Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Skript zur Vorlesung

Diskrete Mathematik

Teil I der Veranstaltung
Einführung in diskrete Mathematik und Lineare Algebra

Dr. Marco Hülsmann

Wintersemester 2024/25
Zuletzt bearbeitet: 18.02.2025

GeTEXt von Maximilian Räthel und Simon Bürvenich.

Inhaltsverzeichnis

0 Grundlagen

0.1 Mengen

Definition 0.1 (Menge)**.** Eine *Menge* A ist eine Sammlung verschiedener Objekte, auch *Elemente* $a, b, c, d, \ldots$ genannt, die aus einem *Universum* U stammen. Man schreibt $a \in A$, wenn a ein Element der Menge A ist, andernfalls $a \notin A$.

Aufzählende Darstellung.

$$A = \{\, a, b, c, d \,\}$$
$$A = \{\, a, b, c, \ldots, z \,\}$$
$$A = \{\, 1, 2, 3, 4, \ldots \,\}$$

Beschreibende Darstellung.

$$A = \{\, x \in U \mid x \text{ hat bestimmte Eigenschaft } p \,\}$$
$$A = \{\, x \in U \mid x \notin B \,\}$$

Definition 0.2 (Leere Menge)**.** Die Menge $\varnothing = \{\ \} := \{\, x \mid x \neq x \,\}$ heißt *leere Menge*. Für alle Elemente x des Universums U gilt: $x \notin \varnothing$, d.h. die leere Menge enthält keine Elemente.

Definition 0.3 (Kardinalität)**.** Die *Kardinalität* $|A|$ einer Menge ist die Anzahl ihrer Elemente.

Beispiel 0.1 (Zahlenmengen)**.**

(i) Aufzählende Darstellung.

$$A = \{\, 1, 2, 3 \,\} = \{\, 3, 1, 2 \,\} = \{\, 1, 2, 2, 3 \,\}$$
$$|A| = 3$$

Natürliche Zahlen.

$$\mathbb{N} := \{\, 1, 2, 3, 4, 5, 6, 7, \ldots \,\}$$
$$\mathbb{N}_0 := \{\, 0, 1, 2, 3, 4, 5, 6, 7, \ldots \,\}$$
$$|\mathbb{N}| = |\mathbb{N}_0| = \infty$$

(ii) Beschreibende Darstellung.
Ganze Zahlen.

$$\mathbb{Z} := \{\, x \in \mathbb{U} \mid x \in \mathbb{N}_0 \text{ oder } -x \in \mathbb{N}_0 \,\}$$

Rationale Zahlen.

$$\mathbb{Q} := \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\, q \in \mathbb{N} \right\}$$

Komplexe Zahlen.

$$\mathbb{C} := \{\, a + ib \mid a, b \in \mathbb{R},\ i^2 = -1 \,\}$$

Sonstige.

$$\begin{aligned} B &:= \{\, x \in \mathbb{Z} \mid x^2 \leq 9 \,\} \\ |B| &= 7 \end{aligned}$$

(iii) Leere Menge.

$$\begin{aligned} &x \notin \emptyset \text{ für alle } x \in \mathbb{U} \\ &|\emptyset| = 0 \end{aligned}$$

Definition 0.4 (Teilmenge)**.** Eine Menge B ist eine *Teilmenge* der Menge A, wenn alle Elemente von B auch in A enthalten sind, wenn also für alle $x \in B$ gilt: $x \in A$. Schreibweise: $B \subseteq A$.

Beispiel 0.2.

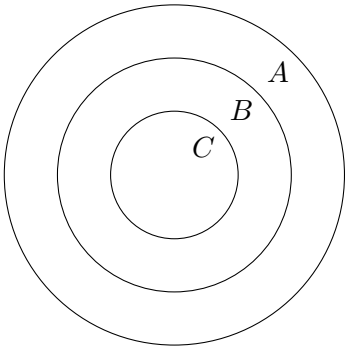
(i) $\{1, 2, \quad 5 \quad\}$
$\subseteq \{1, 2, 3, 4, 5 \quad\}$
$\subseteq \{1, 2, 3, 4, 5, 6\}$

(ii) $\{1, 2, 3, 4, 5\}$
$\supseteq \{1, 2, \quad 5\}$
$\supseteq \{1, 2 \qquad\}$

(iii) $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

(iv) $\emptyset \subseteq A$ für jede Menge A

Venn-Diagramme.



$C \subseteq B \subseteq A$

Satz 0.1. *Falls $B \subseteq A$, so gilt $|B| \leq |A|$. Falls $B \subseteq A$ und $A \subseteq C$, so gilt auch $B \subseteq C$ ($B \subseteq A \subseteq C$).*

Beweis. Sei $B \subseteq A$. Falls $|B| > |A|$, so hat B mind. ein Element x mehr als A. Für dieses x gilt $x \notin A$. Dann kann aber $B \subseteq A$ nicht mehr gelten, also muss $|B| \leq |A|$ gelten. Sei nun $x \in B$ beliebig. Wegen $B \subseteq A$ gilt auch $x \in A$ und wegen $A \subseteq C$ auch $x \in C$. Insgesamt gilt für jedes $x \in B$ auch $x \in C$, also $B \subseteq C$. □

Definition 0.5 (Gleiche Mengen)**.** Zwei Mengen A und B heißen *gleich*, wenn sie dieselben Elemente besitzen, wenn also aus $x \in A$ $x \in B$ folgt und umgekehrt, bzw. wenn sowohl $A \subseteq B$ als auch $B \subseteq A$ gilt.

Bemerkung 0.1. Möchte man beweisen, dass zwei Mengen gleich sind, dass also $A = B$ gilt, so zeigt man zwei Teilmengenbeziehungen: $A \subseteq B$ und $B \subseteq A$.

Definition 0.6 (Vereinigungsmenge)**.** Seien A und B Mengen. Dann heißt

$$A \cup B := \{\, x \in U \mid x \in A \text{ oder } x \in B \,\}$$

die *Vereinigungsmenge* von A und B. Ist $(A_i)_{i \in \mathbb{N}}$ eine Familie von Mengen, so ist deren Vereinigungsmenge gegeben durch:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

Definition 0.7 (Schnittmenge)**.** Seien A und B Mengen. Dann heißt

$$A \cap B := \{\, x \in U \mid x \in A \text{ und } x \in B \,\}$$

die *Schnittmenge* von A und B. Ist $(A_i)_{i \in \mathbb{N}}$ eine Familie von Mengen, so ist deren Schnittmenge gegeben durch:

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

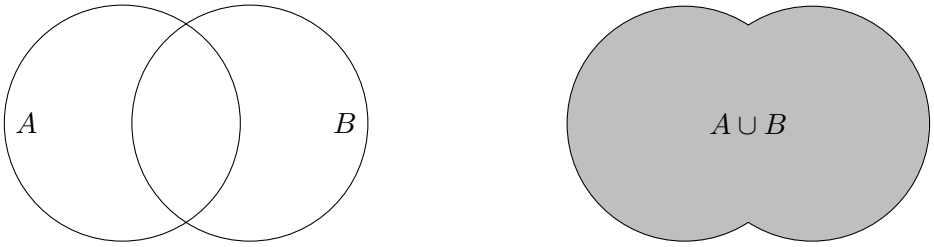


Abbildung 2: Vereinigungsmenge von A und B.

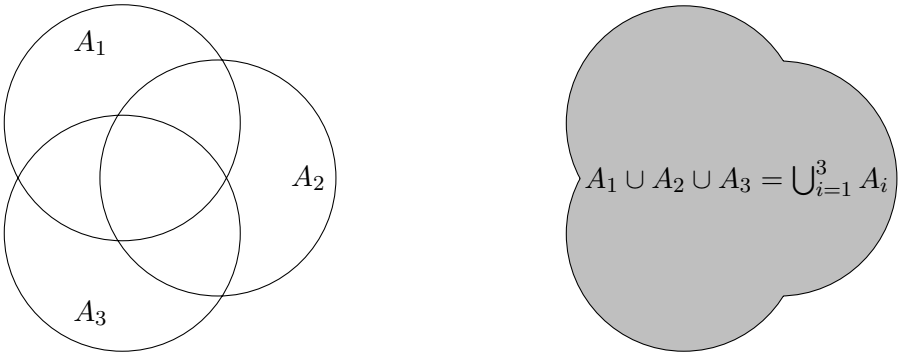


Abbildung 3: Vereinigungsmenge einer Familie von Mengen.

Beispiel 0.3. $A_1 = \{\, 1, 3, 5, 7 \,\},\ A_2 = \{\, 2, 3, 5 \,\}$.

$$
\begin{aligned}
A_1 &= \{1, \quad 3, 5, 7\} \\
A_2 &= \{\quad 2, 3, 5 \quad\} \\
A_1 \cup A_2 &= \{1, 2, 3, 5, 7\} = \bigcup_{i=1}^{2} A_i \\
A_1 \cap A_2 &= \{\qquad 3, 5 \quad\} = \bigcap_{i=1}^{2} A_i
\end{aligned}
$$

Definition 0.8 (Komplement)**.** Die Menge $\overline{A} := \{\, x \in U \mid x \notin A \,\}$ ist das *Komplement* von A. Weiterhin definiert man: $A \setminus B := \{\, x \in A \mid x \notin B \,\}$ (gesprochen: „A ohne B“).

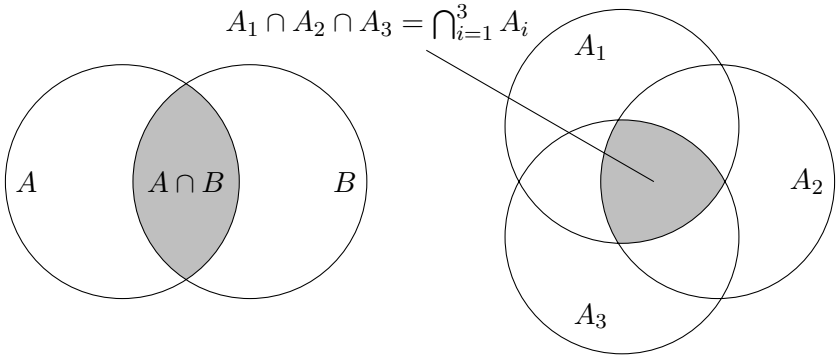


Abbildung 4: Schnittmengen.

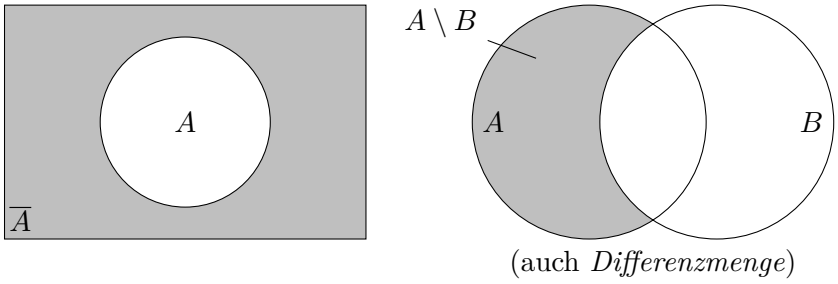


Abbildung 5: Komplemente von Mengen.

