Logik und Diskrete Strukturen

AOR Dr. Thoralf Räsch

Mathematisches Institut
der Universität Bonn

Version 1.2

22. Dezember 2009

Inhaltsverzeichnis

⋆ ⋆ ⋆

Dieses Skript entstand während meiner Vorlesung im Wintersemester 2007/08. Es basiert teilweise auf Vorlagen zu verschiedenen Vorlesungen der Herren Professoren Gräter (Universität Potsdam), Jensen (Humboldt-Universität zu Berlin) und Koepke (Universität Bonn).

⋆ ⋆ ⋆

Ich danke meinem Tutorenteam für die tatkräftige Unterstützung, vor allem Alexander Kränzlein, Julian Külshammer und Benjamin Seyfferth für das Korrekturlesen sowie Anika Markgraf und Melanie Schirmer darüber hinaus für das Erstellen einer LaTeX-Vorlage der Tafelbilder.

⋆ ⋆ ⋆

Im Wintersemester 2009/10 danke ich meiner Tutorin Karen Räsch für die Aktualisierung und Erweiterung des Skripts. Diesbezüglich danke ich allen Studierenden der Informatik für die Möglichkeit, ein solches Projekt durch Studiengebühren finanzieren zu können.

⋆ ⋆ ⋆

Teil 1. Grundlagen der Mathematik

In diesem ersten Abschnitt der Vorlesung lernen wir grundlegende Begriffe der Mathematik kennen. Wir lernen, wie man innerhalb der Mathematik mit ihnen umgehen muss, um korrekt und effizient mit ihnen zu arbeiten.

1. Logische Zeichen

In der Sprache der Mathematik kommen Sätze vor wie

(a) Kommutativgesetz: Für beliebige x,y gilt $x + y = y + x$.
(b) Existenz der Null: Es gibt 0, so dass $x + 0 = x$.
(c) Additive Inverse: Für jedes x gibt es ein $-x$ mit $x + (-x) = 0$.

Um auch in einem komplexen Kontext übersichtlich arbeiten zu können, werden in der Mathematik Abkürzungen verwendet.

Wir betrachten folgende so genannte *Aussagenlogische Verknüpfungen*: Für eine *Konjunktion*, das heißt, für "A und B" bzw. "es gelten A und B" schreiben wir kurz $A \wedge B$. Für eine *Disjunktion*, das heißt, für "A oder B" bzw. "es gilt A oder B" schreiben wir kurz $A \vee B$. Darüber hinaus schreiben wir für eine *Negation*, das heißt, für "nicht A", kurz $\neg A$.

Außerdem gibt es die so genannten *Quantorenlogischen Verknüpfungen*: Wir unterscheiden Existenzaussagen, wie "es existiert ein x mit A" bzw. "es existiert ein x, so dass A" und schreiben dafür kurz "$\exists x\, A$"; und es gibt Allaussagen der Form "für alle x gilt A" bzw. "für alle x ist A" und schreiben hierfür kurz "$\forall x\, A$". Manchmal nutzen wir auch Klammern und schreiben "$\exists x\, (A)$" bzw. "$\forall x\, (A)$".

Die obigen einführenden Beispiele könnte man etwa wie folgt formalisieren:

(a) $\forall x, y(x + y = y + x)$

(b) Es gibt ein Symbol "0", so dass gilt: $\forall x(x + 0 = x)$.

(c) $\forall x\ \exists y(x + y = 0)$

Manchmal setzen wir den quantorenfreien Bereich (Wirkungsbereich der Quantoren) in Klammern, um anzudeuten, auf welchen Bereich der Formel sich die Quantoren beziehen. So ist es schwierig, folgende Formel $\forall x\ x = 0 \rightarrow x + x = x$ zu lesen. Ohne Konventionen bzw. eindeutige Bildungsvorschriften könnte dies als $(\forall x\ x = 0\ ) \rightarrow 2x = x$ oder $\forall x(x = 0 \rightarrow 2x = x)$ gelesen werden.

Wir führen außer den oben genannten Verknüpfungen noch einige zusätzliche aussagenlogische Verknüpfungen ein, die uns das Lesen mathematischer Formeln erleichtern werden. Die Formeln werden dadurch teilweise kürzer und damit übersichtlicher. Für eine *Implikation*, das heißt, für "A impliziert B" bzw. "A folgt B", schreiben wir kurz $A \Rightarrow B$; für eine *Äquivalenz*, das heißt, für "A ist äquivalent zu B" schreiben wir kurz $A \Leftrightarrow B$. Hierbei meinen wir mit einer solchen Äquivalenz, dass beide Implikationen gelten, also aus A folgt B und umgekehrt.

Eigenschaften bzw. Aussagen haben Wahrheitswerte, die wir beispielsweise mit "wahr" und "falsch" bezeichnen können. Mithilfe dieser Wahrheitswerte können wir anhand von so genannten *Wahrheitswertetabellen* schließlich auch formal die aussagenlogischen Verknüpfungen wie folgt definieren:

$\wedge$	w	f
w	w	f
f	f	f

$\vee$	w	f
w	w	w
f	w	f

$\Rightarrow$	w	f
w	w	f
f	w	w

$\Leftrightarrow$	w	f
w	w	f
f	f	w

Mithilfe dieser Wahrheitswertetabellen können wir auch schnell einfache Zusammenhänge nachprüfen. Dies werden wir aber später im Kapitel 11 noch detaillierter prüfen. An dieser Stelle geben wir einfache Zusammenhänge an, wie beispielsweise $\neg\,(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ und $\neg\,(A \vee B) \Leftrightarrow \neg A \wedge \neg B$, aber auch $\neg \forall x A \Leftrightarrow \exists x \neg A$ und $\neg \exists x A \Leftrightarrow \forall x \neg A$.

Betrachten wir nun einfache Aussagen aus unserem täglichen (mathematischen) Leben und ihre Wahrheitswerte.

(a) Die Aussage "3 ist kleiner als 6" ist wahr.

(b) Die Aussage "Jede gerade natürliche Zahl größer als 2 ist Summe von zwei Primzahlen" ist wahr oder falsch. Allerdings ist bis heute nicht bekannt, welche der beiden Wahrheitswerte zutrifft.

(c) Die Aussagen "p ist ein Primteiler von 6" und "$p = 2 \vee p = 3$" sind äquivalent.

(d) Ist $\mathbb{Q}$ die Menge der rationalen Zahlen, so ist die Aussage

$$\forall q \in \mathbb{Q}\, \exists r \in \mathbb{Q}\ (r + r = q)$$

wahr, denn sie besagt, dass jede rationale Zahl durch 2 teilbar ist. Falsch dagegen ist die Aussage

$$\forall q \in \mathbb{Q}\, \exists r \in \mathbb{Q}\ (r \cdot r = q)\,,$$

denn sie besagt, dass jede rationale Zahl ein Quadrat ist. Um dies zu zeigen, benötigt man ein Gegenbeispiel, d.h. eine rationale Zahl, die kein Quadrat ist. Dies überlegen wir uns jetzt.

Satz 1.1. *Die reelle Zahl $\sqrt{2}$ ist nicht rational, mit anderen Worten: Die rationale Zahl 2 ist kein Quadrat einer rationalen Zahl.*

Beweis: Angenommen, 2 ist ein rationales Quadrat. Dann hat sie folgende Gestalt: $2 = (\frac{p}{q})^2$, wobei $p, q \in \mathbb{Z}$. Ohne Beschränkung der Allgemeinheit ("O.B.d.A.") seien p und q teilerfremd (sonst kürzten wir einen potentiellen gemeinsamen Teiler heraus). Unser Ziel ist es, einen Widerspruch zu finden.

Wir wissen $2 = (\frac{p}{q})^2 = \frac{p^2}{q^2}$. Also gilt $p^2 = 2q^2$. Somit ist p^2 gerade. Also ist auch p gerade nach $(\star)$. (Dies zeigen wir unabhängig im Anschluss dieses Beweises.) Damit hat p die Form $p = 2m$ für ein $m \in \mathbb{Z}$. Somit gilt $4m^2 = (2m)^2 = p^2 = 2q^2$, also auch $2m^2 = q^2$. Also ist q^2 gerade und damit nach $(\star)$ auch q. Hiermit sind sowohl p als auch q gerade und haben einen gemeinsamen Teiler, waren daher nicht teilerfremd. Widerspruch zur Annahme. Folglich gilt die Behauptung. ⊠

Beweis von $(\star)$: Wir beweisen die noch fehlende Aussage:

Für jede ganze Zahl q gilt: Ist q^2 gerade, so auch q.

Schauen wir uns zunächst folgende Aussage an:

Ist q ungerade, so auch q^2.

Letztere können wir direkt zeigen: Sei q eine ungerade Zahl, dann ist sie von der Gestalt $q = 2n + 1$ für ein $n \in \mathbb{Z}$, und es gilt

$$q^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1 = 2m + 1,$$

wobei wir $m := 2n^2 + 2n$ setzen. Damit ist q^2 wie gewünscht ungerade und die Behauptung $(\star)$ folgt durch die als Kontraposition bekannte Beweismethode. Dies wird im nächsten Abschnitt noch einmal näher betrachtet. $\boxtimes(\star)$

Schauen wir uns zwei wichtige *Beweismethoden* an, die wir im Folgenden immer wieder anwenden werden. Zum einen haben wir den *Widerspruchsbeweis*. Dieser beruht auf der Tatsache, dass $A \Rightarrow B$ und $\neg\,(A \wedge \neg B)$ äquivalent sind (leicht mittels Wahrheitswertetabelle überprüfbar, wie wir im Teil II sehen werden). Statt $A \Rightarrow B$ zu beweisen, zeigt man, dass $A \wedge \neg B$ falsch ist. Es wird daher $A \wedge \neg B$ zum Widerspruch geführt.

Eine weitere wichtige Beweismethode ist die *Kontraposition*, die auf der Tatsache beruht, dass $A \Rightarrow B$ und $\neg B \Rightarrow \neg A$ äquivalent sind. Äquivalenz bedeutet hier im Einzelfall nicht, dass beide Versionen der Behauptung gleich schwer zu beweisen sind; unter Umständen kann durchaus eine Variante einfacher sein als die andere, da man –wie im Beispiel von $(\star)$– dann vielleicht besser verwertbare Voraussetzungen zur Verfügung hat.

2. Mengen

In diesem Kapitel werden wir uns einfache Eigenschaften von Mengen anschauen, um den Umgang mit ihnen zu erlernen. Dabei werden wir keine Mengenlehre betreiben und nicht sagen, was Mengen eigentlich sind. Wir gehen naiv an die Sache heran und sehen Mengen als eine Ansammlung von Objekten, die eine gewisse Eigenschaft erfüllen – etwa die Menge der Studierenden der Informatik im ersten Semester in diesem Kurs.

Ist M eine Menge und x ein Element von M, so schreibt man $x \in M$; andernfalls $x \notin M$. Wir schreiben $\varnothing$ für die leere Menge, das heißt,

die Menge, die keine Elemente enthält. Eine uns auch bekannte Menge ist die Menge der natürlichen Zahlen, also $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Eine Menge A heißt *Teilmenge* einer Menge M, wenn jedes Element von A auch Element von M ist. Wir schreiben:

$$A \subseteq M \quad :\Longleftrightarrow \quad \forall x \in A\,(x \in M)$$

Gilt $A \subseteq M$ und $A \neq M$, so heißt A *echte Teilmenge* von M und wir schreiben in diesem Fall $A \subset M$ oder $A \subsetneq M$. Für jede Menge M gilt offenbar $M \subseteq M$ und $\varnothing \subseteq M$, denn würde $\forall x \in \varnothing\,(x \in M)$ nicht gelten, hätten wir $\neg(\forall x \in \varnothing\,(x \in M))$, also $\exists x \in \varnothing\,(x \notin M)$. Dies wäre ein Widerspruch, denn es gibt kein Element in der leeren Menge.

Eine wichtige Frage ist die nach der *Gleichheit von Mengen*. Stellen Sie sich vor, Sie haben fünf Äpfel einmal in einer weißen und einmal in einer roten Tüte verpackt. Da es jeweils (die gleichen) fünf Äpfel sind, würden Sie mir sicherlich zustimmen, dass es die gleiche Menge von Äpfeln ist – obwohl die Verpackung eine andere war. Dieses Konzept übertragen wir und sagen, dass zwei Mengen A und B gleich sind, also $A = B$, wenn sie die gleichen Elemente enthalten, das heißt, wenn beide Inklusionen, $A \subseteq B$ und $B \subseteq A$, gelten.

Weiterhin sagen wir: Ist für alle Elemente x aus M die Aussage bzw. Eigenschaft $\mathcal{A}(x)$ definiert, so ist

$$A := \{x \in M \mid \mathcal{A}\,(x)\}$$

eine Teilmenge von M und es gilt, dass jedes x aus M genau dann in A ist, wenn $\mathcal{A}(x)$ wahr ist.

Beispiel: $A = \{\, n \in \mathbb{N} \mid n \text{ ist ein Quadrat und } n \leq 10 \,\} = \{0, 1, 4, 9\}$

Definition 2.1. *Es seien A und B Teilmengen einer Menge M.*

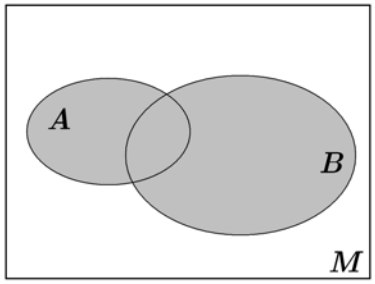
(a) *Die Menge $A \cup B := \{x \in M \mid x \in A \vee x \in B\}$ heißt die* Vereinigung *der Mengen A und B.*

(b) *Die Menge $A \cap B := \{x \in M \mid x \in A \wedge x \in B\}$ heißt der* Durchschnitt *der Mengen A und B.*

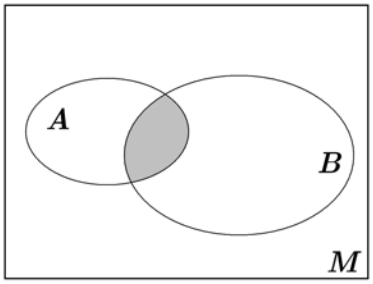
(c) *Die Menge $A \setminus B := \{x \in M \mid x \in A \wedge x \notin B\}$ heißt die* Differenz *der Mengen A und B.*

(d) *Die Menge* $A^c := M \setminus A$ *heißt das* Komplement *der Menge* A *bezüglich* M*.*

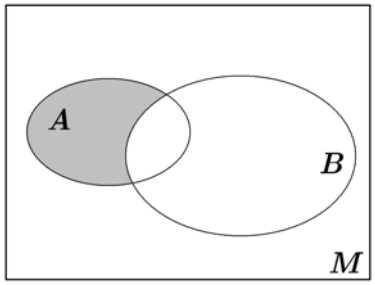
Folgende Abbildungen veranschaulichen die gerade definierten Begriffe in so genannten Venn-Diagrammen:



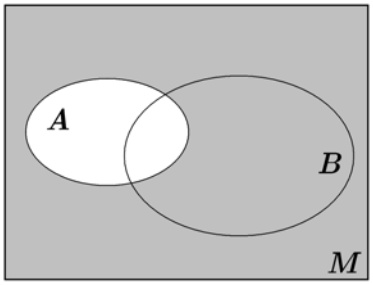
Vereinigung $A \cup B$



Durchschnitt $A \cap B$



Differenz $A \setminus B$



Komplement A^c

Schauen wir uns erste Eigenschaften an.

Satz 2.2. *Sind* A *und* B *Teilmengen der Menge* M*, so gilt*

(a) $(A \cup B)^c = A^c \cap B^c$

(b) $(A \cap B)^c = A^c \cup B^c$

Beweis: Wir beschränken uns darauf, die erste Gleichung zu zeigen. Dafür müssen wir beide geforderten Inklusionen zeigen:

$$(A \cup B)^c \subseteq A^c \cap B^c \text{ und } (A \cup B)^c \supseteq A^c \cap B^c$$

Fixiere x in M, so dass $x \in (A \cup B)^c$. Dann können wir schließen

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \Leftrightarrow \neg (x \in A \cup B) \\ &\Leftrightarrow \neg (x \in A \vee x \in B) \Leftrightarrow x \notin A \wedge x \notin B \\ &\Leftrightarrow x \in A^c \wedge x \in B^c \Leftrightarrow x \in A^c \cap B^c \end{aligned}$$

Da wir nur äquivalente Umformungen durchgeführt haben, sind damit beide Inklusionen gleichzeitig bewiesen.

Die zweite Gleichung folgt analog. ⊠

Einige andere wichtige Zusammenhänge sind in dem folgenden Satz zusammengefasst, den Sie zum Teil als Übungsaufgabe beweisen werden.

Satz 2.3. *Für beliebige Mengen A, B und C gilt*

Kommutativität:	$A \cup B = B \cup A, \qquad A \cap B = B \cap A$
Assoziativität:	$A \cup (B \cup C) = (A \cup B) \cup C =: A \cup B \cup C$
	$A \cap (B \cap C) = (A \cap B) \cap C =: A \cap B \cap C$
Distributivität:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Idempotenz:	$A \cup A = A, \qquad A \cap A = A$
Adjunktivität:	$A \cap (A \cup B) = A, \qquad A \cup (A \cap B) = A$
Komplementarität:	$A \cup A^c = M, \qquad A \cap A^c = \varnothing$

Wir können die Vereinigung und den Durchschnitt auch für mehr als zwei Mengen definieren:

Definition 2.4. *Sei I eine (Index-)Menge und für jedes $i \in I$ sei A_i eine Teilmenge der Menge M. Dann heißen*

- $\bigcup_{i\in I} A_i := \{x \in M \mid \exists i \in I\ (x \in A_i)\}$ *die* Vereinigung
- $\bigcap_{i\in I} A_i := \{x \in M \mid \forall i \in I\ (x \in A_i)\}$ *der* Durchschnitt

der Mengen A_i für $i \in I$.

Insbesondere gilt für $I = \{0, 1\}$ dann offenbar $\bigcup_{i\in I} A_i = A_0 \cup A_1$ und $\bigcap_{i\in I} A_i = A_0 \cap A_1$, so dass die Definition 2.4 als Verallgemeinerung der Definition 2.1 gesehen werden kann.

Betrachten wir folgende Beispiele: Es sei $I = \mathbb{N} \setminus \{0\}$ eine Indexmenge, sowie $A_i := \left\{x \in \mathbb{Q} \mid 0 < x < \frac{1}{i}\right\}$, so gilt $\bigcap_{i\in I} A_i = \varnothing$. Sei nun weiterhin $B_i := \left\{x \in \mathbb{Q} \mid 0 \leq x < \frac{1}{i}\right\}$. Dann überlegt man sich leicht, dass gilt $\bigcap_{i\in I} B_i = \{0\}$ und $\bigcup_{i\in I} A_i = A_1$ sowie die Mengengleichheit $\bigcup_{i\in I} B_i = B_1 = A_1 \cup \{0\}$.

Seien nun A und B Mengen sowie $a \in A$, $b \in B$. Dann heißt (a, b) das *geordnete Paar* von a und b. Sind $a, a' \in A$ und $b, b' \in B$, so definiert

man

$$(a, b) = (a', b') \;:\Leftrightarrow\; a = a' \wedge b = b'.$$

Alle geordneten Paare zweier Grundmengen fassen wir zusammen im so genannten *(Kreuz-)Produkt* der Mengen A und B, definiert durch

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

Entsprechend definiert man

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

als (endliches) (Kreuz-)Produkt der Mengen $A_1, \ldots, A_n$. Die Elemente $(a_1, \ldots, a_n)$ von $A_1 \times \cdots \times A_n$ heißen *n-Tupel*. Weiterhin definieren wir

$$A^n := \underbrace{A \times \cdots \times A}_{n\text{-mal}} = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in A\}.$$

Definition 2.5. *Ist $A \subseteq M$ eine Menge, so heißt die Menge aller Teilmengen von A die* Potenzmenge *von A (bezüglich M), geschrieben $\mathcal{P}(A)$, also gegeben durch $\mathcal{P}(A) := \{B \subseteq M \mid B \subseteq A\}$.*

Betrachten wir einfache Beispiele für Potenzmengen.

(a) Für $A = \varnothing$ gilt $\mathcal{P}(A) = \{\varnothing\}$. Denn angenommen es existiert eine weitere Teilmenge $B \neq \varnothing$, dann existiert ein $b \in B$, wobei $B \subseteq \varnothing$, also $b \in \varnothing$. Widerspruch!

(b) Für $A = \{a\}$ gilt $\mathcal{P}(A) = \{\varnothing, \{a\}\}$.

(c) Für $A = \{a, b\}$ gilt $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

Es gibt bei der Elementbeziehung "$\in$" Eigenschaften, an die Sie sich vielleicht erst gewöhnen müssen. So gilt offenbar die folgende Kette, gegeben durch $\varnothing \in \{\varnothing\} \in \{\{\varnothing\}\} \ldots$ oder wie die in Beispiel (b) gerade betrachtete Kette $a \in \{a\} \in \mathcal{P}(\{a\})$. Insbesondere sind Mengen selbst wieder Elemente größerer Mengen.

Weiterhin sagen wir, dass eine Menge A *endlich* ist, wenn es eine natürliche Zahl n und eine Aufzählung $f : \{0, \ldots, n-1\} \to A$ gibt. Wenn keine natürliche Zahl ausreicht, um eine Menge A aufzuzählen, das heißt, wenn für alle n keine solche Bijektion f existiert, dann nennen wir A *unendlich*. Wir werden in Kapitel 10 noch einmal darauf zurückkommen und verschiedene Arten der Unendlichkeit betrachten.

Ist A eine endliche Menge, so bezeichnet $|A|$ die *Anzahl der Elemente* von A. Hat A unendlich viele Elemente, so schreibt man auch $|A| = \infty$.

Satz 2.6. *Ist A eine endliche Menge mit n Elementen, so hat $\mathcal{P}(A)$ genau 2^n Elemente, das heißt, wenn $|A| = n$, so gilt $|\mathcal{P}(A)| = 2^n$.*

Bevor wir Satz 2.6 durch das Prinzip der *vollständigen Induktion* beweisen, soll diese Beweismethode kurz vorgestellt werden: Den Beweis durch vollständige Induktion können wir formal wie folgt zusammenfassen: Ist $\mathcal{A}(n)$ für alle $n \in \mathbb{N}, n \geq n_0$ eine Aussage, so ist $\mathcal{A}(n)$ für alle $n \in \mathbb{N}, n \geq n_0$ wahr, wenn folgendes gilt

- (Induktionsanfang) Es gelte $\mathcal{A}(n_0)$ für ein fixiertes $n_0 \in \mathbb{N}$.
- (Induktionsschritt) $\forall n \geq n_0 \; (\; \mathcal{A}(n) \Rightarrow \mathcal{A}(n+1) \;)$

Wir illustrieren das Prinzip der vollständigen Induktion am folgenden Beispiel:

$$\mathcal{A}(n): \quad 0 + 1 + 2 + \cdots + n \; = \; \frac{n \cdot (n+1)}{2}$$

Wir behaupten, dass für alle $n \in \mathbb{N}$ jeweils $\mathcal{A}(n)$ gelte.

Induktionsanfang. $\mathcal{A}(0): \quad 0 = \frac{1}{2} \cdot 0 \cdot (0+1)$
Also stimmt die Ausage für $n = 0$.

Induktionsschritt. Wir zeigen den Übergang $\mathcal{A}(n) \Rightarrow \mathcal{A}(n+1)$:

$$\begin{aligned}
0 + 1 + 2 + \cdots + n + (n+1) &= (0 + 1 + 2 + \cdots + n) + n + 1 \\
&= \left(\frac{1}{2} \cdot n \cdot (n+1) \right) + (n+1) \\
&= \frac{1}{2} \cdot n \cdot (n+1) + (n+1) \\
&= (n+1) \cdot \left(\frac{1}{2} \cdot n + 1 \right) \\
&= (n+1) \cdot \frac{1}{2} \cdot (n+2) \\
&= \frac{1}{2} \cdot (n+1) \cdot ((n+1)+1) \, .
\end{aligned}$$

Beim zweiten Gleichheitszeichen benutzten wir die Induktionsvoraussetzung. Damit ist die Behauptung des Beispiels bewiesen.

In der Analysisvorlesung werden Sie für solche Summen eine Abkürzungen einführen. Wir schreiben kurz $\sum_{i=0}^{n} i = 0 + 1 + 2 + \cdots + n$ bzw.

für ganze Zahlen i_0 und i_1 sowie Abbildungsvorschriften f allgemein

$$\sum_{i=i_0}^{i_1} f(1) = f(i_0) + f(i_0+1) + \cdots + f(i_1-1) + f(i_1).$$

In dieser Schreibweise lässt sich die gerade bewiesene Aussage als

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

ausdrücken. Andere Beispiele für häufig genutzte Summationsformeln, die man ebenfalls leicht per Induktion zeigen kann, sind etwa die folgenden:

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1) \qquad \sum_{i=1}^{n} i^3 = \frac{1}{4}n^2(n+1)^2$$

$$\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q} \text{ für } q \neq 1 \qquad \sum_{i=n}^{2n-1} \frac{1}{i} = \sum_{i=1}^{2n-1} \frac{(-1)^{i+1}}{i}$$

Vergessen wir aber nicht, den noch ausstehenden Satz zu beweisen:

Beweis von Satz 2.6: Zunächst betrachten wir den Induktionsanfang $\mathcal{A}(0)$. Wenn $|A| = 0$, so ist A die leere Menge und somit gilt $\mathcal{P}(A) = \{\varnothing\}$. Damit haben wir aber auch wie gewünscht, dass $|\mathcal{P}(A)| = 1 = 2^0$. Kommen wir zum Induktionsschritt und zeigen den Übergang von $\mathcal{A}(n)$ zu $\mathcal{A}(n+1)$: Sei dafür A eine Menge mit der Mächtigkeit $|A| = n+1$; dann hat A etwa die Gestalt $A = \{a_1, \ldots, a_n, a_{n+1}\}$. Definiere nun $A' := \{a_1, \ldots, a_n\}$. Dann gilt offenbar $|A'| = n$ und die Induktionsvoraussetzung ist anwendbar, so dass wir wissen $|\mathcal{P}(A')| = 2^n$. Dabei nehmen wir an, die Menge habe folgende Gestalt $\mathcal{P}(A') = \{M_1, \ldots, M_{2^n}\}$. Die M_i sind genau die Teilmengen von A, die a_{n+1} *nicht* enthalten. Es folgt daher

$$\mathcal{P}(A) \;=\; \{M_1, \ldots, M_{2^n}, M_1 \cup \{a_{n+1}\}, \ldots, M_{2^n} \cup \{a_{n+1}\}\}$$

das heißt, es gilt $|\mathcal{P}(A)| = |\mathcal{P}(A')| + |\mathcal{P}(A')| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ und der Induktionsbeweis ist vollständig geführt. ☒(Satz 2.6)

3. Abbildungen und Relationen

Sind A und B Mengen, so heißt eine Vorschrift f, die jedem a aus A genau ein b aus B zuordnet, eine *Abbildung* oder *Funktion* von A nach B, geschrieben $f : A \to B$. Wird einem a aus A das Element b aus B zugeordnet, so schreibt man dafür $a \mapsto b$ oder $f(a) = b$. Dabei heißt A der *Definitionsbereich* von f und B der *Bildbereich* oder *Wertebereich* von f. Funktionen haben also eine Eindeutigkeitseigenschaft in ihrer Vorschrift: Es ist nicht möglich, dass einem a aus A mehr als ein b aus B zugeordnet wird.

Wie auch schon bei Mengen ist es eine wichtige Frage, wann zwei Funktionen als gleich anzusehen sind. Wir sagen daher, dass zwei Funktionen $f : A \to B$, $f' : A' \to B'$ *gleich* heißen, wenn gilt $A = A'$ und $f(a) = f'(a)$ für alle $a \in A = A'$.

Betrachten wir beispielsweise die Abbildungen

$$f : \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto \frac{1}{2}\left(1 - (-1)^x\right) \quad \text{und}$$

$$g : \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto \begin{cases} 0 & \text{falls } x \text{ gerade,} \\ 1 & \text{falls } x \text{ ungerade.} \end{cases}$$

Dann sind diese beiden Abbildungen f und g gleich.

Definition 3.1. *Ist $f : A \to B$ eine Abbildung, so heißt*

$$f[A] := \{b \in B \mid \exists a \in A \ (f(a) = b)\}$$

das Bild von f. Außerdem heißt für eine Teilmenge $B' \subseteq B$

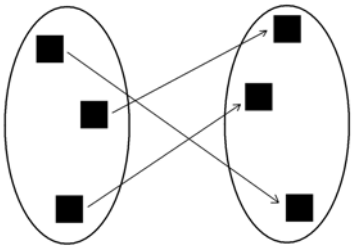
$$f^{-1}[B'] := \{a \in A \mid f(a) \in B'\} = \{a \in A \mid \exists b \in B' \ (f(a) = b)\}$$

die Menge der Urbilder von B' unter f.

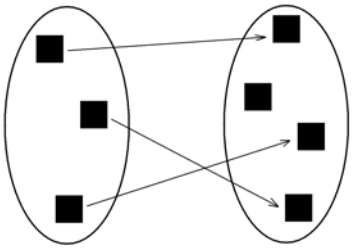
Es ist sofort klar, dass $f[A] \subseteq B$ und $f^{-1}[B'] \subseteq A$.

Definition 3.2. *Wir sagen, dass eine Abbildung f surjektiv ist, wenn $f[A] = B$, das heißt, wenn es zu jedem $b \in B$ ein $a \in A$ mit $f(a) = b$ gibt. Weiterhin heißt f injektiv, wenn für alle a und a' aus A gilt: Aus $f(a) = f(a')$ folgt immer schon $a = a'$. Und schließlich heißt eine Abbildung $f : A \to B$ bijektiv, wenn f injektiv und surjektiv ist.*

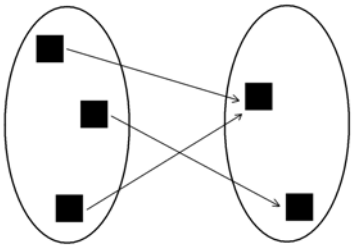
Surjektivität bedeutet, dass jedes Element im Bildbereich auch mit der Abbildung erreicht werden kann. Injektivität bedeutet gerade, dass zwei Elemente aus A nicht auf dasselbe Element in B abgebildet werden können. Folgende Abbildungsschemata veranschaulichen dies ein wenig:



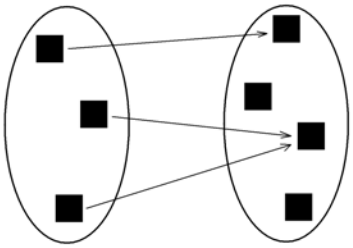
injektiv, surjektiv



injektiv, nicht surjektiv



nicht injektiv, surjektiv



nicht injektiv, nicht surjektiv

Schauen wir uns darüber hinaus folgende Beispiele an: $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Dann ist $f[\mathbb{R}] = \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ das Bild von f. Insbesondere ist f nicht surjektiv; aber auch nicht injektiv, da -1 und 1 beide auf 1 abgebildet werden. Dagegen gilt für $g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^3$ offenbar $g[\mathbb{R}] = \mathbb{R}$ und somit ist g surjektiv. Die Abbildung ist sogar injektiv. Somit ist g insbesondere bijektiv.

Stellen Sie sich vor, Sie möchten Abbildungen hintereinander anwenden, um auf diese Art komplizierte Abbildungen aus einfacheren zusammenzusetzen. Wir befassen uns daher jetzt mit der so genannten *Komposition von Abbildungen*. Sind $f : A \to B$ und $g : B' \to C$ für $f[A] \subseteq B'$ Abbildungen, so definiert man $g \circ f : A \to C$ durch die Vorschrift $a \mapsto g(f(a))$. Wir sagen zu $g \circ f$ auch "g nach f". Dabei heißt $g \circ f$ die *Komposition* von g und f.

Betrachten wir etwa folgende Abbildungen: Es sei $f : \mathbb{Z} \to \mathbb{N}$, $z \mapsto z^2$ und $g : \mathbb{N} \to \mathbb{Z}$, $n \mapsto 2n - 9$. Dann ist $g \circ f : \mathbb{Z} \to \mathbb{Z}$ gegeben durch die Vorschrift $z \mapsto 2z^2 - 9$ und $f \circ g : \mathbb{N} \to \mathbb{N}$ gegeben durch die Vorschrift $n \mapsto (2n - 9)^2 = 4n^2 - 36n + 81$. Dieses Beispiel zeigt auch, dass im Allgemeinen keine Kommutativität der Komposition gilt; wie etwa hier in diesem Beispiel: $f \circ g \neq g \circ f$.

Satz 3.3. *Sind $f : A \to B$ und $g : B \to C$ Abbildungen, so gilt*

(a) *Sind f, g surjektiv, so auch $g \circ f$.*
(b) *Sind f, g injektiv, so auch $g \circ f$.*
(c) *Sind f, g bijektiv, so auch $g \circ f$.*

Beweis: Die Beweise sind sehr einfach. Wir beweisen zunächst (a). Wir wissen nach Voraussetzung, es gibt zu jedem $c \in C$ ein $b \in B$ mit $g(b) = c$, da g surjektiv ist. Außerdem gibt es zu diesem $b \in B$ ein $a \in A$ mit $f(a) = b$, da f surjektiv ist. Also gilt $(g \circ f)(a) = g(f(a)) = g(b) = c$, so dass es zu jedem $c \in C$ ein $a \in A$ mit $(g \circ f)(a) = c$ gibt. Somit ist $g \circ f$ surjektiv.

Für (b) sei $(g \circ f)(a) = (g \circ f)(a')$, dann gilt offenbar $g(f(a)) = g(f(a'))$. Nun ist g injektiv, so dass $f(a) = f(a')$ gilt. Und da f ebenfalls injektiv ist, gilt schließlich $a = a'$. Also ist $g \circ f$ injektiv.

Der dritte Teil (c) ist sofort klar mit (a) und (b). ⊠

Als Übungsaufgabe überlasse ich Ihnen den Beweis des folgenden Satzes:

Satz 3.4. *Es seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen. Dann gilt*

(a) *Wenn g injektiv und $g \circ f : A \to C$ surjektiv, so ist f surjektiv.*
(b) *Wenn f surjektiv und $g \circ f : A \to C$ injektiv, dann ist auch g injektiv.*

Für eine Menge C nennen wir die Abbildung $\mathrm{id}_C : C \to C$, gegeben durch die Vorschrift $c \mapsto c$ die *identische Abbildung* auf C. Damit können wir folgenden Satz formulieren:

Satz 3.5. *Eine Abbildung $f : A \to B$ ist genau dann bijektiv, wenn es eine Abbildung $g : B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$ gibt.*

Beweis: Dies ist eine Äquivalenz. Wir müssen daher beide Richtungen zeigen. Zunächst kümmern wir uns um die Richtung von links nach rechts: Es sei also f bijektiv. Da f insbesondere surjektiv ist, existiert zu jedem $b \in B$ ein $a \in A$ mit $f(a) = b$. Da f darüber hinaus auch injektiv ist, ist dieses a eindeutig. Dies ist klar: Angenommen es gäbe a' mit $f(a') = b = f(a)$. Dann folgt sofort $a = a'$.

Sei nun $g : B \to A$ die Funktion, die jedem $b = f(a)$ genau dieses (eindeutig bestimmte) a zuordnet. Dann gilt $(g \circ f)(a) = g(f(a)) = a = \mathrm{id}_A(a)$. Also auch $g \circ f = \mathrm{id}_A$.

Für die zweite Gleichung beobachten wir, dass sich jedes $b \in B$ in der Form $b = f(a)$ schreiben lässt, also gilt $(f \circ g)(b) = f(g(b)) = f(g(f(a))) = f(a) = b = \mathrm{id}_B(b)$ und somit $f \circ g = \mathrm{id}_B$.

Wir zeigen nun die Richtung von rechts nach links: Für jedes $b \in B$ gilt zunächst $b = \mathrm{id}_B(b) = f(g(b)) \in f[A]$, somit ist f surjektiv. Andererseits folgt für $a, a' \in A$ mit $f(a) = f(a')$ trivialerweise, dass $g(f(a)) = g(f(a'))$, so dass wir schließlich

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = (g \circ f)(a') = \mathrm{id}_A(a') = a'$$

haben. Also gilt $a = a'$, so dass f injektiv ist. ⊠

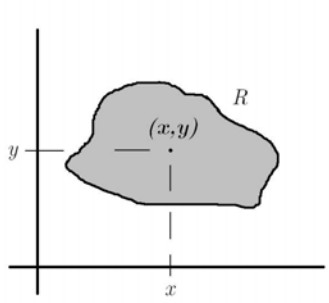
Wir gehen jetzt einen Schritt weiter und betrachten so genannte Relationen.

Definition 3.6. *Wir sagen:*

(a) *R ist eine n-stellige Relation, wenn R eine Menge von n-Tupeln ist. Statt $(x_0, \ldots, x_n) \in R$ schreiben wir auch $R(x_0, \ldots, x_n)$. Im Fall $n = 2$ schreiben wir statt $R(x, y)$ auch xRy (und somit die bekannte Infix-Notation).*

(b) *R ist eine Relation auf A und B, wenn $R \subseteq A \times B$. R ist eine zweistellige Relation auf A, wenn $R \subseteq A \times A$.*

Zweistellige Relationen lassen sich 2-dimensional graphisch darstellen; dabei kann eine Relation mit ihrem Graphen identifiziert werden.



Bekommen Sie ein Gefühl dafür und stellen Sie als Übungsaufgabe die Relation "$<$" auf $\mathbb{R}$ graphisch dar.

Wir definieren nun wichtige Eigenschaften von Relationen, die wir im Folgenden immer wieder benutzen werden:

Definition 3.7. *Für eine zweistellige Relation R auf A sagen wir:*

(a) R *ist* **symmetrisch**, *wenn* $\forall a, b \in A\ (aRb \to bRa)$

(b) R *ist* **antisymmetrisch**, *wenn* $\forall a, b \in A\ ((aRb \wedge bRa) \to a = b)$

(c) R *ist* **reflexiv**, *wenn* $\forall a \in A\ (aRa)$

(d) R *ist* **transitiv**, *wenn* $\forall a, b, c \in A\ ((aRb \wedge bRc) \to aRc)$

(e) R *ist eine* **Äquivalenzrelation**, *wenn R symmetrisch, reflexiv und transitiv ist.*

Schauen wir uns bekannte Relationen an: Offensichtlich ist "$=$" symmetrisch, "$\leq$" und "$\subseteq$" sind antisymmetrisch. Nun ist "$\leq$" reflexiv, "$<$" dagegen nicht. Darüber hinaus ist "$\neq$" nicht transitiv.

Die bereits eingeführten Funktionen können als spezielle Relationen aufgefasst werden. Funktionen von A nach B sind Relationen auf $A \times B$, bei denen jedem $a \in A$ genau ein $b \in B$ zugeordnet ist.

