

---

# Linear Algebra

---

## Contents

<b>0</b>	<b>Präliminarien</b>	<b>3</b>
0.1	Annulatoren	3
0.2	Berechnen von Annulatoren, Beziehung zu HGS	5
0.2	Bi-Dualraum	6
0.3	Vorlesung 3	8
0.5	Skript 5	12
0.5.1	4 Quotientraum	12
<b>1</b>	<b>Polynomialgebren</b>	<b>17</b>
1.6	Skript 6	17
1.6.1	Algebren	17
1.6.2	Polynomialgebra	19
1.7	Skript 7	19
1.8	Skript 8	21
1.8.1	Divisionsalgorithmus	22
1.9	Skript 9	23
1.9.1	Formale Ableitung	24
1.10	Skript 10	27
1.10.5	Primzerlegung (Faktorisierung)	29
<b>2</b>	<b>Multilinearformen und Determinanten</b>	<b>31</b>
2.11	Skript 11	31
2.11.6	Die symmetrischen Gruppen $S_n$	31
2.12	Skript 12	34
2.13	Skript 13	38
2.13.7	Multilinear Formen	38
2.13.8	Alternierende Multilineare Formen auf $K^n$	39
2.14	Skript 14	40
2.15	Skript 15	45
2.16	Skript 16	47
<b>3</b>	<b>Normalformen</b>	<b>52</b>
3.17	Skript 17	52
3.17.9	Eigenwerte und Eigenvektoren	52
3.18	Skript 18	56
3.19	Skript 19	59
3.19.10	Annihilator Ideal	59
3.20	Skript 20	62
3.20.1	Trigonalisierbarkeit	63

---

3.21 Skript 21 . . . . .	64
3.21.12 Invariante Unterräume . . . . .	64
3.22 Skript 22 . . . . .	65
3.23 Skript 23 . . . . .	69
3.23.13 Direkte Summe und Primzerlegung . . . . .	69

## 0 Preliminarien

### Ansatz:

$K$  Körper und  $V$  ein endlich dimensionaler  $K$ -Vektorraum

### 0.1 Annulatoren

Erinnerung (s. Skript 22 LA I)

#### Theorem Charakterisierung von Dualbasen)

$K$  Körper

Sei  $V$  ein  $n$ -dim.  $K$ -Vektorraum und  $\mathcal{B} = (\alpha_1, \dots, \alpha_n)$  eine geordnete Basis für  $V$ . Es gibt genau eine geordnete Dualbasis für  $V^*$ ,  $\mathcal{B}^* = (f_1, \dots, f_n)$ , sodass:

$$(1) f_i(\alpha_j) = \delta_{ij}$$

$$(2) \forall f \in V^* : f = \sum_{i=1}^n f(\alpha_i) f_i$$

$$(3) \forall \alpha \in V : \alpha = \sum_{i=1}^n f_i(\alpha) \alpha_i$$

Das heißt:  $\forall f \in V^*$  und  $\forall \alpha \in V$  gilt:

$$[f]_{\mathcal{B}^*} = \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_n) \end{pmatrix} \text{ und}$$

$$[\alpha]_{\mathcal{B}} = \begin{pmatrix} f_1(\alpha) \\ \vdots \\ f_n(\alpha) \end{pmatrix}$$

(Dualität)

#### Definition 0.1.1

Sei  $V$  ein  $n$ -dim.  $K$ -Vektorraum und  $S \subseteq V$ . Der Annihilator (Annulator) von  $S$ , was wir mit  $S^0$  bezeichnen, ist die folgende Untermenge von  $V^*$ :  $S^0 := \{f \in V^* : S \subseteq \ker(f)\}$

#### Proposition 0.1.2

Folgende Aussagen gelten:

$$(i) S_1 \subseteq S_2 \implies S_2^0 \subseteq S_1^0$$

$$(ii) S^0 = (\text{span}(S))^0$$

$$(iii) S^0 \subseteq V^* \text{ ist ein Unterraum}$$

$$(iv) \text{span}(S) = \{0\} \iff S^0 = V^*$$

$$(v) \text{span}(S) = V \iff S^0 = \{0\}$$

**Proof Proposition 0.1.2**

“ $\implies$ ” trivial

“ $\impliedby$ ” z.z.  $\text{span}(S) = \{0\}$  Zum Widerspruch sei  $\alpha \neq 0$  und  $\alpha \in \text{span}(S)$ , dann ist  $\{\alpha\}$  l.u. Wir ergänzen zu einer Basis  $\mathcal{B}$  für  $V$ .  $\mathcal{B} = (\alpha = \alpha_1, \dots, \alpha_n)$  Sei  $\mathcal{B}^* = (f_1, \dots, f_n)$  die Dualbasis für  $V^*$ . Es gilt:  $f_1(\alpha_1) = 1$ , also  $f_1 \notin S^0$

(v)

“ $\implies$ ” folgt aus (ii) und (iv)

“ $\impliedby$ ” Sei  $S^0 = \{0\}$  z.z.  $\text{span}(S) = V$ .

