Noch zu A13: euklidisch $\underset{13.6}{\Rightarrow}$ HIB $\overset{!}{\Rightarrow}$ faktoriell

↳ Eind. der PFZ

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

"unzerlegbar"

$p \in A$ prim $:\Leftrightarrow \forall a, b \in A: p \mid ab \Rightarrow p \mid a \vee p \mid b$

Bem.: Stets: prim $\overset{\not\Leftarrow}{\Rightarrow}$ irred. in bel. IB A

$\ulcorner p = ab \Rightarrow p \mid ab \underset{p \text{ prim}}{\Rightarrow} p \mid a \vee p \mid b$

$\left(\begin{array}{l} \text{Falls } p \mid a, \text{ ist } a = pa' \text{ und } p = ab = pa'b \overset{IB}{\Rightarrow} 1 = a'b \Rightarrow b \in A^\times \\ \text{Falls } p \mid b, \text{ ist } b = pb' \text{ und } p = ab = pab' \overset{IB}{\Rightarrow} 1 = ab' \Rightarrow a \in A^\times \end{array}\right)$

$\Rightarrow b \in A^\times \vee a \in A^\times$. $\lrcorner$

13.13. **Def.:** IB A heißt faktoriell $:\Leftrightarrow$ (1) $\forall a \neq 0, a \notin A^\times \; \exists$ irred. $p_1, \dots, p_m \in A: a = p_1 \cdots p_m$

& (2) $p_1, \dots, p_m, q_1, \dots, q_n \in A$ irred., $u, v \in A^\times$

$u p_1 \cdots p_m = v q_1 \cdots q_n$

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

A IB

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

Bew.: $(a) = (b) \Leftrightarrow \left\{\begin{array}{l} \exists u \in A: a = ub \\ \exists v \in A: b = va \end{array}\right\} \Leftrightarrow \left(\begin{array}{c} uv = vu = 1 \\ \hline a = ub \end{array}\right) \Leftrightarrow a$ assoz. b. $\square$

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

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

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

$\Leftrightarrow$ (p irred. $\Rightarrow$ p prim)

"Lemma von Euklid"

Dann ist A faktoriell.

Bew.: z.z.: Ex & Eind. der PFZ

Ex: 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 $a_0 := a$. Dann $n \rightsquigarrow n+1$: Sei a_n Gegenbsp.

$\Rightarrow a_n$ nicht irred. $\Rightarrow \exists b, c \in A: a_n = bc$, $b, c \notin A^\times$

$\Rightarrow b$ oder c Gegenbsp., OE 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)

$[a_n = bc]$

Eind.: Sei $u p_1 \cdots p_m = v q_1 \cdots q_n$

VI nach $m \in \mathbb{N}_0$: $m = 0$: $n = 0$ ✓,

$m \rightsquigarrow m+1$: (F2): $p_{m+1} \mid q_1 \cdots q_n \underset{(F2)}{\Rightarrow} \exists j \leq n: p_{m+1} \mid q_j$

$\Rightarrow \exists w \in A^\times: q_j = w p_{m+1} \Rightarrow u p_1 \cdots p_m \cdot p_{m+1} = v \; q_1 \cdots q_{j-1} \cdot w p_{m+1} \cdot q_{j+1} \cdots q_n$

$\Rightarrow u p_1 \cdots p_m = vw \, q_1 \cdots q_{j-1} q_{j+1} \cdots q_n \Rightarrow$ darauf IV $\Rightarrow$ ✓ □

13.16 Lemma: Sei A HIB, $a, b \in A$, d ein ggT(a,b). Dann:

$\exists x, y \in A: d = xa + yb$. "Bézout für HIBe"

Bew.: $I := (a,b) \underset{A \text{ HIB}}{=} (d)$ mit $d \in A$, d ist ggT(a,b).

sowie $d \in I = Aa + Ab \Rightarrow d = xa + yb$ für geeignete $x, y \in A$.

□

13.17 Satz: HIBe sind faktoriell.

Bew.: Sei A HIB, z.z. (F1) & (F2) nach 13.15.

