Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil II: RINGE (und Moduln)

A11: Ideale, Faktorringe, Homomorphismen

Stichworte: Ideal, Ideale in $R_1 \times \dots \times R_n$, Schnitt und Summe von Idealen, Faktorring R/I, Faktorringe von $\mathbb{Z}$, Ringhomomorphismus, Urbilder und Kerne sind Ideale (Bilder nur bei surj. R-Hom.), Einheiten werden auf Einheiten abgebildet, Homomorphiesatz, Isomorphiesätze, Primring, Charakteristik

---

11.1. Einleitung: Als geeignete Unterstrukturen von Ringen erhält man deren Ideale. Wir führen damit den Faktorring ein und untersuchen das Verhalten von Idealen unter Ringhomomorphismen. Wie für Gruppen gilt der Homomorphiesatz / Isomorphiesätze für Ringe. Wir führen noch den Primring und die Charakteristik eines Ringes ein.

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

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

11.4. Bem.: 0, R sind Ideale in R.

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

11.6. Bem.: Sei $I \subseteq R$ Ideal. Äquivalent sind: (1) $I = R$
(2) $1 \in I$
(3) $I \cap R^\times \neq \emptyset$

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

11.7. Bem.: K Körper $\Rightarrow$ 0, K einzige Ideale.

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

Bew.: Sei $R := R_1 \times \dots \times R_m$, $I \subseteq R$ Ideal, $I_j := \pi_j(I)$.

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

Bew.: „$\subseteq$": Klar nach der Def. des I_j.

„$\supseteq$": Zeige nur: $I \supseteq \{0\} \times \dots \times \{0\} \times I_j \times \{0\} \times \dots \times \{0\}$: (I_j an j-te Stelle)

Sei $i_j \in I_j$ (i_j an j-te Stelle)

$\Rightarrow \exists (i_1, \dots, i_j, \dots, i_m) \in I$. Dann: $\underbrace{(0, \dots, 0, 1, 0, \dots, 0) \cdot (i_1, \dots, i_j, \dots, i_m)}_{= (0, \dots, 0, i_j, 0, \dots, 0)} \in I$ ✓ □

11.9. **Bem.:** Sei $(I_\mu)_{\mu \in M}$ eine Familie von Idealen in R.

Dann: $\bigcap_{\mu \in M} I_\mu =: D$ ist Ideal.

Bew.: $\forall b \in R \; \forall a \in D: ab, ba \in D$. □

11.10. **Bem.:** $I, J \subseteq R$ Ideale $\Rightarrow I + J$ Ideal.

Bew.: $a = a_1 + a_2 \in I + J$ mit $a_1 \in I$, $a_2 \in J$, $b \in R$

$\Rightarrow ba = b(a_1 + a_2) = ba_1 + ba_2 \in I + J$. □

11.11. **Lemma:** Sei R Ring, $I \subseteq R$ Ideal. Dann R/I Ring bzgl.

$+: (a+I) + (b+I) := (a+b) + I$

$\cdot: (a+I) \cdot (b+I) := (a \cdot b) + I$ mit $\bar{0} = 0 + I = I$, $\bar{1} = 1 + I$.

Bew.: * R/I ist ab. Gruppe bzgl. $+$

* $\cdot$ ist wohldef.: Seien $a + I = a' + I$, $b + I = b' + I$

$\Rightarrow a - a' \in I \Rightarrow b - b'$

$\Rightarrow ab - a'b' = ab - ab' + ab' - a'b'$

$= a(\underbrace{b - b'}_{\in I}) + (\underbrace{a - a'}_{\in I})b \in I$

$\Rightarrow ab + I = a'b' + I$.

* Axiome nachrechnen. □

11.12 **Def.**: R/I heißt Faktorring (Quotientenring) R modulo I.

11.13 **Bem.**: Die Faktorringe von $\mathbb{Z}$: $\mathbb{Z}/\mathbb{Z}r$, $r \in \mathbb{N}$.

Def.: $\mathbb{Z}/\mathbb{Z}r$ heißt Restklassenring modulo r,

$\mathbb{Z}/\mathbb{Z}r = \{\underline{0}, \underline{1}, \dots, \underline{r-1}\}$,

Restklassenabbildung $\pi_r : \mathbb{Z} \longrightarrow \mathbb{Z}/\mathbb{Z}r$

$n \longmapsto \underline{n} := n + \mathbb{Z}r$.

Fall 1: $r = p$ prim. Dann: $\mathbb{F}_p := \mathbb{Z}/\mathbb{Z}p$ Körper.

Bew.: $\underline{n} \in \mathbb{F}_p \setminus \{\underline{0}\} \Rightarrow p \nmid n \Rightarrow p, n$ teilerfremd

$\overset{7.3}{\Rightarrow} \exists u, v \in \mathbb{Z}: 1 = up + vn \Rightarrow 1 - vn = up \in \mathbb{Z}p$

$\Rightarrow \underline{1} = \underline{vn} = \underline{v} \cdot \underline{n} \Rightarrow (\underline{n})^{-1} = \underline{v}$. □

Fall 2: $r = s \cdot t$, $s, t \neq \pm 1$. Dann in $\mathbb{Z}/\mathbb{Z}(st)$:

$\underline{s} \cdot \underline{t} = \underline{st} = \underline{0}$, aber $\underline{s} \neq \underline{0} \neq \underline{t}$, d.h. $\underline{s}, \underline{t}$ Nullteiler.

