Gruppen

Grundbegriffe

Einführung in die Algebra
27.10.2005

Wiederholung

Relationen und mehr

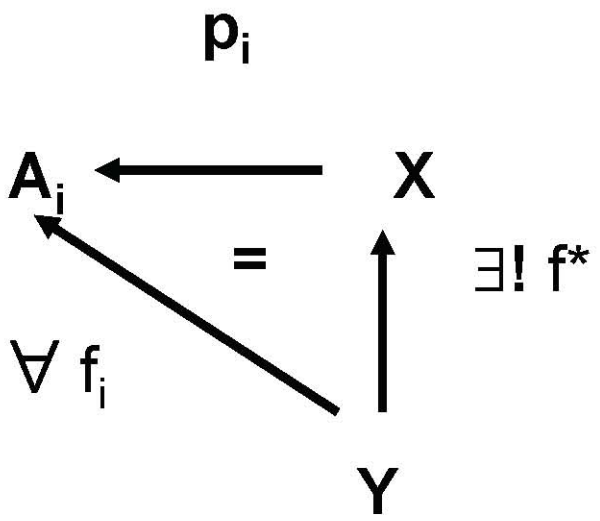
Produkt von Mengen

Sei $(A_i, i \in I)$ **eine Familie von Mengen.**

Eine Menge X zusammen mit einer Familie von Abbildungen p_i: X → A_i heißt **Produkt** der $(A_i, i \in I)$**, wenn folgendes gilt:**

Zu jeder Menge Y und jeder Familie von Abbildungen f_i : Y → A_i existiert genau eine Abbildung f*: Y → X mit

$$p_i^* \, f^* = f_i$$



Relationen

Definition

Eine n-stellige Relation R ist eine Teilmenge des karthesischen Produktes von n Mengen $A_1, A_2,...,A_n$:

$$R \subseteq A_1 \times A_2 \times ... \times A_n$$

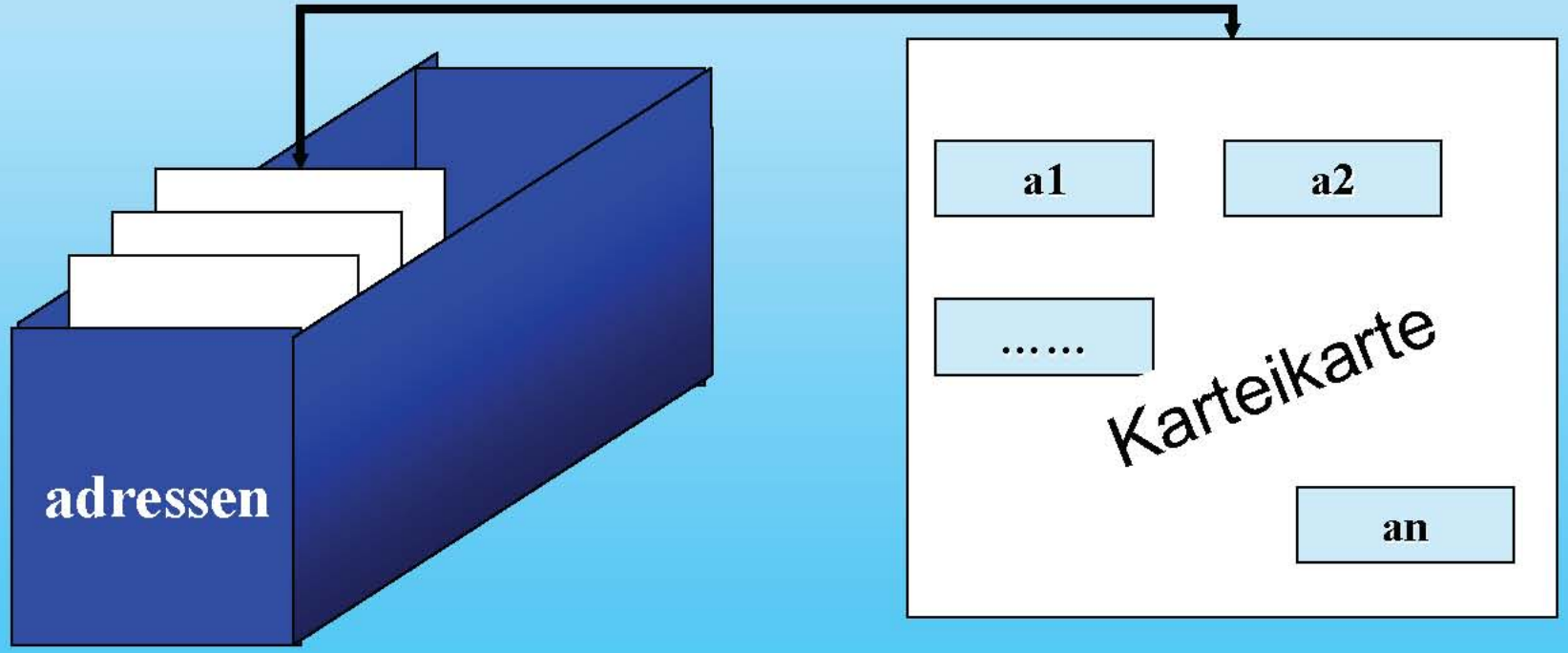
Schreibweise:

