Lineare Algebra II

Woche 07

26.05.2026 und 28.05.2026

§ 29.3 Algebren über kommutativen Ringen

Einsetzen geeigneter Elemente in ein Polynom

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

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

Welche algebraische Struktur benötigen wir für das Einsetzen?

$$+ \colon A \times A \to A$$

$$\cdot \colon R \times A \to A$$

$$\star \colon A \times A \to A$$

Algebren über kommutativen Ringen

Definition 29.22

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

1. $(A, +, \cdot)$ ist ein R-Modul.
2. $(A, +, \star)$ ist ein Ring.
3. Die **Multiplikation** $\star$ ist verträglich mit der S-Multiplikation:

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

Algebren über kommutativen Ringen

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.
5. Die Algebra A heißt **unitär**, wenn R ein Ring mit Eins und $(A, +, \cdot)$ ein unitärer R-Modul ist.
6. Die Algebra A heißt eine **Algebra mit Eins**, wenn es ein bzgl. $\star$ neutrales Element $e \in A$ gibt.

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

$$\begin{aligned}(\alpha \cdot a + \beta \cdot b) \star c &= \alpha \cdot (a \star c) + \beta \cdot (b \star c)\\ a \star (\beta \cdot b + \gamma \cdot c) &= \beta \cdot (a \star b) + \gamma \cdot (a \star c)\end{aligned}$$

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

Algebren über kommutativen Ringen

Beispiel 29.27

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

   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.

   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).

Beispiel 29.27

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 Unteralgebra der R-Algebra $(R, +, \cdot, \cdot)$.

   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.

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

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

Algebren über kommutativen Ringen

Beispiel 29.27

5. Es seien X eine beliebige Menge, $(R, +, \cdot)$ ein kommutativer Ring und $(A, +, \cdot, \star)$ eine R-Algebra. Dann bildet $A^X = \{f \mid f : X \to A\}$ 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 $(\operatorname{Endo}(V), +, \cdot, \circ)$ mit der Komposition $\circ$ als „Multiplikation" eine unitäre, i. A. nicht-kommutative Algebra über K mit dem Einselement id_V.

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

Algebren über kommutativen Ringen

Beispiel 29.27

7. Allgemeiner bilden die Endomorphismen $(\operatorname{Endo}(M), +, \cdot, \circ)$ 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 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 **Polynomalgebra**.

Homomorphismen von Algebren

Definition 29.28

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

$$\begin{aligned} f(a + b) &= f(a) + f(b) && \text{für alle } a, b \in A_1, \\ f(\alpha \cdot a) &= \alpha \cdot f(a) && \text{für alle } a \in A_1 \text{ und } \alpha \in R, \\ f(a \star b) &= f(a) \star f(b) && \text{für alle } a, b \in A_1. \end{aligned}$$

   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.

Homomorphismen von Algebren

Beispiel 29.33

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

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

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

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

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

   isomorph zu einer Unteralgebra 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 $n \geqslant 2$ ist die Determinante $\det\colon \operatorname{Endo}(V) \to K$ kein Homomorphismus von Algebren.

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

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

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

§ 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.

Für $a \in A$ und

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

heißt die Bildung von

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

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

Einsetzen eines Algebra-Elements in ein Polynom

Beispiel 30.2

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

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

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

Für die Matrix $A = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ erhalten wir beispielsweise

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

Beispiel 30.2

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

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

$$\begin{aligned} \text{ergibt} \quad p(f) &= \frac{1}{3}\, f^0 - \frac{3}{2}\, f^1 + \frac{4}{7}\, f^3 \qquad \in \operatorname{Endo}(V) \\ &= \frac{1}{3}\, \mathrm{id}_V - \frac{3}{2}\, f + \frac{4}{7}\, f \circ f \circ f \end{aligned}$$

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

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

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

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 $\operatorname{ev}_a \colon R[t] \to A$ ein Homomorphismus von Algebren mit Eins.

Beweis.

Einsetzungshomomorphismus

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 $\operatorname{ev}_a \colon R[t] \to A$ zu gegebenem $a \in A$ ist durch einen einzigen Funktionswert

$$\operatorname{ev}_a(t) = a$$

eindeutig festgelegt.

Polynome kommutieren mit Algebrahomomorphismen

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 $f\colon A_1 \to A_2$ ein Homomorphismus von Algebren mit Eins.

