

Mathematik und Logik für Wirtschaftsinformatik  
2012W

V. Pillwein

January 30, 2013

# Contents

<b>1</b>	<b>Mengen</b>	<b>2</b>
<b>2</b>	<b>Logik</b>	<b>7</b>
2.1	Aussagenlogik . . . . .	7
2.2	Prädikatenlogik . . . . .	10
<b>3</b>	<b>Beweisen</b>	<b>17</b>
3.1	Modus Ponens . . . . .	17
3.2	Fallunterscheidung . . . . .	18
3.3	Induktionsbeweis . . . . .	20
3.4	Widerspruchsbeweis . . . . .	23
<b>4</b>	<b>Funktionen</b>	<b>25</b>
<b>5</b>	<b>Relationen</b>	<b>31</b>
5.1	Äquivalenzrelationen . . . . .	34
5.2	Ordnungsrelationen . . . . .	36
<b>6</b>	<b>Elementare Begriffe der Zahlentheorie</b>	<b>39</b>
6.1	Modulare Arithmetik . . . . .	39
6.2	Euklidischer Algorithmus und Diophantische Gleichungen . . . . .	42
6.3	Stellenwertsysteme . . . . .	47
<b>7</b>	<b>Algebren</b>	<b>49</b>
7.1	Algebraische Strukturen . . . . .	49
7.2	Abbildungen zwischen algebraischen Strukturen . . . . .	52
<b>8</b>	<b>Übungsaufgaben</b>	<b>53</b>

# 1 Mengen

Eine Menge ist eine Zusammenfassung von Objekten, wobei klar sein muss, ob ein Objekt zur Menge gehört oder nicht. Beispiele für Menge sind

- $M = \{1, 3, 7, 12, 47\}$
- $M = \{\text{rot, schwarz, blau}\}$
- $M = \{\Delta, \bigcirc, \spadesuit, \square, \diamond\}$

Diesen Beispielen ist gemeinsam, dass die Mengen aufzählend angegeben sind und die Mengen *endlich* sind. Die Reihenfolge der Objekte spielt in einer Menge keine Rolle, d.h.,  $\{a, b, c\} = \{c, b, a\}$ .

**Definition 1.1.** Die Objekte einer Menge  $M$  heissen Elemente von  $M$ . Wir schreiben  $m \in M$  für “ $m$  ist ein Element der Menge  $M$ ” und  $m \notin M$  für “ $m$  ist kein Element der Menge  $M$ ”.

Unendliche Mengen sind zum Beispiel die *natürlichen Zahlen*

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}.$$

Für die natürlichen Zahlen ohne 0 schreiben wir

$$\mathbb{N}^* = \{1, 2, 3, 4, \dots\}.$$

Die *ganzen Zahlen* bezeichnen wir mit

$$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}.$$

Mengen können aufzählend oder beschreibend angegeben werden. Zum Beispiel sei  $G$  die Menge der geraden natürlichen Zahlen (Beachte: 0 ist eine gerade Zahl!). Zuerst aufzählend gegeben:

$$G = \{0, 2, 4, 6, 8, 10, 12, \dots\},$$

Und beschreibend:

$$G = \{m \in \mathbb{N} \mid m \text{ ist gerade}\} \quad \text{oder} \quad G = \{2k \mid k \in \mathbb{N}\}.$$

Die *rationalen Zahlen* sind alle Zahlen, die sich als Bruch darstellen lassen

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}^* \right\}.$$

Die *reellen Zahlen* werden mit  $\mathbb{R}$  bezeichnet. Weiters verwenden wir

$$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}, \quad \mathbb{R}^- = \{x \in \mathbb{R} \mid x < 0\},$$

bzw.,

$$\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}, \quad \mathbb{R}_0^- = \{x \in \mathbb{R} \mid x \leq 0\}.$$

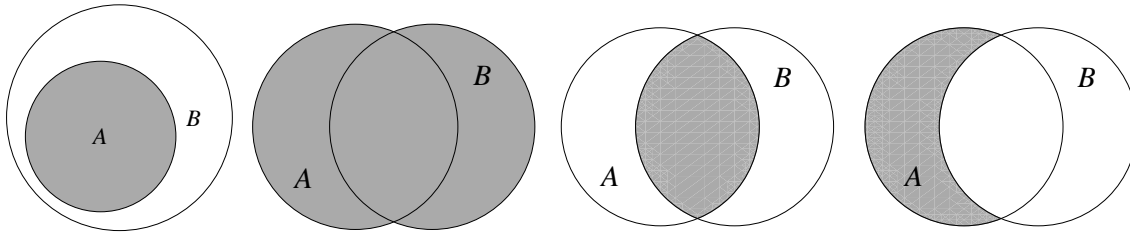


Abb. 1.1: von links nach rechts:  $A \subseteq B$ ,  $A \cup B$ ,  $A \cap B$  und  $A \setminus B$

Das *geschlossene Intervall*  $[a, b]$  für reelle Zahlen  $a, b$  bezeichnet die Menge aller reellen Zahlen, die grösser oder gleich als  $a$  und kleiner oder gleich als  $b$  sind, bzw. kurz:

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}.$$

Das *offene Intervall*  $]a, b[$  für reelle Zahlen  $a, b$  bezeichnet die Menge aller reellen Zahlen, die grösser als  $a$  und kleiner als  $b$  sind, bzw. kurz:

$$]a, b[ = \{x \in \mathbb{R} \mid a < x < b\}.$$

Analog werden die *halboffenen Intervalle*  $]a, b]$  und  $[a, b[$  wie folgt definiert

$$]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\} \quad \text{und} \quad [a, b[ = \{x \in \mathbb{R} \mid a \leq x < b\}.$$

**Definition 1.2.** 1. Die leere Menge ist jene Menge, die kein einziges Element besitzt; in Zeichen:  $\emptyset$  oder  $\{\}$

2. Eine Menge  $A$  heisst Teilmenge der Menge  $B$ , wenn jedes Element der Menge  $A$  auch ein Element der Menge  $B$  ist; in Zeichen:  $A \subseteq B$

3. Eine Menge  $A$  heisst Obermenge der Menge  $B$ , wenn  $B$  Teilmenge von  $A$  ist; in Zeichen:  $A \supseteq B$ .

4. Zwei Mengen  $A, B$  sind gleich genau dann wenn sowohl  $A \subseteq B$  als auch  $B \subseteq A$  gilt (d.h. sie enthalten die gleichen Elemente)

Für *echte* Teilmengen (Obermengen) wird das Zeichen  $\subsetneq$  (bzw.  $\supsetneq$ ) verwendet. Es gilt  $A \subseteq A$  und  $\emptyset \subseteq A$  für jede Menge  $A$ . Ausserdem gilt, falls  $A \subseteq B$  und  $B \subseteq C$ , dann ist auch  $A$  eine Teilmenge von  $C$ , d.h.,  $A \subseteq C$ . Eigenschaften von Mengen werden oft mittels *Venn Diagrammen* dargestellt, wie z.B. in Abbildung 1.1 links für  $A \subseteq B$ .

**Definition 1.3.** Seien  $A, B$  Mengen. Dann definieren wir

- die Vereinigung von  $A$  und  $B$  als die Menge, die alle Element enthält, die in  $A$  oder in  $B$  liegen in Zeichen:  $A \cup B$  (“ $A$  vereinigt  $B$ ”); d.h.,

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}.$$

- den Durchschnitt von  $A$  und  $B$  als die Menge, die alle Elemente enthält, die sowohl Element von  $A$  als auch Element von  $B$  sind, in Zeichen  $A \cap B$  (“ $A$  geschnitten  $B$ ”); d.h.:

$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}.$$

- die Differenzmenge von  $B$  in  $A$  als die Menge, die alle Element enthält, die in  $A$  aber nicht in  $B$  liegen, in Zeichen  $A \setminus B$  ("A ohne B"); d.h.:

$$A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}.$$

Zwei Mengen heissen disjunkt, wenn  $A \cap B = \emptyset$  gilt.

**Beispiel 1.4.** Seien  $A = \{1, 2, 3, 4, 5, 6\}$  und  $B = \{4, 5, 6, 7, 8\}$ , dann:

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\},$$

$$A \cap B = \{4, 5, 6\},$$

$$A \setminus B = \{1, 2, 3\}, \quad \text{und} \quad B \setminus A = \{7, 8\}.$$

**Beispiel 1.5.** Seien  $A = \mathbb{N}$  und  $B = \mathbb{Z}$ , dann:

$$A \cup B = \mathbb{Z}, \quad A \cap B = \mathbb{N}, \quad A \setminus B = \emptyset, \quad B \setminus A = \{\dots, -3, -2, -1\}.$$

**Beispiel 1.6.** Seien  $I_1 = [-1, 4]$ ,  $I_2 = [1.3, 2.8]$ ,  $I_3 = [2, 5]$ . Bestimme (a)  $I_2 \cap \mathbb{N}$  (b)  $I_1 \cup I_3$  (c)  $I_2 \cap I_3$  (d)  $I_1 \setminus I_2$ .

**Beispiel 1.7.** Seien  $A, B$  zwei Mengen für die gilt:  $A \subseteq B$ . Was ist (a)  $A \cup B$  (b)  $A \cap B$  (c)  $A \setminus B$  (d)  $B \setminus A$ ?

Einige Rechenregeln für die Mengenoperationen aus Definition 1.3 sind im folgenden Satz zusammengefasst. Aus diesen können andere Rechenregeln abgeleitet werden.

**Satz 1.8.** Seien  $A, B, C$  Mengen. Dann gilt:

(1)  $A \cup B = B \cup A$  und  $A \cap B = B \cap A$  (Kommutativgesetz)

(2)  $(A \cup B) \cup C = A \cup (B \cup C)$  und  $(A \cap B) \cap C = A \cap (B \cap C)$  (Assoziativgesetz)

(3)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  (Distributivgesetz)

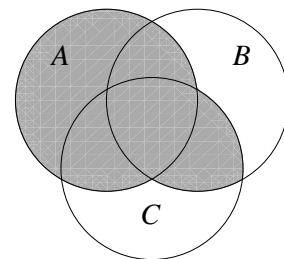
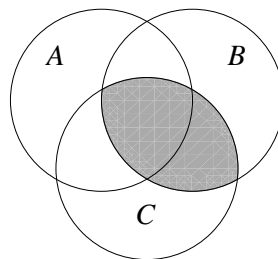
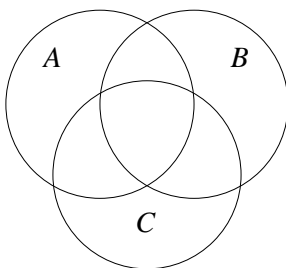
(4)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  (Distributivgesetz)

(5)  $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

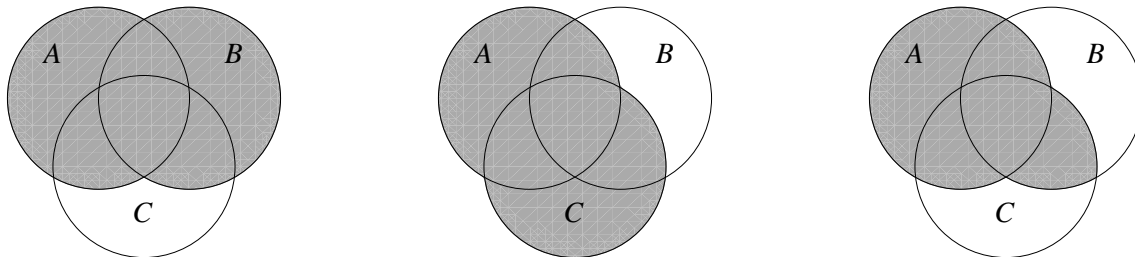
(6)  $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

*Beweis.* über Venn-Diagramme: die Venn-Diagramme für die rechte und die linke Seite der Identität müssen übereinstimmen. Wir betrachten den Beweis für das Distributivgesetz (3):

Für die linke Seite beginnen wir mit drei Mengen und zeichnen zunächst  $B \cap C$  ein und im zweiten Schritt bilden wir die Vereinigung davon mit  $A$ :



Für die rechte Seite bilden wir zunächst die beiden geklammerten Ausdrücke  $A \cup B$  und  $A \cup C$  und bilden dann den Durchschnitt:



□

**Beispiel 1.9.** Stellen mittels Venn-Diagrammen Sie fest, welche der folgenden Aussagen stimmen:

- $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$
- $(A \setminus B) \setminus C = A \setminus (B \setminus C)$

Eine weitere Operation auf Mengen ist die *Komplementbildung*. Sei  $A$  eine Menge, dann enthält das Komplement von  $A$  (in Zeichen  $A^c$ ) alle Objekte, die *nicht* in  $A$  liegen, d.h.,

$$A^c = \{x \mid x \notin A\}.$$

Mit dieser Notation gilt zum Beispiel

$$A \setminus B = A \cap B^c.$$

Oft ist die Grundmenge (das Universum) über der Mengen betrachtet werden bekannt. Wenn klar ist, über welcher fixen *Grundmenge*  $\Omega$  gerechnet wird, dann schreiben wir einfach

$$A^c = \Omega \setminus A.$$

In dem Sinn (mit  $A = \Omega$ ) können die Identitäten (5) und (6) aus Satz 1.8 auch so geschrieben werden:

$$(5a) \quad (B \cap C)^c = B^c \cup C^c$$

$$(6a) \quad (B \cup C)^c = B^c \cap C^c$$

**Definition 1.10.** Die Kardinalität (oder: Mächtigkeit) einer Menge  $M$  ist definiert als

$$|M| = \begin{cases} n, & \text{falls } M \text{ genau } n \text{ Elemente besitzt} \\ \infty, & \text{falls } M \text{ eine unendliche Menge ist.} \end{cases}$$

**Beispiel 1.11.**

$$|\{1, 3, 7, 12\}| = 4, \quad |\emptyset| = 0, \quad |\mathbb{N}| = \infty.$$

**Satz 1.12.** Für endliche Mengen  $A, B$  gilt:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

**Definition 1.13.** Sei  $A$  eine gegebene Menge. Die Potenzmenge (engl.: power set) von  $A$  (in Zeichen:  $P(A)$ ) ist die Menge aller Teilmengen von  $A$ :

$$P(A) = \{B \mid B \subseteq A\}.$$

**Beispiel 1.14.** Sei  $A = \{1, 2, 3\}$ , dann ist

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Es gilt immer  $\emptyset \in P(A)$  und  $A \in P(A)$ . Vorerst ohne Beweis notieren wir den folgenden

**Satz 1.15.** Sei  $A$  eine endliche Menge, dann gilt:  $|P(A)| = 2^{|A|}$ .

**Definition 1.16.** Seien  $A, B$  nichtleere Mengen. Die Produktmenge (oder das kartesische Produkt)  $A \times B$  von  $A$  und  $B$  ist definiert als

$$A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\}.$$

Die Elemente  $(a, b)$  in  $A \times B$  heissen Tupel oder geordnetes Paar. Zwei Tupel sind gleich, wenn sie in allen Komponenten übereinstimmen, d.h.,  $(a, b) = (c, d)$  genau dann, wenn  $a = c$  und  $b = d$ .

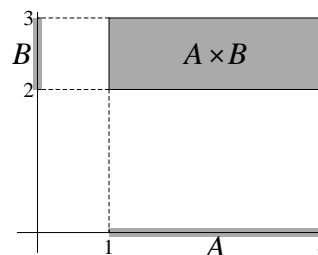
Falls  $B = A$  ist, dann schreibt man für die Produktmenge  $A \times A = A^2$ .

**Beispiel 1.17.** Sei  $A = \{a, b, c\}$  und  $B = \{1, 2\}$ . Dann ist

$$A \times B = \{(a, 1), (b, 1), (c, 1), (a, 2), (b, 2), (c, 2)\}.$$

**Beispiel 1.18.** Sei  $A = [1, 4]$  und  $B = [2, 3]$ . Dann ist

$$A \times B = \{(x, y) \mid 1 \leq x \leq 4 \text{ und } 2 \leq y \leq 3\}.$$



**Definition 1.19.** Produktmengen können auch aus mehr als zwei Mengen gebildet werden und analog gilt

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Die Elemente dieser Produktmenge werden  $n$ -Tupel (oder nur Tupel) genannt. Zwei Tupel  $(a_1, a_2, \dots, a_n)$  und  $(b_1, b_2, \dots, b_n)$  sind gleich, wenn sie in allen Komponenten übereinstimmen, d.h., wenn für alle Indizes  $k = 1, \dots, n$  gilt, dass  $a_k = b_k$ .

Wenn  $A_1 = A_2 = \cdots = A_n = A$  gilt, dann wird die Produktmenge wieder kurz mit  $A^n$  bezeichnet.

**Bemerkung 1.20.** Für endliche Mengen  $A, B$  gilt:  $|A \times B| = |A| \cdot |B|$ .

## 2 Logik

### 2.1 Aussagenlogik

Eine *Aussage* ist jeder Satz (der Umgangssprache), dem die Eigenschaft *wahr* oder *falsch* zugesprochen werden kann.

Beispiele für Aussagen sind

- Meine Haare sind schwarz.
- $3^3 = 81$
- $-1 < 14$
- Die letzte Stelle der 247. Primzahl ist 3.

Keine Aussagen sind

- Ist  $\pi$  eine ganze Zahl?
- $(a + b)^2$

Aus gegebenen Aussagen können durch Negation oder Verknüpfungen (Junktoren) neue Aussagen gebildet werden.

**Negation** (Symbol:  $\neg$ ) Gegeben eine Aussage  $A$ , dann ist  $\neg A$  ("nicht  $A$ ") die Aussage, die genau dann wahr ist, wenn  $A$  falsch ist und genau dann falsch ist, wenn  $A$  wahr ist.

Wahrheitstafel:

$A$	$\neg A$
W	F
F	W

**Konjunktion (UND)** (Symbol:  $\wedge$ ) Seien  $A, B$  Aussagen, dann ist  $A \wedge B$  (" $A$  und  $B$ ") die Aussage, die genau dann wahr ist, wenn  $A$  und  $B$  wahr sind.

Wahrheitstafel:

$A$	$B$	$A \wedge B$
W	W	W
W	F	F
F	W	F
F	F	F

Wahrheitstafel:

$A$	$B$	$A \vee B$
W	W	W
W	F	W
F	W	W
F	F	F

**Disjunktion (ODER)** (Symbol:  $\vee$ ) Seien  $A, B$  Aussagen, dann ist  $A \vee B$  (" $A$  oder  $B$ ") die Aussage, die genau dann wahr ist, wenn mindestens eine der beiden Aussagen  $A, B$  wahr ist.

Konjunktion und Disjunktion sind *kommutativ* und *assoziativ*, d.h.,

$$A \wedge B = B \wedge A \quad \text{und} \quad A \vee B = B \vee A,$$



und

$$(A \wedge B) \wedge C = A \wedge (B \wedge C) \quad \text{und} \quad (A \vee B) \vee C = A \vee (B \vee C).$$

Was aber bedeute “gleich” (oder “äquivalent”) für Aussagen? Im Moment können wir Gleichheit von Aussagen überprüfen, indem wir die Wahrheitstafeln für jede Seite bestimmen und vergleichen. Zwei Aussagen sind gleich, wenn sie für alle möglichen Eingaben (gibt nur endlich viele Möglichkeiten), den gleichen Wahrheitswert haben.

**Beispiel 2.1.** *Wir zeigen  $(A \wedge B) \wedge C = A \wedge (B \wedge C)$  und bestimmen dazu die Wahrheitstafeln für beide Seiten.*

$A$	$B$	$C$	$A \wedge B$	$(A \wedge B) \wedge C$	$A$	$B$	$C$	$B \wedge C$	$A \wedge (B \wedge C)$
W	W	W	W	W	W	W	W	W	W
W	W	F	W	F	W	W	F	F	F
W	F	W	F	F	W	F	W	F	F
W	F	F	F	F	W	F	F	F	F
F	W	W	F	F	F	W	W	W	F
F	W	F	F	F	F	W	F	F	F
F	F	W	F	F	F	F	W	F	F
F	F	F	F	F	F	F	F	F	F

Mithilfe von Negation, Konjunktion und Disjunktion können Komplement, Durchschnitt und Vereinigung von Mengen auch wie folgt geschrieben werden: Seien  $A, B$  Mengen, dann gilt

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

Für Mengen haben wir unter anderem das Distributivgesetz (Satz 1.8(3))

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

für Mengen  $A, B, C$  gezeigt. Analog gilt für Aussagen  $A, B, C$

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$

Wir zeigen diese Aussage jetzt über Wahrheitstafeln:

$A$	$B$	$C$	$B \wedge C$	$A \vee (B \wedge C)$	$A$	$B$	$C$	$A \vee B$	$A \vee C$	$(A \vee B) \wedge (A \vee C)$
W	W	W	W	W	W	W	W	W	W	W
W	W	F	F	W	W	W	F	W	W	W
W	F	W	F	W	W	F	W	W	W	W
W	F	F	F	W	W	F	F	W	W	W
F	W	W	W	W	F	W	W	W	W	W
F	W	F	F	F	F	W	F	W	F	F
F	F	W	F	F	F	F	W	F	W	F
F	F	F	F	F	F	F	F	F	F	F

**Satz 2.2.** *Seien  $A, B, C$  Aussagen, dann gelten die Distributivgesetze*

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$

und

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$

Die Aussagen (5) und (6) aus Satz 1.8 betrachten wir die alternativen Formulierungen (5a) und (6a):

$$(5a) \quad (B \cap C)^c = B^c \cup C^c$$

$$(6a) \quad (B \cup C)^c = B^c \cap C^c$$

Ihre Entsprechungen für Aussagen sind die *Gesetze von De Morgan*.

**Satz 2.3.** (De Morgan) Seien  $A, B$  Aussagen. Dann gilt

$$\neg(A \wedge B) = \neg A \vee \neg B \tag{2.1}$$

und

$$\neg(A \vee B) = \neg A \wedge \neg B \tag{2.2}$$

*Beweis.* Wir zeigen (2.1) mittels Wahrheitstafeln, der Beweis zu (2.2) geht analog.

$A$	$B$	$A \wedge B$	$\neg(A \wedge B)$
W	W	W	F
W	F	F	W
F	W	F	W
F	F	F	W

$A$	$B$	$\neg A$	$\neg B$	$\neg A \vee \neg B$
W	W	F	F	F
W	F	F	W	W
F	W	W	F	W
F	F	W	W	W

□

**Implikation** (Symbol:  $\Rightarrow$ ) Seien  $A, B$  Aussagen, dann ist  $A \Rightarrow B$  (“ $A$  impliziert  $B$ ” oder “aus  $A$  folgt  $B$ ”) die Aussage, die genau dann *falsch* ist, wenn  $A$  wahr und  $B$  falsch ist.

Wahrheitstafel:

$A$	$B$	$A \Rightarrow B$
W	W	W
W	F	F
F	W	W
F	F	W

**Äquivalenz** (Symbol:  $\Leftrightarrow$ ) Seien  $A, B$  Aussagen, dann ist  $A \Leftrightarrow B$  (“ $A$  äquivalent zu  $B$ ” oder “ $A$  genau dann wenn  $B$ ”) die Aussage, die genau dann wahr ist, wenn  $A$  und  $B$  beide wahr sind oder beide falsch sind.

Wahrheitstafel:

$A$	$B$	$A \Leftrightarrow B$
W	W	W
W	F	F
F	W	F
F	F	W

Zwei logische Aussagen sind also gleich, wenn sie äquivalent sind. Zwei Aussagen  $A, B$  sind äquivalent wenn  $B$  aus  $A$  folgt und  $A$  aus  $B$  folgt, d.h.,

$$A \Leftrightarrow B = (A \Rightarrow B) \wedge (B \Rightarrow A).$$

Auch diese Aussage kann mittels Wahrheitstafeln bewiesen werden.