$$(a_1, a_2,...,a_n) \in R \leftrightarrow R\ (a_1, a_2,...,a_n)$$

Relationen
Beispiele

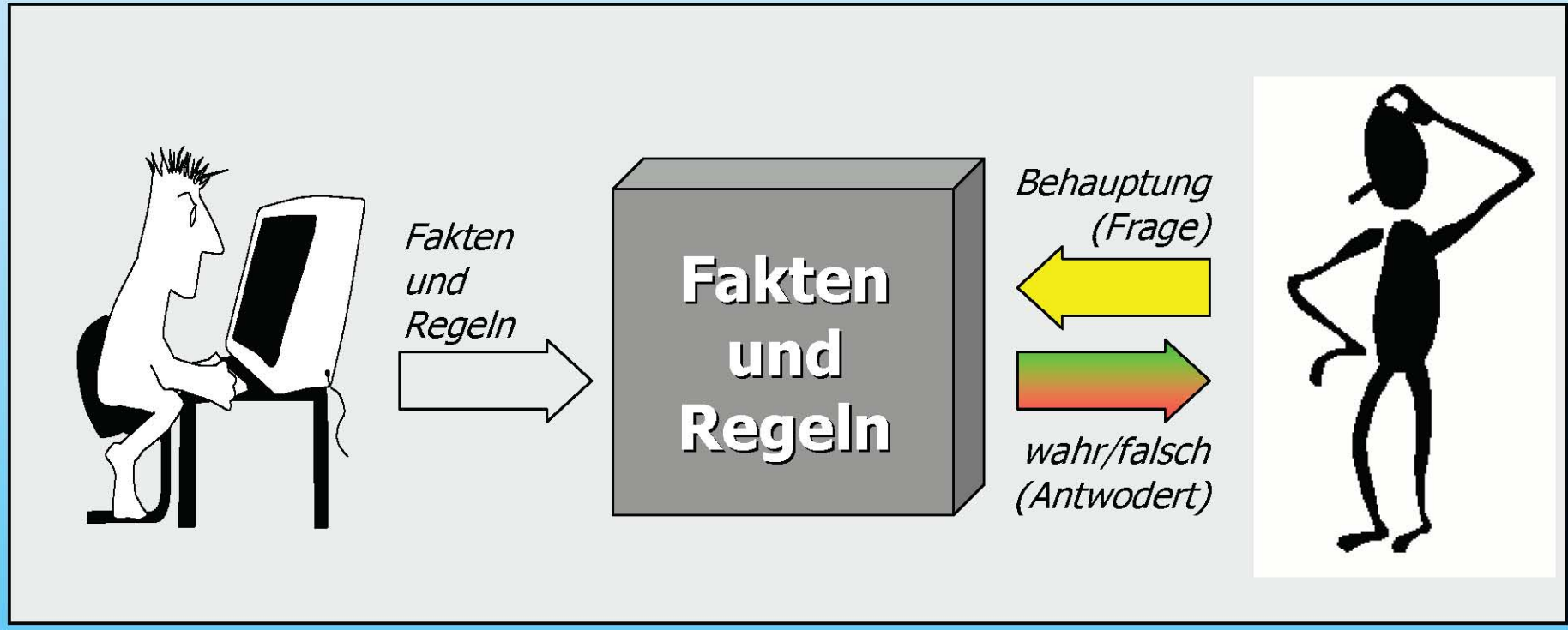
1. **Datenbanken: Tabelle**

   Beispiel: adressen(a1,a2,…,an)



