

Lineare Algebra I

für die Fachrichtung Informatik

Wintersemester 2023/24

$$\mathbb{Z}$$

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{Komm. Gruppe}$$

$$\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{Monoid}$$

$$(x + y)z = xz + yz \quad \text{Distributivgesetz}$$

Def. 3.3.1 (Ringe)

$(R, +, \cdot)$ heißt **Ring**, falls

- (i) $(R, +)$ ist kommutative Gruppe
- (ii) $(R, \cdot)$ ist Monoid
- (iii) $\forall x, y, z \in R: \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
und $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$

$(R, +, \cdot)$ heißt **kommutativer Ring**, wenn $(R, \cdot)$ kommutativ.

Das Neutralelement der additiven Gruppe $(R, +)$

wird mit $0_R = 0$ bezeichnet.

Das Inverse von $x \in R$ bzgl. $+$ wird mit $\boxed{-x}$ bezeichnet.

Das Neutralelement des multiplikativen Monoids $(R, \cdot)$

wird mit $1_R = 1$ bezeichnet.

$x \in R$ heißt **invertierbar**, wenn x multiplikativ invertierbar ist.

$R^\times = (R, \cdot)^\times$ Einheitengruppe von $(R, +, \cdot)$

x^{-1} multiplikative Inverse.

Notation:

$R = (R, +, \cdot)$

$G = (G, *)$

Beispiele: $(\mathbb{R}, +, \cdot)$ komm. Ring mit $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

$(\mathbb{Q}, +, \cdot)$ komm. Ring mit $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

$(\mathbb{Z}, +, \cdot)$ komm. Ring mit $\mathbb{Z}^\times = \{-1, 1\}$

Lemma 2.2.12 $\Rightarrow (\mathbb{R}^{n \times n}, +, \cdot)$ Ring $GL(n, \mathbb{R}) := (\mathbb{R}^{n \times n}, \cdot)^\times$ allgemeine lineare Gruppe

$m \neq n$ $(\mathbb{R}^{m \times n}, +, \cdot)$ $\because \mathbb{R}^{m \times n} \times \mathbb{R}^{m \times n} \rightarrow \mathbb{R}^{n \times n}$ kein Ring!

$(\mathbb{N}, +, \cdot)$ kein Ring, weil $(\mathbb{N}, +)$ kein Neutralelement hat

$(\mathbb{N}_0, +, \cdot)$ kein Ring, weil $(\mathbb{N}_0, +)$ keine Gruppe ist.

$(2\mathbb{Z}, +, \cdot) = (\{\dots, -4, -2, 0, 2, 4, \dots\}, +, \cdot)$ kein Ring, weil $(2\mathbb{Z}, \cdot)$ kein Neutralelement hat.

$\{0\}$ komm. Ring „Nullring“ $0_R = 0 = 1_R$

Lemma 3.3.4: $(R, +, \cdot)$ Ring $x \in R$.

$$(a) \quad 0 \cdot x = 0 = x \cdot 0$$

$$(b) \quad -x = (-1) \cdot x = x \cdot (-1)$$

Bw: (a) $x \in R$

$$f: \begin{pmatrix} R \longrightarrow R \\ y \longmapsto y \cdot x \end{pmatrix}$$

Rechtsmultiplikation mit x .

Distr.gesetz

$$f(y_1 + y_2) = (y_1 + y_2) \cdot x \stackrel{\text{Distr.gesetz}}{=} y_1 \cdot x + y_2 \cdot x = f(y_1) + f(y_2)$$

$$\Rightarrow f: (R, +) \longrightarrow (R, +) \text{ Gruppenhomo}$$

$$\Rightarrow f(0) = 0$$

$$\Rightarrow 0 \cdot x = 0$$

$$\text{Analog: } x \cdot 0 = 0$$

$$f(-y) = -f(y)$$

$$(-y) \cdot x = -(y \cdot x)$$

Inbesondere $y = 1_R = 1 = \text{Neutralement von } (R, \cdot)$.

$$(-1) \cdot x = -(1 \cdot x) = -x.$$

□

Notation:

a

$n \in \mathbb{N}$

$$\boxed{(0_R)^0 = 1_R}$$

$$na = \underbrace{a + \dots + a}_n$$

$$a^n = \underbrace{a \cdot \dots \cdot a}_n$$

$$0a = 0_R$$

$$a^0 = 1_R$$

$$\Rightarrow a^{m+n} = a^m \cdot a^n$$

$$(m+n)a = ma + na$$

Achtung:

$$(ab)^2 \neq a^2 b^2$$

$$(a+b)^2 \neq a^2 + 2ab + b^2$$

$$(ab)^2 = abab$$

$$\boxed{(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2}$$

Def: $(R, +, \cdot)$ Ring

$T \subseteq R$ heißt Unterring, wenn

(i) T ist Untergruppe von $(R, +)$

(ii) $1_R \in T$

(iii) T ist abgeschlossen unter $\cdot$, d.h. $\forall a, b \in T \quad a \cdot b \in T$

T Unterring von R

$\Rightarrow (T, +, \cdot)$ Ring mit $0_T = 0_R$
 $1_T = 1_R$.

z.B. $\mathbb{Z}$ Unterring von $\mathbb{Q}$, $\mathbb{Q}$ Unterring von $\mathbb{R}$.

$\{0\}$ kein Unterring von $\mathbb{Z}$, weil $1 = 1_{\mathbb{Z}} \notin \{0\}$.

z.B.: $(\mathbb{R}, +, \cdot) = (\mathbb{R}^{2 \times 2}, +, \cdot)$

(a) $C = \left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{R} \right\}$ ist Unterring von $\mathbb{R}^{2 \times 2}$.

