Diskrete Mathematik

Zahlenmengen

$\mathbb{N}$	natürliche Zahlen
$\mathbb{N}_0$	natürliche Zahlen mit 0
$\mathbb{Z}$	ganze Zahlen
$\mathbb{Q}$	rationale Zahlen
$\mathbb{R}$	reelle Zahlen
$\mathbb{C}$	komplexe Zahlen

Aussagenlogik

Aussage	Ein Satz, der entweder wahr (w) oder falsch (f) ist.
Prädikat	Eine Aussage mit Variablen. n-stellige Prädikate.

Grundidee

Aus gegebenen Prädikaten/Aussagen lassen sich durch Junktoren neue Aussagen bilden. (z. B. Kombinationen mit $\land, \lor, \neg, \Rightarrow, \Leftrightarrow$).

Definitionen

- **Negation:** $\neg A$ ist genau dann wahr, wenn A falsch ist. (Doppelte Negation: $A \Leftrightarrow \neg\neg A$.)
- **Konjunktion:** $A \land B$ ist wahr genau dann, wenn A und B wahr sind. (assoziativ, kommutativ, idempotent)
- **Disjunktion:** $A \lor B$ ist wahr, wenn mindestens eine der Aussagen wahr ist. (assoziativ, kommutativ, idempotent)
- **Implikation:** $A \Rightarrow B$ ist äquivalent zu $\neg A \lor B$. (Kontraposition: $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$.)
- **Äquivalenz:** $A \Leftrightarrow B$ genau dann, wenn $A \Rightarrow B \land B \Rightarrow A$.

Wichtige Regeln

- **De Morgan:** $\neg(A \land B) \Leftrightarrow \neg A \lor \neg B$ $\neg(A \lor B) \Leftrightarrow \neg A \land \neg B$
- **Distributivität:** $A \land (B \lor C) \Leftrightarrow (A \land B) \lor (A \land C)$ $A \lor (B \land C) \Leftrightarrow (A \lor B) \land (A \lor C)$
- **Syntaktische Bindung:** $\neg$ bindet stärker als $\land, \lor$; diese binden stärker als $\Rightarrow, \Leftrightarrow$.
- **Modus Ponens:** Aus $A \land (A \Rightarrow B)$ folgt B.
- **Transitivität:** Aus $(A \Rightarrow B) \land (B \Rightarrow C)$ folgt $A \Rightarrow C$.

Hinweis zur Redundanz

Jeder Ausdruck mit den Junktoren $\neg, \land, \lor, \Rightarrow$ lässt sich ausschliesslich mit $\neg$ und $\lor$ darstellen. z.B.

$$A \land B \Leftrightarrow \neg(\neg A \lor \neg B)$$
$$A \lor B \Leftrightarrow \neg(\neg A \land \neg B)$$

Quantoren

Quantoren dienen zur Formalisierung von Aussagen wie:

- $\forall x\, A(x)$: *Für alle x gilt $A(x)$*
- $\exists x\, A(x)$: *Es existiert ein x mit $A(x)$*

Mehrere gleichartige Quantoren:

$$\forall x, y\; A(x, y) \quad \text{statt} \quad \forall x \forall y\; A(x, y)$$

Eingeschränkte Quantoren

$$\forall x \in M\; A(x) : \text{Für alle } x \in M \text{ gilt } A(x)$$
$$\exists x \in M\; A(x) : \text{Es gibt } x \in M \text{ mit } A(x)$$

Auch möglich mit Relationen:

$$\forall x < y\; A(x) \quad \text{oder} \quad \exists x \leq y\; A(x)$$

Als Junktoren

Für endliche Mengen $M = \{x_1, \ldots, x_n\}$ gilt:

$$\forall x \in M\; A(x) \Leftrightarrow A(x_1) \land \cdots \land A(x_n)$$
$$\exists x \in M\; A(x) \Leftrightarrow A(x_1) \lor \cdots \lor A(x_n)$$

Als Makros

$$\exists x \in M\; A(x) \Leftrightarrow \exists x\, (x \in M \land A(x))$$
$$\forall x \in M\; A(x) \Leftrightarrow \forall x\, (x \in M \Rightarrow A(x))$$