**Beispiel 2.4.** Was ist die Wahrheitstafel von  $\neg A \vee B$ ?

$A$	$B$	$\neg A$	$\neg A \vee B$
$W$	$W$	$F$	$W$
$W$	$F$	$F$	$F$
$F$	$W$	$W$	$W$
$F$	$F$	$W$	$W$

Wenn wir mit oben vergleichen, sieht man, dass diese Aussage zu  $A \Rightarrow B$  äquivalent ist. Damit haben wir eine weitere Umformungsregel:

**Lemma 2.5.** *Seien  $A, B$  Aussagen. Dann gilt:  $A \Rightarrow B = \neg A \vee B$ .*

**Beispiel 2.6.** *Zeigen Sie, dass  $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$  einmal mittels Wahrheitstafeln und einmal durch Anwenden von Umformungsregeln.*

**Beispiel 2.7.** *Seien  $A, B$  Aussagen: Die Aussage  $\neg(A \Rightarrow B)$  kann durch Anwenden von Umformungsregeln so expandiert werden, dass sie nur mittels  $\neg, \vee, \wedge$  ausgedrückt wird:*

$$\neg(A \Rightarrow B) \Leftrightarrow \neg(\neg A \vee B) \Leftrightarrow A \wedge \neg B.$$

**Definition 2.8.** *Aussagen, die immer wahr sind heissen Tautologie. Aussagen, die immer falsch sind heissen Kontradiktion.*

Ein einfaches Beispiel für eine Tautologie ist  $A \vee (\neg A)$ , ein einfaches Beispiel für eine Kontradiktion ist  $A \wedge (\neg A)$ .

**Beispiel 2.9.** *Welche der folgenden Aussagen sind Tautologien, Kontradiktionen oder weder noch?*

- $A \vee (A \Rightarrow B)$
- $(A \Rightarrow \neg A) \wedge A$
- $(A \Rightarrow \neg B) \wedge (A \Rightarrow B)$
- $(A \wedge (A \Rightarrow B)) \Rightarrow B$

## 2.2 Prädikatenlogik

Ein Beispiel für eine Aussage ist  $A \equiv -1 < 14$ . Wenn die Konstante  $-1$  durch eine Variable ersetzt wird, d.h., wenn wir

$$A(x) \equiv x < 14$$

betrachten, dann erhalten wir die *parametrisierte Aussage* (das Prädikat) “ $x$  ist kleiner als 14”. Für eine spezielle Wahl von  $x$  erhalten wir wieder eine Aussage, zum Beispiel für  $x = 1$ ,  $A(1) \equiv 1 < 14$  (wahr) oder  $x = 27$ ,  $A(27) \equiv 27 < 14$  (falsch). Die *Variable*  $x$  kommt *frei* vor.

**Beispiel 2.10.** •  $G(x) \equiv x$  ist gerade. Dann ist  $G(2) \equiv W$  und  $G(27) \equiv F$ .

- Die Eigenschaft “ist rot”, also  $ist\_rot(x)$ . Zum Beispiel

$$ist\_rot(Blut) \equiv W \quad \text{und} \quad ist\_rot(Banane) \equiv F$$

- $A(x, M) \equiv x \in M$  ist eine parametrisierte Aussage, die von zwei freien Variablen abhängt.

Negation, Konjunktion, Disjunktion von parametrisierten Aussagen sind wieder parametrisierte Aussagen. Zum Beispiel sei  $A(x) \equiv 1 \leq x$  und  $B(x) \equiv x < 7$ , dann ist

$$A(x) \wedge B(x) \equiv 1 \leq x \wedge x < 7.$$

Üblicherweise verwenden wir für dieses Prädikat die Kurzschreibweise

$$1 \leq x < 7 \quad \text{oder} \quad x \in [1, 7[.$$

Die Negation von  $A(x)$  ist

$$\neg A(x) \Leftrightarrow \neg(1 \leq x) \Leftrightarrow 1 > x.$$

**Beispiel 2.11.** Sei  $A(x) \equiv x \geq \frac{1}{3}$  und  $B(x) \equiv x \geq 1$ . Was ist (a)  $\neg A(x)$  (b)  $A(x) \wedge \neg B(x)$  (c)  $B(x) \Rightarrow A(x)$ ? Für welche Wahl von  $x$  ist (a) wahr? Für welche (b)? Für welche (c)?

Ein weiteres Beispiel ist die folgende parametrisierte Aussage, in der die Variable  $x$  frei vorkommt:

$$A(x) \equiv (x \in \mathbb{N} \implies x > -1). \quad (2.3)$$

In Worten: “wenn  $x$  eine natürliche Zahl ist, dann ist  $x$  grösser als  $-1$ “. Diese Aussage ist für alle  $x$  wahr und um *Allaussagen* mathematisch beschreiben zu können wird der *Allquantor*  $\forall$  verwendet:

$$B \equiv \forall x: x \in \mathbb{N} \implies x > -1 \quad (2.4)$$

bedeutet “Für alle  $x$  gilt, wenn  $x$  eine natürliche Zahl ist, dann ist sie grösser als  $-1$ “. Mit  $A(x)$  wie oben, lautet die Aussage kurz  $\forall x: A(x)$ . Die Aussage  $B$  enthält keine freien Variablen. Die Variable  $x$  ist durch den Allquantor *gebunden*.

**Beispiel 2.12.** Was sind die gebundenen bzw. die freien Variablen der folgenden Aussagen:

- $x \in \mathbb{N} \wedge y \in \mathbb{R} \Rightarrow -y^2 \leq x$
- $\forall x: x \in \mathbb{N} \wedge y \in \mathbb{N} \Rightarrow x + y \in \mathbb{N}$
- $\forall x: x \in \mathbb{R} \wedge -1 \leq x \leq 1 \Rightarrow x^2 \geq 1$

$B$  in (2.4) ist also eine Aussage, die einen eindeutig bestimmten Wahrheitsgehalt hat, d.h.,  $B$  ist entweder wahr oder falsch. Um festzustellen, ob  $B$  wahr ist, muss die Aussage bewiesen werden. Dazu geht man wie folgt vor:

1. Sei  $x$  beliebig.
2. Angenommen  $x \in \mathbb{N}$
3. zu zeigen ist:  $x > -1$

**Beispiel 2.13.** (a) “Jede natürliche Zahl ausser 0 ist kleiner als ihr Dreifaches.” Diese Aussage mit Quantoren formuliert:

$$B \equiv \forall x: x \in \mathbb{N} \wedge x \neq 0 \implies x < 3x.$$

Der quantorfreie Teil dieser Aussage ist

$$A(x) \equiv x \in \mathbb{N} \wedge x \neq 0 \quad \Rightarrow \quad x < 3x.$$

Welchen Wahrheitswert nimmt  $A(x)$  an für (1)  $x = 2$  (2)  $x = 0$  (3)  $x = \pi$ ? Was ist der Wahrheitswert von  $B$ ?

- (b) “Alle Vögel im Uniteich sind Schwäne.” Wir führen die Prädikate  $ist\_Vogel(x)$ ,  $im\_Uniteich(x)$  und  $ist\_Schwan(x)$  ein und können die Aussage mit Quantoren so anschreiben:

$$B \equiv \forall x: ist\_Vogel(x) \wedge im\_Uniteich(x) \quad \Rightarrow \quad ist\_Schwan(x).$$

Der quantorfreie Teil dieser Aussage ist das Prädikat

$$A(x) \equiv ist\_Vogel(x) \wedge im\_Uniteich(x) \quad \Rightarrow \quad ist\_Schwan(x).$$

Welchen Wahrheitswert hat  $A(x)$  wenn wir für  $x$  (1) Schildkröte (2) Ente (3) Schwan einsetzen? Welchen Wahrheitswert hat die Aussage  $B$ ?

- (c) “Das Quadrat jeder reellen Zahl ist grösser als diese Zahl.” Diese Aussage mit Quantoren formuliert:

$$B \equiv \forall x: x \in \mathbb{R} \quad \Rightarrow \quad x^2 > x.$$

Der quantorfreie Teil dieser Aussage ist das Prädikat

$$A(x) \equiv x \in \mathbb{R} \quad \Rightarrow \quad x^2 > x.$$

Für welche Werte von  $x$  ist die parametrisierte Aussage  $A(x)$  wahr? Was ist der Wahrheitswert von  $B$ ?

Was ist die Negation einer Allaussage? Betrachten wir die Aussage aus Beispiel 2.13(b): “Alle Vögel im Uniteich sind Schwäne”. Das Gegenteil davon ist “Es gibt mindestens einen Vogel im Uniteich, der kein Schwan ist”. Um diese Aussage mathematisch beschreiben zu können benötigen wir den *Existenzquantor*:

$$\exists x: ist\_Vogel(x) \wedge im\_Uniteich(x) \wedge \neg(ist\_Schwan(x)).$$

Die Variable  $x$  ist hier durch den Existenzquantor *gebunden*. Die Negation der Aussage in Beispiel 2.13(c) ist “Es gibt eine reelle Zahl, die kleiner oder gleich ist als ihr Quadrat” oder in Quantorenschreibweise

$$\exists x: x \in \mathbb{R} \wedge \neg(x^2 > x) \quad \Leftrightarrow \quad \exists x: x \in \mathbb{R} \wedge x^2 \leq x.$$

Wir fassen die beiden Quantoren noch einmal zusammen.

**Definition 2.14.** (*Allaussagen und Existenzaussagen*)

- Die Aussage “Für alle  $x$  gilt  $P(x)$ ” ist wahr genau dann, wenn für alle  $x$  die Eigenschaft (das Prädikat)  $P(x)$  wahr ist. In Quantorenschreibweise:  $\forall x: P(x)$ . Das Symbol  $\forall$  heisst Allquantor. Wenn  $P(x)$  von der Form  $A(x) \Rightarrow B(x)$  ist, dann schreibt man auch kurz

$$\forall x: A(x) \Rightarrow B(x) \quad \Leftrightarrow \quad \forall x, A(x): B(x).$$

- Die Aussage “Es gibt (mindestens) ein  $x$ , sodass  $P(x)$ ” (oder “Es existiert (mindestens) ein  $x$ , sodass  $P(x)$ ”) ist wahr genau dann, wenn  $P(x)$  für zumindest ein  $x$  wahr ist. In Quantorenschreibweise:  $\exists x: P(x)$ . Das Symbol  $\exists$  heisst Existenzquantor. Wenn  $P(x)$  von der Form  $A(x) \wedge B(x)$  ist, dann schreibt man auch kurz

$$\exists x: A(x) \wedge B(x) \quad \Leftrightarrow \quad \exists x, A(x): B(x).$$

- All- und Existenzaussagen werden wie folgt negiert:

$$\neg(\forall x: P(x)) \quad \Leftrightarrow \quad \exists x: \neg P(x) \quad \text{und} \quad \neg(\exists x: P(x)) \quad \Leftrightarrow \quad \forall x: \neg P(x).$$

Um zu zeigen, dass eine Existenzaussage wahr ist, reicht es also eine *Wahl* des Parameters (*Instanz*) zu finden, die den quantorfreien Teil der Aussage erfüllt. Zurück zum letzten Beispiel: Die Aussage

$$\exists x: x \in \mathbb{R} \wedge x^2 \leq x$$

ist somit wahr, da zum Beispiel für die Wahl  $x = 0$  gilt

$$0 \in \mathbb{R} \wedge 0^2 \leq 0,$$

da  $0^2 = 0$  gilt. Um zu zeigen, dass eine Allaussage *falsch* ist, genügt es zu zeigen, dass ihre Negation *wahr* ist, d.h. es reicht ein *Gegenbeispiel* zu finden.

Bei der Negation von quantifizierten Aussagen in der Kurzschreibweise

$$\forall x, A(x): B(x) \quad \text{und} \quad \exists x, A(x): B(x)$$

ist zu beachten, dass das Prädikat beim Quantor *nicht* verändert wird, also

$$\neg(\forall x, A(x): B(x)) \quad \Leftrightarrow \quad \exists x, A(x): \neg B(x) \quad \text{und} \quad \neg(\exists x, A(x): B(x)) \quad \Leftrightarrow \quad \forall x, A(x): \neg B(x).$$

**Beispiel 2.15.** Sei  $A \equiv \forall x, x \in \mathbb{R}: x^2 < 0$ . Wir bestimmen die Negation dieser Aussage:

$$\begin{aligned} \neg A &\Leftrightarrow \neg(\forall x, x \in \mathbb{R}: x^2 < 0) \\ &\Leftrightarrow \neg(\forall x: x \in \mathbb{R} \implies x^2 < 0) \\ &\Leftrightarrow \exists x: \neg(x \in \mathbb{R} \implies x^2 < 0) \\ &\Leftrightarrow \exists x: \neg(\neg(x \in \mathbb{R}) \vee (x^2 < 0)) \\ &\Leftrightarrow \exists x: (x \in \mathbb{R}) \wedge \neg(x^2 < 0) \\ &\Leftrightarrow \exists x: (x \in \mathbb{R}) \wedge (x^2 \geq 0) \\ &\Leftrightarrow \exists x, x \in \mathbb{R}: x^2 \geq 0. \end{aligned}$$

Der quantorfreie Teil dieser Aussage ist zum Beispiel für  $x = 0$  erfüllt, d.h.,  $\neg A$  ist wahr, damit ist die ursprüngliche Aussage falsch.

Um zwischen “es existiert (mindestens) ein” und “es existiert *genau* ein” zu unterscheiden wird der Quantor  $\exists!$  verwendet, z.B.,

$$\exists! x \in \mathbb{R}: x = -x^2.$$

**Beispiel 2.16.** Formulieren Sie die folgenden Aussagen mit Quantoren:

- (a) Es gibt eine ganze Zahl, deren Quadrat 16 ist.
- (b) Alle Katzen sind grau.
- (c) Reelle Zahlen sind genau dann grösser als eins, wenn ihre Kuben grösser als eins sind.
- (d) Es gibt natürliche Zahlen, die gerade sind.

Antwort zu (d): Wir definieren die parametrisierte Aussage

$$G(x) \equiv x \text{ ist eine gerade Zahl.}$$

Damit erhalten wir als Lösung

$$\exists x: x \in \mathbb{N} \wedge G(x)$$

bzw., in Kurzschreibweise,

$$\exists x \in \mathbb{N}: G(x).$$

Quantoren können auch *kombiniert* werden. Die Aussage (d) im letzten Beispiel kann umgeschrieben werden, wenn wir uns überlegen, was es bedeutet für eine Zahl gerade zu sein: Eine gerade natürliche Zahl ist durch 2 teilbar, oder anders gesagt,  $x \in \mathbb{N}$  ist gerade, wenn ein  $y \in \mathbb{N}$  gefunden werden kann, sodass  $x = 2y$ . In Quantorenschreibweise erhalten wir so:

$$\exists x: x \in \mathbb{N} \wedge (\exists y: y \in \mathbb{N} \wedge x = 2y)$$

oder kürzer

$$\exists x, x \in \mathbb{N}: (\exists y, y \in \mathbb{N}: x = 2y)$$

oder noch kürzer

$$\exists x \in \mathbb{N} \exists y \in \mathbb{N}: x = 2y.$$

Wenn, wie in diesem Beispiel, alle Quantoren vom gleichen Typ sind, dann kann die Reihenfolge der Quantoren vertauscht werden, d.h., wir können die Aussage auch so schreiben

$$\exists y \in \mathbb{N} \exists x \in \mathbb{N}: x = 2y$$

und daher werden die Inhalte von Existenzquantoren häufig zusammengezogen:

$$\exists x, y \in \mathbb{N}: x = 2y.$$

Betrachten wir ein Beispiel von kombinierten Allquantoren: “Das Produkt zweier beliebiger natürlicher Zahlen ist positiv”:

$$\forall x: x \in \mathbb{N} \Rightarrow (\forall y: y \in \mathbb{N} \Rightarrow xy \geq 0)$$

Wir kürzen ab:

$$\forall x \in \mathbb{N}: (\forall y \in \mathbb{N}: xy \geq 0)$$

und kürzen weiter:

$$\forall x \in \mathbb{N} \forall y \in \mathbb{N}: xy \geq 0.$$

Auch für Allquantoren gilt (da sie vom gleichen Typ sind), dass die Reihenfolge vertauscht werden kann. Daher ist die obige Aussage gleich zu

$$\forall y \in \mathbb{N} \forall x \in \mathbb{N}: xy \geq 0$$

und man zieht die Inhalte von hintereinander stehenden Allquantoren oft zusammen, z.B.,

$$\forall x, y \in \mathbb{N}: xy \geq 0.$$

Die Reihenfolge von Existenzquantor und Allquantor darf *nicht* vertauscht werden - nur hintereinander ausgeführte Quantoren vom *selben* Typ dürfen vertauscht oder zusammengezogen werden. Wir betrachten ein einfaches Beispiel:

$$A \equiv \text{Zu jeder reellen Zahl gibt es eine grössere reelle Zahl.}$$

Zunächst übersetzen wir diese Aussage in Quantoren:

$$A \equiv \forall x \in \mathbb{R} \exists y \in \mathbb{R}: x < y.$$

*Frage:* Ist diese Aussage wahr oder falsch?

*Antwort:* Wir arbeiten die Quantoren von links nach rechts ab. Wir beginnen mit dem Allquantor: Sei  $x \in \mathbb{R}$  beliebig. Dann ist zu zeigen, dass für dieses beliebige (aber fixe)  $x$  eine reelle Zahl existiert, die grösser ist, die als *eine* Instanz von  $y$  gewählt werden kann. Wenn wir auf Schulwissen zurückgreifen, dann wissen wir, dass wenn  $x \in \mathbb{R}$  ist, dann ist auch  $x + 1 \in \mathbb{R}$  und  $x < x + 1$ . D.h., zu beliebigem, aber fixem,  $x$  ist  $y = x + 1$  eine Wahl, die  $x < y$  erfüllt.

Jetzt vertauschen wir die Reihenfolge der Quantoren und betrachten die Aussage:

$$\tilde{A} \equiv \exists y \in \mathbb{R} \forall x \in \mathbb{R}: x < y.$$

In Worten: Es gibt eine reelle Zahl, die grösser ist als jede andere reelle Zahl. Anders gesagt: es gibt eine grösste reelle Zahl. Das ist nicht nur eine andere Aussage als  $A$ , es klingt auch falsch. Um zu zeigen, dass  $\tilde{A}$  tatsächlich falsch ist gehen wir wie oben vor und beweisen, dass die Negation wahr ist. Wir negieren die Aussage schrittweise:

$$\begin{aligned} & \neg(\exists y \in \mathbb{R} \forall x \in \mathbb{R}: x < y) \\ \Leftrightarrow & \forall y \in \mathbb{R}: \neg(\forall x \in \mathbb{R}: x < y) \\ \Leftrightarrow & \forall y \in \mathbb{R}: \exists x \in \mathbb{R}: \neg(x < y) \\ \Leftrightarrow & \forall y \in \mathbb{R}: \exists x \in \mathbb{R}: \neg x \geq y. \end{aligned}$$

Der Beweis dieser Aussage kann analog zum Beweis von  $A$  durchgeführt werden.

**Beispiel 2.17.** Gegeben ist die folgenden Aussage: “Für alle natürlichen Zahlen gilt, dass sie entweder gerade sind, oder ungerade, aber nicht beides”. (a) Geben Sie die Aussage mit Quantoren an. (b) Negieren Sie die quantifizierte Aussage. (c) Formulieren Sie die Negation als Satz in der Umgangssprache.

Man beachte, dass bei Quantoren oft versteckt vorkommen, wie zum Beispiel in Satz 1.15: “Sei  $A$  eine endliche Menge, dann gilt:  $|P(A)| = 2^{|A|}$ ”. Gemeint ist, dass für jede endliche Menge  $A$ , die Kardinalität der Potenzmenge 2 hoch der Kardinalität der Menge ist. In Quantorenschreibweise:

$$\forall A, \text{ist\_Menge}(A) \wedge |A| < \infty: |P(A)| = 2^{|A|}.$$

Oft wird die Einschränkung auf (z.B. hier) Mengen im Text gemacht: Für Mengen gilt

$$\forall A, |A| < \infty: |P(A)| = 2^{|A|}.$$

Bei Aussagen wie dieser muss aus dem Kontext der Bereich aus dem die Variablen gewählt werden klar sein.



**Beispiel 2.18.** *Wir betrachten die Aussage*

$$\forall \varepsilon, \varepsilon \in \mathbb{R}^+ \exists n_\varepsilon, n_\varepsilon \in \mathbb{N} \forall n, n \in \mathbb{N} \wedge n \geq n_\varepsilon: \left| \frac{3-n}{n^2} \right| < \varepsilon.$$

*Wenn aus dem Kontext klar ist (d.h., wenn irgendwo steht), dass  $\varepsilon \in \mathbb{R}$  und  $n, n_\varepsilon \in \mathbb{N}$ , dann schreibt man auch kürzer:*

$$\forall \varepsilon > 0 \exists n_\varepsilon \forall n \geq n_\varepsilon: \left| \frac{3-n}{n^2} \right| < \varepsilon.$$

*Beschreiben Sie in Worten, was diese Formel aussagt. Wie lautet die Negation dieser Aussage?*

### 3 Beweisen

Der Zweck von Beweisen ist ausgehend von Aussagen, die in einer bestimmten Realität gelten, die Gültigkeit einer Aussage in derselben Realität zu erschliessen. Dabei muss jeder Schlußschritt abstrakt, korrekt und kontrollierbar sein.

Ein *Beweis* einer Aussage  $A$  mit Hilfe eines “Grundwissens” (über der betrachteten) Realität) ist eine Folge von Aussagen, wobei jede Aussage der Folge entweder aus dem Grundwissen ist oder aus den vorherigen Aussagen der Folge in einem Schlußschritt entsteht und die letzte Aussage dieser Folge  $A$  ist.

Das Grundwissen besteht zum Beispiel aus früher bewiesenen Aussagen, aus allgemeingültigen Aussagen, Definitionen, usw. Die Beweisschritte sollen nicht zu gross sein (damit der Beweis nachvollziehbar bleibt) und nicht zu klein (damit der Beweis überschaubar bleibt).

Um eine Aussage zu beweisen (oder zu widerlegen) muss man sich zunächst klar darüber sein, was die *Voraussetzungen* sind und was zu zeigen ist. Eine zu zeigende Aussage  $A$  kann aus dem Grundwissen (inklusive der Voraussetzungen) hergeleitet werden (zum Beispiel indem es durch Äquivalenzumformungen auf bekanntes Wissen zurückgeführt wird). Eine Aussage kann *indirekt* bewiesen werden, indem ihre Negation ( $\neg A$ ) mit dem Grundwissen auf einen Widerspruch geführt wird. Um eine Aussage zu widerlegen, kann man versuchen  $\neg A$  aus dem Grundwissen zu beweisen oder die Aussage (mit Hilfe des Grundwissens) auf einen Widerspruch führen.

Wir betrachten verschiedene grundlegende Beweistechniken, die auch kombiniert werden können. Bei den ersten drei Arten handelt es sich um direkte Beweise.

#### 3.1 Modus Ponens

Gegeben sind zwei Aussagen  $A, B$ . Angenommen  $A$  gilt und  $B$  kann (durch Umformen) aus  $A$  abgeleitet werden, dann gilt  $B$ , wenn  $A$  erfüllt ist, d.h.,

$$(A \wedge (A \Rightarrow B)) \Rightarrow B.$$

$A$  ist in diesem Fall die Voraussetzung, oder Hypothese und  $B$  die Schlussfolgerung oder Konklusion.

