Teil II: Ringe (und Moduln)

A10: Ringe: Definitionen und Beispiele

10.1. Einleitung: Ring: $\underbrace{"+"}$, $\underbrace{"\cdot"}$ } Distr. gesetze
neutr. El.: 0   1 $\rightsquigarrow$ Einheitengruppe $R^\times$

10.2. Def.: R Ring $:\Leftrightarrow$ R Menge, $\exists$ Verknüpfungen $+, \cdot : R \times R \to R$ $\exists\, 0, 1 \in R$:
$\rightsquigarrow R \neq \emptyset$

$\forall a, b, c \in R$:

$(R, +, 0)$ ab. Gruppe:
- (1) $(a+b)+c = a+(b+c)$
- (2) $0 + a = a$
- (3) $\exists\, a' : a' + a = 0$ $\rightsquigarrow a' = -a$,
- (4) $a + b = b + a$ $\to$ entbehrlich, folgt aus anderen Axiomen $\hookrightarrow$ LA I, L 7.16 (i)

$(R, \cdot, 1)$ Halbgruppe mit 1:
- (5) $(ab)c = a(bc)$
- (6) $1a = a1 = a$

Distributivgesetze:
- (7) $a \cdot (b+c) = ab + ac$
- (8) $(a+b) \cdot c = ac + bc$

R Kommutativer Ring $:\Leftrightarrow$ zusätzlich: (9) $ab = ba$

R Integritätsbereich $:\Leftrightarrow$ $R \neq \{0\}$ Komm. Ring mit zusätzlich:
Kurz: IB   ($\{0\}$: trivialer Nullring, wo $0 = 1$)   (10) $ab = 0 \Rightarrow (a = 0 \vee b = 0)$

10.3. Bsp.:
- Körper sind Integritätsbereiche
- $\mathbb{Z}$ ist Integritätsbereiche
- $\mathbb{Z}/15\mathbb{Z}$ ist kein IB, da $\underbrace{\underline{3}}_{\neq 0} \cdot \underbrace{\underline{5}}_{\neq 0} = \underline{15} = \underline{0}$
- $\mathbb{Z}/5\mathbb{Z}$ ist IB, sogar Körper
- $\{0\}$ mit $0 = 1$ heißt Nullring, ist per Def. kein IB

10.4. Bsp.: K Körper, $n \geq 1$. Dann: $K^{n \times n}$ = Ring der $(n \times n)$-Matrizen.
(Ab $n \geq 2$ ist $K^{n \times n}$ nicht komm.)

Sei V n-dim. K-VR, dann $\operatorname{End}(V) \cong K^{n \times n}$:   Ring-Iso: $M_A(f+g) = M_A(f) + M_A(g)$
(A sei Basis von V, M_A = Matrixdarst. bzgl. A) $f \mapsto M_A(f)$, $M_A(f \circ g) = M_A(f) \cdot M_A(g)$

→ „Produktring"

10.5. Bsp.: Seien $R_1, \ldots, R_m$ Ringe. Dann $R_1 \times \ldots \times R_m$ Ring bzgl. komponentenweise Add. und Mult.

$$(a_1, \ldots, a_m) \overset{+}{\cdot} (b_1, \ldots, b_m) := (a_1 \overset{+}{\cdot} b_1, \ldots, a_m \overset{+}{\cdot} b_m)$$

mit $\underline{0} := (0_1, \ldots, 0_m)$, $\underline{1} := (1_1, \ldots, 1_m)$.

$R_1, \ldots, R_m$ komm. $\Leftrightarrow$ $R_1 \times \ldots \times R_m$ komm.

10.6. Bsp.: Sei $I \subseteq \mathbb{R}$ ein Intervall, $\mathcal{C}(I, \mathbb{R})$ die Menge der reellwertigen stetigen Funktionen, ist komm. Ring: $\forall x \in I$:

$(f+g)(x) := f(x) + g(x)$, $(f \cdot g)(x) := f(x) \cdot g(x)$,

$0(x) := 0$, $1(x) := 1$.

