

LOGIK UND ZAHLEN¹

Prof. Dr. Hans Babovsky

Institut für Mathematik

Technische Universität Ilmenau

WS 2004/05

¹Korrekturen, Kommentare und Verbesserungsvorschläge bitte an:

babovsky@mathematik.tu-ilmenau.de

Contents

0	Einleitung	3
1	Grundlagen der Mengenlehre	4
1.1	Mengen	4
1.2	Logische Kürzel	5
1.3	Mengeninklusionen	6
1.4	Vereinigung, Durchschnitt und Komplement	7
1.5	Potenzmengen	9
2	Algebraische Strukturen	10
2.1	Algebraische Rechengesetze	10
2.2	Boolesche Algebren	10
3	Relationen und Funktionen	14
3.1	Kartesische Produkte und Relationen	14
3.1.1	Kartesische Produkte	14
3.1.2	Definition und Eigenschaften von Relationen	14
3.1.3	Spezielle Relationen	15
3.2	Funktionen	19
3.2.1	Grundbegriffe	19
3.2.2	Surjektive, injektive und bijektive Abbildungen	19
3.2.3	Zusammengesetzte und inverse Funktionen	21
3.2.4	Strukturübertragung mit Hilfe bijektiver Abbildungen	23
4	Die natürlichen Zahlen und das Induktionsprinzip	25
4.1	Die Peano-Axiome	25
4.2	Induktion und Rekursion	28
4.3	Einige Anwendungen	29
4.3.1	Probleme aus der Kombinatorik	29
4.3.2	Rekursive Strukturen	31
4.3.3	Datenstrukturen in PASCAL	33
5	Kardinalzahlen	35
6	Grundbegriffe der Logik	38
6.1	Boolesche Ausdrücke	38
6.2	Wahrheitstabellen und logische Äquivalenz	41

6.3	Realisierungen und Folgerungen	45
6.4	Über das mathematische Beweisen	47
6.5	Disjunktive Normalformen	53
7	Fuzzy-Methoden	57
7.1	Mehrwertige und Fuzzy-Logik	57
7.2	Unscharfe Mengen	59

Literaturliste:

- (i) H. Babovsky: Logik und Zahlen, Vorlesungsskript, WS 2003/04, TU Ilmenau (erhältlich im Copyshop)
- (ii) K.U. Witt: Algebraische Grundlagen der Informatik, vieweg, 2001
- (iii) Ch. Meinel, M. Mundhenk: Mathematische Grundlagen der Informatik, Teubner, 2002
- (iv) L. J. Gerstein: Introduction to Mathematical Structures and Proofs, Springer, 1996

0 Einleitung

Mathematik als wissenschaftliche Sprache: Naturwissenschaftler, Ingenieure und Informatiker benutzen die mathematische Sprache zur präzisen Darstellung von Sachverhalten. Diese Sprache gilt es zu erlernen.

Mathematik als "toolbox": Mathematik ist eine Strukturwissenschaft. Sie erstellt Konzepte zur Modellierung, analytischen Beschreibung und Simulation für vielfältige Fragestellungen in der Entwicklung von komplexen Systemen. Gerade in der Informatik spielen Strukturen (Datenkonzepte, Softwareentwicklung etc.) eine äußerst wichtige Rolle.

Mathematische Abstraktion: Die große Stärke der Mathematik liegt in der Abstraktion. Diese löst eine Fragestellung von ihren Ausgangsbezügen und führt das Problem auf eine Ebene, auf welcher die abstrakten Eigenschaften sichtbar werden. Gelegentlich erkennt man bei anscheinend völlig unterschiedlichen Fragestellungen eine identische zugrunde liegende Struktur. Im Einzelnen trägt die Abstraktion zu folgenden Problemstellungen bei. Konkrete Hilfestellungen werden geliefert in folgenden Fällen.

- *Formalisierung von Problemen:* ...
- *Erkennen formaler Strukturen:* Z.B. kann erkannt werden, dass zwei anscheinend völlig unterschiedliche Objekte eine gemeinsame Struktur aufweisen. Ein Beispiel im vorliegenden Skript werden die Mengenlehre auf der einen Seite und die Logik, wie sie zum Entwurf von Schaltkreisen benötigt sind, auf der anderen Seite sein. Da gemeinsame Band werden sog. *Boolesche Algebren* sein.

1 Grundlagen der Mengenlehre

1.1 Mengen

Georg Cantor (1845–1918): "Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche *Elemente* von M genannt werden) zu einem Ganzen."

"Naive" Definition: Eine *Menge* ist eine Zusammenfassung von Objekten; diese Objekte heißen *Elemente*.

Mengen können definiert werden durch

- Aufzählung ihrer Elemente
- Benennung der die Elemente charakterisierenden Eigenschaften.

" $x \in M$ " bedeutet: x ist Element der Menge M ;

" $x \notin M$ " bedeutet: x ist nicht Element der Menge M .

(1.1) Beispiele: a) $M = \{a, b, c\}$ Menge mit den Elementen a , b und c .

b) $M = \{c, c, b, c, a\}$ Menge mit den Elementen a , b und c .

c) $M = \{0, 2, 4, 6, \dots\} = \{n \mid n \text{ natürliche Zahl, } n \text{ gerade}\}$ Menge der geraden natürlichen Zahlen.

d) $M = \{\{0\}, \{2\}, \{0, 2\}\}$ Menge mit den Elementen $\{0\}$, $\{2\}$ und $\{0, 2\}$.

(1.2) Definition: Zwei Mengen A und B sind *gleich* (Schreibweise: $A = B$), wenn sie die gleichen Elemente haben, d.h. wenn gilt

(i) Ist $x \in A$, so ist $x \in B$ (Schreibweise: $x \in A \Rightarrow x \in B$);

(ii) Ist $x \in B$, so ist $x \in A$ (Schreibweise: $x \in B \Rightarrow x \in A$).

Andernfalls heißen A und B *nicht gleich*, $A \neq B$.

Beispielsweise ist $\{a, b, c\} = \{c, c, c, b, a\}$, aber $\{a, b, c\} \neq \{\{a\}, \{b\}, \{c\}\}$.

(1.3) Wichtige Mengen:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ Menge der natürlichen Zahlen
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ Menge der ganzen Zahlen
- $\mathbb{Q} = \{q \mid \text{es gibt } a, b \in \mathbb{Z} \text{ mit } q = a/b\}$ Menge der rationalen Zahlen

- *Reelle Zahlen:*
 - \mathbb{R} Menge der reellen Zahlen
 - $\mathbb{R}_+ = \{x \in \mathbb{R} | x \geq 0\}$ Menge der nichtnegativen reellen Zahlen
 - $\mathbb{R}_- = \{x \in \mathbb{R} | x \leq 0\}$
- *Intervalle:* Zu $a, b \in \mathbb{R}$ definiere
 - $[a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$ (abgeschlossenes Intervall)
 - $(a, b) = \{x \in \mathbb{R} | a < x < b\}$ (offenes Intervall)
 - $[a, b) = \{x \in \mathbb{R} | a \leq x < b\}$
 - $(a, b] = \{x \in \mathbb{R} | a < x \leq b\}$
- *Leere Menge:* Menge ohne Elemente; Schreibweisen: $\emptyset, \{\}$
- *Universalmenge:* die den Problemkreis umfassende Menge.

(1.4) Beispiele: a) $\{x \in \mathbb{Z} | \text{es gibt ein } y \in \mathbb{Z} \text{ mit } x = 2y\}$ Menge der geraden Zahlen;
 b) $\{x \in \mathbb{Z} | \text{es gibt ein } y \in \mathbb{Z} \text{ mit } x = 2y + 1\}$ Menge der ungeraden Zahlen;
 c) $\{n \in \mathbb{Z} | n > 0 \text{ und es gibt Zahlen } 0 \neq x, y, z \in \mathbb{Z} \text{ mit } x^n + y^n = z^n\}$;
 Fermatsche Vermutung: Menge ist gleich $\{1, 2\}$. (Beweis von A. Wiles, 1994)
 d) $\{x \in \mathbb{Z} | x^2 = 2\} = \emptyset$; es ist $\emptyset \neq \{\emptyset\}$.

1.2 Logische Kürzel

P und Q seien Aussagen.

- $P \Rightarrow Q$ bedeutet: "aus Aussage P folgt Aussage Q ";
 z.B. gilt: $(x \text{ ist durch } 12 \text{ teilbar}) \Rightarrow (x \text{ ist durch } 3 \text{ teilbar})$;
- $P \Leftrightarrow Q$ bedeutet: "aus Aussage P folgt Aussage Q und aus Aussage Q folgt Aussage P " (d.h. die Aussagen P und Q sind *äquivalent*);
 z.B. gilt: $(x \text{ ist durch } 6 \text{ teilbar}) \Leftrightarrow (x \text{ ist durch } 3 \text{ und durch } 2 \text{ teilbar})$.
- $\neg P$ ist die Negation der Aussage P .

Quantoren:*Existenzquantoren:* $(\exists x)P$ bedeutet: "es gibt (mindestens) ein x mit der Eigenschaft P "; $(\exists!x)P$ bedeutet: "es gibt genau ein x mit der Eigenschaft P ";*Allquantor:* $(\forall x)P$ bedeutet: "für alle x gilt P ".**(1.5) Beispiele:** Es gelten die folgenden Aussagen.a) $(\exists x)(x \in \mathbb{R} \text{ und } x^2 + \pi x - 2\pi^2 = 0)$; auch: $(\exists x \in \mathbb{R})(x^2 + \pi x - 2\pi^2 = 0)$;b) $(\forall x \geq 0)(\exists y \in \mathbb{R})(y^2 = x)$, sowie $(\forall x \geq 0)(\exists!y \geq 0)(y^2 = x)$;c) in der Menge der natürlichen Zahlen gilt *Bertrands Postulat* $(\forall n > 1)(\exists p)(p \text{ ist Primzahl und } n < p < 2n)$.**1.3 Mengeninklusionen****(1.6) Definition:** Eine Menge A ist *Teilmenge* einer Menge B (Schreibweise: $A \subseteq B$), wenn jedes Element von A auch Element von B ist. Formal:

$$A \subseteq B \quad \Leftrightarrow_{\text{def}} \quad (\forall x)(x \in A \Rightarrow x \in B) \quad .$$

(1.7) Beispiele: a) $\{1, 3\} \subseteq \{1, \pi, 3\}$;b) $\{\emptyset\} \subseteq \{\emptyset, 5\}$;c) $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.d) Nach Definition (1.2) gilt $A = B \Leftrightarrow (A \subseteq B \text{ und } B \subseteq A)$.*Beweis einer Inklusion $A \subseteq B$ mittels einer Hintereinanderreihung von Folgerungen:*direkt: $x \in A \Rightarrow \dots \Rightarrow x \in B$;indirekt: $x \notin B \Rightarrow \dots \Rightarrow x \notin A$.Beweis von $A \not\subseteq B$: Zeige, $(\exists x)(x \in A \text{ und } x \notin B)$.**(1.8) Satz:** A sei Menge; dann ist $A \subseteq A$ und $\emptyset \subseteq A$.**Beweis:** Die Gültigkeit der Aussage $A \subseteq A$ ist offensichtlich. Der Beweis der Aussage $\emptyset \subseteq A$ ist logisch subtiler. Zu zeigen ist: $x \in \emptyset \Rightarrow x \in A$. Offenbar ist die Prämisse

$x \in \emptyset$ nie erfüllt. Solche Aussagen werden im Logikteil untersucht. Wir begnügen uns an dieser Stelle mit der Feststellung, dass es kein Element von \emptyset gibt, welches nicht in A liegt, da \emptyset gar kein Element enthält. \circ

(1.9) Satz: Ist $A \subseteq B$ und $B \subseteq C$, so ist $A \subseteq C$.

Beweis (direkt): Sei $x \in A$ (beliebig). Aus $x \in A$ und $A \subseteq B$ folgt nach Definition (1.6) $x \in B$. Ebenso folgt aus $x \in B$ und $B \subseteq C$, dass $x \in C$. Damit ist $A \subseteq C$. \circ

(1.10) Definition: A heißt *echte Teilmenge* von B (Schreibweise: $A \subset B$), wenn A Teilmenge von B , aber nicht gleich B ist. Formal:

$$(A \subset B) \Leftrightarrow_{\text{def}} (A \subseteq B \text{ und } A \neq B).$$

Offenbar gilt: $(A \subset B) \Leftrightarrow (A \subseteq B \text{ und } (\exists x)(x \in B \text{ und } x \notin A))$.

(1.11) Beispiel: a) $\{1, 7\} \not\subset \{1, 7\} \subset \{1, 2, 7\}$.

b) Ist A eine nicht leere Menge, so ist $\emptyset \subset A$.

c) Ist $A \subset B$ und $B \subset C$, so gilt $A \subset C$.

d) Seien $A = \{1, 2\}$, $B = \{1, 2, 3\}$, $C = \{3, \{1, 2\}\}$ und $D = \{1, 2, \{1, 2\}\}$. Dann gilt $A \subset B$, $A \not\subset C$, $A \in C$, $A \not\subset D$, $A \in D$, $A \subseteq D$.

1.4 Vereinigung, Durchschnitt und Komplement

(1.12) Definition: Gegeben seien die Mengen A und B .

Die Menge $A - B = \{x \in A \mid x \notin B\}$ heißt *Differenz* von A und B , *Komplement* von B in A .

Ist U Universalmenge, so heißt $A' = U - A$ das *Komplement* von A .

(1.13) Beispiele: a) Seien $A = \{1, 2, 3\}$ und $B = \{2, 3, 4\}$; dann ist $A - B = \{1\}$ und $B - A = \{4\}$.

b) $\{\emptyset, \{\emptyset\}\} - \{\emptyset\} = \{\{\emptyset\}\}$.

(1.14) Definition: *Vereinigung* $A \cup B$ von A und B : $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$.
Durchschnitt $A \cap B$ von A und B : $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$.

(1.15) Beispiel: Seien $A = \{1, 2, 3, 4\}$, $B = \{0, 1, 3, 5, 7\}$ und $C = \{2, 4, 6, 8\}$; dann ist $A \cup B = \{0, 1, 2, 3, 4, 5, 7\}$, $A \cap B = \{1, 3\}$, $B \cap C = \emptyset$ und $(A \cup B) \cap C = \{2, 4\} = A \cap C$.

[Einschub: Venn-Diagramme]

(1.16) Satz: a) *Kommutativgesetz:* $A \cap B = B \cap A$, $A \cup B = B \cup A$;
 b) *Assoziativgesetz:* $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$;
 c) *Distributivgesetz:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
 d) $A \cup \emptyset = A$, $A \cup U = U$, $A \cap \emptyset = \emptyset$, $A \cap U = A$.
 e) $A \cup A' = U$, $A \cap A' = \emptyset$.

(1.17) Satz: a) Ist $X \subseteq Z$ und $Y \subseteq Z$, so ist $X \cup Y \subseteq Z$.
 b) Ist $Z \subseteq X$ und $Z \subseteq Y$, so ist $Z \subseteq X \cap Y$.

Indizierte Mengen:

(1.18) Beispiele: a) B_1, B_2, B_3 und B_4 seien Mengen; zur Bezeichnung der Menge $\{B_1, B_2, B_3, B_4\}$ schreiben wir abkürzend $\{B_i | i \in I\}$ bzw. $\{B_i\}_{i \in I}$ mit der *Indexmenge* $I = \{1, 2, 3, 4\}$.

b) Zu reellen Zahlen x_0 und y_0 sei $K_{(x_0, y_0)}$ definiert als der Kreis um (x_0, y_0) mit Radius 1, d.h. $K_{(x_0, y_0)} = \{(x, y) \in \mathbb{R}^2 | (x - x_0)^2 + (y - y_0)^2 \leq 1\}$. Dann ist $\{K_{z_0} | z_0 \in \mathbb{R}^2\} = \{K_{z_0}\}_{z_0 \in \mathbb{R}^2}$ die Menge der Einheitskreise in \mathbb{R}^2 . (\mathbb{R}^2 ist hier die Indexmenge.)

(1.19) Definition: Es sei $\{A_i\}_{i \in I}$ eine indizierte Menge von Mengen.

Die *Vereinigung* $\bigcup_{i \in I} A_i$ ist definiert durch $\bigcup_{i \in I} A_i = \{x | \exists i \in I : x \in A_i\}$;

der *Durchschnitt* $\bigcap_{i \in I} A_i$ ist definiert durch $\bigcap_{i \in I} A_i = \{x | \forall i \in I : x \in A_i\}$.

(1.20) Beispiele: a) $A_1 := \{1, 3, 5, 7, 9\}$, $A_2 := \{1, 4, 9, 16\}$ und $A_3 := \{2, 4, 6, 8, 10\}$; es ist $I = \{1, 2, 3\}$ und $\bigcup_{i \in I} A_i = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 16\}$ sowie $\bigcap_{i \in I} A_i = \emptyset$.

b) Ist $I = \{1, 2\}$, so ist $\bigcup_{i \in I} A_i = A_1 \cup A_2$ und $\bigcap_{i \in I} A_i = A_1 \cap A_2$.

c) $M_n := [-n, n]$ für $n \in \mathbb{N}$. Es ist $\bigcup_{n \in \mathbb{N}} M_n = \mathbb{R}$ und $\bigcap_{n \in \mathbb{N}} M_n = \emptyset$.

(1.21) Satz: Es sei A eine Menge und $\{B_i\}_{i \in I}$ eine indizierte Menge von Mengen.

Dann gilt

a) $A - \bigcap_{i \in I} B_i = \bigcup_{i \in I} (A - B_i)$,

b) $A - \bigcup_{i \in I} B_i = \bigcap_{i \in I} (A - B_i)$,

- c) $(\bigcap_{i \in I} B_i)' = \bigcup_{i \in I} B_i'$,
 d) $(\bigcup_{i \in I} B_i)' = \bigcap_{i \in I} B_i'$.

1.5 Potenzmengen

(1.22) Definition: A sei eine Menge. Die *Potenzmenge* $\mathcal{P}(A)$ ist die Menge der Teilmengen von A : $\mathcal{P}(A) = \{X \mid X \subseteq A\}$.

- (1.23) Beispiele:** a) $\mathcal{P}(\{3\}) = \{\emptyset, \{3\}\}$;
 b) $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$;
 c) $\mathcal{P}(\emptyset) = \{\emptyset\}$;
 d) $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Eine Inspektion der Beispiele lässt den Verdacht aufkommen, dass die Potenzmenge einer n -elementigen Menge 2^n Elemente umfasst. Dies ist in der Tat richtig.

(1.24) Satz: Die Potenzmenge $\mathcal{P}(A)$ einer n -elementigen Menge A hat 2^n Elemente.

Mehrere **Beweise** werden wir später sehen.

(1.25) Satz: A und B seien Mengen. Dann gilt

- a) $\{\emptyset, A\} \subseteq \mathcal{P}(A)$;
 b) $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$;
 c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$;
 d) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Beweis: Exemplarisch führen wir die Beweise von (b) und (c) durch. Die fehlenden Beweise bleiben dem Leser als Übung überlassen. ... \circ

Im folgenden Beispiel soll gezeigt werden, dass eine Verschärfung der Aussage (c), $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$, i.A. nicht richtig ist.

(1.26) Beispiel: Seien $A = \{1, 2\}$ und $B = \{2, 3\}$; dann ist $A \cup B = \{1, 2, 3\}$ und damit $\{1, 2, 3\} \in \mathcal{P}(A \cup B)$.

Wegen $\{1, 2, 3\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$ folgt $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

2 Algebraische Strukturen

Im Verlauf der Vorlesung haben wir es mit recht unterschiedlichen mathematischen Objekten zu tun, beginnend bei Mengen über Funktionen bis zu logischen Aussagen. Möglicherweise überraschend ist, daß es in all diesen Bereichen wichtige Gemeinsamkeiten gibt. Diese spiegeln sich in den folgenden recht allgemeinen Rechengesetzen wider.

2.1 Algebraische Rechengesetze

M sei eine Menge. Eine Vorschrift " \circ ", welche jedem Element $x \in M$ ein Element $x' \in M$ zuordnet, heißt **einstelliger Operator**; eine Vorschrift " \circ ", welche jedem Paar (x, y) von Elementen aus M ein Element $x \circ y \in M$ zuordnet, heißt **zweistelliger** oder **binärer Operator**.

Einige häufig auftretende algebraische Gesetze sind wie folgt definiert.

