Junktoren

Kommutativität:

$A \wedge B \Leftrightarrow B \wedge A$ und

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

Rechenregeln

Assoziativitat:

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

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

Distributivität:

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

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

Regeln von De Morgan:

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

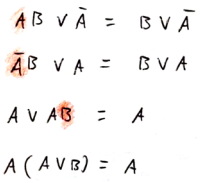
$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

Allgmein

X & !X = 0

X # !X = 1

Reduktion (Benachbarte Terme)



Kontraposition:

A⇒B ⇔ ¬A∨B ⇔ ¬B⇒¬A

A⇒B ist nur falsch wenn A wahr und B falsch

Beispiele Distributivität:

(A∧B)∨(A∨B) ⇔ (A∨(A∨B))∧(B∨(A∨B))

((A∧¬B)∨¬A) ⇔ ((A∨¬A)∧(¬B∨¬A)

Boolesch Vereinfachung

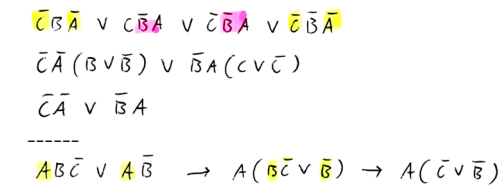
Ziel ist die disjunktive Normalform (DNF). Jede boolesche Funktion besitzt genau eine DNF.

Beachten beim Vereinfachen:

¬P∨P∨¬Q ⇔ T∨¬Q ⇔ T T bei ∨ beibehalten.

Bei ∧ kann auf T verzichtet werden: A∧(¬B∨T) ⇔ A∧T ⇔ A

Bsp:



Quantoren

Eingeschränkt und uneingeschränkt (Angabe von Bezugsmengen):

∀x ∈ ℕ P(x) ⇔ ∀x(x∈ℕ ⇒ P(x))

∀x ∈ ℕ P(x) ⇔ ∀x(x∈ℕ ⇒ P(x))

$\exists \bigvee_x \quad \forall \bigwedge_x$

Vertauschungsregel

∀x P(x) ⇔ ¬∃x ¬P(x) ∃x P(x) ⇔ ¬∀x ¬P(x)

Beispiele Existenz. Es gibt ...

Genau ein:

$$\exists! x\big(A(x)\big) = \underbrace{\exists x\big(A(x)\big)}_{mind\ eins} \wedge \underbrace{\forall y, z(A(y) \wedge A(z) \Rightarrow y = z)}_{nicht\ zwei}$$

$$= \exists x\, P(x) \wedge \forall y(P(y) \Rightarrow y = x)$$

Höchsens ein:

∀x,y P(x) ∧ P(y) ⇒ x = y oder

¬(∃x,y(P(x) ∧ P(y) ∧ x ≠ y)) nicht mindestens x ⇔ höchstens x

Mindestens zwei: ∃x,y P(x) ∧ P(y) ∧ x ≠ y

Höchsens zwei:

¬(∃x,y,z(P(x) ∧ P(y) ∧ P(z) ∧ x ≠ y ∧ x ≠ z ∧ y ≠ z))

Mindestens drei: ∃x,y,z(P(x) ∧ P(y) ∧ P(z) ∧ x ≠ y ∧ x ≠ z ∧ y ≠ z)

Keine: ¬∃x P(x) ⇔ ∀x ¬P(x)

Nicht alle: ¬∀x P(x) ⇔ ∃x ¬P(x)

Keine Distributivität bei Quantoren!

¬(∀x ¬P(x)) ⇔ ¬∀x ¬P(x)

¬(¬∃x(P(x) ∨ S(x)) ⇔ ∃x(P(x) ∨ S(x)) ⇏ ∃x P(x) ∨ ∃x S(x)

Beispiele:

«Alle Männer rauchen.»

⇔ «Für jedes x gilt, wenn es ein Mann ist, dann raucht x.

∀x M(x) ⇒ R(x)

«Alle Schweine sind nicht Rosa.»

⇔ «Wenn x ein Schwein ist, dann ist es nicht Rosa.»

⇔ «Keine Schweine sind Rosa.»

∀x S(x) ⇒ ¬R(x) ⇔ ¬∃x S(x) ∧ R(S)

Weitere Beispiele:

∀x ∃y P(x,y) = Für alle x gibt es ein y, so dass P(x,y) gilt.

∃y ∀x P(x,y) = Es gibt ein y, so dass für alle x P(x,y) gilt.

«Primzahlen sind genau die Zahlen die sich selbst als Primfaktor haben.»

$\forall x \left(\mathrm{Prim}(x) \Leftrightarrow \mathrm{PF}(x, x)\right)$

Alle Vielfachen einer natürlichen Zahl mit der Eigenschaft E haben selbst die Eigenschaft E: ∀x (V(x, n) ∧ E(n) ⇒ E(x))

Normalformen

NNF (Negations Normalform)

– Alle Negationen kommen in Literalen vor

– Es gibt keine Implikationen

DNF (Disjunktiver Normalform): (A∧B)∨(A∧B)∨(A∧B)

KNF (Konjunktiver Normalform): (A∨B)∧(A∨B)∧(A∨B)

–> Formeln können mehreren Normalformen zugeordnet werden.

-> Für jede Formel gibt es äquivalente Formeln in NNF, KNF und DNF.

Beispiele:

p∨q ist in NNF, KNF und DNF weil

(p∨q)∧¬1 ist KNF und NNF

(p∧1)∨(q∧1) ist DNF

p is in KNF und DNF.

$(p \wedge (\neg q \wedge p_1))$ is in KNF und DNF.

$p \vee (q \rightarrow p)$ ist nicht in KNF und nicht in DNF.

$p \vee (\neg p \wedge (p \vee q))$ ist weder KNF noch in DNF.

$(p \vee q) \wedge (p \vee (p \vee p))$ is in KNF aber nicht in DNF.

Grundsätzlich kann eine Formel mittels Distribitivität in die andere Form gebracht werden.

Beispiel KNF in DNF bringen:

(¬A∨¬B)∧(¬C∨¬D)

(¬A∧(¬C∨¬D))∨(¬B∧(¬C∨¬D))

(¬A∧¬C)∨(¬A∧¬D)∨(¬B∧¬C)∨(¬B∧¬D)

Beispiel DNF in KNF bringen:

$$\underbrace{\neg p \vee (q \vee (p_1 \wedge p_2))}_{DNF}$$

$$\neg p \vee ((q \vee p_1) \wedge (q \vee p_2))$$

$$\underbrace{(\neg p \vee q \vee p_1) \wedge (\neg p \vee q \vee p_2)}_{KNF}$$

Minterm und Maxterm

A	B	C		gesamt		Minterme		Maxterme
1	0	0		0				$\neg A \vee B \vee C$
1	1	0		0				$\neg A \vee \neg B \vee C$
1	0	1		1		$A \wedge \neg B \wedge C$		
1	1	1		1		$A \wedge B \wedge C$		
0	0	0		0				$A \vee B \vee C$
0	1	0		0				$A \vee \neg B \vee C$
0	0	1		1		$\neg A \wedge \neg B \wedge C$		
0	1	1		1		$\neg A \wedge B \wedge C$		

DNF:

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

KNF:

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

Semantische Eigenschaften

Eine aussagenlogische Formel *A* heisst

- Allgemeingültig — Alle Belegungen — $\forall \hat{B}(A) = true$
- Unerfüllbar — Alle Belegungen — $\forall \hat{B}(A) = false$
- Erfüllbar — Min. Eine Belegung — $\exists \hat{B}(A) = true$
- Widerlegbar — Min. Eine Belegung — $\exists \hat{B}(A) = false$
  - Gültig: Unter einer einzigen Belegung B (Nur eine Beleung wird angeschaut) — B(A) = true

Bsp. für eine aussagenlogische Formel: $p \vee (p \Rightarrow \neg(q \wedge p))$
Quantoren gehören nicht dazu.

Operationsfolge (Gewichtung): $\neg,\ \wedge,\ \vee,\ \Rightarrow$

Tautologie = Allgemeingülltige Aussage.

Belegung

Eine Belegung ist eine Zuordnung/Funktion von Variablen zu Wahrheitswerten. Mittels einer Belegung kann jeder aussagenlogischen Formel einen Wahrheitswert zugeordnet werden.

Die Funktion $\hat{B}$ ordnet jeder aussagenlogischen Formel ihren Wahrheitswert bezüglich dessen Belegung B zu. $\hat{B}: \mathbb{F} \to \{false, true\}$

- $\hat{B}(F \wedge G) = and\left(\hat{B}(F), \hat{B}(G)\right)$
- $\hat{B}(F \vee G) = or\left(\hat{B}(F), \hat{B}(G)\right)$
- $\hat{B}(\neg G) = not\left(\hat{B}(F), \hat{B}(G)\right)$

Beispiel: Bestimmen Sie $\hat{B}$ der Formel $(u \to r) \wedge s$

- $B(p) = B(q) = B(r) = B(s) = true$
- $B(u) = B(v) = false$

$$\hat{B}\big((u \to r) \wedge s\big) = and\left(\hat{B}(u \to r), \underbrace{\hat{B}(s)}_{true}\right) = \hat{B}(u \to r) = or\left(\neg\hat{B}(u), \underbrace{\hat{B}(r)}_{true}\right) = \boldsymbol{true}$$

Beispiel:
Zeigen Sie, dass die aussagenlogische Formel F **genau dann** unerfüllbar ist, wenn die Formel ¬F allgemeingültig ist.

