Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil II: RINGE (und Moduln)

A12: Kommutative Ringe, Integritätsbereiche

Stichworte: Chinesischer Restsatz (Ringversion und für $\mathbb{Z}$), Einheiten in $\mathbb{Z}/(n)$, Eulersche φ-Fkt., Formel für $\varphi(n)$ mit PFZ von n, das von $S \subseteq R$ erzeugte Ideal (S), Hauptideal, maximales Ideal, Primideal, max. Ideale $\not\Rightarrow$ prim, Primideale in $\mathbb{Z}$, Quotientenkörper $\mathrm{Quot}(R)$

12.1. **Einleitung:** Wir zeigen den chinesischen Restsatz in der allgemeinen Version für kommutative Ringe und die (ev. aus der elementaren Zahlentheorie bekannten) Version für $\mathbb{Z}$. Die Einheiten im Restklassenring $\mathbb{Z}/(n)$ führen uns auf die Definition der Eulerschen φ-Funktion. Die verschiedenen Eigenschaften von Idealen – Hauptideal, maximal, prim – werden untersucht und in Beziehung gesetzt, indem die zugehörigen Faktorringe betrachtet werden. Die Primideale von $\mathbb{Z}$ sind genau die von Primzahlen erzeugten Hauptidealen sowie das Nullideal. Zuletzt führen wir den Quotientenkörper eines Integritätsbereichs ein und zeigen dessen Existenz und Eindeutigkeit.

12.2. **Vereinbarung:** In diesem Kapitel A12: Alle Ringe kommutativ.

12.3. **Lemma:** $I_1, \dots, I_m$ Ideale in R, $\pi_i : R \to R/I_i$, $\pi := \pi_1 \times \dots \times \pi_m$,

d.h. $\pi : R \longrightarrow R/I_1 \times \dots \times R/I_m$

$a \longmapsto (a+I_1, \dots, a+I_m)$.

Dann: π Ringhom., $\ker \pi = I_1 \cap \dots \cap I_m$.

Somit (nach Hom.satz A11.22):

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/I_1 \times \dots \times R/I_m \\ \downarrow & \nearrow_{\bar{\pi}, \text{injektiv}} & \\ R/I_1 \cap \dots \cap I_m & & \end{array}$$

kurz: CRS

12.4. **Chinesischer Restsatz**: $I_1,\dots,I_m$ Ideale in R, paarweise coprim, d.h. $\forall i,j,\ i\neq j: I_i+I_j=R$.
Dann: π surj. $\Rightarrow \bar\pi$ surj., also $\bar\pi$ Isomorphismus (nach 12.3).
Somit:
$$\boxed{R/I_1\cap\dots\cap I_m \cong R/I_1\times\dots\times R/I_m}.$$

Bew.: * $e_i:=(0,\dots,0,\underset{\text{Stelle } i}{1},0,\dots,0)\in \operatorname{im}\pi$. Bew.: Sei $0\neq i=1$. $\forall j\geq 2: I_1+I_j=R$.
$\Rightarrow a_j\in I_1, b_j\in I_j: 1=a_j+b_j \quad \forall 2\leq j\leq m$.
Dann: $\pi(b_2\cdot\ldots\cdot b_m)=e_1$, denn:
$$\pi_1(b_2\cdot\ldots\cdot b_m)=\pi_1(b_2)\cdot\ldots\cdot\pi_1(b_m)=\pi_1(1-a_2)\cdot\ldots\cdot\pi_1(1-a_m)$$
$$=\pi_1(1)\cdot\ldots\cdot\pi_1(1)=1\cdot\ldots\cdot 1=1,$$
$$j\geq 2:\ \pi_j(b_2\cdot\ldots\cdot b_m)=\pi_j(b_2)\cdot\ldots\cdot\underbrace{\pi_j(b_j)}_{=0}\cdot\ldots\cdot\pi_j(b_m)=0.$$

* Sei $c:=(\bar c_1,\dots,\bar c_m)\in R/I_1\times\dots\times R/I_m$, $c_1,\dots,c_m\in R$.
Wählen $a_j\in R$ mit $\pi(a_j)=e_j$ $(1\leq j\leq m)$, setzen: $a:=\sum_{i=1}^m c_i a_i$.
Dann: $\pi_j(a)=\sum_{i=1}^m \pi_j(c_i)\pi_j(a_i)=\sum_{i=1}^m \pi_j(c_i)\delta_{ij}=\pi_j(c_j)=\bar c_j$.
Also $\pi(a)=c$, d.h. π surjektiv. □

12.5. **Chinesischer Restsatz für $\mathbb{Z}$**: Seien $r_1,\dots,r_m\in\mathbb{Z}$ paarweise teilerfremd.
Dann gilt: $\mathbb{Z}/(r_1\cdot\ldots\cdot r_m)\cong\mathbb{Z}/(r_1)\times\dots\times\mathbb{Z}/(r_m)$.