(2.1) Definition: Im Folgenden seien \circ und $*$ binäre Operatoren.

(a) *Kommutativgesetz* $K(\circ)$: $\forall a, b \in M : a \circ b = b \circ a$.

(b) *Assoziativgesetz* $A(\circ)$: $\forall a, b, c \in M : a \circ (b \circ c) = (a \circ b) \circ c$ ($=: a \circ b \circ c$) .

(c) *Distributivgesetz* $D(\circ, *)$: $\forall a, b, c \in M : a \circ (b * c) = (a \circ b) * (a \circ c)$.

(d) *Absorptionsgesetz* $Ab(\circ, *)$: $\forall a, b \in M : a \circ (a * b) = a$.

(2.2) Beispiele: (a) In \mathbb{N} , \mathbb{Z} , \mathbb{R} gelten $K(+)$, $K(\cdot)$, $A(+)$, $A(\cdot)$, $D(\cdot, +)$, aber nicht $D(+, \cdot)$; die Absorptionsgesetze gelten nicht.

(b) Ist M eine Menge, so gelten in $\mathcal{P}(M)$ laut Satz ... $K(\cap)$, $K(\cup)$, $A(\cap)$, $A(\cup)$, $D(\cap, \cup)$, $D(\cup, \cap)$, $Ab(\cap, \cup)$, $Ab(\cup, \cap)$.

2.2 Boolesche Algebren

M sei eine Menge, auf denen die binären Operatoren \oplus und \otimes definiert sind. Auf M ein einstelliger Operator $'$ definiert. Ferner gebe es zwei ausgezeichnete Elemente von M , welche wir als das *Nullelement* (kurz: 0) und das *Einselement* (kurz: 1) bezeichnen.

(2.3) Definition: Das Sixtupel $\mathcal{M} := (M, 0, 1, \oplus, \otimes, ')$ heißt **Boolesche Algebra**, falls die folgenden Gesetze gelten.

- (i) $K(\oplus), K(\otimes), A(\oplus), A(\otimes);$
- (ii) $D(\oplus, \otimes), D(\otimes, \oplus), Ab(\oplus, \otimes), Ab(\otimes, \oplus);$
- (iii) $\forall a \in M : a \oplus 0 = a, a \oplus 1 = 1, a \otimes 0 = 0, a \otimes 1 = a .$
- (iv) $\forall a \in M : a \oplus a' = 1, a \otimes a' = 0 .$

(2.4) Beispiele: (a) M sei eine nicht-leere Menge. Das Sixtupel $(\mathcal{P}(M), \emptyset, M, \cup, \cap, ')$ ist eine Boolesche Algebra.

Beweis: Die Kommutativ-, Assoziativ- und Distributivgesetze sowie (iii) und (iv) gelten nach Satz (1.16). Zu beweisen sind die Absorptionsgesetze $Ab(\cup, \cap) : A \cup (A \cap B) = A$ sowie $Ab(\cap, \cup) : A \cap (A \cup B) = A$. Dies bleibt dem Leser als Übung überlassen.

(b) Es sei $A = \{a_1, a_2, \dots, a_6\}$ eine beliebige sechselementige Menge; $M := \mathcal{P}_2(A)$ sei die Menge aller Teilmengen von A , welche eine gerade Anzahl von Elementen haben. Das Sixtupel $(M, \emptyset, A, \cup, \cap, ')$ ist keine Boolesche Algebra. Dies liegt unter anderem daran, dass \cap kein zweistelliger Operator *innerhalb* M ist. Z.B. sind $C_1 := \{a_1, a_2\}$ und $C_2 := \{a_2, a_3\}$ Elemente von M , nicht aber das Ergebnis $C_1 \cap C_2$. (Man sagt hierzu auch: *Die Menge M ist nicht abgeschlossen bezüglich der Operation \cap .*)

(c) Auf der zweielementigen Menge $M = \{x, y\}$ seien die zweistelligen Operatoren \circ und $*$ definiert durch die Wertetabellen

$$\begin{array}{c|cc} \circ & x & y \\ \hline x & x & y \\ y & y & y \end{array} , \quad \begin{array}{c|cc} * & x & y \\ \hline x & x & x \\ y & x & y \end{array} . \tag{2.1}$$

Der *einstellige* Operator $'$ sei definiert durch $x' = y$ und $y' = x$. Dann ist $(M, x, y, \circ, *, ')$ eine Boolesche Algebra.

Beweis: Wir vergleichen die obige Konstruktion mit der uns bekannten Booleschen Algebra $(\mathcal{P}(A), \emptyset, A, \cup, \cap, ')$, wobei A eine beliebige einelementige Menge ist. Die Wertetabellen für \cup und \cap sind gegeben durch

$$\begin{array}{c|cc} \cup & \emptyset & A \\ \hline \emptyset & \emptyset & A \\ A & A & A \end{array} , \quad \begin{array}{c|cc} \cap & \emptyset & A \\ \hline \emptyset & \emptyset & \emptyset \\ A & \emptyset & A \end{array} . \tag{2.2}$$

Weiterhin ist $\emptyset' = A$ und $A' = \emptyset$. Wir erkennen, dass die Boolesche Algebra $(\mathcal{P}(A), \emptyset, A, \cup, \cap, ')$ in das Sixtupel $(M, x, y, \circ, *, ')$ übergeführt wird, wenn wir folgende *Umbenennungen* vornehmen: $\mathcal{P}(A) \rightarrow M, \emptyset \rightarrow x, A \rightarrow y, \cup \rightarrow \circ, \cap \rightarrow *$. Da

Rechengesetze durch diese Umbenennungen nicht angetastet werden, müssen alle für $(\mathcal{P}(A), \emptyset, A, \cup, \cap, ')$ gültigen Gesetze auch nach der Umbenennung gültig bleiben.

(d) Auf der Menge $M = \{a, b, c, d\}$ seien zwei binäre Operatoren \oplus und \otimes durch folgende Tabellen gegeben.

$$\begin{array}{c|cccc} \oplus & a & b & c & d \\ \hline a & a & a & c & d \\ b & a & b & c & d \\ c & c & c & c & c \\ d & d & d & c & d \end{array} , \quad \begin{array}{c|cccc} \otimes & a & b & c & d \\ \hline a & a & b & a & a \\ b & b & b & b & b \\ c & a & b & c & d \\ d & a & b & d & d \end{array} . \quad (2.3)$$

Hat M ein Nullelement (d.h. ein Element ν mit $m \oplus \nu = m$ und $m \otimes \nu = \nu$ für alle $m \in M$) ? (Ja, es ist $\nu = b$.)

Hat M ein Einselement (d.h. ein Element η mit $m \oplus \eta = \eta$ und $m \otimes \eta = m$ für alle $m \in M$) ? (Ja, es ist $\eta = c$.)

Gibt es einen einstelligen Operator $'$ mit $m \oplus m' = c$ und $m \otimes m' = b$? (Nein, denn es gibt z.B. kein Element a' .)

Für Boolesche Algebren lassen sich weitere Rechengesetze herleiten.

(2.5) Satz: Ist $\mathcal{M} := (M, 0, 1, \oplus, \otimes, ')$ eine Boolesche Algebra, so gelten

(i) die Idempotenzgesetze $a \oplus a = a$ und $a \otimes a = a$

(ii) die de Morganschen Gesetze $(a \oplus b)' = a' \otimes b'$ und $(a \otimes b)' = a' \oplus b'$.

Beweis: Zu (i):

$$\begin{aligned} a &= a \oplus 0 = a \oplus (a \otimes a') = (a \oplus a) \otimes (a \oplus a') = (a \oplus a) \otimes 1 = a \oplus a \quad , \\ a &= a \otimes 1 = a \otimes (a \oplus a') = (a \otimes a) \oplus (a \otimes a') = (a \otimes a) \oplus 0 = a \otimes a \quad . \end{aligned}$$

Zu (ii): Hierfür benötigen wir folgendes Hilfsresultat bezüglich der Eindeutigkeit des Komplements x' von x :²

$$\text{Sind } x, y \in M \text{ und gilt } x \oplus y = 1 \text{ und } x \otimes y = 0, \text{ so ist } y = x'.$$

Hiermit ist die erste de Morgansche Formel bewiesen, wenn wir zeigen können, dass

²Obwohl der Beweis nicht sehr schwierig ist, wollen wir hier darauf verzichten. Der Leser findet ihn z.B. in Ch. Meinel, M. Mundhenk: Mathematische Grundlagen der Informatik, Satz 10.5 (6), Teubner, 2002.

$$(\alpha) \quad (a \oplus b) \oplus (a' \otimes b') = 1$$

$$(\beta) \quad (a \oplus b) \otimes (a' \otimes b') = 0$$

Zu (α) :

$$(a \oplus b) \oplus (a' \otimes b') = [(a \oplus a') \oplus b] \otimes [a' \oplus (b \oplus b')] = 1 \otimes 1 = 1$$

Zu (β) :

$$(a \oplus b) \otimes (a' \otimes b') = (a \otimes a' \otimes b') \oplus (a' \otimes b \otimes b') = (0 \otimes b') \oplus (a' \otimes 0) = 0 \oplus 0 = 0$$

3 Relationen und Funktionen

3.1 Kartesische Produkte und Relationen

3.1.1 Kartesische Produkte

(3.1) Definition: (a) Ein Paar (a, b) ist die geordnete Zusammenfassung zweier Elemente. Zwei Paare (a, b) und (a', b') heißen *gleich*, wenn $a = a'$ und $b = b'$.

(b) Die Menge

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

heißt *kartesisches Produkt* von A und B .

(c) Die geordnete Zusammenfassung (a_1, \dots, a_n) von n Elementen heißt *n -Tupel*. Die Menge

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) | (\forall i = 1, \dots, n)(a_i \in A_i)\}$$

heißt *kartesisches Produkt* der Mengen A_1, \dots, A_n . Die folgenden Regeln können leicht hergeleitet werden.

(3.2) Satz: A, B und C seien Mengen. Dann gilt

a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;

b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;

c) $(A - B) \times C = (A \times C) - (B \times C)$;

d) Sind A und B nicht leer, so gilt $(A \times B = B \times A) \Leftrightarrow (A = B)$;

e) Ist $A_1 \in \mathcal{P}(A)$ und $B_1 \in \mathcal{P}(B)$, so ist $A_1 \times B_1 \in \mathcal{P}(A \times B)$;

f) $\emptyset \times A = \emptyset$.

3.1.2 Definition und Eigenschaften von Relationen

(3.3) Definition: A und B seien Mengen. Jede Teilmenge $R \subseteq A \times B$ heißt *Relation*.

Für $(x, y) \in R$ schreiben wir abkürzend: xRy .

(3.4) Beispiele: A sei definiert durch $A := \{0, 1, 2, 3\}$; Beispiele für Relationen $R \subseteq A \times A$ sind

a) $R := \{(0, 1), (0, 2), (2, 2)\}$; in diesem Fall ist z.B. $0R1$, aber nicht $1R0$.

b) $R := \{(x, y) \in A \times A | x + y = 3\}$; dann ist

$$R = \{(0, 3), (1, 2), (2, 1), (3, 0)\}.$$

- c) $R := \{(x, y) \in A \times A \mid x + y = 7\}$; man überzeugt sich leicht, daß gilt $R = \emptyset$.
- d) $R := \{(x, y) \in A \times A \mid x < y\}$; nach Definition von R gilt $(x, y) \in R \Leftrightarrow x < y$; es folgt $R = \{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}$.
- e) Ein Beispiel für eine Relation auf $\mathcal{P}(A)$ ist gegeben durch $R \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$,
 $R = \{(B, C) \mid B \subseteq A, C \subseteq A \text{ und } B \subseteq C\}$;
es gilt z.B. $(\emptyset, \{0\}) \in R$, $(\{0, 1\}, \{0, 1, 2\}) \in R$, $(\{3\}, A) \in R$, aber $(\{0\}, \emptyset) \notin R$,
 $(A, \emptyset) \notin R$.
(Übung: Bestimmen Sie R ; wie viele Elemente hat R ?)

(3.5) Definition: A sei Menge, R Relation auf A (d.h. $R \subseteq A \times A$).

- a) R heißt *reflexiv*, falls xRx gilt für alle $x \in A$, und
irreflexiv, falls für alle $x \in A$ gilt $(x, x) \notin R$;
b) R heißt *symmetrisch*, falls für alle $x, y \in A$ gilt:
 $xRy \Rightarrow yRx$;
 R heißt *antisymmetrisch*, falls für alle $x, y \in A$ gilt:
ist xRy und yRx , so ist $x = y$;
c) R heißt *transitiv*, falls aus xRy und yRz folgt, daß xRz .

(3.6) Beispiele: $A := \{1, 2, 3\}$.

- a) $R := \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (3, 2)\}$; R ist reflexiv, nicht symmetrisch (es ist $1R2$, aber nicht $2R1$), nicht antisymmetrisch (es ist $2R3$ und $3R2$, aber nicht $3R2$) und nicht transitiv (da $1R2$ und $2R3$, aber nicht $1R3$).
- b) $R := \{(1, 2), (2, 3), (1, 3)\}$; R ist nicht reflexiv (es ist nicht $(1, 1) \in R$), nicht symmetrisch ($1R2$, aber nicht $2R1$), aber antisymmetrisch und transitiv.
- c) $R := \{(1, 2), (2, 1)\}$; R ist irreflexiv und symmetrisch, aber nicht antisymmetrisch und nicht transitiv (letzteres, da $1R2$ und $2R1$, aber nicht $1R1$).

[Einschub: Relationsdiagramm, -graph, -matrix]

3.1.3 Spezielle Relationen

A) Ordnungsrelationen

(3.7) Definition: A sei eine Menge. $R \subseteq A \times A$ heißt *Ordnungsrelation*, falls R reflexiv, antisymmetrisch und transitiv ist. Eine Ordnung R heißt *Totalordnung*, falls $(\forall x, y \in A)(xRy \text{ oder } yRx)$.

(3.8) Beispiele: A sei eine der Mengen \mathbb{N} , \mathbb{Z} oder \mathbb{R} .

a) Die Relation $R = \{(x, y) \in A \times A \mid x \leq y\}$ ist eine Ordnungsrelation.

b) Die Relation $S = \{(x, y) \in A \times A \mid x < y\}$ ist keine Ordnungsrelation, da sie nicht reflexiv ist.

c) Die Relation $T = \{(x, y) \in A \times A \mid x^2 \leq y^2\}$ ist reflexiv (da $x^2 \leq x^2$) und transitiv (da aus $x^2 \leq y^2$ und $y^2 \leq z^2$ folgt, daß $x^2 \leq z^2$).

(i) Im Fall $A = \mathbb{N}$ ist T auch antisymmetrisch, da $x^2 \leq y^2$ gleichbedeutend ist mit $x \leq y$, und daher aus xTy und yTx folgt, daß $x = y$. Damit ist T eine Ordnungsrelation.

(ii) In den Fällen $A = \mathbb{Z}$ und $A = \mathbb{R}$ ist T nicht antisymmetrisch: für $x \neq 0$ ist $xT(-x)$ und $(-x)Tx$, aber $x \neq (-x)$.

d) Relation U auf $\mathcal{P}(A)$: $BUC \Leftrightarrow_{\text{def}} B \subseteq C$; U ist Ordnung, aber i.a. keine Totalordnung. Da die Aussage $B \subseteq C$ äquivalent ist zur Aussage $B \cap C = B$, lässt sich dieses Beispiel als Spezialfall der folgenden Aussage interpretieren.

e) Auf der Booleschen Algebra $\mathcal{A} = (A, 0, 1, \oplus, \otimes, ')$ sei die Relation V definiert durch $xVy \Leftrightarrow_{\text{def}} x \otimes y = x$. Dann ist V eine Ordnungsrelation.

Beweis: Die Reflexivität folgt aus dem Idempotenzgesetz $x \otimes x = x$. Es gelte xVy und yVx . Dann folgt aufgrund des Kommutativgesetzes $x = x \otimes y = y \otimes x = y$. Schließlich gelte xVy und yVz . Aus dem Assoziativgesetz und dem Idempotenzgesetz folgt dann $x \otimes z = (x \otimes y) \otimes z = x \otimes (y \otimes y) \otimes z = (x \otimes y) \otimes (y \otimes z) = x \otimes y = x$.

B) Äquivalenzrelationen, Partitionen

(3.9) Definition: $M \neq \emptyset$ sei eine Menge. Eine *Partition* Π von M (d.h. eine Zerlegung von M in Blöcke) ist eine (indizierte) Menge $\Pi = \{A_i\}_{i \in I}$ von nicht leeren Teilmengen von M mit den Bedingungen

- (i) $\bigcup_{i \in I} A_i = M$,
- (ii) $A_i \cap A_j = \emptyset$, falls $i \neq j$.

(3.10) Beispiele: a) $M := \{1, 2, 3, 4\}$; zu M gibt es

– eine 1-Block-Partition: $\Pi = \{\{1, 2, 3, 4\}\}$;

– sieben 2-Block-Partitionen: $\Pi_1 = \{\{1\}, \{2, 3, 4\}\}$, $\Pi_2 = \{\{2\}, \{1, 3, 4\}\}$, $\Pi_3 = \{\{3\}, \{1, 2, 4\}\}$, $\Pi_4 = \{\{4\}, \{1, 2, 3\}\}$, $\Pi_5 = \{\{1, 2\}, \{3, 4\}\}$, $\Pi_6 = \{\{1, 3\}, \{2, 4\}\}$ und $\Pi_7 = \{\{1, 4\}, \{2, 3\}\}$;

– sechs 3-Block-Partitionen: $\Pi_1 = \{\{1, 2\}, \{3\}, \{4\}\}$, $\Pi_2 = \{\{1, 3\}, \{2\}, \{4\}\}$, $\Pi_3 = \{\{1, 4\}, \{2\}, \{3\}\}$, $\Pi_4 = \{\{2, 3\}, \{1\}, \{4\}\}$, $\Pi_5 = \{\{2, 4\}, \{1\}, \{3\}\}$ und $\Pi_6 = \{\{3, 4\}, \{1\}, \{2\}\}$;

– eine 4-Block-Partition: $\Pi = \{\{1\}, \{2\}, \{3\}, \{4\}\}$.

b) $M := \mathbb{R}^2$, $A_1 := \{(x, y) \mid x < y\}$, $A_2 := \{(x, y) \mid x = y\}$ und $A_3 := \{(x, y) \mid x > y\}$; mit

diesen Definitionen ist $\Pi = \{A_i\}_{i \in \{1,2,3\}}$ eine Partition von M .

c) $M := \mathbb{Z}$, $A_0 := \{\dots, -4, -2, 0, 2, 4, \dots\}$ Menge der geraden Zahlen und $A_1 := \{\dots, -3, -1, 1, 3, 5, \dots\}$ Menge der ungeraden Zahlen; dann ist $\{A_0, A_1\}$ eine Partition von M .

d) $M := \mathbb{N}$; für $i = 0, \dots, 4$ definiere $A_i := \{n \in \mathbb{N} | n-i \text{ ist durch } 5 \text{ teilbar}\}$. Es ist $A_0 = \{0, 5, 10, 15, \dots\}$, $A_1 = \{1, 6, 11, 16, \dots\}$, $A_2 = \{2, 7, 12, 17, \dots\}$, $A_3 = \{3, 8, 13, 18, \dots\}$ und $A_4 = \{4, 9, 14, 19, \dots\}$. Man überzeugt sich leicht, daß $\Pi = \{A_i\}_{i \in \{0,1,2,3,4\}}$ eine Partition von M ist. (Π heißt auch *Zerlegung von \mathbb{N} in Restklassen bzgl. 5*.)

(3.11) Definition: Eine Relation R auf einer Menge M heißt *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist.

Ist $m \in M$, so heißt $[m]_R := \{x \in M | xRm\}$ die *Äquivalenzklasse* von m .

$M/R := \{[m]_R | m \in M\}$ ist die Menge aller Äquivalenzklassen. M/R ist damit eine spezielle Menge von Teilmengen von M , und sogar – wie weiter unten gezeigt wird – eine Partition.

