

MENGEN (LEHRE)

geht auf CANTOR zurück

Def.: Eine Menge (A) ist eine Ansammlung wohlunterschiedener Objekte (unserer Anschauung), sodass für jedes solche Objekt entschieden werden kann, ob es zur Menge A gehört oder nicht.

Fall 1: es gehört dazu

Objekt x ist Element von A

$$x \in A \quad (x \in A)$$

[Epsilon]

Fall 2: es gehört nicht dazu

x ist nicht Element von A

$$x \notin A \quad (x \notin A)$$

[Epsilon]

zwei mögliche Fälle \Rightarrow zweiwertige LOGIK
jedes Objekt nur 1x pro Menge

kritisch: kein Entscheidungsverfahren in Definition

Einschränkung: Objekte eines Teils unserer Anschauung
Gesamtheit der "interessanten" Objekte

heißt UNIVERSUM M

dann: interessante Menge ist Menge interessanter
Objekte \Rightarrow Teil des Universums

"Beschreibung" einer Menge A :

1. Angabe aller Elemente der Menge A :

z.B.: $\{a_1, a_2, a_3, a_4\}$

$\{\text{Müller, Meyer, Schmidt}\} =$

$= \{\text{Meyer, Schmidt, Müller}\}$

Zwei Mengen sind \neq gleich, wenn sie dieselben
Elemente enthalten.

AUFZÄHLENDE BESCHREIBUNG (ENUMERATIV)

2.1 DESKRIPTIVES (BESCHREIBENDES) VERFAHREN

Betrachtung verschiedener Eigenschaften,
anhand derer festgestellt werden kann,
ob ein Element zur Menge gehört oder
nicht:

Eigenschaften

P_1, P_2, \dots

$P_1(x)$ x hat die Eigenschaft P_1

$\neg P_1(x)$ x hat nicht die Eigenschaft P_1

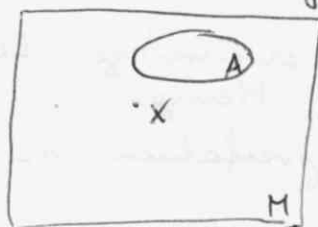
$\neg P_1(x), \sim P_1(x), \bar{P}_1(x)$

$$A = \{x \mid P_1(x), P_2(x), \dots\}$$

↑

mit (auch Doppelpunkt)

"Grafische" Notiz (Diagramme):



Universum

VENN-Diagramme

Probleme: zu viele / zu wenig Elemente
 \Rightarrow mathematisch exakter notwendig

Mathematisches Vorgehen:

Gegeben Universum M

A (interessante Menge)

für jedes $x \in M$ (interessantes Objekt)

angeben, ob es zu A gehört oder nicht [chi]

\Rightarrow Funktion:

$$x_A(x) = 1, \text{ wenn } x \in A$$

$$x_A(x) = 0, \text{ wenn } x \notin A$$

$$\overline{x_A(x)}$$

Definitionsbereich dieser Funktion: M

Wertebereich: $\{0, 1\}$

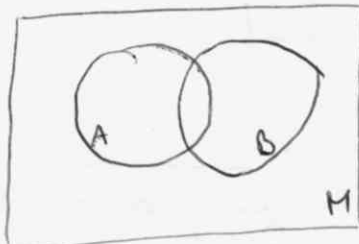
Diese Funktion charakterisiert die Menge A

\Rightarrow CHARAKTERISTISCHE Funktion von A

Spezialfall 1: $\chi_M(x) = 1$ für alle $x \in M$
konstante Funktion M

Betrachtung zweier Mengen A, B in M :

χ_A, χ_B



Spezielles Fall: jedes Element von B ist auch Element von A

f.ä. $x \in B$ gilt auch $x \in A$

ODER: wenn $x \in B$, dann $x \in A$

ODER: $x \in B$ impliziert $x \in A$

ODER: aus $x \in B$ folgt $x \in A$

$$x \in B \Rightarrow x \in A$$

$$x: \quad \chi_B(x) = 1 \Rightarrow \chi_A(x) = 1$$

$$\chi_B(x) = 0 \Rightarrow \chi_A(x) = 0 \text{ oder } \chi_A(x) = 1$$

$$\text{nicht erlaubt: } \chi_B(x) = 1 \Rightarrow \chi_A(x) = 0 \quad !!!$$

$$\text{Situation: } \chi_B(x) \leq \chi_A(x) \text{ f.ä. } x \in M$$

$$\text{kurz } \chi_B \leq \chi_A$$

daher schreibt man: $B \subseteq A$

B ist Teilmenge von A

in Literatur auch $B \subset A$

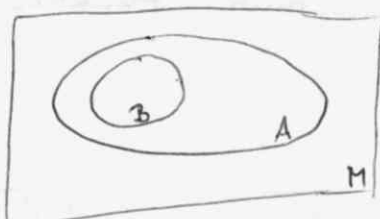
$B \subseteq A$, aber $B \neq A$

\Rightarrow es existiert ein $x \in M$ mit $x \in A$, aber $x \notin B$

$\Rightarrow B$ ist eine echte Teilmenge von A : $B \subset A$

in Literatur auch: $B \subsetneq A$

VENN-Diagramm:



$B \subset A$

Nach diesem Diagramm muss B nicht echte Teilmenge von A sein!

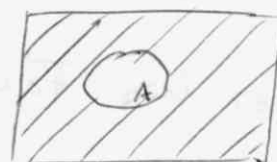
Bemerkung: $A \in M$

Erzeugung neuer Mengen aus zwei Mengen

1.,

A

$$\bar{A} = \{x \mid x \notin A\}$$



$$x_A(x) = 0$$

\Rightarrow

$$x_{\bar{A}}(x) = 1$$

$$x_A(x) = 1$$

\Rightarrow

$$x_{\bar{A}}(x) = 0$$

$$\bar{A} = C(A), C_M(A)$$

\bar{A} ist Komplement von A in M:

$$x_{\bar{A}}(x) = 1 - x_A(x) = x_M(x) - x_A(x)$$

$$x_{\bar{A}} = x_M - x_A$$

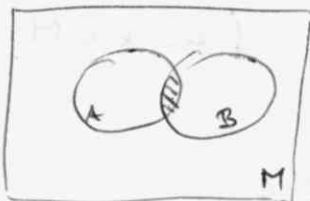
Daher ist klar:

$$\overline{\bar{A}} = A$$

$$x_{\bar{\bar{A}}} = \cancel{1 - x_{\bar{A}}} = 1 - (1 - x_A) = x_A$$

2.,

A, B: Menge in M



„Gemeinsames“ von A und B

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

$$x_C(x) = 1, \text{ wenn } x_A(x) = 1 \text{ und } x_B(x) = 1$$

$x_C(x) = 0$ in allen anderen Fällen,
d.h. wenn mindestens eine
char. Funktion 0 ist.

$$x_C(x) = x_A(x) \cdot x_B(x)$$

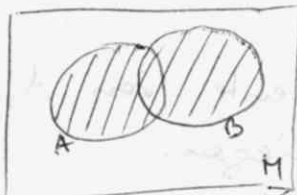
$$x_C = x_A \cdot x_B$$

$$x_C(x) = \min(x_A(x), x_B(x))$$

Operation: $A, B \rightarrow C$

C ist Durchschnitt von A und B : $C = A \cap B$

3., $D = \{x \mid x \in A \text{ oder } x \in B \text{ oder beides}\}$



$$x_D(x) = \max(x_A(x), x_B(x))$$

lat.: vel (einschließendes ODER)

1. oder 2. oder beides

ant (ausschließendes ODER)

1. oder 2., nicht aber beides

$\Rightarrow D = \{x \mid x \in A \vee x \in B\}$ (\vee von vel)

