

Logik

Junktorenregeln

Doppel Negation: $\neg\neg A \Leftrightarrow A$

Kommutativität: $A \wedge B \Leftrightarrow B \wedge A$

$A \vee B \Leftrightarrow B \vee A$

Assoziativität: $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$

$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

$(A \wedge (B \wedge C)) \vee (A \wedge C) \Leftrightarrow A \wedge ((B \wedge C) \vee C)$

Distributivität: $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

$A \wedge ((B \wedge C) \vee (B \wedge D)) \Leftrightarrow (A \wedge (B \wedge C)) \vee (A \wedge (B \wedge D))$

$A \vee ((B \vee C) \wedge (B \vee D)) \Leftrightarrow (A \vee (B \vee C)) \wedge (A \vee (B \vee D))$

$(A \vee B) \wedge (C \vee D) \Leftrightarrow (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$

$(A \wedge B) \vee (C \wedge D) \Leftrightarrow (A \vee C) \wedge (A \vee D) \wedge (B \vee C) \wedge (B \vee D)$

$(A \wedge \neg B) \vee (\neg B \vee A) \Leftrightarrow (A \vee (\neg B \wedge A)) \wedge (\neg B \vee (\neg B \wedge A))$

De Morgan: $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

$(A \wedge \neg B) \Leftrightarrow \neg(\neg A \vee B)$

Kontraposition: $A \Rightarrow B \Leftrightarrow \neg A \vee B$

$\Leftrightarrow \neg B \Rightarrow \neg A$

Äquivalenz: $A \Leftrightarrow B \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$

$\Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A)$

Idempotenz: $A \wedge A \Leftrightarrow A$

$A \vee A \Leftrightarrow A$

Absorption: $A \wedge (A \vee B) \Leftrightarrow A$

$A \vee (A \wedge B) \Leftrightarrow A$

Tautologie (T): $A \vee A$ ist immer wahr

Widerspruch (\perp): $A \wedge \neg A$ ist immer falsch

Bindung: 1. \neg , 2. \wedge , 3. \vee , 4. \Rightarrow

Quantoren

All - Quantor	: $\forall x \rightarrow$ "für alle..." $\neg\forall x \rightarrow$ "nicht für alle..."
Existenz - Quantor	: $\exists x \rightarrow$ "es gibt mindestens ein..." $\neg\exists x \rightarrow$ "es gibt kein..."

Junktorenregeln

Quantoren binden stärker als Junktoren

Vertauschregel:	$\exists x A(x) \Leftrightarrow \neg\forall x \neg A(x)$
	$\forall x A(x) \Leftrightarrow \neg\exists x \neg A(x)$
	$\forall x \in M A(x) \Leftrightarrow \forall x (x \in M \wedge A(x))$
	$\exists x \in M A(x) \Leftrightarrow \exists x (x \in M \wedge A(x))$
Negation:	$\neg\exists x \in M A(x) \Leftrightarrow \forall x \in M \neg A(x)$
	$\neg\forall x \in M A(x) \Leftrightarrow \exists x \in M \neg A(x)$

Junktoren

		Implikation	
Zeichen	Prädikat	Bezeichnung	Beschreibung
\neg	$\neg A$	Negation	nicht A
\wedge	$A \wedge B$	Konjunktion	A und B
\vee	$A \vee B$	Disjunktion	A oder B
\Rightarrow	$A \Rightarrow B$	Implikation	wenn A dann B
\Leftrightarrow	$A \Leftrightarrow B$	Äquivalenz	A gleich B

Wahrheitstafel

z.B. $(P \vee \neg Q) \wedge \neg P$

P	Q	$\neg P$	$\neg Q$	$P \vee \neg Q$	$(P \vee \neg Q) \wedge \neg P$
1	1	0	0	1	0
1	0	0	1	1	0
0	1	1	0	0	0
0	0	1	1	1	1

Beispiele

P Menge aller Prüfungen und $E(x)$ Prädikat "x ist einfach"

Alle Prüfungen sind einfach: $\forall x \in P E(x)$

Eine Prüfung ist einfach: $\exists x \in P E(x)$

Keine Prüfung ist einfach: $\neg\exists x \in P E(x)$

Alle Prüfungen sind nicht einfach: $\forall x \in P \neg E(x)$

Nur eine Prüfung ist einfach: $(\exists x \in P E(x)) \wedge (\forall x, y \in P (E(x) \wedge E(y) \Rightarrow x=y))$

Nur eine Prüfung ist nicht einfach: $(\exists x \in P \neg E(x)) \wedge (\forall x, y \in P (\neg E(x) \wedge \neg E(y) \Rightarrow x=y))$

Nicht alle Prüfungen sind einfach: $\neg\forall x \in P E(x)$

Eine Prüfung ist nicht einfach: $\exists x \in P \neg E(x)$

Es gibt mind. 3 Elemente mit $P(x)$: $\exists x, y, z (P(x) \wedge P(y) \wedge P(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z)$

Es gibt max. 2 Elemente mit $P(x)$: $\forall x, y, z P(x) \wedge P(y) \wedge P(z) \Rightarrow (x=y \vee x=z \vee y=z)$

Prädikat

Eine Ausdruck, welcher unbekannte Variablen enthält. Bei Belegung geht der Ausdruck in eine Aussage über. Nach einer Belegung handelt es sich um ein 0-stelliges Prädikat.

Aussage

Ein "sprachliches Gebilde", welchem "wahr" oder "falsch" zugeordnet werden kann. Darf keine unbekannten

Variablen aufweisen, falls schon, müssen diese in einem Quantor vorkommen.

z.B. $\forall x \exists y P(x, y)$ (), $\forall x P(x, y)$ (), "x ist ungerade" (), "es gibt ein x mit $P(x)$ " () (Existenz-Quantor $\exists x$)

Semantik

\mathbb{V} : Menge aller Variablen
 \mathbb{A} : Menge aller atomaren Formeln
 \mathbb{IF} : Menge aller aussagenlogischen Formeln

Normalformen

Literale : atomare Formel (Variablen / Konstanten (T, \perp))

Negationsnormalform (NNF) : Keine Implikationen (\Rightarrow) und Negationen nur direkt beim Literal ($\neg p$)
z.B. $\neg F \vee G$

Disjunktivennormalform (DNF): Literale $L_{i,j}$

z.B. $(L_{1,1} \wedge L_{1,2} \wedge \dots) \vee (L_{2,1} \wedge L_{2,2} \wedge \dots) \vee (\dots)$

Konjunktivenormalform (KNF): Literale $L_{i,j}$

z.B. $(L_{1,1} \vee L_{1,2} \vee \dots) \wedge (L_{2,1} \vee L_{2,2} \vee \dots) \wedge (\dots)$

! DNF und KNF sind immer auch NNF.

