# Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

## Teil II: RINGE (und Moduln)

## A13: Hauptidealbereiche

Stichworte: Hauptidealbereich, euklidischer Integritätsbereich, eukl. IB ⇒ HIB, Bsp. für HIBe: $\mathbb{Z}$, K (aber nicht $\mathbb{Z}[T]$), irreduzibel, assoziiert, teilt, ggT, faktorieller IB, IB mit (F1)&(F2) ⇒ faktoriell, Ex. von ggT's in HIB (≙ Bézout), HIB ⇒ faktoriell!, K[T] faktoriell, im faktoriellen Ring gilt (F2), Teiler in faktoriellen Ringen

---

13.1. Einleitung: Ist in einem IB jedes Ideal ein Hauptideal (d.h. von einem einzigen El. erzeugt), nennt man ihn Hauptidealbereich. IBe, in denen eine "Division mit Rest" möglich ist, heißen euklidisch. Euklidische IBe sind HIBe, u.a. also $\mathbb{Z}$ und K[T]. Der Satz von der eind. PFZ ist auf IBe übertragbar, diese nennt man faktoriell. Z.B. gilt: HIBe sind faktoriell. In HIBen ex. stets ein ggT(a,b) von bel. El. a,b, und der Satz von Bézout über $\mathbb{Z}$ kann in diesen Ringen auf natürliche Art übertragen werden.

13.2. Def.: Ein IB, in dem jedes Ideal Hauptideal ist, heißt Hauptidealbereich (kurz: HIB).

13.3. Bsp.: Körper sind HIB, $\mathbb{Z}$ ist HIB

13.4. Def.: Ein IB A heißt euklidisch :⇔ ∃ Fkt. $\delta : A \setminus \{0\} \to \mathbb{N}$ :

$$\forall a, b \in A \setminus \{0\}\ \exists r, s \in A: \quad a = sb + r \text{ und } (\delta(r) < \delta(b) \text{ oder } r = 0).$$

13.5. Bsp: $\mathbb{Z}$ ist euklidisch und $\delta(a) = |a|$.

13.5. Bsp.: K Körper ⇒ K[T] ist euklidisch mit $\delta(f) = \text{grad}(f) = \deg(f)$.

13.6. Satz: Euklidische IB sind HIB.

Bew.: Sei A eukl. bzgl. $\delta$, $I \subseteq A$ Ideal, $0 \subsetneq I \neq 0$,
sei $b \in I$, $b \neq 0$, mit $\delta(b)$ minimal.
Beh.: $I = (b)$.
Bew.: "$\supseteq$": ✓ da $b \in I$, Def. von $(b)$.
"$\subseteq$": Sei $a \in I$, $a \neq 0$. Dann ex. $r, s \in A$:
$a = sb + r$, $\delta(r) < \delta(b)$ oder $r = 0$.
Ann: $r \neq 0 \Rightarrow \delta(r) < \delta(b) \Rightarrow r = a - sb \in I$,
↯ zur Wahl von b. □

13.7. **Bsp.:** $\mathbb{Z}[T]$ ist Kein HIB.

**Bew.:** $\underbrace{\mathbb{Z}[T]\cdot T + \mathbb{Z}[T]\cdot 2}_{=: I = \{f \in \mathbb{Z}[T];\ 2 \mid f(0)\}}$ ist Kein Hauptideal:

Ann.: $I=(g)$, $g = a_n T^n + \dots + a_1 T + a_0$. Sei $p := T+2 \in I = (g)$.

$\Rightarrow \exists f \in \mathbb{Z}[T]: p = f \cdot g$, $\deg(p) = 1 = \deg(f) + \deg(g)$.

$\Rightarrow \deg(g) = 1$, $\deg(f) = 0$, also $I = (p)$.

