

# Lineare Algebra II

## Woche 07

26.05.2026 und 28.05.2026

# § 29.3 Algebren über kommutativen Ringen

# Polynome als Baupläne

## Einsetzen geeigneter Elemente in ein Polynom

$$p = 5 + 2t - 4t^3 \in \mathbb{Z}[t]$$

$$p(B) = 5I + 2B - 4B^3 \in \mathbb{Z}^{n \times n}$$

Welche algebraische Struktur benötigen wir für das Einsetzen?

$$+ : A \times A \rightarrow A$$

Addition

$$\cdot : R \times A \rightarrow A$$

S-Mult.

$$\ast : A \times A \rightarrow A$$

inneres Mult.

Modul

Algebra

$$2B - 4B^3$$

$$4B^3$$

$$B^3$$

## Definition 29.22

Es sei  $(R, +, \cdot)$  ein kommutativer Ring. Eine  **$R$ -Algebra**  $(A, +, \cdot, \star)$  besitzt zwei innere Verknüpfungen  $+$ :  $A \times A \rightarrow A$  und  $\star$ :  $A \times A \rightarrow A$  sowie eine äußere Verknüpfung  $\cdot$ :  $R \times A \rightarrow A$ , die die folgenden Bedingungen erfüllen:

①  $(A, +, \cdot)$  ist ein  $R$ -Modul.

②  $(A, +, \star)$  ist ein Ring.  
↳ assoziativ

③ Die **Multiplikation**  $\star$  ist verträglich mit der  $S$ -Multiplikation:

Gemischtes  
Assoziations-  
gesetz

$$(\alpha \cdot a) \star b = \alpha \cdot (a \star b) = a \star (\alpha \cdot b)$$

für alle  $\alpha \in R$  und  $a, b \in A$

(assoziativ)

## Definition 29.22

Es seien  $(R, +, \cdot)$  ein kommutativer Ring und  $(A, +, \cdot, \star)$  eine (assoziative)  $R$ -Algebra.

- ④ Die Algebra  $A$  heißt **kommutativ**, wenn  $\star$  kommutativ ist.

$$a \star b = b \star a$$

- ⑤ Die Algebra  $A$  heißt **unitär**, wenn  $R$  ein Ring mit Eins und  $(A, +, \cdot)$  ein unitärer  $R$ -Modul ist.

$$1 \cdot a = a$$

- ⑥ Die Algebra  $A$  heißt eine **Algebra mit Eins**, wenn es ein bzgl.  $\star$  neutrales Element  $e \in A$  gibt.

$$e \star a = a \star e = a$$

Inverse werden als  $a^{-1}$  notiert.

# Multiplikation in einer Algebra ist bilinear

## Lemma 29.24

Es sei  $(A, +, \cdot, \star)$  eine Algebra über dem kommutativen Ring  $R$ .

Dann ist die Multiplikation  $\star$  bilinear, d. h., es gilt

$$(\alpha \cdot a + \beta \cdot b) \star c = \alpha \cdot (a \star c) + \beta \cdot (b \star c)$$

$$a \star (\beta \cdot b + \gamma \cdot c) = \beta \cdot (a \star b) + \gamma \cdot (a \star c)$$

für alle  $a, b, c \in A$  und alle  $\alpha, \beta, \gamma \in R$ .

folgt aus: Distributivität im Ring  $(A, +, \cdot)$   
gem. Assoziativgesetz

## Beispiel 29.27

- ① Jeder kommutative Ring  $(R, +, \cdot)$  ist eine kommutative Algebra  $(R, +, \cdot, \star)$  über sich selbst mit der Multiplikation  $\star = \cdot$ .

Die Algebra ist gleichzeitig unitär und eine Algebra mit Eins genau dann, wenn  $R$  ein Einselement besitzt.

- ② Jeder kommutative Ring  $(R, +, \cdot)$  ist eine kommutative Algebra  $(R, +, \cdot, \star)$  über jedem seiner Unterringe  $U$ .  $\star = \cdot$ .

Die Algebra ist gleichzeitig unitär und eine Algebra mit Eins genau dann, wenn  $R$  ein Einselement besitzt und dieses auch in  $U$  liegt (wenn also  $U$  ein Unterring mit Eins von  $R$  ist).

$\mathbb{Q}$  ist komm., unitäre  $\mathbb{Z}$ -Algebra mit Eins

## Beispiel 29.27

$$R \cdot \begin{matrix} \uparrow \\ \downarrow \end{matrix} \subseteq \begin{matrix} \uparrow \\ \downarrow \end{matrix} R$$

- ③ Es sei  $(R, +, \cdot)$  ein kommutativer Ring und  $J \subseteq R$  ein Ideal von  $R$ . Dann ist  $(J, +, \cdot, \cdot)$  eine  $R$ -Algebra, und zwar eine Unter algebra der  $R$ -Algebra  $(R, +, \cdot, \cdot)$ .