12.6. Bez.: $(r):=\mathbb{Z}r$ für $r\in\mathbb{Z}$.
Bew.: Es gilt: $(r_1\cdot\ldots\cdot r_m)=(r_1)\cap\dots\cap(r_m)$,
Sowie: $(r_i)+(r_j)=\mathbb{Z}$ für $i\neq j$, denn:
$\exists u,v\in\mathbb{Z}: 1=ur_i+vr_j\in(r_i)+(r_j)$.
Somit: Anwendung von 12.4. □

12.7. Def.: Seien $a,b,r\in\mathbb{Z}$. **a kongruent b modulo r**:
$a\equiv b\ (\mathrm{mod}\ r) :\Leftrightarrow a+(r)=b+(r)\Leftrightarrow a-b\in(r)$.

12.8. **Kor.:** Seien $r_1,\dots,r_m \in \mathbb{Z}$ paarweise teilerfremd. Dann gilt:

$$\forall k_1,\dots,k_m \in \mathbb{Z}\ \exists x \in \mathbb{Z}: \quad \left|\begin{array}{l} x \equiv k_1 \pmod{r_1} \\ \vdots \\ x \equiv k_m \pmod{r_m}, \end{array}\right.$$

„simultane Kongruenzen"

wobei $0 \le x < r_1 \cdot \ldots \cdot r_m$ wählbar.

Bew.: $\exists x \in \mathbb{Z}$, $0 \le x < r_1 \cdot \ldots \cdot r_m$ mit:

$$\underbrace{\pi(x)}_{=\pi(x+(r_1\cdots r_m))} = (k_1+(r_1), k_2+(r_2), \dots, k_m+(r_m)),$$

d.h. $\forall 1 \le j \le m: x+(r_j) = \pi_j(x) = k_j + (r_j) \Rightarrow x \equiv k_j \pmod{r_j}$. □

12.9. **Lemma:** Für $r \in \mathbb{Z}$ sei $U_r := (\mathbb{Z}/(r))^\times$. Dann gilt für $u \in \mathbb{Z}$:

$$u+(r) \in U_r \Leftrightarrow u, r \text{ teilerfremd.}$$

Bew.: „$\Rightarrow$": $u \in U_r \Rightarrow \exists v \in \mathbb{Z}: u \cdot v = 1$ in $\mathbb{Z}/(r)$

$\Rightarrow uv - 1 \in (r) \Rightarrow r \mid (uv-1) \Rightarrow u, r$ teilerfremd.

„$\Leftarrow$": u, r teilerfremd $\Rightarrow \exists v, s \in \mathbb{Z}: 1 = uv + rs$

$\Rightarrow 1 = uv = u \cdot v \Rightarrow u \in U_r$. □

12.10. **Def.:** $\varphi(r) := \#U_r = \#\{s \in \mathbb{Z};\ 1 \le s \le r,\ s, r \text{ teilerfremd}\}$ heißt Eulersche φ-Funktion.

12.11. **Bem.:** Sei $r = p$ prim. Dann: $\varphi(p) = p-1$, da $\mathbb{Z}/(p) = \mathbb{F}_p$ Körper.

Sei $r = p^e$, p prim. Dann: $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = p^e\left(1-\frac{1}{p}\right)$.

Denn: $0 \le m < p^e$: $p \mid m \Leftrightarrow m = p \cdot m$ mit $0 \le m < p^{e-1}$.

12.12. **Bem.:** Seien $r_1,\dots,r_m \in \mathbb{Z}$ paarweise teilerfremd. Dann:

$$U_{r_1\cdot\ldots\cdot r_m} = (\mathbb{Z}/(r_1\cdot\ldots\cdot r_m))^\times \underset{\text{CRS}}{\cong} (\mathbb{Z}/(r_1) \times \ldots \times \mathbb{Z}/(r_m))^\times$$

$$\underset{\text{A10.17}}{=} (\mathbb{Z}/(r_1))^\times \times \ldots \times (\mathbb{Z}/(r_m))^\times = U_{r_1} \times \ldots \times U_{r_m}.$$

Also: $\varphi(r_1 \cdot \ldots \cdot r_m) = \varphi(r_1) \cdot \ldots \cdot \varphi(r_m)$.