Setze  $W := \text{span}(S)$ . Zum Widerspruch: sei  $\alpha \in V \setminus W$  und  $(\alpha_1, \dots, \alpha_k) \subseteq W$  eine geordnete Basis für  $W$ . Dann ist  $(\alpha_1, \dots, \alpha_k, \alpha)$  l.u. in  $V$ .

Ergänze zu einer geordneten Basis  $(\alpha_1, \dots, \alpha_k, \alpha_{k+1} = \alpha, \dots, \alpha_n)$ . Sei nun  $\mathcal{B}^* := (f_1, \dots, f_k, f_{k+1}, \dots, f_n)$  die Dualbasis für  $V^*$ .

Es gilt

$$\underbrace{f_{k+1}(\alpha_j) = 0 : \forall j = 1, \dots, k}_{f_{k+1} \in S^0} \text{ und } \underbrace{f_{k+1}(\alpha_{k+1}) = 1}_{f_{k+1} \notin S^0} \quad \blacksquare$$

**Corollary 0.1.3 Trennung Eigenschaft**

$V$   $n$ -dim  $K$ -VR

Sei  $W \subsetneq V$  ein Unterraum und  $\alpha \in V \setminus W$ . Es existiert ein  $f \in V^*$  so, dass:

$$f(W) = \{0\} \text{ und } f(\alpha) \neq 0$$

**Proof Korollar 0.1.3**

Wir werden aus Proposition 0.1.2 (v) herleiten.

(v) ist äquivalent zur Aussage

$$\forall S \subseteq V : \text{span}(S) \subsetneq V \iff S^0 \neq \{0\}$$

Sei nun  $S$  eine Basis für  $W$  dann ist  $\text{span}(S) \subsetneq V$ , es folgt  $S^0 \neq \{0\}$ , d.h.  $\exists f \in V^*, f \neq 0 \wedge \underbrace{f \in S^0}_{f \in W^0}$

Sei  $(\alpha_1, \dots, \alpha_k)$  eine geordnete Basis für  $W$ .  $\alpha \notin \text{span}(\alpha_1, \dots, \alpha_k)$ , also  $(\alpha_1, \dots, \alpha_k, \alpha)$  l.u. Ergänze zur Basis

$$\mathcal{B} = (\alpha_1, \dots, \alpha_k, \alpha_{k+1} = \alpha, \dots, \alpha_n)$$

Sei  $\mathcal{B}^* = (f_1, \dots, f_k, f_{k+1}, \dots, f_n)$  Dualbasis. Setzte  $f := f_{k+1}$ . ■

**Theorem 0.1.4 Dimensionsformel für Annihilatoren**

Sei  $V$  ein  $n$ -dim  $K$ -VR und  $W \subseteq V$  ein Unterraum

Es gilt:

$$\dim W + \dim W^0 = \dim V$$

**Proof Satz 0.1.4**

Sei  $(\alpha_1, \dots, \alpha_k)$  eine geordnete Basis für  $W$ . Ergänze zu einer geordneten Basis

$$\mathcal{B} = (\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n)$$

für  $V$ . Sei

$$\mathcal{B}^* = (f_1, \dots, f_k, f_{k+1}, \dots, f_n)$$

die Dualbasis für  $V^*$ .

**Beh.**  $(f_{k+1}, \dots, f_n)$  eine Basis für  $W^0$ .

**Bew. der Beh.** bemerke dass  $\forall i = k+1, \dots, n$  ist  $f_i \in W^0$ , weil  $f_i(\alpha_j) = 0$ , wenn  $i \geq k+1$  und  $j \leq k$ .