Zusammenhang mit Junktoren

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

Leere Quantoren

Wenn x in B nicht vorkommt:

$$\forall x\, B \Leftrightarrow B, \quad \exists x\, B \Leftrightarrow B$$

Mengen

- **Menge / Element:** Eine Menge fasst mathematische Objekte (Elemente) zu einem Ganzen zusammen. Für Menge X und Element y gilt $y \in X$ bzw. $y \notin X$.
- **Aufzählende Schreibweise:** $\{x_1, \ldots, x_n\}$ bezeichnet die Menge, die genau die genannten Elemente enthält. Die leere Menge heisst $\varnothing$.
- **Extensionalitätsprinzip:** Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente haben:
$$A = B \iff \forall x\, (x \in A \Leftrightarrow x \in B).$$
- **Teilmenge:** $A \subseteq B$ genau dann, wenn $\forall x\, (x \in A \Rightarrow x \in B)$. Ist $A \subseteq B$ und $A \neq B$, so ist A eine *echte* Teilmenge, geschrieben $A \subset B$.
- **Folgerungen:** Mengen sind ungeordnet; Mehrfachaufzählung desselben Elements ändert die Menge nicht. Für jede Menge A gilt $\varnothing \subseteq A$.

Eindeutigkeit der leeren Menge

Seien e_1, e_2 leere Mengen. Dann ist für alle x die Aussage $x \in e_1$ falsch, also ist die Implikation $x \in e_1 \Rightarrow x \in e_2$ wahr; somit $e_1 \subseteq e_2$. Analog $e_2 \subseteq e_1$. Nach Extensionalität folgt $e_1 = e_2$.

Aussonderungsprinzip

Ist A eine Menge und $E(x)$ eine Eigenschaft, dann gilt:

$$\{x \in A \mid E(x)\} = \text{Menge aller } x \in A \text{ mit } E(x).$$
$$a \in \{x \in A \mid E(x)\} \iff a \in A \land E(a)$$

Beispiele:

- Gerade Zahlen: $\{x \in \mathbb{N} \mid \exists y \in \mathbb{N}(x = 2y)\}$
- Primzahlen: $\{x \in \mathbb{N} \mid \exists y \in \mathbb{N}(y > 1) \land \forall a, b \in \mathbb{N}(ab = x \Rightarrow x = a \lor x = b)\}$

Ersetzungsprinzip

Ist A eine Menge und $t(x)$ ein Ausdruck, so gilt:

$$\{t(x) \mid x \in A\} = \text{Menge aller Werte von } t(x) \text{ mit } x \in A.$$
$$a \in \{t(x) \mid x \in A\} \iff \exists x \in A(a = t(x))$$

Beispiele:

- Quadratzahlen: $\{x^2 \mid x \in \mathbb{N}\}$
- Ungerade Zahlen: $\{2x + 1 \mid x \in \mathbb{N}\}$
- Rationale Zahlen: $\left\{\frac{a}{b} \mid a, b \in \mathbb{Z},\, b \neq 0\right\}$
- Anfangsabschnitte von $\mathbb{N}$: $\{\{x \in \mathbb{N} \mid x < y\} \mid y \in \mathbb{N}\}$

Vereinigung

Die Vereinigung von zwei Mengen beinhaltet genau die Elemente, die in mindestens einer der beiden Mengen enthalten sind:

$$A \cup B := \{x \mid x \in A \lor x \in B\}.$$

Schnitt

Die Schnittmenge von zwei Mengen beinhaltet genau die Elemente, die in beiden Mengen enthalten sind:

$$A \cap B := \{x \mid x \in A \land x \in B\}.$$

Allgemeine Vereinigung / Schnitt

Sei I eine beliebige Indexmenge (z. B. $I = \{1, 2, \ldots, n\}$ oder $I = \mathbb{N}$). Für jedes $i \in I$ sei A_i eine Menge.

Allgemeine Vereinigung

x gehört zur Vereinigung genau dann, wenn es in *mindestens einer* der Mengen A_i enthalten ist.

$$\bigcup_{i \in I} A_i := \{\, x \mid \exists i \in I : x \in A_i \,\}.$$

Allgemeiner Schnitt

x gehört zum Schnitt genau dann, wenn es in *allen* Mengen A_i enthalten ist.

$$\bigcap_{i \in I} A_i := \{\, x \mid \forall i \in I : x \in A_i \,\}.$$

Differenz

Die Differenz von zwei Mengen beinhaltet genau die Elemente, die in der ersten Menge, aber nicht in der zweiten Menge enthalten sind:

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

Disjunkte Mengen

Zwei Mengen A und B heissen disjunkt, wenn sie keine gemeinsamen Elemente besitzen.

$$A \cap B = \varnothing.$$

Paarweise disjunkt

Eine Familie von Mengen $(A_i)_{i \in I}$ heisst paarweise disjunkt, wenn keine zwei verschiedenen Mengen ein gemeinsames Element haben. Es gilt:

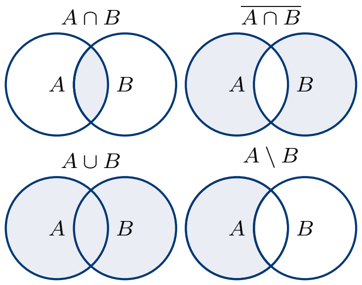
$$\forall i, j \in I\; (i \neq j \Rightarrow A_i \cap A_j = \varnothing).$$

