{N}\cdot\ln\left(2^N\right),$$

*[Rob] Alain M. Robert: *Nonstandard Analysis*. Dover Publ. New York. 1988

und mit $\ln\big(2^{N-1}\big) = (N-1)\cdot\ln(2)$ und $\ln\big(2^N\big) = N\cdot\ln(2)$ folgt:

$$\big(1-\tfrac{1}{N}\big)\cdot 2\pi\cdot\ln(2) < \tfrac{2\pi}{N}\cdot\ln\big(2^N-1\big) < 2\pi\cdot\ln(2)$$

Weil nun $\mathrm{st}\,(1+\tfrac{1}{N}\big) = 1$, folgt

$$\mathrm{st}\,\big(\tfrac{2\pi}{N}\cdot\ln\big(2^N-1\big)\big) = 2\pi\cdot\ln(2)\,,$$

und somit ist

$$\int_0^{2\pi} \ln(2-e^{ix})dx \;=\; 2\pi\cdot\ln(2) \;=\; \pi\cdot\ln(4)\,.$$

8. GRUNDBEGRIFFE DER GRAPHENTHEORIE

KNOTEN, KANTEN, GRADE

Ein **Graph** kann aufgefasst werden als eine $\mathscr{L}$-Struktur mit einem Bereich V, wobei die Signatur $\mathscr{L}$ aus einer oder mehreren binären Relationssymbolen E bzw. $E_0, \ldots, E_k$ (für k endlich) besteht. Ein Graph G besteht also aus einer Menge V, den sogenannten **Knoten** (engl. *vertices*), und einer oder mehrerer Mengen $E \subseteq V \times V$ bzw. $E_0, \ldots, E_k \subseteq V \times V$, den sogenannten **Kanten** (engl. *edges*). Wir schreiben also $G = (V, E)$ bzw. $G = (V, E_0, \ldots, E_k)$.

xEy bzw. $\langle x, y\rangle \in E$ bedeutet, dass x und y durch eine Kante von x nach y verbunden sind; x und y heissen dann **adjazent**. Ist $G = (V, E)$ ein Graph und ist die Relation E symmetrisch, d. h. $\forall x, y \in V\,(xEy \leftrightarrow yEx)$, so ist G ein **ungerichteter** Graph, andernfalls ist G ein **gerichteter** Graph, auch **Digraph** genannt. Ist $G = (V, E)$ ein ungerichteter Graph, so indentifizieren wir die Kanten $\langle x, y\rangle$ und $\langle y, x\rangle$ und schreiben $\{x, y\} \in E$.

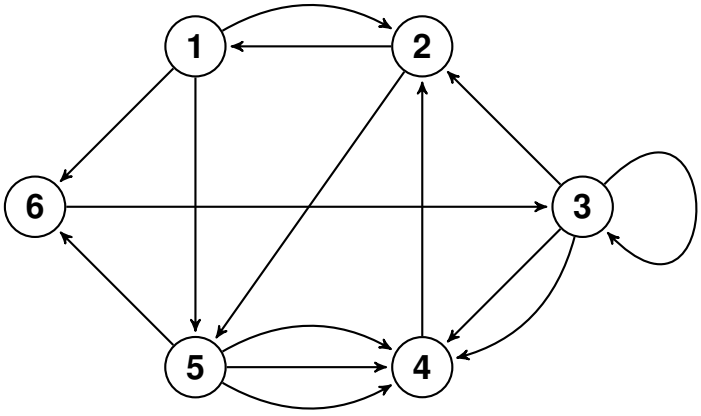
Eine Kante $\langle x, x\rangle$ heisst **Schlinge** (engl. *loop*). Ein Graph $G = (V, E)$ ist **schlingenfrei**, wenn er keine Schlingen besitzt, wenn also $\forall x \in V\,(\neg xEx)$ gilt. Wenn wir mehrere Relationen $E_0, \ldots, E_k$ in $\mathscr{L}$ haben, so kann der Graph $(V, E_0, \ldots, E_k)$ auch mehrere Kanten zwischen zwei Knoten x und y besitzen. Solche *Mehrfachkanten* sind verschieden, da sie zu verschiedenen Relationen E_i gehören. Ein Graph ohne Schlingen und Mehrfachkanten heisst **schlicht**.

Ist $G = (V, E)$ ein endlicher Graph, d. h. $V = \{v_1, \ldots v_n\}$ für ein endliches n und $E \subseteq V \times V$, so können wir den Graphen G mit einer $(n \times n)$-Matrix $A(G) = (a_{ij})$, der sogenannten **Adjazenzmatrix** von G, darstellen, welche wie folgt definiert ist:

$$a_{ij} = \begin{cases} 1 & \text{falls } \langle v_i, v_j\rangle \in E, \\ 0 & \text{sonst.} \end{cases}$$

Ist $G = (V, E_0, \ldots, E_k)$ ein endlicher Graph mit Mehrfachkanten, so ist die Adjazenzmatrix $A(G)$ von G die Summe der Adjazenzmatrizen $A(G_l)$ der Graphen $G_l = (V, E_l)$, d. h. $A(G) = \sum_{l=0}^{k} A(G_l)$. Die Adjazenzmatrix $A(G)$ eines Graphen G ist genau dann symmetrisch, wenn G ein ungerichteter Graph ist.

Beispiel eines gerichteten Graphen und seiner Adjazenzmatrix:



$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Der Grad eines Knotens $x \in V$ "misst" wie viele Kanten von x ausgehen bzw. in x zusammenkommen.

Wir definieren Grade von Knoten zuerst für Digraphen: Sei $G = (V, E)$ ein Digraph. Für $x \in V$ seien

$$\Gamma^+(x) := \big\{y \in V : \langle x, y\rangle \in E\big\} \quad \text{und} \quad \Gamma^-(x) := \big\{y \in V : \langle y, x\rangle \in E\big\}.$$

Weiter seien

$$\deg^+(x) := |\Gamma^+(x)| \quad \text{und} \quad \deg^-(x) := |\Gamma^-(x)|.$$

Für $x \in V$ heisst $\deg^+(x)$ **positiver Halbgrad** von x und $\deg^-(x)$ heisst **negativer Halbgrad** von x. Manchmal wird $\deg^+(x)$ auch mit $d_{\text{out}}(x)$ und $\deg^-(x)$ auch mit $d_{\text{in}}(x)$ bezeichnet. Schliesslich sei $\deg(x) := \deg^+(x) + \deg^-(x)$ der **Grad** von x. Beachte: Schlingen werden für den Grad doppelt gezählt.

Ist $G = (V, E)$ ein ungerichteter Graph, so definieren wir für $x \in V$:

$$\Gamma(x) := \big\{y \in V : \{x, y\} \in E\big\} \quad \text{und} \quad \deg(x) := |\Gamma(x)| + |\big\{x \in V : \{x\} \in E\big\}|.$$

Ein ungerichteter Graph $G = (V, E)$ mit $\deg(x) = r$ für alle $x \in V$ heisst **regulär** vom Grad r.

Ein ungerichteter Graph heisst **vollständig**, falls für alle Knoten $x \neq y$ gilt $\{x, y\} \in E$. Der vollständige, ungerichtete, schlichte Graph mit n Knoten wird mit K_n bezeichnet. K_n ist ein regulärer Graph vom Grad $n - 1$.

Teilgraphen, Pfeil- und Kantenzüge

Seien $G = (V, E)$ und $G' = (V', E')$ Graphen mit $V' \subseteq V$ und $E' \subseteq E$, so ist G' ein **Teilgraph** von G, geschrieben $G' \subseteq G$.

Spezialfälle

- Sei $U \subseteq V$. Der **durch U erzeugte** Teilgraph $G' = G_U \subseteq G$ ist definiert durch
$$V' := U \quad \text{und} \quad E' := \big\{\langle x, y\rangle \in E : \{x, y\} \subseteq U\big\}.$$
- Sei $F \subseteq E$. Der **durch F erzeugte** Teilgraph $G' = G_F \subseteq G$ ist definiert durch
$$V' := \bigcup \big\{\{x, y\} \subseteq V : \langle x, y\rangle \in F\big\} \quad \text{und} \quad E' := F.$$

Sei $G = (V, E)$ ein Digraph (nicht notwendigerweise schlingenfrei) und sei $H \subseteq E$ eine nicht-leere, endliche Kantenteilmenge sodass für ein $l \geq 1$ gilt:

$$|H| = l \quad \text{und} \quad H = \big\{\langle x_0, x_1\rangle, \langle x_1, x_2\rangle, \ldots, \langle x_{l-1}, x_l\rangle\big\}.$$

Der durch H erzeugte Teilgraph G_H heisst **Pfeilzug von x_0 nach x_l** der Länge l. Wir unterscheiden:

- **offener Pfeilzug**, falls $x_0 \neq x_l$
- **geschlossener Pfeilzug** falls $x_0 = x_l$,

Beachte, dass in einem Pfeilzug die Kanten paarweise verschieden sind. Falls auch die x_i paarweise verschieden sind, so heisst G_H **Bahn von x_0 nach x_l** der Länge l. Falls die x_i paarweise verschieden sind ausser $x_0 = x_l$, so ist G_H ein **Wirbel**.

Aus den Definitionen folgt, dass jeder offene Pfeilzug von a nach b eine Bahn von a nach b als Teilgraphen enthält, und dass jeder geschlossene Pfeilzug immer einen Wirbel als Teilgraphen enthält.

Für ungerichtete Graphen sind die Definitionen analog und wir sprechen im ungerichteten Fall von **offenen** bzw. **geschlossenen Kantenzügen** (anstelle von Pfeilzügen), sowie von **Wegen** und **Kreisen** (anstelle von Bahnen und Wirbeln).

Die Definition sind analog für Graphen mit Mehrfachkanten, wobei Mehrfachkanten wieder als verschieden betrachtet werden.

Ein Graph (gerichtet oder ungerichtet) heisst **zusammenhängend**, wenn jedes Paar von verschiedenen Knoten durch einen Weg (ungerichtet) verbunden ist.

Pfeilfolgen bestimmter Länge

Eine Folge der Länge l von Kanten $\langle x_0, x_1\rangle$, $\langle x_1, x_2\rangle$, $\ldots$, $\langle x_{l-1}, x_l\rangle$ eines Graphen $G = (V, E_0, \ldots, E_k)$, in der Kanten auch mehrfach vorkommen können, nennen wir eine **Pfeilfolge von x_0 nach x_l der Länge l.**

Mit der Adjazenzmatrix eines Digraphen $G = (V, E_0, \ldots, E_k)$ können wir bestimmen, wie viele verschiedene Peilfolgen einer bestimmten Länge es zwischen zwei Knoten gibt.

Proposition 8.1. *Sei $G = (V, E_0, \ldots, E_k)$ mit $V = \{v_1, \ldots, v_n\}$ ein endlicher Digraph und sei A die Adjazenzmatrix von G. Sei A^k die k-te Potenz von A für ein $k \geq 1$. Ist $A^k := \left(a_{ij}^{[k]}\right)$, so ist $a_{ij}^{[k]}$ die Anzahl der verschiedenen Pfeilfolgen von v_i nach v_j der Länge k.*

Beweis. Mit Induktion nach k. Für $k = 1$ folgt die Behauptung aus der Definition der Adjazenzmatrix. Es gilt also für alle $l, j \in \{1, \ldots, n\}$:

$$a_{lj}^{[1]} \text{ ist die Anzahl der Pfeilfolgen der Länge } 1 \text{ von } v_l \text{ nach } v_j.$$

Sei die Behauptung richtig für ein $k \geq 1$. Dann gilt für alle $i, l \in \{1, \ldots, n\}$:

$$a_{il}^{[k]} \text{ ist die Anzahl der Pfeilfolgen der Länge } k \text{ von } v_i \text{ nach } v_l.$$

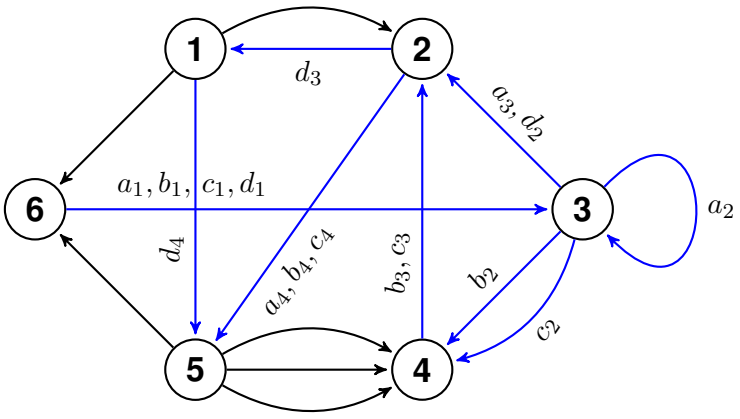
Somit gilt für jedes i, für jedes j und für jedes l:

$$a_{il}^{[k]} \cdot a_{lj}^{[1]} \text{ ist die Anzahl der Pfeilfolgen der Länge } k+1 \text{ von } v_i \text{ nach } v_j \text{ via } v_l,$$

und

$$a_{ij}^{[k+1]} = \sum_{l=1}^{n} a_{il}^{[k]} \cdot a_{lj}^{[1]} \text{ ist die Anzahl der Pfeilfolgen der Länge } k+1 \text{ von } v_i \text{ nach } v_j. \qquad \dashv$$

Obiges Beispiel mit A^4: Es gibt 4 verschiedene Pfeilfolgen a, b, c, d der Länge 4 vom Knoten 6 zum Knoten 5.



$$\begin{pmatrix} 5 & 7 & 4 & 7 & 5 & 1 \\ 3 & 6 & 3 & 7 & 4 & 2 \\ 4 & 9 & 3 & 14 & 7 & 7 \\ 1 & 3 & 2 & 3 & 1 & 1 \\ 1 & 6 & 1 & 11 & 4 & 6 \\ 3 & 4 & 1 & 5 & \mathbf{4} & 2 \end{pmatrix}$$

EULER'SCHE LINIEN & EULER'SCHE PFEILZÜGE

PROPOSITION 8.2. *Sei $G = (V, E_0, \ldots, E_k)$ ein endlicher, ungerichteter Graph. Dann gilt:*

(a) Ist $\sum_{i=0}^{k} |E_i| = m$, d. h.

$$\sum_{i=0}^{k} \left|\left\{\{x, y\} \subseteq V : \langle x, y\rangle \in E_i\right\}\right| = m,$$

so ist $\sum_{x\in V} \deg(x) = 2m$.

