<u>Noch zu A12:</u> R Komm. Ring, $S \subseteq R \rightsquigarrow (S) := \bigcap \{ I \subseteq R \text{ Id.}, \ S \subseteq I \}$

Bsp.: $R = \mathbb{Z}$: $\underbrace{(2,3)}_{= \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot 3} = (\{2,3\}) \subseteq \mathbb{Z}$

12.16. $(S) = \sum_{s \in S} Rs := \{ \sum_{i=1}^{n} a_i s_i ; \ a_i \in R, \ s_i \in S \}$

$S = \{b_1, \dots, b_n\} \rightsquigarrow (S) = Rb_1 + \dots + Rb_n$

Def.: Ideale $I = (a)$, die von einem El. a erz. werden, heißen <u>Hauptidealen</u>.

$\ulcorner (2) = (-2) \Leftrightarrow \mathbb{Z}\cdot 2 = \mathbb{Z}\cdot(-2) \lrcorner$

12.17. Bem.: Sei $a \in R$, dann: $(a) = R \Leftrightarrow a \in R^\times$.

Bew.: „$\Rightarrow$": $\exists b \in R: 1 = b \cdot a \Rightarrow a \in R^\times$

„$\Leftarrow$": $\exists b \in R: 1 = b \cdot a \in (a) \Rightarrow (a) = R$ nach A11.6. $\square$

12.18. Def.: Ideal $I \subseteq R$ (Komm. Ring) <u>maximal</u> $:\Leftrightarrow$ (1) $I \neq R$

und (2) $\nexists$ Ideal J, $I \subsetneq J \subsetneq R$.

12.19. Bem.: $R = K$ Körper $\Rightarrow \{0\}$ maximales Id.

Bew.: Sonst: $0 \subsetneq J \subsetneq K \Rightarrow J$ enthält Einheit von $K \underset{A11.6.}{\Rightarrow} J = K$ ↯ $\square$

12.20. Bem.: $I \subsetneq R$ maximal $\Leftrightarrow R/I$ Körper.

Bew.: Betr. $\pi: R \to R/I$. Dann: $R \supsetneq I$ maximal

$\Leftrightarrow \nexists$ Id. in R/I außer 0, R/I (nach A11.23)

$\Leftrightarrow \left(\forall \underline{a} \in R/I, \ \underline{a} \neq 0: \underbrace{(\underline{a}) = R/I}_{\underset{12.17.}{\Leftrightarrow} \underline{a} \in (R/I)^\times} \right) \Leftrightarrow R/I$ Körper. $\square$

12.21. Bem.: Sei $R = \mathbb{Z}$, $r, s \in \mathbb{N}$. Dann: $(r) \subseteq (s) \Leftrightarrow s \mid r$

$\ulcorner \mathbb{Z}\cdot 15 \subseteq \mathbb{Z}\cdot 3 \lrcorner$ "s über r"

Also hier: (r) maximal $\Leftrightarrow r$ prim.

- - - - -

12.22. Def.: R (komm.) Ring, $I \subsetneq R$ Ideal.
I heißt <u>prim</u> (<u>Primideal</u>) $:\Leftrightarrow \forall a,b \in R: \; a \cdot b \in I \Rightarrow (a \in I \vee b \in I)$

12.23. Bem.: I prim $\Leftrightarrow$ R/I Integritätsbereich
Bew.: „$\Leftarrow$": $a \cdot b \in I$, d.h. $\underline{a} \cdot \underline{b} = \underline{0} \Rightarrow \underline{a} = 0 \vee \underline{b} = 0 \Rightarrow a \in I \vee b \in I$.
„$\Rightarrow$": $\underline{a} \cdot \underline{b} = 0 \Rightarrow a \cdot b \in I \Rightarrow a \in I \vee b \in I \Rightarrow \underline{a} = 0 \vee \underline{b} = 0$. $\square$