DNF und KNF wenn alle Junktoren identisch sind oder nur eine Literale. ($p \vee (q \vee p_1)$) oder (p)

Umformung

NNF: 1. Implikation eliminieren mit $F \Rightarrow G = \neg F \vee G$

2. Negationen, welche nicht zu einem Literal gehören mit der De Morgan und Doppel Negation Regel eliminieren.

DNF/KNF: 1. Jede Formel in NNF kann mit der Distributivregel wahlweise in KNF oder DNF gebracht werden.

z.B.

$$\neg(P \Leftrightarrow Q) \equiv \neg((P \Rightarrow Q) \wedge (Q \Rightarrow P)) \quad \text{Äquivalenz}$$

$$\equiv \neg(\neg P \vee Q) \wedge (\neg Q \vee P) \quad \text{Kontraposition}$$

$$\equiv \neg(\neg P \vee Q) \vee \neg(\neg Q \vee P) \quad \text{De Morgan}$$

$$\equiv (P \wedge \neg Q) \vee (Q \wedge \neg P) \quad \text{De Morgan (in DNF)}$$

Formel ist in DNF und NNF. Mit der Distributiv Regel erhält man den KNF.

$$\equiv (P \vee (Q \wedge \neg P)) \wedge (\neg Q \vee (Q \wedge \neg P)) \quad \text{Distributivität}$$

$$\equiv (P \vee Q) \wedge (P \vee \neg P) \wedge (\neg Q \vee Q) \wedge (\neg Q \vee \neg P) \quad \text{Distributivität (in KNF)}$$

Teilformeln

echte Teilformel (nur ein Teil der Formel, nicht die ganze)				
p_0	q	p_1	$q \vee p_1$	$p_0 \rightarrow (q \vee p_1)$
0	0	0	0	1
...

atomare Formel (Variablen) unechte Teilformel

Konsequenz

F ist Konsequenz von G , falls F unter jeder Belegung wahr ist, unter der G wahr ist.

z.B. $\forall_B (\hat{B}(G) = \text{true} \Rightarrow B(F) = \text{true})$

Logisch äquivalent

F und G sind logisch äquivalent, wenn G und F unter jeder Belegung denselben Wahrheitswert annehmen.

$\forall_B (\hat{B}(G) = \text{true} \Leftrightarrow \hat{B}(F) = \text{true}) \Leftrightarrow F \equiv G$

Eigenschaften

Gültig / Wahr : Unter einer Belegung wahr $\rightarrow \hat{B}(A) = \text{true}$

Allgemeingültig : Alle Belegungen wahr $\rightarrow \forall \hat{B}(A) = \text{true}$

Unbefüllbar : Keine Belegung wahr $\rightarrow \forall \hat{B}(A) = \text{false}$

Erfüllbar : Mindestens eine Belegung wahr $\rightarrow \exists \hat{B}(A) = \text{true}$

Widerlegbar : Mindestens eine Belegung falsch $\rightarrow \exists \hat{B}(A) = \text{false}$

Belegung

Eine Belegung B ist eine Zuordnung von Variablen zu Wahrheitswerten. $B: \mathbb{V} \rightarrow \{\text{true}, \text{false}\}$

z.B. $(p \vee q) \wedge \neg p$, Belegung $B(p) = \text{true}$, Belegung $B(q) = \text{false}$

$$\hookrightarrow p \vee q = \text{true}, \neg p = \text{false}$$

Funktion \hat{B} ordnet jeder aussagenlogischen Formel ihren Wahrheitswert bezüglich dessen Belegung B zu.

z.B. Funktion $\hat{B}((p \vee q) \wedge \neg p) = \text{false}$

z.B. Von Belegung $B: \mathbb{V} \rightarrow \{\text{false}, \text{true}\}$ seien folgende Werte bekannt:

$$B(p) = B(q) = B(r) = B(s) = \text{true}$$

$$B(u) = B(v) = \text{false}$$

Bestimmung von \hat{B}

$$p \rightarrow s : \hat{B}(p \rightarrow s) = \hat{B}(\neg p \vee s) = \text{or}(\hat{B}(\neg p), \hat{B}(s)) = \text{true}$$

$$(u \rightarrow r) \wedge s : \text{and}((\text{or}(\hat{B}(\neg u), \hat{B}(r)), \hat{B}(s))) = \text{true}$$

für beliebige Variablen v gilt: $\hat{B}(v) = B(v)$

$$\hat{B}(\perp) = \text{immer false}$$

$$\hat{B}(T) = \text{immer true}$$

$$\hat{B}(F \wedge G) = \text{and}(\hat{B}(F), \hat{B}(G))$$

$$\hat{B}(F \vee G) = \text{or}(\hat{B}(F), \hat{B}(G))$$

$$\hat{B}(\neg F) = \text{not}(\hat{B}(F))$$

Mengen

Element

$y \in X$: y ist ein Element von X

$y \notin X$: y ist kein Element von X

z.B. $A = \{2, 3, 4, 5, 6, 7\}$, $3 \in A$, $9 \notin A$

Teilmenge

$X \subseteq Y$: X ist eine Teilmenge von Y , jedes Element von X ist auch ein Element von Y . ($X \subseteq Y \Leftrightarrow \forall x (x \in X \Rightarrow x \in Y)$)

z.B. $\{1, 2\} \subseteq \{1, 2\} \rightarrow$ alle echten Teilmengen sind auch Teilmengen

Ist $A \subseteq B$ so gilt: $A \cap B = A$, $A \cup B = B$, $A \cap (B \setminus A) = \emptyset$, $A \cap \emptyset = \emptyset$, $A \cup \emptyset = A$, $A \cup B \setminus A = B$

$X \subsetneq Y$: X ist eine echte Teilmenge von Y , X ist nicht die gleiche Teilmenge wie Y . ($X \subsetneq Y \Leftrightarrow X \subseteq Y \wedge X \neq Y$)

z.B. $\{1, 2\} \subsetneq \{1, 2, 3\} \rightarrow X$ enthält weniger Elemente als Y

! \emptyset ist Teilmenge jeder Menge, aber \emptyset ist nicht Element (\in) jeder Menge z.B. $\emptyset \in \{2\}$

Vereinigung

wobei
 $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$

Mehrere Mengen: $\bigcup_{j=1}^n A_j = A_1 \cup \dots \cup A_n$

z.B. $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $A \cup B = \{1, 2, 3, 4\}$, $\emptyset \cup A = A$

Venn-Diagramm



Komplement Darstellung mit definierenden Eigenschaften

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

$A = (A \setminus B) \cup B$

z.B. $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $A \setminus B = \{1\}$

$\mathbb{N} \setminus (\mathbb{N} \setminus \mathbb{Z})$, $\mathbb{N} \setminus \mathbb{Z} = \emptyset$ (\mathbb{Z} beinhaltet alle \mathbb{N}), $\mathbb{N} \setminus \emptyset = \mathbb{N}$



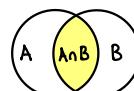
Schnittmenge

wobei
 $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$

Mehrere Mengen: $\bigcap_{j=1}^n A_j = A_1 \cap \dots \cap A_n$

z.B. $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $A \cap B = \{2, 3\}$, $\emptyset \cap A = \emptyset$

$\{3 \mid x \in \mathbb{N}\} \cap \{5 \mid x \in \mathbb{N}\} =$ alle \mathbb{N} die ein Vielfaches von 15 sind $\{15 \mid x \in \mathbb{N}\}$

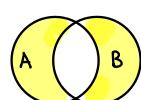


Symmetrische Differenz

$A \Delta B := (A \setminus B) \cup (B \setminus A)$

$= \{x \in A \cup B \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$

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



Disjunkt

$X \cap Y = \emptyset$: Mengen haben keine gemeinsamen Elemente

(A) (B) C nicht paarweise disjunkt ($A \cap B \cap C = \emptyset$)

(A) (B) C paarweise disjunkt

Mächtigkeit

Die Anzahl der Elemente einer Menge A heißt Mächtigkeit $|A|$ der Menge.