Wichtige Eigenschaften

Für beliebige Mengen A, B, C gelten:

- Idempotenz: $A \cup A = A,\; A \cap A = A$.
- Kommutativität: $A \cup B = B \cup A,\; A \cap B = B \cap A$.
- Assoziativität: $A \cup (B \cup C) = (A \cup B) \cup C$ und analog für $\cap$.
- Teilmengen: $A \subseteq A \cup B$ und $A \cap B \subseteq A$.
- Distributivität:
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
- De Morgansche Regeln:
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B),$$
$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).$$

Venn-Diagramm



Potenzmenge

Für eine Menge A bezeichnet die Potenzmenge $\mathcal{P}(A)$ die Menge aller Teilmengen von A:

$$\mathcal{P}(A) := \{X \mid X \subseteq A\}$$

Beispiele:

$$\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\},$$
$$\mathcal{P}(\varnothing) = \{\varnothing\},$$
$$\mathcal{P}(\{\{a\}\}) = \{\varnothing, \{\{a\}\}\}.$$

Eigenschaften:

- $A \in \mathcal{P}(A)$ und $\varnothing \in \mathcal{P}(A)$.
- Aus $A \subseteq B$ folgt $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- Für die leere Menge gilt $\mathcal{P}(\varnothing) = \{\varnothing\} \neq \varnothing$.
- $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$
- $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$
- $\mathcal{P}(A)$ einer endlichen Menge mit $|A| = n$ hat $|\mathcal{P}(A)| = 2^n$ Elemente.

Tupel

Ein n-Tupel ist ein *geordneter* Vektor

$$(a_1, \ldots, a_n).$$

Der i-te Eintrag eines Tupels $a = (a_1, \ldots, a_n)$ wird mit $a[i]$ bezeichnet. Zwei Tupel sind genau dann gleich, wenn sie dieselbe Länge haben und alle entsprechenden Einträge übereinstimmen:

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_k) \iff n = k \ \wedge\ a_1 = b_1 \ \wedge \cdots \wedge a_n = b_k$$

Kartesisches Produkt

Das kartesische Produkt $A_1 \times \cdots \times A_n$ ist die Menge aller n-Tupel, deren Einträge aus den Mengen $A_1, \ldots, A_n$ stammen.

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \le i \le n\}.$$

Besonderheiten:

- Für das n-fache Produkt von A mit sich selbst gilt $A^n := A \times \cdots \times A$ (n-mal).
- Für ein kartesisches Produkt von der Form $A_1 \times \cdots \times A_n$ wird auch die Kurzschreibweise $\prod_{i=1}^{n} A_i$ verwendet.

Beispiele:

$$\{1\} \times \{a, b\} = \{(1, a), (1, b)\}$$
$$\mathbb{N}^2 = \{(x, y) \mid x \in \mathbb{N} \wedge y \in \mathbb{N}\}$$

Projektionen

Für eine Menge A von n-Tupeln und ist $k \le n$ eine natürliche Zahl, definiert man die k-te Projektion:

$$\mathrm{pr}_k(A) := \{x[k] \mid x \in A\}.$$

Insbesondere gilt:

$$\mathrm{pr}_k(A_1 \times \cdots \times A_n) = A_k.$$

Beispiele:

$$\mathrm{pr}_1(\{1, 2\} \times \{a, b\}) = \{1, 2\}$$
$$\mathrm{pr}_2(\{1, 2\} \times \{a, b\}) = \{a, b\}$$

Relationen

Eine *Relation* von A nach B ist ein Tripel

$$R = (G, A, B)$$

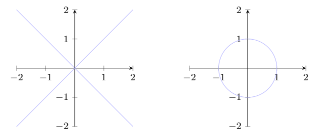
wobei A die Quellmenge, B die Zielmenge und $G \subseteq A \times B$ der *Graph* von R ist. Ist $A = B$, so heisst R *homogen* auf A.

Notation

Sei $R = (G, A, B)$ eine Relation von A nach B.

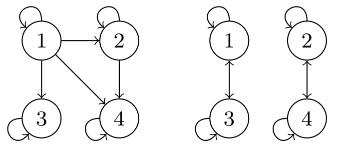
- Ist G der Graph von R, so schreibt man G_R
- Ist $(x, y) \in G$, dann schreibt man xRy (x steht in Relation zu y bezüglich R).
- Sind A und B Teilmengen von $\mathbb{R}$, so kann man R auch als Menge von Punkten in der Ebene darstellen: $\{(x, y) \mid xRy\}$.