F unerfüllbar ⇔ ¬F allgemeingültig
Beweis geht **in beide Richtungen**. Wir müssen beide Richtungen beweisen:

(a) Wenn F unerfüllbar ist, dann gilt für jede Belegung B, die Gleichung $\hat{B}(F) =$ false und somit $\hat{B}(\neg F) =$ not$(\hat{B}(F)) =$ true. Also ist $\neg F$ allgemeingültig.

(b) Ist $\neg F$ allgemeingültig, dann gilt für jede Belegung B die Gleichung $\hat{B}(\neg F) =$ true und somit auch $\hat{B}(F) =$ false. Also ist F unerfüllbar. □

Beweisttechniken

Direkter Beweis einer Implikation: Wenn eine Aussage von der Form A⇒B vorliegt. Es gilt eine Aussage A⇒B zu beweisen. Verwendung von schon bestehenden und bewiesenen Aussagen/Regeln.

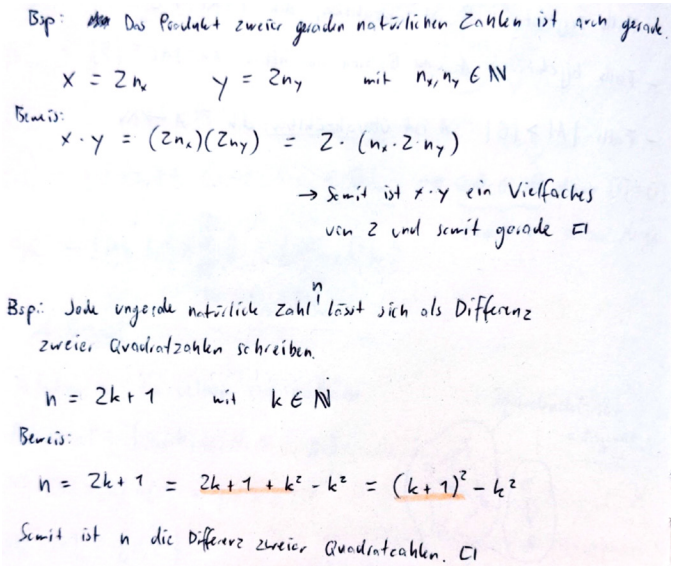
Kontraposition: Wenn eine Aussage von der Form A⇒B vorliegt.
Zu beweisen: ¬A∨B, oder ¬B⇒¬A.

Beweis durch Widerspruch: Ziel ist eine Aussage herzuleiten, von der bekannt ist, dass sie falsch ist.

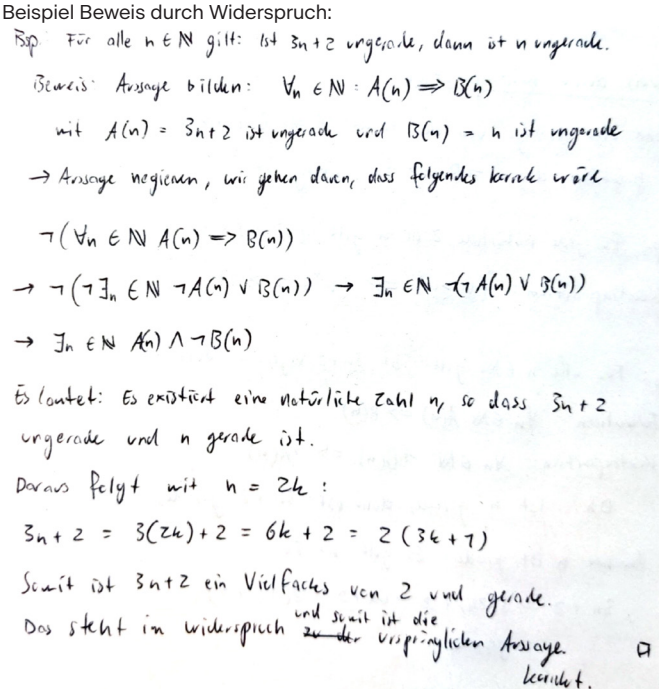
Gegenbeispiel: Wenn eine Aussage von der Form ∀x P(x) vorliegt.
Ziel: Es gilt zu zeigen, dass eine bestimmte Eigenschaft nicht auf alle Objekte (aus einem Kontext) zutrifft. D.h. zu beweisen, dass ¬∀x P(x) bzw. ∃x ¬P(x) ist wahr.
Es genügt ein einziges Objekt x anzugeben, für das P(x) falsch ist.

Äquivalenz: Wenn eine Aussage von der Form A⇔B vorliegt.
Zu beweisen: 1) A⇒B sowohl als auch 2) B⇒A
Es können beliebige (passende) Beweistecniken eingesetzt werden.

Beispiel Direkter Beweis:



Beispiel Beweis durch Widerspruch:



Beispiel Kontraposition:

Beispiel: "Für jede natürliche Zahl n gilt: $(n^2 + 1 = 1) \Rightarrow (n = 0)$"

Beweis. Ist $n \neq 0$ so folgt, dass auch $n^2 \neq 0$ gilt. Dies impliziert, dass für jede weitere natürliche Zahl m die Ungleichung $n^2 + m \neq m$ erfüllt ist. Insbesondere gilt daher, dass (der Fall $m = 1$) $n^2 + 1 \neq 1$ gilt. □

Mengen

Explizite Schreibweise: {..., 1, 2, 3, 4, ...}, {a, b, c}, etc.

Prädikative/definierende Schreibweise (Beschreibende Form):
$\{x \in \mathbb{N} \mid x>3 \wedge x<10\}$

$$A = \{x \mid -5 < x < 3\}$$

$$\underbrace{A}_{\text{A}} \quad \underbrace{=}_{\text{ist}} \quad \underbrace{\{}_{\text{die Menge aller}} \quad \underbrace{x}_{\text{x}} \quad \underbrace{\mid}_{\text{für die gilt:}} \quad \underbrace{-5 < x < 3}_{\text{x ist größer als -5 und kleiner als 3}} \quad \}$$

Leere Menge: {} oder ∅

Mengenoperationen:

Teilmenge	$X \subseteq Y \coloneqq \forall x(x \in X \Rightarrow x \in Y)$	
Vereinigung	$X \cup Y \coloneqq \{x \mid x \in X \vee x \in Y\}$	
Schnittmenge	$X \cap Y \coloneqq \{x \mid x \in X \wedge x \in Y\}$	
Differenz	$X \setminus Y \coloneqq \{x \mid x \in X \wedge x \notin Y\}$	A ohne B
Komplement	$\overline{Y}$	

Rechenregeln:

Kommutativität der Vereinigung und des Schnittes:
$A \cup B = B \cup A \; und \; A \cap B = B \cap A$

Assoziativgestze von Schnitt und Vereinigung:
$A \cup (B \cup C) = (A \cup B) \cup C \; und \; A \cap (B \cap C) = (A \cap B) \cap C$

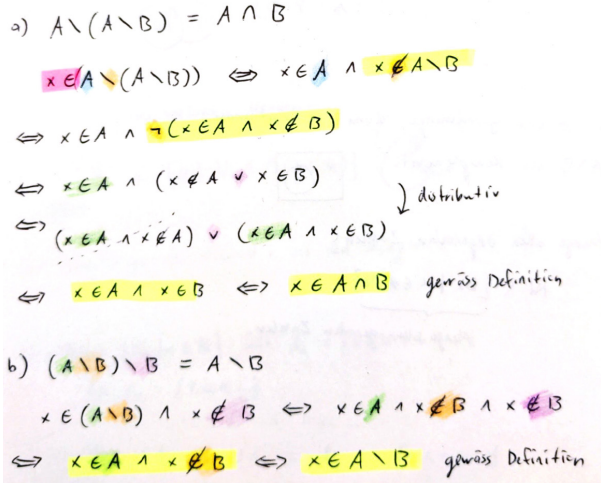
Distributivgesetze von ∩ und ∪:
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \; und \; A \cup (B \cap /C) = (A \cup B) \cap (A \cup C)$

Idempotenzgesetz:
$A \cap A = A \; und \; A \cup A = A$

Regeln von De Morgan:
$(C \setminus A) \cap (C \setminus B) = C(A \cup B) \; und \; (C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$

Disjunkt: A∩B∩C = ∅
– disjunkt Paarweise: Alle Mengen sind einzigartig (und haben kein gemeinsamen Elemente)
– Nicht paarweise disjunkt: Einzelne Mengen haben eine nichtleere Schnittmenge

Beispiel Beweis:



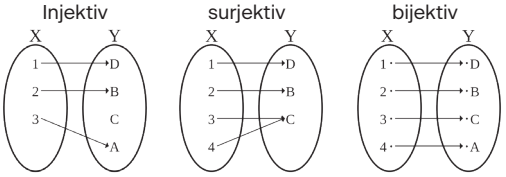
$\overline{A} \coloneqq G \setminus A$ Wenn G eine Grundmenge ist

|A∪B| = |A| + |B| - |A∩B|
|A∪B∪C| = |A| + |B| + |C| - |A∩B| - |A∩C| - |B∩C| + |A∩B∩C|

Venn-Diagramm:

Abzählbarkeit und unendlichen Mengen

Abbildiung $f: X \to Y$



Injektiv: Jedes Outputlement kann nut mittels einem einzigen (evtl. gar keiem) Inputlement erreicht werden. Für jedes Outputelement exisitert eine Umkehrfunktion. Für jedes y höchstens ein x.

surjektiv: Elemente der Zielmenge werden mindestens einmal getroffen. Wenn Wertebereich (Outputlemente) = Bildmenge

bijektiv: Injektiv und surjektiv

Bsp: Geg. $f: \mathbb{N} \to \mathbb{N}$
F(n) = Die Zahl n rückwärts gelesen und fürende Nullen gestrichen.
F(324) = 423, F(0) = 0 und F(10) = 1
Ist F surjektiv? Antwort: Nein, weil 10 in der Bildmenge $\mathbb{N}$ nicht erreicht wird.
Wäre aber die Bildmenge $\mathbb{N}$\{10,20,30,...}, dann wäre F surjektiv.