! Anzahl bezieht sich nur auf 1. Level: $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, |A|=3$

z.B. $A = \{1, 3, 5, 7, 9\}$, $|A|=5$ / $A = \{1, 2, 7\}$, $|A|=2$

$$|A|=2, |B|=3 \rightarrow |A^3 \times B^2| = 2^3 \cdot 3^2 = 72$$

Potenzmenge

Ist A eine beliebige Menge, dann bezeichnen wir mit $P(A) = \{X \mid X \subseteq A\}$ die Potenzmenge von A , die genau die Teilmengen von A als Element enthält.

$\emptyset \in P(A)$: jede Potenzmenge enthält die leere Menge.

z.B. $P(\{\emptyset\}) = \{\emptyset\} \neq \emptyset$, $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

$$P(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

$$P(\{a, \{c\}\}) = \{\emptyset, \{a\}, \{\{c\}\}, \{a, \{c\}\}\}$$

$$P(P(\{a\})) = P(\{\emptyset, \{a\}\}) = \{\emptyset, \{\emptyset\}, \{\{a\}\}, \{\emptyset, \{a\}\}\}$$

! Schema: {leer}, {einzelne Werte}, {Kombinationen}, {ganze Menge}

Mächtigkeit der Potenzmenge: $|P(A)| = 2^{|A|}$

z.B. Mächtigkeit der Potenzmenge der Menge $A = \{a, b\}$

1. Mächtigkeit der Menge $\rightarrow |A|=2$

2. Mächtigkeit der Potenzmenge $\rightarrow |P(A)| = 2^{|A|} = 2^2 = 4$

$$\hookrightarrow P(A) = \{\{\emptyset\}, \{a\}, \{b\}, \{a, b\}\}$$

Tupel

Eine geordnete Zusammenfassung von Objekten heißt Tupel.

Reihenfolge ist relevant: $(1, 2, 3) \neq (2, 1, 3)$

! Bei Mengen ist die Reihenfolge irrelevant: $\{1, 2, 3\} = \{2, 1, 3\}$

Rechenregeln

Kommutativität: $A \cap B \Leftrightarrow B \cap A$

$A \cup B \Leftrightarrow B \cup A$

Assoziativität: $A \cup (B \cup C) \Leftrightarrow (A \cup B) \cup C$

$A \cap (B \cap C) \Leftrightarrow (A \cap B) \cap C$

Distributivität: $A \cap (B \cup C) \Leftrightarrow (A \cap B) \cup (A \cap C)$

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

Idempotenz: $A \cap A \Leftrightarrow A$

$A \cup A \Leftrightarrow A$

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

$C \setminus (A \cup B) \Leftrightarrow (C \setminus A) \cap (C \setminus B)$

Bindung: 1. \wedge , 2. \cap , 3. \cup , 4. \setminus

Intervall

$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

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

$]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$

$[a, b[= \{x \in \mathbb{R} \mid a \leq x < b\}$

Falls Intervall nach links/rechts nicht begrenzt

so schreibt man $-\infty$ bzw. ∞ für a bzw. b

$]-\infty, b[= \{x \in \mathbb{R} \mid x < b\}$

Zahlen

\mathbb{N} : natürliche Zahlen $\{0, 1, 2, 3, \dots\}$

\mathbb{Z} : ganze Zahlen $\{\dots, -2, -1, 0, 1, 2, \dots\}$

\mathbb{Q} : rationale Zahlen $\{\dots, -\frac{2}{3}, -\frac{1}{2}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{2}, \frac{2}{3}, \dots\}$

\mathbb{R} : reelle Zahlen $\sqrt{2}, \pi, e, \dots$

Identische Mengen

Zwei Mengen X und Y sind gleich, wenn $X \subseteq Y$ und $Y \subseteq X$ gilt.

Kartesisches Produkt

Das kartesische Produkt $A \times B$ zweier Mengen A, B ist definiert als Menge aller geordneten Paare (a, b) , $a \in A, b \in B$. Es wird jedes Element aus A mit jedem Element aus B kombiniert. Es beschreibt alle möglichen Kombinationen aus Elementen von A und B .

$$\prod_{i=1}^n A_i$$

z.B. $A = \{1, 3\}$, $B = \{0, 2\}$

$$A \times B = \{(1, 0), (1, 2), (3, 0), (3, 2)\}$$

$$A^2 = \{(1, 1), (1, 3), (3, 1), (3, 3)\}$$

$$(B \times A) \times B \rightarrow B \times A = \{(0, 1), (0, 3), (2, 1), (2, 3)\}$$
$$= \{((0, 1), 0), ((0, 1), 2), ((0, 3), 0), ((0, 3), 2), ((2, 1), 0), ((2, 1), 2), ((2, 3), 0), ((2, 3), 2)\}$$

$A \times B \neq B \times A \rightarrow$ Tupel haben eine innere Ordnung

$$\{\emptyset\} \times \emptyset = \emptyset, \emptyset \times \{1\} = \emptyset, \{\emptyset\} \times \{1\} = \{(\emptyset, 1)\}, \{\emptyset\} \times \{\emptyset\} = \{(\emptyset, \emptyset)\}$$

Partitionen

Partition einer Menge ist die Zerlegung einer Menge in Teilmengen, sodass jedes Element der Menge in genau einer dieser Teilmengen enthalten ist.

Ein Element von P wird Block (Blöcke) genannt und erfüllen folgendes:

- Nicht leer und paarweise disjunkt
- Vereinigung der Teilmengen ergibt die Menge

z.B. Menge $A = \{1, 2, 3\}$

✓ Mögliche Partitionen: $P_1 = \{\{1\}, \{2, 3\}\} / P_2 = \{\{1, 2, 3\}\} / P_3 = \{\{1\}, \{2\}, \{3\}\}$

✗ Keine Partition: $Q = \{\{1, 2\}, \{2, 3\}\}$ von $A = \{1, 2, 3\}$

Abzählbar

Falls eine surjektive Funktion $F: \mathbb{N} \rightarrow X$ existiert

- Endliche Menge
- Jede Teilmenge einer endlichen Menge
- Kartesisches Produkt von abzählbaren Mengen
- Vereinigung (\cup) von abzählbaren Mengen

z.B. $\{1, 2, 3\}, \emptyset, \mathbb{P}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}$

Überabzählbar

Menge die nicht abzählbar ist

- Menge aller unendlichen Binärsequenzen
- Intervalle z.B. $[0, 1]$
- Potenzmengen z.B. von \mathbb{N} $\mathcal{P}(\mathbb{N})$
- Menge aller Funktionen z.B. $F: \mathbb{N} \rightarrow \mathbb{N}$

z.B. $\mathbb{I}, \mathbb{C}, \mathbb{R}, \mathbb{R} \setminus \mathbb{N}, \mathbb{R} \setminus \mathbb{Q}, (0, 1)$

Abzählbar / Überabzählbar Beweis

Sei $X \cup Y$ überabzählbar, können Sie etwas über die Abzählbarkeit von X und Y sagen?

$X \cup Y$ überabzählbar $\Rightarrow X$ überabzählbar \vee

Y überabzählbar

■ Kontraposition:

X abzählbar $\wedge Y$ abzählbar $\Rightarrow X \cup Y$ abzählbar

Mindestens eines muss überabzählbar sein.

Sei $X \setminus Y$ abzählbar und X überabzählbar, können Sie etwas über die Abzählbarkeit von Y sagen?

