

# **Skript Lineare Algebra & Geometrie 2, Hertrich-Jeromin**

Studierendenmitschrift

9. März 2016

# Inhaltsverzeichnis

<b>4</b>	<b>Volumenmessung</b>	<b>3</b>
4.3	Polynome & Polynomfunktionen . . . . .	3

## 4 Volumenmessung

### 4.3 Polynome & Polynomfunktionen

Warum? (Vielleicht eher „Algebra“ – allgemein – als „lineare“ Algebra) Wichtig: das charakteristische Polynom eines Endomorphismus – wichtiges Hilfsmittel im Kontext der Struktursätze.

**Beispiel** Wir definieren Polynomfunktionen  $p, q : K \rightarrow K$  eines Körpers  $K$  in sich durch

$$\begin{aligned} p : K &\rightarrow K, \quad x \mapsto p(x) := 1 + x + x^2 \\ q : K &\rightarrow K, \quad x \mapsto q(x) := 1 \end{aligned}$$

Falls  $K = \mathbb{Z}_2$  so gilt dann

$$\begin{aligned} \forall x \in K : x(x+1) &= 0 \\ \Rightarrow \forall x \in K : p(x) &= q(x) \end{aligned}$$

d.h., unterschiedliche „Polynome“ liefern die gleiche Polynomfunktion: Koeffizientenvergleich funktioniert nicht.

**Wiederholung** Auf dem Folgenraum  $K^{\mathbb{N}}$  betrachten wir die Familie  $(e_k)_{k \in \mathbb{N}}$  mit

$$e_k : \mathbb{N} \rightarrow K, \quad j \mapsto e_k(j) := \delta_{jk}$$

Wir wissen:  $(e_k)_{k \in \mathbb{N}}$  ist linear unabhängig, aber kein Erzeugendensystem:

$$\forall k \in \mathbb{N} : e_k \notin [(e_j)_{j \neq k}] \text{ und } [(e_j)_{j \in \mathbb{N}}] \neq K^{\mathbb{N}}$$

Insbesondere gilt:

$$\forall x \in [(e_j)_{j \in \mathbb{N}}] \quad \exists n \in \mathbb{N} \quad \forall k > n : x_k = 0$$

### 4.3.1 Idee & Definition

Wir fassen ein Polynom als (endliche) Koeffizientenfolge auf,

$$\sum_{k=0}^n t^k a_k \cong \sum_{k \in \mathbb{N}} e_k a_k \text{ mit } a_k = 0 \text{ für } k > n$$

und führen darauf das *Cauchyprodukt* (vgl. Analysis) als Multiplikation ein:

$$(a_k)_{k \in \mathbb{N}} \odot (b_k)_{k \in \mathbb{N}} := (c_k)_{k \in \mathbb{N}}$$

wobei

$$c_k := \sum_{j=0}^k a_j b_{k-j}.$$

Insbesondere gilt damit

$$\forall j, k \in \mathbb{N} : e_j \odot e_k = e_{j+k} \Rightarrow \forall k \in \mathbb{N} : \begin{cases} e_0 \odot e_k = e_k \\ e_1^k = \underbrace{e_1 \odot \cdots \odot e_1}_{k \text{ mal}} = e_k \end{cases}$$

Mit  $1 := e_0$ ,  $t := e_1$  und  $t^0 := 1$ , wie üblich, liefert dies:

$$\sum_{k=0}^n t^k a_k = \sum_{k \in \mathbb{N}} e_k a_k \in [(e_k)_{k \in \mathbb{N}}] \subset K^{\mathbb{N}}$$

### 4.3.2 Definition

$$K[t] := [(e_k)_{k \in \mathbb{N}}], \odot,$$

mit dem Cauchyprodukt  $\odot$ , ist die *Polynomialalgebra* über dem Körper  $K$ ; die Elemente von  $K[t]$ ,

$$p(t) = \sum_{k=0}^n t^k a_k = \sum_{k \in \mathbb{N}} e_k a_k,$$

heißen *Polynome in der Variablen  $t := e_1$* . Der *Grad* eines Polynoms ist

$$\deg \sum_{k=0}^n t^k a_k := \max\{k \in \mathbb{N} \mid a_k \neq 0\} \quad (\text{bzw. } \deg 0 := -\infty)$$

Ist (der „höchste“ Koeffizient)  $a_n = 1$  für  $\deg p(t) = n$ , so heißt das Polynom  $p(t)$  *normiert*.