$xRy :\Leftrightarrow x^2 = y^2$ $\quad$ $xRy :\Leftrightarrow x^2 + y^2 = 1$



- Als gerichteter Graph: Elemente von A und B als Knoten; für jedes $(x, y) \in G$ ein Pfeil $x \to y$.

$xRy :\Leftrightarrow x$ teilt y $\quad$ $xRy :\Leftrightarrow x + y$ ist gerade



Domäne und Bild

Die Domäne und das Bild einer Relation geben an, welche Elemente der Quell- bzw. Zielmenge tatsächlich in der Relation vorkommen.

$$\mathrm{dom}(R) := \mathrm{pr}_1(G_R) = \{a \in A \mid \exists b \in B(aRb)\}$$
$$\mathrm{im}(R) := \mathrm{pr}_2(G_R) = \{b \in B \mid \exists a \in A(aRb)\}$$

Im gerichteten Graphen entsprechen die Elemente der Domäne den Knoten mit ausgehenden Kanten, die des Bildes den Knoten mit eingehenden Kanten.

Klassifizierungen

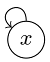
Sei $R \subseteq A \times A$ eine (homogene) Relation auf A.

Reflexivität

Eine Relation R heisst *reflexiv*, wenn jedes Element in Relation zu sich selbst steht:

$$\forall x \in A(xRx)$$

- $\{(a, a) \mid a \in A\} \subseteq R$.
- Im gerichteten Graphen hat jeder Knoten eine Kante zu sich selbst. Für jeden Wert $x \in A$ gilt:



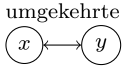
- In der Koordinatendarstellung enthält R die Winkelhalbierende $y = x$.

Symmetrie

Eine Relation R heisst *symmetrisch*, wenn für alle $x, y \in A$ gilt:

$$\forall x, y\ (xRy \Rightarrow yRx).$$

- Zu jedem Pfeil im gerichteten Graph existiert der umgekehrte Pfeil. Für alle $x, y \in A$ gilt:



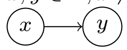
- Symmetrie spiegelt die Koordinatendarstellung an der Geraden $y = x$.

Antisymmetrie

Eine Relation R heisst *antisymmetrisch*, wenn für alle $x, y \in A$ gilt:

$$\forall x, y\ (xRy \wedge yRx \Rightarrow x = y).$$

- Es gibt keine zwei verschiedenen Knoten, die wechselseitig verbunden sind. Für alle $x, y \in A, x \neq y$ gilt:

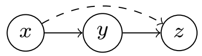


Transitivität

Eine Relation R heisst *transitiv*, wenn für jeden endlichen Pfad ein direkter Pfeil existiert. Für alle $x, y, z \in A$ gilt:

$$\forall x, y, z\ (xRy \wedge yRz \Rightarrow xRz).$$

- Im gerichteten Graphen: Aus $x \to y$ und $y \to z$ folgt $x \to z$. Für alle $x, y, z \in A$ gilt:



Totalität und Eindeutigkeit

Sei $R \subseteq A \times B$ eine Relation von A nach B mit

- **Linksvollständig / linkstotal:** $\mathrm{dom}(R) = A$ (jedes Element in A hat min. eine *ausgehende* Kante).
- **Rechtsvollständig / rechtstotal:** $\mathrm{im}(R) = B$ (jedes Element in B hat min. eine *eingehende* Kante).
- **Linkseindeutig:** $\forall x_1, x_2, y\ (x_1Ry \wedge x_2Ry \Rightarrow x_1 = x_2)$ (jedes Element in B hat max. eine *eingehende* Kante).
- **Rechtseindeutig:** $\forall x, y_1, y_2\ (xRy_1 \wedge xRy_2 \Rightarrow y_1 = y_2)$ (jedes Element in A hat max. eine *ausgehende* Kante).

Inverse Relationen

Für eine Relation $R = (G, A, B)$ ist die *inverse Relation* definiert durch

$$R^{-1} = (G', B, A), \quad G' := \{(y, x) \mid (x, y) \in G\}.$$

Eigenschaften:

- $(R^{-1})^{-1} = R$
- R ist linksvollständig $\Leftrightarrow$ R^{-1} ist rechtsvollständig
- R ist linkseindeutig $\Leftrightarrow$ R^{-1} ist rechtseindeutig
- Für jede symmetrische Relation R gilt $R = R^{-1}$

Funktionen

Eine *Funktion* f von der Menge A nach B ist eine Relation, die *linksvollständig* und *rechtseindeutig* ist. Man schreibt:

$$f : A \to B,$$

und für jedes $x \in A$ existiert genau ein $y \in B$ mit $y = f(x)$.