Konkret können wir sagen: Eine Relation R ist eine Funktion von A nach B, geschrieben als $R : A \to B$, wenn

$$\forall\, a \in A\ \exists\, b \in B\ (\, aRb \wedge (\, \forall\, b' \in B\ (\, aRb' \to b = b'\,)))\,.$$

Zusätzlich gilt: Eine Relation R ist eine injektive Funktion von A nach B, wenn

$$R : A \to B\ \wedge\ \forall\, a, a' \in A\ \forall\, b, b' \in B\ ((\, aRb \wedge a'Rb' \wedge a \neq a'\,) \to b \neq b'\,);$$

und R ist eine surjektive Funktion von A nach B, wenn

$$R : A \to B \ \wedge \ \forall\, b \in B \ \exists a \in A \ (\, aRb\,).$$

Damit haben wir unsere bisherigen Definitionen formalisiert.

Definition 3.8. *Sei R eine Äquivalenzrelation auf A. Für $a \in A$ ist*

$$[\![a]\!] := [\![a]\!]_R := \{b \in A \mid bRa\}$$

die Äquivalenzklasse *von a bezüglich R.*

Sie kennen die Äquivalenzklasse der durch 3 teilbaren Zahlen; diese ist gleich der Menge $\{0, 3, 6, \dots\}$. Die Menge $\{1, 4, 7, 10, \dots\}$ ist die Menge der Zahlen, die bei der Division durch 3 den Rest 1 lassen. Daher ist letztere repräsentiert durch $[\![1]\!]$ und es gilt offenbar $[\![1]\!] = [\![373]\!]$. Hierbei ist R definiert durch: aRb, wenn $a - b$ durch 3 teilbar ist.

Satz 3.9. *Sei R eine Äquivalenzrelation auf A. Dann gilt*

(a) $\forall\, a, b \in A \ (\, [\![a]\!] = [\![b]\!] \vee [\![a]\!] \cap [\![b]\!] = \varnothing \,)$.
(b) $A = \bigcup_{a \in A} [\![a]\!]$.

Beweis: zu (1): Seien $a, b \in A$. Betrachten wir zunächst den Fall: aRb. Wir werden nun zeigen, dass in diesem Fall $[\![a]\!] = [\![b]\!]$ gilt. Dafür zeigen wir zunächst, dass $[\![a]\!] \subseteq [\![b]\!]$ gilt: Sei $x \in [\![a]\!]$, das heißt nach Definition xRa. Wegen Transitivität und xRa, aRb gilt xRb. Also nach Definition $x \in [\![b]\!]$. Analog zeigt man $[\![b]\!] \subseteq [\![a]\!]$ und der erste Fall ist erfolgreich abgehandelt.

Betrachten wir den verbleibenden Fall $(a, b) \notin R$, also $(a \not R b)$. Wir zeigen nun, dass in diesem Fall $[\![a]\!] \cap [\![b]\!] = \varnothing$ gilt und führen einen Beweis durch Widerspruch: Angenommen es gibt ein $x \in [\![a]\!] \cap [\![b]\!]$, so gilt $x \in [\![a]\!]$ und $x \in [\![b]\!]$, also xRa und xRb. Wegen Symmetrie gilt insbesondere auch aRx und xRb. Und folglich gilt aRb wegen der Transitivität von R. Widerspruch! Damit ist (1) vollständig bewiesen.

Um (2) zu beweisen, zeigen wir zunächst: $A \subseteq \bigcup_{a \in A} [\![a]\!]$. Sei dafür $\bar{a} \in A$. Insbesondere gilt dann $\bar{a} R \bar{a}$, also $\bar{a} \in [\![\bar{a}]\!] \subseteq \bigcup_{a \in A} [\![a]\!]$, also $\bar{a} \in \bigcup_{a \in A} [\![a]\!]$. Es bleibt noch zu zeigen: $\bigcup_{a \in A} [\![a]\!] \subseteq A$. Dies ist aber klar, weil $\forall\, a \in A \ (\, [\![a]\!] \subseteq A \,)$. ⊠

Achtung: Achten Sie bei Beweisen mit Fallunterscheidungen immer darauf, dass *alle* Fälle abgedeckt werden!

4. Gruppen, Ringe, Körper

Wenn wir uns die bekannten Zahlbereiche mit den dazugehörigen Operationen anschauen, so können wir Eigenschaften erkennen, die immer wieder auftauchen – etwa die Kommutativität der Addition. Auf der anderen Seite können wir auch Unterschiede erkennen; so gibt es bei den ganzen Zahlen zwar im Gegensatz zu den natürlichen Zahlen immer additive Inverse, aber im Gegensatz zu den rationalen Zahlen keine multiplikativen Inverse. Um hier Ordnung in die Begrifflichkeiten zu bringen, führen wir der Reihe nach Strukturbegriffe ein, die immer wieder gemeinsam auftretende Eigenschaften zusammenfassen. Diesen werden wir noch oft begegnen.

Definition 4.1. *Für eine Menge A heißt eine Abbildung $\circ\colon A\times A \to A$, $(a, a') \mapsto a \circ a'$ Verknüpfung auf A. Eine Verknüpfung heißt*

- *assoziativ, wenn für alle $a, b, c \in A$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$;*
- *kommutativ, wenn für alle $a, b \in A$ gilt $a \circ b = b \circ a$.*

Betrachten wir ein bekanntes Beispiel: Sei A die Menge der reellen Zahlen. Die Addition und Multiplikation sind assoziative und kommutative Verknüpfungen auf $\mathbb{R}$. Die Subtraktion $a \circ b = a - b$ ist weder assoziativ noch kommutativ, denn es gilt

$$0 \circ (0 \circ 1) \;=\; 0 - (0 - 1) \;=\; 1 \;\neq\; -1 \;=\; (0 - 0) - 1 \;=\; (0 \circ 0) \circ 1$$
$$1 \circ 0 \;=\; 1 - 0 \;=\; 1 \;\neq\; -1 \;=\; 0 - 1 \;=\; 0 \circ 1$$

Man kann mit vollständiger Induktion zeigen, dass bei einer assoziativen Verknüpfung die Verknüpfung von n Elementen unter Beibehaltung der Reihenfolge unabhängig von der Klammerung ist. Somit können bei einer assoziativen Verknüpfung Klammern weggelassen werden.

Definition 4.2. *Ist A eine Menge mit einer Verknüpfung "$\circ$", so heißt $e \in A$ neutrales Element oder Einselement, wenn für alle $a \in A$*

$$e \circ a = a \circ e = a.$$

Gibt es ein neutrales Element e, so ist es eindeutig bestimmt, denn ist e' auch ein neutrales Element, so gilt $e' = e' \circ e = e$.

Betrachten wir diesmal die rationalen Zahlen: $A = \mathbb{Q}$. Dann ist die Zahl 0 das neutrale Element der Addition und die Zahl 1 das neutrale Element der Multiplikation.
Gehen wir nun einen Schritt weiter und betrachten eine beliebige (nichtleere) Menge M und die Menge A der Abbildungen $f : M \to M$, so ist $\mathrm{id}_M : M \to M$, $m \mapsto m$ das neutrale Element bezüglich der Komposition. Dies sieht man wie folgt: Für alle $f \in A$ gilt $f \circ \mathrm{id}_M = f$ und $\mathrm{id}_M \circ f = f$, da für alle $m \in M$ gilt $(f \circ \mathrm{id}_M)(m) = f(\mathrm{id}_M(m)) = f(m)$ und $(\mathrm{id}_M \circ f)(m) = \mathrm{id}_M(f(m)) = f(m)$.

Definition 4.3. *Es sei A eine Menge mit einer Verknüpfung "$\circ$" und einem neutralen Element e. Ist $a \in A$, so heißt $b \in A$ inverses Element oder Inverses von a, wenn $a \circ b = b \circ a = e$ gilt. Existiert für a ein Inverses, so heißt a invertierbar oder Einheit.*

Bezüglich der Addition besitzen die ganzen Zahlen offensichtlich als neutrales Element die Zahl 0 und es ist sogar jedes $a \in \mathbb{Z}$ invertierbar. Bezüglich der Multiplikation ist bei den ganzen Zahlen die Zahl 1 das neutrale Element, aber nur die Zahlen 1 und -1 sind invertierbar.

Satz 4.4. *Ist A eine Menge mit einer assoziativen Verknüpfung "$\circ$" und einem neutralen Element e, so gibt es zu jedem invertierbaren Element $a \in A$ genau ein $b \in A$ mit $a \circ b = e$ und $b \circ a = e$.*

Beweis: Sind b, b' Inverse von a, so gilt $b = e \circ b = (b' \circ a) \circ b = b' \circ (a \circ b) = b' \circ e = b'$. ⊠

Das unter den Voraussetzungen von Satz 4.4 eindeutig bestimmte Inverse von a wird mit a^{-1} bezeichnet.

Definition 4.5. *Ist G eine Menge und "$\circ$" eine Verknüpfung auf G, so heißt G Gruppe (bzgl. "$\circ$"), wenn gilt*

(a) *"$\circ$" ist assoziativ.*
(b) *Es existiert ein neutrales Element $e \in G$.*
(c) *Jedes $g \in G$ ist invertierbar.*

Ist weiterhin "$\circ$" kommutativ, so heißt G abelsche Gruppe.

Offensichtlich bilden die ganzen Zahlen bezüglich der Addition eine abelsche Gruppe. Darüber hinaus bilden die reellen Zahlen zusammen mit der Multiplikation keine Gruppe; dagegen ist $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ bezüglich der Multiplikation eine abelsche Gruppe.

Achtung: Eine Verknüpfung "$\circ$" auf G bedeutet, dass "$\circ$" eine Abbildung von $G \times G$ nach G ist, also $\circ : G \times G \to G$, insbesondere ist eine Verknüpfung immer abgeschlossen innerhalb der Menge und kann also nicht aus der Grundmenge G herausführen. Dies dürfen Sie bei einem Nachweis der Gruppeneigenschaften nicht vergessen – wie auch der Beweis der folgenden Aussage zeigt:

Satz 4.6. *Ist M eine Menge mit einer assoziativen Verknüpfung "$\circ$" und einem neutralen Element e, so ist die Menge G der invertierbaren Elemente von M bezüglich "$\circ$" eine Gruppe.*

Ist M selbst eine Gruppe, so gilt offenbar $M = G$.

Beweis von Satz 4.6: Wir zeigen zunächst, dass die auf M gegebene Verknüpfung "$\circ$" auch eine Verknüpfung auf G ist – eigentlich zeigen wir dies für die Einschränkung von "$\circ$" auf $G \times G$. Wir weisen also nach, dass für alle $a, b \in G$ stets gilt $a \circ b \in G$: Seien a, b aus G, so sind diese invertierbar, also folgt $a^{-1}, b^{-1} \in M$. Wegen

$$\begin{aligned}(a \circ b) \circ (b^{-1} \circ a^{-1}) &= (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} \\ &= a \circ a^{-1} = e\end{aligned}$$

und analog

$$\begin{aligned}(b^{-1} \circ a^{-1}) \circ (a \circ b) &= (b^{-1} \circ (a^{-1} \circ a)) \circ b = (b^{-1} \circ e) \circ b \\ &= b^{-1} \circ b = e\end{aligned}$$

ist $a \circ b$ invertierbar, also $a \circ b \in G$.

Die restlichen drei Gruppeneigenschaften folgen unmittelbar: Die Aussage $(a \circ b) \circ c = a \circ (b \circ c)$ gilt sogar für alle $a, b, c \in M$, insbesondere für $G \subseteq M$. Wegen $e \circ e = e$ gilt $e \in G$ und e ist damit insbesondere das neutrale Element von G. Schließlich gilt für alle $a \in G$ jeweils $a \circ a^{-1} = e$ und $a^{-1} \circ a = e$. Also ist auch a^{-1} in M invertierbar, das heißt $a^{-1} \in G$ und a ist das Inverse von a^{-1}. ⊠(Satz 4.6)

Wir haben sogar etwas mehr im letzten Beweis gezeigt: Für invertierbare Gruppenelemente a, b gilt $(a^{-1})^{-1} = a$ sowie $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Wir führen nun eine etwas mächtigere Struktur ein – den Ring.

Definition 4.7. *Ist R eine Menge mit den Verknüpfungen "$+$" und "$\cdot$", so heißt $(R, +, \cdot)$ Ring, wenn gilt*

(a) *R ist bzgl. "$+$" eine abelsche Gruppe,*

(b) *"$\cdot$" ist assoziativ,*

(c) *Es gelten die Distributivgesetze, das heißt, für alle $a, b, c \in R$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.*

Ist weiterhin "$\cdot$" kommutativ, so heißt R kommutativer Ring.
Hat ein Ring R ein neutrales Element bezüglich "$\cdot$", so heißt R Ring mit Eins und dann heißt weiterhin $a \in R$ invertierbar oder Einheit, wenn a bezüglich "$\cdot$" invertierbar ist.

Wir vereinfachen uns das Leben im Umgang mit Ringen und führen daher folgende Vereinbarungen ein:

- Punktrechung geht vor Strichrechnung, das heißt, um Produkte werden keine Klammern gesetzt.
- Das neutrale Element eines Ringes bezüglich "$+$" wird mit dem Symbol "0" bezeichnet.
- Ist R ein Ring mit Eins, so wird das neutrale Element der Multiplikation mit dem Symbol "1" bezeichnet. In diesem Falle ist $E(R) := \{a \in R \mid a \text{ Einheit in } R\}$ eine Gruppe bezüglich der Multiplikation (siehe Satz 4.4) und wird als *Einheitengruppe* bezeichnet.
- Für alle $a \in R$ bezeichnet $-a$ das Inverse von a bezüglich "$+$". Für alle $a, b \in R$ definiert man weiterhin $a - b := a + (-b)$.

Wir wissen, dass die ganzen Zahlen $\mathbb{Z}$ bezüglich der gewöhnlichen Addition und Multiplikation einen kommutativen Ring mit Eins bilden und es gilt $E(\mathbb{Z}) = \{1, -1\}$.

Beachten Sie, dass die Angabe der neutralen Elemente (sofern existent) mit den Symbolen 0 und 1 lediglich ein symbolischer Akt ist, der uns das Leben erleichtern soll. Welche Ring-Elemente dann letztendlich hinter diesen Symbolen stehen, geht dabei nicht hervor – insbesondere müssen

es nicht zwangsweise die Zahlen 0 und 1 sein. So können wir etwa eine einelementige Menge $R := \{0\}$ betrachten und auf eindeutige Art und Weise eine Addition und Multiplikation einführen, nämlich $0 + 0 = 0$ und $0 \cdot 0 = 0$. Mehr Möglichkeiten haben wir auch gar nicht, da nicht mehr Elemente zur Verfügung stehen. Wie Sie aber sehen können, ist in diesem Fall das einzige Element sowohl das neutrale Element der Addition als auch der Multiplikation, so dass in diesem Fall (in diesem Ring R) $0 = 1$ gilt. Solche pathologischen Fälle möchten wir insbesondere mit der nächsten Definition ausschließen:

Definition 4.8. *Ist K ein kommutativer Ring mit Eins, so heißt K Körper, wenn $0 \neq 1$ und jedes $a \in K$ mit $a \neq 0$ eine Einheit ist.*

Wir können feststellen, dass bezüglich der gewöhnlichen Addition und Multiplikation die bekannten Zahlbereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (und $\mathbb{C}$) kommutative Ringe mit Eins sind. Darüber hinaus sind $\mathbb{Q}, \mathbb{R}$ (und $\mathbb{C}$) sogar Körper, $\mathbb{Z}$ aber nicht.

Nachdem Sie nun wissen, wie die Strukturen heißen, werden exemplarisch interessante Eigenschaften in Ringen untersucht. Beachten Sie, dass die Eigenschaften, die wir jetzt nachweisen, in beliebigen (kommutativen) Ringen (mit Eins) gelten – nicht nur in den bekannten Ringen über die Zahlbereiche.

Satz 4.9. *Sei $(R, +, \cdot, 0, 1)$ ein kommutativer Ring mit Eins. Dann erfüllt R für beliebige $\lambda \in R$ die folgenden Bedingungen:*

(a) $0 \cdot \lambda = 0$
(b) $(-1) \cdot \lambda = -\lambda$
(c) $-(-\lambda) = \lambda$
(d) $(-1) \cdot (-1) = 1$

Beweis: Wir beweisen die erste Behauptung mit der folgenden Gleichungskette:

$$\begin{aligned}
0 \cdot \lambda &= \lambda \cdot 0 && \text{(Kommutativität der Mult.)} \\
&= \lambda \cdot 0 + 0 && \text{(Neutrales Element der Add.)} \\
&= \lambda \cdot 0 + (\lambda \cdot 0 + (-(\lambda \cdot 0))) && \text{(Inverses El. der Add.)} \\
&= (\lambda \cdot 0 + \lambda \cdot 0) + (-(\lambda \cdot 0)) && \text{(Assoziativität der Add.)}
\end{aligned}$$

$$
\begin{aligned}
&= \lambda \cdot (0+0) + (-(\lambda \cdot 0)) && \text{(Distributivität)}\\
&= \lambda \cdot 0 + (-(\lambda \cdot 0)) && \text{(Neutrales Element der Add.)}\\
&= 0 && \text{(Inverses Element der Add.)}
\end{aligned}
$$

Für die zweite Behauptung lässt sich ähnlich argumentieren:

$$
\begin{aligned}
(-1)\cdot\lambda &= (-1)\cdot\lambda + 0 && \text{(Neutrales Element der Add.)}\\
&= (-1)\cdot\lambda + (\lambda + (-\lambda)) && \text{(Inverses Element der Add.)}\\
&= ((-1)\cdot\lambda + \lambda) + (-\lambda) && \text{(Assoziativität der Add.)}\\
&= ((-1)\cdot\lambda + \lambda\cdot 1) + (-\lambda) && \text{(Neutrales El. der Mult.)}\\
&= (\lambda\cdot(-1) + \lambda\cdot 1) + (-\lambda) && \text{(Kommutativität der Mult.)}\\
&= (\lambda\cdot((-1)+1)) + (-\lambda) && \text{(Distributivität)}\\
&= \lambda\cdot 0 + (-\lambda) && \text{(Inverses Element der Add.)}\\
&= 0\cdot\lambda + (-\lambda) && \text{(Kommutativität der Mult.)}\\
&= 0 + (-\lambda) && \text{(nach (1))}\\
&= -\lambda && \text{(Neutrales Element der Add.)}
\end{aligned}
$$

Die restlichen beiden Teile bleiben eine Übungsaufgabe. ⊠

Das zweite Argument im letzten Beweis hätte man auch einfacher gestalten können. Wir kamen mittels einer längeren Gleichungskette durch Anwendung der Axiome schrittweise zum Ziel. Hierbei stand die Idee im Vordergund, Ihnen die Axiome in der Anwendung zu zeigen. In diesem speziellen Fall hätte man auch die Eindeutigkeit der Inversen ins Spiel bringen können, die wir uns nach Definition 4.2 überlegt hatten, und schließlich zeigen, dass

$$
\begin{aligned}
(-1)\cdot\lambda + \lambda &= \lambda\cdot(-1) + \lambda = \lambda\cdot(-1) + \lambda\cdot 1\\
&= \lambda\cdot((-1)+1) = \lambda\cdot 0 = 0
\end{aligned}
$$

gilt. Sie sehen, es führen viele Wege zum Ziel.

Abschließend stellen wir fest, dass wir auch die bekannten binomischen Formeln allgemein wie folgt in beliebige Ringe übertragen können:

Satz 4.10. *Sei $(R, +, \cdot, 0, 1)$ ein kommutativer Ring mit Eins. Dann gilt für alle λ und μ in R*

(a) $(\lambda+\mu)\cdot(\lambda+\mu) = \lambda\cdot\lambda + (1+1)\lambda\cdot\mu + \mu\cdot\mu$

(b) $(\lambda+(-\mu))\cdot(\lambda+(-\mu)) = \lambda\cdot\lambda + (-(1+1)\cdot\lambda\cdot\mu) + \mu\cdot\mu$

(c) $(\lambda + \mu) \cdot (\lambda + (-\mu)) = \lambda \cdot \lambda + (-\mu \cdot \mu)$

Beweis: Wir beschränken uns darauf, die erste Aussage zu beweisen. Die restlichen beiden bleiben eine (leichte) Übungsaufgabe. Wir geben jetzt auch nicht mehr im Detail an, welche Ringeigenschaft wir jeweils ausnutzen, sondern überlassen es dem geübten Auge des Lesers, dies zu erkennen.

Es gilt

$$\begin{aligned}
(\lambda + \mu) \cdot (\lambda + \mu) &= (\lambda + \mu) \cdot \lambda + (\lambda + \mu) \cdot \mu \\
&= \lambda \cdot (\lambda + \mu) + \mu \cdot (\lambda + \mu) \\
&= \lambda \cdot \lambda + (\lambda \cdot \mu + \mu \cdot \lambda) + \mu \cdot \mu \\
&= \lambda \cdot \lambda + (\mu \cdot \lambda + \mu \cdot \lambda) + \mu \cdot \mu \\
&= \lambda \cdot \lambda + (\mu \cdot \lambda \cdot 1 + \mu \cdot \lambda \cdot 1) + \mu \cdot \mu \\
&= \lambda \cdot \lambda + (\mu \cdot \lambda \cdot (1 + 1)) + \mu \cdot \mu \\
&= \lambda \cdot \lambda + (1 + 1) \cdot \mu \cdot \lambda + \mu \cdot \mu
\end{aligned}$$

⊠

5. Teilbarkeit und modulare Arithmetik

In diesem Kapitel werden wir spezielle Ringe untersuchen. Bisher haben wir die bekannten Zahlbereiche betrachtet, die alle unendlich sind. Wir werden uns jetzt endlichen Ringen und Körpern widmen, die insbesondere in der Informatik zu Kodierungszwecken eine Anwendung finden, wie wir in den nächsten Kapiteln sehen werden. Aber zunächst werden wir grundlegende Begriffe klären und arbeiten dabei innerhalb der ganzen Zahlen.

Definition 5.1. *Seien m und n ganze Zahlen. Dann definieren wir "m teilt n", wenn es ein $l \in \mathbb{Z}$ gibt mit $m \cdot l = n$. Wir schreiben in diesem Fall "m ist Teiler von n" bzw. $m|n$.*

Satz 5.2. *Es gelten folgende einfache Eigenschaften:*

(a) *Für jede ganze Zahl m gilt $1|m$ und $m|m$.*
(b) *Für alle ganzen Zahlen a, b und c mit $a|b$ und $b|c$ gilt $a|c$.*

Beweis: Die Aussagen in (a) sind offensichtlich wahr, da $1 \cdot m = m$ und $m \cdot 1 = m$. Wir zeigen die zweite Behauptung: Wegen $a|b$ existiert ein $l_1 \in \mathbb{Z}$ mit $a \cdot l_1 = b$. Wegen $b|c$ existiert $l_2 \in \mathbb{Z}$ mit $b \cdot l_2 = c$. Also gilt $c = b \cdot l_2 = (a \cdot l_1) \cdot l_2 = a \cdot (l_1 \cdot l_2) = a \cdot l$, wobei $l = l_1 \cdot l_2$. Damit ist $a|c$ bewiesen. ⊠

Da wir später darauf zurückgreifen werden, definieren wir jetzt formal, wann eine natürliche Zahl eine Primzahl ist.

Definition 5.3. *Sei p eine natürliche Zahl, dann heißt p eine Primzahl, wenn $p \neq 0$, $p \neq 1$ und für alle t mit $t|p$ gilt: $t = 1$ oder $t = p$.*

Erkennen Sie die Implikation in der Formulierung des letzten Teils der Definition? – Testen Sie sich und formalisieren Sie die Eigenschaft "n ist Primzahl" entsprechend der Definition.

Der nächste Satz wird uns die so genannte Division mit Rest garantieren, die wir im Folgenden ausnutzen werden.

Satz 5.4. *Sei n eine natürliche Zahl, $n \neq 0$. Dann gibt es für jede ganze Zahl a eindeutig bestimmte ganze Zahlen q und r, so dass $a = q \cdot n + r$ gilt, mit $0 \leq r < n$.*

Beweis: Sei n eine natürliche Zahl. Wie Sie sich leicht klarmachen können, ist $\mathbb{Z} = \bigcup_{q \in \mathbb{Z}} \{\, m \in \mathbb{Z} \mid q \cdot n \leq m \leq (q+1) \cdot n \,\}$.
Sei nun $a \in \mathbb{Z}$, so gibt es also ein $q \in \mathbb{Z}$ mit $q \cdot n \leq a \leq (q+1) \cdot n$. Definieren wir für dieses q nun $r := a - q \cdot n$, so gilt $a = q \cdot n + r$ und $0 \leq r < n$. Letzteres ergibt sich sofort, wenn Sie von $q \cdot n \leq a \leq (q+1) \cdot n$ die Zahl $q \cdot n$ subtrahieren. ⊠

Das heißt, dass wir jede natürliche Zahl durch n mit Rest r teilen können; dabei bezeichnet r den *Rest von a modulo n* und dieser wird mit $[a]_n$ bezeichnet. Wenn n im Kontext fixiert ist, schreiben wir manchmal auch nur $[a]$. Wir möchten nun mit Resten der Division rechnen und insbesondere Zahlen mit gleichen Resten (bei fixiertem n) identifizieren, so dass wir folgende Relation definieren:

Definition 5.5. *Seien a, b ganze Zahlen und n eine natürliche Zahl. Dann sei*

$$a \equiv b \ mod \ n,$$

wenn n ein Teiler der Differenz $a - b$ ist.

Wenn "$a \equiv b \bmod n$" gilt, spricht man dies als "a ist kongruent zu b modulo n". Insbesondere bedeutet es, dass a und b denselben Rest modulo n haben.

Satz 5.6. *Für fixiertes n ist die durch*

$$aRb \iff a \equiv b \bmod n$$

definierte Relation eine Äquivalenzrelation auf den ganzen Zahlen.

Den Beweis überlasse ich Ihnen als Übungsaufgabe. Mit unserer bisherigen Terminologie können wir feststellen, dass die folgende Gleichung gilt:

$$[-1]_3 = [5]_3 = [17]_3 = 2.$$

Aber für die so genannten Restklassen haben wir

$$\begin{aligned} [\![-1]\!]_3 &= [\![5]\!]_3 = [\![17]\!]_3 \\ &= \{\, a \in \mathbb{Z} \mid 3 \text{ ist ein Teiler von } (a - 17) \,\} \\ &= \{\ldots, -4, -1, 2, 5, \ldots, 17, \ldots\}. \end{aligned}$$

Sie müssen daher ganz genau wissen, worüber Sie sprechen und die Klammern entsprechend setzen. Ich gebe zu bedenken, dass diese Art der Unterscheidung der Klammern kein allgemeines Prinzip ist, welches Sie überall in der Literatur finden können. Das obige Beispiel soll lediglich den Unterschied zwischen beiden Betrachtungsweisen verdeutlichen, da wir beide Notationen benutzen werden.

Mithilfe dieser Äquivalenzrelation, gegeben durch die Möglichkeit der Division mit Rest, können wir nun Operationen auf einer endlichen Menge (der Reste) einführen.

Definition 5.7. *Sei n eine natürliche Zahl, $n \geq 2$. Wir definieren die Menge $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ und auf ihr folgende zwei Verknüpfungen:*

- *Die Addition modulo n ist die folgende Operation*

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad a \oplus_n b = [a + b]_n.$$

- *Die Multiplikation modulo n ist die folgende Operation*

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad a \otimes_n b = [a \cdot b]_n.$$

Diese modulare Arithmetik kennen Sie aus Ihrem täglichen Leben. Betrachten Sie etwa die Tageszeit. Dann ist dies formal die Addition modulo 24; so ist etwa $20 \oplus_{24} 8 = 4$ (Uhr). Oder betrachten Sie einfache 8-Bit Mikroprozessoren; diese benutzen die Arithmetik modulo $2^8 (= 256)$. Dabei gilt $100 \oplus_{256} 156 = 0$, das heißt, dass das additive Inverse von 100 bezüglich dieser Addition 156 ist und somit die Gleichung "$-100 = 156$" gilt.

Weiterhin gilt in $\mathbb{Z}_n$ immer $(-1) \otimes_n (-1) = 1$. Eigentlich können wir nicht über -1 sprechen, sondern müssten den Rest $[-1]$ betrachten; dieser entspricht dann $-1 \equiv n - 1 \bmod n$, so dass $[-1] = n - 1$ und damit gilt

$$\begin{aligned} [-1] \otimes_n [-1] &= (n-1) \otimes_n (n-1) = [\,(n-1) \cdot (n-1)\,] \\ &= [\,n^2 - 2n + 1\,] = [\,n \cdot (n-2) + 1\,] = 1. \end{aligned}$$

Betrachten wir den Spezialfall $n = 2$. In diesem Fall lauten die Additions- und Multiplikationstafeln wie folgt:

$\oplus_2$	0	1
0	0	1
1	1	0

$\otimes_2$	0	1
0	0	0
1	0	1

Vergleichen Sie nun diese Tafeln mit den Tafeln für die logischen Verknüpfungen "xor" und "und", die wir bereits gesehen haben – Sie erkennen, dass diese beiden jeweils korrespondieren.

xor	falsch	wahr
falsch	falsch	wahr
wahr	wahr	falsch

und	falsch	wahr
falsch	falsch	falsch
wahr	falsch	wahr

Betrachten wir abschließend etwas größere Verknüpfungstafeln, etwa für den Fall $n = 5$:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Wie Sie sehen können, sind diese Verknüfungen nicht nur assoziativ und kommutativ, sondern es gibt für beide Operationen neutrale Elemente und darüber hinaus sind alle Elemente (bis auf die Null bezüglich der Multiplikation) invertierbar. Ganz allgemein können wir festhalten:

Satz 5.8. *Für beliebige n ist $(\mathbb{Z}_n, \oplus, \otimes, 0, 1)$ ein kommutativer Ring mit Eins. Dabei ist $\mathbb{Z}_n$ genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis: Der Nachweis der Ringeigenschaften ist einfaches Nachrechnen. Für die zusätzliche Körpereigenschaft betreffs existierender Inverser zeigen wir nun beide geforderten Richtungen der Äquivalenz: Sei zunächst $n = p$ eine Primzahl, sowie $a \in \mathbb{Z}_p, a \neq 0$. Wegen $a \neq 0$ ist p kein Teiler von a. Da p eine Primzahl ist, haben a und p keine gemeinsamen Teiler außer der Eins, und es existieren $x, y \in \mathbb{Z}$ mit $ax+py = 1$. (Auf diese Stelle gehen wir hier nicht weiter ein. Die Existenz von x, y garantiert uns Lemma 6.3, welches wir im nächsten Kapitel beweisen werden.) Insbesondere heißt das aber, dass gilt $ax = -py+1$ und somit auch

$$a \cdot [x] = [a] \cdot [x] = [ax] = [\, -py + 1\,] = [\, p \cdot (-y) + 1\,] = 1.$$

Somit ist $[x]_p$ das gewünschte multiplikative Inverse zu a in $\mathbb{Z}_p$. Wegen $1 \neq 0$ ist $\mathbb{Z}_p$ damit ein Körper.

Sei nun andererseits n keine Primzahl. Gilt $n = 1$, so folgt $0 = 1$, das heißt, das neutrale Element der Addition ist gleich dem neutralen Element der Multiplikation. Somit ist $\mathbb{Z}_1$ kein Körper.

Sei daher im Folgenden $n > 1$. Dann existieren $a, b \in \mathbb{N}$ mit $n = a \cdot b$, $1 < a < n$ und $1 < b < n$, da n keine Primzahl ist. Also gilt $a \neq 0$, $b \neq 0$ und $a \otimes b = [a] \otimes [b] = [a \cdot b] = [n] = 0 \notin E(\mathbb{Z}_n)$. Folglich

ist a oder b keine Einheit in $\mathbb{Z}_n$, da wir schon aus dem Beweis von Satz 4.6 wissen, dass sonst $(ab)^{-1} = b^{-1}a^{-1}$ gelten würde und damit 0 invertierbar wäre. Damit ist $\mathbb{Z}_n$ insbesondere kein Körper. ⊠

6. Chinesischer Restsatz

Wir treffen nun die Vorbereitungen für das nächste Kapitel und arbeiten auf den so genannten Chinesischen Restsatz hin, der eine Aussage über die Lösbarkeit von Kongruenzsystemen macht. Als Grundlage dafür betrachten wir zunächst den Euklidischen Algorithmus.

Definition 6.1. *Seien $x, y \in \mathbb{Z}$. Dann heißt $d \in \mathbb{Z}$ größter gemeinsamer Teiler von x und y, wenn folgende zwei Bedingungen erfüllt sind:*

(a) *d ist gemeinsamer Teiler von x und y, das heißt, $d \mid x$ und $d \mid y$*

(b) *Für jeden weiteren gemeinsamen Teiler d' von x und y gilt $d' \mid d$; formalisiert: $\forall d' \, (\, (d' \mid y \wedge d' \mid x) \Rightarrow d' \mid d \,)$.*

Offensichtlich ist der größte gemeinsame Teiler zweier Zahlen mit der Einschränkung $d \geq 0$ eindeutig, so dass wir diesen für Zahlen x und y als

$$d = \mathrm{ggT}(x, y)$$

bezeichnen können. Weiterhin gilt

$$\mathrm{ggT}(\pm x, \pm y) = \mathrm{ggT}(x, y) \quad \text{und} \quad \mathrm{ggT}(0, 0) = 0.$$

Definition 6.2. *Zwei ganze Zahlen x und y sind teilerfremd, wenn $ggT(x, y) = 1$.*

Die Existenz des ggT zweier ganzer Zahlen ist durch den *Euklidischen Algorithmus* gesichert. Diesen werden wir jetzt angeben.

Es genügt den Fall $x \geq y > 0$ zu betrachten. Wir setzen $x_0 := x$ und $x_1 := y$ und führen nach folgendem Schema sukzessive Division mit Rest durch, bis sich der Rest 0 ergibt

$$\begin{aligned} x_0 &= q_1 \cdot x_1 + x_2, && \text{wobei } 0 < x_2 < x_1 \\ x_1 &= q_2 \cdot x_2 + x_3, && \text{wobei } 0 < x_3 < x_2 \\ &\vdots \end{aligned}$$

$$\begin{aligned} x_{n-2} &= q_{n-1} \cdot x_{n-1} + x_n, \qquad \text{wobei } 0 < x_n < x_{n-1} \\ x_{n-1} &= q_n \cdot x_n + 0. \end{aligned}$$

Da die Folge der Zahlen $x_1, x_2, \ldots$ streng monoton abnimmt, wird nach endlich vielen Schritten der Rest 0 erreicht.

Nun ist $d := x_n$ der größte gemeinsame Teiler von x und y – warum? Das können Sie sich wie folgt überlegen: Schauen Sie sich die Zeilen des Euklidischen Algorithmus an und Sie werden feststellen, dass $d = x_n$ ein Teiler von x_{n-1} ist. Damit ist aber auch d ein Teiler von x_{n-2}. Wiederholt man dieses Argument oft genug, folgt schließlich: d teilt $x_1 = y$ und d teilt auch $x_0 = x$.

Es bleibt also Bedingung (2) aus Definition 6.1 zu zeigen. Sei dazu d' ein beliebiger Teiler von $x = x_0$ und $y = x_1$. Wieder verrät ein Blick auf obige Zeilen unmittelbar: d' teilt auch x_2 und x_3 ... und x_n, insbesondere $d' \mid d$.

Wir führen ein Beispiel vor und berechnen $\mathrm{ggT}(238, 35)$ und initialisieren den Euklidischen Algorithmus mit $x := 238$ und $y := 35$. Dann erhalten wir

$$\begin{aligned} 238 &= 6 \cdot 35 + 28 \\ 35 &= 1 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Damit wissen wir, es gilt $\mathrm{ggT}(238, 35) = 7$.

Kommen wir nun zu einem vielleicht überraschenden und oft angewendeten Resultat:

Lemma 6.3. *Sind $x, y \in \mathbb{Z}$ und $d = \mathrm{ggT}(x, y)$, so existieren $m, n \in \mathbb{Z}$ mit $m \cdot x + n \cdot y = d$.*

Sind x, y teilerfremd, so schließt das Lemma die Lücke im Beweis von Satz 5.8, denn liefert genau $m, n \in \mathbb{Z}$ mit $m \cdot x + n \cdot y = 1$.

Beweis von Lemma 6.3: Wir haben bereits gesehen, wie wir mittels $x_0 := x$, $x_1 := y$ und dem Euklidischen Algorithmus d bestimmen können. Stellen Sie für alle $i \in \{0, \ldots, n-2\}$ die dabei entstandenen

Gleichungen in die Form $x_{i+2} = x_i - q_{i+1} \cdot x_{i+1}$ um, so erhalten Sie durch sukzessives (Rückwärts-)Einsetzen

$$\begin{aligned} d \;=\; x_n \;&=\; x_{n-2} - q_{n-1} \cdot x_{n-1} \\ &=\; x_{n-2} - q_{n-1} \cdot (x_{n-3} - q_{n-2} \cdot x_{n-2}) \\ &=\; -q_{n-1} \cdot x_{n-3} + (\,1 + q_{n-1}\, q_{n-2}\,) \cdot x_{n-2} \\ &=\; \ldots \;=\; m \cdot x_0 + n \cdot x_1 \;=\; m \cdot x + n \cdot y \end{aligned}$$

für arithmetische Ausdrücke m, n aus den q_i. ⊠(Lemma 6.3)

Das Lemma hat eine weitere nützliche Anwendung: Stellen Sie sich vor, Sie möchten das multiplikative Inverse eines x in $\mathbb{Z}_p$ bestimmen, wobei p eine Primzahl ist. Wie gehen Sie vor? Sehr schlau wäre der folgende Ansatz: Da p eine Primzahl ist, sind x und p teilerfremd und es gibt nach Lemma 6.3 ganze Zahlen m, n mit $m \cdot x + n \cdot p = 1$. Aber somit haben wir

$$\begin{aligned} [m] \otimes x \;&=\; [\,[m] \cdot x\,] \;=\; [\,(m + k{\cdot}p) \cdot x\,] \;=\; [\,m \cdot x + kx \cdot p\,] \\ &=\; [\,1 - n \cdot p + kx \cdot p\,] \;=\; [\,1 + (kx - n) \cdot p\,] \;=\; 1 \end{aligned}$$

für ein geeignetes $k \in \mathbb{Z}$; das heißt: Finden wir m, so auch das multiplikative Inverse von x in $\mathbb{Z}_p$ als dessen Rest modulo p. Wie Sie m ermitteln, haben Sie bereits im Beweis von Lemma 6.3 gesehen.