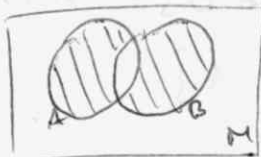
$$C = \{x \mid x \in A \wedge x \in B\}$$

$$D = A \cup B$$

D ist Vereinigung von A und B

für bessere Lesbarkeit auch: \vee statt \vee
& statt \wedge

4.,



$$E = \{x \mid x \in A \text{ oder } x \in B, \text{ aber nicht beides}\}$$

$$E = \{x \mid x \in A \text{ ant } x \in B\}$$

$x_A \backslash x_B$	0	1
0	0	1
1	1	0

$x_A(x) + x_B(x)$ wird durch 2 dividiert \Rightarrow Rest

$$E = A \Delta B$$

Fälle 2-4: zweistellige Operationen

Fall 1: einstellige Operation

$$A \Delta B = B \Delta A$$

⇒ symmetrische Differenz

5. $\bar{A} = C_M(A)$ Menge jener Elemente von M , die nicht in A liegen
 'wie haben A von M wegggenommen'

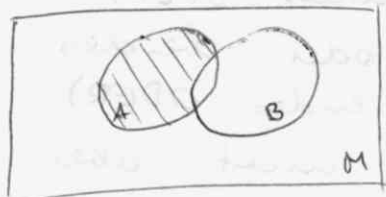
$$\bar{A} = M - A = M \setminus A$$

Differenz von M und A

2 Mengen A, B : $A \setminus B$

Menge aller Elemente von A , die nicht in B liegen

Differenz von A und B



$$x_{A \setminus B}(x) = \max(x_A(x) - x_B(x), 0)$$

$$m - n = \max(m - n, 0)$$

nicht negative ~~Differenz~~ Differenz

meistens: $A \setminus B + B \setminus A$

$$A \setminus B \subseteq A$$

$$B \setminus A \subseteq B$$

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

$$x_{A \setminus A}(x) = 0 \text{ f. a. } x \in M$$

leere Menge \emptyset

6., Universum M : interessante Objekte

interessante Menge $A \subseteq M$

$$M \subseteq M, \emptyset \subseteq M$$

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

Potenzmenge von M

$$M \in \mathcal{P}(M), \emptyset \in \mathcal{P}(M)$$

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

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

$\mathcal{P}(M)$... Menge von Mengen

M ... Menge von Objekten

7., Erzeugung neuer Objekte:

Objekte x, y : Elemente aus Mengen

Elemente der Anschauung

Geordnetes Paar $\langle x, y \rangle$ neues Objekt

1. Element

2. Element

Bemerkungen:

a, ungeordnetes Paar: "Reihenfolge" der Objekte
egal: (x, y)

ACHTUNG: Koordinaten von Punkten in Ebene:

$$P(x|y), P(x,y)$$

hier: geordnete Paare mit runden Klammern!

Frage: "gilt" $(a, b) = \{a, b\}$?

$$(a, b) = (b, a)$$

$(a, b) = \{a, b\}$ gilt nicht immer
oft richtig
oft falsch!

$$a = a \Rightarrow (a, a) \Rightarrow \{a, a\}$$

keine Menge

MULTIMENGE

Multimenge: mehrfaches Auftreten von Objekten erlaubt
Vielfachheit der Objekte als Elemente der
Multimenge A

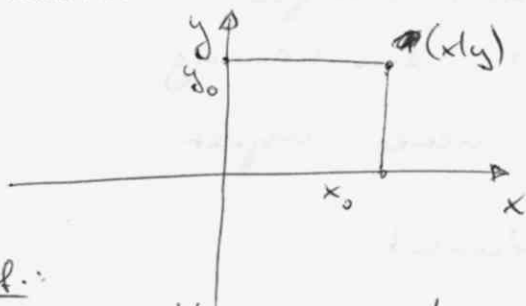
Vielfachheit endlich \Rightarrow Erweiterung der charakteristischen
Funktion

$\chi_A(x)$... Vielfachheit von x als Element der
Multimenge A

\rightarrow Trägermenge: jedes Element nur einfach
vorhanden

Multimenge - System von Mengen

Koordinaten in der Ebene:
kartesisches Koordinatensystem



Def.:

A, B ... Mengen; A im Universum M

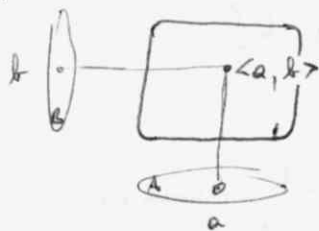
B im Universum N

(A, B im Universum $M \cup N$)

$$\{ \langle a, b \rangle \mid a \in A, b \in B \} = A \times B$$

kartesisches Produkt von A und B

graphische Skizze:



abgerundete Ecken -
Unterscheidung vom Universum

$$A \times \emptyset = ?$$



$$\Rightarrow A \times \emptyset = \emptyset$$

Charakteristische Funktion:

A im Universum M
 B im Universum N
 $A \times B$ im Universum $M \times N$

Definitionsbereiche
 der charakteristische
 Funktionen

$$\chi_{A \times B}(\langle x, y \rangle) = \chi_A(x) \cdot \chi_B(y) = \min(\chi_A(x), \chi_B(y))$$

Definitionsbereich: $M \times N$

Bekannte kartesische Produkte in Mengen

(bzw. Teilmengen von kartesischen Produkten)

($A \times B$ als neues Universum)

Bsp.: Funktion $y = x^2$

$A = \mathbb{R}$ (reelle Zahlen)

$B = \mathbb{R}$

$\mathbb{R} \times \mathbb{R}$: Ebene

kartesische Koordinaten
werden verwendet:

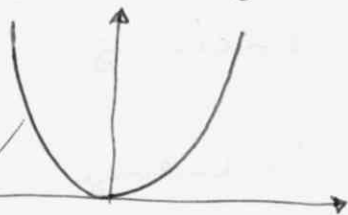


Schaubild der Funktion $\{\langle x, y \rangle \mid y = x^2\} \subseteq \mathbb{R} \times \mathbb{R}$

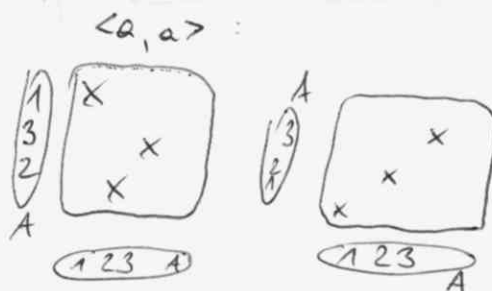
$y = x^2$ (Graph der Funktion)

$$\{\langle x, y \rangle \mid y = x^2\} = \{\langle x, x^2 \rangle \mid x \in \mathbb{R}\}$$

Andere Beispiele:

Spezialfall $A = B$

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



$$\Delta(A) = \{ \langle a, a \rangle \mid a \in A \} \subseteq A \times A$$

Diagonale von $A \times A$

$$\Delta(A) = \{ \langle a, b \rangle \mid (a, b \in A) \wedge (a = b) \}$$

$$\{ \langle a, b \rangle \mid a \in b \}$$

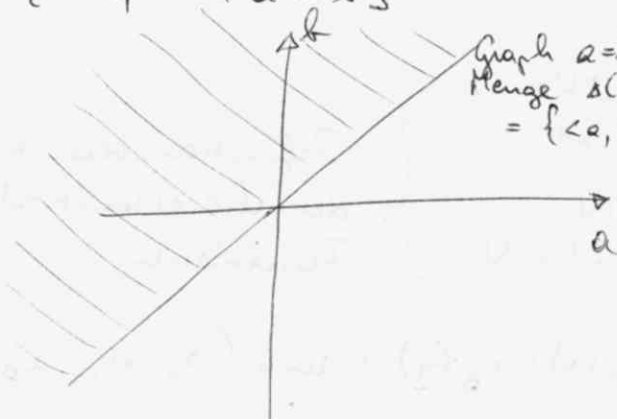
BEZIEHUNG:

$$\boxed{a = b}$$

$$\boxed{a \leq b}$$

Ebene = $\mathbb{R} \times \mathbb{R}$

Graph $a=b$
Menge $\Delta(\mathbb{R}) =$
 $= \{ \langle a, a \rangle \mid a \in \mathbb{R} \}$