(b) Es gilt: $\left|\left\{x \in V : \deg(x)$ ist ungerade$\right\}\right|$ ist gerade.

Beweis. (a) In der Summe $\sum_{x\in V} \deg(x)$ wird jede Kante zweimal gezählt (auch bei Schlingen), denn jede Kante verbindet entweder zwei verschiedene Knoten oder sie ist eine Schlinge.

(b) Dies folgt direkt aus (a). ⊣

Enthält ein geschlossener Kantenzug eines Graphen G sämtliche Kanten von G, so heisst der Kantenzug **Euler'sche Linie** des Graphen G, und G heisst **Euler'scher Graph**.

PROPOSITION 8.3. *Ein endlicher, ungerichteter, zusammenhängender Graph G ist genau dann ein Euler'scher Graph, wenn jeder Knoten von G geraden Grad besitzt.*

Beweis. ($\Rightarrow$) Besitzt G eine Euler'sche Linie, so kann G in einem Zug gezeichnet werden. Somit ist beim Durchlaufen der Kanten jeder Knoten genauso oft Endpunkt wie Anfangspunkt einer Kante.

($\Leftarrow$) Hat jeder Knoten geraden Grad, so hat, weil der Graph zusammenhängend ist, jeder Knoten mindestens Grad 2.

Wir starten nun in irgend einem Knoten x_0. Da jeder Knoten geraden Grad hat, können wir von jedem von x_0 verschiedenen Knoten aus weiter gehen, und da der Graph endlich ist, müssen wir nach endlich vielen Schritten wieder zu x_0 kommen. Folglich gibt es einen geschlossenen Kantenzug beginnend in x_0.

Haben wir auf diesem Kantenzug alle Kanten besucht, so sind wir fertig. Andernfalls gibt es auf dem Kantenzug ein Knoten x_1, von dem unbesuchte Kanten ausgehen. Deren Anzahl ist notwendigerweise gerade.

Wir beginnen nun im Knoten x_1 und gehen so lange entlang von noch nicht durchlaufenen Kanten, bis wir wieder beim Knoten x_1 ankommen. Die beiden so erhaltenen Kantenzüge können wir zu einem einzigen Kantenzug zusammenfügen, der in x_0 beginnt und endet.

Haben wir nun auf diesem Kantenzug alle Kanten besucht, so sind wir fertig. Andernfalls machen wir weiter wie oben. Da nun der Graph zusammenhängend ist, wird schliesslich jede Kante besucht und der resultierende geschlossene Kantenzug ist eine Euler'sche Linie. ⊣

Eine Umformulierung der obigen Proposition gibt uns den folgenden Satz von Euler.

THEOREM 8.4 (Euler). *Sämtliche Kanten eines endlichen, ungerichteten, zusammenhängenden Graphen G können genau dann in einem geschlossenen Kantenzug durchlaufen werden, wenn jeder Knoten von G geraden Grad besitzt.*

Enthält ein offener Kantenzug eines Graphen G sämtliche Kanten von G, so heisst der Kantenzug **offene Euler'sche Linie** des Graphen G.

Wie oben können wir folgende Proposition beweisen:

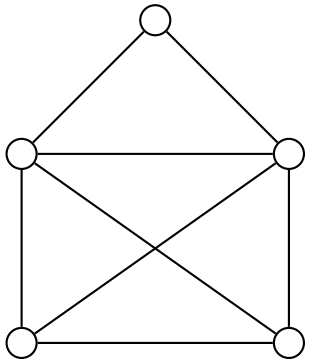
PROPOSITION 8.5. *Ein endlicher, ungerichteter, zusammenhängender Graph G besitzt genau dann eine offene Euler'sche Linie, wenn genau zwei Knoten von G ungeraden Grad besitzen.*

Analog zu (offene) Euler'sche Linie definieren wir **(offener) Euler'scher Pfeilzug**. Wie oben, können wir folgende Proposition beweisen.

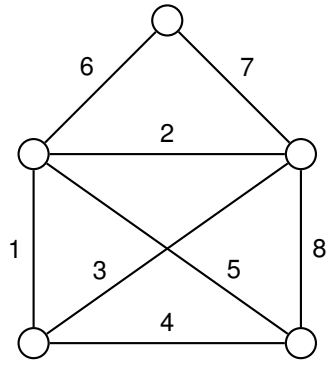
PROPOSITION 8.6. *Ein endlicher, gerichteter, zusammenhängender Graph* $G = (V, E_0, \ldots, E_k)$ *besitzt genau dann einen Euler'schen Pfeilzug, bzw. einen offenen Euler'schen Pfeilzug, wenn für alle* $x \in V$ *gilt* $\deg^+(x) = \deg^-(x)$*, bzw. für genau zwei Knoten* $x_1, x_2 \in V$ *gilt* $\deg^+(x_1) - \deg^-(x_1) = 1$ *und* $\deg^+(x_2) - \deg^-(x_2) = -1$.

Beispiele:

- Der folgende Graph kann in einem Zug gezeichnet werden.



Eine Möglichkeit ist zum Beispiel:



- **Dominoproblem**: Die Aufgabe ist, sämtliche Dominosteine eines Dominospiels, in dem die Augenzahlen der Steine von 0 bis 16 gehen und auch Doppelsteine mit zweimal derselben Augenzahl vorkommen, so zu einer fortlaufenden (unverzweigten) geschlossenen Kette aneinanderzureihen, dass die aneinander grenzenden Hälften zweier Steine stets dieselbe Augenzahl aufweisen.

  Um dieses Problem zu lösen betrachten den Graphen $G = (V, E)$ mit

$$\begin{aligned} V &:= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}, \\ E &:= \big\{\{a, b\} : a, b \in V\big\}. \end{aligned}$$

  G ist dann ein regulärer Graph vom Grad 18 (der K_{17} mit 16 Schlingen enthält). Da 18 gerade ist, besitzt G eine Euler'sche Linie, und weil jede Kante als ein Dominostein aufgefasst werden kann (die Nummern der Knoten, welche durch eine Kante verbundenen werden, bezeichnen die Augenzahlen auf dem zur Kante gehörenden Dominostein), entspricht jede Euler'sche Linie in G einer Lösung des Dominoproblems.

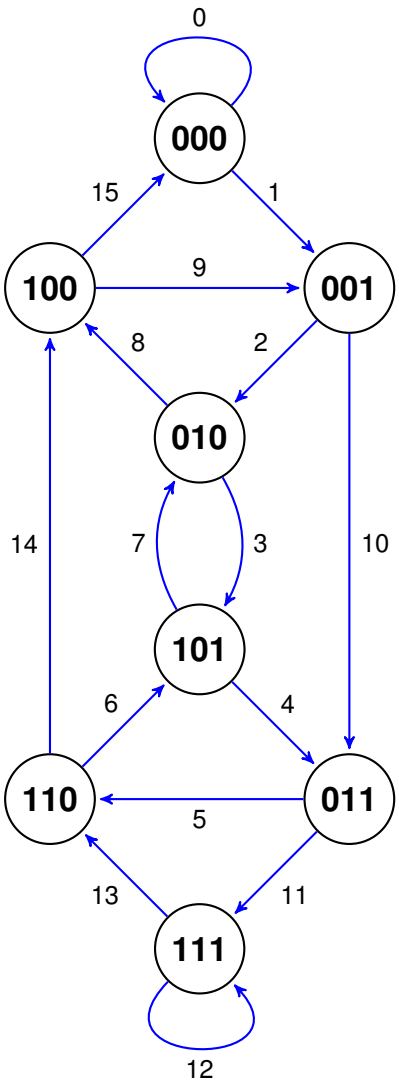
- Eine zyklische 0-1–Folge der Länge l heisst **De Bruijn–Folge**, wenn für ein $k \geq 1$ jedes binäre Wort der Länge k genau einmal als Teilwort (zyklisch) auftritt. Aus der Definition folgt, dass, falls eine solche Folge existiert, $l = 2^k$ ist.

  Wir zeigen nun, dass zu jedem k eine De Bruijn–Folge existiert: Für $k = 1$ ist die zyklische Folge 01 der Länge 2 eine De Bruijn–Folge. Sei nun $k \geq 2$. Wir betrachten den Graphen $G_k = (V, E)$ mit

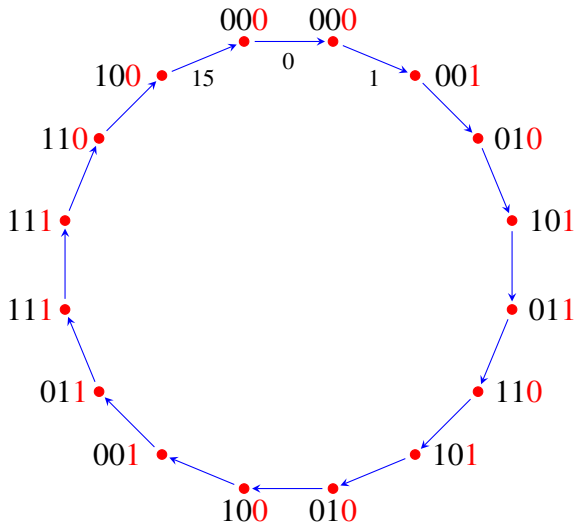
$$V := \{\langle b_1, \ldots, b_{k-1}\rangle : b_i \in \{0,1\}\},$$
$$E := \left\{\left\langle \langle b_1, \ldots, b_{k-1}\rangle, \langle b_2, \ldots, b_k\rangle \right\rangle : \langle b_1, \ldots, b_{k-1}\rangle, \langle b_2, \ldots, b_k\rangle \in V\right\}.$$

  Es ist $|V| = 2^{k-1}$ und $|E| = 2^k$. Weiter gilt für alle $x \in V$, $\deg^+(x) = \deg^-(x) = 2$, und somit enthält G_k einen Euler'schen Pfeilzug. Jeder Euler'sche Pfeilzug von G_k der Länge 2^k erzeugt in natürlicher Weise eine De Bruijn–Folge. Ein Beispiel für $k = 4$:

Euler'scher Pfeilzug



De Bruijn–Folge

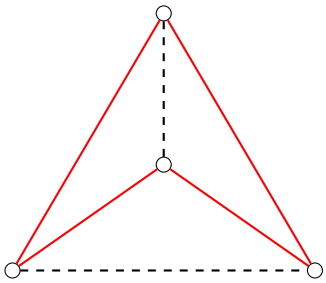


Bemerkung: Zu jedem $k \geq 1$ existieren bis auf zyklische Vertauschung genau $2^{2^{k-1}-k}$ De Bruijn–Folgen. Für $k = 1$ und $k = 2$ existieren somit nur die De Bruijn–Folgen 01 bzw. 0011, und für $k = 3$ existieren die beiden De Bruijn–Folgen 00010111 und 00011101.

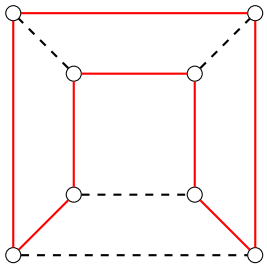
HAMILTON'SCHE GRAPHEN

Ein endlicher ungerichteter Graph $G = (V, E)$ ist ein **Hamilton'scher Graph**, bzw. G ist **hamiltonsch**, wenn G einen Kreis – einen sogenannten **Hamilton-Kreis** – besitzt der alle Knoten von G enthält. Mit anderen Worten, G ist hamiltonsch genau dann, wenn es in G einen Kreis gibt, der alle Knoten von G enthält. Es ist kein einfaches Kriterium bekannt, mit welchem entschieden werden kann, ob ein Graph hamiltonsch ist (im Gegensatz zum Beispiel zu Euler'schen Graphen).

