Mathematik und Logik für Wirtschaftsinformatik
2013W

V. Pillwein

24. Januar 2014

Inhaltsverzeichnis

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

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

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!), einmal aufzählend

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

und einmal beschreibend

$$G = \{m \in \mathbb{N} \mid m \text{ ist gerade}\}.$$

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

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

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.,

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

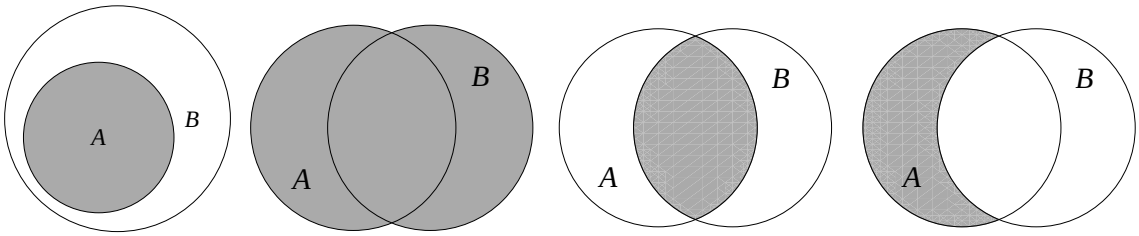


Abbildung 1.1: von links nach rechts: $A \subseteq B$, $A \cup B$, $A \cap B$ und $A \backslash B$

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:

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

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

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

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. *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)*

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 enth'alt, 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 $A\backslash B$ ("A ohne B"); d.h.:*

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

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:*

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 6, 7, 8\}, \\ A \cap B &= \{4, 5, 6\}, \\ A\backslash B = \{1, 2, 3\}, &\quad \text{und} \quad B\backslash A = \{7, 8\}. \end{aligned}$$

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

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

Beispiel 1.6. *Seien $I_1 = [0, 5]$, $I_2 = [2.4, 4]$, $I_3 = [3, 7]$. Bestimme (a) $I_2 \cap \mathbb{N}$ (b) $I_1 \cup I_3$ (c) $I_2 \cap I_3$ (d) $I_1\backslash I_2$.*

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

Einige Rechenregeln für die Mengenoperationen aus Defintion 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)*

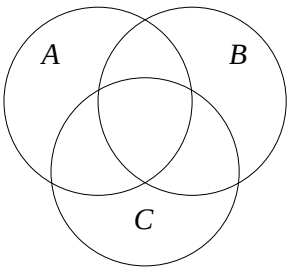
(4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(Distributivgesetz)*

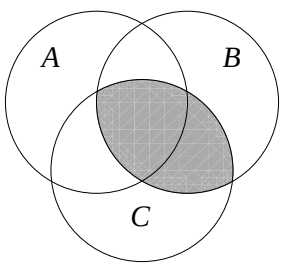
(5) $A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$

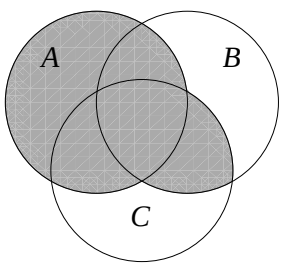
(6) $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$

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):

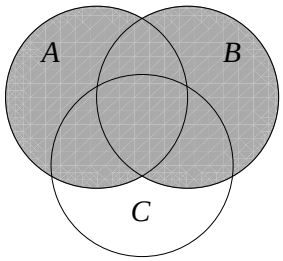
Für die linke Seite beginnen wir mit drei Mengen und zeichnen zunächst $B \cap C$ ein und im zweiten Schritt bilden wir die Vereinigung davon mit A:

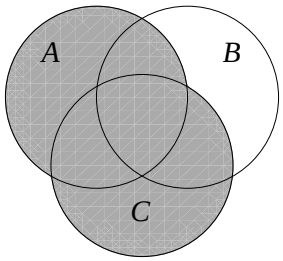


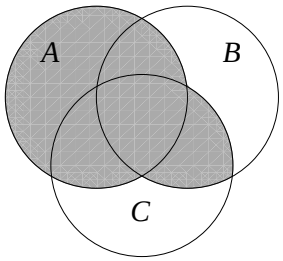




Für die rechte Seite bilden wir zunächst die beiden geklammerten Ausdrücke $A \cup B$ und $A \cup C$ und bilden dann den Durchschnitt:







□

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

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

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

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

Oft kann man von einem "Universum" ausgehen in dem gerechnet wird, d.h., es wird zum Beispiel angenommen, dass wir über den natürlichen Zahlen operieren. Wenn klar ist über welcher fixen *Grundmenge* Ω (Universum) gerechnet wird, dann schreibt man einfach A^c für $\Omega \backslash A$. In dem Sinn, mit $A = \Omega$, können die Identitäten (5) und (6) aus Satz 1.8 auch so geschrieben werden:

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

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

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.

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

Die Kardinalität gibt die Anzahl der Elemente und nicht die Länge an, d.h., (siehe oben), die Kardinalität des reellen Intervalls $[0, 1]$ ist unendlich (die Länge ist 1). Die Kardinalität der reellen Zahlen ist gleich der Kardinalität jedes (endlichen oder unendlichen) reellen Intervalls und *echt größer* als die Kardinalität der natürlichen Zahlen.

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

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

Beweis. Sei $A = \{x_1, x_2, \ldots, x_m\}$ und $B = \{y_1, y_2, \ldots, y_n\}$ für beliebige aber fixe natürliche Zahlen m, n. Dann gilt $|A| = m$ und $|B| = n$.

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

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

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. $A \cap B = \{x_1, x_2, \ldots, x_k\} = \{y_1, y_2, \ldots, y_k\}$ (beachte: bei Mengen spielt die Reihenfolge keine Rolle). Dann gilt für die Vereinigung

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

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 $|A| + |B| - |A \cap B| = m + n - k$. □

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*

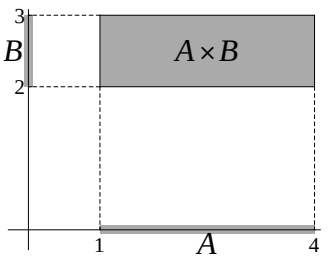
$$A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\}.$$

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*

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

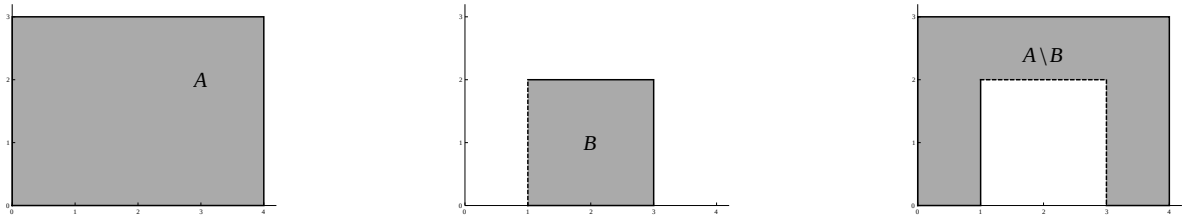


Beispiel 1.18. *Sei $A = [1, 4]$ und $B = [2, 3]$. Dann ist*

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

Beispiel 1.19. *Seien* $A = [0,4] \times [0,3]$, $B = (1,3] \times [0,2]$, *und* $C = [-1,2] \times [0,3]$. *Bestimmen Sie die Mengen* $A \cap B$, $A \cap C$, $A \cup C$, *und* $A \setminus B$. *Für die Differenzmenge gilt*

$$A \setminus B = [0,1] \times [0,3] \cup (3,4] \times [0,3] \cup (1,3] \times (2,3].$$



Definition 1.20. *Produktmengen können auch aus mehr als zwei Mengen gebildet werden und analog gilt*

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

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

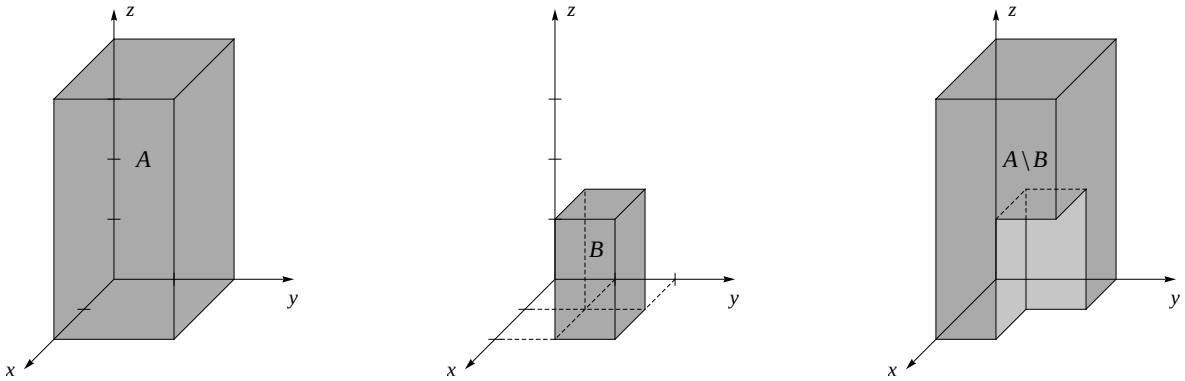
Wenn $A_1 = A_2 = \cdots = A_n = A$ *gilt, dann wird die Produktmenge wieder kurz mit* A^n *bezeichnet.*

Im dredimensionalen lassen sich die Produktmengen auch noch graphisch veranschaulichen:

Beispiel 1.21. *Gegeben sind die Mengen* $A = [0,2] \times [0,2] \times [0,4]$ *und* $B = [1,2] \times [1,2] \times [0,2]$ *wie im Bild unten links skizziert. Die Menge* $A \setminus B$ *ist zum Beispiel gegeben durch*

$$A \setminus B = [0,2] \times [0,1) \times [0,4] \cup [0,1) \times [1,2] \times [0,4] \cup [1,2] \times [1,2] \times (2,4],$$

siehe die Skizze ganz rechts. Die Flächen $[1,2] \times \{1\} \times [0,2]$, $\{1\} \times [1,2] \times [0,2]$ *und* $[1,2] \times [1,2] \times \{2\}$ *sind* nicht *in der Menge* $A \setminus B$ *enthalten.*



Die Anzahl der Elemente in einer Produktmenge ist gleich dem Produkt der Kardinalitäten der jeweiligen (endlichen) Mengen:

Bemerkung 1.22. *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 π 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	$A \wedge B$	$(A \wedge B) \wedge C$
W	W	W	W	W
W	W	F	W	F
W	F	W	F	F
W	F	F	F	F
F	W	W	F	F
F	W	F	F	F
F	F	W	F	F
F	F	F	F	F

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

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

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

A	B	C	$A \vee B$	$A \vee C$	$(A \vee B) \wedge (A \vee C)$
W	W	W	W	W	W
W	W	F	W	W	W
W	F	W	W	W	W
W	F	F	W	W	W
F	W	W	W	W	W
F	W	F	W	F	F
F	F	W	F	W	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) $(B \cap C)^c = B^c \cup C^c$

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

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.,

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

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 mittles $\neg, \vee, \wedge$ ausgedrückt wird:*

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

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 $A \wedge (\neg A)$. Wir fassen diese Aussagen und noch ein paar weitere einfache Beispiele in folgendem Lemma zusammen.