PROLOG

PROgrammieren in LOGig



**Prolog-
Progammierer**

**Prolog-
Programiersystem**

Benutzer

Programmierparadigmen

Imperatives Programmieren

Funktionales Programmieren

Deklaratives Programmieren

Objektorientiertes Programmieren

PROLOG

PROgrammieren in LOGig

Prologprogramm

- **Fakten**
- **Regeln**
- **Anfragen**

$p(a_1,\ldots,a_n).$

- p ist der Name des Fakts
- $a_1, \ldots, a_n$ sind die Argumente des Fakts

Fakten

Beispiele:

Schreibweise in Prolog:	Natürliche Bedeutung:
• ‘die Sonne scheint‘.	• Die Sonne scheint.
• es_regnet.	• Es regnet.
• mensch(sokrates).	• Sokrates ist ein Mensch.
• männlich(daniel).	• Daniel ist männlich.
• mag(johann,maria).	• Johann mag Maria.
• besitzt(johann,gold).	• Johann besitzt Gold.
• vater(hans, gabriel).	• Hans ist der Vater von Gabriel.

PROLOG

PROgrammieren in LOGig

Prologprogramm

- **Fakten**
- **Regeln**
- **Anfragen**

Regel

b1 und b2,…und bn → f

Wenn b1 und b2,..,und bn gelten,dann gilt auch f.

Prologschreibweise

f :- b1,b2,…,bn.

PROLOG

PROgrammieren in LOGig

Prologprogramm

- **Fakten**
- **Regeln**
- **Anfragen**

Gelten die Fakten p1, p2,…, pn ?

Prologschreibweise

? p1, p2,…, pn

Fakten

Sokrates ist ein Mensch.

•Regeln

Alle Menschen sind sterblich.

Anfragen

Ist Sokrates sterblich?

Prologschreibweise

mensch(sokrates).

mensch(X) → sterblich(X)

sterblich(X):- mensch(X).

? sterblich(sokrates)