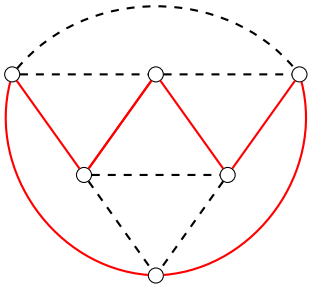
Beispiele für hamiltonsche Graphen sind die vollständigen Graphen K_n (für $n \geq 2$) sowie die Kantengraphen der fünf platonischen Körper:



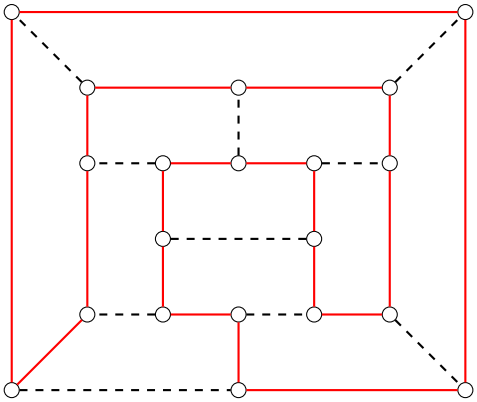
Tetraeder



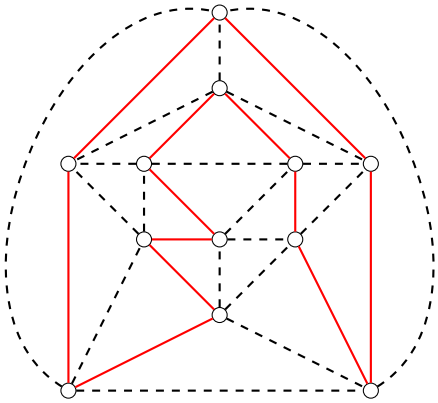
Würfel



Oktaeder



Dodekaeder



Ikosaeder

Ebenfalls hamiltonsch sind die Kantengraphen der k-dimensionalen Würfel (für $k \geq 2$). Dafür zeigen wir zuerst den folgenden Satz über *Gray-Codes*: Eine zyklische Folge, bestehend aus den 2^k verschiedenen binären Wörtern der Länge $k \geq 1$, heisset **Gray-Code**, falls sich je zwei aufeinander folgende Wörter in genau einer Stelle unterscheiden.

PROPOSITION 8.7. *Zu jedem $k \geq 1$ existiert ein Gray-Code.*

Beweis. Mit Induktion nach k. Für $k = 1$ ist die zyklische Folge $0, 1$ der einzige Gray-Code. Ist

$$(a_1, \ldots, a_{2^k})$$

ein Gray-Code für k, wobei jedes a_i ein binäres Wort der Länge k ist, so sind die 2^{k+1} binären Wörter

$$\big(0\,a_1, \ldots, 0\,a_{2^k}, 1\,a_{2^k}, 1\,a_{2^k-1}, \ldots, 1\,a_1\big)$$

der Länge $k + 1$ ein Gray-Code für $k + 1$. ⊣

KOROLLAR 8.8. *Der Kantengraph des k-dimensionalen Würfels (für $k \geq 2$) ist hamiltonsch.*

Beweis. Die binären Wörter der Länge k können als Ecken eines k-dimensionalen Würfels aufgefasst werden. Ein Gray-Code entspricht dann einem Hamilton-Kreis im Kantengraphen des k-dimensionalen Würfels. ⊣

Beispiel: Im Fall $k = 4$ gibt uns der Beweis von Proposition 8.7 den folgenden Gray-Code mit dem entsprechenden Hamilton-Kreis im Kantengraphen des 4-dimensionalen Würfels.

Gray-Code

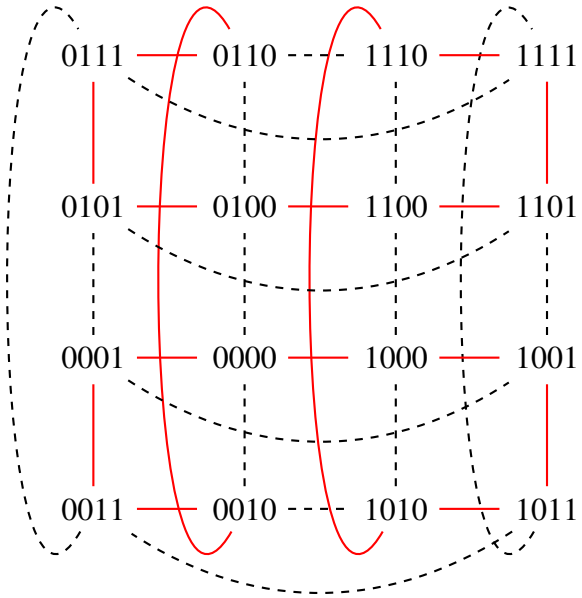
0 0 0 0
0 0 0 1
0 0 1 1
0 0 1 0

0 1 1 0
0 1 1 1
0 1 0 1
0 1 0 0

1 1 0 0
1 1 0 1
1 1 1 1
1 1 1 0

1 0 1 0
1 0 1 1
1 0 0 1
1 0 0 0

Hamilton-Kreis



9. Der Verallgemeinerte Euklid'sche Algorithmus

Vom ggT zu Kettenbrüchen

Euklid gibt im zehnten Buch seiner *Elemente* einen Algorithmus an, um von *zwei gegebenen kommensurablen Grössen ihr grösstes gemeinsames Mass zu finden*. In neuerer Terminologie heisst das, von zwei gegebenen (positiven) Zahlen ihren *grösster gemeinsamer Teiler* (ggT) zu finden, wobei vorausgesetzt ist, dass solch ein gemeinsamer Teiler existiert.

Der Algorithmus wird wie folgt beschrieben:

() Die beiden Grössen seien a_0 und a_1, wobei a_0 und a_1 beide positiv sein sollen.

(a) Ist $a_0 = a_1$, so ist $a_1 = \mathrm{ggT}(a_0, a_1)$ und wir sind fertig.

(b) Sonst existiert eine grösste *natürliche Zahl* b_0, so dass gilt:

$$a_0 \geq b_0 a_1$$

b_0 ist also die kleinste natürliche Zahl für die gilt: $a_0 < (b_0 + 1) \cdot a_1$.
Beachte: Im Falle $a_0 < a_1$ ist $b_0 = 0$.

(c) Ist $a_0 = b_0 a_1$, so ist wieder $a_1 = \mathrm{ggT}(a_0, a_1)$.

(d) Ist $a_0 > b_0 a_1$, so muss gelten $a_0 - b_0 a_1 < a_1$, sonst wäre $a_0 \geq (b_0 + 1) \cdot a_1$, was der Definition von b_0 im Schritt (b) widerspricht. Weil $a_0 > b_0 a_1$ ist $a_0 - b_0 a_1 > 0$. Definieren wir nun $a_2 := a_0 - b_0 a_1$, so ist $a_0 = b_0 a_1 + a_2$ und $0 < a_2 < a_1$.

(e) Nun gehen wir mit den Zahlen a_1 und a_2 zurück zum Schritt (b) und finden eine grösste natürliche Zahl b_1, so dass $a_1 \geq b_1 a_2$.

Betrachten wir die Zahlen a_0 und a_1 als Streckenlängen (wie dies Euklid getan hat), so ist es nicht schwierig einzusehen, dass dieser Algorithmus die grösste Strecke liefert, welche in beiden Strecken enthalten ist. Mit Zahlen ausgedrückt liefert der Algorithmus also den grössten gemeinsamen Teiler der Zahlen a_0 und a_1.

Ein Vorteil des Euklid'schen Algorithmus zur Berechnung des ggT's zweier Zahlen ist, dass wir nicht zuerst die Primfaktorzerlegung der beiden Zahlen bestimmen müssen, und wir somit auch von relativ grossen Zahlen den ggT berechnen können.

Beispiel: Für $a_0 = 986$ und $a_1 = 357$ erhalten wir:

$$\begin{aligned} 986 &= 2 \cdot 357 + 272 \\ 357 &= 1 \cdot 272 + 85 \\ 272 &= 3 \cdot 85 + 17 \\ 85 &= 5 \cdot 17 + 0 \end{aligned}$$

Damit ist $\mathrm{ggT}(986, 357) = 17$. Insbesondere erhalten wir $a_2 = 272$, $a_3 = 85$, $a_4 = 17$, $a_5 = 0$, und ferner ist $b_0 = 2$, $b_1 = 1$, $b_2 = 3$, $b_3 = 5$.

Von diesem Algorithmus ist es nun ein kleiner Schritt zu den sogenannten *Kettenbrüchen*: Ein **endlicher Kettenbruch** ist ein Bruch von der Form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots \cfrac{1}{b_{n-1} + \cfrac{1}{b_n}}}}}}$$

wobei $b_0, \ldots, b_n$ ganze Zahlen und höchstens mit Ausnahme von b_0 alle b_i positiv sind.

Wir stellen uns nun die Frage, ob sich jeder Bruch der Form $\frac{a_0}{a_1}$ als endlicher Kettenbruch schreiben lässt, und wenn ja, wie wir den entsprechenden Kettenbruch berechnen können. Um dies zu beantworten, gehen wir wie folgt vor:

Zuerst berechnen wir mit dem Euklid'schen Algorithmus den ggT von a_0 und a_1.

$$\begin{array}{rcll}
a_0 &=& b_0 \cdot a_1 + a_2 & \Rightarrow \quad \dfrac{a_0}{a_1} = b_0 + \dfrac{a_2}{a_1} = b_0 + \dfrac{1}{\frac{a_1}{a_2}} \\
a_1 &=& b_1 \cdot a_2 + a_3 & \Rightarrow \quad \dfrac{a_1}{a_2} = b_1 + \dfrac{a_3}{a_2} = b_1 + \dfrac{1}{\frac{a_2}{a_3}} \\
a_2 &=& b_2 \cdot a_3 + a_4 & \Rightarrow \quad \dfrac{a_2}{a_3} = b_2 + \dfrac{a_4}{a_3} = b_2 + \dfrac{1}{\frac{a_3}{a_4}} \\
&\vdots & & \qquad\quad \vdots \\
a_n &=& b_n \cdot a_{n+1} + 0 & \Rightarrow \quad \dfrac{a_n}{a_{n+1}} = b_n
\end{array}$$

Es gilt also

$$\frac{a_0}{a_1} = b_0 + \frac{1}{\frac{a_1}{a_2}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\frac{a_2}{a_3}}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\frac{a_3}{a_4}}}}$$

und allgemein erhalten wir

$$\frac{a_0}{a_1} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots \cfrac{1}{b_{n-1} + \cfrac{1}{b_n}}}}}}$$

Dieser letzte Ausdruck ist nun ein endlicher Kettenbruch, den wir der besseren Lesbarkeit wegen mit $[b_0, b_1, \ldots, b_n]$ bezeichnen.

Da der Bruch $\frac{a_0}{a_1}$ beliebig war, können wir also *jeden* Bruch (d. h. jede rationale Zahl) als endlichen Kettenbruch schreiben. Es gilt natürlich auch das Umgekehrte, nämlich dass jeder endliche Kettenbruch einer rationalen Zahl entspricht, denn jeder endliche Kettenbruch kann in einen normalen Bruch umgewandelt werden.

Zum Beipiel haben wir $\frac{986}{357} = [2, 1, 3, 5]$, denn:

$$\frac{986}{357} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5}}}$$

Verwandeln wir den Kettenbruch $[2, 1, 3, 5]$ in einen normalen Bruch, so erhalten wir nicht $\frac{986}{357}$, sondern $\frac{58}{21}$, also einen gekürzten Bruch (es gilt $\frac{58}{21} = \frac{58 \cdot 17}{21 \cdot 17} = \frac{986}{357}$). Aus Proposition 9.1 und Lemma 9.2 wird folgen, dass dies immer der Fall ist, denn verwandeln wir einen Kettenbruch in einen normalen Bruch, so ist dieser Bruch *immer* gekürzt.

Wir wollen nun untersuchen, was passiert, wenn die Grössen (bzw. reellen Zahlen) a_0 und a_1 keinen gemeinsamen Teiler haben. Dafür setzen wir zum Beispiel $a_0 = \sqrt{2}$ und $a_1 = 1$:

$$\begin{array}{ccccccc}
 & & \frac{\sqrt{2}}{1} & = & 1 & + & (\sqrt{2} - 1) \\
\frac{1}{\sqrt{2}-1} & = & \frac{\sqrt{2}+1}{1} & = & 2 & + & (\sqrt{2} - 1) \\
\frac{1}{\sqrt{2}-1} & = & \frac{\sqrt{2}+1}{1} & = & 2 & + & (\sqrt{2} - 1) \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

Der Euklid'sche Algorithmus angewandt auf $a_0 = \sqrt{2}$ und $a_1 = 1$ bricht nie ab und liefert uns somit unendlich viele positive natürliche Zahlen b_n. Das heißt, dass der Kettenbruch von $\frac{a_0}{a_1} = \sqrt{2}$ *unendlich* ist. In unserem Fall erhalten wir den Kettenbruch

$$[1, 2, 2, 2, 2, \ldots] = [1, \overline{2}\,].$$

Ein **unendlicher Kettenbruch** ist ein nicht abbrechender Bruch von der Form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ldots}}}$$

wobei $b_0, b_1, b_2 \ldots$ ganze Zahlen und höchstens mit Ausnahme von b_0 alle b_i positiv sind.

Ist $\xi \in \mathbb{R}$ eine beliebige, positive, irrationale Zahl, so können wir ξ immer als unendlichen Kettenbruch schreiben. Dazu definieren wir für positive reelle Zahlen α,

$$\lfloor \alpha \rfloor := \max\{n \in \mathbb{N} : n \leq \alpha\}.$$

Dann gilt:

$$\begin{array}{ccccccl}
\xi & = & b_0 & + & r_1 & & \text{mit } b_0 := \lfloor \xi \rfloor \text{ und } r_1 := \xi - b_0, \text{ wobei } 0 < r_1 < 1 \text{ bzw. } \frac{1}{r_1} > 1 \\
\frac{1}{r_1} & = & b_1 & + & r_2 & & \text{mit } b_1 := \lfloor \frac{1}{r_1} \rfloor \text{ und } r_2 := \frac{1}{r_1} - b_1, \text{ wobei } 0 < r_2 < 1 \text{ bzw. } \frac{1}{r_2} > 1 \\
\frac{1}{r_2} & = & b_2 & + & r_3 & & \text{mit } b_2 := \lfloor \frac{1}{r_2} \rfloor \text{ und } r_3 := \frac{1}{r_2} - b_2, \text{ wobei } 0 < r_3 < 1 \text{ bzw. } \frac{1}{r_3} > 1 \\
\vdots & & \vdots & & \vdots & &
\end{array}$$

und wir erhalten den Kettenbruch $[b_0, b_1, b_2, \ldots]$.