Lemma 2.9. *Sei A eine Aussage. Dann gilt:*

$$\begin{array}{llll} A \wedge A \equiv A & A \wedge \neg A \equiv F & A \wedge W \equiv A & A \vee W \equiv W \\ A \vee A \equiv A & A \vee \neg A \equiv W & A \wedge F \equiv F & A \vee F \equiv A \end{array}$$

Die Eigenschaft aus der ersten Spalte nennt man auch Idempotenz.

Beispiel 2.10. *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 2.11.

- *$G(x) \equiv x$ ist gerade. Dann ist $G(2) \equiv W$ und $G(27) \equiv F$.*
- *Die Eigenschaft "ist rot", also $ist\_rot(x)$. Zum Beispiel*

$$ist\_rot(Blut) \equiv W \qquad und \qquad ist\_rot(Banane) \equiv F$$

- *$A(x, M) \equiv x \in M$ 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

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

Die Negation von $A(x)$ ist

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

Beispiel 2.12. *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)?*

Beispiel 2.13. *Wir betrachten noch einmal die Mengen $A = [0, 4] \times [0, 3]$ und $B = (1, 3] \times [0, 2]$ aus Beispiel 1.19 und die Differenzmenge $A \setminus B$. Die Mengen A und B können geschrieben werden als*

$$A = \{(x, y) \mid A_1(x) \wedge A_2(y)\}, \quad und \quad B = \{(x, y) \mid B_1(x) \wedge B_2(y)\}$$

mit Hilfe der parametrisierten Aussagen

$$\begin{aligned} A_1(x) &= 0 \leq x \leq 4 = 0 \leq x \wedge x \leq 4, & A_2(y) &= 0 \leq y \leq 3 = 0 \leq y \wedge y \leq 3, \\ B_1(x) &= 1 < x \leq 3 = 1 < x \wedge x \leq 3, & B_2(y) &= 0 \leq y \leq 2 = 0 \leq y \wedge y \leq 2. \end{aligned}$$

Für die Differenzmenge gilt $A \setminus B = \{(x, y) \mid (x, y) \in A \wedge \neg\big((x, y) \in B\big)\}$. Die Bedingung für $(x, y) \in A \setminus B$ kann wie folgt äquivalent umgeschrieben werden:

$$\begin{aligned} &(A_1(x) \wedge A_2(y)) \wedge \neg(B_1(x) \wedge B_2(y)) \\ \Leftrightarrow &(A_1(x) \wedge A_2(y)) \wedge (\neg B_1(x) \vee \neg B_2(y)) \\ \Leftrightarrow &(A_1(x) \wedge \neg B_1(x) \wedge A_2(y)) \vee (A_1(x) \wedge A_2(y) \wedge \neg B_2(y)). \end{aligned}$$

Für die Bedingung an x in der ersten Klammer gilt weiter

$$\begin{aligned} (A_1(x) \wedge \neg B_1(x) &\Leftrightarrow (0 \leq x \wedge x \leq 4) \wedge (x \leq 1 \vee x > 3) \\ &\Leftrightarrow (0 \leq x \wedge x \leq 4 \wedge x \leq 1) \vee (0 \leq x \wedge x \leq 4 \wedge x > 3) \\ &\Leftrightarrow 0 \leq x \leq 1 \vee 3 < x \leq 4. \end{aligned}$$

Damit gilt (wieder unter Verwendung des Distributivgesetzes), dass

$$A_1(x) \wedge \neg B_1(x) \wedge A_2(y) \Leftrightarrow (0 \leq x \leq 1 \wedge 0 \leq y \leq 3) \vee (3 < x \leq 4 \wedge 0 \leq y \leq 3).$$

Analog kann man zeigen, dass

$$\begin{aligned} A_2(y) \wedge \neg B_2(y) &\Leftrightarrow (0 \leq y \wedge y \leq 3) \wedge (y < 0 \vee y > 2) \\ &\Leftrightarrow (\underbrace{0 \leq y \wedge y < 0}_{=F}) \vee (y \leq 3 \wedge y > 2) \Leftrightarrow 2 < y \leq 3, \end{aligned}$$

also insgesamt

$$A_1(x) \wedge A_2(y) \wedge \neg B_2(y) \Leftrightarrow 0 \leq x \leq 4 \wedge 2 < y \leq 3.$$

Damit erhalten wir die Beschreibung

$$\begin{aligned} A \setminus B &= \{(x,y) \mid 0 \leq x \leq 1 \wedge 0 \leq y \leq 3\} \cup \{(x,y) \mid 3 < x \leq 4 \wedge 0 \leq y \leq 3\} \\ &\quad \cup \{(x,y) \mid 1 < x \leq 3 \wedge 2 < y \leq 3\} \\ &= [0,1] \times [0,3] \cup (3,4] \times [0,3] \cup (1,3] \times (2,3]. \end{aligned}$$

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

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

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:

$$B \equiv \forall\, x \colon x \in \mathbb{N} \Longrightarrow x > -1 \tag{2.4}$$

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 $\forall\, x \colon A(x)$. Die Aussage B enthält keine freien Variablen. Die Variable x ist durch den Allquantor *gebunden*.

Beispiel 2.14. *Was sind die gebundenen bzw. die freien Variablen der folgenden Aussagen:*

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

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 2.15. *(a) "Jede natürliche Zahl ausser* 0 *ist kleiner als ihr Dreifaches." Diese Aussage mit Quantoren formuliert:*

$$B \equiv \forall\, x \colon x \in \mathbb{N} \wedge x \neq 0 \quad \Rightarrow \quad x < 3x.$$

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:

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

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:

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

Der quantorfreie Teil dieser Aussage ist das Prädikat

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

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 2.15(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*:

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

Die Variable x ist hier durch den Existenzquantor *gebunden*. Die Negation der Aussage in Beispiel 2.15(c) ist "Es gibt eine reelle Zahl, die kleiner oder gleich ist als ihr Quadrat" oder in Quantorenschreibweise

$$\exists\, x\colon x \in \mathbb{R} \wedge \neg(x^2 > x) \qquad \Leftrightarrow \qquad \exists\, x\colon x \in \mathbb{R} \wedge x^2 \leq x.$$

Wir fassen die beiden Quantoren noch einmal zusammen.

Definition 2.16. *(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: $\forall\, x\colon P(x)$. Das Symbol $\forall$ heisst* Allquantor*. Wenn $P(x)$ von der Form $A(x) \Rightarrow B(x)$ ist, dann schreibt man auch kurz*

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

- *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: $\exists\, x\colon P(x)$. Das Symbol $\exists$ heisst* Existenzquantor*. Wenn $P(x)$ von der Form $A(x) \wedge B(x)$ ist, dann schreibt man auch kurz*

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

- *All- und Existenzaussagen werden wie folgt negiert:*

$$\neg(\forall\, x\colon P(x)) \quad \Leftrightarrow \quad \exists\, x\colon \neg P(x) \quad \textit{und} \quad \neg(\exists\, x\colon P(x)) \quad \Leftrightarrow \quad \forall\, x\colon \neg P(x).$$

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

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

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

$$\forall\, x, A(x)\colon B(x) \qquad \text{und} \qquad \exists\, x, A(x)\colon B(x)$$

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

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

Beispiel 2.17. *Sei $A \equiv \forall\, x, x \in \mathbb{R}\colon x^2 < 0$. Wir bestimmen die Negation dieser Aussage:*

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

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.,

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

Beispiel 2.18. *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

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

Damit erhalten wir als Lösung

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

bzw., in Kurzschreibweise,

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

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:

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

oder kürzer

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

oder noch kürzer

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

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

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

und daher werden die Inhalte von Existenzquantoren häufig zusammengezogen:

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

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

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

Wir kürzen ab:

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

und kürzen weiter:

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

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

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

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

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

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:

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

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:

$$\widetilde{A} \equiv \exists\, y \in \mathbb{R}\ \forall\, x \in \mathbb{R} \colon x < y.$$

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 $\widetilde{A}$ tatsächlich falsch ist gehen wir wie oben vor und beweisen, dass die Negation wahr ist. Wir negieren die Aussage schrittweise:

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

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

Beispiel 2.19. *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:

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

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

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

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

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:

$$\forall\, x, y, z \in \mathbb{N}\colon z \mid x \ \wedge z \mid y \quad \Longrightarrow \quad z \mid x + y \ \wedge \ z \mid xy$$

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. □

Wir betrachten ein weiteres einfaches Beispiel und führen dazu zwei einfache Definitionen ein.

