① 

# Algebraische Strukturen

$(G, \circ)$ Menge $G$, Verknüpfung $\circ$ — Kurzform

**Halbgruppe** $\circ$ ist assoziativ $[a \circ (b \circ c) = (a \circ b) \circ c]$

**Monoid** $\circ$ ist assoziativ, es ex. ein neutrales Element $e$ $[a \circ e = a = e \circ a]$

**Gruppe** $\circ$ ist assoziativ, es ex. ein neutrales Element $e$, jedes Element ist invertierbar $[a^{-1} \circ a = e = a \circ a^{-1}]$

**abelsche Gruppe** $\circ$ ist assoziativ, es ex. ein neutrales Element $e$, jedes Element ist invertierbar, $\circ$ ist kommutativ $[a \circ b = b \circ a]$

---

$(M, \circ)$ Monoid $a, b$ invertierbar $\Rightarrow$ $a \circ b$ invertierbar, $b^{-1} \circ a^{-1}$ ist Inverses zu $a \circ b$

**Theorem 4.21** $(M, \circ)$ Monoid, $G \subseteq M$ invertierbare Elemente, $*$ entspricht $\circ$ auf $G$

folgt daraus

$* : G \times G \to G$ abgeschlossen, wohldefiniert

$\Rightarrow (G, *)$ ist eine Gruppe

BSP $\mathbb{Z}_4$ <u>Verknüpfungstabellen</u> 1

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ $\mathbb{Z}/4\cdot\mathbb{Z}$ $\mathbb{Z}_4$

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\boxed{\bar{1}}$ | $\bar{2}$ | $\boxed{\bar{3}}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\boxed{\bar{3}}$ | $\bar{2}$ | $\boxed{\bar{1}}$ |

$(\mathbb{Z}_4, \odot)$

$(\{\bar{1}, \bar{3}\}, \odot)$ Gruppe

$e \circ e = e = e \circ e$

$(\mathbb{Z}_4, \oplus)$

Gruppe, abelsch

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

## 4.3.2 Ringe und Körper

**Strukturen mit zwei Verknüpfungen**

$(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}\setminus\{0\}, \cdot)$ abelsche Gruppen

Mult.! Add.!

Gleichung: $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

$(-c) \cdot (-b) = c \cdot b$ "Minus & Minus ergibt Plus!" ?

Anwendung: Setze: $a = (-c) \Rightarrow (-c) \cdot (-b) = (-(-c)) \cdot b = c \cdot b$ ✓

$-(-c) = c$

$\Uparrow$

$(-c) + c = e = c + (-c)$

Sind solche Rechnungen korrekt?

<u>Definition 4.22</u> Sei $R$ eine Menge mit zwei <u>Verknüpfungen</u> $+, \circ$

Dann heißt $(R, +, \circ)$ ein Ring, wenn folgende Axiome gelten.

a) $(R, +)$ ist <u>abelsche Gruppe</u> mit neutralem Element $\mathbb{0}$.

b) $\circ$ ist assoziativ

c) Es gelten die Distributivgesetze i) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

ii) $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$

Falls $(R, \circ)$ ein neutrales Element hat (Notation $\underline{\mathbb{1}}$)

so heißt $(R, +, \circ)$ <u>Ring mit Eins</u>.

$x \in R$ <u>heißt invertierbar</u> oder auch <u>Einheit</u> von $R$ falls

$x$ bzgl. $\circ$ invertierbar. $R^* \subseteq R$ heißt die Menge der Einheiten.

$(R^*, \cdot)$ ist die Einheitengruppe

Falls $\cdot$ kommutativ ist, heißt $(R, +, \cdot)$ kommutativer Ring.

BSP

1) $(\mathbb{Z}, +, \cdot)$ komm. Ring mit Eins
$\mathbb{Z}^* = \{1, -1\}$ $\quad (\mathbb{Z}^*, \cdot)$ Einheitengruppe.