Für jede solche Beziehung zwischen Elementen in A existiert die entsprechende Teilmenge in $A \times A$.

$$\{ \langle a, b \rangle \mid a \text{ zu } b \text{ in dieser Beziehung} \}$$

Graph Darstellung dieser Beziehung

auch umgekehrt möglich: Teilmenge $R \subseteq A \times A$

Def. Beziehung ρ : 1 Element aus a und b stehen in Beziehung ρ genau dann, wenn a steht zu b in Bezug $\langle a, b \rangle \in R$

$$\rho \rightarrow R \rightarrow \rho' = \rho$$

Beziehung zwischen Elementen einer Menge A

Bsp.: Gleichheit = ; bei Zahlen : $=$
bei Mengen : \subseteq

allgemein: ρ : $a \rho b$; $a, b \in A$

Beziehung: Begriff RELATION üblich ; ρ [rho]

$a \rho b$ a steht in Relation ρ zu b

$a \not\rho b$ a steht nicht in Relation ρ zu b

$a \in B$ (im Universum M)

$\Rightarrow a \in M$

$B \subseteq \mathcal{P}(M)$

jetzt : $A = M \cup \mathcal{P}(M)$

dann : Relation auf A

$$R = \{ \langle a, b \rangle \mid (a, b \in A) \ a \rho b \} \subseteq A \times A$$

$R(\rho)$

$R \subseteq A \times A$ gegeben

Relation $\rho = \rho(R)$ wird ~~zu~~ definiert:

$a \rho b$ genau dann, wenn $\langle a, b \rangle \in R$

Bemerkung: $R \rightarrow \rho = \rho(R) \rightarrow R = R(\rho)$

$R \longleftrightarrow \rho$

\uparrow
gegeben

daher oft $R \subseteq A \times A$ Relation genannt.

$a \rho b$ gleichbedeutend mit $\langle a, b \rangle \in R$

ρ, R : zweistellige Relation (zwei Elemente von A zueinander in Beziehung)

Wichtige Eigenschaften der Relationen:

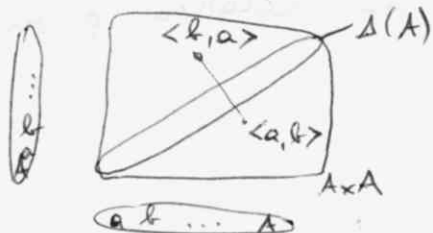
1, $a \rho a, \quad \langle a, a \rangle \in R \quad \text{f. a. } a \in A$

Diese Relation ist REFLEXIV.

(Relation reflexiv $\Leftrightarrow \Delta(A) \in R$)

genau dann, wenn

2, $a \rho b \Rightarrow b \rho a \quad \text{f. a. } a, b \in A$



f. a. a, b aus $a \rho b$

$\langle a, b \rangle \in R$ folgt

$b \rho a \quad \langle b, a \rangle \in R$

$\Rightarrow a \not\rho b \Leftrightarrow a \not\rho b$

$\langle a, b \rangle \notin R \Leftrightarrow \langle b, a \rangle \notin R$

Wäre $\langle b, a \rangle \in R$, dann auch $\langle a, b \rangle \in R$!

$a \rho b \Leftrightarrow b \rho a \quad \text{f. a. } a, b \in A$

Die graphische Darstellung der Menge R ist dann symmetrisch bezüglich $\Delta(A)$.

\Rightarrow Diese Relation ist SYMMETRISCH.

3, $a \rho b, b \rho c \Rightarrow a \rho c \quad \text{f. a. } a, b, c \in A$

Diese Eigenschaft nennt man TRANSITIVITÄT,
die Relation ist TRANSITIV.

Bsp.: Gleichheitsrelation $= : R, S, T$

$a \equiv b \pmod{2} \quad a \text{ kongruent } b \text{ modulo } 2$
 $a, b \in \mathbb{N} \quad (\text{derselbe Rest bei Division durch } 2)$

mögliche Reste: 0, 1

Rest 0 \Rightarrow gerade Zahlen

Rest 1 \Rightarrow ungerade Zahlen

$$a \equiv b \pmod{2} :$$

$$| R, S, T$$

Def.: Eine zweistellige Relation ρ (R) auf der Menge A mit den Eigenschaften R, S, T (eine RST-Relation) heißt ÄQUIVALENZRELATION.

$$a, b \in R, C$$

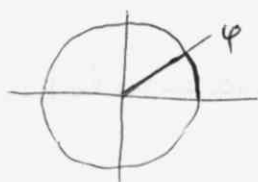
$$m \in R, C$$

Def.: $a \equiv b \pmod{m}$ a kongruent modulo m genau dann, wenn eine ganze Zahl q existiert, sodass $a = b + q \cdot m$

$$\varphi \equiv \psi \pmod{2\pi}$$

$$\varphi - \psi = q \cdot 2\pi \quad \text{mit ganzzahligem } q,$$

d.h. $q \in \mathbb{Z}$



Behauptung: ~~$a \equiv b$~~

$$a \equiv b \pmod{m}$$

$$\text{Rel. } \rho: \equiv \pmod{m}$$

$$A = \mathbb{R} \quad (\text{analog für } A = \mathbb{Z}, A = \mathbb{N}, \dots)$$

$$1, R: a \equiv a \pmod{m}$$

$$a = a + 0 \cdot m \quad \text{f. a. } a \in A$$

$$2, S: a \equiv b \pmod{m} \Leftrightarrow \begin{matrix} 0 \in \mathbb{Z} \\ \text{f. } a = b + q \cdot m \\ q \in \mathbb{Z} \end{matrix}$$

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

$$(-q) \in \mathbb{Z}$$

$$\text{f. a. } a, b \in A$$

$$3, \quad \top \quad a \equiv b \pmod{m}, \quad b \equiv c \pmod{m}$$

$$\text{d.h. } a = b + p \cdot m$$

$$p \in \mathbb{Z}$$

$$a = b + (q+p) \cdot m$$

$$: q+p \in \mathbb{Z}$$

$$\text{d.h. } a \equiv c \pmod{m}$$

$$b = c + q_1 \cdot m$$

$$q_1 \in \mathbb{Z}$$

\Rightarrow RST-Relation - Äquivalenzrelation

$$\equiv \pmod{m}$$

$$a \in A : \{x \mid a \equiv x \pmod{m}\}$$

Restklasse (von) a

Illustration: $R = A \times A$ Eigenschaften: R, S, \top

ρ Äquivalenzrelation; $x \in A$

$$K(x) = \{y \mid x \rho y\} = K_{\rho}(x)$$

Äquivalenzklasse (bzgl. der Äquivalenzrelation ρ)
von x

$$K(x) = \{y \mid y \rho x\}$$

$$K(x) \subseteq A ; K(x) \neq \emptyset$$

Reflexivität: $x \in K(x)$

$$x, y \in A \rightarrow K(x), K(y)$$

$$K(x) \cap K(y) = \emptyset \quad \text{oder} \quad K(x) \cap K(y) = K(x) = K(y)$$

genau dann, wenn $x \not\rho y$ genau dann, wenn $x \rho y$

Bemerkung: Wenn $A \cap B = \emptyset$, so sagt man,
 A und B sind DISJUNKT.

für jedes $x \in A$ existiert eine Äquivalenz-
klasse K mit $x \in K$

d.h. insgesamt:

Ist ρ eine Äquivalenzrelation auf der Menge A , dann liefert die Gesamtheit aller Äquivalenzklassen (Menge) bezüglich ρ eine Zerlegung von A in paarweise disjunkte, nicht leere Teilmengen.

$$A = K(x_1) \cup K(x_2) \cup \dots$$

Und umgekehrt: Jede Zerlegung von A in paarweise disjunkte, nicht leere Teilmengen definiert eindeutig eine Äquivalenzrelation, deren Zerlegung von A in Äquivalenzklassen die gegebene Zerlegung liefert.

$\rho: x \rho y$ genau dann, wenn x, y in derselben Teilmenge liegen.

