1 Zahlensysteme

Umrechnen von Dezimalzahlen in andere Zahlensysteme

Die Dezimalzahl 338 wird ins 5er-System umgewandelt:

- 338 : 5 = 67 Rest 3
- 67 : 5 = 13 Rest 2
- 13 : 5 = 2 Rest 3
- 2 : 5 = 0 Rest 2
- Rückwärts gelesen: 2323

Umrechnen von anderen Zahlensystemen in Dezimalzahlen

Die Zahl 20022 (3er-System) wird ins Dezimalsystem umgewandelt:

- $2 * 3^0 = 2$
- $2 * 3^1 = 6$
- $0 * 3^2 = 0$
- $0 * 3^3 = 0$
- $2 * 3^4 = 162$
- 2 + 6 + 0 + 0 + 162 = 170

2 Zahlenmengen

- **Natürliche Zahlen**
  $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, ...\}$
- **Ganze Zahlen**
  $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- **Rationale Zahlen**
  $\mathbb{Q} = \left\{\frac{1}{2}, \frac{2}{3}, \frac{5}{4}, -\frac{3}{7}, 0, 1, -2, ...\right\}$
- **Reele Zahlen**
  $\mathbb{R} = \{-2, 0, 1.5, \sqrt{2}, \pi, e, ...\}$

3 Prädikate

Es sei n eine natürliche Zahl. Ein Ausdruck, in dem n viele (verschiedene) Variablen frei vorkommen und der bei Belegung (= Ersetzen) aller freien Variablen in eine Aussage übergeht, nennen wir ein n-stelliges Prädikat.

- $x > 3$ ist ein 1-stelliges Prädikat.
- $x + y = z$ ist ein 3-stelliges Prädikat.
- x ist eine natürliche Zahl 1-stelliges Prädikat.

3.1 Aussagen

Aussagen sind 0-stellige Prädikate. Sie sind entweder wahr oder falsch.

3.2 Quantoren

- $\forall A$ (Allquantor aka für jedes Element)
- $\exists A$ (Existenzquantor aka mind. ein Element)

3.3 Junktoren

- $A \neg B$ (Negation)
- $A \wedge B$ (Konjunktion)
- $A \vee B$ (Disjunktion)
- $A \Rightarrow B$ (Implikation)
- $A \Leftrightarrow B$ (Äquivalenz)

4 Gesetze und Umformungen

- Distributiv:
  - $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$
  - $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
- Assoziativ:
  - $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$
  - $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
- de Morgan:
  - $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

5 Aussonderung

Ist A eine Menge und ist E(x) eine Eigenschaft (ein Prädikat), dann bezeichnen wir mit dem Term:

$$x \in A \mid E(x)$$

Beispiel: Menge aller Geraden Zahlen:

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

6 Ersetzung

Ist A eine Menge und t(x) ein Ausdruck in x , dann schreiben wir

$$t(A) = \{t(x) \mid x \in A\}$$

für die Menge, die als Elemente alle Objekte von der Form t(x) mit x ∈ A enthält.

Beispiel: Menge aller Quadratzahlen

$$\{x^2 \mid x \in \mathbb{N}\}$$

7 Mengenoperationen

7.1 Teilmengen

Eine Menge A ist Teilmenge einer Menge B, geschrieben $A \subseteq B$, falls alle Elemente von A auch Elemente von B sind. Formal gilt:

$$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$$

Eine Teilmenge A von B ist eine echte Teilmenge, wenn $A \neq B$ gilt. Wir schreiben $A \subset B$, wenn A eine echte Teilmenge von B ist.

7.1.1 Extensionalitätsprinzip

Mithilfe der Teilmengenrelation lässt sich das Extensionalitätsprinzip wie folgt formulieren:

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

7.2 Potenzmengen

die Potenzmenge $\mathcal{P}(A)$ einer Menge A ist die Menge aller Teilmengen von A. Formal gilt:

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

Beispiel:

- $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $\mathcal{P}(\{\{a\}\}) = \{\emptyset, \{\{a\}\}\}$

Es gilt für beliebige Mengen A:

- $A \in \mathcal{P}(A)$, weil jede Megne eine Teilmenge von sich selbst ist.
- $\emptyset \in \mathcal{P}(A)$, weil die leere Menge Teilmenge jeder Menge ist.

! Sanity-Check: $\mathcal{P}(A)$ hat $2^{|A|}$ Elemente.

7.3 Verenigung

Die Verenigung von zwei Mengen beinhaltet genau die Elemente, die in mindestens einer der beiden Mengen enthalten sind. Formal gilt:

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

Beispiel:

- $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$
- $\mathbb{Z} = \{-n \mid n \in \mathbb{N} \cup \mathbb{N}\}$
- Möchte man beliebig viele Mengen vereinigen, d.h. alle Mengen, die Element einer beliebigen Menge M von Mengen sind, dann ist ein Existenzquantor nötig.

$$\bigcup_{A \in M} A := \{x \mid \exists A \in M(x \in A)\}$$

- Sind die Mengen die man vereinigen möchte indexiert, d.H. M ist in der Form $M = \{A_i \mid i \in I\}$, dann verwenden wir auch die folgenden Notation:

$$\bigcup_{i \in I} A_i := \bigcup_{A \in M} = \{x \mid \exists i \in I(x \in A_i)\}$$

Eigenschaften von $\cup$

- Kommutativität $A \cup B = B \cup A$
- Assoziativität $(A \cup B) \cup C = A \cup (B \cup C)$
- Idempotenz $A \cup A = A$
- $A \subseteq A \cup B$
- $A \subseteq B \Leftrightarrow B = A \cup B$

