

Wiederholung

$K[X] := (K^{(\mathbb{N}_0)}, +, \cdot)$  heißt

Polynomialalgebra,

(27.6)  $K[X]$  ist eine  $K$ -Algebra mit Basis  $\{X^m \mid m \in \mathbb{N}_0\}$   
 $\text{grad}(\sum_{i=0}^n \alpha_i X^i) = n$ , falls  $\alpha_n \neq 0$ .

Einsetzhomomorphismus

Sei  $\mathcal{O}$   $K$ -Algebra mit 1, (z.B.  $\mathcal{O} = K$   
 $\alpha \in \mathcal{O}$ .  $\mathcal{O} = K^{(n,n)}$   
 $\mathcal{O} = \text{End}_K V$ )

(27.7)  
 Abb.

$$\left\{ \begin{array}{l} K[X] \rightarrow \mathcal{O} \\ P = \sum_{i=0}^n \alpha_i X^i \mapsto P(\alpha) := \sum_{i=0}^n \alpha_i \alpha^i \end{array} \right. \quad \alpha \text{ fest}$$

Eigenschaften von Polynomen:

Var.  $K$  Körper,  $P \in K[X] \setminus \{0\}$ ,  $\text{grad } P = n$ .

27.9 Beh.  $P$  hat höchstens  $n$  Nullstellen.  
 (im Fall  $K = \mathbb{C}$  genau  $n$  Nullstellen  
 mit Mehrfachzählung)

$$P = \beta \cdot \prod_{i=1}^n (X - \alpha_i) \quad \beta \in K$$

27.12

Teilen mit Rest:

Var.  $P, Q \in K[X]$ ,  $Q \neq 0$ .

Beh.  $\exists R, S \in K[X]$ :  $P = Q \cdot S + R$  und  
 $\text{grad } R < \text{grad } Q$

Folgerung:

$\alpha$  Nullstelle von  $P$ :  $\Rightarrow \exists Q \in K[X]: P = (X - \alpha)Q$

Def.  $Q \in K[X]$  heißt Teiler von  $P \in K[X]$ ,  
falls  $\exists S \in K[X]: P = Q \cdot S$   
"  $Q | P$ "

$Q$  echter Teiler, falls  
 $1 \leq \text{Grad } Q < \text{Grad } P$

$P \in K[X]$  heißt irreduzibel, falls  
 $P$  keine echten Teiler hat  
( $\cong$  Primzahlen in  $\mathbb{Z}$ )

(27.16) Zerlegung in irreduzible Faktoren:

Jedes  $P \in K[X] \setminus \{0\}$  lässt sich (bis auf die  
Reihenfolge der Faktoren) eindeutig darstellen als

$$P = \alpha \cdot P_1 \cdots P_r \text{ mit } \alpha \in K \setminus \{0\}$$

und normierten ( $\rightarrow$  höchster Koeffizient 1)  
irreduziblen Polynomen  $P_i$ .

$$x^2 - 1 = (x+1)(x-1)$$

Def. Ideal in einem Ring

Doc.  $(R, +, \cdot)$  kommutativer Ring mit 1

Def.  $\mathcal{I} \subseteq R$  heißt Ideal, falls

$\mathcal{I}$  UG von  $(R, +)$  und

$$R \cdot \mathcal{I} \subseteq \mathcal{I}.$$

Def.  $\mathcal{I} \subseteq R$  heißt Hauptideal, wenn

$$\exists a \in R: \mathcal{I} = Ra =: (a)$$

Beispiele :  $R = \mathbb{Z}$

•  $(2) = 2\mathbb{Z}$  Ideal der geraden ganzen Zahlen

•  $(4, 6) = 4\mathbb{Z} + 6\mathbb{Z} \subseteq 2\mathbb{Z}$

$$\text{ggT}(4, 6) = 2 = 1 \cdot \underline{6} + (-1) \cdot \underline{4}$$

$$\Rightarrow 2 \in 4\mathbb{Z} + 6\mathbb{Z}$$

$$\Rightarrow 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$$

$R = K[X]$

Für  $P \in K[X]$  ist

$$(P) = \{ P \cdot Q \mid Q \in K[X] \}$$

das Ideal der durch  $P$  teilbaren Polynome

z. B.:  $(X-1) = (X-1) \cdot K[X]$

$$(2) = (1) = K[X]$$

(27.17) Satz

In  $\mathbb{Z}$  und in  $K[X]$  ist jedes Ideal

Hauptideal.

Dinge mit dieser Eigenschaft heißen

Hauptidealringe

Genauer: ...