Aber: $3T+2 \in I$ und $3T+2 \notin (p)$. ↯ □

13.8. **Def.:** IB $A \ni p$ irreduzibel (prim), falls $p \notin A^\times$ und $\forall a,b \in A: (p = ab \Rightarrow a \in A^\times \vee b \in A^\times)$.

$a, b \in A$ assoziiert: $\Leftrightarrow \exists u \in A^\times: a = ub$

Notation: a teilt b: $a \mid b :\Leftrightarrow \exists c \in A: b = ac \Leftrightarrow b \in (a)$.

13.9. **Bem.:** $p$ prim $\Rightarrow$ Jeder Teiler von $p$ ist Einheit oder assoziiert zu $p$.

13.10. **Bem.:** Assoziiertheit def. Äquivalenz-Relation auf $A$.

**Bew.:** reflexiv: $a = 1 \cdot a \Rightarrow a$ assoz. $a$

symmetrisch: $a$ assoz. $b \Rightarrow b = ub$, $1 = uv \Rightarrow va = b \Rightarrow b$ assoz. $a$

transitiv: $a$ assoz. $b \wedge b$ assoz. $c \Rightarrow a = ub$, $b = vc \Rightarrow a = uvc \Rightarrow a$ assoz. $c$ □

13.11. **Def.:** $A$ IB. $d \in A$ größter gemeinsamer Teiler von $a, b \in A$: $d = \mathrm{ggT}(a,b)$

$:\Leftrightarrow d \mid a \wedge d \mid b \wedge (\forall d': d' \mid a \wedge d' \mid b \Rightarrow d' \mid d)$.

13.12. **Bem.:** $d$ ist bis auf Assoziiertheit eind. bestimmt

**Bew.:** $d_1, d_2 \neq 0$ seien ggT von $a, b \in A$. Dann: $d_2 \mid d_1$, d.h.

$d_1 = r \cdot d_2$, ebenso: $d_1 \mid d_2 : d_2 = s d_1$. Somit:

$d_2 = (rs) d_2 \Rightarrow rs = 1 \Rightarrow r, s \in A^\times \Rightarrow d_1$ assoz. $d_2$. □

13.13. **Def:** Ein IB $A$ heißt faktoriell (Ring mit eind. PFZ)

$:\Leftrightarrow$ (1) $\forall a \neq 0, a \notin A^\times \exists$ prime $p_1, \dots, p_m \in A: a = p_1 \cdot \dots \cdot p_m$ (Existenz)

(2) $p_1, \dots, p_m, q_1, \dots, q_n \in A$ prim, $u, v \in A^\times$, $u p_1 \cdots p_m = v q_1 \cdots q_n$

$\Rightarrow m = n$ und: $\exists \sigma \in S_m \ \forall 1 \leq i \leq m: p_i$ assoz. $q_{\sigma(i)}$. (Eindeutigkeit)

13.14. **Bem.:** $\forall a,b \in A: (a)=(b) \iff a$ assoz. $b$.

**Bew.:** $(a)=(b) \iff \begin{cases} \exists u \in A: a = ub \\ \exists v \in A: b = va \end{cases} \iff \begin{cases} uv = vu = 1 \\ a = ub \end{cases} \iff a$ assoz. $b$. □

13.15. **Lemma:** Sei $A$ ein IB mit den Eigenschaften

(F1) $\exists$ keine unendl., echt aufsteigende Folge
$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ von Hauptidealen in $A$.

(F2) $\forall p \in A$ prim $\forall a,b \in A$:
$p \mid (ab) \Rightarrow p \mid a \vee p \mid b$.

Dann ist $A$ faktoriell.

