II Ringe & Körper

9. Definitionen und Beispiele

[Die Signatur von Ringen und Körpern ist $\mathcal{L} = \{0, 1, +, \cdot\}$ — wir betrachten nur Ringe mit 1; $0, 1$: Konst. Symb.; $+, \cdot$: binäre Fkt.-Symbole]

Def. • Die Struktur $(R, 0, 1, +, \cdot)$ ist ein **Ring**, falls $(R, 0, +)$ eine abelsche Gruppe ist, $(R, 1, \cdot)$ ein Monoid ist (d.h. $\cdot$ ist assoz., "1" ist Neutralelement), und die Distributivgesetze gelten:

("sesqui-Gruppe")

$$\forall a, b, c \in R \left(a \cdot (b+c) = (a \cdot b) + (a \cdot c) \wedge (a+b) \cdot c = (a \cdot c) + (b \cdot c) \right)$$

• Ein Ring $R = (R, 0, 1, +, \cdot)$ ist **kommutativ** falls die Operation $\cdot$ kommutativ ist.

• Die Struktur $(F, 0, 1, +, \cdot)$ ist ein **Körper** (field) falls $(F, 0, +)$ und $(F \setminus \{0\}, 1, \cdot)$ abelsche Gruppen sind und das Distributivgesetz gilt:

("doppel-Gruppe")

$$\forall a, b, c \in F \left(a \cdot (b+c) = (a \cdot b) + (b \cdot c) \right)$$

[Schiefkörper]

Bem. • Die 1 in einem Ring ist eindeutig. $1 \cdot 1' = \begin{cases} 1 \text{ wegen } 1' \\ 1' \text{ wegen } 1 \end{cases}$

• Ist in einem Ring $1 = 0$, so ist $R = \{0\}$ der triviale Ring.

• $\{0\}$ ist kein Körper, d.h. in einem Körper gilt immer $1 \neq 0$.

Beispiele für Ringe:

• $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ • $\mathrm{Mat}(n, \mathbb{R})$ ist für $n \geq 2$ ein nicht-kom. Ring

• Für $m \in \mathbb{Z}$ ist $\mathbb{Z}/m\mathbb{Z}$ ein Ring; $\bar{a} := a + m\mathbb{Z}$ (für $a \in \mathbb{Z}$)

Beispiele für Körper:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{Z}/2\mathbb{Z}$, allg. $\mathbb{Z}/p\mathbb{Z}$ für p prim (später)

Rechenregeln für Ringe und Körper:

(1) für alle a: $0 \cdot a = a \cdot 0 = 0$

(2) für alle a, b: $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$

(3) für alle a, b: $(-a) \cdot (-b) = a \cdot b$

(4) $\left(\sum_{i=1}^{m} a_i\right) \cdot \left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i \cdot b_j$

Bew. (1) $0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a) \Rightarrow 0 \cdot a = 0$ [analog $a \cdot 0 = 0$]

(2) $(-a) \cdot b + (a \cdot b) = (-a + a) \cdot b = 0 \cdot b = 0 \Rightarrow (-a) \cdot b = -(a \cdot b)$

(3) $(-a) \cdot (-b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b$ [analog $a \cdot (-b) = -(a \cdot b)$]

(4) mit Induktion (Distributivges.) ⊣

Def. Ist R ein Ring und $S \subseteq R$, dann ist S ein Unterring von R falls S abgeschlossen ist bzgl. Add. & Mult., $0, 1 \in S$ und $(S, 0, 1, +, \cdot)$ ein Ring ist.

Bsp.

- $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sind Unterringe von $\mathbb{C}$; $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
- Der Ring der Gauss'schen Zahlen

$$\mathbb{Z}[i] := \{(a + ib) : a, b \in \mathbb{Z}\}$$

ist ein Unterring von $\mathbb{C}$. Allg. ist für $a \in \mathbb{C}$, $\mathbb{Z}[a]$ der kl. Unterring von $\mathbb{C}$ welcher $\mathbb{Z}$ und a enthält.

Def. Ein Ringhomomorphismus zwischen zwei Ringen R und S ist eine Abbildung $\varphi : R \to S$ für die gilt:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$\Rightarrow \varphi(0_R) = 0_S$ und $\varphi(-a) = -\varphi(a)$

(iii) $\varphi(1_R) = 1_S$ [für $S \neq \{0\}$ ist $\varphi[R] \neq \{0_S\}$]

Faktum 9.1 Ist $\varphi: R \to S$ ein Ringhomom. so ist $\varphi[R]$ ein Unterring von S.
$:= \{\varphi(a) : a \in R\}$

Beweis:
- $\varphi[R] \leq S$ ist eine additive Untergruppe von S.
- $\varphi[R]$ ist bzgl. Multiplikation abgeschlossen.
- die Distr.-gesetze gelten
- $1_S \in \varphi[R]$. ⊣

