

Mathematik I WS 15/16

Thomas Dinges¹ Jonas Wolf²

25. Januar 2016

Inoffizielles Skript für die Vorlesung Mathematik I im WS 15/16, bei Britta Dorn.
Alle Angaben ohne Gewähr. Fehler können gerne via E-Mail gemeldet werden.

¹thomas.dinges@student.uni-tuebingen.de

²mail@jonaswolf.de

Inhaltsverzeichnis

1	Logik	6
1.1	Negation	6
1.2	Konjunktion	7
1.3	Disjunktion	7
1.4	XOR	8
1.5	Implikation	8
1.6	Äquivalenz	9
1.7	Beispiel	9
1.8	Definition (logische Äquivalenz)	10
1.9	Satz (Eigenschaften logischer Aussagen)	11
1.10	Bemerkung	12
1.11	Bemerkung (Logisches Umformen)	12
1.12	Definition (Tautologie, Kontradiktion, Erfüllbarkeit)	13
1.13	Beispiel	13
1.14	Definition (Prädikatenlogik)	14
1.15	Beispiel / Bemerkung	14
1.16	Negation von All- und Existenzaussagen	15
2	Mengen	17
2.1	Definition (Georg Cantor, 1845-1918)	17
2.2	Bemerkung (Verallgemeinerung von Vereinigung und Durchschnitt)	20
2.3	Definition (kartesisches Produkt)	20
2.4	Beispiel	21
2.5	Satz (Rechenregeln für Mengen)	21
3	Beweismethoden	24
3.1	Direkter Beweis	24
3.2	Beweis durch Kontraposition	25
3.3	Beweis durch Widerspruch, indirekter Beweis	25
3.4	Vollständige Induktion	26
3.4.1	Prinzip der vollständigen Induktion	27
3.4.2	Bemerkung	28
3.4.3	Verschärftes Induktionsprinzip	30
3.5	Schubfachprinzip	31
3.5.1	Idee	31
3.5.2	Satz (Schubfachprinzip, engl.: <i>pigeon hole principle</i>)	31
3.5.3	Beispiel	32
3.6	Weitere Beweistechniken (Werkzeugkiste)	32

4	Abbildungen	35
4.1	Definition	35
4.2	Beispiele	35
4.3	Beispiele	35
4.4	Definition (Gleichheit von Abbildungen)	36
4.5	Beispiel	36
4.6	Definition (Bild, Urbild, Injektivität, Surjektivität, Bijektivität)	36
4.7	Beispiele	37
4.8	Definition (Umkehrfunktion)	38
4.9	Beispiel	38
4.10	Bemerkung	39
4.11	Definition (Hintereinanderausführung/Komposition)	39
4.12	Beispiel	39
4.13	Satz (Eigenschaften der Komposition)	39
4.14	Satz (Charakterisierung bijektiver Abbildungen)	40
4.15	Bemerkung / Definition (Endlichkeit, Mächtigkeit)	41
4.16	Satz (Wichtiger Satz für endliche Mengen)	42
4.17	Das Prinzip der rekursiven Definition von Abbildungen	43
4.18	Beispiel	43
4.19	Bemerkung	44
4.20	Beispiel (Fibonacci-Zahlen)	44
5	Relationen	46
5.1	Definition	46
5.2	Beispiel	46
5.3	Definition (Ordnungsrelation, partielle/totale/vollständige/lineare Ordnung)	47
5.4	Beispiele	47
5.5	Definition (Äquivalenzrelation)	48
5.6	Beispiele	49
5.7	Definition (Äquivalenzklassen)	49
5.8	Beispiel	50
5.9	Definition (paarweise disjunkte Mengen, disjunkte Vereinigung, Zer- legung/Partition)	50
5.10	Satz (Klasseneinteilung, Zerlegung durch Äquivalenzklassen)	50
5.11	Satz zu Äquivalenzrelationen	52
5.12	Definition (Repräsentantensystem)	53
5.13	Beispiel	53
6	Elementare Zahlentheorie	54
6.1	Definition (Teiler und Vielfaches)	54

6.2	Satz (Betrag, Eigenschaften von Teiler und Vielfachem)	54
6.3	Satz und Definition: Division mit Rest	55
6.4	Beispiel	55
6.5	Definition (Gaußklammer / Ab- und Aufrundungsfunktion)	57
6.6	Beispiel	57
6.7	Satz (b-adische Darstellung)	57
6.8	Beispiel	58
6.9	Korollar	60
6.10	Beispiel	60
6.11	Satz (Rechenregeln für modulo)	61
6.12	Bemerkung	62
6.13	Beispiele	62
6.14	Definition (Kongruenzrelationen modulo m)	64
6.15	Satz (zu Kongruenzrelationen)	64
6.16	Beispiel	65
6.17	Satz und Definition (Äquivalenzklassen, Kongruenzrelation, Repräsentantensysteme)	66
6.18	Satz (Eigenschaften der Kongruenzrelation)	66
6.19	Beispiel	67
6.20	Definition (größter gemeinsamer Teiler, kleinste gemeinsame Vielfache)	67
6.21	Bemerkung	68
6.22	Definition (teilerfremd, paarweise teilerfremd)	68
6.23	Lemma (Bestimmung des ggT)	68
6.24	Euklidischer Algorithmus	69
6.25	Satz (Bachét de Méziriac (1581 - 1638))	70
6.26	Erweiterter Euklidischer Algorithmus	71
6.27	Korollar	72
6.28	Bemerkung	72
6.29	Definition (Primzahl)	73
6.30	Satz	73
6.31	Fundamentalsatz der elementaren Zahlentheorie	73
6.32	Korollar (Euklids Lemma)	74
6.33	Korollar	75
7	Kombinatorik	76
7.1	Satz	76
7.2	Beispiel	76
7.3	Geordnete Auswahl ohne Wiederholung	77
7.4	Definition	77
7.5	Satz	78

7.6	Beispiel	78
7.7	Korollar	79
7.8	Definition	79
7.9	Geordnete Auswahl mit Wiederholung	79
7.10	Satz	80
7.11	Bemerkung / Korollar	80
7.12	Ungeordnete Auswahl ohne Wiederholung	80

1 Logik

Aussagenlogik

Eine **logische Aussage** ist ein Satz, der entweder wahr oder falsch (also nie beides zugleich) ist. Wahre Aussagen haben den Wahrheitswert 1 (auch wahr, w, true, t), falsche den Wert 0 (auch falsch, f, false).

Notation: Aussagenvariablen $A, B, C, \dots A_1, A_2$.

Beispiele:

- 2 ist eine gerade Zahl (1)
- Heute ist Montag (1)
- 2 ist eine Primzahl (1)
- 12 ist eine Primzahl (0)
- Es gibt unendlich viele Primzahlen (1)
- Es gibt unendlich viele Primzahlzwillinge (Aussage, aber unbekannt, ob 1 oder 0)
- 7 (keine Aussage)
- Ist 173 eine Primzahl? (keine Aussage)

Aus einfachen Aussagen kann man durch logische Verknüpfungen (**Junktoren**, z.B. und, oder, ...) kompliziertere bilden. Diese werden Ausdrücke genannt (auch Aussagen sind Ausdrücke). Durch sogenannte **Wahrheitstafeln** gibt man an, wie der Wahrheitswert der zusammengesetzten Aussage durch die Werte der Teilaussagen bedingt ist. Im folgenden seien A, B Aussagen.

Die wichtigsten Junktoren:

1.1 Negation

Verneinung von A : $\neg A$ (auch \bar{A}), *nicht* A , ist die Aussage, die genau dann wahr ist, wenn A falsch ist.

Wahrheitstafel:

A	$\neg A$
1	0
0	1

Beispiele:

- A : 6 ist durch 3 teilbar. (1)
- $\neg A$: 6 ist nicht durch 3 teilbar. (0)
- B : 4,5 ist eine gerade Zahl (0)
- $\neg B$: 4,5 ist keine gerade Zahl. (1)

1.2 Konjunktion

Verknüpfung von A und B durch *und*: $A \wedge B$ ist genau dann wahr, wenn A und B gleichzeitig wahr sind.

Wahrheitstafel:

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Beispiele:

- $\underbrace{6 \text{ ist eine gerade Zahl}}_{A(1)} \text{ und } \underbrace{\text{durch 3 teilbar}}_{B(1)}$. (1)
- $\underbrace{9 \text{ ist eine gerade Zahl}}_{A(0)} \text{ und } \underbrace{\text{durch 3 teilbar}}_{B(1)}$. (0)

1.3 Disjunktion

oder: $A \vee B$

Wahrheitstafel:

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

\triangle Einschließendes oder, kein entweder...oder.

Beispiele:

- 6 ist gerade oder durch 3 teilbar. (1)

- 9 ist gerade oder durch 3 teilbar. (1)
- 7 ist gerade oder durch 3 teilbar. (0)

1.4 XOR

entweder oder: $A \text{ xor } B$, $A \oplus B$ (ausschließendes oder, exclusive or).

Wahrheitstafel:

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

1.5 Implikation

wenn, dann, $A \Rightarrow B$:

- wenn A gilt, dann auch B
- A impliziert B
- aus A folgt B
- A ist hinreichend für B,
- B ist notwendig für A

Wahrheitstafel:

A	B	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Merke: *ex falso quodlibet* : aus einer falschen Aussage kann man alles folgern!

(Die Implikation $A \Rightarrow B$ sagt nur, dass B wahr sein muss, falls A wahr ist. Sie sagt nicht, dass B tatsächlich wahr ist.)

Beispiele:

- Wenn $1 = 0$, bin ich der Papst. (1)

1.6 Äquivalenz

genau dann wenn, $A \Leftrightarrow B$ (dann und nur dann wenn, g.d.w, äquivalent, if and only if, iff)

Wahrheitstafel:

A	B	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Beispiele:

- Heute ist Montag genau dann wenn morgen Dienstag ist. (1)
- Eine natürliche Zahl $\underbrace{\text{ist durch 6 teilbar}}_A$ g. d. w. sie $\underbrace{\text{durch 3 teilbar ist.}}_B$ (0)

$$A \Rightarrow B \text{ (1)}$$

$$B \Rightarrow A \text{ (0)}$$

Festlegung

\neg bindet stärker als alle anderen Junktoren: $(\neg A \wedge B)$ heißt $(\neg A) \wedge B$

1.7 Beispiel

a)

Wann ist der Ausdruck $(A \vee B) \wedge \neg(A \wedge B)$ wahr?

→ Wahrheitstafel

A	B	$(A \vee B)$	$(A \wedge B)$	$\neg(A \wedge B)$	$(A \vee B) \wedge \neg(A \wedge B)$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

△ Klammerung relevant

Welche Wahrheitswerte ergeben sich für

- $A \vee (B \wedge \neg A) \wedge B$?

- $A \vee B \wedge \neg A \wedge B$?

$(A \vee B) \wedge \neg(A \wedge B)$ und $(A \oplus B)$ haben dieselben Wahrheitstafeln. Ausdrücke sehen unterschiedlich aus (Syntax), aber haben dieselbe Bedeutung (Semantik). Dies führt zu *1.8 Definition*.

b)

Wann ist $(A \wedge B) \Rightarrow \neg(C \vee A)$ falsch?

→ Wahrheitstafel: alle möglichen Belegungen von A, B, C mit 0/1

A	B	C	$(A \wedge B)$	$\neg(C \vee A)$	$(A \wedge B) \Rightarrow \neg(C \vee A)$
1	1	1	1	0	0
1	1	0	1	0	0
1	0	1	0	0	1
1	0	0	0	0	1
0	1	1	0	0	1
0	1	0	0	1	1
0	0	1	0	0	1
0	0	0	0	1	1

oder überlegen:

$(A \wedge B) \Rightarrow \neg(C \vee A)$ ist nur 0, wenn

$(A \wedge B) = 1$, also $A = 1$ und $B = 1$

und

$\neg(C \vee A) = 0$ ist.

(Wissen: $A = 1$), also $C = 0$ oder $C = 1$ möglich.

1.8 Definition

Haben zwei Ausdrücke α und β bei jeder Kombination von Wahrheitswerten ihrer Aussagevariablen den gleichen Wahrheitswert, so heißen sie logisch äquivalent; man schreibt $\alpha \equiv \beta$. (\equiv ist kein Junktor, entspricht '=')

Es gilt: Falls $\alpha \equiv \beta$ gilt, hat der Ausdruck $\alpha \Leftrightarrow \beta$ immer den Wahrheitswert 1.

1.9 Satz

Seien A, B, C Aussagen. Es gelten folgende logische Äquivalenzen:

a) **Doppelte Negation:** $A \equiv \neg(\neg A)$

b) **Kommutativität von $\wedge, \vee, \oplus, \Leftrightarrow$:**

- $(A \wedge B) \equiv (B \wedge A)$
- $(A \vee B) \equiv (B \vee A)$
- $(A \oplus B) \equiv (B \oplus A)$
- $(A \Leftrightarrow B) \equiv (B \Leftrightarrow A)$

\triangleq gilt nicht für ' \Rightarrow ' !! ($A \Rightarrow B \not\equiv B \Rightarrow A$)

c) **Assoziativität von $\wedge, \vee, \oplus, \Leftrightarrow$:**

- $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$
- $(A \vee B) \vee C \equiv A \vee (B \vee C)$
- $(A \oplus B) \oplus C \equiv A \oplus (B \oplus C)$
- $(A \Leftrightarrow B) \Leftrightarrow C \equiv A \Leftrightarrow (B \Leftrightarrow C)$

d) **Distributivität:**

- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

e) **Regeln von DeMorgan:**

- $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $\neg(A \vee B) \equiv \neg A \wedge \neg B$

f) $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

g) $A \Rightarrow B \equiv \neg A \vee B$

h) $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

(Alle Äquivalenzen gelten auch, wenn die Aussagevariablen durch Ausdrücke ersetzt werden.)

Beweis: Jeweils mittels Wahrheitstafel (Übung!), zum Beispiel:

a)

A	$\neg A$	$\neg(\neg A)$
1	0	1
0	1	0

e)

A	B	$(A \wedge B)$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A \vee \neg B)$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

1.10 Bemerkung

(1.9 f): $(A \Rightarrow B) \equiv \underbrace{(\neg B \Rightarrow \neg A)}$

wird Kontraposition genannt, wichtig für Beweis. Wird im Sprachgebrauch oft falsch verwendet.

Beispiel: Pit ist ein Dackel. \Rightarrow Pit ist ein Hund.
 \underset{A} \underset{B}

äquivalent zu: $(\neg B) \Rightarrow (\neg A)$

Pit ist kein Hund. \Rightarrow Pit ist kein Dackel.

aber nicht zu: $B \Rightarrow A$

Pit ist ein Hund. \Rightarrow Pit ist ein Dackel.

und nicht zu: $\neg A \Rightarrow \neg B$

Pit ist kein Dackel. \Rightarrow Pit ist kein Hund.

Beispiel: Sohn des Logikers / bellende Hunde (\rightarrow Folien)

1.11 Bemerkung (Logisches Umformen)

Sei α ein Ausdruck. Ersetzen von Teilausdrücken von α durch logisch äquivalente Ausdrücke liefert einen zu α äquivalenten Ausdruck. So erhält man eventuell kürzere/einfachere Ausdrücke, zum Beispiel:

$$\neg(A \Rightarrow B) \stackrel{1.9 \text{ g)}}{=} \neg(\neg A \vee B) \stackrel{1.9 \text{ e)}}{=} \neg(\neg A) \wedge (\neg B) \stackrel{1.9 \text{ a)}}{=} A \wedge \neg B$$

1.12 Definition

Ein Ausdruck heißt Tautologie, wenn er für jede Belegung seiner Aussagevariablen, immer den Wert 1 annimmt. Hat er immer den Wert 0, heißt er Kontradiktion. Gibt es mindestens eine Belegung der Aussagevariablen, so dass der Ausdruck Wert 1 hat, heißt er erfüllbar.

1.13 Beispiel

- a) $A \vee \neg A$ Tautologie
 $A \wedge \neg A$ Kontradiktion
- b) $\neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$ Tautologie (vergleiche Beispiel in 1.11).
 $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$ Tautologie (vergleiche Beispiel in 1.9g).
- c) $A \wedge \neg B$ ist erfüllbar (durch $A = 1, B = 0$).

Prädikatenlogik

Eine Aussageform ist ein sprachliches Gebilde, dass formal wie eine Aussage aussieht, aber eine oder mehrere Variablen enthält.

Beispiel: $P(x) : \underbrace{x}_{\text{Variable}} \underbrace{< 10}_{\text{Prädikat (Eigenschaft)}}$

$Q(x) : x$ studiert Informatik

$R(y) : y$ ist Primzahl und $y^2 + 2$ ist Primzahl.

Eine Aussageform $P(x)$ wird zur Aussage, wenn man die Variable durch ein konkretes Objekt ersetzt. Dies ist nur dann sinnvoll, wenn klar ist, welche Werte für x erlaubt sind, daher wird oft die zugelassene Wertemenge mit angegeben. (hier Vorgriff auf Kapitel *Mengen*)

Im Beispiel:

$P(3)$ ist wahr, $P(42)$ falsch.