Bsp.: 1, $\rho = "=" \Rightarrow K(x) = \{x\}$

2, ρ Allrelation $\Rightarrow K(x) = A$

3, modul ~~zu~~ m ; $A = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{N}, \mathbb{Z}$

$$\Rightarrow K(x) = \{y \mid y \equiv x \pmod{m}\}$$

$m \in \mathbb{N}, A \in \mathbb{Z} \Rightarrow$ es gibt m solche Äquivalenzklassen

$$K(0), K(1), K(2), \dots, K(m-1)$$

$$K(m) = K(0)$$

Es gilt sogar: $a, b, c, d \in \mathbb{R}, \dots, \mathbb{Z}$
Modul m

$$a \equiv c \pmod{m}$$

$$\text{und } b \equiv d \pmod{m}$$

Dann gilt:

$$a \cdot b \equiv c \cdot d \pmod{m}$$

$$a + b \equiv c + d \pmod{m}$$

$$a - b \equiv c - d \pmod{m}$$

Beispiel:

$$m=4; a=2; b=2; c=6; d=2$$

$$a \equiv c \pmod{4} \Rightarrow 2 \equiv 6 \pmod{4}$$

$$b \equiv d \pmod{4} \Rightarrow 2 \equiv 2 \pmod{4}$$

$$\frac{a}{b} = \frac{2}{2} = 1 \quad \frac{c}{d} = \frac{6}{2} = 3$$

$$\Rightarrow 1 \not\equiv 3 \pmod{4} \quad !!!$$

$$\frac{a}{b} \not\equiv \frac{c}{d} \pmod{m} \quad !!!$$

Modul m :

$$x \cdot y$$

$$x \in K(a), y \in K(b)$$

$$x \cdot y \in K(a \cdot b)$$

$$x + y \in K(a + b)$$

$K(x)$ bzgl. der Relation $\equiv \pmod{m}$

$$K \equiv \pmod{m} (x) = \{y \mid y \equiv x \pmod{m}\}$$

$$\bar{x} = [x] = [x]_m = [x]_{(m)} = \{y \mid y \equiv x \pmod{m}\}$$

Wenn Modul klar

$$x \in [a], y \in [b] \Rightarrow x + y \in [a + b]$$

$$\text{Def.: } \begin{aligned} [a] \cdot [b] &= [a \cdot b] \\ [a] + [b] &= [a + b] \\ ([a] - [b] &= [a - b]) \end{aligned}$$

Restklasse $[a]_m = \{x \mid x \in \mathbb{Z}, x \equiv a \pmod{m}\}$

|
A

Menge der Restklassen:

$$\{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\} = \\ = \{[1]_m, [2]_m, [3]_m, \dots, [m]_m\}$$

Addition, Multiplikation (Subtraktion)

Assoziativgesetz, Kommutativgesetz, Distributivgesetz

kein KÜRZEN!

$$[a]_m \oplus_m [b]_m = [a+b]_m$$

$$[a]_m \odot_m [b]_m = [a \cdot b]_m$$

häufig in Informatik: $m=2$

auch schon verwendet bei $A \triangle B$

$m=p$ (Primzahl): besondere Situation

$m=p \cdot q$ (Produkt zweier Primzahlen):

Verwendung in der Kryptographie (RSA-System)

$$m=1 \Rightarrow a \equiv b \pmod{1} \quad A = \mathbb{Z}$$

es existiert $q_1 \in \mathbb{Z}$, sodass $a = b + q_1 \cdot 1$

\rightarrow Wähle $q_1 = a - b$

$m=1$ liefert die Äquivalenzrelation auf \mathbb{Z}

$$(A = \mathbb{R} \Rightarrow a \equiv b \pmod{1})$$

„der Teil hinter dem Komma stimmt überein“)

$$m=0 \quad a \equiv b \pmod{m}$$

es existiert $q_1 \in \mathbb{Z}$, sodass $a = b + \underbrace{q_1 \cdot 0}_{=0}$

$$\Rightarrow a = b$$

$m=0$ liefert die Gleichheitsrelation

Relation: Äquivalenzrelation R, S, T

Menge A ; Verallgemeinerung der Gleichheitsrelation
 \leq auf $\mathbb{R}, \mathbb{Z}, \mathbb{N}, \dots$

1, $R: a \leq a$ f. a. $a \in \mathbb{R}$

2, siehe unten

3, $T: a \leq b, b \leq c \Rightarrow a \leq c$ f. a. $a, b, c \in \mathbb{R}$

ad 2, Symmetrie: $a \leq b \stackrel{?}{\Rightarrow} b \leq a$

$2 < 3 \not\Rightarrow 3 < 2$
falsch

$a \leq b, b \leq a \Rightarrow a = b$ f. a. $a, b \in \mathbb{R}$

Identität (Id): $a = b$

Universum M

$\mathcal{P}(M)$ Potenzmenge von M

$A, B \in \mathcal{P}(M)$ (also $A, B \subseteq M$)

$A \subseteq B$ Teilmengenrelation

1, $R: A \subseteq A$ f. a. $A \in \mathcal{P}(M)$

2, Id: $A \subseteq B, B \subseteq A \Rightarrow A = B$ f. a. $A, B \in \mathcal{P}(M)$

3, $T: A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$ f. a. $A, B, C \in \mathcal{P}(M)$

Def.: Eine ^{zweistellige} Relation R (ρ) auf der Menge A heißt Halbordnung (HO), wenn sie die Eigenschaften R, Id, T hat (f. a. $a, b, c \in A$)

gilt: 1, $a \rho a \Rightarrow R$

2, $a \rho b, b \rho a \Rightarrow a = b \Rightarrow Id$

3, $a \rho b, b \rho c \Rightarrow a \rho c \Rightarrow T$

$\langle A, \rho \rangle \dots$ HALBORDNUNG

$\neq \emptyset$ Halbordnungrelation

Weitere Halbordnungen: $\langle \mathbb{R}, \geq \rangle$; $\langle \mathbb{Z}, \geq \rangle$, ...

$$\langle \{2^n \mid n \in \mathbb{N}\}, \leq \rangle$$

$$\{1, 2, 4, 8, 16, \dots\}$$

$$\langle \mathcal{P}(M), \supseteq \rangle$$

Obermengenrelation

A ist Obermenge von $B \Leftrightarrow$

B ist Teilmenge (Untermenge) von A

$$A \supseteq B \Leftrightarrow B \subseteq A$$

Bei der Halbordnung $\langle \mathbb{R}, \leq \rangle$ gilt sogar:

Für je zwei Elemente $a, b \in \mathbb{R}$ gilt entweder $a \leq b$ oder $b \leq a$ (oder beides).
(voll)

D.h. je zwei reelle Zahlen bezüglich \leq vergleichbar.

M hat mindestens 2 Elemente

$$A, B \subseteq M$$

Hier kann sein: $A \not\subseteq B$, $B \not\subseteq A$

$x \neq y$ sind Elemente von M

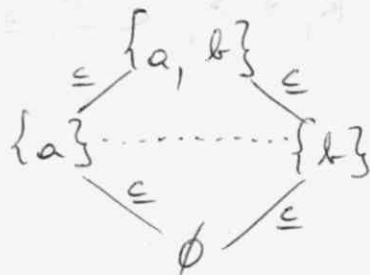
$\{x\}, \{y\}$ nicht vergleichbar bezüglich \subseteq

reelle Zahlen: Zahlengerade bekannt

 Zahlengerade

Mengen: $M = \{a, b\}$ (d.h. immer $a \neq b$)