Wir betrachten ein konkretes Beispiel und definieren dazu zuerst den Begriff *Teilbarkeit*.

**Definition 3.1.** Seien  $a, b$  ganze Zahlen. Wir sagen, dass  $a$  teilt  $b$ , wenn eine ganze Zahl  $q$  existiert so dass  $b = aq$ . In Zeichen  $a \mid b$ .

**Satz 3.2.** Für natürliche Zahlen  $x, y, z \in \mathbb{N}$  gilt, dass wenn  $z$  sowohl  $x$  als auch  $y$  teilt, dann teilt  $z$  auch die Summe  $x + y$  und das Produkt  $xy$ .

Mit Quantoren angeschrieben lautet die Aussage:

$$\forall x, y, z \in \mathbb{N}: z \mid x \wedge z \mid y \implies z \mid x + y \wedge z \mid xy$$

*Beweis.* Seien  $x, y, z$  natürliche Zahlen. Angenommen  $z \mid x$  und  $z \mid y$ . Zu zeigen ist, dass  $z$  dann auch die Summe und das Produkt von  $x$  und  $y$  teilt.

Nach Definition wissen wir, dass wenn  $z \mid x$  ein  $q \in \mathbb{N}$  existiert mit der Eigenschaft  $x = qz$ . Analog folgt, dass wenn  $z \mid y$ , dass ein  $r \in \mathbb{N}$  existiert mit  $y = rz$ . Seien also  $q, r$  diese Zahlen. Dann gilt für die Summe

$$x + y = qz + rz = (q + r)z.$$

Wenn  $q, r \in \mathbb{N}$ , dann ist auch  $q + r \in \mathbb{N}$ . Aus der Definition von Teilbarkeit folgt damit, dass  $x + y$  durch  $z$  teilbar ist. Für das Produkt gilt

$$xy = qz \cdot rz = (qrz)z.$$

Da  $q, r, z \in \mathbb{N}$  ist auch deren Produkt  $qrz \in \mathbb{N}$ . Aus der Definition von Teilbarkeit folgt damit, dass  $xy$  durch  $z$  teilbar ist.  $\square$

## 3.2 Fallunterscheidung

Die Fallunterscheidung wird bei der Voraussetzung getroffen:

$$(A \Rightarrow B \wedge \neg A \Rightarrow B) \Rightarrow B.$$

Die Fallunterscheidung muss so sein, dass insgesamt *alle* Voraussetzungen abgedeckt sind. Wir betrachten als erstes Beispiel den Beweis von Satz 1.12. Zur Erinnerung:

**Satz 3.3.** *Für endliche Mengen  $A, B$  gilt:*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Oder mit Quantoren ausgedrückt:

$$\forall A, B \text{ Menge: } |A| < \infty \wedge |B| < \infty \implies |A \cup B| = |A| + |B| - |A \cap B|.$$

*Beweis.* Seien  $A, B$  endliche Mengen, d.h., es gibt natürliche Zahlen  $m, n < \infty$  mit  $|A| = m$  und  $|B| = n$ . Das heisst wir können annehmen, dass  $A = \{x_1, x_2, \dots, x_m\}$  für paarweise unterschiedliche  $x_k$ , und  $B = \{y_1, y_2, \dots, y_n\}$  für paarweise unterschiedliche  $y_k$ .

Die Fallunterscheidung betrifft den Durchschnitt von  $A$  und  $B$ : entweder die beiden Mengen haben leeren Durchschnitt (sind disjunkt) oder sie haben nichttrivialen Durchschnitt. Wir betrachten die beiden Fälle getrennt:

Angenommen  $A$  und  $B$  sind disjunkt ( $A \cap B = \emptyset$ ). Dann gilt

$$A \cup B = \{x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n\},$$

d.h.  $|A \cup B| = m + n = |A| + |B|$ .

Andererseits, falls  $A \cap B \neq \emptyset$ , dann gibt es Elemente, die im Durchschnitt liegen, z.B.  $A \cap B = \{x_1, x_2, \dots, x_k\} = \{y_1, y_2, \dots, y_k\}$  (beachte: bei Mengen spielt die Reihenfolge keine Rolle). Dann gilt für die Vereinigung

$$A \cup B = \{x_1, \dots, x_k, x_{k+1}, \dots, x_m, y_{k+1}, \dots, y_n\}.$$

Wenn wir die Anzahl der Elemente in  $A \cup B$  zählen, kommen wir auf

$$|A \cup B| = k + (m - k) + (n - k) = m + n - k.$$

Wenn wir die rechte Seite der Identität betrachten erhalten wir  $|A| + |B| - |A \cap B| = m + n - k$ .  $\square$

Es können auch mehr als zwei Fälle unterschieden werden. Wir betrachten wieder ein Beispiel und führen dazu zuerst den Absolutbetrag ein.

**Definition 3.4.** Sei  $x$  eine reelle Zahl. Dann definieren wir den Absolutbetrag  $|x|$  als

$$|x| = \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases}$$

**Satz 3.5.** (Dreiecksungleichung) Für alle  $x, y \in \mathbb{R}$  gilt:

$$|x + y| \leq |x| + |y|.$$

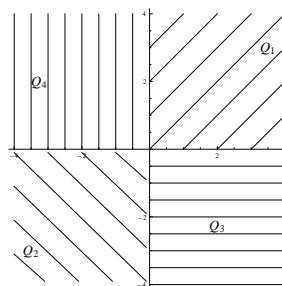
*Beweis.* Die Aussage ist für alle  $x, y \in \mathbb{R}$  zu zeigen, das heisst für alle Tupel  $(x, y) \in \mathbb{R}^2$ . Wir unterteilen den Raum  $\mathbb{R}^2$  in die vier Teilbereiche:

$$Q_1 = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0 \wedge y \geq 0\},$$

$$Q_2 = \{(x, y) \in \mathbb{R}^2 \mid x < 0 \wedge y < 0\},$$

$$Q_3 = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0 \wedge y < 0\},$$

$$Q_4 = \{(x, y) \in \mathbb{R}^2 \mid x < 0 \wedge y \geq 0\}.$$



Für diese Unterteilung gilt  $Q_1 \cup Q_2 \cup Q_3 \cup Q_4 = \mathbb{R}^2$  und jeder Punkt in  $\mathbb{R}^2$  liegt *genau* in einem der Quadranten, d.h., die Quadranten sind *paarweise disjunkt*, d.h.,  $Q_i \cap Q_j = \emptyset$  für alle  $i \neq j$ .

Wir teilen den Beweis der Dreiecksungleichung in vier Fälle auf entsprechend der vier Teilbereiche (Quadranten) auf:

1. Seien  $(x, y) \in Q_1$ , d.h.,  $x \geq 0$  und  $y \geq 0$ . Dann gilt  $|x| = x$  und  $|y| = y$ . Außerdem gilt  $x + y \geq 0$  und damit gilt  $|x + y| = x + y$  nach Definition des Absolutbetrags. Zusammengefasst folgt damit:

$$|x + y| = x + y = |x| + |y|.$$

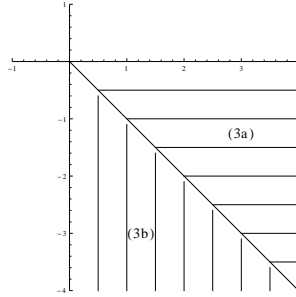
Damit ist die Dreiecksungleichung in  $Q_1$  erfüllt. In diesem Quadranten gilt sogar Gleichheit.

2. Seien  $(x, y) \in Q_2$ , d.h.,  $x < 0$  und  $y < 0$ . Dann gilt  $|x| = -x$  und  $|y| = -y$ . Außerdem gilt  $x + y < 0$  und damit  $|x + y| = -(x + y) = -x - y$ . Zusammengefasst folgt damit

$$|x + y| = -x - y = (-x) + (-y) = |x| + |y|.$$

Damit ist die Dreiecksungleichung in  $Q_2$  erfüllt. Auch in diesem Quadranten gilt Gleichheit.

3. Seien  $(x, y) \in Q_3$ , d.h.,  $x \geq 0$  und  $y < 0$ . Damit gilt in diesem Quadranten gilt  $|x| = x$  und  $|y| = -y$ . Um den Absolutbetrag von  $|x + y|$  auswerten zu können, müssen wir eine weitere Fallunterscheidung treffen. Wir betrachten für  $(x, y) \in Q_3$  zwei Unterfälle: (3a)  $x \geq -y$  und (3b)  $x < -y$



(3a) Aus  $x \geq -y$  folgt, dass  $x + y \geq 0$  und damit gilt  $|x + y| = x + y$ . Für die Dreiecksungleichung ist zu zeigen, dass  $|x + y| \leq |x| + |y|$ . Wenn wir einsetzen, was wir wissen, ist zu zeigen, dass  $x + y \leq x - y$  für alle  $x, y$  in  $Q_3$ , die der Bedingung (3a) genügen. Es gilt

$$y < 0 \implies 0 < -y \implies y < -y.$$

Damit gilt

$$|x + y| = x + y < x + (-y) = |x| + |y|.$$

D.h. für diesen Teilbereich gilt die Dreiecksungleichung (hier sogar mit strikt kleiner).

(3b) Wenn  $x < -y$  gilt, dann ist  $x + y < 0$  und damit  $|x + y| = -(x + y) = -x - y$ . Ähnlich zu dem letzten Fall schließen wir

$$x \geq 0 \implies 0 \geq -x \implies x \geq -x.$$

Damit gilt

$$|x + y| = -x - y = (-x) + (-y) \leq x + (-y) = |x| + |y|,$$

was zu zeigen war.

4. Dieser Fall kann analog zu Punkt 3 gezeigt werden und wird eine Übungsaufgabe sein.

Wenn  $Q_4$  in der Übung abgehandelt wurde, haben wir die Dreiecksungleichung für alle vier Teilbereiche gezeigt. Da die Vereinigung der vier Teilbereiche ganz  $\mathbb{R}^2$  ist, haben wir die Dreiecksungleichung bewiesen.  $\square$

### 3.3 Induktionsbeweis

Mathematische Induktion ist eine grundlegende Beweistechnik für Aussagen, die für alle natürlichen Zahlen gelten. Der Schlüssel dazu ist der spezielle Aufbau der natürlichen Zahlen:

- $0 \in \mathbb{N}$
- für jedes  $n \in \mathbb{N}$  gilt:  $n + 1 \in \mathbb{N}$

Damit sind die natürlichen Zahlen eindeutig bestimmt (und können aufzählend generiert werden).

**Induktionsprinzip** Gegeben eine Aussage  $P(x)$ . Falls

- (1)  $P(0)$  ist wahr (*Induktionsanfang*) und
- (2)  $P(n) \Rightarrow P(n+1)$  (*Induktionsschritt*) ( $P(n)$  wird die *Induktionsvoraussetzung* oder *Induktionshypothese* genannt)

Dann gilt:  $P(n)$  ist wahr für alle  $n \in \mathbb{N}$ .

Bevor wir ein Beispiel betrachten führen wir das *Summensymbol* ein:

$$\sum_{k=0}^n a_k = a_0 + a_1 + a_2 + \cdots + a_{n-1} + a_n$$

**Beispiel 3.6.** *Einfache Beispiele sind:*

$$\begin{aligned}\sum_{k=0}^5 k &= 0 + 1 + 2 + 3 + 4 + 5 \\ \sum_{k=1}^7 k^2 &= 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2 \\ \sum_{k=0}^n (2k+1) &= 1 + 3 + 5 + 7 + \cdots + (2n+1)\end{aligned}$$

Was ist  $\sum_{k=1}^n 1$ ? Was  $\sum_{k=0}^n 1$ ?

Falls die untere Summationsgrenze *grösser* als die obere Summationsgrenze ist, dann hat die Summe den Wert 0, z.B.,  $\sum_{k=7}^3 a_k = 0$ .

**Satz 3.7.** *Für alle natürlichen Zahlen  $n$  gilt*

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

*Beweis.* Wir führen einen Induktionsbeweis durch:

*Induktionsanfang:* Wir zeigen, dass die Identität für  $n = 0$  stimmt durch Einsetzen in beiden Seiten:

$$\sum_{k=0}^0 k = 0 = \frac{0(0+1)}{2}.$$

*Induktionsannahme:* Wir nehmen an, dass die Formel für eine beliebige natürliche Zahl  $n$  gilt, d.h., wir nehmen an, dass

$$\sum_{k=0}^n k = \frac{n(n+1)}{2}. \tag{3.1}$$

*Induktionsschritt:* ( $n \rightarrow n+1$ ) Unter der Annahme, dass (3.1) gilt zeigen wir, dass die Aussage auch gilt, wenn  $n$  durch  $n+1$  ersetzt wird, d.h., wir zeigen:

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

Wir beginnen mit der linken Seite und formen schrittweise um. Zuerst kann der letzte Summand aus der Summe herausgezogen werden:

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^n k + (n+1).$$

Für die verbleibende Summe kann die Induktionshypothese verwendet werden:

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

Im letzten Schritt fassen wir alles auf einen Bruch zusammen und heben heraus:

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

□

**Beispiel 3.8.** Zeigen Sie, dass für alle  $n \in \mathbb{N}$  gilt:  $\sum_{k=0}^n (2k+1) = (n+1)^2$ .

**Bemerkung 3.9.** Allgemeiner kann der Induktionsanfang bei jeder natürlichen Zahl  $n_0$  gesetzt werden, ab der  $P(x)$  gilt, d.h.,

- (1)  $P(n_0)$  ist wahr (Induktionsanfang) und
- (2)  $P(n) \Rightarrow P(n+1)$  (Induktionsschritt) ( $P(n)$  wird die Induktionsvoraussetzung oder Induktionshypothese genannt)

Dann gilt:  $P(n)$  ist wahr für alle  $n \in \mathbb{N}$  mit  $n \geq n_0$ .

**Beispiel 3.10.** Wir zeigen, dass für alle  $n \in \mathbb{N}$  gilt,  $6 \mid 7^n - 1$  mittels Induktion.

*Induktionsanfang:* Für  $n = 0$  haben wir  $7^0 - 1 = 1 - 1 = 0$  und  $0 = 6 \cdot 0$ , d.h.,  $6 \mid 0$ .

*Induktionsschritt:* Angenommen  $P(n) \equiv 6 \mid 7^n - 1$  gilt. Zu zeigen ist, dass  $6 \mid 7^{n+1} - 1$ .

Aus der Induktionshypothese  $6 \mid 7^n - 1$  folgt nach Definition, dass es eine natürliche Zahl  $q$  gibt, sodass  $7^n - 1 = 6q$ . Wir formen  $P(n+1)$  wieder so um, dass wir die Hypothese verwenden können:

$$7^{n+1} - 1 = 7 \cdot 7^n - 1 = (6+1) \cdot 7^n - 1 = 6 \cdot 7^n + 7^n - 1 = 6 \cdot 7^n + 6q = 6(7^n + q).$$

Da  $n \in \mathbb{N}$  ist und  $q \in \mathbb{N}$  ist, ist auch  $\tilde{q} = 7^n + q \in \mathbb{N}$ . Damit haben wir gezeigt, dass  $7^{n+1} - 1 = 6\tilde{q}$ , d.h.,  $6 \mid 7^{n+1} - 1$ .

Wir holen den Beweis von Satz 1.15 nach und wiederholen dazu hier:

**Satz 3.11.** (Kardinalität von Potenzmengen) Sei  $A$  eine endliche Menge mit  $|A| = n$ . Dann gilt  $|P(A)| = 2^n$ .

*Beweis.* Sei  $n = 0$ , d.h.,  $A = \emptyset$ . Dann ist die Potenzmenge  $P(A) = \{\emptyset\}$  und es gilt  $|P(A)| = 1 = 2^0$ .

Angenommen die Aussage stimmt für ein  $n \in \mathbb{N}$ . Wir betrachten jetzt eine  $(n + 1)$ -elementige Menge  $A$ :

$$A = \{a_1, a_2, \dots, a_n, a_{n+1}\} = \{a_1, a_2, \dots, a_{n-1}, a_n\} \cup \{a_{n+1}\}.$$

Sei  $A_1 = \{a_1, a_2, \dots, a_{n-1}, a_n\}$  (d.h.,  $A = A_1 \cup \{a_{n+1}\}$ ). Da  $|A_1| = n$  gilt laut Induktionsvoraussetzung, dass  $|P(A_1)| = 2^n$ .

Wir konstruieren die Potenzmenge von  $A$  jetzt folgendermassen: Für jedes  $B \in P(A_1)$  gilt  $B \in P(A)$ . Weiters gilt für jedes  $B \in P(A_1)$ , dass  $C = B \cup \{a_{n+1}\} \in P(A)$ . Die Potenzmenge von  $A$  ist also die Vereinigung von  $P(A_1)$  mit der Menge aller Mengen  $C$ , die so gebildet werden können. Die Mächtigkeit dieser Menge ist damit doppelt so gross wie die Mächtigkeit von  $P(A_1)$ , d.h.,  $|P(A)| = 2|P(A_1)| = 2 \cdot 2^n = 2^{n+1}$ .  $\square$

### 3.4 Widerspruchsbeweis

Die Grundidee ist es statt die zu beweisende Aussage zu zeigen, ihr Gegenteil zu widerlegen (indem man auf einen Widerspruch führt)

$$(\neg A \Rightarrow F) \Rightarrow A.$$

Wir illustrieren das an Beispielen.

**Satz 3.12.** Die Quadratwurzel aus 2 lässt sich nicht als rationale Zahl darstellen ( $\sqrt{2} \notin \mathbb{Q}$ ).

*Beweis.* Angenommen  $\sqrt{2} \in \mathbb{Q}$ . Dann existieren natürliche Zahlen  $p, q$ , mit  $q \neq 0$ , sodass  $\sqrt{2} = \frac{p}{q}$ . Wir nehmen an, dass  $p, q$  minimal gewählt sind, d.h., dass nicht mehr gekürzt werden kann.

Aus  $\sqrt{2} = \frac{p}{q}$  folgt durch Quadrieren, dass  $2 = \frac{p^2}{q^2}$  ist. Wenn bei  $\frac{p}{q}$  nicht gekürzt werden konnte, dann kann auch bei  $\frac{p^2}{q^2}$  nicht mehr gekürzt werden. Da aber  $\frac{p^2}{q^2} = 2$ , also gleich einer ganzen Zahl ist, muss der Nenner eins sein, also  $q = 1$ .

Jetzt wissen wir, dass wenn  $\sqrt{2}$  eine rationale Zahl ist, dann muss es sogar eine ganze Zahl sein ( $\sqrt{2} = p$ ). Da  $1 < \sqrt{2} < 2$  gilt, muss  $p$  eine ganze Zahl sein, die zwischen 1 und 2 liegt. So eine ganze Zahl gibt es nicht, daher sind wir bei einem Widerspruch angekommen und die Annahme muss falsch gewesen sein.  $\square$

**Satz 3.13.** Für jede positive reelle Zahl  $x$  gilt  $\frac{x+1}{x+2} < \frac{x+3}{x+4}$ .

*Beweis.* Sei  $x > 0$  eine beliebige reelle Zahl. Angenommen, es gilt das Gegenteil der zu zeigenden Aussage, d.h., angenommen es gilt

$$\frac{x+1}{x+2} \geq \frac{x+3}{x+4}. \quad (3.2)$$

Wenn  $x > 0$  ist, dann gilt auch  $x+2 > 0$  und  $x+4 > 0$ . Damit können wir die Ungleichung in (3.2) mit  $(x+2)(x+4)$  multiplizieren und erhalten die äquivalente Ungleichung

$$(x+1)(x+4) \geq (x+3)(x+2) \iff x^2 + 5x + 4 \geq x^2 + 5x + 6.$$



Im letzten Schritt haben wir auf beiden Seiten ausmultipliziert. Durch Abziehen von  $x^2 + 5x$  auf beiden Seiten erhalten wir die Ungleichung

$$4 \geq 6$$

die falsch ist (eine Kontradiktion). Damit muss die ursprüngliche Aussage richtig sein.  $\square$

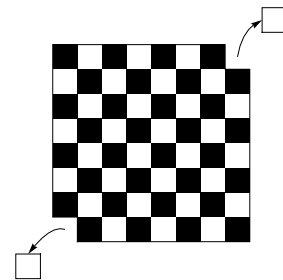
**Bemerkung 3.14.** Wenn eine Ungleichung mit einer positiven Zahl  $a > 0$  multipliziert wird, ändert sich das Ungleichheitszeichen nicht, also gilt zum Beispiel für  $a > 0$

$$x < y \iff ax < ay.$$

Wenn eine Ungleichung mit einer negativen Zahl  $b < 0$  multipliziert wird, dann dreht sich das Ungleichheitszeichen um, also gilt zum Beispiel für  $b < 0$

$$x < y \iff bx > by.$$

**Beispiel 3.15.** Wir betrachten ein Schachbrett, bei dem zwei (weiße) Felder an gegenüberliegenden Ecken entfernt wurden. Für dieses Brett gilt: Es gibt keine überlappungsfreie Überdeckung des Bretts mit  $2 \times 1$ -Dominosteinen (d.h. von der Größe von zwei Feldern).



Wir zeigen diese Aussage mittels Widerspruch: Angenommen, es gibt eine überlappungsfreie Überdeckung. Jeder Stein in dieser Überdeckung müsste dann ein weißes und ein schwarzes Feld abdecken. Von den ursprünglich 64 Feldern sind noch 62 übrig (nach Wegnahme der zwei weißen Felder). Damit brauchen wir 31 Steine um 32 schwarze Felder und 30 weiße Felder abzudecken. Egal wie die Überdeckung gelegt wird, es wird mit jedem der 30 Steine jeweils ein weißes und ein schwarzes Feld abgedeckt und am Ende bleiben zwei schwarze Felder übrig. Die können aber nicht mit einem Stein abgedeckt werden, da sie nicht nebeneinander liegen.

## 4 Funktionen

**Definition 4.1.** Eine Funktion  $f: X \rightarrow Y$  (wobei  $X, Y$  Mengen sind) ist eine Vorschrift, die jedem  $x \in X$  genau ein  $y \in Y$  zuordnet. Das zu  $x \in X$  eindeutig bestimmte  $y \in Y$  wird  $y = f(x)$  bezeichnet.

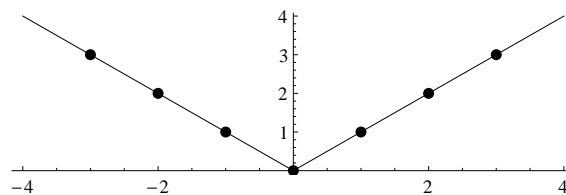
**Beispiel 4.2.** Absolutbetrag wie in Definition 3.4 eingeführt ist eine Funktion, zum Beispiel, von  $\mathbb{R}$  nach  $\mathbb{R}$ :

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto |x|$$

Diese Funktion kann in  $\mathbb{R}^2$  graphisch dargestellt werden.

Wertetabelle:

$x$	$y$
-3	3
-2	2
-1	1
0	0
1	1
2	2
3	3

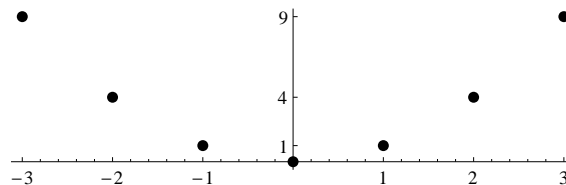


**Beispiel 4.3.** Eine Funktion kann auch nur auf diskreten Werten definiert sein, zum Beispiel

$$f: \{-3, -2, -1, 0, 1, 2, 3\} \rightarrow \{0, 1, 4, 9\}, \quad x \mapsto x^2$$

Wertetabelle:

$x$	$y$
-3	9
-2	4
-1	1
0	0
1	1
2	4
3	9



Eine Funktion  $f: X \rightarrow Y$  kann als eine Menge von eindeutig bestimmten Paaren  $(x, y)$  betrachtet werden mit  $x \in X$  und  $y \in Y$ . Die Funktion aus dem letzten Beispiel ist gegeben durch

$$f = \{(-3, 9), (-2, 4), (-1, 1), (0, 0), (1, 1), (2, 4), (3, 9)\} \subseteq \{-3, -2, -1, 0, 1, 2, 3\} \times \{0, 1, 4, 9\}.$$

Damit ist  $f$  eine Teilmenge der Produktmenge  $X \times Y$ .