(3.12) Beispiele: a) $M := \{1, 2, 3, 4, 5\}$;

$R := \{(1, 1), (1, 5), (2, 2), (2, 4), (3, 3), (4, 2), (4, 4), (5, 1), (5, 5)\}$ ist eine Äquivalenzrelation mit den Äquivalenzklassen $[1]_R = \{1, 5\}$, $[2]_R = \{2, 4\}$, $[3]_R = \{3\}$, $[4]_R = \{2, 4\}$ und $[5]_R = \{1, 5\}$.

b) $M := \mathbb{N}$; es sei $p \in \mathbb{N} - \{0\}$; durch $nRm \Leftrightarrow (n-m \text{ ist durch } p \text{ teilbar})$ ist eine Äquivalenzrelation definiert; für $p = 5$ sind die Äquivalenzklassen die Mengen A_i , $i = 0, \dots, 4$ aus Beispiel 2.8 d).

c) Äquivalenzrelation G auf $M := \mathbb{R} \times \mathbb{R}$:

$$(x_1, y_1)G(x_2, y_2) \Leftrightarrow_{\text{def}} 2x_1 - y_1 = 2x_2 - y_2$$

Die zu (\hat{x}, \hat{y}) gehörige Äquivalenzklasse: Definiere $\hat{c} := 2\hat{x} - \hat{y}$. Damit ist

$$[(\hat{x}, \hat{y})]_G = \{(x, y) | 2x - y = \hat{c}\} \quad .$$

Dies ist eine Gerade, gegeben durch $y = 2x - \hat{c}$.

d) Nichtnegative rationale Zahlen: $M := \mathbb{N} \times (\mathbb{N} \setminus \{0\})$; Äquivalenzrelation Q :

$$(x_1, y_1)Q(x_2, y_2) \Leftrightarrow_{\text{def}} x_1y_2 = x_2y_1.$$

Die übliche Schreibweise für die Äquivalenzklassen lautet $[(x, y)]_Q = x/y$.

(3.13) Satz: Ist R eine Äquivalenzrelation auf M , so ist M/R eine Partition von M .

Beweis: (i) Zunächst ist zu zeigen, daß M/R aus *disjunkten* (d.h. *elementfremden*) Teilmengen von M besteht, daß also gilt: $(\forall A, B \in M/R)(A \neq B \Rightarrow A \cap B = \emptyset)$. (Überlegen Sie sich, daß hierzu die folgende Aussage äquivalent ist: $(\forall A, B \in M/R)(A \cap B \neq \emptyset \Rightarrow A = B)$.)

Seien also $A, B \in M/R$. Mit Hilfe zweier Elemente $m, n \in M$ können wir schreiben: $A = [m]_R$ und $B = [n]_R$. Es sei $A \cap B \neq \emptyset$; dann gibt es ein $y \in A \cap B$. Zu zeigen ist, daß $A = B$, daß also $A \subseteq B$ und $B \subseteq A$; da beide Schritte analog verlaufen, zeigen wir nur $A \subseteq B$.

Es sei $x \in A$; dann ist xRm . Wegen $y \in [m]_R$ gilt yRm und aus der Symmetrie folgt mRy , sodaß aus der Transitivität von R folgt xRy . Wegen $y \in B$ ist yRn , also auch xRn und damit $x \in B$.

(ii) Wir wählen aus jeder Menge $A \in M/R$ genau ein Element i aus (das Auswahlaxiom der Mengenlehre sagt aus, daß dies möglich ist) und fassen diese Elemente zu einer Indexmenge I zusammen. Es ist damit M/R gleich der indizierten Menge $\{[i]_R\}_{i \in I}$; aus Beweisschritt (i) folgt, daß für $i, j \in I$ gilt $[i]_R \cap [j]_R = \emptyset$, falls $i \neq j$. Zu zeigen ist nur noch, daß gilt $M \subseteq \bigcup_{i \in I} [i]_R$. Hierzu sei $x \in M$. Da $[x]_R$ eine Äquivalenzklasse ist, gibt es ein $j \in I$ mit $[x]_R = [j]_R$. Wegen der Reflexivität von R ist $x \in [x]_R$ und damit auch $x \in [j]_R \subseteq \bigcup_{i \in I} [i]_R$. \circ

(3.14) Bemerkung: Gilt für eine Äquivalenzrelation R auf M und für zwei Elemente $m, n \in M$ die Beziehung mRn , so zeigt man wie im Beweis des vorhergehenden Satzes, daß $[m]_R = [n]_R$. Jedes Element $x \in [m]_R$ heißt *Repräsentant* von $[m]_R$.

(3.15) Satz: Ist $\Pi = \{A_i\}_{i \in I}$ eine Partition von M und ist R definiert durch xRy , falls x und y im selben Block liegen, so ist R eine Äquivalenzrelation. R heißt die *durch Π induzierte Äquivalenzrelation*.

Beweis: R ist formal definiert durch $xRy \Leftrightarrow (\exists i \in I)(x \in A_i \text{ und } y \in A_i)$. Wegen $\bigcup A_i = M$ gilt xRx für alle $x \in M$, also die Reflexivität von R . Die Symmetrie ist offensichtlich. Gilt xRy und yRz , so gibt es ein $i \in I$ mit $x \in A_i$ und $y \in A_i$ sowie ein $j \in I$ mit $y \in A_j$ und $z \in A_j$. Wegen $A_i \cap A_j = \emptyset$ für $i \neq j$ muß gelten $i = j$ und damit xRz . \circ

(3.16) Beispiele: a) Ist $p \in \mathbb{N} \setminus \{0\}$, so ist durch $xRy \Leftrightarrow (x - y \text{ ist durch } p \text{ teilbar})$ eine Äquivalenzrelation definiert; vgl. Beispiel 2.8 d).

b) $M := \{1, 2, 3, 4\}$, $\Pi := \{\{1\}, \{2, 3, 4\}\}$; die zugehörige Äquivalenzrelation ist

$R = \{(1, 1), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}$.

c) Auf $M = \{1, 2, 3, 4, 5, 6\}$ sei die Relation $R_0 = \{(2, 1), (2, 3), (4, 6)\}$ gegeben. R_0 soll durch Hinzufügen möglichst weniger Paare zu einer Äquivalenzrelation ergänzt werden.

(i) Wir fügen zunächst alle fehlenden Paare (z, z) hinzu:

$$R_1 = R_0 \cup \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}.$$

(ii) Wir stellen R_1 grafisch dar und bestimmen die Partition, welche sich aus den zusammenhängenden Komponenten der Grafik ergibt:

$\Pi = \{\{1, 2, 3\}, \{4, 6\}, \{5\}\}$. Die gesuchte Äquivalenzrelation ist diejenige, welche durch diese Partition bestimmt ist:

$$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), \\ (4, 4), (4, 6), (5, 5), (6, 4), (6, 6)\}.$$

3.2 Funktionen

3.2.1 Grundbegriffe

(3.17) Definition: A und B seien Mengen; eine *Funktion* (Abbildung) f von A nach B (Schreibweise: $f : A \rightarrow B$) ist eine Relation $f \subseteq A \times B$ mit der Eigenschaft: Zu jedem $x \in A$ gibt es genau ein $y \in B$ mit $(x, y) \in f$, oder formal:

$(\forall x \in A)(\exists! y \in B)(x, y) \in f$. In diesem Fall benutzen wir anstelle $(x, y) \in f$ auch die intuitivere Schreibweise $y = f(x)$.

Die Menge $A =: D(f)$ heißt *Definitionsbereich* von f ; die Menge $f(A) := \{y \in B \mid \exists x \in A : (x, y) \in f\}$ heißt *Wertebereich* oder *Bild* von f .

Ist $(x, y) \in f$, so heißt y *das Bild* von x und x heißt *ein Urbild* von y .

(3.18) Beispiele: a) $A := \{a, b, c, d, e\}$, $B := \{1, 2, 3\}$. $f := \{(a, 2), (b, 1), (c, 1), (d, 1), (e, 1)\}$ ist eine Funktion von A nach B . Der Wertebereich ist $f(A) = \{1, 2\} \subset B$.

[Graphische Darstellung von f]

b) Es sei $A = B = \mathbb{R}$ und $f(x) = x^2$.

Der Wertebereich ist $f(\mathbb{R}) = \mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$.

Der *Graph* von f ist definiert als die Menge $\{(x, f(x)) \mid x \in D(f)\} = \{(x, x^2) \mid x \in \mathbb{R}\}$.

[Darstellung von f mit Hilfe des Graphen]

3.2.2 Surjektive, injektive und bijektive Abbildungen

(3.19) Definition: Gegeben sei die Funktion $f : A \rightarrow B$.

a) f heißt *surjektiv*, wenn $f(A) = B$, wenn es also zu jedem $y \in B$ (mindestens) ein

$x \in A$ gibt mit $f(x) = y$;

b) f heißt *injektiv*, wenn zwei verschiedene Elemente aus A auch verschiedene Bilder haben, wenn also gilt $(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2))$

(oder äquivalent dazu: $(f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$).

(3.20) Beispiele: a) Es seien $A = \{a, b, c, d\}$ und $B = \{1, 2, 3, 4\}$. Die Funktion $f = \{(a, 2), (b, 2), (c, 4), (d, 1)\}$ ist weder surjektiv ($3 \notin f(A)$) noch injektiv ($f(a) = f(b)$).

Dagegen ist die Funktion $\tilde{f} = \{(a, 3), (b, 2), (c, 4), (d, 1)\}$ sowohl surjektiv als auch injektiv.

(Übung: Wie kann man aus Relationsdiagramm, -graph und -matrix ablesen, ob eine Funktion surjektiv bzw. bijektiv ist?)

b) A sei eine der Mengen \mathbb{R} oder \mathbb{R}_+ , ebenso B . $f : A \rightarrow B$ und $g : A \rightarrow B$ seien definiert durch $f(x) = x^2$ und $g(x) = x^3$.

(i) Ist $A = B = \mathbb{R}$, so ist f weder surjektiv (da z.B. $-1 \notin f(A)$) noch injektiv (da z.B. $f(1) = f(-1)$).

(ii) Ist $A = \mathbb{R}$ und $B = \mathbb{R}_+$, so ist f nicht injektiv (vgl. (i)), jedoch surjektiv; Urbilder zu $y \in B$ sind \sqrt{y} und $-\sqrt{y}$.

(iii) Ist $A = B = \mathbb{R}_+$, so ist f surjektiv und injektiv.

(iv) Dagegen ist die Funktion g in allen Fällen surjektiv und injektiv.

(v) $\Sigma := \{a, b, \dots, z\}$ sei die Menge aller Kleinbuchstaben. Funktionen $w : \{1, 2, 3, 4\} \rightarrow \Sigma$ bezeichnen wir als *Vier-Buchstaben-Worte*. Definieren wir $a_1 := w(1), \dots, a_4 := w(4)$, so schreiben wir für w kurz $w = a_1 a_2 a_3 a_4$. Ist z.B. $w(1) = f, w(2) = o, w(3) = t$ und $w(4) = o$, so ist $w = foto$. Die Menge aller Vier-Buchstaben-Worte werde mit W_4 bezeichnet. Die Abbildung $f : W_4 \rightarrow \mathcal{P}(\Sigma)$ sei definiert durch $f(a_1 a_2 a_3 a_4) := \{a_1, a_2, a_3, a_4\}$. f ist nicht injektiv, da z.B. $f(otto) = f(toto) = \{o, t\}$. f ist nicht surjektiv, da $f(w)$ für alle $w \in W_4$ höchstens vier Elemente enthält.

(3.21) Bemerkung: f sei eine Funktion von A nach B .

a) Es ist $f(A) \subseteq B$ und $f \subseteq A \times f(A) \subseteq A \times B$. Damit kann f auch interpretiert werden als Funktion von A nach der (möglicherweise kleineren) Menge $f(A)$. Die Funktion $f : A \rightarrow f(A)$ ist immer surjektiv.

b) Die Relation $xRy \Leftrightarrow f(x) = f(y)$ ist eine Äquivalenzrelation auf A . (Beweis: Übung.) Durch $f_R([m]_R) := f(m)$ ist eine injektive Abbildung von A/R nach B definiert. (Beweis: Übung.)

(3.22) Definition: Eine Funktion $f : A \rightarrow B$ heißt *bijektiv*, falls sie injektiv und sur-

ektiv ist.

(3.23) Bemerkung: A und B seien endliche Mengen; $|A|$ und $|B|$ bezeichnen die Anzahl der Elemente von A und B . Anschaulich ist klar:

- (i) Gibt es eine Surjektion von A nach B , so ist $|A| \geq |B|$;
- (ii) Gibt es eine Injektion von A nach B , so ist $|A| \leq |B|$;
- (iii) Gibt es eine Bijektion von A nach B , so ist $|A| = |B|$;

3.2.3 Zusammengesetzte und inverse Funktionen

(3.24) Definition: Zu den Menge A , B und C gegeben seien Funktionen $f : A \rightarrow B$ und $g : B \rightarrow C$. Die Funktion $g \circ f : A \rightarrow C$, welche definiert ist durch $g \circ f(x) = g(f(x))$, heißt die *aus f und g zusammengesetzte Funktion*.

(3.25) Beispiele: a) $f, g : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) := x + 3$, $g(x) := x^2$; es ist $f \circ g(x) = f(g(x)) = f(x^2) = x^2 + 3$ und $g \circ f(x) = g(f(x)) = g(x + 3) = (x + 3)^2 = x^2 + 6x + 9$.
 b) $h : \mathbb{R} \rightarrow \mathbb{R}$ sei definiert durch $h(x) = (x^2 + 1)^3$; h ist zusammengesetzt aus $p(x) = x^3$, $q(x) = x + 1$ und $r(x) = x^2$ in der folgenden Form: $h = (p \circ q) \circ r$, denn es ist $(p \circ q) \circ r(x) = p \circ q(r(x)) = p(q(r(x))) = p(q(x^2)) = p(x^2 + 1) = (x^2 + 1)^3$.

(3.26) Satz: Gegeben seien $f : A \rightarrow B$, $g : B \rightarrow C$ und $h : C \rightarrow D$; dann ist $h \circ (g \circ f) = (h \circ g) \circ f$. (Wir können daher die Klammern weglassen und kurz schreiben $h \circ g \circ f$.)

Beweis: Es ist $(h \circ (g \circ f))(x) = h(g \circ f(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. \circ

(3.27) Satz: Gegeben seien $f : A \rightarrow B$, $g : B \rightarrow C$ und damit $g \circ f : A \rightarrow C$. Dann gilt:

- a) Sind f und g injektiv, so auch $g \circ f$;
- b) Sind f und g surjektiv, so auch $g \circ f$;
- c) Sind f und g bijektiv, so auch $g \circ f$.

Beweis: a) Seien $a_1, a_2 \in A$ und $g \circ f(a_1) = g \circ f(a_2)$, also $g(f(a_1)) = g(f(a_2))$; aus der Injektivität von g folgt $f(a_1) = f(a_2)$; aus der Injektivität von f folgt damit $a_1 = a_2$.

b) Gegeben sei ein $c \in C$; g ist surjektiv $\Rightarrow (\exists b \in B)g(b) = c$; f ist surjektiv $\Rightarrow (\exists a \in A)f(a) = b$; es folgt $g \circ f(a) = g(f(a)) = g(b) = c$.

c) folgt aus a) und b). \circ

(3.28) Bemerkung und Definition: a) Ist $f : A \rightarrow B$ bijektiv, so ist $f^{-1} := \{(b, a) \in B \times A \mid (a, b) \in f\}$ eine Abbildung von B nach A . (Beweis: Übung.) f^{-1} heißt die zu f inverse Abbildung (oder auch die Inverse von f).

b) Die durch $i_A(a) = a \forall a \in A$ definierte Abbildung $i_A : A \rightarrow A$ heißt identische Abbildung auf A .

(3.29) Satz: Gegeben seien $f : A \rightarrow B$ und $g : B \rightarrow A$.

a) Es gilt $i_B \circ f = f = f \circ i_A$.

b) Äquivalent sind die folgenden Aussagen:

(i) f ist bijektiv und es ist $g = f^{-1}$;

(ii) $g \circ f = i_A$ und $f \circ g = i_B$.

Beweis von b): "(i) \Rightarrow (ii)": Es sei f eine Bijektion und $g = f^{-1}$; dann ist $g \circ f = i_A$, denn für $a \in A$ gilt mit $b := f(a)$ die Gleichung $g \circ f(a) = f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a$.

Beweis von $f \circ g = i_B$: Übung.

"(ii) \Rightarrow (i)": Es seien $g \circ f = i_A$ und $f \circ g = i_B$. Dann gilt für $a_1, a_2 \in A$ wegen $g \circ f = i_A$: $f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow g \circ f(a_1) = g \circ f(a_2) \Rightarrow a_1 = a_2$; damit ist f injektiv.

Ist $b \in B$, so ist $g(b) \in A$, und wegen $f \circ g = i_B$ gilt $f(g(b)) = f \circ g(b) = b$; damit ist f auch surjektiv, also bijektiv.

Es gilt $g \circ i_B = g$, $i_A \circ f^{-1} = f^{-1}$ sowie $f \circ f^{-1} = i_B$ (Beweis: Übung). Hieraus folgt $g = g \circ i_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1}$. \circ

(3.30) Folgerung: Ist f bijektiv, so gelten die "Kürzungsregeln"

$f \circ g = f \circ h \Rightarrow f^{-1} \circ f \circ g = f^{-1} \circ f \circ h \Rightarrow g = h$ und

$r \circ f = s \circ f \Rightarrow r \circ f \circ f^{-1} = s \circ f \circ f^{-1} \Rightarrow r = s$.

(3.31) Satz: $f : A \rightarrow B$ und $g : B \rightarrow C$ seien bijektiv. Für $(g \circ f)^{-1} : C \rightarrow A$ gilt dann $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Beweis: Nach Satz ... genügt es zu zeigen, daß gilt $(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$ sowie $(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C$. Die erste Gleichung folgt aus $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ i_B \circ f = f^{-1} \circ f = i_A$.

$(g \circ f) = f^{-1} \circ ((g^{-1} \circ g) \circ f) = f^{-1} \circ (i_B \circ f) = f^{-1} \circ f = i_A$. Die zweite Gleichung folgt entsprechend. \circlearrowleft

(3.32) Beispiel: $h : \mathbb{R}_+ \rightarrow B = \{x \in \mathbb{R} | x \geq 5\}$ sei definiert durch $h(x) = x^2 + 5$. h setzt sich zusammen aus $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+$, $f(x) = x^2$, und $g : \mathbb{R}_+ \rightarrow B$, $g(x) = x + 5$; es ist $h = g \circ f$. Die Inversen von f und g sind $f^{-1}(y) = \sqrt{y}$ und $g^{-1}(y) = y - 5$; damit ist $h^{-1}(y) = f^{-1} \circ g^{-1}(y) = f^{-1}(g^{-1}(y)) = f^{-1}(y - 5) = \sqrt{y - 5}$.

3.2.4 Strukturübertragung mit Hilfe bijektiver Abbildungen

Ist auf einer Menge A ein binärer Operator \oplus definiert, und ist $f : A \rightarrow B$ bijektiv, so lässt sich auf B ein binärer Operator \oplus_f definieren durch $b_1 \oplus_f b_2 := f(f^{-1}(b_1) \oplus f^{-1}(b_2))$. Schreiben wir $a_1 = f^{-1}(b_1)$ und $a_2 = f^{-1}(b_2)$, so lässt sich diese Definition auch kurz schreiben als

$$f(a_1) \oplus_f f(a_2) = f(a_1 \oplus a_2)$$

Wesentliche Eigenschaften übertragen sich hierbei von \oplus auf \oplus_f .

(3.33) Beispiele: (a) Ist \oplus kommutativ, so auch \oplus_f .

Beweis: $b_1 \oplus_f b_2 = f(f^{-1}(b_1) \oplus f^{-1}(b_2)) = f(f^{-1}(b_2) \oplus f^{-1}(b_1)) = b_2 \oplus_f b_1$.

(b) Gilt das Assoziativgesetz $A(\oplus)$, so gilt auch $A(\oplus_f)$.

Beweis: $b_1 \oplus_f (b_2 \oplus_f b_3) = f(f^{-1}(b_1) \oplus f^{-1}(b_2 \oplus_f b_3)) = f[f^{-1}(b_1) \oplus f^{-1}\{(f(f^{-1}(b_2) \oplus f^{-1}(b_3)))\}] = f[f^{-1}(b_1) \oplus f^{-1} \circ f\{f^{-1}(b_2) \oplus f^{-1}(b_3)\}] = f(f^{-1}(b_1) \oplus (f^{-1}(b_2) \oplus f^{-1}(b_3))) = f((f^{-1}(b_1) \oplus f^{-1}(b_2)) \oplus f^{-1}(b_3)) = \dots = (b_1 \oplus_f b_2) \oplus_f b_3 \quad \circlearrowleft$

Ähnlich lassen sich komplexere Strukturen, z.B. Boolesche Algebren übertragen.