Beispiel 0.4. Sei $U = \{\, 1, \ldots, 7 \,\}$.

$$
\begin{aligned}
U &= \{1, 2, 3, 4, 5, 6, 7\} \\
\overline{A} &= \{\quad 2, \quad 4, \quad 6 \quad\} \\
A &= \{1, \quad 3, \quad 5, \quad 7\} \\
A \setminus B &= \{1, \qquad\qquad 7\} \\
B \setminus A &= \{\quad 2 \qquad\qquad\quad\} \\
B &= \{\quad 2, 3, \quad 5 \qquad\} \\
\overline{B} &= \{1, \qquad 4, \quad 6, 7\} \\
B \cap (A \setminus B) &= \emptyset \quad \text{(das ist immer so!)}
\end{aligned}
$$

Satz 0.2. *Für zwei Mengen A und B gilt*

$$
\begin{aligned}
A \cap B &= \overline{\overline{A} \cup \overline{B}} \\
A \subseteq B &\implies \overline{B} \subseteq \overline{A} \quad \textit{(Antitonie)}
\end{aligned}
$$

Beweisskizze durch Venn-Diagramme in Abbildung 6. □

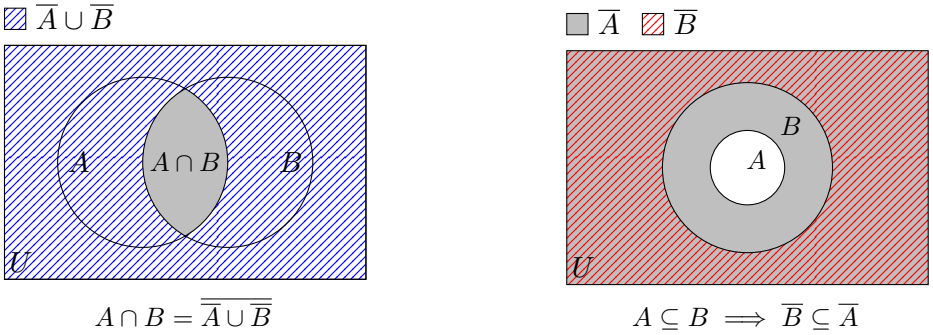


Abbildung 6: Beweisskizze für Satz 0.2.

Definition 0.9 (Kartesisches Produkt)**.** Das n-*äre* (*binäre* für $n = 2$ und *ternäre* für $n = 3$) *kartesische Produkt* von Mengen A_i, $i = 1, \ldots, n$ (auch *Kreuzprodukt*), ist die Menge aller Tupel der Länge n, bestehend aus Elementen der entsprechenden Mengen:

$$\bigotimes_{i=1}^{n} A_i = A_1 \times A_2 \times \ldots \times A_n := \{\, (a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\, i = 1, \ldots, n \,\}$$

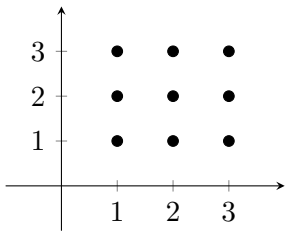
Beispiel 0.5.

(i) $A_1 = \{\, 1, 3, 5, 7 \,\}$, $A_2 = \{\, 2, 3, 5 \,\}$, $A_3 = \{\, 0 \,\}$.

$$\bigotimes_{i=1}^{2} A_i = A_1 \times A_2 = \left\{ \begin{array}{lll} (1,2) & (1,3) & (1,5) \\ (3,2) & (3,3) & (3,5) \\ (5,2) & (5,3) & (5,5) \\ (7,2) & (7,3) & (7,5) \end{array} \right\}$$

$$\begin{aligned} |A_1 \times A_2| &= |A_1| \cdot |A_2| = 12 \\ A_2 \times A_1 &= \{\, (2,1), \ldots \,\} \neq A_1 \times A_2 \quad \text{(Tupel sind geordnet!)} \\ A_1 \times A_2 \times A_3 &= \{\, (1,2,0), (1,3,0), (1,5,0), (3,2,0), \ldots \,\} \end{aligned}$$

(ii) $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$



0.2 Aussagenlogik

(Logische) Aussage.
„Satz“, dem ein sog. *Wahrheitswert* zugeordnet werden kann: wahr (w) oder falsch (f), engl. True (T) oder False (F). $\longrightarrow$ *Boolesche Variablen*: 1 oder 0.

Junktoren.
…verknüpfen Aussagen miteinander wie bspw. *und*, *oder*, *entweder-oder*.

Aussagenlogische Formeln.
…bestehen aus

- Variablen ($A, B, C, \ldots$ oder $p, q, r, \ldots$) für Aussagen (können also Wahrheitswerte annehmen)
- logischen Operatoren (Junktoren):

$\wedge$: (logisches) und
$\vee$: (logisches) oder
$\oplus$: ausschließendes oder, XOR
$\neg$: (logische) Negation
$\longrightarrow, \implies$: Subjunktion : $A \implies B$ („aus A folgt B“ oder „A impliziert B“)
$\longleftrightarrow, \iff$: Bijunktion : $A \iff B$ („A ist äquivalent zu B“)

Strukturierung durch runde Klammern!

0.3 Rechenregeln in der Aussagenlogik

Idempotenz.

$$p \vee p \iff p, \quad p \wedge p \iff p$$

Doppelnegation.

$$\neg(\neg p) \iff p$$

Tautologie.

$$p \vee \neg p \iff 1, \quad p \wedge \neg p \iff 0$$

Unerfüllbarkeit.

$$0 \wedge p \iff 0, \quad 1 \vee p \iff 1$$

Absorption.

$$p \vee (p \wedge q) \iff p, \quad p \wedge (p \vee q) \iff p$$

Kommutativität.

$$p \vee q \iff q \vee p, \quad p \wedge q \iff q \wedge p$$

Assoziativität.

$$(p \vee q) \vee r \iff p \vee (q \vee r), \quad (p \wedge q) \wedge r \iff p \wedge (q \wedge r)$$

Distributivität.

$$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r), \quad p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$$

De Morgan.

$$\neg(p \vee q) \iff \neg p \wedge \neg q, \quad \neg(p \wedge q) \iff \neg p \vee \neg q$$

Implikation.

$$(p \Longrightarrow q) \iff \neg p \vee q$$

Bikonditional.

$$p \iff q \iff (p \Longrightarrow q) \wedge (q \Longrightarrow p)$$

Vorsicht!

$$(A \Longrightarrow B) \not\Longrightarrow (B \Longrightarrow A)$$

Es gilt jedoch:

$$(A \Longrightarrow B) \Longrightarrow (\neg B \Longrightarrow \neg A)$$

Sprechweise: B ist *notwendig*, aber nicht *hinreichend* für A.
A ist *hinreichend* für B.

Beispiel 0.6.

(i)

A	B	$A \Longrightarrow B$	$\neg A$	$\neg A \vee B$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

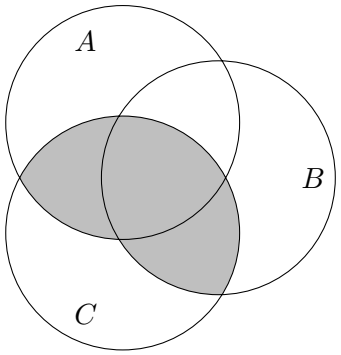
(ii)

A	B	$A \Longrightarrow B$	$B \Longrightarrow A$	$A \Longleftrightarrow B$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

(iii) „Äquivalenzumformungen“:

$$\begin{aligned}
& A \wedge \neg(B \Longrightarrow C) \\
\equiv\ & A \wedge \neg(B \Longrightarrow C) \wedge (C \Longrightarrow B) \\
\equiv\ & A \wedge \neg(\neg B \vee C) \wedge (\neg C \vee B) \\
\equiv\ & A \wedge (\neg(\neg B \vee C) \vee \neg(\neg C \vee B)) \\
\equiv\ & A \wedge ((B \wedge \neg C) \vee (C \wedge \neg B))
\end{aligned}$$

Beispiel 0.7 (Mengengleichheitsbeweis)**.** A, B, C Mengen.



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

Beweis. Für Mengen A_1, A_2 gilt:

$$\begin{aligned}
A_1 = A_2 &\iff A_1 \subseteq A_2 \wedge A_2 \subseteq A_1 \\
&\iff A_1 \subseteq A_2 \wedge A_1 \supseteq A_2
\end{aligned}$$

$\rightsquigarrow$ zwei „Teilmengenbeweise“.

"$\subseteq$" : Sei $x \in (A \cup B) \cap C$ beliebig. Zeige $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

$$
\begin{aligned}
&\implies && x \in (A \cup B) && \wedge x \in C \\
&\implies && (x \in A \vee x \in B) && \wedge x \in C \\
&\overset{\text{Distr.}}{\implies} && (x \in A \wedge x \in C) && \vee (x \in B \wedge x \in C) \\
&\implies && x \in (A \cap C) && \vee x \in (B \cap C) \\
&\implies && x \in (A \cap C) && \cup (B \cap C)
\end{aligned}
$$

Zur besseren Übersicht der Umformungen dient folgende Darstellung des Beweises:

$$
\begin{aligned}
&\implies && x \in (&& A \cup && B) \wedge && && x \in C \\
&\implies && && (x \in A \vee x \in B) \wedge && && x \in C \\
&\overset{\text{Distr.}}{\implies} && && (x \in A \wedge x \in C) \vee && (x \in B \wedge x \in C) \\
&\implies && x \in (&& A \cap && C) \vee x \in (&& B \cap && C) \\
&\implies && x \in (&& A \cap && C) \cup (&& B \cap && C)
\end{aligned}
$$

"$\supseteq$" : Sei $x \in (A \cap C) \cup (B \cap C)$ beliebig. Zeige $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$.

$$
\begin{aligned}
&\implies && x \in (A \cap C) && \vee x \in (B \cap C) \\
&\implies && (x \in A \wedge x \in C) && \vee (x \in B \wedge x \in C) \\
&\overset{\text{Distr.}}{\implies} && (x \in A \vee x \in B) && \wedge x \in C \\
&\implies && x \in (A \cup B) && \wedge x \in C \\
&\implies && x \in (A \cup B) && \cap C
\end{aligned}
$$

Zur besseren Übersicht der Umformungen dient folgende Darstellung des Beweises:

$$
\begin{aligned}
&\implies && x \in (&& A \cap && C) \vee x \in (&& B \cap && C) \\
&\implies && && (x \in A \wedge x \in C) \vee && (x \in B \wedge x \in C) \\
&\overset{\text{Distr.}}{\implies} && && (x \in A \vee x \in B) \wedge && && x \in C \\
&\implies && x \in (&& A \cup && B) \wedge && && x \in C \\
&\implies && x \in (&& A \cup && B) \cap && && C
\end{aligned}
$$

□

Man hätte auch direkt die Äquivalenz beweisen können!

0.4 Quantoren

$\forall\, x \in M : P(x)$ – „Für alle x aus der Menge M gilt die Aussage $P(x)$."

$\exists\, x \in M : P(x)$ – „Es existiert ein x aus M, so dass $P(x)$ für dieses x gilt."

$\exists! x \in M : P(x)$ – „Es existiert genau ein x aus M, so dass $P(x)$ für dieses x gilt."

Verneinung/Negation.
Umkehrung sämtlicher Quantoren, Negation der Aussage.

Anwendung.
…bei beschreibender Darstellung von Mengen, z.B.

$$Q := \{n \in \mathbb{N}_0 \mid \exists m \in \mathbb{N}_0,\, m^2 = n\} \quad \text{(Menge der Quadratzahlen)}$$

0.5 Abbildungen / Funktionen

Definition 0.10. Eine *Abbildung* oder *Funktion* $f : A \to B$ ist eine Teilmenge von $A \times B$ mit der zusätzlichen Eigenschaft:

$$\forall x \in A : \exists! y \in B : (x, y) \in f \subseteq A \times B$$

Man schreibt statt $(x, y) \in f$ auch $x \mapsto y$ oder $y = f(x)$.
A heißt *Definitionsbereich* von f.

Definition 0.11 (Hintereinanderschaltung/Komposition)**.**
Seien $f : A \to B$ und $g : B \to C$ zwei Funktionen. Dann ist die *Hintereinanderschaltung* oder *Komposition* $h := g \circ f : A \to C$ definiert durch $h(x) := g(f(x))$.

0.6 Beweisprinzip der vollständigen Induktion

Sei $A(n)$ eine Aussage für ein $n \in \mathbb{N}$. Falls

- $A(1)$, sog. *Induktionsanfang (IA)*, und
- für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$,

dann gilt $A(n)$ für alle $n \in \mathbb{N}$.