Schauen wir uns das folgende Beispiel an: Gesucht ist das multiplikative Inverse von 13 in $\mathbb{Z}_{89}$. Wir wollen also m, n mit $m \cdot 13 + n \cdot 89 = 1$ bestimmen. Der Euklidische Algorithmus liefert uns

$$\begin{aligned} 89 \;&=\; 6 \cdot 13 + 11 \\ 13 \;&=\; 1 \cdot 11 + 2 \\ 11 \;&=\; 5 \cdot 2 + 1 \\ 2 \;&=\; 2 \cdot 1 + 0 \end{aligned}$$

und durch sukzessives Rückwärtseinsetzen bekommen wir

$$\begin{aligned} 1 \;&=\; 11 - 5 \cdot 2 \;=\; 11 - 5 \cdot (13 - 1 \cdot 11) \\ &=\; 6 \cdot 11 - 5 \cdot 13 \;=\; 6 \cdot (89 - 6 \cdot 13) - 5 \cdot 13 \\ &=\; -41 \cdot 13 + 6 \cdot 89. \end{aligned}$$

Damit ist das Inverse von 13 in $\mathbb{Z}_{89}$ bezüglich der Multiplikation gegeben durch $[m] = [-41] = 48$.

Wir kommen jetzt im zweiten Teil des Kapitels zur ersten Anwendung der Kongruenzen.

Satz 6.4 (Chinesischer Restsatz)**.** *Sei $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$ das Produkt paarweise teilerfremder natürlicher Zahlen $n_1, \ldots, n_r$, wobei $n_i \geq 2$ für $i = 1, \ldots, r$. Dann ist $\mathbb{Z}_n$ isomorph zum direkten Produkt $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.*

Diese Formulierung findet man häufig in der Literatur, allerdings werden hierbei die Begriffe des direkten Produktes und der Isomorphie benutzt.

Unter dem direkten Produkt versteht man das Kreuzprodukt versehen mit den durch komponentenweise Anwendung der vorhandenen Verknüpfungen auf den $\mathbb{Z}_{n_i}$ für $i = 1, \ldots, r$ entstehenden Verknüpfungen "+" und "$\cdot$". Auch die neutralen Elemente sind in jeder Komponente das neutrale Element des jeweiligen $\mathbb{Z}_{n_i}$.

Den Begriff des Isomorphismus werden wir erst in Kapitel 14 allgemein einführen. Vorab sei nur kurz erwähnt, dass es bedeutet, dass zwischen den beiden betrachteten Strukturen $\mathbb{Z}_n$ und $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ eine Bijektion existiert und dass sich beide Strukturen samt der dazugehörigen Operationen, Addition und Multiplikation, kompatibel verhalten, das heißt, es ist egal, ob man zwei Zahlen in $\mathbb{Z}_n$ addiert und dann mittels der Bijektion zum direkten Produkt übergeht oder ob man jeweils erst zum direkten Produkt übergeht und dann dort addiert – man erhält das gleiche Ergebnis.

Wir werden eine andere, dazu äquivalente Version nützlich finden:

Satz 6.5 (Chinesischer Restsatz, andere Formulierung)**.** *Es seien nun $n_1, n_2, \ldots, n_r$ paarweise teilerfremde natürliche Zahlen und $a_1, a_2, \ldots, a_r$ beliebige ganze Zahlen. Dann gibt es genau eine natürliche Zahl x mit $0 \leq x \leq n_1 \cdot n_2 \cdot \ldots \cdot n_r - 1$, die das folgende Kongruenzsystem löst:*

$$x \equiv a_1 \mod n_1$$

$$\vdots$$

$$x \equiv a_r \mod n_r$$

Wir geben hier einen Lösungsalgorithmus an:

Schritt 1: Berechne $n := n_1 \cdot \ldots \cdot n_r$.

Schritt 2: Berechne $N_i := \frac{n}{n_i}$.

Schritt 3: Berechne die Inversen y_i wie folgt:

$$y_i \cdot N_i \equiv 1 \mod n_i.$$

Schritt 4: Setze $x := (\sum_i a_i\, y_i\, N_i) \bmod n = [\sum_i a_i\, y_i\, N_i]_n$.

Wie auch beim Euklidischen Algorithmus machen wir uns zunächst klar, dass dieser Algorithmus korrekt ist: Sei $j \in \{1, \ldots, r\}$, so ist zu zeigen $x \equiv a_j \bmod n_j$. Es ist für ein geeignetes $k \in \mathbb{Z}$

$$\begin{aligned} x - a_j &= \left(\sum_{i=1}^{r} a_i\, y_i\, N_i + k\, n \right) - a_j \\ &= \sum_{i=1,\, i \neq j}^{r} a_i\, y_i\, N_i + a_j\, (\, y_j\, N_j - 1\,) + k\, n. \end{aligned}$$

Betrachte zuerst alle Summanden $a_i\, y_i\, N_i$ für ein $i \neq j$. Dann

$$a_i\, y_i\, N_i = a_i\, y_i\, \frac{n}{n_i} = a_i\, y_i\, (\, n_1 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_r\,).$$

Da $i \neq j$, ist dies ein Vielfaches von n_j. Andererseits ist nach der Wahl von y_j in Schritt 3 auch $y_j\, N_j - 1$ –und damit ebenso $a_j\, (\, y_j\, N_j - 1\,)$– ein Vielfaches von n_j. Insgesamt erhalten wir wie gewünscht, dass n_j ein Teiler von $x - a_j$ ist.

Haben Sie bemerkt, dass wir die Teilerfremdheit von $n_1, \ldots, n_r$ dabei gar nicht benutzt haben? Diese braucht man jedoch, um in Schritt 3 die Existenz eines y_i mit der geforderten Eigenschaft zu garantieren! (siehe Lemma 6.3)

Schauen wir uns ein Beispiel an und betrachten das folgende System von Kongruenzen, wobei wir eine Lösung x suchen:

$$x \equiv 3 \mod 4$$

$$x \equiv 2 \mod 5$$

$$x \equiv 1 \mod 3$$

Nach Schritt 1 setzen wir $n := 4 \cdot 5 \cdot 3 = 60$. Nach Schritt 2 definieren wir $N_1 := \frac{60}{4} = 15$, $N_2 := \frac{60}{5} = 12$ und schließlich $N_3 = \frac{60}{3} = 20$. Nach Schritt 3 suchen wir $y_1 \cdot 15 \equiv 1 \bmod 4$ und finden etwa $y_1 = -1$; aber auch jedes andere Element von $[\![-1]\!]_4$ erfüllt die Bedingung. Analog suchen wir $y_2 \cdot 12 \equiv 1 \bmod 5$, also etwa $y_2 = -2$ und schließlich für $y_3 \cdot 20 \equiv 1 \bmod 3$ finden wir etwa $y_3 = -1$. Im Schritt 4 finden wir unsere gesuchte Lösung durch

$$x := [\, 3 \cdot (-1) \cdot 15 + 2 \cdot (-2) \cdot 12 + 1 \cdot (-1) \cdot 20 \,]_{60} = [-113]_{60} = 7.$$

Wählt man andere Repräsentanten, so ergibt sich beispielsweise für $y_2 := 3$ (denn $3 \in [\![-2]\!]_5$) die Rechnung

$$x = [\, 3 \cdot (-1) \cdot 15 + 2 \cdot 3 \cdot 12 + 1 \cdot (-1) \cdot 20 \,]_{60} = [7]_{60} = 7.$$

Eine kurze Probe bestätigt, dass 7 eine Lösung des gegebenen Systems von Kongruenzen ist.

An dieser Stelle schließen wir unsere Betrachtungen und gehen zur Anwendung des Ganzen im nächsten Kapitel über.

7. Der RSA-Algorithmus

Der so genannte RSA-Algorithmus ermöglicht eine vertrauliche Kommunikation ohne Schlüsselvereinbarung. Er wurde 1977 von den Herren Rivest, Shamir, Adleman entwickelt. Wir werden diesen Teil der Kryptographie als Anwendung der gerade entwickelten Grundlagen in der modularen Arithmetik bis hin zum Chinesischen Restsatz betrachten.

Schauen wir uns zunächst die *RSA-Schlüsselzerlegung* an. Der RSA-Schlüssel besteht aus zwei Teilen – einem öffentlichen Schlüssel zum Kodieren und einem privaten Schlüssel zum Dekodieren der Daten.

Die Schlüssel werden durch die folgende Abfolge von Arbeitsschritten erzeugt:

- Für große Primzahlen p und q definiere $n := p \cdot q$.
- Berechne das Produkt $\varphi(n) := (p-1) \cdot (q-1)$. Durch einen Satz von Euler weiß man, dass $\varphi(n)$ gerade die Anzahl der zu n teilerfremden natürlichen Zahlen kleiner n ist. Diese Tatsache zitieren wir hier nur.

- Wähle eine natürliche Zahl e, so dass e und $\varphi(n)$ teilerfremd sind und $1 \leq e \leq \varphi(n)$ gilt.
- Man berechne weiterhin $d \equiv e^{-1} \bmod \varphi(n)$, welches äquivalent ist zu der Wahl von d, so dass $d \cdot e \equiv 1 \bmod \varphi(n)$ gilt.

Der öffentliche Schlüssel besteht nun aus den Zahlen e und n; der private dagegen aus d und n. Die Zahlen p, q und $\varphi(n)$ sind keine Bestandteile des Schlüssels und müssen geheim bleiben.

Die *RSA-Verschlüsselung* funktioniert nun wie folgt: Der Klartext sei gegeben als (eine Zahl) m. Ein vorgegebener Text könnte in einer geeigneten Art in eine Zahl umgewandelt werden, indem man etwa die Eindeutigkeit der Zerlegung von natürlichen Zahlen in Potenzen von Primzahlen ausnutzt und auf diese Art und Weise Zeichenketten mittels ASCII-Tabelle umkehrbar eindeutig in natürliche Zahlen umwandelt. Hat man eine einzige Zahl, die kodiert werden soll, definiert man den kodierten Text (Chiffretext) als c mit $c \equiv m^e \bmod n$.

Für die *RSA-Entschlüsselung* berechnen Sie schließlich $m \equiv c^d \bmod n$. Hierfür ist natürlich wichtig, dass $m < n$ ist, damit bei der modularen Arithmetik der Klartext nicht aus Versehen abgeschnitten wird. Also muss n im ersten Schritt der Schlüsselfindung sehr groß gewählt oder die Ausgangsdaten in mehrere kleinere Datenpakete geteilt werden. Wie Sie sehen können, ist die Wahl der Zahl d als Inverse zu e modulo n wesentlich, denn dadurch gilt wie gewünscht

$$c^d = (m^e)^d = m^{e \cdot d} \equiv m \bmod n.$$

Nun wird es kurz technisch: Die zuletzt gesehene Kongruenz beruht auf der Tatsache, dass der kleine Fermatsche Satz gilt, der insbesondere in unserem Fall aussagt, dass $m^{q-1} \equiv 1 \bmod q$ gilt und somit auch für beliebige $l \in \mathbb{Z}$ gilt $m^{1+l(p-1)(q-1)} \equiv m \bmod q$. Durch Fallunterscheidung, ob p ein Primteiler von m ist oder nicht, lässt sich schließlich in beiden Fällen mittels des Chinesischen Restsatzes zeigen, dass sogar $m^{1+l(p-q)(q-1)} \equiv m \bmod pq$. (Dies müssen Sie mir an dieser Stelle glauben.) Weil d derart gewählt wurde, dass gilt $e \cdot d \equiv 1 \bmod (p-1)(q-1)$

und $1+l\cdot\varphi(n) \equiv 1 \equiv ed \bmod \varphi(n)$, kann man schließlich die gewünschte Kongruenz $m^{ed} \equiv m \bmod n$ folgern. Dies alles hier im Detail zu rechtfertigen, würde allerdings den Rahmen sprengen.

Die *Sicherheit des RSA-Algorithmus* beruht grundsätzlich auf der Komplexität der Primfaktorzerlegung der Zahl n. Beachten Sie, dass n ein Bestandteil des öffentlichen Schlüssels ist und somit bekannt ist. Könnte man n faktorisieren, so könnte man auch entsprechend $\varphi(n)$ berechnen und somit den privaten Schlüssel d ermitteln. Für die RSA-Verschlüsselung sollten deswegen Zahlen gewählt werden, die mindestens 512 Bit lang sind (also ca. 150 Dezimalstellen). Der Rechenaufwand ist enorm, so dass die Kodierung relativ sicher ist – enorm, aber nicht unmöglich.

Die Firma RSA vergibt Preise für das Primfaktorzerlegen großer Zahlen. So wurde die so genannte Zahl `RSA-140`, bestehend aus 140 Dezimalstellen, nämlich

$$\begin{aligned}&21290246318258757547497882016271517497806703963\\&27721627823338321538194998405649591136657385302\\&19183167831073879953172308895692308734419364 71,\end{aligned}$$

im Jahre 1999 in folgende Primfaktoren

$$\begin{aligned}&33987174230284385545301236276138758\\&35633986495969597423490929302771479\end{aligned}$$

und

$$\begin{aligned}&62642001874012850961516549482644422\\&19302037178623509019111660653946049\end{aligned}$$

zerlegt. Bonner Mathematiker haben Ende 2003 die Zahl `RSA-576`, bestehend aus 174 Ziffern, geknackt. Ihre Leistung wurde mit dem Preisgeld von 10.000 US-Dollar prämiert. Soweit ich weiß, ist die Zerlegung der so genannten Zahl `RSA-1024`, bestehend aus 309 Dezimalstellen, nämlich

$$\begin{aligned}&13506641086599522334960321627880596993888147560566 70\\&27524485143851526510604859533833940287150571909441 79\\&82072821644715513736804197039641917430464965892742 56\\&23934102086438320211037295872576235850964311056407 35\end{aligned}$$

01508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563,

noch offen. Es winken 100.000 US-Dollar. Für die ebenfalls offene Zahl `RSA-2048`, bestehend aus 617 Ziffern, winken sogar 200.000 Dollar. Interessiert, es zu versuchen?

Aber kommen wir wieder zurück zum Thema. Ein weiterer *Zusammenhang zum Chinesischen Restsatz* (CRS) ist nun der folgende: Die RSA-Entschlüsselung lässt sich mithilfe des CRS bei großen Werten von d beschleunigen. Wir müssen in diesem Fall zwar mehrere (kleinere) Rechenaufgaben lösen, aber gemessen an dem gesparten Rechenaufwand einer sehr großen Potenzierung (bei großem d) könnte sich dies immer noch lohnen.

Konkret bedeutet dies, dass wir die Potenzierung $m \equiv c^d \bmod n$ in kleinere Berechnungen wie folgt verteilen:

- Die Chiffre c wird in c_p und c_q geteilt:
  $$c_p :\equiv c \bmod p \quad \text{und} \quad c_q :\equiv c \bmod q.$$
- Der Exponent d wird entsprechend in d_p und d_q geteilt:
  $$d_p :\equiv d \bmod (p-1) \quad \text{und} \quad d_q :\equiv d \bmod (q-1).$$
- Man berechne $m_p :\equiv c_p^{d_p} \bmod p$ und $m_q :\equiv c_q^{d_q} \bmod q$.

Mithilfe des CRS wird nun der Klartext aus m_p und m_q wieder zusammengesetzt, indem man das folgende System von Kongruenzen löst:

$$\begin{aligned} m &\equiv m_p \bmod p, \\ m &\equiv m_q \bmod q, \end{aligned}$$

das heißt, man finde die Inversen y_q und y_p mit $y_q \cdot q \equiv 1 \bmod p$ bzw. $y_p \cdot p \equiv 1 \bmod q$. Dann gilt (nach dem CRS) offenbar wie gewünscht

$$m \equiv (m_p \cdot y_q \cdot q + m_q \cdot y_p \cdot p) \bmod n.$$

Mit diesem Ausblick schließen wir unsere Betrachtungen.

8. Komplexe Zahlen

Wie Sie wissen, besitzen quadratische Gleichungen nicht immer eine (reelle) Lösung, wie etwa die Gleichung

$$x^2 + 1 = 0 \text{ oder äquivalent } x^2 = -1.$$

Um u.a. trotzdem mit Lösungen von solchen Gleichungen rechnen zu können, führte Euler 1777 eine neue Zahl i ein. Für dieses i gilt dann per Definition

$$i^2 = -1 \quad \text{bzw.} \quad i = \sqrt{-1}.$$

Man bezeichnet diese neue Zahl i als *imaginäre Einheit*. Offensichtlich ist i keine reelle Zahl.

Wir führen ganz naiv, ausgehend von dieser neuen Zahl, die so genannten komplexen Zahlen ein, indem wir zunächst mit i rechnen, als würden die Gesetze gelten, die wir von den reellen Zahlen her kennen. So können wir beispielsweise Vielfache dieser imaginären Einheit bilden, indem wir eine reelle Zahl b an i heran multiplizieren, etwa $b \cdot i$ oder kurz bi bzw. ib. Weiterhin können wir gemischte Summen bilden: Die Summe aus einer reellen Zahl a und einer rein imaginären Zahl $b \cdot i$ heißt dann *komplexe Zahl*. Die Menge der komplexen Zahlen wird mit $\mathbb{C}$ bezeichnet

$$\mathbb{C} := \{a + i \cdot b \mid a, b \in \mathbb{R}\}.$$

Wir vereinbaren, dass zwei komplexe Zahlen genau dann gleich sind, wenn sie sowohl im Realteil, als auch im Imaginärteil übereinstimmen. Hierbei bezeichnet für $z := a + i \cdot b \in \mathbb{C}$ das a den *Realteil* von z und b den *Imaginärteil*; kurz $a = \mathsf{Re}(z)$ und $b = \mathsf{Im}(z)$. Insbesondere gilt, dass für $0 = b = \mathsf{Im}(z)$ die komplexe Zahl z reell ist; auf diese Weise haben wir unsere bekannten Zahlen in den neuen Zahlbereich eingebettet: $\mathbb{R} \subsetneq \mathbb{C}$.

Eigentlich haben wir bisher nur die Zahlenmengen ineinander eingebettet; es wäre sehr schön, wenn sich die Operationen auch übertragen lassen würden, das heißt, dass die komplexe Addition und Multiplikation so definiert wird, dass sie eine Fortsetzung der reellen ist – mit anderen Worten: Wenn wir die komplexen Operationen auf die reellen Zahlen einschränken, sollten wir wieder unsere bekannten reellen

Verknüpfungen erhalten. Außerdem wäre es wünschenswert, dass die Fortsetzung der uns bekannten Operationen auf den neuen Zahlbereich dennoch eine schöne Struktur hervorbringt: Unser Ziel ist es, die komplexen Zahlen als Körper zu definieren.

Diese Ziele vor Augen definieren wir die gewünschten Verknüpfungen wie folgt – zunächst die *komplexe Addition.*

Für $z_1 := a + i \cdot b$ und $z_2 := c + i \cdot d$ setze

$$z_1 +_{\mathbb{C}} z_2 := (a +_{\mathbb{R}} c) + i \cdot (b +_{\mathbb{R}} d) \in \mathbb{C}.$$

Damit ist $+_{\mathbb{C}} \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ offensichtlich eine Fortsetzung der reellen Addition, denn für $b = d = 0$ sind $z_1, z_2 \in \mathbb{R}$, $\mathsf{Im}(z_1 +_{\mathbb{C}} z_2) = 0$ und $z_1 +_{\mathbb{C}} z_2 = z_1 +_{\mathbb{R}} z_2$. In diesem Sinne verzichten wir auf die Indizierung beim Operationszeichen.

Die *komplexe Multiplikation* ist für $z_1 := a + i \cdot b$ und $z_2 := c + i \cdot d$ gegeben durch

$$z_1 \cdot_{\mathbb{C}} z_2 := (ac -_{\mathbb{R}} bd) + i \cdot (ad +_{\mathbb{R}} bc) \in \mathbb{C}.$$

Wie man leicht sieht, ist auch $\cdot_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ eine Fortsetzung der reellen Multiplikation. Es ist eine leichte Übungsaufgabe nachzurechen, dass folgender Satz gilt:

Satz 8.1. *Die Struktur* $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}}, \mathbb{0}, \mathbb{1})$ *ist ein Körper, wobei* $\mathbb{0} := 0+i\cdot 0$ *und* $\mathbb{1} := 1 + i \cdot 0$. *Weiterhin ist der Körper* $\mathbb{C}$ *eine Erweiterung des Körpers* $\mathbb{R}$ *(inklusive der Verknüpfungen).*

Im Folgenden verzichten wir –aufgrund der erfolgreichen Einbettung der reellen Zahlen in die komplexen– auf die formale Unterscheidung von "$+_{\mathbb{C}}$" bzw. "$\cdot_{\mathbb{C}}$" und "$+_{\mathbb{R}}$" bzw. "$\cdot_{\mathbb{R}}$" und schreiben einfach "$+$" bzw. "$\cdot$". Auch bei den neutralen Elementen stellen wir fest: $\mathbb{0} = 0$ und $\mathbb{1} = 1$.

Bevor wir nun die Division komplexer Zahlen behandeln, führen wir den dabei nützlichen Begriff des Konjugierten einer komplexen Zahl ein: Für $z = a + i \cdot b$ nennen wir $\bar{z} := a - i \cdot b$ das *Konjugierte* zu

z. Diese Operation hat beispielsweise folgende Eigenschaften, die man leicht als Übungsaufgabe nachrechnet:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \quad \text{und} \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}.$$

Wir betrachten nun die Division zweier komplexer Zahlen.

Betrachte für $z = a + i \cdot b$ mit $z \neq 0$ die komplexe Zahl $z' := \frac{1}{a^2+b^2} \cdot \bar{z}$. Beachten Sie, dass insbesondere $a^2 + b^2 \neq 0$ gilt und weiterhin

$$z \cdot z' = z' \cdot z = \frac{1}{a^2 + b^2} \cdot \bar{z} \cdot z = \frac{1}{a^2 + b^2} \cdot (a^2 + b^2) = 1.$$

Damit ist z' das multiplikative Inverse von z und wir bezeichnen im Folgenden z' mit z^{-1}.

Die *Division komplexer Zahlen* können wir jetzt wie folgt einführen:

$$\frac{z_1}{z_2} := z_1 : z_2 := z_1 \cdot z_2^{-1}$$

Insbesondere gilt

$$\frac{1}{z} = z^{-1} = \frac{1}{\overline{z} \cdot z} \cdot \overline{z} = \frac{\overline{z}}{\overline{z} \cdot z},$$

wobei $\overline{z} \cdot z = a^2 + b^2$ für $z = a + ib$ eine reelle Zahl ist, so dass man diese Formel bequem für die Berechnung komplexer Inverser ausnutzen kann.

Schauen wir uns ein Beispiel an und berechnen $\frac{3-2i}{4+5i}$. Dann gilt

$$\begin{aligned} \frac{(3-2i)(4-5i)}{(4+5i)(4-5i)} &= \frac{12 - 15i - 8i + 10i^2}{16 - 25i^2} = \frac{12 - 10 - 23i}{16 + 25} \\ &= \frac{2 - 23i}{41} = \frac{2}{41} - i \cdot \frac{23}{41} \end{aligned}$$

Insbesondere gilt für den Real- und Imaginärteil dieser komplexen Zahl $\mathsf{Re}(\frac{3-2i}{4+5i}) = \frac{2}{41}$ und $\mathsf{Im}(\frac{3-2i}{4+5i}) = -\frac{23}{41}$. Beachten Sie, dass der Imaginärteil einer komplexen Zahl immer eine reelle Zahl ist; es gilt für $z = a + ib$ stets $\mathsf{Re}(z) = a$ und $\mathsf{Im}(z) = b$, wobei a und b reelle Zahlen sind.

Als eine erste Anwendung komplexer Zahlen betrachten wir *quadratische Gleichungen* und suchen nach Lösungen. Zur Erinnerung: Eine quadratische Gleichung über den reellen Zahlen hat allgemein die Form

$$ax^2 + bx + c = 0,$$

wobei $a, b, c \in \mathbb{R}$ und $a \neq 0$. Aus der Theorie der reellen Zahlen kennen wir für $b^2 - 4ac \geq 0$ die Lösungsformel:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Hierbei wird $D := b^2 - 4ac$ als *Diskriminante* bezeichnet.

Mithilfe der komplexen Zahlen können wir Wurzeln aus negativen Zahlen ziehen, beispielsweise ist $\sqrt{-4} = \sqrt{(-1) \cdot 4} = \sqrt{-1} \cdot \sqrt{4} = \pm 2i$. Dieses Argument zeigt auch, dass für $z = \sqrt{a}$ mit $a < 0$ stets gilt $z = \pm i \cdot \sqrt{-a}$.

Man kann leicht zeigen, dass sich dies auch für den Fall einer negativen Diskriminante bei quadratischen Gleichungen ausnutzen lässt; in diesem Fall (wenn $D < 0$) finden wir auch die beiden komplexen Lösungen

$$z_{1,2} = \frac{-b \pm i \cdot \sqrt{4ac - b^2}}{2a} = -\frac{b}{2a} \pm i \cdot \frac{\sqrt{4ac - b^2}}{2a}.$$

Man kann sogar noch mehr zeigen: Diese Lösungsformel gilt auch für komplexe Koeffizienten a, b, c. Allerdings muss man dann ggf. die Quadratwurzel einer komplexen Zahl berechnen und dies kann aufwendig sein.

In diesem Zusammenhang möchte ich den folgenden Satz erwähnen, den wir (wahrscheinlich) in der Vorlesung über lineare Algebra im kommenden Semester näher betrachten werden:

Satz 8.2 (Fundamentalsatz der Algebra)**.** *Jede Gleichung n-ten Grades hat genau n komplexe Lösungen (Vielfachheiten mitgezählt).*

Kommen wir nun zu einem anderen Thema und befassen uns mit der *Darstellung komplexer Zahlen als Paare reeller Zahlen*: Wir können eine komplexe Zahl $z = a + ib$ mit einem geordneten Paar reeller Zahlen $(a, b) \in \mathbb{R} \times \mathbb{R}$ identifizieren, das heißt, wir können folgende Abbildung angeben:

$$\mathbb{C} \to \mathbb{R} \times \mathbb{R}, \quad a + ib \mapsto (a, b)$$

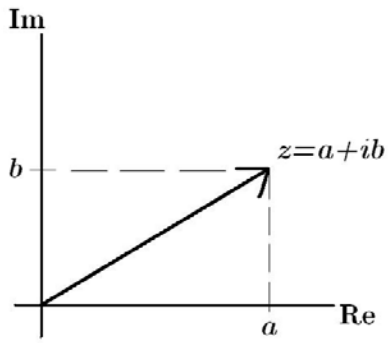
Diese Abbildung bildet eine komplexe Zahl z auf das Paar $(\mathsf{Re}(z), \mathsf{Im}(z))$ ab und ist damit bijektiv. Die Operationen "+" und "$\cdot$" sehen in dieser

Darstellung wie folgt aus:

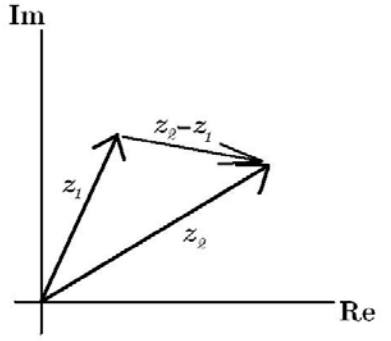
$$\begin{aligned}(a,b)+(c,d) &:= (a+c, b+d)\\ (a,b)\cdot(c,d) &:= (ac-bd, ad+bc)\end{aligned}$$

Insbesondere sieht man leicht, dass $1 \mapsto (1,0)$ und $i \mapsto (0,1)$.

Mithilfe dieser Überlegung können wir uns eine geometrische Darstellung komplexer Zahlen überlegen. Da eine komplexe Zahl genau einem Paar von reellen Zahlen entspricht, können wir komplexe Zahlen in eine Ebene einzeichnen – die so genannte Gaußsche Zahlenebene:



Dabei interpretieren wir eine komplexe Zahl entweder als den Punkt (a,b) in der Ebene oder als den dazugehörigen so genannten *Ortsvektor*. Im Folgenden werden wir beides parallel verwenden, vorzugsweise aber mit den Ortsvektoren arbeiten. Diese Art der Sichtweise können wir insbesondere ausnutzen, wenn wir die *Addition* geometrisch interpretieren wollen, wie etwa im folgenden Bild dargestellt (hier sogar der spezielle Fall der *Subtraktion*, denn es gilt $z_2 - z_1 = z_2 + (-z_1)$).

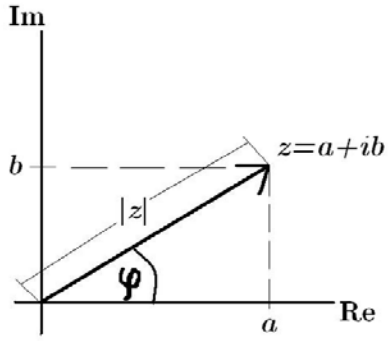


Wenn wir uns die Multiplikation geometrisch vorstellen wollen, dann ist eine andere Sichtweise auf die komplexen Zahlen besser geeignet: die *Darstellung der komplexen Zahlen durch Polarkoordinaten.*

Zunächst definieren wir den *Betrag* einer komplexen Zahl $z = a + ib$. Dieser ist gegeben durch

$$|z| := \sqrt{a^2 + b^2} = \sqrt{\overline{z} \cdot z}$$

Wenn Sie sich überlegen, dass in der Darstellung mittels Ortsvektoren immer ein rechtwinkliges Dreieck entsteht, welches aus den beiden Katheten a und b und der Hypothenuse $|z|$ besteht, dann wird Ihnen auch klar, dass der Betrag einer komplexen Zahl gerade der Länge des Ortsvektors entspricht. Schauen wir uns dafür folgende Abbildung an:



Der Ortsvektor eines Punktes (a, b) kann auch durch den Winkel φ und die Länge des Ortsvektors charakterisiert werden – was wiederum einfach eine andere Sichtweise der komplexen Zahlen ist.

Dabei gilt –aufgrund des Kosinussatzes im rechtwinkligen Dreieck– die Gleichung $a = |z| \cdot \cos\varphi$ und entsprechend $b = |z| \cdot \sin\varphi$ wegen des Sinussatzes, also insbesondere

$$z = a + ib = |z| \cdot \cos\varphi + i \cdot |z| \cdot \sin\varphi = |z| \cdot (\cos\varphi + i \cdot \sin\varphi)$$

In der Vorlesung über Analysis im kommenden Semester werden Sie (wahrscheinlich) die komplexe Exponentialfunktion kennenlernen und beweisen, dass gilt

$$e^{i\varphi} = \cos\varphi + i \cdot \sin\varphi$$

Dann gilt offenbar auch $z = |z| \cdot e^{i\varphi}$.

Damit haben wir eine weitere Darstellung komplexer Zahlen gefunden. Wir können einer komplexen Zahl $z = a + ib$ mit $z \neq 0$ auf eindeutige Art und Weise das Paar $(|z|, \varphi)$ zuordnen, wobei φ der zum Ortsvektor gehörende Winkel entsprechend der obigen Abbildung ist. Dieser Winkel wird dabei derart gewählt, dass $-\pi < \varphi \leq \pi$ gilt; damit werden der obere und der untere Halbkreise beschrieben. Dass wir hier nicht einen Vollkreis (also $0 \leq \varphi < 2\pi$) nutzen, hat technische Aspekte.

Schauen wir uns die nicht ganz einfache *Umwandlung in Polarkoordinaten* an: Es sei dafür eine komplexe Zahl $z = a + ib$ gegeben. Dann gilt $|z| = \sqrt{a^2 + b^2}$ und den gewünschten Winkel erhalten wir durch

$$\varphi = \begin{cases} \arccos \frac{a}{|z|}, & \text{für } b \geq 0 \\ \arccos(-\frac{a}{|z|}) - \pi, & \text{für } b < 0 \end{cases}$$

Mit dieser Darstellung wird auch die geometrische Deutung der Multiplikation komplexer Zahlen einfacher, denn es gilt

$$(|z_1| \cdot e^{i\varphi_1}) \cdot (|z_2| \cdot e^{i\varphi_2}) = |z_1| \cdot |z_2| \cdot e^{i(\varphi_1 + \varphi_2)}$$

Wir erkennen, dass sich die Winkel bei der Multiplikation addieren, also der eine Ortsvektor um den Winkel des anderen Ortsvektors gedreht wird. Die Längen der Ortsvektoren multiplizieren sich dabei.

Abschließend noch eine kurze Bemerkung zu den *Anwendungen* komplexer Zahlen: Komplexe Zahlen werden beispielsweise in der Physik als sehr nützlich angesehen und verdienen daher den Namen "imaginäre Zahlen" eigentlich nicht (allerdings ist dieser historisch gewachsen und so bleibt man natürlich dabei). Sie werden u.a. in der Quantentheorie und Relativitätstheorie angewendet, um Schwingungsvorgänge oder Phasenverschiebungen zu untersuchen.

9. Kombinatorik – Schubfachprinzip und Zählformeln

In diesem Abschnitt schauen wir uns einfache kombinatorische Prinzipien an, die grundlegende Konzepte aus dem ersten Teil der Vorlesung anwenden.

Kommen wir zunächst zum so genannten *Schubfachprinzip*. Die einfachste Variante ist etwa die folgende, die jedem aus dem täglichen Leben bereits bekannt ist:

> "Wenn $n+1$ Gegenstände in n Schubfächer gelegt werden, so gibt es in mindestens einem der Schubfächer mindestens zwei Gegenstände."

Etwas mathematischer liest sich dies wie folgt:

Satz 9.1. *Seien A und B zwei endliche Teilmengen mit $|A| > |B|$ und $f : A \to B$ eine Funktion. Dann gibt es $a, a' \in A, a \neq a'$ mit $f(a) = f(a')$, das heißt, die Abbildung $f : A \to B$ ist nicht injektiv.*

Es gibt auch allgemeinere Schubfachprinzipien für unendliche Mengen, also etwa wenn wir die Voraussetzungen des Satzes für unendliche Mengen A und B abändern, wobei A überabzählbar und B abzählbar ist. Dann muss es ebenfalls ein "Schubfach" geben, in dem mehr als ein Element vorkommt; genauer gesagt muss es eines geben, welches bereits überabzählbar viele Elemente enthält.

Ein typisches und bekanntes Szenario für den endlichen Fall haben wir bei Geburtstagen: Wir wissen, dass von 13 Personen mindestens zwei im gleichen Monat Geburtstag haben.

Auf dem Weg zu den eigentlichen Zählformeln führen wir zunächst den *Binomialkoeffizienten* ein.

Definition 9.2. *Der Quotient $\binom{n}{k} := \frac{n!}{k!(n-k)!}$, gelesen "n über k", wird für natürliche Zahlen n, k mit $k \leq n$ als* Binomialkoeffizient *bezeichnet.*

Formal können wir diesen für $k > n$ gleich 0 setzen. Hierbei wird $n!$ für beliebige $n \in \mathbb{N}$ rekursiv durch $0! = 1$ und $(n+1)! = (n+1) \cdot n!$ definiert und als "*n Fakultät*" gelesen.

Die Bezeichnung als Binomialkoeffizient wird durch den folgenden Satz gerechtfertigt, den man relativ leicht durch vollständige Induktion beweisen kann:

Satz 9.3 (Binomischer Lehrsatz)**.** *Für alle $n \in \mathbb{N}$ und $x, y \in \mathbb{R}$ gilt*

$$\begin{aligned}(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}\cdot y + \cdots + \binom{n}{n-1}x\cdot y^{n-1} + \binom{n}{n}y^n \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}\cdot y^k\end{aligned}$$

Wir schauen uns hier nur das aus der Schule bekannte Beispiel für $n = 2$ an – in diesem Fall gilt

$$\binom{2}{0} = \frac{2!}{0!\cdot(2-0)!} = 1 \qquad \binom{2}{1} = \frac{2!}{1!\cdot(2-1)!} = 2 \qquad \binom{2}{2} = 1$$

Somit haben wir

$$(x+y)^2 = 1\cdot x^2\cdot y^0 + 2\cdot x^1\cdot y^1 + 1\cdot x^0\cdot y^2 = x^2 + 2xy + y^2.$$

Folgende Eigenschaften des Binomialkoeffizienten können hilfreich sein:

Satz 9.4. *Für alle $n, k \in \mathbb{N}, k \leq n$ gilt folgende Symmetrie- und Additionseigenschaft:*

$$\text{(a)}\quad \binom{n}{k} = \binom{n}{n-k} \qquad \text{(b)}\quad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Beweis: Seien $n, k \in \mathbb{N}$ und $k \leq n$. Wir beweisen beide Eigenschaften direkt und beginnen mit der ersten – zu (a):

$$\begin{aligned}\binom{n}{n-k} &= \frac{n!}{(n-k)!\cdot(n-(n-k))!} \\ &= \frac{n!}{(n-k)!\cdot(n-n+k)!} \\ &= \frac{n!}{k!\cdot(n-k)!} = \binom{n}{k}\end{aligned}$$

Zu (b):

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!\cdot((n-1)-k)!} + \\ &\qquad \frac{(n-1)!}{(k-1)!\cdot((n-1)-(k-1))!} \\ &= \frac{(n-1)!}{k!\cdot(n-k-1)!} + \frac{(n-1)!}{(k-1)!\cdot(n-k)!}\end{aligned}$$

$$
\begin{aligned}
&= \frac{(n-1)! \cdot (n-k) + (n-1)! \cdot k}{k! \cdot (n-k)!} \\
&= \frac{(n-1)! \cdot ((n-k)+k)}{k! \cdot (n-k)!} \\
&= \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k}
\end{aligned}
$$

⊠

Wie wir gerade bewiesen haben, lassen sich Binomialkoeffizienten leicht mithilfe des so genannten *Pascal'schen Dreiecks* berechnen, welches entsteht, indem man die jeweiligen oberen Elternknoten addiert und so den Tochterknoten erhält:

n	Binomialkoeffizienten
0	1
1	1 1
2	1 2 1
3	1 3 3 1
4	1 4 6 4 1
5	1 5 10 10 5 1
⋮	⋮

Damit lassen sich die allgemeinen binomischen Formeln leicht herleiten, beispielsweise für $n = 4$:

$$(x+y)^4 = \underline{1}x^4 + \underline{4}x^3y + \underline{6}x^2y^2 + \underline{4}xy^3 + \underline{1}y^4.$$

Kommen wir nun zu den wichtigen *Zählformeln*, die vielerorts inner- und außerhalb der Mathematik Anwendung finden. In der Mathematik modelliert man die Situation, um die es uns im Folgenden gehen soll, indem man über *Urnen* und *Kugeln* spricht. Stellen wir uns daher vor, dass wir nacheinander k Kugeln aus einer Urne ziehen möchten. Dabei haben wir verschiedene Möglichkeiten:

(a) Wir ziehen nacheinander eine Kugel und legen diese wieder in die Urne zurück oder nicht.

(b) Wir ziehen nacheinander Kugeln aus der Urne und merken uns dabei die Reihenfolge der gezogenen Kugeln oder nicht.

