WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

10-24-2003

Beispiel

$A_1 = \{2, 4, 6, 8\}$;

$A_2 = \{0, 2, 4, 6, \ldots\} = \{n \in \mathbb{N}_0; n \text{ gerade}\}$

Beispiel

$A_1 = \{2, 4, 6, 8\}$;
$A_2 = \{0, 2, 4, 6, \ldots\} = \{n \in \mathbb{N}_0; n \text{ gerade}\}$

Bezeichnungen:

$x \in A \Leftrightarrow A \ni x$	x Element A
$x \notin A$	x nicht Element A
$B \subseteq A$	B Teilmenge von A
$B \subsetneq A$	B echte Teilmenge von A
$\emptyset$	leere Menge, dagegen: $\{\emptyset\}$ — Menge, die als Element die leere Menge enthält

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \triangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt

Operationen auf Mengen:

- $A \uplus B$ Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^{n} A_i$ Vereinigung der Mengen $A_0, A_1, \ldots, A_n$
- $\bigcap_{i \in I} A_i$ Schnittmenge der Mengen A_i mit $i \in I$
- $\mathrm{P}(M) := 2^M := \{N; N \subseteq M\}$ Potenzmenge der Menge M

Operationen auf Mengen:

- $A \uplus B$ Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^{n} A_i$ Vereinigung der Mengen $A_0, A_1, \ldots, A_n$
- $\bigcap_{i \in I} A_i$ Schnittmenge der Mengen A_i mit $i \in I$
- $\mathrm{P}(M) := 2^M := \{N; N \subseteq M\}$ Potenzmenge der Menge M

Operationen auf Mengen:

- $A \uplus B$ Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^{n} A_i$ Vereinigung der Mengen $A_0, A_1, \ldots, A_n$
- $\bigcap_{i \in I} A_i$ Schnittmenge der Mengen A_i mit $i \in I$
- $\mathrm{P}(M) := 2^M := \{N; N \subseteq M\}$ Potenzmenge der Menge M

Operationen auf Mengen:

- $A \uplus B$ Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^{n} A_i$ Vereinigung der Mengen $A_0, A_1, \ldots, A_n$
- $\bigcap_{i \in I} A_i$ Schnittmenge der Mengen A_i mit $i \in I$
- $\mathrm{P}(M) := 2^M := \{N; N \subseteq M\}$ Potenzmenge der Menge M

Seien $A_1, A_2, \ldots, A_n$ Mengen. Eine Relation über $A_1, \ldots, A_n$ ist eine Teilmenge

$$R \subseteq A_1 \times A_2 \times \ldots \times A_n = \bigtimes_{i=1}^{n} A_i$$

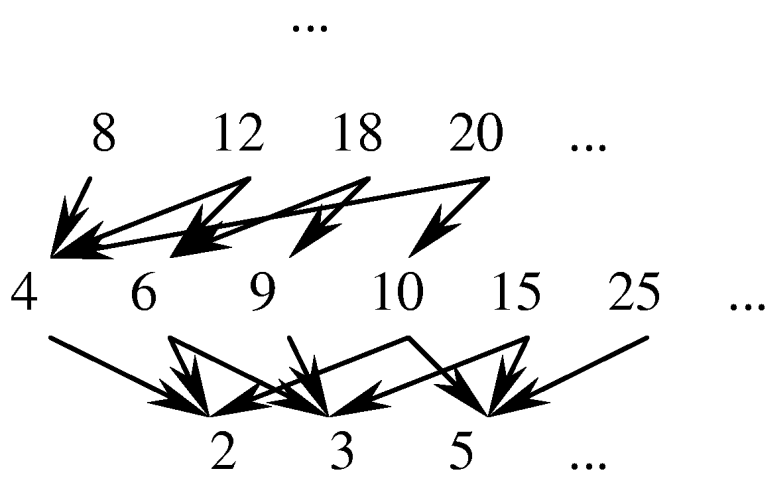
Andere Schreibweise (Infixnotation) für $(a, b) \in R$: aRb.
Eigenschaften von Relationen ($R \subseteq A \times A$)

- reflexiv: $(a, a) \in R \quad \forall a \in A$
- symmetrisch: $(a, b) \in R \Rightarrow (b, a) \in R \quad \forall a, b \in A$
- asymmetrisch: $(a, b) \in R \Rightarrow (b, a) \notin R \quad \forall a, b \in A$
- antisymmetrisch: $\big[(a, b) \in R \wedge (b, a) \in R\big] \Rightarrow a = b \quad \forall a, b \in A$
- transitiv: $\big[(a, b) \in R \wedge (b, c) \in R\big] \Rightarrow (a, c) \in R \quad \forall a, b, c \in A$
- Äquivalenzrelation: reflexiv, symmetrisch und transitiv
- Partielle Ordnung (aka *partially ordered set*, *poset*): reflexiv, antisymmetrisch und transitiv

Beispiel

$(a, b) \in R$ sei $a|b$ „a teilt b“.