Schreibweise

Oft werden Funktionen durch Angabe von Definitions- und Zielmenge sowie einer Zuordnungsvorschrift beschrieben. Beispielsweise gilt:

$$f = (\{(x, x^3) \mid x \in \mathbb{N}\}, \mathbb{N}, \mathbb{N})$$

bzw. äquivalent in der gebräuchlicheren Schreibweise:

$$f : \mathbb{N} \to \mathbb{N}, \quad f(x) = x^3.$$

Injektive Funktionen

Eine Funktion $f : A \to B$ ist *injektiv*, falls die Relation *linksvollständig*, *rechtseindeutig* und zusätzlich *linkseindeutig* ist:

$$\forall x_1, x_2 \in A(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$
$$\forall x_1, x_2 \in A(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$$

Jedes Element in A wird auf ein eigenes unterschiedliches Element in B abgebildet.
Notation: $f : A \hookrightarrow B$.

Umkehrbarkeit

Eine Funktion $f : A \to B$ ist genau dann *umkehrbar*, wenn sie injektiv ist. Dann gilt:

$$f^{-1} : \mathrm{im}(f) \to A.$$
$$(G'_f, \mathrm{im}(f), A), \quad G'_f = \{(y, x) | (x, y) \in G_f\}$$

Surjektivität

Eine Funktion $f : A \to B$ ist *surjektiv*, falls die Relation *linksvollständig*, *rechtseindeutig* und zusätzlich *rechtsvollständig* ist:

$$\mathrm{im}(f) = B$$

Jedes Element in B wird von mindestens einem Element in A erreicht.
Notation: $f : A \twoheadrightarrow B$

Bijektivität

Eine Funktion $f : A \to B$ ist *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist. Die Umkehrfunktion ist dann definiert durch:

$$f^{-1} : B \to A.$$

J Notation: $f : A \rightleftharpoons B$

Umkehrfunktion

Für eine bijektive Funktion $f : A \rightleftharpoons B$ gilt:

$$f^{-1} \circ f = \mathrm{id}_A, \qquad f \circ f^{-1} = \mathrm{id}_B .$$

Komposition

Für $g : A \to B$ und $f : B \to C$ definiert man die *Komposition*:

$$(f \circ g)(x) = f(g(x)), \quad f \circ g : A \to C.$$

Komposition ist *assoziativ*:

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Eigenschaften der Komposition

Für Funktionen $f : A \to B$ und $g : B \to C$ gilt:

- Sind f und g injektiv, dann ist $g \circ f$ injektiv.
- Sind f und g surjektiv, dann ist $g \circ f$ surjektiv.
- Sind f und g bijektiv, dann ist $g \circ f$ bijektiv.

Äquivalenzrelationen

Eine Relation $\sim$ auf einer Menge A heisst *Äquivalenzrelation*, falls sie für alle $x, y, z \in A$ die folgenden Eigenschaften erfüllt:

- **reflexiv:** $x \sim x$,
- **symmetrisch:** $x \sim y \Rightarrow y \sim x$,
- **transitiv:** $x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Beispiele

- Die Gleichheitsrelation $=$ auf jeder Menge.
- Auf $\mathbb{Z}$: $a \equiv_n b :\Leftrightarrow n \mid (a-b)$ (Restklasse modulo n).
- Relation „sitzen in derselben Sitzreihe" in einem Kinosaal.

Klein. und grösst. Äquivalenzrelation

Auf jeder Menge A existiert:

- die *kleinste* Äquivalenzrelation: die Gleichheitsrelation $\{(a,a) \mid a \in A\}$.
- die *grösste* Äquivalenzrelation: das ganze $A \times A$ (alles ist äquivalent).

Äquivalenzklassen und Faktormenge

Für $a \in A$ ist die *Äquivalenzklasse*

$$[a]_\sim := \{x \in A \mid x \sim a\}.$$

Die Menge aller Äquivalenzklassen heisst *Faktormenge* $A/\sim := \{[a]_\sim \mid a \in A\}$. Jedes Element einer Äquivalenzklasse ist ein *Repräsentant* dieser Klasse.

Wichtige Eigenschaften

Für eine Äquivalenzrelation $\sim$ und $a, b \in A$ sind äquivalent:

1. $a \sim b$,
2. $[a]_\sim = [b]_\sim$,
3. $[a]_\sim \cap [b]_\sim \neq \varnothing$,
4. $a \in [b]_\sim$,
5. $b \in [a]_\sim$.

Daraus folgt: Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.