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

$I := \bigcup_{i \geq 1} (a_i) = \{b \in A; \exists i: b \in (a_i)\}$ ist Ideal

$\overset{A \text{ HIB}}{\Longrightarrow} I = (a)$ für ein $a \in A$. Also: $\exists j: a \in (a_j) \Rightarrow I = (a) = (a_j) = (a_{j+1}) = \dots$

(F2): Sei $p \in A$ irred. Seien $a, b \in A$ mit $p \mid ab$, $\not\mid p \nmid a$.

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

$\Rightarrow b = \underbrace{(ab)}_{p \mid ab} x + pby \Rightarrow p \mid b$.

$\square$

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

($\Rightarrow K[T]$ euklidisch $\Rightarrow K[T]$ HIB $\Rightarrow K[T]$ faktoriell)

$\mathbb{Z}$ euklid. $\Rightarrow \mathbb{Z}$ HIB $\Rightarrow \mathbb{Z}$ faktoriell.

13.19. Satz: A sei faktoriell. Dann: $\forall a, b \in A$ $\forall A \ni p$ irred.: $(p \mid ab \Rightarrow p \mid a \vee p \mid b)$

(d.h. (F2) gilt)

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

Schreibe a, b, c als Produkt von irred. Elementen.

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

$\Rightarrow$ Eind. der PFZ, da A fakt.

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

$\square$ prim = irred. in fakt. Ring

13.20 Satz: A faktoriell, seien $p_1, \dots, p_m \in A$ prim, pw nicht assoz,

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

Dann ist jeder Teiler von a von der Gestalt

$v\, p_1^{f_1} \cdots p_m^{f_m}$ mit $v \in A^\times$, $0 \leq f_i \leq e_i$, $1 \leq i \leq m$. ✓

Bsp.: $A = \mathbb{Z}[\underbrace{\sqrt{-5}}_{\in \mathbb{C}}] = \{a + b\sqrt{-5};\ a, b \in \mathbb{Z}\}$ ist nicht faktoriell!

2 ist Bsp. irred. $\not\Rightarrow$ prim

$2 \mid 2 \cdot 3 = 6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$

2 ist nicht prim, denn $2 \nmid 1+\sqrt{-5}$ und $2 \nmid 1-\sqrt{-5}$ in A

2 ist irred in A: $2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \Rightarrow \dots \Rightarrow a = 2 \wedge c = 1, b = d = 0$

A14: Polynomringe

14.1. Einleitung: Polynomringe $\rightsquigarrow$ CRS

14.2. Alle Ringe kommutativ!

14.3. Def.: A UR von B, $x_1, \dots, x_n \in B$.

$$A[x_1, \dots, x_n] := \bigcap \{ A' \text{ UR von } B;\ A \subseteq A' \wedge x_1, \dots, x_n \in A' \}$$

heißt der von $x_1, \dots, x_n$ über A erzeugte Ring.

Sprechweise: "$A[\underline{x}]$ entsteht aus A durch (Ring-) Adjunktion von $x_1, \dots, x_n$"

Kurz "A adjungiert $x_1, \dots, x_n$".

Bsp.: $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$,

$$\mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5};\ a, b \in \mathbb{Z} \} = \{ a + b\sqrt{-5} + c\underbrace{(\sqrt{-5})^2}_{=-5} + d(\sqrt{-5})^3 + \dots$$

14.4. Bem.: $A[x_1, \dots, x_n][y_1, \dots, y_m] = A[x_1, \dots, x_n, y_1, \dots, y_m]$

14.5. Bem.: $A[x] = \{ \sum_{i=0}^{n} a_i x^i;\ n \in \mathbb{N}_0,\ \text{die } a_i \in A \}$

Bew.: "$\supseteq$": Klar nach Def. von $A[x]$ ✓

"$\subseteq$": r.S. ist Ring, der A umfasst und enthält x. $\square$

14.6. Bem.: $A[x_1, \dots, x_n] = A[x_1][x_2] \dots [x_n]$

$$= \{ \sum_{(i_1, \dots, i_n) \in E} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n};\ E \subseteq \mathbb{N}_0^n \text{ endlich} \}$$

14.7. Def.: Seien $A \subseteq P$ Ringe, $X_1, \dots, X_n \in P$.

P heißt ein Polynomring in "den Unbestimmten" $X_1, \dots, X_n$ über A

$:\Leftrightarrow$ (1) $P = A[X_1, \dots, X_n]$

$\wedge$ (2) Aus $\sum_{\underline{i} \in E} a_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n} = 0$, $E \subseteq \mathbb{N}_0^n$ endl.,

folgt stets $a_{\underline{i}} = 0$ für alle $\underline{i} \in E$.

