

Lineare Algebra II

Woche 06

19.05.2026 und 21.05.2026

Kapitel 7 Die Algebra der Polynome

§ 28 Polynome über kommutativen Ringen mit Eins

Was ist ein Polynom?

verschiedene mögliche Antworten

- 1 ein formaler Ausdruck der Gestalt

$$\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \dots + \alpha_n t^n$$

in einer Variablen/Unbestimmten t mit Koeffizienten $\alpha_0, \alpha_1, \dots, \alpha_n$

- 2 eine endlich getragene Folge von Koeffizienten

$$(\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n, 0, 0, \dots)$$

- 3 ein Element einer Ringerweiterung von R , die über eine universelle Eigenschaft definiert ist

Polynome in der linearen Algebra

Polynome sind „Baupläne“

$$p = 5 + 2t - 4t^3$$

$$p(A) =$$

$$p(f) =$$

Definition 28.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

- 1 Jedes Element von $(R^{\mathbb{N}_0})_{00}$ — also jede endlich getragene Folge $p = (\alpha_n)_{n \in \mathbb{N}_0}$ mit Gliedern $\alpha_n \in R$ — heißt ein **Polynom über R** .
- 2 Auf $(R^{\mathbb{N}_0})_{00}$ definieren wir eine **Addition** durch die gliederweise Addition. Sind also $p = (\alpha_n)_{n \in \mathbb{N}_0}$ und $q = (\beta_n)_{n \in \mathbb{N}_0}$ endlich getragene Folgen in R , so ist

$$p + q := (\alpha_n + \beta_n)_{n \in \mathbb{N}_0}$$

Definition 28.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

- ③ Auf $(R^{\mathbb{N}_0})_{00}$ definieren wir eine **Multiplikation** durch die **Faltung**. Sind also $p = (\alpha_n)_{n \in \mathbb{N}_0}$ und $q = (\beta_n)_{n \in \mathbb{N}_0}$ endlich getragene Folgen in R , so ist

$$p \cdot q := (\gamma_n)_{n \in \mathbb{N}_0} \quad \text{mit} \quad \gamma_n := \sum_{k=0}^n \alpha_k \cdot \beta_{n-k}$$

- ④ Die algebraische Struktur $((R^{\mathbb{N}_0})_{00}, +, \cdot)$ heißt der **Polynomring über dem Koeffizientenring R** .

Lemma 28.2

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

- 1 Der Polynomring $((R^{\mathbb{N}_0})_{00}, +, \cdot)$ ist ebenfalls ein kommutativer Ring mit Eins. Das Nullelement ist das **Nullpolynom** $(0, 0, \dots)$. Das additive Inverse eines Polynoms erhalten wir durch Negation aller Koeffizienten.

Das Einselement ist das **Einspolynom** $(1, 0, 0, \dots)$.

- 2 Die Abbildung

$$i: R \ni \alpha_0 \mapsto (\alpha_0, 0, 0, \dots) \in (R^{\mathbb{N}_0})_{00}$$

ist ein injektiver Ringhomomorphismus. Sie heißt die **Einbettung des Koeffizientenringes in seinen Polynomring**.

Beweis. Übung

Bemerkung 28.3

- 1 Die Bilder der Elemente von R unter der Einbettung

$$i: R \ni \alpha_0 \mapsto (\alpha_0, 0, 0, \dots) \in (R^{\mathbb{N}_0})_{00}$$

heißen **konstante Polynome**.

Dadurch können wir den Koeffizientenring R mit dem Unterring der konstanten Polynome in $(R^{\mathbb{N}_0})_{00}$ identifizieren.

Wir schreiben daher auch einfach

Bemerkung 28.3

② Mithilfe der Einbettung

$$i: R \ni \alpha_0 \mapsto (\alpha_0, 0, 0, \dots) \in (R^{\mathbb{N}_0})_{00}$$

können wir die (äußere) Multiplikation

$$\begin{aligned}\alpha_0 \cdot q &:= i(\alpha_0) \cdot q \\ &= (\alpha_0, 0, 0, \dots) \cdot (\beta_0, \dots, \beta_n, 0, 0, \dots) \\ &= (\alpha_0 \cdot \beta_0, \dots, \alpha_0 \cdot \beta_n, 0, 0, \dots)\end{aligned}$$

definieren.