Abzählbarkeit

f: A → B

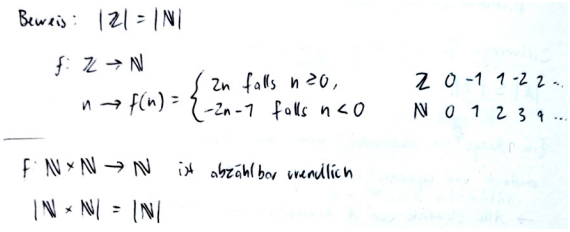
– Wenn Injektiv, dann ist A abzählbar, d.h. es gibt eine Abbildung $f: A \to \mathbb{N}$
– Wenn surjektiv, dann ist B ist abzählbar, d.h. Abbildung ist $f: \mathbb{N} \to B$
– Wenn bijektiv, d.h. |A| = |ℕ| (gleichmächtig), dann ist A und B abzählbar
– Wenn $f: \mathbb{N} \to B$ und |A| > |ℕ|, dann ist A überabzählbar

Eine Menge (X) heisst abzählbar, wenn:
$f: \mathbb{N} \to X$ surjektiv ist und $X \neq \emptyset$
$f: X \to \mathbb{N}$ injektiv ist und $X \neq \emptyset$
Elemente können mit natürlichen Zahlen durchnummeriert werden.

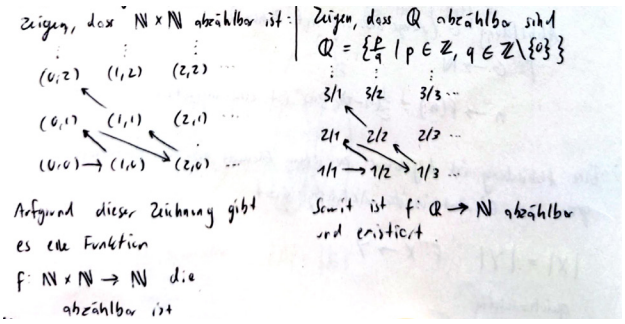
Endliche Mengen sind immer abzählbar. Eine Vereinigung abzählbarer Menge ist abzählbar.

Eine Menge A ist genau dann **abzählbar unendlich**, wenn A und ℕ gleichmächtig sind, d.h. |A| = |ℕ|

Überabzählbar wenn |A| > |ℕ|
Elemente können mit nicht durchnummeriert werden.
Irrationale Zahlen, reelle Zahlen, Potenzmengen sind überabzählbar.



Beweis durch Diagonalisierungsverfahren:



Funktionen

Funktionen sind binäre Relationen $f \subset A \times B$ mit $(x, y) \in f$ von A nach B, man schreibt $f: A \to B$

Inputelemente (A): Definitionsbereich *Dom(f)*
Urmenge/-bild bei Mengen

Outputelement (B): Funktionswert *Im(f)*, Wertebereich, $f(x)$
Menge aller Funktionswert nennt man **Bild**menge.
Abbildung bei Mengen.

Eine Funktion lässt sich auf verschiedene Arten beschreiben:

$f = \{(x,y) \in \mathbb{N}^2 \mid y = x^2\}$

$f: \mathbb{N} \to \mathbb{N}$

$f(x) = x^2$

oder

$|x| = \sqrt{x^2}$

$|x| = \begin{cases} -x & \text{wenn } x < 0 \\ x & \text{sonst} \end{cases}$

Potenzmenge

$\mathcal{P}(X)$
P(A) := {x | x⊂A}
Die Potenzmänge enthält genau **alle möglichen Teilmengen** eine Menge.

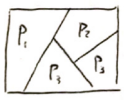
Beispiele:
$P(\emptyset) = \{\emptyset\} \neq \emptyset$ d.h. eine Potenzmenge ist **nie leer.**
$P(\{a\}) = \{\emptyset, \{a\}\}$
$P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
$P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
$P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
$P(P(a)) = \{\emptyset, \{\emptyset\}, \{\{a\}\}, \{\emptyset, \{a\}\}\}$

Beispiel Beweis:

Beweisen: $P(A \cap B) = P(A) \cap P(B)$ mit P = Potenzmenge

$x \in P(A \cap B) \Leftrightarrow x \subset A \cap B$ → Definition
$\Leftrightarrow x \subset A \wedge x \subset B$
$\Leftrightarrow x \in P(A) \wedge x \in P(B)$
$\Leftrightarrow x \in P(A) \cap P(B)$

Partition



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

– Alle Teilmengen der Partition sind paarweise disjunkt .
– Anzahl Äquivalenzrelationen M x M.
– Jede Potenzmenge enthält die leere Menge

Voraussetzungen:
1. Die Vereinigungen(U) aller Partitionsmengen = Menge
2. {} darf nicht leer sein und {{1},{1, 2, 3}} dürfen nicht mehrmals vorkommen -> paarweise disjunkt

Beispiel: Menge {1,2,3} hat genau 5 Partitionen:
{{1,2, 3}}, {{1}, {2, 3}}, {{2}, {3,1}}, {{3}, {1,2}}, {{1}, {2}, {3}}

Partition Beispiele:

a) Partition von $\mathbb{N}$ mit unendlich grossen Blöcken.

$P_1 = \{x \in \mathbb{N} \mid x \text{ ist ungerade}\}$

$P_2 = \{x \in \mathbb{N} \mid x \text{ ist gerade}\}$

b) Partition rationaler Zahlen mit unendlich vielen und unendlich grossen Blöcke.

$P_i = \{x \in \mathbb{Q} \mid i < x < i+1\}$ mit $i \in \mathbb{Z}$

z.B. $P_1 = \{1.000\ldots, 1.999\}$

Relation

Zum formulieren von Relationen werden Tupeln verwendet.

Tupel
Definierte Reihenfolge und kann wiederholende Elemnte enthalten. Entspricht in etwa Listen und Arrays. Im Vergleich zur Menge: Keine Reihenfolge und nur einzigartige Elemente (keine Wiederholungen).

2-Tupel: (a,b) n-Tupel: $(x_1, x_2, \ldots, x_n)$

Kartesisches Produkt
Gesamtheit aller Tupel aus einer oder mehreren Mengen.
(Jedes Element aus A kombiniert mit jedem anderem aus B.)

$$A_1 \times \cdots \times A_n := (a_1, \ldots, a_n)$$

$X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}$. Alle Kombinatinospaare.

Beispiel: A={0,1}, B={2,3} A×B={(0,2), (0,3), (1,2), (1,3)}

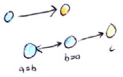
Relationen auf Mengen sind Teilmengen: $R \subset X \times Y$
R ist eine Teilmenge aller möglichen Relation zwischen X und Y.

Eine **binäre** Relation R, mit $(x,y) \in R$ kann auch xRy geschrieben werden.
x und y stehen zueinander in Realation R.

Relationseigenschaften
– **Reflexis:** Für alle $x \in M$ gilt xRx.
Relation mit sich selbst.

– **Symmetrisch:** Für alle $\forall x \in M$ gilt $xRy \Rightarrow yRx$
Relation in beide Richtungen.

– **Antisymmetrisch:** Für alle $\forall x,y \in M$ gilt $xRy \wedge yRx \Rightarrow x=y$
Relation nur in eine Richtung, ausser x und y sind gleich.



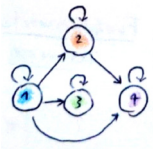
– **Transitiv:** Für alle $\forall x,y \in M$ gilt $xRy \wedge yRx \Rightarrow xRz$
z kann auch x sein.
Z.B. $x \leq y \leq z$ denn $x \leq z$

Jede binäre Relation auf einer Menge mit nur einem einzigen Element ist reflexiv: R = {(a,a)}

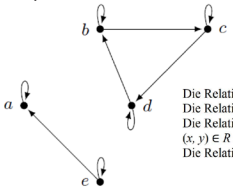
Beispiele:
$uRv \Leftrightarrow ggT(u,v) = 1$ in $\mathbb{N}_{>0}$. symmertrisch
$uRv \Leftrightarrow u$ ist unmittelbarer Nachfolger von v in $\mathbb{N}$. antisymmetrisch
$xRy \Leftrightarrow x$ hat dieselbe Quersumme wie y in $\mathbb{N}$. reflexiv, symmetrisch, transitiv
$xRy \Leftrightarrow x \leq y$ in $\mathbb{Z}$. reflexiv, antisymmetrisch, transitiv
$xRy \Leftrightarrow x > y$ in $\mathbb{R}$ antisymmetrisch, transitiv
$xRy \Leftrightarrow x \geq y$ in $\mathbb{R}$ reflexiv, antisymmetrisch, transitiv
$xRy \Leftrightarrow x \neq y$ in $\mathbb{R}$ symmetrisch
$xRy \Leftrightarrow x = y$ in $\mathbb{R}$ reflexiv, symmetrisch, antisymmetrisch, transitiv

Binäre Relationen als **direkter Graph** G = (V, E) dargestellt.
V = Knoten = Elemente
E = Kanten = Relationen

binäre Relation $E \subset V \times V$ (Kanten)
$V = \{1, 2, 3, 4\}$
$E = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$



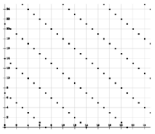
Beispiel:



Die Relation ist reflexiv, weil für alle Elemente $x \in \{a, b, c, d, e\}$ gilt, dass $(x, x) \in R$.
Die Relation ist nicht symmetrisch, weil z. B. *eRa* gilt, aber nicht *aRe*.
Die Relation ist antisymmetrisch, weil für alle $x, y \in \{a, b, c, d, e\}$, so dass $x \neq y$ gilt, dass wenn $(x, y) \in R$ ist, $(y, x) \notin R$ gilt.
Die Relation ist nicht transitiv, weil z.B. *bRc* und *cRd* gelten, aber nicht *bRd*.