$X \setminus Y$ abzählbar $\wedge X$ überabzählbar $\Rightarrow Y$ überabzählbar

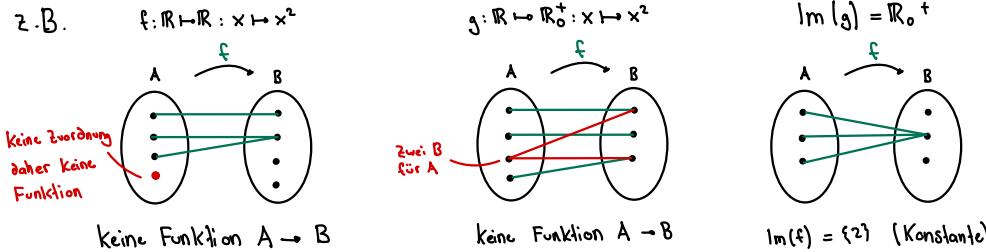
■ Kontraposition:

Y abzählbar $\Rightarrow X \setminus Y$ überabzählbar $\vee X$ abzählbar

Y muss überabzählbar sein.

Funktionen

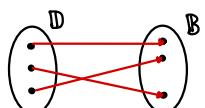
Funktion ist eine Beziehung zwischen zwei Mengen, die jedem Element der einen Menge genau ein Element der anderen Menge zuordnet.
Zu jedem $x \in A$ gibt es ein eindeutig bestimmtes $y \in B$ mit (x, y) .



Bijektiv

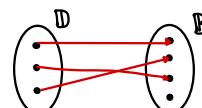
Funktion $f: \mathbb{D} \rightarrow \mathbb{B}$, $x \mapsto y = f(x)$ heißt bijektiv, falls jedes Element in der Bildmenge B genau einmal getroffen wird.

Eine Funktion ist bijektiv, falls sie injektiv und surjektiv ist.



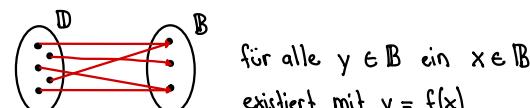
Injektiv

Funktion $f: \mathbb{D} \rightarrow \mathbb{B}$, $x \mapsto y = f(x)$ heißt injektiv, falls jedes Element in der Bildmenge B höchstens einmal getroffen wird.
Falls $f: X \rightarrow Y$ und $g: Y \rightarrow Z$ injektiv sind, ist auch $g \circ f: X \rightarrow Z$ injektiv.



Surjektiv

Funktion $f: \mathbb{D} \rightarrow \mathbb{B}$, $x \mapsto y = f(x)$ heißt surjektiv, falls jedes Element in der Bildmenge B mindestens einmal getroffen wird.
Falls $f: X \rightarrow Y$ und $g: Y \rightarrow Z$ surjektiv sind, ist auch $g \circ f: X \rightarrow Z$ surjektiv.



für alle $y \in \mathbb{B}$ ein $x \in \mathbb{D}$
existiert mit $y = f(x)$

Umkehrfunktion / Inversfunktion

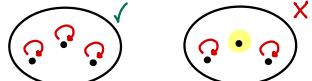
Die Funktion muss injektiv sein $f^{-1}(x)$. Anhand des Funktionsbildes kann die Umkehrfunktion erstellt werden.

Relationen

Reflexiv

Alle Elemente stehen immer mit sich selbst in Beziehung.

xRx



Symmetrisch

Zwei Elemente stehen immer wechselseitig in Beziehung zueinander.

$xRy \Rightarrow yRx$



Anti-Symmetrisch

Zwei Elemente stehen niemals wechselseitig in Beziehung zueinander, es sei denn es handelt sich um die gleichen Elemente.

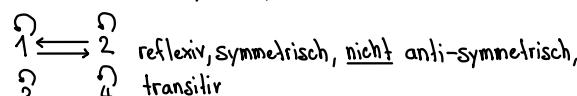
$xRy \wedge yRx \Rightarrow x=y$



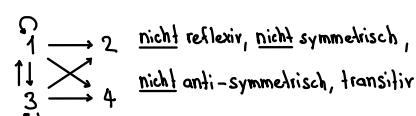
Beispiel

Menge A = {1, 2, 3, 4}

$R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$



$(x,y) \in R_2$, wenn $x+2y$ ungerade ist



Äquivalenzklassen

Sei R eine Äquivalenzrelation auf Menge X und $x \in X$. Die Äquivalenzklasse $[x]_R$ von x bezüglich R, ist die Menge aller Elemente von X, die zu x in Relation R stehen. $[x]_R := \{y \in X | xRy\}$ paarweise disjunkt, nicht leer, Vereinigung gibt X

Repräsentanten

Faktormenge

Faktormenge X/R von X modulo R ist Menge aller Äquivalenzklassen.

$X/R := \{[x]_R | x \in X\}$

$$\text{z.B. } \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} \quad \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} \quad \begin{array}{c} A = \{0, 1, 2, 3\}, R = \{(0,0), (1,1), (1,2), (2,1), (2,2), (3,3)\} \\ [0]_R = \{0\}, [1]_R = \{1, 2\}, [2]_R = \{3\} \\ A/R = \{[0]_R, [1]_R, [2]_R\} \end{array}$$

äquivalente Elemente

Transitiv

Wenn es einen Pfeil von x nach y und y nach z gibt, gibt es einen Pfeil von x nach z. Die Elemente stehen immer in einer Dreiecksbeziehung zueinander.

$xRy \wedge yRz \Rightarrow xRz$



Äquivalenzrelationen

Identifizierung ähnlicher Relationen. Müssen reflexive, symmetrische und transitive Relationen sein. Ist \sim eine Äquivalenzrelation auf einer Menge X und gilt $x, y \in X$ mit $x \sim y$ dann gilt $[x]_{\sim} = [y]_{\sim}$

! Äquivalente Elemente repräsentieren stets dieselbe Äquivalenzklasse.

Wohldefiniert

\sim Relation ist nicht wohldefiniert.

z.B. $\mathbb{Q} \rightarrow \mathbb{Z}$, $\frac{m}{n} \mapsto m$ nicht wohldefiniert

$$\left. \begin{aligned} f(\frac{5}{4}) &= 5 \\ f(\frac{10}{8}) &= 10 \end{aligned} \right\} \frac{5}{4} = \frac{10}{8} \quad \text{Bild muss eindeutig sein}$$

Lösung das wohldefiniert: z.B. fordern das Bruch vollständig gekürzt ist und n natürliche Zahl ist.