Es stellt sich nun die Frage, wie der Kettenbruch $[b_0, b_1, b_2, \ldots]$ mit ξ zusammenhängt. Ein natürlicher Ansatz ist, den unendlichen Kettenbruch jeweils nach endlich vielen Schritten abzubrechen und die entsprechenden rationalen Zahlen zu berechnen. Wie wir zeigen werden, nähern sich diese rationalen Zahlen der irrationalen Zahl ξ an, deshalb werden sie *Näherungsbrüche* genannt. Zum Beispiel erhalten wir für den unendlichen Kettenbruch $[1, \overline{2}]$ die folgenden Näherungsbrüche $\frac{P_n}{Q_n}$:

$$\frac{P_0}{Q_0} = \frac{1}{1}, \quad \frac{P_1}{Q_1} = \frac{3}{2}, \quad \frac{P_2}{Q_2} = \frac{7}{5}, \quad \frac{P_3}{Q_3} = \frac{17}{12}, \quad \frac{P_4}{Q_4} = \frac{41}{29}, \ldots$$

Näherungsbrüche sind immer gekürzte Brüche welche, wie wir sehen werden, relativ schnell konvergieren. Wir können also zum Beispiel $\sqrt{2}$ beliebig genau berechnen. Was uns noch fehlt, ist ein einfacher Algorithmus, welcher uns erlaubt, die Näherungsbrüche ohne grossen Aufwand zu berechnen; dies liefert die folgende rekursive Formel:

$$\begin{aligned} P_{-2} &:= 0, \qquad P_{-1} := 1, \qquad P_n := b_n P_{n-1} + P_{n-2} \\ Q_{-2} &:= 1, \qquad Q_{-1} := 0, \qquad Q_n := b_n Q_{n-1} + Q_{n-2} \end{aligned}$$

Graphisch dargestellt erhalten wir für den Kettenbruch $[1, \overline{2}]$ folgendes Schema:

n	*-2*	*-1*	*0*	*1*	*2*	*3*	*4*	...
b_n			1	2	2	2	2	...
P_n	**0**	**1**	1	3	7	17	41	...
Q_n	**1**	**0**	1	2	5	12	29	...

Jede Zahl der dritten Zeile entsteht, indem man die darüberstehende mit der vorausgehenden Zahl der dritten Zeile multipliziert und die nächstvorausgehende addiert; analog für die vierte Zeile.

Diesen Algorithmus zur Berechnung von Näherungsbrüchen nennen wir **verallgemeinerter Euklid'scher Algorithmus**, abgekürzt **vEA**. Wir zeigen nun, dass der vEA korrekt ist, bzw. dass die Brüche $\frac{P_n}{Q_n}$ tatsächlich Näherungsbrüche sind.

PROPOSITION 9.1. *Sei $[b_0, b_1, \ldots]$ ein unendlicher Kettenbruch. Dann gilt für alle natürlichen Zahlen n:*

$$[b_0, \ldots, b_n] = \frac{P_n}{Q_n}$$

wobei die Zahlen P_n und Q_n mit dem vEA *berechnet werden.*

Beweis. Den Beweis führen wir mit Induktion nach n.

$n = 0$: Es gilt $P_0 = b_0$ und $Q_0 = 1$, also ist $\frac{P_0}{Q_0} = b_0 = [b_0]$.

Annahme: $[b_0, \ldots, b_n] = \frac{P_n}{Q_n}$ für ein $n \in \mathbb{N}$.

Wir müssen nun zeigen, dass aus der Annahme folgt: $[b_0, \ldots, b_n, b_{n+1}] = \frac{P_{n+1}}{Q_{n+1}}$. So, wie die Kettenbrüche aufgebaut sind, gilt:

$$[b_0, \ldots, b_n, b_{n+1}] = [b_0, \ldots, b_n + \frac{1}{b_{n+1}}]$$

Setzen wir $b'_n := b_n + \frac{1}{b_{n+1}}$, so erhalten wir

$$[b_0, \ldots, b_{n-1}, b_n + \frac{1}{b_{n+1}}] = [b_0, \ldots, b_{n-1}, b'_n]\,.$$

Wenn wir nun mit dem Algorithmus den Näherungsbruch $\frac{P'_n}{Q'_n}$ von $[b_0, \ldots, b'_n]$ berechnen, so erhalten wir $P'_n = b'_n P_{n-1} + P_{n-2}$, also

$$P'_n = \Big(b_n + \frac{1}{b_{n+1}}\Big) P_{n-1} + P_{n-2} = \quad \cdots \quad = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}}\,,$$

und entsprechend

$$Q'_n = \frac{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}}{b_{n+1}}\,.$$

Somit haben wir:

$$[b_0, \ldots, b_{n-1}, b'_n] = \frac{P'_n}{Q'_n} = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}}$$

Da nun

$$[b_0, \ldots, b_{n-1}, b'_n] = [b_0, \ldots, b_{n-1}, b_n + \frac{1}{b_{n+1}}] = [b_0, \ldots, b_{n-1}, b_n, b_{n+1}]$$

müssen wir nur noch zeigen, dass die Gleichung $\frac{P'_n}{Q'_n} = \frac{P_{n+1}}{Q_{n+1}}$ gilt. Dazu schreiben wir P_{n+1} und Q_{n+1} etwas um: Mit dem Algorithmus erhalten wir $P_{n+1} = b_{n+1}P_n + P_{n-1}$, und wenn wir P_n durch $b_n P_{n-1} + P_{n-2}$ ersetzen, erhalten wir

$$P_{n+1} = b_{n+1}(b_n P_{n-1} + P_{n-2}) + P_{n-1} = b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}\,,$$

und entsprechend

$$Q_{n+1} = b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}\,.$$

Somit ist $\frac{P'_n}{Q'_n} = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}} = \frac{P_{n+1}}{Q_{n+1}}$ und der Algorithmus ist korrekt. ⊣

Bemerkung: Als Folgerung aus Proposition 9.1 erhalten wir, dass wenn $[b_0, \ldots, b_n]$ der endliche Kettenbruch von $\frac{a}{b} \in \mathbb{Q}$ ist, immer $\frac{P_n}{Q_n} = \frac{a}{b}$ gilt.

Das folgende Lemma ist wichtig, um multiplikativ Inverse in speziellen Ringen, sogenannten *euklidischen Ringen*, zu berechnen.

LEMMA 9.2. *Sind $\frac{P_n}{Q_n}$ (für $n \in \mathbb{N}$) die zum Kettenbruch $[b_0, b_1, b_2, \ldots]$ gehörenden Näherungsbrüche, so gilt für alle $n \geq -1$:*

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$$

Beweis. Für den Beweis verwenden wir Induktion über n.
Für $n = -1$ ist $P_n = Q_{n-1} = 1$ und $P_{n-1} = Q_n = 0$, also

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}.$$

Gilt $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$ für ein $n \geq -1$, so ist

$$P_{n+1}Q_n - P_n Q_{n+1} = (b_{n+1}P_n + P_{n-1})Q_n - P_n(b_{n+1}Q_n + Q_{n-1}) = \\ P_{n-1}Q_n - P_n Q_{n-1} = -(-1)^{n-1} = (-1)^n,$$

womit die Behauptung bewiesen ist. ⊣

Bemerkung: Als Folgerung aus Lemma 9.2 erhalten wir, dass die Näherungsbrüche $\frac{P_n}{Q_n}$ immer gekürzt sind. Denn wäre $\mathrm{ggT}(P_n, Q_n) = d > 1$, so hätten wir $d \mid (qP_n - p\,Q_n)$ (für alle $p, q \in \mathbb{Z}$), und somit $|qP_n - p\,Q_n| \neq 1$.

EINDEUTIGKEIT DER PRIMFAKTORZERLEGUNG

Als Anwendung des vEA zeigen wir die Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen $n \geq 2$. Dazu beweisen wir zuerst folgendes Hilfsresultat:

LEMMA 9.3. *Seien $a, b, c \in \mathbb{N}$ positive Zahlen mit $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt $a \mid c$.*

Beweis. Sei $[b_0, \ldots, b_n]$ der Kettenbruch von $\frac{a}{b}$. Ist $n = 0$, so ist $b = 1$ und $a \mid c$. Ist $n > 1$, so ist, weil $\mathrm{ggT}(a, b) = 1$, $P_n = a$ und $Q_n = b$, und mit Lemma 9.2 gilt $a \cdot Q_{n-1} - b \cdot P_{n-1} = (-1)^{n-1}$. Somit existieren $k, l \in \mathbb{Z}$ mit $|k| = Q_{n-1}$ und $|l| = P_{n-1}$ sodass gilt $ak + bl = 1$. Weil $a \mid bc$ existiert ein $s \in \mathbb{N}$ mit $as = bc$. Nun ist

$$c = c \cdot 1 = c \cdot (ak + bl) = ack + bcl = ack + asl = a \cdot \underbrace{(ck + sl)}_{=:t} = a \cdot t$$

und wir erhalten $a \mid c$. ⊣

Eine Zahl $p \in \mathbb{N}$, $p > 1$, ist eine **Primzahl**, wenn aus $n \mid p$ folgt $n = 1$ oder $n = p$. Mit Induktion über $m \in \mathbb{N}$ lässt sich einfach zeigen, dass sich jede Zahl $m \in \mathbb{N}$ mit $m > 1$ als Produkt von Primzahlen schreiben lässt. Der folgende Satz besagt, dass dieses Produkt (bis auf die Reihenfolge der Faktoren) eindeutig ist.

THEOREM 9.4. *Für positive Zahlen $n, m \in \mathbb{N}$ seien*

$$a = \prod_{i \in n} p_i \quad \text{und} \quad b = \prod_{j \in m} q_j$$

wobei die p_i und q_j Primzahlen sind. Ist $a = b$, so ist $n = m$ und es existiert eine Bijektion $\pi : n \to m$ mit $p_i = q_{\pi(i)}$ für alle $i \in n$.

Beweis. Beweis mit Induktion nach n: Ist $n = 1$, so ist $a = p_0$ und $b = q_0$ und aus $a = b$ folgt $p_0 = q_0$. Sei $n > 1$ und sei der Satz bewiesen für $n - 1$. Für $n > 1$ gilt $p_0 \mid a$ und aus $a = b$ folgt somit $p_0 \mid b$ also

$$p_0 \mid q_0 \cdot \prod_{j \in m-1} q_{j+1}.$$

Gilt $p_0 \mid q_0$, so erhalten wir, weil p_0 und q_0 prim sind, $p_0 = q_0$ und wir können die Induktionsvoraussetzung anwenden auf

$$\prod_{i \in n-1} p_{i+1} = \prod_{j \in m-1} q_{j+1}.$$

Gilt $p_0 \nmid q_0$, so erhalten wir mit Lemma 9.3

$$p_0 \mid q_1 \cdot \prod_{j \in m \setminus 2} q_j.$$

Gilt $p_0 \mid q_1$, so ist $p_0 = q_1$, andernfalls wenden wir wieder Lemma 9.3 an. So fortgefahren, finden wir schliesslich ein $j_0 \in m$ für das gilt $p_0 = q_{j_0}$ und wir können die Induktionsvoraussetzung anwenden auf

$$\prod_{i \in n-1} p_{i+1} = \prod_{j \in m \setminus \{j_0\}} q_j.$$

⊣

Als Folgerung aus Theorem 9.4 erhalten wir nun leicht

KOROLLAR 9.5. *Jede natürliche Zahl $n \geq 2$ lässt sich, bis auf Vertauschung der Faktoren, eindeutig als Produkt von Primzahlen schreiben.*

10. MODULORECHNEN

In diesem Kapitel sind Ringe immer kommutative Ringe mit 1. Erinnerung: Ein kommutativer Ring mit 1 ist ein Modell der Ringaxiome $\mathsf{RT}_0 - \mathsf{RT}_8$, also eine $\mathscr{L}_{\mathsf{RT}}$-Struktur mit Bereich R, wobei $\mathscr{L}_{\mathsf{RT}} = \{0, 1, +, \cdot\}$. Wie üblich identifizieren wir einen Ring $(R, 0, 1, +, \cdot)$ mit seinem Bereich R, oder wir schreiben $(R, +, \cdot)$ um auch die binären Operationen hervorzuheben.

IDEALE

Sei $(R, 0, 1, +, \cdot)$ ein kommutativer Ring. Eine Menge $I \subseteq R$ ist ein **Ideal** in R, falls die folgenden Bedingungen erfüllt sind:

(I_0) $I \neq \emptyset$
(I_1) $\forall a, b \in I\,(a + b \in I)$
(I_2) $\forall x \in R \forall a \in I\,(x \cdot a \in I)$

Da mit $1 \in R$ auch $-1 \in R$ ist, folgt aus (I_2), dass mit jedem $a \in I$ auch $(-1) \cdot a = -a$ in I ist. Mit (I_0) und (I_1) ist das Ideal also eine additive Untergruppe von R, d. h. eine Untergruppe der abelschen Gruppe $(R, 0, +)$. Ist $1 \in I$, so ist $I = R$ (also ein Ring), ist aber $1 \notin I$ und $I \neq \{0\}$, so ist I kein Unterring von R (nicht-triviale Unterringe von R müssen die 1 enthalten). Beachte, dass $\{0\}$ ein Ring mit 1 ist – in $\{0\}$ gilt $0 = 1$.