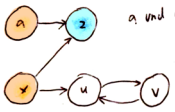
Relationsgraph:

$R = \{(x, y) \mid x, y \in \mathbb{N} \wedge x, y < 100 \wedge x + y \text{ ist ein Vielfaches von } 7\}$



Ordnungsrelationen

- **Unvergleichbar:** Wenn weder xRy noch yRx gilt.
- **Minimal:** x ist R-minimal wenn nichts auf x zeigt, nur xRy
- **Maximal:** x ist R-maximal wenn x auf nichts zeigt, nur yRx



a und u sind R-unvergleichbar.

	Reflexiv	Symmetrisch	Antisymmetrisch	Transitiv
Äquivalenzrelation	X	X		X
Prä-Ordnung	X			X
Halb-Ordnung	X		X	X
Totale Ordnung	X		X	X
Wohl-Ordnung	X		X	X

Vergleichbar: Wenn xRy und yRx gilt (=symmetrisch)

Präordnung (auch Quasiordnung): Wenn eine R-Unvergleichbarkeit besteht. Die Ist-Teiler-von-Beziehung xIy auf $\mathbb{Z}$ ist eine Präordnung. Jede **Äquivalenzklasse ist eine Präordnung.**

Halbordnung (auch Partielle-Ordnung): Wenn eine Relation $\preceq$ gilt und es R-Minimale und R-Maximale Elemente gibt

Totalordnung (auch Linearordnung):
Eine Halbordnung ohne R-unvergleichbare Elemente,
d.h. alle Elem. können miteinander verglichen werden.

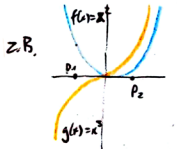
Wohlordnung: Eine Totalordnung und mind. ein R-Minimum.
Wir wissen, wo gestratet wird.

Halbordnung < Totalordnung < Wohlordnung

Das heisst eine Wohlordnung ist auch eine Totalordnung und eine Totalordnung ist auch eine Halbordnung.

Beispiele:

- Relation $\leq$ auf Menge $\mathbb{R}$ ist eine **Totalordnung**, aber keine Wohlordnung. $\mathbb{R}$ hat kein kleinstes Element.
- Eine Potenzmenge (oder eine Menge von Mengen) ist eine **Halbordnung** auf dei Teilmengenrelation $\subset$.
  Die Teilbarkeitsrelatoin ist auch eine Halbordnung.
  $\preceq$ ist eine Halbordnung
- $\preceq$-Relation auf $\mathbb{Q}$ ist keine Wohlordnung weil 1/n kein minimales Element besitzt.
- **Präordnung:** f(x) $\preceq^*$ g(x), g wächst **nicht** schneller als f, das macht f und g zu unvergleichbaren Funktionen.



Unvergleichbar weil bei P_1 $g < f$
und dann aber bei P_2 $g > f$

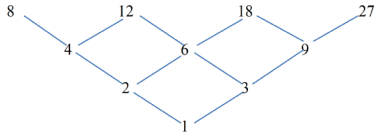
U.a. sind periodische Funktionen immer unvergleichbar, z.B. f=sin, g=cos

Oder: $f(x) = \begin{cases} 1 \text{ falls } x \text{ ungerade} \\ 0 \text{ sonst} \end{cases}$ $g(x) = \begin{cases} 0 \text{ falls } x \text{ ungerade} \\ 1 \text{ sonst} \end{cases}$

Beispiel Beweis Halbordnung:

9. Zeigen Sie, dass die Teilbarkeit auf der Menge $M = \{1,2,3,4,6,8,9,12,18,27\}$ eine Halbordnung darstellt und zeichnen Sie das dazugehörige Hasse-Diagramm.

Lösung: $k,n \in \mathbb{Z}$, $x,y,z \in M$
Reflexiv, weil jede Zahl Teiler von sich selbst ist: $x \mid x$
Antisymmetrisch, weil für alle Zahlen $x \neq y$, für welche x Teiler von y, y nicht Teiler von x sein kann. $x \mid y \wedge y \mid x \Rightarrow x = y$
Transitiv, weil wenn x Teiler von y und y Teiler von z, dann teilt x auch z: $x \mid y \wedge y \mid z \Rightarrow x \mid z$
$y = kx \wedge z = ny \Rightarrow z = knx \Leftrightarrow x \mid z$



Äquivalenzrelationen

Wenn eine Relation auf eine Menge, reflexiv, symmetrisch und transitiv ist
-> wichtig für einen Beweis («Wie müssen zeigen, dass...»).
Und wenn (a,b)∈M den selben Betrag haben.

Gleichheitsrelation ist kleinste Äquivalenzrelation $\{(x,x) \mid x \in X\}$
$X \times Y$ ist grösste Äquivalenzrelation

Äquivalenzklasse

- Äquivalenzklassen sind disjunkte Teilmengen einer grösseren Menge.
- Alle Elemente in einer Äquivalenzklasse sind transitiv, reflexiv und symmetrisch (Definition)

$$[x]_R := \{y \in X \mid xRy\}$$

Alle Elemente in der Äquivalenzklasse die zu x in Relation R stehen.
x ist Vertreter der Äquivalenzklasse.

Faktormenge:
Menge aller Äquivalenzklassen.

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

Beispiele Äquivalenzklassen:

- a ist gleich alt wie b.
- a kostet gleich viel wie b
- Seite a gehört zum selben Kapitel wie Seite b.

8. Beschreiben Sie für jede der folgenden Äquivalenzrelation die Menge der Äquivalenzklassen.
   a) R ist so definiert, dass xRy genau dann gilt, wenn x und y gleich alt sind.
   b) R ist so definiert, dass xRy genau dann gilt, wenn x und y das gleiche Geschlecht haben.

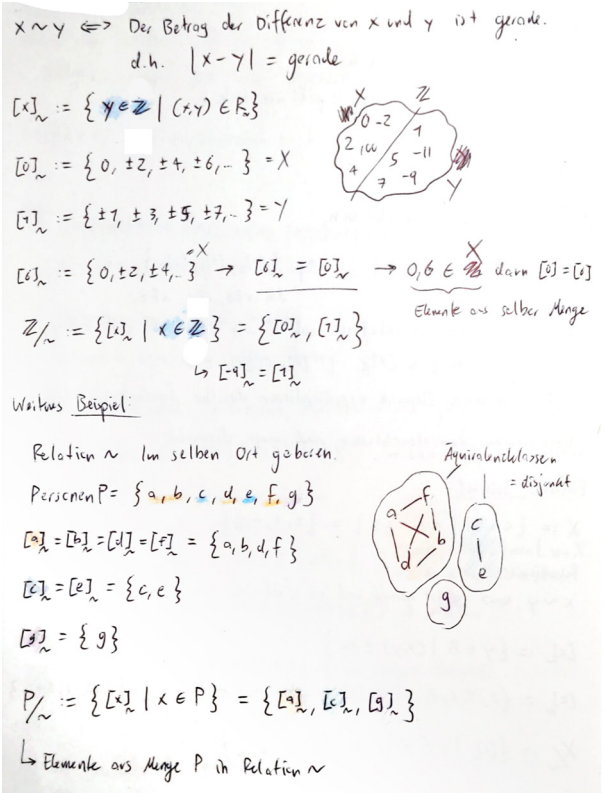
Lösung:
a) Jede Altersklasse entspricht einer Äquivalenzklasse.
b) Es gibt zwei Äquivalenzklassen: Die Menge der Frauen und die Menge der Männer.

Beispiel Beweis:

6. $\mathbb{R}$ sei die Menge der reellen Zahlen. xRy genau dann, wenn $x - y$ eine ganze Zahl ist.
   Zeigen Sie, dass R eine Äquivalenzrelation ist und bestimmen Sie die Äquivalenzklasse von 0, 0.5 und $\sqrt{2}$.