Beispiel 0.8 („Der kleine Gauß“)**.** Addiere alle Zahlen von 1 bis 100.
Lösung von Gauß:

$$\begin{array}{rccccc} & 1 & 2 & \dots & 99 & 100 \\ + & 100 & 99 & \dots & 2 & 1 \\ \hline & 101 & 101 & \dots & 101 & 101 \end{array} \quad \Longrightarrow \quad \sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = \frac{10100}{2} = 5050$$

Allgemein:

$$\forall n \in \mathbb{N} : \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Beweis durch vollständige Induktion.
IA. $n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1 \cdot 2}{2} = 1 \quad \checkmark$$

Induktionsvoraussetzung (IV). Die Behauptung sei für bel. $n \in \mathbb{N}$ erfüllt.
Induktionsschritt (IS). $n \mapsto n+1$: Zeige, dass sie dann auch für $n+1$ erfüllt ist, dass also gilt:

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

Es gilt:

$$\begin{aligned} & \sum_{i=1}^{n+1} i \\ = \quad & \sum_{i=1}^{n} i + (n+1) \\ \overset{\text{IV}}{=} \quad & \frac{n(n+1)}{2} + (n+1) \\ = \quad & \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ = \quad & \frac{(n+1)(n+2)}{2} \end{aligned}$$

□

Beispiel 0.9.

$$\forall n \in \mathbb{N} : \prod_{l=0}^{n} l^l \leq n^{\frac{n(n+1)}{2}}$$

Beweis durch vollständige Induktion.
IA. $n = 1$:

$$\prod_{l=0}^{1} l^l = 0^0 \cdot 1^1 = 1 \leq 1 = 1^2 = 1^{\frac{1\cdot(1+1)}{2}} \quad \checkmark$$

IV.

$\prod_{l=0}^{n} l^l \leq n^{\frac{n(n+1)}{2}}$ gelte für bel. $n \in \mathbb{N}$.

IS. $n \mapsto n+1$: Zeige, dass sie dann auch für $n+1$ gilt, also:

$$\prod_{l=0}^{n+1} l^l \leq (n+1)^{\frac{(n+1)(n+2)}{2}}$$

Es gilt:

$$\begin{aligned}
& \prod_{l=0}^{n+1} l^l \\
= & \prod_{l=0}^{n} l^l \cdot (n+1)^{n+1} \\
\overset{\text{IV}}{\leq} & n^{\frac{n(n+1)}{2}} \cdot (n+1)^{n+1} \\
\leq & (n+1)^{\frac{n(n+1)}{2}} \cdot (n+1)^{n+1} \\
= & (n+1)^{\frac{n(n+1)}{2}+n+1} \\
= & (n+1)^{\frac{n(n+1)}{2}+\frac{2(n+1)}{2}} \\
= & (n+1)^{\frac{n(n+1)+2(n+1)}{2}} \\
= & (n+1)^{\frac{(n+1)(n+2)}{2}}
\end{aligned}$$

□

0.7 Algebraische Strukturen

Eine *algebraische Struktur* $\mathcal{A} = (M, *)$ besteht aus einer *Trägermenge* M und einer *Verknüpfung* $* : M \to M \to M$. Grundsätzlich muss $\mathcal{A} = (M, *)$ *algebraisch abgeschlossen* sein, d.h. $\forall a, b \in M : a * b \in M$. Dann ist die Verknüpfung $*$ *wohldefiniert* (auch: *total definiert*).

Definition 0.12. Sei $\mathcal{A} = (M, *)$ algebraisch abgeschlossen.

(i) $\mathcal{A}$ heißt *assoziativ bzgl.* $*$, falls

$$\forall a, b, c \in \mathcal{A} : (a * b) * c = a * (b * c)$$

(ii) $e \in \mathcal{A}$ heißt *Einselement* oder *neutrales Element* von A, wenn

$$\forall a \in \mathcal{A} : a * e = e * a = a$$

(iii) Hat $\mathcal{A}$ ein Einselement e und falls

$$\forall a \in \mathcal{A} : \exists b \in \mathcal{A} : a * b = b * a = e$$

dann heißt b *inverses Element* oder *Inverses* zu a. Bezeichnung: a^{-1}. Falls $a^{-1} = a$, dann heißt a *selbstinvers* oder *involutiv*.

(iv) $\mathcal{A}$ heißt *kommutativ bzgl.* $*$, wenn

$$\forall a, b \in \mathcal{A} : a * b = b * a$$

Definition 0.13 (Gruppe)**.** Eine algebraische Struktur $\mathcal{G} = (M, *)$ heißt *Gruppe*, falls $\mathcal{G}$ assoziativ bzgl. $*$ ist, ein Einselement besitzt und es zu jedem Element ein Inverses gibt. Falls $\mathcal{G}$ zusätzlich kommutativ bzgl. $*$ ist, so spricht man von einer *kommutativen* oder *abelschen Gruppe*.

Eigenschaften von Gruppen.
In einer Gruppe $\mathcal{G} = (M, *)$ gilt:

- Das Einselement ist eindeutig.
- Jedes inverse Element ist eindeutig.
- Für $a, b \in \mathcal{G}$ gilt: $(a * b)^{-1} = b^{-1} * a^{-1}$.
- $\forall a, b, c \in \mathcal{G} : a * c = b * c \implies a = b$ (sog. *Kürzungsregel*).
- Gleichungen sind eindeutig lösbar:

  $$\forall a, b \in \mathcal{G} : \exists! x, y \in \mathcal{G} : a * x = b \wedge y * a = b$$

  (Lösungen: $x = a^{-1} * b,\ y = b * a^{-1}$).

Ab jetzt zwei Verknüpfungen/Operationen $+$, $\cdot$ mit 0 Einselement bzgl. $+$ und 1 Einselement bzgl. $\cdot$.

Definition 0.14 (Ring)**.** Eine algebraische Struktur $\mathcal{R} = (M, +, \cdot)$ heißt *Ring*, falls

1. $(M, +)$ eine abelsche Gruppe ist,
2. $\mathcal{R}$ bzgl. $\cdot$ assoziativ ist,
3. ein Einselement bzgl. $\cdot$ existiert und
4. das *Distributivgesetz* für $+$ und $\cdot$ erfüllt ist:

$$\forall a, b, c \in \mathcal{R}: \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad \wedge \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

Falls $\mathcal{R}$ bzgl. $\cdot$ zusätzlich kommutativ ist, so spricht man von einem *kommutativen Ring*.

Definition 0.15 (Körper)**.** Eine algebraische Struktur $\mathcal{K} = (M, +, \cdot)$ heißt *Körper*, falls:

1. $(\mathcal{K}, +, \cdot)$ ein kommutativer Ring ist und
2. jedes $x \in \mathcal{K} \setminus \{0\}$ ein multiplikatives Inverses hat.

Satz 0.3. *Sei $\mathcal{K}$ ein Körper und $a, b, c, d \in \mathcal{K}$. Dann gilt:*

(i) $a \cdot 0 = 0$

(ii) $ab = 0 \implies a = 0 \ \vee \ b = 0$

(iii) $ab + (-a)b = 0$

(iv) $(-a)b = -(ab)$

(v) $(-a)(-b) = ab$

(vi) $a^{-1}b^{-1} = (ab)^{-1}$

(vii) $(ab^{-1}) \cdot (cd^{-1}) = (ac) \cdot (b^{-1}d^{-1})$

(viii) $ab^{-1} + cd^{-1} = (ad + bc)\,(bd)^{-1}$

(ix) $\forall n \in \mathbb{Z}: a^n \cdot b^n = (ab)^m$

(x) $\forall n, m \in \mathbb{Z}: a^m \cdot a^n = a^{m+n}$

(xi) $\forall n, m \in \mathbb{Z}: (a^m)^n = a^{mn}$

(xii) $(a + b)(a - b) = a^2 - b^2$

(xiii) Die Gleichung $a + x = b$ ist eindeutig lösbar.

(xiv) Die Gleichung $ax + b = c$ ist mit $a \neq 0$ eindeutig lösbar.

(xv) (i), (iii)-(v), (ix)-(xiii) gelten auch in $\mathbb{Z}$.

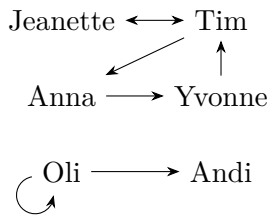
1 Relationen

1.1 Relationen und Funktionen

Beispiel 1.1. $U :=$ {Andi, Anna, Jeanette, Tim, Oli, Yvonne}
Relation.

$$R := \{\, (a, b) \in U^2 \mid a \text{ ist in } b \text{ verliebt} \,\} \subseteq U^2$$

Graphische Darstellung.



Tabellarische Darstellung.

♥	Andi	Anna	Jeanette	Tim	Oli	Yvonne
Andi	0	0	0	0	0	0
Anna	0	0	0	0	0	1
Jeanette	0	0	0	1	0	0
Tim	0	1	1	0	0	0
Oli	1	0	0	0	1	0
Yvonne	0	0	0	1	0	0

Es gilt (Jeanette, Tim) $\in R$, jedoch (Anna, Oli) $\notin R$.

Definition 1.1 (Binäre Relation)**.** Eine *binäre Relation* $R : X \to Y$ ist eine Teilmenge des Kreuzprodukts

$$R \subseteq X \times Y$$

X heißt auch *Domäne* von R. ($\mathrm{dom}(R) = X$)
Y heißt auch *Kodomäne* von R. ($\mathrm{cod}(R) = Y$)
Eine binäre Relation mit $\mathrm{dom}(R) = \mathrm{cod}(R)$ heißt *homogen* oder *Endorelation*.
Schreibweise: $(x, y) \in R$ oder xRy ($x \in X$, $y \in Y$).

Allgemeiner Relationsbegriff.
Sei $(U_i)_{i\in\mathbb{N}}$ eine Familie von Mengen. Eine *Relation* R ist eine Teilmenge des Kreuzprodukts

$$R \subseteq \bigotimes_{i\in\mathbb{N}} U_i$$

Gilt $\forall i,j : U_i = U_j$, so heißt die Relation *homogen*. Eine *n-äre Relation* ist Teilmenge des Kreuzprodukts

$$R \subseteq U_1 \times U_2 \times \ldots \times U_n$$

bei endlich vielen U_i.

Bezeichnungen.
$n = 2 \rightarrow$ binäre Relation
$n = 3 \rightarrow$ ternäre Relation
$n = 4 \rightarrow$ quaternäre Relation
$\ldots$

Universelle/All-Relation.

$$\prod = \bigotimes_{i=1}^{n} U_i$$

Leere Relation.

$$\coprod = \emptyset$$

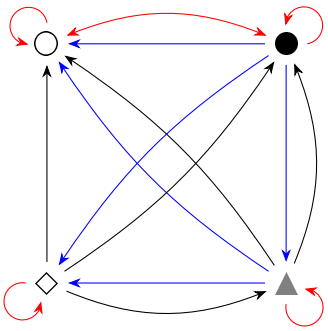
Was oftmals verdrängt wird: **Relationen sind Mengen!!!**
Alle Mengenoperationen $(\subseteq, \cup, \cap, \setminus, \times, \ldots)$ können auch auf Relationen ausgeführt werden.

Beispiel 1.2.

(i) $R := \left\{ (x,y) \in \mathbb{N}_0^2 \mid x+2 = y \right\} \subseteq \mathbb{N}_0^2$.
Es gilt:

$$xRy \iff x+2 = y$$
$$R = \{ (0,2), (1,3), (2,4), \ldots \}$$

(ii) $U = \{ \bigcirc, \bullet, \diamond, \blacktriangle \}$.



„hat mehr Ecken als“

„ist dunkler als“ $= \left\{ \begin{array}{l} (\bullet, \bigcirc)\ (\blacktriangle, \bigcirc) \\ (\bullet, \diamond)\ (\blacktriangle, \diamond) \\ (\bullet, \blacktriangle) \end{array} \right\}$

„hat genauso viele Ecken wie“	$\bigcirc$	$\bullet$	$\diamond$	$\blacktriangle$
$\bigcirc$	1	1	0	0
$\bullet$	1	1	0	0
$\diamond$	0	0	1	0
$\blacktriangle$	0	0	0	1

(iii) $\leq : \mathbb{N}_0 \to \mathbb{N}_0$.

$$\begin{aligned} 3 \leq 7 &\iff (3,7) \in \leq \subseteq \mathbb{N}_0^2 \\ &\quad\ (4,8) \in \leq \\ 6 \not\leq 3 &\iff (6,3) \notin \leq \\ &\iff (6,3) \in \overline{\leq} = > \\ &\iff 6 > 3 \end{aligned}$$

allgemein: $x \overline{R} y \iff \neg\, xRy$

Definition 1.2 (Bild und Urbild von Relationen)**.** Sei $R : X \to Y$ eine binäre Relation, $U \subseteq X$, $V \subseteq Y$.