12.13. **Bem.:** Sei $r \in \mathbb{Z}$, $r = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m}$ die PFZ von r, die p_i paarw. versch. Primzahlen.

$$\Rightarrow \varphi(r) = \varphi(p_1^{e_1}) \cdot \ldots \cdot \varphi(p_m^{e_m}) = p_1^{e_1}\left(1-\tfrac{1}{p_1}\right) \cdot \ldots \cdot p_m^{e_m}\left(1-\tfrac{1}{p_m}\right) = r\left(1-\tfrac{1}{p_1}\right) \cdot \ldots \cdot \left(1-\tfrac{1}{p_m}\right).$$

12.14. **Def.:** Sei R (komm.) Ring, $S \subseteq R$. Das Ideal $(S) := \bigcap \{I;\ I \subseteq R \text{ Ideal},\ S \subseteq I\}$ heißt das von S erzeugte Ideal.

12.15. **Bem.:** Für $a \in R$ gilt: $a \in (S) \Leftrightarrow \exists n \in \mathbb{N}\ \exists s_1, \dots, s_n \in S\ \exists a_1, \dots, a_n \in R$: $a = \sum_{i=1}^{n} a_i s_i$. (*)

Bew.: Sei $T := \{a \in R;\ (*)\}$. Zeige: $T = (S)$. „$\subseteq$": ✓ da (S) Ideal.

„$\supseteq$": T ist Ideal, $S \subseteq T \Rightarrow (S) \subseteq T$ nach Def. von (S). □

12.16. **Def.:** Schreibweise: $(S) = \sum_{s \in S} Rs$, insb. $S = \{b_1, \dots, b_n\}$: $(S) = Rb_1 + \dots + Rb_n$.

Ideale $I = (a)$, die von einem El. erzeugt werden, heißen Hauptideale.

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

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. □

12.18. **Def.:** Ideal $I \subseteq R$ (Komm. Ring) maximal $:\Leftrightarrow$ (1) $I \neq R$ und (2) $\nexists$ Ideal J, $I \subsetneq J \subsetneq R$.

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

Bew.: Sonst: $0 \subsetneq J \subsetneq K \Rightarrow J$ enthält Einheit von $K \Rightarrow J = K$ ↯. □

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

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

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

$\Leftrightarrow \left(\forall\, \bar{a} \in \bar{R} = R/I,\ \bar{a} \neq \bar{0}: (\bar{a}) = \bar{R} \Leftrightarrow \bar{a} \in \bar{R}^\times\right) \Leftrightarrow R/I$ Körper. □

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

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

12.22. **Def.:** R (komm.) Ring, $I \subsetneq R$ Ideal. I heißt prim $:\Leftrightarrow$

$\forall a, b \in R: a \cdot b \in I \Rightarrow (a \in I \vee b \in I)$

12.23. **Bem.:** I prim $\Leftrightarrow R/I$ Integritätsbereich.

Bew.: „$\Leftarrow$": $a \cdot b \in I$, d.h. $\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \bar{a} = 0 \vee \bar{b} = 0 \Rightarrow a \in I \vee b \in I$,

„$\Rightarrow$": $\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow a \cdot b \in I \Rightarrow a \in I \vee b \in I \Rightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$. □

12.24. **Bem.:** Maximale Ideale sind prim.

Bew.: I max. $\Rightarrow R/I$ Körper nach Bem. 12.20 $\Rightarrow R/I$ Integritätsbereich
$\Rightarrow I$ prim nach Bem. 12.23. □

12.25. **Bem.:** $0 \subseteq R$ prim $\Leftrightarrow R$ Integritätsbereich.

12.26. **Bem.:** $0 \subseteq \mathbb{Z}$ prim, aber nicht maximal (vgl. Bem. 12.24).

12.27. **Bem.:** $\varphi: R \to R'$ Ringhom., R' Integritätsbereich $\Rightarrow \ker\varphi$ Primideal.

Bew.:
$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\bar\varphi} & \\ R/\ker\varphi & & \end{array}$$
$\bar\varphi(R/\ker\varphi) \subseteq R'$ ist IB
$\Rightarrow R/\ker\varphi$ ist IB
$\Rightarrow \ker\varphi$ prim nach Bem. 12.23. □

12.28. **Bem.:** Die Primideale 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.