Lösung:
$xRy \Leftrightarrow x - y \in \mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}(x - y = k)$
Reflexiv: $xRx \Leftrightarrow x - x = 0 \in \mathbb{Z}$
Symmetrisch: es gelte $xRy \Leftrightarrow \exists k \in \mathbb{Z}(x - y = k)$
dann gilt $y - x = -k \in \mathbb{Z} \Rightarrow yRx$
Transitiv: es gelte xRy ∧ yRz $\Leftrightarrow \exists k \in \mathbb{Z}(x - y = k) \wedge \exists k' \in \mathbb{Z}(y - z = k')$
$\Rightarrow x - z = x - y + y - z = k + k' \in \mathbb{Z} \Rightarrow xRz$
Es liegt eine Äquivalenzrelation vor mit den Äquivalenzklassen (es gibt noch viel mehr):
1. M_0: $[0] = \{m \in \mathbb{R} \mid mR0\} \Rightarrow m \in \mathbb{Z} \Rightarrow M_0 = \mathbb{Z}$
2. $M_{0.5}$: $[0.5] = \{k + 0.5 \mid k \in \mathbb{Z}\}$
3. $M_{\sqrt{2}}$: $[\sqrt{2}] = \{k + \sqrt{2} \mid k \in \mathbb{Z}\}$

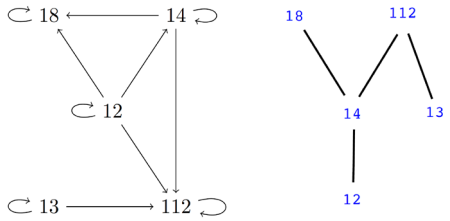
Beispiel Äquivalenzklassen:



Hasse-Diagram

Nur Halbordnungen, Totalordnung und Wohlordnung (**≤-Relation**) können dargestellt werden.

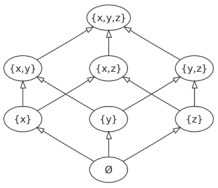
Der Graph G = ({12, 13, 14, 18, 112}, ≤) ist wie folgt gegeben.



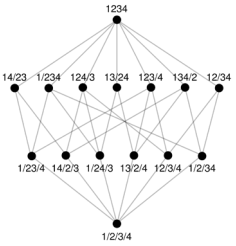
minimale Elemente: 12 und 13 maximale Elemente: 18 und 112

Relationsmenge M = {(12, 12), (13, 13), (14, 14), (18, 18), (112, 112), (12, 14), (12, 18), (12, 112), (14,18), (14, 112), (13,113) }

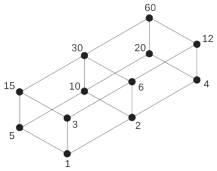
Beispiele:



Potenzmenge (Teilmengenrelation)

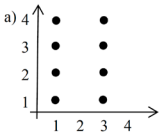


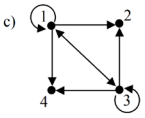
Partition



Teilbarkeitsrelation

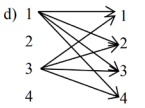
Weitere Graphen





b)

(u,v)	1	2	3	4
1	1	1	1	1
2	0	0	0	0
3	1	1	1	1
4	0	0	0	0



a) Koordinatensystem
b) 01-Matrix
c) gerichteter Graph
d) bipartiter Graph

Vollständige Induktion

Beweismethode für alle natürlichen Zahlen.

Beweisprinzip in 2 Schritten:

Es sei $A(n)$ ein Prädikat von natürlichen Zahlen. Es gelte:

1. **Induktionsverankerung:** $A(0)$ ist wahr,
2. **Induktionsschritt:** Für alle $\ell \in \mathbb{N}$: ist $A(\ell)$ wahr, so auch $A(\ell+1)$.

Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Summenwert

Es sei $A(n)$ das Prädikat: $0+1+2+3+\ldots+n = \frac{n(n+1)}{2}$

1. Wir zeigen zuerst die Induktionsverankerung:
   $A(0)$ gilt, weil $0 = \frac{0\cdot 1}{2}$ offensichtlich korrekt ist.
2. Induktionsschritt:
   Wir nehmen an, dass $A(\ell)$ richtig ist, d.h.: $0+1+\ldots+\ell = \frac{\ell(\ell+1)}{2}$. Mit Hilfe der **Induktionsannahme** zeigen wir den **Induktionsschluss** „$A(\ell+1)$ ist auch richtig“:

$$0+1+\ldots+\ell+(\ell+1) = (0+1+\ldots+\ell)+(\ell+1) \overset{A(\ell)}{=} \frac{\ell(\ell+1)}{2}+(\ell+1)$$
$$= \frac{(\ell+1)(\ell+2)}{2}$$

also ist auch $A(\ell+1)$ richtig. Die Implikation gilt für alle $\ell \in \mathbb{N}$.

oder

B 1: $1 + 2 + 3 + \ldots + n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ **(für alle n ≥ 1)**

Induktionsanfang: n = 1: linke Seite: nur ein Summand: 1
rechte Seite: $\frac{1\cdot(1+1)}{2} = 1$

Induktionsschluss:

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

Ungleichung

$$\forall n \in \mathbb{N}_{\geq 2} \quad (1+x)^n > 1+nx.$$

Lösung:
Das Prädikat $A(n)$ sei: $(1+x)^n > 1+nx$.

1. *Induktionsverankerung $A(2)$: Die Verankerung gilt, wegen*
$$(1+x)^2 = 1+2x+x^2 > 1+2x.$$
2. *Induktionsschritt:*
Es sei $\ell \in \mathbb{N}_{\geq 2}$ gegeben. Wir nehmen an, dass $A(\ell)$ wahr ist, d.h.: $(1+x)^\ell > 1+\ell x$.
Wir zeigen die Aussage für $\ell+1$:
$$(1+x)^{\ell+1} = (1+x)^\ell(1+x) \overset{A(\ell)}{>} (1+\ell x)(1+x) = 1+\ell x+x+\underbrace{\ell x^2}_{>0} > 1+(\ell+1)x.$$

Somit haben wir $A(\ell+1)$ aus $A(\ell)$ erhalten. Die Implikation gilt für alle $\ell \in \mathbb{N}_{\geq 2}$.

Insgesamt folgt aus 1. und 2., dass $A(n)$ für alle $\mathbb{N}_{\geq 2}$ gilt.

Mengen

$|\mathcal{P}(X)| = 2^{|X|}$.

- **Verankerung** ($|X| = 0$)**:** Die einzige Menge mit 0 Elementen ist die leere Menge, es gilt also wie gewünscht
$$|\mathcal{P}(X)| = |\mathcal{P}(\varnothing)| = |\{\varnothing\}| = 1 = 2^0 = 2^{|X|}.$$
- **Schritt:** Es sei nun X eine $n+1$ elementige Menge. Aufgrund der Induktionsannahme können wir davon ausgehen, dass für alle Mengen Y mit n Elementen die Gleichung
$$|\mathcal{P}(Y)| = 2^{|Y|}$$
erfüllt ist. Da $X \neq \varnothing$ gilt, können wir ein $x \in X$ auswählen. Wir unterteilen die Potenzmenge von X in zwei disjunkte, gleich grosse Teile A und B:
$$A = \{Y \subseteq X \mid x \notin Y\} \qquad |A| = 2^n$$
$$B = \{Y \subseteq X \mid x \in Y\}. \qquad |B| = 2^n$$

Es gilt:
$$|\mathcal{P}(X)| = |A \cup B| = |A| + |B|$$
$$= |A| + |A| = 2|A| = 2|\mathcal{P}(X \setminus \{x\})|$$
$$\overset{I.A.}{=} 2 \cdot 2^n = 2^{n+1}. \qquad \square$$

Summenwert

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

- Verankerung $A(n)$
- Schritt $\forall n \in \mathbb{N}($ $\underbrace{A(n)}_{\text{Induktions-Annahme}}$ $\Rightarrow A(n+1))$

Induktions-Annahme *IA*

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

Induktions-Verankerung $IV\ (n=0)$

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

Zu zeigen

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

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

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

n + 1 -> Summen immer in zwei aufteilen

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

Rekursion

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

Zeigen Sie mit Induktion, dass für alle $n \in \mathbb{N}$ mit $n > 0$

$$F(n) = 2^{n-1}$$

IA $n = 1$: $F(1) = 2^0$

IV: $F(n) = 2^{n-1}$

IS: $F(n) = 2^{n-1} \Rightarrow F(n+1) = 2^n$

$$F(n+1) = \sum_{k=0}^{n} F(k) = \sum_{k=0}^{n-1} F(k) + F(n) = F(n) + F(n)$$
$$= 2F(n) = 2 \cdot 2^{n-1} = 2^n$$

Teilbarkeit

$n^3 + 5n$ ist durch 6 teilbar für alle $n \geq 0$

Induktionsanfang: n = 0: $0^3 + 5 \cdot 0 = 0$ –> ist durch 6 ohne Rest teilbar

Induktionsannahem: $n^3 + 5n = 6k$

Induktionsschritt:

$(n+1)^3 + 5(n+1) = n^3 + 3n^2 + 3n + 1 + 5n + 6$

$= (n^3 + 5n) + 3n(n + 1) + 6$

Jeder summand ist durch 6 teilbar.

3n(n + 1) ist Vielfaches von 3 und 2.

Das Prädikat $A(n)$ sei: $4^n - 1$ ist durch 3 teilbar.

1. *Induktionsverankerung $A(0)$: Die Verankerung gilt, weil*

$$4^0 - 1 = 1 - 1 = 0$$

ist durch 3 teilbar. Somit ist die Aussage $A(0)$ wahr.

2. *Induktionsschritt:*
*Wir zeigen, dass die **Implikation** $A(\ell) \Rightarrow A(\ell+1)$ für alle $\ell \in \mathbb{N}$ gilt.*
Es sei $\ell \in \mathbb{N}$ gegeben. Wir nehmen an, dass $A(\ell)$ wahr ist, d.h.:

$$\exists k \in \mathbb{N} \quad 4^\ell - 1 = 3k$$

Es gilt:

$$\begin{aligned} 4^{\ell+1} - 1 &= 4 \cdot 4^\ell - 1 = (1+3)4^\ell - 1 = 4^\ell + 3 \cdot 4^\ell - 1 \\ &\overset{A(\ell)}{=} \underbrace{4^\ell - 1}_{=3k} + 3 \cdot 4^\ell = 3k + 3 \cdot 4^\ell \\ &= 3\underbrace{(k + 4^\ell)}_{\in \mathbb{N}} \end{aligned}$$

Dies bedeutet, dass $4^{\ell+1} - 1$ durch 3 teilbar ist. Somit haben wir $A(\ell+1)$ aus $A(\ell)$ erhalten. Die Implikation gilt für alle $\ell \in \mathbb{N}$.