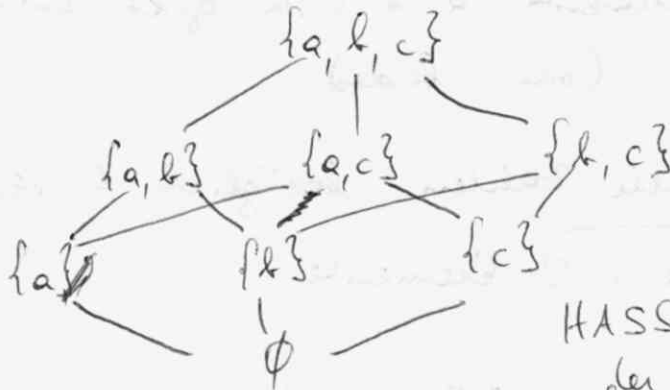
$$\mathcal{P}(M) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$



zwischen $\{a\}$ und $\{b\}$ keine Vergleichsmöglichkeit!
 Ist die Vergleichbarkeit gegeben, spricht man
 von einer LINEAREN (TOTALEN) ORDNUNG

Mengen: für Mengen mit mind. 2 Elemente
keine lineare Ordnung

$$M = \{a, b, c\}$$

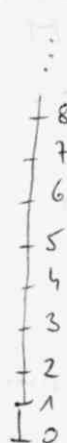


HASSE-Diagramm
 der Halbordnung

1-10:



N:



\mathbb{N}

3
1
:
6
4
2
0

1-10:

9
7
5
3
1
10
8
6
4
2



direkter Nachfolger
← ← ←

direkter Vorgänger (außer 0)

Axiomensystem für die natürlichen Zahlen
(durch PEANO):

\mathbb{N} : Menge von Objekten mit folgenden Eigenschaften:

1, $0 \in \mathbb{N}$

2, jedes Element $a \in \mathbb{N}$ hat ^{genau} einen Nachfolger a'

3, jedes Element $b \neq 0 \in \mathbb{N}$ ist ^{höchstens} Nachfolger eines Elementes $a \in \mathbb{N}$

d.h. es existiert $a \in \mathbb{N} \Rightarrow b = a'$

4, 0 ist nicht Nachfolger eines Elementes $a \in \mathbb{N}$

5, $S \subseteq \mathbb{N}$ und gilt

a, $0 \in S$

b, für jedes $a \in \mathbb{N}$ gilt:

Ist $a \in S$, so ist auch $a' \in S$

Dann folgt: $S = \mathbb{N}$

Bsp.: Damit definieren wir für $a, b \in \mathbb{N}$ die Summe $a+b$, und zwar durch: f. a. $a \in \mathbb{N}$ gilt:

$$a+0=a$$

f. a. $a, b \in \mathbb{N}$ gilt: $a+b' = (a+b)'$

Sei S_a die Menge $b \in \mathbb{N}$, sodass $a+b$ definiert ist.

1, $0 \in S_a$ ($a+0=a$)

2, für jedes $b \in \mathbb{N}$ gilt:

aus $b \in S_a$ (d.h. $a+b$ definiert) folgt $b' \in S_a$ (d.h. $a+b'$ definiert), da $a+b' = (a+b)'$

also $S_a = \mathbb{N}$

Berechnen wir $0'$ mit 1: $0' = 1$

$$a+0' = a+1 = a' = \underbrace{(a+0)'}_a$$

$$a' = a+1$$

$$a+b' = a+(b+1) = (a+b)' = (a+b)+1$$

Definition: Multiplikation: $a \cdot b$

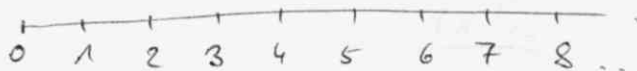
1, $a \cdot 0 = 0$

2, $a \cdot b' = a \cdot b + a$

\Rightarrow REKURSIVE DEFINITION

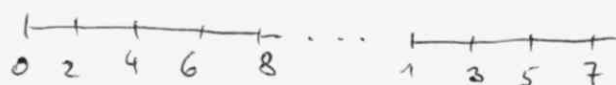
$$\mathbb{N} = \{0, 1, 2, \dots\}$$

Zahlengerade



linear geordnet

Auch andere Anordnungen natürlicher Zahlen:



nicht die lineare
Ordnung nach Peano

Beweisverfahren:

Beweisverfahren: VOLLSTÄNDIGE INDUKTION:

Sei $A(n)$ eine Aussage, die von der natürlichen Zahl n abhängt.

Und gilt:

1, $A(0)$ ist wahr.

2, für alle $n \in \mathbb{N}$ folgt aus der Annahme $A(n)$ ist wahr, die Behauptung $A(n+1)$ ist wahr.

Dann ist $A(n)$ wahr f.a. $n \in \mathbb{N}$.

$S = \{n \mid A(n) \text{ ist wahr}\}$

1, $0 \in S$

2, f.a. $n \in \mathbb{N}$ folgt aus $n \in S$, dass $n+1 \in S$

5. Axiom von Peano: $S = \mathbb{N}$

Bemerkungen: 1, $A(0)$ ist wahr: Induktionsstart

2, Induktionsschritt: für jedes $n \in \mathbb{N}$ folgt aus der Induktionsannahme ($A(n)$ ist wahr) die Induktionsbehauptung ($A(n+1)$ ist wahr)

I. A (Induktionsannahme) = I. V. (Induktionsvoraussetzung)

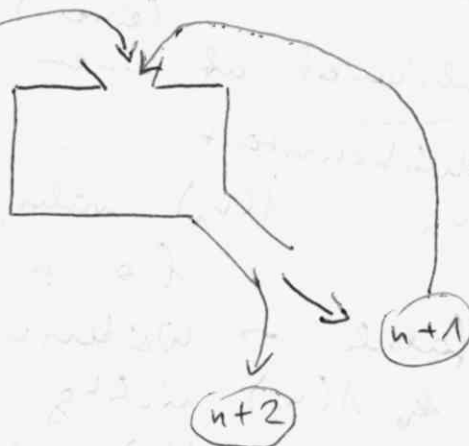
I. B.: Induktionsbehauptung

$A(n)$ ist wahr
 $n \in \mathbb{N}$

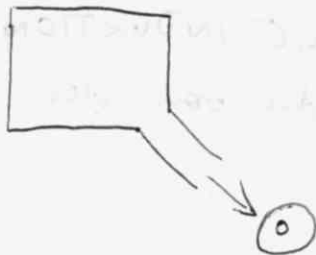
Setzen

(n)

2, Automat für Induktionsschritt



1, Automat für Induktionstaut:



VARIANTE:

- 1, Induktionstaut: $A(n_0)$ wahr
- 2, Induktionsschritt: f. a. $n \geq n_0$ ($n, n_0 \in \mathbb{N}$)
folgt aus 1A $A(n)$ wahr
die 1B $A(n+1)$ wahr

Dann gilt: $A(n)$ wahr f. a. $n \geq n_0$

$$B(k) = A(n_0 + k)$$

Aufgabe: Für welche $n \in \mathbb{N}$ ist $A(n)$ wahr?

Vorgehensweise:

Vermutung: es existieren endlich viele n mit
 $A(n)$ falsch

d.h. es existiert ein n_0 , sodass f. a. $n \geq n_0$
 $A(n)$ wahr ist

Dann: Ich konstruiere den Induktionsschrittautomat,
(einen!)
funktioniert ab einem n_1

Suche Induktionstaut

Versuch: n_1 $A(n_1)$ wahr, dann $A(n)$ wahr
f. a. $n \geq n_1$

$A(n_1)$ ist falsch \rightarrow Weiterprobe: $A(n_1+1), A(n_1+2), \dots$
bis $A(n_2)$ richtig

\Rightarrow f. a. $n \geq n_2$: $A(n)$ wahr

Wie hatten in 2. Teil der Induktion (im Induktionsschritt) die IV, da $A(n)$ ist wahr.