**Beweis von Satz 0.1.4 (Fortsetzung)**

Nun ist  $\{f_{k+1}, \dots, f_n\} \subseteq V^*$  l.u. (weil Teil einer Basis). Also genügt es nun z.z.:

$$\text{span}\{f_{k+1}, \dots, f_n\} = W^0,$$

also sei  $f \in W^0$ . Es gilt (wegen (2) Charakteristik von Dualbasen), dass  $f = \sum_{i=1}^n f(\alpha_i) f_i$ . Da aber  $f \in W^0$  und  $\alpha_1, \dots, \alpha_k \in W$  folgt  $f(\alpha_1) = \dots = f(\alpha_k) = 0$ . Also  $f = \sum_{i=k+1}^n f(\alpha_i) f_i$ , also  $f \in \text{span}(f_{k+1}, \dots, f_n)$

**Corollary zum Trennungssatz**

Seien  $W_1, W_2 \subseteq V$  Unterräume.

**Es gilt:**  $W_1^0 = W_2^0 \iff W_1 = W_2$

**Proof Korollar 0.1**

“ $\Leftarrow$ ” trivial

“ $\Rightarrow$ ” Zum Widerspruch

Sei  $\alpha \in W_2 \setminus W_1$ . Nach Trennungssatz  $\exists f \in V^*$  so dass  $f(W_1) = 0$  und  $f(\alpha) \neq 0$ , also  $f \in W_1^0$ , aber  $f \notin W_2^0$  ■

**0.2 Berechnen von Annulatoren, Beziehung zu HGS****Example 0.2.1**

$V = \mathbb{R}^5$   $S := \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \subseteq V$ , wobei:  $\alpha_1 = (2, -2, 3, 4, -1)$ ,  $\alpha_2 = (-1, 1, 2, 5, 2)$ ,  $\alpha_3 = (0, 0, -1, -2, 3)$ ,  $\alpha_4 = (1, -1, 2, 3, 0)$

Setze  $W := \text{span}(S)$ . Finde  $W^0$

**Lösung:**

Wir wollen beschreiben  $f \in V^*$  wofür gilt:  $f \in S^0$ , d.h.  $f(\alpha_1) = f(\alpha_2) = f(\alpha_3) = f(\alpha_4) = 0$

Es gilt allgemein (s. Bsp. 22.3 LA I) für  $f \in V^*$ ,  $\exists c_1, c_2, c_3, c_4, c_5 \in K$  s.d.  $\forall (x_1, x_2, \dots, x_5) \in \mathbb{R}^5$ :  $f(x_1, x_2, \dots, x_5) = \sum_{j=1}^5 c_j x_j$

Insbesondere  $f \in W^0 \iff c_1, \dots, c_5$  erfüllen  $\sum_{j=1}^5 A_{ij} c_j = 0 \quad \forall 1 \leq i \leq 4$ , wobei  $A_{ij}$  die

Koeffizienten der Matrix

$$\begin{pmatrix} 2 & -2 & 3 & 4 & -1 \\ -1 & 1 & 2 & 5 & 2 \\ 0 & 0 & -1 & -2 & 3 \\ 1 & -1 & 2 & 3 & 0 \end{pmatrix},$$

d.h. Wir müssen HGS lösen und zwar

$$A \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Gauß-Eliminations-Verfahren  $\Rightarrow$  r.Z.S.F:

$$R = \begin{pmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ (c_1) & & (c_3) & & (c_5) \end{pmatrix}$$

$c_1, c_3, c_5$  Hauptvariablen  $c_2, c_4$  freie Variablen

Wir bekommen

$$\begin{aligned} c_1 - c_2 - c_4 &= 0 \\ c_3 + 2c_4 &= 0 \\ c_5 &= 0 \end{aligned}$$

Lösungsraum. Setze  $c_2 := a \in \mathbb{R}, c_4 := b \in \mathbb{R}$

$c_1 = a + b, c_3 = -2b, c_5 = 0$  also einsetzen.

$$W^0 = \{f : f(x_1, x_2, x_3, x_4, x_5) = (a + b)x_1 + ax_2 - 2bx_3 + bx_4 : a, b \in \mathbb{R}\}$$

## 0.2 Bi-Dualraum

Als Motivation, wollen wir die folgenden Fragen betrachten:

- (1)  $V \rightarrow V^*, \mathcal{B} \mapsto \mathcal{B}^*$

sie ist die Umkehrung? Genauer:

Sei  $\mathbb{B}$  eine geordnete Basis für  $V^*$ , gibt es eine geordnete  $\mathcal{B}$  für  $V$  s.d.  $\mathcal{B}^* = \mathbb{B}$ ?

- (2)  $V \rightarrow V^*, W \mapsto W^0$  Wie ist die Umkehrung= Genauer formuliert:

Sei  $U$  ein Unterraum von  $V^*$ , gibt es ein Unterraum  $W$  von  $V$  so dass  $W^0 = U$ ?