**Definition 4.4.** Seien  $X, Y$  Mengen. Eine Funktion von  $X$  nach  $Y$  ist eine Teilmenge  $f \subseteq X \times Y$  für die gilt

$$(1) \forall x \in X \exists y \in Y: (x, y) \in f$$

$$(2) \forall x \in X \forall y, z \in Y: (x, y) \in f \wedge (x, z) \in f \Rightarrow y = z$$

**Beispiel 4.5.** Welche der folgenden Teilmengen von  $X \times Y$  definiert eine Funktion von  $X$  nach  $Y$ ?

$$(a) f = \{(x, 5) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

$$(b) f = \{(5, x) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

$$(c) f = \{(x, y) \mid x^2 + y^2 = 1\} \subseteq [-1, 1] \times \mathbb{R}$$

$$(d) f = \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

**Definition 4.6.** Sei  $f: X \rightarrow Y$  eine Funktion. Die Menge  $X$  heisst der Definitionsbereich (engl.: domain) von  $f$ . Die Menge

$$f(X) = \{y \in Y \mid \exists x \in X: f(x) = y\} \subseteq Y$$

heisst das Bild oder der Bildbereich oder der Wertebereich (engl.: range oder image) von  $f$  unter  $X$ . Ist  $y \in f(X)$ , dann wird ein  $x \in X$  mit  $f(x) = y$  als Urbild bezeichnet. Sei  $Z \subseteq Y$ . Die Menge

$$f^{-1}(Z) = \{x \in X \mid \exists y \in Z: y = f(x)\} \subseteq X$$

heisst Urbildbereich (engl.: preimage) von  $f$  in  $Z$ .

**Beispiel 4.7.** Sei  $X = [-5, 5]$  und  $Y = \mathbb{R}$  und  $f: X \rightarrow Y$  die Abbildung  $x \mapsto |x|$ .

(a) Was ist  $f(X)$ ?

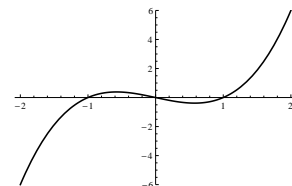
(b) Sei  $Z = [1, 3]$ . Was ist  $f^{-1}(Z)$ ?

**Beispiel 4.8.** Seien  $X = \{a, b, c, d\}$ ,  $Y = \{1, 2, 3\}$  und seien  $f_1 = \{(a, 1), (b, 3), (c, 2), (d, 3)\}$  und  $f_2 = \{(a, 1), (b, 2), (b, 3), (c, 1), (d, 3)\}$  und  $f_3 = \{(a, 1), (b, 2), (c, 3)\}$  gegeben. Welche dieser Teilmengen von  $X \times Y$  sind Funktionen?

**Beispiel 4.9.** Gegeben sind die Mengen  $X_1 = [-2, 2]$ ,  $X_2 = \mathbb{R}_0^+$ ,  $X_3 = ]-1, 1[$  und  $Y_1 = [-6, 6]$ ,  $Y_2 = \mathbb{R}$ ,  $Y_3 = \mathbb{R}$ . Wir betrachten die Abbildung  $f: X_k \rightarrow Y_k, x \mapsto x^3 - x$  für  $k = 1, 2, 3$ .

(a) Wie sieht der Funktionsgraph aus?

(b) Was ist jeweils der Bildbereich von  $f$  unter  $X_k$  ( $k = 1, 2, 3$ )?



**Definition 4.10.** Sei  $f: X \rightarrow Y$  eine Funktion.

(1)  $f$  heisst surjektiv, wenn jedes  $y \in Y$  im Bild von  $f$  liegt.

(2)  $f$  heisst injektiv, wenn jedes Element im Bild von  $f$  genau ein Urbild in  $X$  besitzt.

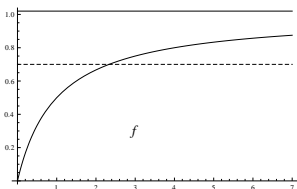
(3)  $f$  heisst bijektiv, wenn  $f$  sowohl injektiv als auch surjektiv ist.

**Bemerkung 4.11.** •  $f$  ist genau dann surjektiv, wenn  $Y = f(X)$ .

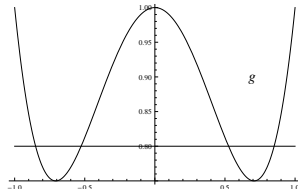
- $f$  ist genau dann injektiv, wenn für alle  $x_1, x_2 \in X$  gilt  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ .
- $f$  ist genau dann injektiv, wenn für alle  $x_1, x_2 \in X$  gilt  $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ .
- $f$  ist genau dann bijektiv, wenn  $Y = f(X)$  und  $x = y \Leftrightarrow f(x) = f(y)$ .

**Beispiel 4.12.** Für welche Mengen  $X_k, Y_k$  ist  $f \subseteq X_k \times Y_k$  aus Beispiel 4.8 (a) injektiv (b) surjektiv (c) bijektiv?

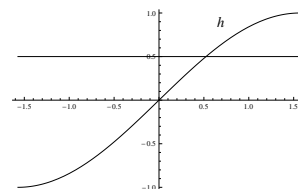
Die Begriffe injektiv und surjektiv hängen mit der Lösbarkeit der Gleichung  $f(x) = y$  bei gegebener Funktion  $f: X \rightarrow Y$  und gegebenem  $y \in Y$  zusammen. Wenn  $f$  injektiv ist, dann besitzt die Gleichung  $f(x) = y$  höchstens eine Lösung  $x \in X$ . Wenn  $f$  surjektiv ist, dann besitzt die Gleichung  $f(x) = y$  mindestens eine Lösung  $x \in X$ . Diese Lösung kann gefunden werden, indem die Kurve der Funktion mit der horizontalen Gerade durch  $y$  geschnitten wird.



$$f: \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+, \\ x \mapsto 1 - \frac{1}{x+1}$$



$$g: [-1, 1] \rightarrow \left[\frac{3}{4}, 1\right], \\ x \mapsto x^4 - x^2 + 1$$



$$h: \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \rightarrow [-1, 1] \\ x \mapsto \sin(x)$$

**Satz 4.13.** Zwei Mengen  $X, Y$  besitzen die gleiche Anzahl von Elementen (Kardinalität) genau dann, wenn ein bijektive Funktion  $f: X \rightarrow Y$  existiert.

**Beispiel 4.14.** Es gibt gleich viele gerade wie ungerade natürliche Zahlen. Wir bezeichnen die geraden natürlichen Zahlen mit  $\mathbb{N}_{ger}$  und die ungeraden natürlichen Zahlen mit  $\mathbb{N}_{unger}$ . Eine Bijektion  $f: \mathbb{N}_{ger} \rightarrow \mathbb{N}_{unger}$  ist z.B. gegeben durch  $x \mapsto x + 1$ .

**Beispiel 4.15.** Die Abbildung

$$f: [0, 4] \rightarrow [-1, 1], \quad x \mapsto \frac{x}{2} - 1$$

ist bijektiv. Folglich haben  $[0, 4]$  und  $[-1, 1]$  die gleiche Anzahl von Elementen.

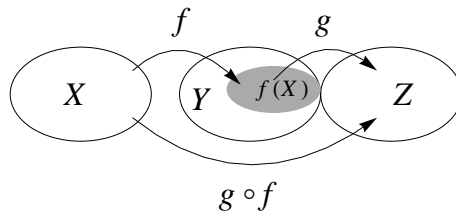
**Definition 4.16.** Sei  $X$  eine Menge. Die Funktion von  $X$  nach  $X$ , die jedes Element  $x \in X$  auf sich selbst abbildet heisst die identische Abbildung auf  $X$  und wird mit  $id_X$  bezeichnet.

Die Identität  $id_X: X \rightarrow X, x \mapsto x$  ist eine bijektive Funktion.

**Definition 4.17.** Seien  $X, Y, Z$  Mengen und seien  $f: X \rightarrow Y$  und  $g: f(X) \rightarrow Z$  Funktionen. Dann ist die Komposition (Hintereinanderausführung) von  $f$  und  $g$  definiert als

$$g \circ f: X \rightarrow Z, \quad x \mapsto (g \circ f)(x) = g(f(x)).$$

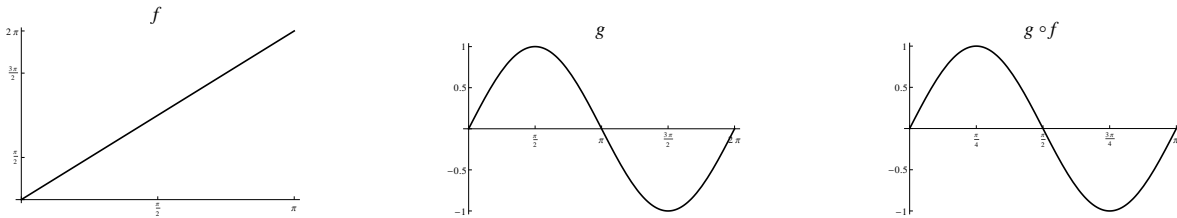
In Worten ist  $g \circ f$  "g nach f".



**Satz 4.18.** Die Komposition von zwei Funktionen ist eine Funktion.

**Beispiel 4.19.** Seien  $X = [0, \pi], Y = [0, 2\pi], Z = [-1, 1]$  und seien die Funktionen  $f, g$  gegeben durch

$$f: X \rightarrow Y, \quad x \mapsto 2x, \quad \text{und} \quad g: Y \rightarrow Z, \quad x \mapsto \sin(x).$$



Die Hintereinanderausführung  $g \circ f$  ist gegeben durch

$$g \circ f: [0, \pi] \rightarrow [-1, 1], \quad x \mapsto \sin(2x).$$

**Beispiel 4.20.** Die Funktionen  $f, g$  seien gegeben durch

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^3, \quad \text{und} \quad g: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x + 1.$$

Bestimmen Sie  $g \circ f$  und  $f \circ g$ .

**Bemerkung 4.21.** Sei  $f: X \rightarrow Y$  eine Funktion. Dann gilt:

$$(id_Y \circ f)(x) = id_Y(f(x)) = f(x), \quad \forall x \in X,$$

und

$$(f \circ id_X)(x) = f(id_X(x)) = f(x), \quad \forall x \in X.$$

**Definition 4.22.** Sei  $f: X \rightarrow Y$  eine Funktion.  $f$  heisst invertierbar, wenn es eine Funktion  $f^{-1}: Y \rightarrow X$  gibt, sodass

$$f^{-1} \circ f = id_X \quad \text{und} \quad f \circ f^{-1} = id_Y.$$

$f^{-1}$  heisst die inverse Funktion (oder Umkehrfunktion) zu  $f$ .

Eine Funktion ist also invertierbar, wenn jedem  $y \in Y$  ein eindeutig bestimmtes  $x \in X$  zugeordnet werden kann für das  $f(x) = y$  gilt. Damit sind die invertierbaren Funktionen genau die bijektiven Funktionen. Die Umkehrfunktion kann auch mittels Produktmengen definiert werden: Sei  $f \subseteq X \times Y$  eine Funktion. Wenn

$$f^{-1} = \{(y, x) \mid y \in Y, x \in X \text{ und } (x, y) \in f\} \subseteq Y \times X$$

eine Funktion ist, dann ist  $f$  invertierbar und  $f^{-1}$  heisst die inverse Funktion zu  $f$ .

Wie berechnet man die Umkehrfunktion? Wenn auf die Identität  $f(x) = y$  (für eine bijektive Funktion  $f: X \rightarrow Y$ ) auf beiden Seiten die Umkehrfunktion angewandt wird, dann erhalten wir

$$f(x) = y \Leftrightarrow f^{-1}(f(x)) = f^{-1}(y) \Leftrightarrow id_X(x) = f^{-1}(y) \Leftrightarrow x = f^{-1}(y).$$

**Beispiel 4.23.** Sei  $f: [0, 4] \rightarrow [-1, 1], x \mapsto \frac{x}{2} - 1$ . Um die Umkehrfunktion  $f^{-1}: [-1, 1] \rightarrow [0, 4]$  zu bestimmen formen wir  $y = f(x)$  um auf  $x = f^{-1}(y)$ :

$$y = \frac{x}{2} - 1 \rightarrow y + 1 = \frac{x}{2} \rightarrow x = 2y + 2.$$

Damit erhalten wir die Umkehrfunktion

$$f^{-1}: [-1, 1] \rightarrow [0, 4], y \mapsto 2y + 2.$$

Zur Probe berechnen wir  $f \circ f^{-1}$  und  $f^{-1} \circ f$  (ob da die Identität herauskommt):

$$\begin{aligned} f \circ f^{-1}(x) &= f(f^{-1}(x)) = f(2x + 2) = \frac{2x + 2}{2} - 1 = x \\ f^{-1} \circ f(x) &= f^{-1}(f(x)) = f^{-1}\left(\frac{x}{2} - 1\right) = 2\left(\frac{x}{2} - 1\right) + 2 = x \end{aligned}$$

**Beispiel 4.24.** Welcher der folgenden Funktionen ist invertierbar? Wie lautet die Umkehrfunktion der invertierbaren Funktionen?

- $f = \{(x, 5) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$
- $g: ]1, \infty[ \rightarrow ]1, \infty[, x \mapsto \frac{x}{x-1}$
- $h: [-2, 2] \rightarrow [0, 4], x \mapsto 4 - x^2$

**Definition 4.25.** Sei  $f: X \rightarrow Y$  eine Funktion.

- (a)  $f$  heisst streng monoton wachsend wenn für alle  $x_1, x_2 \in X$  mit  $x_1 < x_2$  gilt:  $f(x_1) < f(x_2)$ .
- (b)  $f$  heisst monoton wachsend wenn für alle  $x_1, x_2 \in X$  mit  $x_1 < x_2$  gilt:  $f(x_1) \leq f(x_2)$ .
- (c)  $f$  heisst streng monoton fallend wenn für alle  $x_1, x_2 \in X$  mit  $x_1 < x_2$  gilt:  $f(x_1) > f(x_2)$ .
- (d)  $f$  heisst monoton fallend wenn für alle  $x_1, x_2 \in X$  mit  $x_1 < x_2$  gilt:  $f(x_1) \geq f(x_2)$ .

**Beispiel 4.26.** • Die Betragsfunktion  $f: [-5, 5] \rightarrow [0, 5], x \mapsto |x|$  ist im Intervall  $[-5, 0]$  streng monoton fallend und im Intervall  $[0, 5]$  streng monoton wachsend.

- Die Vorzeichenfunktion

$$\text{sign}: [-5, 5] \rightarrow [-1, 1], x \mapsto \begin{cases} 1, & x \geq 0 \\ -1, & x < 0 \end{cases}$$

ist monoton wachsend.

**Satz 4.27.** Die Hintereinanderausführung zweier Funktionen  $f$  und  $g$  ist monoton wachsend, wenn  $f$  und  $g$  beide monoton wachsend oder beide monoton fallend sind.

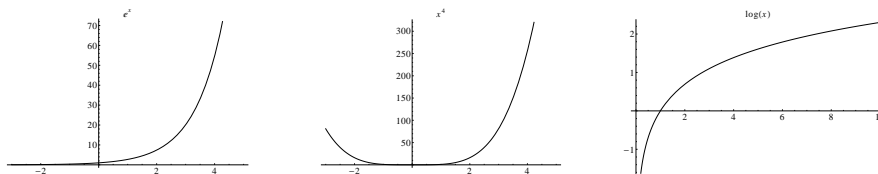
Die Hintereinanderausführung zweier Funktionen  $f$  und  $g$  ist monoton fallend, wenn  $f$  monoton wachsend und  $g$  monoton fallend ist, oder, wenn  $f$  monoton fallend und  $g$  monoton wachsend ist.

**Definition 4.28.** Eine Funktion  $p: X \rightarrow Y$  heisst ein Polynom, wenn es reelle Zahlen  $a_0, \dots, a_d$  gibt mit  $p(x) = a_0 + a_1x + \dots + a_dx^d$ . Wenn  $a_d \neq 0$  gilt, dann nennt man den Grad von  $p$  und schreibt  $\deg(p(x)) = d$ .

Eine Funktion  $r: X \rightarrow Y$  heisst eine rationale Funktion, wenn es Polynome  $p, q$  gibt sodass  $r(x) = p(x)/q(x)$ .

**Bemerkung 4.29.** Die Hintereinanderausführung zweier Polynome ist wieder ein Polynom. Wenn  $p_1(x)$  ein Polynom vom Grad  $d_1$  ist und  $p_2(x)$  ein Polynom vom Grad  $d_2$ , dann ist  $p_1(p_2(x))$  ein Polynom vom Grad  $d_1d_2$ .

Ebenso ist die Hintereinanderausführung zweier rationaler Funktionen wieder eine rationale Funktion.



Sei  $a \in \mathbb{R}^+ \setminus \{1\}$ . Jede Funktion der Form  $f: x \mapsto a^x$  (z.B. von  $\mathbb{R}$  nach  $\mathbb{R}^+$ ) heisst *Exponentialfunktion*. Ein Spezialfall ist die Funktion  $\exp: x \mapsto e^x$ , wobei  $e \approx 2.7182818284590452354$  die *Eulersche Zahl* ist. Die Exponentialfunktion ist bijektiv als Abbildung von  $\mathbb{R}$  nach  $\mathbb{R}^+ = ]0, \infty[$ . Die inverse Abbildung zur Exponentialfunktion  $\exp$  wird als *natürlicher Logarithmus* bezeichnet,

$$y = e^x \Leftrightarrow x = \ln(y), \quad \text{oder anders,} \quad y = e^{\ln(y)} = \exp(\ln(y)). \quad (4.1)$$

Allgemein ist die inverse Funktion zu einer Exponentialfunktion  $f: x \mapsto a^x$  ( $a \in \mathbb{R}^+ \setminus \{1\}$ ) der *Logarithmus zur Basis  $a$* ,

$$y = a^x \Leftrightarrow x = \log_a(y), \quad \text{oder anders,} \quad y = a^{\log_a(y)}.$$

Sei  $a \in \mathbb{R}^+ \setminus \{1\}$ , dann gilt mit (4.1):

$$a = e^{\ln(a)} \Rightarrow a^x = e^{x \ln(a)}.$$

Für Logarithmen gelten die folgenden Rechenregeln, für  $x, y > 0$

$$\log_a(xy) = \log_a(x) + \log_a(y), \quad , \log_a(x^d) = d \log_a(x).$$

Der Logarithmus bezüglich jeder Basis kann mithilfe des natürlichen Logarithmus ausgerechnet werden:

$$\log_a(x) = \frac{\ln(x)}{\ln(a)} \quad \left( \text{da } \log_a(x) \ln(a) = \ln \left( a^{\log_a(x)} \right) = \ln(x) \right)$$

## 5 Relationen

**Definition 5.1.** Seien  $X, Y$  Mengen. Eine (binäre) Relation  $R$  auf  $X, Y$  ist eine Teilmenge von  $X \times Y$  (d.h.,  $R \subseteq X \times Y$ ). Wir schreiben für  $x \in X$  und  $y \in Y$

$$(x, y) \in R \quad \text{oder} \quad xRy$$

für “ $x$  steht in Relation zu  $y$ ”.

Jede Funktion ist also auch eine Relation.

**Beispiel 5.2.** Seien  $X = \{0, 1, 2\}$ ,  $Y = \{a, b, c\}$  dann definieren

$$R_1 = \{(0, a), (0, b), (2, c)\} \subseteq X \times Y,$$

und

$$R_2 = \{(0, c), (1, b), (2, a)\} \subseteq X \times Y,$$

Relationen auf  $X, Y$ .

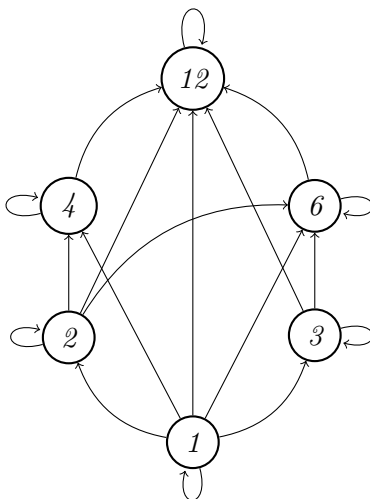
**Beispiel 5.3.** Sei  $X = \{1, 2, 3, 4, 6, 12\}$  dann wird durch die Bedingung  $x$  teilt  $y$  eine Relation auf  $X$  definiert. In Zeichen:

$$xR_3y \iff x \mid y, \quad R_3 \subseteq X \times X.$$

Wir können  $R_3$  auch explizit anschreiben als Teilmenge des kartesischen Produkts  $X \times X = X^2$ :

$$R_3 = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (1, 12), (2, 2), (2, 4), (2, 6), (2, 12), (3, 3), (3, 6), (3, 12), (4, 4), (4, 12), (6, 6), (6, 12), (12, 12)\}$$

oder graphisch darstellen, wobei Pfeile  $x \rightarrow y$  für  $xR_3y$  stehen:





**Beispiel 5.4.** Sei  $X$  eine Menge von Geraden im  $\mathbb{R}^2$  und zu  $g, h \in X$  definieren wir  $gRh$  genau dann, wenn  $g$  und  $h$  parallel sind.

**Beispiel 5.5.** Sei  $A = \{1, 2\}$  und  $X = P(A)$  (die Potenzmenge von  $A$ ). Wir definieren die Relation  $R \subseteq X \times X$  durch  $aRb$ , genau dann wenn  $a \subseteq b$ .

**Definition 5.6.** Sei  $R$  eine Relation auf den Mengen  $X, Y$ . Dann ist der Vorbereich (engl. domain) von  $R$  definiert als

$$\text{dom}(R) = \{x \in X \mid \exists y \in Y : xRy\}.$$

Der Nachbereich (engl. codomain) von  $R$  ist definiert als

$$\text{cod}(R) = \{y \in Y \mid \exists x \in X : xRy\}.$$

Das Komplement von  $R$  ist  $\bar{R} = (X \times Y) \setminus R$ . Die Inverse ist eine Relation  $R^{-1} \subseteq Y \times X$ , die durch

$$(y, x) \in R^{-1} \iff (x, y) \in R$$

definiert ist.

$R \subseteq X \times Y$  heisst rechtseindeutig, wenn gilt

$$\forall x \in X \forall y, z \in Y : (xRy \wedge xRz) \Rightarrow y = z,$$

und rechtstotal, wenn  $\text{cod}(R) = Y$ .  $R$  heisst linkseindeutig, wenn  $R^{-1}$  rechtseindeutig ist, bzw. linkstotal, wenn  $R^{-1}$  rechtstotal ist.

Noch einmal zurück zu Funktionen: Seien  $X, Y$  Mengen. Eine Relation  $f \subseteq X \times Y$  heisst *partielle Funktion*, wenn  $f$  rechtseindeutig ist.  $f$  heisst *Funktion* (oder auch *totale Funktion*, wenn  $f$  ausserdem linkstotal ist, was unserer Definition einer Funktion aus dem letzten Kapitel entspricht).