Die graphische Darstellung ohne transitive Kanten heißt *Hasse-Diagramm*:



Die Relation | stellt eine *partielle Ordnung* dar.

Funktionen

Sei $f : A \to B$ eine *Funktion* von A nach B (also eine Relation mit genau einem Paar $\big(a, f(a)\big) \quad \forall a \in A$).

- Das *Urbild* von $b \in B$: $f^{-1}(b) = \{a \in A; f(a) = b\}$.
- Schreibweisen: $(A' \subseteq A, B' \subseteq B)$
- $f(A') = \bigcup_{a \in A'} \{f(a)\}$
- $f^{-1}(B') = \bigcup_{b \in B'} f^{-1}(b)$

Funktionen

Sei $f : A \to B$ eine *Funktion* von A nach B (also eine Relation mit genau einem Paar $\big(a, f(a)\big) \quad \forall a \in A$).

- Das *Urbild* von $b \in B$: $f^{-1}(b) = \{a \in A; f(a) = b\}$.
- Schreibweisen: $(A' \subseteq A, B' \subseteq B)$
- $f(A') = \bigcup_{a \in A'} \{f(a)\}$
- $f^{-1}(B') = \bigcup_{b \in B'} f^{-1}(b)$

Eigenschaften von $f : A \to B$:

- f injektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \leq 1\right]$
- f surjektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \geq 1\right]$
- f bijektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| = 1\right]$, d.h. injektiv und surjektiv
- Ist $f : A \to B$ eine Bijektion, dann ist auch f^{-1} eine bijektive Funktion.

Eigenschaften von $f : A \to B$:

- f injektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \leq 1\right]$
- f surjektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \geq 1\right]$
- f bijektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| = 1\right]$, d.h. injektiv und surjektiv
- Ist $f : A \to B$ eine Bijektion, dann ist auch f^{-1} eine bijektive Funktion.

Eigenschaften von $f : A \to B$:

- f injektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \leq 1\right]$
- f surjektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \geq 1\right]$
- f bijektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| = 1\right]$, d.h. injektiv und surjektiv
- Ist $f : A \to B$ eine Bijektion, dann ist auch f^{-1} eine bijektive Funktion.

Eigenschaften von $f : A \to B$:

- f injektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \leq 1\right]$
- f surjektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| \geq 1\right]$
- f bijektiv: $(\forall b \in B)\left[\left|f^{-1}(b)\right| = 1\right]$, d.h. injektiv und surjektiv
- Ist $f : A \to B$ eine Bijektion, dann ist auch f^{-1} eine bijektive Funktion.

Eigenschaften von $f : A \to B$:

- Existiert eine Bijektion von A nach B, haben A und B *gleiche Kardinalität*.
  Warnung: Es gibt A, B mit $A \subsetneq B$, aber $|\mathbb{Z}| = |\mathbb{N}_0|$! Beispiel:

$$f : \mathbb{Z} \ni z \mapsto \begin{cases} 2z & z \geq 0 \\ -2z-1 & z < 0 \end{cases} \in \mathbb{N}_0$$

- Sei R eine Relation über A, $\tilde{R}$ eine Relation über B. Eine Bijektion $f : A \to B$ heißt *Isomorphismus* zwischen R und $\tilde{R}$, falls gilt:

$$(a_1, \ldots, a_k) \in R \iff \Big(f(a_1), \ldots, f(a_k)\Big) \in \tilde{R}$$

Eigenschaften von $f : A \to B$:

- Existiert eine Bijektion von A nach B, haben A und B *gleiche Kardinalität*.
  Warnung: Es gibt A, B mit $A \subsetneq B$, aber $|\mathbb{Z}| = |\mathbb{N}_0|$! Beispiel:

$$f : \mathbb{Z} \ni z \mapsto \begin{cases} 2z & z \geq 0 \\ -2z-1 & z < 0 \end{cases} \in \mathbb{N}_0$$

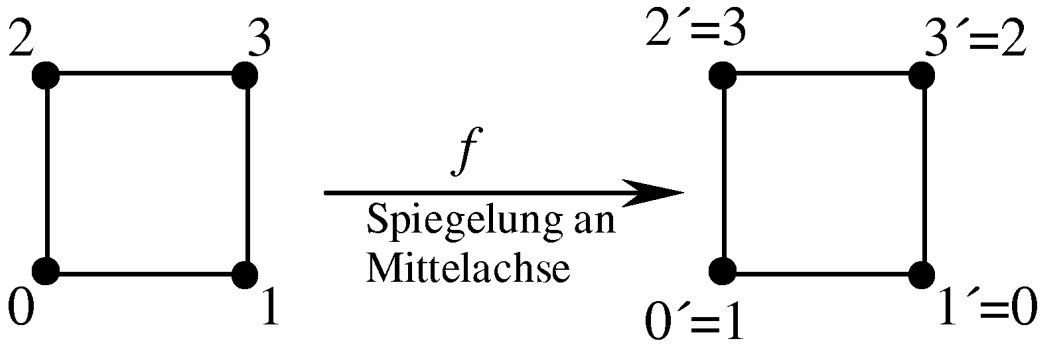
- Sei R eine Relation über A, $\tilde{R}$ eine Relation über B. Eine Bijektion $f : A \to B$ heißt *Isomorphismus* zwischen R und $\tilde{R}$, falls gilt:

$$(a_1, \ldots, a_k) \in R \iff \Big(f\big(a_1\big), \ldots, f\big(a_k\big)\Big) \in \tilde{R}$$

Beispiel

Relation: Kanten eines Graphen

$E = \{\{0,1\},\{0,2\},\{1,3\},\{2,3\}\}$



$E' = f(E) = \{\{0',1'\},\{0',2'\},\{1',3'\},\{2',3'\}\}$

f ist ein Isomorphismus.

Schreibweisen für wichtige Funktionen:

- $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lfloor x \rfloor := \max\{y \in \mathbb{Z}; y \leq x\} \in \mathbb{Z}$
  („untere Gaußklammer“, „*floor*“, „*entier*“)
- $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lceil x \rceil := \min\{y \in \mathbb{Z}; y \geq x\} \in \mathbb{Z}$
  („obere Gaußklammer“, „*ceiling*“)

Beispiel

$$\lfloor \pi \rfloor = 3, \lfloor -\pi \rfloor = -4, \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ 1 & \text{sonst} \end{cases}$$

Schreibweisen für wichtige Funktionen:

- $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lfloor x \rfloor := \max\{y \in \mathbb{Z}; y \leq x\} \in \mathbb{Z}$
  („untere Gaußklammer“, „*floor*“, „*entier*“)
- $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lceil x \rceil := \min\{y \in \mathbb{Z}; y \geq x\} \in \mathbb{Z}$
  („obere Gaußklammer“, „*ceiling*“)

Beispiel

$$\lfloor \pi \rfloor = 3, \lfloor -\pi \rfloor = -4, \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ 1 & \text{sonst} \end{cases}$$

Schreibweisen für wichtige Funktionen:

- $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lfloor x \rfloor := \max\{y \in \mathbb{Z}; y \leq x\} \in \mathbb{Z}$
  („untere Gaußklammer“, „*floor*“, „*entier*“)
- $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lceil x \rceil := \min\{y \in \mathbb{Z}; y \geq x\} \in \mathbb{Z}$
  („obere Gaußklammer“, „*ceiling*“)

Beispiel

$$\lfloor \pi \rfloor = 3, \lfloor -\pi \rfloor = -4, \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ 1 & \text{sonst} \end{cases}$$

Schreibweisen für wichtige Funktionen:

- $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lfloor x \rfloor := \max\{y \in \mathbb{Z}; y \leq x\} \in \mathbb{Z}$
  („untere Gaußklammer“, „*floor*“, „*entier*“)
- $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$
  $\mathbb{R} \ni x \mapsto \lceil x \rceil := \min\{y \in \mathbb{Z}; y \geq x\} \in \mathbb{Z}$
  („obere Gaußklammer“, „*ceiling*“)