12.24. Bem.: Maximale Ideale sind prim. $\ulcorner$ max. $\Rightarrow$ prim $\lrcorner$
Bew.: $I \subseteq R$ max. $\underset{12.20}{\Leftrightarrow}$ R/I Körper $\not\Leftarrow$
$\Downarrow$ $\Downarrow$
$I \subseteq R$ prim $\underset{12.23}{\Leftrightarrow}$ R/I IB. $\square$

12.25. Bem.: $0 \subseteq R$ prim $\Leftrightarrow$ R IB.
12.26. Bem.: $0 \subseteq \mathbb{Z}$ prim, aber nicht max. (12.24).

12.27. Bem.: $\varphi: R \to R'$ Ringhom., R' I.B. $\Rightarrow$ $\ker\varphi$ Primid.
Bew.:
$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & R' \\ R/\ker\varphi \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$
$\bar{\varphi}(R/\ker\varphi) \subseteq R'$ ist I.B.
$\Rightarrow R/\ker\varphi$ ist I.B.
$\Rightarrow \ker\varphi$ prim nach Bem. 12.23. $\square$

"Kerne sind prim"

12.28. Bem.: Die Primidealen in $\mathbb{Z}$ sind 0 und die (p), $p \in \mathbb{Z}$ prim.
Bew.: „$\subseteq$": $(r) \neq 0$ prim $\Rightarrow \forall a,b \in \mathbb{Z}: r \mid ab \Rightarrow r \mid a \vee r \mid b \Rightarrow r$ prim
$\ulcorner$vgl. A13.19, "Lemma von Euklid" für $\mathbb{Z}$$\lrcorner$
„$\supseteq$": r prim $\Rightarrow \mathbb{Z}/(r)$ Körper, ist insb. endl. IB
$\underset{12.20}{\Rightarrow}$ (r) maximal $\underset{12.24}{\Rightarrow}$ (r) prim. $\square$

12.29. Def.: Sei R ein IB. Körper Q heißt <u>Quotientenkörper von R</u>,

Bez.: $Q = \mathrm{Quot}(R)$

$:\Leftrightarrow \exists$ inj. Ringhom. $R \overset{\varepsilon}{\hookrightarrow} Q : \forall r \in Q \; \exists a, b \in R :$

$(b \neq 0 \wedge r = (\varepsilon a) \cdot (\varepsilon b)^{-1})$

$\ulcorner \mathbb{Z} \hookrightarrow \mathbb{Q} : \forall r \in \mathbb{Q} \; \exists a, b \in \mathbb{Z}, b \neq 0 : r = a \cdot b^{-1} \lrcorner$

12.36. Satz: Zu jedem IB gibt es bis auf Isomorphie genau einen Quot. Körper.

Bew.: <u>Ex.:</u> $Q := R \times (R \setminus \{0\}) / \sim$

$(a, b) \sim (c, d) :\Leftrightarrow ad = cb$ $\Big\}$ $\frac{a}{b} + \frac{c}{d} \ldots$

<u>Eind.:</u> * Univ. Eig. von Quot. Körpern:

$$\begin{tikzcd} R \arrow[r, hook, "i"] \arrow[d, hook, "\varepsilon"'] \arrow[dr, phantom, "\circlearrowright"] & K \\ Q \arrow[ur, dashed, hook] & \end{tikzcd}$$

✓

* Q, Q' zwei Quot. Körper von R

$$\begin{tikzcd} R \arrow[r, hook, "\varepsilon'"] \arrow[d, hook, "\varepsilon"'] & Q' \\ Q \arrow[ur, dashed, hook, "\varphi_1"'] & \end{tikzcd} \quad \text{und} \quad \begin{tikzcd} R \arrow[r, hook, "\varepsilon"] \arrow[d, hook, "\varepsilon'"'] & Q \\ Q' \arrow[ur, dashed, hook, "\varphi_2"'] & \end{tikzcd} \quad \Rightarrow Q \cong Q'$$