Definition 3.3. *Eine ganze Zahl a ist* gerade*, genau dann, wenn es eine ganze Zahl b gibt, sodass $a = 2b$.*

Definition 3.4. *Eine ganze Zahl a ist* ungerade*, genau dann, wenn es eine ganze Zahl b gibt, sodass $a = 2b + 1$.*

Und hier der Satz, den wir beweisen wollen:

Satz 3.5. *Das Quadrat einer ungeraden natürlichen Zahl ist ungerade.*

Beweis. Sei $n \in \mathbb{N}$ eine beliebige ungerade natürliche Zahl. Nach Definition existiert dann ein $k \in \mathbb{N}$ mit der Eigenschaft, dass $n = 2k + 1$.

Zu zeigen ist, dass n^2 ungerade ist, d.h., nach Definition ist zu zeigen, dass eine natürliche Zahl m existiert mit der Eigenschaft, dass $n^2 = 2m + 1$. Basierend auf den Voraussetzungen konstruieren wir jetzt so eine Zahl m.

Wenn $n = 2k + 1$, dann gilt

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Wenn $k \in \mathbb{N}$, dann gilt auch $2k^2 + 2k \in \mathbb{N}$, d.h., mit $m = 2k^2 + 2k \in \mathbb{N}$ gilt $n^2 = 2m + 1$. □

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. Ein Beispiel, bei dem wir bereits (informal) eine Fallunterscheidung durchgeführt haben war im Beweis von Satz 1.12, hier noch einmal zur Erinnerung:

Satz 3.6. *Für endliche Mengen A, B gilt:*

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

Oder mit Quantoren ausgedrückt:

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

In dem Beweis hatten wir zwischen $A \cap B = \emptyset$ und $A \cap B \neq \emptyset$ unterschieden, es können auch mehr als zwei Fälle unterschieden werden. Wir betrachten ein Beispiel und führen dazu zuerst den Absolutbetrag ein.

Definition 3.7. *Sei x eine reelle Zahl. Dann definieren wir den Absolutbetrag $|x|$ als*

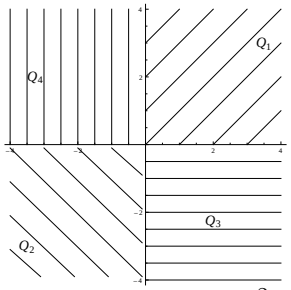
$$|x| = \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases}$$

Satz 3.8. *(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:

$$\begin{aligned} Q_1 &= \{(x, y) \in \mathbb{R}^2 \mid x \geq 0 \wedge y \geq 0\}, \\ Q_2 &= \{(x, y) \in \mathbb{R}^2 \mid x < 0 \wedge y < 0\}, \\ Q_3 &= \{(x, y) \in \mathbb{R}^2 \mid x \geq 0 \wedge y < 0\}, \\ Q_4 &= \{(x, y) \in \mathbb{R}^2 \mid x < 0 \wedge y \geq 0\}. \end{aligned}$$



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:

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

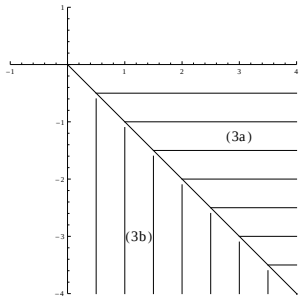
   Damit ist die Dreiecksungleichung in Q_1 erfüllt. In diesem Quadranten gilt sogar Gleichheit.

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

$$y < 0 \quad \Longrightarrow \quad 0 < -y \quad \Longrightarrow \quad y < -y.$$

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

$$x \geq 0 \quad \Longrightarrow \quad 0 \geq -x \quad \Longrightarrow \quad x \geq -x.$$

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. □

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 3.9. *Einfache Beispiele sind:*

$$\sum_{k=0}^{5} k = 0 + 1 + 2 + 3 + 4 + 5$$

$$\sum_{k=1}^{7} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2$$

$$\sum_{k=0}^{n} (2k+1) = 1 + 3 + 5 + 7 + \cdots + (2n+1)$$

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 3.10. *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: ($n \to n+1$) 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 letzt 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 3.11. *Zeigen Sie mittels vollständiger Induktion, dass für alle $n \in \mathbb{N}$ gilt: $\sum_{k=0}^{n}(2k+1) = (n+1)^2$.*

Induktionsanfang: wir überprüfen die Identität für $n = 0$:

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

Induktionsannahme: Wir nehmen an, dass die Formel für eine beliebige natürliche Zahl n gilt, d.h., wir nehmen an, dass $\sum_{k=0}^{n}(2k+1) = (n+1)^2$.

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

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

Wir beginnen mit der linken Seite, ziehen den letzten Summanden heraus und verwenden die Induktionshypothese und erhalten durch Umformen:

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

Bemerkung 3.12. *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 3.13. *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 3.14. *(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:

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

Sei $A_1 = \{a_1, a_2, \ldots, a_{n-1}, a_n\}$ (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., $|P(A)| = 2|P(A_1)| = 2 \cdot 2^n = 2^{n+1}$. □

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 3.15. *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. □

Satz 3.16. *Für jede positive reelle Zahl x gilt $\frac{x+1}{x+2} < \frac{x+3}{x+4}$.*

Beweis. Angenommen es existiert ein $x > 0$ für das das Gegenteil der zu zeigenden Aussage gilt, d.h., angenommen es gilt

$$\frac{x+1}{x+2} \geq \frac{x+3}{x+4}. \tag{3.2}$$

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

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

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) und so ein x kann nicht existieren. Damit muss die ursprüngliche Aussage richtig sein. □

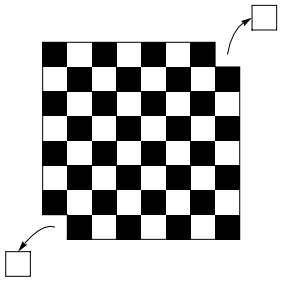
Bemerkung 3.17. *Wenn eine Ungleichung mit einer positiven Zahl $a > 0$ multipliziert wird, ändert sich das Ungleichheitszeichen nicht, also gilt zum Beispiel für $a > 0$*

$$x < y \quad \Longleftrightarrow \quad ax < ay.$$

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

$$x < y \quad \Longleftrightarrow \quad bx > by.$$

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 2×1-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 $f\colon X \to Y$ *(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. Die Menge X heisst der* Definitionsbereich *(engl.:* domain*) von f und die Menge Y der* Zielbereich *von f.*

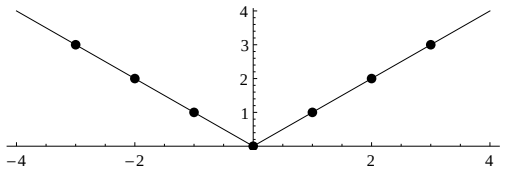
Beispiel 4.2. *Absolutbetrag wie in Definition 3.7 eingeführt ist eine Funktion, zum Beispiel, von $\mathbb{R}$ nach $\mathbb{R}$:*

$$f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x|$$

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



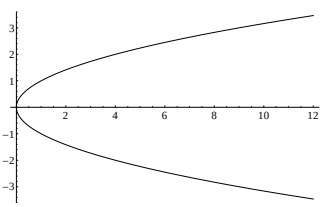
Beispiel 4.3. *Die "Wurzelfunktion", also die Abbildung, die einem $x > 0$ ein $y \in \mathbb{R}$ zuordnet für das gilt $x = y^2$ ist* keine *Funktion von R_0^+ nach $\mathbb{R}$, d.h., die Abbildung*

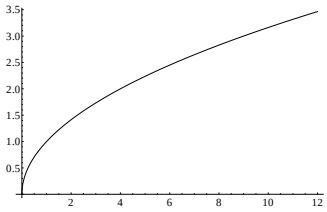
$$f\colon \mathbb{R}_0^+ \to \mathbb{R}, \quad x \mapsto \sqrt{x},$$

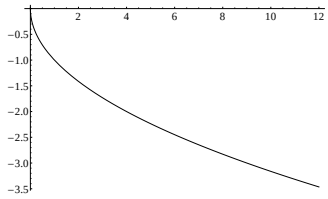
weil der Funktionswert nicht *eindeutig definiert ist. Zum Beispiel gilt $f(4) = 2$ und $f(4) = -2$. Wenn der Zielbereich (sinnvoll) eingeschränkt wird, dann kann man tatsächlich von einer Funktion sprechen, d.h., die Abbildungen*

$$f_+\colon \mathbb{R}_0^+ \to \mathbb{R}_0^+, \quad x \mapsto \sqrt{x}, \quad und f_-\colon \mathbb{R}_0^+ \to \mathbb{R}_0^-, \quad x \mapsto \sqrt{x}$$

sind jeweils Funktionen. Unten abgebildet sind die Graphen der Abbildung f, und der Funktionen f_+ und f_-:





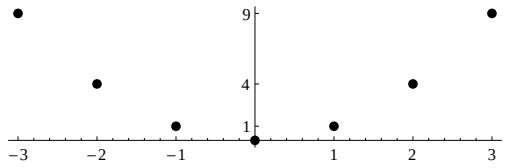


Beispiel 4.4. *Eine Funktion kann auch nur auf diskreten Werten definiert sein, zum Beispiel*

$$f\colon \underbrace{\{-3,-2,-1,0,1,2,3\}}_{=X} \to \underbrace{\{0,1,4,9\}}_{=Y}, \quad x \mapsto x^2$$

Wertetabelle:

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



Eine Funktion $f\colon X \to Y$ 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 4.5. *Seien X, Y Mengen. Eine* Funktion *von X nach Y ist eine Teilmenge $f \subseteq X \times Y$ für die gilt*

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

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

Beispiel 4.6. *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 4.7. *Welche der folgenden Teilmengen von $X \times Y$ definiert eine Funktion von X nach Y? Skizzieren Sie die angegebenen Punktmengen.*

(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 4.8. *Sei $f\colon X \to Y$ eine Funktion. Die Menge*

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

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*

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

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

Beispiel 4.9. *Wir betrachten wieder die Funktion aus Beispiel 4.4. Was ist $f(X)$? Was ist $f^{-1}(\{4,9\})$? Was ist $f^{-1}(\{1\})$? Was ist $f^{-1}(\{5\})$?*

Beispiel 4.10. *Sei $X = [-5,5]$ und $Y = \mathbb{R}$ und $f\colon X \to Y$ die Abbildung $x \mapsto |x|$.*

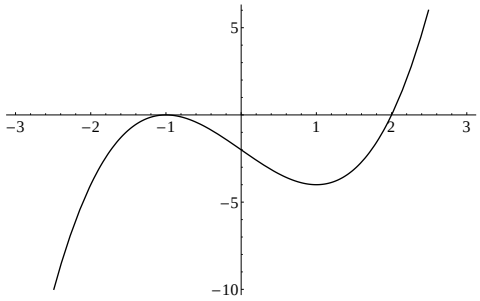
(a) Was ist $f(X)$?