Daher unterscheiden wir grundsätzlich vier Arten von Ziehungen: nämlich *mit* oder *ohne* Wiederholung (d.h. mit oder ohne Zurücklegen) und *mit* oder *ohne* Berücksichtigung der Reihenfolge (der gezogenen Kugeln).

Zunächst schauen wir uns den Fall **"mit Reihenfolge"** an. Diese Art der Ziehung wird allgemein als *Variation* bezeichnet. Wir unterscheiden erneut zwei Unterfälle:

(a) **Variation ohne Wiederholung** (ohne Zurücklegen), d.h. wir ziehen k Kugeln aus einer Urne mit insgesamt n Kugeln und legen dabei die gezogenen Kugeln nicht wieder in die Urne zurück und achten auf die Reihenfolge während der Ziehung. Dann gibt es insgesamt $\boxed{\frac{n!}{(n-k)!}}$ Möglichkeiten.

Erklärung: Es gibt für die erste gezogene Kugel n, für die zweite $n-1$, ... und für die letzte $n-k+1$ Möglichkeiten. Insgesamt somit $n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$.

Beispiel: Wir wollen aus einer Gruppe von 8 Schülern eine 4er-Staffel zusammenstellen. Hier ist $n = 8$ und $k = 4$; ohne Wiederholung, mit Reihenfolge:

$$\frac{8!}{(8-4)!} = \frac{8!}{4!} = 8 \cdot 7 \cdot 6 \cdot 5 = 1680.$$

(b) **Variation mit Wiederholung** (mit Zurücklegen), d.h. wir ziehen k Kugeln aus einer Urne mit insgesamt n Kugeln und legen dabei die gezogene Kugel immer wieder zurück und achten penibel auf die Reihenfolge während der Ziehung. Dann gibt es insgesamt $\boxed{n^k}$ Möglichkeiten.

Erklärung: Die gleiche Herangehensweise wie gerade liefert uns insgesamt $\underbrace{n \cdot n \cdot \ldots \cdot n}_{k-\text{mal}} = n^k$ Möglichkeiten.

Beispiel: Wir wollen einen Safe knacken. Der Code besteht aus vier Stellen mit jeweils zehn möglichen Ziffern. Dann ist $n = 10$ und $k = 4$ und es gibt somit $n^k = 10^4 = 10.000$ Möglichkeiten.

Es bleibt der Fall **"ohne Reihenfolge"**. Diese Art der Ziehung wird allgemein als *Kombination* bezeichnet. Wir unterscheiden zwei Unterfälle:

(a) **Kombination ohne Wiederholung** (ohne Zurücklegen), d.h. wir möchten k Kugeln aus einer Urne mit n Kugeln ziehen, wobei wir die gezogenen Kugeln nicht wieder in die Urne legen, aber auch nicht auf die Reihenfolge während der Ziehung achten. Dann gibt es insgesamt $\boxed{\binom{n}{k}}$ Möglichkeiten.

Erklärung: Sie wissen bereits, dass es mit Berücksichtigung der Reihenfolge $\frac{n!}{(n-k)!}$ viele Möglichkeiten gibt. Nun müssen wir aber durch die Anzahl der verschiedenen Anordnungen einer festen Auswahl von k Elementen teilen. Dies ist wieder eine Variation ohne Wiederholung von k aus k Kugeln; es gibt also $k!$ Möglichkeiten dafür. Fassen wir beides zusammen, erhalten wir wie gewünscht $\frac{1}{k!} \cdot \frac{n!}{(n-k)!} = \binom{n}{k}$ viele Möglichkeiten.

Beispiel: Wir spielen Lotto: 6 aus 49. Wir planen den Jackpot und fangen zunächst langsam mit einem 6er an. Es gibt insgesamt

$$\binom{49}{6} = \frac{49!}{6!(49-6)!} = \frac{49 \cdot 48 \cdot \ldots \cdot 44}{6 \cdot 5 \cdot \ldots \cdot 1} = 13.983.816,$$

also knapp 14 Millionen Möglichkeiten. $(n = 49, k = 6)$

(b) **Kombination mit Wiederholung** (mit Zurücklegen), d.h. wir möchten k Kugeln aus einer Urne mit n Kugeln ziehen und legen dabei die gezogenen Kugeln immer wieder in die Urne zurück; wir achten während der Ziehung nicht auf die Reihenfolge. Dann gibt es insgesamt $\boxed{\binom{n+k-1}{k}}$ Möglichkeiten.

Erklärung: Auch hier führen wir das Problem auf einen bereits betrachteten Fall zurück. Stellen Sie sich vor, es wäre eine Auswahl von k aus n Kugeln gegeben. Da die Reihenfolge keine Rolle spielt, suchen wir uns eine Anordnung aus: Wir sortieren die Ergebnisse der einzelnen Ziehungen nach der Nummer der jeweils gezogenen Kugel. Dann reicht es aber, wenn wir uns das Folgende notieren: Zuerst einen Kreis "◯" für jedes Mal, bei dem die erste Kugel gezogen wurde mit einem anschließenden Strich "|"; nun wieder einen Kreis für jedes Mal, bei dem die zweite Kugel gezogen wurde mit einem anschließenden Strich; ... und zuletzt einen Kreis für jedes Mal, bei dem die n-te Kugel gezogen wurde. Würde zweimal die dritte und sonst nur die n-te Kugel gezogen werden, entspräche dies beispielsweise der Folge

$$||\bigcirc\bigcirc\underbrace{|\cdots|}_{(n-3)-\text{mal}}\overbrace{\bigcirc\cdots\bigcirc}^{(k-2)-\text{mal}}.$$

Dies gibt uns eine Bijektion von den möglichen Auswahlen von k aus n Kugeln ohne Berücksichtigung der Reihenfolge und mit Wiederholung auf die Möglichkeiten k Kugeln (nämlich die Positionen der Striche) aus $n+k-1$ Kugeln (der Gesamtanzahl von Positionen) zu ziehen. Die Gesamtanzahl von Positionen ergibt sich dabei als Summe der Anzahl an Kreisen und der Anzahl an Strichen $= k+n-1$. Aber damit erkennen Sie sofort, dass es $\binom{n+k-1}{k}$ Möglichkeiten gibt.

Beispiel: Wir spielen Kniffel und würfeln mit fünf Würfeln. Wie viele Konstellationen der Würfel gibt es? Wir würfeln mit fünf Würfeln, d.h. wir erhalten fünf Zahlen, also $k = 5$. Woher bekommen wir n? Hier müssen wir überlegen, woher die Zahlen kommen – in diesem Fall von einem Würfel mit sechs Möglichkeiten, d.h. $n = 6$. Es gibt dann

$$\begin{aligned}\binom{n+k-1}{k} &= \frac{(n+k-1)!}{k!(n-1)!} = \frac{(6+5-1)!}{5!(6-1)!} \\ &= \frac{10!}{5!\cdot 5!} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 256\end{aligned}$$

Möglichkeiten.

Fassen wir die vier prinzipiellen Möglichkeiten noch einmal übersichtlich in einer Tabelle zusammen.

Die jeweils in Klammern stehende Bezeichnung für die einzelnen Fälle wird mitunter in der Literatur verwendet und soll hier vollständigkeitshalber angegeben sein.

	Variation (mit Reihenfolge)	Kombination (ohne Reihenfolge)
mit Wiederholung	n^k $(k\text{-}Stichprobe)$	$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}$ $(k\text{-}Auswahl)$
ohne Wiederholung	$\frac{n!}{(n-k)!}$ $(k\text{-}Permutation)$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ $(k\text{-}Kombination)$

Schauen wir uns folgendes typisches und gleichsam verblüffendes Beispiel an, nämlich das *Geburtstagsparadoxon*:

Betrachten Sie eine Menge von 20 Personen. Die Folge der Geburtstage (pro Jahr auf Tag und Monat) kann als Variation mit Wiederholung, also als k-Stichprobe für $k = 20$, aus der Grundmenge $\{1, \ldots, 365\}$, d.h. $n = 365$, aufgefasst werden. Es gibt daher 365^{20} solcher Folgen.

Die Menge der Variationen ohne Wiederholung, also die k-Permutation für $k = 20$, aus der Menge $\{1, \ldots, 365\}$ für $n = 365$ besteht aus allen Konfigurationen, in denen keine zwei Personen den gleichen Geburtstag haben. Dann gibt es davon $\frac{365!}{(365-20)!} = \frac{365!}{345!}$ Möglichkeiten.

Das Verhältnis von Konfigurationen mit paarweise verschiedenen Geburtstagen zu den Gesamtmöglichkeiten ist

$$\frac{\frac{365!}{345!}}{364^{20}} = \frac{365!}{345! \cdot 365^{20}} \approx 0{,}58856 \mathrel{\widehat{=}} 58{,}9 \text{ Prozent}$$

Also gibt es bei mehr als 41 Prozent der Konfigurationen gemeinsame Geburtstage. Man kann diese Zahl als Wahrscheinlichkeit für das Auftreten gemeinsamer Geburtstage (bei 20 Personen) auffassen.

Bei $k = 50$ Personen kann man sogar bereits fast sicher sein, dass gemeinsame Geburtstage auftauchen, es gilt nämlich

$$\frac{\frac{n!}{(n-k)!}}{n^k} = \frac{365!}{315! \cdot 365^{50}} \approx 0{,}02962 \mathrel{\widehat{=}} 2{,}96 \text{ Prozent},$$

das heißt, dass gemeinsame Geburtstage unter 50 Personen mit einer Wahrscheinlichkeit von mehr als 97% vorkommen.

Betrachten wir ein ähnliches Beispiel, welches übersichtlicher ist: Zwei Personen wählen jeweils unabhängig eine von drei Türen aus. Wie hoch ist die Wahrscheinlichkeit, dass beide dieselbe Tür wählen? Wie im Beispiel gerade wählen wir den Ansatz über Variationen und erhalten folgendes Ergebnis (für das komplementäre Ereignis)

$$\frac{\frac{n!}{(n-k)!}}{n^k} = \frac{\frac{3!}{(3-2)!}}{3^2} = \frac{6}{9} = \frac{2}{3} \mathrel{\widehat{=}} 66 \text{ Prozent}.$$

Fälschlicherweise könnte man versuchen, das Ganze als Kombinationen zu interpretieren. Man erhielte dann insgesamt

$$\frac{\binom{n}{k}}{\binom{n+k-1}{k}} = \frac{\binom{3}{2}}{\binom{4}{2}} = \frac{\frac{3!}{2! \cdot 1!}}{\frac{4!}{2! \cdot 2!}} = \frac{1}{2} \mathrel{\widehat{=}} 50 \text{ Prozent}.$$

Im zweiten Fall begeht man den Fehler, das Verhältnis aufgrund unterschiedlicher Gewichtung der (Tür-)Wahlergebnisse zu verfälschen. Als Kombination betrachtet, ist uns die Reihenfolge der Türwahl nicht wichtig, das heißt, wir zählen das Szenario $\{1, 2\}$ und $\{2, 1\}$ nur einmal. Betrachten wir es als Variation, sind die beiden Folgen $(1, 2)$ bzw. $(2, 1)$ verschieden und werden auch einzeln untersucht. Im Falle der Kombinationen fallen auf diese Art drei Fälle aus dem Rennen, so dass sich eine Gesamtanzahl von 6 potentiellen Möglichkeiten ergibt, nämlich $\{1, 1\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 2\}$, $\{2, 3\}$ und $\{3, 3\}$. Drei davon sind die erwünschten Endergebnisse, so dass wir ein Gesamtverhältnis von $\frac{3}{6} = \frac{1}{2}$ erhalten – vergleichen Sie dies mit der obigen Rechnung.

Im Falle der korrekten Interpretation als Variation erhalten wir nicht 6, sondern 9 Möglichkeiten, so dass sich ein Gesamtverhältnis von $\frac{3}{9} = \frac{1}{3}$

ergibt. Da wir oben das Komplement berechnet haben, kommen wir auf das gewünschte Ergebnis von $\frac{1}{3} = 1 - \frac{2}{3}$. Dies bestärkt unsere Interpretation dieses Szenarios als Variation.

Sie sehen, wie wichtig es ist, das richtige Gefühl für die verschiedenen Interpretationen der in der Tabelle auf Seite 52 dargestellten Urnenmodelle zu entwickeln. Folgen Sie mir daher in die wunderbare Welt des Glückspiels und lassen Sie uns noch mehr Beispiele anschauen:

Betrachten wir zunächst das bereits angedeutete *Lottospiel*: 6 aus 49, d.h. wir haben eine Urne mit 49 Kugeln und wir ziehen nacheinander 6 Zahlen, ohne Wiederholung und ohne Berücksichtigung der Reihenfolge. Kombinatorisch ist dies eine Kombination ($n = 49$, $k = 6$) und es gibt $\binom{n}{k} = \binom{49}{6}$ Möglichkeiten (d.h. 13.983.816). Damit ist die Chance einen 6er zu bekommen $1 : 13.983.816 \approx 0,000.000.072 \mathrel{\widehat{=}} 0,000.007.2$ Prozent.

Wie sieht die Wahrscheinlichkeit für einen 3er bzw. 5er aus? Plötzlich gilt es, verschiedene Ansätze zu kombinieren. Zunächst betrachten wir den 3er, d.h. 3 der 6 Gewinnzahlen stimmen überein. Somit suchen wir die Wahrscheinlichkeit dafür, dass genau 3 Zahlen aus den 6 Gewinnzahlen und genau 3 Zahlen aus den restlichen 43 Zahlen stammen:

- Es gibt $\binom{6}{3}$ Möglichkeiten 3 Zahlen aus 6 zu wählen,
  also $\frac{6!}{3!\cdot 3!} = \frac{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 3\cdot 2\cdot 1} = 20$.
- Es gibt $\binom{43}{3}$ Möglichkeiten 3 Zahlen aus 43 zu wählen,
  also $\frac{43!}{3!\cdot 40!} = 12.341$.

Die Gesamtmöglichkeit ergibt sich multiplikativ aus beiden Werten, denn jede Wahl des einen kann beliebig mit einer Wahl der anderen kombiniert werden, insgesamt daher

$$\binom{6}{3} \cdot \binom{43}{3} = 20 \cdot 12.341 = 246.820,$$

das heißt, die Gesamtwahrscheinlichkeit für einen 3er ist

$$\frac{246.820}{13.983.816} = 0,01765 \mathrel{\widehat{=}} 1,8 \text{ Prozent}.$$

Kommen wir nun zu den Möglichkeiten eines 5ers, d.h. 5 der getippten Zahlen stimmen mit den 6 Gewinnzahlen überein. Wie oben können

wir analog schließen, dass es insgesamt

$$\binom{6}{5} \cdot \binom{43}{1} = 6 \cdot 43 = 258$$

Möglichkeiten gibt, einen 5er zu erhalten, so dass die Gewinnwahrscheinlichkeit nur

$$\frac{258}{13.983.816} = 0,000.018.4 \mathrel{\widehat{=}} 0,001.84 \text{ Prozent}$$

beträgt.

Wie sieht es mit dem Jackpot aus? – Das heißt, einen 6er mit Superzahl. Wir wissen bereits, dass durch die Superzahl noch einmal jeweils 10 Möglichkeiten dazukommen, so dass es insgesamt 139.838.160 Möglichkeiten gibt. Dies ergibt eine Gewinnchance von (frustrierenden)

$$0,000.000.007.2 \mathrel{\widehat{=}} 0,000.000.72 \text{ Prozent.}$$

Vergleichen wir diese Gewinnmöglichkeiten mit einer anderen Lotterieart, der *Glücksspirale*: Dort suchen wir möglichst viele der letzten Ziffern einer 7-stelligen Zahl, d.h. wir ziehen 7 Zahlen aus einer Urne mit 10 Zahlen, nämlich den Ziffern 0 bis 9. Die Ziehung erfolgt unter Berücksichtigung der Reihenfolge, also eine Variation, und mit Wiederholung ($n = 10$, $k = 7$).

Jede Stelle der Losnummer hat eine Gewinnchance von $\frac{1}{10}$, so dass 6 Richtige (also die letzten 6 Zahlen der Losnummer) eine Gewinnwahrscheinlichkeit von $\frac{1}{10^6} = \frac{1}{1.000.000}$ haben. Alle 7 Zahlen –und somit die gesamte Losnummer– werden mit einer Wahrscheinlichkeit von $\frac{1}{10^7} = \frac{1}{10.000.000}$ gezogen.

Betrachten wir eine Variante dieser Art Lottorie: Man ziehe 5 Buchstaben mit Wiederholung und mit Reihenfolge ($n = 26$, $k = 5$). Die Chance auf 5 Richtige beträgt dann $\frac{1}{26^5} \approx \frac{1}{12.000.000}$. Somit ist die Gewinnwahrscheinlichkeit geringer als bei der 7-stelligen Variante in der Glückspirale, obwohl man sich durchaus von der kürzeren Länge des Lösungswortes täuschen lassen kann.

Wie wichtig es ist, sich über die Art und Weise der Ziehung Gedanken zu machen, können Sie anhand des folgenden Gedankenspiels erkennen:

Stellen Sie sich vor, wir würden die Losnummer der Glückspirale anders ermitteln. Man nehme eine Urne mit 7mal 10 Ziffern, jeweils von 0 bis 9, also insgesamt 70 Kugeln. Nun ziehe man ohne Wiederholung aber mit Reihenfolge.
Diese Variante hat allerdings unerwünschte Nebeneffekte: Sie ziehen die erste Ziffer mit einer Wahrscheinlichkeit von $\frac{7}{70} = \frac{1}{10}$. Für die zweite Ziffer haben wir eine Chance von $\frac{6}{69}$, falls sie gleich der Zahl an der ersten Stelle ist, oder $\frac{7}{69}$, falls eine andere als die erste Zahl gezogen wird.

Konkret bedeutet dies, dass die Losnummer 1.111.111 eine Chance von

$$\frac{7}{70} \cdot \frac{6}{69} \cdot \frac{5}{68} \cdot \frac{4}{67} \cdot \frac{3}{66} \cdot \frac{2}{65} \cdot \frac{1}{64} \mathrel{\widehat{=}} 0,000.000.083 \text{ Prozent}$$

hat; dagegen hat die Losnummer 1.234.567 eine Gewinnchance von

$$\frac{7}{70} \cdot \frac{7}{69} \cdot \frac{7}{68} \cdot \frac{7}{67} \cdot \frac{7}{66} \cdot \frac{7}{65} \cdot \frac{7}{64} \mathrel{\widehat{=}} 0,000.013.631 \text{ Prozent.}$$

Damit hätten verschiedene Losnummern unterschiedliche Wahrscheinlichkeiten, gezogen zu werden; dies möchte man vielleicht vermeiden.

Fassen wir unsere Ergebnisse in einer Tabelle zusammen:

Spiel	*Gewinnchance*	*typische Auszahlung*
5er (Lotto)	0,00184 %	2.000 – 3.000 €
6er (Glücksspirale)	0,0001 %	100.000 €
7er (Glücksspirale)	0,00001 %	2 Mio €
6er (Lotto)	0,000.000.72 %	0,5 Mio – 2 Mio €
Jackpot (Lotto)	0,000.000.072 %	4 Mio €

Man kann erkennen, dass sich diese Wahrscheinlichkeiten jeweils etwa um den Faktor 10 unterscheiden. Aber lassen Sie sich dennoch nicht täuschen, selbst der (sehr unterschiedliche) Lospreis spielt eine Rolle, wenn Sie ihr Glück bis ins Letzte berechnen möchten.

Teil 2. Mathematische Logik

In diesem Teil des Kurses werden wir uns mit Aspekten der mathematischen Logik befassen. Zunächst betrachten wir einfache und für uns interessante unendliche Mengen, die so genannten abzählbaren Mengen. Danach wenden wir uns der Aussagenlogik zu, die wir im Detail behandeln werden. Nachdem wir die (formale) Sprache definiert haben, befassen wir uns mit ihrer Semantik und Syntax. Höhepunkt wird der Beweis des Vollständigkeitssatzes für die Aussagenlogik werden.

Nach der Aussagenlogik widmen wir uns der Prädikatenlogik und befassen uns allgemein mit (prädikatenlogischen) formalen Sprachen und deren Strukturen.

10. Abzählbare Mengen

Wir befassen uns zunächst mit einfachen unendlichen Mengen und zeigen einige nützliche Eigenschaften darüber. Unser Ziel in diesem Kapitel ist es unter anderem, den Beweis des Vollständigkeitssatzes vorzubereiten und dafür festzustellen, dass wir die Anzahl der Formeln nach oben beschränken können, wenn wir das Alphabet als nicht all zu groß ansetzen.

Definition 10.1. *Zwei Mengen A und B heißen* gleichmächtig*, wenn es eine Bijektion f mit $f : A \to B$ gibt. In diesem Fall schreiben wir kurz: $A \sim B$.*

Satz 10.2. *Die Relation $\sim$ ist eine Äquivalenzrelation, das heißt, es gilt:*

(a) $A \sim A$

(b) *Wenn $A \sim B$, dann $B \sim A$.*

(c) *Wenn $A \sim B$ und $B \sim C$, dann $A \sim C$.*

Der Beweis ist einfach und wir lassen ihn als Übungsaufgabe.

Definition 10.3. *Eine Menge A heißt* abzählbar*, wenn $A \sim \mathbb{N}$.*

Damit ist eine Menge abzählbar, wenn es eine geeignete Bijektion gibt. In vielen Fällen möchten wir dies gern scheinbar abschwächen und folgende Äquivalenz nutzen:

Satz 10.4. *Eine Menge ist genau dann abzählbar, wenn es eine Injektion $f : \mathbb{N} \to A$ und eine Surjektion $g : \mathbb{N} \to A$ gibt.*

Diesen mengentheoretischen Beweis werden wir nicht führen, aber wir können diesen glauben, wenn wir die Vorstellung nutzen, dass eine derartige Injektion impliziert, dass die natürlichen Zahlen in die Menge A eingebettet werden können. Somit gibt es in der Menge A mindestens so viele Elemente wie es natürliche Zahlen gibt. Auf der anderen Seite, eine oben genannte Surjektion besagt, dass wir alle Elemente aus A mit natürlichen Zahlen überdecken können, so dass es höchstens so viele Elemente in A wie natürliche Zahlen gibt.

Satz 10.5. *Unendliche Teilmengen von abzählbaren Mengen sind abzählbar.*

Beweis: Sei $A \subseteq B$ unendlich und B abzählbar. Da A unendlich ist, existiert eine Injektion $f : \mathbb{N} \to A$. Da B abzählbar ist, existiert eine Surjektion $h : \mathbb{N} \to B$. Mithilfe von h lässt sich leicht eine Surjektion $g : \mathbb{N} \to A$ finden, indem wir die natürlichen Zahlen, die auf Elemente aus $B \setminus A$ abgebildet werden, neu zuordnen, nämlich auf ein beliebiges Element aus A. Zusammen mit Satz 10.4 folgt dann die Behauptung. ⊠

Satz 10.6. *Für abzählbare Mengen A und B ist auch $A \cup B$ abzählbar.*

Beweis: Seien A und B zwei abzählbare Mengen, so dass zwei Surjektionen $g_A : \mathbb{N} \to A$ und $g_B : \mathbb{N} \to B$ existieren. Definiere eine Abbildung $g : \mathbb{N} \to A \cup B$ durch $g(2n) = g_A(n)$ und $g(2n+1) = g_B(n)$. Dann ist g eine Surjektion.

Da $A \subseteq A \cup B$ und A unendlich ist, muss auch $A \cup B$ unendlich sein, so dass eine Injektion $f : \mathbb{N} \to A \cup B$ existiert. Nach Satz 10.4 ist $A \cup B$ damit abzählbar. ⊠

Satz 10.7. *Seien $A_1, \ldots, A_n$ abzählbare Mengen, dann ist $A_1 \cup \ldots \cup A_n$ ebenfalls abzählbar.*

Der Beweis folgt durch vollständige Induktion entsprechend Satz 10.6.

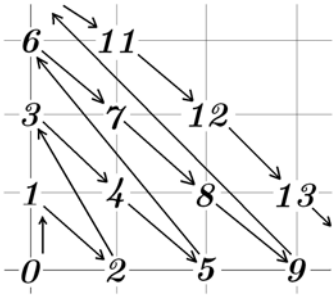
Wir beweisen auf unserem Weg als nächstes ein scheinbar sehr spezielles Resultat, welches uns schnell weiterhelfen wird.

Satz 10.8. *Es gilt:* $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Beweis: Wir nutzen die so genannte *Cantorsche Paarungsfunktion*

$$p : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \text{ definiert durch } p(i,j) := \frac{(i+j)(i+j+1)}{2} + i.$$

Man kann zeigen, dass diese Funktion eine Bijektion ist. Wir werden diesen Beweis nicht führen, uns stattdessen aber den Werteverlauf von p graphisch anschauen und versuchen, diesen zu interpretieren.



Wir sehen, dass die erste Spalte (also für $i = 0$) die Gestalt 0, 1, 3, 6, 10, 15, ... hat und somit für wachsendes j der Anfang der Summen $\sum_{k=0}^{j} k$ ist. Wir wissen aus Kapitel 2, dass $\sum_{k=0}^{j} k = \frac{1}{2}j(j+1)$ gilt. Damit lässt sich nun einsehen, dass sich $p(i,j)$ daraus ergibt, dass man jeweils noch den Spaltenindex i miteinbezieht. ⊠

Allgemeiner erhalten wir sofort folgende Aussage als Folgerung:

Satz 10.9. *Sei A abzählbar. Dann ist $A^n = \underbrace{A \times \ldots \times A}_{n-mal}$ abzählbar.*

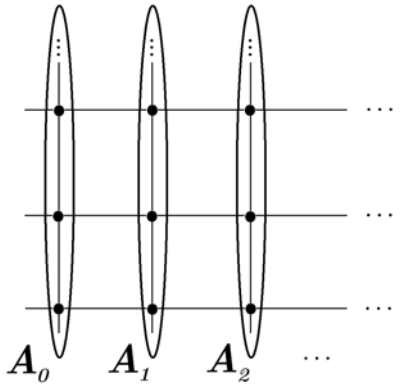
Dies folgt induktiv aus Satz 10.8.

Schließlich können wir mithilfe von Satz 10.8 zeigen, dass die abzählbare Vereinigung abzählbarer Mengen wieder abzählbar ist.

Satz 10.10. *Seien A_n für $n \in \mathbb{N}$ abzählbare Mengen. Dann ist auch $A := \bigcup_{n\in\mathbb{N}} A_n$ abzählbar.*

Beweis: Für jedes $n \in \mathbb{N}$ sei $f_n : \mathbb{N} \to A_n$ bijektiv. Definiere nun

$$g : \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n \text{ durch } (n, i) \mapsto f_n(i)$$



Dann ist g offenbar eine Surjektion.

Sei nun $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ eine Bijektion, dann ist auch $g \circ h : \mathbb{N} \to A$ nach Satz 3.3 eine Surjektion.

Da $A_0 \subseteq A$ und A_0 unendlich ist, muss auch A unendlich sein und damit existiert eine Injektion $t : \mathbb{N} \to A$. Mithilfe von Satz 10.4 folgt dann wieder die Behauptung. ⊠

Wir werden diesen Satz später im Beweis des Satzes 11.2 noch zu schätzen wissen. Doch als Abschluss dieses Kapitels wenden wir uns noch einmal den bekannten Zahlenmengen zu und untersuchen deren Mächtigkeiten:

Satz 10.11. *Die ganzen und die rationalen Zahlen sind abzählbar.*

Dies folgt unmittelbar aus den Sätzen 10.6 und 10.8. Weiterhin gilt:

Satz 10.12. *Die reellen Zahlen sind unendlich, aber nicht abzählbar.*

Man sagt, dass die reellen Zahlen *überabzählbar* sind.

Beweis: Angenommen, $\mathbb{R}$ wäre abzählbar. Insbesondere ist dann auch das Intervall $(0, 1) \subseteq \mathbb{R}$ abzählbar; hierbei bezeichne $(0, 1)$ die Menge $\{x \mid 0 < x < 1\}$. Sei also $a_0, a_1, \ldots, a_n, \ldots$ eine Aufzählung der reellen

Zahlen im Intervall $(0, 1)$ als Dezimalzahlen. Dann können wir die einzelnen Stellen in der Dezimalentwicklung selbst mittels der natürlichen Zahlen nummerieren und erhalten etwa folgende Situation:

$$\begin{aligned} a_0 &: \quad 0, a_{00}\, a_{01}\, a_{02} \ldots \\ a_1 &: \quad 0, a_{10}\, a_{11}\, a_{12} \ldots \\ a_2 &: \quad 0, a_{20}\, a_{21}\, a_{22} \ldots \\ &\vdots \end{aligned}$$

Wir definieren nun die folgende Dezimalzahl

$$b : \quad 0, b_0\, b_1\, b_2 \ldots$$

indem wir setzen

$$b_i := \begin{cases} 2, & \text{wenn } a_{ii} \neq 2 \\ 3, & \text{wenn } a_{ii} = 2 \end{cases}$$

Dann ist diese Zahl offensichtlich eine reelle Zahl im Intervall $(0, 1)$. Somit muss b auch in der obigen Aufzählung vorkommen, aber es gilt: $b \neq a_j$ für alle $j \in \mathbb{N}$. Damit haben wir wie gewünscht einen Widerspruch, so dass die ursprüngliche Annahme falsch gewesen sein muss. Diese Argumentation ist unter der Bezeichnung "Cantorsches Diagonalargument" bekannt. ⊠

An dieser Stelle schließen wir unsere Betrachtungen über unendliche Mengen. Sie können sich vorstellen, dass –nachdem wir eingesehen haben, dass die reellen Zahlen einen neuen Typ von Mächtigkeit unendlicher Mengen darstellen– wir die so genannten überabzählbaren Mengen noch tiefer betrachten könnten und viele interessante Eigenschaften finden würden.

11. Semantik aussagenlogischer Formeln

Aussagenlogische Formeln begegnen uns im Alltag sehr häufig. So können wir beispielsweise die Zulassungsvoraussetzungen für die Klausur unseres Kurses wie folgt beschreiben. Betrachten Sie dazu folgende Aussagen:

- p_0:= "Student erfüllt am Ende des Semesters 70% der ÜA."

- p_1:= "Student erfüllt am Ende des Semesters 30% der ÜA."
- p_2:= "Student erfüllt am Ende des Semesters 85% der Testate."
- q_1:= "Student wird zur Klausur zugelassen."
- q_2:= "Student wird nicht zur Klausur zugelassen."

Dann können Sie folgende Beziehungen zwischen den einzelnen Aussagen aufstellen, die Ihnen bereits inhaltlich bekannt sind:

- $p_0 \wedge p_2 \rightarrow q_1$
- $p_1 \rightarrow q_2$
- $p_1 \wedge p_2 \rightarrow q_2$
- $\neg(\, p_1 \wedge p_2 \rightarrow q_1\,)$

Sie sehen, wie schnell und übersichtlich wir dies mit den wenigen Symbolen ausdrücken können.

Wir werden uns zunächst damit beschäftigen, welche Zeichenfolgen uns interessieren. Stellen Sie sich vor, wir haben eine gegebene Grundmenge E von Zeichen, die wir aneinanderreihen können, um so Zeichenketten zu erhalten. Wir setzen weiterhin voraus, dass die Menge E folgende uns bekannte Grundzeichen enthält:

$$\wedge,\ \vee,\ \rightarrow,\ \leftrightarrow,\ \neg,\ (,\ )$$

Außerdem sei eine Menge $A \subseteq E$ von so genannten *Primaussagen* gegeben. Wir verwenden die Buchstaben $p, q, r, \ldots, p_0, p_1, \ldots$ als Variablen für Primaussagen. Natürlich sind die Elemente der Menge A von den oben genannten speziellen Grundzeichen verschieden, das heißt, es kann nicht sein, dass das Symbol "$\wedge$" und die Variable p_{17} übereinstimmen.

Aus diesen Grundzeichen E können wir nun Zeichenketten bilden, wie etwa oben im Beispiel zu erkennen ist, aber auch Zeichenketten der Form "$p_0 = p_1 \rightarrow \wedge\,(\,q$". Nicht alle solche Zeichenketten sind für uns interessant bzw. sinnvoll (wie bei der letztgenannten zu erkennen ist). Deswegen werden wir die Worte oder Sätze unserer so genannten aussagenlogischen Sprache, die wir gerade entwickeln, schrittweise definieren.

Die für uns interessanten Zeichenketten nennen wir *Formeln*, die induktiv wie folgt definiert sind:

Definition 11.1. *Die Menge* $\texttt{Fml} = \texttt{Fml}_E$ *der* aussagenlogischen *E-Formeln ist die kleinste Menge* F *mit:*

(a) $A \subseteq F$
(b) $\varphi \in F \Rightarrow \neg\varphi \in F$
(c) $\varphi, \psi \in F \Rightarrow (\varphi\, e\, \psi) \in F$ *für* $e \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

Zur Erinnerung: Wir verwenden das Symbol "$\rightarrow$", um eine Implikation innerhalb unserer formalen Sprache zu kennzeichen und das Symbol "$\Rightarrow$", um eine Implikation unserer Metasprache anzudeuten; letzteres hätten wir auch mit den Worten "Wenn ..., dann ..." umschreiben können.

Im Folgenden verwenden wir die griechischen Buchstaben $\varphi, \psi, \chi, \ldots$ als Variablen für Formeln.

Aus der Definition ergibt sich das folgende Induktionsprinzip für (aussagenlogische) Formeln:

> **Wenn** B eine Bedingung ist, die auf jedes $p \in A$ zutrifft
> und außerdem gilt
> - wenn $B(\varphi)$ auch $B(\neg\varphi)$ und
> - wenn $B(\varphi)$ und $B(\psi)$ auch $B((\varphi e \psi))$
>
> für $e \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.
>
> **Dann** trifft B für alle Formeln zu.

Beweis: Die Menge der Formeln $\{\varphi \,|\, B(\varphi)\}$, die die Bedingung B erfüllen, hat alle drei Eigenschaften der Definition; die Menge $\texttt{Fml}$ war aber die kleinste solche Menge, also ist $\texttt{Fml}$ eine Teilmenge von $\{\varphi \mid B(\varphi)\}$. ⊠

Eine wichtige Eigenschaft der Formeln ist ihre *eindeutige Lesbarkeit*, die unter anderem besagt, dass $(\varphi \wedge \psi)$ nicht mit einer Formel $(\varphi' \wedge \psi')$ verwechselt werden kann; im Einzelnen kann man Folgendes für beliebige Aussagenvariablen p sowie Formeln φ, ψ und χ beweisen:

(a) Wenn $(\varphi\, e\, \psi) = (\varphi'\, e'\, \psi')$, dann $e = e', \varphi = \varphi'$ und $\psi = \psi'$.
(b) Wenn $\neg\varphi = \neg\psi$, dann $\varphi = \psi$.
(c) $(\varphi\, e\, \psi) \neq \neg\chi$
(d) $p \neq (\varphi\, e\, \psi)$ und $p \neq \neg\chi$

Kommen wir zu einer anderen Problematik: Im Kapitel 10 haben wir uns bereits mit kleinen unendlichen Mengen beschäftigt. Wir werden nun sehen, dass auch die Menge der Formeln abzählbar ist, wenn wir das Alphabet (minimal) beschränken: Wir können o.B.d.A. annehmen, dass unser betrachtetes Alphabet E abzählbar ist, denn nach obiger Wahl haben wir nur die sieben Grundzeichen hineingesteckt und zusätzlich eine Menge von Aussagenvariablen A. Da unsere Formeln selbst immer endlich sind, brauchen wir pro Formel nur endlich viele Variablen. Damit genügen insgesamt abzählbar viele solche, so dass insgesamt auch E nur abzählbar sein muss.

Satz 11.2. *Wenn die Menge E abzählbar ist, so ist die Menge der Formeln $\texttt{Fml}_E$ über dem Alphabet E abzählbar.*

Beweis: Sei A_n die Menge der Formeln der Länge n für ein $n \in \mathbb{N}\setminus\{0\}$. Dabei ist die Länge einer Formel gleich der (endlichen) Anzahl der in ihr vorkommenden Symbole, das heißt, es gilt beispielsweise $p \in A_1$, $\neg p \in A_2$, $(p \wedge p) \in A_5$, ... usw.

Dann ist A_n jeweils eine abzählbare Menge für beliebige natürliche Zahlen n: Für ein festes n haben wir n Möglichkeiten, je ein Symbol aus dem abzählbaren Alphabet E auszuwählen, so dass A_n in die Menge $E^n \sim \mathbb{N}^n \sim \mathbb{N}$ eingebettet werden kann. Also ist A_n endlich oder abzählbar. Aber schon für die Auswahl des ersten Symbols eines Elements in A_n haben wir unendlich viele Möglichkeiten, eine Aussagenvariable aus $A \subseteq E$ auszuwählen, so dass A_n in der Tat unendlich ist und somit selbst abzählbar.

Offenbar gilt auch, dass $\texttt{Fml} = \bigcup_{n\in\mathbb{N}\setminus\{0\}} A_n$ und somit ist nach Satz 10.10 dies wie gewünscht eine abzählbare Menge. ⊠

Wenn wir den obigen Beweis analysieren, stellen wir fest, dass wir analog zeigen können, dass die Menge der Formeln aus einem endlichen Alphabet ebenfalls abzählbar ist.

Wir machen jetzt einen Gedankensprung. Bisher haben wir die Syntax aussagenlogischer Sprachen betrachtet. Wir haben verstanden, welche

Zeichenketten für uns interessant sind – nämlich die Menge der Formeln. Jetzt werden wir uns um die Bedeutung, die so genannte Semantik der Formeln bzw. der Sprache, kümmern. Dafür definieren wir den Begriff des *Modells* oder der *Interpretation* $\mathfrak{A}$ einer aussagenlogischen Sprache A wie folgt: Es sei $\mathfrak{A}$ eine Abbildung, die die Wahrheitswerte ("0" oder "1") für alle Primaussagen festlegt, das heißt, wir haben eine Abbildung der Gestalt: $\mathfrak{A} : A \to \{0, 1\}$.

Wir werden nun, ausgehend von der fixierten Abbildung $\mathfrak{A}$, *rekursiv* (bzw. *induktiv*) eine Abbildung $\mathfrak{A}^* : \texttt{Fml} \to \{0, 1\}$ (als Erweiterung von $\mathfrak{A}$) definieren:

$$\begin{aligned}
\mathfrak{A}^*(p) &:= \mathfrak{A}(p) \\
\mathfrak{A}^*(\neg\varphi) &:= 1 - \mathfrak{A}^*(\varphi) \\
\mathfrak{A}^*(\varphi \vee \psi) &:= \max(\mathfrak{A}^*(\varphi), \mathfrak{A}^*(\psi)) \\
\mathfrak{A}^*(\varphi \wedge \psi) &:= \min(\mathfrak{A}^*(\varphi), \mathfrak{A}^*(\psi)) \\
\mathfrak{A}^*(\varphi \to \psi) &:= \max(1 - \mathfrak{A}^*(\varphi), \mathfrak{A}^*(\psi)) \\
\mathfrak{A}^*(\varphi \leftrightarrow \psi) &:= \begin{cases} 1 & \text{falls } \mathfrak{A}^*(\varphi) = \mathfrak{A}^*(\psi) \\ 0 & \text{sonst} \end{cases}
\end{aligned}$$

Wir erleichtern uns das Leben, indem wir im Folgenden oft $\mathfrak{A}(\varphi)$ statt $\mathfrak{A}^*(\varphi)$ schreiben, da es aufgrund der Überlagerung beider Abbildungen keine Probleme bereitet.