Jeder Ring R besitzt die beiden *trivialen* Ideale R und $\{0\}$; das Ideal $\{0\}$ heisst **Nullideal**. Wie wir später sehen werden, sind Körper dadurch charakterisiert, dass sie nur die trivialen Ideale enthalten.

Beispiele: (a) Für $m \in \mathbb{Z}$ sei

$$m\mathbb{Z} := \{x \cdot m : x \in \mathbb{Z}\}.$$

Dann ist $m\mathbb{Z}$ ein Ideal im Ring $(\mathbb{Z}, 0, 1, +, \cdot)$. Denn mit $xm \in m\mathbb{Z}$ ist auch $y \cdot (xm) = (yx) \cdot m \in I$, und mit $xm, ym \in I$ ist auch $xm + ym = (x + y)m \in I$.

(b) Sei $\mathbb{Z}[X]$ der Ring der Polynome mit Koeffizienten in $\mathbb{Z}$ (siehe Aufgabe 11), und sei $f \in \mathbb{Z}[X]$, zum Beispiel $f = 1 - X^2 + 7X^3$. Dann ist

$$(f) := \big\{g \cdot f : g \in \mathbb{Z}[X]\big\}$$

ein Ideal in $\mathbb{Z}[X]$: Nach Definition sind (I_0) und (I_2) erfüllt, und weil $\mathbb{Z} \subseteq \mathbb{Z}[X]$, ist mit ($\mathrm{I}_2$) auch ($\mathrm{I}_1$) erfüllt.

Für Beispiel (a) gilt auch eine Art Umkehrung.

PROPOSITION 10.1. *Ist $I \subseteq \mathbb{Z}$ ein Ideal, dann existiert ein $m \in \mathbb{Z}$, sodass gilt:*

$$I = m\mathbb{Z}$$

Beweis. Ist I das Nullideal, so ist $I = 0\mathbb{Z}$ und wir sind fertig. Ist $I \neq \{0\}$, so enthält I mit (I_2) positive Zahlen. Sei

$$m := \min\big\{n \in \mathbb{N} \setminus \{0\} : n \in I\big\}.$$

Wir zeigen $I = m\mathbb{Z}$. Für einen Widerspruch nehmen wir an, dass ein $a \in I$ existiert mit $a \notin m\mathbb{Z}$. Wir dürfen annehmen, dass $a > 0$, denn mit $a \in I$ ist immer auch $-a \in I$. Nach Definition von m ist $m < a$. Sei $d := \mathrm{ggT}(a, m)$. Dann ist $1 \leq d < m$, weil $a \notin m\mathbb{Z}$. Mit dem vEA finden wir $k, l \in \mathbb{Z}$ mit $ka + lm = d$. Aus (I_2) folgt, dass sowohl ka wie auch lm in I sind, und mit (I_1) ist somit auch $ka + lm$, also $d < m$ in I, was aber der Definition von m widerspricht. ⊣

FAKTORRINGE

Sei R ein kommutativer Ring und sei $I \subseteq R$ ein Ideal, zum Beispiel $R = \mathbb{Z}$ und $I = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Für $x \in R$ definieren wir die sogenannte **Restklasse** von x durch

$$\bar{x} := x + I = \{x + a : a \in I\}.$$

Weiter definieren wir auf R die binäre Relation "$\sim$" durch:

$$x \sim y \iff \bar{x} = \bar{y}$$

Weil "$=$" eine Äquivalenzrelation ist, ist auch "$\sim$" eine Äquivalenzrelation. Gilt $x \sim y$, so sagen wir "x ist kongruent y modulo I" und schreiben

$$x \equiv y \pmod{I}.$$

Sei $R/I := \{\bar{x} : x \in R\}$ (gesprochen "R *modulo* I") die Menge der Äquivalenzklassen. Auf R/I definieren wir die beiden binären Operationen $\oplus$ und $\otimes$ auf Repräsentanten von Äquivalenzklassen wie folgt:

$$\bar{x} \oplus \bar{y} := \overline{x + y} \qquad \text{und} \qquad \bar{x} \otimes \bar{y} := \overline{x \cdot y}$$

Das folgenden Lemma zeigt, dass die Operationen $\oplus$ und $\otimes$ wohldefiniert (d. h. unabhängig von der Wahl der Repräsentanten) sind.

LEMMA 10.2. *Seien $x_0, x_1, y_0, y_1 \in R$, sodass gilt $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$. Dann gilt:*

$$\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1 \qquad \textit{und} \qquad \bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$$

Beweis. Beachte, dass für alle $x, y \in R$ gilt:

$$x \in I \Rightarrow (x + I) = I \qquad \text{und} \qquad x + I = y + I \iff x - y \in I$$

$\oplus$ ist wohldefiniert: Seien nun $x_0, x_1, y_0, y_1 \in R$, sodass gilt $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$. Es gilt nun:

$$\begin{aligned}\overline{x_0 + y_0} = (x_0 + y_0) + I = (x_0 + I) + (y_0 + I) = \\ \big(x_0 + \big(\underbrace{(x_1 - x_0)}_{\in I} + I\big)\big) + \big(y_0 + \big(\underbrace{(y_1 - y_0)}_{\in I} + I\big)\big) = \\ (x_1 + I) + (y_1 + I) = (x_1 + y_1) + I = \overline{x_1 + y_1}\end{aligned}$$

Somit ist $\overline{x_0 + y_0} = \overline{x_1 + y_1}$, d. h. $\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1$.

$\otimes$ ist wohldefiniert: Weil nach Voraussetzung $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$, gilt $x_0 - x_1 \in I$ und $y_0 - y_1 \in I$. Somit haben wir

$$\left.\begin{aligned} x_0 \cdot (y_0 - y_1) = \quad x_0 y_0 - x_0 y_1 \in I \\ y_1 \cdot (x_0 - x_1) = -x_1 y_1 + x_0 y_1 \in I \end{aligned}\right\} \Rightarrow (x_0 y_0 - x_1 y_1) \in I,$$

woraus folgt $x_0 y_0 + I = x_1 y_1 + I$, d. h. $\overline{x_0 \cdot y_0} = \overline{x_1 \cdot y_1}$. Somit ist $\bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$. ⊣

Mit Lemma 10.2 können wir die Ringstruktur vom Ring R auf R/I übertragen und erhalten, dass $\big(R/I, \bar{0}, \bar{1}, \oplus, \otimes\big)$ ein kommutativer Ring ist (den Beweis lassen wir weg). Der Ring R/I ist ein sogenannter **Faktorring**.

DIE RINGE $\mathbb{Z}_m$

In diesem Abschnitt betrachten wir den Faktorring $\mathbb{Z}/I$, wobei $I \subseteq \mathbb{Z}$ ein Ideal ist, d. h. $I = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Die Elemente von $\mathbb{Z}/I$ bezeichnen wir wieder mit $\bar{x}, \bar{y}, \ldots$, aber anstelle von "$\oplus$" und "$\otimes$" schreiben wir "$+$" bzw. "$\cdot$", wobei wir den Multiplikationspunkt wie üblich auch manchmal weglassen. Da Ideale $I \subseteq \mathbb{Z}$ immer von der Form $I = m\mathbb{Z}$ sind für ein $m \in \mathbb{Z}$, schreiben wir $\mathbb{Z}_m$ anstelle von $\mathbb{Z}/m\mathbb{Z}$.

Für $m \geq 1$ ist somit $\mathbb{Z}_m$ ein Ring mit den m Elementen $\bar{0}, \ldots, \overline{m-1}$, insbesondere ist $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z}$ der Nullring $\{\bar{0}\}$. Weiter ist die Struktur $(\mathbb{Z}_m, \bar{0}, +)$ eine Gruppe welche durch $\bar{1}$ erzeugt wird, d. h. jedes Element $a \in \mathbb{Z}_m$ ist von der Form $a = \bar{1} + \ldots + \bar{1}$. Andererseits ist für $m \geq 2$, $(\mathbb{Z}_m \setminus \{\bar{0}\}, \bar{1}, \cdot)$ im Allgemeinen keine Gruppe (z. B. hat $\bar{6}$ in $\mathbb{Z}_{15}$ kein multiplikativ Inverses). Mit der folgenden Proposition lassen sich die Elemente von $\mathbb{Z}_m$ bestimmen, welche ein multiplikativ Inverses haben.

PROPOSITION 10.3. *Sei $m \geq 2$ und sei $\bar{a} \in \mathbb{Z}_m$. Dann existiert genau dann ein $\bar{b} \in \mathbb{Z}_m$ mit $\bar{a} \cdot \bar{b} = \bar{1}$, wenn $\mathrm{ggT}(a, m) = 1$.*

Beweis. Sei $d := \mathrm{ggT}(a, m)$. Existiert ein $\bar{b} \in \mathbb{Z}_m$ mit $\bar{a} \cdot \bar{b} = \bar{1}$, so erhalten wir $ab = ml + 1$ für ein $l \in \mathbb{Z}$. Aus $d \mid a$ und $d \mid m$ folgt dann $d \mid (ab - ml)$, d. h. $d \mid 1$. Somit muss $d = 1$ sein.

Ist nun $\mathrm{ggT}(a, m) = 1$, so finden wir mit dem vEA Zahlen $b, l \in \mathbb{Z}$ mit $ab + ml = 1$. Das heisst $ab \equiv 1 \pmod{m}$, woraus folgt $\overline{ab} = \bar{a} \cdot \bar{b} = \bar{1}$. ⊣

Wenn wir nur die Elemente aus $\mathbb{Z}_m \setminus \{\bar{0}\}$ betrachten, welche ein multiplikativ Inverses haben, so bilden diese Elemente bezüglich der Multiplikation eine Gruppe, die sogenannte **Einheitengruppe** des Rings $\mathbb{Z}_m$, welche wir mit $\mathbb{Z}_m^*$ bezeichnen. Um zu sehen, dass $\mathbb{Z}_m^*$ eine multiplikative Gruppe ist, genügt es zu zeigen, dass mit $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ auch $\bar{a}\bar{b}$ in $\mathbb{Z}_m^*$ ist. Das folgt aber direkt aus den Eigenschaften des ggT, denn wenn $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ggT}(b, m) = 1$, dann ist auch $\mathrm{ggT}(ab, m) = 1$. Die Ordnung der Gruppe $\mathbb{Z}_m^*$ wird mit $\varphi(m)$ bezeichnet, also $\varphi(m) := |\mathbb{Z}_m^*|$ und φ heisst **Euler'sche φ-Funktion**. Es gilt der folgende Satz (den wir nicht beweisen):

EULER'SCHER SATZ. *Für $m \geq 2$ und $\mathrm{ggT}(a, m) = 1$ gilt:*

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \textit{bzw.} \quad m \mid a^{\varphi(m)} - 1$$

Als Spezialfall des Euler'schen Satzes erhalten wir für Primzahlen m den folgenden Satz (beachte, dass für Primzahlen m gilt $\varphi(m) = m - 1$):

KLEINER SATZ VON FERMAT. *Für p prim und $\mathrm{ggT}(a, p) = 1$ gilt:*

$$a^{p-1} \equiv 1 \pmod{p} \quad \textit{bzw.} \quad p \mid a^p - a$$

Beweis. Sei p prim und $\mathrm{ggT}(a, p) = 1$. Wir betrachten die Punkte eines regelmässigen p-Ecks, welche wir mit a verschiedenen Farben färben. Es existieren a^p verschiedene Färbungen, wobei es neben den a einfarbigen Färbungen $a^p - a$ Färbungen gibt, welche mindestens zwei Farben haben. Da p prim ist, kann keine Färbung, die mindestens zwei Farben hat, durch eine Drehung um $k\frac{2\pi}{p}$ mit $k \in \{1, \ldots, p-1\}$ in sich übergeführt werden. Zwei Färbungen, die mindestens zwei Farben haben, seien äquivalent, wenn sie durch eine Drehung um $k\frac{2\pi}{p}$ für ein $k \in \{0, \ldots, p-1\}$ ineinander übergeführt werden können. Dann hat jede Äquivalenzklasse genau p Element und somit lässt sich $a^p - a$ durch p teilen. ⊣

DIE KÖRPER $\mathbb{F}_p$

Für $m \geq 2$ ist der Ring $(\mathbb{Z}_m, \bar{0}, \bar{1}, +, \cdot)$ genau dann ein Körper, wenn jedes Element aus $\mathbb{Z}_m \setminus \{\bar{0}\}$ ein multiplikativ Inverses besitzt. Mit Proposition 10.3 ist dies genau dann der Fall, wenn für jedes $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$ gilt $\mathrm{ggT}(a, m) = 1$. Das ist genau dann erfüllt, wenn m eine Primzahl ist: Denn ist m eine Primzahl und $1 \leq a < m$, so ist $\mathrm{ggT}(a, m) = 1$. Ist andererseits m keine Primzahl, so existiert ein $1 < a < m$ mit $a \mid m$. Das heisst $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$, $\mathrm{ggT}(a, m) > 1$ und $\bar{a}$ hat kein multiplikativ Inverses.

Der Ring $\mathbb{Z}_m$ ist also genau dann ein Körper (engl. *field*), wenn m eine Primzahl ist. Die Körper $\mathbb{Z}_p$ für p prim werden mit $\mathbb{F}_p$ bezeichnet.

Etwas allgemeiner erhalten wir für Ringe R, dass R/I genau dann ein Körper ist, wenn das Ideal I maximal ist, wobei ein Ideal I ein **maximales Ideal** ist, wenn $I \neq R$ und I in keinem echten Ideal $J \subsetneq R$ echt enthalten ist.