Beispiele in $\mathbb{R}^2$

- $(a,b) \approx (c,d) := a = c$
  Äquivalenzklassen $=$ vertikale Geraden.
- $(a,b) \simeq (c,d) := \sqrt{a^2+b^2} = \sqrt{c^2+d^2}$
  Äquivalenzklassen $=$ Kreise um den Ursprung.
- Auf $\mathbb{R}^2 \setminus \{(0,0)\}$:
  $(a,b) \sim (c,d) := \exists r \in \mathbb{R}(ra, rb) = (c,d)$
  Äquivalenzklassen $=$ Geraden durch den Ursprung.

Partitionen

Eine *Partition* einer Menge A ist eine Menge $\{A_i\}_{i \in I}$ paarweise disjunkter, nichtleerer Teilmengen mit

$$\bigcup_{i \in I} A_i = A.$$

Die A_i nennt man auch *Blöcke* der Partition.

Beispiele

- Gerade und ungerade natürliche Zahlen: $A_0 = \{2n\},\ A_1 = \{2n+1\}$.
- Einzelmengen $\{n\}$ liefern eine feine Partition.
- Es gibt Partitionen von $\mathbb{N}$ in unendlich viele unendliche Blöcke.

Induzierte Partition

Ist $\sim$ eine Äquivalenzrelation auf A, so sind die Äquivalenzklassen $[a]_\sim$ die Blöcke der Partition $A/\sim$. Insbesondere sind die Klassen nichtleer und paarweise disjunkt.

Induzierte Äquivalenzrelation

Ist $P = \{A_i\}_{i \in I}$ eine Partition von A, definiert

$$a \sim b \quad :\Leftrightarrow \quad \exists i \in I\ (a \in A_i \wedge b \in A_i)$$

eine Äquivalenzrelation auf A mit Quotientenmenge $A/\sim = P$.

Äquivalenzrelationen und Funktionen

Eine Relation $\sim$ auf A ist genau dann eine Äquivalenzrelation, wenn es eine Menge B und eine Abbildung $f \colon A \to B$ gibt, mit der Eigenschaften:

$$x \sim y \quad \Leftrightarrow \quad f(x) = f(y).$$

(Äquivalenzklassen sind dann die Urbilder einzelner Werte von f.)

Halbordnungen

Eine *Halbordnung* (poset) ist eine homogene Relation $\preceq$ auf einer Menge A, die

- *reflexiv*: $\forall a \in A:\ a \preceq a$,
- *transitiv*: $\forall a, b, c \in A:\ (a \preceq b \wedge b \preceq c) \Rightarrow a \preceq c$,
- *antisymmetrisch*:
  $\forall a, b \in A:\ (a \preceq b \wedge b \preceq a) \Rightarrow a = b$.

Typische Beispiele

- $(\mathcal{P}(A), \subseteq)$, die Mengeninklusion auf der Potenzmenge.
- Teilbarkeitsrelation auf $\mathbb{N}$.
- Die üblichen $\leq$-Relationen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- Versionen in der Informatik, z. B. Commit-Historien in Git (Ursprungsrelation).

Zyklenfreiheit

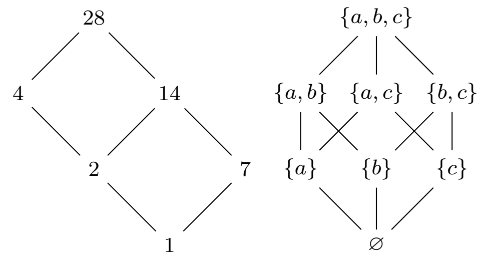
In einer Halbordnung sind echte Zyklen ausgeschlossen: Aus $a_1 \preceq a_2 \preceq \cdots \preceq a_n \preceq a_1$ folgt $a_1 = \cdots = a_n$. Dies folgt aus der Antisymmetrie und der Transitivität.

Hasse-Diagramme

Zur Visualisierung nutzt man Hasse-Diagramme:

- Relative Höhe zeigt die Ordnungsrichtung.
- Kanten werden nur zwischen *benachbarten* Elementen ohne Zwischenelement gezeichnet (Transitivitätskanten weglassen).
- Schleifen entfallen.

Beispiele: Hesse-Diagramm des Poset der Teilbarkeitsrelation auf 28 (*Rechts*) und $(\mathcal{P}(\{a,b,c\}), \subseteq)$ (*Links*):



Spezielle Elemente

Sei $X \subseteq A$ in einer Halbordnung $(A, \preceq)$. Ein Element $x \in X$ heisst:

- **minimales Element:** $\forall y\ (y \preceq x \Rightarrow y = x)$
  (Knoten zu *denen* kein Pfeil zeigt)
- **kleinstes Element:** $\forall y\ (x \preceq y)$
  (Knoten von *dem* ein Pfeil zu jedem anderen zeigt)
- **maximales Element:** $\forall y\ (x \preceq y \Rightarrow y = x)$
  (Knoten von *denen* kein Pfeil ausgeht)
- **grösstes Element:** $\forall y\ (y \preceq x)$
  (Knoten zu *dem* jeder Pfeil zeigt)

Existenz in endlichen Mengen

Ist $X \subseteq A$ nichtleer und endlich, so existiert mindestens ein minimales und mindestens ein maximales Element in X.