**Notation** Mit  $t^k = e_k$ , also  $K[t] = [(e_k)_{k \in \mathbb{N}}]$  wird das Cauchyprodukt auf  $K[t]$  eine „normale“ Multiplikation, gefolgt von einer Sortierung nach den Potenzen der Variablen  $t$ . Wir werden das „ $\odot$ “ daher oft unterdrücken, und z.B.  $p(t)q(t)$  schreiben, anstelle von  $p(t) \odot q(t)$ .

**Bemerkung (Koeffizientenvergleich)** Mit dieser Definition von „Polynom“ gilt

$$p(t) = \sum_{k=0}^n t^k a_k = 0 \Rightarrow \forall k \in \mathbb{N} : a_k = 0,$$

da  $(t^k)_{k \in \mathbb{N}} = (e_k)_{k \in \mathbb{N}}$  linear unabhängig ist. Koeffizientenvergleich funktioniert!

**Bemerkung** Die Polynomalgebra  $K[t]$  über  $K$  ist eine assoziative und kommutative  $K$ -Algebra, weiters ist  $K[t]$  unitär mit Einselement  $1 = e_0$ .

### 4.3.3 Definition

Eine  $K$ -Algebra ist ein  $K$ -VR mit einer *bilinearen Abbildung*,

$$\odot : V \times V \rightarrow V, (v, w) \mapsto v \odot w,$$

d.h. es gilt

- (i)  $\forall w \in V : V \ni v \mapsto v \odot w \in V$  ist linear;
- (ii)  $\forall v \in V : V \ni w \mapsto v \odot w \in V$  ist linear.

Eine  $K$ -Algebra heißt

- unitär (mit Einselement 1), falls

$$\exists 1 \in V \forall v \in V : 1 \odot v = v \odot 1 = v$$

- assoziativ, falls

$$\forall u, v, w \in V : (u \odot v) \odot w = u \odot (v \odot w)$$

- kommutativ, falls

$$\forall v, w \in V : v \odot w = w \odot v$$

**Beispiel**  $\text{End}(V)$  ist (mit Komposition) eine unitäre assoziative Algebra.

**Bemerkung** In jeder Algebra  $(V, \odot)$  gilt:

$$\forall v \in V : 0 \odot v = v \odot 0 = 0$$

da z.B. für  $v \in V$  gilt

$$v \odot 0 = v \odot (0 + 0) = v \odot 0 + v \odot 0 \Rightarrow 0 = v \odot 0$$

Ist  $(V, \odot)$  unitär, so liefert  $[1] \subset V$  wegen  $1 \odot 1 = 1$  einen Körper:

$$([1], +|_{[1] \times [1]}, \odot|_{[1] \times [1]}) \cong K$$

vermöge  $K \ni x \mapsto 1 \cdot x \in [1]$  (siehe Aufgabe 5).

#### 4.3.4 Definition

Ein *Algebra-Homomorphismus* zwischen  $K$ -Algebren  $(V, \odot)$  und  $(W, *)$  ist eine lineare Abbildung  $\psi \in \text{Hom}(V, W)$ , für die gilt:

$$\forall v, v' \in V : \psi(v \odot v') = \psi(v) * \psi(v')$$

**Bemerkung**  $\text{Hom}(V, W)$  wird oft auch für den (Vektor-)Raum der Algebra-Homomorphismen verwendet. In dieser LVA bedeutet „ $\text{Hom}(V, W)$ “ immer VR-Homomorphismen, bei allen „anderen“ Homomorphismen wird erwähnt, was gemeint ist.