Beispiel Modulo Äquivalenzrelation

$x \equiv_5 y \Leftrightarrow (x-y)$ ist ein Vielfaches von 5

$\Leftrightarrow x \equiv_5 y \pmod{5} \Leftrightarrow x-y \Leftrightarrow \exists k \in \mathbb{Z} : x-y = k \cdot 5$

z.B. $3 \equiv_5 8 \rightarrow 3-8 = -5 \quad \text{OK}, [3] \equiv_5 \{8\}$

! Restklasse 3 von modulo 5 mit 8

Reflexivität: $x-x = 0 = 0 \cdot 5 \Rightarrow x \sim x$, da $0 \in \mathbb{Z}$

Symmetrie: $x \sim y \Rightarrow \exists k \in \mathbb{Z} : x-y = k \cdot 5$

$$\Rightarrow -(y-x) = k \cdot 5$$

$$\Rightarrow y-x = (-k) \cdot 5$$

$$\Rightarrow y \sim x, -k \in \mathbb{Z} \text{ weil } k \in \mathbb{Z}$$

Transitivität: $x \sim y \Rightarrow \exists k_1 \in \mathbb{Z} : x-y = k_1 \cdot 5$

$$\Rightarrow y = x - k_1 \cdot 5$$

$$y \sim z \Rightarrow \exists k_2 \in \mathbb{Z} : y-z = k_2 \cdot 5$$

$$\Rightarrow y = z + k_2 \cdot 5$$

$$\Rightarrow x - k_1 \cdot 5 = z + k_2 \cdot 5$$

$$\Rightarrow x - z = k_2 \cdot 5 + k_1 \cdot 5$$

$$\Rightarrow x - z = (k_2 + k_1) \cdot 5, k_1 \text{ und } k_2 \in \mathbb{Z}, \text{ also ist auch } k_1 + k_2 \in \mathbb{Z}$$

$$\mathbb{Z}/_5 = \{[0] \equiv_5, [1] \equiv_5, [2] \equiv_5, [3] \equiv_5, [4] \equiv_5\}$$

Binäre Relation

Relation zwischen zwei Elementen einer Menge.

xRy für $x, y \in R$

DAG (Directed Acyclic Graph)

Gerichteter, zyklusfreier (keine Wiederholung) Graph mit mind. einer topologischen Sortierung. z.B. Hasse-Diagramm

Kreuztabelle / Digraph

z.B. $A = \{1, 2, 3, 4\}, R = \{(1,2), (2,3), (3,4)\}$

	1	2	3	4
1	X			$1 \rightarrow 2$
2		X		
3			X	$3 \rightarrow 4$
4				

Ordnungsrelation (kleinste Ordnungsrelation → Präordnung)

Zusammenfassung von Relationsarten, mithilfe deren man Objekte vergleichen oder sortieren kann.

R-unvergleichbar: Zwei Elemente $x, y \in M$, falls weder $x R y$ noch $y R x$ gilt.

Beispiel 1: $(3,5), (3,10), \dots$ 3 teilt 5 nicht und 5 teilt 3 nicht, 3 teilt 10 nicht und 10 teilt 3 nicht

Beispiel 2: $(z,u), (y,z), \dots$ zwei Knoten haben keinen Pfeil direkten oder indirekten Pfeil

R-minimal

: Ein Element $x \in X$ einer Teilmenge $X \subseteq M$, falls es kein anderes Element $y \in X$ mit $x R y$ gibt.

Beispiel 1: keine wegen Reflexivität, da jede Zahl sich selbst teilt, es gibt keine Zahl die nur andere teilt

Beispiel 2: a, x keine Pfeile enden an diesen Knoten. Alle Pfeile dieser Knoten zeigen weg

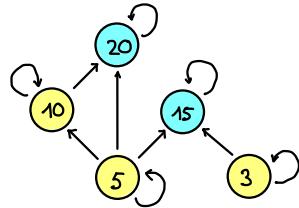
R-maximal

: Ein Element $x \in X$ einer Teilmenge $X \subseteq M$, falls es kein anderes Element $y \in X$ mit $y R x$ gibt.

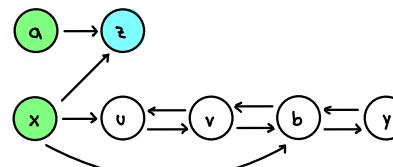
Beispiel 1: $15, 20$ sind keine Teiler einer anderen Zahl in M

Beispiel 2: z auf diesen Knoten führen Pfeile hin, aber keine weg

Beispiel 1: "x teilt y", $\subseteq M \times M$ mit $M = \{3, 5, 10, 15, 20\}$



Beispiel 2:



Ordnungstypen

Präordnung

: Ist reflexiv und transitiv

z.B. Teilrelation \mid auf \mathbb{Z} , reflexiv, transitiv aber nicht anti-symmetrisch ($5 \mid -5, -5 \mid 5$ aber $5 \neq -5$)

: R ist reflexiv, anti-symmetrisch und transitiv

z.B. Teilrelation \mid auf \mathbb{N} , da es R-unvergleichbare Elemente gibt.

A eine Menge von Mengen, dann ist Teilmenge-Relation \subseteq eine Halbordnung

: R ist eine Halbordnung und es existieren keine R-unvergleichbaren Elemente

z.B. $\lessdot \subseteq \{x \in \mathbb{R} \mid 0 < x < 1\}$ die Menge hat kein kleinstes Element und alle sind mit \lessdot vergleichbar, $\lessdot \subseteq \mathbb{Z}$

: R ist eine Totaleordnung und jede Teilmenge von M hat mind. ein R-minimales Element

z.B. $\leq \subseteq \mathbb{N}$

Abschlüsse

Transitiver-Abschluss

: Kleinste (bezüglich \subseteq) transitive Relation, welche R als Teilmenge enthält. R^+

z.B. R gegeben durch zwei Tupel (a,b) und (b,c) , R^+ enthält zusätzlich (a,c)

Reflexiv-Transitiver-Abschluss

: Kleinste Relation, welche R^+ enthält und reflexiv ist. R^*

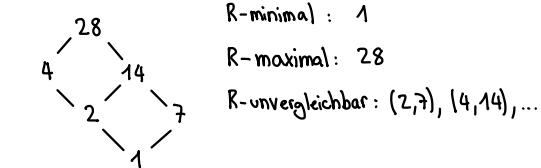
z.B. R^* enthält zusätzlich $(a,a), (b,b), (c,c)$

Hasse-Diagramm

Eine vereinfachte Darstellung einer Halbrelation.

- Pfeile werden weggelassen, Graph geht nach "oben"
- Verbindung zwischen zwei Punkten werden weggelassen, wenn es bereits eine "indirekte Verbindung" gibt
- Verbindung von einem Punkt zu sich selbst wird weggelassen

z.B. Teilbarkeitsrelation auf der Menge der Teilmengen von 28 ($\{1, 2, 4, 7, 14, 28\}$)



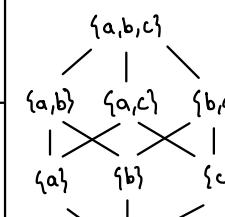
R-minimal: 1

R-maximal: 28

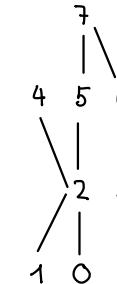
R-unvergleichbar: $(2,7), (4,14), \dots$

Teilmengenrelation \subseteq auf

der Menge $P(\{a, b, c\})$



Gegebenes Diagramm:

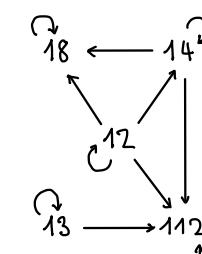


R-minimal: 0, 1, 3

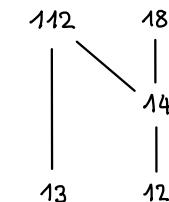
R-maximal: 4, 7

R-unvergleichbar: $(1,0,3), (4,5,6), \dots$

Diagramm zu Hasse-Diagramm:



12 → 112 entfernen
weil indirekt über 14



R-minimal: 13, 12

R-maximal: 112, 18

R: $\{(12,12), (13,13), (14,14), (18,18), (112,112), (13,112), (12,112), (12,18)\}$

Vollständige Induktion

Rekursive Definition

z.B. $a_n = 3n + 7$ für alle $n \in \mathbb{N}$

$$\begin{aligned}1. \quad a_0 &= 3 \cdot 0 + 7 = 7 \\2. \quad a_{n+1} &= 3(n+1) + 7 \\&= 3n + 3 + 7 \\&= \underline{\underline{3n+7}} + 3 \\a_{n+1} &= a_n + 3, \quad a_0 = 7\end{aligned}$$

z.B. $c_n = (n-1)2^{n+1} + 2$ für alle $n \in \mathbb{N}^*$

$$\begin{aligned}1. \quad c_1 &= (1-1)2^{1+1} + 2 = 2 \\2. \quad c_{n+1} &= ((n+1)-1) \cdot 2^{n+1+1} + 2 \\c_{n+1} &= ((n-1)+1) \cdot 2^{n+1} \cdot 2 + 2 \\c_{n+1} &= 2((n-1)+1) \cdot 2^{n+1} + 2 \\c_{n+1} &= (2(n-1)+2) \cdot 2^{n+1} + 2 \\c_{n+1} &= 2(n-1) \cdot 2^{n+1} + 2 \cdot 2^{n+1} + 2 \\c_{n+1} &= 2^{n+1}(n-1) + 2^{n+1}(n-1) + 2 + 2 \cdot 2^{n+1} \quad \text{!} \quad 2x=x+x \\c_{n+1} &= 2^{n+1}(n-1) + c_n + 2 \cdot 2^{n+1} \\c_{n+1} &= 2^{n+1}((n-1)+2) + c_n \\c_{n+1} &= 2^{n+1}(n+1) + c_n, \quad c_1 = 2\end{aligned}$$

Summen

$$\text{z.B. } \forall n \in \mathbb{N} : \sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q} \quad / \quad q^0 + q^1 + q^2 + \dots + q^n = \frac{n(n+1)}{2}$$

$$\text{I.A. } n=0 : q^0 = \frac{1-q^{0+1}}{1-q}, \quad q^0 = \frac{1-q^1}{1-q}, \quad 1=1 \quad \checkmark$$

$$\text{I.V. } \forall n \in \mathbb{N} : \sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q}$$

$$\begin{aligned}\text{I.S. } \sum_{k=0}^n q^k &= \frac{1-q^{n+1}}{1-q} \Rightarrow \sum_{k=0}^{n+1} q^k = \frac{1-q^{(n+1)+1}}{1-q} = \frac{1-q^{n+2}}{1-q} \\&\quad \boxed{\sum_{k=0}^{n+1} q^k = \sum_{k=0}^n q^k + q^{(n+1)}} = \frac{1-q^{n+1}}{1-q} + q^{(n+1)} \\&\quad \text{!} \quad n+1 \text{ für } k \text{ einsetzen} = \frac{1-q^{n+1} + (1-q) \cdot q^{n+1}}{1-q} \\&= \frac{1-q^{n+1} + q^{n+1} - q^{n+2}}{1-q} \\&= \frac{1-q^{n+2}}{1-q}\end{aligned}$$

Ungleichungen

z.B. $\forall n \in \mathbb{N}_{\geq 2} : 2^n > n+1$

$$\text{I.A. } n=2 : 2^2 > 2+1 = 4 > 3 \quad \checkmark$$

I.V. $\forall n \in \mathbb{N}_{\geq 2} : 2^n > n+1$

$$\text{I.S. } 2^n > n+1 \Rightarrow 2^{n+1} > (n+1)+1$$

$$\begin{aligned}&\quad \boxed{2^{n+1}} \\&= 2^n \cdot 2^1 \\&> \underbrace{(n+1) \cdot 2^1}_{2n+2} \\&= n+n+2 > n+2 > 0 \\&\quad \text{kein Einfluss mehr} \\&\rightarrow \text{es gilt } n \geq 2 \\&\text{muss 2 größer als 0 sein}\end{aligned}$$

Fakultät

$$\text{z.B. } \forall n \in \mathbb{N} : \sum_{k=0}^n k \cdot k! = (n+1)! - 1$$

$$\text{I.A. } n=0 : \sum_{k=0}^0 0 \cdot 0! = (0+1)! - 1, \quad 0 \cdot 1 = 1 - 1 \quad \checkmark$$

$$\text{I.V. } \forall n \in \mathbb{N} : \sum_{k=0}^n k \cdot k! = (n+1)! - 1 \quad (n+2)! - 1 = (n+2) \cdot \frac{(n+1)}{(n+2-1)} \cdot \frac{n!}{(n+2-1-1)}$$

$$\text{I.S. } \sum_{k=0}^n k \cdot k! = (n+1)! - 1 \Rightarrow \sum_{k=0}^{n+1} k \cdot k! = ((n+1)+1)! - 1 = (n+2) \cdot (n+1) \cdot n! - 1$$

$$\begin{aligned}&\quad \boxed{\sum_{k=0}^{n+1} k \cdot k!} = \sum_{k=0}^n k \cdot k! + (n+1) \cdot (n+1)! = (n+1)! - 1 + (n+1) \cdot (n+1)! \\&= (n+1) \cdot n! - 1 + (n+1) \cdot (n+1) \cdot n! \\&= (n+1) \cdot n! - 1 + n(n+1) \cdot n! + (n+1) \cdot n! \\&= n!((n+1) + n(n+1) + (n+1)) - 1 \\&= n!(2n+2+n^2+n) - 1 \\&= n!(3n+2+n^2) - 1 \\&= n!(n+2)(n+1) - 1 \\&= (n+2)(n+1)n! - 1\end{aligned}$$

Rekursionsgleichung / Folgen

z.B. $a_n = b_n$ für alle $n \geq 1$

$$a_1 = 3, \quad a_n = 10 \cdot a_{n-1} + 3, \quad b_n = \frac{10^{n-1}}{3}$$

$$\text{I.A. } n=1 : a_1 = \frac{10^1 - 1}{3}, \quad 3 = 3 \quad \checkmark$$

$$\text{I.V. } \forall n \in \mathbb{N}^* : 10 \cdot a_{n-1} + 3 = \frac{10^{n-1}}{3}$$

$$\text{I.S. } 10 \cdot a_{n-1} + 3 = \frac{10^{n-1}}{3} \Rightarrow 10 \cdot a_{(n+1)-1} + 3 = \frac{10^{n+1}-1}{3}$$

$$\begin{aligned}&\quad \boxed{a_{n+1} = 10 a_n + 3} = 10 \cdot \frac{10^n - 1}{3} + 3 \\&\quad \text{weil } a_n = b_n, \quad a_n \text{ durch } b_n \text{ ersetzen} \\&= \frac{10 \cdot 10^n - 10}{3} + 3 \\&= \frac{10 \cdot 10^n - 10 + 9}{3} \\&= \frac{10^{n+1} - 1}{3}\end{aligned}$$

Gerade

z.B. $\forall n \in \mathbb{N} : (2a-1)^n - 1$ ist eine gerade Zahl

$$\text{I.A. } n=0 : (2a-1)^0 - 1 = 0 \text{ ist eine gerade Zahl} \quad \checkmark$$

I.V. $\forall n \in \mathbb{N} : (2a-1)^n - 1$ ist eine gerade Zahl

$$\text{I.S. } (2a-1)^n - 1 \Rightarrow (2a-1)^{n+1} - 1$$

$$\begin{aligned}&\quad \boxed{(2a-1)^{n+1} - 1} \\&= (2a-1)^n \cdot (2a-1)^1 - 1 \\&= 2a \cdot (2a-1)^n - (2a-1)^n - 1 \\&\quad 2k : k \in \mathbb{N}\end{aligned}$$

$$\begin{aligned}&= 2a \cdot (2a-1)^n - 2k \\&= \underline{\underline{2(a \cdot (2a-1)^n - k)}} \\&\quad \text{Vielfaches von 2 daher durch 2 teilbar}\end{aligned}$$