$R(2)$ ist falsch, $R(3)$ ist wahr.

Oft ist die Frage interessant, ob es wenigstens ein x gibt, für das $P(x)$ wahr ist, oder ob $P(x)$ sogar für alle zugelassenen x wahr ist.

1.14 Definition

Sei $P(x)$ eine Aussageform.

a) Die Aussage *Für alle x (aus einer bestimmten Menge M) gilt $P(x)$* ist wahr genau dann wenn $P(x)$ für alle in Frage kommenden x wahr ist.

Schreibweise: $\underbrace{\forall}_{\text{für alle, für jedes}} \underbrace{x}_{\text{aus der Menge } M} \underbrace{\in M}_{\text{gilt}} \underbrace{:}_{\text{Eigenschaft}} \underbrace{P(x)}_{\text{Eigenschaft}}$

auch $\underbrace{\forall}_{x \in M} P(x)$.

Das Symbol \forall heißt All-Quantor, die Aussage All-Aussage.

b) Die Aussage *Es gibt (mindestens) ein x aus M , das die Eigenschaft $P(x)$ besitzt* ist wahr, g.d.w $P(x)$ für mindestens eines der in Frage kommenden x wahr ist.

Schreibweise: $\underbrace{\exists}_{\text{es gibt, es existiert}} \underbrace{x \in M}_{\text{so dass gilt}} \underbrace{:}_{\text{Eigenschaft}} \underbrace{P(x)}_{\text{Eigenschaft}}$

\exists heißt Existenzquantor, die Aussage Existenzmenge.

1.15 Beispiel / Bemerkung

Übungsgruppe G: $\underbrace{a}_{\text{Anna}} \underbrace{b}_{\text{Bob}} \underbrace{c}_{\text{Clara}}$

$B(x)$: x ist blond.

$W(x)$: x ist weiblich.

$B(a) = 1$

$W(b) = 0$

1. Alle Studenten der Gruppe sind blond. (1)

$\forall x \in G: x \text{ ist blond}$

$\forall x \in G: B(x)$ (1)

Das bedeutet: $a \text{ blond} \wedge b \text{ blond} \wedge c \text{ blond}$

$\underbrace{B(a)}_1 \wedge \underbrace{B(b)}_1 \wedge \underbrace{B(c)}_1$

\forall ist also eine Verallgemeinerung der Konjunktion.

2. Alle Studenten der Gruppe sind weiblich. (0)

$$\underbrace{W(a)}_1 \wedge \underbrace{W(b)}_0 \wedge \underbrace{W(c)}_1 \quad (0)$$

3. Es gibt einen Studenten der Gruppe, der weiblich ist. (1)

$$\exists x \in G: W(x) \quad (1)$$

$$\text{bedeutet: } \underbrace{W(a)}_1 \vee \underbrace{W(b)}_0 \vee \underbrace{W(c)}_1 = 1$$

\exists ist verallgemeinerte Disjunktion.

4. Aussage A: Alle Studenten der Gruppe sind weiblich. (0)

Verneinung von A? $\neg A$

△ Nicht korrekt wäre: Alle Studenten der Gruppe sind männlich. (Wahrheitswert ist auch 0)

Korrekt: Nicht alle Studenten der Gruppe sind weiblich (1) Es gibt (mindestens) einen Studenten der Gruppe, der nicht weiblich ist. (1)

allgemeiner:

1.16 Negation von All- und Existenzaussagen

$$\text{a) } \neg(\forall x \in M : P(x)) \equiv \exists x \in M : \neg P(x)$$

$$\text{b) } \neg(\exists x \in M : P(x)) \equiv \forall x \in M : \neg P(x)$$

(Verallgemeinerung der Regeln von DeMorgan) (vergleiche Beispiel 1.15, 4):

$$\neg(\forall x \in G : W(x))$$

$$\equiv \neg(W(a) \wedge W(b) \wedge W(c))$$

$$\underbrace{\equiv}_{\text{DeMorgan}} (\neg W(a)) \vee (\neg W(b)) \vee (\neg W(c))$$

$$\equiv \exists x \in G : \neg W(x)$$

Bemerkung

Aussageformen können auch mehrere Variablen enthalten, Aussagen mit mehreren Quantoren sind möglich.

Zum Beispiel:

$$\exists x \in X \quad \exists y \in Y : P(x, y)$$

$$\exists x \in X \quad \forall y \in Y : P(x, y)$$

$$\forall x \in X \quad \exists y \in Y : P(x, y)$$

$$\forall x \in X \quad \forall y \in Y : P(x, y)$$

Negation dann durch mehrfaches Anwenden von 1.16, zum Beispiel:

$$\neg(\forall x \in X \quad \forall y \in Y \quad \exists z \in Z : P(x, y, z))$$

$$\equiv \exists x \in X : \neg(\forall y \in Y \quad \exists z \in Z : P(x, y, z))$$

$$\equiv \exists x \in X \quad \exists y \in Y : \neg(\exists z \in Z : P(x, y, z))$$

$$\equiv \exists x \in X \quad \exists y \in Y \quad \forall z \in Z : \neg P(x, y, z)$$

Also:

ändere \exists in \forall ,

\forall in \exists ,

verneine Prädikat.

2 Mengen

2.1 Definition (Georg Cantor, 1845-1918)

Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterscheidbaren Objekten (Elementen) unserer Anschauung oder unseres Denkens zu einem Ganzen.

Im Folgenden seien A, B Mengen.

- a) $x \in A : x$ ist Element der Menge A
 $x \notin A : x$ ist nicht Element der Menge A
oder auch:
 $A \ni x : x$ ist Element der Menge A
 $A \not\ni x : x$ ist nicht Element der Menge A

- b) Eine Menge kann beschrieben werden durch:

- Aufzählung ihrer Elemente, zum Beispiel:
 $M_1 = \{a, b, c\}$ ($= \{c, a, b\}$, d.h. Reihenfolge spielt keine Rolle)
Achtung: Keine Wiederholungen!
 $M_2 = \{\odot, \odot\}$
 $M_3 = \{3, \{1, 2\}, M_1\}$
geht nur bei endlichen Mengen oder bestimmten unendlichen Mengen, zum Beispiel:
 $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ Menge der natürlichen Zahlen
 $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}$ Menge der natürlichen Zahlen mit der Null
 $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ Menge der ganzen Zahlen
- Charakterisierung ihrer Elemente:
 $A = \{x \mid x \text{ besitzt die Eigenschaft } E\}$, z.B.:
 $A = \{n \mid n \in \mathbb{N} \text{ und } n \text{ ist gerade}\}$

sprich: "mit der Eigenschaft"

 $= \{2, 4, 6, 8, \dots\}$
 $= \{x \mid \exists k \in \mathbb{N} \text{ mit } x = 2 \cdot k\} = \{2k \mid k \in \mathbb{N}\}$

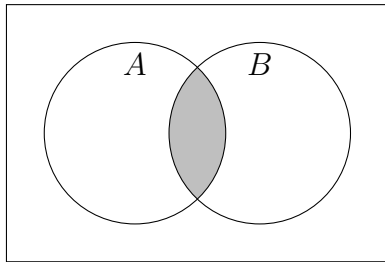
Bsp: $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ Menge der rationalen Zahlen

- c) Mit \emptyset bezeichnen wir die Menge ohne Elemente (leere Menge)
- d) Mit $|A|$ bezeichnen wir die Anzahl der Elemente der Menge A (Kardinalität oder Mächtigkeit von A), zum Beispiel:

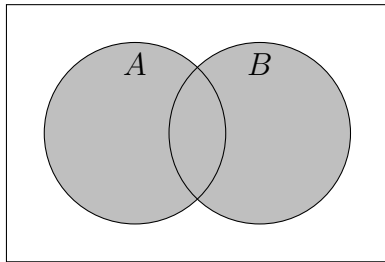
$$|\{1, a, *\}| = 3, \quad |\emptyset| = 0, \quad |\mathbb{N}| = \infty, \quad |\{\mathbb{N}\}| = 1$$

- e) $A \cap B \underbrace{:= \{x \mid x \in A \wedge x \in B\}}_{\text{wird definiert als}}$ heißt Durchschnitt oder Schnittmenge von A und B .

Grafische Veranschaulichung: Venn-Diagramm (\triangle gilt nicht als Beweis)



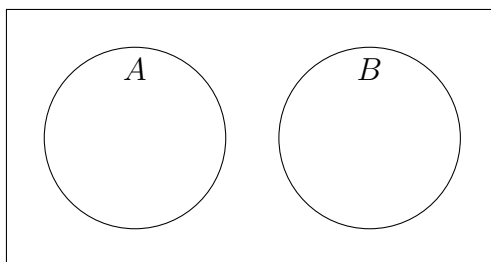
- f) $A \cup B := \{x \mid x \in A \vee x \in B\}$ heißt Vereinigung von A und B .



Beispiele: $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $C = \{4\}$

$$\begin{aligned} A \cap B &= \{2, 3\}, \\ A \cap C &= \emptyset, \\ B \cap C &= \{4\} = C, \\ A \cup B &= \{1, 2, 3, 4\} \end{aligned}$$

- g) A und B heißen disjunkt, falls gilt $A \cap B = \emptyset$



- h) A heißt Teilmenge von B , $A \subseteq B$, falls gilt:
 $x \in A \Rightarrow x \in B$

Oder in Worten: Jedes Element von A ist auch Element von B .

Dasselbe bedeutet die Notation

$$B \supseteq A$$

(B ist Obermenge von A)

Beispiel: $\{1, 2\} \subseteq \{1, 2, 3\} \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{R}$ (reelle Zahlen)

Es gilt: $\emptyset \subseteq A$ für jede Menge A .

Achtung: Unterschied \subseteq, \in !

Zum Beispiel:

$A = \{1, \mathbb{N}\}$ (hier ist die Menge \mathbb{N} ein Element von A , keine Teilmenge!)

$$1 \in A, \quad \mathbb{N} \in A, \quad \mathbb{N} \not\subseteq A, \quad 2 \notin A, \quad \{1\} \subseteq A$$

- i) Zwei Mengen A, B heißen gleich ($A = B$, falls gilt: $A \subseteq B$ und $B \subseteq A$ (also $x \in A \Rightarrow / \Leftarrow / \Leftrightarrow x \in B$).

Darin liegt ein Beweisprinzip: Man zeigt $A = B$, indem man zeigt:

- $x \in A \Rightarrow x \in B$
- $x \in B \Rightarrow x \in A$ (mehr später)

Beispiel:

$$A = \{2, 3, 4\}, \quad B = \{x \in \mathbb{N} \mid x > 1 \text{ und } x < 5\}$$

$$A = B$$

- j) $A \subsetneq B$ ($A \subsetneq B$) bedeutet $A \subseteq B$, aber $A \neq B$.

(d.h. $\exists x \in B$ mit $x \notin A$, aber $x \in B$)

(A ist echte Teilmenge von B .)

- k) Mit $P(A) := \{B \mid B \text{ ist eine Teilmenge von } A\} = \{B \mid B \subseteq A\}$ bezeichnen wir die Menge aller (echten oder nicht echten) Teilmengen von A , die sogenannte Potenzmenge von A . ($\emptyset \subseteq A \forall A, A \subseteq A \forall A$)

Beispiel:

$$A = \{1, \}, P(A) = \{\emptyset, \underbrace{\{1\}}_A\}$$

$$B = \{1, 2\}, P(B) = \{\emptyset, \{1\}, \{2\}, \underbrace{\{1, 2\}}_B\}$$

$$C = \{1, 2, 3\}, P(C) = \dots \text{ (8 Elemente)}$$

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

Was ist $P(P(A))$?

$$P(P(A)) = P(\{\emptyset, \{1\}\}) = \{\emptyset, \{\emptyset\}, \{1\}, \{\emptyset, \{1\}\}\}$$

l) $A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}$ heißt die Differenz (*A ohne B*).

Ist $A \subseteq X$ mit einer Obermenge X , so heißt $X \setminus A$ das Komplement von A (bezüglich X). Wir schreiben A_X^C oder kurz A^C (wenn X aus dem Kontext klar ist).

m) $A \triangle B := (A \setminus B) \cup (B \setminus A)$ heißt die symmetrische Differenz von A und B .

2.2 Bemerkung

Verallgemeinerung der Vereinigung und des Durchschnitts:

$$A_1 \cap A_2 \cap \dots \cap A_n = \{x \mid x \in A_1 \wedge x \in A_2 \wedge \dots \wedge x \in A_n\}$$

$$=: \bigcap_{i=1}^n A_i$$

$$A_1 \cup \dots \cup A_n = \{x \mid x \in A_1 \vee \dots \vee x \in A_n\}$$

$$=: \bigcup_{i=1}^n A_i$$

Beziehungsweise noch allgemeiner:

Sei S eine Menge von Mengen (*System von Mengen*)

$$\cap A = \{x \mid x \in A \forall A \in S\}$$

$$A \subset S$$

$$\cup A = \{x \mid \exists A \in S \text{ mit } x \in A\}$$

$$A \in S$$

2.3 Definition

Seien A, B Mengen.

$$\underbrace{A \times B}_{\text{Kreuz}} := \{(a, b) \mid a \in A, b \in B\}$$

Die Menge aller geordneten Paare, heißt kartesisches Produkt von A und B (nach René Descartes, 1596 - 1650).

Dabei legen wir fest: $(a, b) = (a', b')$ mit $(a, a' \in A, b, b' \in B) :$
 $\Leftrightarrow a = a'$ und $b = b'$.

Allgemein sei für Mengen $A_1, \dots, A_n (n \in \mathbb{N})$

$A_1 \times A_2 \times \dots \times A_n := \{a_1, a_2, \dots, a_n \mid a_i \in A_i, \forall i = 1 \dots n\}$

die Menge aller geordneten n-Tupel (mit analoger Gleichheitsdefinition).

($n = 2$: Paare, $n = 3$: Tripel)

Schreibweise:

$$A_1 \times \dots \times A_n : n =: \bigtimes_{i=1}^n A_i$$

Ist eine der Mengen A_1, \dots, A_n leer, setzen wir $A_1 \times \dots \times A_n = \emptyset$.

Statt $A \times A$ schreiben wir auch A^2 , statt $\underbrace{A \times \dots \times A}_{n\text{-Faktoren}} = A^n$.

2.4 Beispiel

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

$$(1, 3) \in A \times B, \underbrace{(3, 1)}_{B \times A} \notin A \times B,$$

$$\left(\underbrace{3}_{B \times B}, \underbrace{3}_{A \times A}\right) \in A \times B \in B \times A$$

$$(1, 2) \in A \times B, \in A \times A$$

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$$

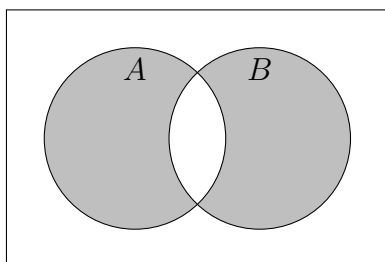
$$B \times A = \dots$$

$$B \times B = B^2 = \{(3, 3), (3, 4), (4, 3), (4, 4)\}$$

2.5 Satz (Rechenregeln für Mengen)

Seien A, B, C, X Mengen. Dann gilt:

- a) $A \cup B = B \cup A$
 $A \cap B = B \cap A$
 (Kommutativgesetz)
- b) $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$
 (Assoziativgesetz)
- c) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
 $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
 (Distributivgesetz)
- d) $A, B \subseteq X$, dann
 $(A \cap B)_X^C = A_X^C \cup B_X^C$
 $(A \cup B)_X^C = A_X^C \cap B_X^C$
 (Regeln von DeMorgan)
- e) $A \subseteq X$, dann $(A_X^C)_X^C = A$
- f) $A \Delta B = (A \cup B) \setminus (A \cap B)$
 $(= \{x \mid x \in A \oplus x \in B\})$



- g) $A \cap B = A$ genau dann, wenn $A \subseteq B$
 $(A \cap B) = A \Leftrightarrow A \subseteq B$
- h) $A \cup B = A \Leftrightarrow B \subseteq A$

Beweis

a) $A \cup B = \{x \mid x \in A \vee x \in B\}$
 $\stackrel{1.9 \text{ b)}}{=} \{x \mid x \in B \vee x \in A\} = B \cup A$

$A \cap B$ analog

- b), c) Übung, wie a)
 benutze Assoziativgesetz (1.9 c)) bzw. Distributivgesetz (1.9 d)) für logische

Äquivalenzen.

$$\begin{aligned} \text{d) } (A \cap B)_X^C &= \{x \mid x \in X \setminus (A \cap B)\} \\ &= \{x \mid x \in X \wedge (x \notin (A \cap B))\} \\ &= \{x \mid x \in X \wedge \neg(x \in (A \cap B))\} \\ &= \{x \mid x \in X \wedge \neg(x \in A \wedge x \in B)\} \\ &= \{x \mid x \in X \wedge (x \notin A \vee x \notin B)\} \end{aligned}$$

De Morgan 1.9 e)

$$\begin{aligned} &= \{x \mid ((x \in X) \wedge (x \notin A)) \vee ((x \in X) \wedge (x \notin B))\} \\ &= A_X^C \cup B_X^C \end{aligned}$$

2. Regel analog

e) ähnlich

f) g) h) später

3 Beweismethoden

Ein mathematischer Beweis ist die Herleitung der Wahrheit (oder Falschheit) einer Aussage aus einer Menge von Axiomen (nicht beweisbare Grundtatsachen) oder bereits bewiesenen Aussagen mittels logischen Folgerungen.