**Bew.:** Existenz: Sonst sei $a \in A$ Gegenbsp.

Konstruieren unendl. Folge $(a_0, a_1, \dots) \subseteq A$ von Gegenbsp.
mit $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ (dann ↯ zu (F1)):

Sei $a_0 := a$. $n \rightsquigarrow n+1$: Sei $a_n$ Gegenbsp.
$\Rightarrow a_n$ nicht prim $\Rightarrow \exists b, c \in A: a_n = bc$, $b,c \notin A^\times$
$\Rightarrow b$ oder $c$ Gegenbsp., o.E. $b$. Dann: $a_{n+1} := b$,
ferner: $(a_n) \subsetneq (a_{n+1})$, da $a_{n+1} \mid a_n$,
und $\neq$, da $a_n$ und $a_{n+1}$ nicht assoz. (Bem. 13.14).

Eindeutigkeit: Sei $u p_1 \cdot \dots \cdot p_m = v q_1 \cdot \dots \cdot q_n$.
VI nach $m \in \mathbb{N}_0$: $m=0$: $n=0$ ✓,
$m \rightsquigarrow m+1$: (F2) $\Rightarrow \exists j$, $1 \le j \le n$: $p_{m+1} \mid q_j$
$\Rightarrow \exists w \in A^\times: q_j = w p_{m+1}$
$\Rightarrow u p_1 \cdot \dots \cdot p_m = v w q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_n$, darauf IV $\Rightarrow$ ✓. □

13.16. **Lemma:** Sei $A$ HIB, $a,b \in A$, $d$ ein ggT$(a,b)$. Dann:
$\exists x,y \in A: d = xa + yb$.

**Bew.:** $I = (a,b) = (d)$ mit $d \in A$, $d$ ggT$(a,b)$,
sowie $d = xa + yb$ für geeignete $x,y \in A$. □

13.17. **Satz:** HIB sind faktoriell.

**Bew.:** Sei $A$ ein HIB, zeige: (F1), (F2) nach 13.15.

(F1): Sei $(a_1) \subseteq (a_2) \subseteq \dots$ unendl. Folge von Hauptidealen.

$I := \bigcup_{i \geq 1} (a_i)$ ist Ideal $\Rightarrow \exists a \in A: I = (a)$.

$\Rightarrow \exists j: a \in (a_j) \Rightarrow I = (a) = (a_j) = (a_{j+1}) = \dots$

(F2): Seien $a, b \in A$, $A \ni p$ prim, $p \mid (ab)$, $\not\subseteq p \nmid a$.

$\Rightarrow 1$ ist $\operatorname{ggT}(a,p) \overset{13.16}{\Rightarrow} \exists x, y \in A: 1 = ax + py$

$\Rightarrow b = (ab)x + pby \Rightarrow p \mid b$. □

13.18. **Kor.:** $K$ Körper $\Rightarrow K[T]$ faktoriell.

13.19. **Satz:** $A$ sei faktorieller Ring. Dann:

$\forall a, b \in A \ \forall A \ni p$ prim: $(p \mid (ab) \Rightarrow p \mid a \vee p \mid b)$

**Bew.:** Seien $\not\subseteq a, b \notin A^\times \Rightarrow \exists c \in A: ab = pc$ $(c \notin A^\times)$.

Schreiben $a, b, c$ als Produkt von Primelementen.

$\Rightarrow \underbrace{p_1 \cdot \dots \cdot p_m}_{a} \cdot \underbrace{q_1 \cdot \dots \cdot q_n}_{b} = p \cdot \underbrace{r_1 \cdot \dots \cdot r_k}_{c}$, die $p_i, q_i, r_i$ prim.

$\Rightarrow$ Eines der Primel. links ist assoz. zu $p$ $\Rightarrow (p \mid a \vee p \mid b)$.

↑ Eind. der PFZ □

13.20. **Satz:** Seien $p_1, \dots, p_m \in A$ prim ($A$ faktoriell), paarw. nicht assoz.,

$e_1, \dots, e_m \geq 1$, $u \in A^\times$, $a := u p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$.

Dann ist jeder Teiler von $a$ von der Gestalt

$v p_1^{f_1} \cdot \dots \cdot p_m^{f_m}$ mit $v \in A^\times$, $0 \leq f_i \leq e_i$ $(1 \leq i \leq m)$.