(also $s \in \mathbb{Z}(st)$, da $st \nmid s$)

Später: s, t teilerfremd $\Rightarrow \mathbb{Z}/\mathbb{Z}(st) \cong \mathbb{Z}/\mathbb{Z}s \times \mathbb{Z}/\mathbb{Z}t$ (vgl. A12.5)

11.14 **Def.**: R, R' Ringe. $\varphi : R \to R'$ Ringhomomorphismus

$:\Leftrightarrow \forall a, b \in R$: (1) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(2) $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

(3) $\varphi(1) = 1$.

11.15 **Bem.**: Die Projektionen $\pi_i : R_1 \times \dots \times R_m \longrightarrow R_i$

$(a_1, \dots, a_m) \longmapsto a_i$

sind Homomorphismen.

11.16 **Bem.**: Sei $\varphi : R \to R'$ Ringhom. Dann: (1) $I' \subseteq R'$ Ideal $\Rightarrow \varphi^{-1}(I')$ Ideal in R

(2) $\ker \varphi$ ist Ideal

(3) φ injektiv $\Leftrightarrow \ker \varphi = 0$

(4) $\varphi(R^\times) \subseteq (R')^\times$.

Bew.: (1): Sei $a \in \varphi^{-1}(I')$, $b \in R$. Dann: $\varphi(ab) = \underbrace{\varphi(a)}_{\in I'} \varphi(b) \in I' \Rightarrow ab \in \varphi^{-1}(I')$, ba analog.

(2): $a \in \ker \varphi$, $b \in R \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 0\,\varphi(b) = 0 \Rightarrow ab \in \ker \varphi$.

(3): φ injektiv $\Leftrightarrow (\varphi(a) = \varphi(b) \Rightarrow a = b) \Leftrightarrow (\varphi(a-b) = 0 \Rightarrow a - b = 0) \Leftrightarrow \ker \varphi = 0$.

(4): Sei $u \in R^\times$, etwa $uv = vu = 1$. Dann: $1 = \varphi(uv) = \varphi(u)\varphi(v) \Rightarrow \varphi(u) \in (R')^\times$. □

11.17. **Bem.:** Bilder von Idealen sind i.a. keine Ideale.

Bew.: $\iota: \mathbb{Z} \hookrightarrow \mathbb{Q}$, $I = \mathbb{Z}\cdot 2 \to \mathbb{Z}\cdot 2$ kein Ideal von $\mathbb{Q}$. □

11.18 **Def.:** Ringisomorphismen, Ringendomorphismen, Ringautomorphismen analog wie bei Gruppen.

11.19 **Def.:** R Ring. $R' \subseteq R$ heißt Unterring (UR) $:\Leftrightarrow$ (1) R' UG der add. Gr. von R
(2) R' abg. bzgl. $\cdot$
(3) $1 \in R'$.

11.20 **Bem.:** * $\mathbb{Z}$ ist UR von $\mathbb{Q}$.
* $\mathbb{Q}^{n\times n}$ ist UR von $\mathbb{R}^{n\times n}$
* Körper $K \subseteq L \Rightarrow K^{n\times n}$ ist UR von $L^{n\times n}$
* $\varphi: R \to R'$ Ringhom. $\Rightarrow \varphi(R)$ UR von R'

11.21. **Bem.:** $I \subseteq R$ Ideal, $\varphi: R \twoheadrightarrow R'$ surj. Ringhom. $\Rightarrow \varphi(I) \subseteq R'$ Ideal.

Bew.: Sei $a \in I$, $b' \in R' \Rightarrow \exists\, b \in R: \varphi(b) = b'$.
Dann: $\varphi(a)\cdot b' = \varphi(a)\varphi(b) = \varphi(\underbrace{ab}_{\in I}) \in \varphi(I)$, $b'\cdot\varphi(a)$ analog. □

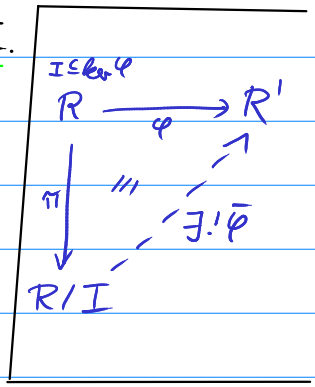
11.22. **Homomorphiesatz (für Ringe):**

Vor.: R Ring, $I \subseteq R$ Ideal.

Beh.: (i) $\pi: R \to R/I$ „Projektion" zu I
$a \mapsto a + I$ ist surjektiver Ringhom., $\ker \pi = I$.

(ii) „Universelle Eigenschaft":
$\forall\, \varphi \in R\text{-Hom}(R, R')$, R' Ring, $I \subseteq \ker\varphi$,
$\exists!\, \bar\varphi \in R\text{-Hom}(R/I, R')$: $\bar\varphi \circ \pi = \varphi$.