Expertensysteme

Prinzipieller Aufbau

Benutzer :
Experte …. Laie

Dialogkomponente

Erklärungskomponente

Inferenzkomponente

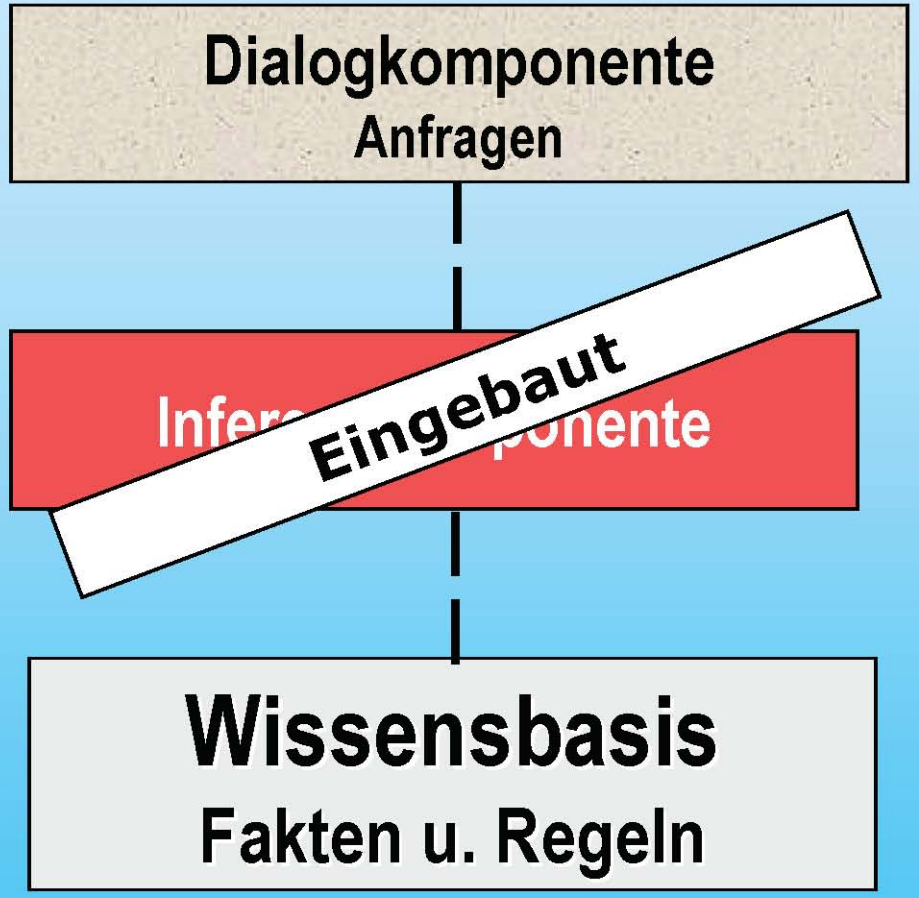
Wissensbasis

Wissenserwerbskomponente

Datenbank

Experte

Prologprogramm <-> Expertensystem



Arithmetik

+ - * /	Addition, Subtraktion, Multiplikation, Division
mod	Modulo
// ^	Gleitzahl-Division, Potenzierung
( )	Priorität
is	Zuweisen eines arith. Ausdruckes
> <	größer, kleiner
=> =<	größer gleich, kleiner gleich (zuerst = dann > !)
=:=	gleich (arithmetisch)
=\=	ungleich (arithmetisch)

Beispiel: Berechnen der Fakultät

```
fak(0,1).
fak(N,X) :-   N > 0,   M is N - 1,   fak(M,Y),   X is N * Y.
```

Aufruf:

```
?- fak(0,N).
N = 1
```

```
?- fak(6,N).
N = 720
```

A, B und C stehen vor Gericht.

- A sagt aus, dass B lügt.
- B sagt aus, dass C lügt.
- C sagt aus, dass A und B lügen.

Wer lügt, wer sagt die Wahrheit?

Prologprogramm

```
ist_Lügner(wahr,lügt).
ist_Lügner(lügt,wahr).
beide_lügen(wahr,lügt,lügt).
beide_lügen(lügt,wahr,lügt).
beide_lügen(lügt,lügt,wahr).
beide_lügen(lügt,wahr,wahr).
```

```
?- ist_Lügner(A,B),
   ist_Lügner(B,C),
   beide_lügen(C,A,B).
```

Relationen

Binäre Relation

Definition

Eine **binäre Relation R** ist eine Teilmenge des karthesischen Produktes zweier Mengen A und B:

$$R \subseteq A \times B$$

Für

$$(a,b) \in R$$

schreibt man auch

$$aRb \text{ oder } R(a,b)$$

Binäre Relationen
Beispiele

a) die Ordnungsrelation $\leq$ auf $\mathbb{N}$ und $\mathbb{R}$,

b) die Enthaltenseinsbeziehung zwischen Mengen: $A \subseteq B$,

c) die Ähnlichkeit von $(n \times n)$-Matrizen A and A': $\exists\ S$ such that $A' = S^{-1}AS$

d) die Kongruenz $(\mod n)$ auf $\mathbb{Z}$, z.B. $6 \equiv 21 (\mod 5)$.

Binäre Relationen und Graphen

Eine binäre Relation R kann durch einen Graphen veranschaulicht werden in dem jedes Tupel (a,b) als Kante zwischen den Knoten a und b interpretiert wird.

$(a,b) \in R$  a  b

Umgekehrt entspricht jede Kante (a,b) eines Graphen die zwei Knoten a und b verbindet einer Relation R für die

aRb als „a ist mit b direkt verbunden“ interpretiert werden kann.

Reflexivität

Eine binäre Relation $R \subseteq S \times S$ ist reflexiv, wenn jedes Element von S zu sich selbst in Relation steht:

$$\forall\, x: x \in S: xRx$$

zB: die Relation „hat dieselbe Mutter wie“ ist reflexiv

Reflexive Relationen können durch einen Graphen modelliert werden, bei dem alle Knoten Schlaufen haben.

Symmetrie

Eine binäre Relation $R \subseteq S \times S$ ist symmetrisch, wenn aus xRy auf yRx geschlossen werden kann:

$$\forall\ x,y: x,y \in S: xRy \Rightarrow yRx$$

zB: die Relation „ist verheiratet mit“ ist symmetrisch

Symmetrische Relationen entsprechen ungerichteten Graphen.

