

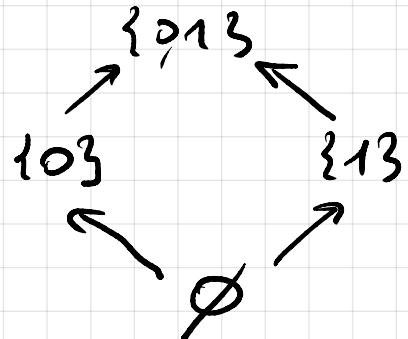
# Agenda: Relationen Gruppen

## 1.6. Relationen

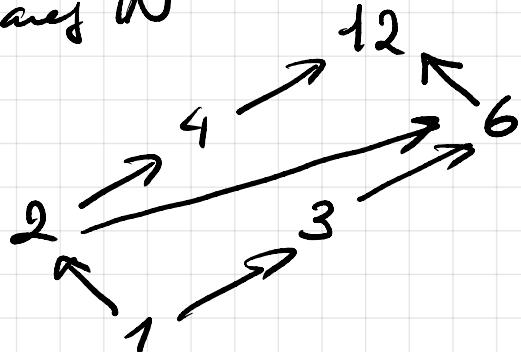
1.6.1. Relationen Seien  $X, Y$  Mengen. Dann heißt  $R \subseteq X \times Y$  eine Relation zwischen den Elementen von  $X$  und den Elementen von  $Y$ . Man sagt, dass ein  $x \in X$  in Relation  $R$  zu einem  $y \in Y$  steht, wenn  $(x, y) \in R$  gilt. Man schreibt dann  $x R y$ . Ist  $X = Y$ , so spricht man von einer bipären Relation auf  $X$ , d.h.  $R \subseteq X^2$ .

### Bsp

- $\leq, <, \geq, \geq, =, \neq$  sind bipäre Relationen auf  $\mathbb{R}$ .
- $\subseteq$  ist eine Relation auf  $\mathcal{P}^X$  für eine gegebene Menge  $X$ .



- Die Relation  $a|b$  (heißt:  $a$  teilt  $b$ ) auf  $\mathbb{N}$



- Wir fixieren einen Wert von  $\text{EN}$  und nennen  $a \in \mathbb{Z}$  und  $b \in \mathbb{Z}$  kongruent modulo, wenn  $a - b$  durch  $n$  teilbar ist. Kongruenz modulo  $n$  ist eine binäre Relation auf  $\mathbb{Z}$ .

**1.6.2. Äquivalenzrelation** Sei  $X$  Menge und  $\sim$  eine binäre Relation auf  $X$ . Man nennt  $\sim$  eine Äquivalenzrelation, wenn Folgendes gilt:

- (i)  $\sim$  ist reflexiv, d.h.  $x \sim x$  für alle  $x \in X$ .
- (ii)  $\sim$  ist symmetrisch, d.h.  $x \sim y$  ist äquivalent zu  $y \sim x$  für alle  $x, y \in X$ .
- (iii)  $\sim$  ist transitiv, d.h. :

$$\forall x \in X \forall y \in X \forall z \in X : (x \sim y) \wedge (y \sim z) \Rightarrow (x \sim z).$$

Ist  $\sim$  Äquivalenzrelation auf  $X$ , so führt man für  $x \in X$ , die Äquivalenzklasse von  $x$  wie folgt ein:

$$[x]_{\sim} := \{y \in X : y \sim x\}.$$

Für die Menge aller Äquivalenzklassen bzgl. der Relation  $\sim$  führen wir die folgende Bezeichnung ein:

$$X/\sim := \{[x]_{\sim} : x \in X\}.$$

Bsp

- Für  $X = \mathbb{Z} \times \mathbb{N}$  führen wir die folgende binäre Relation auf  $X$  ein:

$$(z_1, n_1) \sim (z_2, n_2) :\Leftrightarrow$$

$$z_1 \cdot n_2 = z_2 \cdot n_1.$$

Es ist eine Äquivalenzrelation auf  $X$ .