#### 4.3.5 Einsetzungssatz & Definitionen

Seien  $(V, \odot)$  eine unitäre assoziative Algebra und  $v \in V$ . Dann ist

$$\psi_v : K[t] \rightarrow V, \sum_{k=0}^n t^k a_k = p(t) \mapsto \psi_v(p(t)) := \sum_{k=0}^n v^k a_k$$

– wobei  $v^0 = 1$  sinnvoll ist, da die Algebra unitär ist – ein Algebra-Homomorphismus;  $\psi_v$  heißt *Einsetzungshomomorphismus*.

$$p : V \rightarrow V, v \mapsto p(v) := \psi_v(p(t))$$

heißt die zu  $p(t) \in K[t]$  gehörige *Polynomfunktion* auf  $V$ .

**Bemerkung** Wie üblich:  $v^k := \underbrace{v \odot \cdots \odot v}_{k\text{-mal}}$  und  $v^0 := 1$ .

#### Beweis

1.  $\psi_v$  ist linear:

- für  $p(t) = \sum_{k \in \mathbb{N}} t^k a_k$  und  $a \in K$  gilt:

$$\psi_v(p(t)a) = \psi_v\left(\sum_{k \in \mathbb{N}} t^k a_k a\right) = \sum_{k \in \mathbb{N}} v^k a_k a = \psi_v(p(t))a;$$

- für  $p(t) = \sum_{k \in \mathbb{N}} t^k a_k$  und  $q(t) = \sum_{k \in \mathbb{N}} t^k b_k$  gilt:

$$\psi_v(p(t) + q(t)) = \psi_v\left(\sum_{k \in \mathbb{N}} t^k (a_k + b_k)\right) = \sum_{k \in \mathbb{N}} v^k (a_k + b_k) = \psi_v(p(t)) + \psi_v(q(t))$$

2.  $\psi_v$  ist „multiplikativ“, d.h. verträglich mit der beteiligten Multiplikation:

Für die Vektoren der Basis  $(t^k)_{k \in \mathbb{N}}$  von  $K[t]$  gilt, da  $(V, \odot)$  assoziativ ist,

$$\psi_v(t^m t^n) = \psi_v(t^{m+n}) = v^{m+n} = v^m \odot v^n = \psi_v(t^m) \odot \psi_v(t^n).$$

Da aber  $\psi_v$  linear und die Multiplikation in  $K[t]$  und in  $(V, \odot)$  bilinear sind, folgt die Behauptung.

**Bemerkung (Fortsetzungssatz für bilineare Abbildungen)** Im Beweis haben wir verwendet: Die Abbildungen

$$K[t] \times K[t] \rightarrow V, (p(t), q(t)) \mapsto \begin{cases} \psi_v(p(t)q(t)) & \text{(Cauchyprodukt)} \\ \psi_v(p(t)) \odot \psi_v(q(t)) & \text{(Produkt in } (V, \odot)) \end{cases}$$

sind bilinear (da  $\psi_v$  linear ist), sind also gleich, sobald sie auf einer Basis übereinstimmen. Dies ist die Eindeutigkeit eines Fortsetzungssatzes für bilineare Abbildungen:

Sind  $V, W$   $K$ -VR,  $(b_i)_{i \in I}$  eine Basis von  $V$  und  $(\beta_{ij})_{i,j \in I}$  eine Familie in  $W$ , so gibt es eine eindeutige bilineare Abbildung

$$\beta : V \times V \rightarrow W$$

mit

$$\forall i, j \in I : \beta(b_i, b_j) = \beta_{ij}$$

Dieser Fortsetzungssatz folgt direkt aus dem Fortsetzungssatz für lineare Abbildungen, da

$$\{\beta : V \times V \rightarrow W \text{ bilinear}\} \cong \text{Hom}(V, \text{Hom}(V, W))$$

vermittels des Isomorphismus

$$\beta \mapsto \left( v \mapsto \underbrace{\beta(v, \cdot)}_{\in \text{Hom}(V, W)} \right),$$

d.h. durch Nacheinandereinsetzen der Argumente.

**Bemerkung** Die Abbildung eines Polynoms auf seine Polynomfunktion auf dem Körper,

$$K[t] \ni p(t) \mapsto (x \mapsto p(x)) = \psi_x(p(t)) \in K^K$$

ist für  $\text{Char } K \neq 0$  nicht injektiv<sup>1</sup>. Das heißt: Koeffizientenvergleich (für Polynomfunktionen) kann nur funktionieren, wenn  $\text{Char } K = 0$ .