(i) $R(U) := \{ y \in Y \mid \exists x \in U : xRy \}$ heißt *Bild von* U.

(ii) $R^{-1}(V) := \{ x \in X \mid \exists y \in V : xRy \}$ heißt *Urbild von* V.

(iii) $R(X)$ heißt *Bild von* R.

(iv) $R^{-1}(Y)$ heißt *Urbild von* R.

Beispiel 1.3 ($\to$ Beispiel 1.1)**.**

- $\mathrm{dom}(R) = \mathrm{cod}(R) \implies R$ homogen/Endorelation
- $R(U) = U$
- $R^{-1}(U) = U \setminus \{ \text{Andi} \}$
- $R(\{ \text{Oli} \}) = \{ \text{Oli, Andi} \}$

- $R(\{\text{ Jeanette, Yvonne }\}) = \{\text{ Tim }\}$
- $R^{-1}(\{\text{ Tim }\}) = \{\text{ Jeanette, Yvonne }\}$
- $R^{-1}(\{\text{ Anna, Yvonne }\}) = \{\text{ Tim, Anna }\}$

Beispiel 1.4. Die Addition (Plus: $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$) ist auch eine Relation:

$$\begin{aligned} \text{Plus} &\subseteq \mathbb{N}_0^3 \\ \text{Plus} &= \left\{ (x,y,z) \in \mathbb{N}_0^3 \mid x+y=z \right\} \\ (x,y)\ \text{Plus}\ z &\iff x+y=z \\ \text{Plus} &= \{ (0,0,0),(0,1,1),(1,0,1),(2,0,2),\dots \} \end{aligned}$$

Beispiel 1.5. Sei $\mathcal{U}$ ein beliebiges Universum. $\subseteq\colon \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$ ist eine Relation:

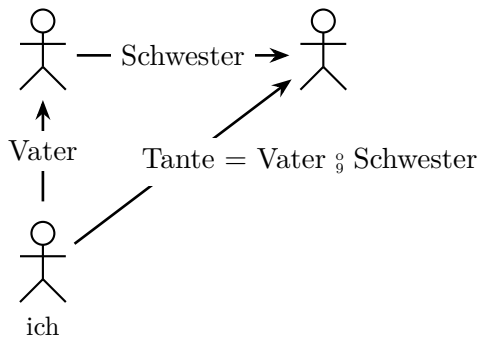
$$U \subseteq V \iff \forall x \in U : x \in U \implies x \in V$$
$$U = \mathbb{R} \implies (\mathbb{N}, \mathbb{N}_0), (\mathbb{Q}, \mathbb{R}) \in \subseteq$$

Definition 1.3 (Komposition)**.** Seien $R : X \to Y$ und $S : Y \to Z$ zwei Relationen. Die *Komposition* $P = R \fatsemi S : X \to Z$ ist definiert durch

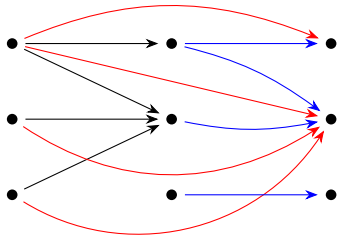
$$P := \{ (x,z) \in X \times Z \mid \exists y \in Y : xRy \wedge ySz \}$$

Beispiel 1.6.

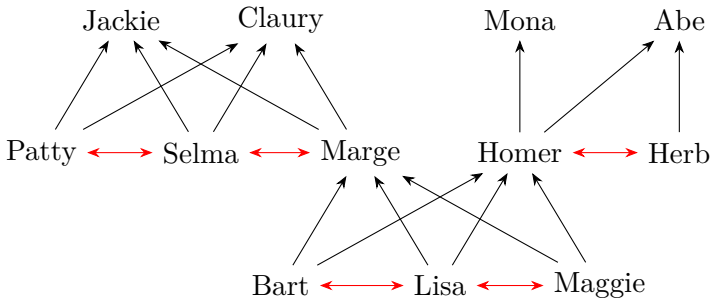
(i)



(ii) $U \xrightarrow{P} V \xrightarrow{Q} W$, $P \fatsemi Q$



(iii)



$xKy \iff x$ ist Kind von y

$xSy \iff x$ ist Geschwister von y
$S = \{ (x,y) \mid \exists z : xKz \wedge yKz \}$

$xEy \iff x$ ist Enkel von y
$E = \{ (x,y) \mid \exists z : xKz \wedge zKy \} = K \fatsemi K$

$xNy \iff x$ ist Nichte/Neffe von y
$N = \{ (x,z) \mid \exists y : xKy \wedge ySz \} = K \fatsemi S$

Satz 1.1.

(i) Die Komposition von Relationen ist assoziativ, d.h. für drei Relationen R, S, T (mit passenden Domänen/Kodomänen) gilt:

$$(R \fatsemi S) \fatsemi T = R \fatsemi (S \fatsemi T)$$

(ii) …aber i.a. nicht kommutativ, d.h. (selbst wenn $X = Y = Z$) kann gelten

$$R \fatsemi S \neq S \fatsemi R$$

Beweis.

(i) Es gelte $U \xrightarrow{R} V \xrightarrow{S} W \xrightarrow{T} X$. Sei $(u, x) \in (R \fatsemi S) \fatsemi T \subseteq U \times X$ beliebig.

$$\begin{aligned}
&\Longrightarrow && \exists y \in W : u(R \fatsemi S)y \wedge yTx \\
&\Longrightarrow && \exists y \in W : \exists v \in V : uRv \wedge vSy \wedge yTx \\
&\Longrightarrow && \exists v \in V : uRv \wedge \exists y \in W : vSy \wedge yTx \\
&\Longrightarrow && \exists v \in V : uRv \wedge v(S \fatsemi T)x \\
&\Longrightarrow && u(R \fatsemi (S \fatsemi T))x \\
&\Longrightarrow && (u, x) \in R \fatsemi (S \fatsemi T)
\end{aligned}$$

Zur besseren Übersicht der Umformungen dient folgende Darstellung des Beweises:

$$\begin{aligned}
&\Longrightarrow && \exists y \in W : && u(R \fatsemi && S)y \wedge yT && x \\
&\Longrightarrow && \exists y \in W : \exists v \in V : && u\ Rv \wedge && v\ S\ y \wedge yT && x \\
&\Longrightarrow && \exists v \in V : && u\ Rv \wedge \exists y \in W : && v\ S\ y \wedge yT && x \\
&\Longrightarrow && \exists v \in V : && u\ Rv \wedge && v(S \fatsemi T) && x \\
&\Longrightarrow && && u(R \fatsemi && (S \fatsemi T))x \\
&\Longrightarrow && (u, x) \in R \fatsemi (S \fatsemi T)
\end{aligned}$$

(ii) Gegenbeispiel: Nichte/Neffe ist Kind eines eigenen Geschwisters, aber nicht Geschwister der eigenen Kinder.

□

Definition 1.4 (Identitätsrelation)**.** Seien $x, y \in \mathcal{U}$. Die Relation

$$1 := \{ (x, y) \mid x = y \}$$

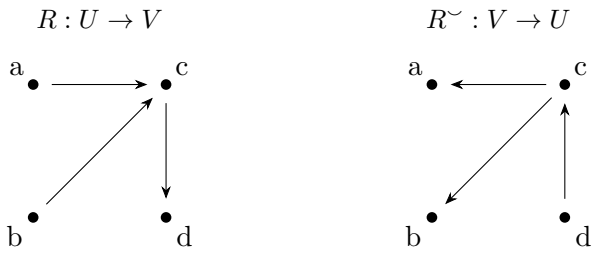
heißt *Identitätsrelation.* $(x1y \iff x = y)$

Definition 1.5 (Konverse Relation)**.** Für eine Relation $R : U \to V$ heißt $R^\smile : V \to U$ mit

$$xR^\smile y :\Longleftrightarrow yRx \quad (x \in U,\, y \in V)$$

konverse Relation oder *Konverse von R.*

$$R^\smile = \{ (x, y) \mid (y, x) \in R \}$$



Definition 1.6 (Relationenoperationen)**.** Seien P, Q, R Relationen auf $\mathcal{U}$. Dann sind definiert:

(i) $x(P \cup Q)y \iff (x,y) \in P \cup Q \iff xPy \vee xQy$

(ii) $x(P \cap Q)y \iff (x,y) \in P \cap Q \iff xPy \wedge xQy$

(iii) $x\overline{R}y \iff \neg xRy$

Satz 1.2 (Rechenregeln für Relationsoperationen)**.** *Seien P, Q, R Relationen auf $\mathcal{U}$. Dann gilt:*

(i) $1 \fatsemi R = R = R \fatsemi 1$ *(Neutralität von 1)*

(ii) $\coprod \fatsemi R = \coprod = R \fatsemi \coprod$ *(Annihilation durch $\coprod$)*

(iii) $R^{\smile\smile} = R$ *(Konverse ist involutorisch)*

(iv) $\overline{R^\smile} = \overline{R}^\smile$

(v) $(P \fatsemi Q)^\smile = Q^\smile \fatsemi P^\smile$ *(Antidistributivität)*

(vi) $P \fatsemi (Q \cap R) = (P \fatsemi Q) \cup (P \fatsemi R)$ *(Distributivität von $\fatsemi$ über $\cup$)*

(vii) $P \fatsemi (Q \cap R) \subsetneq (P \fatsemi Q) \cap (P \fatsemi R)$ *(Subdistributivität von $\fatsemi$ über $\cap$)*

(viii) $P \subseteq Q \implies P \fatsemi R \subseteq Q \fatsemi R \quad \wedge \quad R \fatsemi P \subseteq R \fatsemi Q$ *(Isotonie)*

(ix) $(P \cap Q)^\smile = P^\smile \cap Q^\smile$
$(P \cup Q)^\smile = P^\smile \cup Q^\smile$

Beweis. Seien $x, y \in \mathcal{U}$. Dann gilt:

(i)

$$\begin{aligned} & x(1 \fatsemi R)y \\ \iff\ & \exists z \in U : x\ 1\ z \wedge zR\ y \\ \implies\ & x = z \wedge xR\ y \\ \implies\ & xR\ y \end{aligned} \qquad \begin{aligned} & xR\ y \\ \implies\ & x\ 1x \wedge xR\ y \\ \overset{z=x}{\implies}\ & \exists z \in U : x\ 1z \wedge zR\ y \\ \implies\ & x(1 \fatsemi R)y \end{aligned}$$

$R = R \fatsemi 1$ analog.

(ii)
$$
\begin{aligned}
& x(\coprod \ {}^{\circ}_{9} \ R)y \\
\Longrightarrow \quad & \exists z \in U : x \ \coprod z \wedge zR \ y \\
\Longrightarrow \quad & \coprod \ {}^{\circ}_{9} \ R \ = \coprod
\end{aligned}
$$

$\coprod = R \, {}^{\circ}_{9} \coprod$ analog.