*↖ wieder  $\cdot = \cdot$*

Die Algebra ist unitär genau dann, wenn  $R$  ein Ring mit Eins ist. Sie ist eine Algebra mit Eins genau dann, wenn es in  $J$  ein multiplikativ neutrales Element gibt.

- ④ Es sei  $(R, +, \cdot)$  ein kommutativer Ring. Dann ist  $(R^{n \times n}, +, \cdot, \cdot)$  mit der Matrix-Matrix-Multiplikation  $\cdot$  eine  $R$ -Algebra.

*$n \in \mathbb{N}_0$*   
*S.-Mult.*  
 $\downarrow$   
*Matrix-M.*  
 $\uparrow$

Diese **Matrixalgebra** ist gleichzeitig unitär und eine Algebra mit dem Einselement  $I_n$  genau dann, wenn  $R$  ein Einselement besitzt.

Im Fall  $n \geq 2$  ist die Matrixalgebra nicht kommutativ.

*↖ i.A.*

## Beispiel 29.27

- 5 Es seien  $X$  eine beliebige Menge,  $(R, +, \cdot)$  ein kommutativer Ring und  $(A, +, \cdot, \star)$  eine  $R$ -Algebra. Dann bildet  $A^X = \{f \mid f: X \rightarrow A\}$  mit der punktweisen Addition, der punktweisen  $S$ -Multiplikation und punktweisen inneren Multiplikation eine  $R$ -Algebra.

Diese ist kommutativ, wenn  $A$  kommutativ ist.

- 6 Ist  $(K, +, \cdot)$  ein Körper und  $(V, +, \cdot)$  ein Vektorraum über  $K$ , dann bildet  $(\text{Endo}(V), +, \cdot, \circ)$  mit der Komposition  $\circ$  als „Multiplikation“ eine unitäre, i. A. nicht-kommutative Algebra über  $K$  mit dem Einselement  $\text{id}_V$ .

Diese wird die **Endomorphismenalgebra des Vektorraumes  $V$**  genannt.

## Beispiel 29.27

- ⑦ Allgemeiner bilden die Endomorphismen  $(\text{Endo}(M), +, \cdot, \circ)$  eines Moduls über einem kommutativen Ring  $(R, +, \cdot)$  mit der Komposition  $\circ$  als „Multiplikation“ eine i. A. nicht-kommutative Algebra über  $R$  mit dem Einselement  $\text{id}_M$ .

Diese wird die **Endomorphismenalgebra des Moduls  $M$**  genannt.

Sie ist unitär genau dann, wenn  $M$  ein unitärer  $R$ -Modul ist.

- ⑧ Ist  $(R, +, \cdot)$  ein kommutativer Ring mit Eins, dann bilden die Polynome  $(R[t], +, \cdot, \cdot)$  eine unitäre, kommutative  $R$ -Algebra mit dem Einselement  $1$  (Einspolynom), genannt die **Polynomialgebra**.

S-Mult.

Poly-Mult.

# Homomorphismen von Algebren

## Definition 29.28

- ① Eine Abbildung  $f: A_1 \rightarrow A_2$  heißt **strukturverträglich** oder ein **Homomorphismus von Algebren** von  $(A_1, +, \cdot, \star)$  in  $(A_2, +, \cdot, \star)$ , wenn gilt:

*über denselben kommut. Ring  $R$*

$$f(a + b) = f(a) + f(b) \quad \text{für alle } a, b \in A_1,$$

$$f(\alpha \cdot a) = \alpha \cdot f(a) \quad \text{für alle } a \in A_1 \text{ und } \alpha \in R,$$

$$f(a \star b) = f(a) \star f(b) \quad \text{für alle } a, b \in A_1.$$

Besitzen beide Algebren ein Einselement und fordern wir zusätzlich

$$f(e_1) = e_2$$

dann heißt  $f$  einen **Homomorphismus von Algebren mit Eins**.

- ② Wie üblich definieren wir auch die Begriffe **Endomorphismus**, **Isomorphismus** und **Automorphismus** von Algebren.