Wir widmen uns nun einem weiteren wichtigen Begriff in der Aussagenlogik: Der Begriff der *Gültigkeit* von Formeln bezüglich einer gegebenen Interpretation oder eines Modells:

Definition 11.3. *Wir definieren:* $\mathfrak{A} \vDash \varphi \ :\Longleftrightarrow\ \mathfrak{A}(\varphi) = 1$. *In diesem Fall sagt man: "*$\mathfrak{A}$ *ist ein* Modell *von* φ*" oder "*$\mathfrak{A}$ *erfüllt* φ*".*

Entsprechend bekannter Konventionen schreiben wir $\mathfrak{A} \nvDash \varphi$ im Falle, dass $\mathfrak{A} \vDash \varphi$ nicht gilt.

Satz 11.4. *Es gilt:*

$$\mathfrak{A} \vDash p \quad \Leftrightarrow \quad \mathfrak{A}(p) = 1$$

$$\begin{aligned}
\mathfrak{A} \models \neg\varphi \quad &\Leftrightarrow \quad \mathfrak{A} \not\models \varphi \\
\mathfrak{A} \models (\varphi \wedge \psi) \quad &\Leftrightarrow \quad (\, \mathfrak{A} \models \varphi \;\; \textit{und} \;\; \mathfrak{A} \models \psi \,) \\
\mathfrak{A} \models (\varphi \vee \psi) \quad &\Leftrightarrow \quad (\, \mathfrak{A} \models \varphi \;\; \textit{oder} \;\; \mathfrak{A} \models \psi \,) \\
\mathfrak{A} \models (\varphi \to \psi) \quad &\Leftrightarrow \quad (\, \mathfrak{A} \models \varphi \Rightarrow \mathfrak{A} \models \psi \,) \\
\mathfrak{A} \models (\varphi \leftrightarrow \psi) \quad &\Leftrightarrow \quad (\, \mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{A} \models \psi \,)
\end{aligned}$$

Der Beweis ist aufgrund der Definition von $\mathfrak{A}^*$ leicht zu führen. Wir überlassen dies als Übungsaufgabe. Die letzte Zeile der Definition ist wieder ein sehr schönes Beispiel für die unterschiedliche Verwendung der Symbole "$\leftrightarrow$" und "$\Leftrightarrow$". Sie besagt, dass $\mathfrak{A} \models (\varphi \leftrightarrow \psi)$ genau dann gilt, wenn aus $\mathfrak{A} \models \varphi$ immer $\mathfrak{A} \models \psi$ und umgekehrt folgt.

Definition 11.5. *Wir schreiben "$\models \varphi$", wenn für jedes Modell $\mathfrak{A}$ gilt: $\mathfrak{A} \models \varphi$. Wir sagen in diesem Fall "φ ist logisch gültig" oder φ ist eine Tautologie.*

Wir erweitern unsere Sprechweise und kürzen ab sofort mit der Schreibweise $\mathfrak{A} \models W$ für eine Formelmenge W ab, dass $\mathfrak{A} \models \varphi$ für alle $\varphi \in W$ gilt. Darüber hinaus sagen wir für Formelmengen W und U, dass $W \models U$, wenn für jedes Modell $\mathfrak{A}$ mit $\mathfrak{A} \models W$ auch $\mathfrak{A} \models U$ gilt. Entsprechend definieren wir $W \models \varphi$, wenn $W \models \{\varphi\}$. Offensichtlich gilt $\models \varphi$ genau dann, wenn $\varnothing \models \varphi$.

Tautologien spielen eine wichtige Rolle. Sie sind per Definition unabhängig vom gewählten Modell und immer gültig. Offensichtlich gibt es aber auch Formeln, die keine Tautologien sind, wie beispielsweise $(p \wedge p)$, denn wenn p in einem Modell $\mathfrak{A}$ auf Null gesetzt wird, dann gilt diese Formel nicht in $\mathfrak{A}$. Es gibt sogar Formeln, die immer falsch interpretiert werden, beispielsweise die Formel $(p \wedge \neg p)$ – unabhängig vom Wahrheitswert für p wird diese Formel immer mit "falsch" interpretiert.

Nach diesen beiden negativen Beispielen zählen wir eine Reihe von wichtigen und uns später nützlichen Tautologien auf:

Satz 11.6. *Die folgenden Formeln sind Tautologien:*

(a) $\varphi \to \varphi$
(b) $\neg\varphi \vee \varphi$

(c) $\neg(\varphi \wedge \neg\varphi)$
(d) $\neg\neg\varphi \leftrightarrow \varphi$
(e) $(\varphi \wedge (\varphi \rightarrow \psi)) \rightarrow \psi$
(f) $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \chi)) \rightarrow (\varphi \rightarrow \chi)$
(g) $\varphi \rightarrow (\psi \rightarrow \varphi)$
(h) $((\neg\varphi \rightarrow \varphi) \rightarrow \varphi)$
(i) $((\varphi \rightarrow \neg\varphi) \rightarrow \neg\varphi)$
(j) $((\varphi \wedge \psi) \rightarrow \chi) \leftrightarrow (\varphi \rightarrow (\psi \rightarrow \chi))$
(k) $((\varphi \wedge \psi) \wedge \chi) \leftrightarrow (\varphi \wedge (\psi \wedge \chi))$
(l) $(\varphi \vee \psi) \vee \chi) \leftrightarrow (\varphi \vee (\psi \vee \chi))$
(m) $((\varphi \leftrightarrow \psi) \leftrightarrow \chi) \leftrightarrow (\varphi \leftrightarrow (\psi \leftrightarrow \chi))$
(n) $(\varphi \wedge \psi) \leftrightarrow (\psi \wedge \varphi)$
(o) $(\varphi \vee \psi) \leftrightarrow (\psi \vee \varphi)$
(p) $(\varphi \leftrightarrow \psi) \leftrightarrow (\psi \leftrightarrow \varphi)$
(q) $(\varphi \wedge (\psi \vee \chi)) \leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$
(r) $(\varphi \vee (\psi \wedge \chi)) \leftrightarrow ((\varphi \vee \psi) \wedge (\psi \vee \chi))$
(s) $(\varphi \rightarrow (\psi \wedge \chi)) \leftrightarrow ((\varphi \rightarrow \psi) \wedge (\varphi \rightarrow \chi))$
(t) $((\psi \vee \chi) \rightarrow \varphi) \leftrightarrow ((\psi \rightarrow \varphi) \wedge (\chi \rightarrow \varphi))$
(u) $\neg(\varphi \wedge \psi) \leftrightarrow (\neg\varphi \vee \neg\psi)$
(v) $\neg(\varphi \vee \psi) \leftrightarrow (\neg\varphi \wedge \neg\psi)$
(w) $\neg(\varphi \leftrightarrow \psi) \leftrightarrow (\varphi \leftrightarrow \neg\psi)$
(x) $(\varphi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\varphi)$
(y) $(\varphi \rightarrow \psi) \leftrightarrow (\neg\varphi \vee \psi)$
(z) $(\varphi \leftrightarrow \psi) \leftrightarrow ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$

Beweis: Betrachten wir exemplarisch die Formel $\varphi \rightarrow (\psi \rightarrow \varphi)$. Wir nutzen die Definition, um diese Formel als Tautologie nachzuweisen: Wir müssen zeigen, dass $\models (\varphi \rightarrow (\psi \rightarrow \varphi))$ gilt. Nach Definition ist dies äquivalent dazu, dass für beliebige Modelle $\mathfrak{A}$ gilt: $\mathfrak{A} \models (\varphi \rightarrow (\psi \rightarrow \varphi))$. Nach Satz 11.4 ist dies äquivalent zu der Behauptung: Wenn $\mathfrak{A} \models \varphi$, dann auch $\mathfrak{A} \models (\psi \rightarrow \varphi)$. Nehmen wir daher an, dass $\mathfrak{A}$ ein Modell von φ sei. Es bleibt zu zeigen, dass $\mathfrak{A} \models (\psi \rightarrow \varphi)$. Dies ist wiederum nach Satz 11.4 äquivalent zu der Behauptung: Wenn nun zusätzlich $\mathfrak{A} \models \psi$, dann $\mathfrak{A} \models \varphi$. Nehmen wir daher an, dass $\mathfrak{A}$ auch noch ein Modell von ψ sei. Wir müssen jetzt zeigen, dass $\mathfrak{A}$ ein Modell von φ

ist, aber das entspricht exakt unserer ersten Voraussetzung und somit ist die Behauptung bewiesen. Die betrachtete Formel ist also immer wahr und somit eine Tautologie. ⊠

Es gibt eine übersichtliche und kürzere Methode des Beweises, nämlich per Wahrheitswertetabelle. Dabei berechnen wir ausgehend von den Wahrheitswerten der Grundbestandteile einer Formel die jeweiligen Wahrheitswerte der nächstgrößeren (Teil-)Formel, bis am Schluss der Wahrheitswert für die gesamte Formel feststeht. Dabei nutzen wir schrittweise (nämlich induktiv über den Formelaufbau) die Definition der Gültigkeit. Wir zeigen dieses Prinzip an einem Beispiel:

φ	ψ	$\psi \to \varphi$	$\varphi \to (\psi \to \varphi)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

oder kürzer geschrieben, indem wir die entsprechende Teilformel mit dem Verknüpfungszeichen derselben identifizieren und den entsprechenden Wahrheitswert darunter schreiben:

φ	ψ	φ	$\to$	$(\psi$	$\to$	$\varphi)$
0	0	0	1	0	1	0
0	1	0	1	1	0	0
1	0	1	1	0	1	1
1	1	1	1	1	1	1

Sie sehen, es kommt nur auf die entsprechenden Wahrheitswerte von φ und ψ an, um den Wahrheitsheitswert der gesamten Formel zu bestimmen. Insbesondere kommt es nicht auf die spezielle Gestalt von φ und ψ an. Deswegen können wir diese Methode benutzen.

Wenn wir die Wahrheitswertetabelle aufstellen, dann schauen wir am Ende, welcher Wahrheitswert unter dem äußersten Verknüpfungszeichen (hier "$\to$") steht. Wenn dort nur der Wahrheitswert "1" zu finden ist, haben wir eine Tautologie.

Wir beweisen nun einfache erste Zusammenhänge. Das grundlegende Prinzip "Modus Ponens" besagt:

Satz 11.7. *Wenn* $W \models \varphi$ *und* $W \models (\varphi \to \psi)$*, dann* $W \models \psi$*.*

Beweis: Sei dafür ein aussagenlogisches Modell $\mathfrak{A}$ gegeben, so dass $\mathfrak{A} \models W$ gilt. Wir behaupten, dass dann auch $\mathfrak{A} \models \psi$ gilt. Nach Voraussetzung gilt insbesondere $\mathfrak{A} \models \varphi$ und $\mathfrak{A} \models \varphi \to \psi$, also auch die (Meta-)Implikation: Wenn $\mathfrak{A} \models \varphi$, dann $\mathfrak{A} \models \psi$. Aber damit folgt dann auch sofort die Behauptung. ⊠

Satz 11.8. *Es gilt* $W \models (\varphi \wedge \psi)$ *genau dann, wenn* $W \models \varphi$ *und* $W \models \psi$*.*

Der Beweis verläuft analog, so dass wir diesen als Übungsaufgabe überlassen.

Wir schreiben kurz $W, \varphi_1, \ldots, \varphi_n \models \varphi$ für $W \cup \{\varphi_1, \ldots, \varphi_n\} \models \varphi$ sowie $\mathfrak{A} \models W, \varphi$ für $\mathfrak{A} \models W \cup \{\varphi\}$ und beweisen den folgenden

Satz 11.9. $W \models (\varphi \to \psi)$ *gdw.* $W, \varphi \models \psi$*.*

Beweis: Zunächst die behauptete Richtung von links nach rechts: Es sei $\mathfrak{A} \models W, \varphi$. Dann gilt nach Voraussetzung, dass $\mathfrak{A} \models \varphi \to \psi$, das heißt, wenn $\mathfrak{A} \models \varphi$, so $\mathfrak{A} \models \psi$. Also $\mathfrak{A} \models \psi$.
Und schließlich die noch fehlende Richtung von rechts nach links: Sei $\mathfrak{A} \models W$. Wenn $\mathfrak{A} \models \varphi$, dann gilt (nach Voraussetzung), dass $\mathfrak{A} \models \psi$, das heißt, $\mathfrak{A} \models \varphi \to \psi$. ⊠

Dieser Satz beinhaltet ein sehr wichtiges Prinzip und wird als *Deduktionssatz* (für "⊨") bezeichnet. Etwas allgemeiner können wir beweisen:

Satz 11.10. $W \models ((\varphi_1 \wedge \ldots \wedge \varphi_n) \to \psi)$ *gdw.* $W, \varphi_1, \ldots, \varphi_n \models \psi$*.*

Wir definieren induktiv (oder rekursiv) über den Formelaufbau die Menge $\mathsf{prim}(\varphi)$ der *Primaussagen in einer Formel* φ, so dass beispielsweise gilt: $\mathsf{prim}(\, p \wedge q \to r \,) = \{p, q, r\}$, wie folgt:

$$\begin{aligned} \mathsf{prim}(p) &:= \{p\} \\ \mathsf{prim}(\neg\varphi) &:= \mathsf{prim}(\varphi) \\ \mathsf{prim}(\, \varphi \, e \, \psi \,) &:= \mathsf{prim}(\varphi) \cup \mathsf{prim}(\psi) \text{ für } e \in \{\wedge, \vee, \to, \leftrightarrow\} \end{aligned}$$

Für eine Formelmenge W definieren wir $\mathsf{prim}(W)$ als die Vereinigung der Mengen der Primaussagen in den Formeln in W, also

$$\mathsf{prim}(W) := \bigcup_{\varphi \in W} \mathsf{prim}(\varphi).$$

Analog definieren wir die *Ersetzung von p durch ψ in φ*, kurz $\varphi(p/\psi)$. Sei etwa $\varphi := (p \wedge q \to r)$, dann ist $\varphi(p/q) = (q \wedge q \to r)$ und etwa komplexer $\varphi(p/\psi) = (\psi \wedge q \to r)$.

Induktiv über den Formelaufbau definieren wir für Primaussagen p und q sowie einer Formel ψ:

$$\begin{aligned} q(p/\psi) &:= \begin{cases} \psi & \text{falls } q = p \\ q & \text{sonst} \end{cases} \\ (\neg\varphi)(p/\psi) &:= \neg(\, \varphi(p/\psi)\,) \\ (\varphi\, e\, \chi)(p/\psi) &:= \varphi(p/\psi)\, e\, \chi(p/\psi) \quad \text{für } e \in \{\wedge, \vee, \to, \leftrightarrow\} \end{aligned}$$

Satz 11.11. *Wenn $p \notin \mathsf{prim}(W)$ und $W \vDash \varphi$, dann gilt: $W \vDash \varphi(p/\chi)$.*

Beweis: Sei also ein Modell $\mathfrak{A}$ mit $\mathfrak{A} \vDash W$ gegeben. Wir müssen zeigen, dass $\mathfrak{A} \vDash \varphi(p/\chi)$: Sei dafür $\overline{\mathfrak{A}} := \mathfrak{A}_{p,\chi}$ die Abbildung $\overline{\mathfrak{A}} : A \to \{0,1\}$ definiert durch:

$$\overline{\mathfrak{A}}(q) := \begin{cases} \mathfrak{A}^*(\chi), & \text{falls } q = p \\ \mathfrak{A}(q), & \text{sonst} \end{cases}$$

Durch Induktion auf φ folgt, dass

$$(\star) \qquad \overline{\mathfrak{A}}^*(\varphi) = \mathfrak{A}^*(\, \varphi(p/\chi)\,)$$

Wir zeigen nur den Induktionsanfang – sei dafür zunächst $\varphi := p$ eine Primaussage. Dann gilt:

$$\overline{\mathfrak{A}}^*(\varphi) = \overline{\mathfrak{A}}^*(p) = \overline{\mathfrak{A}}(p) = \mathfrak{A}^*(\chi) = \mathfrak{A}^*(\, p(p/\chi)\,) = \mathfrak{A}^*(\, \varphi(p/\chi)\,).$$

Sei nun $\varphi := q \neq p$. Dann gilt entsprechend:

$$\overline{\mathfrak{A}}^*(\varphi) = \overline{\mathfrak{A}}^*(q) = \overline{\mathfrak{A}}(q) = \mathfrak{A}(q) = \mathfrak{A}(\, q(p/\chi)\,) = \mathfrak{A}(\, \varphi(p/\chi)\,).$$

Damit ist der Induktionsanfang gezeigt. Der Induktionsschritt geht ähnlich.

Insbesondere gilt dann: $\overline{\mathfrak{A}}^*(\psi) = \mathfrak{A}^*(\psi) = 1$ für $\psi \in W$, da $p \notin \mathsf{prim}(W)$, und deswegen folgt $\psi(p/\chi) = \psi$. Somit folgt $\overline{\mathfrak{A}} \vDash W$ und damit nach Voraussetzung schließlich $\overline{\mathfrak{A}} \vDash \varphi$.

Nun gilt nach Konstruktion und $(\star)$, dass $\mathfrak{A}^*(\ \varphi(p/\chi)\ ) = \overline{\mathfrak{A}}(\varphi) = 1$.

⊠

Die gleiche Beweisidee lässt sich auch für die folgende Behauptung verwenden:

Satz 11.12. *Es gilt:* $\vDash (\varphi \leftrightarrow \psi) \rightarrow (\ \chi(p/\varphi) \leftrightarrow \chi(p/\psi)\ )$.

Beweis: Sei $\mathfrak{A}$ ein beliebiges aussagenlogisches Modell. Wir müssen zeigen, dass dieses Modell die Formel erfüllt. Da es sich um eine Implikation handelt, nutzen wir Satz 11.4, um diese aufzusplitten und nehmen zusätzlich an, dass $\mathfrak{A} \vDash (\varphi \leftrightarrow \psi)$ gilt. Es genügt nun zu zeigen, dass $\mathfrak{A} \vDash \chi(p/\varphi) \leftrightarrow \chi(p/\psi)$ gilt. Wie angekündigt nutzen wir die Idee aus dem Beweis von Satz 11.11 und setzen in Analogie $\overline{\mathfrak{A}} := \mathfrak{A}_{p,\varphi}$. Da nach Voraussetzung $\mathfrak{A}^*(\varphi) = \mathfrak{A}^*(\psi)$ gilt, wissen wir, dass $\overline{\mathfrak{A}}$ auch gleich $\mathfrak{A}_{p,\psi}$ ist. Also gilt wie gewünscht:

$$\mathfrak{A}^*(\ \chi(p/\varphi)\ ) = \overline{\mathfrak{A}}^*(\chi) = \mathfrak{A}^*(\ \chi(p/\psi)\ ).$$ ⊠

12. Formale Beweise in der Aussagenlogik

Ein wesentlicher Zug der Mathematik ist die Verifizierbarkeit der mathematischen Behauptungen. Behauptet ein Mathematiker einen Satz, so legt er auch einen Beweis vor. Beweise sind berechenbar in dem Sinne, dass man anhand eines Algorithmus feststellen kann, ob die Beweisschritte richtig durchgeführt worden sind. Wenn ja, so liegt wirklich ein Beweis vor und die Behauptung wird geglaubt. Wenn nicht, können wir wegen mangelnder Verifizierung die Behauptung noch nicht glauben.

Wir erhoffen uns, den Begriff des *formalen Beweises* zu charakterisieren, so dass wir schließlich haben:

$$W \vDash \varphi \text{ gdw. Es gibt einen formalen Beweis von } \varphi.$$

Dazu geben wir eine Menge von Axiomen und eine Schluss- bzw. Ableitungsregel vor. Daraus werden wir den gewünschten Begriff von Beweisbarkeit definieren.

Aber zunächst widmen wir uns der Menge der Axiome; diese sollten wir nicht anzweifeln (müssen). Die Menge von Axiomen sollte aus Formeln bestehen, die wir sehr leicht glauben, die also immer gültig sind, Tautologien. Wir definieren:

(A1)	$\varphi \to (\psi \to \psi), \quad \neg(\psi \to \psi) \to \varphi$
(A2)	$\varphi \to (\psi \to \varphi), \quad \varphi \to (\neg\varphi \to \psi)$
(A3)	$(\varphi \to \neg\varphi) \to \neg\varphi, \quad (\neg\varphi \to \varphi) \to \varphi$
(A4)	$\varphi \to (\psi \to (\varphi \wedge \psi))$
(A5)	$(\varphi \wedge \psi) \to \varphi, \quad (\varphi \wedge \psi) \to \psi$
(A6)	$((\varphi \to \psi) \wedge (\varphi \to (\psi \to \chi))) \to (\varphi \to \chi)$
(A7)	$(\varphi \leftrightarrow \psi) \to ((\varphi \to \psi) \wedge (\psi \to \varphi))$
(A8)	$(\varphi \vee \psi) \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$
(A9)	$(\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$
(A10)	$(\varphi \leftrightarrow \psi) \leftrightarrow ((\varphi \to \psi) \wedge (\psi \to \varphi))$

Beim genauen Betrachten werden Sie beispielsweise feststellen, dass Axiom 7 und Axiom 10 sehr ähnlich sind. Der Grund ist, dass wir beide Versionen unterschiedlich benutzen möchten: Axiom 7 wird uns helfen, um aus Äquivalenzen zwei Implikationen zu schlussfolgern; Axiome 8 bis 10 dagegen stellen eine Liste von nützlichen Äquivalenzen dar.

Lassen Sie mich eine grundsätzliche Bemerkung zur Auswahl der Axiome machen: Die Wahl der Axiome ist nicht eindeutig. Es existieren verschiedene Auswahlen, die äquivalente Ergebnisse produzieren – wir werden dies zu Anfang des Kapitels 13 genauer beleuchten. Unsere Auswahl ist so gewählt, dass wir mit minimalem Aufwand durch die Beweise (einschließlich des Vollständigkeitssatzes 13.19) kommen und auf der anderen Seite trotzdem die Menge der Axiome so klein (und damit übersichtlich) wie möglich zu halten.

Weiterhin nutzen wir unser bekanntes Wissen aus Satz 11.6, um festzustellen, dass jedes Axiom eine Tautologie ist. Hierbei sind die Formeln φ, ψ und χ Variablen für aussagenlogische Formeln, das heißt, dass wir

nicht nur die Axiome so verwenden können, wie diese oben aufgezählt werden, sondern wir verstehen diese Aufzählung als Schema, in das wir beliebige Formeln für die gegebenen einsetzen können. So ist etwa der erste Teil des Axioms 1 zu lesen als folgendes Template:

$$\texttt{Erste\_Formel} \to (\texttt{Zweite\_Formel} \to \texttt{Zweite\_Formel}).$$

Somit gibt uns dieses Axiom auch die folgenden beiden Versionen, die wir in späteren Beweisen verwenden können: zum einen $\psi \to (\varphi \to \varphi)$, aber auch die etwas komplexere Formel

$$(\varphi \to \psi) \to ((\varphi \wedge \chi \to \psi) \to (\varphi \wedge \chi \to \psi)).$$

Weiterhin benutzen wir für die Menge der Axiome die Abkürzung `Axiome`, das heißt, dass in dieser so bezeichneten Menge alle Axiome enthalten sind, die wir durch Substitution im obigen Sinne aus dem Schema –gegeben durch (A1) bis (A10)– erhalten.

In der Aussagenlogik werden wir nur eine Deduktionsregel verwenden, nämlich das Prinzip "*Modus Ponens*":

(MP) Aus φ und $\varphi \to \psi$ folgt ψ.

Wir sind jetzt soweit, das aussagenlogische Beweiskalkül zu definieren, welches wir im Folgenden verwenden werden:

Definition 12.1. *Wir sagen $W \vdash \varphi$, "φ ist aus W herleitbar", genau dann, wenn $\varphi \in W^*$, wobei W^* die kleinste Menge mit folgenden Eigenschaften ist:*

(a) $\texttt{Axiome} \subseteq W^*$
(b) $W \subseteq W^*$
(c) *Die Menge W^* ist unter Modus Ponens abgeschlossen, das heißt, wenn $\varphi \in W^*$ und $(\varphi \to \psi) \in W^*$, so $\psi \in W^*$.*

Folgende Aussage wird uns im Weiteren helfen, die obige Definition besser anwenden zu können:

Satz 12.2. *Seien X und W Formelmengen, so dass $(\texttt{Axiome} \cup W) \subseteq X$ gilt und X unter (MP) abgeschlossen ist. Dann ist $\{\varphi \mid W \vdash \varphi\} \subseteq X$.*

Dies gilt offensichtlich, weil das in der Definition 12.1 auftauchende W^* die kleinste Menge mit den geforderten Eigenschaften ist und somit eine Teilmenge der hier erscheinenden Menge X sein muss.

Wir definieren in Anlehnung an den Gültigkeitsbegriff aus Kapitel 11, dass "$\vdash \varphi$" gelte, wenn $\varnothing \vdash \varphi$. Damit gilt "$\vdash \varphi$" genau dann, wenn die Formel φ nur aus den Axiomen herleitbar ist. Weiterhin setze für eine Formelmenge U, dass $W \vdash U$, wenn für jedes $\varphi \in U$ gilt $W \vdash \varphi$. Mithilfe dieser Bezeichnung erhalten wir eine Art Transitivitätseigenschaft wie folgt:

Satz 12.3. *Wenn $W \vdash U$ und $U \vdash \varphi$, dann $W \vdash \varphi$.*

Beweis: Hierfür setze $X := \{\psi \mid W \vdash \psi\}$. Dann genügt es zu zeigen, dass $\varphi \in X$. Nun ist X aber unter (MP) abgeschlossen und es gilt, dass: $(\texttt{Axiome} \cup U) \subseteq X$. Nach Satz 12.2, angewendet für die Formelmenge U, gilt dann wie gewünscht: $\varphi \in \{\psi \mid U \vdash \psi\} \subseteq X$ ⊠

Unser Herleitungsbegriff ist *richtig* (oder *korrekt*) in dem Sinne, dass aus W nur Formeln herleitbar sind, die aus W auch logisch folgen:

Satz 12.4 (Korrektheitssatz)**.** *Wenn $W \vdash \varphi$, so $W \vDash \varphi$.*

Beweis: Setze $X := \{\varphi \mid W \vDash \varphi\}$. Dann gilt:

(a) $\texttt{Axiome} \subseteq X$, denn jedes Axiom ψ ist eine Tautologie und somit gilt $\vDash \psi$. Insbesondere gilt $W \vDash \psi$, also $\psi \in X$.

(b) $W \subseteq X$; dies ist klar, denn für ein $\varphi \in W$ gilt offensichtlich $W \vDash \varphi$ und damit $\varphi \in X$.

(c) Die Menge X ist nach Satz 11.7 unter (MP) abgeschlossen.

Damit gilt nach Satz 12.2 wie gewünscht: $\{\varphi \mid W \vdash \varphi\} \subseteq X$, so dass herleitbare Formeln auch gültig sind. ⊠

Wir führen jetzt den Begriff des *formalen Beweises* ein, der uns auf dem Weg zum Verständnis des Herleitungsbegriffs am meisten interessiert.

Definition 12.5. *Ein (formaler) Beweis einer Formel φ aus einer Formelmenge W, kurz W-Beweis, ist eine Folge $b := (b_i | i < n)$ von Formeln mit folgenden Eigenschaften:*

(a) *Es existiert ein Index $i < n$, so dass $\varphi = b_i$.*

(b) *Für jedes $i < n$ gilt eine der folgenden Bedingungen:*

  (i) *b_i ist ein Axiom oder $b_i \in W$.*

  (ii) *Es existieren Indizes $h, j < i$ mit $b_j = (b_h \to b_i)$, das heißt: b_i folgt aus früheren b_h, b_j durch (MP), etwa schematisch dargestellt durch:*

$$\begin{array}{ll} \text{Indexstelle } h\text{:} & b_h \\ \text{Indexstelle } j\text{:} & b_h \to b_i \\ \text{Indexstelle } i\text{:} & b_i \end{array}$$

Der für uns interessante Zusammenhang zwischen beiden Begriffen wird in der folgenden Aussage formuliert:

Satz 12.6. *Es ist $W \vdash \varphi$ genau dann, wenn es einen Beweis für φ aus W gibt.*

Beweis: Wir zeigen zunächst die Rückrichtung ($\Leftarrow$): Sei dafür $b = (b_i \mid i < n)$ ein Beweis von φ aus W. Wir zeigen per Induktion auf i, dass sich jedes b_i aus W herleiten lässt. Für den Induktionsanfang betrachten wir den Fall $i = 0$. Dann gilt per Definition eines formalen Beweises, dass $b_0 \in (\texttt{Axiome} \cup W)$. Mit den ersten beiden Eigenschaften aus Definition 12.1 gilt somit offensichtlich, dass $b_0 \in W^*$, also insbesondere $W \vdash b_0$. Die analoge Analyse und die Tatsache, dass W^* unter (MP) abgeschlossen ist, zeigt den Induktionsschritt.

Es bleibt die Richtung ($\Rightarrow$) zu zeigen. Hierfür definieren wir die Menge $X := \{\psi \mid \psi \text{ hat einen Beweis aus } W\}$ und zeigen nun, dass $\varphi \in X$ gilt. Hierfür nutzen wir wieder den Satz 12.2 und zeigen die geforderten Eigenschaften: Es gilt $(W \cup \texttt{Axiome}) \subseteq X$, denn für ein Axiom ψ ist die Folge $b = (\psi)$ ein Beweis für ψ.

Darüber hinaus ist X unter (MP) abgeschlossen: Um dies zu sehen, betrachten wir zwei Formeln χ und $\chi \to \chi'$ aus X und zeigen nun, dass damit auch χ' in X liegt: Nach Voraussetzung existiert jeweils ein Beweis $b = (b_i \mid i < n)$ für die Formel χ und $b' = (b'_i \mid i < m)$ für $(\chi \to \chi')$. Wir werden nun beide Beweise hintereinander setzen, danach die Formel χ' anhängen und erhalten damit einen Beweis für

χ'. Definiere also $\tilde{b} := (\tilde{b_i} \mid i < m + n + 1)$ durch:

$$\tilde{b_i} := \begin{cases} b_i & \text{falls } i < n \\ b'_{i-n} & \text{falls } n \leq i < n + m \\ \chi' & \text{falls } i = n + m \end{cases}$$

Dann ist $\tilde{b}$ ein Beweis von χ' aus der Formelmenge W.

Nach Satz 12.2 gilt damit $\{\psi \mid W \vdash \psi\} \subseteq X$, so dass jede herleitbare Formel auch einen Beweis hat. ⊠

Hieraus gewinnen wir den *Endlichkeitssatz*.

Satz 12.7 (Endlichkeitssatz)**.** *Wenn $W \vdash \varphi$, dann gibt es eine endliche Teilmenge $U \subseteq W$, so dass $U \vdash \varphi$.*

Beweis: Sei $W \vdash \varphi$. Nach Satz 12.6 existiert eine (endliche) Folge $b = (b_i \mid i < n)$, die einen Beweis von φ aus W darstellt. Setze nun $U := \{b_i \mid b_i \in W\}$. Dann ist b offensichtlich ein Beweis von φ aus U, wobei die zugrunde liegende Formelmenge U endlich ist. ⊠

13. Vollständigkeitssatz der Aussagenlogik

In den vorhergehenden Abschnitten haben wir einen Herleitungsbegriff "$\vdash$" unter Angabe von Axiomen und Beweisregeln definiert. Die Wahl der Axiome und Regeln war zwangsläufig etwas willkürlich. In der Literatur gibt es viele analog definierte Herleitungsbegriffe "$\vdash'$" , die alle im folgenden Sinne äquivalent sind, dass gilt:

$$\{\varphi \mid W \vdash \varphi\} \;=\; \{\varphi \mid W \vdash' \varphi\}.$$

In diesem Abschnitt beweisen wir die folgende Äquivalenz:

$$W \vdash \varphi \iff W \vDash \varphi.$$

Die Richtung von links nach rechts wird als Richtigkeitssatz oder Korrektheitssatz bezeichnet und haben wir bereits mit Satz 12.4 gesehen.

Auf dem Weg zur verbleibenen Richtung müssen wir uns zunächst mit einigen technischen Aussagen beschäftigen, die uns gleichzeitig den Begriff des formalen Beweises näher bringen.

Satz 13.1. *$W \vdash \varphi$ und $W \vdash \psi$ genau dann, wenn $W \vdash (\varphi \wedge \psi)$.*

Beweis: Zunächst die Richtung von links nach rechts ($\Rightarrow$): Dann gilt nach Voraussetzung, dass $W \vdash \varphi$ und $W \vdash \psi$. Nach Axiom 4 gilt weiterhin: $W \vdash (\varphi \to (\psi \to (\varphi \wedge \psi)))$. Danach wissen wir durch Anwendung von (MP), dass $W \vdash (\psi \to (\varphi \wedge \psi))$. Wenden wir nochmals (MP) an, erhalten wir schließlich: $W \vdash (\varphi \wedge \psi)$.

Von nun an schreiben wir solche Herleitungen als formale Beweise im Sinne von Definition 12.5. In unserem Fall sieht dies wie folgt aus:

$W \vdash \phi$	nach Voraussetzung
$W \vdash \psi$	nach Voraussetzung
$W \vdash (\varphi \to (\psi \to (\varphi \wedge \psi)))$	(A4)
$W \vdash (\psi \to (\varphi \wedge \psi))$	(MP)
$W \vdash (\varphi \wedge \psi)$	(MP)

Die noch verbleibende Richtung ($\Leftarrow$) ist eine Übungsaufgabe. ⊠

Achtung. Laut Definition 12.5 müssten wir eigentlich "$W \vdash$" weglassen, aber wir werden auch in Zukunft nicht darauf verzichten, um stets in Erinnerung zu haben, welche Formelmenge W wir gerade betrachten. (Dies wird später im Zusammenhang mit Satz 13.4 wichtig.)

Satz 13.2. *Es gilt für beliebige Formeln φ und χ:*

(a) *Wenn $W \vdash \varphi$, dann $W \vdash \chi \to \varphi$*
(b) *Wenn $W \vdash \varphi$, dann $W \vdash \neg\varphi \to \chi$*

Beweis: Der Beweis ist eine Übungsaufgabe – wende etwa Axiom (A2) in der substituierten Form $W \vdash \varphi \to (\chi \to \varphi)$ an. ⊠

Satz 13.3. *Es gilt: $W \vdash \varphi \to \varphi$.*

Beweis: Das Axiom (A1) heißt: $\varphi \to (\psi \to \psi)$ und ist somit aus (beliebigem und insbesondere dem gegebenen) W ableitbar. Durch Substitution erhalten wir damit: $W \vdash \psi \to (\varphi \to \varphi)$. Wähle nun ψ als ein beliebiges Axiom, etwa die substituierte Variante des Axioms (A2): $\psi := p \to (p \to p)$ für eine Aussagenvariable $p \in A$. Dann gilt offenbar:

$W \vdash \psi$	ψ ist Axiom
$W \vdash \psi \to (\varphi \to \varphi)$	(A1)
$W \vdash \varphi \to \varphi$	(MP)

Damit haben wir einen formalen Beweis angegeben. ⊠

Wenden wir uns nun einem bekannten Prinzip zu, welches wir bereits für den Begriff der Gültigkeit beweisen konnten. Hierfür definieren wir in Analogie zum Gültigkeitsbegriff: $W, \chi_1, \ldots, \chi_n \vdash \varphi$, wenn $W \cup \{\chi_1, \ldots, \chi_n\} \vdash \varphi$.

Satz 13.4 (Deduktionssatz für "$\vdash$")**.** *Es gilt $W \vdash \varphi \to \psi$ genau dann, wenn $W, \varphi \vdash \psi$.*

Beweis: Die eine Richtung ($\Rightarrow$) ist leicht einzusehen:

$W, \varphi \vdash \varphi$	Voraussetzung, Element von W, φ
$W, \varphi \vdash \varphi \to \psi$	Voraussetzung, da $W \vdash \varphi \to \psi$
$W, \varphi \vdash \psi$	(MP)

Für die zweite Richtung ($\Leftarrow$) setzen wir $X := \{\, \chi \mid W \vdash \varphi \to \chi \,\}$ und behaupten nun, dass

$$\text{wenn } \; W, \varphi \vdash \psi, \text{ dann } \; \psi \in X$$

gilt. Hierfür zeigen wir die folgenden zwei Bedingungen:

(a) $W \cup \{\varphi\} \cup \texttt{Axiome} \subseteq X$

(b) X ist unter (MP) abgeschlossen, das heißt, wenn $\chi \in X$ und $(\chi \to \chi') \in X$, so auch $\chi' \in X$.

Wenn diese Eigenschaften gezeigt sind, wissen wir nach Satz 12.2, dass

$$\{\chi \mid W, \varphi \vdash \chi\} \subseteq X = \{\chi \mid W \vdash \varphi \to \chi\}.$$

Somit folgte die gewünschte Behauptung insbesondere auch für ψ und wir wären fertig.

Zu (a): Es gilt $W \cup \texttt{Axiome} \subseteq X$, denn für ein Element aus W oder ein Axiom, nennen wir es in beiden Fällen χ, gilt offenbar $W \vdash \chi$ und somit nach Satz 13.2 auch $W \vdash \varphi \to \chi$, also $\chi \in X$.

Darüber hinaus gilt nach Satz 13.3 auch $W \vdash \varphi \to \varphi$, so dass auch hier $\varphi \in X$ folgt.