Bewiesene Aussagen werden Sätze genannt.

Lemma - Hilfssatz, der nur als Grundlage für wichtigeren Satz formuliert und bewiesen wird.

Theorem - wichtiger Satz

Korollar - einfache Folgerung aus Satz, z.B. Spezialfall

Definition - Benennung/Bestimmung eines Begriffs/Symbols

□ - Zeichen für Beweisende (■, q.e.d., wzbw...)

Mathematische Sätze haben oft die Form:

Wenn V (Voraussetzung) gilt, dann gilt auch B (Behauptung)

(V, B : Aussagen), kurz: $V \Rightarrow B$

Zu zeigen ist also, dass $V \Rightarrow B$ eine wahre Aussage ist.

3.1 Direkter Beweis

Gehe davon aus, dass V wahr ist, folgere daraus, dass B wahr ist.

[Sei V wahr, \Rightarrow ...
 \Rightarrow ...
 \Rightarrow ...
 \vdots
 $\Rightarrow B$ ist wahr]

Beispiel: $\underbrace{\text{Sei } n \in \mathbb{N}. \text{ Ist } n \text{ gerade}}_V, \underbrace{\text{so ist auch } n^2 \text{ gerade}}_B$.

Beweis: Sei $n \in \mathbb{N}$ gerade. // V ist wahr $\Rightarrow n = 2 \cdot k$ für ein $k \in \mathbb{N}$
($\exists k \in \mathbb{N}$ mit $n = 2 \cdot k$)

$$\Rightarrow n^2 = (2 \cdot k)^2 = 4 \cdot k^2 = 2 \cdot (2k^2)$$

$$\Rightarrow n^2 \text{ ist gerade.}$$

// B ist wahr

□

3.2 Beweis durch Kontraposition

vgl. Satz 1.9 f) $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Statt $V \Rightarrow B$ zu zeigen, können wir also auch $\neg B \Rightarrow \neg V$ zeigen.

[Es gelte $\neg B \Rightarrow \dots$
 $\Rightarrow \dots$
 $\Rightarrow \dots$
 \vdots
 \Rightarrow es gilt $\neg V$]

Beispiel: Sei $n \in \mathbb{N}$.

Ist n^2 gerade, so ist auch n gerade.

$\underbrace{\hspace{10em}}_V \quad \underbrace{\hspace{10em}}_B$

Beweis durch Kontraposition:

Sei n ungerade.

// $\neg B$ gilt.

$$\Rightarrow n = 2k + 1 \text{ für ein } k \in \mathbb{N}_0$$

$$\Rightarrow n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = \underbrace{2(2k^2 + 2k)}_{\text{gerade}} + 1$$

$$\underbrace{\hspace{10em}}_{\text{ungerade}}$$

$\Rightarrow n^2$ ist ungerade.

// $\neg V$ gilt.

□

3.3 Beweis durch Widerspruch, indirekter Beweis

Zu zeigen ist Aussage A . Wir gehen davon aus, dass A nicht gelte ($\neg A$ ist wahr) und folgern durch logische Schlüsse eine zweite Aussage B , von der wir wissen, dass sie falsch ist. Wenn alle logischen Schlüsse korrekt waren, muss also $\neg A$ falsch gewesen sein, also A wahr.

($((\neg A \Rightarrow B) \wedge (\neg B)) \Rightarrow A$ ist Tautologie)

Beispiel: [Euklid] $\sqrt{2} \notin \mathbb{Q}$

Beweis: Wir nehmen an, dass die Aussage falsch ist, also $\sqrt{2} \in \mathbb{Q}$ gilt, das heißt $\sqrt{2} = \frac{p}{q}$ mit $p, q \in \mathbb{Z} (q \neq 0)$ teilerfremd (vollständig gekürzter Bruch)

$$\Rightarrow 2 = \frac{p^2}{q^2}$$

$\Rightarrow p^2 = 2q^2$, also ist p^2 gerade, damit aber auch p gerade (Beispiel in 3.2), also $p = 2 \cdot r$ mit $r \in \mathbb{Z}$.

$$\Rightarrow p^2 = (2r)^2 = 2q^2$$

$$\Rightarrow 4r^2 = 2q^2$$

$$\Rightarrow 2r^2 = q^2$$

$$\Rightarrow q^2 \text{ gerade}$$

$$\Rightarrow q \text{ gerade}$$

Also: p gerade, q gerade, Widerspruch zu p, q teilerfremd.

Also war die Annahme falsch, es muss $\sqrt{2} \notin \mathbb{Q}$ gelten. \square

3.4 Vollständige Induktion

Eine Methode, um Aussagen über natürliche Zahlen zu beweisen.

Beispiel: Gauß

$$1 + 2 + \dots + 100 = ?$$

$$\begin{array}{rrrrr} 1 & 2 & 3 & \dots & 50 \\ + 100 & 99 & 98 & \dots & 51 \\ \hline 101 & 101 & 101 & \dots & 101 \end{array}$$

$$50 \cdot 101 = 5050$$

$$(= \frac{100}{2} \cdot 101)$$

Allgemein:

$$1 + 2 + 3 + \dots + n \quad \underbrace{=}_{\text{Vermutung}} \quad \frac{n(n+1)}{2}$$

$$(n \in \mathbb{N})$$

3.4.1 Prinzip der vollständigen Induktion

Sei $n_0 \in \mathbb{N}$ fest vorgegeben (oft $n_0 = 1$).

Für jedes $n \geq n_0, n \in \mathbb{N}$, sei $A(n)$ eine Aussage, die von n abhängt.

Es gelte:

1. $A(n_0)$ ist wahr (*Induktionsanfang*)
2. $\forall n \in \mathbb{N}, n \geq n_0$: $\underbrace{\text{Ist } A(n) \text{ wahr,}}_{\text{Induktionsvoraussetzung}} \quad \underbrace{\text{so ist } A(n+1) \text{ wahr.}}_{\text{Induktionsbehauptung}} \text{ (Induktionsschritt)}$

Dann ist die Aussage $A(n)$ für alle $n \geq n_0$ wahr. (*Dominoprinzip*)

(Bemerkung: gilt auch für \mathbb{N}_0 ($n_0 = 0$ auch möglich) und für $n_0 \in \mathbb{Z}$, Behauptung gilt dann für alle $n \in \mathbb{Z}$ mit $n \geq n_0$).

Beispiel:

a) Kleiner Gauß $1 + 2 + \dots + n = \frac{n(n+1)}{2} \forall n \in \mathbb{N}$

Beweis:

$$A(n) : 1 + 2 + \dots + n = \frac{n(n+1)}{2}$$

- Induktionsanfang ($n = 1$) : $A(1) : 1 = \frac{1 \cdot (1+1)}{2}$
- Induktionsschritt:

Induktionsvoraussetzung:

sei $n \geq 1$. Es gelte $A(n)$, d.h. $1 + \dots + n = \frac{n(n+1)}{2}$

Induktionsbehauptung:

Es gilt $A(n+1)$, d.h. $1 + \dots + n + (n+1) = \frac{(n+1)(n+1+1)}{2}$

$$\begin{aligned} \text{Beweis: } \underbrace{1 + 2 + \dots + n}_{\text{Ind.vor.}} + (n+1) &= \underbrace{\frac{n(n+1)}{2}}_{\text{Ind.vor.}} + (n+1) \\ &= \frac{n^2 + n + 2n + 2}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

$$A(n+1)$$

□

b) $A(n) : 2^n \geq n \forall n \in \mathbb{N}$

- Induktionsanfang: ($n = 1$) : $A(1)$ gilt: $2^1 \geq 1$

- Induktionsschritt:

Induktionsvoraussetzung:

Sei $n \geq 1$. Es gelte $A(n)$, d.h. $2^n \geq n$

Induktionsbehauptung: (Zu zeigen!):

Es gilt $A(n+1)$, d.h. $2^{n+1} \geq n+1$.

Beweis: $2^{n+1} = 2 \cdot 2^n \underset{\text{Ind.vor.}}{\geq} 2 \cdot n$

$$= n + n$$

$$\geq n + 1,$$

$$\text{also} \quad 2^{n+1} \geq n + 1$$

□

3.4.2 Bemerkung

Für Formeln wie in Beispiel 3.4.1a) benutzen wir das *Summenzeichen* Σ (Sigma, großes griechisches S)

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} \quad 1 + 2 + 3 + \dots + n \quad k = 1k = 2k = 3k = n$$

weitere Bsp:

$$\sum_{k=1}^n 2k = 2 \cdot 1 + 2 \cdot 2 + \dots + 2 \cdot n \quad \sum_{k=4}^n 2k = 2 \cdot 4 + 2 \cdot 5 + \dots + 2 \cdot n$$

$$\sum_{k=1}^3 7 = 7 + 7 + 7 = 21$$

$$\text{allg. } \sum_{k=m}^n a_k = a_m + a_{m+1} + \dots + a_n \quad (a_m, a_{m+1}, \dots, a_n \in \mathbb{R})$$

k heißt Summationsindex

$$\sum_{k=m}^n a_k = \sum_{i=m}^n a_i$$

Schreibweisen:

$$\sum_{k=1}^n a_k, \sum_{k=1}^n a_k, \sum_{k \in \mathbb{N}} a_k, \sum_{k=1, k \neq 2}^4 a_k = a_1 + a_3 + a_4$$

Für $n < m$ setzt man

$$\sum_{k=m}^n a_k = 0 \quad (\text{leere Summe}), \text{ z.B. } \sum_{k=7}^3 k = 0$$

Produktzeichen Π (Pi, großes griechisches P)

$$\prod_{k=m}^n a_k = a_m \cdot a_{m+1} \dots a_n,$$

für $n < m$ setze $\prod_{k=m}^n a_k = 1$

Rechenregeln für Summen (zu beweisen z.B. durch vollständige Induktion)

a)

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

$$(\sum_{k=3}^5 a = a + a + a = (5 - 3 + 1) \cdot a)$$

b)

$$\sum_{k=m}^n (c \cdot a_k) = c \cdot \sum_{k=m}^n a_k$$

c) **Indexverschiebung**

$$\sum_{k=m}^n a_k = a_m + a_{m+1} + \dots a_n$$

$$= a_{(m+e)-e} + a_{(m+e+1)-e} + \dots + a_{(n+e)-e}$$

neuer Summationsindex $j := k + e$
 (k durchläuft Werte: $m, m + 1, \dots, n$,
 j durchläuft Werte: $m + e, m + e + 1, \dots, n + e$)

$$\text{also gilt } \sum_{k=m}^n a_k = \sum_{j=m+e}^{n+e} a_{j-e}$$

$$(\text{Beispiel: } \sum_{k=0}^5 a_k \cdot x^{k+2} = \sum_{j=2}^7 a_{j-2} \cdot x^j)$$

d) **Addition von Summen gleicher Länge**

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

e) **Aufspalten**

$$\sum_{k=m}^n a_k = \sum_{k=m}^l a_k + \sum_{k=l+1}^n a_k \text{ für } m < l < n$$

f) **Teleskopsumme**

$$\sum_{k=m}^n (a_k - a_{k+1}) = a_m - a_{n+1}$$

$$\sum_{k=m}^n (a_k - a_{k+1}) = (a_m - a_{m+1} + (a_{m+1} - a_{m+2} + (a_{m+2} - a_{m+3} + \dots + (a_n - a_{n+1}))))$$

g) **Doppelsummen**

$$\sum_{i=1}^n \sum_{j=1}^m a_{ij}$$

$$= \sum_{i=1}^n (a_{i1} + a_{i2} + \dots + a_{im})$$

$$= a_{11} + a_{12} + a_{13} + \dots + a_{1m}$$

$$\begin{aligned}
&+a_{21} + a_{22} + a_{2m} \\
&+ \dots \\
&+a_{n1} + a_{n2} + \dots + a_{nm} \\
&\sum_{j=1}^m \sum_{i=1}^n a_j
\end{aligned}$$

3.4.3 Verschärftes Induktionsprinzip

$A(n), n_0$ wie in 3.4.1

Es gelte:

- (1) $A(n_0)$ ist wahr
- (2) $\forall n \geq n_0$:
Sind $A(n_0), \dots, A(n)$ wahr, so ist $A(n+1)$ wahr.
(d.h. $A(n_0) \wedge A(n_0+1) \wedge \dots \wedge A(n) \Rightarrow A(n+1)$)

Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}, n \geq n_0$

Beispiel: $A(n)$: Jede natürliche Zahl $n > 1$ ist Primzahl oder Produkt von Primzahlen.

Beweis:

Induktionsanfang: ($n_0 = 2$). $n = 2$ ist Primzahl ✓

Induktionsschritt: Sei $n \geq n_0$ ($n \geq 2$)

• Induktionsvoraussetzung:

Aussage gilt für $2, 3, 4, \dots, n$

($A(2), A(3), A(4), \dots, A(n)$ wahr)

• Induktionsbehauptung:

$A(n+1)$ gilt, d.h. $n+1$ ist Primzahl oder Produkt von Primzahlen.

Beweis:

- falls $n+1$ Primzahl, so gilt $A(n+1)$
- falls $n+1$ keine Primzahl, dann ist $n+1 = k \cdot l$, für $k, l \in \mathbb{N}$,
 $1 < k < n+1, 1 < l < n+1$ ($k = l$ möglich).

Nach Induktionsvoraussetzung:

Aussage gilt für k und $l \Rightarrow n + 1$ ist Produkt von Primzahlen.
 $A(n + 1)$ ist wahr. □

3.5 Schubfachprinzip

3.5.1 Idee

In einem Schrank befinden sich n verschiedene Paar Schuhe. Wie viele Schuhe muss man maximal herausziehen, bis man sicher ein zusammenpassendes Paar hat?

(Antwort: $n + 1$)

3.5.2 Satz (Schubfachprinzip, engl.: *pigeon hole principle*)

Seien $k, n \in \mathbb{N}$.

Verteilt man n Objekte auf k Fächer, so gibt es ein Fach, das mindestens $\lceil \frac{n}{k} \rceil$ Objekte enthält.

(Dabei bezeichnet $\lceil x \rceil$ die kleinste ganze Zahl z mit $x \leq z$.)

Beweis (durch Kontraposition):

$$\underbrace{(n \text{ Objekte, } k \text{ Fächer})}_A \Rightarrow \underbrace{\exists \text{ Fach mit mind. } \lceil \frac{n}{k} \rceil \text{ Objekten}}_B$$

statt $A \Rightarrow B$ zeige $\neg B \Rightarrow \neg A$

($\neg B$) Jedes Fach enthalte höchstens $\lceil \frac{n}{k} \rceil - 1$ Objekte.

Dann ist die Gesamtzahl von Objekten höchstens

$$k \cdot \underbrace{(\lceil \frac{n}{k} \rceil - 1)}_{< \frac{n}{k}} < k \cdot \frac{n}{k} = n$$

($\neg A$) es gibt also weniger als n Objekte □

3.5.3 Beispiel

- a) Wieviele Menschen müssen auf einer Party sein, damit sicher 2 am selben Tag Geburtstag haben?

367

- b) Auf jeder Party mit mindestens 2 Gästen gibt es 2 Personen, die dieselbe Anzahl Freunde auf der Party haben.

Beweis: Sei n die Anzahl der Partygäste. Jeder Gast kann mit $0, 1, 2, \dots, n-1$ Gästen befreundet sein (n Möglichkeiten).

Aber: Es kann nicht sein, dass ein Gast 0 Freunde hat und gleichzeitig ein Gast $n-1$ (=alle) Freunde hat.

\Rightarrow Es gibt $n-1$ mögliche Werte für die Anzahl der Freunde, entspricht $n-1$ Fächern.

Jeder der n Gäste trägt sich in ein Fach ein

\Rightarrow mindestens 2 Gäste sind im selben Fach. \square

- c) In Berlin gibt es mindestens 2 Personen, die genau dieselbe Anzahl Haare auf dem Kopf haben.

Beweis: Anzahl Haare im Durchschnitt:

blond	150.000
braun	110.000
schwarz	100.000
rot	90.000

zur Sicherheit: maximal 1 Millionen Haare möglich
entspricht 1 Mio Fächer.

Anzahl Einwohner in Berlin: 3,5 Millionen \Rightarrow Behauptung 3.5.2 \square

3.6 Weitere Beweistechniken (Werkzeugkiste)

- a) Wichtigste Technik: Ersetzen eines mathematischen Begriffs durch seine Definition (und umgekehrt). $A \subset B = \{x \mid x \in A \vee x \in B\}$
- b) Aussagen der Form $\forall a \in S$ gilt $P(a)$:
beginne mit: Sei $a \in S$, zeige $P(a)$.