PROPOSITION 10.4. *Sei R ein Ring und sei $I \neq R$ ein Ideal von R. Dann ist R/I genau dann ein Körper, wenn I ein maximales Ideal ist.*

Beweis. ($\Leftarrow$): Wir zeigen diese Richtung mit Kontraposition. Sei $I \subsetneq R$ ein Ideal und sei R/I kein Körper. Dann existiert ein $a_0 \in R \setminus I$ (d. h. $\bar{a}_0 \neq \bar{0}$), sodass für alle $x \in R$ gilt $\bar{a}_0 \cdot \bar{x} \neq \bar{1}$. Sei

$$J_0 := \{x \cdot a_0 + y \cdot b : x, y \in R \wedge b \in I\}.$$

Dann ist $J_0 \subseteq R$ ein Ideal mit $a_0 \in J_0$ und $1 \notin J_0$. Um $1 \notin J_0$ zu sehen, beachte, dass aus $x \cdot a_0 + y \cdot b = 1$ mit $b \in I$ (d. h. $\overline{y \cdot b} = \bar{0}$), $\bar{x} \cdot \bar{a}_0 = \bar{1}$ folgt, im Widerspruch zu unserer Annahme. Es gilt somit

$$I \underset{a_0 \notin I}{\subsetneq} J_0 \underset{1 \notin J_0}{\subsetneq} R$$

und I ist nicht maximal.

($\Rightarrow$): Sei R/I ein Körper und sei $I \subsetneq J \subseteq R$. Weiter sei $a_0 \in J \setminus I$. Weil R/I ein Körper ist, existiert ein $\bar{x}$ mit $\bar{a}_0 \cdot \bar{x} = \bar{1}$. Das heisst, $a_0 \cdot x = 1 + b$ für ein $b \in I$. Weil $a_0 \in J$, ist mit (I_2) auch $a_0 \cdot x \in J$, und weil $I \subseteq J$, ist $b \in J$. Somit ist mit (I_1) auch $a_0 \cdot x - b = 1 \in J$. Weil $1 \in J$, haben wir $J = R$, und somit ist I ein maximales Ideal. ⊣

Als Folgerung erhalten wir:

KOROLLAR 10.5. *Ein Ideal $m\mathbb{Z} \subseteq \mathbb{Z}$ ist genau dann maximal, wenn m eine Primzahl ist.*

11. FORMALE POTENZREIHEN

Eine **Reihe** ist eine Summe mit unendlich vielen Summanden. Zum Beispiel ist die Summe aller natürlichen Zahlen

$$0 + 1 + 2 + 3 + \dots$$

eine Reihe. Eine endliche Summe lässt sich immer auch als Reihe schreiben, indem wir einfach unendlich viele Nullen addieren. Zum Beispiel ist $3 + 4$ eine Summe, aber

$$3 + 4 + 0 + 0 + 0 + \dots$$

ist eine Reihe. Eine **formale Potenzreihe** (oder einfach Potenzreihe) ist eine Reihe der Form

$$a_0 z^0 + a_1 z^1 + a_2 z^2 + \dots + a_n z^n + \dots$$

wobei die Koeffizienten $a_0, a_1, \dots, a_n, \dots$ (für $n \in \mathbb{N}$) Elemente aus einem Körper K sind (z. .B. aus $\mathbb{R}$) und z (oder x, oder s, etc.) irgend eine *Unbestimmte* ist, wobei eine Unbestimmte weder ein Körperelement noch eine Variable ist. Zum Beispiel sind $(1z^0 + 2z^1 + 3z^2 + \dots)$ und $(0z^0 - 1z^1 + 0z^2 - 1z^3 + 0z^4 - 1z^5 + \dots)$ Potenzreihen.

Üblicherweise schreiben wir bloss a_0 anstelle von $a_0 z^0$, und anstelle von $a_1 z^1$ schreiben wir bloss $a_1 z$. Wenn $a_n = 0$ (für irgend $n \in \mathbb{N}$), so schreiben wir $a_n z^n$ nicht. Die obigen Potenzreihen können also wie folgt geschrieben werden:

- $(1z^0 + 2z^1 + 3z^2 + \dots) = (1 + 2z + 3z^2 + \dots)$
- $(0z^0 - 1z^1 + 0z^2 - 1z^3 + 0z^4 - 1z^5 + \dots) = (-z - z^3 - z^5 - \dots)$

Wie oben erwähnt, darf anstelle von z auch irgend eine andere Unbestimmte geschrieben werden, wie zum Beispiel x oder y.

Formal kann die n-te Potenz der Unbestimmten z, also z^n, aufgefasst werden als ein Vektor mit abzählbar unendlich vielen Koordinaten, wobei nur an der n-ten Stelle eine 1 und sonst überall 0-en stehen:

$$[0, 0, 0, \dots, 0, 0, \underset{\substack{\uparrow \\ n\text{-te Stelle}}}{1}, 0, 0, 0, 0, \dots]$$

Der Ausdruck $a_n z^n$ entspricht dann dem Vektor

$$[0, 0, 0, \dots, 0, 0, \underset{\substack{\uparrow \\ n\text{-te Stelle}}}{a_n}, 0, 0, 0, 0, \dots]$$

und die Potenzreihe $\sum_{n \in \mathbb{N}} a_n z^n$ entspricht dem Vektor

$$[a_0, a_1, a_2, \dots, a_n, \dots].$$

Formale Potenzreihen können also als Vektoren in einem ω-dimensionalen Vektorraum über dem Körper K aufgefasst werden, wobei die Potenzen $z^0, z^1, \dots, z^n, \dots$ der Unbestimmten z die Rolle der Basisvektoren $e_0, e_1, \dots, e_n, \dots$ übernehmen.

Ist für eine natürliche Zahl $n_0 \in \mathbb{N}$ und für alle $n \geq n_0$, $a_n = 0$, so entspricht die Potenzreihe

$$(a_0 + a_1 z + a_2 z^2 + \dots)$$

einem **Polynom**. Das heisst, Polynome sind Potenzreihen bei denen nur endlich viele Koeffizienten von Null verschieden sind.

Jede Potenzreihe $\sum_{n \in \mathbb{N}} a_n z^n$ definiert eine Funktion $A : \mathbb{N} \to K$ dadurch, dass wir für alle $n \in \mathbb{N}$ festsetzen $A(n) := a_n$. Umgekehrt definiert jede Funktion $A : \mathbb{N} \to K$ eine Potenzreihe $\sum_{n \in \mathbb{N}} a_n z^n$ dadurch, dass wir festsetzen $a_n := A(n)$. Diese Beziehung zwischen Funktionen $A : \mathbb{N} \to K$ (bzw. abzälbaren Folgen in K) und Potenzreihen kann benutzt werden, um sogenannte *generierende Funktionen* von Zahlenfolgen (für $K = \mathbb{R}$) zu berechnen.

Die wohl einfachste (echte) Potenzreihe ist die *geometrische Reihe*:

$$\mathrm{geo}(z) := (1 + z + z^2 + z^3 + z^4 + \ldots) = \sum_{n\in\mathbb{N}} z^n$$

Wenn wir in der Potenzreihe $\mathrm{geo}(z)$ die Unbestimmte z ersetzen durch $-z$ oder z^2, so erhalten wir wieder eine Potenzreihe, welche wir mit $\mathrm{geo}(-z)$ bzw. $\mathrm{geo}(z^2)$ bezeichnen. Es gilt:

$$\begin{aligned}\mathrm{geo}(-z) &= ((-z)^0 + (-z)^1 + (-z)^2 + \ldots) = (1 - z + z^2 - z^3 + \ldots) = \textstyle\sum_{n\in\mathbb{N}} (-1)^n z^n \\ \mathrm{geo}(z^2) &= ((z^2)^0 + (z^2)^1 + (z^2)^2 + \ldots) = (1 + z^2 + z^4 + z^6 + \ldots) = \textstyle\sum_{n\in\mathbb{N}} z^{2n}\end{aligned}$$

Rechnen mit formalen Potenzreihen

Formale Potenzreihen können addiert und multipliziert werden, jede Potenzreihe hat ein additiv Inverses und manche Potenzreiehn haben sogar ein multiplikativ Inverses: Im Folgenden seien

$$(a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots) \quad \text{und} \quad (b_0 + b_1 z + b_2 z^2 + b_3 z^3 \ldots)$$

zwei beliebige Potenzreihen.

Die Addition und Subtraktion (bzw. Addition mit dem additiv Inversen) dieser beiden Potenzreihen geschieht komponentenweise:

$$(a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots) \pm (b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots) = (c_0 + c_1 z + c_2 z^2 + c_3 z^3 + \ldots)$$

mit $c_n = a_n \pm b_n$.

Die Multiplikation folgt direkt aus dem Distributivgesetz und ist eine Art "Faltung":

$$(a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots) \cdot (b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots) = (c_0 + c_1 z + c_2 z^2 + c_3 z^3 + \ldots)$$

mit $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0$.

Damit eine Potenzreihe $(b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots)$ ein multiplikativ Inverses $(b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots)^{-1}$ besitzt, muss $b_0 \neq 0$ sein. Sei $(c_0 + c_1 z + c_2 z^2 + c_3 z^3 + \ldots)$ die Potenzreihe $(b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots)^{-1}$. Dann gilt

$$(b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots) \cdot (c_0 + c_1 z + c_2 z^2 + c_3 z^3 + \ldots) = 1$$

und mit der Regel für die Multiplikation lassen sich dann die Koeffizienten c_n durch sogenannten *Koeffizientenvergleich* Schrit für Schritt berechnen: Es ist $1 = b_0 c_0$, also $c_0 = {b_0}^{-1}$ (beachte, dass $b_0 \neq 0$). Weiter ist $0 = b_0 c_1 + b_1 c_0$ und mit $c_0 = {b_0}^{-1}$ ist $c_1 = {b_0}^{-1}(-b_1 {b_0}^{-1})$, etc.

Für die Potenzreihe $(a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots) \cdot (b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots)^{-1}$ schreiben wir auch

$$\frac{(a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots)}{(b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots)}.$$

Als Anwendung der Multiplikation von Potenzreihen berechnen wir nun drei Produkte geometrischer Potenzreihen. Es gilt:

$$\begin{aligned}\mathrm{geo}(z) \cdot \mathrm{geo}(-z) &= 1 + z^2 + z^4 + z^6 + \ldots = \sum_{n\in\mathbb{N}} z^{2n} = \mathrm{geo}(z^2) \\ \mathrm{geo}(z) \cdot \mathrm{geo}(z) = \mathrm{geo}(z)^2 &= 1 + 2z + 3z^2 + 4z^3 + \ldots = \sum_{n\in\mathbb{N}} (n+1) z^n \\ \mathrm{geo}(z)^2 \cdot \mathrm{geo}(-z) &= 1 + z + 2z^2 + 2z^3 + 3z^4 + 3z^5 + 4z^6 + \ldots\end{aligned}$$

Als letztes Beispiel berechnen wir $(1-z)\cdot \mathrm{geo}(z)$. Es ist leicht zu sehen, dass gilt

$$(1-z)\cdot \mathrm{geo}(z) = 1\,,$$

woraus folgt:

$$\mathrm{geo}(z) = (1-z)^{-1} \quad \text{bzw.} \quad \mathrm{geo}(z) = \frac{1}{1-z}$$

Damit erhalten wir zum Beispiel

$$\mathrm{geo}(z)\cdot\mathrm{geo}(-z) = \frac{1}{1-z}\cdot\frac{1}{1+z} = \frac{1}{1-z^2} = \mathrm{geo}(z^2),$$

was wir oben bereits ausgerechnet haben.

UNENDLICHE PRODUKTE FORMALER POTENZREIHEN

Sei Pr die Menge aller Potenzreihen (über einem Köper K) in der Unbestimmten z. Eine unendliche Familie $\mathscr{F} = \{f_l \in \mathrm{Pr} : l \in \mathbb{N}\}$ von Potenzreihen heisst **multiplizierbar**, falls

$$\prod_{l\in\mathbb{N}} f_l \in \mathrm{Pr}\,.$$

Die Aussage $\prod_{l\in\mathbb{N}} f_l \in \mathrm{Pr}$ bedeutet, dass die *endlichen* Produkte $\prod_{l\in L} f_l \in \mathrm{Pr}$ für $L\to\infty$ gegen eine Potenzreihe $f\in\mathrm{Pr}$ *konvergieren*. Um dies formaler auszudrücken, definieren wir für jedes $m\in\mathbb{N}$ die Menge Pr_m wie folgt.

$$\mathrm{Pr}_m := \{z^m\cdot f : f\in\mathrm{Pr}\}$$

Beachte, dass Pr_m ein Ideal ist im Ring $(\mathrm{Pr}, 0_K, 1_K, +, \cdot)$. Insbesondere ist Pr_1 ein maximales Ideal und es gilt $\mathrm{Pr}\,/\,\mathrm{Pr}_1 \cong K$.