Zu (b): Nehmen wir an, es gelte: $W \vdash \varphi \to \chi$ und $W \vdash \varphi \to (\chi \to \chi')$. Dann gilt nach Satz 13.1:

$$W \vdash (\varphi \to \chi) \wedge (\varphi \to (\chi \to \chi'))$$

und damit nach Axiom (A6) auch:

$$W \vdash ((\varphi \to \chi) \wedge (\varphi \to (\chi \to \chi'))) \to (\varphi \to \chi').$$

Insgesamt folgt mit (MP) wie gewünscht: $W \vdash (\varphi \to \chi')$. ⊠

Mithilfe des gerade gezeigten Deduktionssatzes können wir die Prämisse φ aus einer zu zeigenden Implikation $(\varphi \to \psi)$ der Ausgangsformelmenge W hinzufügen. Damit müssen wir nur noch einen (formalen) Beweis für die Konklusion ψ finden. Dies ist in der Regel einfacher, da wir die Komplexität der Formel, für die wir einen formalen Beweis suchen, verringert haben. Schauen wir uns folgendes Beispiel an:

Satz 13.5. *Es gilt:* $\vdash (\varphi \wedge \psi) \to (\psi \wedge \varphi)$

Beweis: Setze $W := \{\varphi \wedge \psi\}$. Dann genügt es nach dem Deduktionssatz 13.4 zu zeigen, dass $W \vdash \psi \wedge \varphi$ gilt. Dies zeigen wir durch den folgenden (formalen) Beweis:

$W \vdash \varphi \wedge \psi$	Element von W
$W \vdash (\varphi \wedge \psi) \to \varphi$	(A5)
$W \vdash (\varphi \wedge \psi) \to \psi$	(A5)
$W \vdash \varphi$	(MP)
$W \vdash \psi$	(MP)
$W \vdash \psi \to (\varphi \to (\psi \wedge \varphi))$	(A4)
$W \vdash \varphi \to (\psi \wedge \varphi)$	(MP)
$W \vdash \psi \wedge \varphi$	(MP)

⊠

Wir können das formale Prinzip Modus Ponens auch (formal) herleiten. Dies ist aufgrund der Wahl unserer Ableitungsregel nicht verwunderlich, ist aber gleichzeitig eine gute Übung, das Konzept des formalen Beweises zu üben:

Satz 13.6 (Modus Ponens)**.** *Es gilt:* $\vdash \varphi \wedge (\varphi \to \psi) \to \psi$.

Beweis: Setze $W := \{\varphi \wedge (\varphi \to \psi)\}$. Dann genügt es nach dem dem Deduktionssatz zu zeigen, dass $W \vdash \psi$ gilt:

$W \vdash \varphi \wedge (\varphi \to \psi)$	Element von W
$W \vdash \varphi \wedge (\varphi \to \psi) \to \varphi$	(A5)
$W \vdash \varphi \wedge (\varphi \to \psi) \to (\varphi \to \psi)$	(A5)
$W \vdash \varphi$	(MP)
$W \vdash \varphi \to \psi$	(MP)
$W \vdash \psi$	(MP)

$\boxtimes$

Selbst semantisch klare Zusammenhänge müssen formal mühselig bewiesen werden:

Satz 13.7. *Für eine beliebige Formelmenge W gilt: Wenn $W \vdash \varphi \leftrightarrow \psi$, so auch $W \vdash \varphi \to \psi$ und $W \vdash \psi \to \varphi$.*

Beweis:

$W \vdash (\varphi \leftrightarrow \psi)$	Voraussetzung
$W \vdash (\varphi \leftrightarrow \psi) \to ((\varphi \to \psi) \wedge (\psi \to \varphi))$	(A7)
$W \vdash ((\varphi \to \psi) \wedge (\psi \to \varphi)) \to (\varphi \to \psi)$	(A5)
$W \vdash ((\varphi \to \psi) \wedge (\psi \to \varphi)) \to (\psi \to \varphi)$	(A5)
$W \vdash ((\varphi \to \psi) \wedge (\psi \to \varphi))$	(MP)
$W \vdash (\varphi \to \psi)$	(MP)
$W \vdash (\psi \to \varphi)$	(MP)

$\boxtimes$

Ebenso die Umkehrung lässt sich formal herleiten:

Satz 13.8. *Für eine beliebige Formelmenge W gilt: Wenn $W \vdash \varphi \to \psi$ und $W \vdash \psi \to \varphi$ gelten, so auch $W \vdash \varphi \leftrightarrow \psi$.*

Beweis:

$W \vdash (\psi \leftrightarrow \varphi) \leftrightarrow ((\psi \to \varphi) \wedge (\varphi \to \psi))$	(A10)
$W \vdash ((\psi \leftrightarrow \varphi) \leftrightarrow ((\psi \to \varphi) \wedge (\varphi \to \psi))) \to$ $(((\psi \leftrightarrow \varphi) \to ((\psi \to \varphi) \wedge (\varphi \to \psi))) \wedge$ $((\psi \to \varphi) \wedge (\varphi \to \psi)) \to (\psi \leftrightarrow \varphi))$	(A7)
$W \vdash (((\psi \leftrightarrow \varphi) \to ((\psi \to \varphi) \wedge (\varphi \to \psi))) \wedge$ $((\psi \to \varphi) \wedge (\varphi \to \psi)) \to (\psi \leftrightarrow \varphi))$	(MP)

$$
\begin{aligned}
W \vdash\ & ((\psi \leftrightarrow \varphi) \rightarrow ((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi))) \wedge \\
& \qquad (((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)) \rightarrow (\psi \leftrightarrow \varphi)) \rightarrow \\
& \qquad (((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)) \rightarrow (\psi \leftrightarrow \varphi)) && \text{(A5)} \\
W \vdash\ & (((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)) \rightarrow (\psi \leftrightarrow \varphi)) && \text{(MP)} \\
W \vdash\ & ((\psi \rightarrow \varphi) \rightarrow ((\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)))) && \text{(A4)} \\
W \vdash\ & ((\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi))) && \text{(MP)} \\
W \vdash\ & ((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)) && \text{(MP)} \\
W \vdash\ & (\psi \leftrightarrow \varphi) && \text{(MP)}
\end{aligned}
$$

$\boxtimes$

Folgende so genannte *Schnittregel* wird sich als nützlich erweisen:

Satz 13.9 (Schnittregel)**.** *Für eine beliebige Formelmenge W gilt: Wenn $W \vdash \varphi \rightarrow \psi$ und $W \vdash \psi \rightarrow \chi$ gilt, so auch $W \vdash \varphi \rightarrow \chi$.*

Beweis: Nach dem Deduktionssatz 13.4 ist die Behauptung äquivalent zu der Aussage: $W' \vdash \chi$ für die Formelmenge $W' := W \cup \{\varphi\}$. Diese zeigen wir nun wie folgt:

$W' \vdash \varphi$	Element von W'
$W' \vdash \varphi \rightarrow \psi$	Voraussetzung für W
$W' \vdash \psi \rightarrow \chi$	Voraussetzung für W
$W' \vdash \psi$	(MP)
$W' \vdash \chi$	(MP)

$\boxtimes$

Schauen wir uns einen längeren formalen Beweis an, indem wir folgenden, grundsätzlich einfachen (semantischen) Zusammenhang herleiten:

Satz 13.10. *Es gilt:* $\vdash$ ($\neg\neg\varphi \leftrightarrow \varphi$).

Beweis: Diesen Beweis teilen wir in mehrere Teilbehauptungen:

$$(\star) \qquad \vdash (\varphi \rightarrow \neg\neg\varphi)$$

Beweis von ($\star$): Hierfür beweisen wir mithilfe des Deduktionssatzes $W \vdash \neg\neg\varphi$ für $W := \{\varphi\}$ durch den folgenden formalen Beweis:

$W \vdash \varphi$	Element von W
$W \vdash \varphi \rightarrow (\neg\varphi \rightarrow \neg\neg\varphi)$	(A2)

$W \vdash (\neg\varphi \to \neg\neg\varphi)$ (MP)
$W \vdash (\neg\varphi \to \neg\neg\varphi) \to \neg\neg\varphi$ (A3)
$W \vdash \neg\neg\varphi$ (MP)
$\boxtimes((\star))$

$(\star\star)$ $\vdash (\varphi \to \neg\neg\varphi)$

Beweis von $(\star\star)$: Hierfür beweisen wir mithilfe des Deduktionssatzes $W \vdash \varphi$ für $W := \{\neg\neg\varphi\}$ durch den folgenden formalen Beweis:

$W \vdash \neg\neg\varphi$ Element von W
$W \vdash \neg\neg\varphi \to (\neg\varphi \to \neg\neg\varphi)$ (A2)
$W \vdash (\neg\varphi \to \neg\neg\varphi)$ (MP)
$W \vdash (\neg\varphi \to \neg\neg\varphi) \to \varphi$ (A2)
$W \vdash ((\neg\varphi \to \neg\neg\varphi) \wedge$
$(\neg\varphi \to (\neg\neg\varphi \to \varphi))) \to (\neg\varphi \to \varphi)$ (A6)
$W \vdash ((\neg\varphi \to \neg\neg\varphi) \to ((\neg\varphi \to (\neg\neg\varphi \to \varphi)) \to$
$((\neg\varphi \to \neg\neg\varphi) \wedge (\neg\varphi \to (\neg\neg\varphi \to \varphi))))$ (A4)
$W \vdash ((\neg\varphi \to (\neg\neg\varphi \to \varphi)) \to$
$((\neg\varphi \to \neg\neg\varphi) \wedge (\neg\varphi \to (\neg\neg\varphi \to \varphi))))$ (MP)
$W \vdash ((\neg\varphi \to \neg\neg\varphi) \wedge (\neg\varphi \to (\neg\neg\varphi \to \varphi)))$ (MP)
$W \vdash (\neg\varphi \to \varphi)$ (MP)
$W \vdash (\neg\varphi \to \varphi) \to \varphi$ (A3)
$W \vdash \varphi$ (MP)
$\boxtimes((\star\star))$

Aus $(\star)$ und $(\star\star)$ folgt nun unter Anwendung des Satzes 13.8 die gewünschte Behauptung: $\vdash \neg\neg\varphi \leftrightarrow \varphi$.

$\boxtimes$

$\star \quad \star \quad \star$

Wir gehen nun einen Schritt weiter auf unserem Weg zum Vollständigkeitssatz und betrachten das Konzept der *Widerspruchsfreiheit einer Formelmenge*. Es gibt verschiedene Ansätze, dies zu definieren und wir werden insgesamt drei äquivalente Formulierungen dafür sehen.

Wir werden eine Formelmenge W widerspruchsfrei nennen, wenn es überhaupt eine Formel gibt, die wir nicht herleiten können. Wenn wir nämlich alles, also jede beliebige Formel, aus der betrachteten Formelmenge herleiten könnten, dann könnten wir auch Widersprüchliches ableiten. Dies wird unsere Definition sein. Dies ist aber äquivalent dazu, dass aus der widerspruchsfreien Menge W kein Widerspruch folgt. Darüber hinaus ist dies äquivalent, dass aus einer konsistenten Menge nicht gleichzeitig eine Formel und deren Negation bewiesen werden kann. Aber eines nach dem anderen.

Zunächst definieren wir:

Definition 13.11. *Eine Formelmenge W heißt widerspruchsfrei oder konsistent, wenn es eine Formel φ gibt, so dass $W \nvdash \varphi$ gilt.*

Wenn W konsistent ist, schreiben wir hierfür kurz "$\mathtt{con}(W)$".

Satz 13.12. *Eine Formelmenge W ist genau dann widerspruchsfrei, wenn gilt: $W \nvdash \neg(\varphi \to \varphi)$.*

Beweis: Die Richtung ($\Leftarrow$) ist sofort klar nach Definition. Wir zeigen die fehlende Richtung ($\Rightarrow$) wie folgt: Es gelte dafür $W \vdash \neg(\varphi \to \varphi)$. Dann gilt nach Axiom (A1): $W \vdash \neg(\varphi \to \varphi) \to \chi$ und somit nach (MP) auch $W \vdash \chi$ für eine beliebige Formel χ. Also ist jede Formel aus W herleitbar, so dass $\neg\mathtt{con}(W)$ gilt. Mittels Kontraposition folgt die fehlende Richtung der Behauptung. ⊠

Satz 13.13. *Eine Formelmenge W ist genau dann widerspruchsfrei, wenn gilt: $W \nvdash \varphi$ oder $W \nvdash \neg\varphi$.*

Beweis: Die Richtung ($\Leftarrow$) ist wieder klar nach Definition. Wir zeigen wieder die Rückrichtung ($\Rightarrow$) mittels Kontraposition: Sei also $W \vdash \varphi$ und $W \vdash \neg\varphi$. Dann gilt insbesondere $W \vdash \varphi \to (\neg\varphi \to \chi)$ für eine beliebige Formel χ nach Axiom (A2). Nach zweimaligem Anwenden von (MP) erhalten wir schließlich: $W \vdash \chi$. Wie oben lässt sich somit wiederum alles aus W herleiten, also $\neg\mathtt{con}(W)$. ⊠

Wir haben bereits das Prinzip des indirekten Beweises gesehen und können dies jetzt sogar formalisieren.

Satz 13.14. *Es gilt:*

$$W \vdash \varphi \quad \textit{gdw.} \quad \neg\mathtt{con}(W \cup \{\neg\varphi\})$$
$$W \vdash \neg\varphi \quad \textit{gdw.} \quad \neg\mathtt{con}(W \cup \{\varphi\})$$

Beweis: Da die zweite aus der ersten Aussage folgt, beweisen wir nur die erste. Zunächst die eine Richtung ($\Rightarrow$): Sei $W \vdash \varphi$. Dann gilt offenbar $W, \neg\varphi \vdash \varphi$ und $W, \neg\varphi \vdash \neg\varphi$ und somit nach Satz 13.13 auch $\neg\mathtt{con}(W \cup \{\neg\varphi\})$.

Die andere Richtung ($\Leftarrow$) folgt ähnlich: Es gelte $\neg\mathtt{con}(W \cup \{\neg\varphi\})$. Insbesondere gilt dann nach Definition: $W, \neg\varphi \vdash \varphi$. Nach dem Deduktionssatz folgt: $W \vdash \neg\varphi \to \varphi$ und nach Axiom 3 schließlich auch: $W \vdash (\neg\varphi \to \varphi) \to \varphi$. Also gilt: $W \vdash \varphi$ nach MP. ⊠

Satz 13.15. *Wenn* $\mathtt{con}(W)$*, dann* $\mathtt{con}(W \cup \{\varphi\})$ *oder* $\mathtt{con}(W \cup \{\neg\varphi\})$.

Beweis: Angenommen dies gilt nicht. Dann gilt neben $\mathtt{con}(W)$ auch $\neg\mathtt{con}(W \cup \{\varphi\})$ und $\neg\mathtt{con}(W \cup \{\neg\varphi\})$. Nach Satz 13.14 folgt sowohl $W \vdash \neg\varphi$ als auch $W \vdash \varphi$. Dies ist nach Satz 13.13 ein Widerspruch zur Voraussetzung: $\mathtt{con}(W)$. ⊠

Satz 13.16. *Sei* $W \vdash (\varphi \leftrightarrow \psi)$*. Dann gilt:* $W \vdash \varphi$ *gdw.* $W \vdash \psi$.

Der Beweis ist eine leichte Übungsaufgabe.

Ein letztes Hilfsmittel für den eigentlichen Beweis des Vollständigkeitssatzes benötigen wir noch und werden dies jetzt einführen.

Definition 13.17. *Eine* Kette *ist eine Menge* K *von Mengen. Wenn* $X, Y \in K$*, dann* $X \subseteq Y$ *oder* $Y \subseteq X$.

Satz 13.18. *Sei* K *eine Kette von Formelmengen, so dass jedes* $W \in K$ *widerspruchsfrei ist. Dann ist auch* $\overline{W} := \bigcup_{W \in K} W$ *widerspruchsfrei.*

Beweis: Angenommen, die Aussage des Satzes ist falsch, dann gilt: $\neg\mathtt{con}(\overline{W})$. Insbesondere haben wir, dass $\overline{W} \vdash p \wedge \neg p$. Nach dem Endlichkeitssatz existieren endlich viele Formeln $\varphi_1, \ldots, \varphi_n \in \overline{W}$ mit

$$\varphi_1, \ldots, \varphi_n \vdash p \wedge \neg p.$$

Nun ist $\overline{W} = \bigcup_{W \in K} W$ eine Vereinigung, so dass $W_1, \ldots, W_n \in K$ mit $\varphi_1 \in W_1, \ldots, \varphi_n \in W_n$ existieren. O.B.d.A. seien $W_1 \subseteq \cdots \subseteq W_n$, da K eine Kette ist. Dann sind $\varphi_1, \ldots, \varphi_n$ aber Elemente von W_n. Insbesondere gilt damit: $W_n \vdash p \wedge \neg p$. Das ist ein Widerspruch zur Voraussetzung, dass $\mathtt{con}(W_n)$. ⊠

Wir werden nun den eigentlichen Teil des Vollständigkeitssatzes beweisen:

Satz 13.19 (Vollständigkeitssatz)**.** *Ist W eine konsistente Formelmenge, so existiert ein Modell $\mathfrak{A}$ mit $\mathfrak{A} \vDash W$.*

Beweis: Es sei $\mathtt{con}(W)$. Wir wissen, dass die Menge der Formeln nach Satz 11.2 abzählbar ist. Damit können wir die Menge der Formeln durch die natürlichen Zahlen aufzählen, etwa: $\mathtt{Fml} = \{\varphi_i | i \in \mathbb{N}\}$. Durch Induktion über die natürlichen Zahlen definieren wir:

$$\begin{aligned} W_0 &:= W \\ W_{i+1} &:= \begin{cases} W_i \cup \{\varphi_i\} & \text{falls } \mathtt{con}(W_i \cup \{\varphi_i\}) \\ W_i \cup \{\neg\varphi_i\} & \text{sonst} \end{cases} \end{aligned}$$

Dies ist überhaupt erst nach Satz 13.15 möglich. Durch Induktion auf $i \in \mathbb{N}$ folgt dann, dass die Formelmengen W_i alle widerspruchsfrei sind. Setze nun $\overline{W} = \bigcup_{i \in \mathbb{N}} W_i$. Dann ist $\overline{W}$ nach Satz 13.18 ebenfalls widerspruchsfrei.

Darüber hinaus ist $\overline{W}$ im Sinne der Inklusionsbeziehung maximal, das heißt

(1) Für jedes $\varphi \in \mathtt{Fml}$ gilt: $\varphi \in \overline{W}$ oder $\neg\varphi \in \overline{W}$,

denn für $W' \supsetneq \overline{W}$ und $\varphi \in W' \setminus \overline{W}$ folgt $\neg\varphi \in \overline{W}$ nach Konstruktion von $\overline{W}$. Damit gilt, dass sowohl φ als auch $\neg\varphi$ Element von W' ist. Somit wäre W' widerspruchsvoll.

Außerdem gelten die folgenden Eigenschaften:

(2) Weiterhin gilt: $\varphi \in \overline{W}$ gdw. $\overline{W} \vdash \varphi$

Beweis von (2): Die Richtung ($\Rightarrow$) ist klar. Die andere Richtung ($\Leftarrow$) lässt sich wie folgt zeigen: Sei $\varphi \notin \overline{W}$. Nach (1) gilt $\neg\varphi \in \overline{W}$, also $\overline{W} \vdash \neg\varphi$. Da $\mathtt{con}(\overline{W})$ gilt auch $\overline{W} \nvdash \varphi$. $\boxtimes((2))$

Aus (1) und (2) folgt:

(3) $$\overline{W} \vdash \neg\varphi \quad \text{gdw.} \quad \overline{W} \nvdash \varphi$$
$$\overline{W} \vdash \varphi \quad \text{gdw.} \quad \overline{W} \nvdash \neg\varphi$$

Wir wissen aufgrund des Satzes 13.1, dass gilt:

(4) $$\overline{W} \vdash (\varphi \wedge \psi) \quad \text{gdw.} \quad \overline{W} \vdash \varphi \text{ und } \overline{W} \vdash \psi$$

Und folglich:

(5) $$\overline{W} \vdash (\varphi \vee \psi) \quad \text{gdw.} \quad \overline{W} \vdash \varphi \text{ oder } \overline{W} \vdash \psi$$

Beweis von (5): Es gelte $\overline{W} \nvdash \varphi$ und $\overline{W} \nvdash \psi$.
Dies gilt nach (3) genau dann, wenn $\overline{W} \vdash \neg\varphi$ und $\overline{W} \vdash \neg\psi$. Dies gilt nach (4) genau dann, wenn $\overline{W} \vdash (\neg\varphi \wedge \neg\psi)$. Dies gilt nach (3) genau dann, wenn $\overline{W} \nvdash \neg(\neg\varphi \wedge \neg\psi)$. Und schließlich gilt dies nach (A8) und Satz 13.16 genau dann, wenn $\overline{W} \nvdash (\varphi \vee \psi)$. $\boxtimes((5))$

(6) $$\overline{W} \vdash (\varphi \to \psi) \quad \text{gdw.} \quad (\overline{W} \vdash \varphi \Rightarrow \overline{W} \vdash \psi)$$

Beweis von (6): Es gelte die (Meta-)Implikation $(\overline{W} \vdash \varphi \Rightarrow \overline{W} \vdash \psi)$. Dies gilt genau dann, wenn $\overline{W} \nvdash \varphi$ oder $\overline{W} \vdash \psi$. Dies gilt nach (3) genau dann, wenn $\overline{W} \vdash \neg\varphi$ oder $\overline{W} \vdash \psi$. Dies gilt nach (5) genau dann, wenn $\overline{W} \vdash \neg\varphi \vee \psi$. Dies gilt nach (A9) und Satz 13.16 genau dann, wenn $\overline{W} \vdash \varphi \to \psi$. $\boxtimes((6))$

(7) $$\overline{W} \vdash (\varphi \leftrightarrow \psi) \quad \text{gdw.} \quad \overline{W} \vdash \varphi \Leftrightarrow \overline{W} \vdash \psi$$

Beweis von (7): Es gelte $\overline{W} \vdash \varphi \Leftrightarrow \overline{W} \vdash \psi$. Dies gilt genau dann, wenn $(\overline{W} \vdash \varphi \Rightarrow \overline{W} \vdash \psi)$ und $(\overline{W} \vdash \psi \Rightarrow \overline{W} \vdash \varphi)$. Dies gilt nach (6) genau dann, wenn $\overline{W} \vdash \varphi \to \psi$ und $\overline{W} \vdash \psi \to \varphi$. Dies gilt nach (4) genau dann, wenn $\overline{W} \vdash (\varphi \to \psi) \wedge (\psi \to \varphi)$. Und dies gilt nach (A10) und Satz 13.16 genau dann, wenn $\overline{W} \vdash (\varphi \leftrightarrow \psi)$. $\boxtimes((7))$

Damit sind alle Vorbereitungen getroffen und wir können das gesuchte Modell definieren. Setze daher

$$\mathfrak{A}(p) := \begin{cases} 1 & \text{falls } p \in W \\ 0 & \text{falls } p \notin W \end{cases}$$

Dann gilt nach Definition

$$\mathfrak{A} \vDash p \quad \text{gdw.} \quad \overline{W} \vdash p. \tag{8}$$

Mithilfe der Eigenschaften (3) bis (7) folgt durch Induktion auf φ:

$$\overline{W} \vdash \varphi \quad \text{gdw.} \quad \mathfrak{A} \vDash \varphi. \tag{9}$$

Also gilt $\mathfrak{A} \vDash \overline{W}$ und somit insbesondere auch wie gewünscht $\mathfrak{A} \vDash W$, da $W \subseteq \overline{W}$. ⊠

Diesen (Vollständigkeits-)Satz ausnutzend bekommen wir schließlich die gängige Variante, die manchmal auch in der Literatur als Vollständigkeitssatz zitiert wird:

Satz 13.20. *Es gilt:* $W \vdash \varphi$ *gdw.* $W \vDash \varphi$.

Beweis: Die Richtung ($\Rightarrow$) folgt aus dem Korrektheitssatz 12.4. Wir beweisen noch die andere Richtung ($\Leftarrow$): Angenommen, es gilt $W \nvdash \varphi$. Dann ist $W \cup \{\neg\varphi\}$ widerspruchsfrei. Nach Satz 13.19 existiert dann ein Modell $\mathfrak{A}$, so dass $\mathfrak{A} \vDash W \cup \{\neg\varphi\}$. Somit muss gelten, dass $W \nvDash \varphi$. ⊠

Abschließend bekommen wir noch eine semantische Variante der Widerspruchsfreiheit:

Satz 13.21. *Es gilt* $\mathtt{con}(W)$ *genau dann, wenn ein* $\mathfrak{A}$ *mit* $\mathfrak{A} \vDash W$ *existiert.*

Beweis: Wir haben folgende Kette von Äquivalenzen:

$$\begin{aligned} \neg\mathtt{con}(W) \quad & \text{gdw.} \quad W \vdash p \wedge \neg p \\ & \text{gdw.} \quad W \vDash p \wedge \neg p \\ & \text{gdw.} \quad \text{für jedes Modell } \mathfrak{A} \text{ gilt: } \mathfrak{A} \nvDash W. \end{aligned}$$

Daraus folgt die Behauptung. ⊠

Schließlich können wir zeigen, dass man aus einem Widerspruch, stets beliebige Formeln (und damit "alles") herleiten können:

Satz 13.22. *Für eine Primaussage p und die Menge $W := \{p \wedge \neg p\}$ gilt stets $W \vdash \varphi$ für beliebige (aussagenlogische) Formeln φ.*

Beweis: Sei φ eine beliebige Formel. Dann können wir folgende Herleitung dafür angeben:

$W \vdash p \wedge \neg p$	Element von W
$W \vdash (p \wedge \neg p) \to p$	(A5)
$W \vdash (p \wedge \neg p) \to \neg p$	(A5)
$W \vdash p$	(MP)
$W \vdash \neg p$	(MP)
$W \vdash p \to (\neg p \to \varphi)$	(A2)
$W \vdash \neg p \to \varphi$	(MP)
$W \vdash \varphi$	(MP)

$\boxtimes$

Und zum Abschluß geben wir noch einen formalen Beweis für das Prinzip der *Kontraposition*:

Satz 13.23 (Kontraposition)**.** *Es gilt:* $\vdash$ ($(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$).

Beweis: Nach dem Deduktionssatz 13.4 ist die Behauptung äquivalent zu $W \vdash (\neg\psi \to \neg\varphi)$ für $W := \{\varphi \to \psi\}$. Dies wiederum ist erneut wegen des Deduktionssatzes äquivalent zu $W' \vdash \neg\varphi$ für die Formelmenge $W' := W \cup \{\neg\psi\} = \{\varphi \to \psi, \neg\psi\}$.

Hierfür geben wir die folgende Herleitung an:

$W' \vdash \neg\psi$	Element von W'
$W' \vdash \neg\psi \to (\neg\neg\psi \to \neg\varphi)$	(A2)
$W' \vdash \neg\neg\psi \to \neg\varphi$	(MP)
$W' \vdash \neg\neg\psi \leftrightarrow \psi$	(Satz 13.10)
$W' \vdash \psi \to \neg\neg\psi$	(Satz 13.9)
$W' \vdash \varphi \to \psi$	Element von W'
$W' \vdash \varphi \to \neg\neg\psi$	(Satz 13.7)
$W' \vdash \varphi \to \neg\varphi$	(Satz 13.7)

$W' \vdash (\varphi \to \neg\varphi) \to \neg\varphi$ (A3)

$W' \vdash \neg\varphi$ (MP)

$\boxtimes$

Damit verlassen wir die Welt der (aussagenlogischen) formalen Beweise.

14. Signaturen und Strukturen

Wir haben eine Fülle von Strukturen kennengelernt: die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ und allgemein verschiedene Gruppen, Ringe und Körper. Gemeinsames Merkmal von Strukturen ist das Vorhandensein von Trägermengen, auf denen die Funktionen und Relationen wirken.

Beispiel A. Wir betrachten zunächst den Körper $\mathbb{R}$ der reellen Zahlen, das heißt, es existiert eine Addition $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, eine Multiplikation $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ sowie Konstantensymbole 0 und 1 als neutrale Elemente der jeweiligen Operation. Dies kann man etwa als: $(\mathbb{R}; +, \cdot; 0, 1)$ zusammenfassen.

Wir können die reellen Zahlen auch als angeordneten Körper betrachten, also etwa $(\mathbb{R}; +, \cdot; \leq; 0, 1)$, dann haben wir neben den obigen Symbolen noch ein zweistelliges Relationszeichen "$\leq$".

Beispiel B. Betrachten wir als nächstes den Körper $\mathbb{C}$ der komplexen Zahlen. Wir haben hier, dem ersten Beispiel A folgend, eine Addition $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$, eine Multiplikation $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ sowie Konstantensymbole 0 und 1. Dies schreiben wir kurz als: $(\mathbb{C}; +, \cdot; 0, 1)$. Damit sieht diese Struktur der in Beispiel A betrachteten sehr ähnlich – nur dass sich die Trägermenge, also die Zahlen selbst, unterscheiden und damit auch die Definitions- und Bildbereiche der Operationen.

Beispiel C. Wir können allerdings die komplexen Zahlen $\mathbb{C}$ auch als Menge der (Orts-)Vektoren in der Ebene auffassen und Operationen auf den "Vektoren" zulassen. Dies haben wir bereits im Kapitel 8 gesehen. Dann haben wir eine Vektoraddition $+_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$, eine Skalarmultiplikation $\cdot_{\mathbb{C}} : \mathbb{R} \times \mathbb{C} \to \mathbb{C}$ sowie ein Konstantensymbol $0_{\mathbb{C}}$, den so genannten Nullvektor. Beachten Sie, dass sich diese Multiplikation von der im Beispiel B unterscheidet. Wir wollen hier die Vektoren

nur stauchen und strecken, also skalieren, und erlauben daher nur die Multiplikation mit den Skalaren, also den reellen Zahlen. Natürlich ist dies ein Spezialfall der obigen Multiplikation im Beispiel B, allerdings hat diese Multiplikation eine gänzlich neue Gestalt und damit auch andere Eigenschaften. Dadurch unterscheidet sich die Sichtweise der komplexen Zahlen als Vektorraum auch deutlich von der als Körper.

Diese Art der Sichtweise werden wir im nächsten Semester in der Linearen Algebra vertiefen und allgemein so genannte Vektorräume betrachten. Am Beispiel der komplexen Zahlen können wir dies schon ansatzweise vorziehen: Wir haben hier zwei Trägermengen, nämlich die eigentlichen Vektoren $\mathbb{C}$ und Skalare $\mathbb{R}$. Im Sinne der obigen Kurzschreibweise können wir dies zusammenfassen als:

$$(\mathbb{C}, \mathbb{R}; +_{\mathbb{C}}, \cdot_{\mathbb{C}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}; 0_{\mathbb{C}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$$

Innerhalb dieser Struktur können wir bekannte Beziehungen formal schreiben, so beispielsweise auch die Gleichung: $r_1 v + r_2 v = (r_1 + r_2)v$, wobei v eine Variable über Vektoren, hier komplexe Zahlen, ist und r_1, r_2 Variablen über Skalaren, hier reelle Zahlen, sind. Eigentlich –etwas genauer betrachtet– haben wir:

$$r_1 \cdot_{\mathbb{C}} v +_{\mathbb{C}} r_2 \cdot_{\mathbb{C}} v = (r_1 +_{\mathbb{R}} r_2) \cdot_{\mathbb{C}} v.$$

Darüber hinaus gilt ebenfalls: $r_1(r_2 v) = (r_1 r_2)v$, genauer:

$$r_1 \cdot_{\mathbb{C}} (r_2 \cdot_{\mathbb{C}} v) = (r_1 \cdot_{\mathbb{R}} r_2) \cdot_{\mathbb{C}} v.$$

Sie können an diesen einfachen Beziehungen deutlich die Verwendung der verschiedenen Operationen erkennen und sehen dadurch auch die Verwendung der beiden Trägermengen.

Die Relationen und Funktionen einer Struktur können sich –wie die Skalarmultiplikation– auf verschiedene Trägermengen beziehen und können verschiedene Stellenanzahlen (Stelligkeiten) haben. Zur Organisation des Systems von Trägermengen, Funktionen und Relationen führen wir allgemein den Begriff der *Signatur* ein:

Definition 14.1. *Ein 5-Tupel $\sigma = (S, F, R, K, \mathtt{fct})$ ist eine Signatur, wenn folgendes gilt:*

(a) *S, F, R, K sind paarweise disjunkte Mengen von* Sorten, Funktionssymbolen, Relationssymbolen *und* Konstantensymbolen;
(b) `fct` *ist eine auf* $F \cup R \cup K$ *definierte Funktion, die als* Funktionalität *bezeichnet wird;*
(c) *für alle* $f \in F$ *gibt es ein* $n \in \mathbb{N}$ *mit* $\texttt{fct}(f) \in S^{n+1}$;
(d) *für alle* $r \in R$ *gibt es ein* $n \in \mathbb{N}$ *mit* $\texttt{fct}(r) \in S^n$;
(e) *für* $k \in K$ *ist* $\texttt{fct}(k) \in S$.

Die Sorten entsprechen den verschiedenen Trägermengen von Strukturen. Die Funktion `fct` legt die Typen der Symbole fest: Wenn $f \in F$ ein Funktionssymbol ist und $\texttt{fct}(f) = (s_1, \ldots, s_n, s_{n+1}) \in S^{n+1}$, so bedeutet das, dass f eine n-stellige Funktion ist, die Argumente aus den mit den Sorten $s_1, \ldots, s_n$ bezeichneten Trägermengen bezieht und einen Wert in der mit s_{n+1} bezeichneten Trägermenge liefert.

Im Beispiel C haben wir etwa die Sortenmenge: $S := \{Vektor, Skalar\}$, die Menge der Funktionssymbole $F := \{+_V, \cdot_V, +_{Sk}, \cdot_{Sk}\}$, die Menge der Relationssymbole $R := \varnothing$ und schließlich die Menge der Konstantensymbole $K := \{0_V, 0_{Sk}, 1_{Sk}\}$. Die Funktionalität hat folgende Eigenschaften:

$$
\begin{aligned}
\texttt{fct}(+_{Sk}) &= (Skalar, Skalar, Skalar) \\
\texttt{fct}(+_V) &= (Vektor, Vektor, Vektor) \\
\texttt{fct}(\cdot_V) &= (Skalar, Vektor, Vektor) \\
\texttt{fct}(\cdot_{Sk}) &= (Skalar, Skalar, Skalar) \\
\texttt{fct}(0_{Sk}) &= Skalar \\
\texttt{fct}(1_{Sk}) &= Skalar \\
\texttt{fct}(0_V) &= Vektor
\end{aligned}
$$

Damit haben wir allgemein die Signatur für die so genannten Vektorräume eingeführt, die wir bereits jetzt am Beispiel der komplexen Zahlen immer wieder exemplarisch zu Rate ziehen werden. Diese Signatur hat dann folgende Gestalt:

$$\sigma_{\mathrm{VR}} = (\underbrace{\{Vektor, Skalar\}}_{S}, \underbrace{\{+_{Sk}, \cdot_{Sk}, +_V, \cdot_V\}}_{F}, \underbrace{\varnothing}_{R}, \underbrace{\{0_{Sk}, 1_{Sk}, 0_V\}}_{K}, \texttt{fct})$$

Um Klammern und leere Mengen zu sparen, werden wir manchmal abkürzend auf die Mengenschreibweise verzichten und die einzelnen Symbole als Folge, jeweils mit Semikolon getrennt, wie folgt schreiben:

$$\sigma_{\mathrm{VR}} = (Vektor, Skalar; +_{Sk}, \cdot_{Sk}, +_V, \cdot_V; 0_{Sk}, 1_{Sk}, 0_V; \mathtt{fct})$$

Kommen wir nun zu einem neuen zentralen Begriff. Nachdem wir das Alphabet unserer Sprache eingeführt haben, können wir diese Symbole mit Leben erfüllen und so genannte *Strukturen* einer gegebenen Signatur betrachten. Eine Signatur wird durch Strukturen interpretiert. In einer Struktur werden den Symbolen entsprechende Strukturkomponenten zugeordnet.

Definition 14.2. *Sei $\sigma = (S, F, R, K, \mathtt{fct})$ eine Signatur. Eine* Struktur mit Signatur σ *oder kurz eine* σ-Struktur *ist ein Tupel:*

$$\mathfrak{A} = ((A_s)_{s\in S}, (f^{\mathfrak{A}})_{f\in F}, (r^{\mathfrak{A}})_{r\in R}, (k^{\mathfrak{A}})_{k\in K})$$

mit den Eigenschaften:

(a) *für $s \in S$ ist A_s eine nicht-leere Menge; jedes A_s ist eine* Trägermenge *der Struktur.*

(b) *für $f \in F$ mit $\mathtt{fct}(f) = (s_1, \ldots, s_n, s_{n+1})$ ist $f^{\mathfrak{A}}$ eine Funktion:*

$$f^{\mathfrak{A}} : A_{s_1} \times \ldots \times A_{s_n} \to A_{s_{n+1}},$$

(c) *für $r \in R$ mit $\mathtt{fct}(r) = (s_1, \ldots, s_n)$ ist $r^{\mathfrak{A}}$ eine Relation:*

$$r^{\mathfrak{A}} \subseteq A_{s_1} \times \ldots \times A_{s_n},$$

(d) *für $k \in K$ mit $\mathtt{fct}(k) = s$ ist $k^{\mathfrak{A}}$ eine Konstante: $k^{\mathfrak{A}} \in A_s$*

Im Fall der oben diskutierten Vektorräume am Beispiel der komplexen Zahlen haben wir die Sortenmenge $S = \{Vektor, Skalar\}$, wobei $A_{Vektor} = \mathbb{C} \neq \varnothing$ und $A_{Skalar} = \mathbb{R} \neq \varnothing$. Weiterhin haben wir etwa das Funktionszeichen $\cdot_V$ als Element der Menge $F = \{+_V, \cdot_V, +_{Sk}, \cdot_{Sk}\}$, wobei $\mathtt{fct}(\cdot_V) = (Skalar, Vektor, Vektor)$, welches als Funktion

$$\cdot_V{}^{\mathbb{C}} : A_{Skalar} \times A_{Vektor} \to A_{Vektor}$$

interpretiert wird. Konkret bedeutet dies, dass wir mithilfe der Einsetzung der obigen Trägermengen eine Funktion $\cdot_V{}^{\mathbb{C}} : \mathbb{R}\times\mathbb{C} \to \mathbb{C}$ haben. Im Beispiel C haben wir die Funktion "$\cdot_V{}^{\mathbb{C}}$" kurz als "$\cdot_{\mathbb{C}}$" bezeichnet.

Gehen wir in unseren Betrachtungen einen Schritt weiter: Zu einer gegebenen Signatur σ gibt es eine Vielzahl von σ-Strukturen. Eine Aufgabe einer mathematischen Theorie ist es, durch Klassifizierung einen Überblick über die Klasse aller Möglichkeiten zu erlangen. Wir wollen nun diesbezüglich nützliche Definitionen allgemein studieren, die wir etwa in der Linearen Algebra im nächsten Semester im Speziellen mit Vektorräumen und so genannten linearen Abbildungen vertiefen werden.

