Lineare Algebra 2, Tutorium 8

2.6.2021

Warm-Up

Richtig oder Falsch?

1. Jeder faktorielle Ring ist ein Hauptidealring. ✗
2. Falls R ein Hauptidealring ist, ist auch $R[x]$ ein Hauptidealring ✗
3. In jedem Hauptidealring hat jedes Element $0 \neq x \in R$ eine eindeutige Primzerlegung. ✓
4. Der Ring $\mathbb{R}[x]/(x^2+1)$ ist ein Körper.
5. Der Ring $\mathbb{F}_2[x]/(x^2+1)$ ist ein Körper.

R Hauptidealring (principal ideal domain) PID

$\forall I \trianglelefteq R$ Ideal $\exists f \in R$: $I = (f)$

R faktoriell (unique factorization domain (UFD))

Integritätsbereich

Jedes $x \in R$, $x \neq 0$ (Integritätsbereich) lässt sich (bis auf Multiplikation mit Elementen aus $R^\times = \{a \in R \text{ invertierbar}\}$) eindeutig schreiben als $x = \underbrace{x_1 \cdots x_r}_{\text{Primfaktorzerlegung}}$ mit x_i = Primelemente.

Einheitengruppe von R

$a \in R$ heißt prim $\iff \forall r,s \in R: a \mid rs \Rightarrow a \mid r$ oder $a \mid s$

Satz: R UFD $\Rightarrow$ [$x \in R$ irred. $\iff x \in R$ prim.]

i.A. ist das falsch

Beispiele:

$\mathbb{Z}$	$K[x]$ (Körper)	$K[x,y] := K[x][y]$
UFD	UFD	UFD
PID	PID	kein PID

UFD $\not\Rightarrow$ PID

Fakt: R UFD $\Rightarrow$ $R[x]$ UFD

$(x,y) \trianglelefteq K[x,y]$ Ideal, ist nicht erzeugt von einem Element.

Angenommen $(x,y) = (f)$, $f \in \underbrace{K[x,y]}_{=:R}$

$x \in (f) \iff f \mid x \Rightarrow f \sim 1$ oder $f \sim x$

$y \in (f) \iff f \mid y \Rightarrow f \sim 1$ oder $f \sim y$

$\Rightarrow x \sim y$

irred.

$\iff \exists a \in R^\times: af = x$

$\exists a \in K^\times: ax = y$

Falls $f \sim 1 \iff \underset{\substack{\| \\ k\setminus\{0\}}}{\exists a \in k^\times} : f = a \implies (f) = k[X,Y]$

$$\underbrace{\begin{matrix} (f) & = & k[X,Y] \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ f\cdot(f^{-1}p) & = & p \end{matrix}}$$

auch Widerspruch,

da $\underset{\substack{\uparrow \\ \text{Grad } 0}}{1} \in \underset{\substack{\uparrow \\ \text{Grad } \geq 1}}{(X,Y)} = (f)$

(Allg.: $r \in R^\times \iff (r) = R$)

Alternativ: $R = \mathbb{Z}[x]$ UFD, aber $(2, X)$ ist kein PI.

4. $\mathbb{R}[X]/(X^2+1) \ni [x] = \bar{x}$

$$\left[\text{ in } R/I : \quad \underset{\substack{\| \\ [a]_{\mathrm{mod}\, I}}}{(a+I)}(b+I) := ab + I \right]$$

$$\left(\mathbb{C} := \mathbb{R}[x]/(x^2+1) \qquad i := \bar{x}. \right)$$

$\mathbb{C}$ ist eine $\mathbb{R}$-Algebra

⇝ Es gibt Einsetzung $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{C}$, $x \mapsto i$

$\mathbb{C}$ ist als $\mathbb{R}$-Algebra erzeugt von i $\implies \varphi$ surjektiv

$\mathbb{R}[x]/\ker\varphi \cong \mathbb{C}$, $\ker\varphi \overset{?}{=} (x^2+1)$

$$\varphi(x^2+1) = i^2 + 1 = 0$$

maximales Ideal!

$\implies (x^2+1) \subseteq \ker\varphi$

„$\supseteq$" ? $f \in \ker\varphi \implies f(i) = 0$

über $\mathbb{C}[x]$: $(x-i) \mid f \in \mathbb{R}[x]$

komplexe Konjugation: $\overline{(x-i)} \mid \overline{f} = f$

$\overline{(x-i)} = x+i$

$\Rightarrow x^2+1 \mid f. \quad \Rightarrow f \in (x^2+1)$

in $\mathbb{F}_p$: $(x+y)^p = x^p + y^p$

$\mathbb{F}_2[x] / (x^2+1)$ kein Körper: $x^2+1 = x^2+1^2 = (x+1)^2$ ($\operatorname{char} \mathbb{F}_2 = 2$)

$(\overline{x+1})^2 = \overline{x^2+1} = 0.$

$\overline{x+1} \neq 0 \leftarrow x^2+1 \nmid x+1$

$\mathbb{F}_2[x] / (x^2+x+1) \leftarrow$ Körper mit 4 Elementen

Aufgabe 1

Finde eine Lösung für das folgende System von Kongruenzen:

$a \equiv 5 \mod 8, \; n_1 \qquad n_1' = 25 \cdot 81 = 2025$
$a \equiv 12 \mod 25, \; n_2 \qquad n_2' = 8 \cdot 81 = 648$
$a \equiv 47 \mod 81 = n_3$

wobei $a \in \mathbb{Z}$ sein soll. Ist diese Lösung eindeutig?