7.4 Schnittmengen

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

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

Beispiel:

- $\{1, 2, 3\} \cap \{2, 3, 4, 5\} = \{2, 3\}$
- $\mathbb{N} = \{r \in \mathbb{R} \mid r \geq 0\} \cap \mathbb{Z}$
- Möchte man beliebig viele Mengen schneiden, d.h. alle Mengen, die Element einer beliebigen Menge M von Mengen sind, dann ist ein Allquantor nötig.

$$\bigcap_{A \in M} A := \{x \mid \forall A \in M(x \in A)\}$$

- Wenn man sie indexiert haben möchte d.H. M ist in der Form $M = \{A_i \mid i \in I\}$, dann so:

$$\bigcap_{i \in I} A_i := \bigcap_{A \in M} A = \{x \mid \forall i \in I(x \in A_i)\}$$

Eigenschaften von $\cap$

- Kommutativität $A \cap B = B \cap A$
- Assoziativität $(A \cap B) \cap C = A \cap (B \cap C)$
- Idempotenz $A \cap A = A$
- $A \cap B \subseteq A$
- $A \subseteq B \Leftrightarrow A \cap B = A$

7.5 Disjunkte Mengen

- zwei Mengen A und B heissen **disjunkt**, wenn $A \cap B = \emptyset$ gilt.
- Eine Menge $M = \{A_i \mid i \in I\}$ von Mengen heissen **paarweise disjunkt**, wenn für alle aus $i \neq j$ gilt $A_i \cap A_j = \emptyset$ folgt.

7.6 Differenzmengen

Sind A und B Mengen, dann bezeichnen wir mit

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

die Differenz (A ohne B) von A und B

7.6.1 Interaktion von $\cup$,$\cap$ und $\setminus$

Sind A, B und C beliebige Mengen, dann gilt:

- De Morgan: $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$
- De Morgan: $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$
- Distributivität: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Distributivität: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

8 Relationen

8.1 Definition

Eine relation von A nach B ist ein Tripel $R = (G, A, B)$ bestehend aus:

- Einer (beliebigen) Menge A, genannt die Quellmenge der Relation.
- Einer (beliebigen) Menge B, genannt die Zielmenge der Relation.
- Einer Menge $G \subseteq A \times B$ genannt der Graph der Relation. Gilt $A = B$m dann nennen wir R eine homogene Relation auf A.

8.1.1 Notationen

- G_r ist der Graph
- (G, A, A) kann man auch als (G, A) schreiben.
- Ist $(x, y) \in G$, dann schreiben wir auch xRy und sagen x steht in Relation zu y.

8.2 Tupel und Produktmengen

8.2.1 Tupel

- Ein n-Tupel ist ein Objekt von der Form $(a_1, ..., a_n)$
- Der i-ten (für $1 \leq i \leq n$) Eintrag a_i eines Tupels $a = (a_1, ..., a_n)$ bezeichnen wir auch mit $a[i]$.

Damit Tupel gleich sind müssen sie genau die gleiche innere Struktur haben.

- $(1, 2, 3) \neq (1, 3, 2)$
- $(1, 2) \neq (1, 1, 2)$

8.2.2 Kartesisches Produkt

Das kartesische Produkt von Mengen $A_1, ..., A_n$, ist die Menge aller n-Tupel mit Einträgen aus $A_1, ..., A_n$

$$A_1 \times ... \times A_n := \{(a_1, ..., a_n) \mid a_1 \in A_1 \wedge ... \wedge a_n \in A_n\}$$

Beispiel:

- $\{1\} \times \{a, b\} = \{(1, a), (1, b)\}$
- $\mathbb{N}^2 \times \{0, 1\} = \{((x, y), 0) \mid x \in \mathbb{N} \wedge y \in \mathbb{N}\} \cup \{((x, y), 1) \mid x \in \mathbb{N} \wedge y \in \mathbb{N}\}$

8.2.3 Projektionen

Ist A eine Menge von n-Tupeln und ist $k \leq n$ eine natürliche Zahl, dann nennen wir die Menge

$$pr_k(A) = \{x[k] \mid x \in A\}$$

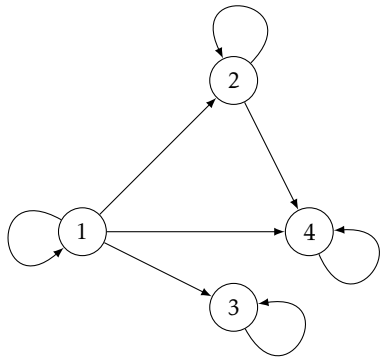
die k-te Projektion von A.

Beispiel:

- $pr_1(\{(a, b)\}) = \{a\}$
- $pr_1(\{(1, 2), (2, 7), (1, 5)\}) = \{1, 2\}$
- $pr_2(\{(1, 2), (2, 7), (1, 5)\}) = \{2, 7, 5\}$

8.3 Darstellung von Relationen

8.3.1 Gerichteter Graph



$xRy :\Leftrightarrow x$ teilt y

8.3.2 Domain

Es sei $R = (G, A, B)$ eine Relation.

- Die Domäne von R entpsricht der Projektion auf die erste Komponente vom Graph von R:

$$\text{dom}(R) = pr_1(G_R)$$

- Ist die Relation R als gerichteter Graph dargestellt, dann entspricht die Domäne der Menge aller Punkte, von denen mindestens ein Pfeil ausgeht.