2) $M = \{2 \cdot a \mid a \in \mathbb{Z}\}$ <u>komm. Ring ohne Eins</u>
$(M, +, \cdot)$

3) $(\mathbb{R}, +, \cdot)$ komm. Ring mit Eins
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

4) $(\mathbb{Z}_4, +, \cdot)$ komm. Ring mit Eins $\bar{1}$
$(\{\bar{1}, \bar{3}\}, \cdot)$ Einheitengruppe

5

Ring ⇝ Rechenregeln

$$a \cdot (-b) = -(a \cdot b) = (-a) \cdot b \qquad a, b \in R$$

$$\Big( 0 \overset{!}{=} 0 \cdot b \Big) = \big(a + (-a)\big) \cdot b \underset{\text{Distributivität}}{=} (a \cdot b) + (-a) \cdot b \Big)$$

(verwenden)

$$\Rightarrow -(a \cdot b) = (-a) \cdot b$$

---

Definition 4.23 Ist $(R, +, \circ)$ ein Ring.

$(R \setminus \{0\}, \cdot)$ abelsche Gruppe.

Dann heißt $(R, +, \cdot)$ Körper (Field).

$\Rightarrow$ Gemäß Definition mindestens 2 Elemente müssen vorhanden sein? $(1, 0 \quad 1 \neq 0.)$

6

Bsp

1) $(\mathbb{Z}_2, \oplus, \odot)$ $\qquad \bar{0}, \bar{1}$

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

| $\circ$ | $\bar{1}$ |
|---|---|
| $\bar{1}$ | $\bar{1}$ |

2) $(\mathbb{Z}_3, \oplus, \odot)$ $\qquad (\mathbb{Z}_3, \oplus, \odot)$ ist Körper!

| $\circ$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{1}$ |

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

3) $(\mathbb{Z}_n, \oplus_n, \odot_n)$ Ring mit Eins "Sind Körper $\Leftrightarrow$ $n$ ist eine Primzahl."

$n \in \mathbb{N}$

**Lemma 4.25** Sei $(\mathbb{K}, +, \cdot)$ Körper

Dann besitzt das neutrale Element der Add. ($\mathbb{0}$) kein multiplikatives Inverses.

**Beweis:** Es ex. kein $x \in K$ mit $x \cdot \mathbb{0} = \mathbb{1}$

$\forall a \in K \quad a \cdot \mathbb{0} = \mathbb{0}$

$$
\begin{aligned}
a \cdot \mathbb{0} &= (a \cdot \mathbb{0}) + \mathbb{0} && (\mathbb{0} \text{ neutrale Element bzgl. Addi}) \\
&= (a \cdot \mathbb{0}) + ((a \cdot \mathbb{0}) + (-(a \cdot \mathbb{0}))) && (\text{add. Inverse zu } (a \cdot \mathbb{0})) \\
&= \underline{((a \cdot \mathbb{0}) + (a \cdot \mathbb{0}))} + (-(a \cdot \mathbb{0})) && (\text{Assoz. von } +) \\
&= \underline{(a \cdot (\mathbb{0} + \mathbb{0}))} + (-(a \cdot \mathbb{0})) && (\text{Distributivgesetz}) \\
&= (a \cdot \mathbb{0}) + (-(a \cdot \mathbb{0})) && (\text{neutrales Element der Add. } \mathbb{0}) \\
&= \mathbb{0} && (\text{add. Inverses zu } (a \cdot \mathbb{0}) \text{ war } -(a \cdot \mathbb{0})) \quad \square
\end{aligned}
$$

Nur Ringeigenschaften verwendet!

**Theorem 4.26** $(\mathbb{Z}_n, \oplus_n, \odot_n)$ ist Körper $\Longleftrightarrow$ $n$ Primzahl.

**Beweis:** $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{n-1}\}$

$(\mathbb{Z}_n, \oplus_n)$ abelsche Gruppe. Distributivität etc. erfüllt.