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

Beispiel 4.11. *Gegeben sind die Mengen $X_1 = [-3,3]$, $X_2 = \mathbb{R}_0^+$ $X_3 = [-1,1]$ und $Y_1 = [-20,16]$, $Y_2 = \mathbb{R}$, $Y_3 = [-4,0]$. Wir betrachten die Abbildung $f\colon X_k \to Y_k, x \mapsto (x+1)^2(x-2)$ für $k = 1,2,3$. (a) Wie sieht der Funktionsgraph aus? (b) Was ist jeweils der Bildbereich von f unter X_k ($k = 1,2,3$)?*

Wertetabelle:

x	y
-3	-20
-2	-4
-1	0
0	-2
1	-4
2	0
3	16



Definition 4.12. *Sei $f\colon X \to Y$ 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 4.13.

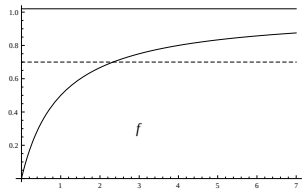
- *f ist genau dann surjektiv, wenn $Y = f(X)$.*
- *f ist genau dann injektiv, wenn für alle $x_1, x_2 \in X$ gilt $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.*
- *f ist genau dann injektiv, wenn für alle $x_1, x_2 \in X$ gilt $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.*
- *f ist genau dann bijektiv,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

Beispiel 4.14. *Für welche Mengen X_k, Y_k ist $f \subseteq X_k \times Y_k$ aus Beispiel 4.11 (a) injektiv (b) surjektiv (c) bijektiv?*

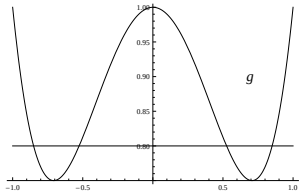
Die Begriffe injektiv und surjektiv hängen mit der Lösbarkeit der Gleichung $f(x) = y$ bei gegebener Funktion $f\colon X \to Y$ und gegebenen $y \in Y$ zusammen:

- 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 $x \in X$.
- Wenn f *bijektiv* ist, dann besitzt die Gleichung $f(x) = y$ *genau* eine Lösung $x \in X$.

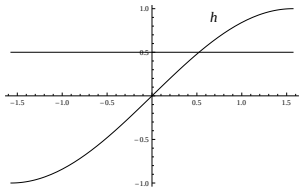
Die Lösung (falls existent) kann gefunden werden, indem die Kurve der Funktion mit der horizontalen Gerade durch y geschnitten wird.



$f\colon \mathbb{R}_0^+ \to \mathbb{R}_0^+,$
$x \mapsto 1 - \dfrac{1}{x+1}$



$g\colon [-1,1] \to [\frac{3}{4},1],$
$x \mapsto x^4 - x^2 + 1$



$h\colon [-\frac{\pi}{2},\frac{\pi}{2}] \to [-1,1]$
$x \mapsto \sin(x)$

Satz 4.15. *Zwei Mengen X, Y besitzen die gleiche Anzahl von Elementen (Kardinalität) genau dann, wenn eine bijektive Funktion $f\colon X \to Y$ existiert.*

Beispiel 4.16. *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 $f\colon \mathbb{N}_{ger} \to \mathbb{N}_{unger}$ ist z.B. gegeben durch $x \mapsto x+1$.*

Beispiel 4.17. *Die Abbildung*

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

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

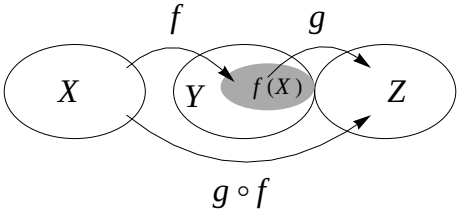
Definition 4.18. *Sei X eine Menge. Die Funktion von X nach X, die jedes Element $x \in X$ auf sich selbst abbildet heisst die* identische Abbildung *auf X und wird mit id_X bezeichnet.*

Die Identität $id_X\colon X \to X, x \mapsto x$ ist eine bijektive Funktion.

Definition 4.19. *Seien X, Y, Z Mengen und seien $f\colon X \to Y$ und $g\colon f(X) \to Z$ Funktionen. Dann ist die* Komposition *(*Hintereinanderausführung*) von f und g definiert als*

$$g \circ f\colon X \to Z, \quad x \mapsto (g \circ f)(x) = g(f(x)).$$

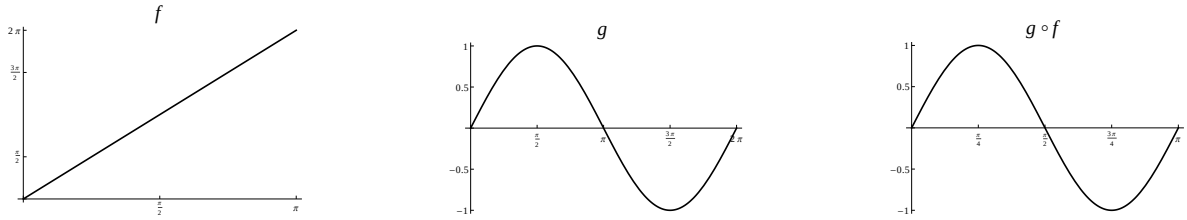
In Worten ist $g \circ f$ "g nach f".



Satz 4.20. *Die Komposition von zwei Funktionen ist eine Funktion.*

Beispiel 4.21. *Seien $X = [0,\pi], Y = [0,2\pi], Z = [-1,1]$ und seien die Funktionen f, g gegeben durch*

$$f\colon X \to Y, \quad x \mapsto 2x, \quad \textit{und} \quad g\colon Y \to Z, \quad x \mapsto \sin(x).$$



Die Hintereinanderausführung $g \circ f$ ist gegeben durch

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

Beispiel 4.22. *Die Funktionen f, g seien gegeben durch*

$$f \colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^3, \quad \textit{und} \quad g \colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x + 1.$$

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

Bemerkung 4.23. *Sei $f \colon X \to Y$ 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 4.24. *Sei $f \colon X \to Y$ eine Funktion. f heisst* invertierbar*, wenn es eine Funktion $f^{-1} \colon Y \to X$ gibt, sodass*

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

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 $f \colon X \to Y$) auf beiden Seiten die Umkehrfunktion angewandt wird, dann erhalten wir

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

Beispiel 4.25. *Sei $f \colon [0, 4] \to [-1, 1], x \mapsto \frac{x}{2} - 1$. Um die Umkehrfunktion $f^{-1} \colon [-1, 1] \to [0, 4]$ zu bestimmen formen wir $y = f(x)$ um auf $x = f^{-1}(y)$:*

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

Damit erhalten wir die Umkehrfunktion

$$f^{-1} \colon [-1, 1] \to [0, 4], \quad y \mapsto 2y + 2.$$

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

$$f \circ f^{-1}(x) = f(f^{-1}(x)) = f(2x+2) = \frac{2x+2}{2} - 1 = x$$
$$f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}\left(\tfrac{x}{2} - 1\right) = 2\left(\tfrac{x}{2} - 1\right) + 2 = x$$

Beispiel 4.26. *Welche der folgenden Funktionen ist invertierbar? Wie lautet die Umkehrfunktion der invertierbaren Funktionen?*

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

Definition 4.27. *Sei $f\colon X \to Y$ 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 4.28.

- *Die Betragsfunktion $f\colon [-5, 5] \to [0, 5], x \mapsto |x|$ ist im Intervall $[-5, 0]$ streng monoton fallend und im Intervall $[0, 5]$ streng monoton wachsend.*
- *Die Vorzeichenfunktion*

$$\operatorname{sign}\colon [-5, 5] \to [-1, 1], x \mapsto \begin{cases} 1, & x \geq 0 \\ -1, & x < 0 \end{cases}$$

ist monoton wachsend.

Satz 4.29. *Die Hintereinanderausführung zweier Funktionen f und g ist monoton wachsend, wenn f und g beide monoton wachsend oder beide monoton fallend sind.*

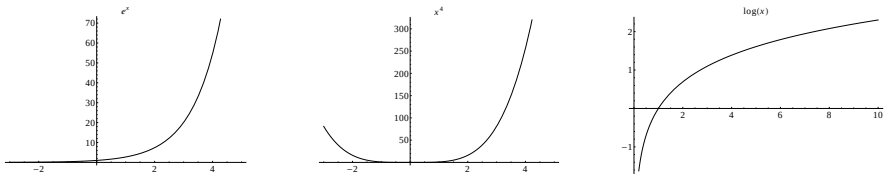
Die Hintereinanderausführung zweier Funktionen f und g ist monoton fallend, wenn f monoton wachsend und g monoton fallend ist, oder, wenn f monoton fallend und g monoton wachsend ist.