**Beispiel & Bemerkung** Ist  $V$   $K$ -VR, so ist  $\text{End}(V)$  eine  $K$ -Algebra (mit Komposition  $\circ$ ). Man erhält also für  $f \in \text{End}(V)$  einen Einsetzungshomomorphismus

$$\psi_f : K[t] \rightarrow \text{End}(V), \quad p(t) \mapsto \psi_f(p(t)) = p(f);$$

und für jedes Polynom  $p(t) \in K[t]$  eine zugehörige Polynomfunktion

$$p : \text{End}(V) \rightarrow \text{End}(V), \quad f \mapsto \psi_f(p(t)) = p(f).$$

Dieses Beispiel ist der Schlüssel zum Satz von Cayley-Hamilton (im nächsten Abschnitt).

#### 4.3.6 Lemma

Für Polynome  $p(t), q(t) \in K[t]$  gilt:

- $\deg p(t) \odot q(t) = \deg p(t) + \deg q(t)$ ,
- $\deg p(t) + q(t) \leq \max\{\deg p(t), \deg q(t)\}$ .

**Beweis** Für  $p(t) = \sum_{k \in \mathbb{N}} t^k a_k$  und  $q(t) = \sum_{k \in \mathbb{N}} t^k b_k$  ist

$$p(t) \odot q(t) = \sum_{k \in \mathbb{N}} t^k c_k \text{ mit } c_k = \sum_{j=0}^k a_j b_{k-j}$$

Gilt nun  $\deg p(t) = n$  und  $\deg q(t) = m$ , d.h.

$$a_n, b_m \neq 0 \wedge \forall k > n, k' > m : a_k = b_{k'} = 0$$

so folgt

$$\left. \begin{array}{l} \forall k > m+n : c_k = 0 \\ c_{m+n} = a_n b_m \end{array} \right\} \Rightarrow \deg p(t) \odot q(t) = m+n$$

Gilt andererseits  $\deg p(t) = -\infty$  oder  $\deg q(t) = -\infty$ , also  $p(t) = 0 \vee q(t) = 0$ , so folgt

$$p(t) \odot q(t) = 0 \Rightarrow \deg p(t) \odot q(t) = -\infty.$$

Die zweite Behauptung ist offensichtlich wahr.

---

<sup>1</sup>sonst wäre  $K^K$  unendlich dimensional.



**Beispiel** Für  $p(t), q(t), d(t) \in K[t]$  mit  $d(t) \neq 0$  gilt

$$d(t)p(t) = d(t)q(t) \Rightarrow p(t) = q(t).$$

Nämlich: da  $\deg d(t) \geq 0$ ,

$$\begin{aligned} -\infty &= \deg d(t)(p(t) - q(t)) \\ &= \deg d(t) + \deg (p(t) - q(t)) \\ \Rightarrow \deg (p(t) - q(t)) &= -\infty \\ \Rightarrow p(t) &= q(t) \end{aligned}$$

### 4.3.7 Euklidischer Divisionsalgorithmus

Seien  $p(t), d(t) \in K[t]$ ,  $d(t) \neq 0$ . Dann existieren eindeutig  $q(t), r(t) \in K[t]$ , sodass

$$p(t) = d(t)q(t) + r(t) \text{ und } \deg r(t) < \deg d(t).$$

**Bemerkung** Ist  $\deg p(t) \leq \deg d(t)$ , so ist die Aussage trivial.

**Beweis** Eindeutigkeit folgt wie im Beispiel; mit

$$\begin{aligned} p(t) &= \begin{cases} d(t)q(t) + r(t) \\ d(t)\tilde{q}(t) + \tilde{r}(t) \end{cases} \\ \Rightarrow d(t)(q(t) - \tilde{q}(t)) &= \tilde{r}(t) - r(t) \end{aligned}$$

erhält man

$$\begin{aligned} \deg d(t) + \deg (q(t) - \tilde{q}(t)) &= \deg (r(t) - \tilde{r}(t)) \\ &\leq \max\{\deg r(t), \deg \tilde{r}(t)\} < \deg d(t). \end{aligned}$$

