

## A12: Kommutative Ringe, Integritätsbereiche

12.1. Stichworte: CRS (Ringversion /  $\mathbb{Z}$ ), max. & prime Ideale, Quotientenlängen

Motivation: HS über eeb. Gr.:  $\hookrightarrow$

$$\mathbb{Z}/\mathbb{Z}(p_1^{e_1} p_2^{e_2}) \cong \mathbb{Z}/\mathbb{Z}p_1^{e_1} \times \mathbb{Z}/\mathbb{Z}p_2^{e_2} \quad (p_1 \neq p_2 \text{ prim}),$$

(begl. +)

(z.B.  $\mathbb{Z}/\mathbb{Z}15 \cong \mathbb{Z}/\mathbb{Z}5 \times \mathbb{Z}/\mathbb{Z}3$  (" ")

$$\mathbb{Z}/\mathbb{Z}n_1 n_2 \cong \mathbb{Z}/\mathbb{Z}n_1 \times \mathbb{Z}/\mathbb{Z}n_2 \quad (\text{Bem. A7.8}) \quad (\text{begl. +})$$

$$\mathbb{Z}/\mathbb{Z}p_1^{e_1} p_2^{e_2} p_3^{e_3} \cong \mathbb{Z}/\mathbb{Z}p_1^{e_1} p_2^{e_2} \times \mathbb{Z}/\mathbb{Z}p_3^{e_3} \cong \mathbb{Z}/\mathbb{Z}p_1^{e_1} \times \mathbb{Z}/\mathbb{Z}p_2^{e_2} \times \mathbb{Z}/\mathbb{Z}p_3^{e_3}$$

$\uparrow \qquad \qquad \qquad \uparrow$   
 $p_3 \neq p_1, p_3 \neq p_2 \qquad p_1 \neq p_2$

$$\mathbb{Z}/\mathbb{Z}n_1 n_2 n_3 \cong \mathbb{Z}/\mathbb{Z}n_1 n_2 \times \mathbb{Z}/\mathbb{Z}n_3 \cong \mathbb{Z}/\mathbb{Z}n_1 \times \mathbb{Z}/\mathbb{Z}n_2 \times \mathbb{Z}/\mathbb{Z}n_3 \quad (\text{begl. +})$$

pw. t.f.r.!

Beachten: Tripel, das teilerfremd, aber nicht pw. teilerfremd:  
(6, 10, 15)

Ringisom. ? ja, Allgemeinere Ringe ? ja

12.2. Vereinbarung: In A12: Alle Ringe kommutativ (mit 1).

12.3. Lemma:  $I_1, \dots, I_m$  Ideale in  $R$ ,  $\pi_i: R \rightarrow R/I_i$  (d.h.  $\pi_i(a) = a + I_i$ ),  
 $\pi := \pi_1 \times \dots \times \pi_m$ , d.h.  $\pi: R \rightarrow R/I_1 \times \dots \times R/I_m$   
 $a \mapsto (a + I_1, \dots, a + I_m)$ .

Dann:  $\pi$  Ringhom.,  $\text{Ker } \pi = I_1 \cap \dots \cap I_m$ .

✓, denn in jeder komp. "Null".

Somit (nach Hom. Satz A11.22):  $R \xrightarrow{\pi} R/I_1 \times \dots \times R/I_m$

$$\downarrow \quad \quad \quad \nearrow$$

$\pi$  injektiv

$R/I_1 \cap \dots \cap I_m$   
beim

Nach 2.2.:  $\pi$  surj. ? Wann ?

12.4. Chinesischer Restsatz (CRS):  $I_1, \dots, I_m$  Ideale in  $R$ , paarweise coprime, d.h.  $\forall i \neq j: \underline{I_i + I_j = R}$ . Dann:  $\pi$  surj.  $\Rightarrow \bar{\pi}$  surj., also  $\bar{\pi}$  Iso.

Somit:

$$R/I_1 \cap \dots \cap I_m \cong R/I_1 \times \dots \times R/I_m.$$

(Regio!)

Bew.: z.z.:  $\pi$  surj.

\*  $e_i := (0, \dots, 0, \underline{1}, 0, \dots, 0) \in \text{im } \pi$ : Bew.:  $\forall i=1. \forall j \geq 2: I_1 + I_j = R$ .  
 $\rightarrow 1 \in I_i$   $\nearrow$  Stelle  $i$   $\Rightarrow a_i \in I_1, b_j \in I_j: 1 = a_i + b_j \quad (\forall j \geq 2)$

Dann:  $\pi(b_2 \dots b_m) = e_1,$

denn  $\pi_1(b_2 \dots b_m) = \pi_1(b_2) \dots \pi_1(b_m) \stackrel{!}{=} \pi_1(1-a_2) \dots \pi_1(1-a_m) = \pi_1(1) \dots \pi_1(1)$

$j \geq 2: \pi_j(b_2 \dots b_m) = \pi_j(b_2) \dots \pi_j(b_m) \stackrel{\substack{\text{ist in } I_j \\ = 0}}{=} 0.$   $\boxed{=1}$

\* Sei  $c := (\bar{c}_1, \dots, \bar{c}_m) \in R/I_1 \times \dots \times R/I_m, c_1, \dots, c_m \in R$ .