Transitivität

Eine binäre Relation $R \subseteq S \times S$ ist transitiv, wenn aus xRy und yRz auf xRz geschlossen werden kann:

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

zB: die Relation „ist Vorfahre von“ ist transitiv

Äquivalenzrelationen

Definition:

Eine Äquivalenzrelation auf einer Menge M ist eine binäre Relation ~ auf M, die

- **reflexiv,**
- **symmetrisch und**
- **transitiv ist.**

Definition Äquivalenzklasse

Sei ~ eine Äquivalenzrelation auf M und a ∈M. Dann heißt die Menge der zu a äquivalenten Elemente die Äquivalenzklasse von a.

$$\bar{a} := \{x \in M \mid a \sim x\} \subseteq M$$

Äquivalenzrelationen
Funktionen

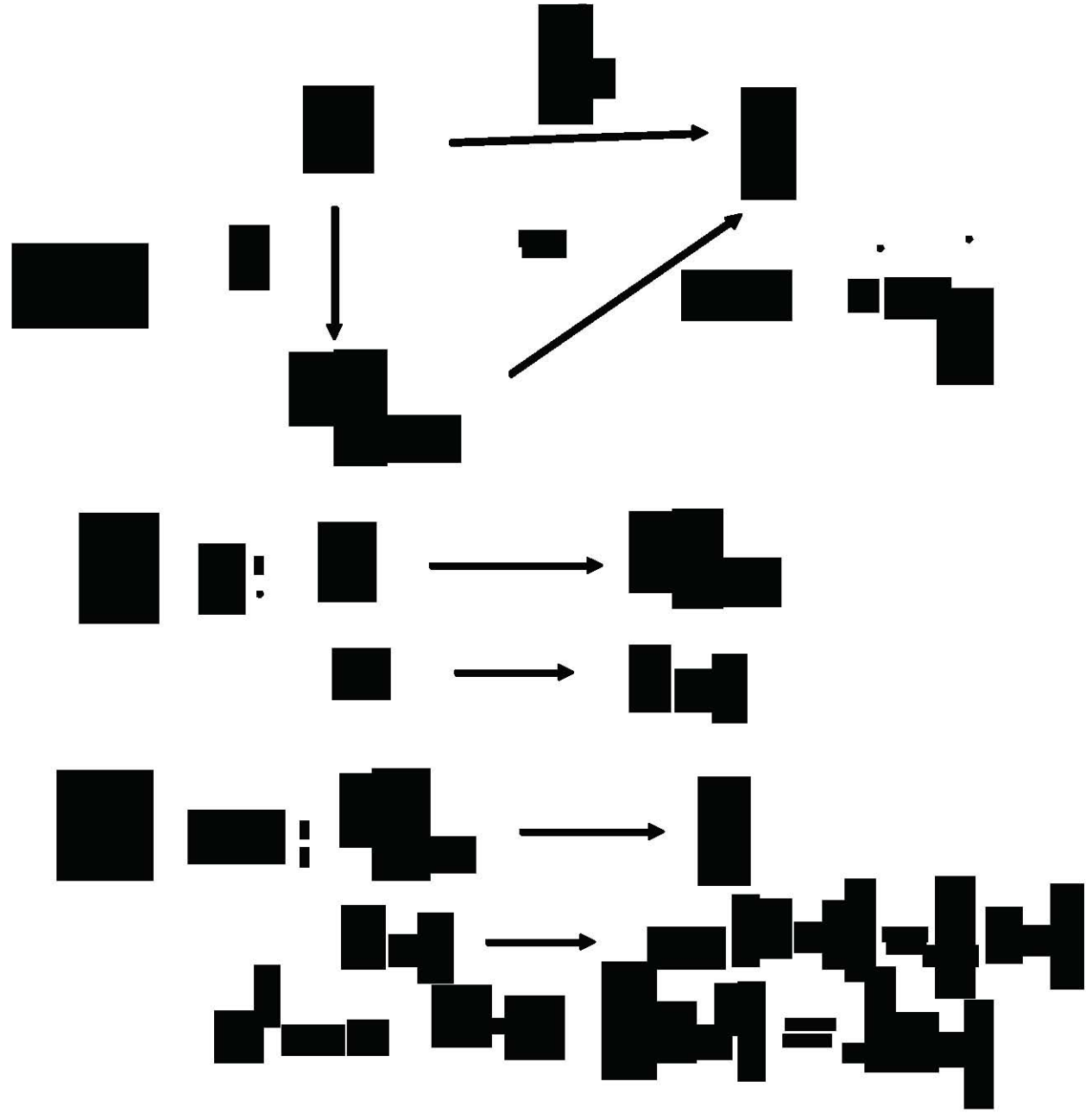
Sei f: A → B eine Funktion, dann definiert