**Schlüssel:** wir arbeiten mit  $(V^*)^* := V^{**}$

### Example 0.2.2

$$\dim(V^{**}) = \dim(V^*) = \dim V$$

**Definition 0.2.3 Bi-Dualraum**

$V^{**}$  heißt **Bidualraum** zu  $V$ .

**Proposition 0.2.4**

Sei  $\alpha \in V$ ,  $\alpha$  induziert (kanonisch) eine lineare Funktionale  $L_\alpha \in V^{**}$  wie folgt

$$L_\alpha : V^* \rightarrow K$$

definiert durch:  $L_\alpha(f) := f(\alpha) \quad \forall f \in V^*$

**Proof Proposition 0.2.4**

Wir berechnen für  $\forall c \in K, f, g \in V^*$ :

$$L_\alpha(cf + g) = (cf + g)(\alpha) = cf(\alpha) + g(\alpha) = cL_\alpha(f) + L_\alpha(g). \quad \blacksquare$$

**Theorem 0.2.5**

Die Abbildung  $\chi : V \rightarrow V^{**}, \alpha \mapsto L_\alpha$  definiert eine (kanonische) Isomorphie.

**Proof Satz 0.2.5**

$\lambda$  ist linear. Zu prüfen:

$$\chi(c\alpha + \beta) \stackrel{?}{=} c\lambda(\alpha) + \lambda(\beta)? \quad \forall c \in K, \alpha, \beta \in V, f \in V^*.$$

Wir berechnen:

$$\begin{aligned} [\lambda(c\alpha + \beta)](f) &= L_{c\alpha + \beta}(f) \\ &= f(c\alpha + \beta) \\ &= cf(\alpha) + f(\beta) \\ &= cL_\alpha(f) + L_\beta(f) \\ &= c\lambda(\alpha)(f) + \lambda(\beta)(f) \\ &= [c\lambda(\alpha) + \lambda(\beta)](f) \end{aligned}$$

Wir müssen noch zeigen dass  $\lambda$  bijektiv ist. Da aber  $\dim V = \dim V^{**}$  ist (folgt aus Satz 19.10 LA I)

es genügt zu zeigen:  $\lambda$  ist injektiv, d.h. z.z. dass  $\ker(\lambda) = \{0\}$ . Zum Widerspruch nehmen wir an  $\exists \alpha \in V$  s.d.:

$$\lambda(\alpha) = 0 \quad \text{aber} \quad \alpha \neq 0$$

$$L_\alpha \equiv 0 \quad \text{aber} \quad \alpha \neq 0$$

Aber:  $\alpha \neq 0 \implies \{\alpha\}$  ist l.u.  $\implies \mathcal{B} = (\alpha_1 = \alpha, \dots, \alpha_n)$  eine geordnete Basis. Sei  $\mathcal{B}^* = (f_1, \dots, f_n)$  Dualbasis. Es gilt dann:  $f_1(\alpha) = f_1(\alpha_1) = 1$ , d.h.  $L_\alpha(f_1) = 1 \neq 0$  Widerspruch  $\blacksquare$

## 0.3 Vorlesung 3

**Corollary 0.3.1**

Sei  $L \in V^{**}$  bzw. Sei  $L$  eine lineare Funktionale auf  $V^*$ .

$\exists! \alpha \in V$  s.d.  $L = L_\alpha$ , d.h. s.d.:

$$L(f) = f(\alpha) \quad \forall f \in V^*. \quad (1)$$

**Proof Korollar 0.3.1**

Setze:  $\alpha := \lambda^{-1}(L)$  ■

**Corollary 0.3.2**

Sei  $\mathbb{B}$  eine geordnete Basis für  $V^*$ . Dann gibt es eine geordnete Basis  $\mathcal{B}$  für  $V$ , so dass  $\mathcal{B}^* = \mathbb{B}$ .