(iii)
$$
\begin{aligned}
& x \ R^{\smile\smile} \ y \\
\Longleftrightarrow \quad & x(R^{\smile})^{\smile} y \\
\Longleftrightarrow \quad & y \ R^{\smile} \ x \\
\Longleftrightarrow \quad & x \ R \ y
\end{aligned}
$$

(iv)
$$
\begin{aligned}
& x\overline{R^{\smile}}y \\
\Longleftrightarrow \quad & \neg x R^{\smile} y \\
\Longleftrightarrow \quad & \neg y R \ x \\
\Longleftrightarrow \quad & y\overline{R} \ x \\
\Longleftrightarrow \quad & x\overline{R}^{\smile} y
\end{aligned}
$$

(v)
$$
\begin{aligned}
& x(P \ {}^{\circ}_{9} \ Q \ )^{\smile} y \\
\Longleftrightarrow \quad & y(P \ {}^{\circ}_{9} \ Q \ ) \ x \\
\Longleftrightarrow \quad & \exists z \in U : y \ P \ z \wedge zQ \ x \\
\Longleftrightarrow \quad & \exists z \in U : z \ P^{\smile} y \wedge xQ^{\smile} \ z \\
\Longleftrightarrow \quad & \exists z \in U : x \ Q^{\smile} z \wedge zP^{\smile} \ y \\
\Longleftrightarrow \quad & x(Q^{\smile} \ {}^{\circ}_{9} \ P^{\smile}) \ y
\end{aligned}
$$

(vi)
$$
\begin{aligned}
& x(P \, {}^{\circ}_{9} \, (Q \cup R))y \\
\Longleftrightarrow \quad & \exists z \in U : xPz \wedge z(Q \cup R)y \\
\Longleftrightarrow \quad & \exists z \in U : xPz \wedge (zQy \vee zRy) \\
\overset{\text{Distr.}}{\Longleftrightarrow} \quad & \exists z \in U : (xPz \wedge zQy) \vee (xPz \wedge zRy) \\
\Longleftrightarrow \quad & x((P \, {}^{\circ}_{9} \, Q) \cup (P \, {}^{\circ}_{9} \, R))y
\end{aligned}
$$

Zur besseren Übersicht der Umformungen dient folgende Darstellung des Beweises:

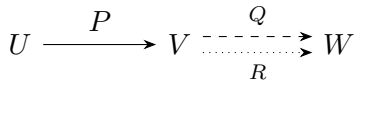
$$
\begin{aligned}
& x(\ P \ {}^{\circ}_{9} \ \ (Q \ \ \cup \ \ R))y \\
\Longleftrightarrow \quad & \exists z \in U : \ x \ \ Pz \wedge \ z(Q \ \ \cup \ \ R) \ y \\
\Longleftrightarrow \quad & \exists z \in U : \ x \ \ Pz \wedge (z \ Q \ y \ \vee \ \ zR \ \ y) \\
\overset{\text{Distr.}}{\Longleftrightarrow} \quad & \exists z \in U : (x \ \ Pz \wedge \ z \ Q \ y) \vee (xPz \wedge zR \ \ y) \\
\Longleftrightarrow \quad & x((P \ {}^{\circ}_{9} \ \ Q) \ \ \cup (\ P \ {}^{\circ}_{9} \ \ R))y
\end{aligned}
$$

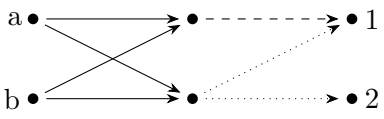
(vii)
$$
\begin{aligned}
& x(P \,⨾\, (Q \cap R))y \\
\iff\ & \exists z \in U : xPz \wedge z(Q \cap R)y \\
\iff\ & \exists z \in U : xPz \wedge (zQy \wedge zRy) \\
\iff\ & \exists z \in U : (xPz \wedge (zQy \wedge zRy) \\
\implies\ & \exists z \in U : (xPz \wedge zQy) \wedge \exists z \in U : (xPz \wedge zRy) \\
\iff\ & x((P \,⨾\, Q) \cap (P \,⨾\, R))y
\end{aligned}
$$

Zur besseren Übersicht der Umformungen dient folgende Darstellung des Beweises:

$$
\begin{aligned}
& x\ (P\ \ ⨾\ \ (Q\ \ \cap\ \ R\ ))y \\
\iff\ & \exists z \in U :\ x\ \ Pz \wedge\ z(Q\ \ \cap\ \ R\ )\ y \\
\iff\ & \exists z \in U :\ x\ \ Pz \wedge (z\ Qy\ \ \wedge\ \ zRy) \\
\iff\ & \exists z \in U : (x\ \ Pz \wedge (z\ Qy\ \ \wedge\ \ zRy) \\
\implies\ & \exists z \in U : (x\ \ Pz \wedge\ z\ Qy) \wedge \exists z \in U : (xPz \wedge zRy) \\
\iff\ & x((P\ \ ⨾\ \ Q\ \ ) \cap (\ P\ \ ⨾\ \ R\ ))y
\end{aligned}
$$

Für die folgenden Relationen gilt tatsächlich $P \,⨾\, (Q \cap R) \subsetneq (P \,⨾\, Q) \cap (P \,⨾\, R)$:
Seien $U, V, W \subseteq \mathcal{U}$:





$$
Q \cap R = \coprod \overset{\text{(ii)}}{\implies} P \,⨾\, (Q \cap R) = \coprod
$$

$$
\begin{aligned}
\textbf{aber: } P \,⨾\, Q &= \{(a,1), \quad (b,1) \quad\} \\
P \,⨾\, R &= \{(a,1),(a,2),(b,1),(b,2)\} \\
\implies \quad \coprod &\subsetneq \{(a,1), \quad (b,1) \quad\} \\
&= (P \,⨾\, Q) \cap (P \,⨾\, R)
\end{aligned}
$$

(viii) Unter der Voraussetzung $P \subseteq Q \iff (xPy \implies xQy)$ gilt:

$$
\begin{aligned}
& x(P\ \ ⨾\ \ R)y \\
\implies\ & \exists z \in U : x\ \ Pz \wedge zR\ y \\
\overset{P \subseteq Q}{\implies}\ & \exists z \in U : x\ \ Qz \wedge zR\ y \\
\implies\ & x(Q\ \ ⨾\ \ R)y
\end{aligned}
$$

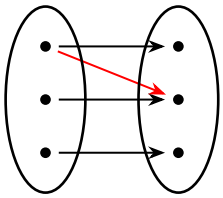
$R \,⨾\, P \subseteq R \,⨾\, Q$ analog.

(ix)

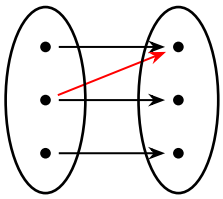
$$
\begin{array}{lll}
 & x(P \cap Q)^\smile y & \\
\iff & y(P \cap Q)\ x & \\
\iff & y\ P\ x \wedge yQ\ \ x & \\
\iff & x\ P^\smile y \wedge xQ^\smile\ \ y & \\
\iff & x(P^\smile \cap Q^\smile)\ y &
\end{array}
\qquad
\begin{array}{lll}
 & x(P \cup Q)^\smile y & \\
\iff & y(P \cup Q)\ x & \\
\iff & y\ P\ x \vee yQ\ \ x & \\
\iff & x\ P^\smile y \vee xQ^\smile\ \ y & \\
\iff & x(P^\smile \cup Q^\smile)\ y &
\end{array}
$$

□

Sei $R : A \to B$ eine Relation.

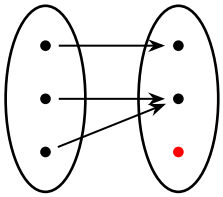


- eindeutige Zuordnung
  $\rightsquigarrow$ R ist [nicht] *funktional* (*rechtseindeutig*)
- $xRy_1 \wedge xRy_2 \implies y_1 = y_2$



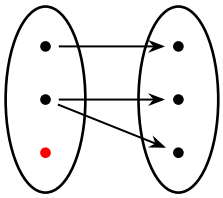
- eindeutige Zuordnung
  $\rightsquigarrow$ R ist [nicht] *injektiv* (*linkseindeutig*)
- $x_1Ry \wedge x_2Ry \implies x_1 = x_2$

$\text{Bild}(R) = \text{im}(R) = \{\, y \in B \mid \exists x \in A : xRy \,\}$



- $\text{im}(R) = B \rightsquigarrow R$ ist [nicht] *surjektiv* (*rechtstotal*)
- R ist nicht mehr injektiv!

$\text{Urbild}(R) = \text{im}(R^\smile) = \{\, x \in A \mid \exists y \in B : xRy \,\}$



- $\text{im}(R^\smile) = A \rightsquigarrow R$ ist [nicht] *linkstotal*
- R ist nicht mehr funktional!

Definition 1.7 (FLIS-Eigenschaften von Relationen)**.**
Seien A, B Mengen und $R : A \to B$ eine Relation.

(i) R heißt *funktional* oder *rechtseindeutig*, falls

$$\forall x \in A : \forall y, z \in B : (xRy \wedge xRz \implies y = z)$$

(ii) R heißt *injektiv* oder *linkseindeutig*, falls

$$\forall x_1, x_2 \in A : \forall y \in B : (x_1Ry \wedge x_2Ry \implies x_1 = x_2)$$

(iii) Das *Bild von* R ist gegeben durch

$$\mathrm{Bild}(R) = \mathrm{im}(R) := \{\, y \in B \mid \exists x \in A : xRy \,\}$$

(iv) R heißt *surjektiv* oder *rechtstotal*, falls

$$\mathrm{im}(R) = B = \mathrm{cod}(R) \iff \forall y \in B : \exists x \in A : xRy$$

(v) Das *Urbild* von R ist gegeben durch

$$\mathrm{Urbild}(R) = \mathrm{im}(R^\smile) := \{\, x \in A \mid \exists y \in B : xRy \,\}.$$

(vi) R heißt *linkstotal*, falls

$$\mathrm{im}(R^\smile) = A = \mathrm{dom}(R) \iff \forall x \in A : \exists y \in B : xRy.$$

(vii) R heißt *Funktion* (oder *Abbildung*), falls R linkstotal und funktional ist.
Schreibweise: $xRy \iff y = R(x)$.

(viii) Falls R eine Funktion ist, so heißt $\mathcal{D}(R) := \mathrm{dom}(R)$ *Definitionsmenge* von R.

(ix) Falls R eine Funktion ist, so heißt $\mathcal{W}(R) := \mathrm{im}(R)$ *Wertemenge* von R.

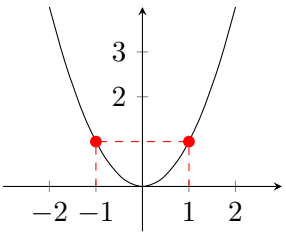
Beispiel 1.7.

(i) $f : \{$ Studierende der HBRS $\} \to \mathbb{N},\ x \in \{$ Studierende der HBRS $\},\ y \in \mathbb{N}$.

$$xfy :\iff y \text{ ist Matrikelnummer von } x$$

$$dom(f) = \{\text{Studierende der HBRS}\} \implies f \text{ linkstotal}$$
$$f \text{ funktional} \implies f \text{ Funktion}$$
$$f \text{ ist (hoffentlich) injektiv}$$
$$f \text{ ist offensichtlich nicht surjektiv}$$

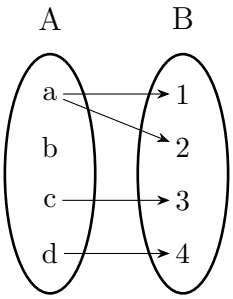
(ii) Sei $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ eine Funktion.



Definitionsmenge: $\mathcal{D}(f) = \mathbb{R}$
Wertemenge: $\mathcal{W}(f) = \mathbb{R}_{\geq 0}$

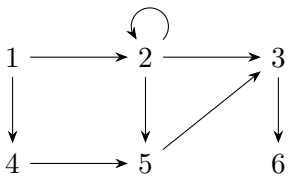
Ist f injektiv?
Nein, denn z.B. $f(-1) = f(1) = 1$.
Ist f surjektiv?
Nein, denn negative Werte werden nicht angenommen! ($\text{im}(f) = \mathbb{R}_{\geq 0}$)

(iii)



- nicht funktional
- nicht linkstotal
- injektiv
- surjektiv

(iv)



- nicht funktional
- nicht linkstotal
- nicht injektiv
- surjektiv

(v) $R \subseteq \mathbb{Z} \times \mathbb{Z}$, $(x, y) \in R \iff ax = b + 2y$ ist funktional.

- a, b gerade: linkstotal, nicht injektiv für $a = 0$, surjektiv für $a = \pm 1$ und $a = \pm 2$
- a gerade, b ungerade: $R = \coprod$
- a ungerade: nicht linkstotal, injektiv, surjektiv für $a = \pm 1$

Gegenbeispiel:

- linkstotal: x angeben, sodass

$$y = \frac{ax - b}{2} \in \mathbb{Z}$$

- surjektiv: y angeben, sodass

  $$x = \frac{b + 2y}{a} \notin \mathbb{Z}$$

1.2 Ordnungs- und Äquivalenzrelationen

Definition 1.8 (Eigenschaften von Endorelationen)**.** Sei $R : U \to U$ eine Endorelation.