10.7. Def.: Sei R Ring. Ein El. $a \in R$ heißt linker (bzw. rechter) Nullteiler

$:\Leftrightarrow \exists b \neq 0$ mit $a \cdot b = 0$ (bzw. $b \cdot a = 0$)

("teilt die 0 von li/re")

10.8. Bsp.: $\mathbb{Z} \times \mathbb{Z}$ hat Nullteiler: $(1,0) \cdot (0,1) = (0,0) = \underline{0}$

⌜vgl. Konstruktion von $\mathbb{C} := \mathbb{R} \times \mathbb{R}$⌟

10.9. Bem.: Nach 10.2 (1)–(4) ist $(R, +, 0)$ ab. Gruppe.

Daher ist für $n \in \mathbb{N}$: na bzw. $-a$ bzw. $(-n)a$ def.

10.10. Bem.: Sei $e \in R$ mit $ea = ae = a$ für alle $a \in R$. Dann: $e = 1$,

da: $e = e \cdot 1 = 1$.

Rechenregeln:
$$a \cdot 0 = 0 \cdot a = 0$$
$$(-a) \cdot b = a \cdot (-b) = -(ab)$$
$$(-a) \cdot (-b) = a \cdot b \quad \leftarrow \text{„Minus mal Minus gibt Plus"}$$

→ vgl. LA I, L4.16 (ii)–(iv).

$$\left[\, a * b = a * c \Rightarrow b = c \quad \Leftarrow \; a^{-1} * a * b = a^{-1} * a * c \,\right]$$

10.11. Def.: Sei $m \in \mathbb{Z}$. Dann: $m_R := m \cdot 1_R$ mit 1_R Eins im Ring R.

⌜$2_R := 1_R + 1_R = 2 \cdot 1_R$⌟

10.12. Bem.: $\forall a \in R$: $\underset{\in R}{m_R} \cdot \underset{\in R}{a} = \underset{m \in \mathbb{N}}{m \cdot a}$. ⌜✓⌟

$m \cdot a = (\underbrace{a + \ldots + a}_{m\text{-mal}})$

10.13. Bem.: In komm. Ringen gilt: $(a+b)^n = \sum_{i=0}^{n} \underbrace{\binom{n}{i}}_{\in \mathbb{N}} \cdot \underbrace{a^i b^{n-i}}_{\in R}$
⌜Bew. s. früher⌟
nicht aber in nichtkomm. Ringen!
⌜wo $ab \neq ba$⌟

10.14. Def.: $u \in R$ Einheit $:\Leftrightarrow \exists v \in R: uv = vu = 1$ {"invertierbares El. bzgl. ·"}
$R^\times := \{u \in R;\ u \text{ Einheit}\}$ Einheitengruppe von R.

10.15. Bem.: $R^\times$ ist Gruppe (bzgl. ·)
Bew.: * Abgeschl. bzgl. ·: $u_1, u_2 \in R^\times \Rightarrow \exists v_1, v_2 \in R$: $u_1 v_1 = v_1 u_1 = 1$, $u_2 v_2 = v_2 u_2 = 1$
$\Rightarrow (v_2 v_1)(u_1 u_2) = v_2 \underbrace{(v_1 u_1)}_{=1} u_2 = 1 = (u_1 u_2)\cdot(v_2 v_1)$.
$\hookrightarrow \underline{(u_1 u_2)^{-1}} = v_2 v_1 = \underline{u_2^{-1}} \cdot \underline{u_1^{-1}}$.

* Ex. des Inversen:
$u \in R^\times \Rightarrow \exists v \in R: vu = uv = 1 \Rightarrow v \in R^\times$ Inv. von u ⌜$u^{-1} := v$⌟
* $1 \in R^\times$: $1 \cdot 1 = 1$ □

10.16. Bsp.: $\mathbb{Z}^\times = \{1, -1\}$ $(\cong C_2)$
$K^\times = K \setminus \{0\}$ $(= K^*)$, K Körper

10.17. Bsp.: $(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times$.
Bew.: $(u_1, \ldots, u_n) \in (R_1 \times \ldots \times R_n)^\times$
$\Leftrightarrow \underbrace{(v_1, \ldots, v_n)\cdot(u_1, \ldots, u_n)}_{=(v_1 u_1, \ldots, v_n u_n)} = \underline{1} = (1, \ldots, 1)$
$\Leftrightarrow u_1 \in R_1^\times, \ldots, u_n \in R_n^\times$. □

