

# Lineare Algebra 2,

# Tutorium 8

2.6.2021

Warm-Up

Richtig oder Falsch?

1. Jeder faktorielle Ring ist ein Hauptidealring. 3.
2. Falls  $R$  ein Hauptidealring ist, ist auch  $R[x]$  ein Hauptidealring. 4.
3. In jedem Hauptidealring hat jedes Element  $0 \neq x \in R$  eine eindeutige Primzerlegung. 5.
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)

$\nexists \text{ Ideal } I \neq \{0\} \text{ mit } I \neq R$   
 $\exists f \in R: I = (f)$   
 $\text{PID}$

$R$  faktoriell

(unique factorization domain (UFD))

Integritätsbereich

Jedes  $x \in R$  lässt sich (bis auf Multiplikation mit Elementen aus  $R^\times = \{a \in R \text{ invertierbar}\}$ ) schreiben

Einheitengruppe von  $R$

als  $x = x_1 \cdots x_r$  mit  $x_i = \text{Primelemente}$ .

Primfaktorzerlegung

$a \in R$  heißt prim

$\Leftrightarrow \forall r, s \in R: a \mid rs \Rightarrow a \mid r \text{ oder } a \mid s$

Satz:  $R \text{ UFD} \Rightarrow [x \in R \text{ irred.}]$

$\Leftrightarrow [x \in R \text{ prim.}]$

$\uparrow$   
i.A. ist das falsch

Beispiele:

$\mathbb{Z}$

UFD

PID

Körper

$K[x]$

UFD

PID

$K[x, y] := K[x][y]$

UFD

kein PID

$\text{UFD} \not\Rightarrow \text{PID}$

Fakt:  $R \text{ UFD} \Rightarrow R[x] \text{ UFD}$

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

Angenommen

$(x, y) = (f)$

$f \in K[x, y]$

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

$x \in (f) \Leftrightarrow f \mid x$

$\Rightarrow f \sim 1 \text{ oder } f \sim x$

$y \in (f) \Leftrightarrow f \mid y$

$\Rightarrow f \sim 1 \text{ oder } f \sim y \Rightarrow x \sim y$

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

$$\text{Falls } f \sim 1 \Leftrightarrow \exists a \in \underbrace{k^{\times}}_{k \setminus \{0\}} : f = a \Rightarrow (f) = k[X, Y]$$

$$f \cdot (f^{-1}p) = p$$

$$(\text{Alg.: } r \in R^{\times} \Leftrightarrow (r) = R)$$

$\underbrace{\quad}_{\text{auch Widerspruch,}}$   
 da  $1 \in (X, Y) = (f)$   
 $\uparrow \quad \quad \uparrow$   
 Grad 0      Grad  $\geq 1$

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

$$u. \quad \frac{R[x]}{(x^2+1)} \quad \omega \quad [x] = \bar{x}$$

$$\left[ \text{in } R/I : \begin{array}{l} [a]_{\text{mod } I} \\ (a+I)(b+I) \\ := ab+I \end{array} \right]$$

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

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

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

$\mathbb{C}$  ist als  $R$ -Algebra erzeugt von  $i \Rightarrow \varphi$  surjektiv  
 $\frac{R[x]}{\ker \varphi} \cong \mathbb{C}, \quad \ker \varphi = (x^2+1)$

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

$$\Rightarrow \text{maximaler Ideal! } (x^2+1) \subseteq \ker \varphi$$

" $\supseteq$ " ?  $f \in \ker \varphi \Rightarrow f(i) = 0$   
 über  $\mathbb{C}[x]$ :  $(x-i) \mid f \in R[x]$

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

"  
 $x+i$

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

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

kein Körper:  $x^2+1 = x^2+1^2 = (x+1)^2$   
 $\uparrow$   
 da  $\mathbb{F}_2 = 2$

$$\mathbb{F}_2[x] / (x^2+1)$$

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

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

## Aufgabe 1

Finde eine Lösung für das folgende System von Kongruenzen:

$$\begin{aligned} a &\equiv 5 \pmod{8, n_1} & n_1' &= 25 \cdot 81 = 2025 \\ a &\equiv 12 \pmod{25, n_2} & n_2' &= 8 \cdot 81 = 648 \\ a &\equiv 47 \pmod{81, n_3} \end{aligned}$$

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

Chinesischer Restsatz:

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

$$\bar{a} \mapsto (\bar{a}_1, \dots, \bar{a}_m)$$

Falls  $n_i$  paarweise teilerfremd.

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

$$a? \mapsto (\bar{5}, \bar{12}, \bar{47})$$

Einzigartigkeit?

Allgemeines Lösungsverfahren:

$$a \equiv a_1 \pmod{n_1}$$

;

$$a \equiv a_m \pmod{n_m}$$

Setze  $n_i' := n_1 \cdots n_{i-1} n_{i+1} \cdots n_m$

Wissen  $\text{ggT}(n_i, n_i') = 1$ .