## Beispiel 29.33

- ① Es sei  $V$  ein Vektorraum über dem Körper  $K$  mit  $\dim(V) = n \in \mathbb{N}_0$ .

$$\begin{array}{ll} \text{Endomorphismenalgebra} & \text{Matrixalgebra} \\ (\text{Endo}(V), +, \cdot, \circ) & \rightarrow (K^{n \times n}, +, \cdot, \cdot) \\ f & \mapsto \mathcal{M}_{B_V \leftarrow B_V}(f) \end{array}$$

ist — für jede Wahl einer Basis  $B_V$  von  $V$  — ein Isomorphismus von Algebren mit Eins.

$$\begin{array}{ll} f+g & \mapsto A+B \\ \alpha f & \mapsto \alpha A \\ f \circ g & \mapsto A \cdot B \end{array}$$

## Beispiel 29.33

- ② Der Körper  $\mathbb{C}$  ist ein zweidimensionaler Vektorraum über dem Körper  $\mathbb{R}$ . Genauer ist  $(\mathbb{C}, +, \cdot, \cdot)$  sogar eine unitäre, kommutative  $\mathbb{R}$ -Algebra mit Eins.

Diese ist über die Abbildung

$$a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

isomorph zu einer Unter algebra der  $\mathbb{R}$ -Matrixalgebra  $(\mathbb{R}^{2 \times 2}, +, \cdot, \cdot)$ .

## Beispiel 29.33

- ③ Es sei  $V$  ein Vektorraum über dem Körper  $K$  mit  $\dim(V) = n \in \mathbb{N}_0$ . Für  $n \geq 2$  ist die Determinante  $\det: \text{Endo}(V) \rightarrow K$  **kein** Homomorphismus von Algebren.

Sie ist zwar verträglich mit der Multiplikation, nicht aber mit der Addition und der S-Multiplikation.  $\uparrow \det(AB) = \det(A)\det(B)$

- ④ Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(R[t], +, \cdot, \cdot)$  die  $R$ -Algebra der Polynome über  $R$ . Die Ableitungsabbildung  $\frac{d}{dt}: R[t] \rightarrow R[t]$  ist **kein** Homomorphismus von Algebren.

Sie ist zwar verträglich mit der Addition und der S-Multiplikation, nicht aber verträglich mit der Multiplikation. *Produktregel!*

# § 30 Einsetzungshomomorphismen und Polynomfunktionen

# Einsetzen eines Algebra-Elements in ein Polynom

## Definition 30.1

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit dem Einselement  $e$ .

$1 \cdot a = a$   $a \star e = e \star a = a$   
Für  $a \in A$  und

„Bauplan“ 
$$p = \alpha_0 t^0 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} + \alpha_n t^n \in R[t]$$

heißt die Bildung von

$$\boxed{p(a)} = \alpha_0 e + \alpha_1 a + \cdots + \alpha_{n-1} a^{n-1} + \alpha_n a^n \in A$$

das **Einsetzen** von  $a \in A$  in das Polynom  $p$  oder die **Auswertung** des Polynoms  $p$  an der Stelle  $a$ .

Die Komm. von  $\star$  wird nicht benötigt und nicht gefordert.

# Einsetzen eines Algebra-Elements in ein Polynom

## Beispiel 30.2

unitäre  $\mathbb{Z}$ -Algebra  
mit Eins  $I_n$

- ① Wir betrachten den Ring  $(\mathbb{Z}, +, \cdot)$  und die Matrixalgebra  $(\mathbb{Z}^{n \times n}, +, \cdot, \cdot)$ . Das Einsetzen einer Matrix  $A \in \mathbb{Z}^{n \times n}$

in das Polynom  $p = -1 + 5t - 3t^2 \in \mathbb{Z}[t]$

$$\begin{aligned} \text{ergibt } p(A) &= -1A^0 + 5A^1 - 3A^2 \in \mathbb{Z}^{n \times n} \\ &= -I_n + 5A - 3A^2 \end{aligned}$$

Für die Matrix  $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$  erhalten wir beispielsweise

$$p(A) = - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 5 \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 3 \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 25 & 40 \\ 60 & 85 \end{bmatrix}$$
$$\begin{bmatrix} -17 & -20 \\ -30 & -47 \end{bmatrix}$$

# Einsetzen eines Algebra-Elements in ein Polynom

## Beispiel 30.2

unitäre  $\mathbb{Q}$ -Algebra mit Einselement  $\text{id}_V$

- ② Wir betrachten den Ring  $(\mathbb{Q}, +, \cdot)$  und die Endomorphismenalgebra  $(\text{Endo}(V), +, \cdot, \circ)$  eines  $\mathbb{Q}$ -Vektorraumes  $V$ . Das Einsetzen eines Endomorphismus  $f \in \text{Endo}(V)$

in das Polynom  $p = \frac{1}{3} - \frac{3}{2}t + \frac{4}{7}t^3 \in \mathbb{Q}[t]$

ergibt  $p(f) = \frac{1}{3}f^0 - \frac{3}{2}f^1 + \frac{4}{7}f^3 \in \text{Endo}(V)$   
 $= \frac{1}{3}\text{id}_V - \frac{3}{2}f + \frac{4}{7}f \circ f \circ f$

## zwei verschiedene Standpunkte

- 1 Wir halten das einzusetzende Element  $a \in A$  fest und variieren das Polynom  $p \in R[t]$ , in das wir  $a$  einsetzen.