Polynome in einer Variablen

Polynome als ...

Koeffizientenfolge $(\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n, 0, 0, \dots)$

formale Summe $\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \dots + \alpha_n t^n$

Polynome in einer Variablen

Definition 28.4

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und t ein Symbol, das nicht in R enthalten ist.

Wir definieren $R[t]$ als die Menge der **formalen Summen** der Gestalt

$$\alpha_0 + \alpha_1 t + \dots + \alpha_n t^n$$

mit $n \in \mathbb{N}_0$, Koeffizienten $\alpha_0, \dots, \alpha_k \in R$ und Verknüpfungen $+$ und \cdot .

Dann heißt $(R[t], +, \cdot)$ der **Polynomring in der Variablen t über dem Koeffizientenring R** .

$$(R^{\mathbb{N}_0})_{00} \ni (\alpha_0, \dots, \alpha_n, 0, 0, \dots) \mapsto \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n \in R[t]$$

ist ein Isomorphismus von Ringen mit Eins

Bemerkung 28.5

- $(R^{\mathbb{N}_0})_{00}$ ist eine „neutrale“ Formulierung des Polynomringes
- zwei Polynome sind gleich, wenn die Folgen übereinstimmen
- **konstante Polynome**
 $(\alpha_0, 0, 0, \dots)$
- **lineare Polynome**
 $(\alpha_0, \alpha_1, 0, 0, \dots)$
- $R[t]$ ist eine isomorphe Darstellung unter Verwendung der Variable t
- zwei Polynome sind gleich, wenn die Koeffizienten aller Potenzen von t übereinstimmen
- **konstante Polynome**
 $\alpha_0 t^0$
- **lineare Polynome**
 $\alpha_0 t^0 + \alpha_1 t^1$

Beispiel 28.7

$$\textcircled{1} \quad p = \frac{1}{2} - 7t + \frac{3}{4}t^2 \in \mathbb{Q}[t] \quad \text{und} \quad q = 1 - t - \frac{1}{2}t^3 \in \mathbb{Q}[t]$$

$$p + q =$$

$$p \cdot q = \left(\frac{1}{2} - 7t + \frac{3}{4}t^2\right) \cdot \left(1 - t - \frac{1}{2}t^3\right)$$

Beispiel 28.7

$$\textcircled{2} \quad p = [2]X + X^2 + X^3 \in (\mathbb{Z}/4\mathbb{Z})[X]$$

$$q = [3] + [3]X \in (\mathbb{Z}/4\mathbb{Z})[X]$$

$$p + q =$$

$$p \cdot q = ([2]X + X^2 + X^3) \cdot ([3] + [3]X)$$

Definition 28.8

Es sei $p = (\alpha_0, \alpha_1, \dots, \alpha_n, 0, 0, \dots)$ ein Polynom über dem kommutativen Ring R mit Eins.

- ① Der **Grad** des Polynoms p ist definiert als

$$\deg(p) := \begin{cases} -\infty, & \text{im Fall } p = 0 \\ \max\{j \in \mathbb{N}_0 \mid \alpha_j \neq 0\} & \text{sonst} \end{cases}$$

- ② Wir bezeichnen die Menge der Polynome über R vom Höchstgrad $n \in \mathbb{N}_0$ in der Variablen t mit $R_n[t]$.

Definition 28.8

Es sei $p = (\alpha_0, \alpha_1, \dots, \alpha_n, 0, 0, \dots)$ ein Polynom über dem kommutativen Ring R mit Eins.

- ③ Wenn $p \neq 0$ ist, dann heißt $\ell(p) := \alpha_{\deg(p)} \in R \setminus \{0\}$ auch der **führende Koeffizient** oder der **Leitkoeffizient** von p . Das Nullpolynom $p = 0$ erkennen wir an der Definition $\ell(0) := 0$.

- ④ Das Polynom der Form $(0, \dots, 0, 1, 0, 0, \dots) \in (R^{\mathbb{N}_0})_{00}$ bzw. der Form $t^n \in R[t]$ mit $n \in \mathbb{N}_0$ heißt das **Monom vom Grad** $n \in \mathbb{N}_0$.