„$\supseteq$": r prim $\Rightarrow \mathbb{Z}/(r)$ Körper, insb. endl. IB
$\Rightarrow (r)$ maximal nach Bem. 12.20 $\Rightarrow (r)$ prim nach Bem. 12.24. □

12.29. **Def.:** Sei R ein IB. Körper Q heißt Quotientenkörper von R, Bez.: $\mathrm{Quot}(R)$,
$:\Leftrightarrow \exists$ inj. Ringhom. $\varepsilon: R \hookrightarrow Q$: $\forall r \in Q\ \exists a,b \in R$:
$$(b \neq 0 \wedge r = (\varepsilon a)(\varepsilon b)^{-1}).$$

12.30. **Satz:** Zu jedem IB gibt es bis auf Isomorphie genau einen Quotientenkörper.

Bew.: Existenz: * Def. $\dot{A}$-Relation auf $R \times (R \setminus \{0\})$ vermöge: $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$

reflexiv: $(a,b) \sim (a,b)$, weil $ab = ba$,

symm.: $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$, weil $ad = bc \Rightarrow cb = da$,

trans.: $(a,b) \sim (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$, weil:
$$ad = bc,\ cf = de \Rightarrow adcf = bcde \underset{IB}{\Rightarrow} af = be.$$

* Setzen $Q := R \times (R \setminus \{0\})/\sim$, Bez.: $\frac{a}{b} :=$ $\dot{A}$-Klasse von (a,b),

Def. $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$, $0_Q := \frac{0}{1}$, $1_Q := \frac{1}{1}$.

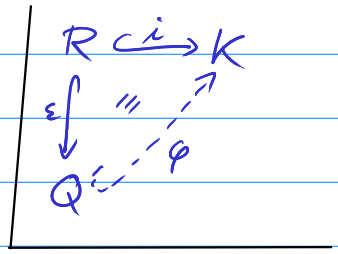
Dabei sind $+$ und $\cdot$ wohldef., nachrechnen!

* Q Körper bzgl. $+, \cdot, 0_Q, 1_Q$: Axiome nachrechnen!

* $\varepsilon: R \to Q$, $a \mapsto \varepsilon(a) := \frac{a}{1}$ ist inj. Ringhom., $\forall r \in Q\ \exists a,b \in R: b \neq 0 \wedge r = (\varepsilon a)(\varepsilon b)^{-1}$.

Nachrechnen!

Eindeutigkeit: * Universelle Eigenschaft von Quotientenkörpern:
$R \neq \{0\}$, Q Quot.körper zu R, $\varepsilon: R \hookrightarrow Q$.
$\Rightarrow \forall$ Körper K $\forall$ inj. Ringhom. $i: R \hookrightarrow K$ $\exists!$ $\varphi: Q \to K$,
φ inj. Ringhom., mit $i = \varphi \circ \varepsilon$.



Bew.: Setzen für $r = (\varepsilon a)(\varepsilon b)^{-1} \in Q$: $\varphi(r) := i(a) \cdot (i(b))^{-1}$

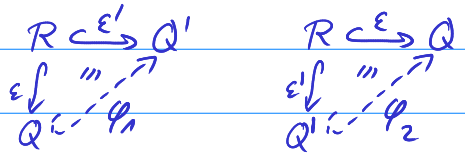
wohldef.: $(\varepsilon a)(\varepsilon b)^{-1} = (\varepsilon a')(\varepsilon b')^{-1} \Rightarrow \varepsilon(ab') = \varepsilon(a'b)$
$\Rightarrow ab' = a'b \Rightarrow (ia)(ib)^{-1} = (ia')(ib')^{-1}$.

genügt: $a \in R \Rightarrow \varphi(\varepsilon a) = i(a) \Rightarrow i = \varphi \circ \varepsilon$.

φ inj.: $\varphi(r) = 0 = i(a)(i(b))^{-1} \Rightarrow i(a) = 0 \Rightarrow a = 0 \Rightarrow r = 0$.
Somit $\ker \varphi = 0$, d.h. φ injektiv.

φ eind.: $\bar{\varphi}(r) = \bar{\varphi}((\varepsilon a)(\varepsilon b)^{-1}) = \bar{\varphi}(\varepsilon a)\left(\bar{\varphi}(\varepsilon b)\right)^{-1} = i(a)(i(b))^{-1}$
$\Rightarrow \bar{\varphi} = \varphi$. □

* Q, Q' zwei Quotientenkörper von R. Dann:



Es ex. also zwei inj. Ringhom. $\varphi_1: Q \hookrightarrow Q'$
und $\varphi_2: Q' \hookrightarrow Q$.
Dies ist nur möglich, wenn φ_1 und φ_2 zueinander inverse Isomorphismen sind.
Also: $Q \cong Q'$.

□