Die Äquivalenzklassen entsprechen den rationalen Zahlen. D.h.  $X/\sim$  entspricht der Menge  $\mathbb{Q}$  der rationalen Zahlen.

- Kongruenz modulo  $m$  ist eine Äquivalenzrelation auf  $\mathbb{Z}$ . Bezeichnung:

a kongress zu b modulo m bedeutet man als

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

## 2.

### Ausgewählte algebraische Strukturen

#### 2.1. Gruppen

##### 2.1.1. Binäroperation

Sei  $X$  Menge. Eine Binäroperation auf  $X$  ist eine Abbildung  $*: X \times X \rightarrow X$ .

Bei einer Binäroperation schreiben wir  $x * y$  und der Stelle von  $*(x, y)$ .

Man nennt  $*$  assoziativ, wenn

$$x * (y * z) = (x * y) * z$$

für alle  $x, y, z \in X$  erfüllt ist

Bsp.

Ist  $X$  die Menge aller Abbildungen von  $M$  nach  $M$  (für eine gegebene Menge  $M$ ), so ist  $\circ$  (die Komposition von Abbildungen) eine assziative Operation.

Bem

Ist  $*$  assziativ, so hängt der Wert von  $x_1 * \dots * x_n$

(bei  $x_1, \dots, x_n \in X$  und  $n \in \mathbb{N}$ )

nicht von der Wahl der Klammerung ab.

z.B.

$$(x_1 * (x_2 * x_3)) * x_4 = x_1 * (x_2 * (x_3 * x_4))$$

||

|||

$$x_1 * ((x_2 * x_3) * x_4)$$

## 2.1.2. Gruppe

Sei  $G$  Menge und  $*: G \times G \rightarrow G$ .

Dann heißt  $(G, *)$  (d.h.  $G$ , das ausgestattet ist mit einer Binäroperation) eine Gruppe, wenn Folgendes gilt:

(G1)  $*$  ist assoziativ, d.h.  $a * (b * c) = (a * b) * c$   
gilt für alle  $a, b, c \in G$ .

(G2) Es existiert ein Element  $e \in G$ ,  
so dass für jedes  $a \in G$ :

(a)  $e * a = a$

(b) ein  $b \in G$  existiert mit  $b * a = e$ .

$e$  heißt ein linkes neutrales Element und mit  $b * e = e$

heißt ein linkes inverses Element von  $a$ .

Wenn zusätzlich das Kommutativgesetz  $u * v = v * u$   
für alle  $u, v \in G$  gilt, so nennt man die

Gruppe  $(G, *)$  kommutativ oder Abel sch.

Man wählt die Bezeichnung für die Gruppenverknüpfung

- (Mal) und nennt die Operation die  
Multiplikation. Bei kommutativen Gruppen  
nutzt man oft  $\cdot$  als die Bezeichnung für die  
Gruppenverknüpfung.

Bem

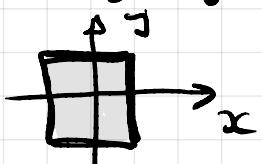
Für  $n \in \mathbb{N}$  bezeichnen wir als

$$a^n := \underbrace{a * \dots * a}_{n \text{ mal}}$$

$$a^0 := e \quad (\text{wir werden in Kürze zeigen, dass } e \text{ eindeutig ist}).$$

Bsp

Belegungssymmetrien eines Quadrats



$$[-1, 1]^2$$



**Bsp** Für  $n \in \mathbb{N}$  ist die Menge  $S_n$  aller bijektiven Abbildungen  $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$  eine Gruppe bzgl. der Komposition. Die Komposition bezeichnen wir als  $\circ$ .