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

$$\Rightarrow 1 \equiv \beta n_i' \pmod{n_i}$$

$$\Rightarrow t_i := \beta \text{ ist die Inverse von } n_i'$$

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

$$\overline{a} = \sum_{i=1}^m \overline{a_i} \overline{t_i u_i'} = \overline{q_j} \overline{t_j} \overline{u_j'} = \overline{a_j} \quad \forall j$$

$$u_j \mid u_i' \Leftrightarrow i=j$$

Beispiel:  $\text{ggT}(a, b) =: (a, b)$

$$\begin{aligned} (u_2, u_2') &= (25, 648) = (25, 648 - 25 \cdot 25) \\ &= (25, 23) = (25 - 1 \cdot 23, 23) \\ &= (2, 23) = (2, 23 - 2 \cdot 11) \\ &= (2, 1) = 1 \end{aligned}$$

$$\begin{aligned} 1 &= 2 - 1 = 2 - (23 - 2 \cdot 11) = \\ &= 12 \cdot 2 - 23 = 12(25 - 23) - 23 = \\ &= 12 \cdot 25 - 13 \cdot 23 = \\ &= 12 \cdot 25 - 13(648 - 25 \cdot 25) \\ &= 25 \cdot (12 + 25 \cdot 13) - 13 \cdot 648 \end{aligned}$$

$\underbrace{\quad}_{u_2} \quad \quad \quad \underbrace{\quad}_{t_2} \quad \underbrace{\quad}_{u_2'}$

$$\begin{aligned} t_1 &= 1 & t_2 &= -13 & 1 &= (8, 2025) \stackrel{?}{=} \alpha \cdot 8 + \beta \cdot 2025 \\ t_3 &= 32 & & & 1 &= (81, 200) = \alpha \cdot 81 + \beta \cdot 200 \\ & & & & & \quad \quad \quad -79 \quad \quad \quad 32 \end{aligned}$$

$$\begin{aligned} (3, 2) &= 1 \\ 1 &= 3 - 2 \\ 2 \cdot 2 - 3 &= 1 \end{aligned}$$

$$\begin{aligned} 2000 &= 8 \cdot 250 \\ 24 &= 8 \cdot 3 \\ 1 &= 2025 - 2024 \\ &= 2025 - 253 \cdot 8 \end{aligned}$$

$$a = a_1 t_1 u_1' + \dots = 209 \cdot 837 = 15 \cdot 437 \pmod{8 \cdot 25 \cdot 81 = 16200}$$

## Aufgabe 2

Bestimme die letzten zwei Ziffern der Zahl  $49^{2021}$ .

*Hinweis:*  $100 = 5^2 \cdot 2^2$ .

### Aufgabe 3

Sei  $R$  ein kommutativer Ring und  $I \subseteq R$  ein Ideal. Zeige:

1.  $I \cdot R[X] = \{\sum_{i=0}^n a_i X^i : n \in \mathbb{N}_0, a_i \in I\} \subseteq R[X]$  ist ein Ideal.
2.  $R[X]/(I \cdot R[X])$  ist isomorph zu  $(R/I)[X]$ .

## Aufgabe 5

Es sei  $f = x^2 - 2 \in \mathbb{Q}[x]$ .

1. Zeige: Der Einsetzungshomomorphismus  $\mathbb{Q}[x] \rightarrow \mathbb{C}, g \mapsto g(\sqrt{2})$  induziert einen Isomorphismus von Ringen  $\mathbb{Q}[x]/(f) \xrightarrow{\cong} \mathbb{Q}(\sqrt{2})$ .
2. Zeige: Der Ring  $\mathbb{Q}[x]/(f)$  ist ein Körper.
3. Bestimme die  $\mathbb{Q}$ -Dimension, wenn man  $\mathbb{Q}[x]/(f)$  als  $\mathbb{Q}$ -Vektorraum betrachtet.

## Aufgabe 4

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

$$g \text{ hat keine reellen Nullstellen}$$

$$(g \geq 1 \text{ auf } \mathbb{R})$$

$$\Rightarrow g \text{ hat keinen Linearfaktor.}$$

Falls  $g$  reduzibel ist, so  $g = (ax^2 + bx + c)(dx^2 + ex + f)$

$$x^4 + 1 \quad //$$

$$(ad)x^4 + x^3(\dots) +$$

$$+ x^2(af + be + cd) +$$

$$+ x(bf + ce) + cf$$

$$\mathbb{Z}_{\neq 0} \quad \mathbb{Z}^\times = \{\pm 1\}$$

$$ad = 1 \Rightarrow a = d = \pm 1$$

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

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

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

$$\Rightarrow e^2 = \pm 2 \Rightarrow \text{↯}$$

$$\sqrt{2} \notin \mathbb{Q} = \mathbb{Z}$$

### Anmerkungen zur CRT

Induktionsvoraus.:

$$\forall a \in \mathbb{Z} : a \equiv r_i \pmod{I_i} \quad i = 1, \dots, n-1,$$

fixiere  $a$ .

$$( \text{Wir hätten gerne } a \equiv r_n \pmod{I_n} )$$

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

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

$$r \equiv a \pmod{J_1}$$

$$r \equiv r_n \pmod{J_2}$$

fixiere  $r$ .



Jetzt gilt  $r \equiv a \pmod{J_1}$



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

$$r - a \in J_1 \subseteq I_j$$

$$\Rightarrow r - a \in I_j \Rightarrow r \equiv a \pmod{I_j} \quad \forall j$$

Gleichzeitig:  $r \equiv r_n \pmod{J_2 = I_n}$

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