8.3.3 Image

Es sei $R = (G, A, B)$ eine Relation. Die Bildmenge einer Relation R besteht aus den Elementen aus der Ziemlenge welche zu mind. einem Element aus der Quellmenge in Relation stehen:

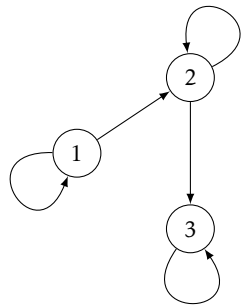
$$\text{im}(R) =: \{b \in B \mid \exists a \in A(aRb)\}$$

8.4 Klassifizierung von Relationen

8.4.1 Reflexivität

Eine (homogene) Relation R auf A heisst reflexiv, wenn jedes Element (aus der Quellmenge) mit sich selbst in Relation steht:

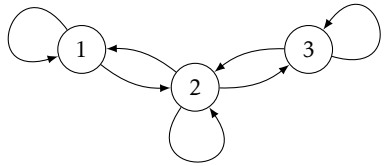
$$\forall x \in A(xRx)$$



8.4.2 Symmetrie

Eine (homogene) Relation R auf A ist symetrisch, falls:

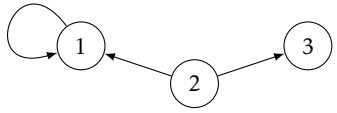
$$\forall x, y(xRy \Rightarrow yRx)$$



8.4.3 Antisymmetrie

Eine (homogene) Relation R auf A ist antisymetrisch, falls:

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



Ein Graph kann symmetrisch, antisymmetrisch, weder noch, oder beides zusammen sein.

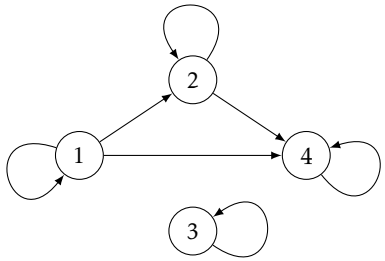
8.4.4 Transitivität

Eine (homogene) Relation R auf einer Menge A heisst transitiv, falls

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

gilt.

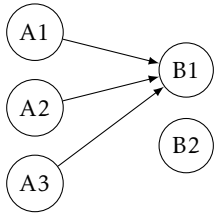
Ein Graph ist transitiv, wenn jede "Abkürzung" drin ist:



8.4.5 linksvollständig / linkstotal

Für $R = (G, A, B)$...

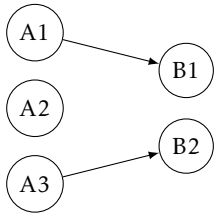
$$A = dom(R)$$



8.4.6 rechtsvollständig / rechtstotal

Für $R = (G, A, B)$...

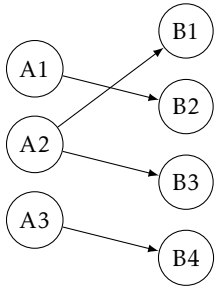
$$B = im(R)$$



8.4.7 linkseindeutig

Für $R = (G, A, B)$...

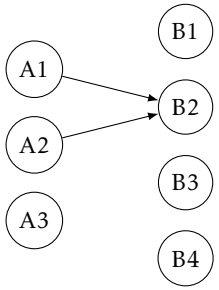
$$\forall x_1, x_2, y(x_1 R y \wedge x_2 R y \Rightarrow x_1 = x_2)$$



8.4.8 rechtseindeutig

Für $R = (G, A, B)$...

$$\forall x, y_1, y_2(xRy_1 \wedge xRy_2 \Rightarrow y_1 = y_2)$$



9 Funktionen →

Damit eine Relation eine Funktionen ist, muss sie folgende Eigenschaften haben:

- **rechtseindeutig**
- **linksvollständig**

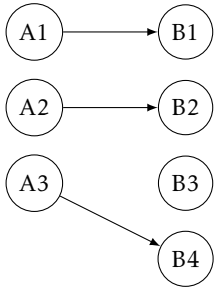
9.1 Injektive Funktionen ↪

Damit eine Funktionen injektiv ist muss sie folgende Eigenschaften haben:

- **linksvollständig**
- **rechtseindeutig**
- **linkseindeutig**

Eine Funktionen $f : A \to B$ heisst injektiv, falls unterschiedliche Ipunts stets in unterschiedlichen Outputs resultieren:

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

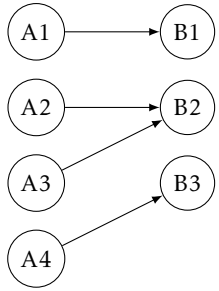


9.2 Surjektive Funktionen ↠

Damit eine Funktionen surjektiv ist muss sie folgende Eigenschaften haben:

- **linksvollständig**
- **rechtseindeutig**
- **rechtsvollständig**

Eine Funktion $f = (G, A, B)$ heisst surjektiv, falls $im(f) = B$ gilt.



9.3 Bijektive Funktionen ⇌

Damit eine Funktionen bijektiv ist muss sie folgende Eigenschaften haben:

- **linksvollständig**
- **rechtsvollständig**
- **rechtseindeutig**
- **linkseindeutig**

Oder anders gesagt: Eine Funktion $f : A \to B$ heisst bijektiv, falls sie sowohl injektiv als auch surjektiv ist.

9.4 Umkehrfunktionen

Für die Umkehrfunktionen einfach nach x auflösen und dann x und y vertauschen.
Eigenschaften von Umkehrfunktionen:

- Für jede Relation R gilt $R^{-1^{-1}} = R$
- R ist genau dann linksvollständig, wenn R^{-1} rechtseindeutig ist.
- R ist genau dann linkseindeutig, wenn R^{-1} rechtseindeutig ist.