Teilbarkeit

z.B. $\forall n \in \mathbb{N}$ $5^n + 7$ ist durch 4 teilbar

I.A. $n=0$: $5^0 + 7 = 8$ ist durch 4 teilbar ✓

I.V. $4|5^n + 7$

I.S. $4|5^n + 7 \Rightarrow 4|5^{n+1} + 7$

$$\begin{aligned} & \boxed{5^{n+1} + 7} \\ &= 5^n \cdot 5 + 7 \quad 5 = 4 + 1 \text{ für Teilbarkeit} \\ &= 5^n \cdot (4+1) + 7 \\ &= 4 \cdot 5^n + \boxed{5^n + 7} \\ &\quad 4k : k \in \mathbb{N} \\ &= 4 \cdot 5^n + 4k \\ &= \boxed{4(5^n + k)} \end{aligned}$$

Vielfaches von 4 daher
durch 4 teilbar

Rekursionsgleichung

z.B. $F(0) = 1$, $F(n+1) = \sum_{i=0}^n F(i)$

$$F(0) = 1$$

$$F(1) = F(0) = 1$$

$$F(2) = F(0) + F(1) = 2$$

$$F(3) = F(0) + F(1) + F(2) = 4$$

$$F(4) = F(0) + F(1) + F(2) + F(3) = 8$$

$$\forall n \in \mathbb{N}^* (F(n) = 2^{n-1})$$

I.A. $n=1$: $F(1) = 2^0$ ✓

$$\forall n \in \mathbb{N}^* (F(n) = 2^{n-1})$$

I.S. $F(n) = 2^{n-1} \Rightarrow F(n+1) = 2^n$

$$\boxed{F(n+1) = \sum_{i=0}^n F(i)}$$

$$= \sum_{i=0}^{n-1} F(i) + F(n)$$

$$= F(n) + F(n)$$

$$= 2(F(n))$$

$$= 2 \cdot 2^{n-1}$$

$$= 2^n$$

z.B. $F(0) = 1$, $F(n+1) = H(n)$, $H(0) = 0$, $H(n+1) = F(n)$

$$F(0) = 1$$

$$H(0) = 0$$

$$F(1) = H(0) = 0$$

$$H(1) = F(0) = 1$$

$$F(2) = H(1) = 1$$

$$H(2) = F(1) = 0$$

$$F(3) = H(2) = 0$$

$$H(3) = F(2) = 1$$

$$F(4) = H(3) = 1$$

$$\forall n \in \mathbb{N} (F(n) = 1 - H(n))$$

I.A. $n=0$: $F(0) = 1 = 1 - H(0)$ ✓

$$\forall n \in \mathbb{N} (F(n) = 1 - H(n))$$

I.S. $F(n) = 1 - H(n) \Rightarrow F(n+1) = 1 - H(n+1)$

$$\boxed{F(n+1) = H(n) = 1 - F(n) = 1 - H(n+1)}$$

Für welche $n \in \mathbb{N}$ gilt $H(n) = 1$ und für welche $F(n) = 1$

$$\forall k \in \mathbb{N} (F(2k) = H(2k+1) = 1)$$

I.A. $k=0$: $F(0) = H(1) = 1$ ✓

$$\forall k \in \mathbb{N} (F(2k) = H(2k+1) = 1)$$

I.S. $F(2k) = H(2k+1) = 1 \Rightarrow F(2(k+1)) = H(2(k+1)+1) = 1$

$$\begin{aligned} \boxed{F(2(k+1))} &= F((2k+1)+1) = H(2k+1) = 1 \\ &= F(2(k+1)) = H(2(k+1)+1) \end{aligned}$$

Zahlentheorie

Teilbarkeit

Sind $x, y \in \mathbb{Z}$ ganze Zahlen, so sagen man, dass x ein Teiler von y ist, falls es ein $k \in \mathbb{Z}$ gibt mit $x \cdot k = y$. In diesem Fall schreibt man $x | y$.

$$x | y : \exists k \in \mathbb{Z} \quad y = x \cdot k$$

$T(y)$ bezeichnet die Menge aller natürlichen Zahlen, welche Teiler von y sind.

$$T(y) = \{x \in \mathbb{N} \mid x | y\}$$

$$\text{z.B. } T(0) = \mathbb{N}, \forall z \in \mathbb{Z} \quad (1 \in T(z)), \quad T(-32) = \{1, 2, 4, 8, 16, 32\}$$

Erweiterter Euklidischer Algorithmus (Lemma von Bézout)

Finden einer ganzzahligen Lösung für die Gleichungsform:

$$ax + by = \text{ggT}(a, b), \quad x, y \in \mathbb{Z} \text{ und } x, y \neq 0$$

① Diophantische Gleichung = Gleichung in der nur ganzzahlige Lösungen gesucht

$$\text{z.B. } \text{ggT}(168, 133) = 168x + 133y$$

$$\begin{aligned} 168 &= 1 \cdot 133 + 35 & \Rightarrow 35 &= 168 + (-1) \cdot 133 \\ 133 &= 3 \cdot 35 + 28 & \Rightarrow 28 &= 133 + (-3) \cdot 35 = 133 + (-3) \cdot (168 + (-1) \cdot 133) \\ &&&= 133 + (-3) \cdot 168 + 3 \cdot 133 \\ &&&= 4 \cdot 133 + (-3) \cdot 168 \\ 35 &= 1 \cdot 28 + 7 & \Rightarrow 7 &= 35 + (-1) \cdot 28 = 168 + (-1) \cdot 133 + (-1) \cdot (4 \cdot 133 + (-3) \cdot 168) \\ &&&= 168 + (-1) \cdot 133 + (-4) \cdot 133 + 3 \cdot 168 \\ &&&= 4 \cdot 168 + (-5) \cdot 133 \\ 28 &= 4 \cdot 7 + 0 & \hookrightarrow x = 4, y = -5, \quad \{x, y\} = \{(4, -5)\} & \end{aligned}$$

Hat genau dann eine ganzzahlige Lösung, wenn $c = n \cdot \text{ggT}(a, b)$

$$\text{z.B. } 168x + 133y = 7000, \quad 7000 = 1000 \cdot \text{ggT}(168, 133) \quad \checkmark$$

$$168x + 133y = 10, \quad 10 = \frac{10}{\cancel{10}} \cdot \text{ggT}(168, 133) \quad \text{X}$$

Prime Restklassen

Restklassen welche teilerfremd zu n sind. \mathbb{Z}_n^*

$$\text{z.B. } \mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

Additive Inverse

Von negativer Restklasse zu positiver.