Das führt zum Konzept des **Einsetzungshomomorphismus**.

- 2 Wir wählen ein bestimmtes Polynom  $p \in R[t]$  aus und variieren das einzusetzende Element  $a \in A$ .

Das führt zum Konzept der **Polynomfunktion**.

# § 30.1 Einsetzungshomomorphismen

# Einsetzungshomomorphismus

## Definition 30.3

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit Eins.

Für  $a \in A$  heißt die Abbildung

$$\text{ev}_a: R[t] \ni \underline{p} \mapsto \text{ev}_a(p) := \underline{p(a)} \in A$$

*Algebra*  
*Algebra*  
Poly  $p$  variiert  
Stelle  $a$  fest

der **Einsetzungshomomorphismus** oder  
der **Auswertungshomomorphismus** zu  $a$ .

# Einsetzungshomomorphismus

## Satz 30.4

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit Eins.

Für jedes  $a \in A$  ist der Einsetzungshomomorphismus  $\text{ev}_a: R[t] \rightarrow A$  ein Homomorphismus von Algebren mit Eins.

*zu prüfen*  
Beweis. •  $(p+q)(a) = p(a) + q(a)$

•  $(\alpha p)(a) = \alpha p(a)$

•  $(p \cdot q)(a) = p(a) \star q(a)$

•  $1(a) = 1a^0 = 1e = e$   
*Einselement*

## Bemerkung 30.5

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit dem Einselement  $e$ .

Der Einsetzungshomomorphismus  $ev_a: R[t] \rightarrow A$  zu gegebenem  $a \in A$  ist durch einen einzigen Funktionswert

$$ev_a(t) = a$$

eindeutig festgelegt.

$$ev_a(t^k) = a^k \quad \text{für } k \in \mathbb{N}_0$$

$$ev_a(\alpha_k t^k) = \alpha_k a^k \quad \text{für } \alpha_k \in R$$

$$ev_a(p+q) = p(a) + q(a)$$

# Polynome kommutieren mit Algebromorphismen

## Satz 30.7

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $A_1, A_2$  zwei unitäre  $R$ -Algebren mit Eins. Weiter sei  $f: A_1 \rightarrow A_2$  ein Homomorphismus von Algebren mit Eins.

Dann gilt für die Einsetzungshomomorphismen  $\text{ev}_a^{A_1}$  und  $\text{ev}_{f(a)}^{A_2}$ :

$$f \circ \text{ev}_a^{A_1} = \text{ev}_{f(a)}^{A_2}$$

Das heißt, für jedes  $a \in A_1$  und jedes Polynom  $p \in R[t]$  gilt:

$$f(\underbrace{p(a)}_{\in A_1}) = \underbrace{p(f(a))}_{\in A_2}$$

**Beweis.**

$$\begin{aligned} f(p(a)) &= f\left(\sum_{k=0}^n a_k a^k\right) = \sum_{k=0}^n f(a_k a^k) \\ &= \sum_{k=0}^n a_k f(a^k) = \sum_{k=0}^n a_k f(a)^k = p(f(a)) \end{aligned}$$

**Beispiel:**  $A = M_{\mathbb{B} \leftarrow \mathbb{R}}(f)$ ,  $A^2 - 3A + I = M_{\mathbb{B} \leftarrow \mathbb{B}}(f^2 - 3f + \text{id})$

# § 30.2 Polynomfunktionen

# Polynomfunktion

## Definition 30.8

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit Eins.

Für  $p \in R[t]$  mit  $p = \sum_{k=0}^n \alpha_k t^k$  heißt die Abbildung

$$p(\cdot): \underline{A} \ni \underline{a} \mapsto p(\underline{a}) = \sum_{k=0}^n \alpha_k \underline{a}^k \in \underline{A}$$

Stelle  $a$  variiert  
Poly  $p$  fest

die **durch  $p$  induzierte Polynomfunktion** auf der Algebra  $A$ .