**Proof Korollar 0.3.2**

Setze  $\mathbb{B} = (f_1, \dots, f_n)$  und  $\mathbb{B}^* := (L_1, \dots, L_n)$  für  $V^{**}$  so dass  $L_i(f_j) = \delta_{ij}$

Korollar 0.3.1 liefert:  $\forall i : \exists! \alpha_i \in V$  mit (1) d.h.  $L_i(f) = f(\alpha_i) \forall 1 \leq i \leq n, f \in V^*$  Insbesondere  $L_i(f_j) = f_j(\alpha_i) = \delta_{ij} \quad \forall 1 \leq i, j \leq n$ . Setze  $\mathcal{B} := (\alpha_1, \dots, \alpha_n)$ . ■

**Example 0.3.3**

$E \subseteq V^*$

$E^0 = \{L \in (V^*)^* : \forall f \in E : L(f) = 0\}$  Betrachte  $\lambda : V \rightarrow V^{**}, \alpha \mapsto L_\alpha$

$$\begin{aligned} \lambda^{-1}(E^0) &= \{\alpha \in V : \lambda(\alpha) \in E^0\} \\ &= \{\alpha \in V : L_\alpha \in E^0\} \\ &= \{\alpha \in V : \forall f \in E : L_\alpha(f) = 0\} \\ &= \{\alpha \in V : \forall f \in E : f(\alpha) = 0\} \end{aligned}$$

**Theorem 0.3.4**

Sei  $W \subseteq V$  Unterraum, dann gilt

$$\lambda^{-1}(W^{00}) = W$$

**Proof Satz 0.3.4**

**Dimensionsformel** für Annihilatoren (Satz 0.1.4) liefert

$$\dim W + \dim W^0 = \dim V = \dim V^* = \dim W^0 + \dim W^{00}$$

Daraus folgt  $\dim W = \dim W^{00} = \dim(\lambda^{-1}(W^{00}))$

Es genügt zu zeigen:  $W \subseteq \lambda^{-1}(W^{00})$

Sei  $\alpha \in W$  beliebig aber fest, dann berechne  $\lambda(\alpha) = L_\alpha$ . Zu zeigen:  $L_\alpha \in W^{00} = (W^0)^0$ , d.h. zu zeigen ist

$$L_\alpha(f) = 0 \text{ für alle } f \in W^0$$

Sei  $f \in W^0$  beliebig aber fest, dann gilt  $L_\alpha(f) = f(\alpha) = 0$  da  $f(W^0) = 0$  und  $\alpha \in W$  ■ Also wurde



gezeigt, dass  $W$  ein Unterraum von  $\lambda^{-1}(W^{00})$  ist und

$$\dim W = \dim \lambda^{-1}(W^{00}), \text{ also folgt } W = \lambda^{-1}(W^{00}) \quad \blacksquare$$

### Corollary 0.3.5

Sei  $U \subseteq V^*, W := \lambda^{-1}(U^0) \subseteq V$ , dann gilt

$$W^0 = U$$

### Proof Korollar 0.3.5 Dimensionsformel für Annihilatoren (Satz 0.1.4)

$$\dim U + \dim^0 = \dim V^* = \dim V = \dim W + \dim W^0$$

Bemerke  $\dim W = \dim \lambda^{-1}(U^0) = \dim U^0$ . Es folgt  $\dim U = \dim W^0$ . Es genügt zu zeigen:  $U \subseteq W$

Bemerke

$$\begin{aligned} W &= \lambda^{-1}(U^0) \\ &= \{\alpha \in V : \lambda(\alpha \in U^0)\} \\ &= \{\alpha \in V : L_\alpha \in U^0\} \\ &= \{\alpha \in V : \forall f \in U : L_\alpha = 0\} \\ &= \{\alpha \in V : \forall f \in U : f(\alpha) = 0\}. \end{aligned}$$

Sei  $f \in U$  beliebig aber fest. Zu zeigen  $f \in W^0$ , d.h. z.z. für alle  $\alpha \in W : f(\alpha) = 0$

Sei  $\alpha \in W$  beliebig aber fest, dann gilt

$$f(\alpha) = L_\alpha(f) = 0$$

Also folgt  $U \subseteq W^0$  der gleichen Dimension, also  $U = W^0$

## DIE TRANSPONIERTE ABBILDUNG

Sei  $T : V \rightarrow W$  eine lineare Abbildung, dann induziert diese eine Abbildung  $T^t : W^* \rightarrow V^*, g \mapsto g \circ T$

**Behauptung:**  $T^t$  ist linear.

**Beweis:** Sei  $g_1, g_2 \in W^*, c \in K$ , dann gilt

$$\begin{aligned} T^t(g_1 + cg_2) &= (g_1 + cg_2) \circ T \\ &= g_1 \circ T + (cg_2) \circ T \\ &= g_1 \circ T + c(g_2 \circ T) \\ &= T^t(g_1) + cT^t(g_2) \end{aligned}$$