- c) Aussage der Form $\exists a \in S$ mit $P(a)$
oft: finde/gebe konkretes Element a an, für das $P(a)$ gilt.
- d) Gleichheit von Mengen zeigt man oft mittels Inklusion (vgl. Definition 2.1(i))

Zu zeigen: $A = B$ (A, B Mengen)

zeige: $A \subseteq B$ (Sei $a \in A \Rightarrow \dots \Rightarrow a \in B$) 2.1 (i))

und $B \subseteq A$ (Sei $b \in B \Rightarrow \dots \Rightarrow b \in A$)

$\subseteq \dots$

$\supseteq \dots$

Beispiel: 2.5f)

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

Beweis:

• \subseteq

Sei $x \in A \Delta B = (A \setminus B) \cup (B \setminus A)$

1. Fall :

$x \in A \setminus B$, dann gilt $x \in A$, also $x \in A \cup B$

Außerdem $x \notin B$, also gilt auch $x \notin A \cap B$

$\Rightarrow x \in (A \cup B) \setminus (A \cap B)$

2. Fall

Ist $x \in B \setminus A$, so argumentiere analog.

• \supseteq

Sei $x \in (A \cup B) \setminus (A \cap B)$

$\Rightarrow x \in A$ oder $x \in B$.

1. Fall

$x \in A$, so ist $x \notin B$, da $x \notin A \cap B$

$\Rightarrow x \in A \setminus B \subseteq (A \setminus B) \cup (B \setminus A)$

$= A \Delta B$,

d.h. $x \in A \Delta B$.

2. Fall (1. Fall analog)

$x \in B$, so $x \notin A$, da $x \notin A \cap B$

$\Rightarrow x \in B \setminus A \subseteq A \Delta B$

Also $x \in A \Delta B$

- e) Äquivalenzen ($A \Leftrightarrow B$, A, B Aussagen) werden meist in 2 Schritten bewiesen:

Hinrichtung zeigt $A \Rightarrow B$,
Rückrichtung zeigt $B \Rightarrow A$.

\Rightarrow : ...

\Leftarrow : ...

(oft auch eine von beiden mittels Kontraposition)

Beispiel: 2.5g) $A \cap B = A \Leftrightarrow A \subseteq B$

Beweis:

\Rightarrow : Sei $A \cap B = A$. Dann ist $A = A \cap B \subseteq B$

\Leftarrow : Sei $A \subseteq B$. Dann ist $A \subseteq A$ und $A \subseteq B$,
also ist $A \subseteq A \cap B$

außerdem $A \cap B \subseteq A$

$\Rightarrow A = A \cap B$

□

2.5h) analog.

f) Äquivalenzen der Form:

Sei Dann sind folgende Aussagen äquivalent:

- a) ...
- b) ...
- c) ..
- d) ...

Zeigt man durch *Ringschluss*:

Zeige $a) \Rightarrow b) \Rightarrow c) \Rightarrow d) \Rightarrow a)$

(oder andere Reihenfolge, soll *Ring* geben.)

4 Abbildungen

4.1 Definition

- a) Eine Abbildung (oder Funktion)

$$f: A \rightarrow B$$

besteht aus

- zwei nicht-leeren Mengen:
 A , dem Definitionsbereich von f
 B , dem Bildbereich von f
- und einer Zuordnungsvorschrift, die jedem Element $a \in A$ genau ein Element $b \in B$ zuordnet

Wir schreiben dann $b = f(a)$, nennen b das Bild oder den Funktionswert von a (unter f), und a (ein) Urbild von b (unter f).

Notation:

$$f: A \rightarrow B$$

$$a \mapsto f(a)$$

- b) Die Menge $G_f := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ heißt der Graph von f .

4.2 Beispiele

Siehe Folien!

4.3 Beispiele

- a) A Menge

$$\begin{aligned} id_A: A &\rightarrow A \\ x &\mapsto x \end{aligned}$$

identische Abbildung

- b) $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto x^2$ ist Abbildung (aus der Schule bekannt als $f(x) = x^2$)

c) \wedge kann als Abbildung aufgefasst werden, $+$ ebenso:

$$\begin{aligned} \wedge: \{0, 1\} \times \{0, 1\} &\rightarrow \{0, 1\} \\ (A, B) &\mapsto A \wedge B \end{aligned}$$

$$\begin{aligned} +: \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} \\ (a, b) &\mapsto a + b \end{aligned}$$

Allgemein bezeichnet man eine Abbildung $\{0, 1\}^n \rightarrow \{0, 1\}^m$ ($n, m \in \mathbb{N}$) als boolesche Funktion.

4.4 Definition

Zwei Abbildungen $f: A \rightarrow B$, $g: C \rightarrow D$ heißen gleich (in Zeichen: $f = g$), wenn:

- $A = C$
- $B = D$
- $f(a) = g(a)$

$$\forall a \in A (= C)$$

4.5 Beispiel

$$\begin{aligned} f: \{0, 1\} &\rightarrow \{0, 1\}, x \mapsto x \\ g: \{0, 1\} &\rightarrow \{0, 1\}, x \mapsto x^2 \end{aligned}$$

$$f = g$$

4.6 Definition

Sei $f: A \rightarrow B$, seien $A_1 \subseteq A$, $B_1 \subseteq B$ Teilmengen.

Dann heißt

a) $f(A_1) := \{f(a) \mid a \in A_1\} \subseteq B$ das Bild von A_1 (unter f) (Bildmenge).

(Beispiel: $f: \mathbb{N} \rightarrow \mathbb{N}$

$$x \mapsto 2x$$

$$A_1 = \{1, 3\}$$

$$f(A_1) = \{f(1), f(3)\} = \{2, 6\})$$

- b) $f^{-1}(B_1) := \{a \in A \mid f(a) \in B_1\} \subseteq A$
das Urbild von B_1 (unter f).
(Beispiel oben: $B_1 = \{8, 14, 100\}, f^{-1}(B_1) = \{4, 7, 50\}$
 $B_2 = \{3\}, f^{-1}(B_2) = \emptyset$)
- c) f surjektiv, falls gilt: $f(a) = B$
(d.h. $\forall b \in B \exists a \in A : f(a) = b$)
[alle Elemente von B werden getroffen]
- d) f injektiv, falls gilt:
 $\forall a_1, a_2 \in A$ mit $a_1 \neq a_2$ gilt $f(a_1) \neq f(a_2)$
(äquivalent: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$)
[kein Element von B wird doppelt getroffen]
- e) f bijektiv, falls f surjektiv und injektiv (f ist Bijektion).
[jedes Element wird genau einmal getroffen]

4.7 Beispiele

siehe Folien

- a) f aus Beispiel in 4.6 a) ist injektiv, aber nicht surjektiv:

$f(\mathbb{N})$ ist Menge der geraden natürlichen Zahlen, nicht \mathbb{N} .

- b) $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto x^2$

nicht surjektiv:

$$f(\mathbb{R}) = \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\} \neq \mathbb{R}$$

nicht injektiv:

$$f(1) = f(-1) = 1$$

$$f(2) = f(-2) = 4$$

$$g: \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+ \\ x \mapsto x^2$$

injektiv, surjektiv, bijektiv

c) $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto 2x + 1$

ist surjektiv:

Sei $y \in \mathbb{R}$. Zeige: $\exists x \in \mathbb{R}$ mit $y = 2x + 1$ (vgl. 3.6 b))

Wähle $x = \frac{y-1}{2}$

f ist injektiv:

angenommen, es gibt $x_1, x_2 \in \mathbb{R}$

mit $f(x_1) = f(x_2)$, d.h.

$$2x_1 + 1 = 2x_2 + 1,$$

dann folgt $x_1 = x_2$. \circledast

4.8 Definition

Sei $f: A \rightarrow B$ bijektiv. Dann definieren wir die Umkehrfunktion.

$f^{-1}: B \rightarrow A$, indem wir jedem $b \in B$ dasjenige $a \in A$ zuordnen, für das $f(a) = b$ gilt.

4.9 Beispiel

$$A(a_1, a_2, a_3) \quad B(b_1, b_2, b_3)$$

$f: (A \rightarrow B)$ bijektiv

$$a_1 \rightarrow b_2$$

$$a_2 \rightarrow b_3$$

$$a_3 \rightarrow b_1$$

$$f^{-1}: B \rightarrow A$$

$$b_1 \rightarrow a_3$$

$$b_2 \rightarrow a_1$$

$$b_3 \rightarrow a_2$$

4.10 Bemerkung

Man kann jedem $b \in B$ wirklich ein $a \in A$ zuordnen, das $f(a) = b$ erfüllt, denn f ist surjektiv. Nur ein solches a , denn f ist injektiv.

4.11 Definition

Seien $g: A \rightarrow B$ $f: B \rightarrow C$
Abbildungen.

Dann heißt die Abbildung: $f \circ g: A \rightarrow C$
 $a \mapsto (f \circ g)(a) :=$
 $f(g(a)) \forall a \in A$

die Hintereinanderausführung oder Komposition von f mit g .

f nach g

$$A \xrightarrow{\underbrace{\quad}_g} B \xrightarrow{\underbrace{\quad}_f} C$$

4.12 Beispiel

$$A = B = C = \mathbb{R}$$

$$\begin{array}{ll} f: \mathbb{R} \rightarrow \mathbb{R} & g: \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto x + 1 & x \mapsto 2x \end{array}$$

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1$$

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g(x + 1) = 2 \cdot (x + 1) \\ &= 2x + 2 \end{aligned}$$

hier also $f \circ g \neq g \circ f$!

4.13 Satz

Die Komposition $\{\text{inj.}, \text{surj.}, \text{bij}\}$ Abbildungen ist $\{\text{inj.}, \text{surj.}, \text{bij}\}$

Beweis: Pü / Ü

4.14 Satz (Charakterisierung bijektiver Abbildungen)

Sei $f: A \rightarrow B$ eine Abbildung.

f ist bijektiv genau dann, wenn es eine Abbildung $g: B \rightarrow A$ gibt mit $g \circ f = id_A$ und $f \circ g = id_B$.

Diese Abbildung g ist eindeutig und genau die Umkehrfunktion von f , also $g = f^{-1}$.

f^{-1} ist ebenfalls bijektiv und es gilt $(f^{-1})^{-1} = f$

Beweis:

" \Rightarrow " Sei f bijektiv. Dann existiert für jedes $b \in B$ genau ein $a \in A$ mit $b = f(a)$.

Definiere nun also $g: B \rightarrow A$ mit $g(b) = a$, dann gilt die Aussage:

$$(g \circ f)(a) = g(f(a)) = g(b) = a = id_A(a)$$

$$(f \circ g)(b) = f(g(b)) = f(a) = b = id_B(b)$$

" \Leftarrow " Es existiere Abbildung g wie angegeben (zu zeigen: f ist bijektiv)

- **f surjektiv:** Sei $b \in B$. Dann ist $g(b) \in A$, $f(\underbrace{g(b)}) = id_B(b) = b$, d.h.
das ist das gesuchte a ! ($a := g(b)$)
 $g(b)$ ist Urbild von b unter f .

- **f injektiv:**

$$\text{Sei } \underline{f(a_1) = f(a_2)}$$

$$\text{Dann ist } \underline{a_1} = g(\underline{f(a_1)}) = g(f(a_2)) = \underline{a_2}$$

- **Eindeutigkeit von g :**

Angenommen es gäbe Abbildungen g_1, g_2 mit angegebenen Eigenschaften.

Sei $b \in B$. Dann gibt es genau ein $a \in A$ mit $\underline{f(a) = b}$.

$$\text{Also } g_1(b) = g_1(\underline{f(a)}) = a = g_2(\underline{f(a)}) = g_2(\underline{b}),$$

d.h. $g_1 = g_2$

- **f^{-1} bijektiv, $(f^{-1})^{-1} = f$:**

folgt aus $f \circ f^{-1} = id_B$, $f^{-1} \circ f = id_A$,
wende Aussage des Satzes auf f^{-1} an.

□

4.15 Bemerkung / Definition

Bijektivität erlaubt präzise Definition der Endlichkeit / Unendlichkeit von Mengen:

- a) Menge $M \neq \emptyset$ heißt endlich $\Leftrightarrow \exists n \in \mathbb{N} : \exists$ bijektive Abbildung $f: \{1, \dots, n\} \rightarrow M$.

(\emptyset wird auch als endlich bezeichnet).

Andernfalls heißt M unendlich.

[Hilberts Hotel]

- b) Zwei Mengen M_1, M_2 heißen gleichmächtig, falls es eine bijektive Abbildung $g: M_1 \rightarrow M_2$ gibt.

Beispiel: $\mathbb{N}, 2\mathbb{N}$ (alle geraden natürlichen Zahlen) gleichmächtig:

$$g: \mathbb{N} \rightarrow 2\mathbb{N}$$

$$n \mapsto 2n$$

ist bijektiv.

- c) Menge M heißt abzählbar unendlich, wenn M gleichmächtig ist wie \mathbb{N} , d.h. \exists bijektive Abbildung.

$$h: \mathbb{N} \rightarrow M.$$

Beispiel:

- \mathbb{N} abzählbar unendlich: $h = id_{\mathbb{N}}$
- \mathbb{N} abzählbar unendlich: $h: \mathbb{N} \rightarrow \mathbb{N}_0 (x \mapsto x - 1)$ ist bijektiv.
- \mathbb{Z} ist abzählbar unendlich: (Geschichte vom Teufel: $h \rightarrow \mathbb{Z}$)

$$1 \rightarrow 0$$

$$2 \rightarrow 1$$

$$3 \rightarrow -1$$

$$4 \rightarrow 2$$

$$\underbrace{5}_{\text{Tag}} \rightarrow \underbrace{-2}_{\text{Zahl}}$$

\vdots

allgemein:

$$x \rightarrow \begin{cases} k & \text{falls } x = 2k + 1 (\text{für } k = 0, 1, 2, \dots) \\ -k & \text{falls } x = 2k (\text{für } k = 1, 2, 3, \dots) \end{cases}$$

- \mathbb{Q} ist abzählbar unendlich:

$$\frac{1}{1} \frac{1}{2} \frac{1}{3} \frac{1}{4} \frac{1}{5} \dots$$

$$\frac{2}{1} \frac{2}{2} \frac{2}{3} \frac{2}{4} \frac{2}{5} \dots$$

$$\frac{3}{1} \frac{3}{2} \frac{3}{3} \frac{3}{4} \frac{3}{5} \dots$$

\vdots

Cantorsches Diagonalverfahren.

- \mathbb{R} ist nicht abzählbar unendlich!
(Beweis von Cantor, 2. Diagonalisierungsargument) \rightarrow eventuell später
- $P(\mathbb{N})$ ist nicht abzählbar unendlich (allgemein: $|A| < |P(A)|$ | Satz von Cantor.)

4.16 Satz (Wichtiger Satz für endliche Mengen)

Seien $A, B \neq \emptyset$ endliche Mengen, $|A| = |B|$, und $f: A \rightarrow B$ eine Abbildung.

Dann gilt f injektiv $\Leftrightarrow f$ surjektiv $\Leftrightarrow f$ bijektiv.

Beweis:

Wir setzen $n := |A| = |B|$. Es genügt zu zeigen f injektiv $\Leftrightarrow f$ surjektiv.

\Rightarrow Sei f injektiv, d.h. falls $a_1, a_2 \in A$ mit $a_1 \neq a_2$, dann gilt $f(a_1) \neq f(a_2)$.

D.h., verschiedene Elemente aus A werden auf verschiedene Elemente aus B abgebildet, die n Elemente aus A also auf n verschiedene Elemente aus B .

Da B genau n Elemente besitzt, ist f surjektiv. ($f(A) = B$).

[formaler: d.h. $|f(A)| = |A| = |B|$.

Da $f(A) \subseteq B$ endlich, folgt $f(A) = B$. □

4.17 Das Prinzip der rekursiven Definition von Abbildungen

Sei $B \neq \emptyset$ Menge, $n_0 \in \mathbb{N}$, $A = \{n \in \mathbb{N} \mid n \geq n_0\}$.

Man kann eine Funktion $f : A \rightarrow B$ definieren durch

- Angabe des Startwerts $f(n_0)$
- Beschreibung, wie man für jedes $n \in A$ den Funktionswert $f(n+1)$ aus $f(n)$ berechnet (Rekursionsschritt).

4.18 Beispiel

a) Die Fakultätsfunktion: $f : \mathbb{N}_0 \rightarrow \mathbb{N}$
mit $f(0) = 0 \underbrace{!}_{\text{Fakultät}} = 1$ (Startwert)

$$f(n+1) = (n+1)! = n!(n+1) \text{ für alle } n \geq 0$$

Also:

$$f(1) = 1! = 0! \cdot 1$$

$$f(2) = 2! = 1! \cdot 2 = 1 \cdot 2 = 2$$

$$f(3) = 3! = 2! \cdot 3 = 1 \cdot 2 \cdot 3$$

$$f(4) = 4! = 3! \cdot 4 = 1 \cdot 2 \cdot 3 \cdot 4$$

\vdots

$$f(70) = 70! \approx 1,2 \cdot 10^{100}$$

b) Potenzen: für festes $x \in \mathbb{R}$ definiere

$$x^0 = 1$$

$$x^{n+1} = x^n \cdot x \text{ für alle } n \geq 0$$

$$(P_x : \mathbb{N}_0 \rightarrow \mathbb{R} \quad n \rightarrow x^n)$$

c) Eine Pflanze verdopple jeden Tag die Anzahl ihrer Knospen und produziere eine zusätzliche.