## Beispiel 30.9

- ① Auf der Matrixalgebra  $(\mathbb{Z}^{n \times n}, +, \cdot, \cdot)$  induziert

das Polynom  $p = 5 + 2t - 4t^3 \in \mathbb{Z}[t]$

die Polynomfunktion  $\mathbb{Z}^{n \times n} \ni A \mapsto p(A) = 5I + 2A - 4A^3 \in \mathbb{Z}^{n \times n}$

- ② Auf der Algebra  $(\mathbb{Z}_2, +, \cdot, \cdot)$  induziert

das Polynom  $p = t + t^2 \in \mathbb{Z}_2[t]$

die Polynomfunktion  $\mathbb{Z}_2 \ni \alpha \mapsto p(\alpha) = \alpha + \alpha^2 \in \mathbb{Z}_2$

$$p(0) = 0 + 0^2 = 0$$

$$p(1) = 1 + 1^2 = 0$$

↑ Nullfunktion

# Zuordnung Polynom zu Polynomfunktion

## Satz 30.10

Es seien  $(R, +, \cdot)$  ein kommutativer Ring mit Eins und  $(A, +, \cdot, \star)$  eine unitäre  $R$ -Algebra mit Eins.

Die Abbildung

$$\Phi: (R[t], +, \cdot, \cdot) \ni p \mapsto p(\cdot) \in (A^A, +, \cdot, \star)$$

ist ein Homomorphismus von Algebren mit Eins.

- $\Phi$  ist i. A. nicht injektiv
- $\Phi$  ist i. A. auch nicht surjektiv.

# § 31 Polynome über einem Körper

# der Polynomring ist kein Körper

## Lemma 31.1

Es sei  $K$  ein Körper.

- 1 Ein Polynom  $p \in K[t]$  ist multiplikativ invertierbar genau dann, wenn  $p = \alpha \neq 0$ . *Konstantes Polynom  $\neq$  Nullpoly*
- 2 Der Polynomring  $K[t]$  ist **kein Körper**.

Die „meisten“ Polynome besitzen also keine multiplikativen Inversen!

*z.B.  $p = t$  ist nicht invertierbar*

*Es gibt kein  $q \in K[t]$  mit  $p \cdot q = 1$ .*

# § 31.1 Polynomdivision

# Polynomdivision mit Rest

## Definition 31.2

Es seien  $K$  ein Körper und  $p_1, p_2 \in K[t]$  zwei Polynome.

$p_2$  heißt ein **Teiler** von  $p_1$ , wenn es ein  $q \in K[t]$  gibt, sodass gilt:

$$p_2 \mid p_1$$

$$p_1 = q \cdot p_2$$

## Satz 31.3

vgl.  $13 = 3 \cdot 4 + 1$  in  $\mathbb{Z}$

Es seien  $K$  ein Körper und  $p_1, p_2 \in K[t]$  zwei Polynome. Ist  $p_2 \neq 0$  (Nullpolynom), dann gibt es eindeutig bestimmte Polynome  $q, r \in K[t]$ , sodass gilt:

Quotient Rest

$$p_1 = \underline{q} \cdot p_2 + \underline{r} \quad \text{und} \quad \deg(r) < \deg(p_2)$$

# Polynomdivision mit Rest

Beispiel 31.5 *von hohen Potenzen starten*

Was ist  $(3t^3 + 2t + 1) : (t^2 - 4t)$  in  $\mathbb{Q}[t]$ ?

$$\begin{array}{r} (3t^3 + 2t + 1) = (t^2 - 4t) \left( \underbrace{3t + 12}_{\neq} \right) + \left( \underbrace{50t + 1}_{\checkmark} \right) \\ - (3t^3 - 12t^2) \\ \hline 12t^2 + 2t + 1 \\ - (12t^2 - 48t) \\ \hline 50t + 1 \end{array}$$

# Polynomdivision mit Rest

Was ist  $(3t^3 + 2t + 1) : (t^2 - 4t)$  in  $\underline{\mathbb{Z}_5[t]}$ ?

$$\begin{array}{r} 3t^3 + 2t + 1 = (t^2 - 4t) ( \underbrace{3t + 2}_{\eta} ) + ( \underbrace{1}_{\gamma} ) \\ - (3t^3 - 2t^2) \\ \hline 2t^2 + 2t + 1 \\ - (2t^2 - 3t) \\ \hline 1 \end{array}$$

# § 31.2 Die Hauptidealring-Eigenschaft

# Hauptidealring

## Definition 31.6

kommutativ mit  $1 \neq 0$   
nullteilerfrei

„Prototyp“  $\mathbb{Z}$

Ein **Integritätsring**  $R$  mit der Eigenschaft, dass jedes Ideal in  $R$  ein Hauptideal ist, heißt ein **Hauptidealring**.  $\mathbb{Z} \cdot R \subseteq \mathbb{Z}$