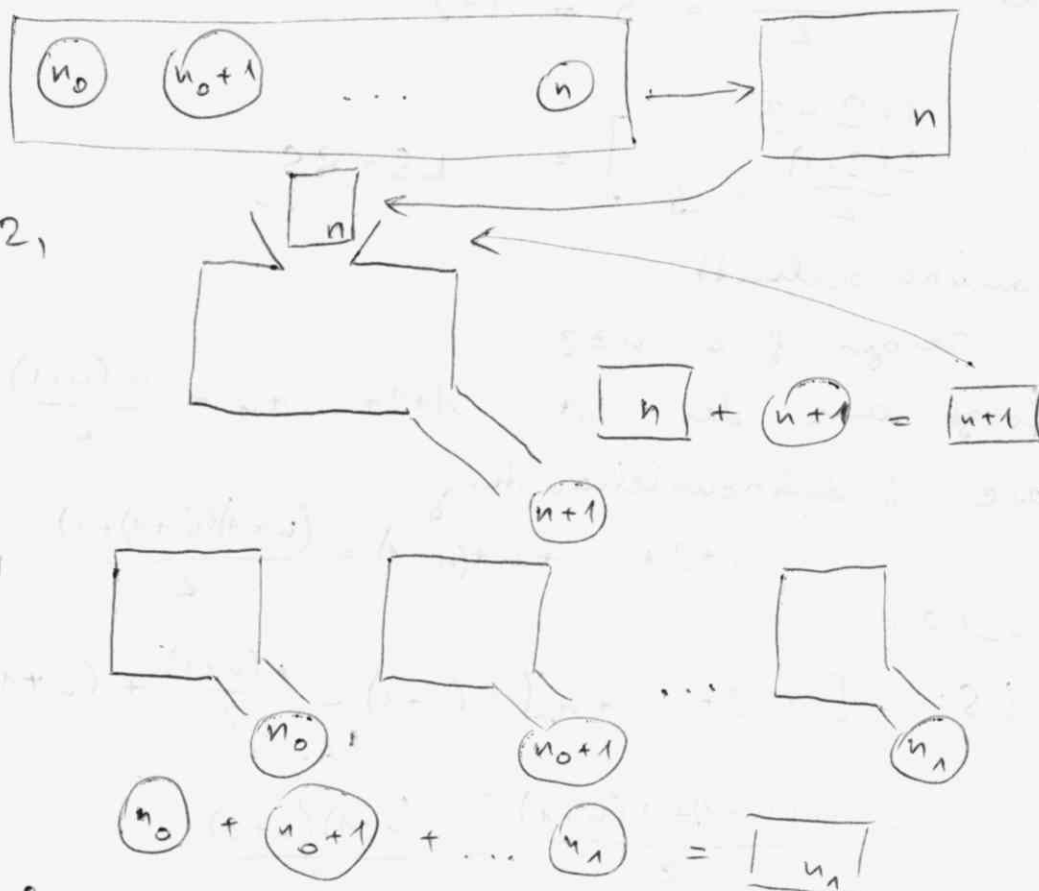
Variante: Aussage $A(n)$

und gilt

1, Induktionsstart $A(n_0), \dots, A(n_1)$

2, Induktionsschritt: für jedes $n \geq n_1$ folgt aus der SA: $A(k)$ ist wahr f.a. $k \geq n_0$ $k \leq n$

die Induktionsbehauptung $A(n+1)$ wahr, dann ist $A(n)$ wahr f.a. $n \geq n_0$



Bsp. für die vollständige Induktion:

Summe der natürlichen Zahlen von 1 bis n

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

~~es~~ gilt f.a. natürlichen Zahlen ≥ 2

Beweis mittels vollständiger Induktion:

1, Induktionsstart: $n=2$

$$1+2 = \frac{2 \cdot (2+1)}{2} = 3 \quad \checkmark$$

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

$$3 = 3$$

so kein Beweis! $\uparrow\uparrow$

analog: $-1=1$

daraus folgt: $1=1$?!

genauer: $\frac{2(2+1)}{2} = 3 = 1+2$

LS: $1+2=3$

RS: $\frac{2(2+1)}{2} = 3$] = LS = RS \checkmark

2, Induktionsschritt:

Zu zeigen f. a $n \geq 2$

folgt aus der SA $1+2+\dots+n = \frac{n(n+1)}{2}$

die Induktionsbehauptung

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

BEWEIS:

LS: $[1+2+\dots+n] + (n+1) = \frac{n(n+1)}{2} + (n+1) =$
I.A.
 $= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$

RS: $\frac{(n+1)(n+2)}{2}$

LS = RS

Rekursion: FIBONACCI-Zahl

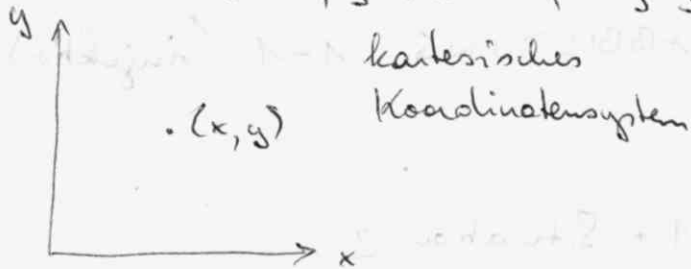
$$F_0 = 0; F_1 = 1$$

Def.: $F_n = F_{n-1} + F_{n-2}$ f. a. $n \geq 2$

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

Relation ρ ; $R \subseteq A \times A$

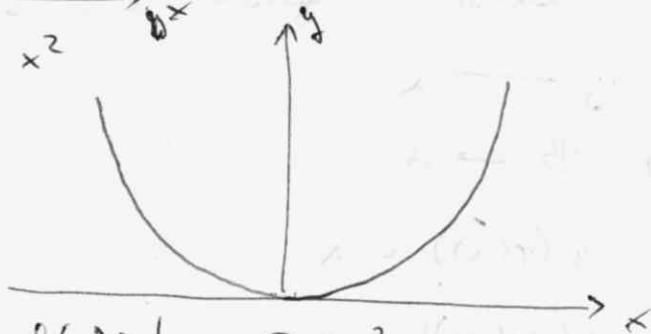
$$\{ \langle x, y \rangle \mid x \in A; x \rho y \}$$



Bsp.: $y = f(x)$ $A = \mathbb{R}$

• $A(x \mid f(x))$

$y = f(x) = x^2$



$$\{ \langle x, f(x) \rangle \mid x \in \text{Def}_f \}$$

$\text{Def}_f \dots$ Definitionsbereich von f



~~genau~~ jedem $x \in A$ genau ein $y \in B$ zuordnen

Zuordnung φ
 $y = \varphi(x)$

Man nennt eine solche Zuordnung Abbildung von A in B : $\varphi: A \rightarrow B$

Situation 1: jedes $y \in B$ tritt als Bild auf
d.h. zu jedem $y \in B$ existiert mindestens
ein $x \in A$ mit $y = \varphi(x)$

ABBILDUNG VON A AUF B (surjektiv)

$$\varphi: A \rightarrow B$$

Situation 2: zu jedem $y \in B$ existiert höchstens
ein $x \in A$ mit $y = \varphi(x)$

EINEINDEUTIGE ABBILDUNG 1-1 (injektiv)

$$\varphi: A \xrightarrow{1-1} B$$

Situation 3: Situation 1 + Situation 2

$$\varphi: A \xrightarrow{1-1} B$$

surjektiv + injektiv

bijektiv

zu jedem $y \in B$ existiert genau ein $x \in A$ mit
 $y = \varphi(x)$

$$y \text{ --- } x$$

$$\varphi: B \rightarrow A$$

$$\text{f. a. } x \in A: \quad \varphi(\varphi(x)) = x$$

$$\text{f. a. } y \in B: \quad \varphi(\varphi(y)) = y$$

UMKEHRABBILDUNG von $\varphi: \varphi^{-1} \neq \frac{1}{\varphi} \quad !$

endlich viele Elemente in A : m Elemente
 endlich viele Elemente in B : n Elemente

$$\varphi: A \xrightarrow{1-1} B \text{ (bijektiv)} \Rightarrow \underline{m=n}$$

A und B heißen gleichmächtig (äquipotent)
 und die Anzahl der Elemente heißt

Mächtigkeit: $|A|$

(Kardinalität): $\text{card}(A)$

zwei unendliche ~~to~~ Mengen A, B heißen
 gleichmächtig (äquipotent), wenn eine Bijektion

$$\varphi: A \xrightarrow{1-1} B \text{ existiert: } A \sim B \text{ bzw. } |A| = |B|$$