Definition 4.30. *Eine Funktion $p\colon X \to Y$ heisst ein* Polynom*, wenn es reelle Zahlen $a_0, \ldots, a_d$ gibt mit $p(x) = a_0 + a_1 x + \cdots + a_d x^d$. Wenn $a_d \neq 0$ gilt, dann nennt man d den* Grad *von p und schreibt $\deg(p(x)) = d$.*

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

Bemerkung 4.31. *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 $d_1 d_2$.*

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



Sei $a \in \mathbb{R}^+\backslash\{1\}$. Jede Funktion der Form $f\colon x \mapsto a^x$ (z.B. von $\mathbb{R}$ nach $\mathbb{R}^+$) heisst *Exponentialfunktion*. Ein Spezialfall ist die Funktion $\exp\colon x \mapsto e^x$, 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,

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

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

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

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

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

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

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

Wir betrachten die erste dieser Identitäten: Sei $u = \log_a(x)$ und $v = \log_a(y)$, d.h. nach Definition des Logarithmus gilt $x = a^u$ und $y = a^v$. Damit erhalten wir:

$$xy = a^u + a^v = a^{u+v}, \quad \text{und somit} \quad \log_a(xy) = \log_a\left(a^{u+v}\right) = u + v = \log_a(x) + \log_a(y).$$

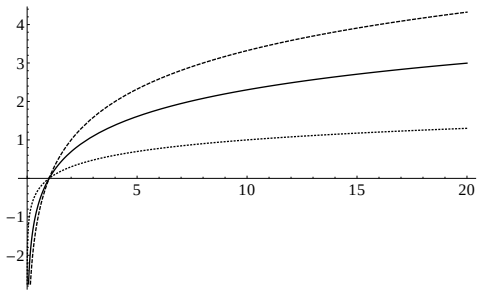
Der Logarithmus bezüglich jeder Basis kann mithilfe des natürlichen Logarithmus ausgerechnet werden:

$$\log_a(x) = \frac{\ln(x)}{\ln(a)},$$

weil

$$\log_a(x)\ln(a) = \ln\left(a^{\log_a(x)}\right) = \ln(x).$$

Damit unterscheiden sich die Logarithmen bezüglich verschiedener Basen nur um ein (konstantes) Vielfaches. Unten abgebildet sind der natürliche Logarithmus $\ln(x)$ (durchgezogene Linie), der Logarithmus zur Basis 10 $\log(x)$ (gepunktete Linie) und der Logarithmus zur Basis 2 $\log_2(x)$ (gestrichelte Linie).



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 $y \in Y$*

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

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.

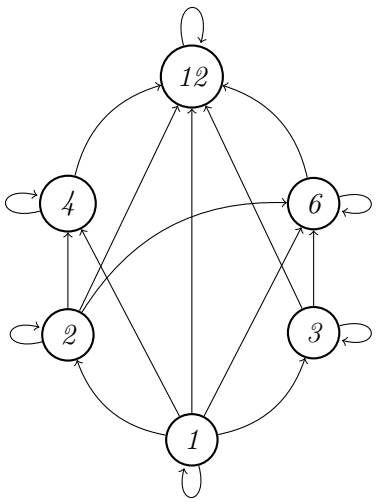
Beispiel 5.3. *Sei $X = \{1, 2, 3, 4, 6, 12\}$ dann wird durch die Bedingung x teilt y eine Relation auf X definiert. In Zeichen:*

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

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

$$\begin{aligned} R_3 = &\{(1,1), (1,2), (1,3), (1,4), (1,6), (1,12), (2,2), (2,4), (2,6), (2,12), (3,3)(3,6), (3,12), \\ &(4,4), (4,12), (6,6), (6,12), (12,12)\} \end{aligned}$$

oder graphisch darstellen, wobei Pfeile $x \to y$ 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*

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

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

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

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

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

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 $\mathrm{cod}(R) = Y$. 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 Defintion 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 $y = pq \cdot y$ 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*

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

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*

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

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*

$$(x_1, x_2) \in id_X \quad \Longleftrightarrow x_1 = x_2,$$

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

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

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 $a \equiv b \mod n$.*

Äquivalent dazu kann Kongruenz modulo n auch so definiert werden, dass $a \equiv b \mod n$ genau dann, wenn beide Zahlen a, b bei Division durch n den gleichen Rest haben. Dazu führen wir zuerst formal die Begriffe Quotient und Rest ein.

Definition 5.17. *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.*

Es gilt also $a \equiv b \mod n$, genau dann, wenn bei Division durch n gilt

$$a = q \cdot n + r \quad \text{und} \quad b = p \cdot n + r.$$

Beispiel 5.18. *Einige Beispiele:*

$7 \equiv 5 \mod 2$, *weil* $7 - 5 = 2$ *und* $2 \mid 2$, *oder* $7 = 3 \cdot 2 + 1$ *und* $5 = 2 \cdot 2 + 1$
$1 \equiv 3 \mod 2$, *weil* $1 - 3 = -2$ *und* $2 \mid -2$, *oder* $1 = 0 \cdot 2 + 1$ *und* $3 = 1 \cdot 2 + 1$
$27 \equiv 12 \mod 5$, *weil* $27 - 12 = 15$ *und* $5 \mid 15$, *oder* $27 = 5 \cdot 5 + 2$ *und* $12 = 2 \cdot 5 + 2$

Satz 5.19. *Kongruenz modulo n ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h., die Relation $\sim_n \subseteq \mathbb{Z} \times \mathbb{Z}$ definiert durch*

$$a \sim_n b \quad \Longleftrightarrow \quad a \equiv b \mod n.$$

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

$$n \mid a - a = 0 \quad \Leftrightarrow \quad a \equiv a \mod n \quad \Leftrightarrow \quad a \sim_n a.$$

  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.,

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

  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 $a \equiv c \mod n$, 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 5.20. *Sei $f \colon X \to Y$ eine Funktion. Dann ist $\sim_f \subseteq X \times X$ definiert durch*

$$a \sim_f b \quad \Longleftrightarrow f(a) = f(b)$$

eine Äquivalenzrelation.

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

Definition 5.21. *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 5.22. *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 5.23. *Für jede Äquivalenzrelation* $\sim$ *auf einer Menge* X *ist die Familie der Äquivalenzklassen* $\{[a] \mid a \in X\}$ *eine Partition von* X.

Beispiel 5.24. *Auf* $\mathbb{Z}$ *definieren wir die Äquivalenzrelation*

$$a \sim b \quad \Longleftrightarrow a \equiv b \mod 5.$$

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

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

was dem entspricht, dass der Rest *der Division durch* 5 *als Repräsentant gewählt wird, oder alternativ*

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

5.2 Ordnungsrelationen

Definition 5.25. *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*

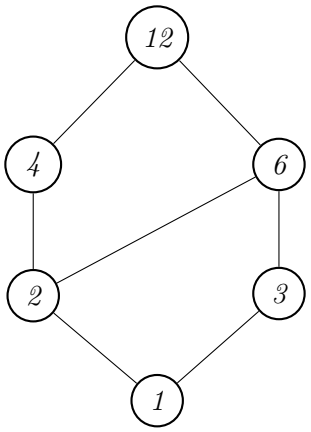
$$\forall\, x, y \in X : xRy \vee yRx$$

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 5.26. *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 5.27. *Die Relation R aus Beispiel 5.5 auf $X = P(\{1,2\})$ definiert als*

$$aRb \quad \Longleftrightarrow a \subseteq b$$

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

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

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.,*

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

Fallunterscheidung:

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

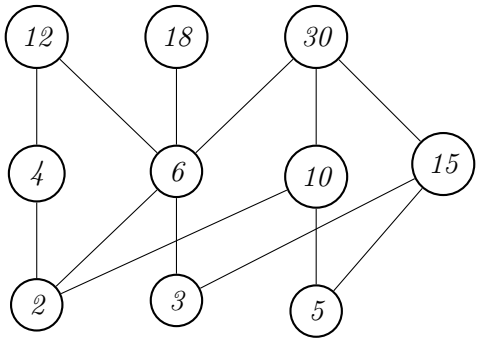
$\trianglelefteq$ ist eine Totalordnung: Seien $(a,b),(c,d) \in \mathbb{N}^2$. Für a,c gilt entweder $a < c$, $a > c$ oder $a = c$. Im ersten Fall ist $(a,b) \trianglelefteq (c,d)$, im zweiten Fall $(c,d) \trianglelefteq (a,b)$. Im dritten Fall betrachten wir b,d. Auch hier gilt $b < d$ oder $b > d$ 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 5.29. *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 5.30. *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 5.31. *Wir betrachten die Relation aus Beispiel 5.28 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, Teil 1

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

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

Diese Menge kann als Menge von Repräsentanten der Äquivalenzrelation *Kongruenz modulo n* (siehe Satz 5.19) betrachtet werden (also auch 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, d.h., jeweils der Rest bei Division durch n.

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

$$a + b = (a + b) \mod n \in \mathbb{Z}_n$$
$$a \cdot b = (a \cdot b) \mod n \in \mathbb{Z}_n$$

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

$$3 + 4 = 7 = 0 \mod 7, \quad 3 \cdot 4 = 12 = 5 \mod 7, \quad 4 \cdot 5 = 20 = 6 \mod 7, \ldots$$

Da $\mathbb{Z}_n$ eine endliche Menge ist können die Ergebnisse der Addition und Multiplikation von allen Kombinationen von Zahlen in $\mathbb{Z}_n$ berechnet und in Tabellen angegeben werden.

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*

$\cdot$	*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*

$\cdot$	*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, d.h., es gilt $a + 0 = 0 + a = a$ für jedes $a \in \mathbb{Z}_n$. Zu gegebenem $a \in \mathbb{Z}_n$ ist die* additive Inverse *definiert als jenes $b \in \mathbb{Z}_n$ für das gilt*

$$a + b = 0 \mod n.$$

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: für $a \in \mathbb{Z}_n \setminus \{0\}$ gilt $-a = n - a$ und für $a = 0$ gilt $-a = 0$.*

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

Buchstaben können als Zahlen in $\mathbb{Z}_{26}$ codiert werden, d.h., $A = 0, B = 1, \ldots, Y = 24, Z = 25$. 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

$$y = x + k \mod 26.$$

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

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

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

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

$$17 - 5 = 12 \mod 26, \quad 5 - 5 = 0 \mod 26, \quad 24 - 5 = 19 \mod 26, \ldots$$

zu MATHEMATIK im Klartext.