$\downarrow \quad \downarrow$   
 $c_1 + I_1 \quad c_m + I_m$

Wählen  $a_j \in R$  mit  $\pi(a_j) = c_j \quad (1 \leq j \leq m)$ , setzen:  $a := \sum_{i=1}^m c_i a_i$ .

Dann:  $\pi(a) = \sum_{i=1}^m \pi_i(c_i) \pi_j(a_i) = \pi_j(c_j) = \bar{c}_j.$

$\stackrel{!}{=} \delta_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$

Also  $\pi(a) = c$ , d.h.  $\pi$  surj.

□

12.5. Chinesischer Restsatz für  $\mathbb{Z}$ : Sei  $r_1, \dots, r_m \in \mathbb{Z}$  paarweise teilerfremd.

Dann gilt:

(d.h.  $\text{ggT}(r_i, r_j) = 1$  für  $i \neq j$ )

$$\mathbb{Z}/\mathbb{Z}_{r_1 \dots r_m} \cong \mathbb{Z}/\mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}/\mathbb{Z}_{r_m},$$

Abb.:  $a + \mathbb{Z}_{r_1 \dots r_m} \mapsto (a + \mathbb{Z}_{r_1}, \dots, a + \mathbb{Z}_{r_m})$ .

12.6. Bez.:  $(r) := \mathbb{Z}_{r, \text{rel}}$   $\hookrightarrow \mathbb{Z}/(r_1 \dots r_m) \cong \mathbb{Z}/(r_1) \times \dots \times \mathbb{Z}/(r_m)$ .

Bew.: Es gilt:  $(r_1 \dots r_m) = (r_1) \cap \dots \cap (r_m)$ .

benötige lt. gem. Vielf. von  $r_1, \dots, r_m$ , z.z.:  $= r_1 \dots r_m$

" $\leq$ " ✓, " $\geq$ ": VI nach m, brauche pw. t.fremd  $\leadsto$  Zahlentheorie

Bsp.:  $(3 \cdot 10) = (30) = (3) \cap (10) = (3) \cap (2) \cap (5)$ .

Sowie:  $(r_i) + (r_j) = \mathbb{Z}$  für  $i \neq j$ , denn (Bézout A7.3):  $1 = \mu r_i + \nu r_j \in (r_i) + (r_j) = \mathbb{Z}$ .

Jetzt: Anw. von 12.4.

□

12.7. Def.: Seien  $a, b \in \mathbb{Z}$ ,  $r \in \mathbb{N}$ .

$a$  kongruent zu  $b$  modulo  $r$  :  $a \equiv b \pmod{r}$

$$\begin{aligned} &: \Leftrightarrow a + (\underbrace{r}_{=\mathbb{Z}r}) = b + (\underbrace{r}_{=\mathbb{Z}r}) \Leftrightarrow a - b \in (\underbrace{r}_{=\mathbb{Z}r}) \\ &\Leftrightarrow r \mid (a - b). \end{aligned}$$

↪ Sprechweise für:  $a$  und  $b$  in derselben Restklasse mod  $r$ ,  
d.h.  $a + \mathbb{Z}r = b + \mathbb{Z}r$  in  $\mathbb{Z}/\mathbb{Z}r$   
bzw.  $a + (r) = b + (r)$  in  $\mathbb{Z}/(r)$ .

(CRS-Bsp.:  $\mathbb{Z}/(15) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(5)$ )

$$a + (15) \mapsto (a + (3), a + (5))$$

$$\underline{12 + (15)} \mapsto (\underline{12 + (3) = 0}, \underline{12 + (5) = 2})$$

$$\quad \quad \quad = 0 + (3) \quad \quad = 2 + (5)$$

$$\boxed{12 \equiv 0 \pmod{3} \text{ und } 12 \equiv 2 \pmod{5}}$$

$$m \equiv k_1 \pmod{r_1} \text{ und } m \equiv k_2 \pmod{r_2} \text{ und } m \equiv k_3 \pmod{r_3} \dots$$

$$\rightarrow \left[ m \equiv 2 \pmod{3} \text{ \& } m \equiv 6 \pmod{10} \text{ \& } m \equiv 4 \pmod{11} \right]$$

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

$$\forall k_1, \dots, k_m \in \mathbb{Z} \quad \exists x \in \mathbb{Z} : \quad x \equiv k_1 \pmod{r_1}$$

$$\wedge x \equiv k_2 \pmod{r_2}$$

$$\vdots$$

$$\wedge x \equiv k_m \pmod{r_m}$$

„simultane Kongruenzen“

wobei  $0 \leq x < r_1 \cdots r_m$  wählbar.