(3.34) Satz: Es seien $\mathcal{A} = (A, 0, 1, \oplus, \otimes, ')$ eine Boolesche Algebra und B eine Menge. $f : A \rightarrow B$ sei eine Bijektion. Definieren wir

$$\begin{aligned} 0_f &:= f(0) & , & & 1_f &:= f(1) & , \\ b_1 \oplus_f b_2 &:= f(f^{-1}(b_1) \oplus f^{-1}(b_2)) & , & & b_1 \otimes_f b_2 &:= f(f^{-1}(b_1) \otimes f^{-1}(b_2)) & , \\ \kappa(b) &:= f((f^{-1}(b))') & , & & & & \end{aligned}$$

so ist $\mathcal{B} = (B, 0_f, 1_f, \oplus_f, \otimes_f, \kappa)$ eine Boolesche Algebra.

(In diesem Fall heißt f *Isomorphismus* von \mathcal{A} nach \mathcal{B} . \mathcal{A} und \mathcal{B} heißen *isomorph*.)

(3.35) Satz (Stone'scher Isomorphisatz): Jede endliche Boolesche Algebra ist isomorph

zu einer Potenzmengen-Algebra $(\mathcal{P}(M), \emptyset, M, \cup, \cap, ')$.

(3.36) Beispiel: Die Menge $A := \{a, b, c, d\}$ soll zu einer Booleschen Algebra erweitert werden. Hierzu suchen wir zunächst eine gleichmächtige Potenzmenge, z.B. $\mathcal{P}(M)$ mit $M = \{0, 1\}$. Anschließend definieren wir eine f Bijektion zwischen $\mathcal{P}(M)$ und A , z.B. $f = \{(\emptyset, a), (\{0\}, b), (\{1\}, c), (\{0, 1\}, d)\}$. Auf A wird beispielsweise die folgende Addition induziert: $a_1 \oplus a_2 = f(f^{-1}(a_1) \cup f^{-1}(a_2))$. Dies ergibt die folgende Wertetabelle:

\oplus_f	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

Übung: Ergänzen Sie diese Struktur zu einer Booleschen Algebra.

4 Die natürlichen Zahlen und das Induktionsprinzip

4.1 Die Peano-Axiome

Peano, Giuseppe, 1858–1932, ital. Mathematiker.

Die Menge \mathbb{N} der natürlichen Zahlen wird charakterisiert durch die folgenden fünf "Axiome". Dies sind keine Axiome im eigentlichen Sinn, da sie aus den Axiomen der Mengenlehre hergeleitet werden können (vgl. Anhang C).

(4.1) Das Peanosche Axiomensystem: \mathcal{N} sei eine Menge; \mathcal{N} hat die *Struktur der natürlichen Zahlen*, falls gilt

- a) es gibt ein Element $\aleph \in \mathcal{N}$;
- b) jedes Element $n \in \mathcal{N}$ hat einen (eindeutigen) Nachfolger n^+ ;
- c) \aleph ist nicht Nachfolger eines Elements aus \mathcal{N} ;
- d) kein Element aus \mathcal{N} ist Nachfolger zweier verschiedener Elemente aus \mathcal{N} ;
- e) ist M eine Teilmenge von \mathcal{N} , welche \aleph und für jedes $n \in M$ auch den Nachfolger n^+ enthält, so ist $M = \mathcal{N}$ (*Induktionsprinzip*).

(Formal: $(\aleph \in M \text{ und } (\forall n \in M)(n^+ \in M)) \Rightarrow M = \mathcal{N}$.)

Die für uns wesentlichen Aspekte ergeben sich aus dem letzten der fünf Axiome, das *Induktions-* und das *Rekursionsprinzip*. Das Induktionsprinzip ist insbesondere wichtig, um Aussagen zu beweisen, welche für alle $n \in \mathbb{N}$ richtig sind.

(4.2) Satz (Induktionsprinzip): Gegeben sei eine Aussage $P(n)$ über natürliche Zahlen; es gelte

- (i) $P(0)$ ist wahr;
- (ii) ist $P(n)$ wahr für ein $n \in \mathbb{N}$, so ist auch $P(n^+)$ wahr.

Dann ist die Aussage richtig für alle $n \in \mathbb{N}$.

Beweis: Es sei $M := \{n \in \mathbb{N} \mid \text{Aussage richtig für } n\}$. Diese Menge erfüllt die Voraussetzungen des Axioms e). Damit ist $M = \mathbb{N}$. \circ

(4.3) Beispiel: Die Aussage " $0 + 1 + \dots + n = n(n + 1)/2$ " ist für alle $n \in \mathbb{N}$ richtig.

Beweis: Für $n = 0$ ist die Aussage offensichtlich richtig. Für ein $n \in \mathbb{N}$ gelte " $0 + 1 + \dots + n = n(n + 1)/2$ ". Zu zeigen ist, daß dann für den Nachfolger $n^+ = n + 1$ gilt

" $0 + 1 + \dots + n^+ = n^+(n^+ + 1)/2$ ". Dies kann wie folgt nachgewiesen werden. Es ist $0 + 1 + \dots + n^+ = 0 + 1 + \dots + n + n^+ = n(n + 1)/2 + n^+ = (n + 1) \cdot (n/2 + 2/2) = n^+ \cdot (n + 1)^+/2$; damit ist die Aussage also auch für n^+ richtig. Damit gilt die Aussage nach dem Induktionsprinzip für alle $n \in \mathbb{N}$. \circ

Das Induktionsprinzip kann leicht wie folgt modifiziert werden.

(4.4) Übung: Gegeben seien eine natürliche Zahl n_0 sowie eine Aussage über natürliche Zahlen; es gelte

(i) die Aussage ist richtig für n_0 ,

(ii) ist die Aussage richtig für ein $n \in \mathbb{N}$, so ist sie auch richtig für den Nachfolger n^+ .

Begründen Sie: Dann ist die Aussage richtig für alle natürlichen Zahlen $n \geq n_0$.

(4.5) Satz (Rekursionsprinzip): Gegeben seien eine Menge A und eine Funktion $g : A \rightarrow A$, sowie ein festes $a \in A$; dann gibt es genau eine Funktion $f : \mathbb{N} \rightarrow A$ mit den Eigenschaften

(i) $f(0) = a$,

(ii) $f(n^+) = g(f(n))$.

Beweis: Die Menge $M := \{n \in \mathbb{N} \mid f(n) \text{ ist eindeutig definiert}\}$ erfüllt die Voraussetzungen des Axioms e). Damit ist $M = \mathbb{N}$. \circ

(4.6) Beispiel: Es sei $g : \mathbb{N} \rightarrow \mathbb{N}$, $g(n) := 2n + 1$, sowie $a = 0$; die Funktion $f : \mathbb{N} \rightarrow \mathbb{N}$, welche definiert ist durch das Rekursionsprinzip, ist eindeutig definiert, und es gilt $f(0) = 0$, $f(1) = g(0) = 1$, $f(2) = g(f(1)) = g(1) = 3$, etc.

Addition und Multiplikation

Addition und Multiplikation natürlicher Zahlen sind uns aus unserer Schulzeit längst vertraut; sie wurden daher oben immer als bekannt vorausgesetzt. Dennoch wollen wir der Vollständigkeit halber zeigen, wie diese Operationen als rekursive Funktionen mathematisch streng definiert werden können, und wie danach die bekannten Rechenregeln bewiesen werden können.

(4.7) Rekursive Definition der Addition: Zu $m \in \mathbb{N}$ definiere $f_m : \mathbb{N} \rightarrow \mathbb{N}$ rekursiv durch

(i) $f_m(0) = m$,

$$(ii) f_m(n^+) = (f_m(n))^+.$$

Für f_m führen wir die intuitivere, da bekannte Schreibweise ein: $f_m(n) =: m + n$.

(4.8) Bemerkung: Aus der rekursiven Definition lassen sich die wohlbekanntesten Eigenschaften der Addition beweisen. Dies sind die folgenden Gesetze: Zu $m, n, p \in \mathbb{N}$ gelten

- (i) das Assoziativgesetz: $m + (n + p) = (m + n) + p$;
- (ii) das Kommutativgesetz: $m + n = n + m$;
- (iii) die Neutralität des Nullelements: $m + 0 = 0 + m = m$;
- (iv) Die Kürzungsregel $m + p = n + p \Rightarrow m = n$.

Zur Illustration beweisen wir exemplarisch die Neutralität des Nullelements. Hierzu sei $M := \{m \mid m + 0 = 0 + m = m\}$. Es ist $0 \in M$, da nach Definition $0 + 0 = f_0(0) = 0$. Ist $m \in M$, so auch m^+ , da $m^+ + 0 = f_{m^+}(0) = m^+$ und wegen $f_0(m) = m$ gilt $0 + m^+ = f_0(m^+) = (f_0(m))^+ = m^+$. Daher ist $M = \mathbb{N}$. \circ

(4.9) Rekursive Definition der Multiplikation: Zu $m \in \mathbb{N}$ definiere $g_m : \mathbb{N} \rightarrow \mathbb{N}$ rekursiv durch

- (i) $g_m(0) = 0$,
- (ii) $g_m(n^+) = g_m(n) + m$.

Intuitivere Schreibweise: $g_m(n) =: m \cdot n$.

(4.10) Bemerkung: Auch für die Multiplikation lassen sich die grundlegenden Eigenschaften aus der rekursiven Definition beweisen. Dies sind: Zu $m, n, p \in \mathbb{N}$ gelten

- (i) das Assoziativgesetz: $m \cdot (n \cdot p) = (m \cdot n) \cdot p$;
- (ii) das Kommutativgesetz: $m \cdot n = n \cdot m$;
- (iii) die Neutralität des Einselements: $m \cdot 1 = 1 \cdot m = m$;
- (iv) das Distributivgesetz: $m \cdot (n + p) = m \cdot n + m \cdot p$.

Ordnung auf \mathbb{N}

Die wohlbekannteste Ordnung auf \mathbb{N} läßt sich folgendermaßen definieren.

(4.11) Definition: Die Relation " \leq " auf \mathbb{N} sei definiert durch

$$n \leq m \Leftrightarrow (\exists q \in \mathbb{N}) n + q = m.$$

Hierdurch ist eine Ordnungsrelation definiert. (Der Beweis hierfür ist nicht ganz einfach; ein mengentheoretischer Beweis findet sich in [...].)

4.2 Induktion und Rekursion

Induktionsbeweise werden folgendermaßen definiert.

(4.12) Aufbau eines Induktionsbeweises: Gegeben sei eine Aussage $P(n)$ für natürliche Zahlen $n \in \mathbb{N}$. Es gelte

(i) *Induktionsanfang:* $P(a)$ ist wahr;

(ii) *Induktionsschritt:* Ist $P(n)$ wahr, so auch $P(n+1)$;

dann ist $P(n)$ wahr für alle $n \in \mathbb{N}$, $n \geq a$.

(4.13) Beispiel: Für $n \geq 10$ gilt die Aussage $P(n) := "2^n > n^3"$.

Beweis: Induktionsanfang: Für $n = 10$ ist $2^n = 1024$ und $n^3 = 1000$; damit ist $P(10)$ richtig.

Induktionsschritt: Für $n \geq 10$ gelte $P(n)$, es sei also $2^n > n^3$. Für $n \geq 10$ ist

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1 \leq n^3 + 3n^2 + 3n^2 + n^2 < n^3 + 10n^2 \leq 2n^3.$$

Außerdem ist $2^{n+1} = 2 \cdot 2^n > 2n^3$. Damit ist auch $P(n+1)$ wahr. \circ

Der Begriff rekursiv definierter Funktionen, wie er in Satz (3.4) dargestellt wurde, kann in verschiedene Richtungen verallgemeinert werden. Wir skizzieren kurz zwei Möglichkeiten.

(4.14) Rekursive Funktionen: (a) Als *einfache Rekursion auf einer Menge M* wollen wir eine Funktion $f : \mathbb{N} \rightarrow M$ bezeichnen, welche mit Hilfe eines Anfangswerts $a \in M$ und einer fest vorgegebenen Rekursionsfunktion $g : \mathbb{N} \times M \rightarrow M$ rekursiv definiert werden kann durch $f(0) = a$, $f(n+1) = g(n, f(n))$.

(b) Drei-Term-Rekursionen: Zu gegebenem $g : M \times M \rightarrow M$ und zu $a_0, a_1 \in M$ definiere $f(0) := a_0$, $f(1) := a_1$ und $f(n+1) := g(f(n), f(n-1))$ für $n \geq 1$.

(4.15) Beispiele: (a) (" *n Fakultät*") Die Funktion $n! = 1 \cdot 2 \cdot \dots \cdot n$ ist rekursiv definiert durch den Anfangswert $f(0) = 1$ und die Rekursionsfunktion $g(m, n) = (m+1) \cdot n$.

(b) (Fibonacci-Zahlen): Definiere $f(0) := 0$, $f(1) := 1$ und $g(a, b) := a + b$, also $f(n+1) := f(n) + f(n-1)$ für $n \geq 1$. Dann ist $f(2) = 1$, $f(3) = 2$, $f(4) = 3$, $f(5) = 5$, $f(6) = 8$ etc.

(4.16) Übung: Die Folge $f(n)$ sei definiert als Drei-Term-Rekursion durch die Vorschriften $f(0) = c_0$, $f(1) = c_1$, $(\forall n \geq 1)(f(n+1) = f(n) + 2f(n-1))$.

(a) Bestimmen Sie die Funktion g aus (3.13)(b).

(b) Zeigen Sie durch Induktion: $(\forall n \in \mathbb{N})(f(n) = ((c_0 + c_1) \cdot 2^n + (2c_0 - c_1) \cdot (-1)^n) / 3$.

(4.17) Beispiel: Zwei Eigenschaften der natürlichen Zahlen sind uns wohl vertraut: (a) die *lineare Anordnung*, gegeben durch die Nachfolgerrelation $(n, n + 1)$ und (b) die *Totalordnung*, repräsentiert durch die Relation " \leq ". Mit Hilfe des Rekursionsprinzips kann man zeigen, dass für *endliche* Mengen aus einer Totalordnung eine lineare Anordnung erzeugt werden kann. (Vgl. Vorlesung)

4.3 Einige Anwendungen

Es gibt eine Vielzahl von Anwendungen, welche auf die Ideen der Rekursion und der Induktion zurückgreifen. Wir geben hier einige wenige "typische" Beispiele an.

4.3.1 Probleme aus der Kombinatorik

Viele Beispiele aus der Kombinatorik³ betreffen die Abzählung von Möglichkeiten im Zusammenhang mit endlichen Mengen. Hier bieten sich häufig Induktionsschlüsse an. Ein erster Problemkreis befasst sich mit der Anzahl von Anordnungen endlicher Mengen.

(4.18) Beispiele und Übungen: (a) Zu $n \in \mathbb{N} \setminus \{0\}$ sei die n -elementige Menge $M_n = \{a_1, \dots, a_n\}$ definiert. Es bezeichne α_n die Anzahl der Möglichkeiten, die Elemente von M_n zu sortieren, d.h. in eine bestimmte Reihenfolge zu bringen. Wir behaupten: $(\forall n \geq 1)(\alpha_n = n!)$.

Beweis durch vollständige Induktion: Induktionsanfang: Offenbar ist $\alpha_1 = 1$.

Induktionsvoraussetzung: Es sei $\alpha_n = n!$.

Induktionsschritt: Wir müssen die Anzahl der Möglichkeiten herausfinden, die Elemente von M_{n+1} in eine lineare Anordnung zu bringen. Alle solchen Anordnungen können durch die folgenden zwei Schritte erzeugt werden.

³**Kombinatorik:** Bezeichnung für denjenigen Zweig der Mathematik, in welchem untersucht wird, auf welche und auf wie viele verschiedene Arten gewisse Mengen von Dingen angeordnet und zu Gruppen zusammengefasst werden können ... (Meyers großes Taschenlexikon); Anwendung finden Ergebnisse der Kombinatorik insbesondere auch in der diskreten Wahrscheinlichkeitstheorie.

- S1: bringe die Elemente von M_n in eine beliebige lineare Anordnung;
 hierzu gibt es nach Voraussetzung $\alpha_n = n!$ Möglichkeiten;
 S2: füge das Element a_{n+1} an einer beliebigen Stelle an die zuvor geordneten Elemente von M_n an; hierzu gibt es $n + 1$ Möglichkeiten.

Die Kopplung der beiden Schritte ergibt $\alpha_n \cdot (n + 1) = (n + 1)!$ Möglichkeiten. (Vergewissern Sie sich, dass jede beliebige Kopplung unterschiedlicher Möglichkeiten in S1 oder in S2 auf verschiedene Ergebnisse führt, und dass hiermit alle möglichen Anordnungen erfasst werden.)

(b) Im Gegensatz zu (a) sollen jetzt nur Sortierungen von M_n zugelassen werden, bei denen das erste Element a_1 nicht hinter dem letzten Element a_n vorkommt. Leiten Sie eine Rekursionsformel für die Anzahl β_n der Möglichkeiten her und bestimmen Sie β_n .

(c) $P(n)$ sei die Anzahl der Wörter der Länge $n + 1$, die man aus dem Zeichensatz $\{a_1, \dots, a_n\}$ bilden kann, wobei das Zeichen a_1 genau zweimal und die anderen Zeichen a_i genau einmal vorkommen. Eine rekursive Beschreibung von $P(n)$ kann wie folgt hergeleitet werden.

(i) Offenbar ist $P(1) = 1$, denn das einzig mögliche Wort ist $a_1 a_1$.

(ii) Ist $\alpha_1 \dots \alpha_{n+1}$ ein wie oben definiertes Wort aus den Zeichen a_1, \dots, a_n , so erhält man durch Einfügen des Zeichens a_{n+1} an einer der möglichen $n + 2$ Stellen ein Wort zum Zeichensatz $\{a_1, \dots, a_{n+1}\}$. Man überzeugt sich damit leicht von der Richtigkeit der Formel $P(n + 1) = (n + 2) \cdot P(n)$.

Ein zweiter Problemkreis befasst sich mit der Anzahl von Abbildungen zwischen endlichen Mengen.

(4.19) Übung: Aufgabe bei einem Totospiel ist es, jedem von elf Spielen den Zahlenwert 0, 1 oder 2 zuzuordnen. Eine solcher Tip kann interpretiert werden als Abbildung $f : \{1, \dots, 11\} \rightarrow \{0, 1, 2\}$. Wir wollen hier allgemeiner Tips mit n Spielen ($n \in \mathbb{N} \setminus \{0\}$) betrachten.

(a) Zeigen Sie mit vollständiger Induktion: Es gibt 3^n Möglichkeiten für einen Tip.

(b) Zeigen Sie mit vollständiger Induktion: Zu einem festen Ergebnis $f_0 : \{1, \dots, n\} \rightarrow \{0, 1, 2\}$ gibt es genau $2n$ Tips mit " $n - 1$ Richtigen" (d.h. Tip und Ergebnis stimmen an genau $n - 1$ Stellen überein). Stellen Sie hierzu zunächst eine Rekursionsformel auf. Wie viele Tips mit " $n - 2$ Richtigen" gibt es? Leiten Sie eine Rekursionsformel her.

Als letztes wollen wir kurz Binomialkoeffizienten behandeln. Diese treten auf bei der Berechnung von Termen der Form $(a + b)^n$, aber auch bei vielen weiteren Problemen

der Kombinatorik.

(4.20) Definition: Für $n, k \in \mathbb{N}$, $k \leq n$, ist der Binomialkoeffizient $\binom{n}{k}$ definiert durch

$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}.$$

(4.21) Übung: Zeigen Sie durch vollständige Induktion (über k), dass gilt

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}.$$

4.3.2 Rekursive Strukturen

Beispiele für rekursive Strukturen sind rekursiv definierte Unterprogramme in höheren Programmiersprachen ebenso wie z.B. Polynomsysteme, welche rekursiv berechnet werden.

Rekursiv definierte Unterprogramme sind sich selbst aufrufende Programme. Sie sind häufig klarer und kürzer als nicht-rekursive Lösungen.