$\square$

A13: Hauptidealbereiche

13.1. euk. Ring $\Rightarrow$ HIB $\Rightarrow$ faktoriell
↑ ↑ Eind. der PFZ

13.2. Def.: Ein IB, in dem jedes Ideal Hauptideal ist, heißt H.I.B.
D.h. ein IB R heißt HIB $:\Leftrightarrow \forall I \subseteq R$ Id.: $\exists a \in R: I = (a)$

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

13.4. Def.: Ein IB A heißt euklidisch $:\Leftrightarrow \exists$ FKt. $\delta: A \setminus \{0\} \to \mathbb{N}$:
$\forall a, b \in A \setminus \{0\}\ \exists r, s \in A: a = sb + r$
und ($\delta(r) < \delta(s)$ oder $r = 0$)
„Division mit Rest"
δ heißt euklidische FKt.

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

13.6. Bsp.: K Körper $\Rightarrow K[T]$ ist euklidisch mit $\delta(f) = \text{grad}(f) = \deg(f)$.
"Polynomdivision"

13.7. Satz: Euklidische IBe sind HIBe.

Bew.: Sei A euk. bzgl. δ, $I \subseteq A$ Ideal, $0 \neq I \neq 0$.

vgl. A0.5 Sei $b \in I$, $b \neq 0$, mit $\delta(b)$ minimal.

Beh.: $I = (b)$. Bew.: „$\supseteq$": ✓, da $b \in I$, Def. von $\underbrace{(b)}_{R \cdot b} \subseteq I$.

„$\subseteq$": Sei $a \in I$, $a \neq 0$.

Dann: Dann a 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.

□

13.8. Bsp.: $\mathbb{Z}[T]$ ist kein HIB.

Bew.: $(2,T) = \mathbb{Z}[T]\cdot 2 + \mathbb{Z}[T]\cdot T$ ist kein Hauptideal.

$= I = \{f \in \mathbb{Z}[T];\ 2 \mid f(0)\}$ Ann.: $I = (g)$, $g = a_n T^n + \dots + a_1 T + a_0$, $\deg(g) \geq 1$.

Sei $p := T+2 \in I = (g) \Rightarrow T+2 = f\cdot g$ mit $f \in \mathbb{Z}[T]$

$\Rightarrow \deg(p) = 1 = \deg(f) + \deg(g)$

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

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

13.8. Def.: IB $A \ni p$ irreduzibel (prim), falls $p \notin A^\times$

und $\forall a,b \in A: p = a\cdot b \Rightarrow a \in A^\times \vee b \in A^\times$.

(Gegenteil: reduzibel = zerlegbar in Produkt von Nichteinheiten)

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

(Bsp.: $5 = (-1)\cdot(-5)$)

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

13.9. Bem.: p prim (irred.) $\Rightarrow$ Jeder Teiler von p ist Einheit oder assoz. zu p.

13.10. Bem.: Assoziiertheit ist Ä-Rel. ✓

13.11. Def.: A IB $d \in A$ größter gem. Teiler von $a,b \in A$: $d = ggT(a,b)$

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

13.12. Bem.: d ist bis auf Assoz. eind. best.

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

d.h. $d_1 = r d_2$, ebenso: $d_1 \mid d_2$, d.h. $d_2 = s d_1$.

Somit: $d_2 = (sr) d_2 \Rightarrow \underbrace{d_2}_{\neq 0}(1-sr) = 0 \overset{IB}{\Rightarrow} rs = 1 \Rightarrow r,s \in A^\times$

$\Rightarrow d_1$ assoz. d_2. $\square$

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

$:\Leftrightarrow$ (1) $\forall a \neq 0, a \notin A^\times\ \exists$ prime $p_1, \dots, p_m \in A: a = p_1 \cdots p_m$ (Ex. der PFZ)

& (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. $q_{\sigma(i)}$. (Eind. der PFZ)