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

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

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

$$f(p(a)) = p(f(a))$$

Beweis.

§ 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

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

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

Polynomfunktion

Beispiel 30.9

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

$$\begin{aligned} &\text{das Polynom} && p = 5 + 2\,t - 4\,t^3 && \in \mathbb{Z}[t] \\ &\text{die Polynomfunktion} && \mathbb{Z}^{n \times n} \ni A \mapsto p(A) = 5\,I + 2\,A - 4\,A^3 && \in \mathbb{Z}^{n \times n} \end{aligned}$$

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

$$\begin{aligned} &\text{das Polynom} && p = t + t^2 && \in \mathbb{Z}_2[t] \\ &\text{die Polynomfunktion} && \mathbb{Z}_2 \ni \alpha \mapsto p(\alpha) = \alpha + \alpha^2 && \in \mathbb{Z}_2 \end{aligned}$$

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

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

ist ein Homomorphismus von Algebren mit Eins.

- Φ ist i. A. nicht injektiv
- Φ 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 $p = \alpha \neq 0$.
2. Der Polynomring $K[t]$ ist kein Körper.

Die „meisten“ Polynome besitzen also keine multiplikativen Inversen!

§ 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:

$$p_1 = q \cdot p_2$$

Satz 31.3

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:

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

Beispiel 31.5

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

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

§ 31.2 Die Hauptidealring-Eigenschaft

Hauptidealring

Definition 31.6

Ein Integritätsring R mit der Eigenschaft, dass jedes Ideal in R ein Hauptideal ist, heißt ein **Hauptidealring**.

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

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

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 ein Integritätsring (nach Folgerung 28.11, da $\mathbb{Z}$ ein Integritätsring ist), jedoch kann beispielsweise das Ideal

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

nicht von einem einzigen Polynom erzeugt werden.

Polynomringe über Körpern sind Hauptidealringe

Satz 31.8

Es sei K in Körper. Dann gilt:

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

Beweis.

Polynomringe über Körpern sind Hauptidealringe

Satz 31.8

Es sei K in Körper. Dann gilt:

2. Gilt $J = (p)$, dann ist p ist also bis auf einen Faktor $\alpha \in K$ eindeutig bestimmt.

Beweis.

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. $p(\cdot) \colon \mathbb{Q} \to \mathbb{Q}$ gilt: $p(t) = 1 + t^2 \geqslant 1$ für alle $t \in \mathbb{Q}$.
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

$$p(0) = 0 \cdot_5 0 +_5 1 = \qquad p(3) = 3 \cdot_5 3 +_5 1 =$$
$$p(1) = 1 \cdot_5 1 +_5 1 = \qquad p(4) = 4 \cdot_5 4 +_5 1 =$$
$$p(2) = 2 \cdot_5 2 +_5 1 =$$

Lemma 31.11

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

1. $\lambda \in K$ ist eine Nullstelle von p.
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 $\lambda_1, \ldots, \lambda_s \in K$ sowie Exponenten $n_1, \ldots, n_s \in \mathbb{N}$ und ein Polynom $q \in K[t]$ ohne Nullstelle in K, sodass gilt:

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

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

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

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 $\lambda \in K$ eine Nullstelle von p, dann gilt

$$n = \max\big\{m \in \mathbb{N} \,\big|\, (t-\lambda)^m \mid p\big\}.$$

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 λ_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

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

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

Zerlegung eines Polynoms mithilfe seiner Nullstellen

Beispiel 31.14

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

   Abdividieren von $t - 2$ ergibt

   $$3\,t^3 + t^2 + 2 = (t - 2) \cdot (3\,t^2 + 2\,t + 4)$$

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

   Erneutes Abdividieren von $t - 2$ liefert

   $$p_1 = 3\,t^2 + 2\,t + 4 = (t - 2) \cdot (3\,t + 3)$$

   $p_2 := 3\,t + 3$ 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. $p = t^3 + 2\,t \in \mathbb{Z}_5[t]$ hat (Probieren) die Nullstelle $\lambda = 0$.

   Abdividieren von $t - 0$ ergibt

   $$t^3 + 2\,t = (t - 0) \cdot (t^2 + 2)$$

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

insgesamt: $p = (t - 0)^2 \cdot (t^2 + 2)$

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 Algebrahomomorphismus

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

injektiv.

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:

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