Summenwert

B 8: $3 + 7 + 11 + \ldots + (4n - 1) = \sum_{k=1}^{n}(4k - 1) = 2n^2 + n$ (für alle n ≥ 1)

Induktionsanfang: n = 1: linke Seite: 3
rechte Seite: $2 \cdot 1^3 + 1 = 3$

Induktionsschluss:

$\sum_{k=1}^{n+1}(4k-1) = \sum_{k=1}^{n}(4k-1) + (4(n+1) - 1) = 2n^2 + n + 4n + 4 - 1 = 2n^2 + 5n + 3$

$= (2n^2 + 4n + 2) + (n + 1) = 2(n + 1)^2 + (n + 1)$ q.e.d.

Rekursive (Folgen)

E 1: $a_1 = 2$; $a_{n+1} = 2 - \frac{1}{a_n}$ ⇒ $a_n = \frac{n+1}{n}$

Induktionsanfang: $a_2 = 2 - \frac{1}{a_1} = 2 - \frac{1}{2} = 1{,}5 = \frac{2+1}{2}$

Induktionsschluss:

$a_{n+2} = 2 - \frac{1}{a_{n+1}} = 2 - \frac{1}{\frac{n+1}{n}} = 2 - \frac{n}{n+1} = \frac{2n+2-n}{n+1} = \frac{n+2}{n+1}$

$$\sum_{k=1}^{n}(k \cdot k!) = (n+1)! - 1$$

1. Induktionsverankerung: $A(1)$:

$\sum_{k=1}^{n}(k \cdot k!) = 1 \cdot 1! = 1 = (1+1)! - 1 = 2 - 1 = 1$: wahr

2.1. Induktionsannahme: $A(n)$: wahr

$\sum_{k=1}^{n}(k \cdot k!) = (n+1)! - 1$

2.2. Induktionsbehauptung: $A(n+1)$: wahr

$\sum_{k=1}^{n}(k \cdot k!) + ((n+1) \cdot (n+1)!) = (n+2)! - 1$

2.3 Induktionsschluss $A(n) \Rightarrow A(n+1)$

$\sum_{k=1}^{n}(k \cdot k!) + ((n+1) \cdot (n+1)!) = (n+1)! - 1 + ((n+1) \cdot (n+1)!)$

$= (n+1)!\,(1 + (n+1)) - 1 = (n+1)!\,(n+2) - 1 = (n+2)! - 1$

Ungleichungen

D 1: $n^2 - 2n - 1 > 0$ (für alle n ≥ 3)

Induktionsanfang: n = 3: $3^2 - 2 \cdot 3 - 1 = 2 > 0$

Induktionsschluss:

$(n+1)^2 - 2(n+1) - 1 = n^2 + 2n + 1 - 2n - 2 - 1 = n^2 - 2 = (n^2 - 2n - 1) + (2n - 1)$

$> 2n - 1 > 0$ für alle n ≥ 3 q.e.d.

Peano-Axiome

Axiome, welche die natürlichen Zahlen und ihre Eigenschaften charakterisieren.

Axiom: Grundlegende Tatsache, die als wahr angenommen wird und nicht bewiesen wird.

P1: Die Zahl 0 ist eine natürliche Zahl: $0 \in \mathbb{N}$.

P2: Jede natürliche Zahl n hat genau einen Nachfolger $n+1$, der wiederum eine natürliche Zahl ist.

P3: Die Zahl 0 ist die einzige natürliche Zahl, die kein Nachfolger ist.

P4: Natürliche Zahlen mit gleichem Nachfolger sind gleich:

$$\forall n, m \in \mathbb{N}: \quad n + 1 = m + 1 \Rightarrow n = m$$

P5: Für jede Teilmenge $M \subseteq \mathbb{N}$ mit den Eigenschaften:

- $0 \in M$
- Ist $n \in M$, so ist auch $n + 1 \in M$

gilt: $M = \mathbb{N}$.

Rekursive Definition

$$f: \quad \mathbb{N} \to \mathbb{N}$$

$$n \mapsto f(n) = \begin{cases} 1 & \text{falls } n = 0, \\ n\,f(n-1) & \text{sonst} \end{cases}$$

Die rekursive Definition einer Funktion f besteht aus
– Rekursionsanfang: Fälle für die die Funktion f nicht wieder aufgerufen wird
– Rekursionsschritt: Vorschrift für die Berechnung des Funktionswertes f(n)

Beispiel Fibonacci

$$fib: \quad \mathbb{N} \to \mathbb{N}$$

$$n \mapsto fib(n) = \begin{cases} 0 & \text{falls } n = 0 \quad \text{(Rekursionsanfang)} \\ 1 & \text{falls } n = 1 \quad \text{(Rekursionsanfang)} \\ fib(n-1) + fib(n-2) & \text{sonst} \quad \text{(Rekursionsschritt)} \end{cases}$$

$$\begin{aligned} fib(3) &= fib(2) + fib(1) && \text{(Rekursionsschritt)} \\ &= fib(1) + fib(0) + fib(1) && \text{(Rekursionsschritt)} \\ &= 1 + 0 + 1 && \text{(Rekursionsanfang)} \\ &= 2 \end{aligned}$$

Bsp:

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

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

Beweisen, dass $F(n) = 2^{n-1}$

IA $n = 1$: $F(1) = 2^0$

IV: $F(n) = 2^{n-1}$

IS: $F(n) = 2^{n-1} \Rightarrow F(n+1) = 2^n$

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

$$= 2F(n) = 2 \cdot 2^{n-1} = 2^n$$

Kleinster Verbrecher (Methode)

Beweismethode um zu zeigen, dass alle natürlichen Zahlen eine Eigenschaft E haben.

– Man geht davon aus, dass es eine kleinste natürliche Zahl (den kleinsten Verbrecher) gäbe, die **nicht** die Eigenschaft E hat.
--> Beweis durch Widerspruch

Bsp:

$$\forall n \in \mathbb{N}: \quad n^2 + n \text{ ist eine gerade Zahl.}$$

Lösung:
Wir nehmen an: es existieren natürliche Zahlen n, für die $n^2 + n$ ungerade ist. Sei n_0 die kleinste natürliche Zahl (der kleinste Verbrecher), für die $n_0^2 + n_0$ ungerade ist.
Weil n_0 nicht Null sein kann (sonst wäre $n_0^2 + n_0$ gerade), muss es eine natürliche Zahl k geben, die n_0 als Nachfolger hat, also: $n_0 = k + 1$.
Da $k < n_0$ gilt, muss $k^2 + k$ aber gerade sein. Daraus folgt:

$$n_0^2 + n_0 = (k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = \underbrace{k^2 + k}_{gerade} + \underbrace{2k + 2}_{gerade}$$

und somit, dass $n_0^2 + n_0$ gerade ist. Dies steht im Widerspruch zur Annahme.

Teilbarkeit

Teilbarkeitsregeln

1. $\forall x, y, z \in \mathbb{Z}$ gilt: $x|y \ \wedge \ y|z \ \Rightarrow \ x|z$ (Transitivität)
2. $\forall x_1, y_1, x_2, y_2 \in \mathbb{Z}$ gilt: $(x_1|y_1 \ \wedge \ x_2|y_2) \ \Rightarrow \ x_1x_2|y_1y_2$
3. $\forall x, y_1, y_2 \in \mathbb{Z}$ gilt: $(x|y_1 \ \wedge \ x|y_2) \ \Rightarrow \ x|(\alpha y_1 + \beta y_2) \ \forall \alpha, \beta \in \mathbb{Z}$
4. $\forall x, y \in \mathbb{Z}$ gilt: $(x|y \ \wedge \ y|x) \ \Rightarrow \ (x = y \vee x = -y)$

Euklidischer Algorithmus

Berechnung ggT:
ggT(n, m) = ggT(n, m − n) = ggT(m, m − n)

ggT(45,25) Satz 24 = ggT(25, 20) kleinste Zahl und Differenz
= ggT(20, 5)
= ggT(5, 15) Satz 24: ggT(n,m) = ggT(n, m−n) = ggT(m, m−n)
= ggT(5, 10)
= ggT(5, 5) = 5

Oder noch besser mittels Rest

ggT(27, 96)
= ggT(27, 15) kleinste Zahl und Rest der Division: 27 ≡15 15
= ggT(15, 12)
= ggT(12, 3) = 3

Teilerfremd

Wenn **ggT(x, y) = 1** d.h. es gibt kein ggT

Lemma von Bézout

a) **ax + by = ggT(a, b)** x, y heissen Bézout Koeffizienten
und
b) **a(nx) + b(ny) = n · ggT(a, b)**
x und y sind Vielfache von n

Bsp.
a·3215 + b·123 = ggT(3215, 123)

1) Euklidischer Algorithmus:
3215 = 123·26 + 17 =>
123 = 17· 7 + 4 =>
17 = 4· 4 + 1 =>