Definition 14.3. *Sei* $\sigma = (S, F, R, K, \mathtt{fct})$ *eine Signatur und seien*

$$\mathfrak{A} = (\,(A_s)_{s\in S}, (f^{\mathfrak{A}})_{f\in F}, (r^{\mathfrak{A}})_{r\in R}, (k^{\mathfrak{A}})_{k\in K}\,) \text{ und}$$
$$\mathfrak{B} = (\,(B_s)_{s\in S}, (f^{\mathfrak{B}})_{f\in F}, (r^{\mathfrak{B}})_{r\in R}, (k^{\mathfrak{B}})_{k\in K}\,)$$

zwei σ*- Strukturen. Dann ist* $\mathfrak{A}$ *eine* Substruktur *oder* Unterstruktur *von* $\mathfrak{B}$*, wenn:*

(a) *für* $s \in S$ *ist* $A_s \subseteq B_s$*;*
(b) *für* $f \in F$ *mit* $\mathtt{fct}(f) = (s_1, \ldots, s_n, s_{n+1})$ *und* $a_1 \in A_{s_1}, \ldots,$ $a_n \in A_{s_n}$ *ist* $f^{\mathfrak{A}}(a_1, \ldots, a_n) = f^{\mathfrak{B}}(a_1, \ldots, a_n)$*;*
(c) *für* $r \in R$ *mit* $\mathtt{fct}(r) = (s_1, \ldots, s_n)$ *und* $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$ *ist* $r^{\mathfrak{A}}(a_1, \ldots, a_n)$ *genau dann, wenn* $r^{\mathfrak{B}}(a_1, \ldots, a_n)$*;*
(d) *für* $k \in K$ *mit* $\mathtt{fct}(k) = s$ *ist* $k^{\mathfrak{A}} = k^{\mathfrak{B}}$*.*

Man schreibt auch $\mathfrak{A} \subseteq \mathfrak{B}$*, wenn* $\mathfrak{A}$ *eine Substruktur von* $\mathfrak{B}$ *ist.*

Eine Substruktur wird duch Einschränkung der Trägermenge gegeben; die übrigen Komponenten der Struktur werden entsprechend eingeschränkt.

In den anfangs formulierten Beispielen kann man erkennen, dass die reellen Zahlen im Beispiel A eine Substruktur der komplexen Zahlen $\mathbb{C}$ im Beispiel B sind, beide Strukturen betrachtet in der Signatur der Körper $\sigma_{\mathbb{K}} := (\mathit{Elemente}; +, \cdot; 0, 1, \mathtt{fct})$, wobei die Funktionalität gegeben ist durch: $\mathtt{fct}(\cdot) = \mathtt{fct}(+) = (\mathit{Elemente}, \mathit{Elemente}, \mathit{Elemente})$ und $\mathtt{fct}(0) = \mathtt{fct}(1) = \mathit{Elemente}$ ist. Insbesondere haben wir in der Signatur der Körper nur eine Sorte, die wir hier künstlich als "*Elemente*" bezeichen.

Darüber hinaus ist beispielsweise die additive Gruppe der ganzen Zahlen $(\mathbb{Z}, +)$ eine Untergruppe der additiven Gruppe der reellen Zahlen $(\mathbb{R}, +)$.

Nicht immer haben wir die Situation, dass die eine Struktur eine Substruktur der anderen ist und dennoch enthält die eine Struktur in einem geeigneten Sinne die andere – etwa wenn wir mit $\mathfrak{A} = (A, \dots)$ die reellen Zahlen (wie in Beispiel A) und mit $\mathfrak{B} = (B, \dots)$ die Menge der Ortsvektoren in der reellen Ebene, nämlich $B = \{(x, y) \,|\, x, y \in \mathbb{R}\}$ (wie in Beispiel C), über einer geeigneten Signatur betrachten. Dann ist $\mathfrak{A}$ keine Substruktur von $\mathfrak{B}$, aber wir finden eine geeignete Teilmenge A' von B, nämlich $\{(x, 0) | x \in \mathbb{R}\}$, so dass $\mathfrak{A}$ und $\mathfrak{A}'$ mittels einer Bijektion miteinander identifiziert werden können und $\mathfrak{A}'$ eine Substruktur von $\mathfrak{B}$ ist. Die identifizierende Bijektion kann derart gewählt werden, dass sie verträglich mit den Operationen ist, die durch die Signatur gegeben sind.

Diese Situation präzisieren wir allgemein:

Definition 14.4. *Sei $\sigma = (S, F, R, K, \mathtt{fct})$ eine Signatur und seien*

$$\begin{aligned} \mathfrak{A} &= ((A_s)_{s\in S}, (f^{\mathfrak{A}})_{f\in F}, (r^{\mathfrak{A}})_{r\in R}, (k^{\mathfrak{A}})_{k\in K}) \text{ und} \\ \mathfrak{B} &= ((B_s)_{s\in S}, (f^{\mathfrak{B}})_{f\in F}, (r^{\mathfrak{B}})_{r\in R}, (k^{\mathfrak{B}})_{k\in K}) \end{aligned}$$

zwei σ-Strukturen. Weiterhin sei $s \in S$, so dass für alle $s' \in S \setminus \{s\}$ gilt, dass $A_{s'} = B_{s'}$. Für eine Abbildung $h : A_s \to B_s$ und $t \in S$ definieren wir nun:

$$h_t : A_t \to B_t, \qquad h_t := \begin{cases} h & \text{falls } t = s \\ \mathrm{id}_{A_t} & \text{falls } t \neq s \end{cases}$$

Dann heißt $h : A_s \to B_s$ ein s-Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$, wenn:

(a) *für $f \in F$ mit $\mathtt{fct}(f) = (s_1, \dots, s_n, s_{n+1})$ und $a_1 \in A_{s_1}, \dots, a_n \in A_{s_n}$ ist:*

$$f^{\mathfrak{B}}(h_{s_1}(a_1), \dots, h_{s_n}(a_n)) = h_{s_{n+1}}(f^{\mathfrak{A}}(a_1, \dots, a_n))$$

(b) *für* $r \in R$ *mit* $\mathtt{fct}(r) = (s_1, \ldots, s_n)$ *und* $a_1 \in A_{s_1}, \ldots, a_n \in A_{s_n}$ *ist:*

$$r^{\mathfrak{B}}(h_{s_1}(a_1), \ldots, h_{s_n}(a_n)) \text{ gdw. } r^{\mathfrak{A}}(a_1, \ldots, a_n)$$

(c) *für* $k \in K$ *mit* $\mathtt{fct}(k) = s_1$ *ist* $k^{\mathfrak{B}} = h_{s_1}(k^{\mathfrak{A}})$

Man schreibt in diesem Falle auch kurz: $h : \mathfrak{A} \to_s \mathfrak{B}$.

Wenn darüber hinaus im Kontext klar ist, welches $s \in S$ das Kanonische ist oder sogar $|S| = 1$ gilt, dann schreibt man auch nur $h : \mathfrak{A} \xrightarrow{hom} \mathfrak{B}$ und spricht von einem *Homomorphismus*. Den ersten Fall haben wir etwa bei Strukturen in der Vektorraumsignatur σ_{VR}: Das kanonisch gewählte $s \in \{Vektor, Skalar\}$ wird $s = Vektor$ sein. Den zweiten Fall haben wir häufiger – beispielsweise in der Signatur der Gruppen.

Schauen wir uns nun aber Beispiele für Homomorphismen entsprechend der obigen Definition an:

Betrachte $h_0 : (\mathbb{Z}, +, 0) \to (\mathbb{Z}, +, 0)$, wobei $h_0(x) = 2x$. Dann überlegen wir uns die entsprechende Version von Eigenschaft (a) aus der obigen Definition:

$$\begin{aligned} +^{\mathfrak{B}}(h_0(x), h_0(y)) &= h_0(x) +^{\mathfrak{B}} h_0(y) = 2x +^{\mathfrak{B}} 2y \\ &= 2 \cdot (x +^{\mathfrak{B}} y) = h_0(x +^{\mathfrak{A}} y) \\ &= h_0(+^{\mathfrak{A}}(x, y)). \end{aligned}$$

Für die Bedingung (c) betreffs des Konstantensymbols gilt:

$$0^{\mathfrak{B}} = 2 \cdot 0^{\mathfrak{B}} = h_0(0^{\mathfrak{A}}).$$

Damit ist h_0 ein Homomorphismus. Hierbei bezeichnet –wie auch im Folgenden– $\mathfrak{A}$ jeweils die Struktur des Definitionsbereiches und $\mathfrak{B}$ jeweils die Struktur im Bildbereich.

Betrachte $h_1 : (\mathbb{R}, +, 0) \to (\mathbb{R}, +, 0)$, wobei $h_1(x) = 2x$. Dann ist auch dies in Analogie zu h_0 ebenfalls ein Homomorphismus.

Betrachte $g : (\mathbb{R}, +, 0) \to (\mathbb{R}, +, 0)$, wobei $g(x) = x + 1$. Dann ist g *kein* (Gruppen-) Homomorphismus, denn:

$$+^{\mathfrak{B}}(g(x), g(y)) = g(x) +^{\mathfrak{B}} g(y)$$

$$\begin{aligned} &= (x +^{\mathfrak{B}} 1) +^{\mathfrak{B}} (y +^{\mathfrak{B}} 1) \\ &= (x +^{\mathfrak{B}} y +^{\mathfrak{B}} 1) +^{\mathfrak{B}} 1 \\ &\neq x +^{\mathfrak{B}} y +^{\mathfrak{B}} 1 \\ &= g(x +^{\mathfrak{A}} y) = g(+^{\mathfrak{A}}(x, y)) \end{aligned}$$

Betrachte $h_2 : (\mathbb{Z}_2, \otimes) \to (\{\mathsf{falsch}, \mathsf{wahr}\}, \wedge)$, wobei $h_2(0) = \mathsf{falsch}$ und $h_2(1) = \mathsf{wahr}$. Durch Fallunterscheidung oder –wie bereits auf Seite 5 gesehen– durch Aufstellen beider Verknüpfungstafeln sieht man, dass h_2 ein Homomorphismus ist. Beachten Sie, dass wir hier zwei Strukturen in der Signatur $\sigma = (S, F, R, K, \mathtt{fct})$ haben, wobei: $|S| = 1$, also etwa $S = \{s\}$, $F = \{f\}$ mit $\mathtt{fct}(f) = (s, s, s)$, $R = \varnothing$ und $K = \varnothing$. Insbesondere gilt für die Interpretationen des Symbols f in beiden Strukturen, dass $f^{(\mathbb{Z}_2, \otimes)} = \otimes$ und $f^{(\{\mathsf{falsch},\mathsf{wahr}\}, \wedge)} = \wedge$. Entsprechend ist die analog definierte Abbildung $h_3 : (\mathbb{Z}_2, \oplus) \to (\{\mathsf{falsch}, \mathsf{wahr}\}, \mathsf{xor})$ ebenfalls ein Homomorphismus.

Außerdem ist $h_4 : (G, +, e) \to (G, +, e)$ mit $h_4(x) := e$ ebenfalls ein Homomorphismus:

$$\begin{aligned} +^{\mathfrak{B}}(h_4(x), h_4(y)) &= h_4(x) +^{\mathfrak{B}} h_4(y) = e +^{\mathfrak{B}} e \\ &= e = h_4(x +^{\mathfrak{A}} y) = h_4(+^{\mathfrak{A}}(x, y)). \end{aligned}$$

Außerdem gilt nach Definition insbesondere, dass: $e = h_4(e)$.

Betrachte nun die Abbildung $h_5 : (\mathbb{Z}, +, \cdot, 0, 1) \to (\mathbb{Z}_7, \oplus_7, \otimes_7, [0]_7, [1]_7)$ mit $h_5(x) := [x]_7$. Dann ist auch diese Abbildung ein Homomorphismus.

$$\begin{aligned} +^{\mathfrak{B}}(h_5(x), h_5(y)) &= h_5(x) +^{\mathfrak{B}} h_5(y) = [x]_7 +^{\mathfrak{B}} [y]_7 \\ &= [\,[x]_7 +^{\mathfrak{A}} [y]_7\,]_7 \;=\; [x +^{\mathfrak{A}} y]_7 \;=\; h_5(x +^{\mathfrak{A}} y) \\ &= h_5(+^{\mathfrak{A}}(x, y)) \end{aligned}$$

Analog zeigt man die entsprechende Bedingung für die Multiplikation. Offensichtlich gilt für die Konstanten: $h_5(0) = [0]_7$ und $h_5(1) = [1]_7$.

Wenn Sie sich die obigen Beispiele genau anschauen, dann erkennen Sie qualitative Unterschiede, die wir entsprechend der nächsten Definition bestimmen können:

Definition 14.5. *Sei $h : \mathfrak{A} \to_s \mathfrak{B}$ ein s-Homomorphismus zwischen σ-Strukturen $\mathfrak{A}$ und $\mathfrak{B}$. Dann ist h eine Abbildung $h : A_s \to B_s$ zwischen den Trägermengen A_s und B_s. Wir definieren:*

(a) *h ist ein* **Monomorphismus**, *wenn h injektiv ist.*
(b) *h ist ein* **Epimorphismus**, *wenn h surjektiv ist.*
(c) *h ist ein* **Isomorphismus**, *wenn h bijektiv ist.*
(d) *h ist ein* **Endomorphismus**, *wenn $A_s = B_s$ ist.*
(e) *h ist ein* **Automorphismus**, *wenn h bijektiv und $A_s = B_s$ ist.*

Mithilfe dieser Bezeichnungen können wir die obigen Begriffe wie folgt anwenden und somit die einzelnen Homomorphismen unterscheiden:

	h_0	h_1	h_2	h_3	h_4	h_5
Monomorphismus	+	+	+	+	−	−
Epimorphismus	−	+	+	+	−	+
Isomorphismus	−	+	+	+	−	−
Endomorphismus	+	+	−	−	+	−
Automorphismus	−	+	−	−	−	−

Hierbei bedeutet "+" das Zutreffen der jeweiligen Eigenschaft und "−", dass die betrachtete Eigenschaft nicht zutrifft. Für h_4 haben wir angenommen, dass $G \neq \{e\}$ und somit nicht trivial ist. Sollte G nur aus dem neutralen Element bestehen, erfüllt h_4 natürlich trivialerweise alle Eigenschaften (wie auch schon der Homomorphismus h_1).

15. Prädikatenlogische Formeln und Interpretationen

Bisher haben wir in den Kapiteln 11, 12 und 13 lediglich aussagenlogische Formeln betrachtet. Nachdem wir uns anschließend über Signaturen unterhalten haben, können wir nun einen Schritt weitergehen. Wir möchten jetzt auch kompliziertere und aussagekräftigere Formeln mithilfe von mächtigeren Alphabeten und mit Quantoren betrachten, also etwa Formeln der Gestalt: $\forall x \, \exists y \, (x + y = z)$. Auch diese Art Formeln werden wieder induktiv in mehreren Schritten eingeführt:

Definition 15.1. *Sei $\sigma = (S, F, R, K, \mathtt{fct})$ eine Signatur. Die zu σ gehörige Sprache $\mathcal{L}^\sigma$ besteht aus mehreren Komponenten:*

(a) *Variablen: für jede Sorte $s \in S$ gibt es abzählbar viele Variablen: $v_0^s, v_1^s, v_2^s, \ldots$*

(b) *Symbole: die Symbolmenge E^σ der Sprache $\mathcal{L}^\sigma$ ist die folgende Vereinigung:*
$F \cup R \cup K \cup \{v_n^s | n \in \mathbb{N}, s \in S\} \cup \{(,), =, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists\}$

(c) *Terme: Die Menge $\mathtt{Tm}^\sigma$ der σ-Terme wird induktiv definiert. Jedem Term t wird außerdem ein Typ $\mathtt{tp}(t) \in S$ zugeordnet:*
   (i) *alle Variablen v_n^s sind Terme vom Typ $\mathtt{tp}(v_n^s) = s$.*
   (ii) *alle Konstantensymbole $k \in K$ sind Terme vom Typ $\mathtt{tp}(k) = \mathtt{fct}(k)$.*
   (iii) *für alle n-stelligen Funktionssymbole $f \in F$ mit der Funktionalität $\mathtt{fct}(f) = (s_1, \ldots, s_n, s_{n+1})$ und beliebigen Termen $t_1, \ldots, t_n$, wobei $\mathtt{tp}(t_1) = s_1, \ldots, \mathtt{tp}(t_n) = s_n$ gilt, $f(t_1, \ldots t_n)$ ist dann ebenfalls ein Term vom Typ $\mathtt{tp}(f(t_1, \ldots, t_n)) = s_{n+1}$.*

(d) *Relationale Formeln: Für eine Sorte $s \in S$ und Terme t_1, t_2 mit $\mathtt{tp}(t_1) = \mathtt{tp}(t_2) = s$ ist $t_1 = t_2$ eine relationale Formel. Außerdem ist für alle n-stelligen Relationssymbole $r \in R$ mit der Funktionalität $\mathtt{fct}(r) = (s_1, \ldots, s_n)$ und Termen $t_1, \ldots, t_n$ mit $\mathtt{tp}(t_1) = s_1, \ldots, \mathtt{tp}(t_n) = s_n$ auch $r(t_1, \ldots, t_n)$ eine relationale Formel. Relationale Formeln werden auch Atomformeln genannt.*

(e) *Formeln: Die Menge $\mathtt{Fml}^\sigma$ der Sprache $\mathcal{L}^\sigma$ wird induktiv definiert:*
   (i) *Jede relationale Formel ist eine Formel.*
   (ii) *Wenn φ eine Formel ist, so ist auch $\neg\varphi$ eine Formel.*
   (iii) *Wenn φ und ψ Formeln sind, so auch $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$.*
   (iv) *Wenn φ eine Formel ist und v_n^s eine Variable, so sind auch $\forall v_n^s \varphi$ und $\exists v_n^s \varphi$ Formeln.*

Schauen wir uns diese Sprachstruktur am Beispiel der komplexen Zahlen im Sinne eines Vektorraumes an – siehe Beispiel C aus dem letzten Kapitel.

So können wir in der Sprache der Vektorräume –gegeben durch die Signatur σ_{VR}– folgendes für die einzelnen Bereiche feststellen:

Variablen: Wir haben $v_n^{Vektor}, v_n^{Skalar}$ für beliebige natürliche Zahlen n. Üblicherweise werden diese Variablen durch besondere Buchstaben $x, y, z, \ldots$ für Vektorvariablen und $\lambda, \mu, \nu, \ldots$ für Skalarvariablen bezeichnet.

Terme: Wir haben beispielsweise Terme der Gestalt $+_{Sk}(\lambda, \mu)$, $\cdot_{Sk}(\lambda, \mu)$, $+_V(x, y)$, aber auch $\cdot_V(\lambda, x)$ und $+_V(\cdot_V(\lambda, x), \cdot_V(\mu, y))$. Die Terme sind in üblichen Infix-Schreibweisen mit Klammersetzung besser zu verstehen als $\lambda +_{Sk} \mu$, $\lambda \cdot_{Sk} \mu$, $\ldots$ bis hin zu $(\lambda \cdot_V x) +_V (\mu \cdot_V y)$. Da die Variablen den Typ der auf sie anwendbaren Funktionen bestimmen, lässt sich ableiten, ob an bestimmten Stellen des Terms $+_{Sk}$ oder $\cdot_V$ stehen muß. Daher schreiben wir in der Regel kurz: $(\lambda \cdot x) + (\mu \cdot y)$. Manchmal gelten auch zusätzliche Konventionen, wie "Punktrechnung geht vor Strichrechnung" und "Multiplikationspunkte schreiben wir nicht", so dass es zu schreiben genügt: $\lambda x + \mu y$.

Relationale Formeln: Hier liegt nur das Gleichheitszeichen "=" vor, so dass wir beispielsweise die Formel $\lambda x + \mu y = 0$ betrachten können. Hierbei ist aus dem Zusammenhang klar, dass $\mathtt{tp}(0) = \mathtt{fct}(0) = Vektor$ gilt, so dass das Symbol "0" eigentlich eine Abkürzung von 0_V ist.

Formeln: In der Signatur der Vektorräume haben wir etwa die Formel

$$\forall v_0^{Skalar}\, \forall v_{17}^{Skalar}\, \forall v_{1018}^{Vektor} \\ \cdot_V(v_0^{Skalar}, \cdot_V(v_{17}^{Skalar}, v_{1018}^{Vektor})) = \cdot_V(\cdot_{Sk}(v_0^{Skalar}, v_{17}^{Skalar}), v_{1018}^{Vektor})$$

bzw. mit den obigen Konventionen kürzer (und vor allem lesbarer) geschrieben:

$$\forall \lambda\, \forall \mu\, \forall x\, (\, \lambda(\mu x) = (\lambda\mu)x\,).$$

Dem roten Faden aus den Kapiteln über Aussagenlogik folgend, kommen wir nun zur Interpretation von prädikatenlogischen Formeln in geeigneten Strukturen:

Definition 15.2. *Sei $\sigma = (S, F, R, K, \mathtt{fct})$ eine Signatur mit zugehöriger Sprache $\mathcal{L}^\sigma$ und sei $\mathfrak{A} = ((A_s)_{s\in S}, (f^{\mathfrak{A}})_{f\in F}, (r^{\mathfrak{A}})_{r\in R}, (k^{\mathfrak{A}})_{k\in K})$ eine σ-Struktur. Die Interpretation von $\mathcal{L}^\sigma$ in $\mathfrak{A}$ wird schrittweise definiert:*

(a) *Eine Belegung in $\mathfrak{A}$ ist eine Funktion $\beta : \{v_n^s | n \in \mathbb{N}, s \in S\} \to \bigcup_{s\in S} A_s$, so dass für alle $n \in \mathbb{N}$ und $s \in S$ gilt: $\beta(v_n^s) \in A_s$.*

Es ist manchmal wichtig, den Wert einer Belegung β an einer Variablen $v_{n'}^{s'}$ zu einem gegebenen $a \in A_{s'}$ zu modifizieren.

Definiere $\beta\frac{a}{v_{n'}^{s'}} : \{v_n^s | n \in \mathbb{N}, s \in S\} \to \bigcup_{s\in S} A_s$, die modifizierte Belegung ausgehend von einer Belegung β, wie folgt:

$$\beta\frac{a}{v_{n'}^{s'}}(v_n^s) = \begin{cases} \beta(v_n^s) & \text{falls } v_n^s \neq v_{n'}^{s'} \\ a & \text{falls } v_n^s = v_{n'}^{s'} \end{cases}$$

(b) *Ein σ-Modell ist ein geordnetes Paar $\mathfrak{M} = (\mathfrak{A}, \beta)$, bestehend aus einer σ-Struktur $\mathfrak{A}$ und einer Belegung β in $\mathfrak{A}$.*

Für die weiteren Definitionen sei ein Modell $\mathfrak{M} = (\mathfrak{A}, \beta)$ fixiert.

(c) *Für einen Term $t \in \mathtt{Tm}^\sigma$ der Sprache $\mathcal{L}^\sigma$ definiere die Interpretation $\mathfrak{M}(t)$ im Modell $\mathfrak{M}$ durch Rekursion über den Aufbau von t:*

(i) *Für eine Variable v_n^s setze: $\mathfrak{M}(v_n^s) = \beta(v_n^s)$.*

(ii) *Für ein Konstantensymbol $k \in K$ setze: $\mathfrak{M}(k) = k^{\mathfrak{A}}$.*

(iii) *Für ein n-stelliges Funktionssymbol $f \in F$ und Terme $t_1, \ldots, t_n \in \mathtt{Tm}^\sigma$ setze:*

$$\mathfrak{M}(f(t_1, \ldots, t_n)) = f^{\mathfrak{A}}(\mathfrak{M}(t_1), \ldots, \mathfrak{M}(t_n)).$$

(d) *Für eine Formel $\varphi \in \mathcal{L}^\sigma$ definiere, dass $\mathfrak{M}$ ein Modell von φ ist, $\mathfrak{M} \vDash \varphi$, durch Rekursion über den Aufbau von φ:*

(i) *für Terme $t_1, t_2 \in \mathtt{Tm}^\sigma$ setze:*

$$\mathfrak{M} \vDash t_1 = t_2 \;:\Longleftrightarrow\; \mathfrak{M}(t_1) = \mathfrak{M}(t_2).$$

(ii) *Für ein n-stelliges Relationssymbol $r \in R$ und Terme $t_1, \ldots, t_n \in \mathtt{Tm}^\sigma$ setze:*

$$\mathfrak{M} \vDash r(t_1, \ldots, t_n) \;:\Longleftrightarrow\; r^{\mathfrak{A}}(\mathfrak{M}(t_1), \ldots, \mathfrak{M}(t_n)).$$

(iii) *Für zusammengesetzte Formeln setzen wir wie folgt:*

$$\begin{aligned}
\mathfrak{M} \vDash \neg\varphi &\quad :\Longleftrightarrow \quad \mathfrak{M} \nvDash \varphi \\
\mathfrak{M} \vDash (\varphi \wedge \psi) &\quad :\Longleftrightarrow \quad \mathfrak{M} \vDash \varphi \text{ und } \mathfrak{M} \vDash \psi \\
\mathfrak{M} \vDash (\varphi \vee \psi) &\quad :\Longleftrightarrow \quad \mathfrak{M} \vDash \varphi \text{ oder } \mathfrak{M} \vDash \psi \\
\mathfrak{M} \vDash (\varphi \to \psi) &\quad :\Longleftrightarrow \quad \mathfrak{M} \vDash \varphi \text{ impliziert } \mathfrak{M} \vDash \psi \\
&\qquad\qquad\quad \text{(d.h. wenn } \mathfrak{M} \vDash \varphi\text{, dann } \mathfrak{M} \vDash \psi\text{)} \\
\mathfrak{M} \vDash (\varphi \leftrightarrow \psi) &\quad :\Longleftrightarrow \quad \mathfrak{M} \vDash \varphi \text{ ist äquivalent zu } \mathfrak{M} \vDash \psi \\
\mathfrak{M} \vDash \forall v_n^s \varphi &\quad :\Longleftrightarrow \quad \text{für alle } a \in A_s \text{ gilt } \mathfrak{M}\frac{a}{v_n^s} \vDash \varphi \\
\mathfrak{M} \vDash \exists v_n^s \varphi &\quad :\Longleftrightarrow \quad \text{es existiert ein } a \in A_s \text{ mit } \mathfrak{M}\frac{a}{v_n^s} \vDash \varphi
\end{aligned}$$

wobei $\mathfrak{M}\frac{a}{v_n^s}$ *definiert ist als* $(\mathfrak{A}, \beta\frac{a}{v_n^s})$.

Man sagt für $\mathfrak{M} \vDash \varphi$ *auch, dass: "*$\mathfrak{M}$ *erfüllt* φ*" oder "*φ *gilt in* $\mathfrak{M}$*".*

Wie schon in der Aussagenlogik benutzen wir hier massiv die eindeutige Lesbarkeit der prädikatenlogischen Formeln, die wir aber nicht weiter zeigen werden.

Ähnlich wie die Primvariablen einer aussagenlogischen Formel, definieren wir nun die Menge der in einer Formel φ *vorkommenden Variablen*, $\mathsf{Var}(\varphi)$, die Menge der in φ *gebundenen Variablen*, $\mathsf{Geb}(\varphi)$, und die Menge der in φ *frei vorkommenden Variablen*, $\mathsf{Fr}(\varphi)$.

Zunächst schauen wir uns die hierfür notwendige Menge von Variablen auf Termen an und setzen (per Induktion über den Termaufbau):

$$\begin{aligned}
&\mathsf{Var}(v) := \{v\} \\
&\mathsf{Var}(k) := \varnothing \\
&\mathsf{Var}(f(t_1, \ldots, t_n)) := \mathsf{Var}(t_1) \cup \ldots \cup \mathsf{Var}(t_n)
\end{aligned}$$

Und schließlich definieren wir die gewünschten Mengen per Induktion über den Formelaufbau allgemein für beliebige Formeln:

$$\begin{aligned}
&\mathsf{Var}(t_1 = t_2) := \mathsf{Var}(t_1) \cup \mathsf{Var}(t_2) \\
&\mathsf{Var}(r(t_1, \ldots, t_n)) := \mathsf{Var}(t_1) \cup \ldots \cup \mathsf{Var}(t_n) \\
&\mathsf{Var}(\neg\varphi) := \mathsf{Var}(\varphi)
\end{aligned}$$

$$\mathsf{Var}((\varphi e \psi)) := \mathsf{Var}(\varphi) \cup \mathsf{Var}(\psi) \quad \text{für } e \in \{\wedge, \vee, \to, \leftrightarrow\}$$
$$\mathsf{Var}(Qv\varphi) := \mathsf{Var}(\varphi) \cup \{v\} \quad \text{für } Q \in \{\forall, \exists\}$$

$$\mathsf{Fr}(t_1 = t_2) := \mathsf{Var}(t_1 = t_2)$$
$$\mathsf{Fr}(r(t_1, \ldots, t_n)) := \mathsf{Var}(r(t_1, \ldots, t_n))$$
$$\mathsf{Fr}(\neg\varphi) := \mathsf{Fr}(\varphi)$$
$$\mathsf{Fr}((\varphi e \psi)) := \mathsf{Fr}(\varphi) \cup \mathsf{Fr}(\psi) \quad \text{für } e \in \{\wedge, \vee, \to, \leftrightarrow\}$$
$$\mathsf{Fr}(Qv\varphi) := \mathsf{Fr}(\varphi) \setminus \{v\} \quad \text{für } Q \in \{\forall, \exists\}$$

$$\mathsf{Geb}(t_1 = t_2) := \varnothing$$
$$\mathsf{Geb}(r(t_1, \ldots, t_n)) := \varnothing$$
$$\mathsf{Geb}(\neg\varphi) := \mathsf{Geb}(\varphi)$$
$$\mathsf{Geb}((\varphi e \psi)) := \mathsf{Geb}(\varphi) \cup \mathsf{Geb}(\psi) \quad \text{für } e \in \{\wedge, \vee, \to, \leftrightarrow\}$$
$$\mathsf{Geb}(Qv\varphi) := \mathsf{Geb}(\varphi) \cup \{v\} \quad \text{für } Q \in \{\forall, \exists\}$$

Mithilfe dieser Mengen können wir uns –analog zu den Überlegungen in der Aussagenlogik im Zusammenhang der Gültigkeit in Modellen– nur auf die Betrachtung der freien Variablen beschränken:

Satz 15.3. *Die Gültigkeit einer Formel φ in einem Modell $\mathfrak{M} = (\mathfrak{A}, \beta)$ hängt nur von der Struktur $\mathfrak{A}$ und den Werten von β auf der Menge der in φ frei vorkommenden Variablen ab, d.h.: für eine Belegung β' mit $\beta(x) = \beta'(x)$ für $x \in \mathsf{Fr}(\varphi)$ gilt:*

$$(\mathfrak{A}, \beta) \vDash \varphi \iff (\mathfrak{A}, \beta') \vDash \varphi.$$

Betrachten wir ein einfaches Beispiel zu diesen Begriffen, indem wir uns den Körper der reellen Zahlen $\mathbb{R}$ und die Formel φ, gegeben durch $\forall x(x+0 = x)$, anschauen. Dann gilt entsprechend der obigen Definition:

$$\begin{aligned} \mathsf{Var}(\ \forall x(x + 0 = x)\ ) &= \mathsf{Var}(x + 0 = x) \cup \{x\} \\ &= (\mathsf{Var}(x + 0) \cup \mathsf{Var}(x)) \cup \{x\} \\ &= (\mathsf{Var}(x) \cup \mathsf{Var}(0) \cup \{x\}) \cup \{x\} \end{aligned}$$

$$\begin{aligned} &= \{x\} \cup \varnothing \cup \{x\} \cup \{x\} \\ &= \{x\} \end{aligned}$$

$$\begin{aligned} \mathsf{Fr}(\,\forall x(x+0=x)\,) &= \mathsf{Fr}(x+0=x) \setminus \{x\} = \mathsf{Var}(x+0=x) \setminus \{x\} \\ &= (\{x\} \cup \varnothing \cup \{x\}) \setminus \{x\} \\ &= \varnothing \end{aligned}$$

$$\begin{aligned} \mathsf{Geb}(\,\forall x(x+0=x)\,) &= \mathsf{Geb}(x+0=x) \cup \{x\} = \varnothing \cup \{x\} \\ &= \{x\} \end{aligned}$$

Schauen wir uns weiterhin an, warum in den reellen Zahlen diese Formel gilt, also warum die Behauptung gilt, dass in den reellen Zahlen die Formel $\forall x(x+0=x)$ gültig ist. Beachten Sie: Da $\mathsf{Fr}(\forall x(x+0=x)) = \varnothing$ brauchen wir nach Satz 15.3 keine Belegung zu betrachten. Um die Definition dennoch im Detail durchzugehen, fixieren wir eine beliebige Belegung β und zeigen

$$(\mathbb{R}, \beta) \vDash \forall x(x+0=x)$$

durch Induktion entsprechend der Definition der Gültigkeit. Beachten Sie hierfür, dass wir bereits die Signatur $\sigma_{\mathbb{K}}$ der Körper auf Seite 93 eingeführt hatten.

Wir haben nach Definition 15.2(d)(iii) die geforderte Behauptung genau dann, wenn für alle $a \in A_{Elemente} = \mathbb{R}$ gilt:

$$(\mathbb{R}, \beta\frac{a}{x}) \vDash x+0=x.$$

Dies ist genau dann der Fall, wenn für alle $a \in \mathbb{R}$ gilt:

$$(\mathbb{R}, \beta\frac{a}{x})(x+0) = (\mathbb{R}, \beta\frac{a}{x})(x).$$

Nun gilt aber für beliebige $a \in \mathbb{R}$ immer die Gleichung:

$$\begin{aligned} (\mathbb{R}, \beta\frac{a}{x})(x+0) &= (\mathbb{R}, \beta\frac{a}{x})(x) +_{\mathbb{R}} 0^{\mathbb{R}} = a +_{\mathbb{R}} 0 = a \\ &= \beta\frac{a}{x}(x) = (\mathbb{R}, \beta\frac{a}{x})(x) \end{aligned}$$

Damit haben wir den Nachweis der Gültigkeit dieser Formel erbracht.

Schauen wir uns noch ein Beispiel zu komplexen Zahlen (d.h. allgemein zu Vektorräumen) an. Sei dafür die Signatur σ_{VR} der Vektorräume

$$\sigma_{\mathrm{VR}} = (Vektor, Skalar; +_{Vk}, \cdot_{Vk}, +_{Sk}, \cdot_{Sk}; 0_{Sk}, 1_{Sk}, 0_{Vk}; \mathtt{fct})$$

gegeben. Betrachten wir weiterhin einen beliebigen Vektorraum:

$$\mathfrak{V} = (V, \mathbb{K}; +_{\mathbb{K}}, \cdot_{\mathbb{K}}, +_V, \cdot_V; 0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_V),$$

etwa die komplexen Zahlen selbst. Erinnern Sie sich an die Zusammenhänge; so ist die Interpretation des Symbols $+_{Vk}$ der Signatur die Funktion $+_{Vk}^{\mathfrak{V}} = +_V$ im speziellen Vektorraum $\mathfrak{V}$.

Betrachten wir weiterhin die Formel:

$$\forall\lambda\, \forall x\, \forall y\, (\ \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y\ ).$$

Nun können wir uns analog zum ersten Beispiel fragen, ob diese Formel in den komplexen Zahlen oder eben allgemein im gegebenen Vektorraum gilt – also konkret, ob gilt:

$$\mathfrak{V} \vDash \forall\lambda\, \forall x\, \forall y\, (\ \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y\ )$$

Betrachten wir daher die folgenden Äquivalenzen – hierbei kürzen wir die Sorten "$Vektor$" mit "Vk" und "$Skalar$" mit "Sk" ab:

$$\begin{aligned}
&\mathfrak{V} \vDash \forall v_0^{Sk}\, \forall v_0^{Vk}\, \forall v_1^{Vk}\, (\ v_0^{Sk} \cdot_{Vk} (v_0^{Vk} +_{Vk} v_1^{Vk}) \\
&\qquad\qquad = v_0^{Sk} \cdot_{Vk} v_0^{Vk} +_{Vk} v_0^{Sk} \cdot_{Vk} v_1^{Vk}\ ) \\
\iff\quad &\text{für alle } a \in \mathbb{K} \text{ gilt:} \\
&\mathfrak{V}\frac{a}{v_0^{Sk}} \vDash \forall v_0^{Vk}\, \forall v_1^{Vk}\, (\ v_0^{Sk} \cdot_{Vk} (v_0^{Vk} +_{Vk} v_1^{Vk}) \\
&\qquad\qquad = v_0^{Sk} \cdot_{Vk} v_0^{Vk} +_{Vk} v_0^{Sk} \cdot_{Vk} v_1^{Vk}\ ) \\
\iff\quad &\text{für alle } a \in \mathbb{K} \text{ gilt: für alle } b \in V \text{ gilt: für alle } c \in V \text{ gilt:} \\
&\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}} \vDash\ v_0^{Sk} \cdot_{Vk} (v_0^{Vk} +_{Vk} v_1^{Vk}) \\
&\qquad\qquad = v_0^{Sk} \cdot_{Vk} v_0^{Vk} +_{Vk} v_0^{Sk} \cdot_{Vk} v_1^{Vk} \\
\iff\quad &\text{für alle } a \in \mathbb{K} \text{ gilt: für alle } b \in V \text{ gilt: für alle } c \in V \text{ gilt:} \\
&\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Sk} \cdot_{Vk} (v_0^{Vk} +_{Vk} v_1^{Vk})) = \\
&\qquad\qquad \mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Sk} \cdot_{Vk} v_0^{Vk} +_{Vk} v_0^{Sk} \cdot_{Vk} v_1^{Vk})
\end{aligned}$$

$\iff$ für alle $a \in \mathbb{K}$ gilt: für alle $b \in V$ gilt: für alle $c \in V$ gilt:

$$\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Sk}) \cdot_V ($$
$$\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Vk}) +_V \mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_1^{Vk})) =$$
$$\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Sk}) \cdot_V \mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Vk}) +_V$$
$$\mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_0^{Sk}) \cdot_V \mathfrak{V}\frac{a}{v_0^{Sk}}\frac{b}{v_0^{Vk}}\frac{c}{v_1^{Vk}}(v_1^{Vk}))$$

$\iff$ für alle $a \in \mathbb{K}$ und für alle $b, c \in V$ gilt:

$$a \cdot_V (b +_V c) = a \cdot_V b +_V a \cdot_V c$$

Mit diesen zwei Beispielen für die Anwendung der Definition der Gültigkeit kommen wir zu einem weiteren Konzept, welches wir von unseren Betrachtungen in der Aussagenlogik her kennen und nun übertragen können – die allgemeingültigen Formeln:

Definition 15.4. *Sei σ eine Signatur und $\varphi \in \mathcal{L}^\sigma$ eine Formel:*

(a) *Eine Formel φ heißt* allgemeingültig *oder* Tautologie*, wenn jedes σ-Modell ein Modell von φ ist.*

(b) *Eine Formel φ ist* erfüllbar*, wenn es ein σ-Modell von φ gibt.*

In diesem Sinne ist die Formel $\forall x(x = x)$ eine prädikatenlogische Tautologie, denn diese gilt in einem beliebigen prädikatenlogischen Modell. Beachten Sie, dass diese Formel sogar in einer beliebigen Signatur formuliert werden kann.