Also folgt

$$\deg (q(t) - \tilde{q}(t)) = -\infty \Rightarrow \deg (r(t) - \tilde{r}(t)) = \deg d(t) - \infty = -\infty$$

und damit

$$\tilde{q}(t) = q(t) \text{ und } \tilde{r}(t) = r(t).$$

Existenz: Mit  $k := \deg d(t) \geq 0$  und

$$K[t]_m := \{q(t) \in K[t] \mid \deg q(t) \leq m\} \text{ für } m \in \mathbb{N}$$

betrachte man die Abbildung

$$K[t]_m \times K[t]_{k-1} \rightarrow K[t]_{k+m}, \quad (q(t), r(t)) \mapsto d(t)q(t) + r(t).$$

Diese Abbildung ist linear (klar) und injektiv, denn: ist  $q(t) \neq 0$ , so folgt wegen

$$\deg r(t) < k = \deg d(t) \leq \deg d(t)q(t)$$

dass

$$\begin{aligned} \deg (d(t)q(t) + r(t)) &= \deg d(t)q(t) \geq k > -\infty \\ \Rightarrow d(t)q(t) + r(t) &\neq 0, \end{aligned}$$

also

$$d(t)q(t) + r(t) = 0 \Rightarrow q(t) = 0 \wedge r(t) = 0.$$

Wegen

$$\dim K[t]_m \times K[t]_{k-1} = (m+1) + k = (k+m) + 1 = \dim K[t]_{k+m}$$

liefert diese Abbildung dann für jedes  $m \in \mathbb{N}$  einen Isomorphismus

$$K[t]_m \times K[t]_{k-1} \rightarrow K[t]_{k+m}$$

#### 4.3.8 Korollar & Definition

Sei  $p(t) \in K[t]$  mit  $\deg p(t) \geq 1$ . Ist  $x \in K$  eine *Nullstelle* von  $p(t)$ , d.h.

$$p(x) = \psi_x(p(t)) = 0,$$

so folgt

$$\exists! q(t) \in K[t] : p(t) = (t - x)q(t)$$

**Beweis** Seien  $p(t) \in K[t]$  mit  $\deg p(t) \geq 1$  und  $x \in K$  eine Nullstelle von  $p(t)$ ; dann gibt es eindeutig  $q(t), r(t) \in K[t]$  mit

$$p(t) = (t - x)q(t) + r(t) \text{ und } \deg r(t) < \deg(t - x) = 1,$$

also

$$p(t) = (t - x)q(t) + r(t) = (t - x)q(t) + c_0.$$

Einsetzen von  $x \in K$  liefert dann

$$0 = p(x) = (x - x)q(x) + c_0 = c_0$$

**Bemerkung und Beispiel** Dies liefert eine Methode, um Polynome zu *faktorisieren*: Für jede gefundene Nullstelle kann man einen *Linearfaktor* abspalten.

$$p(t) = t^4 - t^3 + t^2 - t = \begin{cases} t(t-1)(t-i)(t+i) \in \mathbb{C}[t] \\ t(t-1)(t^2+1) \in \mathbb{R}[t] \end{cases}$$

### 4.3.9 Mehr zu Polynomen

Dies ist der Anfang einer der Teilbarkeitstheorie der natürlichen Zahlen ähnlichen Theorie für Polynome.

Sind  $p(t), d(t) \in K[t]$ , so heißt  $d(t)$  Teiler von  $p(t)$ ,  $d(t) \mid p(t)$ , falls

$$\exists q(t) \in K[t] : p(t) = d(t)q(t).$$

**Primpolynom** Nennt man  $p(t) \in K[t]$  mit  $\deg p(t) > 0$  ein *Primpolynom* (oder *irreduzibel*), falls für  $d(t), q(t) \in K[t]$  gilt:

$$p(t) = d(t)q(t) \Rightarrow (\deg q(t) = 0 \vee \deg d(t) = 0),$$

so gilt der Satz über die *Primfaktorzerlegung*:

Jedes Polynom  $p(t) \in K[t]$  mit  $\deg p(t) > 0$  zerfällt eindeutig in Primpolynome,

$$p(t) = a_n p_1(t) \cdots p_m(t),$$

wobei  $a_n \in K$  und  $p_1(t), \dots, p_m(t) \in K[t]$  normierte Primpolynome sind.