2)
17 = 3215 − 26·123
4 = 123 − 7· 17
1 = 17 − 4· 4

3)
1 = 17 − 4·(123 − 7·17) = **17** − 4·123 + **28·17**
= **29·17** − 4·123 a+ba = (b+1)a
= 29·(3215 − 26·123) − 4·123
= 29·3215 − *754*·**123** − *4*·**123**
= 29·3215 − *758*·**123**
= 1

Ziel nach jedem Schritt: **a·b + c·d**

=> a = 29, b = −758
=> ggT(3215, 123) = 1

Bsp.
Finden Sie eine ganzzahlige Lösung von: 168x + 133y = 7000
1)
ggT(168, 133) = 168x + 133y
168 = 133·1 + 35
133 = 35·3 + 28
35 = 28·1 + **7** => ggT(168, 133) = **7**
28 = 7·4 + 0
2) Methode wie oben
168·4 + 133·5 = **7**
=> 168·4·1000 + 133·5·1000 = **7**·1000 = 7000
=> x = 4000, y = −5000

Besitzt die Gleichung **168x + 133y = 10** eine ganzzahlige Lösung?
Nein, weil 10 ist kein Vielfaches von 7:
168 x·n + 133 y·n = 7·n => n ≠ $\mathbb{Z}$

Bsp:

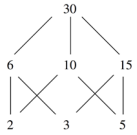
$x|90$ und $x|120$ $\quad x|90 \wedge x|120$
$T(90) \cap T(120) = T(30) = T(\text{ggt}(90,120))$
$x \in \{1,2,3,5,6,10,15,30\}$

$21|x$ und $18|x$ $\quad 21|x \wedge 18|x$
$21 \cdot i = x$
$18 \cdot j = x$
$x = k \cdot \text{kgV}(21,18) = k \cdot 126$
$x \in \{k \cdot 126, k \in \mathbb{N}\}$

Primzahlen

$\mathbb{P}$ = Menge aller Primzahlen
Natürliche Zahlen, die genau zwei natürliche Zahlen als Teiler haben.
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97...

Primzahlen genau die minimalen Elemente der Teilbarkeitsrelation-Halbordnung.



$\forall n, m \in \mathbb{N} \ (p|nm \Rightarrow p|n \vee p|m)$

Jede ganze Zahl (ohne -1, 1) besitzt einen Primfaktor.

Primfaktorenzerlegung
1350 = 10·135
= 2·5·3·45
= 2·5·3·5·9
= 2·5·3·5·3·3
= 2·3·3·3·5·5 = $2 \cdot 5^2 \cdot 3^3$

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

kgV berechnen
kgv(405, 1350) = |450·1350| ÷ ggT(405,1350) = 4050
405 = 3·3·3·3·5
1350 = 2·3·3·3·5·5
2·3·3·3·3·5·5 = 4050

Chinesischer Restsatz

Der Chinesische Restsatz hilft nur, wenn die Module teilerfremd sind. Sind sie nicht teilerfremd, so kann das System keine oder mehrere Lösungen in {0, 1, . . . , n − 1} haben.

Kongruenz: Wenn zwei oder mehrere ganze Zahlen bei der Division durch m denselben Rest haben. Ist genau dann der Fall, wenn sie sich um ein ganzzahliges Vielfaches von m unterscheiden.
a und b sind kongruent modulo m = $a \equiv b \mod m$ = $a \equiv_m b$

System von Kongruenzen

$x \equiv_{n_1} y_1$
$x \equiv_{n_2} y_2$
$\vdots$
$x \equiv_{n_k} y_k$

Lösungsmenge ist Restklasse $[x]_{\prod_{i=1}^{k} n_i}$

Simultane Kongruenz (Algorithmus)

$x \equiv_3 2$ x = 2 mod 3
$x \equiv_5 3$ x = 3 mod 5
$x \equiv_7 2$ x = 2 mod 7

Gesucht: $[x]_n$
n = 3 · 5 · 7 = 105 —> Lösungsmenge $[x]_{105}$
0 ≤ x < 105, x ∈ { 0, 1, . . . , 104 }

1. Wir berechnen:
$N_1 = n_2 \cdot n_3 = 5 \cdot 7 = 35$
$N_2 = n_1 \cdot n_3 = 3 \cdot 7 = 21$
$N_3 = n_1 \cdot n_2 = 3 \cdot 5 = 15$

2. Wir berechnen das multiplikative Inverse:
$[r_1]_{n1} = ([35]_3)^{-1} = ([2]_3)^{-1} = [2]_3$ -> Siehe Abschnitt Modulare Arithmetik
$[r_2]_{n2} = ([21]_5)^{-1} = ([1]_5)^{-1} = [1]_5$
$[r_3]_{n3} = ([15]_7)^{-1} = ([1]_7)^{-1} = [1]_7$

3. Damit berechnen wir:
$y_1N_1r_1 + y_2N_2r_2 + y_3N_3r_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

Restklasse: $[233]_{105} = [23]_{105} = \{ 23 + 105z \mid z \in \mathbb{Z} \}$ Somit: x = 23
23 = 233 mod 105 = $233 - \lfloor 233 / 105 \rfloor \cdot 105$

Modulare Arithmetik

$r \equiv_n s :\Leftrightarrow n \mid (r - s).$ «r ist Rest von s modulo n»

n ist Teiler von (r – s) r = Rest s = beliebige Zahl
$r \equiv_n s \Leftrightarrow s \bmod n = r \Leftrightarrow \text{mod}(s, n)$

Achtung, nicht zu verstehen als r%n = s, sondern s%n = r
d.h. $r \equiv_n s$ ist eine **Relation** und keine Operation.

Restklassen

$[z]_n := \{x \in \mathbb{Z} \mid x \equiv_n z\} \qquad [z]_n = \{z + yn \mid y \in \mathbb{Z}\}$

Schreibweise: $[z]_n$ oder $\bar{k}$ z ist Rest

Die Relation $\equiv_n$ ist für jede natürliche Zahl n eine Äquivalenzrelation.
$\mathbb{Z}/n$ = Menge Äquivalenzklassen: $[z]_n$ --> x mod n = z

Äquivalenzklassen wenn wir durch n teilen: $[0]_n$, $[1]_n$, $[2]_n$ ... $[n\text{-}1]_n = \mathbb{Z}/n$
$\mathbb{Z}$ mod 4 hat Äquivalenzklassen { $[0]_4$, $[1]_4$, $[2]_4$, $[3]_4$ } = $\mathbb{Z}/4$

$[x]_n + [y]_n := [x + y]_n \qquad [x]_n \cdot [y]_n := [xy]_n$

Multiplikationstafel

Verknüpfungstabellen bei Multiplikation von Restklassen:

Bsp: $\mathbb{Z}/6$ $[2]_6 \cdot [x]_6 = [4]_6$ x = 5 → (2 · x) mod 6 = 4

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Rest (= Aquivalenzklassen)

4 = (2 · 5) mod 6

Zwei Lösungen:
$[2]_6 \cdot [2]_6 = [4]_6$ → 4 mod 6 = 4
$[2]_6 \cdot [5]_6 = [10]_6 = [4]_6$ → 10 mod 6 = 4

Bei Addition kann auch eine Tabelle (Additionstafel) verwendet werden, oder so ausgerechnet werden. Bsp: $\mathbb{Z}/12$
$[9]_{12} + [x]_{12} = [2]_{12}$ → $[x]_{12} = [2]_{12} - [9]_{12}$ → $[x]_{12} = [2\text{-}9]_{12}$ → x = (12 + (-7)) = 5

Multiplikative Inverse

$[k]_n$ ist invertierbar wenn $\bar{k} \cdot \bar{r} = \bar{1}$, $(\bar{k})^{-1} = 1 / [k]_n = [r]_n = (\bar{k})^{-1} \cdot \bar{k} = \bar{1}$
$[k]_n$ ist invers zu $[r]_n$, man schreibt auch $(\bar{k})^{-1}$ für $\bar{r}$.

Bsp $\mathbb{Z}/6$: $[2]_6$ ist nicht invertierbar. $[1]_6$ ist invertierbar

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Lösen von $([x]_n)^{-1} = [r]_n$

Wenn x < n: --> Lemma von Bézout
Bsp: $([33]_{73})^{-1} = [31]_{73}$ --> $33r + 73x = 1$

Wenn x > n: --> x mod n = r
$([219]_{11})^{-1} = ([10]_{11})^{-1} = [10]_{11}$ --> 219 mod 11 = 10
d.h. $[219]_{11} \cdot [10]_{11} = [1]_{11}$ --> (219 · 10) mod 11 = 1

Bsp: Bestimmen Sie das multiplikative Inverse von $\overline{123}$ in $\mathbb{Z}/3211$.