Eine (totale) Funktion heisst *injektiv*, wenn jeder Wert im Bildbereich höchstens einmal erreicht wird. In der Sprache der Relationen bedeutet das, dass  $f \subseteq X \times Y$  *injektiv* ist genau dann, wenn  $f$  *linkseindeutig* ist.

Eine (totale) Funktion heisst *surjektiv*, wenn jeder Wert im Bildbereich mindestens einmal erreicht wird. In der Sprache der Relationen bedeutet das, dass  $f \subseteq X \times Y$  *surjektiv* ist genau dann, wenn  $f$  *rechtstotal* ist.

**Definition 5.7.** Eine Relation  $R$  auf einer Menge  $X$  heisst

- reflexiv, falls  $\forall x \in X : xRx$
- symmetrisch, falls  $\forall x, y \in X : xRy \Rightarrow yRx$
- antisymmetrisch, falls  $\forall x, y \in X : xRy \wedge yRx \Rightarrow x = y$
- transitiv, falls  $\forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$

**Beispiel 5.8.** Wir betrachten wieder die Teilbarkeitsrelation  $R_3$  aus Beispiel 5.3. Wir untersuchen diese Relation auf die Eigenschaften aus Definition 5.7

- *Reflexivität:* Jede Zahl teilt sich selbst, daher gilt für jedes  $x \in X = \{1, 2, 3, 4, 6, 12\}$ , dass  $xR_3x \Leftrightarrow x \mid x$ . Somit ist  $R_3$  reflexiv.

- *Symmetrie:* Die Relation ist nicht symmetrisch, was durch ein Gegenbeispiel gezeigt werden kann (Symmetrie müsste für alle Elemente der Relation gelten): es gilt  $2 \mid 4$  aber  $4 \nmid 2$ .
- *Antisymmetrie:* Seien  $x, y \in X$  mit  $x \mid y$  und  $y \mid x$ . Aus  $x \mid y$  folgt, dass es ein  $p \in \mathbb{N}$  gibt sodass  $y = px$ . Aus  $y \mid x$  folgt, dass es ein  $q \in \mathbb{N}$  gibt mit  $x = qy$ . Zusammengefasst heisst das, dass  $y = pq \cdot x$  für natürliche Zahlen  $p, q$ . Das kann nur gelten, wenn  $p = q = 1$  ist, d.h.,  $x = y$ . Die Relation ist also antisymmetrisch.
- *Transitivität:* Seien  $x, y, z \in X$  mit  $x \mid y$  und  $y \mid z$ . Analog zum letzten Punkt bedeutet das, dass  $p, q \in \mathbb{N}$  existieren mit  $y = px$  und  $z = qy$ . Folglich gilt  $z = qp \cdot x$ . Da  $qp \in \mathbb{N}$  ist, folgt daraus, dass  $x \mid z$ . Die Relation ist also transitiv.

**Beispiel 5.9.** Die Relation aus Beispiel 5.4 ist reflexiv, symmetrisch und transitiv, aber nicht antisymmetrisch.

**Definition 5.10.** Es seien  $X, Y, Z$  Mengen und  $R \subseteq X \times Y$  und  $S \subseteq Y \times Z$  Relationen. Die relationale Komposition (bzw. das Relationenprodukt)  $S \circ R \subseteq X \times Z$  von  $R$  und  $S$  ist definiert als

$$(x, z) \in S \circ R \iff \exists y \in Y : (x, y) \in R \wedge (y, z) \in S,$$

oder äquivalent als

$$S \circ R = \{(x, z) \mid \exists y \in Y : xRy \wedge yRz\}.$$

**Beispiel 5.11.** Seien  $X = \{0, 1, 2\}, Y = \{a, b, c\}$  und  $Z = \{x, y, z\}$  und die beiden Relationen  $R_1 \subseteq X \times Y$  und  $R_2 \subseteq Y \times Z$  gegeben durch

$$R_1 = \{(0, a), (0, b), (1, c), (2, a)\} \quad \text{und} \quad R_2 = \{(a, z), (b, y), (c, z)\}.$$

Dann gilt

$$R_2 \circ R_1 = \{(0, y), (0, z), (1, z), (2, z)\} \subseteq X \times Z.$$

**Definition 5.12.** (Potenzen einer Relation) Sei  $X$  eine Menge und  $R \subseteq X \times X$  eine Relation. Mit  $id_X \subseteq X \times X$  bezeichnen wir die Identitätsrelation definiert durch

$$(x_1, x_2) \in id_X \iff x_1 = x_2,$$

für  $x_1, x_2 \in X$ . Die Potenzen von  $R$  werden dann rekursiv definiert durch

$$R^0 := id_X, \quad \text{und} \quad R^n := R \circ R^{n-1}, \quad \text{für } n \geq 1.$$

**Definition 5.13.** Sei  $R$  eine beliebige Relation auf einer Menge  $X$ . Die transitive Hülle  $R^+$  ist die kleinste Relation, die  $R$  einschliesst und die Eigenschaft der Transitivität erfüllt. Die reflexiv transitive Hülle  $R^*$  ist die kleinste Relation, die  $R^+$  einschliesst und zusätzlich die Eigenschaften der Reflexivität erfüllt.

Es gelten die folgenden Beziehungen:

$$R^+ = \bigcup_{n \in \mathbb{N}^*} R^n, \quad \text{und} \quad R^* = \bigcup_{n \in \mathbb{N}} R^n.$$

**Beispiel 5.14.** Sei  $X = \{0, 1, 2\}$  und  $R = \{(0, 1), (0, 2), (1, 0), (2, 2)\} \subseteq X \times X$ . Wir bestimmen die reflexiv transitive Hülle von  $R$ :

$$\begin{aligned} R^0 &= id_X = \{(0, 0), (1, 1), (2, 2)\} \\ R^1 &= R = \{(0, 1), (0, 2), (1, 0), (2, 2)\} \\ R^2 &= R \circ R = \{(0, 0), (0, 2), (1, 1), (1, 2), (2, 2)\} \\ R^3 &= R \circ R^2 = \{(0, 1), (0, 2), (1, 0), (1, 2), (2, 2)\} \\ R^4 &= R \circ R^3 = \{(0, 0), (0, 2), (1, 1), (1, 2), (2, 2)\} = R^2 \\ R^5 &= R \circ R^4 = R \circ R^2 = R^3 \end{aligned}$$

Damit gilt  $R^{2n} = R^2$  und  $R^{2n+1} = R^3$  für alle  $n \geq 2$ . Die reflexiv transitive Hülle ergibt sich also als Vereinigung von  $R^0, R, R^2$  und  $R^3$ :

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

## 5.1 Äquivalenzrelationen

**Definition 5.15.** Eine Relation  $R$  auf einer Menge  $X$  heißt Äquivalenzrelation, genau dann, wenn  $R$  reflexiv, symmetrisch und transitiv ist. Für Äquivalenzrelationen wird häufig die Notation  $\sim$  statt  $R$  verwendet.

Ein typisches Beispiel für eine Äquivalenzrelation ist die Kongruenz modulo einer natürlichen Zahl:

**Definition 5.16.** Seien  $n \in \mathbb{N}^*$  und  $a, b \in \mathbb{Z}$ . Dann sind  $a$  und  $b$  kongruent modulo  $n$  genau dann, wenn  $n \mid a - b$  ( $n$  teilt  $a - b$ ). Man schreibt  $a \equiv b \pmod{n}$ .

**Beispiel 5.17.** Einige Beispiele:

$$\begin{aligned} 7 &\equiv 5 \pmod{2}, & \text{weil } 7 - 5 = 2 \text{ und } 2 \mid 2 \\ 1 &\equiv 3 \pmod{2}, & \text{weil } 1 - 3 = -2 \text{ und } 2 \mid -2 \\ 27 &\equiv 12 \pmod{5}, & \text{weil } 27 - 12 = 15 \text{ und } 5 \mid 15 \end{aligned}$$

**Satz 5.18.** Kongruenz modulo  $n$  ist eine Äquivalenzrelation auf  $\mathbb{Z}$ , d.h., die Relation  $\sim_n \subseteq \mathbb{Z} \times \mathbb{Z}$  definiert durch

$$a \sim_n b \iff a \equiv b \pmod{n}.$$

*Beweis.* Sei  $n \in \mathbb{N}^*$ . Zu überprüfen ist, ob die Relation  $\sim_n$  reflexiv, symmetrisch und transitiv ist.

- Reflexivität: Sei  $a \in \mathbb{Z}$ . Dann gilt

$$n \mid a - a = 0 \iff a \equiv a \pmod{n} \iff a \sim_n a.$$

Somit ist die Relation reflexiv.

- Symmetrie: Seien  $a, b \in \mathbb{Z}$  und es gelte  $a \sim_n b$ . Nach Definition von  $\sim_n$  folgt, dass  $n \mid a - b$ , d.h., es existiert ein  $q \in \mathbb{Z}$ , sodass  $a - b = qn$ . Damit gilt  $b - a = (-q)n$  und auch  $-q \in \mathbb{Z}$ . Daraus folgt, dass  $n \mid b - a$ , was wiederum zu  $b \sim_n a$  äquivalent ist. Somit ist die Relation symmetrisch.

- Transitivität: Seien  $a, b, c \in \mathbb{Z}$  mit  $a \sim_n b$  und  $b \sim_n c$ , d.h.,

$$a \equiv b \pmod{n} \quad \text{und} \quad b \equiv c \pmod{n}.$$

Nach Definition bedeutet das, dass  $p, q \in \mathbb{Z}$  existieren sodass

$$a - b = qn \quad \text{und} \quad b - c = pn.$$

Zu zeigen ist, dass  $a \equiv c \pmod{n}$ , d.h., zu zeigen ist, dass ein  $r \in \mathbb{Z}$  existiert sodass  $a - c = rn$ . Wir zählen bei der Differenz  $a - c$  einmal  $b$  dazu und ziehen es einmal ab und verwenden, was wir bisher hergeleitet haben:

$$a - c = a - b + b - c = qn - pn = (q - p)n.$$

D.h. mit  $r = q - p \in \mathbb{Z}$  folgt  $a \sim_n c$ .

□

**Beispiel 5.19.** Sei  $f: X \rightarrow Y$  eine Funktion. Dann ist  $\sim_f \subseteq X \times X$  definiert durch

$$a \sim_f b \iff f(a) = f(b)$$

eine Äquivalenzrelation.

Eine Äquivalenzrelation auf einer Menge  $X$  teilt  $X$  in Teilmengen auf, die Äquivalenzklassen genannt werden.

**Definition 5.20.** Gegeben eine Äquivalenzrelation  $\sim$  auf einer Menge  $X$  und ein Element  $a \in X$  ist die Äquivalenzklasse von  $a$  definiert als

$$[a] := \{b \in X \mid a \sim b\}.$$

Jedes Element der Äquivalenzklasse  $[a]$  kann als Repräsentant der Klasse verwendet werden.

Äquivalenzklassen liefern disjunkte Zerlegungen der gegebenen Menge.

**Definition 5.21.** Eine Partition einer Menge  $M$  ist eine Familie von Mengen  $\{P_i \mid i \in \mathcal{I}\}$  ( $\mathcal{I}$  bezeichnet eine Indexmenge) sodass

1.  $\forall i \in \mathcal{I} : P_i \neq \emptyset$ ,
2.  $\forall m \in M \exists! P_i : m \in P_i$ .

**Satz 5.22.** Für jede Äquivalenzrelation  $\sim$  auf einer Menge  $X$  ist die Familie der Äquivalenzklassen  $\{[a] \mid a \in X\}$  eine Partition von  $X$ .

**Beispiel 5.23.** Auf  $\mathbb{Z}$  definieren wir die Äquivalenzrelation

$$a \sim b \iff a \equiv b \pmod{5}.$$

Durch diese Relation werden die ganzen Zahlen in die folgenden fünf Äquivalenzklassen partitioniert:

$$\begin{aligned} &= \{5q \mid q \in \mathbb{Z}\} = \{\dots, -10, -5, 0, 5, 10, \dots\} \\ [1] &= \{5q + 1 \mid q \in \mathbb{Z}\} = \{\dots, -9, -4, 1, 6, 11, \dots\} \\ [2] &= \{5q + 2 \mid q \in \mathbb{Z}\} = \{\dots, -8, -3, 2, 7, 12, \dots\} \\ [3] &= \{5q + 3 \mid q \in \mathbb{Z}\} = \{\dots, -7, -2, 3, 8, 13, \dots\} \\ [4] &= \{5q + 4 \mid q \in \mathbb{Z}\} = \{\dots, -6, -1, 4, 9, 14, \dots\} \end{aligned}$$

Jede ganze Zahl liegt in genau einer Äquivalenzklasse. Die Wahl der Repräsentanten aus der jeweiligen Klasse ist dabei beliebig, z.B. gilt

$$[0] = [5] = [105] = [-45] = \dots$$

oder

$$[2] = [12] = [-38] = [-3] = \dots$$

Üblicherweise werden "einfache" Repräsentanten gewählt, also zum Beispiel wie oben

$$[0], [1], [2], [3], [4]$$

oder alternativ

$$[-2], [-1], [0], [1], [2]$$

## 5.2 Ordnungsrelationen

**Definition 5.24.** Eine Relation  $R$  auf einer Menge  $X$  heisst eine Ordnungsrelation genau dann, wenn  $R$  reflexiv, antisymmetrisch und transitiv ist. In diesem Fall heisst  $(X, R)$  eine geordnete Menge. Gilt ausserdem

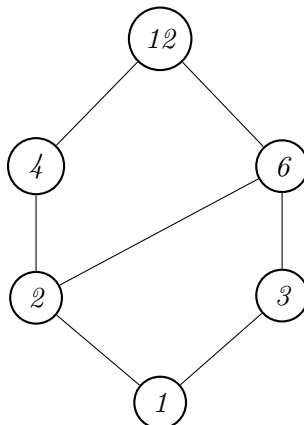
$$\forall x, y \in X : xRy \vee yRx$$

so heisst  $R$  Totalordnung.

D.h. eine Ordnungsrelation ist eine Totalordnung, wenn je zwei beliebige Elemente der Menge  $X$  vergleichbar sind. Eine Ordnungsrelation, die keine Totalordnung ist wird auch *Halbordnung* genannt.

**Beispiel 5.25.** Die Teilbarkeitsrelation aus Beispiel 5.3 ist eine Ordnungsrelation, aber keine Totalordnung. Die Eigenschaften einer Ordnungsrelation haben wir bereits gezeigt. Die Relation ist keine Totalordnung, da nicht alle Elemente miteinander vergleichbar sind. Zum Beispiel gilt weder  $3 \mid 4$  noch gilt  $4 \mid 3$ .

Ordnungsrelationen werden üblicherweise durch sogenannte Hasse-Diagramme dargestellt. Dabei wird auf die Kanten verzichtet, die sich durch Reflexivität oder Transitivität ergeben:



**Beispiel 5.26.** Die Relation  $R$  aus Beispiel 5.5 auf  $X = P(\{1, 2\})$  definiert als

$$aRb \iff a \subseteq b$$

ist eine Ordnungsrelation, aber keine Totalordnung. Wir überprüfen die Eigenschaften einer Ordnungsrelation:

- *Reflexivität:* Für jede Menge gilt, dass sie Teilmenge von sich selbst ist, d.h.  $a \subseteq a$  und somit ist  $R$  reflexiv.
- *Antisymmetrie:* Seien  $a, b \in X$  mit  $a \subseteq b$  und  $b \subseteq a$ . Das ist genau die Definition der Gleichheit von Mengen (siehe Kapitel 1, somit gilt  $a = b$  und die Relation ist folglich antisymmetrisch.
- *Transitivität:* Seien  $a, b, c \in X$  mit  $a \subseteq b$  und  $b \subseteq c$ . Sei  $x \in a$  ein beliebiges Element aus  $a$ . Da  $a \subseteq b$  ist, gilt  $x \in b$ . Da  $b \subseteq c$  ist, gilt  $x \in c$ . Da  $x$  ein beliebiges Element aus  $a$  war folgt  $a \subseteq c$  und die Relation ist somit transitiv.

Die Relation ist keine Totalordnung, da nicht alle Mengen miteinander vergleichbar sind. Zum Beispiel ist  $\{1\}$  weder eine Teilmenge von  $\{2\}$  noch ist  $\{2\}$  eine Teilmenge von  $\{1\}$ .

**Beispiel 5.27.** Die Relation  $\trianglelefteq \subseteq \mathbb{N}^2 \times \mathbb{N}^2$  definiert durch

$$(a, b) \trianglelefteq (c, d) \iff (a < c) \vee (a = c \wedge b \leq d)$$

ist eine Totalordnung. Zuerst überprüfen wir die Eigenschaften einer Ordnungsrelation:

- *Reflexivität:* Seien  $a, b \in \mathbb{N}$ , dann gilt  $a \leq a$  und  $b \leq b$  und somit  $(a, b) \trianglelefteq (a, b)$
- *Antisymmetrie:* Seien  $a, b, c, d \in \mathbb{N}$  und angenommen es gilt sowohl  $(a, b) \trianglelefteq (c, d)$  als auch  $(c, d) \trianglelefteq (a, b)$ . Da nicht  $a < c$  und  $c < a$  gelten kann, muss  $a = c$  und  $b \leq d \wedge d \leq b$  gelten. Daraus folgt  $b = d$  und damit  $(a, b) = (c, d)$ .
- *Transitivität:* Seien  $a, b, c, d, e, f \in \mathbb{N}$  mit  $(a, b) \trianglelefteq (c, d)$  und  $(c, d) \trianglelefteq (e, f)$ , d.h.,

$$\underbrace{(a < c)}_{=A_1} \vee \underbrace{(a = c \wedge b \leq d)}_{=A_2} \wedge \underbrace{(c < e)}_{=B_1} \vee \underbrace{(c = e \wedge d \leq f)}_{=B_2}.$$

Fallunterscheidung:

- Fall 1:  $A_1 \wedge B_1: a < c \wedge c < e \Rightarrow a < e \Rightarrow (a, b) \trianglelefteq (e, f)$
- Fall 2:  $A_1 \wedge B_2: a < c \wedge c = e \wedge d \leq f \Rightarrow a < e \Rightarrow (a, b) \trianglelefteq (e, f)$
- Fall 3:  $A_2 \wedge B_1: a = c \wedge b \leq d \wedge c < e \Rightarrow a < e \Rightarrow (a, b) \trianglelefteq (e, f)$
- Fall 4:  $A_2 \wedge B_2: a = c \wedge b \leq d \wedge c = e \Rightarrow d \leq f \Rightarrow a = e \wedge b \leq f \Rightarrow (a, b) \trianglelefteq (e, f)$

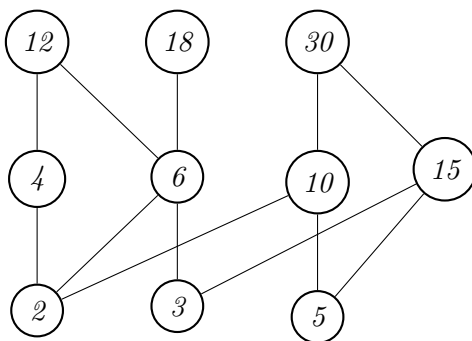
$\trianglelefteq$  ist eine Totalordnung: Seien  $(a, b), (c, d) \in \mathbb{N}^2$ . Für  $a, c$  gilt entweder  $a < c$ ,  $a > c$  oder  $a = c$ . Im ersten Fall ist  $(a, b) \trianglelefteq (c, d)$ , im zweiten Fall  $(c, d) \trianglelefteq (a, b)$ . Im dritten Fall betrachten wir  $b, d$ . Auch hier gilt  $b < d$  oder  $b > d$  oder  $b = d$ . Hier gilt im ersten Fall  $(a, b) \trianglelefteq (c, d)$ , im zweiten  $(c, d) \trianglelefteq (a, b)$  und im dritten gilt beides. Zwei beliebige Elemente sind also immer vergleichbar.

**Definition 5.28.** Sei  $\preceq$  eine Ordnungsrelation auf  $X$ :

- Ein Element  $m \in X$  heisst minimales Element, wenn für alle  $x \in X$  mit  $x \preceq m$  gilt  $x = m$ .
- Ein Element  $k \in X$  heisst kleinstes Element, wenn für alle  $x \in X$  gilt  $k \preceq x$ .
- Ein Element  $M \in X$  heisst maximales Element, wenn für alle  $x \in X$  mit  $M \preceq x$  gilt  $x = M$ .
- Ein Element  $g \in X$  heisst grösstes Element, wenn für alle  $x \in X$  gilt  $x \preceq g$ .

**Beispiel 5.29.** Für die Teilbarkeitsrelation aus Beispiel 5.3 auf der Menge  $X = \{1, 2, 3, 4, 6, 12\}$ , gilt 1 ist das minimale und das kleinste Element und 12 ist das maximale und das grösste Element. In diesem Beispiel gibt es nur ein minimales Element, das mit dem kleinsten Element übereinstimmt, da 1 mit allen anderen Zahlen in  $X$  vergleichbar ist. Da Teilbarkeit keine Totalordnung ist, muss das Gleiche aber nicht für Teilbarkeit als Relation auf beliebigen Mengen gelten.

Sei  $Y = \{2, 3, 5, 4, 6, 10, 12, 15, 18, 30\}$  und  $R \subseteq Y \times Y$  gegeben durch  $xRy \Leftrightarrow x \mid y$ .



Die minimalen Elemente in  $Y$  bezüglich der Relation  $R$  sind  $\{2, 3, 5\}$ , die maximalen Elemente sind  $\{12, 18, 30\}$ . Es gibt weder ein kleinstes noch ein grösstes Element.

**Beispiel 5.30.** Wir betrachten die Relation aus Beispiel 5.27 auf  $X = \{0, 1, 2\}^2$ . Auf dieser Teilmenge gilt:

$$(0, 0) \trianglelefteq (0, 1) \trianglelefteq (0, 2) \trianglelefteq (1, 0) \trianglelefteq (1, 1) \trianglelefteq (1, 2) \trianglelefteq (2, 0) \trianglelefteq (2, 1) \trianglelefteq (2, 2).$$

In  $X$  ist das kleinste Element bezüglich  $\trianglelefteq$  also  $(0, 0)$  und das grösste Element  $(2, 2)$ .

## 6 Elementare Begriffe der Zahlentheorie

### 6.1 Modulare Arithmetik

Wir definieren zu  $n \in \mathbb{N}^*$  die Menge

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}.$$

Diese Menge kann als Menge von Repräsentanten der Äquivalenzrelation *Kongruenz modulo  $n$*  (siehe Satz 5.18) betrachtet werden (oder als die Menge der Zahlen, die als Rest bei einer Division durch  $n$  auftreten können). Addition und Multiplikation können auf dieser Menge so definiert werden, dass jeweils das Ergebnis modulo  $n$  genommen wird.

**Definition 6.1.** Sei  $n \in \mathbb{N}^*$  und seien  $a, b \in \mathbb{Z}_n$ . Wir definieren modulare Addition und modulare Multiplikation durch

$$\begin{aligned} a + b &= (a + b) \pmod{n} \in \mathbb{Z}_n \\ a \cdot b &= (a \cdot b) \pmod{n} \in \mathbb{Z}_n \end{aligned}$$

**Beispiel 6.2.** In  $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$  gilt

$$3 + 4 = 7 \pmod{7} = 0, \quad 3 \cdot 4 = 12 \pmod{7} = 5, \quad 4 \cdot 5 = 20 \pmod{7} = 6, \dots$$

**Beispiel 6.3.** Additions- und Multiplikationstabelle für  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ :

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Additions- und Multiplikationstabelle für  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

**Definition 6.4.** Sei  $n \in \mathbb{N}^*$ . Das neutrale Element bezüglich (modularer) Addition in  $\mathbb{Z}_n$  ist 0. Zu gegebenem  $a \in \mathbb{Z}_n$  ist die additive Inverse definiert als jenes  $b \in \mathbb{Z}_n$  für das gilt

$$a + b = 0 \pmod{n}.$$

Oft wird für die additive Inverse  $b$  auch  $-a$  geschrieben.