(b) $\mathbb{Z}^{2 \times 2} = \left\{ \begin{pmatrix} k & l \\ m & n \end{pmatrix} \mid k, l, m, n \in \mathbb{Z} \right\}$ ist Unterring von $\mathbb{R}^{2 \times 2}$.

(c) $N = \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$ kein Unterring,
weil N kein Neutralelement für $\cdot$ hat.

(d) $T = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$ ist bzgl. $+$, $\cdot$ Ring,
ABER kein Unterring von $\mathbb{R}^{2 \times 2}$
 $1_T \neq 1_{\mathbb{R}} = 1_{2 \times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Def: 3.3.8 (Ringhomomorphismus)

$$(R, +, \cdot)$$

$(T, +, \cdot)$ Ringe

$f: R \rightarrow T$ heißt **Ringhomomorphismus**, wenn

$$\bullet f(x +_R y) = f(x) +_T f(y) \quad (\Rightarrow \begin{matrix} f(0) = 0 \\ f(-x) = -f(x) \end{matrix})$$

$$\bullet f(x \cdot y) = f(x) \cdot f(y)$$

$$\bullet f(1_R) = 1_T$$

Ring Iso

Ring Endo

Ring Auto

analog wie bei Gruppen.

$$(R, +, \cdot) \underset{\text{Ring}}{\simeq} (T, +, \cdot), \text{ wenn } \exists f: R \rightarrow T \text{ Ringisomorph.}$$

z.B.: $T = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$ Ring, Unterring von $\mathbb{R}^{2 \times 2}$.

$$f: (\mathbb{R}, +, \cdot) \longrightarrow (T, +, \cdot) \quad \text{Ringisomorphismus}$$
$$\alpha \longmapsto \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

$$T \cong_{\text{Ring}} \mathbb{R}.$$

Lemma 3.3.9: $\varphi: (\mathbb{R}, +, \cdot) \longrightarrow (T, +, \cdot)$ Ringhomo.

(a) $U \in \mathbb{R} \text{ Unterring} \Rightarrow \varphi(U) \in T \text{ Unterring.}$

$$\text{Bild}(\varphi) = \varphi(\mathbb{R}) \text{ Unterring.}$$

(b) $W \subseteq T \text{ Unterring} \Rightarrow \varphi^{-1}(W) \subseteq \mathbb{R} \text{ Unterring.}$

$$\ker \varphi := \{x \in R \mid \varphi(x) = 0_T\} \quad \text{Kern von } \varphi \\ = \varphi^{-1}(\{0\})$$

ist i. A. kein Untertring von R , weil $1_R \notin \ker \varphi$.

Def 3.3.11 (Körper)

Ein Ring $(K, +, \cdot)$ heißt Körper, wenn

(i) $(K, \cdot)^{\times} = K \setminus \{0\}$

(ii) $(K, \cdot)$ kommutativ

z.B.: $(\mathbb{R}, +, \cdot)$ Körper

$(\mathbb{Q}, +, \cdot)$ Körper

$(\mathbb{Z}, +, \cdot)$ kein Körper!

$(\mathbb{R}^{n \times n}, +, \cdot)$ kein Körper für $n \geq 2$.

$(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}/p\mathbb{Z} \mid p \text{ prim})$

$$a - b = a + (-b)$$

$$\frac{a}{b} = a b^{-1} = b^{-1} a$$

$$(a+b)(a-b) = a^2 - b^2.$$

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^n = \text{bin. Lehrsatz.}$$

Anmerkung:

Ein Ring $(K, +, \cdot)$ heißt **Divisionsring**, wenn

$$(i) \quad (K, \cdot)^{\times} = K \setminus \{0\}$$

K Körper $\Leftrightarrow K$ komm. Divisionsring.

Beispiel für nichtkomm. Divisionsring: Quaternionen

$$R = \{0\}$$

$R^\times = \{0\}$ ist kein Körper, weil $R^\times \neq R \setminus \{0\} = \emptyset$.

K Körper

$0_K \neq 1_K$
↑
niemals
invertierbar
bzgl.
↑
invertierbar

$$K^\times = K \setminus \{0\}$$

Kann man auf $\{0, 1\}$ eine Körperstruktur definieren?

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

$$1 + 1 = 0$$

Man kann

nachrechnen, das ist ein Körper

$$\mathbb{F}_2 := (\{0, 1\}, +, \cdot)$$

$\left(\begin{array}{l} \text{GF}(2) \\ \text{Galois-field} \end{array} \right)$

Auf $\mathbb{F}_4 = \{0, 1, A, B\}$ kann man auch eine Körper-Struktur def.

+	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

.	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

Frage: Auf welchen endl. Mengen gibt es
Körperstrukturen?

Antwort: 2, 3, 4, 5, 7, 8, 9, 11, 13, ...

$\forall q \in \mathbb{N} :$

$\exists \text{ Körper } K \text{ mit } K = q$
$\longleftrightarrow$
$q \text{ ist eine Primzahlpotenz}$

(werden wir nicht beweisen)

Notation: L Körper

$K \subseteq L$ Unterkörper

$\Leftrightarrow$

K Unterring
K Körper

L Körpererweiterung von K

$\varphi: K \longrightarrow L$ Körperhomo.

$\Leftrightarrow \varphi$ Ringhomo. zwischen K und L .

Bem: Ein Körperhomomorphismus ist immer injektiv.

Bw: Übungsaufgabe

$\mathbb{R}$ Körpererw. von $\mathbb{Q}$

$\mathbb{F}_4$ Körpererw. von $\mathbb{F}_2$