9.5 Komposition

Für $g : A \to B$ und $f : B \to C$ definieren wir:

$$f \circ g : A \to C$$

$$(f \circ g)(x) = f(g(x))$$

Wörtlich sagt man auch "f nach g" da f nach g ausgeführt wird bzw. g zuerst ausgeführt wird.

9.5.1 Assoziativität

Für $f : A \to B$, $g : B \to C$ und $h : C \to D$ gilt:

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

9.5.2 Injektivität, Surjektivität und Komposition

Es seien $f : A \to B$ und $g : B \to C$ Funktionen.

- Sind f und g injektiv, so ist auch $g \circ f : A \to C$ injektiv.
- Sind f und g surjektiv, so ist auch $g \circ f : A \to C$ surjektiv.
- Sind f und g bijektiv, so ist auch $g \circ f : A \to C$ bijektiv.

10 Äquivalenzrelationen

Äquivalenzrelationen sind homogene Relationen, die...

- **reflexiv** xRx
- **symmetrisch** $xRy \Rightarrow yRx$
- **transitiv** $xRy \wedge yRz \Rightarrow xRz$

...sind.

10.1 Beispiele

- Die Gleichheitsrelation auf einer beliebigen Menge ist eine Äquivalenzrelation.
- Die Relation $\equiv_n$ ist auf der Menge $\mathbb{Z}$ durch:

  $$a \equiv_n b \Leftrightarrow n \text{ teilt } (a - b)$$

  11 ist kongruent 5 modulo 3 ($\equiv_3$), da 11 : 3 = 3 Rest 2 und 5 : 3 = 1 Rest 2 ist und somit die beiden Reste gleich sind.

10.2 Äquivalenzklassen

Es sei $\sim$ eine Äquivalenzrelation auf einer Menge A.

- Für $a \in A$ ist

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

  die Äquivalenzklasse von a bezüglich $\sim$ und beinhaltet alle Elemente von A, die zu a in Relation $\sim$ stehen.

- Jedes Element einer Äquivalenzklasse nennen wir einen Repräsentanten dieser Äquivalenzklasse.
- Die Faktormenge $A/_\sim$ von A modulo $\sim$ ist die Menge aller Äquivalenzklassen:

$$A/_\sim := \{[a]_R \mid a \in A\}$$

10.2.1 Eigenschaften

Ist $\sim$ eine Relation auf A, dann sind folgende Aussagen äquivalent:

- $a \sim b$
- $[a]_\sim = [b]_\sim$
- $[a]_\sim \cap [b]_\sim \neq \emptyset$
- $a \in [b]_\sim$
- $b \in [a]_\sim$

11 Halbordnungen

Eine Halbordnung ist eine...

- **reflexive**
- **transitive**
- **antisymmetrische**

...Relation.

11.1 Notation

Im Kontext von Ordnungsrelationen wird die Notation $R = (G, A)$ meistens A, G geschrieben.

11.1.1 Beispiele

- Ist A eine beliebige Menge, dann ist $\mathcal{P}(A), \subseteq$ eine Halbordnung.
- Die "normalen"kleiner oder gleich Relationen $(A, \leq)$ mit $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind Halbordnungen.

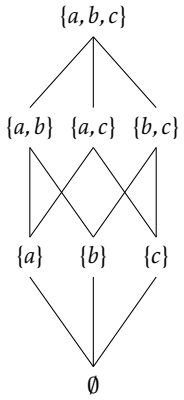
11.2 Hasse-Diagramme

Das Hasse-Diagramm einer Halbordnung $(A, \leq)$ ist eine vereinfachte Darstellung des gerichteten Graphen von $(A, \leq)$ und wird wie folgt konstruiert.

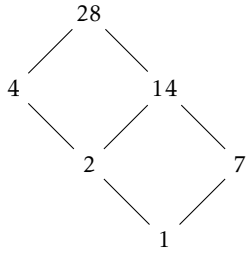
- Die Richtung eines Pfleies $a \to B$ für Elemte $a, b \in A$ wird dadurch zum Ausdruck gebracht, dass sich der Knoten b oberhalb von a befindet.
- Pfeile zwischen zwei Punkten a, b werden gelöscht, wenn es ein c mit $a \preceq c \preceq b$
- Pfeile, die von einem Punkt auf denselben Punkt zeigen (Schleifen), werden weggelassen.

11.2.1 Beispiel

Halbordnung $(\mathcal{P}(\{a, b, c\}), \subseteq)$



Teilbeitskeitrelation auf der Menge aller Teiler von 28:



11.3 Spezielle Elemente

Es sein $(A, \leq)$ eine Halbordnung und $X \subseteq A$. Ein Element $x \in X$ heisst (bezüglich $\leq$):

- minmales Element von X, falls:

$$\forall y \in X(y \leq x \Rightarrow y = x)$$

- kleinstes Element von X, falls:

$$\forall y \in X(x \leq y)$$

- maximals Element von X, falls:

$$\forall y \in X(y \leq x \Rightarrow y = x)$$

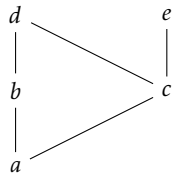
- grösstes Element von X, falls:

$$\forall y \in X(x \leq y)$$

11.3.1 Beispiel

Es sei die Halbordnung $\leq$ gemäss dem untenstehenden gerichteten Graph gegeben. Es gilt:

- maximale Elemente: d, e
- grösste Elemente: keine
- minimale Elemente: a
- kleinste Elemente: a



11.3.2 im Gerichteten Graph

- Maximale Elemente entsprechen den Knoten im gerichteten Graph von denen keine Pfeile weg zeigen (ausser Schleifen).
- Grösste Elemente entsprechen den Knoten im gerichteten Graph zu denen von jedem Knoten ein Pfeil hin zeigt.
- Minimale Elemente entsprechen den Knoten im gerichteten Graph zu denen keine Pfeile hin zeigen (ausser Schleifen).
- Kleinste Elemente entsprechen den Knoten im gerichteten Graph von denen zu jedem Knoten ein Pfeil zeigt.