**Satz 6.5.** Sei  $n \in \mathbb{N}^*$ . Jede Zahl  $a \in \mathbb{Z}_n$  besitzt eine eindeutig bestimmte additive Inverse.



**Beispiel 6.6.** Die Caesar-Verschlüsselung nutzt die Eindeutigkeit der additiven Inversen in  $\mathbb{Z}_{26}$  aus. Die Grundidee ist, dass die Buchstaben des Alphabets verschoben werden, zum Beispiel:

A	B	C	D	E	F	G	...	U	V	W	X	Y	Z
F	G	H	I	J	K	L	...	Z	A	B	C	D	E

Buchstaben können als Zahlen in  $\mathbb{Z}_{26}$  codiert werden, d.h.,  $A = 0, B = 1, \dots, Y = 24, Z = 25$ . Das Verschieben der Buchstaben entspricht dann einer modularen Addition, das heißt das Zeichen  $x$  wird mit dem Schlüssel  $k$  zu einem neuen Zeichen  $y$  durch

$$y = x + k \pmod{26}.$$

Eine Verschiebung um fünf Zeichen wie oben entspricht also  $k = 5$  und

A	B	C	D	E	F	G	...	U	V	W	X	Y	Z
0	1	2	3	4	5	6	...	20	21	22	23	24	25
5	6	7	8	9	10	11	...	25	0	1	2	3	4
F	G	H	I	J	K	L	...	Z	A	B	C	D	E

Zum Decodieren muss  $y = x + k \pmod{26}$  nach  $x$  aufgelöst werden, d.h.,  $x = y - k \pmod{26}$  berechnet werden. (Der Schlüssel muss also bekannt sein).

Das verschlüsselte Wort *RFYMJRFPYNP* (in Zahlen: (17, 5, 24, 12, 9, 17, 5, 24, 13, 15)) mit dem Schlüssel  $k = 5$  wird mit

$$17 - 5 \pmod{26} = 12, \quad 5 - 5 \pmod{26} = 0, \quad 24 - 5 \pmod{26} = 19, \dots$$

zu *MATHEMATIK* im Klartext.

**Definition 6.7.** Sei  $n \in \mathbb{N}^*$ . Das neutrale Element bezüglich (modularer) Multiplikation in  $\mathbb{Z}_n$  ist 1. Falls zu gegebenem  $a \in \mathbb{Z}_n$  ein  $b \in \mathbb{Z}_n$  existiert mit

$$a \cdot b = 1 \pmod{n},$$

dann nennt man  $b$  die multiplikative Inverse zu  $a$  und sagen, dass  $a$  in  $\mathbb{Z}_n$  invertierbar ist. Oft wird als Bezeichnung für die multiplikative Inverse  $b$  auch  $\frac{1}{a}$  oder  $a^{-1}$  geschrieben.

Eine multiplikative Inverse muss nicht zu jeder Zahl in  $\mathbb{Z}_n$  existieren. In  $\mathbb{Z}_4$  ist zum Beispiel  $\frac{1}{3} = 3$  (da  $3 \cdot 3 = 1 \pmod{4}$ ), aber  $a = 2$  besitzt keine multiplikative Inverse. In  $\mathbb{Z}_5$ , besitzt jede Zahl ausser 0 eine multiplikative Inverse:

$$\frac{1}{1} = 1, \quad \frac{1}{2} = 3, \quad \frac{1}{3} = 2, \quad \frac{1}{4} = 4.$$

**Satz 6.8.** Sei  $n \in \mathbb{N}^*$  und  $a \in \mathbb{Z}_n$ , so dass  $n$  und  $a$  keinen gemeinsamen Teiler ausser 1 haben (teilerfremd sind). Dann besitzt  $a$  eine multiplikative Inverse in  $\mathbb{Z}_n$ .

**Beispiel 6.9.** In  $\mathbb{Z}_{26}$  sind genau die untenstehenden Zahlen invertierbar:

$x$	1	3	5	7	9	11	15	17	19	21	23	25
$x^{-1}$	1	9	21	15	3	19	7	23	11	5	17	25

**Definition 6.10.** Eine Zahl  $p \in \mathbb{N}^*$  ist genau dann eine Primzahl, wenn die folgenden zwei Bedingungen erfüllt sind

- $p > 1$
- Für alle  $a, b \in \mathbb{N}$  mit  $p = a \cdot b$  gilt  $a = 1$  oder  $b = 1$ .

Die Primzahlen unter 100 sind:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

**Bemerkung 6.11.** Wenn  $p$  eine Primzahl ist, dann ist in  $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$  jede Zahl ungleich 0 invertierbar, da sie keinen gemeinsamen Teiler mit  $p$  hat, z.B. ist in  $\mathbb{Z}_5$  jede Zahl invertierbar, siehe Beispiel 6.3.

**Satz 6.12.** Jede natürliche Zahl grösser als eins ist entweder selbst eine Primzahl oder lässt sich als Produkt von Primzahlen schreiben (Primfaktorenzerlegung). Bis auf die Reihenfolge sind die Faktoren eindeutig bestimmt und heissen Primfaktoren.

**Beispiel 6.13.** Die Primfaktoren können z.B. durch sukzessives Dividieren von Primzahlen beginnend mit dem kleinsten Teiler gewonnen werden:

$$\begin{aligned}28 &= 2 \cdot 14 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7, \\1235 &= \dots = 5 \cdot 13 \cdot 19, \\102432 &= \dots = 2^5 \cdot 3 \cdot 11 \cdot 97.\end{aligned}$$

Modulare Gleichungen der Form  $a+x = b \pmod n$  besitzen für jedes  $n \in \mathbb{N}^*$  eine eindeutig bestimmte Lösung  $x \in \mathbb{Z}_n$ , da die additive Inverse eindeutig bestimmt ist. Für modulare Gleichungen der Form  $a \cdot x = b \pmod n$  gilt

- Falls  $a$  und  $n$  teilerfremd sind, dann besitzt  $a \cdot x = b \pmod n$  die eindeutig bestimmte Lösung  $x = a^{-1} \cdot b \pmod n$ .
- Falls  $a$  und  $n$  einen (nichttrivialen) gemeinsamen Teiler haben, dann kann die Gleichung  $a \cdot x = b \pmod n$  keine oder mehr als eine Lösung besitzen.

**Beispiel 6.14.** Die Gleichung  $4x = 2 \pmod n$  besitzt für  $n = 17$  eine eindeutig bestimmte Lösung. Die multiplikative Inverse von  $a = 4$  in  $\mathbb{Z}_{17}$  ist  $a^{-1} = 13$  ( $4 \cdot 13 = 52 = 3 \cdot 17 + 1$ ). Multiplikation mit  $a^{-1}$  auf beiden Seiten liefert

$$x = 2 \cdot 13 \pmod{17} = 26 \pmod{17} = 1 \cdot 17 + 9 \pmod{17} = 9 \quad (4 \cdot 9 = 36 = 2 \cdot 17 + 2).$$

Für  $n = 6$  besitzt  $4x = 2 \pmod n$  die beiden Lösungen  $x = 2$  und  $x = 5$  ( $4 \cdot 2 = 8 = 1 \cdot 6 + 2$  und  $4 \cdot 5 = 20 = 3 \cdot 6 + 2$ ).

Zu beliebigem  $n \in \mathbb{N}^*$  wird die Menge der invertierbaren Zahlen in  $\mathbb{Z}_n$  mit  $\mathbb{Z}_n^*$  bezeichnet, d.h.,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z}_n : ab = 1\}.$$

Zum Beispiel gilt

$$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\},$$

und für  $p$  eine Primzahl gilt  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ . Die invertierbaren Zahlen in  $\mathbb{Z}_n$  sind genau die Zahlen ungleich 0, die keinen gemeinsamen Teiler mit  $n$  haben, oder anders gesagt, jene Zahlen, deren grösster gemeinsamer Teiler mit  $n$  gleich 1 ist.

## 6.2 Euklidischer Algorithmus und Diophantische Gleichungen

**Definition 6.15.** Seien  $a, b \in \mathbb{Z}$ , nicht beide 0, dann ist der grösste gemeinsame Teiler  $\text{ggT}(a, b)$  (engl.: greatest common divisor, kurz gcd) die grösste ganze Zahl  $d$  mit  $d \mid a$  und  $d \mid b$ .

Das heisst für jede ganze Zahl  $q$  mit  $q \mid a$  und  $q \mid b$  muss gelten, dass  $q \mid \text{ggT}(a, b)$ . Nach Definition ist der grösste gemeinsame Teiler positiv, also eine natürliche Zahl. Außerdem gilt  $\text{ggT}(a, b) = \text{ggT}(|a|, |b|) = \text{ggT}(b, a)$ .

**Definition 6.16.** Zwei Zahlen  $a, b \in \mathbb{Z}$  mit  $\text{ggT}(a, b) = 1$  heissen  $a, b$  relativ prim (oder teilerfremd).

**Satz 6.17.** Seien  $a, b \in \mathbb{Z}$ . Dann gilt  $\text{ggT}(a, b) = \text{ggT}(a - b, b)$ .

*Beweis.* Sei  $d = \text{ggT}(a, b)$ . Dann existieren  $\alpha, \beta \in \mathbb{Z}$  mit  $a = d\alpha$  und  $b = d\beta$  und  $\text{ggT}(\alpha, \beta) = 1$ . Damit gilt  $a - b = d(\alpha - \beta)$  und  $\text{ggT}(a - b, b) = \text{ggT}(d(\alpha - \beta), d\beta) = d \text{ggT}(\alpha - \beta, \beta) = d$ .  $\square$

Noch allgemeiner gilt:

**Satz 6.18.** Seien  $a, b \in \mathbb{Z}$  und  $z \in \mathbb{Z}$ . Dann gilt  $\text{ggT}(a + zb, b) = \text{ggT}(a, b)$ .

Aus diesem Satz folgt ein Algorithmus zur Bestimmung des ggT, der erstmals von Euklid (ca. 360 v. Chr. bis ca. 280 v. Chr.) schriftlich erwähnt wurde und der daher nach ihm benannt ist. Bevor wir den Algorithmus anschreiben führen wir noch formal die Begriffe Quotient und Rest einer Division ein.

**Definition 6.19.** Seien  $x, y \in \mathbb{N}$ . Dann gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}$  mit

$$x = qy + r, \quad \text{und} \quad r < y.$$

Die Zahlen  $q$  und  $r$  heissen Quotient, bzw., Rest der Division von  $x$  durch  $y$ .

Seien  $a, b \in \mathbb{N}$  mit  $a > b$  gegeben. Die Division dieser beiden Zahlen liefert  $q, r \in \mathbb{N}$  mit  $r < b$  sodass

$$a = qb + r \quad \implies \quad r = a - qb.$$

Laut Satz 6.18 gilt

$$\text{ggT}(a, b) = \text{ggT}(a - qb, b) = \text{ggT}(r, b) = \text{ggT}(b, r).$$

Im letzten Schritt wird nur verwendet, dass der ggT symmetrisch ist und wir ordnen die Einträge in absteigender Grösse an. Der  $\text{ggT}(a, b)$  ist auf den  $\text{ggT}$  der kleineren Zahlen  $b, r$  zurückgeführt worden. Dieser Schritt kann rekursiv wiederholt werden: Wir berechnen den  $\text{ggT}(34, 28)$ :

1. Division liefert  $34 = 28 \cdot 1 + 6$ , d.h.,  $q = 1$  und  $r = 6$ . Dann gilt

$$\text{ggT}(34, 28) = \text{ggT}(34 - 28 \cdot 1, 28) = \text{ggT}(6, 28) = \text{ggT}(28, 6)$$

2. Division liefert  $28 = 6 \cdot 4 + 4$ , d.h.,  $q = 4$  und  $r = 4$ . Dann gilt

$$\text{ggT}(28, 6) = \text{ggT}(28 - 6 \cdot 4, 6) = \text{ggT}(4, 6) = \text{ggT}(6, 4)$$

3. Division liefert  $6 = 4 \cdot 1 + 2$ , d.h.,  $q = 1$  und  $r = 2$ . Dann gilt

$$\text{ggT}(6, 4) = \text{ggT}(6 - 4 \cdot 1, 4) = \text{ggT}(2, 4) = \text{ggT}(4, 2)$$

4. Division liefert  $4 = 2 \cdot 2 + 0$ , d.h.,  $q = 2$  und  $r = 0$ . Dann gilt

$$\text{ggT}(4, 2) = \text{ggT}(4 - 2 \cdot 2, 2) = \text{ggT}(0, 2) = \text{ggT}(2, 0) = 2.$$

In jedem Zwischenschritt, sind die Einträge  $x, y$  im  $\text{ggT}(x, y)$  Linearkombinationen von den Eingangszahlen  $a = 34$  und  $b = 28$ , z.B., im ersten Schritt

$$\text{ggT}(a, b) = \text{ggT}(34, 28) = \text{ggT}(34 - 28, 28) = \text{ggT}(28, \underbrace{34 - 28}_{=6}) = \text{ggT}(b, 1 \cdot a + (-1) \cdot b).$$

Im zweiten Schritt erhalten wir:

$$\begin{aligned} \text{ggT}(a, b) &= \text{ggT}(b, r) = \text{ggT}(28, \underbrace{34 - 28}_{=6}) = \text{ggT}(28 - \underbrace{(34 - 28) \cdot 4}_{=6}, \underbrace{34 - 28}_{=6}) \\ &= \text{ggT}(\underbrace{-4 \cdot 34 + 5 \cdot 28}_{=4}, \underbrace{34 - 28}_{=6}) \\ &= \text{ggT}(\underbrace{34 - 28}_{=6}, \underbrace{5 \cdot 28 - 4 \cdot 34}_{=4}) \\ &= \text{ggT}(1 \cdot a + (-1) \cdot b, (-4) \cdot a + 5 \cdot b). \end{aligned}$$

In einer Tabelle können die Koeffizienten der Linearkombinationen mit berechnet werden:

I	34	1	0
II	28	0	1
III = I-II	6	1	-1
IV = II - 4 III	4	-4	5
V = III-IV	2	5	-6
VI = IV-2V	0	-14	17

Aus dieser Tabelle können die Koeffizienten 5 und  $-6$  abgelesen werden, d.h., die Koeffizienten für die Linearkombination

$$\text{ggT}(34, 28) = 2 = 5 \cdot 34 - 6 \cdot 28.$$

Diese Koeffizienten werden *Bézout-Koeffizienten* genannt. In der letzten Zeile können die Koeffizienten abgelesen werden für die Linearkombination aus  $a, b$ , die null ergibt:

$$0 = -14 \cdot 34 + 17 \cdot 28.$$

Diese Koeffizienten werden auch *Syzygien* genannt.

**Satz 6.20.** Seien  $a, b \in \mathbb{N}^*$ . Dann existieren ganze Zahlen  $s, t \in \mathbb{Z}$  mit

$$\text{ggT}(a, b) = s \cdot a + t \cdot b.$$

Diese Zahlen  $(s, t)$  werden Bézout-Koeffizienten genannt.

Der *Erweiterte Euklidische Algorithmus (EEA)* folgt dem Vorgehen aus dem Beispiel und berechnet den grössten gemeinsamen Teiler, sowie die Bézout-Koeffizienten und die Syzygien: Gegeben  $a, b \in \mathbb{N}$  mit  $a > b$ :

1. Initialisierung:  $x_0 = a, x_1 = b, s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$  und  $k = 1$
2. While  $x_k \neq 0$  Do
  - (i)  $q_k = \text{quot}(x_{k-1}, x_k)$  (Quotient der Division von  $x_{k-1}$  durch  $x_k, x_{k-1} = q_k x_k + r_k$ )
  - (ii)  $x_{k+1} = x_{k-1} - q_k x_k$  (Rest der Division,  $r_k = x_{k-1} - q_k x_k$ )
  - (iii)  $s_{k+1} = s_{k-1} - q_k s_k$  und  $t_{k+1} = t_{k-1} - q_k t_k$  (Bestimmung der Linearkoeffizienten)
  - (iv)  $k = k + 1$
3. Return  $\text{ggT}(a, b) = x_{k-1}$ , Bézout-Koeffizienten  $(s_{k-1}, t_{k-1})$ , Syzygien  $(s_k, t_k)$

In jedem Schritt gilt  $x_k = s_k a + t_k b$ .

**Beispiel 6.21.** Wir bestimmen den  $\text{ggT}(126, 81)$  mit dem EEA. Dazu notieren wir in der Tabelle zusätzlich den Schleifenindex  $k$  und den Quotienten  $q$ :

	$k$	$x$	$s$	$t$	$q$
<i>I</i>	0	126	1	0	
<i>II</i>	1	81	0	1	1
<i>III = I-II</i>	2	45	1	-1	1
<i>IV = II-II</i>	3	36	-1	2	1
<i>V = III-IV</i>	4	9	2	-3	4
<i>VI = IV-4 V</i>	5	0	-9	14	

Das heisst,

$$\text{ggT}(126, 81) = 9 = 2 \cdot 126 + (-3) \cdot 81 \quad \text{und} \quad 0 = -9 \cdot 126 + 14 \cdot 81.$$

Der erweiterte Euklidische Algorithmus kann verwendet werden um *ganzzahlige* Lösungen von linearen Gleichungen mit ganzzahligen Koeffizienten zu bestimmen. Solche Gleichungen werden *diophantische Gleichungen* genannt.

**Beispiel 6.22.** Ein Bauer hat 500 Taler gespart, um neue Hühner und Kühe zu kaufen. Auf dem Markt stellt er fest, dass eine Kuh 17 Taler kostet und ein Huhn 5 Taler. Wie viele Hühner und Kühe kann er kaufen, wenn er die ganzen 500 Taler ausgeben möchte?

Schritt 1: Wir berechnen mit EEA den  $\text{ggT}$  von 17 und 5 sowie die Bézout-Koeffizienten,

$$\text{ggT}(17, 5) = 1 = -2 \cdot 17 + 7 \cdot 5 \tag{6.1}$$

und die Syzygien

$$0 = 5 \cdot 17 - 17 \cdot 5. \tag{6.2}$$

Wenn wir die Gleichung 6.1 mit 500 multiplizieren erhalten wir

$$500 = -1000 \cdot 17 + 3500 \cdot 5, \tag{6.3}$$

d.h., wenn der Bauer -1000 Kühe und 3500 Hühner kauft, gibt er genau 500 Taler aus. Dieser Handel dürfte allerdings schwierig werden. Mithilfe der Syzygien kann man feststellen,

ob ganzzahlige, positive Lösungen existieren. Wenn wir (6.2) mit einer beliebigen Zahl  $x$  multiplizieren erhalten wir

$$0 = 5x \cdot 17 - 17x \cdot 5.$$

Diese Gleichung können wir zu (6.3) addieren und erhalten so

$$500 = (-1000 + 5x) \cdot 17 + (3500 - 17x) \cdot 5.$$

Jetzt bleibt festzustellen, ob es ganzzahlige Werte für  $x$  gibt, sodass sowohl  $-1000 + 5x \geq 0$  als auch  $3500 - 17x \geq 0$ . Wir bestimmen für beide Gleichungen, wann sie null werden:

$$-1000 + 5x = 0 \quad \longrightarrow \quad x = 200, \quad \text{und} \quad 3500 - 17x = 0 \quad \longrightarrow \quad x = \frac{3500}{17} \simeq 205.882.$$

Das heisst, wenn  $200 \leq x \leq 205$  gilt, dann sind beide Koeffizienten nichtnegativ. Das sind nur endliche viele Kombinationen, die wir ausprobieren können:

$$\begin{aligned} x = 200 &\longrightarrow 500 = 0 \cdot 17 + 100 \cdot 5 \\ x = 201 &\longrightarrow 500 = 5 \cdot 17 + 83 \cdot 5 \\ x = 202 &\longrightarrow 500 = 10 \cdot 17 + 66 \cdot 5 \\ x = 203 &\longrightarrow 500 = 15 \cdot 17 + 49 \cdot 5 \\ x = 204 &\longrightarrow 500 = 20 \cdot 17 + 32 \cdot 5 \\ x = 205 &\longrightarrow 500 = 25 \cdot 17 + 15 \cdot 5 \end{aligned}$$

**Satz 6.23.** Die diophantische Gleichung  $ax + by = c$  hat genau dann eine ganzzahlige Lösung, wenn  $c$  ein Vielfaches von  $\text{ggT}(a, b)$  ist, d.h.,  $c = q \text{ggT}(a, b)$  für ein  $q \in \mathbb{Z}$ .

Ist  $(x_0, y_0)$  eine ganzzahlige Lösung von  $ax_0 + by_0 = \text{ggT}(a, b)$  (wobei  $x_0, y_0$  als Bézout-Koeffizienten mit dem erweiterten Euklidischen Algorithmus berechnet werden können), dann ist  $(x, y) = (qx_0, qy_0)$  eine Lösung von  $ax + by = q \text{ggT}(a, b)$ .

Alle weiteren ganzzahligen Lösungen der Gleichung sind gegeben durch

$$\left\{ \left( x + \frac{kb}{\text{ggT}(a, b)}, y - \frac{ka}{\text{ggT}(a, b)} \right) \mid k \in \mathbb{Z} \right\}.$$

**Bemerkung 6.24.** Wenn das Ergebnis von Summe oder Produkt zweier ganzen Zahlen  $a, b$  modulo  $n \in \mathbb{N}^*$  gesucht ist, dann spielt es keine Rolle, ob das Ergebnis  $a + b$ , oder,  $a \cdot b$  modulo  $n$  genommen wird, oder ob die Summe oder das Produkt von  $a$  modulo  $n$  mit  $b$  modulo  $n$  berechnet wird und dann das Ergebnis modulo  $n$  genommen wird.