Dass die endlichen Produkte $\prod_{l\in L} f_l \in \mathrm{Pr}$ für $L\to\infty$ gegen eine Potenzreihe $f\in\mathrm{Pr}$ konvergieren, definieren wir nun wie folgt: Es gibt eine Potenzreihe $f=\sum_{n=0}^{\infty} a_n z^n$, sodass für jedes $m\in\mathbb{N}$ ein $L'\in\mathbb{N}$ existiert, sodass für alle $L\geq L'$ gilt:

$$\left(\prod_{l\in L} f_l - \sum_{n=0}^{m} a_n z^n\right) \in \mathrm{Pr}_{m+1}$$

Wir betrachten folgendes Beispiel: Sei $f_l = \sum_{n\in\mathbb{N}} a_{l,n} z^n$ und nehmen wir an, dass $a_{l,0}=1$ für alle $l\in\mathbb{N}$. Weiter nehmen wir an, dass die endlichen Produkte $\prod_{l\in L} f_l \in \mathrm{Pr}$ für $L\to\infty$ gegen die Potenzreihe $f=\sum_{n\in\mathbb{N}} a_n z^n$ konvergieren. Für den Koeffizienten a_0 gilt somit

$$a_0 = \prod_{l\in\mathbb{N}} a_{l,0} = 1.$$

Nun betrachten wir den Koeffizienten a_n für ein $n\geq 1$. Aus der Definition der Multiplikation von Potenzreihen folgt

$$a_n = \sum_{\varepsilon\in S_n} \prod_{l\in\mathbb{N}} a_{l,\varepsilon(l)}$$

wobei S_n die Menge aller Funktionen $\varepsilon:\mathbb{N}\to n+1$ bezeichnet mit $\sum_{l\in\mathbb{N}}\varepsilon(l)=n$. Eine sicher hinreichende Bedingung für die Existenz von a_n ist, dass nur endlich viele Produkte $\prod_{l\in\mathbb{N}} a_{l,\varepsilon(l)}$ von 0 verschieden sind. Dies ist aber genau dann der Fall, wenn es nur endlich viele $l\in\mathbb{N}$ gibt, sodass $a_{l,k}\neq 0$ für ein $1\leq k\leq n$.

Um zu beweisen, dass spezielle Familien von Potenzreihen multiplizierbar sind, führen wir noch folgenden Begriff ein: Ist $g \in \mathrm{Pr} \setminus \{0\}$ und gilt für ein $m \in \mathbb{N}$, $g \in \mathrm{Pr}_m \setminus \mathrm{Pr}_{m+1}$, so sagen wir, dass die Potenzreihe g den **Minimalgrad** m besitzt, d. h. g ist von der Form $\sum_{n=m}^{\infty} a_n z^n$ mit $a_m \neq 0$. Der Minimalgrad von $g \in \mathrm{Pr}$ wird mit $\deg_{\min}(g)$ bezeichnet.

PROPOSITION 11.1. *Sei $\mathscr{F} = \{f_l \in \mathrm{Pr} : l \in \mathbb{N}\}$ eine Familie von Potenzreihen mit folgenden Eigenschaften: Für alle $l \in \mathbb{N}$ ist $f_l = 1 + g_l$ für ein g_l mit $\deg_{\min}(g_l) > 0$, und für alle $m \in \mathbb{N}$ ist die Menge*

$$\{l \in \mathbb{N} : \deg_{\min}(g_l) \leq m\}$$

endlich. Dann ist $\mathscr{F}$ eine mulitiplizierbare Familie.

Beweis. Weil $\deg_{\min}(g_l) > 0$ ist $a_0 = \prod_{n \in \mathbb{N}} 1 = 1$. Der Beweis ist nun mit Induktion über m. Wir nehmen an, wir hätten die Koeffizienten $a_0, \ldots, a_m$ (für ein $m \geq 0$) der Potenzreihe f, gegen welche $\prod_{l \in \mathbb{N}} f_l$ konvergiert, bereits bestimmt. Das heisst, es gibt ein $L' \in \mathbb{N}$, sodass für alle $L \geq L'$ gilt:

$$\left(\prod_{l \in L} f_l - \sum_{n=0}^{m} a_n z^n\right) \in \mathrm{Pr}_{m+1}$$

Aus der Voraussetzung folgt, dass es für $m+1$ nur endlich viele Potenzreihen g_l gibt mit $\deg_{\min}(g_l) \leq m+1$. Sei $\sum_{n=0}^{m+1} \tilde{a}_n z^n$ das Produkt der entsprechenden Potenzreihen $f_l = 1 + g_l$ und sei $L' \in \mathbb{N}$ so, dass jedes l mit $\deg_{\min}(g_l) \leq m+1$ in L' ist. Dann gilt $\tilde{a}_n = a_n$ für alle $0 \leq n \leq m$. Weiter gilt, dass jedes endliche Produkt von Potenzreihen $f_{l'}$ mit $l' \notin L'$ in Pr_{m+2} ist. Somit gilt für alle $L \geq L'$,

$$\prod_{l \in L} f_l - \left(\sum_{n=0}^{m} a_n z^n + \tilde{a}_{m+1}\, z^{m+1}\right) \in \mathrm{Pr}_{m+2}$$

wobei für $0 \leq n \leq m$ gilt $\tilde{a}_n = a_n$. Setzen wir $a_{m+1} := \tilde{a}_{m+1}$, so ist für alle $L \geq L'$

$$\left(\prod_{l \in L} f_l - \sum_{n=0}^{m+1} a_n z^n\right) \in \mathrm{Pr}_{m+2}$$

wie gewünscht. ⊣

FORMALES ABLEITEN VON FORMALEN POTENZREIHEN

Ist $f = \sum_{n \in \mathbb{N}} a_n z^n \in \mathrm{Pr}$, so ist die formale Ableitung $D(f)$ von f definiert durch

$$D(f) := \sum_{n \in \mathbb{N}} n \cdot a_n z^{n-1}.$$

PROPOSITION 11.2. *Sind $f, g \in \mathrm{Pr}$, so gelten die folgenden Regeln:*

$$D(f+g) = D(f) + D(g) \quad \textit{und} \quad D(f \cdot g) = D(f) \cdot g + f \cdot D(g)$$

Beweis. Die Regel $D(f+g) = D(f) + D(g)$ folgt unmittelbar aus der Definition von D.

Um die Regel $D(f \cdot g) = D(f) \cdot g + f \cdot D(g)$ zu verifizieren, seien $f = \sum_{n \in \mathbb{N}} a_n z^n$ und $g = \sum_{n \in \mathbb{N}} b_n z^n$. Dann gilt für $f \cdot g = \sum_{n \in \mathbb{N}} c_n z^n$, $c_{n+1} = a_0 b_{n+1} + a_1 b_n + \ldots + a_n b_1 + a_{n+1} b_0$, und für $D(f \cdot g) = \sum_{n \in \mathbb{N}} \tilde{c}_n z^n$ erhalten wir

$$\tilde{c}_n = (n+1)\big(a_0 b_{n+1} + a_1 b_n + \ldots + a_n b_1 + a_{n+1} b_0\big).$$

Ist $D(f)\cdot g=\sum_{n\in\mathbb{N}} d_n z^n$ und $f\cdot D(g)=\sum_{n\in\mathbb{N}} e_n z^n$, so ist

$$\begin{array}{rcccccccccc} d_n &=& a_1b_n &+& 2a_2b_{n-1} &+& \ldots &+& na_nb_1 &+& (n+1)a_{n+1}b_0,\\ e_n &=& na_1b_n &+& (n-1)a_2b_{n-1} &+& \ldots &+& a_nb_1 &+& (n+1)a_0b_{n+1}, \end{array}$$

und es gilt $d_n+e_n=\tilde{c}_n$. ⊣

Ist $f\in \mathrm{Pr}$ mit $\deg_{\min}(f)=0$, so ist die **logarithmische Ableitung** $D_{\log}(f)$ definiert durch

$$D_{\log}(f):=\frac{D(f)}{f}.$$

PROPOSITION 11.3. *Ist $\mathscr{F}=\{f_l\in \mathrm{Pr}: l\in\mathbb{N}\}$ eine multiplizierbare Familie mit den Eigenschaften $f_l=1+g_l$ für $g_l\in \mathrm{Pr}_1$ und $\big|\{l\in\mathbb{N}:\deg_{\min}(g_l)\le m\}\big|$ endlich für alle $l,m\in\mathbb{N}$, so ist*

$$D_{\log}\big(\prod_{l\in\mathbb{N}} f_l\big)=\sum_{n\in\mathbb{N}}\frac{D(f_l)}{f_l} \quad \textit{und} \quad \sum_{n\in\mathbb{N}}\frac{D(f_l)}{f_l}\in \mathrm{Pr}\,.$$

Beweis. Nach Definition von D bzw. $D_{\log}$ und mit den Eigenschaften von $\mathscr{F}$ gilt

$$D_{\log}\big(\prod_{l\in\mathbb{N}} f_l\big)=\frac{D(f_0)\cdot\prod_{l\in\mathbb{N}} f_{l+1}+f_0\cdot D\big(\prod_{l\in\mathbb{N}} f_{l+1}\big)}{\prod_{l\in\mathbb{N}} f_l}=$$

$$\frac{D(f_0)}{f_0}+\frac{f_0\cdot D(f_1)\cdot\prod_{l\in\mathbb{N}} f_{l+2}+f_0\cdot f_1\cdot D\big(\prod_{l\in\mathbb{N}} f_{l+2}\big)}{\prod_{l\in\mathbb{N}} f_l}=$$

$$\frac{D(f_0)}{f_0}+\frac{D(f_1)}{f_1}+\frac{f_0\cdot f_1\cdot D(f_2)\cdot\prod_{l\in\mathbb{N}} f_{l+3}+f_0\cdot f_1\cdot f_2\cdot D\big(\prod_{l\in\mathbb{N}} f_{l+3}\big)}{\prod_{l\in\mathbb{N}} f_l}=\ldots$$

und wir erhalten schliesslich

$$D_{\log}\big(\prod_{l\in\mathbb{N}} f_l\big)=\frac{D(f_0)}{f_0}+\frac{D(f_1)}{f_1}+\frac{D(f_2)}{f_2}+\ldots=\sum_{n\in\mathbb{N}}\frac{D(f_l)}{f_l}.$$

Aus $f_l=1+g_l$ und $\deg_{\min} g_l\ge 1$ für alle $l\in\mathbb{N}$, folgt ${f_l}^{-1}=\frac{1}{f_l}\in \mathrm{Pr}$. Weiter folgt aus $f_l=1+g_l$, dass gilt $D(f_l)=D(g_l)$, und mit $\deg_{\min}(D(g_l))=\deg_{\min}(g_l)-1$, erhalten wir schliesslich

$$\deg_{\min}(g_l)-1=\deg_{\min}\Big(\frac{D(f_l)}{f_l}\Big).$$

Weil nun die Menge $\{l\in\mathbb{N}:\deg_{\min}(g_l)\le m\}$ endlich ist für jedes $m\in\mathbb{N}$, folgt, dass die Summe $\sum_{n\in\mathbb{N}}\frac{D(f_l)}{f_l}$ eine formale Potenzreihe ist. ⊣

12. Endliche Körper von Primzahlpotenzordnung

Irreduzible Polynome in $\mathbb{F}_p[X]$

Im Folgenden sei $\mathbb{F}_p[X]$ der Ring der Polynome über dem Körper $\mathbb{F}_p$ (p prim), d. h. $\mathbb{F}_p[X]$ ist die Menge der Polynome mit Koeffizienten in $\mathbb{F}_p$ mit der üblichen Addition und Multiplikation von Polynomen.

Für ein Polynom $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$ ist der **Grad** von f definiert als $\deg(f) := \max\{k \in \mathbb{N} : a_k \neq 0\}$ falls solch eine Zahl existiert, sonst sei $\deg(f) := -\infty$ (d. h. $\deg(0) = -\infty$), wobei wir definieren $-\infty + -\infty = -\infty + n = -\infty$ für alle $n \in \mathbb{N}$.

Faktum 12.1. *Sind $f, g \in \mathbb{F}_p[X]$, so ist $\deg(f \cdot g) = \deg(f) + \deg(g)$.*

Beweis. Ist $f = 0$ oder $g = 0$, so ist $-\infty = \deg(f \cdot g) = \deg(f) + \deg(g)$. Andernfalls seien $f = a_0 + a_1X + \ldots + a_mX^m$ und $g = b_0 + b_1X + \ldots + b_nX^n$ mit $a_m \neq 0 \neq b_n$. Weil $\mathbb{F}_p$ ein Körper ist, gilt $a_mb_n \neq 0$ und aus $f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)X + \ldots + a_mb_nX^{m+n}$ folgt $\deg(f \cdot g) = \deg(f) + \deg(g)$. ⊣

Ein Polynom $f \in \mathbb{F}_p[X]$ mit $\deg(f) > 0$ heisst **irreduzibel** über $\mathbb{F}_p$, wenn aus $g \cdot h = f$ für $g, h \in \mathbb{F}_p[X]$ folgt $\deg(g) = 0$ oder $\deg(h) = 0$, sonst heisst f **reduzibel**. Wie für die Eindeutigkeit der Primfaktorzerlegung (Korollar 9.5) lässt sich zeigen, dass sich jedes Polynom $f \in \mathbb{F}_p[X]$ mit $f \neq 0$ bis auf Vertauschung der Faktoren und bis auf Faktoren aus $\mathbb{F}_p$ eindeutig als Produkt irreduzibler Polynome schreiben lässt.

Für $f \in \mathbb{F}_p[X]$ sei

$$(f) := \{g \cdot f : g \in \mathbb{F}_p[X]\}$$

das von f erzeugte Ideal in $\mathbb{F}_p[X]$. Dann ist mit Lemma 10.2 $\mathbb{F}_p[X]/(f)$ ein Ring.