↑ erzeugt von einem einzigen Element (Def. 9.35)

In kommutativen Ringen  $R$  mit Eins gilt  $(a) = Ra$  (Satz 9.36)

Ist  $a \in R$  multiplikativ invertierbar, dann gilt  $(a) = R$

↑ Generator / Erzeuger

## Beispiel 31.7

- 1  $(\mathbb{Z}, +, \cdot)$  ist ein Hauptidealring, denn jedes Ideal  $J$  in  $\mathbb{Z}$  ist von der Form  $J = m\mathbb{Z} = (m)$  für ein  $m \in \mathbb{N}_0$ .
- 2 Im kommutativen Ring mit Eins  $R = \mathbb{Z}_4$  gibt es die Ideale  $J = \{0\} = (0)$  und  $J = \{0, 2\} = (2)$  sowie  $J = R = (1)$ . Dennoch ist  $R$  **kein** Hauptidealring, da er nicht nullteilerfrei ist.
- 3 Der Polynomring  $\mathbb{Z}[t]$  ist **kein** Hauptidealring. Er ist zwar ein Integritätsring (nach Folgerung 28.11, da  $\mathbb{Z}$  ein Integritätsring ist), jedoch kann beispielsweise das Ideal

$$J = (2, t) = \{2 \cdot p + t \cdot q \mid p, q \in \mathbb{Z}[t]\}$$

nicht von einem einzigen Polynom erzeugt werden.

# Polynomringe über Körpern sind Hauptidealringe

## Satz 31.8

Integritätsring ✓

Es sei  $K$  ein Körper. Dann gilt:

- 1 Zu jedem Ideal  $J$  in  $K[t]$  existiert ein  $p \in K[t]$  mit der Eigenschaft  $J = (p)$ .

**Beweis.** Falls  $J = \{0\}$ , wähle  $p=0 \Rightarrow J = (p)$

Falls  $J \neq \{0\}$ , wähle aus  $J \setminus \{0\}$  ein Poly  $p$  minimalen Grades.

- $(p) \subseteq J$ , denn  $p \in J \Rightarrow (p) \subseteq J = \overline{J}$  ist Ideal
- $J \subseteq (p)$ , denn: Ist  $\hat{p} \in J$ , dann

es. eindeutige  $q, r \in K[t]$  mit  $\deg(r) < \deg(p)$

$$\text{und } \hat{p} = q \cdot p + r.$$

$$\Rightarrow r = \underbrace{\hat{p}}_{\in J} - \underbrace{q}_{\in K[t]} \cdot \underbrace{p}_{\in J} \in J. \quad p \text{ ist grad-minimal in } J \setminus \{0\} \Rightarrow r=0.$$

$$\Rightarrow \hat{p} = q \cdot p \in (p)$$

# Polynomringe über Körpern sind Hauptidealringe

## Satz 31.8

Es sei  $K$  ein Körper. Dann gilt:

- ② Gilt  $J = (p)$ , dann ist  $p$  bis auf einen Faktor  $\alpha \in K$  eindeutig bestimmt.  $J = (p_1) = (p_2) \Rightarrow \exists \alpha \in K$  mit  $p_1 = \alpha p_2$ .

**Beweis.**  $J = (p_1) = K[t] \cdot p_1 = (p_2) = K[t] \cdot p_2$

$$\begin{aligned} p_1 \in J = (p_2) &\Rightarrow p_1 = q_1 \cdot p_2 \\ p_2 \in J = (p_1) &\Rightarrow p_2 = q_2 \cdot p_1 \end{aligned} \quad \left. \vphantom{\begin{aligned} p_1 \in J = (p_2) \\ p_2 \in J = (p_1) \end{aligned}} \right\} \text{mit } q_1, q_2 \in K[t]$$

$$\Rightarrow p_1 = q_1 \cdot q_2 \cdot p_1 \Rightarrow p_1 \cdot (q_1 \cdot q_2 - 1) = 0$$

$K[t]$  ist nullteilerfrei.

$$\bullet p_1 = 0 \Rightarrow J = (0) = \{0\} \Rightarrow p_2 = 0 \quad \checkmark$$

$$\text{oder } q_1 \cdot q_2 = 1 \Rightarrow \deg(q_1 \cdot q_2) = \deg(q_1) + \deg(q_2) = \deg(1) = 0 \Rightarrow q_1 = \alpha \in K \setminus \{0\}, q_2 = \alpha^{-1} \quad \checkmark$$

# Polynomringe über Körpern sind Hauptidealringe

## Satz 31.8

Es sei  $K$  in Körper. Dann gilt:

- ③ Ist  $J \neq \{0\}$ , dann ist  $p$  eines der Polynome minimalen Grades in  $J \setminus \{0\}$ .
- ④ Ist  $J = \{0\}$ , dann gilt  $p = 0$ .