10.18. Def.: Ring $R \neq \{0\}$ mit $R^\times = R \setminus \{0\}$, d.h. jedes El. $\neq 0$ ist Einheit, heißen Schiefkörper (auch: Divisionsringe)

10.19. Bem.: Körper sind also komm. Schiefkörper.

A 11: Ideale, Faktorringe, Homomorphismen

11.1. Einl.: Ideale = Unterstrukturen von Ringen $\rightsquigarrow$ Faktorringe, Ringhom./Hom.sätze

11.2. Def.: R Ring, $I \subseteq R$ heißt **Ideal** $:\Leftrightarrow$

(1) $0 \in I$,

(2) $\forall a, b \in I: \ a + b \in I$

(3) $\forall a \in I \ \forall b \in R: \ ab, ba \in I$.

$\hat{=}$ "Abgeschl. bzgl. der Mult. mit bel. Ringelementen"

11.3. Bem.: I ist UG der add. Gr. von R

11.4. Bem.: $\underbrace{\{0\}}_{=0 \text{ Nullideal}}, R$ sind Ideale in R.

(3_{rechts}): $\forall a \in I \ \forall b \in R: ab \in I \to I$ Rechtsideal

(3_{links}): $\forall a \in I \ \forall b \in R: ba \in I \to I$ Linksideal

11.5. Bem.: Die Ideale in $\mathbb{Z}$ sind genau die UG $\mathbb{Z}r$, $r \in \mathbb{Z}$.

11.6. Bem.: Sei $I \subseteq R$ Ideal. Äquivalent sind:

(1) $I = R$, (2) $1 \in I$, (3) $I \cap R^\times \neq \emptyset$ ⌜d.h. I enthält Einheiten⌟

Bew.: (1) $\Rightarrow$ (2) $\Rightarrow$ (3): ✓, (3) $\Rightarrow$ (1): Sei $u \in I \cap R^\times \Rightarrow \exists v \in R: \underbrace{vu}_{\in I} = 1$

$\underset{\text{wegen 11.2.(3)}}{\Rightarrow} 1 \in I \Rightarrow \underbrace{1 \cdot R}_{=R} \subseteq I$. □

11.7. Bem.: K Körper $\Rightarrow 0, K$ einzige Ideale ⌜11.6 ✓⌟

Bsp.:
- $I = 2\mathbb{Z}$ ist kein Ideal in $R = \mathbb{Z}[T]$ ⌜da $\underbrace{2}_{\in I} \cdot \underbrace{T}_{\in R} \notin 2\mathbb{Z} = I$⌟
- $I = (2\mathbb{Z})[T]$ ist Ideal in $R = \mathbb{Z}[T]$

11.8. Bem.: Ideale in $R_1 \times \ldots \times R_m$ sind genau die $I_1 \times \ldots \times I_m$, mit $I_j \subseteq R_j$ Ideale $(1 \leq j \leq m)$.

Bew.: Sei $R := R_1 \times \ldots \times R_m$, $I \subseteq R$ Ideal. Sei $I_j := \underset{j\text{-te Proj.}}{\pi_j}(I)$

Beh.: $I = I_1 \times \ldots \times I_m$, I_j Ideale.

Bew.: „$\subseteq$": ✓, „$\supseteq$": Zeige nur: $I \overset{?}{\supseteq} \{0\} \times \ldots \{0\} \times I_j \times \{0\} \times \ldots \times \{0\}$

$= (0, \ldots, 0, i_j, 0, \ldots, 0)$

⌜Sei $i_j \in I_j \Rightarrow \exists (i_1, \ldots, i_{j-1}, \underset{j\text{-te Stelle}}{i_j}, \ldots, i_m) \in I$. Dann: $(0, \ldots, 0, 1, 0, \ldots 0) \cdot (i_1, \ldots, i_j, \ldots, i_m) \in I$. □