12 Lineare Ordnungen

Es sei $A, \leq$ eine Halbordnung.

- Zwei Elemente a und b aus A werden als vergleichbar (bezüglich $\leq$) bezeichnet, falls entweder $a \leq b$ oder $b \leq a$ gilt.
- Elemente aus A , die nicht vergleichbar sind heissen unvergleichbar.
- Wenn alle Elemnte von A paarweise vergleichbar sind, dann heisst $A, \leq$ eine totale oder lineare Ordnung.

12.1 Beispiele

- Die Halbordnung $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq)und(\mathbb{R}, \leq)$ sind lineare Ordnungen.
- Die Halbordnung $\mathcal{P}(1, 2), \subseteq$ ist keine lineare Ordnung, da die Elemente {1} und {2} unvergleichbar sind.

12.2 Erweiterung

Definition Eine Halbordnung $(A, \leq A)$ erweitert die Halbordnung $(B, \leq B)$, falls

- $B \subseteq A$
- $\forall x, y \in B(x \leq_B y \Leftrightarrow x \leq_A y)$

gelten.

12.2.1 Beispiel

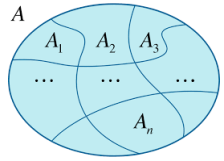
- $(\mathbb{N} \setminus \{0\}, \leq)$ erweitert die Teilbeitskeitrelation auf $\mathbb{N} \setminus \{0\}$.
- Die Relation $\mathcal{P}A, \leq$ mit

$$X \leq Y :\Leftrightarrow |X| \subseteq |Y|$$

erweitert die Teilmengenrelation auf $(\mathcal{P}(A), \subseteq)$.

13 Partition

Partitionen unterteilen eine gegebene Menge in paarweise disjunkte Teilmengen.



Eine Partition einer Menge A ist eine Menge $\{A_i | i \in I\}$ von paarweise disjunkten, nichtleeren Teilmengen von A mit

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

Die Elemente A_i heissen die Klassen der Partition.werden auch deren Blöcke genannt.

13.1 Beispiel

Durch $A_0 = \{2n \mid n \in \mathbb{N}\}$ und $A_1 = \{2n+1 \mid n \in \mathbb{N}\}$ erhält man eine Partition der natürlichen Zahlen in zwei unendlich grosse Blöcke.

13.2 Induzierte Partition

Folgt aus der Reflexivität einer Äquivalenzrelation und der Äquivalenz:

$$[a]_\sim = [b]_\sim \Leftrightarrow [a]_\sim \cap [b]_\sim \neq \emptyset$$

13.3 Induzierte Äquivalenzrelation

Ist $P = \{A_i \mid i \in I\}$ eine Partition einer Menge A, dann ist die Relation $\sim$ mit...

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

...eine Äquivalenzrelation auf A.

14 Unendliche Mengen

Eine Menge A ist nicht endlich, wenn $|A| = \infty$

14.1 Abzählbare Mengen

Eine Menga A heisst abzählbar, wenn $A = \emptyset$ oder es eine der folgenden (äquivalenten) Bedingungen erfüllt:

- $|A| = |\mathbb{N}|$
- Es gibt eine surjektive Funktion $f : \mathbb{N} \twoheadrightarrow A$
- Es gibt eine injektive Funktion $g : A \hookrightarrow \mathbb{N}$

Beispiele sind:

- $\{1, 2, 3\}$
- $\mathbb{N}$
- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{P}$

14.2 Überabzählbare Mengen

Überabzählbare Mengen sind nicht abzählbar. Beispiele sind:

- $\mathbb{R}$: reele Zahlen
- $\mathbb{C}$: komplexe Zahlen
- $\mathbb{I}$: imaginäre Zahlen
- $B(\infty)$: alle unendlichen Binärsequenzen
- $\mathcal{P}(\mathbb{N})$: Potenzmenge von $\mathbb{N}$

14.3 Satz von Canton-Bernstein

Für beliebige nichtleere Mengen A und B sind folgende Aussagen äquivalent:

- $|A| \leq |B| \wedge |B| \leq |A|$
- $|A| = |B|$

14.3.1 Schubfachprinzip

Aus $|A| > |B|$ und $|A| \neq |B|$ folgt $|B| \not\leq |A|$

14.3.2 Definition von Dedekind

Eine Menge A ist genau dann unendlich, wenn es eine injektive und nicht surjektive Funktion $f : A \hookrightarrow A$ gibt.

14.3.3 Hilberts Hotel

Eine Menga A ist genau dann unendlich, wenn eine echte Teilmenge $B \subset A$ mit $|A| = |B|$ existiert.

15 Die Peano Axiome

15.1 Axiom 1

0 ist eine natürliche Zahl.

15.2 Axiom 2

Jede natürliche Zahl k hat genau einen Nachfolger $k + 1$, der wiederum eine natürliche Zahl ist.

15.3 Axiom 3

Die Zahl 0 ist die einzige natürliche Zahl, die kein Nachfolger ist.

15.4 Axiom 4

Jede natürliche Zahl ist Nachfolger von höchstens einer natürlichen Zahl.

15.5 Axiom der vollständigen Induktion

Ist $A(n)$ eine Eigenschaft (ein Prädikat), sodass...