Bsp.: $\mathbb{Z}[\sqrt{-5}]$ kein Polynomring, da $1 \cdot (\sqrt{-5})^2 + 5 = 0$.

14.8. <u>Satz</u>: Universelle Eigenschaft von Polynomringen:

Sei P Polynomring in $X_1, \dots, X_n$ über A. Dann:

$\forall$ Ringhom. $\varphi: A \to B$, B komm. Ring

$\forall$ Folgen $x_1, \dots, x_n \in B$

$\exists!$ Ringhom $\bar{\varphi}: P \to B$: $\bar{\varphi}\restriction_A = \varphi$

und $\bar{\varphi}(X_i) = x_i$, $1 \le i \le n$.

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, hook, "\iota"'] & B \\ P \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd} \qquad X_i \mapsto x_i, \quad X_1, \dots, X_n \mapsto x_1, \dots, x_n$$

Bew.: Setze $\bar{\varphi}\left(\sum_{\underline{i} \in E} a_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n}\right) := \underbrace{\sum_{\underline{i} \in E} \varphi(a_{\underline{i}})\, x_1^{i_1} \cdots x_n^{i_n}}_{\in B \checkmark}$,

ist wohldef. ✓,

ein Ringhom $P \to B$ ✓, $\bar{\varphi}\restriction_A = \varphi$, $\bar{\varphi}(X_i) = x_i$, und eindeutig. $\square$

14.9 Bem.: ....

14.10. <u>Satz</u>: Für $n \ge 1$ gibt es bis auf Isom. genau einen Polynomring in n Unbest. über A.

<u>Bew.</u>: <u>Eind.</u>: Seien P, P' Polynomringe über A.

Univ. Eig.:

$$\begin{tikzcd} A \arrow[r, hook, "\iota'"] \arrow[d, hook, "\iota"'] & P' \\ P \arrow[ur, dashed, "\varphi_1 \text{ inj.}"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[d, hook, "\iota'"'] & P \\ P' \arrow[ur, dashed, "\varphi_2 \text{ inj.}"'] & \end{tikzcd}$$

$\Rightarrow$ Ex. zwei inj. Ringhom. $\varphi_1: P \to P'$, $\varphi_2: P' \to P$.

Also: isomorphien! $P \cong P'$

<u>Ex.</u>: Explizite Konstruktion...

$\square$

14.11/12. <u>Bem.</u>: $A = K[T]/(f)$ sind interessante Ringe

Hauptid., von $f \in K[T]$ erzeugt

$\rightsquigarrow$ K-Algebra, $\dim_K A = \deg(f)$

14.13: Satz: Ist $f \in K[T] \setminus \{0\}$, K Körper und $a \in K$ eine Nst. von f, d.h. $f(a) = 0$, so ist $T - a \mid f$.

Daher hat $f \neq 0$ höchstens $\deg(f)$ viele Nst. in K.

Bew.: Da $K[T]$ euklid., $\underline{f(T) = (T-a) \cdot q(T) + r}$ mit $\deg(r) = 0$, d.h. $r \in K$. Mit $0 = f(a) = 0 + r$ folgt $T - a \mid f$.

Sind $a_1, \dots, a_n$ versch. Nst. von f folgt $(T-a_1) \cdots (T-a_n) \mid f$, also $n = \deg((T-a_1) \cdots (T-a_n)) \leq \deg(f)$. $\square$

14.14. Bem.: R Ring, dann: $\underline{R[T] \text{ euklid.}} \Leftrightarrow \underline{R \text{ Körper}}$ [ohne Bew.]

14.15 Lemma: CRS in $\underbrace{K[T]}_{\text{faktoriell}}$:

Sei $f = p_1^{e_1} \cdots p_m^{e_m}$, die $p_i \in K[T]$ irred., p.w. nicht assoz., $e_i \geq 1$.

Dann: $\underline{\underline{K[T]/(f)}} \cong K[T]/(p_1^{e_1}) \times \dots \times K[T]/(p_m^{e_m})$ [A12.4].