Zusatz: $\left.\begin{array}{l}(\alpha)\ \operatorname{im}\bar\varphi = \operatorname{im}\varphi \\ (\beta)\ \bar\varphi \text{ inj} \Leftrightarrow \ker\varphi = I\end{array}\right\} \Rightarrow (\gamma)\ \operatorname{im}\varphi \cong R/\ker\varphi$
($\bar\varphi$ Isom.)



Bew.: (i): π R-Hom., surj.: ✓, $\ker\pi = I$: $a+I = \pi(a) = \bar{0} = 0+I = I \Leftrightarrow a \in I$.

(ii): Hom.satz für Gruppen $\Rightarrow \exists!\ \bar{\varphi} \in G\text{-Hom}(R, R')$, das genügt.

Zeige noch: $\bar{\varphi}(\bar{a}\bar{b}) = \bar{\varphi}(\bar{a}) \cdot \bar{\varphi}(\bar{b})$.

Bew.: $\bar{\varphi}((a+I)(b+I)) = \bar{\varphi}(ab+I) = \bar{\varphi}(\pi(ab))$

$= \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\pi(a)) \cdot \bar{\varphi}(\pi(b))$

$= \bar{\varphi}(a+I) \cdot \bar{\varphi}(b+I)$. ✓

(α), (β): nach Hom.satz für Gruppen,

(γ): $R \xrightarrow{\varphi} \operatorname{im}\varphi \subseteq R'$

$\pi \downarrow$ $\quad \nearrow \bar{\varphi}$

$R/\underbrace{\ker\varphi}_{=:I}$

$\bar{\varphi}$ surj, da φ surj. (α)
$\bar{\varphi}$ inj., da $\ker\varphi = I$ (β)
$\Big\}$ $\operatorname{im}\varphi \cong R/\ker\varphi$ mit Ringisom. $\bar{\varphi}$.

□

11.3 Satz: Vor.: R Ring, $I \subseteq R$ Ideal, $\pi: R \to R/I =: \bar{R}$ Projektion zu I.

$\mathcal{J} := \{J \subseteq R \text{ Ideal};\ I \subseteq J\}$, $\bar{\mathcal{J}} := \{\bar{J} \subseteq \bar{R} \text{ Ideal}\}$,

$\varphi: \mathcal{J} \to \bar{\mathcal{J}}$, $J \mapsto \pi(J)$; $\Psi: \bar{\mathcal{J}} \to \mathcal{J}$, $\bar{J} \mapsto \pi^{-1}(\bar{J})$

Beh.: (i) φ, Ψ zueinander inverse Bijektionen zwischen $\mathcal{J}$ und $\bar{\mathcal{J}}$.

(ii) $\bar{L} \in \bar{\mathcal{J}}$ Ideal in $\bar{R} \Leftrightarrow L := \pi^{-1}(\bar{L}) \in \mathcal{J}$ Ideal in R

Dann: $R/L \cong \bar{R}/\bar{L} = (R/I)/(L/I)$.

Bew.: wohldef.: $J \subseteq R$ Ideal $\Rightarrow \pi(J) \subseteq R'$ Ideal, da π surj. (Bem. 11.21).

Also: φ wohldef., ebenso Ψ nach Bem. 11.16.

Somit: 11.23 folgt aus A4.22, da bei dieser Bijektion

Ideale in Ideale übergehen. □

11.24. **Bem.:** Sei R Ring, $\varphi: \mathbb{Z} \to R$, $n \mapsto n_R = n \cdot 1_R$. Dann φ Ringhom.

Bew.: Es ist $\varphi(1) = 1_R$, und $\varphi(n+m) = (n+m)_R = (n+m)\cdot 1_R$
$= n 1_R + m 1_R = n_R + m_R = \varphi(n) + \varphi(m)$.

Ferner: $(nm)_R = n_R \cdot m_R$, d.h. $\varphi(nm) = \varphi(n)\cdot\varphi(m)$.

Bew.: $n \geq 0$: VI nach n: $n=0$: $(0\cdot m)_R = 0_R = 0_R \cdot m_R$.

$n \to n+1$: $((n+1)m)_R = (nm+m)_R = (nm)_R + m_R$
$\overset{IV}{=} n_R m_R + m_R = (n_R + 1_R) m_R$
$= (n+1)_R m_R$.

$n < 0$: $(-1\cdot m)_R = -m_R \Rightarrow (nm)_R = (-(-n)m)_R = -((-n)m)_R$
$= -(-n_R)m_R = n_R m_R$. □

11.25 **Def.:** $\varphi\mathbb{Z}$ mit φ aus Bem. 11.24 heißt Primring von R.

11.26 **Bem.:** $\varphi\mathbb{Z}$ ist Kleinster UR $\neq 0$ von R $(\neq 0)$,
und: $\varphi\mathbb{Z} \cong \mathbb{Z}/\ker\varphi = \mathbb{Z}/\mathbb{Z}r$ mit einem $r \in \mathbb{N}_0$.

11.27 **Def.:** $r \in \mathbb{N}_0$ heißt Charakteristik von R.