$$a \sim a' \leftrightarrow f(a) = f(a')$$

eine Äquivalenzrelation auf A

A/~ := Die Menge der Äquivalenzklassen von ~ heißt der Quotientenraum von A bzgl. ~

$$A/\sim := \{[a]; a \in A\}$$



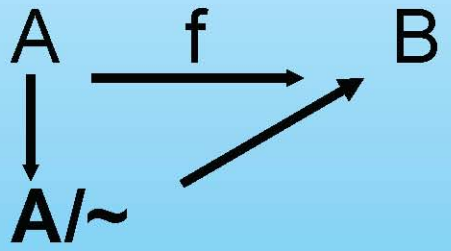
Homomorphiesatz für Abbildungen

Satz Sei f: A → B eine Funktion, und

$$a \sim a' \leftrightarrow f(a) = f(a')$$

die durch f erzeugte Äquivalenzrelation. Dann gelten:

1)



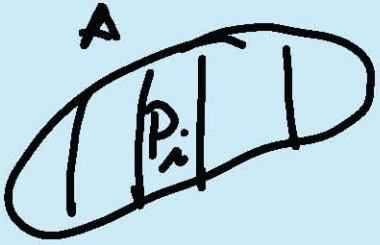
definiert eine kanische Faktorisierung f= e*m mit e: A → A/~ surjektiv und m: A/~ → B injektiv.

2) m: A/~ → f(A) ist bijektiv, d.h

$$A/\sim \approx f(A)$$

Definition $\mathcal{P} = \{P_i \subseteq A ; i \in I\}$

$\mathcal{P}$ heißt **Partition auf A** $\Leftrightarrow$ def.



P1) $\forall_{i \in I} \; P_i \neq \emptyset$

P2) $\forall_{i,j \in I} \; P_i \cap P_j \neq \emptyset \Rightarrow P_i = P_j$

P3) $\bigcup_{i \in I} P_i = A$

Äquivalenzrelation
Beispiele

Betrachte die Relation

$R = \{ (a,b) \in Z \times Z \mid a \equiv b \pmod{m} \}$

- $a \equiv b \pmod{m} \iff m \mid a-b$

  Sprechweise: "a und b sind kongruent modulo *m*"

Satz: Die Relation "Kongruenz modulo *m*" ist eine Äquivalenzrelation auf Z.

R ist reflexiv: (a,a) $\in$ *R* bedeutet dass *m* | *a-a*

– *a-a* = 0, ist teilbar durch *m*

R ist symmetrisch: Wenn (*a,b*) $\in$ *R* dann (*b,a*) $\in$ *R*

(*a,b*) $\in$ *R* bedeutet dass *m* | *a-b*

Oder dass *km* = *a-b*. Multiplikation mit -1 ergibt *b-a* = *-km*

Daher gilt: *m* | *b-a*, und somit (b,a) $\in$ *R*

R ist transitiv: Sind (*a,b*) $\in$ *R* und (*b,c*) $\in$ *R* dann (*a,c*) $\in$ *R*

(*a,b*) bedeutet dass *m* | *a-b*, oder dass *km* = *a-b*

(*b,c*) bedeutet dass *m* | *b-c*, oder dass *lm* = *b-c*

(*a,c*) bedeutet dass *m* | *a-c*, oder dass *nm* = *a-c*

Addiert man die ersten beiden Gleichungen, so erhält man

km+lm = (*a-b*) + (*b-c*) oder (*k+l*)*m* = *a-c*

Damit gilt *m* | *a-c*, mit *n* = *k+l*

Damit ist die Relation "Kongruenz modulo *m*" eine Äquivalenzrelation

Äquivalenzrelationen und Partitionen

Satz: Äquivalenzrelationen und Partitionen stehen in einer bijektiven Relation.

genauer

Satz1: Ist $\sim$ eine Äquivalenzrelation auf M, dann ist die Menge aller Äquivalenzklassen
$\{\bar{a} \mid a \in M\} =: \mathcal{P}_\sim$ eine Partition.