**Definition:** Die lineare Abbildung  $T^t$  wird die **transponierte Abbildung** zu  $T$  genannt

### Theorem 0.3.6

Seien  $V, W$  endlich-dimensionale  $K$ -VR und  $T$  eine lineare Abbildung, dann existiert eine ein-

deutige lineare Abbildung

$$T^t : W^* \rightarrow V^* \text{ s.d. } \forall \alpha \in V : \forall g \in W^* : (T^t(g))(\alpha) = g(T(\alpha)) \quad \blacksquare$$

### Theorem 0.4.2

- (1)  $\ker(T^t) = (R_T)^0$
- (2)  $\text{Rang}(T^t) = \text{Rang}(T)$
- (3)  $R_{T^t} = (\ker(T))^0$

### Proof Satz 0.4.2

- (1) Es gilt

$$\begin{aligned} g \in \ker(T^t) &\iff T^t(g) = 0 \\ &\iff g \circ T = 0 \\ &\iff \forall \alpha \in V : g(T(\alpha)) = 0 \\ &\iff g \in (R_T)^0 \end{aligned}$$

- (2) Setze  $n := \dim V$  und  $m := \dim W$ . Sei ferner  $r = \text{Rang}(T) = \dim R_T$ .  
Dimensionsformel für Annihilatoren (Satz 0.1.4 liefert

$$\begin{aligned} \dim R_T + \dim (R_T)^0 &= \dim W \\ \implies r + \dim (R_T)^0 &= m \\ \implies \dim (R_T)^0 &= m - r \\ \implies \dim \ker T^t &= m - r \end{aligned}$$

Nach dem Homorphiesatz (Satz 18.2) gilt für die lineare Abbildung  $T^t : W^* \rightarrow V^*$  schon

$$\begin{aligned} \dim R_{T^t} &= \dim W^* - \dim \ker T^t \\ \implies \text{Rang}(T^t) &= \dim R_{T^t} = m - \dim \ker T^t = m - (m - r) = r = \text{Rang}(T) \end{aligned}$$

- (3) Dimensionsformel für Annihilatoren (Satz 0.1.4)

$$\begin{aligned} \dim \ker T + \dim (\ker T)^0 &= \dim V \\ \implies \dim (\ker T)^0 &= \dim V - \dim \ker T = \dim R_T = \text{Rang } T = \text{Rang } T^t = \dim R_{T^t} \end{aligned}$$

Es genügt daher zu zeigen, dass  $R_{T^t} \subseteq (\ker T)^0$

Sei daher  $f \in R_{T^t}$  beliebig aber fest. Dann gilt für jedes  $\alpha \in \ker T$  schon  $f(\alpha) = T^t(g)(\alpha) = (g \circ T)(\alpha) = g(T(\alpha)) = g(0) = 0$  somit folgt  $f \in (\ker T)^0$   $\blacksquare$

### Theorem 0.4.3

Seien  $V, W$  endlich-dimensionale  $K$ -Vektorräume und eine lineare Abbildung  $T : V \rightarrow W$  mit transponierter Abbildung  $T^t : W^* \rightarrow V^*$ , seien ferner  $\mathcal{B}$  eine geordnete Basis von  $V$  mit Dualbasis  $\mathcal{B}^*$  und  $\mathcal{B}'$  eine geordnete Basis von  $W$  mit Dualbasis  $(\mathcal{B}')^*$ . Dann gilt

$$[T^t]_{(\mathcal{B}')^*, \mathcal{B}^*} = [T]_{\mathcal{B}, \mathcal{B}'}^t$$

**Proof Satz 0.4.3**

Setze  $A := [T]_{\mathcal{B}, \mathcal{B}'}$  und  $B := [T^t]_{(\mathcal{B}')^*, \mathcal{B}^*}$

$\mathcal{B} = (\alpha_1, \dots, \alpha_n), \mathcal{B}^* = (f_1, \dots, f_n)$

$\mathcal{B}' = (\beta_1, \dots, \beta_m), (\mathcal{B}')^* = (g_1, \dots, g_m)$

**Erinnerung:**  $T(\alpha_j) = \sum_{i=1}^m A_{ij} \beta_i$  für  $j = 1, \dots, n$

$T^t(g_j) = \sum_{i=1}^n B_{ij} f_i$  für  $j = 1, \dots, m$

Für beliebiges  $f \in V^*$  gilt  $f = \sum_{i=1}^n f(\alpha_i) f_i$  (Dualbasis)

Insbesondere ergibt sich damit für  $f := T^t(g_j) \in V^*$  schon

$$\sum_{i=1}^n B_{ij} f_i = T^t(g_j) = \sum_{i=1}^n (T^t(g_j))(\alpha_i) f_i = \sum_{i=1}^n A_{ji} f_i$$