Beweis.

## § 31.3 Nullstellen und Teiler

# Nullstelle eines Polynoms

## Definition 31.9

Es seien  $K$  ein Körper und  $p \in K[t]$ . Das Element  $\lambda \in K$  heißt eine **Nullstelle** oder **Wurzel von  $p$  in  $K$** , wenn  $p(\lambda) = 0$  gilt.

- Wieviele Nullstellen kann ein Polynom besitzen?
- Was sagen die Nullstellen über ein Polynom aus?

## Beispiel 31.10

- ①  $p = 1 + t^2 \in \mathbb{Q}[t]$  besitzt keine Nullstelle in  $\mathbb{Q}$ , weil für die Polynomfkt.  $p(\cdot): \mathbb{Q} \rightarrow \mathbb{Q}$  gilt:  $p(t) = 1 + t^2 \geq 1$  für alle  $t \in \mathbb{Q}$ .  
auch in  $\mathbb{R}$  keine Nullstelle geordn. Körper
- ②  $p = 1 + t^2 \in \mathbb{C}[t]$  besitzt genau die Nullstellen  $i$  und  $-i$  in  $\mathbb{C}$ .

# Nullstelle eines Polynoms

## Beispiel 31.10

③  $p = 1 + t^2 \in \mathbb{Z}_5[t]$  besitzt in  $\mathbb{Z}_5$  genau die Nullstellen  $2$  und  $3$

$$p(0) = 0 \cdot 5 \cdot 0 + 5 \cdot 1 = 1$$

$$p(3) = 3 \cdot 5 \cdot 3 + 5 \cdot 1 = 0$$

$$p(1) = 1 \cdot 5 \cdot 1 + 5 \cdot 1 = 2$$

$$p(4) = 4 \cdot 5 \cdot 4 + 5 \cdot 1 = 2$$

$$p(2) = 2 \cdot 5 \cdot 2 + 5 \cdot 1 = 0$$

## Lemma 31.11

*Nullstellen bringen Teiler!*

Es seien  $K$  ein Körper und  $p \in K[t]$  ein Polynom. Dann sind äquivalent:

- ①  $\lambda \in K$  ist eine Nullstelle von  $p$ . *Linearfaktor*
- ② Das Polynom  $t - \lambda \in K[t]$  ist ein Teiler von  $p$ .

In diesem Fall gilt für das eindeutige  $q \in K[t]$  mit  $p = q \cdot (t - \lambda)$  die Beziehung  $\deg(q) = \deg(p) - 1$ .

# Zerlegung eines Polynoms mithilfe seiner Nullstellen

## Satz 31.12

Es seien  $K$  ein Körper und  $p \in K[t]$  ein Polynom,  $p \neq 0$ . Dann gilt:

- 1 Es existieren  $s \in \mathbb{N}_0$ , paarweise verschiedene Zahlen  $\lambda_1, \dots, \lambda_s \in K$  sowie Exponenten  $n_1, \dots, n_s \in \mathbb{N}$  und ein Polynom  $q \in K[t]$  ohne Nullstelle in  $K$ , sodass gilt:

$$p = (t - \lambda_1)^{n_1} \cdots (t - \lambda_s)^{n_s} \cdot q$$

*ohne Nullstellen*

Weiter gilt  $\deg(p) = n_1 + \cdots + n_s + \deg(q)$ .

- 2 Die Nullstellen von  $p$  sind genau die Zahlen  $\lambda_1, \dots, \lambda_s \in K$ .

# Zerlegung eines Polynoms mithilfe seiner Nullstellen

## Satz 31.12

Es seien  $K$  ein Körper und  $p \in K[t]$  ein Polynom,  $p \neq 0$ . Dann gilt:

- ③ Ist  $\lambda_i \in K$  eine Nullstelle von  $p$ , dann gilt

$$n_i = \max\{m \in \mathbb{N} \mid (t - \lambda_i)^m \mid p\}.$$

- ④ Die Darstellung

$$p = (t - \lambda_1)^{n_1} \cdots (t - \lambda_s)^{n_s} \cdot q$$

ist (bis auf die Nummerierung der Nullstellen) eindeutig bestimmt.

