

# Von Gruppen zu Ringen

Def.:

Gruppe

$G$  sei eine Menge mit einer Verknüpfung

(G1) Assoziativgesetz

(G2) Existenz eines neutralen Elements

(G3) Existenz eines inversen Elements

(G4) Abgeschlossenheit <man landet wieder in der Gruppe>

Bsp.:  $(\mathbb{Z}, +)$   $a+0=a$ ,  $0$ : neutrales Element

$a^{-1} = -a$  : inverses Element

$(\mathbb{Q} \setminus \{0\}, \cdot)$  inverses:  $\frac{1}{a}$

neutrales  $\bar{e}$ :  $1$

Restklassengruppe  $(\mathbb{Z}_m, +)$

Was sind Restklassengruppen?

$$a \equiv b \pmod{m} \iff a - b = m \cdot k, k \in \mathbb{Z}$$

Beispiel:  $(\mathbb{Z}_5, +) = \{\bar{1}; \bar{2}; \bar{3}; \bar{4}; \bar{5} = \bar{0}\}$

| +         | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

neutrales Element:  $\bar{0}$

inverses Element:

| $a$       | $a^{-1}$  |
|-----------|-----------|
| $\bar{1}$ | $\bar{1}$ |
| $\bar{2}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ |
| $\bar{0}$ | $\bar{0}$ |

$$(\mathbb{Z}_5, \cdot)$$

| $\cdot$   | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

neutrales Element:  $\bar{1}$

inverses:

| $a$       | $a^{-1}$  |
|-----------|-----------|
| $\bar{2}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ |

$\nrightarrow$  keine Gruppe:  $\bar{0}$   $\nrightarrow$

### Zyklische Gruppen:

werden von einem Element erzeugt:

Man muss nur das passende Element finden.

Bsp.:  $(\mathbb{Z}_5, +) \stackrel{\text{def.}}{=} \langle \bar{1} \rangle; \bar{1} + \bar{1} = \bar{2}; \bar{2} + \bar{1} = \bar{3}; \bar{3} + \bar{1} = \bar{4}; \bar{4} + \bar{1} = \bar{0}$

Frage: Gibt es ein Element, dass die  $(\mathbb{Z}_5 \setminus \{0\})$  erzeugt?

$$\bar{2} \cdot \bar{2} = \bar{4}$$

$$\langle \bar{2} \rangle = \{ \bar{2}, \bar{4}, \dots \}$$

$$\bar{2} \cdot \bar{4} = \bar{3}$$

$$\bar{3} \cdot \bar{4} = \bar{2}$$

$$\bar{3} \cdot \bar{3} = \bar{1}$$

$$\bar{4} \cdot \bar{4} = \bar{1}$$

Ringe: 2 verschiedene Verknüpfungen  $+$ ,  $\times$

(R1)  $(R, +)$  ist kommutative Gruppe

(R2) Assoziativgesetz für „ $\times$ “:  $(a \times b) \times c = a \times (b \times c)$

(R3) Distributivgesetz  $\forall a, b, c \in R$ :

$$a \times (b + c) = a \times b + a \times c$$

$$a + (b \times c) = a + b \times a + c$$

Beispiele:  $(\mathbb{Z}, +, \cdot)$

$(\mathbb{R}^{n \times n}, +, \cdot)$

Restklassengruppen mit  $+$  &  $\cdot$  sind Ringe!

Übe mit  $\mathbb{Z}_4$ !

| $\cdot$   | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{1}$ |

| $+$       | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

Nullteiler!

Falls für die Verknüpfung „ $\cdot$ “ gilt

$$\forall a, b \in \mathbb{R} \quad a \cdot b = 0 \rightarrow a = 0 \text{ oder } b = 0$$

dann ist der Ring nullteilerfrei

Auswerten nennt man  $\bar{a}, \bar{b}$  Nullteiler

Sind  $(\mathbb{Z}_4, +, \cdot)$  &  $(\mathbb{Z}_5, +, \cdot)$  nullteilerfrei?

↑  
Nein!!!

↑  
ja!

Nullteiler  $\bar{2}$ !

Satz:  $(\mathbb{Z}_m, +, \cdot)$  ist nullteilerfrei  $\Leftrightarrow m$  ist Primzahl

Beweis: „ $\Rightarrow$ “  $\mathbb{Z}_m$  ist nullteilerfrei

Annahme:  $m$  ist keine Primzahl;  $m = n \cdot p$

„ $\Rightarrow$ “  $\bar{m} = \bar{n} \cdot \bar{p} = \bar{0} \nmid \Rightarrow m$  ist Primzahl

„ $\Leftarrow$ “  $m$  ist Primzahl

Sei  $\bar{a} \cdot \bar{b} = \bar{0}$  für  $\bar{a}, \bar{b} \in (\mathbb{Z}_m, +, \cdot)$

$$\Rightarrow ab = 0 \pmod m \Rightarrow m \mid ab \xrightarrow{m \text{ Primzahl}} m \mid a \text{ oder } m \mid b$$

$$\Rightarrow a \equiv 0 \pmod m \text{ oder } b \equiv 0 \pmod m \Rightarrow \bar{a} = \bar{0} \text{ oder } \bar{b} = \bar{0}$$