- **Induktionsverankerung (I.V.):** $A(0)$
- **Induktionsschritt (I.S.):** $\forall n \in \mathbb{N}(A(n) \Rightarrow A(n+1))$

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

16 Induktion

Es sei $A(n)$ eine Eigenschaft von natürlichen Zahlen:

- **Verankerung:** $A(n)$
- **Schritt:** $\forall n \in \mathbb{N} \quad \big(A(n) \implies A(n+1)\big)$

Induktionsannahme:

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

Induktions-Verankerung (IV, $n = 0$):

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

Zu zeigen:

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

Induktions-Schritt (IS, $n \to n+1$)

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

17 Rekursion

- **Verankerung:** $F(0) = c$
- **Schritt:** $F(n) = F(k+1) = G(\underbrace{F(k)}_{Selbsbezug}, k)$

Beispiel Expontenation von $\mathbb{N}$:

$$\begin{aligned}
F(0) &= & x^0 &= 1 \\
F(n) &= & x^n & \\
F(n+1) &= & (F(n), n) & \\
x^{n+1} &= & F(n) \cdot n & \\
x^{n+1} &= & x^n \cdot n &
\end{aligned}$$

18 Formale Aussagenlogik

18.1 Formale Definition

Die Syntax der Aussagenlogik (= Menge aller aussagenlogischen Formeln) ist durch $N(\{x_1, x_2, ...\}, \{and, or, not\})$ mit ...

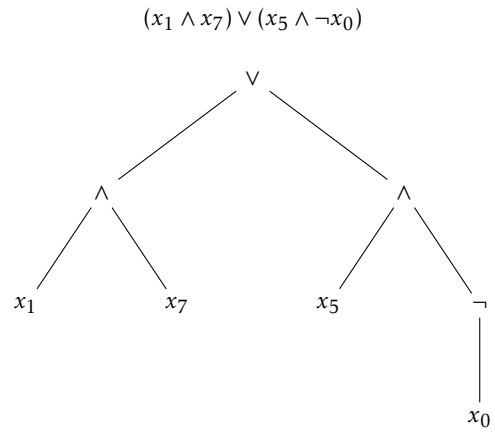
$$\begin{aligned}
and(A, B) &:= A \vee B \\
or(A, B) &:= A \wedge B \\
not(A) &:= \neg A
\end{aligned}$$

... gegeben.

18.1.1 Beispiele

- x_2
- $((x_1 \wedge x_7) \vee (x_5 \wedge \neg x_0))$
- $\neg\neg\neg(x_3 \wedge \neg x_5)$

18.2 Visualisierung



18.3 Strukturelle Rekursion

- $\wedge = min()$
- $\vee = max()$

$$
\begin{aligned}
&[\![(x_1 \wedge x_2) \vee x_3]\!]_3(1,1,0)\\
&= \max([\![x_1 \wedge x_2]\!]_3(1,1,0), [\![x_3]\!]_3(1,1,0))\\
&= \max(\min([\![x_1]\!]_3(1,1,0), [\![x_2]\!]_3(1,1,0)),0)\\
&= \max(\min(1,1),0)\\
&= \max(1,0)\\
&= 1
\end{aligned}
$$

18.4 Normalformen

18.4.1 Definition

- $K_0 := D_0 := \{x_1, x_2 \ldots\} \cup \{\neg x_1, \neg x_2 \ldots\}$
- $K_{n+1} := \{A_1 \wedge \cdots \wedge A_k \mid A_1 \ldots A_k \in D_n\}$
- $D_{n+1} := \{A_1 \vee \cdots \vee A_k \mid A_1 \ldots A_k \in K_n\}$

18.4.2 Beispiele

- $(\neg x_1 \wedge x_2) \vee x_3 \in D_2$
- $(\neg x_1 \vee x_2) \wedge (x_3 \vee x_1) \in K_2$

18.4.3 Bemerkung

Es gelten für alle $n \in \mathbb{N}$:

- $D_n \subsetneq K_{n+1} \cap D_{n+1}$
- $K_n \subsetneq D_{n+1} \cap K_{n+1}$

18.5 KNF und DNF

18.5.1 Definition

Die Formeln in K_2 sind in **konjunktiver Normalform (KNF)**, die Formeln in D_2 sind in **disjunktiver Normalform (DNF)**.

18.5.2 Satz

Zu jeder Formel A existieren äquivalente Formeln A_K in KNF und A_D in DNF.

18.6 Strukturelle Rekursion am Beispiel von tree(A)

Die Tiefe eines Baumes:

$$
\begin{aligned}
depth(a) &:= 0\\
depth(node(l,r)) &:= 1 + max(depth(l), depth(r))
\end{aligned}
$$

Die Summe aller "Blätter":

$$
\begin{aligned}
sumLeaf\,(a) &:= a\\
sumLeaf\,(node(l,r)) &:= sumLeaf\,(l) + sumLeaf\,(r)
\end{aligned}
$$

19 Teilbarkeitslehre

19.1 Teilbarkeitsrelation

Für $x, y \in \mathbb{Z}$ definieren wir:

- y ist genau dann ein Vielfaches von x, wenn eine ganze Zahl $t \in \mathbb{Z}$ mit $y = t \cdot x$ existiert.
- x ist genau dann ein Teiler y, wenn y ein Vielfaches von x ist. Wenn x ein Teiler von y ist, dann schreiben wir $x|y$.
- Die Menga aller natrürlichen Teiler $T(x) := \{n \in \mathbb{N} | n|x\}$ von der Zahl x besteht aus allen natrürlichen Zahlen, die x teilen.