Bew.:  $\exists x \in \mathbb{Z}$ ,  $0 \leq x < r_1 \cdots r_m$ , mit:

$$\underbrace{\pi(x + (r_1 \cdots r_m))}_{= \pi(x)} = \underbrace{(k_1 + (r_1), k_2 + (r_2), \dots, k_m + (r_m))}_{\substack{\uparrow \\ \text{12.5}}}$$

$$\text{d.h. } \forall j \leq m: x + (r_j) = \pi_j(x) = k_j + (r_j) \Rightarrow x \equiv k_j \pmod{r_j}. \quad \square$$

Explizite Lösungsformeln für  $x$ ? Ja  $\rightarrow \mathbb{Z}T$

Dann gilt für  $m \in \mathbb{Z}$ :  $m + (r) \in \mathcal{U}_r \Leftrightarrow m, r$  teilerfremd.

$$\Rightarrow \mu v - 1 \in (\pi) \Rightarrow \pi \mid (\mu v - 1) \Rightarrow \mu, \pi \nmid v.$$

" $\Leftarrow$ ":  $m, n$  teiler  $\Rightarrow \exists v, s \in \mathbb{Z} : 1 = m \boxed{v} + \underline{ns}$   
 $\Rightarrow \underline{1} = \underline{mv} = \underline{m} \cdot \boxed{\underline{v}} \Rightarrow \underline{m} \in \mathcal{U}_R$   
 $\uparrow \quad \uparrow$   
 $v = m^{-1}$

Bsp.:  $(\mathbb{Z}_{(10)})^\times = \{\underline{1}, \underline{3}, \underline{\overline{7}}, \underline{\overline{9}}\}$

12.10. Def.:  $\varphi(r) := \# \mathcal{U}_r = \# \{ s \in \mathbb{Z}; 1 \leq s \leq r, \overbrace{s, r \text{ teilerfremd}}^{\text{ggT}(s, r) = 1} \}$   
heißt Eulersche  $\varphi$ -Fkt.

Bsp.:  $\varphi(1)=1, \varphi(2)=1, \varphi(3)=2, \dots$

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

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

Denn:  $0 \leq m < p^e: p|m \Leftrightarrow m = p \cdot \underline{m}$  mit  $0 \leq m < p^{e-1}$

12.12. Bem.: Seien  $n_1, \dots, n_m \in \mathbb{N}$  p.w. teilerfremd. Dann:

$$U_{d_1 \dots d_m} = \left( \mathbb{Z}/(d_1 \dots d_m) \right)^X \underset{\text{CRS}}{\simeq} \left( \mathbb{Z}/(d_1) \times \dots \times \mathbb{Z}/(d_m) \right)^X \\ \underset{1 \dots m}{=} \left( \mathbb{Z}/(d_1) \right)^X \times \dots \times \left( \mathbb{Z}/(d_m) \right)^X$$

Also:  $\varphi(\sigma_1 \dots \sigma_n) = \varphi(\sigma_1) \dots \varphi(\sigma_n)$ . A10.1

12.13. Bem.: Sei  $r \in \mathbb{N}$ ,  $r = p_1^{e_1} \cdots p_m^{e_m}$  sei die PFZ von  $r$ ,  
 die  $p_i$  p.w.v.  $\Rightarrow \varphi(r) = \varphi(p_1^{e_1}) \cdots \varphi(p_m^{e_m}) = p_1^{e_1-1} \left(1 - \frac{1}{p_1}\right) \cdots p_m^{e_m-1} \left(1 - \frac{1}{p_m}\right)$   

$$= r \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right) = r \cdot \prod_{p|r} \left(1 - \frac{1}{p}\right)$$
  
 (Eulerprodukt)

$(r_1) = \mathbb{Z}r_1$  (vgl.  $\langle S \rangle \leq G$ ,  $S \subseteq G$ )

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

Bsp.:  $(3) = 3 \cdot \mathbb{Z} = \mathbb{Z} \cdot 3$  in  $R = \mathbb{Z}$ ,  $(3, 5) = \mathbb{Z} \cdot 3 + \mathbb{Z} \cdot 5$   
 $(3, 15) = \mathbb{Z} \cdot 3 + \mathbb{Z} \cdot 15 = \mathbb{Z} \cdot 3$

12.15. Bem.: Für  $a \in R$  gilt:  $a \in (S) \Leftrightarrow \exists m \in \mathbb{N} \exists s_1, \dots, s_m \in S \exists a_1, \dots, a_m \in R$ :  
 $a = a_1 s_1 + a_2 s_2 + \dots + a_m s_m$  (\*)

Bew.: Sei  $T := \{a \in R; (*)\}$ . Zeige  $T = (S)$ . „ $\subseteq$ “ ✓ da  $(S)$  Ideal ✓  
 „ $\supseteq$ “:  $T$  ist Ideal,  $S \subseteq T \Rightarrow (S) \subseteq T$ . D  
 Def. 12.14

12.16. Def.: Schreibweise:  $(S) = \sum_{s \in S} R s$ , insb.:  $S = \{s_1, \dots, s_m\}$ :  
 $(S) = R s_1 + \dots + R s_m$

$[(3, 5) = \mathbb{Z} \cdot 3 + \mathbb{Z} \cdot 5]$