$f : \mathbb{N} \rightarrow \mathbb{N}$ beschreibe die Anzahl der Knospen nach n Tagen.

$$f(1) = 1$$

$$f(2) = 2 \cdot 1 + 1 = 3$$

$$f(3) = 2 \cdot 3 + 1 = 7$$

$$f(4) = 2 \cdot 7 + 1 = 15$$

\vdots

$$f(n+1) = 2 \cdot f(n) + 1$$

Wieviele Knospen gibt es nach 100 Tagen?
 \Rightarrow Geschlossene / explizite Form von f gefragt.

Vermutung: $f(n) = 2^n - 1$

(Bemerkung: bessere Methoden (statt vermuten / raten) in der Vorlesung *Algorithmen*, dort z.B. auch mathematische Strukturen wie oben, diese werden *Bäume* (Graphen) genannt.

Beweis: vollständige Induktion

Induktionsanfang:

$$f(1) = 2^1 - 1 = 1$$

Induktionsschritt:

Induktionsvoraussetzung:

sei $f(n) = 2^n - 1 \forall n \geq 1$

Induktionsbehauptung:

$$f(n+1) = 2^{n+1} - 1$$

Beweis:

$$\begin{aligned} f(n+1) & \stackrel{\text{Definition}}{=} 2 \cdot f(n) + 1 \\ & \stackrel{\text{Ind.vor.}}{=} 2(2^n - 1) + 1 \\ & = 2^{n+1} - 2 + 1 \\ & = 2^{n+1} - 1 \end{aligned}$$

□

4.19 Bemerkung

Die rekursive Definition kann verallgemeinert werden: benutze zur Definition von $f(n+1)$ die vorigen k ($k \in \mathbb{N}$) Werte von f , also $\underbrace{f(n), f(n-1), \dots, f(n-k+1)}_{k \text{ Stück}}$

und gebe k Startwerte $f(n_0), f(n_0+1), \dots, f(n_0+k-1)$

4.20 Beispiel (Fibonacci-Zahlen)

$$k = 2$$

$$f(1) = 1$$

$$f(2) = 1$$

$$f(n+1) = f(n) + f(n+1)$$

$$(f(3) = f(2) + f(1) = 1 + 1 = 2,$$

$$f(4) = 2 + 1 = 3,$$

$$f(5) = 3 + 2 = 5,$$

$$f(6) = 8,$$

$$f(7) = 13\dots)$$

explizite Form:

$$f(n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

5 Relationen

5.1 Definition

Seien M_1, \dots, M_n
nicht leere Mengen
($n \in \mathbb{N}$).

a)

Eine n-stellige Relation über M_1, \dots, M_n ist eine Teilmenge von $M_1 \times \dots \times M_n$. Ist $M_1 = \dots = M_n = M$, d.h. $R \subseteq M^n$, so spricht man von einer n-stelligen Relation auf M.

b)

(speziell: $n = 2$, zweistellige Relation auf M :

Sei $M \neq \emptyset$ Menge. Eine Teilmenge $R \subseteq M \times M$ heißt (zweistellige) Relation auf M .
Statt $(a, b) \in R$ (mit $a, b \in M$) schreibt man kurz $a R b$ oder $a \sim b$ (a steht in Relation zu b)

5.2 Beispiel

a)

Relationale Datenbanken (\rightarrow Folie)

b)

$M = \{1, 2, 3\}$,
 $R = \{(1, 2), (1, 3), (2, 3)\}$
also: $1 \sim 2, 1 \sim 3, 2 \sim 3$

Hierfür sind wir die Notation $<$ gewohnt:

$1 < 2, 1 < 3, 2 < 3$ (*Kleiner-Relation*)

Ähnlich: \geq auf M : $R_{\geq} = \{(1, 1), (2, 1), (3, 1), (2, 2), (3, 2), (3, 3)\}$

allgemeiner: kleiner-Relation auf \mathbb{Z} :

$R_{<} = \{(x, y) \mid x, y \in \mathbb{Z}, x < y\}$

$R_{\leq} \dots \leq$

c)

Teiler-Relation R , auf \mathbb{Z} :

$R = \{(x, y) \mid x, y \in \mathbb{Z} \text{ und } \exists k \in \mathbb{Z} \text{ mit } x \mid y \text{ (} x \text{ teilt } y)\}$

z.B. $6|42$, $3|-27$, $7|0$

- d) Sei M die Menge aller Menschen, $R_m = \{(a, b) \mid a, b \in M \text{ und } a \text{ und } b \text{ haben dieselbe Mutter}\}$

Zwei wichtige Typen von Relationen auf einer Menge:
Ordnungsrelationen und Äquivalenzrelationen.

5.3 Definition

Sei $M \neq \emptyset$, R_{\preceq} (oder \preceq) eine Relation auf M mit folgenden Eigenschaften:

1. $\forall x \in M : x \preceq x$ (Reflexivität)
2. $\forall x, y \in M : (x \preceq y \wedge y \preceq x) \Rightarrow x = y$ (Antisymmetrie)
3. $\forall x, y, z \in M : (x \preceq y \wedge y \preceq z) \Rightarrow x \preceq z$ (Transitivität)

Dann heißt \preceq Ordnungsrelation oder (partielle) Ordnung auf M .

Gilt zusätzlich:

4. $\forall x, y \in M : x \preceq y$ oder $y \preceq x$, so heißt \preceq eine totale (oder vollständige, oder lineare) Ordnung.

Ist $x \preceq y$ und $x \neq y$, so schreibt man $x \prec y$.

5.4 Beispiele

- a) R_{\leq} auf \mathbb{Z} (Beispiel 5.2 b)) ist totale Ordnung auf \mathbb{Z} , ebenso auf \mathbb{Q}, \mathbb{R} .

$R_{<}$ ist keine partielle Ordnung; (1),(4) nicht erfüllt:

(1): für kein $x \in \mathbb{Z}$ gilt $x < x$

(4): für $x = y$ gilt weder $x < y$ noch $y < x$.

- b) $R_{|}$ (5.2 c)) auf \mathbb{N} ist partielle Ordnung, nicht total (zum Beispiel gilt für $3, 4 \in \mathbb{N}$ weder $3|4$ noch $4|3$).

$R_{|}$ auf \mathbb{Z} ist keine partielle Ordnung; nicht antisymmetrisch:

z.B. $-3|3$, $3|-3$, aber $3 \neq -3$

- c) Teilmengenrelation (\subseteq) auf $\mathcal{P}(M)$ ist partieller Ordnung, für $|M| > 1$ nicht total (Übung).

d) Beispiel für Relation, die (1),(2) erfüllt, aber nicht (3):

$$M = \{1, 2, 3\}$$

$$R = \{\underbrace{(1, 1), (2, 2), (3, 3)}_{\rightarrow \text{reflexiv}}, (1, 2), * (2, 3)\}$$

* Achtung: $(2, 1) \notin R$, sonst müsste $2 = 1$ gelten (wegen Antisymmetrie).

$(1, 2) \in R, (2, 3) \in R$, aber $(1, 3) \notin R$

\Rightarrow nicht transitiv.

$$(1, \overbrace{2}) \quad (1, 2) \checkmark \quad (1, \overbrace{1}), (1, 2) \quad (1, 2) \checkmark$$

e) Sei \leq partielle Ordnung auf M , $n \in \mathbb{N}$.

Dann definiere die lexikographische Ordnung \leq_{lex} auf M^n wie folgt:

$$x = (x_1, \dots, x_n) \leq_{lex} y = (y_1, \dots, y_n) :\Leftrightarrow$$

$$x = y \text{ oder } x_i < y_i \text{ für das kleinste } i \text{ mit } x_i \neq y_i$$

(Übung: \leq_{lex} ist partielle Ordnung)

(Falls \leq totale Ordnung auf M ist, dann \leq_{lex} totale Ordnung auf M^n , vgl. Wörterbuch)

Beispiel: $M = \{a, b, c\} \quad a < b < c$

dann ist z.B. auf M^4

$$(a, a, a, a) \leq_{lex} (a, a, a, b) \leq_{lex} \dots \leq_{lex} (a, b, a, c) \leq_{lex} \dots \leq_{lex} (a, b, b, a) \leq_{lex}$$

$$\dots \leq_{lex} (c, c, c, c)$$

Äquivalenzrelationen:

2 Elemente äquivalent, falls sie sich bezüglich einer Eigenschaft gleichen/ähnlich sind, z.b. Farbe, gleiche Übungsgruppe, gleicher Rest bei Division durch 3, ...

5.5 Definition

Eine Relation \sim auf einer Menge $M \neq \emptyset$ heißt Äquivalenzrelation falls gilt:

- (1) **Reflexivität:** $x \sim x$ für alle $x \in M$.
- (2) **Symmetrie:** $\forall x, y \in M : x \sim y \Rightarrow y \sim x$
- (3) **Transitivität:** Für alle $x, y, z \in M$ gilt: falls $x \sim y$ und $y \sim z$, dann ist auch $x \sim z$.

5.6 Beispiele

a) $<$ -Relation (Beispiel 5.2 b)) ist keine Äquivalenzrelation (nicht reflexiv, nicht symmetrisch, transitiv).

\geq keine Äquivalenzrelation (reflexiv, nicht symmetrisch, transitiv)

b) $M \neq \emptyset$ beliebig, $a \sim b :\Leftrightarrow a = b$

Gleichheit ist eine Äquivalenzrelation

$$(\sim := \{(a, a) \mid a \in M\})$$

c) R_m (Mutter-Relation) aus Beispiel 5.2 d) ist Äquivalenzrelation

d) $M = \mathbb{Z}$, $a \sim b :\Leftrightarrow b - a$ ist gerade,
d.h. $\exists k \in \mathbb{Z}$ mit $b - a = 2 \cdot k$.

\sim ist Äquivalenzrelation:

– reflexiv: Sei $a \in M$, dann gilt $a \sim a$,
denn $a - a = 0 = 2 \cdot 0$

– symmetrisch: Sei $a \sim b$
 $\Rightarrow b - a = 2 \cdot k$ für ein $k \in \mathbb{Z}$
 $\Rightarrow a - b = -2 \cdot k = 2 \cdot \underbrace{(-k)}_{\in \mathbb{Z}}$
 $\Rightarrow b \sim a$

– transitiv: seien $a \sim b, b \sim c \Rightarrow \exists k, l \in \mathbb{Z}$:
 $b - a = 2 \cdot k, \quad c - b = 2 \cdot l$
 $\Rightarrow c - a = (c - b) + (b - a) = 2l + 2k = 2 \cdot \underbrace{(l + k)}_{\in \mathbb{Z}}$
 $\Rightarrow a \sim c$

e) analog: wähle $r \in \mathbb{N}$ fest, $M = \mathbb{Z}$

$a \sim b :\Leftrightarrow b - a$ ist durch r teilbar (d.h. $\exists k \in \mathbb{Z}$ mit $b - a = r \cdot k$)

\sim ist Äquivalenzrelation.

5.7 Definition

Sei \sim eine Äquivalenzrelation auf $M \neq \emptyset$.

Dann heißt für $x \in M$ die Menge

$[x] := \{y \in M \mid y \sim x\}$ die Äquivalenzklasse von x (bzgl. \sim) auf M .

5.8 Beispiel

a) Gleichheit liefert triviale, nämlich einelementige Äquivalenzen:

$$[x] = \{x\} \forall x \in M$$

b) vgl. Beispiel 5.6d), $M = \mathbb{Z}, a \sim b \Leftrightarrow b - a$ gerade

$$[0] = \{b \in \mathbb{Z} \mid b - 0 \text{ gerade}\} = \text{Menge der geraden Zahlen}$$

$$= [2] = [4] = [-2] = \dots$$

$$[1] = \{b \in \mathbb{Z} \mid b - 1 \text{ gerade}\} = \text{Menge der ungeraden Zahlen}$$

$$= [3] = [5] = [-1] = \dots$$

Es gilt: $[0] \cup [1] = \mathbb{Z}$, und $[0] \cap [1] = \emptyset$

(*disjunkte Vereinigung*, Zerlegung von \mathbb{Z} , siehe folgende Definition.)

5.9 Definition

Sei $M \neq \emptyset, Z \subseteq \mathcal{P}(M)$ eine Menge von Teilmengen von M .

Die Elemente von Z seien paarweise disjunkt, d.h. $\forall A, B \in Z$ mit $A \neq B$ gilt $A \cap B = \emptyset$.

(*Beispiel* : $M := \{1, 2, 3, 4, 5\}$,

$$Z' := \{\{1\}, \{1, 2\}, \{3, 4\}\}$$

$$Z := \{\{1\}, \{2, 3\}, \{4, 5\}\}$$

Elemente von Z' nicht paarweise disjunkt, aber Elemente von Z paarweise disjunkt.)

Dann heißt die Vereinigung $\bigcup_{A \in Z} A$ auch disjunkte Vereinigung, Notation: $\bigcup_{A \in Z} A$

(oder $\biguplus_{A \in Z} A$).

Gilt zusätzlich $\bigcup_{A \in Z} A = M$, so heißt Z Zerlegung oder Partition von M .

5.10 Satz (Klasseneinteilung, Zerlegung durch Äquivalenzklassen)

Sei \sim Äquivalenzrelation auf $M \neq \emptyset$. Dann gilt:

(1) für jedes $x \in M$ ist $[x] \neq \emptyset$

$$(2) \bigcup_{x \in M} [x] = M$$

(3) $\forall x, y \in M$ gilt entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$

In Worten: Über \sim wird M zerlegt in nicht leere, paarweise disjunkte Mengen (die Äquivalenzklassen).

Beweis:

(1) $x \sim x \quad \forall x \in M$ (Reflexivität)
 $\Rightarrow x \in [x]$

(2) zeige $=$, also \subseteq, \supseteq :

$$\subseteq \bigcup_{x \in M} [x]_{\subseteq M} \subseteq M \text{ (nach Definition).}$$

$$\supseteq M = \bigcup_{x \in M} \{x\} \underbrace{\subseteq}_{(1)} \bigcup_{x \in M} [x],$$

$$\text{also } M \subseteq \bigcup_{x \in M} [x].$$

(3) wir zeigen: $[x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]$

Sei dazu $z \in [x] \cap [y]$ (denn Schnitt $\neq \emptyset$)

$\Rightarrow z \sim x$ und $z \sim y$ (*)

$\Rightarrow x \sim z$ und $y \sim z$ (**)

wir zeigen: $[x] = [y]$

• $[x] \subseteq [y]$: sei $u \in [x]$

$\Rightarrow u \sim x$

$\Rightarrow u \sim z$

Transitivität, $x \sim z$ (**)

$\Rightarrow u \sim y$

Transitivität, $z \sim y$ (*)

$\Rightarrow u \in [y]$.

• $[x] \supseteq [y]$: sei $u \in [y]$

$\Rightarrow u \sim y$

$\Rightarrow u \sim z$

(Transitivität, $y \sim z$ (**))

$\Rightarrow u \sim x$

Transitivität, $z \sim x$ (*)
 $\Rightarrow u \in [x]$
 Also insgesamt $[x] = [y]$. □

Eine Äquivalenzrelation auf einer Menge M liefert also eine Zerlegung von M . Es gilt auch die Umkehrung.

5.11 Satz

Sei $M \neq \emptyset$ eine Menge, Z eine Zerlegung von M , $M = \bigcup_{A \in Z} A$.

Definiere für $x, y \in M$:

$x \sim y : \Leftrightarrow x$ und y liegen in derselben Menge $A \in Z$.

Dann ist \sim eine Äquivalenzrelation auf M , und die Äquivalenzklassen bezüglich \sim sind genau die Mengen $A \in Z$.

Beweis:

- \sim ist reflexiv:

Sei $x \in M = \bigcup_{A \in Z} A$
 $\Rightarrow x \in A$ für ein $A \in Z$
 $\Rightarrow x \sim x$

- \sim ist symmetrisch:

Sei $x \sim y$, d.h. $x, y \in A$ für ein $A \in Z$.
 $\Rightarrow y \sim x$

- \sim ist transitiv:

Seien $x \sim y, y \sim z$, d.h. $x, y \in A$ und $y, z \in B$ für passende $A, B \in Z$
 $y \in A \cap B \Rightarrow A = B$ (Zerlegung ist disjunkte Vereinigung)
 $\Rightarrow x, z \in A$
 $\Rightarrow x \sim z$

- Äquivalenzklassen: folgt aus Definition von \sim . □

5.12 Definition

Sei \sim eine Äquivalenzrelation auf M .

Eine Teilmenge von M , die aus jeder Äquivalenzklasse bezüglich \sim genau ein Element (einen sogenannten Repräsentanten) enthält, nennt man ein Repräsentantensystem von \sim .

5.13 Beispiel

Beispiel 5.6 d / 5.8 b:

$a \sim b \Leftrightarrow b - a$ gerade.

Äquivalenzklassen waren $[0], [1]$

Repräsentantensysteme sind zum Beispiel $\{0, 1\}$ oder $\{2, 9\}$ oder $\{-42, 3\}$.