$$\text{z.B. } -\overline{496} \text{ in } \mathbb{Z}/3211$$

$$3211 - 496 = \overline{2715}$$

kgV und ggT

Seien $x, y \in \mathbb{Z}$. Kleinstes gemeinsames Vielfaches von x und y

$$\text{kgV}(x, y) := \min \{k \in \mathbb{N} \mid x|k \wedge y|k\}$$

$$\text{z.B. } \text{kgV}(12, 40) = 120, \quad \text{kgV}(-7, 12) = 84$$

Seien $x \neq 0$ oder $y \neq 0$. Größter gemeinsamer Teiler von x und y

$$\text{ggT}(x, y) := \max \{k \in \mathbb{N} \mid k|x \wedge k|y\}$$

$$\text{z.B. } \text{ggT}(12, 40) = 4, \quad \text{ggT}(-7, 12) = 1$$

Zusammenhang zwischen $\text{ggT}(x, y)$ und $\text{kgV}(x, y)$

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|$$

$$\text{z.B. } \text{ggT}(12, 40) \cdot \text{kgV}(12, 40) = 4 \cdot 120 = 480$$

$$\rightarrow |12 \cdot 40| = 480$$

Euklidischer Algorithmus

Zur Bestimmung des $\text{ggT}(x, y)$

z.B. $\text{ggT}(27, -96)$ Dividiere größere (negativ ignoriert) Zahl durch die kleinere Zahl

$$\begin{array}{r} 27 = (-4) \cdot 96 + 12 \\ 12 = 2 \cdot 12 + 0 \end{array} \rightarrow \text{ggT}(27, -96) = 3$$

oberhalb Rest 0

Zwei ganze Zahlen x, y sind teilerfremd, wenn $\text{ggT}(x, y) = 1$

$$\text{z.B. } \text{ggT}(37, 75)$$

$$75 = 2 \cdot 37 + 1 \rightarrow \text{ggT}(37, 75) = 1$$

$$37 = 1 \cdot 37 + 0$$

Kongruent modulo Relation

Wenn zwei ganze Zahlen a und b bei Division durch $n \in \mathbb{N}$ denselben Rest haben, so sagt man, a und b sind kongruent modulo n . $a = b \pmod{n}$, $a \equiv_n b$ (n heißt Modul)

$$\text{z.B. } 17 \equiv_5 22, \quad 6 \equiv_5 1$$

Rechenregeln Wenn $a \equiv_n b$ und $c \equiv_n d$: $a+c \equiv_n b+d$, $a \cdot c \equiv_n b \cdot d$

Restklassen

Klassen mit demselben Rest bei der Division durch eine Zahl

$$\text{z.B. } 17 \equiv_5 22 \rightarrow [2]_5 \text{ oder } \bar{2} \text{ von } \mathbb{Z}/5 = \{\dots, 17, 22, \dots\}$$

$$\text{Menge aller Restklassen: } \mathbb{Z}/n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$$

$$\text{Rechenregeln: } a \cdot [x]_n := [ax]_n, [x]_n - [y]_n := [x-y]_n, ([x]_n)^k = [x^k]_n$$

$$\text{z.B. } 3a - 2b^4 + 4a^2b, \quad a = [2]_{15}, \quad b = [2]_{15}$$

$$3 \cdot \bar{2} - 2 \cdot \bar{2}^4 + 4 \cdot \bar{2}^2 \cdot \bar{2}$$

$$= \overline{21} - \overline{32} + \overline{32}$$

$$= \overline{381} = \overline{6} \rightarrow 381 : 15 = 25.4, \quad 381 - (25 \cdot 15) = 6$$

Primzahlen

1 ist keine Primzahl

Eine natürliche Zahl $p > 1$, die nur durch sich selbst und durch 1 teilbar ist.

Es gilt: $T(p) = \{1, p\}$, $|T(p)| = 2$, Menge aller Primzahlen: \mathbb{P}

Primfaktorzerlegung: $60 = 10 \cdot 6 = 2 \cdot 5 \cdot 2 \cdot 3 = 2^2 \cdot 3 \cdot 5$, $8 = 2^3$

$$\hookrightarrow \text{kgV}(60, 8) = 2^3 \cdot 3 \cdot 5 = 120 \quad \text{① grösste Primfaktoren}$$

Exponent bei 5

Fakultät Anzahl Nullen am Ende: $15! = 1 \cdot 2^1 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \rightarrow 3$ Nullen

Multiplikative Inverse

Existiert nur wenn k und n teilerfremd ($\text{ggT}(k,n)=1$).

$$k \cdot r + n \cdot x = 1, [a]_n \cdot [a^{-1}]_n = [1]_n$$

$$\text{z.B. } [\overline{123}]^{-1} \text{ in } \mathbb{Z}/3211 \rightarrow \text{ggT}(123, 3211) = 1$$

$$3211 = 26 \cdot 123 + 13 \Rightarrow 13 = 3211 - 26 \cdot 123$$

... lösen mit erweiterter euklidischer Algorithmus

$$= 19 \cdot 3211 + (-496) \cdot \overline{123}$$

$$[\overline{123}]^{-1} = [-496]_{3211} = [\overline{2715}]_{3211}$$

→ Wenn negative Restklasse, muss noch additive Inverse berechnet werden, bei positiver Restklasse ist es bereits das Ergebnis.

Kleine Satz von Fermat

Ist p eine Primzahl, dann gilt für alle teilerfremde ganze Zahlen: $a^{p-1} \equiv_p 1$

$$\text{z.B. } p=13, a=6 \rightarrow 6^{12} \equiv_{13} 1$$

Sind p und a teilerfremd und ist $a^{p-1}-1$ nicht durch n teilbar, dann kann p keine Primzahl sein.

$$\text{z.B. } p=9, a=2 \rightarrow \text{ggT}(9,2)=1, 2^8-1=255 \text{ ist nicht durch } 9 \text{ teilbar} \rightarrow 9 \text{ ist keine Primzahl}$$

Lösbarkeit von Gleichungen

$\bar{a} \cdot x = \bar{b}$ ist in \mathbb{Z}/n lösbar, wenn a und n teilerfremd sind. Es gibt genau $t = \text{ggT}(a,n)$ Lösungen wenn t auch b teilt, ansonsten gibt es keine.

$$\text{z.B. } \bar{5}x - \bar{2} = \bar{4} \text{ für } \mathbb{Z}/9 \rightarrow \text{ggT}(5,9) = 1$$

$$\bar{5}x - \bar{2} = \bar{4} \quad | +\bar{2}$$

$$\bar{5}x = \bar{6} \quad | \cdot \bar{5}^{-1} = \bar{2} \rightarrow \bar{5} \cdot \bar{2} = \bar{9} + \bar{1}$$

$$x = \bar{12} = \bar{3}$$

$$\mathbb{L}_x = \{\bar{3}\}$$

Verknüpfungstabelle

z.B. $\mathbb{Z}/4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Chinesischer Restsatz

$$\text{z.B. } x \equiv_3 2, x \equiv_5 3, x \equiv_7 2$$

$$0. \text{ ggT}(3,5) = \text{ggT}(3,7) = \text{ggT}(5,7) = 1$$

$$1. N_1 = 5 \cdot 7 = 35, N_2 = 3 \cdot 7 = 21, N_3 = 3 \cdot 5 = 15, n = 3 \cdot 5 \cdot 7 = 105$$

$$2. [N_1]_3 = [35]_3 = [2]_3 \quad [2^{-1}]_3 = [2]_3 = [r_1]_3$$

$$[N_2]_5 = [21]_5 = [1]_5 \quad [1^{-1}]_5 = [1]_5 = [r_2]_5$$

$$[N_3]_7 = [15]_7 = [1]_7 \quad [1^{-1}]_7 = [1]_7 = [r_3]_7$$

$$3. x = \sum_{i=1}^3 y_i \cdot N_i \cdot r_i = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

$$233 : 105 = 2.21, 233 - (2 \cdot 105) = 23$$

$$\text{Lösungsmenge: } [233]_{105} = [23]_{105} = \{23 + k \cdot 105 : k \in \mathbb{Z}\}$$