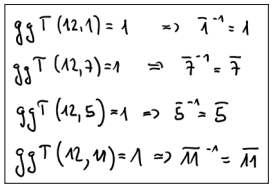
Lösung: Wir suchen die ganze Zahl r so, dass 123r + 3211x = 1.
-> Euklidischer Algorithmus:

```
ggT(3211, 123) =
3211 = 26·123 + 13
 123 =  9·13  +  6
  13 =  2· 6  +  1   ...   r = -496, x = 19
```

Das multiplikative Inverse von $\overline{123}$ in $\mathbb{Z}/3211$ ist Restklasse **$\overline{-496} = \overline{2715}$**

Bsp: Restklassen $\mathbb{Z}/12$

k	$\bar{k} \cdot \bar{x} = \bar{1}$	$ggT(k, n) = \bar{z}$	$\bar{x} = (\bar{k})^{-1}$
1	$\bar{1} \cdot \bar{x} = \bar{1}$	$ggT(1, 12) = \bar{1}$	$\bar{1}$
2	$\bar{2} \cdot \bar{x} = \bar{1}$	$ggT(2, 12) = \bar{2}$	
3	$\bar{3} \cdot \bar{x} = \bar{1}$	$ggT(3, 12) = \bar{3}$	
4	$\bar{4} \cdot \bar{x} = \bar{1}$	$ggT(4, 12) = \bar{4}$	
5	$\bar{5} \cdot \bar{x} = \bar{1}$	$ggT(5, 12) = \bar{1}$	$\bar{5}$
6	$\bar{6} \cdot \bar{x} = \bar{1}$	$ggT(6, 12) = \bar{3}$	
7	$\bar{7} \cdot \bar{x} = \bar{1}$	$ggT(7, 12) = \bar{1}$	$\bar{7}$
8	$\bar{8} \cdot \bar{x} = \bar{1}$	$ggT(8, 12) = \bar{4}$	
9	$\bar{9} \cdot \bar{x} = \bar{1}$	$ggT(9, 12) = \bar{3}$	
10	$\overline{10} \cdot \bar{x} = \bar{1}$	$ggT(10, 12) = \bar{2}$	
11	$\overline{11} \cdot \bar{x} = \bar{1}$	$ggT(11, 12) = \bar{1}$	$\overline{11}$



Bsp: ggT(5, 12) = 1 => $\bar{5}^{-1} = \bar{5} = \bar{x}$

Negative Restklassen
$[-50]_{101} = [51]_{101}$ —> -50 + 101 = 51

Prüfungsaufgaben

Relation

Jede binäre Relation auf einer Menge mit nur einem einzigen Element ist reflexiv: wahr, weil R = {(a,a)}

$s \preceq r :\Leftrightarrow s$ ist ein Anfangsabschnitt von r.

Geben Sie eine unendliche Menge $s_0, s_1, s_2, \ldots$ von Binärsequenzen an, die bezüglich der Relation $\preceq$ paarweise unvergleichbar sind. (5 Punkte)

$s_0 = 0$, $s_1 = 10$, $s_2 = 110$, $s_3 = 1110$, $s_n = 1...10$

Gerichteter Graph	Symmetrisch	Halbordnung	Totale Ordnung
	Ja	Nein	Nein
	NEIN	NEIN	NEIN
	Nein	Ja	Ja
	NEIN	NEIN	NEIN
	Nein	Ja	Nein

Logik

Alle Vielfachen einer natürlichen Zahl mit der Eigenschaft E haben selbst die Eigenschaft E.
$\forall x\,(V(x, n) \wedge E(n) \Rightarrow E(x))$

$F = \neg p \Rightarrow (\neg p \wedge \neg q)$
Ist die Formel F erfüllbar? Begründung?
Ja, wenn p wahr, weil: $\neg p \Rightarrow (\neg p \wedge \neg q) = p \vee (\neg p \wedge \neg q)$

Ist die Formel F allgemeingültig? Begründung?
Nein, wenn (p, q) = (falsch, wahr)

Mengen

Aufgabe 3.2 (4 Punkte). Es sei $X \setminus Y$ abzählbar und X überabzählbar. Können Sie etwas über die Abzählbarkeit/Überabzählbarkeit von Y aussagen? Begründen Sie Ihre Antwort.

Annahme: Y ist abzählbar
X = X\Y (abzählbar) ∪ Y (abzählbar) ist abzählbar.

Das ist ein Widerspruch. Y ist somit überabzählbar. Beweis:
X\Y (abzählbar) ∧ X (überabzählbar) => Y überabzählbar

Vollständige Induktions

Teilbarkeit

A 10: $5^n + 7$ ist durch 4 teilbar für $n \geq 0$

Induktionsanfang: n = 0: $5^0 + 7 = 8$ ist durch 4

Induktionsschluss:

$5^{n+1} + 7 = 5 \cdot 5^n + 7$
$= 4 \cdot 5^n + 5^n + 7$
$= 4 \cdot 5^n + (5^n + 7)$

Rekursion (Folgen)

E 2: $a_1 = 2$; $a_n = a_{n-1} + n \cdot 2^n$ ⇒ $a_n = 2 + (n - 1) \cdot 2^{n+1}$

Induktionsanfang: $a_2 = a_1 + 2 \cdot 2^2 = 2 + 8 = 10 = 2 + 8 = 2 + 1 \cdot 2^3 = 2 + (2 - 1) \cdot 2^{2+1}$

Induktionsschluss:

$a_{n+1} = a_n + (n+1) \cdot 2^{n+1} = 2 + (n-1) \cdot 2^{n+1} + (n+1) \cdot 2^{n+1} = 2 + 2n \cdot 2^{n+1} = 2 + n \cdot 2^{n+2}$

Rekursion

Arithmetisch: a_1 — ***+d*** —> a_2 — ***+d*** —> a_1 ... a_{n-1} — ***+d*** —> a_n

Rekursive Form: $a_{n+1} = a_n + d$

Explizite Form: $a_n = A + (n-1) \cdot d \qquad (n \geq 1)$ *n*-tes Glies

Um alle Glieder zu bestimmen braucht es:
Anfangsglied $\boldsymbol{A = a_1}$ und Differenz $\boldsymbol{d = a_2 - a_1}$

geometrisch: a_1 — **· *q*** —> a_2 — **· *q*** —> a_1 ... a_{n-1} — **· *q*** —> a_n
Wenn der Quotient zweier benachbarter Glieder immer gleich gross.
Bsp:

$$a_k = \frac{1}{2^{k-1}} \quad = \quad (a_k) = \left(1, \frac{1}{2}, \frac{1}{4}, \dots\right) \qquad q = 1/2 \qquad \frac{a_{k+1}}{a_k} = q$$

Rekursive Form: $a_{k+1} = a_k \cdot q$

Explizite Form: $a_n = A \cdot q^{n-1} \qquad (n \geq 1)$ *n*-tes Glies
Anfangsglied $a_1 = A$

Explizite Definition –> Rekursive Definition
Bsp: $a_n = 3n + 7$
$\boldsymbol{a_1} = 3{\cdot}1 + 7 = 10$ **d** = a2 –a1 = 3·2 + 7 – 10 = 3 $\boldsymbol{a_{n+1}} = a_n + 3$

Bsp: $a_n = n^2$
$\boldsymbol{a_1} = 1$
d: $a_2 - a_1 \neq a3 - a2$ –> 2. Folge (b_n), d.h. **d** = b_n und $\boldsymbol{a_{n+1}} = a_1 + b_n$
$b_n = a_{n+1} - a_1 \qquad b_1 = a_2 - a_1 = 3 \qquad b_{\boldsymbol{d}} = a_2 - a_1 = 2$
$b_n = b_1 + b_d(n-1) = 3 + 2(n-1) = 3 + 2n - 2 = \mathbf{2n + 1}$
$\boldsymbol{a_{n+1}} = a_1 + \mathbf{2n + 1}$

Kleiner Fermat

Primzahltests in der Kryptographie.
Um zu Beweisen, ob eien Zahel keine Primzahl ist.

Ist *p* eine Primzahle, dann gilt für teilerfremde ganze Zahlen (ggT(*p*, a) = 1):

$a^{p-1} \equiv_p 1$ d.h. $a^{p-1} - 1$ ist durch *p* teilbar.

Bsp: p = 7, a = –3 $(-3)^6 - 1 = 728$ 728 ist durch 7 teilbar.

Fermatsche Primzahltest
Sind *n* und *a* teilerfremd (d.h. ggT(*n*, *a*) = 1) und ist $a^{n-1} - 1$ nicht durch *n* teilbar, dann kann *n* keine Primzahl (= zusammengesetzte Zahl).

Bsp: n = 9, a = 2 ggT(9, 2) = 1 28 – 1 = 255
255 ist nicht durch 9 teilbar. Somit ist 9 eine zusammengesetzte Zahl.

Varia

Defintion gerade Zahl $\{ x \in \mathbb{N} \mid x = 2k \wedge k \in \mathbb{N} \}$
Defintion ungerade Zahl $\{ x \in \mathbb{N} \mid x = 2k+1 \wedge k \in \mathbb{N} \}$
Zahl ist Teiler von 20 $\{ x \mid x | 20 \}$ oder $\{ x \mid x$ ist Teiler von 20$\}$
Teilbarbarkeit durch drei einer natürlichen Zahl $\{ x \mid x = 3k \wedge k \in \mathbb{N} \}$

Summenzeichen

$$\sum_{k=s}^{n} (c \cdot a_k) \quad = \quad c \cdot \sum_{k=s}^{n} a_k \qquad \sum_{i=0}^{n} (ca_i + cb_i) = c \left(\sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i \right)$$

$$\sum_{k=s}^{n} (a_k + b_k) = \sum_{k=s}^{n} a_k + \sum_{k=s}^{n} b_k$$

$$\left(\sum_{k=0}^{n} (a_k \cdot b_k) \right) \neq \left(\sum_{k=0}^{n} a_k \right) \cdot \left(\sum_{k=0}^{n} b_k \right)$$

$$\sum_{k=s}^{n} a_k = \sum_{k=s-z}^{n-z} a_{k+z}$$

Rekursive Definition einer Summe

$$\sum_{i=0}^{n+1} (ca_i + cb_i) = \sum_{i=0}^{n} (ca_i + cb_i) + (ca_{n+1} + cb_{n+1}) = c \left(\sum_{i=0}^{n+1} a_i + \sum_{i=0}^{n+1} b_i \right)$$