- ⑤ Ist der führende Koeffizient $\ell(p) = 1$, dann heißt das Polynom $p \neq 0$ **normiert** oder **monisch**.

Lemma 28.10

Es seien p, q Polynome über dem kommutativen Ring R mit Eins.

- 1 $\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$
- 2 $\deg(c p) = \deg(p)$ für alle $c \in R \setminus \{0\}$
- 3 $\deg(p \cdot q) \leq \deg(p) + \deg(q)$
- 4 Ist R nullteilerfrei, dann gilt sogar $\deg(p \cdot q) = \deg(p) + \deg(q)$

Beweis. Übung

Folgerung 28.11

Ist R ein Integritätsring, dann ist auch der Polynomring über R ein Integritätsring.

Beweis.

§ 29 Moduln und Algebren über kommutativen Ringen

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?

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

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

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

§ 29.1 Moduln über kommutativen Ringen

Moduln über kommutativen Ringen

Definition 29.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Ein **R -Modul** $(M, +, \cdot)$ hat

$$+ : M \times M \rightarrow M$$

$$\cdot : R \times M \rightarrow M$$

- 1 $(M, +)$ ist abelsche Gruppe
- 2 gemischtes Assoziativgesetz

$$(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$$

gemischte Distributivgesetze

$$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$$

$$(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$$

Definition 11.1

Es sei $(K, +, \cdot)$ ein Körper. Ein **K -Vektorraum** $(V, +, \cdot)$ hat

$$+ : V \times V \rightarrow V$$

$$\cdot : K \times V \rightarrow V$$

- 1 $(V, +)$ ist abelsche Gruppe
- 2 gemischtes Assoziativgesetz

$$(\alpha \cdot \beta) \cdot u = \alpha \cdot (\beta \cdot u)$$

gemischte Distributivgesetze

$$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$$

$$(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v)$$

Moduln über kommutativen Ringen

Definition 29.1

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Ein **R -Modul** $(M, +, \cdot)$ hat

$$+ : M \times M \rightarrow M$$

$$\cdot : R \times M \rightarrow M$$

- ③ M heißt **unitärer Modul**, wenn $1 \in R$ existiert und neutral bzgl. der S -Multiplikation \cdot ist

$$1 \cdot u = u$$

Elemente von M heißen **Vektoren**.
Elemente von R heißen **Skalare**.
 R heißt **Skalarring**.

Definition 11.1

Es sei $(K, +, \cdot)$ ein Körper. Ein **K -Vektorraum** $(V, +, \cdot)$ hat

$$+ : V \times V \rightarrow V$$

$$\cdot : K \times V \rightarrow V$$

- ③ $1 \in K$ ist neutral bzgl. der S -Multiplikation \cdot

$$1 \cdot u = u$$

Elemente von V heißen **Vektoren**.
Elemente von K heißen **Skalare**.
 K heißt **Skalarkörper**.

Definition 29.2

Es sei $(R, +, \cdot)$ ein kommutativer Ring und $(M, +, \cdot)$ ein R -Modul.

- 1 Eine bzgl. $+$ und \cdot abgeschlossene Teilmenge $U \subseteq M$ heißt ein **Untermodul** von $(M, +, \cdot)$, wenn $(U, +, \cdot)$ selbst wieder ein R -Modul ist.

- 2 Ein Untermodul $(U, +, \cdot)$ von $(M, +, \cdot)$ heißt **echt**, wenn $U \subsetneq M$ gilt.

Beispiel 29.4

- 1 Über jedem kommutativen Ring R ist der **Nullmodul** der Modul mit $M = \{0_M\}$ und die dadurch eindeutig bestimmten Verknüpfungen $0_M + 0_M = 0_M$ und $\alpha \cdot 0_M = 0_M$ für $\alpha \in R$.
- 2 Jede kommutative Ring $(R, +, \cdot)$ ist ein Modul $(R, +, \cdot)$ über sich selbst.
- 3 Jeder kommutative Ring $(R, +, \cdot)$ ist ein Modul $(R, +, \cdot)$ über jedem seiner Unterringe U .