19.1.1 Beispiele

- $T(-4) = \{1, 2, 4\}$
- $T(1) = \{1\}$
- $T(0) = \mathbb{N}$

19.2 Teilen mit Rest

Sind $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann gibt es höchstens ein Paar $(m, r) \in \mathbb{Z}^2$ mit:

- $a = mb + r$
- $0 \leq r < |b|$

19.3 Modulo Operator & Ganzzahlige Division

Die Funktion $mod : \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ und $div : \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$ sind so definiert , dass ...

$$
\begin{aligned}
a &= \mathrm{div}(a,b) \cdot b + \mathrm{mod}(a,b)\\
0 &\leq \mathrm{mod}(a,b) < |b|
\end{aligned}
$$

... gilt. Die Funktion mod nennt man Modulo Operator und die Funktion div entspricht für positive Zahlen der ganzzahligen Division.

19.3.1 Beispiele

- Es gilt $17 = 3 \cdot 5 + 2$ und daher $\mathrm{div}(17,5) = 3$ und $\mathrm{mod}(17,5) = 2$.
- Es gilt $22 = -3 \cdot -7 + 1$ und daher $\mathrm{div}(22,-7) = -3$ und $\mathrm{mod}(22,-7) = 1$.
- Es gilt $-22 = 4 \cdot -7 + 6$ und daher $\mathrm{div}(-22,-7) = 4$ und $\mathrm{mod}(-22,-7) = 6$.
- Es gilt $-22 = -4 \cdot 7 + 6$ und daher $\mathrm{div}(-22,7) = -4$ und $\mathrm{mod}(-22,7) = 6$.

19.4 Grösster gemeinsamer Teiler

Es seien $a, a_1, \ldots, a_n$ beliebige ganze Zahlen.

- $T(a_1, \ldots, a_n) := T(a_1) \cap \cdots \cap T(a_n)$ ist die Menge aller gemeinsamer natrürlichen Teiler der Zahlen $a_1, \ldots, a_n$.
- $ggT(a_1, \ldots, a_n) := \max(T(a_1, \ldots, a_n))$ ist der grösste gemeinsame Teiler der Zahlen. Eine der Zahlen muss jedoch von 0 verschieden sein.
- Zwei ganze Zahlen a, b heissen teilerfremd, wenn $ggT(a,b) = 1$ gilt.

19.5 Euklidischer Algorithmus

19.6 Lemma

Für beliebige ganze Zahlen a, b gilt:
$T(a,b) = T(a, b-a)$.

19.6.1 Folgerung

- Für ganze Zahlen a, b gilt: $ggT(a,b) = ggT(a, b-a)$.

- Für ganze Zahlen $b \geq a$, die nicht beide Null sind, gilt:
  $ggT(a,b) = ggT(a, mod(b,a))$
  $ggT(a,b) = ggT(mod(a,b), b)$.

19.6.2 Beispiel

$$
\begin{aligned}
ggT(25,45) &= ggT(25, mod(45,25))\\
&= ggT(25,20)\\
&= ggT(mod(25,20),20)\\
&= ggT(5,20)\\
&= ggT(5, mod(20,5))\\
&= ggT(5,0)\\
&= 5
\end{aligned}
$$

19.7 Lemma von Bézout

Sind $x, y \in \mathbb{Z}$ mit $(x,y) \neq (0,0)$, dann gibt es Zahlen a, b sodass

$$ggT(x,y) = ax + by$$

gilt. Die Zahlen a, b werden Bézout-Koeffizienten genannt.

19.7.1 Beispiel

Gleichung:

$$a \cdot 504 + b \cdot 29 = ggT(504, 29) = 1$$

Schritt 1: Sukzessives Teilen mit Rest.

$$
\begin{aligned}
504 &= 17 \cdot 29 + 11\\
29 &= 2 \cdot 11 + 7\\
11 &= 1 \cdot 7 + 4\\
7 &= 1 \cdot 4 + 3\\
4 &= 1 \cdot 3 + \underbrace{1}_{\mathrm{ggT}(504,29)}
\end{aligned}
$$

Schritt 2: "Rückwärts einsetzen".

$$
\begin{aligned}
1 &= 4 - 3\\
&= (11 - 7) - (7 - 4)\\
&= ((504 - 17 \cdot 29) - (29 - 2 \cdot 11))\\
&\quad - ((29 - 2 \cdot 11) - (11 - 7))\\
&= ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29)))\\
&\quad - ((29 - 2 \cdot (504 - 17 \cdot 29))\\
&\quad - ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29))))
\end{aligned}
$$

Schritt 3: Zusammenfassen (Zählen der Vorkommen von 504 und 29).

$$
\begin{aligned}
a &= 1 + 2 + 2 + 1 + 2 = 8\\
b &= -17 - 1 - (2 \cdot 17) - 1 - (2 \cdot 17) = -139
\end{aligned}
$$

Test:

$$8 \cdot 504 - 139 \cdot 29 = 1$$

20 Primzahlen

20.1 Definition

Eine natürliche Zahl $p \in \mathbb{N}$ ist eine Primzahl, wenn $|T(p)| = 2$ gilt. Die Menge aller Primzahlen nennen wir $\mathbb{P}$.

Eine natürliche Zahl $p > 1$ ist genau dann eine Primzahl, wenn $T(p) = \{1, p\}$ gilt.

20.2 Lemma von Euklid

Die folgenden Aussagen sind für $p \in \mathbb{N}$ äquivalent.

1. p ist eine Primzahl.
2. $\forall n, m \in \mathbb{N}(p|nm \Rightarrow p|n \vee p|m)$

20.3 Eindeutigkeit der Primfaktoren

Sind $p_1,\dots,p_m$ und $q_1,\dots,q_n$ Primzahlen mit

$$\prod_{i=1}^{m} p_i = \prod_{i=1}^{n} q_i$$

dann gilt $n = m$ und $p_i = q_i$ für alle $0 \le i \le n$

20.3.1 Folgerung

Es sei p_i jeweils die i-te Primzahl. Für jede natürliche Zahl $n > 1$ gibt es eine eindeutig bestimmte, endliche Folge $a_1,..,a_k$ von natürlichen Zahlen mit $a_k \neq 0$, so dass

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

gilt.