Seien  $a, b \in \mathbb{Z}$  und  $n \in \mathbb{N}^*$ . Wenn  $\alpha, \beta, c \in \mathbb{Z}_n$  so sind, dass

$$a = \alpha \pmod{n} \quad \text{und} \quad b = \beta \pmod{n},$$

dann gibt es  $q, p \in \mathbb{Z}$  mit

$$a = qn + \alpha \quad \text{und} \quad b = pn + \beta.$$

Damit gilt

$$ab = (qn + \alpha)(pn + \beta) = qp n^2 + (\alpha p + \beta q)n + \alpha\beta = \alpha\beta \pmod{n} = c.$$

Als haben wir insgesamt, dass

$$a \cdot b = c \pmod{n} \quad \Leftrightarrow \quad \alpha \cdot \beta = c \pmod{n}.$$

**Satz 6.25.** (Kleiner Satz von Fermat) Sei  $p$  eine Primzahl. Dann gilt für jedes  $x \in \mathbb{Z}$  mit  $\text{ggT}(x, p) = 1$ :

$$x^{p-1} = 1 \pmod{p}.$$

*Beweis.* Sei  $x \in \mathbb{Z}$  mit  $\text{ggT}(x, p) = 1$ . Dann existiert ein  $y \in \mathbb{Z}_p$  sodass  $xy = 1 \pmod{p}$ . Wir definieren (zu  $x$ ) die Funktion

$$f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad f(a) = x \cdot a \pmod{p}.$$

Diese Funktion ist invertierbar, da

$$f(a) = b \Leftrightarrow b = x \cdot a \pmod{p} \Leftrightarrow y \cdot b = xy \cdot a \pmod{p} = a$$

(Bei der letzten Gleichheit haben wir das Ergebnis aus der obigen Bemerkung verwendet.) Da die Funktion invertierbar ist, ist sie bijektiv, d.h., jedem  $a \in \mathbb{Z}_p$  wird genau ein  $b \in \mathbb{Z}_p$  zugeordnet. Damit wird die Menge  $\{x, 2x, 3x, \dots, (p-1)x\}$  bijektiv auf die Menge  $\{1, 2, 3, \dots, p-1\}$  abgebildet und das Produkt über jeweils alle Zahlen aus diesen Mengen stimmt modulo  $p$  überein:

$$\begin{aligned} x \cdot 2x \cdot 3x \cdots (p-1)x &= 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ \Leftrightarrow x^{p-1} \cdot 2 \cdot 3 \cdots (p-1) &= 2 \cdot 3 \cdots (p-1) \pmod{p} \\ \Leftrightarrow x^{p-1} &= 1 \pmod{p}. \end{aligned}$$

Im letzten Schritt wird auf beiden Seiten mit den multiplikativen Inversen von  $2, 3, \dots, p-1$  (die existieren, da  $p$  eine Primzahl ist) multipliziert. Die letzte Identität ist genau was zu zeigen war.  $\square$

Als Anwendung betrachten wir das Grundkonzept von *Verschlüsselung mit dem RSA-Algorithmus* (Rivest-Shamir-Adleman). Mehr Details und Varianten findet man zum Beispiel im Buch von Teschl&Teschl und den dort aufgeführten Referenzen. Bei der RSA-Verschlüsselung handelt es sich um ein *public key Verschlüsselungsverfahren*, d.h., es gibt einen öffentlichen Schlüssel (public key) und einen privaten Schlüssel (private key).

Wenn Alice eine Nachricht von Bob empfangen will, stellt sie einen öffentlichen Schlüssel  $e$  (wie *encrypt*) zur Verfügung mit dem Bob seine Nachricht codiert und an Alice schickt. Alice verfügt über ihren private key  $d$  (wie *decrypt*), mit dem sie die Nachricht wieder in Klartext übersetzt.

Die Schlüssel werden wie folgt erzeugt:

1. Alice wählt zwei (grosse) unterschiedliche Primzahlen  $p, q$  und berechnet  $n = p \cdot q$  und  $m = (p-1)(q-1)$ .
2. Für den public key wählt Alice eine Zahl  $e$  mit  $\text{ggT}(e, m) = 1$ .
3. Für den private key berechnet sie  $d$  mit  $ed = 1 \pmod{m}$  (so ein  $d$  muss existieren, da  $e$  und  $m$  teilerfremd sind).
4. Alice schickt als public key das Paar  $(n, e)$  an Bob und behält als private key  $(n, d)$ . Die Zahlen  $p, q, m$  werden nicht mehr gebraucht.

Die verschlüsselte Nachricht wird wie folgt erstellt:

1. Bob codiert seine Nachricht (nach einem Alice bekannten System) als eine Zahl  $x < n$ .

2. Bob konstruiert aus  $x$  mit dem public key die verschlüsselte Nachricht  $y$  durch

$$y = x^e \pmod n.$$

Alice verwendet dann ihren private key um die Originalnachricht (oder zumindest deren Zahlencode) zu rekonstruieren:

$$x = y^d \pmod n.$$

Warum funktioniert das? Aus Bemerkung 6.24 folgt, dass  $y^d = (x^e)^d \pmod n$ . Weiters folgt aus  $ed = 1 \pmod m$ , dass  $ed = km + 1$  für ein  $k \in \mathbb{N}$ , d.h.,

$$(x^e)^d = x^{ed} = x^{km+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot x^{\ell(p-1)} = x \cdot (x^{p-1})^\ell,$$

mit  $\ell = k(q-1)$ . Wenn  $x$  und  $p$  einen gemeinsamen Teiler besitzen, dann ist  $x \cdot x^{\ell(p-1)} = 0 \pmod p$ . Wenn  $x$  und  $p$  teilerfremd sind, dann gilt nach dem kleinen Satz von Fermat, dass  $x \cdot x^{\ell(p-1)} = x \cdot 1^\ell = x \pmod p$ . In beiden Fällen gilt also  $x^{ed} = x \pmod p$ . Analog gilt  $x^{ed} = x \pmod q$ . Aus diesen beiden Identitäten folgt, dass sowohl  $p$  als auch  $q$  Teiler von  $x^{ed} - x$  sind, d.h., dass ein  $k_3 \in \mathbb{N}$  existiert sodass:

$$y^d - x = x^{ed} - x = k_1p \quad \text{und} \quad x^{ed} - x = k_2q \quad \implies x^{ed} - x = k_3pq = k_3n,$$

und damit gilt  $y^d = k_3n + x$  und damit  $y^d = x \pmod n$ .

**Beispiel 6.26.** Bob will das Wort "MATHEMATIK" an Alice schicken. Dazu codiert er die einzelnen Buchstaben als Ziffern in  $\mathbb{Z}_{26}$  (wie in Beispiel 6.6), d.h., in das Zahlentupel (12, 0, 19, 7, 4, 12, 0, 19, 8, 10).

Inzwischen konstruiert Alice ihre Schlüssel: sie wählt  $p = 73$  und  $q = 59$  und damit sind  $n = pq = 4307$  und  $m = (p-1)(q-1) = 4176$ . Für den public key wählt sie  $e = 107$  und berechnet die multiplikative Inverse in  $\mathbb{Z}_m$ ,  $d = 2771$ . Den public key (4307, 107) stellt sie Bob zur Verfügung. Bob rechnet

$$12^{107} = 2967517762021717 \dots 9198623553884143178743808 = 3352 \pmod{4307},$$

und erhält insgesamt das codierte Tupel (3352, 0, 123, 2680, 2318, 3352, 0, 123, 940, 2679).

Die Grundidee des RSA-Algorithmus beruht darauf, dass Primzahlen schnell zu multiplizieren sind, aber Primfaktorenzerlegung (im allgemeinen) für grosse Zahlen sehr aufwändig ist. Wenn die Primfaktoren von  $n$  berechnet werden können, dann kann der Code gebrochen werden.

## 6.3 Stellenwertsysteme

Um Zahlen anzuschreiben verwenden wir üblicherweise das *Dezimalsystem*, in dem Zahlen zur Basis 10 dargestellt werden mit Ziffern 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, also zum Beispiel

$$15079 = 1 \cdot 10^4 + 5 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10^1 + 9 \cdot 10^0.$$

Die Schreibweise 15679 notiert also nur wie oft die verschiedenen Potenzen vorkommen, wobei die höchste Potenz am weitesten links und die niedrigste Potenz am weitesten rechts steht. Das gilt auch für Dezimalzahlen mit Nachkommastellen, wobei der Übergang von nichtnegativen zu negativen Potenzen durch einen Punkt/ein Komma markiert wird, also zum Beispiel

$$17.361 = 1 \cdot 10^1 + 7 \cdot 10^0 + 3 \cdot 10^{-1} + 6 \cdot 10^{-2} + 1 \cdot 10^{-3}.$$



**Definition 6.27.** *Eine Zahl in der Darstellung*

$$a_n \cdots a_0 \cdot a_{-1} \cdots a_{-m} = \sum_{k=-m}^n a_k 10^k, \quad a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

heisst Dezimalzahl.

Statt 10 kann auch jede andere Zahl  $b \in \mathbb{N}^*$  als Basis verwendet werden mit Ziffern aus  $\mathbb{Z}_b$  (oder aus einer Menge  $Z$  für die es eine bijektive Abbildung zwischen  $Z$  und  $\mathbb{Z}_b$  gibt). Das heisst die Zahlen werden in der Form

$$a_n \cdots a_0 \cdot a_{-1} \cdots a_{-m} = \sum_{k=-m}^n a_k b^k$$

angeschrieben mit Ziffern  $a_k \in \mathbb{Z}_b$  oder  $a_k \in Z$ .

Im *Binärsystem* wird die Basis  $b = 2$  verwendet mit Ziffern aus  $\mathbb{Z}_2 = \{0, 1\}$ , also zum Beispiel

$$15_{(10)} = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 1111_{(2)}$$

$$20_{(10)} = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1001_{(2)}$$

$$15679_{(10)} = 11111100101111_{(2)}$$

Wenn wir Verwirrung vermeiden und die Basis explizit angeben wollen, dann wird das wie oben durch einen Index ( $b$ ) angezeigt. Die Ziffern können durch sukzessives Dividieren durch die Basis gewonnen werden, zum Beispiel

$$15 = q \cdot 2 + r = 7 \cdot 2 + 1.$$

Der Rest der ersten Division liefert den Koeffizienten  $a_0 = 1$ . Der Quotient wird weiter durch 2 geteilt, wir erhalten den Koeffizienten  $a_1$  und dieser Prozess wird fortgeführt bis der Quotient 0 wird:

$$7 = 3 \cdot 2 + 1 \quad \Rightarrow \quad a_1 = 1$$

$$3 = 1 \cdot 2 + 1 \quad \Rightarrow \quad a_2 = 1$$

$$1 = 0 \cdot 2 + 1 \quad \Rightarrow \quad a_3 = 1$$

Im *Hexadezimalsystem* wird die Basis  $b = 16$  verwendet. Statt als Ziffern  $\mathbb{Z}_{16} = \{0, 1, 2, \dots, 13, 14, 15\}$  zu verwenden, werden die einstelligen Zeichen der gleichmächtigen Menge  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$  benutzt, also zum Beispiel

$$15679_{(10)} = 3 \cdot 16^3 + 13 \cdot 16^2 + 3 \cdot 16^1 + 15 \cdot 16^0 = 3D3F_{(16)}.$$

Das Hexadezimalsystem wird u.a. oft verwendet um RGB-Farbcodes anzugeben. Ein RGB-Code besteht aus drei Zahlen, die den Prozentsatz angeben in dem die Farben rot, blau und grün in der Mischung vorkommen, also zum Beispiel durch Zahlen zwischen 0 und 1, oder durch ganze Zahlen von 0 bis 255, die oft im Hexadezimalsystem angegeben werden. Das blau im RISC-Logo zum Beispiel hat den RGB-Code (66, 88, E6) (oder (102, 136, 230)).

# 7 Algebren

## 7.1 Algebraische Strukturen

**Definition 7.1.** Eine binäre Operation  $\circ$  auf einer Menge  $A$  ist eine Funktion von  $A \times A$  nach  $A$ .

Die Eigenschaft, dass das Bild der Operation auf  $A$  eine Teilmenge von  $A$  ist nennt man *Abgeschlossenheit* ( $\circ$  ist abgeschlossen auf  $A$ ).

**Beispiel 7.2.** 1.  $+$ :  $\mathbb{N} \times \mathbb{N}, (a, b) \mapsto a + b$  ist eine Operation

2.  $-$ :  $\mathbb{N} \times \mathbb{N}, (a, b) \mapsto a - b$  ist keine Operation, da zum Beispiel  $(2, 4)$  auf  $-2 \notin \mathbb{N}$  abgebildet wird

3. Sei  $A$  eine Menge, dann ist  $\cap: P(A) \times P(A) \rightarrow P(A)$  eine Operation: seien  $B, C \in P(A)$ , d.h.,  $B \subseteq A$  und  $C \subseteq A$ . Dann ist auch der Durchschnitt  $B \cap C$  eine Teilmenge von  $A$  (eventuell die leere Menge) und damit  $B \cap C \in P(A)$ .

4. Sei  $X = \{W, F\}$ , dann ist  $\wedge: X \times X \rightarrow X$  eine Operation.

Eine Algebra wird bestimmt durch

- *Objekte:* Elemente einer nichtleeren Menge (Trägermenge)
- *Grundoperationen:* im einfachsten Fall eine binäre (zweistellige) Operation
- *Gesetze:* beschreiben die Eigenschaften von Objekten, die Beziehungen zwischen Operationen, ...

**Definition 7.3.** Sei  $A$  eine Menge und  $\circ$  eine (binäre) Operation auf  $A$ . Dann nennt man das Paar  $(A, \circ)$  eine Algebra.

**Beispiel 7.4.** Die Paare  $(\mathbb{N}, +)$ ,  $(P(X), \cap)$  (wenn  $X$  eine Menge ist) sind Algebren.

**Definition 7.5.** Sei  $\circ$  eine Operation auf einer Menge  $A$ . Dann nennt man  $\circ$

- kommutativ wenn  $\forall a, b \in A: a \circ b = b \circ a$ .
- assoziativ wenn  $\forall a, b, c \in A: (a \circ b) \circ c = a \circ (b \circ c)$ .

Die Operation besitzt ein neutrales Element, wenn ein  $e \in A$  existiert sodass für alle  $a \in A$  gilt

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

Algebren können in verschiedene Klassen eingeteilt werden, je nachdem welche Eigenschaften sie besitzen.

**Definition 7.6.** Eine Algebra  $(A, \circ)$  heisst Halbgruppe, falls die Operation  $\circ$  assoziativ ist. Eine Halbgruppe  $(A, \circ)$  heisst ein Monoid, falls sie ein neutrales Element besitzt. Wenn  $\circ$  ausserdem kommutativ ist spricht man von einer kommutativen Halbgruppe (einem kommutativen Monoid).

**Beispiel 7.7.** •  $(\mathbb{N}, +)$  ist eine Halbgruppe, da für alle  $a, b, c \in \mathbb{N}$  gilt  $(a + b) + c = a + (b + c)$ .  $(\mathbb{N}, +)$  ist ausserdem ein Monoid, mit  $e = 0$  als neutralem Element.

- $(\mathbb{N}^*, +)$  ist eine Halbgruppe, aber kein Monoid.
- Sei  $A$  eine Menge. Dann ist  $(P(A), \cup)$  eine Halbgruppe, da Vereinigung assoziativ ist (siehe Satz 1.8(2)).  $(P(A), \cup)$  ist ausserdem ein Monoid mit neutralem Element  $\emptyset$ : für jede Teilmenge  $B$  von  $A$  (d.h. für jedes Element  $B \in P(A)$ ) gilt  $B \cup \emptyset = B$ .
- Sei  $A$  eine Menge. Dann ist  $(P(A), \cap)$  eine Halbgruppe, da Durchschnittsbildung assoziativ ist (siehe Satz 1.8(2)).  $(P(A), \cap)$  ist ausserdem ein Monoid mit neutralem Element  $A$ : für jede Teilmenge  $B$  von  $A$  (d.h. für jedes Element  $B \in P(A)$ ) gilt  $B \cap A = B$ .
- $(\mathbb{Q}, \cdot)$  ist ein Monoid (mit neutralem Element 1).
- $(\mathbb{Z}, -)$  ist eine Algebra, da die ganzen Zahlen unter Differenzbildung abgeschlossen sind, aber es ist keine Halbgruppe, weil die Operation nicht assoziativ ist:

$$(3 - 4) - 7 = -8 \quad \text{aber} \quad 3 - (4 - 7) = 6.$$

**Definition 7.8.** Sei  $(A, \circ)$  ein Monoid mit neutralem Element  $e$ . Dann heisst  $a \in A$  invertierbar, wenn

$$\exists b \in A: a \circ b = b \circ a = e.$$

In dem Fall heisst  $b$  das zu  $a$  inverse Element.

**Definition 7.9.** Ein Monoid  $(G, \circ)$  heisst Gruppe, wenn jedes  $g \in G$  invertierbar ist. Wenn die Operation  $\circ$  ausserdem kommutativ ist, dann nennt man  $(G, \circ)$  eine Abelsche Gruppe (oder kommutative Gruppe).

**Bemerkung 7.10.** Das neutrale Element einer Gruppe wird auch Einselement genannt. Bezeichnet man das Operationssymbol in einer kommutativen Gruppe mit  $+$ , so nennt man die Algebra oft auch Modul. Das neutrale Element nennt man dann Nullelement.

In einer Gruppe  $(G, \cdot)$  bezeichnet man das inverse Element zu  $g \in G$  mit  $g^{-1}$ , in einem Modul  $(G, +)$  mit  $-g$ .

**Beispiel 7.11.** •  $(\mathbb{Q}, \cdot)$  ist eine Abelsche Gruppe.

- $(\mathbb{N}, \cdot)$  ist ein Monoid (mit neutralem Element 1), aber keine Gruppe (nur 1 ist invertierbar).
- $(\mathbb{Z}_n, +)$  ist eine kommutative Gruppe (ein kommutatives Modul) für jedes  $n \in \mathbb{N}^*$ .
- $(\mathbb{Z}_p, \cdot)$  ist nur dann eine Abelsche Gruppe, wenn  $p$  eine Primzahl ist, da nur dann jedes Element in  $\mathbb{Z}_p$  eine multiplikative Inverse besitzt.

Als nächstes betrachten wir Algebren mit zwei Operationen.

**Definition 7.12.** Sei  $A$  eine Menge auf der die beiden Operationen  $+$  und  $\circ$  definiert sind. Dann ist  $\circ$  distributiv bezüglich  $+$  auf  $A$  wenn für alle  $a, b, c \in A$  gilt

$$a \circ (b + c) = (a \circ b) + (a \circ c).$$

**Beispiel 7.13.** • Auf  $\mathbb{N}$  ist die Multiplikation  $\cdot$  distributiv bezüglich der Addition  $+$ :

$$a(b + c) = ab + ac, \quad \forall a, b, c \in \mathbb{N}.$$

- Auf  $\mathbb{N}$  ist die Addition, nicht distributiv bezüglich der Multiplikation da  $a + (bc) \neq (a + b)(a + c)$ .
- Sei  $M$  eine Menge und  $X = P(M)$ . Dann ist  $\cup$  distributiv bezüglich  $\cap$  auf  $X$ , da laut Satz 1.8(3) für jedes  $A, B, C \in X$  gilt

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

- Sei  $M$  eine Menge und  $X = P(M)$ . Dann ist  $\cap$  distributiv bezüglich  $\cup$  auf  $X$ , da laut Satz 1.8(r) für jedes  $A, B, C \in X$  gilt

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

**Definition 7.14.** Eine Algebra  $(A, +, \circ)$  heisst Ring, wenn  $(A, +)$  eine abelsche Gruppe ist und  $(A, \circ)$  eine Halbgruppe ist und wenn für alle  $a, b, c \in A$  gilt

$$a \circ (b + c) = a \circ b + a \circ c \quad \text{und} \quad (b + c) \circ a = b \circ a + c \circ a,$$

d.h., wenn das Distributivgesetz gilt. Wenn  $\circ$  ausserdem kommutativ ist, nennt man  $(A, +, \circ)$  einen kommutativen Ring. Falls  $(A, \circ)$  ein Einselement besitzt (d.h., wenn  $(A, \circ)$  ein Monoid ist), dann nennt man  $(A, +, \circ)$  einen Ring mit Einselement (oder Ring mit Eins).

**Beispiel 7.15.** •  $(\mathbb{Z}, +, \cdot)$  ist ein kommutativer Ring mit Einselement.

- $(\{W, F\}, \vee, \wedge)$  ist ein kommutativer Ring mit Einselement:

–  $(\{W, F\}, \vee)$  ist eine Abelsche Gruppe:

$$\begin{aligned} (A \vee B) \vee C &= A \vee (B \vee C) && \Rightarrow && \text{Halbgruppe (assoziativ)} \\ A \vee F &= F \vee A = A && \Rightarrow && \text{Monoid (neutrales Element)} \\ A \vee A^c &= A^c \vee A = W && \Rightarrow && \text{jedes Element ist invertierbar} \\ A \vee B &= B \vee A && \Rightarrow && \text{kommutativ} \end{aligned}$$

$(\{W, F\})$  ist eine Halbgruppe ( $\wedge$  ist assoziativ), das Distributivgesetz gilt laut Satz 2.2,

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C).$$

Ausserdem ist  $\wedge$  kommutativ und  $W$  ist das Einselement, d.h.,  $A \wedge W = W \wedge A = A$ .

**Definition 7.16.** Ein kommutativer Ring  $(A, +, \circ)$  heisst Körper, falls  $(A \setminus \{0\}, \circ)$  eine Gruppe ist. (Hier steht 0 für das neutrale Element bezüglich Addition.)

Ein kommutativer Ring ist also genau dann ein Körper, wenn jedes Element auch bezüglich  $\circ$  invertierbar ist.

**Beispiel 7.17.** •  $(\mathbb{R}, +, \cdot)$  ist ein Körper.

- $(\mathbb{Z}_n, +, \cdot)$  ist ein kommutativer Ring mit Einselement.  $(\mathbb{Z}_n, +, \circ)$  ist genau dann ein Körper, wenn  $n$  eine Primzahl ist.
- $(\mathbb{Z}, +, \cdot)$  ist ein kommutativer Ring mit Eins, aber kein Körper.

## 7.2 Abbildungen zwischen algebraischen Strukturen

Ein Homomorphismus ist *strukturerhaltende* Abbildung.

**Definition 7.18.** Seien  $(A_1, \circ_1)$  und  $(A_2, \circ_2)$  zwei algebraische Strukturen. Dann nennt man  $\varphi$  einen Homomorphismus zwischen  $A_1$  und  $A_2$ , wenn für alle  $x, y \in A_1$  gilt:

$$\varphi(x \circ_1 y) = \varphi(x) \circ_2 \varphi(y).$$

Sind  $(A_1, \circ_1)$  und  $(A_2, \circ_2)$  Gruppen, dann nennt man  $\varphi$  einen Gruppenhomomorphismus.

**Beispiel 7.19.** Die Abbildung  $\varphi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_5, +)$  mit  $x \mapsto x \pmod{5}$  ist ein Homomorphismus (die Addition in  $(\mathbb{Z}_5, +)$  ist die modulare Addition). Seien  $x, y \in \mathbb{Z}$ . Dann ist zu zeigen, dass

$$(x + y) \pmod{5} = \varphi(x + y) = \varphi(x) + \varphi(y) = (x \pmod{5}) + (y \pmod{5}).$$

Bezeichnen wir mit  $a, b \in \mathbb{Z}_5$  jene Zahlen für die gilt

$$a = x \pmod{5} = \varphi(x) \quad \text{und} \quad b = y \pmod{5} = \varphi(y),$$

d.h., es existieren ganze Zahlen  $p, q$  sodass

$$x = 5p + a \quad \text{und} \quad y = 5q + b.$$

Damit gilt

$$\varphi(x+y) = (x+y) \pmod{5} = (5p+a+5q+b) \pmod{5} = (a+b)+5(p+q) \pmod{5} = a+b = \varphi(x)+\varphi(y).$$

Durch einen Gruppenhomomorphismus  $\varphi$  zwischen  $(G_1, \circ_1)$  und  $(G_2, \circ_2)$  wird das Einselement von  $G_1$  auf das Einselement von  $G_2$  abgebildet: sei  $g \in G_1$ , und sei  $e_1$  das Einselement von  $G_1$  und  $e_2$  das Einselement von  $G_2$ , dann gilt

$$\varphi(g) = \varphi(g \circ_1 e_1) = \varphi(g) \circ_2 \varphi(e_1),$$

also muss  $\varphi(e_1) = e_2$  gelten. Ausserdem werden die Inversen von Elementen aus  $G_1$  auf die Inversen der Abbildung unter  $G_2$  abgebildet, d.h., für  $g \in G_1$  gilt

$$\varphi(g^{-1}) = \varphi(g^{-1} \circ_2 \varphi(g) \circ_2 \varphi(g)^{-1}) = \varphi(g^{-1} \circ_1 g) \circ_2 \varphi(g)^{-1} = \varphi(e_1) \circ_2 \varphi(g)^{-1} = e_2 \circ_2 \varphi(g)^{-1} = \varphi(g)^{-1}.$$

**Beispiel 7.20.** Für den Homomorphismus aus Beispiel 7.19 gilt:  $\varphi(1) = 1$  und zu  $x \in \mathbb{Z}$  mit  $x = 5q + a$  (für ein  $q \in \mathbb{Z}$ ) gilt

$$\varphi(-x) = \varphi(-5q - a) = -a.$$

**Definition 7.21.** Ein Homomorphismus  $\varphi$  zwischen zwei algebraischen Strukturen  $(A_1, \circ_1)$  und  $(A_2, \circ_2)$  heisst ein Isomorphismus, wenn die Abbildung ausserdem bijektiv ist. Wenn  $(A_1, \circ_1)$  und  $(A_2, \circ_2)$  beide Gruppen sind, dann nennt man  $\varphi$  einen Gruppenisomorphismus. Wenn es einen Isomorphismus zwischen  $(A_1, \circ_1)$  und  $(A_2, \circ_2)$  gibt, dann nennt man die beiden Algebren isomorph und schreibt  $A_1 \simeq A_2$ .