Die Elemente von  $S_n$  nennt man Permutationen von  $n$  Elementen. Die Gruppe  $(S_n, \circ)$  nennt man die symmetrische Gruppe.  $S_n$  hat  $n! = 1 \cdot 2 \cdot \dots \cdot n$  Elemente.

### 2.1.3. Das linke und das rechte Inverse

**Prop** Sei  $(G, \circ)$  Gruppe, sei  $e \in G$  ein linkes neutrales Element von  $(G, \circ)$  und seien  $a, b \in G$  Elemente mit  $a \circ b = e$ . Dann gilt:  $b \circ a = e$ .

Beweis:

Nach (G2)(b) besitzt jedes Element von  $G$  ein linkes inverses Element. Daher existiert für  $a \in G$  ein Element  $c \in G$  mit  $c \circ a = e$ . Nach (G2)(a) gilt

$$b \circ a \stackrel{(G2)}{=} e \circ (b \circ a) = (c \circ a) \circ (b \circ a)$$

$$\stackrel{(G1)}{=} c \circ (a \circ (b \circ a))$$

$$\stackrel{(G1)}{=} c \circ ((a \circ b) \circ a)$$

Voraussetzung

$$= c \circ (e \circ a)$$

$$\stackrel{(G2)}{=} c \circ a$$

$$= e. \quad \square$$

## 2.1.4. Eindeutigkeit des linken neutralen Elements

**Prop.** Sei  $(G, \cdot)$  Gruppe und seien  $e, e' \in G$  linke neutrale Elemente. Dann gilt:  $e = e'$ .

**Beweis:** W<sup>u</sup> e ein linkes neutrales Element ist, gilt  $e \cdot e' = e'$ . Aus der Proposition 2.1.3, die wir zum linken neutralen Element  $e'$  anwenden, folgt  $e' \cdot e = e'$ . Mit aber  $e'$  ein linkes neutrales Element ist, gilt  $e' \cdot e = e$ . Also gilt  $e = e'$ .  $\square$

## 2.1.5. Neutralität von links und rechts

**Proposition** Sei  $(G, \cdot)$  Gruppe und  $e$  das linke neutrale Element von  $G$  (d.h. das eindeutige Element mit  $e \cdot a = a$  für alle  $a \in G$ ). Dann gilt:  $a \cdot e = a$  für alle  $a \in G$  (d.h.  $e$  ist auch das rechte neutrale Element).

**Beweis:** Sei  $a \in G$ . Nach (G2)(b) existiert ein  $b \in G$  mit  $b \cdot a = e$ . Dann gilt:

$$a \cdot e = a \cdot (b \cdot a) \stackrel{(G1)}{=} (a \cdot b) \cdot a \stackrel{2.1.3.}{=} e \cdot a \stackrel{(G2)(a)}{=} a.$$

$\square$

**Bem.** Ab jetzt können wir vom neutralen Element der Gruppe  $(G, \cdot)$  sprechen, das ist das eindeutige Element  $e \in G$  mit  $e \cdot a = a \cdot e = a$  für alle  $a \in G$ .

## 2.1.6. Eindeutigkeit des inversen Elements

**Prop.** Sei  $(G, \cdot)$  Gruppe,  $a, c \in G$  und seien  $b, c \in G$  Elemente mit  $b \cdot a = c \cdot a = e$  (d.h. sowohl  $b$  als auch  $c$  sind linke Inversen von  $a$ ).

Dann gilt:  $b = c$  (d.h. das inverse Elemente von  $a$  ist eindeutig.)

Beweis: Aus  $c \cdot a = e$  folgt wegen 2.1.3  
die Gleichung  $a \cdot c = e$ .

Aus 2.1.5 folgt  $b = b \cdot e$ .

Das ergibt:

$$b = b \cdot e = b \cdot (a \cdot c) \stackrel{(G1)}{=} (b \cdot a) \cdot c$$

Voraussetzung

$$= e \cdot c$$

$$\stackrel{(G2)}{=} c.$$

□