(i) R heißt *reflexiv*, falls $\forall x \in U : xRx$.

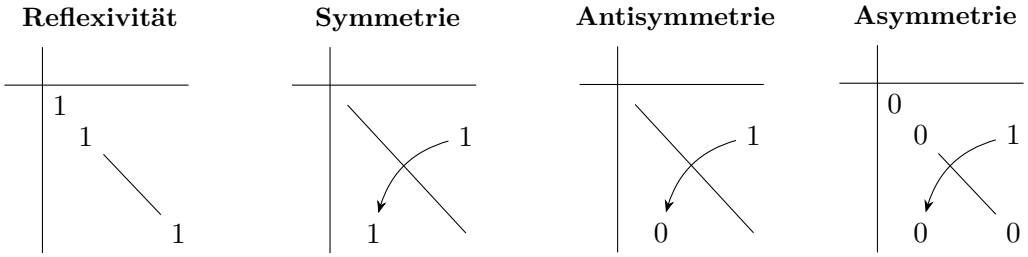
(ii) R heißt *symmetrisch*, falls $\forall x, y \in U : xRy \implies yRx$.

(iii) R heißt *asymmetrisch*, falls $\forall x, y \in U : xRy \implies \neg yRx$.

(iv) R heißt *antisymmetrisch*, falls $\forall x, y \in U : xRy \wedge yRx \implies x = y$.

(v) R heißt *transitiv*, falls $\forall x, y, z \in U : xRy \wedge yRz \implies xRz$.

Auswirkung auf tabellarische Darstellung:



(Anti-)Symmetrie erlaubt Einsen und Nullen auf der Diagonalen!

Beispiel 1.8.

(i) $R : \{ \text{Studenten} \} \to \{ \text{Studenten} \}$, $x, y \in \{ \text{Studenten} \}$.

$xRy :\iff x$ und y studieren im selben Semester

R ist reflexiv, symmetrisch, transitiv, aber weder asymmetrisch noch antisymmetrisch.

(ii) $R : \mathbb{N}_0 \to \mathbb{N}_0$, $x, y \in \mathbb{N}_0$.

$xRy :\iff x - y$ gerade

Reflexiv.

$\forall x \in \mathbb{N}_0 : x - x = 0$ gerade $\implies xRx$

Symmetrisch.

$$\begin{aligned} x, y \in \mathbb{N}_0 : xRy &\implies x - y \text{ gerade} \\ &\implies y - x = -(x - y) \text{ gerade} \\ &\implies yRx \end{aligned}$$

Nicht asymmetrisch.

$$x, y \in \mathbb{N}_0 : xRy \implies yRx$$
$$\text{also} \quad xRy \not\Longrightarrow \neg yRx$$

Nicht antisymmetrisch.

$$x, y \in \mathbb{N}_0 : 2R4 \wedge 4R2$$
$$\text{aber} \quad 2 \neq 4$$

Transitiv.

$$\begin{aligned} x, y, z \in \mathbb{N}_0 : xRy &\implies x - y \text{ gerade} \\ yRz &\implies y - z \text{ gerade} \\ &\implies x - z = \underbrace{(x-y)}_{\text{gerade}} + \underbrace{(y-z)}_{\text{gerade}} \text{ gerade} \\ &\implies xRz \text{ gerade} \end{aligned}$$

Definition 1.9 (Ordnungen)**.** Sei $R : U \to U$.

(i) R heißt *partielle Ordnung* oder *Halbordnung*, falls R reflexiv, anti-symmetrisch und transitiv ist.

(ii) R heißt *totale Ordnung*, falls R eine partielle Ordnung ist und zusätzlich gilt:

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

(iii) R heißt *streng totale Ordnung*, falls R transitiv ist und zusätzlich gilt:

$$\forall x, y \in R : xRy \vee yRx \vee x = y \quad (\textit{Trichotomie})$$

Beispiel 1.9. Seien $x, y, z \in \mathbb{R}$.

(i) Die $\leq$-Relation ist eine partielle, sogar eine totale Ordnung:
Reflexiv.

$$x \leq x$$

Antisymmetrisch.

$$x \leq y \ \wedge \ y \leq x \implies x = y$$

Transitiv.

$$x \leq y \ \wedge \ y \leq z \implies x \leq z$$

Und es gilt:

$$x \leq y \ \vee \ y \leq x \quad (\text{d.h. } x, y \text{ sind } \textit{vergleichbar}.)$$

(ii) Die $<$-Relation ist eine streng totale Ordnung:
Transitiv.

$$x < y \ \wedge \ y < z \implies x < z$$

Trichotom.

$$x < y \ \vee \ y < x \ \vee \ x = y$$

Definition 1.10 (Äquivalenzrelation)**.** Sei $R : U \to U$.
R heißt *Äquivalenzrelation*, falls R reflexiv, symmetrisch und transitiv ist.

Definition 1.11 (Äquivalenzklassen)**.** Sei $R : U \to U$ eine Äquivalenzrelation.
Die *Äquivalenzklasse* eines Elements $x \in U$ ist gegeben durch

$$[x] := \{\, y \in U \mid xRy \,\} \quad (\text{„Bild von } x \text{ unter } R\text{“})$$

Satz 1.3. *Sei I eine Indexmenge.*
Die Äquivalenzklassen A_i, $i \in I$ einer Relation $R : U \to U$ bilden (o.B.d.A.) eine Partition auf U, d.h.

(i) $\forall i \neq j : A_i \cap A_j = \emptyset$ *(A_i, A_j paarweise disjunkt)*

(ii) $\bigcup_{i \in I} A_i = U$

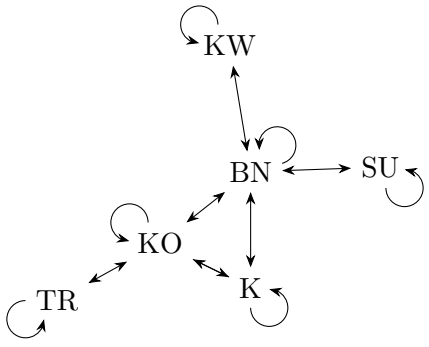
Beispiel 1.10.

(i) Die Relation aus Beispiel 1.8 (ii) ist eine Äquivalenzrelation:

$$\begin{aligned} x \text{ gerade} &\implies [x] = \mathbb{G} \quad (\text{Menge der geraden Zahlen}) \\ x \text{ ungerade} &\implies [x] = \mathbb{U} \quad (\text{Menge der ungeraden Zahlen}) \\ \mathbb{G} \cup \mathbb{U} = \emptyset \ \wedge \ \mathbb{G} \cap \mathbb{U} = \mathbb{N}_0 &\implies \mathbb{G} \text{ und } \mathbb{U} \text{ bilden eine Partition auf } \mathbb{Z}. \end{aligned}$$

(ii) $R : \{\, \text{Städte} \,\} \to \{\, \text{Städte} \,\}$, $x, y \in \{\, \text{Städte} \,\}$.

$xRy :\iff$ „Es gibt eine Autobahn von x nach y“



xRx ist erlaubt!

Definition 1.12 (Reflexiv-transitive Hülle)**.** Sei $R : U \to U$ eine Relation. Dann heißt

$$\begin{aligned} R^* &= 1 \cup R \cup R \fatsemi R \cup R \fatsemi R \fatsemi R \cup \dots \\ &= R^0 \cup R^1 \cup R^2 \cup R^3 \cup \dots \\ &= \bigcup_{i \in \mathbb{N}_0} R^i \end{aligned}$$

reflexiv-transitive Hülle von R.

Beispiel 1.11.

(i) $R^3 \subseteq R^*$.

$$\mathrm{K}R\mathrm{BN} \wedge \mathrm{BN}R\mathrm{KO} \wedge \mathrm{KO}R\mathrm{TR} \iff \mathrm{K}R^3\mathrm{TR}$$

(ii) $R^4 \subseteq R^*$.

$$\mathrm{TR}R\mathrm{TR} \wedge \mathrm{TR}R\mathrm{KO} \wedge \mathrm{KO}R\mathrm{BN} \wedge \mathrm{BN}R\mathrm{SU} \iff \mathrm{TR}R^4\mathrm{SU}$$

Mehrfache Komposition von Relationen.

$$\begin{aligned} R^0 &:= 1 \\ R^1 &:= R \\ &\vdots \\ R^{i+1} &:= R^i \fatsemi R = R \fatsemi R^i \end{aligned}$$

Satz 1.4.

$$\forall i \in \mathbb{N}_0 : (R^i)^\smile = (R^\smile)^i$$

Beweis durch vollständige Induktion.
IA. $i = 0$:

$$(R^0)^\smile = 1^\smile = 1 = (R^\smile)^0 \quad \checkmark$$

IV. Für $i \in \mathbb{N}_0$ gelte die Behauptung.
IS. $i \mapsto i + 1$:

$$\begin{aligned} & (R^\smile \ )^{i+1} \\ = {} & (R^\smile \ )^i \ \fatsemi R^\smile \\ = {} & (R^i \ )^\smile \ \fatsemi R^\smile \\ = {} & (R \ \fatsemi R^i \ )^\smile \\ = {} & (R^{i+1})^\smile \end{aligned}$$

□

1.3 Restklassen, Primzahlen und der ggT

Definition 1.13 (Teilbarkeitsrelation)**.** Die Relation $R : \mathbb{N}_0 \to \mathbb{N}_0$, gegeben durch

$$xRy :\iff x|y :\iff x \text{ ist Teiler von } y \iff \exists k \in \mathbb{N}_0 : y = k \cdot x$$

heißt *Teilbarkeitsrelation*. Ansonsten schreibt man $x \nmid y$.

Beispiel 1.12.

- $1|2$, denn $2 = 2 \cdot 1$
- $2|6$, denn $6 = 3 \cdot 2$
- $5|10$, denn $10 = 2 \cdot 5$
- $4 \nmid 5$
- $\forall n \in \mathbb{N} : 1|n$
- $0|0$ per Definition, aber …
- $\forall n \in \mathbb{N} : 0 \nmid n$

Satz 1.5. *Die Teilbarkeitsrelation ist eine partielle Ordnung.*

Beweis. Reflexiv.

$$\forall x \in \mathbb{N}_0 : x|x \quad \checkmark \quad (k = 1)$$

Antisymmetrisch. $x, y \in \mathbb{N}_0, \quad x|y \implies \exists k_y \in \mathbb{N} : y = k_y \cdot x, \quad y|x \implies \exists k_x \in \mathbb{N} : x = k_x \cdot y.$

$$y = k_y \cdot x = k_y \cdot (k_x \cdot y) \implies k_y \cdot k_x = 1 \implies k_y = k_x = 1 \implies x = y$$

Transitiv. $x, y, z \in \mathbb{N}_0, \quad x|y \implies \exists k_y \in \mathbb{N} : y = k_y \cdot x, \quad y|z \implies \exists k_z \in \mathbb{N} : z = k_z \cdot y.$

$$z = k_z \cdot y = k_z \cdot (k_y \cdot x) = \underbrace{k_z \cdot k_y}_{\in \mathbb{N}} \cdot x \implies x|z$$

□

Bemerkung 1.1.
Die Teilbarkeitsrelation ist keine totale Ordnung, denn es gibt bspw. weder $2|3$ noch $3|2$. Sie ist auch keine Äquivalenzrelation, denn es gilt z.B. nicht $2|4 \implies 4|2$.

Satz 1.6. *Für $m \in \mathbb{N}$ ist die Relation*

$$\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}, \quad a \equiv_m b :\Longleftrightarrow m|a-b, \quad a,b \in \mathbb{Z}$$

eine Äquivalenzrelation.