Wir berechnen ferner

$$\begin{aligned} (T^t(g_j))(\alpha_i) &= (g_j \circ T)(\alpha_i) \\ &= g_j(T(\alpha_i)) \\ &= g_j\left(\sum_{k=1}^m A_{ik} \beta_k\right) \\ &= \sum_{k=1}^m A_{ik} g_j(\beta_k) \\ &= \sum_{k=1}^m A_{ki} \delta_{jk} \\ &= A_{ji} \end{aligned}$$

Somit folgt, dass  $A_{ji} = B_{ij}$  für alle  $i$  und  $j$ . Damit ist  $B = A^t$

**Erinnerung:**

Sei  $A \in \text{Mat}_{m \times n}(K)$

(i)  $\text{Sr}(A) := \dim \text{span Spalten von } A$

(ii)  $\text{Zr}(A) := \dim \text{span Zeilen von } A$

**Corollary 0.4.4**

Sei  $A \in \text{Mat}_{m \times n}(K)$ . Es gilt:  $\text{Zr}(A) = \text{Sr}(A)$ .

**Proof Korollar 0.4.4**

Sei  $\mathcal{E}_n$  die Standardbasis für  $K^{n \times 1}$  und  $\mathcal{E}_m$  die Standardbasis für  $K^{m \times 1}$

Und betrachte die lineare Abbildung

$$T_A : K^{n \times 1} \rightarrow K^{m \times 1}$$

definiert durch

$$T_A \left( \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \right) = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

die  $[T_A]_{\mathcal{E}_n, \mathcal{E}_m} = A$

Bemerke dass  $\text{Sr}(A) = \text{Rang}(T_A)$  weil  $R_{T_A} = \text{span}(\text{Spaltenvektoren von } A)$

Außerdem ist  $\text{Zr } A = \text{Sr } A^t$ , weil die Zeilen von  $A$  sind die Spalten von  $A^t$ . Es folgt nun aus Satz 0.4.2 (1) (anwendung mit  $T := T_A$ )

$$\text{Sr } A = \text{Rang } T_A = \text{Rang } T^t = \text{Sr } A^t = \text{Zr } A$$

(weil  $A^t = [T_A]_{\mathcal{E}_m^*, \mathcal{E}_n^*}$ )

■

### Definition 0.4.5

Sei  $A \in \text{Mat}_{m \times n}(K)$ . Definiere  $\text{Rang } A := r A = \text{Sr } A = \text{Zr } A$

## 0.5 Skript 5

### 0.5.1 4 Quotientraum

**Ansatz:**  $K$  ist ein Körper,  $V$  ist ein  $K$ -Vektorraum. Sei  $W \subseteq V$  ein Unterraum

### Definition 0.5.1

Seien  $\alpha, \beta \in V$ , wenn  $\alpha - \beta \in W$

Bezeichnung:  $\alpha \equiv \beta \pmod{W}$ .  $\alpha$  ist kongruent zu  $\beta$  modulo  $W$

### Lemma 0.5.2

Die Relation " $\alpha \equiv \beta \pmod{W}$ " definiert eine Äquivalenzrelation auf  $V$ .

### Proof Lemma 0.5.2

(1)  $\equiv$  ist reflexiv:  $\forall \alpha \in V$  gilt  $\alpha \equiv \alpha \pmod{W}$ , weil  $\alpha - \alpha = 0 \in W$

(2)  $\equiv$  ist symmetrisch:  $\forall \alpha, \beta \in V$  gilt:  $\alpha \equiv \beta \pmod{W} \implies \beta \equiv \alpha \pmod{W}$ , weil  $(\alpha - \beta) \in W \implies -(\alpha - \beta) \in W \implies \beta - \alpha \in W$ .