6 Elementare Zahlentheorie

6.1 Definition

Seien $a, b \in \mathbb{Z}, b \neq 0$.

b heißt Teiler von a (b teilt a , $b \mid a$), falls $q \in \mathbb{Z}$ existiert mit $a = q \cdot b$.

(d.h. $\frac{a}{b} = q \in \mathbb{Z}$)

a heißt dann Vielfaches von b .

($b \nmid a$ bedeutet: b ist kein Teiler von a)

(Beispiel: $6 \mid 42$, $-5 \mid 10$, $5 \nmid 42$, $1 \mid -1$, $1 \mid 0$, 0 ist nie Teiler einer Zahl.)

6.2 Satz

Seien $a, b, c, d \in \mathbb{Z}$

a) Ist $b \mid a$, dann auch $|b| \mid a$, $b \mid |a|$ und $|b| \mid |a|$.

($|b|$ bezeichnet den Betrag von b ,

$$|b| = \begin{cases} b & , \text{ falls } b \geq 0 \\ -b & , \text{ falls } b < 0 \end{cases})$$

b) Falls $b \mid c$ und $b \mid d$, dann $b \mid k \cdot c + l \cdot d \quad \forall k, l \in \mathbb{Z}$

c) Ist $b \mid a$ und $a \neq 0$, dann $|b| \leq |a|$

d) Ist $b \mid a$ und $a \mid b$, dann $a = \pm b$

Beweis:

a) Sei $b \mid a$.

– Ist $b > 0$, so ist $|b| = b$, also gilt $|b| \mid a$.

– Ist $b < 0$, so ist $|b| = -b$

$b \mid a$, d.h. $\exists q \in \mathbb{Z}$ mit $a = q \cdot b = (-q) \cdot (-b) = (-q) \cdot |b|$.

$(-q) \in \mathbb{Z}$, also gilt $|b| \mid a$.

Restliche Behauptung analog!

b) $b \mid c$, d.h. $\exists q \in \mathbb{Z}$ mit $c = q \cdot b$

$$\Rightarrow k \cdot c = k \cdot q \cdot b \quad \forall k \in \mathbb{Z}$$

$b \mid d$, d.h. $\exists m \in \mathbb{Z}$ mit $d = m \cdot b$

$$\Rightarrow \underline{l \cdot d} = \underline{l \cdot m \cdot b} \quad \forall l \in \mathbb{Z}$$

$$\Rightarrow \underline{k \cdot c} + \underline{l \cdot d} = \underline{k \cdot q \cdot b} + \underline{l \cdot m \cdot b} = \underbrace{(k \cdot q + l \cdot m)}_{\in \mathbb{Z}} \cdot b \quad \forall k, l \in \mathbb{Z}$$

$$\Rightarrow b \mid k \cdot c + l \cdot d \quad \forall k, l \in \mathbb{Z}$$

c) $b \mid a$, nach Teil a) also $|b| \mid |a|$

$$\Rightarrow |a| = \underbrace{q}_{\in \mathbb{N}, \text{ da } |a|, |b| \geq 0 \text{ und } a \neq 0} \cdot |b| = \underbrace{|b| + |b| + \dots + |b|}_{q \text{ Summanden}} \geq |b|$$

d) Da $b \mid a$ und $a \mid b$, sind $a, b \neq 0$

$$\text{Nach c): } |b| \leq |a| \text{ und } |a| \leq |b| \Rightarrow |a| = |b|, \text{ d.h. } a = \pm b. \quad \square$$

Teilbarkeit in \mathbb{Z} ist im Allgemeinen nicht erfüllt. Daher ist Teilen mit Rest wichtig.

6.3 Satz und Definition: Division mit Rest

Seien $a, b \in \mathbb{Z}, b \neq 0$.

Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$\left. \begin{array}{l} (1) \quad a = q \cdot b + r \\ (2) \quad 0 \leq r < |b| \end{array} \right\} \text{ Division mit Rest}$$

q wird Quotient genannt, r Rest.

Bezeichnung: $q = a \text{ div } b$

$r = a \bmod b$ (*modulo*)

Es gilt also $\underbrace{a \bmod b}_{\text{Rest}} = 0 \Leftrightarrow b \mid a$

6.4 Beispiel

- $a = 22, b = 5, 22 = 4 \cdot 5 + 2$
 $22 \text{ div } 5 = 4, 22 \bmod 5 = 2$

- $a = 22, b = -5, 22 = -4 \cdot (-5) + 2$
 $22 \operatorname{div} (-5) = -4, 22 \operatorname{mod} (-5) = 2$
- $a = -22, b = 5, -22 = -5 \cdot 5 + 3$
 $(\underline{\Delta} \ (0 \leq r < 5)!) \\ -22 \operatorname{div} 5 = -5, -22 \operatorname{mod} 5 = 3$
- $a = -22, b = -5, -22 = 5 \cdot (-5) + 3$
 $-22 \operatorname{div} (-5) = 5, -22 \operatorname{mod} (-5) = 3$

Beweis von 6.3:

- Existenz von q und r mit (1), (2):

1. Fall: $b > 0$

Sei q die größte ganze Zahl mit $q \leq \frac{a}{b}$
 $(q = \lfloor \frac{a}{b} \rfloor)$

Dann ist $b \cdot q \leq a$
 (da $b > 0$!)

Setze $r := a - b \cdot q$
 es gilt also $r \geq 0$
 $\Rightarrow a = q \cdot b + r$ ((1) gilt)

Zu zeigen bleibt noch: $r < |b| = b$

Widerspruchsbeweis:

angenommen, $r \geq b$. Dann ist

$$r = b + s \text{ für ein } s \geq 0, \text{ d.h. } a = q \cdot b + \underbrace{(b + s)}_r$$

$$b(q + 1) + s = a$$

$$\Rightarrow q + 1 + \underbrace{\frac{s}{b}}_{\geq 0} = \frac{a}{b}$$

$$\Rightarrow q + 1 \leq \frac{a}{b} \text{ zur Wahl von } q \quad \nexists$$

Also gilt $0 \leq r < b$

2. Fall: $b < 0$

Es gilt (*) mit $|b|$,

$$\text{also gilt } a = q \cdot |b| + r, \underbrace{0 \leq r < |b|}_{\text{schon ok}}$$

für $b < 0$:

$$a = q \cdot (-b) + r \\ = (-q) \cdot b + r$$

- q, r sind eindeutig bestimmt:

angenommen, $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}$, so dass

$$a = \underline{q_1 \cdot b + r_1} = \underline{q_2 \cdot b + r_2}$$

$$0 \leq r_1, r_2 < |b|.$$

Sei o.B.d.A (ohne Beschränkung der Allgemeinheit) $r_2 \geq r_1$

$$\text{Dann ist } (q_1 - q_2) \cdot b = r_2 - r_1 \geq 0,$$

$$\text{also } b \mid (r_2 - r_1)$$

wir zeigen $(r_2 - r_1 = 0)$ durch Widerspruch:

angenommen, $r_2 - r_1 \neq 0$.

$$b \mid (r_2 - r_1), (r_2 - r_1 \neq 0)$$

$$\underbrace{\Rightarrow}_{6.2.c)} |b| \leq |r_2 - r_1| = r_2 - r_1 < r_2 < |b|$$

Also gilt $r_1 = r_2$.

Wegen (*), da $b \neq 0, q_1 = q_2$.

6.5 Definition

Sei $x \in \mathbb{R}$.

$\lceil x \rceil$ = kleinste ganze Zahl z mit $z \geq x$ (*ceiling*-Funktion, aufrunden)

$\lfloor x \rfloor$ = größte ganze Zahl z mit $z \leq x$ (*floor*-Funktion, abrunden)

6.6 Beispiel

$$\lceil 3 \rceil = 3, \lceil \frac{4}{3} \rceil = 2, \lfloor \frac{4}{3} \rfloor = 1, \lceil -\frac{4}{3} \rceil = -1, \lfloor -\frac{4}{3} \rfloor = -2$$

Anwendung: Stellenwertsysteme zur Basis b ($b \in \mathbb{N}, b > 1$)

$b = 2$: Binärsystem

$b = 8$: Oktalsystem

$b = 10$: Dezimalsystem

$b = 16$: Hexadezimalsystem

6.7 Satz (b-adische Darstellung)

Sei $b \in \mathbb{N}, b > 1$. Jede natürliche Zahl $n \in \mathbb{N}_0$, lässt sich eindeutig darstellen in der Form:

$$n = \sum_{i=0}^k x_i \cdot b^i, \text{ wobei für } k \text{ und } x_i \text{ gilt:}$$

(1) $k = 0$ für $n = 0$
 $b^k \leq n < b^{k+1}$ für $n > 0$

(2) $x_i \in \mathbb{N}_0, 0 \leq x_j \leq b - 1, x_k \neq 0$ für $n \neq 0$.

(Die x_i heißen Ziffern von n bzgl. b .
 Schreibweise: $n = (x_k \dots x_0)_b$

oder, falls b klar (z.B. $b = 10$)
 $n = x_k \dots x_0$

6.8 Beispiel

$b = 2$ (Binärsystem)

$$6 = 1 \cdot \underbrace{2^2}_{b^2} + 1 \cdot \underbrace{2^1}_{b^1} + 0 \cdot \underbrace{2^0}_{b^0} \quad (k = 2)$$

$$(6)_{10} = (110)_2$$

$$9 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \quad (9)_{10} = (1001)_2$$

$$0 = (0)_2$$

$$1 = (1)_2$$

$$2 = (10)_2$$

$$3 = (11)_2$$

$$4 = (100)_2$$

$$5 = (101)_2$$

\vdots

Ziffern für $b = 16$: $0, 1, \dots, 9, A, B, C, D, E, F$

$$(11)_{10} = (B)_{16}$$

Beweis (6.7):

verschärfte Induktion nach n :

Induktionsanfang: $n = 0$ (hat Darstellung $(0)_b$)

Induktionsschritt: sei $n > 0$.

- Induktionsvoraussetzung: Die Aussage gelte für alle $n' \in \mathbb{N}_0$ mit $n' < n$,
- Induktionsbehauptung: Die Aussage gilt für n .
- Beweis:

Nach Satz über Division mit Rest (6.3) gilt

$$\exists q, r \in \mathbb{Z} \text{ mit } n = q \cdot b + r$$

Setze $x_0 = r$

(also $x_0 = n \bmod b$ und $n' = q$ und $n' = \frac{n-x_0}{b}$),

dann ist $0 \leq n' < n$

Nach Induktionsvoraussetzung gilt also $n' = \sum_{i=0}^k x'_i \cdot b^i, k, x'_i$ mit (1), (2)

setze $x_{i+1} = x'_i$ für $i = 0, 1, \dots, k$

Dann ist $n = n' \cdot b + x_0$

$$\begin{aligned} &= \sum_{i=0}^k x'_i \cdot b^{i+1} + x_0 \\ &= \sum_{i=1}^{k+1} x_i \cdot b^i + x_0 \\ &= \sum_{i=0}^{k+1} x'_i \cdot b^i \end{aligned}$$

-(1) und (2) gelten:

(2) gilt nach Konstruktoren der x_i (1):

-falls $n' = 0, [z.z : b^0 \leq n < b^1]$

dann ist $n = x_0$.

wegen $x_0 < b$ ist $b^0 = 1 \leq n < b^1$

- falls $n' > 0$ [z.Z: $b^{k+1} \leq n < b^{k+2}$]

dann gilt (Ind.Vor.) $b+ \leq n' < b^{k+1}$

$$\Rightarrow b^{k+1} \leq b \cdot n' \leq \underbrace{b \cdot n' + x_0}_n$$

zeige II: Es ist $n' \leq b^{k+1} - 1$, also

$$bn' \leq b^{k+2} - b$$

$$\Rightarrow \underbrace{bn' + x_0}_n \leq b^{k+2} - b + x_0 < b^{k+2}$$

- Darstellung ist eindeutig:

$$\text{Sei } nj = \sum_{i=0}^k x_i \cdot b^i = \sum_{i=0}^l y_i \cdot b^i$$

$(x_i, y_i, k, l$ mit (1), (2)

Dann ist $x_0 = n \bmod b = y_0$
wende Ind.Vor. an auf $n' = \frac{n-x_0}{b} = \frac{n-y_0}{b}$, Beh. folgt. □

6.9 Korollar

Der Beweis liefert ein Verfahren zur Bestimmung der Darstellung von $n \in \mathbb{N}_0$ zur Basis $b > 1$:

$$\begin{aligned} n_0 &:= n, & x_0 &:= n_0 \bmod b \\ n_1 &:= \frac{n_0 - x_0}{b}, & x_1 &:= n_1 \bmod b \\ &\vdots \\ n_k &:= \frac{n_{k-1} - x_{k-1}}{b}, & x_k &:= n_k \bmod b \end{aligned}$$

solange, bis $n_k < b$ (d.h. $x_k = n_k$)

Dann $n = (n_k n_{k-1} \dots n_0)_b$

6.10 Beispiel

a) $(41)_{10}$ im Binärsystem ($b = 2$) (mit Algorithmus aus 6.9)

$$\begin{array}{lcl} 41 \bmod 2 = 1 & & \\ \frac{41-1}{2} = 20, & 20 \bmod 2 = 0 & \\ \frac{20-0}{2} = 10, & 10 \bmod 2 = 0 & \\ \frac{10-0}{2} = 5, & 5 \bmod 2 = 1 & \\ \frac{5-1}{2} = 2, & 2 \bmod 2 = 0 & \\ \frac{2-0}{1} = 1 < b(=2), \text{ fertig.} & & \end{array} \quad \begin{array}{l} | \quad 01 \\ | \quad 001 \\ | \quad 1001 \\ | \quad 01001 \\ | \quad 101001 \end{array}$$

also $(41)_{10} = (101001)_2$

oder (gut bei kleinen Zahlen):

$$\begin{aligned} \text{höchste 2er-Potenz } \leq 41 &\text{ ist } 2^5 = 32 \\ 41 - 32 &= 9 \\ \text{höchste 2er-Potenz } \leq 9 &\text{ ist } 2^3 = 8 \\ 9 - 8 &= 1 = 2^0 \\ (41)_{10} &= 2^5 + 2^3 + 2^0 = (101001)_2 \end{aligned}$$

b) $(41)_{10}$ im Hexadezimalsystem:

$$\begin{array}{lcl} 41 \bmod 16 = 9 & & \\ \frac{41-9}{16} = 2 < 16, \text{ fertig} & & \end{array} \quad \begin{array}{l} | \quad 9 \\ | \quad 29 \end{array}$$

$$\begin{aligned}
(41)_{10} &= (29)_{16} \\
[\text{oder: } (41)_{10} &= (\underbrace{10}_{(0010)} \underbrace{1001}_{(1001)})_2 = (29)_{16} \\
(0010)_2 &= (2)_{10} = (2)_{16} \\
(1001)_2 &= (9)_{10} = (9)_{16}]
\end{aligned}$$

c) $(41)_5$ im 3er-System:

$$(41)_5 = 4 \cdot 5^1 + 1 \cdot 5^0 = (21)_{10}$$

$$\begin{array}{r|l}
21 \bmod 3 = 0 & 0 \\
\frac{21-0}{3} = 7, \quad 7 \bmod 3 = 1 & 10 \\
\frac{7-1}{3} = 2 < 3, \text{ fertig} & 210 \\
(41)_5 = (210)_3 &
\end{array}$$

6.11 Satz (Rechenregeln für modulo)

Seien $a, b \in \mathbb{Z}, m \in \mathbb{N}$

- $(a \bmod m) \bmod m = a \bmod m$

$$M(M(a)) = M(a)$$

- Platzhalter $*$: $+, -, \cdot$

$$\begin{aligned}
\text{Dann } (a * b) \bmod m &\stackrel{(i)}{=} [(a \bmod m) * (b \bmod m)] \bmod m \\
&\stackrel{(ii)}{=} [(a * (b \bmod m))] \bmod m \\
&\stackrel{(iii)}{=} [(a \bmod m) * b] \bmod m
\end{aligned}$$

Beweis

$$\text{a) } a = q \cdot m + \underbrace{r}_{a \bmod m} \quad r = 0 \cdot m + \underbrace{r}_{r \bmod m}$$

$$\text{b) (i) } \bullet \text{ für } +$$

$$a = q_1 \cdot m + r_1$$

$$b = q_2 \cdot m + r_2$$

$$r_1 = a \bmod m$$

$$r_2 = b \bmod m$$

Wir haben

$$(1) \ a + b = (q_1 + q_2) \cdot m + r_1 + r_2$$

$$(2) \ r_1 + r_2 = q \cdot m + s$$

$$(1, 2) \ (3) \ a + b = (q_1 + q_2 + q) \cdot m + s$$

$$\text{also } (a + b) \bmod m = s = (r_1 + r_2) \bmod m$$

- für $*$ \cong $-$ analog

- für $*$ \cong \cdot .