Beispiel 29.4

- ④ Es sei $(R, +, \cdot)$ ein kommutativer Ring und $J \subseteq R$ ein Ideal von R . Dann ist $(J, +, \cdot)$ ein R -Modul, und zwar ein Untermodul des R -Moduls $(R, +, \cdot)$.

- ⑤ Für $n \in \mathbb{N}_0$ ist $(R^n, +, \cdot)$ mit der komponentenweisen Addition und S-Multiplikation ein Modul über dem kommutativen Ring $(R, +, \cdot)$.

- ⑥ Für $m, n \in \mathbb{N}_0$ ist $R^{n \times m}$ mit der komponentenweisen Addition und S-Multiplikation ein Modul über dem kommutativen Ring $(R, +, \cdot)$.

Beispiel 29.4

- ⑦ Es sei X eine beliebige Menge, $(R, +, \cdot)$ ein kommutativer Ring und $(M, +, \cdot)$ ein R -Modul. Dann bildet $M^X = \{f \mid f: X \rightarrow M\}$ mit der punktweisen Addition und punktweisen S -Multiplikation einen R -Modul.

Beispiel 29.4

vgl. Bemerkung 7.20

⑧ Eine abelsche Gruppe $(G, +)$ ist ein unitärer Modul über $(\mathbb{Z}, +, \cdot)$:

$$n a = \begin{cases} a + a + \cdots + a, & \text{falls } n > 0 \\ 0, & \text{falls } n = 0 \\ -(a + a + \cdots + a), & \text{falls } n < 0 \end{cases}$$

gemischtes Assoziativgesetz

$$(n \cdot m) \cdot a = n \cdot (m \cdot a)$$

gemischte Distributivgesetze

$$\begin{aligned} n \cdot (a + b) &= (n \cdot a) + (n \cdot b) \\ (n + m) \cdot b &= (n \cdot b) + (m \cdot b) \end{aligned}$$

Beispiel 29.4

- 9 Ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins, dann bilden die Polynome $(R[t], +, \cdot)$ einen unitären R -Modul.

Die Polynome $R_n[t]$ vom Höchstgrad $n \in \mathbb{N}_0$ bilden einen Untermodul von $R[t]$.

- 10 Ist $(K, +, \cdot)$ sogar ein Körper, dann bilden die Polynome $(K[t], +, \cdot)$ einen K -Vektorraum.

Die Polynome $K_n[t]$ vom Höchstgrad $n \in \mathbb{N}_0$ bilden einen Unterraum von $K[t]$.

Bemerkung 29.5

Es sei $(R, +, \cdot)$ ein kommutativer Ring und $(M, +, \cdot)$ ein R -Modul.

- Linearkombination einer Familie $F = (v_i)_{i \in I}$ von Vektoren in M
- von einer Familie $F = (v_i)_{i \in I}$ **erzeugter Untermodul**

$$\langle F \rangle := \bigcap \left\{ U \mid \begin{array}{l} U \text{ ist Untermodul von } M \\ \text{und } \{v_i \mid i \in I\} \subseteq U \end{array} \right\}$$

- Wenn M **unitär** ist, dann besteht $\langle F \rangle$ genau aus den Linearkombinationen von F .

Homomorphismen von Moduln

Definition 29.6

Es seien $(M_1, +, \cdot)$ und $(M_2, +, \cdot)$ Moduln über demselben kommutativen Ring $(R, +, \cdot)$.

- 1 Eine Abbildung $f: M_1 \rightarrow M_2$ heißt **strukturverträglich** oder ein **Homomorphismus von Moduln** oder eine **lineare Abbildung** von $(M_1, +, \cdot)$ in $(M_2, +, \cdot)$, wenn gilt:

$$f(u + v) = f(u) + f(v) \quad \text{für alle } u, v \in M_1$$

$$f(\alpha \cdot u) = \alpha \cdot f(u) \quad \text{für alle } u \in M_1 \text{ und } \alpha \in R$$

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

Beispiel 29.12

① Es seien $(R, +, \cdot)$ ein kommutativer Ring und $n, m, \ell \in \mathbb{N}_0$.

Für Matrizen $A \in R^{n \times m}$ und $B \in R^{m \times \ell}$ ist die **Matrix-Matrix-Multiplikation** AB wie für Matrizen über Körpern definiert.