- $n_i \in \mathbb{N}$  heißt die **Vielfachheit** der Nullstelle  $\lambda_i$
- **einfache Nullstelle** im Fall  $n_i = 1$
- **mehrfache Nullstelle** im Fall  $n_i > 1$
- $t - \lambda_i \in K[t]$  heißt ein **Linearfaktor** von  $p$

# Zerlegung eines Polynoms mithilfe seiner Nullstellen

## Folgerung 31.13

Es seien  $K$  ein Körper und  $p \in K[t]$  ein Polynom,  $p \neq 0$ . Dann gilt mit der Darstellung

$$p = (t - \lambda_1)^{n_1} \cdots (t - \lambda_s)^{n_s} \cdot q$$

- ①  $p$  hat höchstens  $\deg(p) \in \mathbb{N}_0$  viele Nullstellen, wenn diese entsprechend ihrer Vielfachheit gezählt werden, also

$$\sum_{i=1}^s n_i = \deg(p) - \deg(q) \leq \deg(p)$$

- ② Insbesondere hat  $p$  höchstens  $\deg(p) \in \mathbb{N}_0$  viele paarweise verschiedene Nullstellen, also  $s \leq \deg(p)$ .

# Zerlegung eines Polynoms mithilfe seiner Nullstellen

## Beispiel 31.14

①  $p = 3t^3 + t^2 + 2 \in \mathbb{Z}_5[t]$  hat (Probieren) die Nullstelle  $\lambda = 2$ .

Abdividieren von  $t - 2$  ergibt

$$3t^3 + t^2 + 2 = (t - 2) \cdot \underbrace{(3t^2 + 2t + 4)}_{p_1}$$

$p_1 := 3t^2 + 2t + 4$  hat (Probieren) nochmal die Nullstelle  $\lambda = 2$ .

Erneutes Abdividieren von  $t - 2$  liefert

$$p_1 = 3t^2 + 2t + 4 = (t - 2) \cdot \underbrace{(3t + 3)}_{p_2}$$

$p_2 := 3t + 3$  hat (Probieren) die Nullstelle  $\lambda = 4$ .

Abdividieren von  $t - 4$  ergibt

$$p_2 = (t - 4) \cdot 3$$

insgesamt:  $p = (t - 2)^2 \cdot (t - 4) \cdot 3$

# Zerlegung eines Polynoms mithilfe seiner Nullstellen

## Beispiel 31.14

②  $p = t^3 + 2t \in \mathbb{Z}_5[t]$  hat (Probieren) die Nullstelle  $\lambda = 0$ .

Abdividieren von  $t - 0$  ergibt

$$t^3 + 2t = (t - 0) \cdot \underbrace{(t^2 + 2)}_{p_1}$$

$p_1 := t^2 + 2$  hat (Probieren) keine Nullstelle in  $\mathbb{Z}_5$ .

$$\text{insgesamt: } p = (t - 0) \cdot \underbrace{(t^2 + 2)}_q$$

## nochmal Zuordnung Polynom zu Polynomfunktion

Folgerung 31.15 (zu Folgerung 31.13 zur Anzahl der Nullstellen)

Es sei  $K$  ein unendlicher Körper.

Dann ist der Algebromorphismus

$$\Phi: (K[t], +, \cdot, \cdot) \ni p \mapsto p(\cdot) \in (K^K, +, \cdot, \cdot)$$

injektiv.

Poly      Polyfkt auf  $K$

Beweis:  $p_1, p_2 \in K[t]$  mit gleicher Polyfkt.

$$q := p_1 - p_2 = 0 \quad q(\lambda) = (p_1 - p_2)(\lambda) = p_1(\lambda) - p_2(\lambda) = 0$$

für alle  $\lambda \in K$

D.h.  $q \in K[t]$  hat unendlich viele Nullstellen!

Satz 31.12

$$\Rightarrow q = 0 \text{ (Nullpoly)} \Rightarrow p_1 = p_2$$

# Fundamentalsatz der Algebra

## Satz 31.16

Jedes Polynom  $p \in \mathbb{C}[t]$  mit  $\deg(p) > 0$  hat mindestens eine Nullstelle.

Beweis meistens mithilfe von Funktionentheorie (komplexe Analysis)

## Folgerung 31.17

Jedes nicht-konstante Polynom  $p \in \mathbb{C}[t]$  zerfällt vollständig in Linearfaktoren:

$$p = (t - \lambda_1)^{n_1} \cdots (t - \lambda_s)^{n_s} \cdot q$$

$\alpha \in \mathbb{C} \setminus \{0\}$   
konstant

↑  
führender  
Koeff.