Bsp. Die kanonische Projektion $\pi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$
$a \mapsto \bar{a} := a + m\mathbb{Z}$
ist ein Ringhomomorphismus. $\left[\overline{a+b} = \bar{a}+\bar{b}\ ;\ \overline{a\cdot b} = \bar{a}\cdot\bar{b}\right]$
wird klar mit "Idealen"

Def. Sei R ein Ring
- Ein Element $a \in R$ heißt Linksnullteiler, falls ein $b \in R$, $b \neq 0$ existiert mit $\boxed{a \cdot b = 0}$ (analog Rechtsnullteiler: $b \cdot a = 0$).
- R heißt nullteilerfrei falls R keine nicht-trivialen (d.h. von 0 versch.) Links- oder Rechtsnullteiler besitzt.
- Ein nicht-trivialer, kommutativer, nullteilerfreier Ring heißt Integritätsring oder Integritätsbereich.

Bsp.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, also Integritätsringe
- $\mathbb{Z}[i]$ ist ein Integritätsring
- $\mathbb{Z}/p\mathbb{Z}$ für p prim ist ein Integritätsring

Unbeispiele
- $\mathbb{Z}/m\mathbb{Z}$ für m nicht prim ist kein Integritätsring $\left[\begin{array}{l} m = 15; \\ \bar{3}\cdot\bar{5} = \bar{0} \end{array}\right]$
- $\mathrm{Mat}(n, \mathbb{R})$ besitzt für $n \geq 2$ Nullteiler [Projektionen]

Bem.
- Jeder Körper ist ein Integritätsring aber nicht umgekehrt.
- Wir werden später sehen, dass sich jeder Integritätsring zu einem Körper erweitern lässt. Beachte: Integritätsringe sind kommutativ.

Def. Sei R ein Ring.

- Ein Element $a \in R$ heisst **Einheit**, falls Elemente $b, c \in R$ existieren mit $a \cdot b = 1_R = c \cdot a$. [$a$ ist invertierbar]

[Beh.] - $R^* := \{a \in R : a \text{ ist Einheit}\}$ ist eine Gruppe bzgl. Multiplikation, die sogenannte **Einheitengruppe** von R. [d.h. die Gruppe der invertierbaren Elemente]

Bew. - Um zu zeigen, dass $(R^*, 1, \cdot)$ eine Gruppe ist, zeigen wir zuerst, dass gilt: $(a \cdot b = 1 \wedge c \cdot a = 1) \rightarrow b = c$

$$b = \underbrace{(a \cdot b)}_{=1} \cdot b = \underbrace{(c \cdot a)}_{=1} \cdot b = c \cdot \underbrace{(a \cdot b)}_{=1} = c$$

d.h. $b = c = a^{-1}$ ist Links- und Rechts-inverses von a. [$\Rightarrow$ eindeutig!]

- Seien $a, b \in R^*$, so ist $(a \cdot b^{-1}) \cdot (b \cdot a^{-1}) = a \cdot a^{-1} = 1$, d.h. $a \cdot b^{-1} \in R^*$. ⊣

[**Bem.** Ist $R^* = R \setminus \{0\}$ und R nicht-komm., so ist R ein Schiefkörper.]

Bsp:

- $\mathbb{Z}^* = \{-1, 1\} \cong C_2$
- $(\mathbb{Z}/10\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} \cong C_4$
- $\mathbb{Z}[i]^* = \{-1, 1, -i, i\} \cong C_4$, $\mathbb{Z}[i] = \langle i \rangle$ notwendige Bed.: ggT = 1
- $(\mathbb{Z}/15\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$ [Erinnerung: Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ "Grundstrukturen"]
  $\cong C_2 \times C_4$ Inverse: $\bar{8}, \bar{4}, \bar{13}, \bar{2}, \bar{11}, \bar{7}, \bar{14}$

Def. Seien $R_1, \ldots, R_n$ Ringe. Die **direkte Summe** $R_1 \oplus \ldots \oplus R_n$ ist wie folgt definiert: $R_1 \oplus \ldots \oplus R_n$ ist die Menge $R_1 \times \cdots \times R_n$ mit komponentenweiser Addition und Multiplikation; es ist $0 = (0_{R_1}, \ldots, 0_{R_n})$ und $1 = (1_{R_1}, \ldots, 1_{R_n})$.

Faktum: Sind $R_1, \ldots, R_n$ Ringe, so ist $R_1 \oplus \ldots \oplus R_n$ auch ein Ring.

Bsp. $\mathbb{R} \oplus \mathbb{R}$ ist ein Ring aber kein Körper; warum? (auch kein Integritätsring)