(4.22) Beispiel: (a) Berechnung von $n!$ (vgl. Beispiel (3.15)(a)) durch eine PASCAL-Funktion.

```
FUNCTION Fak(n: Integer): Longint;
  BEGIN
    IF n > 0 THEN Fak := n * Fak(n-1) ELSE Fak := 1;
  END;
```

(b) Berechnung der n -ten Fibonacci-Zahl (vgl. Beispiel (3.15)(b)) durch eine PASCAL-Funktion.

```
FUNCTION Fib(Zahl: Integer): Integer;
  BEGIN
    IF Zahl > 2 THEN Fib := Fib(Zahl-1) + Fib(Zahl-2)
    ELSE
      BEGIN IF (Zahl=0) THEN Fib := 0 ELSE Fib := 1 END;
    END;
```

(4.23) Übung: (a) Beweisen Sie durch vollständige Induktion, dass der Aufruf $Fak(n)$

in Beispiel (3.22)(a) wirklich $n!$ berechnet und dass der Aufruf von $Fib(n)$ in (3.22)(b) die n -te Fibonacci-Zahl liefert. Entwickeln Sie zu beiden Funktionen nicht-rekursive Varianten.

(b) Gegeben sei die folgende rekursive PASCAL-Funktion:

```

FUNCTION f(x,y: Real): Real;
  BEGIN
  IF x>=y THEN
    f:=0.5*(x+y)
  ELSE
    f:=f(f(x+2.0,y-1.0),f(x+1.0,y-2.0));
  END;

```

Welches ist der Wert von $f(1,10)$?

Wie lässt sich der Wert $f(a,b)$ auf einfachere Weise darstellen und berechnen? (Beweis!)

Polynomsysteme spielen in vielen Bereichen der Mathematik und ihrer Anwendung eine große Rolle, beispielsweise in der Approximation von Funktionen. häufig können solche Systeme rekursiv definiert werden.

(4.24) Beispiele: (a) Die *Legendre-Polynome* $L_n(t) : [-1, 1] \rightarrow \mathbb{R}$ sind definiert durch die Drei-Terme-Rekursion

$$\begin{aligned}
 L_0(t) &= 1, \\
 L_1(t) &= t, \\
 (n+1)L_{n+1}(t) &= (2n+1)tL_n(t) - nL_{n-1}(t) \quad (n \geq 1).
 \end{aligned}$$

Hieraus lassen sich für $n = 2, 3, \dots$ die Polynome bestimmen. Z.B. ist

$$\begin{aligned}
 L_2(t) &= \frac{3}{2}tL_1(t) - \frac{1}{2}L_0(t) = \frac{1}{2}(3t^2 - 1), \\
 L_3(t) &= \frac{5}{3}tL_2(t) - \frac{2}{3}L_1(t) = \frac{1}{2}(5t^3 - 3t) \\
 &\vdots
 \end{aligned}$$

(b) Die *Tschebyscheff-Polynome* $T_n(t) : [-1, 1] \rightarrow \mathbb{R}$ sind definiert durch die Vorschrift

$$T_n(t) = \cos(n \cdot \arccos(t)).$$

Hieraus lässt sich leicht die folgende Drei-Terme-Rekursion herleiten.

$$\begin{aligned}T_0(t) &= 1, \\T_1(t) &= t, \\T_{n+1}(t) &= 2tT_n(t) - T_{n-1}(t) \quad (n \geq 1).\end{aligned}$$

Beweis: Es ist

$$\begin{aligned}T_0(t) &= \cos(0 \cdot \arccos(t)) = \cos(0) = 1, \\T_1(t) &= \cos(1 \cdot \arccos(t)) = t.\end{aligned}$$

Für die Rekursionsformel erinnern wir uns an das Additionstheorem

$$\cos(a \pm b) = \cos(a) \cos(b) \mp \sin(a) \sin(b).$$

Mit $a = n \cdot \arccos(t)$ und $b = \arccos(t)$ folgt

$$\begin{aligned}\cos((n+1) \arccos(t)) &= t \cdot \cos(n \cdot \arccos(t)) - \sin(n \cdot \arccos(t)) \cdot \sin(\arccos(t)), \\ \cos((n-1) \arccos(t)) &= t \cdot \cos(n \cdot \arccos(t)) + \sin(n \cdot \arccos(t)) \cdot \sin(\arccos(t)).\end{aligned}$$

Die Rekursionsformel folgt leicht aus der Addition dieser beiden Gleichungen. \circ

(4.25) Übung: $L_n(t)$ und $T_n(t)$ seien die Polynome aus Beispiel (3.24).

(a) Zeigen Sie durch vollständige Induktion: Für alle $n \in \mathbb{N}$ sind L_n und T_n Polynome n -ten Grades.

(b) Überlegen Sie sich Rekursionsformeln für die führenden Koeffizienten von L_n und T_n (d.h. für die Vorfaktoren vor der höchsten Potenz t^n) und beweisen Sie diese.

(c) Bestimmen Sie $T_n(t)$ für $n = 2, 3, 4$.

4.3.3 Datenstrukturen in PASCAL

Axiomensysteme ähnlich denen der Peano-Axiome lassen sich z.B. in der Programmiersprache PASCAL in Datenstrukturen umsetzen. Beispielsweise entspricht der Aufbau der natürlichen Zahlen dem einer linearen Liste.⁴

(i) Die durch die Peano-Axiome vorgegebene lineare Struktur lässt sich durch die folgenden Typenvereinbarungen erzeugen.

⁴Für die folgenden Ausführungen vergleiche man z.B. das Vorlesungsmanuskript H. Babovsky, Algorithmen und Programmierung I, WS 1999/2000, TU Ilmenau.

```

TYPE          Zeiger = ^Listenelement;
               Listenelement = RECORD
                                   < Vereinbarungen >
                                   Nachfolger: Zeiger;
                               END;

```

Definiert seien die drei Variablen *Anker*, x und y vom Typ *Zeiger*. Das Ursprungselement der Liste (entspricht der Null in \mathbb{N}) wird erzeugt durch

```
New(Anker);
```

Um zu einem gegebenen Element mit Adresse x einen Nachfolger zu erzeugen und auf dessen Adresse zu wechseln, sind folgende Schritte nötig.

```

New(y);
x^.Nachfolger:=y;
x:=y;

```

Stehen diese Anweisungen in einer Schleife, so wird eine (endliche) lineare Liste erzeugt.

(ii) Eine (endliche) *zyklische Struktur* \mathcal{Z} erhält man durch die folgende Abänderung des Peano-Systems.

- a) *Anker* ist ein Element von \mathcal{Z} ;
- b) jedes Element $x \in \mathcal{Z}$ hat einen (eindeutigen) Nachfolger x^+ ;
- c) *Anker* ist Nachfolger eines Elements von \mathcal{Z} ;
- d) Kein Element von \mathcal{Z} ist Nachfolger zweier verschiedener Elemente von \mathcal{Z} ;
- e) Ist M eine Teilmenge von \mathcal{Z} , welche *Anker* enthält und für jedes $x \in \mathcal{Z}$ auch den Nachfolger enthält, so ist $M = \mathcal{Z}$.

(iii) Schließlich soll nun ein *binärer Baum* erzeugt werden. Dieser ist dadurch charakterisiert, dass jedes Element (höchstens) zwei Nachfolger hat. Axiomatisch erhält man eine solche Struktur, indem das Peano-Axiom (3.1)(b) umgewandelt wird in

(b') Jedes Element n hat zwei eindeutig bestimmte Nachfolger n^{1+} und n^{2+} .

Die zugehörige PASCAL-Datenstruktur unterscheidet sich von der obigen dadurch, dass in die RECORD-Definition zwei Zeiger aufgenommen werden:

```

TYPE          Zeiger = ^Listenelement;
Listenelement = RECORD
                < Vereinbarungen >
                Nachfolger1: Zeiger;
                Nachfolger2: Zeiger;
            END;

```

- (4.26) Übung:** (a) Wie müssen die PASCAL-Befehle aus (i) geändert bzw. erweitert werden, um eine zyklische Struktur zu erzeugen?
- (b) Skizzieren Sie eine Befehlsfolge, mittels derer ein binärer Baum erzeugt werden kann.

5 Kardinalzahlen

Kardinalzahlen beschreiben die *Mächtigkeit* von Mengen, d.h. die "Anzahl" der Elemente von Mengen. Dies ist völlig unproblematisch im Falle endlicher Mengen – die entsprechenden Kardinalzahlen sind die natürlichen Zahlen. Sehr viel schwieriger wird dies im Fall unendlicher Mengen. Wir werden sehen, dass es sehr viele Varianten des Begriffs "unendlich" gibt.

(5.1) Definition: Zwei Mengen A, B haben *gleiche Kardinalität* (*gleiche Kardinalzahl*), wenn es eine Bijektion $f : A \rightarrow B$ gibt. In diesem Fall heißen A und B *äquipotent*. (Schreibweise: $A \approx B$; Negation: $A \not\approx B$.)

(5.2) Satz: " \approx " ist eine Äquivalenzrelation.

Beweis: $A \approx A$, denn $i_A A \rightarrow A$ ist eine Bijektion.

Gilt $A \approx B$, so gibt es eine Bijektion $f : A \rightarrow B$. Dann ist $f^{-1} : B \rightarrow A$ eine Bijektion; damit gilt $B \approx A$.

Ist $A \approx B$ und $B \approx C$, so gibt es Bijektionen $f : A \rightarrow B$ und $g : B \rightarrow C$. Die Abbildung $g \circ f : A \rightarrow C$ ist eine Bijektion; damit ist $A \approx C$. \circ

(5.3) Beispiele: (a) $\mathbb{N}_2 := \{2n | n \in \mathbb{N}\}$ ist die Menge der geraden Zahlen. Die Abbildung $f : \mathbb{N} \rightarrow \mathbb{N}_2$, $f(n) := 2n$ ist Bijektion. Damit ist $\mathbb{N} \approx \mathbb{N}_2$.

(b) Für $a, b \in \mathbb{R}$, $a < b$, ist das Intervall $[a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$ equipotent zum

Intervall $[0, 1]$, denn die Abbildung $f(x) := (x - a)/(b - a)$ ist eine Bijektion.

(5.4) Definition: Es sei $\mathbb{N}_n := \{0, \dots, n - 1\}$. A sei eine Menge.

a) A heißt *endlich*, falls $(\exists n \in \mathbb{N}) S \approx \mathbb{N}_n$. In diesem Fall schreiben wir formal $\#A = n$.

b) A heißt *unendlich*, falls sie nicht endlich ist. (Formal: $(\forall n \in \mathbb{N}) \#A \neq n$.)

c) A heißt *abzählbar unendlich*, falls gilt $A \approx \mathbb{N}$. (Formal: $\#A = \#\mathbb{N}$.)

d) A heißt *überabzählbar unendlich*, falls A unendlich ist, und falls gilt $A \not\approx \mathbb{N}$.

Die hier nur formal definierten Größen $\#A$ heißen *Kardinalzahlen*.

(5.5) Beispiele: (a) Für *endliche* Mengen A stimmt die Kardinalzahl $\#A$ überein mit der in Bemerkung (2.21) definierten Zahl $|A|$.

(b) \mathbb{N}_2 ist abzählbar unendlich (vgl. Beispiel 4.3(a)).

(c) Die Menge \mathbb{Z} der ganzen Zahlen ist abzählbar unendlich; eine Bijektion $f : \mathbb{N} \rightarrow \mathbb{Z}$ ist gegeben durch $f(2n) = n$, $f(2n + 1) = -n$.

(d) Die Menge \mathbb{Q} der rationalen Zahlen ist abzählbar unendlich.

(Die Menge \mathbb{Q}_+ der positiven rationalen Zahlen kann durch ein Diagonalabzählverfahren abgezählt werden.)

(e) Die Menge \mathbb{R} der reellen Zahlen ist überabzählbar unendlich. (Die Kardinalzahl $\#\mathbb{R}$ wird auch als *Mächtigkeit des Kontinuums* bezeichnet.)

Zum Beweis zeigen wir, daß bereits das Intervall $I = (0, 1) = \{x \in \mathbb{R} | 0 < x < 1\}$ überabzählbar unendlich ist. Hierzu sei $f : \mathbb{N} \rightarrow (0, 1)$ eine beliebige Abbildung. Die Elemente $f(n)$ können in der Dezimaldarstellung wie folgt geschrieben werden: $f(0) = 0.a_{00}a_{01}a_{02}a_{03} \dots$, $f(1) = 0.a_{10}a_{11}a_{12}a_{13} \dots$, $f(2) = 0.a_{20}a_{21}a_{22}a_{23} \dots$ etc. Wir definieren das Element $m = 0.m_0m_1m_2 \dots \in (0, 1)$ so, daß $m_i \neq a_{ii}$. Man sieht leicht, daß m nicht im Bild von f liegt. Wäre nämlich $m = f(n)$, so müßten insbesondere die beiden n -ten Nachkommastellen übereinstimmen. Nach Konstruktion ist aber $a_{nn} \neq m_n$. f ist also nicht surjektiv.

Somit gibt keine Surjektionen und damit auch keine Bijektionen von \mathbb{N} nach $(0, 1)$. \circ

(5.6) Bemerkung: Auf der Menge der Kardinalzahlen $\{\#A | A \text{ Menge}\}$ ist eine Ordnungsrelation definiert durch

$\#A \leq \#B \Leftrightarrow \exists$ injektive Abbildung $f : A \rightarrow B$. Die Relation $\#A < \#B$ sei definiert durch $\#A \leq \#B$ und $\#A \neq \#B$ (d.h. es gibt eine Injektion von A nach B , aber keine Bijektion). Überabzählbare Mengen A sind dann charakterisiert durch $\#\mathbb{N} < \#A$.

Einen Hinweis darauf, daß es bezüglich der Ordnungsrelation \leq aus Bemerkung ... keine größte Menge geben kann, folgt aus dem folgenden Ergebnis.

(5.7) Satz von Cantor: Für die Potenzmenge $\mathcal{P}(S)$ einer Menge S gilt stets $\#S < \#\mathcal{P}(S)$.

Beweis: Für $S = \emptyset$ ist die Aussage richtig, denn es ist $\#S = 0$ und $\#\mathcal{P}(S) = \#\{\emptyset\} = 1$.
Ist $S \neq \emptyset$, so ist die Abbildung $g : S \rightarrow \mathcal{P}(S)$, mit $g(x) = \{x\}$ injektiv; damit gilt $\#S \leq \#\mathcal{P}(S)$. Um zu zeigen, daß es keine bijektive Abbildung $f : S \rightarrow \mathcal{P}(S)$ gibt, nehmen wir an, daß f eine solche Bijektion sei. Für beliebige $x \in S$ ist dann $f(x) \subseteq S$; wir definieren $E := \{x \in S \mid x \notin f(x)\}$ und zeigen, daß E nicht im Bild von f ist. Wäre $E = f(z)$ für ein geeignetes $z \in S$, so müßte $z \in E$ genau dann gelten, wenn $z \notin E$ – ein Widerspruch. \circ

6 Grundbegriffe der Logik

6.1 Boolesche Ausdrücke

Wir betrachten im Folgenden Abbildungen mit Wertebereich $U = \{0, 1\}$. Je nach Anwendung können die Elemente von U Schaltzustände oder Wahrheitswerte ausdrücken. Wir interpretieren

$$\begin{aligned} 0 &\hat{=} \text{ "aus", "falsch" } \\ 1 &\hat{=} \text{ "an", "wahr" } \end{aligned}$$

Die Werte 0 und 1 heißen auch *Boolesche Konstanten*.

Wir definieren zunächst zweistellige Operatoren \vee ("oder") und \wedge ("und") und den einstelligen Operator \neg auf U durch die Wertetabellen

$$\begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}, \quad \begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}, \quad \begin{array}{c|c} & \neg \\ \hline 0 & 1 \\ 1 & 0 \end{array}. \quad (6.4)$$

(6.1) Hilfssatz: Das Sixtupel $\mathcal{A} = (U, 0, 1, \vee, \wedge, \neg)$ ist eine Boolesche Algebra.

Proof: Wir vergleichen \mathcal{A} mit der Booleschen Algebra $\mathcal{A}' = (\mathcal{P}(M), \emptyset, M, \cup, \cap, ')$, wobei $M = \{\alpha\}$ eine beliebige einelementige Menge ist. Die Wertetabellen für \cup , \cap und $'$ sind

$$\begin{array}{c|cc} \cup & \emptyset & M \\ \hline \emptyset & \emptyset & M \\ M & M & M \end{array}, \quad \begin{array}{c|cc} \cap & \emptyset & M \\ \hline \emptyset & \emptyset & \emptyset \\ M & \emptyset & M \end{array}, \quad \begin{array}{c|c} & ' \\ \hline \emptyset & M \\ M & \emptyset \end{array}. \quad (6.5)$$

Wir erkennen, dass \mathcal{A} aus \mathcal{A}' entsteht durch die Umbenennungen $\emptyset \rightarrow 0$, $M \rightarrow 1$, $\cup \rightarrow \vee$, $\cap \rightarrow \wedge$ und $' \rightarrow \neg$. \circ

Definieren wir das Maximum und das Minimum zweier reeller Zahlen durch

$$\max(x, y) := \begin{cases} x & \text{falls } x > y \\ y & \text{andernfalls} \end{cases}, \quad \min(x, y) := \begin{cases} x & \text{falls } x < y \\ y & \text{andernfalls} \end{cases} \quad (6.6)$$

so erkennen wir leicht, dass \vee und \wedge auch interpretiert werden können durch

$$x \vee y = \max(x, y), \quad x \wedge y = \min(x, y) \quad \text{für } x, y \in U. \quad (6.7)$$

Außerdem ist

$$\neg x = 1 - x \quad \text{für } x \in U \quad . \quad (6.8)$$

Komplexere Strukturen werden wie folgt erzeugt. Wir stellen uns zunächst eine "Black Box" vor mit n Eingängen und einem Ausgang, wie in Bild 1 dargestellt.

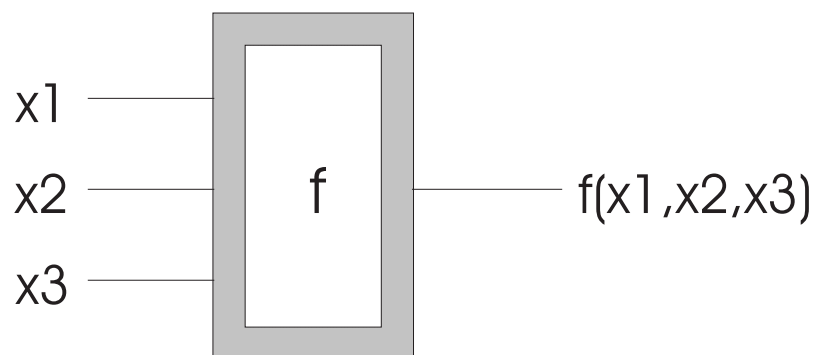


Bild 1: Schalter mit 3 Eingängen und einem Ausgang

Jedem der Eingänge x_1, \dots, x_n wird ein Zustand "an" oder "aus" zugeordnet. Abhängig davon liefert der Ausgang ebenfalls einen Zustand $f(x_1, \dots, x_n)$ "an" oder "aus". Wir können also das System auffassen als eine Abbildung

$$f : U^n \longrightarrow U \quad . \quad (6.9)$$

Mathematisch können diese Schaltungen mit Hilfe *Boolescher Ausdrücke* beschrieben werden. Dies sind Abbildungen der Form (5.6), welche nach und nach aus einfachen Ausdrücken aufgebaut werden können.

(6.2) Definition: (a) Eine Variable x , welche nur die Werte 0 und 1 annehmen kann, heißt *Boolesche Variable*.

(b) Die Menge aller n -stelligen *Booleschen Ausdrücke* ist induktiv definiert durch

- (i) Die Konstanten 0 und 1 sowie die Booleschen Variablen x_1, \dots, x_n sind n -stellige Boolesche Ausdrücke.
- (ii) Sind p und q n -stellige Boolesche Ausdrücke, so auch $(\neg p)$, $(p \vee q)$ und $(p \wedge q)$.