$$a \cdot b = (q_1 \cdot q_2 \cdot m + r_1 \cdot q_1 + r_2 \cdot q_2) \cdot m + r_1 \cdot r_2.$$

$$\Rightarrow (a \cdot b) \bmod m = [r_1 \cdot r_2] \bmod m$$

$$= [(a \bmod m) \cdot (b \bmod m)]$$

$$= 6.11 \text{ a)}$$

$$[(a \cdot b) \bmod m] \bmod m$$

$$(ii) \ \underbrace{[a \cdot (b \bmod m)] \bmod m}_m \underbrace{=}_{so} [a \bmod m \cdot (b \bmod m) \bmod m] \bmod m$$

$$\underbrace{=}_{6.11a)} [(a \bmod m) \cdot (b \bmod m)] \bmod m$$

(iii) analog

□

6.12 Bemerkung

6.11 gilt auch für mehr als 2 Summanden / Faktoren.

z.B. $(a \cdot b \cdot c) \bmod m = [(a \bmod m) \cdot (b \bmod m) \cdot (c \bmod m)] \bmod m$

6.11 wiederholt anwenden

6.13 Beispiele

- $a = 10, b = 7, m = 4$
 $a \bmod m = 2, b \bmod m = 3$

$$\begin{aligned} (+) \quad & [(a \bmod m) + (b \bmod m)] \bmod m = (2 + 3) \bmod 4 = 1 \\ & (a + b) \bmod m = 17 \bmod 4 = 1 \end{aligned}$$

$$(-) [(a \bmod m) - (b \bmod m)] \bmod m = (2 - 3) \bmod 4 = 3$$

$$(a - b) \bmod m = (10 - 7) \bmod 4 = 3$$

$$(\cdot) [(a \bmod m) \cdot (b \bmod m)] \bmod m = (2 \cdot 3) \bmod 4 = 2$$

$$(a \cdot b) \bmod m = 70 \bmod 4 = 2$$

Beobachtung: mod-Regeln können große Zwischenergebnisse vermeiden

- $(11 \cdot 12 \cdot 13) \bmod 7$?

$$(11 \cdot 12 \cdot 13) \bmod 7 = 11 \cdot 12 \cdot 13 \bmod 7 = (1716) \bmod 7 = 1$$

$$\text{oder } (11 \cdot 12 \cdot 13) \bmod 7 = [(11 \bmod 7)(12 \bmod 7)(13 \bmod 7)] \bmod 7$$

$$= (4 \cdot 5 \cdot 6) \bmod 7$$

$$= 120 \bmod 7 = 1$$

$$\text{oder } (11 \cdot 12 \cdot 13) \bmod 7 = [((-3) \bmod 7) \cdot ((-2) \bmod 7) \cdot ((-1) \bmod 7)] \bmod 7$$

$$= ((-3) \cdot (-2) \cdot (-1)) \bmod 7$$

$$= (-6) \bmod 7 = 1$$

- Welchen Rest lässt $(214936)^{1517433}$ bei Division durch 7?

$$[(214936)^{1517433}] \bmod 7 = \left[\left(\begin{array}{c} 210000 \\ +4900 \\ +35 \\ +1 \end{array} \right) \bmod 7 \right]^{1517433} \bmod 7$$

$$= (1 \bmod 7)^{1517433} \bmod 7 = 1$$

- Welchen Rest lässt $(214935)^{1517433} \bmod 7$
→ Rest 0.

- Welchen Rest lässt $(214934)^{1517433} \bmod 7$
 $(214935 - 1)^{1517433} \bmod 7$
 $= (-1)^{1517433} \bmod 7 = (-1) \bmod 7 = 6$

- $(214937)^{1517433} \bmod 7 = (2^{3 \cdot 505811}) \bmod 7$
 $= ((2^3)^{505811}) \bmod 7$
 $= (8^{505811}) \bmod 7$
 $= 1^{505811} \bmod 7 = 1$

- Teilbarkeit und Quersummen

Satz: Sei $a \in \mathbb{N}, n \geq 1, t \in \mathbb{N}, t \mid n$

$$a = \sum_{i=0}^k a(n+1)^i \quad (n+1) \text{ addische Darstellung}$$

$$8 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 = (1000)_2$$

Quersumme

$$Q_{n+1}(a) = \sum_{i=0}^k a_i$$

Es gilt $t \mid a \Leftrightarrow t \mid Q(a)$

3-Regel. 123 durch 3 teilbar

9-Regel 51111 durch 9 teilbar.

- ISBN-10 (veraltet) Internationale Standard-Buch-Nr
9 Kennziffern, 10. Stelle (Prüfziffer)

$$a_1 - a_2 a_3 a_4 - a_5 a_6 a_7 a_8 a_9 - a_{10}$$

$$a_{10} = \left(\sum_{i=0}^9 a_i \cdot i \right) \bmod 11 \quad a_{10} = 10, \rightarrow a_{10} = x$$

WHK:

$$3 - 540 - 20521 - 7$$

$$3 - 5402052 - 5$$

$$1 - 54020523 - 1$$

6.14 Definition (Kongruenzrelationen modulo m)

Sei $m \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ definiere

$$a \equiv b \pmod{m} : \Leftrightarrow m \mid (a - b)$$

”a kongruent b modulo m”

$$\text{Beispiel: } 17 \equiv -4 \pmod{7} \quad 17 \not\equiv -4 \pmod{7} = 3$$

Beachte:

- $\equiv \pmod{m}$ ist Relation auf \mathbb{Z}
- $\text{mod } m : \mathbb{Z} \rightarrow \{0, 1, \dots, m-1\} \quad a \rightarrow a \bmod m$

6.15 Satz

$$\text{a) } a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$$

- b) $a \equiv 0 \pmod{m} \Leftrightarrow m \mid a$
- c) $a \bmod m \equiv a \pmod{m}$
- d) Kongruenzrelation modulo m ist Äquivalenzrelation
- e) $a \equiv b \pmod{m}, c \in \mathbb{Z} \Rightarrow c \cdot a \equiv c \cdot b \pmod{m}$

6.16 Beispiel

- $17 \bmod 7 = 3$
 $17 \equiv 3 \pmod{7}$
 $17 \equiv 10 \pmod{7}$
 $17 \equiv -4 \pmod{7}$
- $2 \cdot 3 \equiv 2 \cdot 2 \pmod{2}$
 $6 \equiv 4 \pmod{2}$
 aber $3 \not\equiv 2 \pmod{2}$

Beweis zu 6.15)

- a) „ \Rightarrow “ $a \equiv b \pmod{m} \Leftrightarrow a = km + b$ für $k \in \mathbb{Z}$
 $\Rightarrow a \bmod m = (k \cdot m) \bmod m + b \bmod m = b \bmod m$

„ \Leftarrow “ $a \bmod m = b \bmod m \Rightarrow$
 $a = a_1 \cdot m + r \quad (1)$
 $b = a_2 \cdot m + r \quad (2)$
 $(1, 2) a - b = (a_1 - a_2) \cdot m$
 $\Rightarrow m(a - b)$

- b) Spezialfall von a) $(b = 0)$
- c) zu zeigen: $a \bmod m \equiv a \pmod{m}$
 $\stackrel{a)}{\Leftrightarrow} (a \bmod m) \bmod m \stackrel{6.11 \text{ a)}}{=} a \bmod m$

- d) reflexiv? symmetrie, transitivität?

$$m \mid (a - a) \checkmark \quad m \mid (a - b) \checkmark \quad \Leftrightarrow m \mid (b - a)$$

$$m \mid (a - b), \quad m \mid (b - c) \Rightarrow m \mid \underbrace{[(a - b) + (b - c)]}_{(a - c)}$$

$$\begin{aligned} \text{e) } m \mid (a - b) &\Rightarrow a - b = k \cdot m \quad k \in \mathbb{Z} \\ &\Rightarrow ca - cb = c \cdot k \cdot m = kc \cdot m \\ &m \mid (ca - cb) \end{aligned}$$

Wiederholung: Kongruenz modulo m $m \in \mathbb{N} \quad a, b \in \mathbb{Z}$

$$\begin{aligned} a &\equiv b \pmod{m} \\ :\Leftrightarrow m &\mid (a - b) \end{aligned}$$

6.17 Satz und Definition

Die Äquivalenzklassen der Kongruenzrelation modulo m sind genau die Mengen

$$\{k \cdot m : k \in \mathbb{Z}\}, \{1 + km : k \in \mathbb{Z}\}, \dots, \{(m-1) + km : k \in \mathbb{Z}\}$$

Kurzschreibweise: $r + m\mathbb{Z} \quad r = 0, \dots, m-1$

Die Menge $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ ein Repräsentantensystem.

Beispiel: mod2 gerade und ungerade

$$\mathbb{Z}_2 = \{0, 1\}$$

Beispiel 6.16:

$$\begin{aligned} x &\equiv 3 \pmod{7} \\ 3 &\equiv 3 \pmod{7} \\ 10 &\equiv 3 \pmod{7} \\ 17 &\equiv 3 \pmod{7} \end{aligned}$$

6.18 Satz

Seien $a_1 \equiv a_2 \pmod{m}$ und $*$: $+, -, \cdot$

$$b_1 \equiv b_2 \pmod{m}$$

Dann $a_1 * b_1 \equiv a_2 * b_2 \pmod{m}$

Beweis: Nach 6.14 a)

$$a_1 \bmod m = a_2 \bmod m \tag{1}$$

$$b_1 \bmod m = b_2 \bmod m \tag{2}$$

$$\begin{aligned}
\text{Dann } (a_1 * b_1) \bmod m &\stackrel{6.11b)}{=} [(a_1 \bmod m) * (b_1 \bmod m)] \bmod m \\
&\stackrel{(1,2)}{=} [(a_2 \bmod m) * (b_2 \bmod m)] \bmod m \\
&\stackrel{6.11b)}{=} (a_2 * b_2) \bmod m
\end{aligned}$$

□

6.19 Beispiel

a) Welche Zahlen erfüllen die Voraussetzung?

$$\begin{aligned}
2x + 1 &\equiv 5 \pmod{6} \\
1 &\equiv 1 \pmod{6} \\
&\stackrel{6.18}{\Leftrightarrow} 2x \equiv 4 \pmod{6}
\end{aligned}$$

Welche $x \in \{0, \dots, 5\} = \mathbb{Z}_6$ erfüllen die Kongruenzrelation?

$$x = 2, \quad x = 5$$

$$2x \equiv 4 \pmod{6} \Leftrightarrow 2 \cdot (x \bmod 6) \equiv 4 \pmod{6}$$

Lösungsmenge: $(2 + 6\mathbb{Z}) \cup (5 + 6\mathbb{Z})$

b) $x^2 + 3y = 3z^2 \quad x, y, z \in \mathbb{Z}$

Trick Mod-Reihe:

$$\begin{aligned}
(x \bmod 3)^2 &\equiv 2 \pmod{3} \\
0^2 &\equiv 0 \pmod{3} \\
1^2 &\equiv 1 \pmod{3} \\
2^2 &\equiv 1 \pmod{3}
\end{aligned}$$

Gleichung hat keine Lösung!

6.20 Definition

Seien $a_1, \dots, a_r \in \mathbb{Z}$

- a) Ist mindestens ein $a \neq 0$, so ist der größte gemeinsame Teiler $ggT(a_1, \dots, a_r)$ die größte natürliche Zahl, die alle a_i teilt.
- b) Sind alle $a \neq 0$, so ist das kleinste gemeinsame Vielfache $kgV(a_1, \dots, a_r)$ die kleinste natürliche Zahl die von allen a_i geteilt wird.

6.21 Bemerkung

- a) $ggT(a_1, \dots, a_r)$ existiert und ist eindeutig.

$$1 \mid a_i \quad \forall i \in \{1, \dots, r\} \quad t \leq |a_i|$$

- b) $kgV(a_1, \dots, a_r)$ existiert und ist eindeutig.

$$|a_1| \cdot \dots \cdot |a_r| \text{ wird von allen } a_i \text{ geteilt.}$$

- c) $ggT(a_1, \dots, a_r) = ggT(|a_1|, \dots, |a_r|)$ $kgV(a_1, \dots, a_r) = kgV(|a_1|, \dots, |a_r|)$.

6.22 Definition

Ist $ggT(a_1, \dots, a_r) = 1$, so heißen a_1, \dots, a_r teilerfremd.

Ist $ggT(a_i, a_j) = 1$ für alle $i \neq j$, so heißen a_1, \dots, a_r paarweise teilerfremd.

Stärker als Teilerfremd

6, 10, 15

$$ggT(6, 10) = 2$$

$$ggT(10, 15) = 5$$

$$ggT(6, 15) = 3$$

$$ggT(6, 10, 15) = 1$$

Berechnung des ggT zweier Zahlen mit Euklidischem Algorithmus (Euklid 365 v.Chr. - 300 v.Chr.)

Grundprinzipien im folgenden Lemma:

6.23 Lemma

Seien $a, b, q \in \mathbb{Z}$ $b \neq 0$. Dann ist

$$ggT(a, b) = ggT(q \cdot a + b, a).$$

[Beachte für den zweiten ggT: ist $a = 0$, so ist $q \cdot a + b = b \neq 0$]

Beweis: $t \mid (q \cdot a + b) \wedge t \mid a \stackrel{6.2 \text{ b)}}{\Leftrightarrow} t \mid a \wedge t \mid b$ □

Gegeben seien jetzt a, b , nicht beide 0, O.B.d.A $b \neq 0$

Wir wollen $ggT(a, b)$ bestimmen.

$$\begin{array}{ll}
 \text{Setze } a_0 = a, & a_1 = b \\
 a_0 = q_1 a_1 + a_2 & \text{(Division mit Rest)} \\
 a_1 = q_2 a_2 + a_3 & \text{(Division mit Rest)} \\
 \vdots & \\
 a_{n-1} = q_n a_n + 0 & \text{erstes Mal Rest 0}
 \end{array}$$

Nun ist $ggT(a, b) = ggT(a_0, a_1) \stackrel{6.23}{=} ggT(a_1, a_2) = \dots = ggT(a_{n-1}, a_n) = |a_n|$.

Beachte: Ist $n \geq 2$, so auch $a_n > 0$, d.h. $ggT(a_{n-1}, a_n) = a_n$.

D.h. nur für $n = 1$, d.h. $b \mid a$, muss man Betrag verwenden (falls $b < 0$).

Beweis für Euklidischen Algorithmus ✓

6.24 Euklidischer Algorithmus

Input: $a, b \in \mathbb{Z}$ nicht beide 0

IF $b = 0$, then $y := |a|$

IF $b \neq 0$ and $b \mid a$, then $y := |b|$

IF $b \neq 0$ and $b \nmid a$ then $x := a, \quad y := b$

while $x \bmod y \neq 0$ do

$r := x \bmod y, \quad x := y, \quad y := r$

Output y ($= ggT(a, b)$)

Beispiel:

a) $ggT(-20, 0) = 20$

b) $ggT(-20, -10) = 10$

c) $a = 48, \quad b = -30$

also $x = 48, \quad y = -30$

$48 \bmod (-30) = 18 \neq 0 \quad x = -30, \quad y = 18$

$(-30) \bmod 18 = 6 \neq 0 \quad x = 18, \quad y = 6$

$$18 \bmod 6 = 0 \\ \rightarrow ggT(48, -30) = 6$$

6.25 Satz (Bachét de Méziriac (1581 - 1638))

Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann existieren s, t mit $ggT(a, b) = sa + tb$

Anmerkung: In Literatur auch Lemma von Bezout.

Beweis:

Ist $b = 0$, $ggT(a, b) = |a| = s \cdot a + t \cdot b$ mit

$$s = \begin{cases} 1 & \text{falls } a > 0 \\ -1 & \text{falls } a < 0 \end{cases}$$

Ist $b \neq 0$, $b|a$ so $ggT(a, b) = |b| = s \cdot a + t \cdot b$ mit

$$t = \begin{cases} 1 & \text{falls } b > 0 \\ -1 & \text{falls } b < 0 \end{cases}$$

Ist $b \neq 0$, $b \nmid a$ $a_0 = a, a_1 = b$

EA: $a_0 = q_1 \cdot a_1 + a_2$,

$a_1 = q_2 \cdot a_2 + a_3, \dots, a_{n-1} = q_n a_n + 0$

$ggT(a, b) = a_n$

Zeige durch Induktion nach j die Existenz von $s_j, t_j \in \mathbb{Z}$ mit

$A(j) : a_j = s_j \cdot a_0 + t_j \cdot a_1$

beachte die Induktion läuft nur solange wie a_j definiert ist.