Satz2: Ist $\mathcal{P}$ eine Partition von M, dann ist

$$\sim_P := \{(x, y) \mid \exists P \in \mathcal{P}.\ x,\ y \in P\}$$

Satz3: Ist $\sim$ eine Äquivalenzrelation, $P := P_\sim$, so gilt: $\sim = \sim_P$

Satz4: Ist P eine Partition, $\sim := \sim_\mathcal{P}$, so ist $\mathcal{P}_\sim = \mathcal{P}$

Gruppen

1.1 Mengen mit Verknüpfung
Definition 1.1.1.
(i) Eine Verknüpfung **T auf einer Menge A ist eine Abbildung**

$$T : A \times A \rightarrow A$$
$$(a, b) \rightarrow a\ T\ b\ ,$$

die jedem geordneten Paar (a, b) von Elementen a, b der Menge A ein weiteres Element (a T b) $\in$ A zuordnet.

(ii) Eine Verknüpfung T heißt assoziativ**, wenn gilt**

$$aT\ (bT\ c) = (aT\ b)Tc \quad \text{für alle } a, b, c \in A.$$

(iii) Die Verknüpfung heißt kommutativ oder abelsch **genau dann, wenn Gilt aT b = bT a für alle a, b $\in$ A.**

Ist eine Verknüpfung assoziativ, so liefern Ausdrücke der Form $a_1 T\ a_2 \ldots T\ a_n$ wohlbestimmte Elemente von A, das Resultat ist unabhängig davon, wie man die Klammern setzt.

Grundlegende Definitionen und Beispiele

Definition 1.2

Es seien **G** eine nichtleere Menge,
eine Abbildung **T** : G x G → G
und e ∈G ein Element.
Man nennt (G, **T**,e) eine **Gruppe**, wenn gilt

ist **assoziativ**, $\forall$ **a,b,c**∈**G: (aTb) Tc = aT (bTc)**

e ist ein **neutrales Element**:

$\forall$ **a** ∈**G: eTa=aTe=a**

alle Elemente haben ein **Inverses**,

$\forall$ **a** ∈**G** $\exists$ $\mathbf{a^{-1}}$ ∈**G** : **aT** $\mathbf{a^{-1}}$ = $\mathbf{a^{-1}}$**Ta = e**

Grundlegende Definitionen und Beispiele

G ist die *Trägermenge* der Gruppe,

*** die *Gruppenoperation*.**

Ist die Gruppenoperation kommutativ,

so spricht man von einer

kommutativen oder *Abelschen* Gruppe**.**

Grundlegende Definitionen und Beispiele

Beispiele für Gruppen sind

- die ganzen Zahlen mit der Addition, $(\mathbb{Z}, +, 0)$
- rationalen Zahlen ohne Null mit der Multiplikation $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$
- Für jede nichtleere Menge M ist die Menge

$$S(M) := \{f : M \to M \mid f \text{ bijektiv}\}$$

aller bijektiven Selbstabbildungen mit der Abbildungskomposition eine Gruppe. S(M) heißt die **symmetrische Gruppe** auf M, ihre Elemente heißen ***Permutationen*** **von M**.

Gruppen

Ist M= {1,..,n} , so schreibt man auch S(n) oder S_n statt S(M).
S_n heißt die **symmetrische Gruppe** über n (oder **Permutationsgruppe**)

Für M= {1,2} besteht S_2 aus den beiden Permutationen id= (1 → 1,2 →2) und
P= (1 → 2 ,2 →1) .

Schreibweise für Elemente aus S_n

Gruppen

Für einen Vektorraum wird die Menge

$$GL(V) := \{f : V \to V \mid f \text{ Isomorphismus}\}$$

aller bijektiven linearen Abbildungen von V in V mit der Abbildungskomposition zu einer Gruppe , der ***allgemeinen linearen Gruppe*** von V .