„sofort“ klar:

$$1, \quad A \sim A \text{ f. a. Mengen } A$$

$$2, \quad A \sim B \Rightarrow B \sim A \text{ f. a. Mengen } A, B$$

$$3, \quad A \sim B, B \sim C \Rightarrow A \sim C \text{ f. a. Mengen } A, B, C$$

$$\text{Achtung: } \mathbb{N} \sim \mathbb{Z}, \text{ obwohl } \mathbb{N} \subset \mathbb{Z}$$

$$\mathbb{N} \sim \mathbb{Q}, \text{ obwohl } \mathbb{N} \subset \mathbb{Q}$$

$$\mathbb{N} \not\sim \mathbb{R}$$

$$\text{aleph } 0: |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$$

$$\aleph_0, \aleph_1$$

$$\varphi: A \rightarrow B$$

$$\psi: B \rightarrow C$$

$$y = \varphi(x)$$

$$z = \psi(y) = \psi(\varphi(x)) = \chi(x)$$

innere Abbildung
 äußere Abbildung

$$\chi: A \rightarrow C$$

$\chi = \psi \circ \varphi(x)$ eine Notation

$$\begin{array}{c} \varphi \circ \varphi \\ x \rightarrow y \rightarrow z \\ \hline x \end{array}$$

andere Notation

$$\begin{array}{ccccccc} A & \xrightarrow{\varphi} & B & \xrightarrow{\varphi} & C & \xrightarrow{x} & D \\ x & & y & & z & & t \end{array}$$

$$\varphi(\varphi(x))$$

$$t = x[\varphi(\varphi(x))]$$

$$t = x(\varphi(y)) = x(\varphi[\varphi(x)])$$

$$(\varphi \circ \varphi) \circ x \quad x \rightarrow t$$

$$\varphi \circ (\varphi \circ x) \quad x \rightarrow t$$

D.h. für Abbildungen mit der Zusammensetzung „Hintereinanderausführen“ gilt das Assoziativgesetz (analog zu natürlichen/reellen Zahlen bezüglich Addition/Multiplikation; analog zu Mengen ($\in \mathcal{P}(M)$) bezüglich \cap, \cup, Δ)

Spezielle Situation: Abbildungen von A in A

Operation: Zusammensetzung
Hintereinanderausführen

jeweils Menge $G \neq \emptyset$

zweistellige Operation $*$

G : $\mathbb{N}, \mathbb{R}, \mathcal{P}(M)$, Menge der Abbildungen von A in A

Operationen: $+, \cdot, \cap, \cup, \Delta, \setminus$

weitere mögliche Operationen: $-, a^x$

$$A^B = \{\varphi \mid \varphi: B \rightarrow A\}$$

Algebraische Strukturen $\langle G; * \rangle$

$G \neq \emptyset$; $*$... zweistellige Operation auf G
 d.h. $a, b \in G$ (binäre Operation)
 $\rightarrow a * b$ definiert

Wichtige Eigenschaften:

G1: Abgeschlossenheit:

f. a. $a, b \in G$ gilt $a * b \in G$

G2: Assoziativität:

 $(a * b) * c = a * (b * c)$ f. a. $a, b, c \in G$ G3: Einheits-element e :Es existiert in G ein Element e mit
 $e * a = a * e = a$ f. a. $a \in G$ G4: inverses Element (Voraussetzung: G3 - es existiert ein Einheits-element e):Zu jedem $a \in G$ existiert (mindestens) ein $a' \in G$, sodass $a * a' = a' * a = e$

G5: Kommutativgesetz:

 $a * b = b * a$ f. a. $a, b \in G$ Bsp.: $\langle \mathbb{N}, + \rangle$ G1, G2, G3 ($e=0$), G5 $\langle \mathbb{R}, + \rangle$ G1, G2, G3 ($e=0$), G4 ($a'=-a$), G5 $\langle \mathcal{P}(M), \cap \rangle$ G1, G2, G3 ($e=M$), G5 $\langle \mathcal{P}(M), \setminus \rangle$ G1, $\langle G, * \rangle$:

G1

GRUPPOID

G1, G2

HALBGRUPPE

G1, G2, G3

HALBGRUPPE MIT EINHEITSELEMENT (MONOID)

G1, G2, G3, G4

GRUPPE

G5 unabhängig: kommutative Struktur
abelsche Struktur

Bemerkungen: 1, G3 $e \dots$ neutrales Element
 $a * e = e * a = a \quad \text{f.ä. } a \in G$

2, In allen gebrachten Beispielen gibt es, wenn G3 erfüllt war, genau ein Einheitselement.

Behauptung: In einem Gruppoïd $\langle G, * \rangle$ gibt es höchstens ein Einheitselement.

Beweis: $\langle G, * \rangle \quad e$: Einheitselement, d.h.

$$e * a = a * e = a \quad \text{f.ä. } a \in G$$

Beweis indirekt: Angenommen, es existieren zwei verschiedene Einheitselemente e_1, e_2 :

$$e_1 \neq e_2$$

Dann: $e_1 * e_2 = e_2$ (e_1 ist Einheitselement)

$$e_1 * e_2 = e_1 \quad (e_2 \text{ ist Einheitselement})$$

$$\Rightarrow e_1 = e_2 \quad \text{Widerspruch zu } e_1 \neq e_2!$$

\Rightarrow Es existiert nun ein Einheitselement!

Restklassen in $\mathbb{Z} \bmod m$ ($m \neq 0$)

mit \oplus_m

bzw. mit \odot_m

$$\langle \mathbb{Z}_m, \oplus_m \rangle; \quad \langle \mathbb{Z}_m, \odot_m \rangle, \quad \langle \mathbb{Z}_m \setminus \{0\}, \odot_m \rangle$$

Menge der Restklassen

in $\mathbb{Z} \bmod m$

Behauptung: Halbgruppe mit Einheitselement e
 $\langle G; * \rangle$ und existiert zu $a \in G$ ein $a' \in G$
 mit $a * a' = a' * a = e$, or existiert kein
 weiteres a'

D.h. a', a'' zu Element a , or folgt $a' = a''$

Beweis:
$$\left. \begin{aligned} (a' * a) * a'' &= e * a'' = a'' \\ a' * (a * a'') &= a' * e = a' \end{aligned} \right\} =$$

 $\Rightarrow a' = a''$; wäre ein Widerspruch zu $a' \neq a''$

$\langle \mathbb{Z}, + \rangle$ $G1, G2, G3 (e=0), G4 (a'=a), G5$
 \Rightarrow abelsche Gruppe

analog: $\langle \mathbb{R}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{C}, + \rangle$

komplexe Zahl: $z = a + i \cdot b$

$i \dots$ imaginäre Einheit: $\boxed{i^2 = -1}$
 $a, b \in \mathbb{R}$

$$z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$$

$$z_1, z_2 \in \mathbb{C}; \quad \begin{aligned} z_1 &= a_1 + i b_1 \\ z_2 &= a_2 + i b_2 \end{aligned}$$

$\langle \mathbb{N}, + \rangle$: Monoid ($e=0$)

$\langle \mathbb{Z}, \cdot \rangle$: Monoid ($e=1$)

$\langle \mathbb{N}, \cdot \rangle$: Monoid ($e=1$)

$\langle \mathbb{Q}, \cdot \rangle$: Monoid ($e=1$)

keine Gruppe, da kein inverses Element für 0 !

$$0 \cdot 0' = 0' \cdot 0 = 1 \quad 0' \text{ existiert nicht!!!}$$

$$\mathbb{Q}_0 = \mathbb{Q} \setminus \{0\} = \{x \in \mathbb{Q} \mid x \neq 0\}$$

$\langle \mathbb{Q}_0, \cdot \rangle$: abelsche Gruppe ($e=1; a'=\frac{1}{a}$)