Beispiel

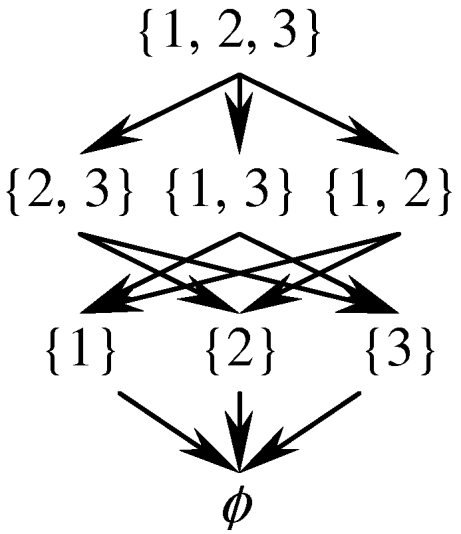
$$\lfloor \pi \rfloor = 3, \lfloor -\pi \rfloor = -4, \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ 1 & \text{sonst} \end{cases}$$

Sei $(S, \preceq)$ eine partielle Ordnung.

Beispiel

$S = \mathcal{P}(A),\ \preceq \equiv \subseteq,\ A = \{1, 2, 3\}$

Hassediagramm:



Eigenschaften partieller Ordnungen:

- $a, b \in S$ heißen *vergleichbar* (bzgl. $\preceq$), falls $a \preceq b$ oder $b \preceq a$, sonst *unvergleichbar*.
- Ein Element $a \in S$ heißt *minimal*, falls $(\nexists b \in S)[b \neq a \wedge b \preceq a]$.
- Ein Element $a \in S$ heißt *maximal*, falls $(\nexists b \in S)[b \neq a \wedge a \preceq b]$.
- Eine partielle Ordnung heißt *linear* oder *vollständig*, falls sie keine unvergleichbaren Elemente enthält $\big($z. B. $(\mathbb{N}_0, \leq)\big)$.

Eigenschaften partieller Ordnungen:

- $a, b \in S$ heißen *vergleichbar* (bzgl. $\preceq$), falls $a \preceq b$ oder $b \preceq a$, sonst *unvergleichbar*.
- Ein Element $a \in S$ heißt *minimal*, falls $(\nexists b \in S)[b \neq a \wedge b \preceq a]$.
- Ein Element $a \in S$ heißt *maximal*, falls $(\nexists b \in S)[b \neq a \wedge a \preceq b]$.
- Eine partielle Ordnung heißt *linear* oder *vollständig*, falls sie keine unvergleichbaren Elemente enthält $\big($z. B. $(\mathbb{N}_0, \leq)\big)$.

Eigenschaften partieller Ordnungen:

- $a, b \in S$ heißen *vergleichbar* (bzgl. $\preceq$), falls $a \preceq b$ oder $b \preceq a$, sonst *unvergleichbar*.
- Ein Element $a \in S$ heißt *minimal*, falls $(\nexists b \in S)[b \neq a \wedge b \preceq a]$.
- Ein Element $a \in S$ heißt *maximal*, falls $(\nexists b \in S)[b \neq a \wedge a \preceq b]$.
- Eine partielle Ordnung heißt *linear* oder *vollständig*, falls sie keine unvergleichbaren Elemente enthält $\big(\text{z. B. } (\mathbb{N}_0, \leq)\big)$.

Eigenschaften partieller Ordnungen:

- $a, b \in S$ heißen *vergleichbar* (bzgl. $\preceq$), falls $a \preceq b$ oder $b \preceq a$, sonst *unvergleichbar*.
- Ein Element $a \in S$ heißt *minimal*, falls $(\nexists b \in S)[b \neq a \wedge b \preceq a]$.
- Ein Element $a \in S$ heißt *maximal*, falls $(\nexists b \in S)[b \neq a \wedge a \preceq b]$.
- Eine partielle Ordnung heißt *linear* oder *vollständig*, falls sie keine unvergleichbaren Elemente enthält $\big($z. B. $(\mathbb{N}_0, \leq)\big)$.

- Direkter Beweis

Satz

1 Sei $n \in \mathbb{N}$ ungerade, dann ist auch n^2 ungerade.

Beweis.