Erweiterungen

Eine Halbordnung $(A, \preceq_A)$ erweitert eine Halbordnung $(B, \preceq_B)$, wenn gilt:

$$B \subseteq A,$$

$$\forall a, b \in B (a \preceq_B b \Rightarrow a \preceq_A b).$$

Man sagt: $(A, \preceq_A)$ *erweitert* $(B, \preceq_B)$.

Lineare Ordnungen

Eine *lineare Ordnung* (auch *totale Ordnung*) ist eine Halbordnung $(A, \preceq)$, in der alle Elemente vergleichbar sind:

$$\forall a, b \in A (a \preceq b \vee b \preceq a).$$

Das heisst, es gibt keine *unvergleichbaren* Paare mehr.

Satz von Marczewski–Szpilrajn

Jede Halbordnung $(A, \preceq)$ lässt sich zu einer linearen Ordnung $(A, \trianglelefteq)$ erweitern, die die ursprüngliche Ordnung bewahrt und *alle* Elemente vergleichbar macht.

Graphentheoretische Sicht

- Eine endliche Halbordnung kann als gerichteter azyklischer Graph (DAG) dargestellt werden.
- Eine *Linearisierung* entspricht einer *topologischen Sortierung* des DAGs.

Unendliche Mengen

Zwei Mengen A und B haben dieselbe Mächtigkeit (Kardinalität) $|A| = |B|$, genau dann, wenn eine bijektive Abbildung $f : A \longleftrightarrow B$ existiert. Eine Menge heisst endlich, falls sie bijektiv zu $\{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ ist; andernfalls heisst sie unendlich.

Wichtige Definitionen

- $|A| = |B|$: Existenz einer Bijektion $f : A \to B$.
- $|A| \leq |B|$: Es existiert eine injektive Abbildung $g : A \hookrightarrow B$ (äquivalent: surjektive Abbildung $B \twoheadrightarrow A$).
- $|A| = \infty$: Abkürzung dafür, dass A nicht endlich ist.
- $|\varnothing| \leq |A|$ für alle Mengen A.

Elementare Eigenschaften

- Die Relation $\sim$ mit $A \sim B \Leftrightarrow |A| = |B|$ ist eine Äquivalenzrelation.
- Für endliche Mengen A und B mit $|A| = n$ und $|B| = m$ gilt $|A| \leq |B| \iff n \leq m$.
- Eine Menge A ist genau dann unendlich, wenn $|\mathbb{N}| \leq |A|$.
- $A \subseteq B \Rightarrow |A| \leq |B|$. Umgekehrt: $|A| \leq |B|$ genau dann, wenn es $A' \subseteq B$ mit $|A'| = |A|$ gibt.

Satz von Cantor–Bernstein

Sind A und B nichtleer, dann gilt

$$(|A| \leq |B| \ \wedge\ |B| \leq |A|) \iff |A| = |B|.$$

(Dieser Satz liefert aus beidseitigen Injektionen eine Bijektion.)

Wichtige Folgerungen

- **Schubfachprinzip (Pigeonhole):** Aus $|A| \leq |B|$ und $|A| \neq |B|$ folgt $|B| \not\leq |A|$.
- **Dedekind:** A ist unendlich $\Leftrightarrow$ es existiert eine injektive, nicht surjektive Abbildung $f : A \hookrightarrow A$. z.B. die Abbildung $f : \mathbb{N}, n \mapsto n+1$.
- **Hilbert's Hotel (Anschaulichkeit):** Eine Menge A ist unendlich genau dann, wenn es eine echte Teilmenge $B \subset A$ mit $|B| = |A|$ gibt.

Abzählbare Mengen

Eine Menge A heisst *abzählbar*, wenn $A = \varnothing$ oder eine der folgenden (äquivalenten) Bedingungen erfüllt ist:

- $|A| \leq |\mathbb{N}|$
- Es existiert eine surjektive Funktion $f : \mathbb{N} \twoheadrightarrow A$.
- Es existiert eine injektive Funktion $f : A \hookrightarrow \mathbb{N}$.

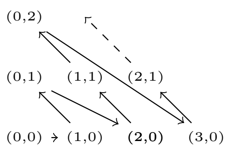
Bemerkung: Ist A abzählbar und unendlich, so gilt $|A| = |\mathbb{N}|$.