Chinesischer Restsatz:

$$\mathbb{Z}/n_1 \cdots n_m \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_m$$

$$\bar{a} \longmapsto (\bar{a}, \ldots, \bar{a})$$

Falls n_i paarweise teilerfremd.

$$\mathbb{Z}/8 \cdot 25 \cdot 81 \cong \mathbb{Z}/8 \times \mathbb{Z}/25 \times \mathbb{Z}/81$$

Surjektivität?

$$a \overset{?}{\longmapsto} (\bar{5}, \overline{12}, \overline{47})$$

Allgemeines Lösungsverfahren:

$a \equiv a_1 \mod n_1$

$\vdots$

$a \equiv a_m \mod n_m$

Setze $n_i' := n_1 \cdots n_{i-1} n_{i+1} \cdots n_m$. Wissen $\operatorname{ggT}(n_i, n_i') = 1$.

Bezout $\Rightarrow 1 = \alpha n_i + \beta n_i'$

$\Rightarrow 1 \equiv \beta n_i' \mod n_i \quad \Rightarrow t_i := \beta$ ist die Inverse von n_i'

$$a := \sum_{i=1}^{m} q_i\, t_i\, n_i' \quad \in \mathbb{Z}$$

$$\bar a \underset{\text{mod } n_j}{=} \sum_{i=1}^{m} \bar a_i\, \overline{t_i n_i'} = \bar q_j\, \overbrace{\bar t_j\, \bar n_j'}^{=1} = \bar a_j \qquad \forall j$$

$$n_j \mid n_i' \iff i \neq j$$

Beispiel: $\quad ggT(a,b) =: (a,b)$

$$(n_2, n_2') = (25, 648) = (25, 648 - 25 \cdot 25)$$
$$= (25, 23) = (25 - 1 \cdot 23, 23)$$
$$= (2, 23) = (2, 23 - 2 \cdot 11)$$
$$= (2, 1) = 1$$

$$1 = 2 - 1 = 2 - (23 - 2 \cdot 11) =$$
$$= 12 \cdot 2 - 23 = 12(25 - 23) - 23 =$$
$$= 12 \cdot 25 - 13 \cdot 23 =$$
$$= 12 \cdot 25 - 13(648 - 25 \cdot 25)$$
$$= \underbrace{25}_{n_2} \cdot (12 + 25 \cdot 13) \underbrace{- 13}_{t_2} \cdot \underbrace{648}_{n_2'}$$

$t_1 = 1 \qquad t_2 = -13$

$t_3 = 32$

$$1 = (8, 2025) \overset{?}{=} \alpha\, 8 + \beta\, 2025$$

$$1 = (81, 200) = \underset{\substack{\| \\ -79}}{\alpha} \cdot 81 + \underset{\substack{\| \\ 32}}{\beta} \cdot 200$$

$(3,2) = 1$

$1 = 3 - 2$

$2 \cdot 2 - 3 = 1$

$2000 = 8 \cdot 250$

$24 = 8 \cdot 3$

$1 = 2025 - 2024$

$= 2025 - 253 \cdot 8$

$$a = a_1 t_1 n_1' + \cdots = 209.837 \underset{\text{mod } 8 \cdot 25 \cdot 81 = 16200}{\equiv} 15.437$$

Aufgabe 4

Zeige, dass $x^4 + 1 \in \mathbb{Z}[x]$ irreduzibel ist.

$\rightsquigarrow g$

g hat keine reellen Nullstellen ($g \geq 1$ auf $\mathbb{R}$)

$\Longrightarrow g$ hat keinen Linearfaktor.

Falls g reduzibel ist, so $g = (aX^2 + bX + c)(dX^2 + eX + f)$

$g = X^4 + 1$

$= (ad)X^4 + X^3(\cdots) + X^2(af + be + cd) + X(bf + ce) + cf$

$\mathbb{Z}^\times = \{\pm 1\}$

$\mathbb{Z} \ni ad = 1 \Rightarrow a = d = \pm 1$

$cf = 1 \Rightarrow c = f = \pm 1$

$0 = bf + ce = \pm 1(b + e) \Rightarrow b = -e$

$0 = af + be + cd = 2af + be = \pm 2 - e^2$

$\Rightarrow e^2 = \pm 2 \Rightarrow$ ↯ $\sqrt{2} \notin \mathbb{Q} \supseteq \mathbb{Z}$

Anmerkungen zum CRT

Induktionsvoraus.: $\exists a \in \mathbb{Z}: \quad a \equiv r_i \mod I_i \quad i = 1, \ldots, n-1$, fixiere a.

(Wir hätten gerne $a \equiv r_n \mod I_n$)

Betrachte $J_1 := I_1 \cap \cdots \cap I_{n-1}$, $J_2 := I_n$

Nach IV (für $n=2$) $\exists r \in \mathbb{Z}$:

$r \equiv a \mod J_1$

$r \equiv r_n \mod J_2$ fixiere r.

Jetzt gilt $r \equiv a \mod J_1$

$\Updownarrow$ $\qquad J_1 = I_1 \cap \dots \cap I_{n-1} \subseteq I_j \quad \forall j \in \{1, \dots, n-1\}$

$r - a \in J_1 \subseteq I_j$

$\Rightarrow r - a \in I_j \Rightarrow r \equiv \overset{\substack{r_j \\ \equiv}}{a} \mod I_j \quad \forall j.$

Gleichzeitig: $r \equiv r_n \mod J_2 = I_n$

$$\left.\begin{array}{l} \Rightarrow \quad r \equiv r_j \quad \forall 1 \le j \le n-1 \\ \qquad\ r \equiv r_n \end{array}\right\} \Rightarrow r \equiv r_j \quad \forall 1 \le j \le n.$$