Die Ausdrücke in (5.2)(b)(ii) sind hierbei zu interpretieren als

$$\begin{aligned}\neg p(x_1, \dots, x_n) &= 1 - p(x_1, \dots, x_n), \\ (p \vee q)(x_1, \dots, x_n) &= \max(p(x_1, \dots, x_n), q(x_1, \dots, x_n)), \\ (p \wedge q)(x_1, \dots, x_n) &= \min(p(x_1, \dots, x_n), q(x_1, \dots, x_n)).\end{aligned}$$

(6.3) Beispiele: (a) 0-stellige Boolesche Ausdrücke sind z.B.

$$0, 1, (\neg 0), (1 \wedge (\neg 0)), (1 \vee 1), (\neg(1 \wedge (\neg 0))), (\neg(1 \wedge (\neg 0))) \vee (1 \vee 1), \dots \quad (6.10)$$

Nullstellige Ausdrücke können mit Hilfe obiger Wertetabellen ausgewertet werden Z.B. ist

$$(\neg(1 \wedge (\neg 0))) \vee (1 \vee 1) = (\neg(1 \wedge 1)) \vee 1 = (\neg 1) \vee 1 = 0 \vee 1 = 1 \quad .$$

(b) 1-stellige Boolesche Ausdrücke sind z.B.

$$0, 1, (\neg 0), \dots, x_1, (\neg x_1), (x_1 \vee 1), (x_1 \vee (\neg(x_1))), ((x_1 \vee 1) \wedge (\neg x_1)), \dots \quad (6.11)$$

(c) k -stellige Boolesche Ausdrücke sind z.B.

$$0, 1, \dots, x_1, \dots, x_k, \dots, (\neg((\neg x_1) \wedge ((\neg(x_1 \vee x_4)))))) \wedge (x_1 \wedge x_k), \dots \quad (6.12)$$

Wir bezeichnen die Menge aller n -stelligen Booleschen Ausdrücke mit A_n .

Sind p, q, r, \dots n -stellige Boolesche Ausdrücke, und wählen wir $x_1, \dots, x_n \in U$ fest, so sind $p(x_1, \dots, x_n), q(x_1, \dots, x_n), r(x_1, \dots, x_n), \dots$ Boolesche Konstanten. Nach Hilfssatz (5.1) gelten damit alle Rechengesetze, welche für die Boolesche Algebra \mathcal{A} gegeben sind, z.B. das Distributivgesetz $p(x_1, \dots, x_n) \wedge [q(x_1, \dots, x_n) \vee r(x_1, \dots, x_n)] = [p(x_1, \dots, x_n) \wedge q(x_1, \dots, x_n)] \vee [p(x_1, \dots, x_n) \wedge r(x_1, \dots, x_n)]$. Da dieses Gesetz für beliebige x_1, \dots, x_n gilt, folgt das Distributivgesetz

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r) \quad . \quad (6.13)$$

In ähnlicher Form lassen sich alle für Boolesche Algebren gültigen Rechengesetze nachweisen. Damit A_n eine Boolesche Algebra wird, müssen wir noch ein geeignetes Nullelement ν und ein Einselement η finden. wir definieren

$$\nu(x_1, \dots, x_n) := 0 \quad \text{für alle } x_1, \dots, x_n \in U \quad , \quad (6.14)$$

$$\eta(x_1, \dots, x_n) := 1 \quad \text{für alle } x_1, \dots, x_n \in U \quad . \quad (6.15)$$

Man weist nun leicht nach, dass gilt

(6.4) Satz: $\mathcal{A}_n = (A_n, \nu, \eta, \vee, \wedge, \neg)$ ist eine Boolesche Algebra.

Damit stehen uns auf A_n eine Reihe von Rechengesetzen zur Verfügung, z.B.

(6.5) Rechengesetze: Es gelten alle Rechengesetze der Definition A.3 und des Satzes A.5; insbesondere:

p, q, r seien n -stellige Boolesche Ausdrücke. Es gelten die

- (i) Kommutativgesetze $K(\vee)$ und $K(\wedge)$, also $p \vee q = q \vee p$ und $p \wedge q = q \wedge p$;
- (ii) Assoziativgesetze $A(\vee)$ und $A(\wedge)$;
- (iii) Distributivgesetze $D(\wedge, \vee)$ und $D(\vee, \wedge)$: $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$;
- (iv) Idempotenzgesetze: $p \wedge p = p$, $p \vee p = p$;
- (v) Absorptionsgesetze $Ab(\wedge, \vee)$, $Ab(\vee, \wedge)$: $P \wedge (P \vee Q) \equiv P$, $P \vee (P \wedge Q) \equiv P$;
- (vi) De Morgans Gesetze: $\neg(p \wedge q) \equiv \neg p \vee \neg q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

6.2 Wahrheitstabellen und logische Äquivalenz

Mit Hilfe der Operatoren \vee , \wedge und \neg können weitere Operatoren definiert werden.

(6.6) Definition: x_1 und x_2 seien Boolesche Variablen. Die Operatoren $x_1 \Rightarrow x_2$ ("wenn x_1 , dann x_2 "), $x_1 \Leftrightarrow x_2$ (" x_1 genau dann, wenn x_2 ") und $x_1 \text{ XOR } x_2$ ("entweder x_1 oder x_2 ; ausschließliches oder) sind definiert durch

$$x_1 \Rightarrow x_2 =_{\text{def}} x_2 \vee (\neg x_1) \quad (6.16)$$

$$x_1 \Leftrightarrow x_2 =_{\text{def}} (x_1 \wedge x_2) \vee ((\neg x_1) \wedge (\neg x_2)) \quad (6.17)$$

$$x_1 \text{ XOR } x_2 =_{\text{def}} (x_1 \wedge (\neg x_2)) \vee ((\neg x_1) \wedge x_2) \quad (6.18)$$

Diese Operatoren können auch durch Aufzählung ihrer Funktionswerte (*Wahrheitstabellen*) beschrieben werden.

x_1	x_2	$x_1 \Rightarrow x_2$	$x_1 \Leftrightarrow x_2$	$x_1 \text{ XOR } x_2$
0	0	1	1	0
0	1	1	0	1
1	0	0	0	1
1	1	1	1	0

Um die Anzahl der zu setzenden Klammern zu reduzieren, führen wir eine Rangfolge der Operatoren ein ähnlich wie z.B. die Regel "Punkt geht vor Strich" im Bereich der Zahlen.

(6.7) Klammerkonvention: \neg bindet stärker als die anderen Konnektoren; damit ist z.B. $(\neg p) \Rightarrow q$ gleichbedeutend mit $\neg p \Rightarrow q$. Klammern um negierte Ausdrücke können also in der Regel weggelassen werden. Entsprechend binden \wedge und \vee stärker als \Rightarrow und \Leftrightarrow , sodaß also z.B. $(p \wedge q) \Rightarrow r$ ersetzt werden kann durch $p \wedge q \Rightarrow r$.

Auch die Wirkung komplexerer Boolescher Ausdrücke kann durch Wahrheitstabellen verdeutlicht werden. Sinnvoll ist es hierbei, die Ausdrücke aus einfacheren Ausdrücken systematisch aufzubauen.

(6.8) Beispiele: (a) Wir leiten die Wahrheitstabelle für den dreistelligen Operator $p(x_1, x_2, x_3) =_{\text{def}} \neg x_1 \vee (\neg x_2 \wedge x_3)$ her.

x_1	x_2	x_3	$\neg x_1$	$\neg x_2 \wedge x_3$	$\neg x_1 \vee (\neg x_2 \wedge x_3)$
0	0	0	1	0	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	0	1
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	0	0	0
1	1	1	0	0	0

(b) Wir leiten die Wahrheitstabelle für den zweistelligen Operator

$q(x_1, x_2) =_{\text{def}} x_1 \Rightarrow (\neg x_2 \Rightarrow x_1) \wedge (x_2 \vee \neg x_1)$ her. Hierzu definieren wir als Hilfsgröße $r(x_1, x_2) =_{\text{def}} (\neg x_2 \Rightarrow x_1) \wedge (x_2 \vee \neg x_1)$.

x_1	x_2	$\neg x_1$	$\neg x_2$	$(\neg x_2) \Rightarrow x_1$	$x_2 \vee (\neg x_1)$	r	q
0	0	1	1	0	1	0	1
0	1	1	0	1	1	1	1
1	0	0	1	1	0	0	0
1	1	0	0	1	1	1	1

(c) Wir erstellen die Wahrheitstabellen für die zweistelligen Ausdrücke

$$s_1(x_1, x_2) =_{\text{def}} (x_1 \Rightarrow x_2) \Rightarrow (\neg x_1 \Rightarrow \neg x_2)$$

$$s_2(x_1, x_2) =_{\text{def}} (x_1 \Rightarrow x_2) \Rightarrow (\neg x_2 \Rightarrow \neg x_1)$$

$$s_3(x_1, x_2) =_{\text{def}} (x_1 \vee x_2) \wedge (\neg x_1 \wedge \neg x_2)$$

x_1	x_2	$\neg x_1$	$\neg x_2$	$x_1 \Rightarrow x_2$	$\neg x_1 \Rightarrow \neg x_2$	s_1	$\neg x_2 \Rightarrow \neg x_1$	s_2	$x_1 \vee x_2$	$\neg x_1 \wedge \neg x_2$	s_3
0	0	1	1	1	1	1	1	1	0	1	0
0	1	1	0	1	0	0	1	1	1	0	0
1	0	0	1	0	1	1	0	1	1	0	0
1	1	0	0	1	1	1	1	1	1	0	0

(6.9) Definition: $p(x_1, \dots, x_n)$ und $q(x_1, \dots, x_n)$ seien n -stellige Boolesche Ausdrücke.

(a) p heißt *Tautologie*, falls

$$p(x_1, \dots, x_n) = 1 \quad \text{für alle } (x_1, \dots, x_n) \in U^n$$

(b) p heißt *widerspruchsvoll*, falls

$$p(x_1, \dots, x_n) = 0 \quad \text{für alle } (x_1, \dots, x_n) \in U^n$$

(c) p und q heißen *logisch äquivalent*, falls

$$p(x_1, \dots, x_n) = q(x_1, \dots, x_n) \quad \text{für alle } (x_1, \dots, x_n) \in U^n$$

Wir schreiben hierfür $p \equiv q$.

Offenbar gilt $p \equiv q$ genau dann, wenn $p \Leftrightarrow q$ eine Tautologie ist.

(6.10) Beispiele: (a) Es gelten die Regeln (vgl. Rechengesetze (5.5))

(i) $\neg(\neg p) \equiv p$,

(ii) $\neg(p \Rightarrow q) \equiv q \wedge \neg p$,

$$(iii) \neg(p \Leftrightarrow q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q).$$

(b) In Beispiel (5.9)(c) ist s_2 eine Tautologie und s_3 widerspruchsvoll.

(c) Die Aussagen $\neg(x_1 \wedge x_2)$ und $\neg x_1 \vee \neg x_2$ sind logisch äquivalent.

(d) Der Ausdruck $q(x_1, x_2)$ aus Beispiel (5.9)(b) ist logisch äquivalent zu $x_1 \Rightarrow x_2$.

(e) Für $p \in A_n$ ist $p \wedge \neg p$ widerspruchsvoll und $p \vee \neg p$ Tautologie.

(f) Sind $p, q, r \in A_n$, und sind q widerspruchsvoll und r Tautologie, so ist $p \wedge q \equiv q$, $p \wedge r \equiv p$, $p \vee q \equiv p$ und $p \vee r \equiv r$. (Dies folgt aus den bekannten Eigenschaften des Null- und des Einselements.)

(6.11) Bemerkungen: (a) Die Relation " \equiv " auf der Menge von logischen Aussagen ist eine Äquivalenzrelation. (Beweis?)

(a) Häufig nützlich ist das *Ersetzungsprinzip*: Ersetze in Ausdrücken Teilausdrücke durch (z.B. einfachere) logisch äquivalente Teilausdrücke.

(6.12) Definition: (a) 1-stellige Boolesche Ausdrücke $p(x)$ der Form x und $\neg x$ heißen *Literale*.

(b) Ein n -stelliger Ausdruck p der Form $p(x_1, \dots, x_n) = p_1(x_1) \wedge p_2(x_2) \wedge \dots \wedge p_n(x_n)$, wobei alle p_i Literale sind, heißt *Atom*.

(c) Ein n -stelliger Ausdruck q der Form $q(x_1, \dots, x_n) = p^{(1)}(x_1, \dots, x_n) \vee \dots \vee p^{(k)}(x_1, \dots, x_n)$, wobei alle $p^{(i)}$ Atome sind, heißt *disjunktive Normalform*.

Man überzeugt sich leicht von der Richtigkeit der folgenden Aussagen. Hierbei definieren wir als *Belegung* einer n -stelligen Booleschen Aussage ein beliebiges n -Tupel $(x_1, \dots, x_n) \in \{0, 1\}^n$.

(6.13) Hilfssatz: (a) Zu jedem Atom p gibt es genau eine Belegung, für die p den Wahrheitswert 1 annimmt.

(b) Ist $q = p^{(1)} \vee \dots \vee p^{(k)}$ eine disjunktive Normalform mit den paarweise verschiedenen Atomen $p^{(i)}$, so gibt es genau k verschiedene Belegungen, für die q den Wert 1 annimmt.

Beweisidee für (a): Ist $p(x_1, \dots, x_n) = p_1(x_1) \wedge \dots \wedge p_n(x_n)$ mit den Literalen p_i , so ist $x_i = 1$ zu wählen für $p_i(x_i) = x_i$ und $x_i = 0$ für $p_i(x_i) = \neg x_i$. \circ

(6.14) Beispiele: (a) $p(x_1, x_2, x_3, x_4, x_5) = x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4 \wedge x_5$ ist ein 5-stelliges Atom. Die einzige Belegung, für die p den Wahrheitswert 1 annimmt, ist $(1, 0, 0, 1, 1)$.

(b) $p(x_1, x_2, x_3) = (x_1 \wedge \neg x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3)$ ist eine disjunktive Normalform; p nimmt den Wahrheitswert 1 an für die Belegungen $(1, 0, 0)$ und $(0, 1, 1)$.

(c) Ein Vergleich mit der Wahrheitstabelle in Beispiel (5.8) (c) zeigt, dass $s_2(x_1, x_2) = (x_1 \Rightarrow x_2) \Rightarrow (\neg x_1 \Rightarrow \neg x_2)$ logisch äquivalent ist zur disjunktiven Normalform $(\neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_2) \vee (x_1 \wedge x_2)$.

(6.15) Satz: Zu jedem nicht widerspruchsvollen n -stelligen Booleschen p Ausdruck gibt es eine logisch äquivalente disjunktive Normalform.

Beweis: Es sei $\{b^{(1)}, \dots, b^{(k)}\} \subseteq \{0, 1\}^n$ die Menge der Belegungen mit $p(b^{(i)}) = 1$; zu $b^{(i)}$ definiere $p^{(i)}$ als das Atom mit $p^{(i)}(b^{(i)}) = 1$. Dann ist p logisch äquivalent zu $p^{(1)} \wedge \dots \wedge p^{(k)}$. \circ

(6.16) Bemerkung: Der Ausdruck *Atom* in obiger Definition lässt sich folgendermaßen interpretieren. Gemäß Beispiel (2.8)(d) ist auf der Algebra der n -stelligen Booleschen Ausdrücke eine Ordnungsrelation \leq definiert durch

$$p \leq q \Leftrightarrow_{\text{def}} p \wedge q \equiv p \quad (6.19)$$

Ist nun p ein Atom, so gibt es genau eine Belegung (y_1, \dots, y_n) mit $p(y_1, \dots, y_n) = 1$. Ist q ein weiterer Boolescher Ausdruck mit $q \leq p$, so ist entweder $q(y_1, \dots, y_n) = 1$; in diesem Fall ist $q \wedge p = p$, also $q = p$; oder es ist $q(y_1, \dots, y_n) = 0$ und damit q das Nullelement.

Das erlaubt es uns, den Begriff der Atome als der kleinsten Nicht-Null-Elemente auf beliebige Boolesche Algebren zu erweitern.

(6.17) Definition: Ist $\mathcal{A} = (A, 0, 1, \oplus, \otimes, ')$ eine Boolesche Algebra mit der Ordnungsrelation

$$p \leq q \Leftrightarrow_{\text{def}} p \otimes q = p \quad (6.20)$$

so heißt p Atom, wenn $p \neq 0$, und wenn für $q \leq p$ gilt: $q = p$ oder $q = 0$.

(Übung: Was sind die Atome in Booleschen Mengenalgebren?)

6.3 Realisierungen und Folgerungen

[Motivation: Beispiel (Kommissar), auf Folie]

(6.18) Definition: $\Sigma = \{p_1, p_2, p_3, \dots\}$ sei eine Menge von n -stelligen Booleschen Aussagen.

(i) Eine Belegung von $(x_1, \dots, x_n) \in \{0, 1\}^n$ heißt *Realisierung* von Σ , wenn jede Aussage aus Σ unter dieser Belegung den Wahrheitswert 1 hat: $1 = p_1(x_1, \dots, x_n) = p_2(x_1, \dots, x_n) = p_3(x_1, \dots, x_n) \dots$

(ii) Σ heißt *widerspruchsfrei*, wenn Σ eine Realisierung besitzt, andernfalls *widerspruchsvoll*.

(iii) s sei eine weitere n -stellige Aussage; s ist *Folgerung aus Σ* , wenn s für jede Realisierung von Σ den Wahrheitswert 1 hat. (Schreibweise: $\Sigma \models s$.) Die Menge der Folgerungen aus Σ wird mit $\text{Ded}(\Sigma)$ bezeichnet.

(6.19) Beispiele: a) $\Sigma := \{x_1, x_1 \Rightarrow x_2\} \subseteq A_2$; die einzige Realisierung ist $(x_1, x_2) = (1, 1)$; Folgerungen sind z.B. x_2 und $x_1 \wedge x_2$.

b) $\Sigma := \{\neg x_1 \Rightarrow (x_2 \Rightarrow x_3), x_3 \wedge (x_1 \Leftrightarrow x_2)\} \subseteq A_3$;

Wahrheitstabelle:

x_1	x_2	x_3	$\neg x_1$	$x_2 \Rightarrow x_3$	$x_1 \Leftrightarrow x_3$	$\neg x_1 \Rightarrow (x_2 \Rightarrow x_3)$	$x_3 \wedge (x_1 \Leftrightarrow x_3)$
0	0	0	1	1	1	1	0
0	0	1	1	1	0	1	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	0
1	0	0	0	1	0	1	0
*	1	0	0	1	1	1	1
1	1	0	0	0	0	1	0
*	1	1	0	1	1	1	1

Realisierungen: $(1, 0, 1)$ und $(1, 1, 1)$;

Folgerungen: z.B. $s_1(x_1, x_2, x_3) = \neg x_1 \Rightarrow x_2$, $s_2(x_1, x_2, x_3) = \neg x_1 \Rightarrow x_3$, $s_3(x_1, x_2, x_3) = \neg x_2 \Rightarrow x_3$.

(c) p, q, r, s seien Boolesche Ausdrücke, und $\Sigma = \{p \wedge q, q \Rightarrow s, r \vee \neg s\}$. Dann sind p, q, r, s Folgerungen aus Σ .

(d) Zu jeder nicht leeren Aussagenmenge $\Sigma = \{p_1, p_2, p_3, \dots\}$ gibt es eine Reihe von *trivialen* Folgerungen: (i) Alle Aussagen aus Σ : p_1, p_2, \dots ; (ii) endliche *und*-Verknüpfungen: $p_1 \wedge p_2, p_1 \wedge p_2 \wedge p_3, \dots$; (iii) endliche *oder*-Verknüpfungen; (iv) jede Tautologie.

(6.20) Bemerkungen: (i) Σ und Δ seien Mengen von Ausdrücken und es sei $\Delta \subseteq \Sigma$. Dann ist jede Realisierung von Σ auch Realisierung von Δ und es gilt $\text{Ded}(\Delta) \subseteq \text{Ded}(\Sigma)$. Außerdem ist $\text{Ded}(\text{Ded}(\Delta)) = \text{Ded}(\Delta)$.

(ii) Ist $\Sigma \models s_1 \Rightarrow s_2$ und $\Sigma \models s_1$, so gilt $\Sigma \models s_2$. (Vgl. Regel des modus ponens im folgenden Abschnitt.)

(iii) $\Sigma \models s_1 \Rightarrow s_2$ gilt genau dann, wenn $\Sigma \cup \{s_1\} \models s_2$.

6.4 Über das mathematische Beweisen

Aufbauend auf den Ergebnissen des letzten Abschnitts wollen wir jetzt einige wichtige Beweiskonzepte und -strukturen analysieren. In den seltensten Fällen liegen diese Konzepte in "reiner" Form vor.