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

Definition 6.7. *Sei $n \in \mathbb{N}^*$. Das neutrale Element bezüglich (modularer) Multiplikation in $\mathbb{Z}_n$ ist 1, d.h., es gilt $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Z}_n$. Falls zu gegebenem $a \in \mathbb{Z}_n$ ein $b \in \mathbb{Z}_n$ existiert mit*

$$a \cdot b = 1 \mod n,$$

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 $3 \cdot 3 = 1 \mod 4$), aber $a = 2$ besitzt keine multiplikative Inverse. In $\mathbb{Z}_5$, besitzt jede Zahl ausser 0 eine multiplikative Inverse:

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

Bevor wir weiter untersuchen, wann eine Zahl in $\mathbb{Z}_n$ invertierbar ist und für welche $n \in \mathbb{N}^*$ jede Zahl invertierbar ist stellen wir den Euklidischen Algorithmus vor und untersuchen sogenannte diophantische Gleichungen.

6.2 Euklidischer Algorithmus und Diophantische Gleichungen

Definition 6.8. *Seien $a, b \in \mathbb{Z}$, nicht beide* 0*, dann ist der* grösste gemeinsame Teiler $\mathrm{ggT}(a, b)$ *(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 $q \mid \mathrm{ggT}(a, b)$. Nach Definition ist der grösste gemeinsame Teiler positiv, also eine natürliche Zahl. Außerdem gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) = \mathrm{ggT}(b, a)$, d.h. der grösste gemeinsame Teiler hängt nicht vom Vorzeichen der gegebenen Zahlen ab und ist in den Argumenten symmetrisch. Die erste Methode, die man in der Schule zur Berechnung des ggT kennenlernt ist über die Primfaktorenzerlegung.

Definition 6.9. *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:

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

Satz 6.10. *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 6.11. *Die Primfaktoren können z.B. durch sukzessives Dividieren von Primzahlen beginnend mit dem kleinsten Teiler gewonnen werden:*

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

Um $ggT(a, b)$ zu berechnen, kann man zuerst die Primfaktorenzerlegung von a und b bestimmen und anschließend wird jeder Faktor, der in beiden Zerlegungen vorkommt aufmultipliziert, also zum Beispiel $\mathrm{ggT}(100, 60) = 20$, da

$$100 = 2^2 \cdot 5^2 = \underline{2} \cdot \underline{2} \cdot \underline{5} \cdot 5 \quad \text{und} \quad 60 = 2^2 \cdot 3 \cdot 5 = \underline{2} \cdot \underline{2} \cdot 3 \cdot \underline{5} \quad \text{also} \quad \mathrm{ggT}(100, 60) = 2 \cdot 2 \cdot 5 = 20.$$

Es ist derzeit kein effizientes Verfahren bekannt, um die Primfaktorenzerlegung einer beliebigen ganzen Zahl zu berechnen und es ist eine der großen offenen Fragen der Informatik, ob Primfaktorenzerlegungen in polynomieller Zeit berechnet werden können. Auf dieser Tatsache basieren Verschlüsselungsverfahren wie RSA, das wir später noch betrachten werden.

Definition 6.12. *Zwei Zahlen $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$ heissen a, b* relativ prim *(oder teilerfremd).*

Satz 6.13. *Seien $a, b \in \mathbb{Z}$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$.*

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

Noch allgemeiner gilt:

Satz 6.14. *Seien $a, b \in \mathbb{Z}$ und $z \in \mathbb{Z}$. Dann gilt* $\mathrm{ggT}(a + zb, b) = \mathrm{ggT}(a, b)$.

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 leiten wir ihn anhand eines Beispiels her.

Seien $a, b \in \mathbb{N}$ mit $a > b$ gegeben. Die Division (siehe Definition 5.17) dieser beiden Zahlen liefert $q, r \in \mathbb{N}$ mit $r < b$ sodass

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

Laut Satz 6.14 gilt

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

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

1. Division liefert $34 = 28 \cdot 1 + 6$, d.h., $q = 1$ und $r = 6$. Dann gilt
$$\mathrm{ggT}(34, 28) = \mathrm{ggT}(34 - 28 \cdot 1, 28) = \mathrm{ggT}(6, 28) = \mathrm{ggT}(28, 6)$$
2. Division liefert $28 = 6 \cdot 4 + 4$, d.h., $q = 4$ und $r = 4$. Dann gilt
$$\mathrm{ggT}(28, 6) = \mathrm{ggT}(28 - 6 \cdot 4, 6) = \mathrm{ggT}(4, 6) = \mathrm{ggT}(6, 4)$$
3. Division liefert $6 = 4 \cdot 1 + 2$, d.h., $q = 1$ und $r = 2$. Dann gilt
$$\mathrm{ggT}(6, 4) = \mathrm{ggT}(6 - 4 \cdot 1, 4) = \mathrm{ggT}(2, 4) = \mathrm{ggT}(4, 2)$$
4. Division liefert $4 = 2 \cdot 2 + 0$, d.h., $q = 2$ und $r = 0$. Dann gilt
$$\mathrm{ggT}(4, 2) = \mathrm{ggT}(4 - 2 \cdot 2, 2) = \mathrm{ggT}(0, 2) = \mathrm{ggT}(2, 0) = 2.$$

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

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

Im zweiten Schritt erhalten wir:

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

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

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

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

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

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) $q_k = \mathrm{quot}(x_{k-1}, x_k)$ (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 $\mathrm{ggT}(a, b) = x_{k-1}$, 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 6.16. *Wir bestimmen den* $\mathrm{ggT}(126, 81)$ *mit dem EEA. Dazu notieren wir in der Tabelle zusätzlich den Schleifenindex k und den Quotienten q:*

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

Das heisst,

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

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

Beispiel 6.17. *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 ggT von 17 und 5 sowie die Bézout-Koeffizienten,

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

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 gannzzahlige 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:

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

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

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

Satz 6.18. *Die* diophantische Gleichung *$ax + by = c$ hat genau dann (mindestens) eine ganzzahlige Lösung, wenn c ein Vielfaches von $\mathrm{ggT}(a, b)$ ist, d.h., $c = q\,\mathrm{ggT}(a, b)$ für ein $q \in \mathbb{Z}$.*

Betrachten wir die Gleichung $ax + by = c$ mit gegebenen $a, b, c \in \mathbb{Z}$. Sei $d = \text{ggT}(a, b)$, dann kann d gemeinsam mit den Bézout-Koeffizienten x_0, y_0 und den Syzygien x_1, y_1 mit dem Erweiterten Euklidischen Algorithmus berechnet werden, d.h., wir erhalten

$$ax_0 + by_0 = d \tag{6.4}$$
$$ax_1 + by_1 = 0. \tag{6.5}$$

Wenn c ein Vielfaches des grössten gemeinsamen Teilers von a, b ist, wenn also gilt $c = qd$, dann kann (6.4) auf beiden Seiten mit q multipliziert werden und es gilt

$$a(qx_0) + b(qy_0) = qd,$$

d.h. $(x, y) = (qx_0, qy_0)$ ist eine ganzzahlige Lösung der gegebenen Gleichung. Außerdem kann (6.5) auf beiden Seiten mit einer ganzen Zahl k multipliziert werden und wir erhalten

$$a(kx_1) + b(ky_1) = 0.$$

Wenn die beiden letzten Gleichungen addiert werden ergibt das

$$a(qx_0 + kx_1) + b(qy_0 + ky_1) = c,$$

d.h., jedes Tupel der Form $(x, y) = (qx_0 + kx_1, qy_0 + ky_1)$ für beliebiges $k \in \mathbb{Z}$ ist eine *ganzzahlige* Lösung der gegebenen diophantischen Gleichung. Die Syzygien, die mit dem EEA berechnet werden, sind genau $x_1 = -b/d$ und $y_1 = a/d$. Zusammengefasst ergibt das folgenden Satz.

Satz 6.19. *(Fortsetzung von Satz 6.18) 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*

$$\{(qx_0 + kx_1, qy_0 + ky_1) \mid k \in \mathbb{Z}\},$$

wobei x_1, y_1 die Syzygien von a, b sind.

Beispiel 6.20.

- *Gegeben ist die diophantische Gleichung $251x + 127y = 16$. Wir wenden den EEA an und erhalten*

$$251 \cdot 42 + 127 \cdot (-83) = 1$$
$$251 \cdot (-127) + 127 \cdot 251 = 0.$$

  Da der ggT dieser beiden Zahlen 1 ist, ist die diophantische Gleichung sogar für jede (ganzzahlige) rechte Seite lösbar (da jede ganze Zahl durch 1 teilbar ist). Als Lösungsmenge erhält man damit

$$L = \{(672 - 127k, -1328 + 251k) \mid k \in \mathbb{Z}\}.$$

- *Gegeben ist die diophantische Gleichung $60x + 128y = c$ für ein $c \in \mathbb{Z}$. Wir berechnen den $\text{ggT}(128, 60) = 4$ mit Bézout-Koeffizienten und Syzygien wie folgt:*

$$60 \cdot 15 + 128 \cdot (-7) = 4$$
$$60 \cdot (-32) + 128 \cdot 15 = 0.$$

Damit gilt, dass die diophantische Gleichung genau dann ganzzahlige Lösungen besitzt, wenn c ein Vielfaches von 4 ist. Zum Beispiel gilt für $c = -12$, dass

$$L = \{(-45 - 32k, 21 + 15k) \mid k \in \mathbb{Z}\}.$$

Wenn c kein Vielfaches von 4 ist, also z.B. $c = 1, 17, -121, \ldots$, dann ist die Lösungsmenge die leere Menge.

6.3 Modulare Arithmetik, Teil 2

Der erweiterte Euklidische Algorithmus kann verwendet werden, um die multiplikative Inverse in $\mathbb{Z}_n$ zu bestimmen, sofern sie existiert.