Beispiele

- Die leere Menge $\varnothing$ ist abzählbar.
- Jede Teilmenge $A \subseteq \mathbb{N}$ ist abzählbar (insbesondere $\mathbb{N}$ selbst).
- $\mathbb{Z}$ ist abzählbar.
- $\mathbb{Q}$ ist abzählbar (als Schlussfolgerung aus Abzählbarkeit von $\mathbb{Z} \times \mathbb{Z}$ und Quotientenbildung).

Wichtige Aussagen

- Jede endliche Menge ist abzählbar. (Beweis: Aufzählung der Elemente liefert eine surjektive Abbildung $\mathbb{N} \twoheadrightarrow A$.)
- Jede Teilmenge einer abzählbaren Menge ist abzählbar. (Bild- bzw. Einschränkungsargument.)
- Bild einer abzählbaren Menge unter einer surjektiven Abbildung ist abzählbar. (Komposition surjektiver Abbildungen.)
- $\mathbb{N} \times \mathbb{N}$ ist abzählbar. Daraus folgt die Abzählbarkeit von $\mathbb{Z} \times \mathbb{Z}$ und damit $\mathbb{Q}$.



- Jede abzählbare Vereinigung abzählbarer Mengen $\bigcup_{i \in \mathbb{N}} A_i$ ist abzählbar. (Beweisidee: doppelte Indizierung und Aufzählung aller Paare (i, n).)

Überabzählbare Mengen

- Es gibt verschiedene "Grössen" unendlicher Mengen; aus $|A| = \infty$ und $|B| = \infty$ folgt nicht notwendigerweise $|A| = |B|$.
- Es existiert eine unendliche *Hierarchie* von Kardinalitäten: Mengen $A_0, A_1, A_2, \ldots$ mit
$$|A_0| < |A_1| < |A_2| < \ldots$$
- Die Menge aller unendlichen Binärsequenzen $B = \{0,1\}^{\mathbb{N}}$ ist *nicht abzählbar.*

Sequenzen

Eine *Sequenz* in einer Menge A ist eine Abbildung $s : \mathbb{N} \to A$. Die Menge aller Sequenzen in A sei $A^{\mathbb{N}}$. Entspricht $s(0) = a_0$, $s(1) = a_1$, $s(2) = a_2$, …, so schreiben wir
$$s = (a_0, a_1, a_2, \ldots).$$

Unendliche Binärsequenzen

Eine *Binärsequenz* ist eine Funktion $s : \mathbb{N} \to \{0,1\}$. Die Menge aller Binärsequenzen sei $B = \{0,1\}^{\mathbb{N}}$.

Cantors Diagonalisierungsargument

Für jede Abbildung $f : \mathbb{N} \to B$ konstruiere man $s \in B$ durch
$$s_n := 1 - f(n)_n$$

$$\begin{aligned}
f(0) &= (a_0^0, a_1^0, a_2^0, \ldots a_n^0, \ldots) \\
f(1) &= (a_0^1, a_1^1, a_2^1, \ldots a_n^1, \ldots) \\
f(2) &= (a_0^2, a_1^2, a_2^2, \ldots a_n^2, \ldots) \\
&\vdots \\
f(n) &= (a_0^n, a_1^n, a_2^n, \ldots a_n^n, \ldots) \\
&\vdots
\end{aligned}$$

s unterscheidet sich von jedem Bild $f(n)$ in der n-ten Stelle. Somit ist $s \notin \mathrm{im}(f)$ und es gibt keine surjektive Abbildung $\mathbb{N} \to B$. Daher ist B nicht abzählbar.

Folgerungen

- Das Intervall $[0, 1)$ und damit $\mathbb{R}$ sind überabzählbar.
- Die Menge aller Funktionen $\mathbb{N} \to \mathbb{N}$ ist überabzählbar.
- Es existieren Funktionen $\mathbb{N} \to \mathbb{N}$, die nicht berechenbar sind.

Potenzmenge und Cantors Theorem

Für jede Menge A gilt streng:
$$|A| < |\mathcal{P}(A)|.$$

Begründung:

1. Es existiert eine Injektion $A \hookrightarrow \mathcal{P}(A)$, $x \mapsto \{x\}$, also $|A| \leq |\mathcal{P}(A)|$.
2. Für jede Abbildung $f : A \to \mathcal{P}(A)$ betrachte die Menge
$$\Delta_f := \{a \in A \mid a \notin f(a)\}.$$
$\Delta_f \in \mathcal{P}(A)$, aber $\Delta_f \notin \mathrm{im}(f)$ (diagonalisiertes Argument), also ist f nicht surjektiv. Damit $|\mathcal{P}(A)| \not\leq |A|$.

By Justin Iven Müller (2025)
github.com/JustinIven/zhaw-cheatsheets