Beweis. Reflexiv.

$$\forall m \in \mathbb{Z} : m|0 \implies m|a-a \implies a \equiv_m a$$

Symmetrisch.

$$a \equiv_m b \implies m|a-b \implies m|(-1)(a-b) \implies m|b-a \implies b \equiv_m a$$

Transitiv.

$$\begin{array}{lccc} & a \equiv_m b & \wedge & b \equiv_m c \\ \implies & m|a-b & \wedge & m|b-c \\ \implies & \exists k_1 \in \mathbb{Z} : a-b = k_1 \cdot m & \wedge & \exists k_2 \in \mathbb{Z} : b-c = k_2 \cdot m \\ \implies & a-c = (a-b)+(b-c) = (k_1 \cdot m)+(k_2 \cdot m) = \underbrace{(k_1+k_2)}_{\in\mathbb{Z}} \cdot m & & \\ \implies & m|a-c & & \end{array}$$

□

Äquivalenzklassen. (auch Restklassen)

$$\begin{aligned} [a]_{\equiv_m} &= \{\, b \in \mathbb{Z} \mid a \equiv_m b \,\} \quad (m \text{ „Modul“}) \\ &= \{\, b \in \mathbb{Z} \mid m|a-b \,\} \\ &= \{\, b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : a-b = k \cdot m \,\} \\ &= \{\, b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : a-k \cdot m = b \,\} \\ &= \{\, a + x \cdot m \mid x \in \mathbb{Z} \,\} \\ &= \{\, b \in \mathbb{Z} \mid b \text{ hat bei Division durch } m \text{ denselben Rest } a \,\} \end{aligned}$$

Beispiel 1.13. Für $m = 3$ gibt es drei Restklassten für die Reste $r = 0, 1, 2 < m$:

$$\left.\begin{aligned} [0]_{\equiv_3} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ [1]_{\equiv_3} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ [2]_{\equiv_3} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}\right\} \text{ bilden Partition auf } \mathbb{Z}$$

Hierbei sind die *Repräsentanten* der Restklassen frei wählbar:

$$\begin{aligned} \ldots &= [-3]_{\equiv_3} = [0]_{\equiv_3} = [3]_{\equiv_3} = \ldots \\ \ldots &= [-2]_{\equiv_3} = [1]_{\equiv_3} = [4]_{\equiv_3} = \ldots \\ \ldots &= [-1]_{\equiv_3} = [2]_{\equiv_3} = [5]_{\equiv_3} = \ldots \end{aligned}$$

Definition 1.14 (Restklasse/Repräsentant)**.** Für $m \in \mathbb{N}$ und $r \in \mathbb{N}$, $0 \leq r < m$ heißt

$$r + m\mathbb{Z} := \{\, r + mx \mid x \in \mathbb{Z} \,\} = [r]_{\equiv_m}$$

Restklasse modulo m.
Ein Element einer Restklasse heißt *Repräsentant* der Restklasse.
Da $r \in r + m\mathbb{Z}$ ist r ein Repräsentant (wähle $x = 0$).
Äquivalente Schreibweisen:

$$\begin{aligned} & a, b \in r + m\mathbb{Z} \\ \iff\ & a \equiv_m b \\ \iff\ & a \equiv b \mod m \\ (\iff\ & a \equiv b \quad (m)\ ) \end{aligned}$$

Beispiel 1.14.

$$\begin{aligned} \text{Grundschule: } & 17 : 7 = 2 \quad (\text{Rest } 3) \\ \iff\ & 17 = 7 * 2 + 3 \\ \iff\ & 17 \equiv 3 \mod 7 \\ \iff\ & 7 | 17 - 3 \\ \iff\ & 17 \equiv_7 3 \\ \iff\ & 17 \in [3]_{\equiv_7} \\ \iff\ & 3, 17 \in 3 + 7\mathbb{Z} \quad (m = 7) \end{aligned}$$

$$[3]_{\equiv_7} = 3 + 7\mathbb{Z} = \{\, \ldots, \underset{\text{-7}}{-25}, \underset{\text{-7}}{-18}, \underset{\text{-7}}{-11}, \underset{\text{-7}}{-4}, \underset{+7}{3}, \underset{+7}{10}, \underset{+7}{17}, \underset{+7}{24}, \underset{+7}{31}, \underset{+7}{38}, \ldots \}$$

Was ist mit negativen Zahlen?

Korollar 1.1 (*Ohne Beweis*)**.** *Für $a, m, q \in \mathbb{N}$, $r \in \mathbb{N}_0$ gilt:*

$$\begin{aligned} & a = m \cdot q + r \quad (q \text{ „}\textit{Quotient}\text{“}) \\ \implies\ & -a = m \cdot (-(q+1)) + (m - r) \end{aligned}$$

Beispiel 1.15.

(i) $a = 4 \iff -a = -4$, $m = 7$

$$\begin{aligned} & 4 = 7 \cdot 0 + 4 \quad (q = 0,\ r = 4,\ m - r = 3) \\ \implies\ & -4 = 7 \cdot (-1) + 3 \\ \implies\ & -4 \equiv 3 \mod 7 \end{aligned}$$

Reste sind immer positiv!!!

(ii) Weitere Beispiele:

$$\begin{aligned} -3 &\equiv 5 \mod 8 \\ -5 &\equiv 4 \mod 9 \\ -17 &\equiv 1 \mod 3 \\ -24 &\equiv 4 \mod 7 \end{aligned}$$

(iii) Andersrum geht es aber auch:

$$16 \equiv \underbrace{-4}_{} \mod 20, \text{ denn } -4 \equiv \underbrace{16}_{} \mod 20$$
$$49 \equiv \underbrace{-1}_{} \mod 50, \text{ denn } -1 \equiv \underbrace{49}_{} \mod 50$$

Hier stehen immer Repräsentanten der Restklassen!

(iv) $3 \equiv -4 \equiv 10 \equiv -11 \equiv -18 \mod 7$ (Immer ein Vielfaches von 7 addieren!)

Satz 1.7 (Rechenregeln der Modulo-Rechnung)**.** *Für $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$ gelten die folgenden Rechenregeln:*

(i) $-b \equiv -(b \mod m) \mod m$

(ii) $a + b \equiv (a \mod m + b \mod m) \mod m$

(iii) $a - b \equiv (a \mod m - b \mod m) \mod m$

(iv) $a \cdot b \equiv (a \mod m \cdot b \mod m) \mod m$

(v) $a^b \equiv (a \mod m)^b \mod m$

Es gibt keine Aussage zur Division: $(m = 4)$

$$6 : 2 \equiv 3 \not\equiv 1 \equiv 2 : 2 \equiv (2 \mod 4) : (2 \mod 4) \equiv (6 \mod 4) : (2 \mod 4) \mod 4$$

Man schreibt das mod ***oft nur ans Ende!***

Beweis. Ohne Beweis. □

Beispiel 1.16.

(i) $m = 7$.

$$\begin{aligned} 11 + 12 &\equiv 23 \equiv 2 \equiv 9 \equiv 4 + 5 \mod 7 \\ 11 \cdot 12 &\equiv 132 \equiv 6 \equiv 20 \equiv 4 \cdot 5 \mod 7 \\ 132 - 50 &\equiv 82 \equiv 5 \equiv 6 - 1 \mod 7 \end{aligned}$$

(ii) $m = 12$.

$$7^4 \equiv 7^2 \cdot 7^2 \equiv 49 \cdot 49 \equiv 1 \cdot 1 \equiv 1 \equiv 1^4 \mod 12$$

(iii) $m = 20$.

$$82^{17} \equiv 2^{17} \equiv 2^{16+1} \equiv 2^{16} \cdot 2^1 \equiv \left(2^4\right)^4 \cdot 2 \equiv 16^4 \cdot 2 \equiv (-4)^4 \cdot 2$$
$$\equiv (-4)^2 \cdot (-4)^2 \cdot 2 \equiv 16 \cdot 16 \cdot 2 \equiv (-4) \cdot (-4) \cdot 2 \equiv 32 \equiv 12 \mod 20$$

(iv) $m = 19$.

$$2^{270} \equiv 2^{9 \cdot 30} \equiv \left(2^9\right)^{30} \equiv \left(2^4 \cdot 2^4 \cdot 2\right)^{30} \equiv (16 \cdot 16 \cdot 2)^{30} \equiv ((-3) \cdot (-3) \cdot 2)^{30}$$
$$\equiv 18^{30} \equiv (-1)^{30} \equiv 1 \mod 19$$

Addition und Multiplikation von Restklassen.

$$[a]_{\equiv_m} \oplus [b]_{\equiv_m} = [a+b]_{\equiv_m} \iff (a + m\mathbb{Z}) \oplus (b + m\mathbb{Z}) = (a+b) + m\mathbb{Z}$$
$$[a]_{\equiv_m} \odot [b]_{\equiv_m} = [a \cdot b]_{\equiv_m} \iff (a + m\mathbb{Z}) \odot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}$$

Neue Rechenstruktur:

$$\mathbb{Z}/m\mathbb{Z} := \{\, m\mathbb{Z},\ 1 + m\mathbb{Z},\ \ldots,\ (m-1) + m\mathbb{Z} \,\} \rightsquigarrow (\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$$

Schreibe nun $[a]_{\equiv_m} := [a]_m$.

Beispiel 1.17.

$$[4]_7 \oplus [5]_7 = [9]_7 = [2]_7$$
$$[4]_7 \odot [5]_7 = [20]_7 = [6]_7$$

Definition 1.15 (Primzahlen)**.**

(i) $p \in \mathbb{N}$ heißt *Primzahl*, wenn sie genau zwei verschiedene Teiler besitzt, nähmlich 1 und sich selbst. Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.

(ii) $q \in \mathbb{N}$ heißt *zusammengesetzt*, falls $q \in \mathbb{N} \setminus \mathbb{P}$.

Korollar 1.2. *1 ist keine Primzahl! Die einzige gerade Primzahl ist 2.*

Beispiel 1.18 (Fermat-Zahlen)**.** $n \in \mathbb{N},\ F_n := 2^{2^n} + 1,\ F_1, F_2, F_3, F_4 \in \mathbb{P}$.
Frage: $F_5 \in \mathbb{P}$? ($F_5 = 4\ 294\ 367\ 297$)
Antwort: Nein, denn $641 | F_5$:

$$641 = 640 + 1 = 5 \cdot 2^7 + 1$$
$$\implies 5 \cdot 2^7 \equiv -1 \mod 641$$
$$\implies \left(5 \cdot 2^7\right)^4 \equiv (-1)^4 \equiv 1 \mod 641$$
$$\implies 5^4 \cdot 2^{28} \equiv 1 \mod 641 \qquad (*)$$

Außerdem:

$$\begin{aligned}
& 641 = 625 + 16 = 5^4 + 2^4 \\
\Longrightarrow \quad & 5^4 \equiv -2^4 \mod 641 \\
\overset{*}{\Longrightarrow} \quad & -2^{32} \equiv 1 \mod 641 \\
\Longrightarrow \quad & -2^{2^5} - 1 \equiv 0 \mod 641 \\
\Longrightarrow \quad & 2^{2^5} + 1 \equiv 0 \mod 641 \\
\Longrightarrow \quad & 641 | F_5
\end{aligned}$$

Anwendung in der Geometrie (Gauß): Ein regelmäßiges Polygon mit n Seiten kann nur dann mit Zirkel und Lineal konstruiert werden, wenn

$$n = 2^k \ \vee \ n = 2^k \cdot \prod_{i \in I} F_i$$

mit $k \in \mathbb{N}_0$, $I \subset N$ und $F_i \in \mathbb{P}$.
Somit sind 17-Ecke konstruierbar: $17 = F_2 = 2^0 \cdot F_2$.

Beispiel 1.19 (Mersenne-Primzahlen)**.** Bis zum frühen Mittelalter glaubte man:

$$p \in \mathbb{P} \implies 2^p - 1 \in \mathbb{P}$$

Gegenbeispiele:
$p = 11$, da $2^{11} - 1 = 2047 = 23 \cdot 89$.
$p = 23$, 37 nach Fermat.
$p = 29$ nach Euler.