Weiterhin ist beispielweise die $\sigma_{\mathbb{K}}$-Formel "$y = 0$" erfüllbar, denn es gibt ein Modell, in dem diese Formel gilt – etwa bestehend aus der Struktur der reellen Zahlen und der Belegung β, die die Variable y auf das neutrale Element der Addition abbildet. Offenbar ist hier wesentlich, dass β die Variable y auf Null abbildet.

Allgemeingültig dagegen ist die Formel "$y = 0 \to y = 0$", denn hier spielt es keine Rolle, wie die freie Variable y in einer $\sigma_{\mathbb{K}}$-Struktur belegt

wird. Beachten Sie hierbei, dass in dieser Formel die Variable y frei vorkommt.

Schauen wir uns weitere Beispiele an:

Satz 15.5. *Folgende Formeln sind allgemeingültig für alle Terme* $t, t_1, t_2, t_3 \in \mathtt{Tm}^\sigma$ *und alle Formeln* $\varphi, \psi, \chi \in \mathcal{L}^\sigma$*:*

(a) $t = t$
(b) $t_1 = t_2 \to t_2 = t_1$
(c) $t_1 = t_2 \wedge t_2 = t_3 \to t_1 = t_3$
(d) $\varphi \to (\psi \to \varphi \wedge \psi))$
(e) $\varphi \wedge \psi \to \varphi$
(f) $\varphi \wedge \psi \to \psi$
(g) $\varphi \to \varphi \vee \psi$
(h) $\psi \to \varphi \vee \psi$
(i) $(\varphi \to \chi) \to ((\psi \to \chi) \to ((\varphi \vee \psi) \to \chi))$

Beweis: Wir beweisen exemplarisch die ersten vier Behauptungen und betrachten hierfür ein beliebiges σ-Modell $\mathfrak{M} = (\mathfrak{A}, \beta)$. Die Formel in (a) ist offensichtlich allgemeingültig, denn $\mathfrak{M} \vDash t = t$ gilt nach Definition 15.2 genau dann, wenn $\mathfrak{M}(t) = \mathfrak{M}(t)$ gilt; und dies ist offenbar wahr, da die Gleichheitsrelation (in der Metasprache) reflexiv ist.

In (b) wird behauptet, dass $\mathfrak{M} \vDash (t_1 = t_2 \to t_2 = t_1)$. Dies gilt wiederum genau dann, wenn $\mathfrak{M} \vDash t_1 = t_2$ auch $\mathfrak{M} \vDash t_2 = t_1$ impliziert, also wenn $\mathfrak{M}(t_1) = \mathfrak{M}(t_2)$ gilt, so auch $\mathfrak{M}(t_2) = \mathfrak{M}(t_1)$. Sei also $\mathfrak{M}(t_1) = \mathfrak{M}(t_2)$. Dann gilt aber $\mathfrak{M}(t_2) = \mathfrak{M}(t_1)$, da die Gleichheitsrelation symmetrisch ist.

Im Teil (c) wird behauptet, dass: $\mathfrak{M} \vDash (t_1 = t_2 \wedge t_2 = t_3 \to t_1 = t_3)$. Dies ist äquivalent zu der Aussage, dass

$$\mathfrak{M} \vDash t_1 = t_2 \wedge t_2 = t_3 \text{ impliziert } \mathfrak{M} \vDash t_1 = t_3$$

gdw. $(\mathfrak{M} \vDash t_1 = t_2$ und $\mathfrak{M} \vDash t_2 = t_3)$ impliziert $\mathfrak{M} \vDash t_1 = t_3$

gdw. $(\mathfrak{M}(t_1) = \mathfrak{M}(t_2)$ und $\mathfrak{M}(t_2) = \mathfrak{M}(t_3))$ impliziert $\mathfrak{M}(t_1) = \mathfrak{M}(t_3)$.

Dies ist aber offenbar wahr, denn wenn $\mathfrak{M}(t_1) = \mathfrak{M}(t_2) = \mathfrak{M}(t_3)$, so auch $\mathfrak{M}(t_1) = \mathfrak{M}(t_3)$, da die Gleichheitsrelation transitiv ist.

Und in (d) behaupten wir schließlich, dass: $\mathfrak{M} \vDash \varphi \to (\psi \to (\varphi \wedge \psi))$. Dies gilt aber

gdw. $\mathfrak{M} \vDash \varphi$ impliziert $\mathfrak{M} \vDash \psi \to (\varphi \wedge \psi)$

gdw. $\mathfrak{M} \vDash \varphi$ impliziert ($\mathfrak{M} \vDash \psi$ impliziert $\mathfrak{M} \vDash \varphi \wedge \psi$)

Sei also $\mathfrak{M} \vDash \varphi$. Wir behaupten, dass: $\mathfrak{M} \vDash \psi$ impliziert $\mathfrak{M} \vDash \varphi \wedge \psi$. Sei also zusätzlich nun $\mathfrak{M} \vDash \psi$. Dann gilt aber wieder nach Definition 15.2 wie gewünscht, dass: $\mathfrak{M} \vDash \varphi \wedge \psi$. ⊠

16. Formale Beweise in der Prädikatenlogik

Dieses Thema werden wir nur kurz streifen. Wir haben bereits in den Kapiteln 12 und 13 das Thema der formalen Beweise ausgiebig am Beispiel der Aussagenlogik betrachtet. Wir fassen uns daher kurz und erweitern unseren Kalkül aus der Aussagenlogik um die folgenden Axiome und Regeln: Neben den Schemata (A1) bis (A10), die wir nun auch für prädikatenlogische Formeln nutzen möchten und bereits auf Seite 72 kennengelernt haben, betrachten wir weiterhin auch die folgenden vier Axiome:

(A11) $\forall v\varphi \to \varphi(v/u)$, für eine Variable u

(A12) $\varphi(v/u) \to \exists v\varphi$, für eine Variable u

(A13) $u = u$, für eine Variable u

(A14) $v = u \to (\varphi(w/v) \leftrightarrow \varphi(w/u))$, für Variablen u, v und w

Hierbei bezeichne im Axiom (A11) die Formel $\varphi(v/u)$ (und analog in (A14) für $\varphi(w/v)$ bzw. $\varphi(w/u)$) die Formel, die wir erhalten, wenn wir v an allen Stellen, an denen v frei vorkommt, durch u ersetzen. (Sie erkennen vielleicht, dass hier technische Probleme entstehen, da diese Operation formal nicht überall definiert sind – so ist etwa die Substitution $[\,\forall x\, r(x,y)\,]\,(y/z)$ definiert als $\forall x\, r(x,z)$, aber $[\,\forall x\, r(x,y)\,]\,(y/x)$ ist nicht definiert, da wir sonst unerwünschte Nebeneffekte bekommen würden. Aber diese Details ersparen wir uns an dieser Stelle.)

Zusätzlich zu den Axiomen kommen drei Ableitungsregeln hinzu:

(MP) Aus φ und $\varphi \to \psi$ ist ψ ableitbar.

(Q1) Aus $\varphi \to \psi$ mit $v \notin \mathtt{Fr}(\varphi)$ ist $\varphi \to \forall v\psi$ ableitbar.

(Q2) Aus $\psi \to \varphi$ mit $v \notin \mathtt{Fr}(\varphi)$ ist $\exists v\psi \to \varphi$ ableitbar.

Wie bereits in der Aussagenlogik in Kapitel 12 bedeutet nun das Symbol "$\vdash_\sigma \varphi$", dass die Formel φ in der Sprache $\mathcal{L}^\sigma$ nach den obigen Axiomen und Regeln beweisbar ist, das heißt konkret:

Definition 16.1. *Wir schreiben "$\vdash_\sigma \varphi$", wenn $\varphi \in X$, wobei X die kleinste Menge $X \subseteq \mathtt{Fml}^\sigma$, die alle Axiome enthält und unter* (MP), (Q1), (Q2) *abgeschlossen ist.*

Wenn –wie im Folgenden– die Sprache $\mathcal{L}^\sigma$ fixiert ist, dann schreiben wir auch nur kurz "$\vdash \varphi$". Allerdings ist es wichtig zu wissen, welche Sprache wir zugrunde legen, da davon die Menge der in den Beweisen verwendbaren Formeln abhängt und sich somit auch die Ausdruckstärke unter Umständen ändern kann.

Wir werden hier nur Ansätze der prädikatenlogischen Beweise entlang der Ideen aus Kapitel 12 aufzeigen. In diesem Sinne kann man leicht den folgenden Richtigkeits- bzw. Korrektheitssatz beweisen:

Satz 16.2 (Korrektheitssatz)**.** *Wenn $\vdash \varphi$, dann ist φ allgemeingültig.*

Wir schreiben auch in der Prädikatenlogik "$\vDash \varphi$" für die Aussage, dass die Formel φ allgemeingültig ist, d.h. sie gilt in jedem beliebigen σ-Modell. Dann sagt der Korrektheitssatz aus, dass:

$$\vdash \varphi \quad \Rightarrow \quad \vDash \varphi$$

Wir definieren den uns eigentlich interessierenden Beweisbegriff:

Definition 16.3. *Ein* Beweis *$b = (b_i | i < n)$ von φ ist eine endliche Folge, so dass $\varphi = b_i$ für $i < n$ und für alle $i < n$ gilt: b_i ist entweder ein Axiom oder b_i folgt aus $b_0, \ldots, b_{i-1}$ durch eine unmittelbare Anwendung von* (MP), (Q1), (Q2).

Und damit können wir analog zu Kapitel 12 zeigen:

Satz 16.4. *Es gilt: $\vdash \varphi$ gdw. φ hat einen Beweis.*

Die ersten formalen Beweise bekommt man für die aussagenlogischen Tautologien, da wir den Beweiskalkül der Aussagenlogik erweitert haben und wir somit die Beweise überführen können.

Satz 16.5. *Alle substituierten aussagenlogischen Tautologien, d.h. Formeln, die durch Substitution der Aussagenvariablen einer aussagenlogischen Tautologie durch prädikatenlogische Formeln entstehen, sind beweisbar.*

Im Beweis nimmt man sich einen formalen Beweis der ursprünglichen Tautologie im aussagenlogischen Kalkül her und substituiert dann entsprechend die einzelnen Beweisschritte, um so einen formalen Beweis der prädikatenlogischen Formel im prädikatenlogischen Kalkül zu erhalten.

Wir geben den ersten prädikatenlogischen formalen Beweis mit der folgenden wichtigen *Schnittregel* an:

Satz 16.6 (Schnittregel)**.** *Wenn* $\vdash \varphi \to \psi$ *und* $\vdash \psi \to \chi$*, so* $\vdash \varphi \to \chi$*.*

Beweis: Wir können hier den Satz 16.5 zusammen mit der Tautologie $[(p \to q) \wedge (q \to r)] \to (p \to r)$ ausnutzen, um dann mittels (MP) zum Ziel zu kommen. (An dieser Stelle wären wir auch mit dem Axiom (A6) schnell zum Ziel gekommen.) ⊠

Eine erste Beweiskette geben wir im Beweis der folgenden Aussage an:

Satz 16.7. *Wenn* $\vdash \varphi$*, dann* $\vdash \forall v\varphi$*.*

Beweis: Es sei $\vdash \varphi$. Dann finden wir den folgenden formalen Beweis:

$\vdash \varphi$	(Vor.)
$\vdash \varphi \to ((\psi \vee \neg\psi) \to \varphi)$	(für $v \notin \mathsf{Fr}(\psi)$) (Tautologie/(A2))
$\vdash (\psi \vee \neg\psi) \to \varphi$	(MP)
$\vdash (\psi \vee \neg\psi) \to \forall v\varphi$	(Q1)
$\vdash \psi \vee \neg\psi$	(Satz 16.5, Tautologie)
$\vdash \forall v\varphi$	(MP)

⊠

Satz 16.8. *Es gilt:* $\vdash \forall v(\varphi \to \psi) \to (\forall v\varphi \to \forall v\psi)$

Beweis:

$\vdash \forall v(\varphi \to \psi) \to (\varphi \to \psi)$	(A11)
$\vdash \varphi \to (\forall v(\varphi \to \psi) \to \psi)$	(nach (MP) und Tautologie: $(p \to (q \to r)) \to (q \to (p \to r))$)

$\vdash \forall v\varphi \to \varphi$ (A11)

$\vdash \forall v\varphi \to (\forall v(\varphi \to \psi) \to \psi)$ (Schnittregel)

$\vdash (\forall v\varphi \wedge \forall v(\varphi \to \psi)) \to \psi$ (nach (MP) und Tautologie: $p \to (q \to r) \to ((q \wedge p) \to r)$)

$\vdash (\forall v\varphi \wedge \forall v(\varphi \to \psi)) \to \forall v\psi$ (Q1)

weil $v \notin \mathsf{Fr}(\ \forall v\varphi \wedge \forall v(\varphi \to \psi)\ )$

$\vdash \forall v(\varphi \to \psi) \to (\forall v\varphi \to \forall v\psi)$ (nach (MP) und Tautologie: $(\ (p \wedge q) \to r\ ) \to (\ q \to (p \to r\ ))$)

$\boxtimes$

Satz 16.9. *Es gilt:* $\vdash \forall v\neg\varphi \leftrightarrow \neg\exists v\varphi$.
Analog zeigt man dann die folgenden Äquivalenzen: $\vdash \exists v\neg\varphi \leftrightarrow \neg\forall v\varphi$, $\vdash \forall v\varphi \leftrightarrow \neg\exists v\neg\varphi$ *und* $\vdash \exists v\varphi \leftrightarrow \neg\forall v\neg\varphi$.

Beweis: Wir zeigen die erste Äquivalenz wie folgt:

($\to$) $\vdash \forall v\neg\varphi \to \neg\varphi$ (A11)

$\vdash \varphi \to \neg\forall v\neg\varphi$ (MP, Tautologie $\vdash (p \to q) \to (\neg q \to \neg p)$)

$\vdash \exists v\varphi \to \neg\forall v\neg\varphi$ (Q2)

$\vdash \forall v\neg\varphi \to \neg\exists v\varphi$ (MP und Tautologie)

($\leftarrow$) $\vdash \varphi \to \exists v\varphi$ (A12)

$\vdash \neg\exists v\varphi \to \neg\varphi$ (MP, Tautologie)

$\vdash \neg\exists v\varphi \to \forall v\neg\varphi$ (Q1)

$\boxtimes$

Die verwendeten aussagenlogischen Tautologien haben wir alle bereits im Satz 11.6 gesehen.

Wie auch schon in der Aussagenlogik in Kapitel 13 führt man nun die Begriffe "Herleitbarkeit aus einer Formelmenge" und die entsprechenden Symbole (semantisch) "$W \vDash \varphi$" sowie (syntaktisch) "$W \vdash \varphi$" für eine Formelmenge W ein. Dann kann man mit weiterer Vorarbeit folgenden Satz beweisen:

Satz 16.10 (Vollständigkeitssatz)**.** *Es gilt:* $W \vDash \varphi \iff W \vdash \varphi$

Dieser Satz geht auf den Mathematiker Kurt Gödel zurück. Der Satz besagt, dass eine semantisch gültige Formel bereits in unserem (syntaktischen) Beweiskalkül beweisbar ist und damit insbesondere ein *endlicher* Beweis für diese Formel existiert.

Eine schwächere Formulierung erhalten wir für den Fall, dass die Formelmenge W die leere Menge ist. Dann liest sich der Satz als: Eine Formel ist genau dann allgemeingültig, wenn sie beweisbar ist, d.h.

$$\models \varphi \iff \vdash \varphi$$

Damit haben wir die Vollständigkeit des Kalküls auch in der Prädikatenlogik nachgewiesen. Hier ist er noch viel aussagekräftiger als in der Aussagenlogik. In der Aussagenlogik gibt es für eine gegebene Formel nur endlich viele Primvariablen, die für die Gültigkeit der Formel wichtig sind und die zu belegen sind. Somit gibt es auch nur endlich viele entscheidene Modelle für die gegebene Formel, die es zu betrachten gilt. Dies ist immer (in endlicher Zeit) möglich, wenn auch mit einem unter Umständen erheblichen Aufwand.

In der Prädikatenlogik ist das viel komplizierter. Im Allgemeinen gibt es unendlich viele Modelle, die wir betrachten müssten, um die Gültigkeit einer Formel nachzuweisen. Mit dem Beweiskalkül wissen wir, dass es einen (endlichen) Beweis gibt, der dies bestätigt (oder widerlegt).

Der Gödelsche Vollständigkeitssatz ist der Hauptsatz der mathematischen Logik. Er verbindet auf bestmögliche Weise Semantik und Syntax formaler Sprachen. Der Erfolg der formalen Methode in der Mathematik regt auch andere Bereiche an, ihre Aussagen und Erkenntnismethoden nach Möglichkeit zu formalisieren: Dies geht einher mit der Erfassung der Welt als Daten, die mit Algorithmen verarbeitet werden.

Anwendungen bzw. Auswirkungen bestehen beispielsweise für das Automatische Beweisen, Logische Programmierung und Künstliche Intelligenz.

Gehen wir in unseren Betrachtungen einen Schritt weiter und machen einen kurzen Ausflug in die weite Welt der (weiterführenden) Logik. Bisher haben wir die so genannte *Prädikatenlogik erster Stufe* betrachtet, das heißt unsere Quantoren laufen über Elemente (der Trägermengen), entsprechend der Definition 15.1.

Darüber hinaus könnten wir auch unsere Formelmengen erweitern und Quantoren über Teilmengen (von Elementen der Trägermengen) zulassen. Damit hätten wir die so genannte *Prädikatenlogik zweiter Stufe* eingeführt. Wenn wir versuchten, die Konzepte der Aussagenlogik und der Prädikatenlogik erster Stufe zu kopieren, dann würden wir recht schnell auf Probleme stoßen; insbesondere gilt der Vollständigkeitssatz im Allgemeinen in diesen ausdrucksstärkeren Logiken nicht.

Nachdem wir in Serie 10 eine Formalisierung der so genannten Peano-Axiome gesehen haben, können wir feststellen, dass wir zwar innerhalb von Modellen dieser Axiome die natürlichen Zahlen nachbilden können, aber dennoch charakterisieren diese Axiome die natürlichen Zahlen nicht – man kann zeigen, dass es nicht isomorphe Modelle dieser Axiome gibt. Insbesondere lassen sich die natürlichen Zahlen nicht in der Prädikatenlogik erster Stufe charakterisieren. Es gilt noch mehr:

Satz 16.11. *In jedem System der Zahlen, das zumindest die Theorie der natürlichen Zahlen enthält, gibt es einen unentscheidbaren Satz, also einen Satz, der (formal) nicht beweisbar und dessen Widerlegung ebenso wenig beweisbar ist.*

Das heißt, man erhält kein vollständiges formales System (also einen Beweiskalkül) für die Zahlentheorie (und insbesondere für die Mathematik). Dieses Phänomen wird als der *erste Gödelsche Unvollständigkeitssatz* bezeichnet.

Im Beweis des Unvollständigkeitssatzes wird die Möglichkeit der Kodierung der eigenen Theorie ausgenutzt. Dieses können wir etwa nachbilden, indem wir folgenden meta-logischen Satz betrachten: “Dieser Satz ist falsch.” Diesem Satz können wir keinen Wahrheitswert zuweisen, da er über die Gültigkeit seiner selbst eine Aussage macht. Auch hier erkennen wir das Prinzip des Diagonalarguments.

Eine etwas populär wissenschaftlichere Art und Weise dieses Argument zu betrachten wäre die folgende Situation: Stellen Sie sich vor, in einem Dorf gibt es genau einen Barbier, der nach folgender Regel arbeitet: *“Ich rasiere jeden, der sich nicht selbst rasiert.”* Stellen Sie sich einmal die Frage, ob der Barbier sich selbst rasieren soll oder nicht.

17. Prädikatenlogische Formelmanipulationen

Die erste Form der Manipulation haben wir bereits in Satz 16.9 gesehen, nämlich die Möglichkeit, ein Negationszeichen durch einen Quantor zu schieben – in Kurzschreibweise:

$$\neg\forall\ldots \rightsquigarrow \exists\neg\ldots \qquad \text{bzw.} \qquad \neg\exists\ldots \rightsquigarrow \forall\neg\ldots.$$

Eine andere Form der Formelmanipulation haben wir in den de' Morganschen Gesetzen gesehen, etwa in Satz 11.6:

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q, \quad \neg(p \vee q) \leftrightarrow \neg p \wedge \neg q, \ldots$$

Alleine mit diesen beiden Arten von Manipulationen können wir jeweils zu einer gegebenen (prädikatenlogischen) Formel eine äquivalente Formel finden, in der die Negationszeichen vor den Atomformeln stehen. Zur Erinnerung, die prädikatenlogischen *Atomformeln* hatten die Form "$t_1 = t_2$" bzw. "$r(t_1, \ldots, t_n)$" für Terme $t_1, t_2, \ldots, t_n$ und Relationszeichen r.

Kommen wir zu weiteren Formelmanipulationen, insbesondere von Quantoren. Betrachten wir dazu folgende Beispiele:

(1) $\forall x(x = x) \wedge y = z$
Diese Formel gefällt uns!

(2) $\forall x(x = x) \wedge y = x + x$
In dieser Formel kommt x gebunden und frei vor.

(3) $\forall x(x = x) \wedge \exists x(x = 1)$
In dieser Formel kommt das x sogar in Wirkungsbereichen von zwei verschiedenen Quantoren vor.

Aber fangen wir langsam an, um uns die Unterschiede verständlich zu machen. Offensichtlich sind die beiden Formeln $\forall x(x + x = x)$ und $\forall y(y + y = y)$ semantisch äquivalent, das heißt, es gilt:

$$\forall x(x + x = x) \iff \forall y(y + y = y)$$

Allgemein können wir eine Variable hinter einem Quantor durch eine andere, neue Variable ersetzen und erhalten eine semantisch äquivalente Formel, wenn wir diese Ersetzung auch vollständig im gesamten

Wirkungsbereich dieses Quantors durchführen, das heißt, es gilt:

$$\forall x\varphi(x) \iff \forall y\varphi(y),$$

wenn y nicht in $\varphi(x)$ vorkommt. Diese Art der potentiellen Umbenennung nennt man *gebundene Umbenennung* und man sagt, dass die eine Formel durch gebundene Umbenennung aus der anderen hervorgeht.

Im Beispiel (3) ändern wir semantisch nichts, wenn wir eine gebundene Umbenennung durchführen und erhalten: $\forall x(x = x) \wedge \exists y(y = 1)$. Aber aufpassen, etwa in Beispiel (2) kann man die Variable x nicht durch y ersetzen, ohne semantisch eine Veränderung zu erhalten: $\forall y(y = y) \wedge y = x + x$. Dagegen funktioniert die Ersetzung x durch z, denn wir erhalten damit die Formel: $\forall z(z = z) \wedge y = x + x$.

Diese bereinigende Wirkung in Formeln können wir etwas formeller erfassen.

Definition 17.1. *Eine Formel heißt* bereinigt, *wenn*

- *alle Variablen hinter Quantoren verschieden sind und*
- *keine Variable gleichzeitig sowohl gebunden als auch frei vorkommt.*

Damit kann man Formeln wie in den Beispielen (2) und (3) vermeiden oder sogar noch unangenehmere Kandidaten wie beispielweise:

$$\forall x(\ \varphi(x) \wedge \forall x\psi(x)\ ),$$

denn hier kommt die Variable x nicht nur an zwei Stellen gebunden vor, sondern der Wirkungsbereich des zweiten Quantors ragt in den Wirkungsbereich des ersten Quantors hinein und ersetzt diesen teilweise. Durch die geschickte gebundene Umbennung, etwa wie in $\forall x(\ \varphi(x) \wedge \forall y\psi(y)\ )$, kann man zusätzlich auch potentielle Fehler vermeiden, denn im Allgemeinen sind Formeln wie $\exists x\varphi(x) \wedge \exists x\psi(x)$ und $\exists x(\ \varphi(x) \wedge \psi(x)\ )$ nicht äquivalent.

Zusammenfassend können wir folgenden Begriff von *Normalform* definieren:

Definition 17.2. *Eine Formel ist in* pränexer Normalform*, wenn alle Quantoren am Anfang stehen und der quantorenfreie Teil in* konjunktiver Normalform *ist, das heißt, die Formel hat die Gestalt:*

$$Qx_1Qx_2\ldots Qx_n\varphi,$$

wobei φ die Gestalt $\bigwedge_i \bigvee_j \varphi_{ij}$ hat und φ_{ij} so genannte Literale *sind, d.h. Atomformeln bzw. negierte Atomformeln.*

Schauen wir uns ein Beispiel in pränexer Normalform an:

$$\exists x_1\forall x_2\forall x_3\exists y\ \underbrace{(\underbrace{(\underbrace{\neg Px_1}_{Literal} \vee \underbrace{\neg Qx_1}_{Literal})}_{Disjunktion} \wedge \underbrace{(\underbrace{Px_2}_{Literal} \vee \underbrace{Rx_2}_{Literal})}_{Disjunktion} \wedge \underbrace{\underbrace{Qx_3}_{Literal}}_{Disjunktion} \wedge \underbrace{\underbrace{Ry}_{Literal}}_{Disjunktion})}_{Konjunktion}$$

Schließlich kann man folgende Aussage beweisen:

Satz 17.3. *Zu jeder prädikatenlogischen Formel gibt es eine (semantisch) äquivalente Formel in pränexer Normalform.*

Die Formel im obigen Beispiel in pränexer Normalform ist äquivalent zu der Formel:

$$\neg\forall x(Px \wedge Qx) \wedge \forall x(\neg Px \to Rx) \wedge \forall x(Qx \wedge \exists y Ry).$$

Anstatt den Beweis dieses Satzes zu führen, geben wir konstruktiv die Idee eines praktischen Algorithmus an, wie man diese Normalform einer Formel finden kann:

Algorithmus zum Finden der pränexen Normalform

(a) Formel bereinigen

(b) Negationszeichen nach innen bringen mithilfe der Umformungen:

- $\neg\forall \rightsquigarrow \exists\neg$, $\neg\exists \rightsquigarrow \forall\neg, \ldots$
- aussagenlogische Transformationen

(c) alle Quantoren nach vorne bringen (Reihenfolge beibehalten!)

18. Boolesche Algebren

In diesem Abschnitt behandeln wir eine Klasse von Strukturen, die in vielen Bereichen der Mathematik, aber auch in der Informatik, Anwendung findet. Gleichzeitig stellt sie für uns eine Anwendung der Begriffe aus den verschiedensten Kapiteln dar, so dass wir diese im Folgenden üben können. Wir definieren daher:

Definition 18.1. *Eine Boolesche Algebra ist eine Struktur* $(B; +, \cdot, -; 0, 1)$ *mit zwei 2-stelligen Funktionen* $+, \cdot$*, einer 1-stelligen Funktion* $-$ *und zwei Konstanten* 0 *und* 1*, die die folgenden Axiome erfüllt:*

(a) $\forall x\, \forall y\, \forall z\ (\ x + (y + z) = (x + y) + z\ )$

$\forall x\, \forall y\, \forall z\ (\ x \cdot (y \cdot z) = (x \cdot y) \cdot z\ )$

(b) $\forall x\, \forall y\ (\ x + y = y + x\ )$

$\forall x\, \forall y\ (\ x \cdot y = y \cdot x\ )$

(c) $\forall x\ (\ 0 + x = x\ );\ \forall x\ (\ 1 \cdot x = x\ )$

(d) $\forall x\, \forall y\, \forall z\ (\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)\ )$

$\forall x\, \forall y\, \forall z\ (\ x + (y \cdot z) = (x + y) \cdot (x + z)\ )$

(e) $\forall x\ (\ x + (-x) = 1\ );\ \forall x\ (\ x \cdot (-x) = 0\ )$

(f) $-\,0 = 1;\ -1 = 0;\ 0 \neq 1$

(g) $\forall x\ (\ x \cdot 0 = 0\ );\ \forall x\ (\ x + 1 = 1\ )$

(h) $\forall x\ (\ -(-x) = x\ )$

(i) $\forall x\ (\ x \cdot x = x\ );\ \forall x\ (\ x + x = x\ )$

(j) $\forall x\, \forall y\ (\ -(x \cdot y) = (-x) + (-y)\ )$

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

Beachten Sie, dass wir eine gewisse Signatur zugrunde legen, in der etwa ein 2-stelliges Funktionszeichen "$+$" vorkommt, welches in der Struktur der Booleschen Algebra ebenfalls nur als "$+$" interpretiert wird. Wir nutzen diese Überlagerung der Symbole, um unser Anliegen möglichst kurz schreiben zu können. Werden Sie sich aber dennoch klar, was welches Symbol wann bedeutet.

Kommen wir zu Beispielen, die wir eigentlich bereits kennen: Die einfachste Boolesche Algebra besteht aus nur zwei Elementen: $B = \{0, 1\}$. Die Verknüpfungen $+, \cdot$ und $-$ müssen aufgrund der Axiome folgendermaßen definiert werden:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$-$	
0	1
1	0

Diese Algebra ist isomorph zur Algebra der Wahrheitswerte:

`oder`	W	F
W	W	W
F	W	F

`und`	W	F
W	W	F
F	F	F

`nicht`	
W	F
F	W

Der Isomorphismus ist offenbar durch die folgende Zuordnung

$$0 \mapsto \texttt{F} \qquad + \mapsto \texttt{oder} \qquad - \mapsto \texttt{nicht}$$
$$1 \mapsto \texttt{W} \qquad \cdot \mapsto \texttt{und}$$

gegeben.

Ein komplexeres Beispiel zu Boolschen Algebren sind die Potenzmengen: Sei X eine nicht-leere Menge. Dann ist die Potenzmenge $\mathcal{P}(X)$ mit den Operationen $\cup, \cap$ und der Komplementbildung

$$-Y := X \setminus Y = \{x \in X \mid x \notin Y\}$$

eine Boolesche Algebra $(\mathcal{P}; \cup, \cap, -; \varnothing, X)$, d.h.:

$$+^{\mathcal{P}(X)} = \cup \qquad \cdot^{\mathcal{P}(X)} = \cap \qquad -^{\mathcal{P}(X)} = X \setminus \cdot$$
$$0^{\mathcal{P}(X)} = \varnothing \qquad 1^{\mathcal{P}(X)} = X$$

Zur Erinnerung: Für eine endliche Menge X mit n Elementen gilt nach Satz 2.6, dass die Potenzmenge $\mathcal{P}(X)$ genau 2^n viele Elemente besitzt. Insbesondere sehen Sie, dass Sie mit dem angegebenen zweiten Beispiel beliebig große Boolesche Algebren (in der Größe von Zweierpotenzen) bekommen können.

In Booleschen Algebren können wir abstrakt rechnen, wie wir es bereits allgemein in Ringen durchgeführt haben. Wir können uns dabei strikt an die Axiome halten, ohne eine spezielle Struktur im Auge zu haben:

Satz 18.2. *Sei $(B; +, \cdot, -; 0, 1)$ eine Boolesche Algebra. Dann gelten in der Struktur B folgende (prädikatenlogische) Formeln:*

(i) $\forall x \, \forall y \ (\, x + y = 0 \ \rightarrow \ (x = 0 \wedge y = 0) \,)$

(ii) $\forall x \, \forall y \ (\, x \cdot (-y) = 0 \ \leftrightarrow \ (x \cdot y = x) \,)$

Beweis: Wir beweisen zunächst (i): Betrachten wir dazu $x, y \in B$ mit $x + y = 0$. Dann ist:

$$x \overset{(b),(c)}{=} x + 0 \overset{(Vor)}{=} x + (x + y) \overset{(a)}{=} (x + x) + y \overset{(i)}{=} x + y \overset{(Vor)}{=} 0.$$

Also ist $x = 0$. Analog folgt $y = 0$.

Es bleibt, (ii) zu beweisen. Betrachten wir $x, y \in B$. Wir zeigen zunächst die Richtung ($\rightarrow$): Hierfür gelte $x \cdot (-y) = 0$. Dann gilt:

$$x \cdot y \overset{(b),(c)}{=} x \cdot y + 0 \overset{(Vor)}{=} (x \cdot y) + (x \cdot (-y)) \overset{(d)}{=} x \cdot (y + (-y)) \overset{(e)}{=} x \cdot 1 \overset{(g)}{=} x.$$

Wir zeigen noch ($\leftarrow$). Sei dafür $x \cdot y = x$ gegeben. Dann gilt:

$$x \cdot (-y) \overset{(Vor)}{=} (x \cdot y) \cdot (-y) \overset{(a)}{=} x \cdot (y \cdot (-y)) \overset{(e)}{=} x \cdot 0 \overset{(g)}{=} 0. \qquad \boxtimes$$

Um dem Verständnis für die Axiome von Booleschen Algebren auf die Sprünge zu helfen, kann man für eine solche Struktur $(B; +, \cdot, -; 0, 1)$ folgende 2-stellige Relation "$\leq$" auf B einführen:

$$x \leq y \quad :\Longleftrightarrow \quad x \cdot (-y) = 0 \qquad (\Longleftrightarrow \ x \cdot y = x \text{ nach Satz 18.2}).$$

Dann können wir folgendes feststellen:

Satz 18.3. *Die Struktur $(B, \leq)$ ist eine* partielle Ordnung*, d.h. es gilt:*

(a) *(Transitivität)* $\forall x \, \forall y \, \forall z \ (\, (x \leq y) \wedge (y \leq z) \rightarrow (x \leq z) \,)$

(b) *(Reflexivität)* $\forall x \ (\, x \leq x \,)$

(c) *(Antisymmetrie)* $\forall x \, \forall y \ (\, (x \leq y) \wedge (y \leq x) \rightarrow (x = y) \,)$

Beweis: Wir zeigen die Transitivität: Betrachten wir $x, y, z \in B$ mit $x \leq y$ und $y \leq z$. Dann gelten: $x \cdot (-y) = 0$ und $y \cdot (-z) = 0$. Hieraus folgt:

$$\begin{aligned} x \cdot (-z) &\overset{(b),(c)}{=} (x \cdot 1) \cdot (-z) \\ &\overset{(e)}{=} (x \cdot (y + (-y))) \cdot (-z) \\ &\overset{(d)}{=} ((x \cdot y) + (x \cdot (-y))) \cdot (-z) \end{aligned}$$

$$\begin{aligned}
&\overset{(Vor)}{=} && ((x \cdot y) + 0) \cdot (-z) \\
&\overset{(b),(c)}{=} && (x \cdot y) \cdot (-z) \\
&\overset{(a)}{=} && x \cdot (y \cdot (-z)) \\
&\overset{(Vor)}{=} && x \cdot 0 \\
&\overset{(g)}{=} && 0.
\end{aligned}$$

Also gilt: $x \leq z$.

Die Reflexivität ist trivial: Betrachte dazu ein $x \in B$. Dann gilt offenbar $x \cdot (-x) \overset{(e)}{=} 0$ und somit $x \leq x$.

Es bleibt noch die Antisymmetrie zu zeigen. Betrachte $x, y \in B$ mit $x \leq y$ und $y \leq x$. Dann gelten $x \cdot (-y) = 0$ und $y \cdot (-x) = 0$. Also:

$$\begin{aligned}
x \quad &\overset{(b),(c)}{=} && x \cdot 1 \\
&\overset{(e)}{=} && x \cdot (y + (-y)) \\
&\overset{(d)}{=} && (x \cdot y) + (x \cdot (-y)) \\
&\overset{(Vor)}{=} && (x \cdot y) + 0 \\
&\overset{(Vor),(b)}{=} && x \cdot y + ((-x) \cdot y) \\
&\overset{(b),(d)}{=} && (x + (-x)) \cdot y \\
&\overset{(e)}{=} && 1 \cdot y \\
&\overset{(c)}{=} && y.
\end{aligned}$$

Also gilt wie gewünscht, dass $x = y$. ⊠

Man kann Boolesche Algebren auch nur im Sinne der $\leq$-Beziehung definieren – und nicht wie oben axiomatisch. In diesem Zusammenhang führt man dann so genannte *obere* bzw. *untere Schranken* von zwei gegebenen Elementen x und y ein. Eine obere Schranke ist ein Element z, welches oberhalb beider liegt, also $x \leq z$ und $y \leq z$. Von diesen oberen Schranken kann es in allgemeinen Strukturen prinzipiell keine oder mehrere geben. Wenn es eine kleinste gibt, so nennt man diese das *Supremum*, die kleinste obere Schranke.

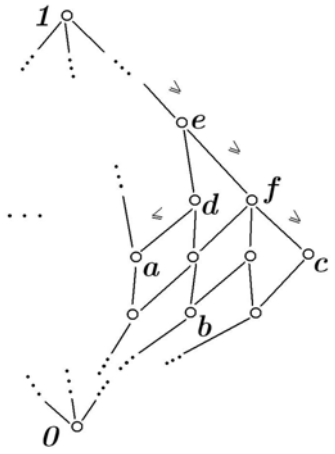
Analog definiert man die größte untere Schranke von zwei Elementen und nennt diese *Infimum*. Strukturen, in denen diese Schranken eine

Rolle spielen, werden *Verbände* genannt, allerdings werden wir diese hier nicht behandeln. In Booleschen Algebren existieren diese kleinsten oberen bzw. die größten unteren Schranken stets. Man sagt auch, dass Boolesche Algebren spezielle Verbände sind.

Den Übergang zwischen diesen beiden Ansätzen, nämlich axiomatisch bzw. verbandstheoretisch, erhält man, indem man die zu definierende Addition als Supremum und die Multiplikation als Infimum interpretiert. Folgender Ausschnitt einer graphischen Darstellung ist hilfreich für das Verständnis der Axiome einer Booleschen Algebra, etwa dem Assoziativgesetz:

$$\begin{aligned}(a+b)+c &= d+c\\ &= e\\ &= a+f\\ &= a+(b+c),\end{aligned}$$

wobei d die kleinste obere Schranke von a und b ist usw.



Abschließend zitieren wir einen wichtigen Satz, der die endlichen Booleschen Algebren exakt klassifiziert: Wir haben bereits im zweiten Beispiel gesehen, dass insbesondere die endlichen Potenzmengenalgebren Boolesche Algebren sind. Der folgende Satz besagt, dass dies bis auf Isomorphie auch genau die endlichen Booleschen Algebren sind.

Satz 18.4. *Sei $(B;+,\cdot,-;0,1)$ eine endliche Boolesche Algebra, d.h. die Trägermenge B ist endlich. Dann ist B isomorph zu einer Potenzmengenalgebra, d.h. es gibt eine Menge A und eine bijektive Abbildung $f : B \to \mathcal{P}(A)$, die mit den Algebraoperationen verträglich ist mit:*

(a) *Es gilt:* $f(0) = \varnothing$; $f(1) = A$.
(b) *Für alle* $x, y \in B$ *gilt:* $f(x+y) = f(x) \cup f(y)$.
(c) *Für alle* $x, y \in B$ *gilt:* $f(x \cdot y) = f(x) \cap f(y)$.
(d) *Für alle* $x \in B$ *gilt:* $f(-x) = A \setminus f(x)$.

Damit schließen wir unsere Betrachtungen ab.

Index