Notation

Seien $x, y \in G$ zwei Gruppenelemente und $1 \leq k \in \mathbb{N}$, dann definieren wir

$$\begin{aligned} x^k &:= x\,x \ldots x \quad (k-\text{mal}) \\ x^0 &:= e \\ x^{-k} &:= x^{-1}x^{-1} \ldots x^{-1} \quad (k-\text{mal}) \\ x^y &:= y\,x\,y^{-1} \\ [x,y] &:= xy\,(yx)^{-1} \end{aligned}$$

Und damit gelten dann für beliebige $x, y, z \in G$ und $k \in \mathbb{Z}$ die Rechenregeln

$$\begin{aligned} (x^{-1})^{-1} &= x \\ (xy)^{-1} &= y^{-1}x^{-1} \\ (x^y)^z &= x^{zy} \\ y^x &= [x,y]\,y \\ xy &= [x,y]\,yx \\ [x,y]^{-1} &= [y,x] \\ [x,y]^z &= [x^z, y^z] \\ xy = yx &\iff [x,y] = e \\ xy = yx &\implies (xy)^k = x^k y^k \end{aligned}$$

Gruppen

Definition
Wir nennen H eine **Untergruppe** der Gruppe $(G, \circ)$, falls erfüllt sind

- $\emptyset \neq H \subseteq G$ ist eine nicht-leere Teilmenge
- $\forall\, x, y \in H$ gilt $xy \in H$ multiplikativ abgeschlossen
- $\forall\, x \in H$ gilt $x^{-1} \in H$ invers abgeschlossen

Und eine Untergruppe H von G heisst ein **Normalteiler** von G falls weiterhin eine der folgenden drei äquivalenten Aussagen erfüllt ist

(a) $\forall\, x \in G$ gilt $xH = Hx$

(b) $\forall\, x \in G$ gilt $H^x = H$ mit $H^x := \{xhx^{-1};\ h \in H\} = \{h^x;\ h \in H\}$

(c) $\forall\, x \in G$ gilt $H^x \subseteq H$

Gruppen

Schreibweise

U ist eine Untergruppe von G:

$$U \leq_g G$$

N ist ein Normalteiler von G:

$$N \leq_n G$$

Gruppen

LEMMA UND DEFINITION

- Ist (H_λ) eine beliebige $(\lambda \in \Lambda)$ Familie von Untergruppen von G, so ist deren Schnitt wiederum eine Untergruppe von G

$$\bigcap_{\lambda \in \Lambda} H_\lambda \;=\; \{\, x \in G \mid \forall\, \lambda \in \Lambda \text{ gilt } x \in H_\lambda \,\} \quad \leq_{\mathbf{g}} \quad G$$

- Analog ist ein beliebiger Schnitt von Normalteilern (N_λ) von G wiederum ein Normalteiler von G.

- Für eine beliebige Teilmenge $A \subseteq G$ definieren wir also die von A in G **erzeugte Untergruppe** durch

$$\begin{aligned} \langle A \rangle_{\mathbf{g}} \;&:=\; \bigcap \{\, H \;\leq_{\mathbf{g}}\; G \mid A \subseteq H \,\} \\ &=\; \{\, a_1^{\varepsilon_1} \ldots a_r^{\varepsilon_r} \mid r \in \mathbb{N}, a_i \in A, \varepsilon_i \in \pm 1 \,\} \end{aligned}$$

Gruppenhomomorphismus $\forall \exists \{ \} | \in$

Definition

Seien (E;*) und (F;*) zwei Gruppen, wobei die jeweiligen neutralen Elemente

mit e $\in$ E bzw. mit f $\in$F bezeichnet seien.

Ist nun φ : E $\rightarrow$ F eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall \; x; y \in E \text{ gilt } \varphi(xy) = \varphi(x)\, \varphi(y)$$

und in diesem Fall erfülllt φ sogar schon die beiden weiteren Eigenschaften

$$\varphi(e) = f \text{ und } \varphi(x^{-1}) = \varphi(x)^{-1}$$

Produkt von Gruppen

Sei $(G_i, i \in I)$ **eine Familie von Gruppen.**

Eine Gruppe X zusammen mit einer Familie von Gruppenhomomorphismen p_i: X → G_i heißt **Produkt** der $(G_i, i \in I)$, **wenn folgendes gilt:**

Zu jeder Gruppe Y und jeder Familie von Gruppenhomomorphismen $f_i : Y \to G_i$ existiert genau ein **Gruppenhomomorphismus** $f^*: Y \to X$ mit

$$p_i^* \, f^* = f_i$$