Aber falls das nicht gilt, heißt $2^p - 1$ *Mersenne-Primzahl.*
(2024: $p = 136\,279\,841$ mit $2^p - 1 \sim 41$ Mio. Stellen)

Definition 1.16 (Größter gemeinsamer Teiler)**.** Seien $a, b \in \mathbb{Z}$ mit $a \neq 0 \vee b \neq 0$. Dann heißt $t \in \mathbb{N}$ *größter gemeinsamer Teiler* von a und b, wenn

$$t|a \quad \wedge \quad t|b \quad \wedge \quad \forall t' \in \mathbb{N} : t'|a \wedge t'|b \implies t'|t$$

Schreibweise: $t := \mathrm{ggT}(a, b), \ \mathrm{ggT}(0, 0) := 0$.

Korollar 1.3. *Der größte gemeinsame Teiler zweier Zahlen $a, b \in \mathbb{Z}$ ist eindeutig.*

Beweis. Seien $t_1, t_2 \in \mathbb{N}$ zwei ggTs von a und b.

$$\begin{aligned}
& t_1|a \quad \wedge \quad t_1|b \quad \wedge \quad \forall t' \in \mathbb{N} : t'|a \wedge t'|b \implies t'|t_1 \\
\wedge \quad & t_2|a \quad \wedge \quad t_2|b \quad \wedge \quad \forall t' \in \mathbb{N} : t'|a \wedge t'|b \implies t'|t_2 \\
\Longrightarrow \quad & \exists k_1, k_2 \in \mathbb{Z} : a = k_1 t_1 = k_2 t_2 \quad \wedge \quad \exists k_3, k_4 \in \mathbb{Z} : b = k_3 t_1 = k_4 t_2 \\
\Longrightarrow \quad & t_1 = \underbrace{\frac{a}{k_1}}_{\in \mathbb{Z}} = \underbrace{\frac{k_2}{k_1}}_{\in \mathbb{Z}} t_2 \implies t_1|t_2 \quad \wedge \quad t_2 = \underbrace{\frac{b}{k_4}}_{\in \mathbb{Z}} = \underbrace{\frac{k_3}{k_1}}_{\in \mathbb{Z}} t_1 \implies t_2|t_1 \\
\Longrightarrow \quad & t_1 = t_2
\end{aligned}$$

□

Korollar 1.4. *Seien* $a \in \mathbb{Z}$, $b, c \in \mathbb{N}$.

$$\mathrm{ggT}(a,b) = 1 \ \wedge \ c|b \implies \mathrm{ggT}(a,c) = 1$$

Beweis durch Widerspruch. Annahme: $\mathrm{ggT}(a,c) =: t > 1$
Es gilt:

$$\begin{aligned} & t|a \quad \wedge \quad t|c \\ \implies & \exists p, q \in \mathbb{Z} : a = tp \wedge c = tq \\ \overset{c|b}{\implies} & \exists r \in \mathbb{Z} : b = cr \\ \implies & b = tqr \\ \implies & t|b \end{aligned}$$

Widerspruch zu $\mathrm{ggT}(a,b) = 1$. □

Euklidischer Algorithmus.
Berechne ggT(r_0 , r_1), wobei $0 \le r_1 < r_0$: (Division mit Rest!)

ggT(1024, 1001)

$$\begin{array}{rcl} r_0 = q_1 \cdot r_1 + r_2 & & 0 \le r_2 < r_1 \\ 1024 = 1 \cdot 1001 + 23 & & 0 \le 23 < 1001 \\ r_1 = q_2 \cdot r_2 + r_3 & & 0 \le r_3 < r_2 \\ 1001 = 43 \cdot 23 + 12 & & 0 \le 12 < 23 \\ \vdots \quad \vdots \quad \vdots \quad \vdots & & \vdots \quad \vdots \quad \vdots \\ r_{n-3} = q_{n-2} \cdot r_{n-2} + r_{n-1} & & 0 \le r_{n-1} < r_{n-2} \\ 23 = 1 \cdot 12 + 11 & & 0 \le 11 < 12 \\ r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n & & 0 \le r_n < r_{n-1} \\ 12 = 1 \cdot 11 + 1 & & 0 \le 1 < 11 \\ r_{n-1} = q_n \cdot r_n + \boxed{0} & \Big\} & r_{n+1} = 0 \\ 11 = 11 \cdot 1 + \boxed{0} & & \\ r_n = \mathrm{ggT}(\ r_0\ ,\ r_1\ ) & & \\ 1 = \mathrm{ggT}(1024, 1001) & & \end{array}$$

Allgemeines Schema. $1 \le k \le n-1, \quad q_k \ge 1, \quad 0 \le r_{k+1} < r_k$.

$$r_{k-1} = q_k \cdot r_k + r_{k+1}$$

Erweiterter Euklidischer Algorithmus.
Berechne 1001^{-1} (1024), also x sodass $1001 \cdot x = 1 \mod 1024$:
Ziel: Finde $x, y \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(1024, 1001) = 1024x + 1001y$

$$
\begin{array}{rcl}
r_0 = q_1 \cdot r_1 + r_2 & \Longleftrightarrow & r_2 = r_0 + (-q_1) \cdot r_1 \\
1024 = 1001 \cdot 1 + 23 & \Longleftrightarrow & 23 = 1024 + (-1) \cdot 1001 \\
r_1 = q_2 \cdot r_2 + r_3 & \Longleftrightarrow & r_3 = r_1 + (-q_2) \cdot r_2 \\
1001 = 23 \cdot 43 + 12 & \Longleftrightarrow & 12 = 1001 + (-43) \cdot 23 \\
\vdots \quad \vdots \quad \vdots \quad \vdots & & \vdots \quad \vdots \quad \vdots \quad \vdots \\
r_{n-3} = q_{n-2} \cdot r_{n-2} + r_{n-1} & \Longleftrightarrow & r_{n-1} = r_{n-3} + (-q_{n-2}) \cdot r_{n-2} \\
23 = 12 \cdot 1 + 11 & \Longleftrightarrow & 11 = 23 + (-1) \cdot 12 \\
r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n & \Longleftrightarrow & r_n = r_{n-2} + (-q_{n-1}) \cdot r_{n-1} \\
12 = 11 \cdot 1 + 1 & \Longleftrightarrow & 1 = 12 + (-1) \cdot 11 \\
r_{n-1} = q_n \cdot r_n + 0 & & \\
11 = 11 \cdot 1 + 0 & &
\end{array}
$$

Einsetzen von unten nach oben: $(\widetilde{q}_1, \ldots, \widetilde{q}_4 \in \mathbb{Z})$

$$
\begin{aligned}
r_n &= r_{n-2} + (-q_{n-1}) \cdot r_{n-1} \\
1 &= 12 + (-1) \cdot 11 \\
&= r_{n-2} + (-q_{n-1}) \cdot (r_{n-3} + (-q_{n-2}) \cdot r_{n-2}) \\
&= 12 + (-1) \cdot (23 + (-1) \cdot 12) \\
&= (1 + q_{n-2}q_{n-1}) \cdot r_{n-2} + (-q_{n-3}) \cdot r_{n-3} \\
&= 2 \cdot 12 + (-1) \cdot 23 \\
\ldots &= \widetilde{q}_1 \cdot (r_1 + (-q_2) \cdot r_2) + \widetilde{q}_2 \cdot r_2 \\
&= 2 \cdot (1001 + (-43) \cdot 23) + (-1) \cdot 23 \\
&= \widetilde{q}_1 \cdot r_1 + \widetilde{q}_3 \cdot r_2 \\
&= 2 \cdot 1001 + (-87) \cdot 23 \\
&= \widetilde{q}_1 \cdot r_1 + \widetilde{q}_3 \cdot (r_0 + (-q_1) \cdot r_1) \\
&= 2 \cdot 1001 + (-87) \cdot (1024 + (-1) \cdot 1001) \\
&= \widetilde{q}_4 \cdot r_1 + \widetilde{q}_3 \cdot r_0 \\
&= 89 \cdot 1001 + (-87) \cdot 1024
\end{aligned}
$$

Ergebnis: $x = 87$, $y = 89$

$$\begin{aligned}
& 1 = (-87) \cdot 1024 + 89 \cdot 1001 && \mod 1024 \\
\implies\ & 1 = \quad 0 \quad\ + 89 \cdot 1001 && \mod 1024 \\
\implies\ & 1 = 89 \cdot 1001 && \mod 1024 \\
\boxed{\implies\ } & \boxed{89 = 1001^{-1}} && \mod 1024
\end{aligned}$$

Allgemein:

$$\begin{aligned}
& 1 = xm + ya && \mod m \\
\implies\ & 1 = \ 0 \ + ya && \mod m \\
\implies\ & 1 = ya && \mod m \\
\boxed{\implies\ } & \boxed{y = a^{-1}} && \mod m
\end{aligned}$$

Falls $\text{ggT}(m, a) \neq 1$, gibt es kein Inverses $a^{-1} \mod m$.
Dann sind aber $x, y \in \mathbb{Z}$ berechenbar mit $\text{ggT}(m, a) = xm + ya$.

Noch was zu Primzahlen.

Satz 1.8. *Für jede natürliche Zahl $a \in \mathbb{N}$ mit $a \geq 2$ gilt, dass der kleinste Teiler $p \geq 2$ eine Primzahl ist.*

Beweis durch Widerspruch. Annahme: $p \geq 2$ ist keine Primzahl. $\implies \exists b \notin \{ 1, p \} : b | p$

$$\text{Vor.} \implies p | a \implies b | a$$

Widerspruch, da p kleinster Teiler von a ist. □

Satz 1.9. *Es gibt unendlich viele Primzahlen.*

Beweis durch Widerspruch. Annahme: Es gibt endlich viele Primzahlen.
Ohne Beschränkung seien $p_1, \ldots, p_n \in \mathbb{P}$ mit $n \geq 1$ alle Primzahlen und sei

$$p := 1 + \prod_{i=1}^{n} p_i \implies \forall i = 1, \ldots, n : p_i \nmid p$$

Widerspruch, da der kleinste Teiler von p nach Satz 1.8 eine Primzahl sein muss und $p_1, \ldots, p_n$ keine Teiler sind. □

Primfaktorzerlegung.

Beispiel 1.20.

$$\begin{aligned}
& \text{(i)} \quad 86 : 2 = 43 \in \mathbb{P} \\
\implies\ & 86 = 2 \cdot 43
\end{aligned}$$

(ii) $114 : 2 = 57$
$57 : 2$ geht nicht!
$57 : 3 = 19 \in \mathbb{P}$
$\Longrightarrow 114 = 2 \cdot 3 \cdot 19$

(iii) $105 : 2$ geht nicht!
$105 : 3 = 35$
$35 : 3$ geht nicht!
$35 : 5 = 7 \in \mathbb{P}$
$\Longrightarrow 105 = 3 \cdot 5 \cdot 7$

(iv) $154 : 2 = 77$
$77 : 2$ geht nicht!
$77 : 3$ geht nicht!
$77 : 5$ geht nicht!
$77 : 7 = 11 \in \mathbb{P}$
$\Longrightarrow 154 = 2 \cdot 7 \cdot 11$

(v) $270 : 2 = 135$
$135 : 2$ geht nicht!
$135 : 3 = 45$
$45 : 3 = 15$
$15 : 3 = 5 \in \mathbb{P}$
$\Longrightarrow 270 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2 \cdot 3^3 \cdot 5$

(vi) $4114 : 2 = 2057$
2057 geht nicht durch 2,3,5,7
$2057 : 11 = 187$
$187 : 11 = 17 \in \mathbb{P}$
$\Longrightarrow 4114 = 2 \cdot 11^2 \cdot 17$

Satz 1.10 (Fundamentalsatz der Zahlentheorie)**.** *Jede natürliche Zahl $n \geq 2$ hat eine eindeutige Primfaktorzerlegung (Faktorisierung).*

$$\forall n \in \mathbb{N}_{\geq 2} : n = \prod_{i=1}^{r} q_r,\ r \in \mathbb{N},\ \forall i = 1, \ldots, r : q_i \in \mathbb{P},\ q_i \leq n$$

Zur Eindeutigkeit: Primzahlen können mehrfach in der Zerlegung vorkommen.
Diejenigen, die nicht in der Zerlegung vorkommen, bekommen den Exponenten 0.

Index