$n \in \mathbb{N}$ ungerade $\Rightarrow (\exists m \in \mathbb{N}_0)\,[n = 2m + 1] \Rightarrow n^2 = (2m+1)^2 = \underbrace{\underbrace{4m^2 + 4m}_{\text{gerade}} + 1}_{\text{ungerade}} \Rightarrow n^2$ ungerade. $\square$

- Indirekter Beweis

  Wir wollen zeigen: $A \Rightarrow B$; wir zeigen stattdessen die (gleichwertige) kontrapositive Behauptung: $\neg B \Rightarrow \neg A$ (gleichwertig)

- Direkter Beweis

Satz

1 Sei $n \in \mathbb{N}$ ungerade, dann ist auch n^2 ungerade.

Beweis.

$n \in \mathbb{N}$ ungerade $\Rightarrow (\exists m \in \mathbb{N}_0)\,[n = 2m + 1] \Rightarrow n^2 = (2m+1)^2 = \underbrace{\underbrace{4m^2 + 4m}_{\text{gerade}} + 1}_{\text{ungerade}} \Rightarrow n^2$ ungerade. $\square$

- Indirekter Beweis

  Wir wollen zeigen: $A \Rightarrow B$; wir zeigen stattdessen die (gleichwertige) kontrapositive Behauptung: $\neg B \Rightarrow \neg A$ (gleichwertig)

- **Satz**
  Sei $n \in \mathbb{N}_0$: Falls n^2 gerade ist, dann ist auch n gerade.

  Beweis.
  Die Aussage ist gleichbedeutend mit „Falls $n \in \mathbb{N}_0$ ungerade, dann ist auch n^2 ungerade.“ Diese Aussage wurde (nach der trivialen Erweiterung von $\mathbb{N}$ auf $\mathbb{N}_0$) in Satz 1 bewiesen. $\square$

(C) Beweis durch Widerspruch

Wir nehmen an, dass die zu zeigende Aussage falsch ist und führen diese Annahme zu einem Widerspruch.

Satz

3 $\sqrt{3}$ *ist irrational, d. h.* $\sqrt{3} \notin \mathbb{Q}$

Beweis.

Widerspruchsannahme: $\sqrt{3} \in \mathbb{Q}$.

$$\Rightarrow \sqrt{3} = \frac{p}{q}, p, q \in \mathbb{N}, \mathrm{ggT}(p,q) = 1 \quad \textbf{(*)}$$

$$\Rightarrow 3q^2 = p^2 \Rightarrow 3|p \Rightarrow (\exists k \in \mathbb{N}_0)\,[p = 3k]$$

$$\Rightarrow 3q^2 = 9k^2 \Rightarrow q^2 = 3k^2 \Rightarrow 3|q \Rightarrow 3|\,\mathrm{ggT}(p,q)$$

Das ist ein Widerspruch zu **(*)**. □

(D) Vollständige Induktion

Wir wollen zeigen, dass eine Aussage $P(n)$ für alle $n \in \mathbb{N}_0$ gilt. Wir zeigen zunächst die *Induktionsvoraussetzung*, also $P(0)$, und folgern dann aus der Annahme $P(n)$ bzw. aus den Annahmen $P(0), P(1), \ldots, P(n)$ die Behauptung $P(n+1)$.

Satz

$$\sum_{i=0}^{n} i = \frac{n \cdot (n+1)}{2}$$

Beweis. Induktionsanfang: $n = 0$ trivial $0 = 0$
Induktionsannahme: $P(n)$, also Satz richtig für n
Induktionsschluss:

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i \; + n + 1 \overset{\text{(IV)}}{=} \frac{n \cdot (n+1)}{2} + n + 1 =$$

$$= \frac{2 \cdot (n+1) + n \cdot (n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Dies ist $P(n+1)$, die Behauptung für $n+1$. □

Das Schubfachprinzip (*pigeon hole principle*)

Satz

5 Sei $f : X \to Y$, *sei* $\infty > |X| > |Y| \geq 1$, *dann* $(\exists y \in Y)\left[|f^{-1}(y)| \geq 2\right]$.

Beweis.