Beispiel 6.21. *Sei $a = 11$ und wir suchen $a^{-1} \in \mathbb{Z}_{26}$, d.h., gesucht ist $b \in \mathbb{Z}_{26}$ mit $11b = 1 \mod 26$. Diese Gleichung ist erfüllt, wenn es ein $q \in \mathbb{Z}$ gibt mit*

$$11b + 26q = 1.$$

Das ist eine diophantische Gleichung, die mit dem EEA gelöst werden kann. Zuerst berechnen wir den $\mathrm{ggT}(11, 26) = 1$. Nach Satz 6.18 existiert eine Lösung der Gleichung (weil der größte gemeinsame Teiler die rechte Seite der Gleichung teilt). Die Bézout-Koeffizienten und Syzygien sind gegeben durch:

$$(-7) \cdot 11 + 3 \cdot 26 = 1 \quad \textit{und} \quad 26 \cdot 11 + (-11) \cdot 26 = 0.$$

Damit sind nach Satz 6.19 die ganzzahligen Lösungen der obigen Gleichung gegeben durch $(b, q) = (-7 + 26k, 3 + 11k)$ für $k \in \mathbb{Z}$. Für die modulare Inverse müssen wir nur ein $b \in \mathbb{Z}_{26}$ aus dieser Lösungsmenge bestimmen und das ergibt sich durch die Wahlt $k = 1$. Damit erhalten wir $a^{-1} = 19$.

Um die multiplikative Inverse b einer gegebenen Zahl $a \in \mathbb{Z}_n$ zu bestimmen, muss also eine Gleichung der Form

$$a \cdot b + n \cdot q = 1$$

gelöst werden. Nach Satz 6.18 besitzt die Gleichung genau dann eine Lösung, wenn $\mathrm{ggT}(a, n) \mid 1$, d.h., genau dann wenn $\mathrm{ggT}(a, n) = 1$, also wenn a und n relativ prim sind.

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

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

und mit dem oben Besprochenen folgt

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid ggT(a, n) = 1\}.$$

Zum Beispiel gilt

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

und für p eine Primzahl gilt $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$.

Satz 6.22. *Sei $n \in \mathbb{N}^*$. Jede Zahl $a \in \mathbb{Z}_n$ mit $\mathrm{ggT}(a, n) = 1$ besitzt eine eindeutig bestimmte multiplikative Inverse.*

Für modulare Gleichungen der Form $a \cdot x = b \mod n$ gilt

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

Beispiel 6.23. *Die Gleichung* $4x = 2 \mod n$ *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*

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

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

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* $\alpha, \beta \in \mathbb{Z}_n$ *so sind, dass*

$$a = \alpha \mod n \quad \textit{und} \quad b = \beta \mod n,$$

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

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

Damit gilt

$$ab = (qn + \alpha)(pn + \beta) = qp\, n^2 + (\alpha p + \beta q)n + \alpha\beta = \alpha\beta \mod n.$$

Als haben wir insgesamt, dass

$$a \cdot b = \alpha \cdot \beta \mod n.$$

6.4 Satz von Fermat und RSA

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

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

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

$$f \colon \mathbb{Z}_p \to \mathbb{Z}_p, \quad a \mapsto x \cdot a \mod p.$$

Diese Funktion ist invertierbar, da

$$f(a) = b \quad \Leftrightarrow \quad b = x \cdot a \mod p \quad \Leftrightarrow \quad y \cdot b = xy \cdot a = a \mod p.$$

Damit ist die zu f inverse Funktion gegeben durch

$$f^{-1} \colon \mathbb{Z}_p \to \mathbb{Z}_p, \quad b \mapsto y \cdot b \mod p.$$

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 $\{x, 2x, 3x, \ldots, (p-1)x\}$ (via Rest modulo p) bijektiv auf die Menge $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ abgebildet. Daher stimmt das Produkt über jeweils alle Zahlen aus diesen Mengen modulo p überein:

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

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

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 $\mathrm{ggT}(e, m) = 1$.
3. Für den private key berechnet sie d mit $ed = 1 \mod m$ (so ein d muss existieren, da e und m teilerfremd sind).
4. Alice schickt als public key das Paar (n, e) and 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

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

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

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

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

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

mit $\ell = k(q-1)$.

Wir unterscheiden jetzt zwei Fälle:

- x und p besitzen einen gemeinsamen Teiler: dann muss x ein Vielfaches der Primzahl p sein und es gilt $x = 0 \mod p$ und damit $x \cdot x^{\ell(p-1)} = 0 \mod p$. Damit gilt $x^{ed} = x \mod p$.
- x und p sind teilerfremd: Dann gilt nach dem kleinen Satz von Fermat

$$x^{ed} = x \cdot x^{\ell(p-1)} = x \cdot 1^{\ell} = x \mod p$$

In beiden Fällen gilt also $x^{ed} = x \mod p$. Analog gilt $x^{ed} = x \mod q$. Aus diesen beiden Identitäten folgt, dass sowohl p als auch q Teiler von $x^{ed} - x$ sind. Da p, q Primzahlen sind muss also auch das Produkt pq ein Teiler von $x^{ed} - x$ sein, d.h., es existiert ein $j \in \mathbb{N}$ sodass

$$y^d - x = x^{ed} - x = j\ pq = j\ n, \quad \text{und damit} \quad y^d - x = 0 \mod n \quad \Rightarrow \quad y^d = x \mod n.$$

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*

$$12^{107} = 2967517762021717 \ldots 91986235538841431787438 08 = 3352 \mod 4307,$$

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 aufwendig ist. Wenn die Primfaktoren von n berechnet werden können, dann kann der Code gebrochen werden.

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. $+\colon \mathbb{N} \times \mathbb{N}, (a, b) \mapsto a + b$ *ist eine Operation*
2. $-\colon \mathbb{N} \times \mathbb{N}, (a, b) \mapsto a - b$ *ist* keine *Operation, da zum Beispiel* $(2, 4)$ *auf* $-2 \notin \mathbb{N}$ *abgebildet wird*
3. *Sei A eine Menge, dann ist* $\cap\colon P(A) \times P(A) \to P(A)$ *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* $\wedge\colon X \times X \to X$ *eine Operation.*
5. *Der größte gemeinsame Teiler ist eine Operation auf den natürlichen Zahlen:* $\mathrm{ggT}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a, b) \mapsto \mathrm{ggT}(a, b)$*, wobei wir für $a = b = 0$ definieren, dass* $\mathrm{ggT}(0, 0) = 0$.

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

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:*

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

- *$(\mathbb{N}, \mathrm{ggT})$ ist eine Halbgruppe, da der größte gemeinsame Teiler assoziativ ist, also für $a, b, c \in \mathbb{N}$ gilt*

$$\mathrm{ggT}\big(\mathrm{ggT}(a,b), c\big) = \mathrm{ggT}\big(a, \mathrm{ggT}(b,c)\big).$$

  Auf beiden Seiten wird hier die größte natürliche Zahl bestimmt, die a, b, und c teilt. $(\mathbb{N}, \mathrm{ggT})$ ist ausserdem ein Monoid mit neutralem Element 0, da $\mathrm{ggT}(a, 0) = \mathrm{ggT}(0, a) = a$ für alle $a \in \mathbb{N}$.

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

$$\exists\, b \in A\colon a \circ b = b \circ a = e.$$

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

Definition 7.9. *Ein Monoid $(G, \circ)$ heisst* Gruppe*, wenn jedes $g \in G$ 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.*

Die Gruppe der *Permutationen*, die wir als nächstes betrachten war historisch die erste Gruppe, die untersucht wurde.

Definition 7.12. *Sei* X *eine nichtleere Menge. Eine bijektive Funktion* $\pi\colon X \to X$ *wird eine* Permutation *von* X *genannt. Die Menge aller Permutationen der Menge* X *bezeichnen wir mit* $\mathrm{Sym}(X)$.

Beispiel 7.13. *Sei* $X = [0, 4]$*, dann sind zum Beispiel* $\pi_1\colon X \to X, x \mapsto 4 - x$ *und* $\pi_2\colon X \to X, x \mapsto \frac{x^3}{16}$ *Permutationen der Menge* X*, also* $\pi_1, \pi_2 \in \mathrm{Sym}(X)$.

Eine Permutation ist also eine Umordnung der Elemente einer gegebenen Menge. Die Menge aller Permutationen bildet eine Gruppe mit Hintereinanderausführung von Funktionen als Operation:

Lemma 7.14. *Sei* $X \neq \emptyset$*. Dann ist* $(\mathrm{Sym}(X), \circ)$ *(wobei* $\circ$ *die Komposition von Funktionen bezeichnet) eine Gruppe gennant die* symmetrische Gruppe *auf* X.

Beweis.
- $(\mathrm{Sym}(X), \circ)$ ist eine Algebra, d.h., die symmetrische Gruppe ist abgeschlossen unter Hintereinanderausführung: Dazu ist zu zeigen, dass die Komposition bijektiver Funktionen wieder bijektiv ist. Seien $\pi, \sigma \in \mathrm{Sym}(X)$, dann gilt, dass $\pi(X) = X$ und $\sigma(X) = X$ und damit $\pi \circ \sigma(X) = X$, also ist $\pi \circ \sigma$ surjektiv. Sei jetzt $z \in X$, dann existiert ein eindeutig bestimmtes Urblid $\pi^{-1}(z) = y$, da π bijektiv ist, und, da σ bijektiv, ein eindeutig bestimmtes Urbild $\sigma^{-1}(y) = x$. Also ist die Kompostion injektiv und somit bijektiv.
- $(\mathrm{Sym}(X), \circ)$ ist eine Halbgruppe, d.h., die Hintereinanderausführung ist assoziativ auf $\mathrm{Sym}(X)$: Seien $\pi_1, \pi_2, \pi_3 \in \mathrm{Sym}(X)$ und $x \in X$, dann gilt
$$((\pi_1 \circ \pi_2) \circ \pi_3)(x) = (\pi_1 \circ \pi_2)(\pi_3(x)) = \pi_1(\pi_2(\pi_3(x))),$$
und
$$(\pi_1 \circ (\pi_2 \circ \pi_3))(x) = \pi_1(\pi_2 \circ \pi_3(x)) = \pi_1(\pi_2(\pi_3(x))).$$
- $(\mathrm{Sym}(X), \circ)$ ist ein Monoid, d.h., es existiert ein neutrales Element in $\mathrm{Sym}(X)$: Das neutrale Element ist durch $id_X \in \mathrm{Sym}(X)$ gegeben.
- $(\mathrm{Sym}(X), \circ)$ ist eine Gruppe, d.h., jedes Element in $\mathrm{Sym}(X)$ ist bezüglich $\circ$ invertierbar: jede bijektive Funktion ist invertierbar und die Inverse ist wieder bijektiv, also ein Element der symmetrischen Gruppe.