**Beweis** Existenz ist einfach zu zeigen (Induktion über  $n$ ), die weniger leicht zu zeigende Eindeutigkeit benutzt die Existenz des *größten gemeinsamen Teilers*  $d(t) = \text{ggT}(p(t), q(t))$  zweier Polynome  $p(t)$  und  $q(t)$ :

Zu  $p(t), q(t) \in K[t] \setminus \{0\}$  gibt es genau ein normiertes Polynom  $d(t) \in K[t]$  mit

$$\begin{aligned} d(t) \mid p(t) \wedge d(t) \mid q(t) \text{ und} \\ d'(t) \mid p(t) \wedge d'(t) \mid q(t) \Rightarrow d'(t) \mid d(t). \end{aligned}$$

**Lemma von Bézout** Für den ggT gilt auch das Lemma von Bézout:

$$\exists p'(t), q'(t) \in K[t] : d(t) = p(t)p'(t) + q(t)q'(t)$$

**Bemerkung** Aus der Gradformel,

$$\deg d(t)q(t) = \deg d(t) + \deg q(t)$$

folgt direkt:

*Jedes Polynom  $p(t) \in K[t]$  mit  $\deg p(t) = 1$  ist Primpolynom.*

**Fundamentalsatz der Algebra** Falls  $K = \mathbb{C}$ , so sind die Polynome mit Grad 1 die einzigen Primpolynome:

*In  $\mathbb{C}$  zerfällt jedes Polynom (mit Grad  $\geq 1$ ) in Linearfaktoren;*

$$\forall p(t) \in \mathbb{C}[t], \deg \geq 1 : \exists x_1, \dots, x_n \in \mathbb{C}$$

*mit*

$$p(t) = a_n \prod_{j=1}^n (t - x_j)$$

Ist  $K = \mathbb{R}$ , so ist dies nicht der Fall; ein Primpolynom vom Grad  $\deg p(t) = 2$  ist z.B.

$$p(t) = t^2 + 1 \in \mathbb{R}[t],$$

denn

$$t^2 + 1 = (t - x_1)(t - x_2) \Rightarrow \begin{cases} 0 = x_1 + x_2 \\ 1 = x_1 \cdot x_2 \end{cases} \Rightarrow 1 = -x^2$$

Andererseits ist  $p(t) \in \mathbb{R}[t] \subset \mathbb{C}[t]$ , also existieren  $x_1, \dots, x_n \in \mathbb{C}$  mit

$$a_n \prod_{j=1}^n (t - x_j) = p(t) = \overline{p(t)} = \overline{a_n} \prod_{j=1}^n (t - \overline{x_j}),$$

d.h. mit der Eindeutigkeit der Primfaktorzerlegung,  $a_n \in \mathbb{R}$  und die  $x_j$  sind entweder reell oder treten in komplex-konjugierten Paaren auf:

$$p(t) = a_n \prod_{j=1}^m (t^2 - t(x_j + \overline{x_j}) + x_j \overline{x_j}) \prod_{j=2m+1}^n (t - x_j).$$

Ist also  $p(t) \in \mathbb{R}[t]$  Primpolynom, so folgt  $\deg p(t) \leq 2$  und

$$\deg p(t) = 2 \Rightarrow \exists x, y \in \mathbb{R} : p(t) = (t - x)^2 + y^2 \text{ mit } y \neq 0$$

In  $K = \mathbb{Q}$  gibt es noch „mehr“ Primpolynome, wie z.B.:

$$p(t) = t^2 - 2 \text{ oder } p(t) = t^4 + 1$$

# Index

Algebra, 5

-Homomorphismus, 6

Cauchyprodukt, 4

Einsetzungshomomorphismus, 6

Polynom, 4

-algebra, 4

funktion, 6

Grad, 4

normiertes, 4