Sei $|X| = n, |Y| = m$, damit $n > m$. Widerspruchsannahme: Kein $y \in Y$ hat mehr als ein Urbild in X. Die Bilder der ersten m Elemente aus X müssen dann notwendigerweise verschieden sein. Damit hat jedes $y \in Y$ ein Urbild in X. Das Bild des $(m+1)$-ten Elements aus X muss dann (f linkstotal) als Bild ein Element aus Y haben, das bereits Bild eines anderen $x \in X$ ist. Dies ist ein Widerspruch zur Annahme. □

Beispiele:

– Seien 13 oder mehr Personen in einem Raum. Dann haben mindestens 2 der Personen im gleichen Monat Geburtstag.

– Behauptung: In jeder Menge P von Personen ($|P| \geq 2$) gibt es immer mindestens 2 Personen, die gleich viele (andere) Personen in der Menge kennen („kennen“ symmetrische Relation).

Beweis.

1. Überlegung: Sei $n = |P|$. Wir betrachten die Abbildung $P \ni p \mapsto \#$ Personen, die p kennt $\in \{0, \ldots, n-1\}$
2. Weitere Überlegung:
   (a) 0 kommt als Bild nicht vor (jeder kennt mindestens eine andere Person).
   $\Rightarrow |\text{Urbildmenge}| = n > |\text{Bildmenge}| = n-1$. Das Schubfachprinzip liefert den Beweis.
   (b) 0 kommt als Bild vor.
   $\Rightarrow$ Es gibt also (wegen der Symmetrie) mindestens eine Person, die kein anderer kennt. Also ist der Wertebereich der Funktion $\subseteq \{0, 1, \ldots, n-2\}$. Das Schubfachprinzip liefert nunmehr ebenfalls den Beweis.

□

Das verallgemeinerte Schubfachprinzip

Satz

Sei $f : X \to Y, \infty > |X| \geq |Y| \geq 1$. *Dann existiert ein* $y \in Y$, *so dass*

$$\left|f^{-1}(y)\right| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil \ .$$

Beweis:

Es gilt $|X| = \left|\bigcup_{y \in Y} f^{-1}(y)\right| = \sum_{y \in Y} \left|f^{-1}(y)\right|$. Das zweite „=“ gilt, da die $f^{-1}(y)$ alle paarweise disjunkt sind! Widerspruchsannahme:

$$(\forall y \in Y)\left[\left|f^{-1}(y)\right| \leq \left\lceil \frac{|X|}{|Y|} \right\rceil - 1\right]$$

Dann gilt:

$$\left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \leq \frac{|X| + |Y| - 1}{|Y|} - 1 = \frac{|X| - 1}{|Y|}$$

Damit:

$$|X| = \sum_{y \in Y} \left|f^{-1}(y)\right| \leq |Y| \cdot \frac{|X| - 1}{|Y|} = |X| - 1$$

Dies stellt einen Widerspruch zur Annahme dar.

Ein Beispiel aus der Ramsey-Theorie:

Beispiel

In jeder Menge von 6 Personen gibt es 3 Personen, die sich gegenseitig kennen, oder 3 Personen, von denen keiner die beiden anderen kennt.

Beweis.

$P = \{p_1, p_2, \ldots, p_6\}$. Betrachte die Abbildung

$$\{2, \ldots, 6\} \to \{0, 1\}$$

$$\{2, \ldots, 6\} \ni i \mapsto \begin{cases} 1 & \text{„}p_1 \text{ kennt } p_i\text{“} \\ 0 & \text{„}p_1 \text{ kennt } p_i \text{ nicht“} \end{cases}$$

Aus dem verallgemeinerten Schubfachprinzip folgt: Es gibt mindestens 3 Leute $\in \{p_2, \ldots, p_6\}$, die p_1 kennen, oder es gibt mindestens 3 Leute, die p_1 nicht kennen.

O. B. d. A. kennt p_1 p_2, p_3 und p_4.

1. Fall:

$\big(\exists p_i, p_j \in \{p_2, p_3, p_4\}\big)\big[i \neq j$ und p_i kennt $p_j\big]$, z. B. $i = 2, j = 4$. Dann erfüllen $\{p_1, p_i, p_j\}$ den ersten Teil der Behauptung.

2. Fall:

$\big(\forall p_i, p_j \in \{p_2, p_3, p_4\}\big)\big[i \neq j \Rightarrow p_i$ kennt p_j nicht$\big]$. Dann erfüllen $\{p_2, p_3, p_4\}$ den zweiten Teil der Behauptung. □