21 Kongruenz Modulo

21.1 Definition

- Für $n \in \mathbb{N}$ und $r,s \in \mathbb{Z}$ gilt:

$$r \equiv_n s \Leftrightarrow n|(r-s)$$

- Wir schreiben alternativ auch $r \equiv s \mod n$
- Für jede ganze Zahl z bezeichnen wir mit

$$[z]_n := \{x \in \mathbb{Z} | x \equiv_n z\}$$

  die Äquivalenzklasse von z bezüglich der Raltion $\equiv_n$ und nennen diese auch die **Restklasse** von z.

- Abkürzend bezeichnen wir $[z]_n$ auch mit $[z]$ oder $\overline{z}$, wenn n aus dem Kontext hervor geht.

21.2 Rechnen mit Restklassen

Für ganze Zahlen x,x' und y,y' gelten

- $[x] = [x'] \wedge [y] = [y'] \Rightarrow [x+y] = [x'+y']$
- $[x] = [x'] \wedge [y] = [y'] \Rightarrow [xy] = [x'y']$

21.2.1 Addition und Multiplikation

Die vorhergehende Bemerkung rechtfertigt die Repräsentatnetnweise Definition der Multiplikation und Addition auf Restklassen.

$$+ : \mathbb{Z}/n^2 \to \mathbb{Z}/n \quad \mapsto \quad [x]_n + [y]_n := [x+y]_n$$
$$\cdot : \mathbb{Z}/n^2 \to \mathbb{Z}/n \quad \mapsto \quad [x]_n \cdot [y]_n := [x \cdot y]_n$$

wobei

$$\mathbb{Z}/n = \mathbb{Z}/\equiv_n = \{[0]_n,[1]_n,\dots,[n-1]_n\}$$

Beispiele:

- $[17]_5 + [3]_5 = [20]_5 = [0]_5$
- $[2]_5 + [3]_5 = [5]_5 = [0]_5$
- $[17]_5 \cdot [3]_5 = [51]_5 = [1]_5$
- $[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$

21.3 Additive Inverse in $\mathbb{Z}/n$

21.3.1 Definition

Sind $x,y \in \mathbb{Z}/n$, dann ist x das additive Inverse von y, falls $x + y = [0]_n$ gilt.

21.3.2 Beispiel

In $\mathbb{Z}/7$ ist $[3]_7$ das additive Inverse von $[4]_7$, weil $[3]_7 + [4]_7 = [7]_7 = [0]_7$ gilt.

21.3.3 $a + x = b$

In $\mathbb{Z}/n$ gilt hat jedes Element ein additives Inverses, weswegen alle Gleichungen von der Form $a + x = b$ mit $a,b \in \mathbb{Z}$ lösbar sind.

Beispiel:
In $\mathbb{Z}/7$ hat die Gleichung

$$[3]_7 + x = [2]_7$$

die Lösung $x = [2 + (7-3)]_7 = [6]_7$.

21.4 Multiplikatives Inverse

21.4.1 Definition

Sind $x,y \in \mathbb{Z}/n$, dann ist x das **multiplikative Inverse** von y, falls $x \cdot y = [1]_n$ gilt. Falls x das multiplikative Inverse von y ist, dann bezeichnen wir x auch als y^{-1}.

21.4.2 Beispiel

In $\mathbb{Z}/7$ ist $[3]_7$ das multiplikative Inverse von $[5]_7$, weil $[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$ gilt.

21.5 Satz

In $\mathbb{Z}/n$existiert genau dann ein multiplikatives Inverses zu $[x]$, wenn $ggT(n,x) = 1$ gilt, Daraus folgt, dass in $\mathbb{Z}/n$ genau dann jedes Element ausser $[0]$ ein multiplikatives Inverses, wenn n eine Primzahl ist.

22 Chinesischer Restsatz

Sind $n_1,\dots,n_k \in \mathbb{N}$ paarweise teilerfremd und $y_1,\dots,y_k \in \mathbb{Z}$, dann hat das Gleichungssystem

$$\begin{aligned} x &\equiv_{n_1} y_1 \\ x &\equiv_{n_2} y_2 \\ &\vdots \\ x &\equiv_{n_k} y_k \end{aligned}$$

eine eindeutige Lösung in $\mathbb{Z}/(n_1,\dots,n_k)$.

22.1 Lösen simultaner Kongruenzen

Gegeben ein System simultaner Kongruenzen mit zwei Gleichungen:

$$\begin{aligned} x &\equiv_{n_1} y_1 \\ x &\equiv_{n_2} y_2 \end{aligned}$$

wobei n_1 und n_2 teilerfremd sind.

1. Bestimme mithilfe des Euklidischen Algorithmus Bézout Koeffizienten a und b mit $an_1 + bn_2 = 1$.
2. Setze $x_0 := y_1 bn_2 + y_2 an_1$.
3. Die resultierende Gleichung ist $x \equiv_{n_1 \cdot n_2} x_0$.

23 Beispiel

$$\begin{aligned} x &\equiv_7 3 \\ x &\equiv_5 2 \\ x &\equiv_9 6 \end{aligned}$$

23.1 Kleiner Fermat

Ist $p \in \mathbb{P}$ und a kein Vielfaches von p, dann gilt:

$$a^{p-1} \equiv_p 1$$