□

Wenn wir die Permutation einer endlichen Menge X mit $|X| = n$ ($n \in \mathbb{N}$) betrachten, kann man sich ohne Beschränkung der Allgemeinheit auf die Mengen $\{1, 2, 3, \ldots, n\}$ beschränken. Wenn eine Menge $X = \{x_1, x_2, x_3, \ldots, x_n\}$ gegeben ist, dann entspricht die Anwendung einer Permutation $\sigma \in \mathrm{Sym}(X)$ mit $\sigma(x_i) = x_j$ einer Permutation der Indizes durch eine Permutation $\pi \in \mathrm{Sym}(\{1, 2, 3, \ldots, n\})$ mit $\pi(i) = j$. Wenn die gegebene Menge $X = \{1, 2, 3, \ldots, n\}$

ist, dann schreiben wir für die symmetrische Gruppe $S_n = \mathrm{Sym}(X)$. Eine übliche Schreibweise für Permutationen in S_n ist wie folgt

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix},$$

d.h., in der zweiten Reihe stehen die Bilder unter π von Elementen aus der ersten Reihe. Mitunter wird auf die erste Reihe verzichtet und nur die zweite Reihe angegeben, also die folgende Schreibweise verwendet:

$$\pi = \big(\pi(1)\ \pi(2)\ \pi(3)\ \dots\ \pi(n)\big).$$

Beispiel 7.15. *Wir betrachten die folgenden Element von $\pi, \sigma \in S_6$,*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 3 & 4 \end{pmatrix}, \quad \textit{und} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

Dann gilt

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 2 & 1 & 3 \end{pmatrix}, \quad \textit{und} \quad \sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

An diesem Beispiel sieht man, dass die symmetrische Gruppe keine *Abelsche Gruppe ist (die Verknüpfung ist im allgemeinen nicht kommutativ). Ausserdem gilt*

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 4 & 1 \end{pmatrix}$$

Beispiel 7.16. *Die Elemente der symmetrischen Gruppe S_4 sind gegeben durch (wobei wir die letztgenannte Schreibweise verwenden):*

$$\begin{array}{llllll}
(1\ 2\ 3\ 4), & (1\ 2\ 4\ 3), & (1\ 3\ 2\ 4), & (1\ 3\ 4\ 2), & (1\ 4\ 2\ 3), & (1\ 4\ 3\ 2), \\
(2\ 1\ 3\ 4), & (2\ 1\ 4\ 3), & (2\ 3\ 1\ 4), & (2\ 3\ 4\ 1), & (2\ 4\ 1\ 3), & (2\ 4\ 3\ 1), \\
(3\ 1\ 2\ 4), & (3\ 1\ 4\ 2), & (3\ 2\ 1\ 4), & (3\ 2\ 4\ 1), & (3\ 4\ 1\ 2), & (3\ 4\ 2\ 1), \\
(4\ 1\ 2\ 3), & (4\ 1\ 3\ 2), & (4\ 2\ 1\ 3), & (4\ 2\ 3\ 1), & (4\ 3\ 1\ 2), & (4\ 3\ 2\ 1).
\end{array}$$

Für die Anzahl der Element der symmetrischen Gruppe gilt also $|S_4| = 24$.

Lemma 7.17. *Sei $n \in \mathbb{N}^*$, dann gilt $|S_n| = n!$ (oder allgemein für eine n-elementige Menge X gilt $|\mathrm{Sym}(X)| = n!$).*

Beweis. Wenn wir die Arten betrachten wie die zweite Reihe einer Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

gebildet werden können, dann gibt es n mögliche Werte für $\pi(1)$, aber nur $n-1$ mögliche Werte für $\pi(2)$ (da der Wert der 1 zugewiesen wurde nicht wieder verwendet werden darf). Für $\pi(3)$ gibt es dann nur mehr $n-2$ mögliche Werte, usw. Damit gibt es insgesamt $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ verschiedene Permutationen der Menge $X = \{1, 2, \dots, n\}$. □

Beispiel 7.18. *(Verknüpfungstabelle für S_3)*

$\circ$	*(1 2 3)*	*(1 3 2)*	*(2 1 3)*	*(2 3 1)*	*(3 1 2)*	*(3 2 1)*
(1 2 3)	*(1 2 3)*	*(1 3 2)*	*(2 1 3)*	*(2 3 1)*	*(3 1 2)*	*(3 2 1)*
(1 3 2)	*(1 3 2)*	*(1 2 3)*	*(3 1 2)*	*(3 2 1)*	*(2 1 3)*	*(2 3 1)*
(2 1 3)	*(2 1 3)*	*(2 3 1)*	*(1 2 3)*	*(1 3 2)*	*(3 2 1)*	*(3 1 2)*
(2 3 1)	*(2 3 1)*	*(2 1 3)*	*(3 2 1)*	*(3 1 2)*	*(1 2 3)*	*(1 3 2)*
(3 1 2)	*(3 1 2)*	*(3 2 1)*	*(1 3 2)*	*(1 2 3)*	*(2 3 1)*	*(2 1 3)*
(3 2 1)	*(3 2 1)*	*(3 1 2)*	*(2 3 1)*	*(2 1 3)*	*(1 3 2)*	*(1 2 3)*

7.2 Abbildungen zwischen algebraischen Strukturen

Ein Homomorphismus ist *strukturerhaltende* Abbildung.

Definition 7.19. *Seien $(A_1, \circ_1)$ und $(A_2, \circ_2)$ zwei algebraische Strukturen. Dann nennt man φ 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 φ einen Gruppenhomomorphismus.

Beispiel 7.20. *Die Abbildung $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}_5, \oplus)$ mit $x \mapsto \mathrm{rem}(x, 5)$ ist ein Homomorphismus, wobei wir mit $\oplus$ die modulare Addition bezeichnen und $\mathrm{rem}(a, b)$ den Rest bei Division a durch b bezeichnet (*rem *als Abkürzung für engl. remainder). Seien $x, y \in \mathbb{Z}$, dann ist zu zeigen, dass*

$$\varphi(x + y) = \mathrm{rem}(x + y, 5) = \mathrm{rem}(x, 5) \oplus \mathrm{rem}(y, 5) = \varphi(x) \oplus \varphi(y).$$

Seien $a, b \in \mathbb{Z}_5$ so dass $\mathrm{rem}(x, 5) = a$ und $\mathrm{rem}(y, 5) = b$, d.h., es gibt $p, q \in \mathbb{Z}$ sodass $x = 5p + a$ und $y = 5q + b$. Dann gilt

$$\varphi(x + y) = \mathrm{rem}(x + y, 5) = \mathrm{rem}(5p + a + 5q + b, 5) = \mathrm{rem}(a + b, 5) = a \oplus b = \varphi(x) \oplus \varphi(y).$$

Durch einen Gruppenhomomorphismus φ 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 7.21. *Für den Homomorphismus aus Beispiel 7.20 gilt: $\varphi(0) = \mathrm{rem}(0, 5) = 0$. Sei $x \in \mathbb{Z}$ so, dass $x = 5q + a$ (also $a = \varphi(x) = \mathrm{rem}(x, 5) \in \mathbb{Z}_5$), dann gilt*

$$\varphi(-x) = \varphi(-5q - a) = \mathrm{rem}(-5q - a, 5) = \mathrm{rem}(-a, 5) = 5 - a = \ominus\varphi(x),$$

wobei $\ominus$ anzeigen soll, dass wir die additive Inverse in $\mathbb{Z}_5$ betrachten.

Definition 7.22. *Ein Homomorphismus φ 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 φ 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)

Beispiel 7.23. *Die Abbildung $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot), x \mapsto e^x$ ist ein Gruppenisomorphismus: $(\mathbb{R}, +)$ ist eine Abelsche Gruppe mit neutralem Element 0, $(\mathbb{R}, \cdot)$ ist eine Abelsche Gruppe mit neutralem Element 1. Es gilt für $x, y \in \mathbb{R}$, dass*

$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x) \cdot \varphi(y), \quad \textit{und} \quad \varphi(0) = e^0 = 1.$$

Die Funktion ist ausserdem bijektiv ($\varphi(\mathbb{R}) = \mathbb{R}^+$ und die Funktion streng monoton steigend).

Beispiel 7.24. *Sei $X = \{x_1, x_2, \ldots, x_n\}$ eine n-elementige Menge, und sei $\varphi\colon (\mathrm{Sym}(X), \circ) \to (S_n, \circ)$ die Funktion, die einer Permutation $\pi \in \mathrm{Sym}(X)$ die Permutation $\sigma \in S_n$ so zuordnet, dass*

$$\pi(x_i) = x_j \quad \Leftrightarrow \quad \sigma(i) = j, \quad \textit{d.h.} \quad \pi(x_i) = x_{\sigma(i)}.$$

Dann ist φ ein Gruppenisomorphismus. Seien $\pi_1, \pi_2 \in \mathrm{Sym}(X)$ mit Bildern $\varphi(\pi_k) = \sigma_k$ ($k = 1, 2$), dann gilt

$$(\pi_1 \circ \pi_2)(x_i) = \pi_1(\pi_2(x_i)) = \pi_1(x_{\sigma_2(i)}) = x_{\sigma_1(\sigma_2(i))} = x_{(\sigma_1 \circ \sigma_2)(i)},$$

also $\varphi(\pi_1 \circ \pi_2) = \varphi(\pi_1) \circ \varphi(\pi_2)$.