$\langle \mathbb{R}_0, \cdot \rangle, \langle \mathbb{C}_0, \cdot \rangle$

$$\boxed{0 + i \cdot 0} \quad e = 1 + i \cdot 0$$

$$M: \langle \mathcal{P}(M), \cup \rangle$$

$$\langle \mathcal{P}(M), \cap \rangle$$

$$\langle \mathcal{P}(M), \Delta \rangle$$

$$\langle \mathcal{P}(M), \setminus \rangle$$

$A \neq \emptyset$ Abbildungen von A in A : A^A

$$\langle \text{Abb}: A \rightarrow A, \circ \rangle$$

$$x = \varphi \circ \varphi \quad \text{hintereinanderausf\u00fchren}$$

$$\Rightarrow x(x) = \varphi(\varphi(x))$$

$$\begin{array}{ccc} A & \rightarrow & A \\ \varphi & & \varphi \end{array}$$

G1 ✓

assoziativ

G2 ✓

identische Abbildung: $\iota(x) = x$

$$\iota \circ \varphi = \varphi \circ \iota = \varphi$$

Einheitsselement: $e = \iota$ G3 ✓

$\langle \text{Bijektionen von } A \text{ auf } A, \circ \rangle$

$$\varphi: A \xrightarrow[1-1]{\rightarrow} A$$

Zu jedem $y \in A$ existiert genau ein $x \in A$ mit $\varphi(x) = y$

$\varphi \circ \varphi$ Bijektion $\Rightarrow \varphi \circ \varphi$ Bijektion

$$z = \varphi(\varphi(x)); z \in A$$

Es existiert genau ein y mit $z = \varphi(y)$

Einheitselement: $e = \text{id}$

inverses Element: φ

Zu jedem y existiert genau ein x mit $y = \varphi(x)$

$x = \varphi^{-1}(y)$ Umkehrabbildung: φ^{-1}

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \text{id}$$

$$\varphi^{-1}(x) \in A$$

f.a. $x \in A$

$$\varphi^{-1}(x) \neq \frac{1}{\varphi(x)}$$

↑
in A

Bewegungen in der Ebene

Bsp.: A : Ebene - Menge der Punkte

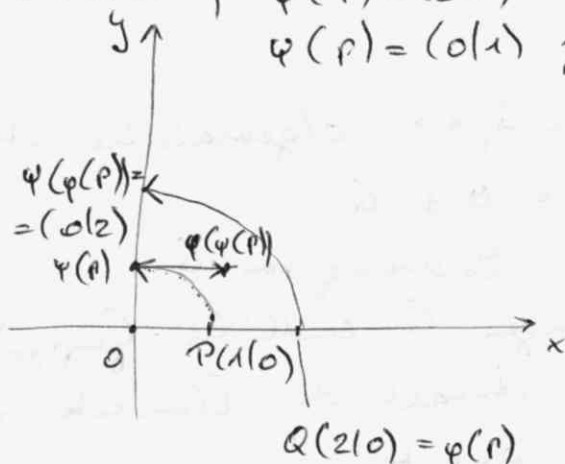
φ ... Verschiebung (Translation) um 1 in Richtung der x -Achse

$$\varphi(p|q) \rightarrow \varphi(p+1|q)$$

ψ ... Drehung um $O(0|0)$ um $+90^\circ$

$$\varphi(1|0) ; \quad \varphi(p) = (2|0) ; \quad \psi(\varphi(p)) = (0|2)$$

$$\varphi(p) = (0|1) ; \quad \psi(\varphi(p)) = (1|1)$$



$$\rightarrow \varphi \circ \psi \neq \psi \circ \varphi$$

< Bewegungen in der Ebene, O > ;
nicht abelsche Gruppe

Frage: Welche Operationen existieren in einer Gruppe $\langle G, * \rangle$

definierende zweistellige Operation $*$: $a * b$

weilers für jedes $a \in G$ gibt es $a' \in G$ als inverses Element definiert; Übergang von a auf a' : einstellige Operation

Außerdem Auszeichnung eines Elementes (Einheits-
element $e \in G$): nullstellige Operation
(kein Argument)

Gruppe: $\langle G, *, e, ' \rangle$
 / | |
 + \neq 2-stellig nullstellig einstellig

durch die 2-stellige Operation $*$ eindeutig e
in der Gruppe definiert (das einzige Element
 $x \in G$ mit $x * x = x$); Beweis trivial

Analog: $'$ eindeutig definiert

a' ist genau das Element aus G (gegeben a)
mit $a' * a = a * a' = e$

Bemerkung: Definition: $\langle G, * \rangle$ algebraische Struktur

$$|G| (= \text{card}(G)) = \text{Ord } G$$

Kardinalität von G

Ordnung von G

Speziell bei endlichen Mengen G (endliche Gruppe)

interessant: Dann $|G|$: Anzahl der Elemente in G

Operation $*$ in Tabelle angeben

a	b
a	$a * b$

Operationstafel
in $\langle G, * \rangle$;
Gruppentafel

Bsp.:

 \mathbb{Z}_3

Restklassen mod 3

$$\mathbb{Z}_3 = \{[0]_3; [1]_3; [2]_3\} = \{\bar{0}, \bar{1}, \bar{2}\}$$

 \oplus_3

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$$\bar{a} \oplus_3 \bar{b} = \overline{a+b}$$

$$[3]_3 = [0]_3$$

$$\bar{3} = \bar{0}$$

Operationstafel

$$G = \{A, B, C\}$$

Gesucht: Operation $*$,so dass $\langle G, * \rangle$ Gruppe

	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

statt $\bar{0}$: Astatt $\bar{1}$: Bstatt $\bar{2}$: C

Definition:

$$\langle G, * \rangle$$

$$\langle H, \circ \rangle$$

$$\varphi: G \xrightarrow{1-1} H \text{ Bijektion}$$

$$\varphi(a) \circ \varphi(b) = \varphi(a * b) \quad a, b \in G$$

$$= \varphi(a * b)$$

Dann heißt φ Isomorphismus.

Bijektion φ von G auf H , die „mit den Operationen verträglich (vertauschbar)“ ist, heißt Isomorphismus von G auf H .

G und H heißen isomorph: $G \cong H$

φ : Gruppenisomorphismus von G auf H

$$\langle G, * \rangle$$

$$U \subseteq G$$

$$\langle U, * \rangle$$

$$U \neq \emptyset$$

$$\langle G, *, e, ' \rangle$$

$$\langle U, *, e, ' \rangle$$

Wenn auch Gruppe, dann sagt man,

$\langle U, * \rangle$ ist Untergruppe von $\langle G, * \rangle$

Satz: $\langle U, * \rangle$ mit $U \neq \emptyset$ ist Untergruppe von $\langle G, * \rangle$ genau dann, wenn für alle $a, b \in U$ (b' sei das inverse Element in G) auch $a * b' \in U$.

Bemerkung: Ist G endlich, so genügt für $\langle U, * \rangle$ Untergruppe von $\langle G, * \rangle$ das $U \neq \emptyset$ und für alle $a, b \in U$ $a * b \in U$, d.h. U ist Untergruppoid von G .

$\langle U_1, * \rangle, \langle U_2, * \rangle$ Untergruppen von $\langle G, * \rangle$

dann auch $\langle U_1 \cap U_2, * \rangle$ Untergruppe von $\langle G, * \rangle$

Cartesisches Produkt:

$$\langle G_1, *_1 \rangle$$

$$\langle G_2, *_2 \rangle$$

$$G = G_1 \times G_2 = \{ \langle x_1, x_2 \rangle \mid x_i \in G_i \}$$

Def.: $\langle x_1, x_2 \rangle * \langle y_1, y_2 \rangle$

$$\langle \underbrace{x_1 *_1 y_1}_{\in G_1}, \underbrace{x_2 *_2 y_2}_{\in G_2} \rangle \in G_1 \times G_2$$

\Rightarrow algebraische Struktur $\langle G, * \rangle$

Einheitselement: $\langle e_1, e_2 \rangle$

inverses Element $\langle a_1', a_2' \rangle$ für $\langle a_1, a_2 \rangle$