I.A:

$A(0) : j = 0 : s_0 = 1, t_0 = 0 \quad a_0 = 1 \cdot a_0 + 0 \cdot a_1 \quad \checkmark$

$A(1) : j = 1 : s_1 = 0, t_1 = 1 \quad a_1 = 0 \cdot a_0 + 1 \cdot a_1 \quad \checkmark$

I.S:

I.V: Sei $2 \leq j \leq n$ und es gelte:

$A(j-2) : a_{j-2} = s_{j-2} \cdot a_0 + t_{j-2} \cdot a_1 \quad A(j-1) : a_{j-1} = s_{j-1} \cdot a_0 + t_{j-1} \cdot a_1$

I.B: $A(j)(A(j-2) \wedge A(j-1)) \Rightarrow A(j)$

EA

$$\begin{aligned}
a_j &= a_{j-2} - q_{j-1} \cdot a_{j-1} \\
&\underbrace{=}_{I.V.} s_{j-2} \cdot a_0 + t_{j-2} \cdot a_1 - q_{j-1} \cdot (s_{j-1} + t_{j-1} a_1) \\
&= \underbrace{(s_{j-2} - q_{j-1} \cdot s_{j-1})}_{=:s_j} \cdot a_0 + \underbrace{(t_{j-2} - q_{j-1} \cdot t_{j-1})}_{=:t_j} \cdot a_1 \\
&\Rightarrow \text{Satz folgt mit } j = n \text{ und } s = s_n, t = t_n
\end{aligned}$$

□

6.26 Erweiterter Euklidischer Algorithmus

Input $a, b \in \mathbb{Z}$ (nicht beide 0)

IF $b = 0$ then

$y = |a|$, if $a > 0$ then $s = 1$ else $s = -1$

$t = 0$

IF $b \neq 0$ and $b|a$ then

$y = |b|$, $s = 0$, if $b > 0$ then $t = 1$ else $t = -1$

IF $b \neq 0$ and $b \nmid a$ then

$x = a, y = b, s_1 = 1, s_2 = 0, t_1 = 0, t_2 = 1$

while $x \bmod y \neq 0$ do

$q = x \operatorname{div} y, r = x \bmod y,$

$s = s_1 - q \cdot s_2, \quad t = t_1 - q \cdot t_2,$

$s_1 = s_2, s_2 = s, \quad t_1 = t_2, t_2 = t,$

$x = y, y = r$

Output:

$y(ggT(a, b))$

$s, t(y = s \cdot a + t \cdot b)$

Bsp: $a = 48, b = -30$

	x	y	s_1	s_2	s	t_1	t_2	t	q	r
$0 \neq 18 = 48 \bmod (-30) = 18 \neq 0$	48	-30	1	0	0	1				
$= 6 \neq 0(-30) \bmod 18$	-30	18	0	1	1	1	1	1	-1	18
$18 \bmod 6 = 0$	18	6	1	2	2	1	3	3	-2	6

$6 = 2 \cdot 48 + 3 \cdot (-30) \rightarrow$ nicht eindeutig

$48 = (-1) \cdot (-30) + 18$

$$s = s_1 \cdot q \cdot s_2$$

$$t = t_1 - q \cdot t_2$$

Beachte: Darstellung ist nicht eindeutig!

$$6 = 7 \cdot 48 + 11 \cdot (-30)$$

6.27 Korollar

(Seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$.

- a) Sind a, b nicht beide 0, so gilt: a und b teilerfremd $\Leftrightarrow \exists s, t \in \mathbb{Z} : s \cdot a + t \cdot b = 1$
- b) Sind a, b nicht beide 0. So gilt: Ist $c|a$ und $c|b$, so gilt $c|ggT(a, b)$
- c) Ist $ggT(a, b) = 1$ und $a|b \cdot c$, so $a|c$
- d) Ist $ggT(c, m) = 1$ und $c \cdot a \equiv c \cdot b \pmod{m}$ so gilt $a \equiv b \pmod{m}$

Beweis:

- a) \Rightarrow : 6.25
 $\Leftarrow d = ggT(a, b)$
 nach 6.2.b): $d | \underbrace{sa + tb}_1 \Rightarrow d = 1$
- b) 6.25 $ggT(a, b) = s \cdot a + t \cdot b$
 $c|a \wedge c|b \xRightarrow{6.2b)} c|sa + tb$
- c) 6.25 $\exists s, t \in \mathbb{Z}$ mit $1 = s \cdot a + t \cdot b$
 also $c = s \cdot c \cdot a + t \cdot c \cdot b$
 Da $a|a$ und $a|bc$, folgt (6.2b)
 $a|sca + tbc \Rightarrow a|c$
- d) $m|c(a - b), ggT(c, m) = 1$
 $\Rightarrow m|(a - b)$ also $a \equiv b \pmod{m}$
 Vergleiche: 6.15e).

6.28 Bemerkung

- a) Ist $k > 2$, so $ggT(a_1, \dots, a_k) = ggT(ggT(a_1, \dots, a_k), a_k)$

- b) $\exists s_1, \dots, s_k, s \in \mathbb{Z}$ mit $ggT(a_1, \dots, a_k) = s_1 a_1 + \dots + s_k a_k$ (Beweis per Induktion)
- c) 6.27c) Verallgemeinerbar auf k Zahlen:
 $c|a_1, \dots, a_k \Rightarrow c|ggT(a_1, \dots, a_k)$
- d) Ist $k > 2$, so $kgV(a_1, \dots, a_k) = kgV(kgV(a_1, \dots, a_k), a_k) a_{k-1}$
und $a \neq 0$ (alle nicht 0)

6.29 Definition

Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn 1 und p die einzigen natürlichen Zahlen sind, die p teilen.

(D.h. $ggT(k, p) = 1$ für alle $1 \leq k \leq p$)

6.30 Satz

Ist p eine Primzahl, $a_1, \dots, a_k \in \mathbb{Z}$ und $p|a_1 \cdot a_2 \cdot \dots \cdot a_k$
so existiert $1 \leq j \leq k$ mit $p|a_j$

Beweis: Induktion nach k :

IA:

$k = 1$ ✓

IS:

$k - 1 \rightarrow k$ Gilt $p|a_k$ ✓

Ist $p \nmid a_k$ so $ggT(p, a_k) = 1$ (p Primzahl)

Nach 6.27c): $p|a_1 \cdot \dots \cdot a_{k-1}$

$\Rightarrow p|a_j$ für ein $1 \leq j \leq k - 1$ □

6.31 Fundamentalsatz der elementaren Zahlentheorie

Zu jeder natürlichen Zahl $a \geq 2$ gibt es endlich viele verschiedene Primzahlen p_1, \dots, p_n und natürliche Zahlen e_1, \dots, e_n mit $a = p_1^{e_1} \cdot \dots \cdot p_n^{e_n}$. Die p_i heißen Primfaktoren von a . Die Darstellung von a als Produkt von Primzahlen ist bis auf die Reihenfolge eindeutig.

$$a = \prod_{i=1}^n p_i^{e_i} = p_1 \cdot \dots \cdot p_n$$

Beweis: Existenz (per Induktion)

IA: $a = 2$ ✓

IS: IV: Aussage gilt für $2, \dots, a-1$

IB: Aussage gilt für a .

Beweis:

Fall 1: a Primzahl ✓

Fall 2: a keine Primzahl

$a = b \cdot c$ für $1 \leq b, c \leq a$

wende I.V. auf b und c an \rightarrow fertig.

Eindeutigkeit (per Induktion) über $s(a) := \sum_{i=1}^n e_i$ $s(2) = 1, s(4) = 2$

IA: $s(a) = 1 \Rightarrow a$ Primzahl ✓

IV: Aussage gelte für alle $a', s(a') < s(a)$

IB: Aussage gilt auch für a

Beweis:

$$a = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_e \quad |s(a) = m \leq l$$

p_i, q_j Primzahl (nicht unbedingt verschieden)

$$p_1 \mid a \Rightarrow p_1 \mid q_1 \cdot \dots \cdot q_e \xrightarrow{6.30} p_1 \mid q_j \text{ für ein } j$$

$$\xrightarrow{q_j \text{ Prim}} p_1 = q_j \rightarrow a' = p_1 \cdot \dots \cdot p_n = q_1 \cdot q_{q-1} \cdot q_{q+1} \cdot \dots \cdot q_e$$

wende I.V. auf a' an, fertig

✓

6.32 Korollar (Euklids Lemma)

Es gibt unendlich viele Primzahlen.

Beweis: Angenommen es gibt nur unendlich viele Primzahlen p_1, \dots, p_n

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

$$\stackrel{6.31}{\Rightarrow} \exists p_i \quad p_i \mid a \quad q = p_i \quad 1 \leq i \leq n$$

$$\text{Dann gilt nach 6.2 b)} \quad q \mid \underbrace{a - p_1 \cdot \dots \cdot p_n}_{=1}$$

$$\Rightarrow q = 1 \nmid$$

6.33 Korollar

Seien $a, b \in \mathbb{N} \quad a, b \geq 2$

Seien $P(a)$ und $P(b)$ die Menge der Primteiler von a und b , d.h.

$$a = \prod_{p \in P(a)} p^{n(p)} b = \prod_{p \in P(b)} p^{m(p)} \quad n(p), m(p) \in \mathbb{N}$$

Dann ist

$$ggT(a, b) = \prod_{p \in P(a) \cap P(b)} p^{\min(n(p), m(p))}$$

(Hinweis: Leeres Produkt = 1)

$$KgV(a, b) = \prod_{p \in P(a) \setminus P(b)} p^{n(p)} \cdot \prod_{p \in P(a) \cap P(b)} p^{\max(n(p), m(p))} \cdot \prod_{p \in P(b) \setminus P(a)} p^{m(p)}$$

insbesondere $a \cdot b = ggT(a, b) \cdot KgV(a, b)$

Beispiel

$$a = 1248 = 2^5 \cdot 3 \cdot 13$$

$$b = 3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$$

$$ggT(a, b) = 2^2 \cdot 3^1 = 12$$

$$KgV(a, b) = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 = 393120$$

7 Kombinatorik

Ziel: Anzahlbestimmungen von endlich vielen verschiedenen Objekten (Kombinationen).

7.1 Satz

a) Seien A, B endliche Mengen.

$$\text{Dann gilt: } |A \cup B| = |A| + |B| - |A \cap B|$$

b) A_1, \dots, A_n endliche Mengen.

$$\text{Dann } |A_1 \times \dots \times A_n| = \prod_{i=1}^n |A_i|$$

$$(q_1, \dots, q_n) \in \prod_{i=1}^n A_i$$

Beweis: klar

Bemerkung: a) lässt sich verallgemeinern \leadsto Ein-/Ausschlussprinzip (WHK 2.32)

Beweis (per Induktion):

IA: $n = 1$ ✓

IS: $n \rightarrow n + 1$

$$\begin{aligned} |A_1 \times \dots \times A_n \times A_{n+1}| &= \sum_{a \in A_{n+1}} |A_1 \times \dots \times A_n \times \{a\}| = |A_{n+1}| \cdot |A_1 \times \dots \times A_n| \stackrel{I.V.}{=} \\ &|A_{n+1}| \cdot \prod_{i=1}^n |A_i| \quad \checkmark \quad \square \end{aligned}$$

7.2 Beispiel

a) Wieviele "Wörter" der Länge n gibt es über dem "Alphabet" $\{0,1\}$

\rightarrow Wort der Länge $n \cong$ n-Tupel.

$$|\{0,1\}^n| = 2^n$$

$$|\{0,1\}^3| = |\{(0,0,0), (0,0,1), \dots\}| = 8$$

b) Wie viele Folgen der Länge 1000 aus den Symbolen A, G, C, T gibt es?

$\rightarrow 4^{1000}$

Auswahlansahlen

Anzahl an möglichen Auswahlen von k Objekten aus einer Menge mit n Objekten.

- Reihenfolge relevant oder nicht
- Wiederholung möglich oder nicht

→ 4 Typen von Auswahlen

7.3 Geordnete Auswahl ohne Wiederholung

Fragestellung I

Menge B ("Urne") mit n verschiedenen Objekten b_1, \dots, b_n . Wähle nacheinander k davon aus und lege sie der Reihenfolge nach aus.

$\leadsto (b_{i_1}, b_{i_2}, \dots, b_{i_k})$ Dabei $i_j \neq i_l \quad j \neq l$

Wie viele solcher k -Tupel sind möglich?

Fragestellung II (nur andere Interpretation)

Wie viele injektive Abbildungen $\pi = \begin{pmatrix} 1 & \dots & k \\ b_{i_1} & \dots & b_{i_k} \end{pmatrix}$

$$\pi(a) = \pi(b) \stackrel{\pi \text{ injektiv}}{\Rightarrow} a = b$$

7.4 Definition

Setze für $k, n \in \mathbb{N}$

$$(n)_k := n \cdot (n-1) \cdot \dots \cdot (n-k+1)$$

Also $(n)_1 = n$ und für $k > n$, $(n)_k = 0$

(Rekursive Definition $(n)_k := (n)_{k-1} \cdot \underbrace{(n-k+1)}_{=n-(k-1)}$)

Für $k \leq n : (n)_k = \frac{n!}{(n-k)!}$

Insbesondere $(n)_n = n!$

7.5 Satz

Es gibt genau $(n)_k$ viele Auswahlen von k Objekten aus einer Menge B mit n Objekten, wenn keine Wiederholungen möglich sind und die Anordnung berücksichtigt wird.

Beispiel: Erste 3 Plätze bei einem Rennen mit 12 Teilnehmern.

Beweis Sei $n \in \mathbb{N}$ beliebig, aber fest. Induktion nach k :

Ind.anf.: $k = 1$: n Möglichkeiten $(n)_1 = n \checkmark$

Ind.schritt: Sei $k \geq 1$.

Ind.vor: Aussage sei wahr für k

Ind.beh: Die Aussage gelte für $k + 1$, d.h. bei $k + 1$ Objekten gibt es $(n)_{k+1}$ Möglichkeiten.

Beweis:

- falls $k + 1 > n$, dann 0 Möglichkeiten $= (n)_{k+1}$
- falls $k + 1 \leq n$: Nach Ind.vor. gibt es $(n)_k$ Möglichkeiten, k Elemente aus B auf die Plätze $1, \dots, k$ zu verteilen.

Für jede davon gibt es $n - k$ Möglichkeiten, Platz $k + 1$ zu besetzen.

\Rightarrow insgesamt $(n)_k \cdot (n - k)$

$$\underbrace{(n)_k}_{\substack{n \cdot (n-1) \cdot \dots \cdot (n-k+1) \\ k \text{ Faktoren}}} \cdot (n - k) = (n)_{k+1}$$

□

7.6 Beispiel

a) Beispiel 7.3 Pferderennen:

$12 \cdot 11 \cdot 10 = 1320$ Möglichkeiten für die ersten drei Plätze.

b) Anzahl der Wörter der Länge 3 über $\{a, b, \dots, z\}$, die keinen Buchstaben enthalten:

$26 \cdot 25 \cdot 24 = 15600$

Wie viele davon enthalten ein x ?

$$26 \cdot 25 \cdot 24 - \underbrace{25 \cdot 24 \cdot 23}_{\text{ohne } x} = 25 \cdot 24 \cdot (26 - 23) = 1800$$

(vergleiche: Anzahl aller Wörter der Länge 3 (7.1b))
 $= 26^3 = 17576$)

Aus 7.3 und 7.5 folgt:

7.7 Korollar

$A, B \neq \emptyset$ endliche Mengen mit $|A| = k, |B| = n$, dann gibt es genau $(n)_k$ injektive Abbildungen $A \rightarrow B$.

$|A| = k, \quad |B| = n$
 $(n)_k$ injektive Abbildungen $A \rightarrow B$

Insbesondere: $|A| = |B| = n$, dann gibt es $(n)_n = n!$

Bijektionen $A \rightarrow B$

7.8 Definition

Eine bijektive Abbildung $A \rightarrow B$ heißt Permutation auf A.

Anzahl der Permutationen auf endlicher Menge $A = |A|!$ (Korollar 7.7)

speziell: $A = \{1, \dots, n\}, |A| = n$

Dann bezeichnet S_n die Menge aller Permutationen auf A , es gilt also $|S_n| = n!$

7.9 Geordnete Auswahl mit Wiederholung

Wähle k mal ein Objekt aus der Urne mit n Objekten aus, dabei wird die Reihenfolge der Ziehungen notiert und das Objekt nach der Auswahl wieder in die Urne zurückgelegt.

Beispiel:

Ziehen einer Losnummer, (Erstellung eines Autokennzeichens)

Oder: Färbe die Objekte $1, \dots, k$ mit jeweils einer von n Farben, die Farbe darf dabei mehrfach verwendet werden.

7.10 Satz

Es gibt genau n^k geordnete Auswahlen mit möglicher Wiederholung von k Elementen aus einer Menge B mit n Elementen.

Beweis:

Menge aller Auswahlen ist $\underbrace{B \times B \times \dots \times B}_k = B^k$

Nach 7.1 gilt $|B^k| = |B|^k = n^k$. □

7.11 Bemerkung / Korollar

Schreibe Auswahl als $\begin{pmatrix} 1 & 2 & \dots & k \\ b_1 & b_2 & \dots & b_k \end{pmatrix}$

($b_i \in B$, nicht notwendig verschieben), dann ist die Anzahl der Auswahlen in 7.10 genau die Anzahl aller Abbildungen $\{1, \dots, k\} \rightarrow B$

Also gibt es genau n^k Abbildungen $A \rightarrow B$, wenn $|A| = k$, $|B| = n$.

7.12 Ungeordnete Auswahl ohne Wiederholung

Urne mit n Objekten, wähle k Objekte aus, Reihenfolge ist unerheblich (*Korb*). Wie viele Möglichkeiten (verschiedene Korbfüllungen) gibt es?

Beispiel:

Lotto ($n = 49, k = 6$)

Feuerwehrproblem