Nur die multiplikativen Inverse sind wichtig!

1. "$\Longleftarrow$" $n$ ist Primzahl $n = p$

Zeige: Sei $1 \leq \underline{a} \leq p-1$

$\Rightarrow \overline{a}$ hat multiplikative Inverse.

**Lemma 4.24** $a, b \in \mathbb{Z}$ **teilerfremd** $(x \mid a$ und $x \mid b \Rightarrow x = 1)$

$\Rightarrow$ es ex. $x, y \in \mathbb{Z}$ mit $a \cdot x + b \cdot y = 1$

Bsp

Lemma 4.24

$10, 17$ ($a$, $p$)

$\underset{x}{10 \cdot (-5)} + \underset{y}{17 \cdot 3} = 1$

$\overline{-5}$ ist Inverses zu $\overline{10}$

$\overline{-5} = \overline{12}$ in $\mathbb{Z}_{17}$

$\overline{12} \cdot \overline{10} = \overline{1}$

---

klar: $a, p$ teilerfremd $\Rightarrow$ (Lemma 4.24)

$\exists\, x, y \in \mathbb{Z} \quad a \cdot x + p \cdot y = 1$

Betrachte das modulo $p$

$a \cdot x \equiv_p a \cdot x + 0 \equiv_p a \cdot x + p \cdot y$

$\equiv 1 \mod p$ ✓ $\square$ (1. Teil)

2. "$\Rightarrow$"

$\ulcorner (A \Rightarrow B) \Leftrightarrow \underline{(\neg B \Rightarrow \neg A)} \lrcorner$

<u>Also:</u> $n$ keine Primzahl

$n = 1 \Rightarrow \mathbb{Z}_1 = \{\overline{0}\}$

$n > 1 \Rightarrow n \geq 4 \qquad n = a \cdot b \qquad a, b \in \{2, 3, 4, \ldots\}$

<u>Ann:</u> $(\mathbb{Z}_n, \oplus_n, \odot_n)$ ist Körper $\Rightarrow$ $\underline{a}$ und $\underline{b}$ invertierbar

$\Rightarrow$ $a \cdot b$ invertierbar $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

gezeigt

aber $\overline{a \cdot b} = \overline{n} = \overline{0}$ ist nicht invertierbar! ↯

$\Rightarrow$ ~~entweder~~ a oder b nicht invertierbar.

$\square$

BSP $\left(\mathbb{Z}_2, \underset{n}{\oplus}, \underset{n}{\odot}\right)$ Körper $\qquad \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$$\mathbb{Z}_2^{2\times 2} := \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\middle|\; a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{Z}_2 \right\}$$

$\oplus$, $\odot$ definieren für $\mathbb{Z}_2^{2\times 2}$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \oplus \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$\left(\mathbb{Z}_2^{2\times 2}, \oplus\right)$ abelsche Gruppe $\mathbb{0} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}$ neutrales Element

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \odot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} (a_{11} \cdot b_{11}) + (a_{12} \cdot b_{21}) & (a_{11} \cdot b_{12}) + (a_{12} \cdot b_{22}) \\ (a_{21} \cdot b_{11}) + (a_{22} \cdot b_{21}) & (a_{21} \cdot b_{12}) + (a_{22} \cdot b_{22}) \end{pmatrix}$$

12

$\begin{pmatrix} \bar{1} & 0 \\ 0 & \bar{1} \end{pmatrix}$ neutrales Element $\qquad \left(\mathbb{Z}_2^{2\times 2} \setminus \mathbb{O}, \odot\right)$

<u>Einheiten</u> $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} = M$

$\left(\mathbb{Z}_2^{2\times 2}, \oplus, \odot\right)$ $\qquad (M, \odot)$ Gruppe mit $\begin{pmatrix} \bar{1} & 0 \\ 0 & \bar{1} \end{pmatrix}$ als neutrales Element

$$\underline{(-a) \overset{?}{=} (-1)\cdot a}$$