A – Direkter Beweis

Die Grundform des direkten Beweises beruht auf der Beobachtung, dass eine Aussage q eine Folgerung der zwei Aussagen p und $p \Rightarrow q$ ist:

$$\{p, p \Rightarrow q\} \models q \quad .$$

Diese Feststellung wird *Regel des modus ponens* genannt. Die Beweisstrategie besteht demnach in

- (i) einer *Hypothese* (d.h. Voraussetzung, Annahme)
- (ii) dem Nachweis der Wahrheit der Aussage $p \Rightarrow q$.

Der Schritt (ii) kann hierbei wiederum aus mehreren Schritten aufgebaut sein.

Betrachten wir daraufhin das folgende Beispiel.

(6.21) Beispiel: $\triangle ABM$ sei ein Dreieck mit den Ecken A , B und M , wobei M der Mittelpunkt eines Kreises ist und A und B auf der Kreislinie liegen. Gezeigt werden soll, dass $\triangle ABM$ zwei gleiche Winkel besitzt.

Zunächst bemerken wir, dass $\triangle ABM$ ein gleichschenkliges Dreieck ist, da die Längen der Strecken \overline{AM} und \overline{BM} gleich sind (nämlich gleich dem Kreisradius). Damit lauten bei unserem Problem die Hypothese p und die zu beweisende Aussage q :

p : $\triangle ABM$ ist gleichschenkliges Dreieck.

q : $\triangle ABM$ hat zwei gleiche Winkel.

Der Nachweis der Aussage $p \Rightarrow q$ ist uns aus der Geometrie wohlbekannt. Damit können wir folgern, dass unter der Hypothese p die Aussage q richtig ist.

Eine leicht zu beweisende Verallgemeinerung der Regel des modus ponens ist

(6.22) Hilfssatz: Es sei p_0, p_1, p_2, \dots eine Folge von Booleschen Aussagen. Dann gilt

$$\{p_0, p_0 \Rightarrow p_1, p_1 \Rightarrow p_2, \dots, p_n \Rightarrow p_{n+1}\} \models p_{n+1} \quad .$$

Beweis durch vollständige Induktion nach n :

Induktionsanfang: Für $n = 0$ ist die Aussage

$$\{p_0, p_0 \Rightarrow p_1\} \models p_1$$

gerade die Regel des modus ponens.

Induktionsvoraussetzung: Es gelte die *Hypothese*

$$\{p_0, p_0 \Rightarrow p_1, p_1 \Rightarrow p_2, \dots, p_n \Rightarrow p_{n+1}\} \models p_{n+1} \quad .$$

Induktionsbehauptung: Dann gilt auch die Aussage

$$\{p_0, p_0 \Rightarrow p_1, \dots, p_1 \Rightarrow p_2, p_{n+1} \Rightarrow p_{n+2}\} \models p_{n+2} \quad .$$

Beweis: Für $k \in \mathbb{N}$ bezeichnen wir $M_k := \{p_0, p_0 \Rightarrow p_1, \dots, p_k \Rightarrow p_{k+1}\}$. Nach Voraussetzung ist $p_{n+1} \in \text{Ded}(M_n)$. Wegen $M_n \subseteq M_{n+1}$ und Bemerkung (5.20)(i) ist $p_{n+1} \in \text{Ded}(M_{n+1})$. Damit sind $p_{n+1}, p_{n+1} \Rightarrow p_{n+2} \in \text{Ded}(M_{n+1})$, und zusammen mit Bemerkung (5.20)(i) folgt $p_{n+2} \in \text{Ded}(\text{Ded}(M_{n+1})) = \text{Ded}(M_{n+1})$. $\quad \circ$

In diesem Fall wird die Gültigkeit der Aussage q aus der Hypothese p_0 und einer "Kette" von Folgerungen $p_i \Rightarrow p_{i+1}$ hergeleitet.

(6.23) Beispiel: Bewiesen werden soll die Aussage "Wenn a durch 6 teilbar ist, so auch durch 3". Hier lautet die Hypothese p_0 : " a ist durch 6 teilbar". Zu beweisen ist die Aussage q : " a ist durch 3 teilbar. Der Beweis (den wir hier ausführlicher durchführen als dies in der Regel getan werden wird), führt über eine Reihe p_1, \dots, p_n von Zwischenaussagen:

p_1 :	$(\exists k \in \mathbb{N})(a = 6 \cdot k)$	$p_0 \Rightarrow p_1$	(Def. Teilbarkeit durch 6)
p_2 :	$(\exists k \in \mathbb{N})(a = (2 \cdot 3) \cdot k)$	$p_1 \Rightarrow p_2$	$(6 = 2 \cdot 3)$
p_3 :	$(\exists k \in \mathbb{N})(a = (3 \cdot 2) \cdot k)$	$p_2 \Rightarrow p_3$	(Kommutativgesetz)
p_4 :	$(\exists k \in \mathbb{N})(a = 3 \cdot (2 \cdot k))$	$p_3 \Rightarrow p_4$	(Assoziativgesetz)
p_5 :	$(\exists k' \in \mathbb{N})(a = 3 \cdot k')$	$p_4 \Rightarrow p_5$	(setze $k' := 2 \cdot k$)
		$p_5 \Rightarrow q$	(Def. Teilbarkeit durch 3)

Die Implikationen $p_i \Rightarrow p_{i+1}$ und $p_5 \Rightarrow q$ folgen hierbei aus der Definition der Teilbarkeit durch 6 bzw. durch 3 und den wohlbekannten Kommutativ- und Assoziativgesetzen.

Bei der praktischen Durchführung direkter Beweise treten häufig auch Modifikationen auf; z.B. Fallunterscheidungen sowie Implikationen wie $p_{i-1} \wedge p_i \Rightarrow p_{i+1}$ etc.

B – Beweis durch Kontraposition

Die Aussagen $p \Rightarrow q$ und $\neg q \rightarrow \neg p$ sind logisch äquivalent. (Beweis?) Demnach führt die Regel des modus ponens auf die modifizierte Regel

$$\{p, \neg q \Rightarrow \neg p\} \models q \quad .$$

Diese Beweisstrategie wird *Beweis durch Kontraposition* genannt.

(6.24) Beispiel: Bewiesen werden soll die Aussage "Wenn a^2 eine ungerade Zahl ist, dann ist a ungerade". Hier lauten Hypothese p und zu beweisende Aussage q

$$\begin{aligned} p : & \quad a^2 \text{ ist ungerade Zahl.} \\ q : & \quad a \text{ ist ungerade.} \end{aligned}$$

Um q aus der Gültigkeit von p zu folgern, ist die Implikation $\neg q \Rightarrow \neg p$ zu beweisen. Wie in Beispiel (5.23) führen wir – startend von der Hypothese $\neg q$: "a ist gerade" eine Reihe von Zwischenaussagen p_i ein und zeigen $p_i \Rightarrow p_{i+1}$ sowie $\neg q \rightarrow p_1$ und $p_n \Rightarrow \neg p$, um zu folgern, dass gilt $\neg p$: "a² ist gerade".

$$\begin{array}{ll} p_1 : (\exists k \in \mathbb{N})(a = 2 \cdot k) & \neg q \Rightarrow p_1 \quad (\text{Def. Teilbarkeit durch 2}) \\ p_2 : (\exists k \in \mathbb{N})(a^2 = (2 \cdot k) \cdot a) & p_1 \Rightarrow p_2 \quad (\text{Multiplikation mit } a) \\ p_3 : (\exists k \in \mathbb{N})(a^2 = 2 \cdot (k \cdot a)) & p_2 \Rightarrow p_3 \quad (\text{Assoziativgesetz}) \\ p_4 : (\exists k' \in \mathbb{N})(a^2 = 2 \cdot k') & p_3 \Rightarrow p_4 \quad (\text{ersetze } a \cdot k \text{ durch } k') \\ & p_4 \Rightarrow \neg p \quad (\text{Def. Teilbarkeit durch 2}) \end{array}$$

C – Widerspruchsbeweis

Wir überzeugen uns zunächst, dass gilt

$$\{r, p \wedge \neg q \Rightarrow \neg r\} \models p \Rightarrow q \quad .$$

Denn: Ist r wahr, so ist $\neg r$ falsch. Damit $p \wedge \neg q \Rightarrow \neg r$ wahr ist, muss also $p \wedge \neg q$ falsch und daher $\neg(p \wedge \neg q) \equiv (\neg p \vee q)$ wahr sein. Letztere Aussage ist aber logisch äquivalent zu $p \Rightarrow q$. Zum Beweis von $p \Rightarrow q$ genügt es also, unter der Hypothese $p \wedge \neg q$ eine Aussage zu beweisen, welche falsch ist. Damit führt die Aussage $p \wedge \neg q$ zum Widerspruch, muss also falsch und ihre Negation daher wahr sein.

(6.25) Beispiel: Bewiesen werden soll die Aussage "Wenn a und b gerade natürliche Zahlen sind, dann ist auch $a \cdot b$ gerade", mit der Hypothese p : "a und b sind gerade natürliche Zahlen" und der zu beweisenden Aussage q : "a · b ist gerade". Zur Durchführung des Beweises wird gezeigt, dass aus der Aussage $p \wedge \neg q$ die falsche Aussage $\neg r$: "(a · b ist gerade) und (a · b ist ungerade)" hergeleitet werden kann. Wir geben hier nur Zwischenaussagen p_i an. Ergänzen Sie den Beweis durch Begründung der Implikationen $p \wedge \neg q \Rightarrow p_1$, $p_i \Rightarrow p_{i+1}$ (für $i = 1, 2, 3$) und $p_4 \Rightarrow \neg r$.

$$p_1 : (a \text{ gerade}) \text{ und } (\exists k \in \mathbb{N})(b = 2 \cdot k) \text{ und } (a \cdot b \text{ ungerade})$$

$$p_2 : (\exists k \in \mathbb{N})(a \cdot b = a \cdot (2 \cdot k)) \text{ und } (a \cdot b \text{ ungerade})$$

$$p_3 : (\exists k \in \mathbb{N})(a \cdot b = 2 \cdot (a \cdot k)) \text{ und } (a \cdot b \text{ ungerade})$$

$$p_4 : (\exists k' \in \mathbb{N})(a \cdot b = 2 \cdot k') \text{ und } (a \cdot b \text{ ungerade})$$

C – Äquivalenzbeweise, Ringbeweise

Die Aussage $p \Leftrightarrow q$ ist äquivalent zu $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Zu ihrem Beweis müssen die beiden Implikationen hergeleitet werden, z.B. durch eine der oben aufgeführten Strategien. Eine interessante Strategie zum Beweis der Äquivalenz mehrerer Aussagen folgt aus dem nächsten Ergebnis.

(6.26) Hilfssatz: Es sei $M_n = \{a_0, \dots, a_n\}$ eine beliebige $(n + 1)$ -elementige Menge von Aussagen. Dann gilt für $\Sigma := \{a_0 \Rightarrow a_1, a_1 \Rightarrow a_2, \dots, a_{n-1} \Rightarrow a_n, a_n \Rightarrow a_0\}$

$$\Sigma \models a_i \Leftrightarrow a_j \quad \text{für alle } i, j \in \{0, \dots, n\} \quad .$$

Außerdem gilt für beliebige $i, j \in \{0, \dots, n\}$

$$\Sigma \cup \{a_i\} \models a_j \quad .$$

Der Beweis kann leicht (z.B. mit Hilfe der vollständigen Induktion?) geführt werden.

Beweise, welche auf dieser Strategie beruhen, werden auch *Ringbeweise* genannt.

Ist Σ eine Aussagenmenge, welche (viele) Implikationen enthält, so ist es u.U. geeignet, sich Äquivalenzen mittels grafischer Darstellung herzuleiten.

(6.27) Beispiele: (i) Für die Aussagen S_1, \dots, S_5 sei bewiesen: $S_3 \Rightarrow S_2, S_3 \Rightarrow S_4, S_4 \Rightarrow S_3, S_4 \Rightarrow S_5, S_5 \Rightarrow S_1$ und $S_5 \Rightarrow S_3$.

Die Gültigkeit welcher Aussagen folgt – aus der Aussage S_1 , – aus der Aussage S_3 , – aus der Aussage S_5 ?

Welche Aussagen sind äquivalent?

[Grafische Darstellung!]

(ii) Für die Aussagen S_1, \dots, S_5 sei bewiesen: $S_1 \Rightarrow S_2, S_3 \Rightarrow S_5, S_4 \Rightarrow S_1, S_4 \Rightarrow S_3$ und $S_5 \Rightarrow S_1$.

Aus der Gültigkeit welcher einzelnen Aussage folgt die Gültigkeit aller anderen Aussagen?

[Grafische Darstellung!]

D – Logische Systeme

Logische Systeme sind geschlossene Systeme von Axiomen (gültigen Aussagen) und Regeln zum Aufbau und zur Herleitung der Gültigkeit weiterer Aussagen.

(6.28) Aufbau eines logischen Systems: Ein logisches System setzt sich zusammen aus den zwei Komponenten

(i) *Axiome:* Aussagen, denen a priori (d.h. ohne weitere Begründung) der Wahrheitswert "wahr" zugeordnet wird;

(ii) *System von Regeln:* diese erlauben es, von auf wahr erkannten Aussagen auf den Wahrheitswert weiterer Aussagen zu schließen.

(6.29) Beispiel: Ein logisches System zur Charakterisierung einer Menge M :

(i) Axiom: $0 \in M$;

(ii) Regel: Ist $n \in M$, so auch $n + 1$.

Mit Hilfe des Axioms (i) und durch ein- bzw. zweimalige Anwendung der Regel (ii) folgt z.B., daß die Aussagen " $1 \in M$ " und " $2 \in M$ " wahr sind. Dagegen ist die Aussage " $-1 \in M$ " unentscheidbar.

(6.30) Definition: (i) Ein *deduktiver Beweis* (kurz: *Deduktion*) ist die sequentielle

Anwendung von Regeln, um Aussagen als wahr zu charakterisieren.

(ii) Als *mathematische Sätze (Theoreme)* werden alle Axiome und alle durch Deduktion bewiesenen Aussagen bezeichnet.

(6.31) Beispiel: Eine formale Sprache – zusammengesetzt aus Zeichen der Liste $\{S, a, b\}$ – werde beschrieben durch das logische System

- (i) Axiom: Die Aussage S ist wahr;
- (ii) Regeln: (a) Wird in einer wahren Aussage das Zeichen S durch die Folge aSb ersetzt, so entsteht wieder eine wahre Aussage;
 (b) das Entfernen des Zeichens S aus einer wahren Aussage führt wieder zu einer wahren Aussage;
 (c) alle Aussagen, die nicht durch (i), (ii)(a) und (ii)(b) als wahr bewiesen werden können, sind falsch.

Daß die Aussage $aaabbb$ wahr ist, kann deduktiv wie folgt gezeigt werden.

S	(Axiom)
aSb	(Regel (ii)(a))
$aaSbb$	(Regel (ii)(a)) .
$aaaSbbb$	(Regel (ii)(a))
$aaabbb$	(Regel (ii)(b))

Alle mathematischen Sätze sind von der Form $a \cdots aSb \cdots b$ oder $a \cdots ab \cdots b$, wobei gleichviele Zeichen a und b vorkommen.

6.5 Disjunktive Normalformen

Disjunktive Normalformen erlauben die effiziente Verknüpfung von Wahrheitstabellen, logischen Ausdrücken und Schaltkreisen.

(6.32) Beispiele: a) Die Aussagen A_1 , A_2 und A_3 zu den Aussagevariablen P , Q und R seien gegeben durch die Wahrheitstabelle

P	Q	R	A_1	A_2	A_3
0	0	0	0	1	1
0	0	1	0	0	1
0	1	0	1	0	0
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	0	0
1	1	1	0	0	0

Darstellung der A_i mit Hilfe "disjunktiver Normalformen":

$$A_1: \neg P \wedge Q \wedge \neg R,$$

$$A_2: (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R),$$

$$A_3: (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R).$$

Vereinfachung von A_3 mit Hilfe der Regeln (5.20), (5.21): Wegen $((\neg P \wedge \neg Q) \wedge \neg R) \vee ((\neg P \wedge \neg Q) \wedge R) \equiv (\neg P \wedge \neg Q) \wedge (\neg R \vee R) \equiv (\neg P \wedge \neg Q)$ (da $\neg R \wedge R$ Tautologie ist) und $((P \wedge \neg Q) \wedge \neg R) \vee ((P \wedge \neg Q) \wedge R) \equiv (P \wedge \neg Q) \wedge (\neg R \vee R) \equiv (P \wedge \neg Q)$ ist $A_3 \equiv (\neg P \wedge \neg Q) \vee (P \wedge \neg Q) \equiv (\neg P \vee P) \wedge \neg Q \equiv \neg Q$.

b) Realisierung von $A : (P \Rightarrow Q) \Leftrightarrow ((Q \Rightarrow R) \wedge \neg P)$ durch einen Schaltkreis:

Wahrheitstabelle:

P	Q	R	\dots	A	$\neg A$
0	0	0		1	0
0	0	1		1	0
0	1	0		0	1
0	1	1		1	0
1	0	0		1	0
1	0	1		1	0
1	1	0		0	1
1	1	1		0	1

Mit den bekannten Rechenregeln folgt

$$\neg A \equiv (\neg P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge R) \equiv \dots \equiv Q \wedge (\neg R \vee (P \wedge R)).$$

[Graphik: Schaltkreis]

(6.33) Definition: a) Ein Ausdruck ist in *verneinungstechnischer Normalform (vNF)*, wenn er nur die Verknüpfungen \neg , \wedge und \vee enthält, wobei \neg höchstens vor den Aussagenvariablen steht.

b) Ein Ausdruck in vNF heißt *Elementarkonjunktion*, falls nur \neg und \wedge auftreten.

c) Ein Ausdruck A ist in *disjunktiver Normalform (DN)*, wenn er von der Form $A = A_1 \vee \dots \vee A_k$ ist, wobei die A_i für $i = 1 \dots k$ Elementarkonjunktionen sind. Eine DN A mit den Aussagenvariablen P_1, \dots, P_r ist in *kanonischer disjunktiver Normalform (kDN)*, wenn jedes P_i in jeder Elementarkonjunktion A_j genau einmal vorkommt.

(6.34) Beispiele: a) Eine vNF von $\neg(P \Rightarrow Q)$ ist $P \wedge \neg Q$; dies ist gleichzeitig eine DN.

b) Gegeben sei $A : \neg(P \Rightarrow Q) \Rightarrow R \vee (Q \Rightarrow P) \equiv: A_1 \Rightarrow A_2 \equiv \neg A_1 \vee A_2$ mit $A_1 : \neg(P \Rightarrow Q) \equiv \neg(\neg P \vee Q)$ und $A_2 : R \vee (Q \Rightarrow P)$. Offenbar ist $(\neg P \vee Q) \vee (R \vee \neg Q \vee P) \equiv \neg P \vee P \vee \neg Q \vee Q \vee R$ eine vNF von A .

Man erkennt hieraus leicht, daß A eine Tautologie ist.

c) Gesucht ist eine DN von $A : \neg(P \wedge (Q \Leftrightarrow P))$.

Es ist $Q \Leftrightarrow P \equiv (\neg Q \vee P) \wedge (\neg P \vee Q)$ und daher

$$A \equiv \neg(P \wedge (\neg Q \vee P) \wedge (\neg P \vee Q)) \equiv \neg P \vee \neg(\neg Q \vee P) \vee \neg(\neg P \vee Q) \equiv \neg P \vee (Q \wedge \neg P) \vee (P \wedge \neg Q).$$

Erweiterung zu kDN erfolgt durch Ansatz

$$(\neg P \wedge (Q \vee \neg Q)) \vee (Q \wedge \neg P) \vee (P \wedge \neg Q) \equiv (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q).$$

(6.35) Bemerkungen: a) Jeder Ausdruck ist äquivalent zu einem Ausdruck in vNF;

b) jeder Ausdruck ist äquivalent zu einem Ausdruck in kDN.

Beweise von a) und b) können leicht durch Induktion über die Länge der Ausdrücke geführt werden; vgl. [TW]⁵ Sätze 1.29 und 1.30.