Für festes $A \in R^{n \times m}$ ist die Abbildung

$$R^{m \times \ell} \ni B \mapsto AB \in R^{n \times \ell}$$

ein Homomorphismus von Moduln.

Insbesondere ist die Matrix-Vektor-Multiplikation

$$R^m \ni x \mapsto Ax \in R^n$$

ein Homomorphismus von Moduln.

Beispiel 29.12

- ② Es seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $(R[t], +, \cdot)$ der R -Modul der Polynome über R .

Die **(formale) Ableitungsabbildung** $f: R[t] \rightarrow R[t]$ ist ein Endomorphismus von R -Moduln mit

$$f\left(\sum_{k=0}^n \alpha_k t^k\right) :=$$

§ 29.2 Freie Moduln

Bemerkung 29.15

- Aus $\alpha \cdot u = 0$ für $\alpha \in R$ und $u \in M$ folgt nicht notwendigerweise $\alpha = 0$ oder $u = 0$.
- Im unitären \mathbb{Z} -Modul $\mathbb{Z} / 4\mathbb{Z}$ sind alle einelementigen Mengen

$$\{[0]\}, \quad \{[1]\}, \quad \{[2]\}, \quad \{[3]\}$$

bereits linear abhängig.

- Daher besitzen selbst unitäre Moduln nicht notwendigerweise eine Basis!

Definition 29.16

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

- 1 Ein unitärer R -Modul $(M, +, \cdot)$ heißt **frei**, wenn es ein linear unabhängiges Erzeugendensystem (eine **Basis**) von M gibt.
- 2 Ein unitärer R -Modul $(M, +, \cdot)$ heißt **endlich frei**, wenn es ein endliches, linear unabhängiges Erzeugendensystem (eine endliche Basis) von M gibt.

Beispiel 29.17

Es sei R ein kommutativer Ring mit Eins, der nicht der Nullring ist.

Freie R -Moduln sind:

- 1 der R -Nullmodul mit der Basis $()$ (leere Familie)
- 2 der R -Modul R^n für $n \in \mathbb{N}_0$ mit der Basis (e_1, \dots, e_n)
- 3 der R -Matrixmodul $R^{n \times m}$ für $m, n \in \mathbb{N}_0$ mit der Basis $(E_{ij})_{(i,j) \in \llbracket 1, n \rrbracket \times \llbracket 1, m \rrbracket}$
- 4 der R -Modul $R_n[t]$ der Polynome vom Höchstgrad $n \in \mathbb{N}_0$ mit der Basis $(1, t, t^2, \dots, t^n)$
- 5 der R -Polynommodul $R[t]$ mit der Basis $(1, t, t^2, \dots)$

Lemma 29.18

Es seien R ein kommutativer Ring mit Eins, M ein unitärer R -Modul und $(v_i)_{i \in I}$ eine Basis von M . Dann gilt:

Jeder Vektor $v \in M$ lässt sich in eindeutiger Weise (bis auf Summanden mit Nullkoeffizienten) aus Basisvektoren linearkombinieren.

Basen eindeutiger Kardinalität

Satz 29.19

Es sei R ein kommutativer Ring **mit Eins**, der **nicht der Nullring** ist. Weiter sei $(M, +, \cdot)$ ein endlich freier, unitärer R -Modul.

Dann haben alle Basen von M dieselbe endliche Kardinalität.

Folgerung 29.20

Unter diesen Voraussetzungen ist $(M, +, \cdot)$ isomorph zum Standardmodul $(R^n, +, \cdot)$ für $n \in \mathbb{N}_0$, wobei n die Kardinalität einer beliebigen Basis von M ist.

Diese heißt der **Rang** von M .

Bemerkung 29.21

- 1 Unter den Voraussetzungen von Satz 29.19 können wir wie in endlich-dimensionalen Vektorräumen basisabhängige Synthese- und Analyseabbildungen definieren.
- 2 Außerdem können wir — wie im Fall endlich-dimensionaler Vektorräume — Homomorphismen durch die Bilder einer Basis definieren.
- 3 Schließlich können wir Homomorphismen mithilfe von Darstellungsmatrizen kodieren.