Isomorph bedeutet

- gleich bis auf die Bezeichnung der Objekte
- nicht unterscheidbar aus der Sicht der Algebra
- alle algebraischen Elemente bleiben erhalten (z.B. die Ordnung eines Elements)
- die Verknüpfungstabellen sind identisch (bis auf Umbenennung der Objekte)

## 8 Übungsaufgaben

1. Seien  $A, B$  Mengen. Wir definieren die *symmetrische Differenz* als

$$A\Delta B = (A\setminus B) \cup (B\setminus A).$$

- (a) Stellen Sie die symmetrische Differenz  $A\Delta B$  mittels Venn-Diagramm dar.  
(b) Zeigen Sie, dass die symmetrische Differenz assoziativ ist mittels Venn-Diagrammen, d.h., zeigen Sie dass

$$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

2. Zeigen Sie mittels Venn-Diagrammen, dass

$$(A\Delta B) \cap C = (A \cap C) \Delta (B \cap C).$$

3. Seien  $A = P(\{1, 3, 8\})$  und  $B = P(\{1, 2\})$ .

- (a) Geben Sie  $A$  und  $B$  explizit an.  
(b) Bestimmen Sie  $A \cup B$ ,  $A \cap B$ ,  $A \setminus B$ ,  $B \setminus A$ .

4. Gegeben sind die reellen Intervalle  $I_1 = ]0, 1[$  und  $I_2 = [-\frac{1}{3}, 2[$ .

- (a) Bestimmen Sie  $I_1 \cap \mathbb{N}$  und  $I_2 \cap \mathbb{N}$ .  
(b) Geben Sie die Mengen  $I_1 \cap I_2$  und  $I_2 \setminus I_1$  sowohl beschreibend als auch mit Intervallen an.  
(c) Geben Sie die Produktmenge  $I_1 \times I_2$  beschreibend an und skizzieren Sie sie.

5. Seien  $A, B, C$  Aussagen.

- (a) Geben Sie die Wahrheitstafel der Aussage  $(A \vee B) \wedge (A \vee C)$  an.  
(b) Zeigen oder widerlegen Sie mittels Wahrheitstafeln die Äquivalenz der Aussagen  $(A \Rightarrow B) \Rightarrow C$  und  $A \Rightarrow (B \Rightarrow C)$ .

6. Seien  $A, B, C$  Aussagen. Bestimmen Sie welche der folgenden Aussagen Tautologien und welche Kontradiktionen sind durch Umformen. Geben Sie dabei an, welche Regeln verwendet werden.

- (a)  $(A \vee \neg B) \vee (B \wedge \neg A)$   
(b)  $(A \Rightarrow B) \vee (A \Rightarrow \neg B)$   
(c)  $\neg(A \vee B \vee \neg C) \wedge (C \wedge B \wedge \neg A)$

7. Gegeben sind die beiden Aussagen “Alle Menschen mögen Mathematik.” und “Es gibt einen Franzosen, der nicht englisch spricht.”. Wie lauten die Negationen der beiden Aussagen? Definieren Sie Prädikate und schreiben Sie die Aussagen und ihre Negationen mit Quantoren und Prädikaten an.

8. Negieren Sie die folgenden Aussagen:

- (a)  $\forall x: x \in M \Rightarrow (x \geq 1 \vee x < \frac{1}{2})$
- (b)  $\exists y: y \geq 0 \wedge P(y)$
- (c)  $\forall a: a \in A \Rightarrow (\exists b: b \in A \wedge b \geq a)$

9. Formulieren Sie den folgenden Satz:

“Wenn  $x$  eine gerade natürliche Zahl ist, dann ist  $x^2$  eine gerade natürliche Zahl.”

mit Quantoren und negieren Sie die quantifizierte Aussage.

10. Negieren Sie die folgenden Aussagen:

- (a)  $\forall x \in \mathbb{R}: x > 1 \Rightarrow (\exists y \in \mathbb{R}^+: x - y > 1)$
- (b)  $\exists n \in \mathbb{N} \forall k \in \mathbb{N}: n \leq k$

11. Seien  $A, B, C$  Mengen. In der Vorlesung haben wir Satz 1.8(5), d.h.,

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$

durch logisches Umformen wie folgt gezeigt: Nach Definition gilt

$$x \in A \setminus (B \cap C) \iff x \in A \wedge \neg(x \in B \wedge x \in C) \quad (8.1)$$

und

$$x \in (A \setminus B) \cup (A \setminus C) \iff (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C). \quad (8.2)$$

Zu zeigen ist also durch Umformen, dass die beiden rechten Seiten in (8.1) und (8.2) logisch äquivalent sind. Die einzelnen Schritte dafür sind:

$$\begin{aligned} & x \in A \wedge \neg(x \in B \wedge x \in C) \\ \stackrel{\text{De Morgan}}{\iff} & x \in A \wedge (x \notin B \vee x \notin C) \\ \stackrel{\text{distributiv}}{\iff} & (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \end{aligned}$$

Zeigen Sie auf die gleiche Art durch logisches Umformen, dass für zwei Mengen  $A, B$  gilt:

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

12. Beweisen Sie den folgenden Satz direkt (Modus Ponens): Für alle natürlichen Zahlen  $x, y, z \in \mathbb{N}$  gilt, dass wenn  $z$  sowohl  $x$  als auch  $y$  teilt, dann teilt  $z$  auch  $2xy - x + y$ .

13. Skizzieren Sie die folgende Teilmenge des  $\mathbb{R}^2$ :

$$A = \{(x, y) \in \mathbb{R}^2 \mid |x| \geq |y| \wedge |y| \geq |x - 1| \wedge |x| \leq 5\}.$$

14. Sei  $Q_4 = \{(x, y) \in \mathbb{R}^2 \mid x < 0 \wedge y \geq 0\}$ . Zeigen Sie, dass für alle  $(x, y) \in Q_4$  die Dreiecksungleichung

$$|x + y| \leq |x| + |y|$$

gilt, d.h., beweisen Sie Fall 4 in der Fallunterscheidung von Satz 3.5.

15. Berechnen Sie die folgenden Werte:

$$a = \sum_{k=0}^7 (-1)^k (2k+1), \quad b = \sum_{k=3}^8 [(k+1)^2 - k^2],$$

$$c = \sum_{k=10}^3 \frac{3k-1}{2k+1}, \quad d = \sum_{k=2}^{17} 3.$$

16. Zeigen Sie mittels Induktion, dass für alle  $n \in \mathbb{N}$  gilt

$$\sum_{k=0}^n (2k+1) = (n+1)^2.$$

17. Zeigen Sie mittels Induktion, dass für jedes  $n \in \mathbb{N}^*$  und für jede Menge  $A$  mit  $|A| = n$  gilt:  $|A \times A| = n^2$ .

*Hinweis:* Die Induktion wird an der Anzahl der Elemente  $n$  durchgeführt. Für den Induktionsanfang verwenden Sie  $n_0 = 1$ . Im Induktionsschritt gehen Sie ähnlich zum Beweis von Satz 3.11 vor: schreiben Sie die  $(n+1)$ -elementige Menge

$$A = \{a_1, a_2, \dots, a_n, a_{n+1}\} = \{a_1, \dots, a_n\} \cup \{a_{n+1}\}.$$

Mit der Bezeichnung  $A_1 = \{a_1, \dots, a_n\}$  ist dann zu überlegen, wie  $A \times A$  und  $A_1 \times A_1$  zusammenhängen.

18. Zeigen Sie mit einem Widerspruchsbeweis, dass für alle reellen Zahlen  $x$  mit  $x < 0$  gilt:

$$\frac{x-1}{x-2} < \frac{x-2}{x-3}.$$

19. Werten Sie die folgenden Abbildungen in verschiedenen Punkten des Definitionsbereichs aus, skizzieren sie und stellen Sie fest ob die Abbildung eine Funktion ist.

(a)

$$f_1: [0, 1] \rightarrow [0, 1], \quad x \mapsto x^2$$

(b)

$$f_2: [-5, 5] \rightarrow [-1, 1], \quad x \mapsto \begin{cases} 1, & x \geq 0 \\ -1, & x < 0 \end{cases}$$

20. Skizzieren Sie die beiden Teilmengen von  $[0, 4] \times [-2, 2]$  und stellen Sie jeweils fest, ob es sich um eine Funktion handelt.

(a)  $f_3 = \{(x, x-2) \mid x \in [0, 4]\} \subseteq [0, 4] \times [-2, 2]$

(b)  $f_4 = \{(y^2, y) \mid y \in [-2, 2]\} \subseteq [0, 4] \times [-2, 2]$

21. Gegeben ist die Funktion  $f: [-2, 2] \rightarrow \mathbb{R}, x \mapsto x(3-x^2)$ . Skizzieren Sie den Graphen dieser Funktion. Was ist der Wertebereich  $Y = f([-2, 2])$ ? Ist  $f$  als Funktion von  $[-2, 2]$  auf  $Y$  injektiv, surjektiv oder bijektiv?



22. Gegeben ist die Funktion  $g: \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+, x \mapsto \frac{2x+1}{x+2}$ . Skizzieren Sie den Graphen dieser Funktion. Ist  $g$  injektiv, surjektiv oder bijektiv? Bestimmen Sie den Urbildbereich  $g^{-1}([1, \frac{3}{2}])$ .
23. Gegeben ist die Funktion  $h: [-3, 3] \rightarrow \mathbb{R}, x \mapsto 4 - x^2$ . Skizzieren Sie den Graphen dieser Funktion. Bestimmen Sie den Wertebereich  $h([-3, 3])$  sowie den Urbildbereich  $h^{-1}([0, 1])$ .
24. Sei  $S$  die Menge aller aktiven Studierenden an der JKU,

$$M = \{m \in \mathbb{N} \mid 0 \leq m \leq 9999999\},$$

und  $SKZ$  die Menge aller Studienkennzahlen von Studien, die aktuell an der JKU angeboten werden.

- (a) Sei  $f_1: S \rightarrow M$  die Funktion, die jeder Person ihre Matrikelnummer zuordnet (dabei entspricht z.B. die Matrikelnummer 0455801 der Zahl 455801). Ist  $f_1$  injektiv, surjektiv oder bijektiv?
- (b) Sei  $f_2: S \rightarrow SKZ$  die Funktion, die jeder Person die Studienkennzahl ihrer ersten Studienrichtung zuordnet. Ist  $f_2$  injektiv, surjektiv oder bijektiv?
25. Zeigen Sie, dass  $|\mathbb{N}| = |\mathbb{Z}|$  indem Sie eine bijektive Funktion zwischen den beiden Mengen  $\mathbb{N}$  und  $\mathbb{Z}$  angeben. Skizzieren Sie diese Abbildung auf einer nichttrivialen Definitionsmenge.
26. Gegeben sind die Funktionen

$$f: [-1, 1] \rightarrow [0, 1], \quad x \mapsto 1 - x^2 \quad \text{und} \quad g: [0, 1] \rightarrow [-2, 0], \quad x \mapsto 2x - 2.$$

Skizzieren Sie die Graphen der beiden Funktionen und stellen Sie fest, ob sie injektiv, surjektiv oder bijektiv sind. Bestimmen Sie die Hintereinanderausführung  $h = g \circ f: [-1, 1] \rightarrow [-2, 0]$ , skizzieren Sie den Graphen von  $h$  und stellen Sie fest, ob  $h$  injektiv, surjektiv oder bijektiv ist.

27. Gegeben ist die Funktion

$$f: [-1, 1] \rightarrow [-\frac{2}{3}, 2], \quad x \mapsto \frac{2x}{2-x}.$$

Bestimmen Sie die Umkehrfunktion  $f^{-1}: [-\frac{2}{3}, 2] \rightarrow [-1, 1]$ . Kontrollieren Sie Ihr Ergebnis indem Sie  $f \circ f^{-1}(x)$  und  $f^{-1} \circ f(x)$  bestimmen.

28. Gegeben ist die Funktion

$$f: [-4, 4] \rightarrow \mathbb{R}, \quad x \mapsto |1 - x| + |x + 2|.$$

Skizzieren Sie den Graphen der Funktion. Geben Sie die maximalen Intervalle an, in denen die Funktion (a) streng monoton wachsend (b) monoton wachsend (c) streng monoton fallend (d) monoton fallend ist.

29. Sei  $f: X \rightarrow Y$  monoton wachsend und  $g: f(X) \rightarrow Z$  monoton fallend. Zeigen Sie, dass die Hintereinanderausführung  $g \circ f: X \rightarrow Z$  monoton fallend ist.

30. Seien  $a \in \mathbb{R}^+ \setminus \{1\}$ ,  $x \in \mathbb{R}^+$  und  $y \in \mathbb{R}$ . Zeigen Sie unter Benutzung der Rechenregeln für Logarithmen im Skriptum daß die Gleichheit

$$\ln(x^2 \cdot a^y) = (2 \cdot \log_a(x) + y) \cdot \ln(a)$$

gilt.

31. Sei  $X = \{1, 2, 3, \star\}$  und  $Y = \{u, v, w\}$ . Überprüfen Sie ob es sich bei den Mengen  $R_1$ ,  $R_2$  und  $R_3$  um Relationen auf  $X, Y$  handelt.

Geben Sie für jede der Mengen  $R_1$ ,  $R_2$ ,  $R_3$  den Vorbereich und den Nachbereich an, sofern es sich bei der vorliegenden Menge um eine Relation auf  $X, Y$  handelt.

- (a)  $R_1 = \{(1, v), (2, w), (\star, u), (\star, w)\}$
- (b)  $R_2 = \{(1, v), (2, \star), (3, u), (\star, w)\}$
- (c)  $R_3 = \{(1, u), (1, v), (2, v), (3, u), (\star, v)\}$

32. Seien  $A = \{a, b, c, d\}$ ,  $B = \{1, 2, 3, 4, 5\}$  und  $R_4 \subset A \times B$  gegeben durch  $R_4 = \{(a, 1), (b, 3), (c, 5), (d, 2)\}$ .

- (a) Bestimmen Sie die Inverse  $R_4^{-1}$  von  $R_4$ .
- (b) Überprüfen Sie ob  $R_4$  rechtseindeutig/linkseindeutig ist.
- (c) Überprüfen Sie ob  $R_4$  rechtstotal/linkstotal ist.
- (d) Handelt es sich bei  $R_4$  um eine Funktion? Wenn ja, ist sie injektiv/surjektiv?

33. Sei  $X = \{a, b, c, d\}$ , und

$$R_5 = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c), (c, b), (d, d), (d, b), (d, c)\}$$

eine Relation auf  $X$ . Überprüfen Sie ob die Relation  $R_5$  reflexiv, symmetrisch, antisymmetrisch oder transitiv ist.

34. Gegeben ist die Menge  $X = \{0, 1, 2, 3, 4\}$  und die Relation  $R \subseteq X \times X$  durch

$$R = \{(0, 4), (1, 2), (2, 3), (3, 0), (4, 1)\}.$$

Bestimmen Sie die transitive Hülle  $R^+$  und die reflexiv transitive Hülle  $R^*$ .

35. Gegeben sind die Mengen  $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  und  $B = \{1, 3, 5, 7\}$ . Ausserdem definieren wir eine Relation  $R$  durch

$$xRy \iff 2x + 1 \equiv y \pmod{2}.$$

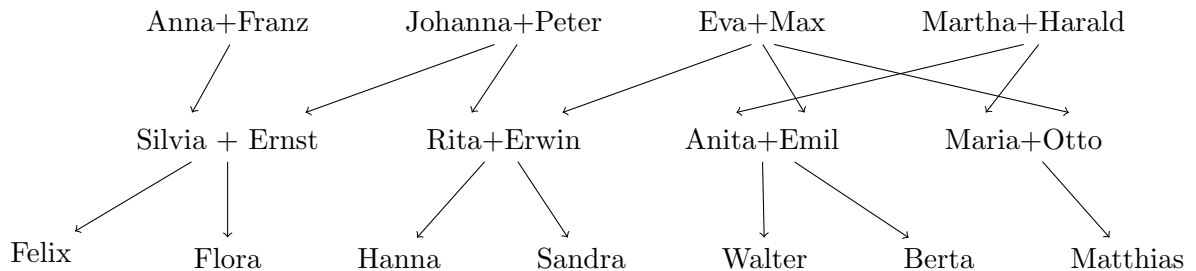
Stellen Sie fest, ob  $R$  eine Äquivalenzrelation (a) auf  $A \times A$  (b) auf  $B \times B$  definiert.

36. Gegeben ist die Relation  $R \subseteq \mathbb{Z} \times \mathbb{Z}$  durch

$$xRy \iff |x| \leq |y|.$$

Überprüfen Sie diese Relation auf Reflexivität, Symmetrie, Antisymmetrie und Transitivität.

37. Gegeben sind der folgende Auszug eines Stammbaums, wobei ein Pfeil  $x + y \rightarrow z$  bedeutet "x und y sind die Eltern von z".



Sei  $E = \{Berta, Felix, Flora, Hanna, Matthias, Sandra, Walter\}$ , dann definieren wir zwei Relationen auf der Menge  $E$ :

- $R \subseteq E \times E$  mit  $xRy$  genau dann wenn,  $x$  und  $y$  eine gemeinsame Großmutter haben.
- $S \subseteq E \times E$  mit  $xSy$  genau dann, wenn  $x$  und  $y$  den gleichen Großvater mütterlicherseits haben.

Geben Sie die beiden Relationen als Teilmengen von  $E \times E$  explizit an. Überprüfen Sie, welche der beiden Relationen eine Äquivalenzrelation ist. Geben Sie für die Äquivalenzrelation alle Äquivalenzklassen an (und die dadurch induzierte Partition der Menge  $E$ ).

38. Die Relation  $\trianglelefteq \subseteq \mathbb{N}^2 \times \mathbb{N}^2$  sei definiert durch

$$(a, b) \trianglelefteq (c, d) \iff (a + b < c + d) \vee (a + b = c + d \wedge a \leq c).$$

Zeigen Sie, dass diese Relation eine Ordnungsrelation ist. Sortieren Sie die Elemente Menge  $X = \{0, 1, 2\} \times \{0, 1, 2\}$  aufsteigend bezüglich dieser Ordnungsrelation.

39. Gegeben ist die Menge

$$X = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 3, 4\}, \{1, 2, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$$

und die Ordnungsrelation  $R \subseteq X \times X$  definiert durch  $aRb \Leftrightarrow a \subseteq b$ . Skizzieren Sie das dazugehörige Hasse-Diagramm. Ist  $R$  eine Totalordnung für die Menge  $X$ ? Bestimmen Sie alle minimalen und maximalen Elemente von  $X$  und (falls existent) das kleinste und das grösste Element.

40. Geben Sie die Additions- und die Multiplikationstabelle von  $\mathbb{Z}_7$  an. Bestimmen Sie die additive und die multiplikative Inverse in  $\mathbb{Z}_7$  von  $a = 4$ .

41. Gegeben sind zwei Abbildungen von  $\mathbb{Z}_n$  nach  $\mathbb{Z}_n$ . Stellen Sie fest, ob es sich jeweils um Funktionen handelt, bestimmen Sie den Bildbereich und überprüfen Sie die Abbildungen auf Injektivität und Surjektivität.

(a)  $f: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7, \quad x \mapsto (x^2 - 2x + 1) \pmod{7}$

(b)  $g: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}, \quad x \mapsto x^3 \pmod{11}$

42. Bestimmen Sie (a)  $\text{ggT}(1024, 484)$  (b)  $\text{ggT}(784, 692)$  und die dazugehörigen Bézout-Koeffizienten und Syzygien mit der im Skript vorgestellten Methode.

43. Bestimmen Sie alle Lösungen in  $\mathbb{Z}_n$  der folgenden Gleichungen

(a) Gesucht sind alle  $x \in \mathbb{Z}_{27}$  für die gilt

$$24x + 3 = 12 \pmod{27}.$$

(b) Gesucht sind alle  $x \in \mathbb{Z}_{127}$  für die gilt

$$123x + 57 = 12 \pmod{127}.$$

Zeigen Sie auch alle Zwischenschritte (zum Beispiel wie die multiplikative Inverse bestimmt wurde, ...).

44. Ein Kind hat zwei Arten von Bausteinen: 30 würfelförmige mit der Seitenlänge  $7\text{cm}$  und 30 quaderförmige mit der Dimension  $7\text{cm} \times 7\text{cm} \times 19\text{cm}$ . Kann mit diesen Bausteinen ein quaderförmiger Turm mit Grundfläche  $7\text{cm} \times 7\text{cm}$  und  $2.2\text{m}$  Höhe gebaut werden? Was ist die Mindestanzahl von Bausteinen, die dafür gebraucht wird?

45. Berechnen Sie alle ganzzahligen Lösungen  $(x, y) \in \mathbb{Z}^2$  der diophantischen Gleichung  $175x + 245y = 105$ . Geben Sie die einzelnen Berechnungsschritte des erweiterten Euklidischen Algorithmus sowie die Lösungsmenge  $L = \{(x, y) \in \mathbb{Z}^2 : 175x + 245y = 105\}$  explizit an.

46. Alice will ein RSA Schlüsselpaar bestehend aus private key und public key erstellen, damit Bob ihr eine verschlüsselte Nachricht schicken kann. Dazu wählt Alice die beiden Primzahlen  $p = 11$  und  $q = 13$ . Berechnen Sie die Schlüsselpaare  $(n, e)$  (public key) und  $(n, d)$  (private key) für die angegebenen Primzahlen  $p = 11$  und  $q = 13$ , laut Skriptum, und wählen Sie  $e = 7$ . Überprüfen Sie ob  $\text{ggT}(m, e) = 1$ . Verschlüsseln Sie die Nachricht  $(3, 2)$  von Bob an Alice mit dem public key  $(n, e)$  von Alice, analog zu Beispiel 6.26 und führen Sie zur Probe die Decodierung durch.

47. Sei  $\preceq \subset \mathbb{N}^2$  die laut Beispiel 5.27 im Skriptum definierte Relation. Zeigen Sie mit Hilfe von Äquivalenzumformungen dass

$$\forall (a, b), (c, d) \in \mathbb{N}^2 : \left( (a, b) \preceq (c, d) \wedge (c, d) \preceq (a, b) \right) \Leftrightarrow (a, b) = (c, d).$$

Geben Sie bei jedem Umformungsschritt das verwendete Gesetz oder die verwendete Rechenregel an.

48. Zeigen Sie mittels vollständiger Induktion daß für alle  $n \in \mathbb{N}$  und für alle  $a_0, a_1, \dots, a_n \in \mathbb{R}$  gilt

$$\sum_{k=1}^n (a_k - a_{k-1}) = a_n - a_0.$$