Verfahren zur Konstruktion disjunktiver Normalformen

(6.36) Verfahren 1: Konstruktion disjunktiver Normalformen:

⁵H. P. Tuschik/ H. Wolter, Mathematische Logik – kurzgefaßt, BI Wissenschaftsverlag, 1994

Schritt 1: Elimination aller Äquivalenzen \Leftrightarrow gemäß der Rechenregel

$$A_1 \Leftrightarrow A_2 \equiv (A_1 \wedge A_2) \vee (\neg A_1 \wedge \neg A_2);$$

Schritt 2: Elimination aller Implikationen \Rightarrow gemäß $A_1 \Rightarrow A_2 \equiv \neg A_1 \vee A_2$;

Schritt 3: Ersetzen aller Ausdrücke der Form $\neg(A_1 \wedge A_2)$ durch $\neg A_1 \vee \neg A_2$ und aller Ausdrücke der Form $\neg(A_1 \vee A_2)$ durch $\neg A_1 \wedge \neg A_2$;

Schritt 4: Ersetzen aller Ausdrücke der Form $A_1 \wedge (A_2 \vee A_3)$ gemäß Distributivgesetz durch $(A_1 \wedge A_2) \vee (A_1 \wedge A_3)$.

(6.37) Beispiel: $A: (\neg P \Rightarrow Q) \Leftrightarrow (Q \Rightarrow P \wedge Q)$;

Schritt 1: $A \equiv B \vee C$ mit

$$B \equiv (\neg P \Rightarrow Q) \wedge (Q \Rightarrow P \wedge Q) \text{ und } C \equiv \neg(\neg P \Rightarrow Q) \wedge \neg(Q \Rightarrow P \wedge Q);$$

$$\text{Schritt 2: } B \equiv (\neg(\neg P) \vee Q) \wedge (\neg Q \vee (P \wedge Q)) \equiv (P \vee Q) \wedge (\neg Q \vee (P \wedge Q))$$

$$\text{und } C \equiv \neg(\neg(\neg P) \vee Q) \wedge \neg(\neg P \vee (P \wedge Q)) \equiv \neg(P \vee Q) \wedge \neg(\neg Q \vee (P \wedge Q));$$

$$\text{Schritt 3: } C \equiv (\neg P \wedge \neg Q) \wedge (\neg(\neg Q) \wedge \neg(P \wedge Q)) \equiv (\neg P \wedge \neg Q) \wedge (Q \wedge (\neg P \vee \neg Q));$$

$$\text{Schritt 4: } B \equiv ((P \vee Q) \wedge \neg Q) \vee ((P \vee Q) \wedge (P \wedge Q))$$

$$\equiv ((P \wedge \neg Q) \vee (Q \wedge \neg Q)) \vee ((P \wedge (P \wedge Q)) \vee (Q \wedge P \wedge Q))$$

$$\equiv (P \wedge \neg Q) \vee (Q \wedge \neg Q) \vee (P \wedge P \wedge Q) \vee (Q \wedge P \wedge Q) \quad \text{dNF für } B;$$

$$\text{Vereinfachung: } B \equiv (P \wedge \neg Q) \vee (P \wedge Q) \equiv P \quad (\text{Distributivgesetz});$$

$$C \equiv (\neg P \wedge \neg Q) \wedge ((Q \wedge \neg P) \vee (Q \wedge \neg Q))$$

$$\equiv ((\neg P \wedge \neg Q) \wedge (Q \wedge \neg Q)) \vee ((\neg P \wedge \neg Q) \wedge (Q \wedge \neg Q))$$

$$\equiv (\neg P \wedge \neg Q \wedge Q \wedge \neg P) \vee (\neg P \wedge \neg Q \wedge Q \wedge \neg Q) \quad \text{dNF für } C;$$

$$\text{Vereinfachung: } C \equiv (\neg P \wedge \neg Q \wedge Q) \vee (\neg P \wedge \neg Q \wedge Q);$$

es folgt, daß C widersprüchlich ist; damit ist eine dNF für A gegeben durch

$$A \equiv B \vee C \equiv B \equiv P.$$

Verfahren 1 liefert immer eine DN, in der Regel jedoch keine kDN.

(6.38) Verfahren 2: Konstruktion kanonischer disjunktiver Normalformen:

Schritt 1: Erstelle eine DN gemäß Verfahren 1; gegebenenfalls vereinfachen; dann taucht jede Aussagevariable in jeder Elementarkonjunktion höchstens einmal auf;

Schritt 2: taucht eine Aussagevariable P nicht in einer Elementarkonjunktion A_i auf, so ersetze A_i durch $A_i \wedge (P \vee \neg P)$; wende Distributivgesetz an;

Schritt 3: streiche gegebenenfalls mehrfach auftretende Elementarkonjunktionen.

(6.39) Beispiel: $A: P \wedge Q$ sei Elementarkonjunktion zu den Aussagevariablen P , Q und R ; ersetze A durch $(P \wedge Q) \wedge (R \vee \neg R) \equiv (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)$.

(6.40) Anwendungsbeispiel: Sind die Aussagen $A: P \Rightarrow (Q \Leftrightarrow R)$ und $B: (P \Leftrightarrow Q) \Rightarrow R$ logisch äquivalent?

Die Antwort erfolgt anhand des Vergleichs der kDN beider Aussagen.

Die Anwendung der oben beschriebenen Schritte ergibt als kDN

- für A : $(\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$ und
- für B : $(\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$;

ein Vergleich zeigt, daß z.B. $\{(P, 0), (Q, 0), (R, 0)\}$ eine Realisierung von A ist, aber nicht von B ; damit sind A und B nicht äquivalent.

7 Fuzzy-Methoden

(fuzzy (engl.) = undeutlich, verschwommen)

7.1 Mehrwertige und Fuzzy-Logik

Mehrwertige Logik: Menge $\{0,1\}$ der Wahrheitswerte wird erweitert auf größere Bereiche.

Bemerkung: Viele Aussagen des Alltags können nicht mit ja oder nein, sondern eher mit z.B. "ein bißchen", "viel" etc. beantwortet werden. (Vgl. Aussage "Es ist kalt".)

Stichworte: – *Intuitionistische Logik*⁶ (pseudo-Boole'sche Verbände);

– *Quantenlogik*⁷ (orthonormale Verbände);

– *Fuzzy-Logik* (Einheitsintervall $[0,1]$).

(7.1) Beispiele: (a) Datenbanksprache *SQL* (System Query Language): Die Wahrheitswerte 0 und 1 für "falsch" und "wahr" werden ergänzt um den Wert ? für "unbestimmbar". Die wichtigsten ein- und zweistelligen Operationen lassen sich problemlos auf diesen vergrößerten Zustandsbereich erweitern. Die Wahrheitstabellen für Negation, Konjunktion und Disjunktion lauten

x_1	x_2	$\neg x_2$	$x_1 \wedge x_2$	$x_1 \vee x_2$
0	0	1	0	0
0	?	?	0	?
0	1	0	0	1
?	0		0	?
?	?		?	?
?	1		?	1
1	0		1	1
1	?		?	1
1	1		1	1

⁶Intuitionismus: von L. E. J. Brouwer 1907 begründete Auffassung, daß die mathematische Existenz als Konstruierbarkeit und das mathematische Beweisen als Angabe der Konstruierbarkeit zu verstehen sind.

⁷Bezeichnung für eine Logik, die die Verschiedenartigkeit quantenmechanischer Aussagen gegenüber den Aussagemöglichkeiten der klassischen Logik berücksichtigt.

Stellen wir diese Operatoren wie folgt dar:

\vee	0	?	1	,	\wedge	0	?	1	,	x	$\neg x$
0	0	?	1		0	0	0	0		0	1
?	?	?	1		?	0	?	?		?	?
1	1	1	1		1	0	?	1		1	0

so sehen wir, dass z.B. die Kommutativgesetze für \vee und \wedge gelten. Das Sixtupel $(\{0, ?, 1\}, 0, 1, \vee, \wedge, \neg)$ kann aber keine Boolesche Algebra sein, da letztere – wie wir wissen – nur Mengen beschreiben können, deren Anzahl von Elementen eine Zweierpotenz ist. Welche Gesetze sind also verletzt? Eine "Regelverletzung" liegt beispielsweise in den Gesetzen für das Null- und das Einselement (vgl. Definition A.3(iv)). So ist beispielsweise $? \vee \neg ? = ? \neq 1$ und $? \wedge \neg ? = ? \neq 0$. Es gehen also gewisse Struktureigenschaften gegenüber der klassischen Logik verloren.

(b) *Linguistische Variable* zur Beschreibung der Lufttemperatur: Definiere zur Temperatur T die Variablen A_{kalt} , A_{warm} und A_{mittel} durch

$$A_{kalt}(T) = \begin{cases} 1 & \text{falls } T \leq 5^\circ \\ 0 & \text{falls } T \geq 15^\circ \end{cases} \quad A_{warm}(T) = \begin{cases} 1 & \text{falls } T \geq 25^\circ \\ 0 & \text{falls } T \leq 15^\circ \end{cases}$$

$$A_{mittel}(T) = \begin{cases} \frac{T-5^\circ}{15^\circ-5^\circ} & \text{falls } 5^\circ \leq T \leq 15^\circ \\ \frac{25^\circ-T}{25^\circ-15^\circ} & \text{falls } 15^\circ \leq T \leq 25^\circ \\ 0 & \text{falls } (T \leq 5^\circ) \vee (T \geq 25^\circ) \end{cases}$$

Alle Funktionen haben als Bildbereich die Menge $[0, 1]$. Außerdem gilt für alle $T \in \mathbb{R}$ $A_{kalt}(T) + A_{mittel}(T) + A_{warm}(T) = 1$.

Variablen mit Werten zwischen 0 und 1 heißen auch *Zugehörigkeitsfunktionen* oder *fuzzy Variable*.

Definition Boole'scher Operatoren:

	Boole	Fuzzy
AND	$C = A \wedge B$	$C = \min(A, B)$
OR	$C = A \vee B$	$C = \max(A, B)$
NOT	$C = \neg A$	$C = 1 - A$

Es ist naheliegend, das "Nullelement" ν durch $(\forall T \in \mathbb{R})(\nu(T) = 0)$ und das "Einselement" $(\forall T \in \mathbb{R})(\eta(T) = 1)$ zu definieren. Wie im vorhergehenden Beispiel erhalten wir allerdings wieder keine Boolesche Algebra.

7.2 Unscharfe Mengen

- Bisher: Die Aussage $x \in M$ hat den Wahrheitswert 0 oder 1;
- jetzt: x hat "Zugehörigkeitsgrad/-Wahrscheinlichkeit zu Menge M , beschrieben durch eine Zugehörigkeitsfunktion $m_M : U \rightarrow [0, 1]$ (U Universalmenge).

Beispiel: A sei die unscharfe Menge der reellen Zahlen, welche nahezu gleich 20 sind; A kann z.B. beschrieben werden durch eine Zugehörigkeitsfunktion $m_A : \mathbb{R} \rightarrow [0, 1]$, $m_A(x) = \max\{0, 1 - (20 - x)^2/4\}$.

Mengenalgebraische Operationen für unscharfe Mengen

Definition: Zwei Mengen A und B seien beschrieben durch Zugehörigkeitsfunktionen m_A und m_B . Durchschnitt $A \sqcap B$ und Vereinigung $A \sqcup B$ sind definiert durch die Zugehörigkeitsfunktionen

$$m_{A \sqcap B}(x) = \min\{m_A(x), m_B(x)\} \text{ und } m_{A \sqcup B}(x) = \max\{m_A(x), m_B(x)\}.$$

Es gelten die meisten der bekannten Rechenregeln (Kommutativ-, Assoziativ- Distributivgesetze etc.).

Definition: Das unscharfe kartesische Produkt zweier unscharfer Mengen A und B wird definiert durch die Zugehörigkeitsfunktion $m_{A \times B}(x, y) = \min\{m_A(x), m_B(y)\}$; entsprechend kann eine unscharfe Relation R als Teilmenge des kartesischen Produkts definiert werden durch eine Zugehörigkeitsfunktion.

Eigenschaften von Relationen lassen sich übertragen.

Anhang B: Die Axiome der Mengenlehre

Eine Aufgabe der Mengenlehre ist es, den zuverlässigen Umgang mit Mengen widerspruchsfrei abzusichern. Solange man mit *endlichen* Mengen arbeitet, scheinen keine *prinzipiellen* Probleme aufzutreten¹ und diese Vorsicht unbegründet. Probleme können spätestens dann auftreten, wenn immer komplexere Mengensysteme konstruiert werden sollen. (Beispiel: Ist die "Menge aller Mengen" eine sinnvolle Konstruktion oder nicht?) Zu Beginn des 20. Jahrhunderts schienen solche Probleme das Fundament der Mathematik ins Wanken zu bringen. (Ein Beispiel ist Russels Paradoxon, s. Abschnitt A.1.) Hierauf wurden große Anstrengungen unternommen, das Gebäude durch ein System von Axiomen zu retten (s. A.2). Wir werden diese Problematik nur streifen, z.B. bei der Konstruktion der (unendlichen) Menge der natürlichen Zahlen (vgl. A.3).

B.1 Russels Paradoxon

Kann man beliebige mathematische Objekte zu einem *Ensemble* zusammenfassen und dieses Ensemble eine *Menge* nennen? Dass dies nicht völlig problemlos ist, zeigt das folgende anschauliche Beispiel.

Wir betrachten die folgende Aussage

Der Barbier M. der Stadt B. rasiert (genau) alle Männer (von B.), welche sich nicht selbst rasieren.

Versuchen wir die Menge aller Männer zu bestimmen, welche von M. rasiert werden, so taucht schnell die Schwierigkeit auf zu entscheiden, ob M. in dieser Menge enthalten ist. Wohnt M. ebenfalls in B., so führt diese Frage zu einem Widerspruch. Keine Probleme ergeben sich dagegen, falls M. nicht in B. wohnt (wieso?).

Ähnliche Probleme treten auf, wenn wir das (mathematische) Universum als ein Mengensystem betrachten, wobei die Elemente aller Mengen ebenfalls Mengen sind und beliebige Mengen zu neuen Mengen zusammengefasst werden können. Beispielsweise könnte man versuchen Mengen zu konstruieren, welche sich selbst als Element enthalten. In welche Schwierigkeiten man in einem solchen Universum geraten kann, zeigt Russels Paradoxon.

¹(was nicht bedeutet, dass nicht schwierige Probleme auftreten können, beispielsweise in der Kombinatorik)

(B.1) Russells Paradoxon: Definiere $S := \{A \mid A \text{ ist Menge und } A \notin A\}$.

Ist S eine Menge? Falls ja: ist $S \in S$?

Annahme $S \in S$: es folgt $S \notin S$;

Annahme $S \notin S$: es folgt $S \in S$.

Auflösung des Widerspruchs: S ist keine Menge.

(B.2) Separationsaxiom: Gegeben sei eine Menge X und eine Eigenschaft P . Dann ist $\{x \mid x \in X \text{ und } x \text{ erfüllt } P\}$ eine Menge.

(Übung: Warum tritt hier Russells Paradoxon nicht in Erscheinung?)

B.2 Die Axiome²

- **Existenzaxiom:** Es gibt eine Menge.
- **Extensionalitätsaxiom:** Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente haben.
- **Aussonderungsaxiom:** Zu jeder Menge \mathbf{M} und jeder Aussage $\mathcal{A}(x)$ gibt es eine Menge \mathbf{A} , deren Elemente genau jene Elemente x von \mathbf{M} sind, für welche die Aussage $\mathcal{A}(x)$ wahr ist.
- **Paarbildungsaxiom:** Sind \mathbf{M} und \mathbf{N} Mengen, so gibt es stets eine Menge, welche genau \mathbf{M} und \mathbf{N} als Elemente enthält.
- **Vereinigungsmengenaxiom:** Zu jedem Mengensystem \mathcal{M} gibt es eine Menge, welche genau alle Elemente enthält, die zu mindestens einer Menge von \mathcal{M} gehören.
- **Potenzmengenaxiom:** Zu jeder Menge \mathbf{M} existiert ein Mengensystem \mathcal{M} , das genau alle Teilmengen von \mathbf{M} als Elemente enthält.

Unter dem **Nachfolger** \mathbf{X}^+ einer Menge \mathbf{X} verstehen wir die Menge $\mathbf{X}^+ := \mathbf{X} \cup \{\mathbf{X}\}$.

- **Unendlichkeitsaxiom:** Es gibt ein Mengensystem \mathcal{M} , das die leere Menge und mit einer Menge zugleich auch deren Nachfolger enthält.
- **Auswahlaxiom:** Das kartesische Produkt einer nichtleeren Familie von Mengen ist nicht leer.
- **Ersetzungsaxiom:** Es sei $\mathcal{A}(a, b)$ eine Aussage, so dass für jedes Element a einer Menge \mathbf{A} die Menge $\mathbf{M}(a) := \{b : \text{die Aussage } \mathcal{A}(a, b) \text{ ist wahr}\}$ gebildet werden kann. Dann existiert genau eine Funktion F mit dem Definitionsbereich \mathbf{A} , so dass $F(a) = \mathbf{M}(a)$ für alle $a \in \mathbf{A}$ gilt.

²vgl. z.B. Teubner-Taschenbuch der Mathematik, Teubner, 1996.

Anhang C: Die natürlichen Zahlen

C.1 Die mengentheoretische Begründung natürlicher Zahlen

Bei der Einführung der Menge \mathbb{N} der natürlichen Zahlen stoßen wir auf die folgenden prinzipiellen Probleme.

- P1:* Wie lassen sich Zahlen auf der Basis der Grundbegriffe der *Mengenlehre* einführen, da sie ihrer "Natur" nach doch völlig andere Objekte als Mengen sein sollten?
- P2:* \mathbb{N} soll offenbar eine *unendliche* Menge darstellen; nach welchem *Konstruktionsprinzip* können unendliche Mengen definiert werden? (Ganz sicher nicht durch explizite Aufzählung ihrer Elemente!)
- P3:* Wie lässt sich die *Existenz* der Menge \mathbb{N} widerspruchsfrei im Rahmen der Mengenlehre absichern?

Zu *P1:* Wir lassen uns von unserer intuitiven Vorstellung natürlicher Zahlen leiten und stellen jede Zahl n als (abkürzende Schreibweise für eine) eindeutig definierte n -elementige Menge dar. Dies geschieht am einfachsten durch die Zuordnung

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

Zu *P2:* Die Bildung der unendlichen Menge \mathbb{N} erfolgt nach einem Prinzip, welches in ähnlicher Form als **Induktionsprinzip** im Verlauf der Vorlesung Aussagen über unendliche Mengen ermöglicht. Die zugrundeliegenden Begriffe sind wie folgt.

Definition: (a) Ist M eine Menge, so sei der **Nachfolger** M^+ definiert durch $M^+ := M \cup \{M\}$.

(b) Eine Menge M heißt **induktiv**, wenn $\emptyset \in M$ und wenn M abgeschlossen bezüglich der Nachfolgeoperation ist, wenn also gilt: Ist $\alpha \in M$, so ist auch $\alpha^+ \in M$.

Wie Sie leicht nachprüfen können, ist der Nachfolger einer natürlichen Zahl n im intuitiven Sinn (also die Zahl $n+1$) gerade auch der Nachfolger im mengentheoretischen Sinn,

wenn natürliche Zahlen wie oben angegeben als Mengen interpretiert werden. Weiterhin wollen wir \mathbb{N} als induktive Menge definieren, denn sie soll ja \emptyset (also die Zahl 0) und mit jeder Zahl n auch den Nachfolger $n + 1$ enthalten.

Zu *P3*: Kann man sich \mathbb{N} als induktive Menge vorstellen, so ist es auch leicht, sich weitere, größere induktive Mengen vorzustellen. Wie kann \mathbb{N} als eindeutige induktive Menge definiert werden? Zunächst stellen wir fest, dass die Existenz mindestens einer induktiven Menge durch das Unendlichkeitsaxiom abgesichert ist. Weiterhin ist es nicht schwer zu zeigen, dass der Durchschnitt

$$\bigcap \{M \mid M \text{ ist induktiv}\}$$

über alle induktiven Mengen ebenfalls eine induktive Menge ist – sozusagen die "kleinste" existierende induktive Menge. Diese ist eindeutig definiert und eignet sich als Definition der Menge \mathbb{N} .

Genauer zum mengentheoretischen Aufbau der natürlichen Zahlen kann nachgelesen werden in [U. Friedrichsdorf und A. Prestel, Mengenlehre für den Mathematiker, Vieweg, 1985]. Für den Verlauf der Vorlesung genügen uns zur Charakterisierung der natürlichen Zahlen die "Peano-Axiome"; nach den bisherigen Ausführungen sind dies keine Axiome im eigentlichen Sinn, da sie für die oben skizzierte Konstruktion *bewiesen* werden können.