Proposition 12.2. *Sei $f \in \mathbb{F}_p[X]$ mit $\deg(f) \geq 1$. Dann ist $\mathbb{F}_p[X]/(f)$ genau dann ein Körper wenn (f) irreduzibel über $\mathbb{F}_p$ ist.*

Beweis. ($\Leftarrow$) Sei $f \in \mathbb{F}_p[X]$ irreduzibel mit $\deg(f) \geq 1$. Für jedes $g \in \mathbb{F}_p[X] \setminus (f)$ finden wir mit dem vEA Polynome $h_1, h_2, d \in \mathbb{F}_p[X]$, sodass gilt $h_1f + h_2g = d$, wobei $d \mid f$ und $d \mid g$. Weil f irreduzibel ist, gilt entweder $d = f$ oder $d \in \mathbb{F}_p$ (also $\deg(d) = 0$). Im ersten Fall gilt $f \mid g$ und somit ist $g \in (f)$, was unserer Annahme widerspricht. Im zweiten Fall ist

$$h_1f + h_2g \equiv h_2g \equiv 1 \pmod{f}$$

(weil $\mathbb{F}_p$ ein Körper ist). Daraus folgt, dass $\bar{h}_2$ im Ring $\mathbb{F}_p[X]/(f)$ ein multiplikativ Inverses von $\bar{g} \neq \bar{0}$ ist, und weil g beliebig war, ist $\mathbb{F}_p[X]/(f)$ ein Körper.

($\Rightarrow$) Mit Kontraposition, d. h. wir nehmen an, dass (f) reduzibel ist. Mit Proposition 10.4 genügt es zu zeigen, dass (f) kein maximales Ideal ist. Ist f reduzibel, so existieren Polynome $g, h \in \mathbb{F}_p[X]$ mit $g \cdot h = f$ und $\deg(g), \deg(h) > 0$, d. h. weder g noch h ist in $\mathbb{F}_p$. Aus Faktum 12.1 folgt $\deg(f) = \deg(g) + \deg(h)$. Weil $\deg(h) > 0$, ist $\deg(g) < \deg(f)$, und mit $g \mid f$ folgt $(f) \subsetneq (g)$. Weiter erhalten wir mit $\deg(g) > 0$, dass $(g) \subsetneq \mathbb{F}_p[X]$. Also gilt $(f) \subsetneq (g) \subsetneq \mathbb{F}_p[X]$ und (f) ist kein maximales Ideal. ⊣

Korollar 12.3. *Ist $f \in \mathbb{F}_p[X]$ mit $\deg(f) = n \geq 1$ irreduzibel, so ist $\mathbb{F}_p[X]/(f)$ ein Körper der Ordnung p^n.*

Beweis. Mit Proposition 12.2 ist $\mathbb{F}_p[X]/(f)$ ein Körper und weil

$$\mathbb{F}_p[X]/(f) \cong \{g \in \mathbb{F}_p[X] : \deg(g) < n\}$$

und $|\mathbb{F}_p| = p$, hat der Körper $\mathbb{F}_p[X]/(f)$ die Ordnung p^n. ⊣

EXISTENZ VON KÖRPERN DER ORDNUNG p^n

Ein Polynom der Form $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$ mit $a_n = 1$ heisst **normiert**. Ist $f = b_0 + b_1X + \ldots + b_nX^n \in \mathbb{F}_p[X]$ mit $b_n \neq 0$ ein irreduzibles Polynom, so ist auch $\frac{b_0}{b_n} + \frac{b_1}{b_n}X + \ldots + \frac{b_n}{b_n}X^n$ ein irreduzibles Polynom. Um die Existenz von Körpern der Ordnung p^n zu beweisen, genügt es also, die Existenz von normierten, irreduziblen Polynomen vom Grad n zu zeigen.

THEOREM 12.4. *Zu jeder positiven Zahl $n \in \mathbb{N}$ und zu jeder Primzahl p existiert ein Körper der Ordnung p^n.*

Beweis. Mit Korollar 12.3 genügt es zu zeigen, dass für jedes $n \geq 1$ und jede Primzahl p mindestens ein normiertes, irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad n existiert.

Sei p prim beliebig, aber fest gewählt. Sei weiter I_n die Menge aller normierten, irreduziblen Polynome in $\mathbb{F}_p[X]$ vom Grad n, d. h.

$$I_n = \{f_{1,n}, \ldots, f_{r_n,n}\}$$

mit $f_{i,n}$ normiert, irreduzibel und $\deg(f_{i,n}) = n$. Ist $r_n = 0$, so ist $I_n = \emptyset$. Wir müssen also zeigen, dass für alle $n \geq 1$ gilt $r_n \geq 1$.

Für ein festes n betrachten wir zuerst die Menge F_n aller normierten (nicht notwendigerweise irreduziblen) Polynome beliebigen Grades, welche wir als Produkte von Polynomen $f_{i,n} \in I_n$ bilden können (beachte, dass Produkte normierter Polynome normiert sind). Der Menge F_n ordnen wir eine abzählende formale Potenzreihe zu: Mit dem Polynom $f_{i,n}$, für ein festes i $(1 \leq i \leq r_n)$, können wir die

Polynome	$f_{i,n}^0$	$f_{i,n}^1$	$f_{i,n}^2$	$\ldots$	$f_{i,n}^k$	$\ldots$	bilden, diese haben
Grad	0	n	$2n$	$\ldots$	kn	$\ldots$	und die abzählende
Potenzreihe ist	$1z^0$ +	$1z^n$ +	$1z^{2n}$ +	$\ldots$ +	$1z^{kn}$ +	$\ldots$	$= \mathrm{geo}(z^n)$.

Mit den beiden Polynomen $f_{i,n}$ und $f_{j,n}$ für $i \neq j$, können wir die

Polynome	$f_{i,n}^0 = f_{j,n}^0$	$f_{i,n}^1, f_{j,n}^1$	$f_{i,n}^2,\ f_{i,n}\cdot f_{j,n},\ f_{j,n}^2$	$\ldots$	bilden, mit
Grad	0	n	$2n$	$\ldots$	und abzählender
Potenzreihe	$1z^0$ +	$2z^n$ +	$3z^{2n}$ +	$\ldots$	$= \mathrm{geo}(z^n)^2$.

Allgemein erhalten wir für die r_n Polynome in I_n die abzählende Potenzreihe

$$\underbrace{a_0}_{=1} z^0 + a_1 z^n + a_2 z^{2n} + \ldots + a_k z^{kn} + \ldots = \mathrm{geo}(z^n)^{r_n}$$

wobei a_k die Anzahl der normierten Polynome vom Grad kn ist, welche als Produkt von Polynomen aus I_n geschrieben werden können.

Sei nun F die Menge *aller* normierten Polynome in $\mathbb{F}_p[X]$. Dann erhalten wir, mit dem vorigen Resultat, die zu F gehörende abzählende Potenzreihe

$$\psi(z) = \mathrm{geo}(z^1)^{r_1} \cdot \mathrm{geo}(z^2)^{r_2} \cdot \mathrm{geo}(z^3)^{r_3} \cdot \ldots = \prod_{n=1}^{\infty} \Big(\frac{1}{1-z^n}\Big)^{r_n}.$$

Andererseits gibt es in $\mathbb{F}_p[X]$ genau p^n normierte Polynome vom Grad n. Somit muss gelten

$$\psi(z) = 1z^0 + pz^1 + p^2z^2 + \ldots + p^nz^n + \ldots = \frac{1}{1-pz}.$$

Wir erhalten also

$$\prod_{n=1}^{\infty}\Big(\frac{1}{1-z^n}\Big)^{r_n}=\frac{1}{1-pz}\quad\text{bzw. für die reziproken Reihen}\quad\prod_{n=1}^{\infty}(1-z^n)^{r_n}=1-pz.$$

Mit logarithmischem Ableiten auf beiden Seiten erhalten wir

$$\sum_{n=1}^{\infty}\frac{D\big((1-z^n)^{r_n}\big)}{(1-z^n)^{r_n}}=\sum_{n=1}^{\infty}\frac{r_n(1-z^n)^{r_n-1}(-nz^{n-1})}{(1-z^n)^{r_n}}=\sum_{n=1}^{\infty}-\frac{r_n\cdot n}{1-z^n}z^{n-1}=$$

$$\frac{D(1-pz)}{1-pz}=\frac{-p}{1-pz}=-p\cdot\mathrm{geo}(pz)=\sum_{n=1}^{\infty}-p^nz^{n-1},$$

also

$$\sum_{n=1}^{\infty}\frac{r_n\cdot n}{1-z^n}z^{n-1}=\sum_{n=1}^{\infty}p^nz^{n-1}$$

Entwickeln wir die Summe auf der linken Seite nach Potenzen z^{n-1}, so erhalten wir:

$$\begin{array}{ccccccccccccccccccc}
r_1 & + & r_1z & + & r_1z^2 & + & r_1z^3 & + & r_1z^4 & + & r_1z^5 & + & r_1z^6 & + & r_1z^7 & + & r_1z^8 & + & \dots\\
 & & 2r_2z & + & & & 2r_2z^3 & + & & & 2r_2z^5 & + & & & 2r_2z^7 & + & & + & \dots\\
 & & & & 3r_3z^2 & + & & & & & 3r_3z^5 & + & & & & & 3r_3z^8 & + & \dots\\
 & & & & & & 4r_4z^3 & + & & & & & & & 4r_4z^7 & + & & & \dots\\
 & & & & & & & & 5r_5z^4 & + & & & & & & & & & \dots\\
 & & & & & & & & & & 6r_6z^5 & + & & & & & & & \dots\\
 & & & & & & & & & & & & 7r_7z^6 & + & & & & & \dots\\
 & & & & & & & & & & & & & & \dots & & & & \dots
\end{array}$$

Addieren wir spaltenweise, so erhalten wir

$$\sum_{n=1}^{\infty}\frac{r_n\cdot n}{1-z^n}z^{n-1}=\sum_{n=1}^{\infty}\Big(\sum_{d|n}d\cdot r_d\Big)\cdot z^{n-1}=\sum_{n=1}^{\infty}p^nz^{n-1}$$

und mit Koeffizientenvergleich erhalten wir:

$$\sum_{d|n}d\cdot r_d=p^n$$

Setzen wir $g(d):=d\cdot r_d$ und $f(n):=p^n$, so ist $\sum_{d|n}g(d)=f(n)$ und mit Aufgabe 44 gilt:

$$g(n)=\sum_{d|n}\mu(d)\cdot f(n/d),\quad\text{d. h.}\quad\underbrace{n\cdot r_n}_{=g(n)}=\sum_{d|n}\mu(d)\cdot\underbrace{p^{n/d}}_{=f(n/d)}\quad\text{also}\quad r_n=\frac{1}{n}\cdot\sum_{d|n}\mu(d)\cdot p^{n/d}.$$

Nach Definition ist $\mu(1)=1$ und allgemein $\mu(d)\in\{-1,0,1\}$, woraus folgt

$$n\cdot r_n=p^n+\ldots+\mu(n)p\geq p^n-\sum_{k=1}^{n-1}p^k\geq 2.$$

Insbesondere ist für alle $n\geq 1$, $n\cdot r_n\geq 2$, also $r_n\geq 1$, was zu zeigen war. ⊣

Beispiele:

- $r_1 = p$: Die p normierten, irreduziblen Polynome vom Grad 1 über $\mathbb{F}_p$ sind X, $X+1$, $\ldots$, $X+(p-1)$.
- $r_2 = \frac{1}{2}(p^2-p)$: $\frac{1}{2}\sum_{d|2}\mu(d)p^{2/d} = \frac{1}{2}(p^2+\mu(2)p) = \frac{1}{2}(p^2-p)$
- $r_3 = \frac{1}{3}(p^3-p)$: $\frac{1}{3}\sum_{d|3}\mu(d)p^{3/d} = \frac{1}{3}(p^3+\mu(3)p) = \frac{1}{4}(p^3-p)$
- $r_4 = \frac{1}{4}(p^4-p^2)$: $\frac{1}{4}\sum_{d|4}\mu(d)p^{4/d} = \frac{1}{4}(p^4+\mu(2)p^2+\mu(4)p) = \frac{1}{4}(p^4-p^2)$
- $r_5 = \frac{1}{5}(p^5-p)$: $\frac{1}{5}\sum_{d|5}\mu(d)p^{5/d} = \frac{1}{5}(p^5+\mu(5)p) = \frac{1}{5}(p^5-p)$
- $r_6 = \frac{1}{6}(p^6-p^3-p^2+p)$: $\frac{1}{6}\sum_{d|6}\mu(d)p^{6/d} = \frac{1}{6}(p^6+\underbrace{\mu(2)}_{=-1}p^3+\underbrace{\mu(3)}_{=-1}p^2+\underbrace{\mu(6)}_{=1}p)$
- Für $p=3$ erhalten wir
$$r_1 = 3, \quad r_2 = 3, \quad r_3 = 8, \quad r_4 = 18, \quad r_5 = 48, \quad r_6 = 116,$$
und für $p=7$ erhalten wir
$$r_1 = 7, \quad r_2 = 21, \quad r_3 = 112, \quad r_4 = 588.$$
- Die 21 normierten irreduziblen Polynome vom Grad 2 über $\mathbb{F}_7$ sind:
  0. X^2+1
  1. X^2+2
  2. X^2+4
  3. X^2+X+3
  4. X^2+X+4
  5. X^2+X+6
  6. X^2+2X+2
  7. X^2+2X+3
  8. X^2+2X+5
  9. X^2+3X+1
  10. X^2+3X+5
  11. X^2+3X+6
  12. X^2+4X+1
  13. X^2+4X+5
  14. X^2+4X+6
  15. X^2+5X+2
  16. X^2+5X+3
  17. X^2+5X+5
  18. X^2+6X+3
  19. X^2+6X+4
  20. X^2+6X+6
- Das Polynom $f = X^{100}+X^6+X^5+X^2+1$ ist irreduzibel über $\mathbb{F}_2$ und somit ist $\mathbb{F}_2[X]/(f)$ ein Körper der Ordnung $2^{100} = 1\,267\,650\,600\,228\,229\,401\,496\,703\,205\,376$.