(3) Seien  $\alpha \equiv \beta \pmod{W}$  und  $\alpha, \beta, \gamma \in V$   
 $\beta \equiv \gamma \pmod{W} \implies (\alpha - \beta) \in W$  und  $(\beta - \gamma) \in W \implies (\alpha - \beta) + (\beta - \gamma) = \alpha - \gamma \in W \implies \alpha \equiv \gamma \pmod{W}$

Also ist  $\equiv$  transitiv

■

### Definition 0.5.3

Sei  $\alpha \in V$ . Die **Restklasse** von  $\alpha \pmod{W}$ , oder auch **Nebenklasse** von  $\alpha \pmod{W}$  ist die Äquivalenzklasse von  $\alpha$  bzgl der Äquivalenzrelation " $\equiv \pmod{W}$ ". Das heißt

$$[\alpha]_W := \{\beta \in V : \alpha \equiv \beta \pmod{W}\}.$$

**Bemerkung:**  $(\beta - \alpha \in W \implies \beta - \alpha = w \in W \implies \beta = \alpha + w \text{ für } w \in W)$

$$[\alpha]_W = \{\alpha + w : w \in W\}$$

**Bezeichnung:** Wir schreiben auch  $\alpha + W$  für die  $[\alpha]_W$ .

**Definition 0.5.4**

Bezeichne mit  $V/W$  Die Menge aller Nebenklassen  $\alpha \bmod W$ , d.h.

$$V/W = \{[\alpha]_W : \alpha \in V\}$$

$V/W$  heißt:  $V$  modulo  $W$

Auf diese Menge  $V/W$  wollen wir jetzt eine  $K$ -Vektorraum Struktur erklären

**Definition 0.5.5**

- (1) Sei  $[\alpha]_W$  die Nebenklasse von  $\alpha \in V$ . Ein Representant der Nebenklasse ist

$$\beta \in [\alpha]_W$$

(Bemerke:  $[\beta]_W = [\alpha]_W$  gdw.  $\alpha \in [\beta]_W$  gdw.  $\beta \in [\alpha]_W$ .)

- (2) Wir definieren Verknüpfung

$$+ : V/W \times V/W \rightarrow V/W$$

Seien  $\alpha_1 + W, \alpha_2 + W \in V/W$  definiere  $(\alpha_1 + W) + (\alpha_2 + W) := \underbrace{(\alpha_1 + \alpha_2)}_{\in V} + W$  Wir definieren eine Skalarmultiplikation, Verknüpfung

$$K \times (V/W) \rightarrow (V/W)$$

$$\forall c \in K, \forall \alpha \in V \text{ definiere } c(\alpha + W) := \underbrace{(c\alpha)}_{\in V} + W.$$

**Lemma 0.5.6**

Die Verknüpfungen (in Def 0.5.5) sind wohldefiniert unabhängig der Wahl der Repräsentanten, d.h.

- (a)  $\alpha \equiv \alpha' \bmod W$  und  $\beta \equiv \beta' \bmod W \implies \alpha + \beta \equiv \alpha' + \beta' \bmod W$   
 (b)  $\alpha \equiv \alpha' \bmod W$  und  $c \in K, c\alpha \equiv c\alpha' \bmod W$

**Proof Lemma 0.5.6**

- (a)  $\alpha - \alpha' \in W$  und  $\beta - \beta' \in W \implies (\alpha - \alpha') + (\beta - \beta') \in W$ , also  $(\alpha + \beta) - (\alpha' + \beta') \in W$   
 $\alpha + \beta \equiv \alpha' + \beta' \bmod W$ .  
 (b)  $\alpha - \alpha' \in W \implies c(\alpha - \alpha') \in W \implies c\alpha - c\alpha' \in W \implies c\alpha \equiv c\alpha' \bmod W$  ■

**Theorem 0.5.7**

Die Menge  $V/W$ , versehen mit Verknüpfungen ist ein  $K$ -Vektorraum.

**Proof 0.5.8 Satz 0.5.7**

Ü.A. Zum Beweis bemerke dass:

nehme  $0_{V/W} := [0_V]_W$

Für additive Inverse:  $-([\alpha]_W) = [-\alpha]_W$

**Definition**

$(V/W, +_{V/W}, \cdot_K)$  ist der **Quotientenraum** von  $V$  modulo  $W$

**Bezeichnung:**  $\alpha + W := \bar{\alpha}$  falls  $W$  klar im Ansatz ist

**Begründung:** die Schreibweise der Verknüpfungen wird einfacher:  $\bar{\alpha}_1 + \bar{\alpha}_2 = \overline{\alpha_1 + \alpha_2} \quad \forall \alpha_1, \alpha_2 \in V$   
 $\forall \alpha, \alpha_1, \alpha_2 \in V, \forall c \in K : c\bar{\alpha} = \overline{c\alpha}$

**Theorem 0.5.9 Die kanonische Projektion**

Die Abbildung

$$\pi_W : V \rightarrow V/W$$

definiert durch

$$\forall \alpha \in V : \pi_W(\alpha) := \bar{\alpha}$$

ist eine surjektive lineare Transformation mit  $\ker(\pi_W) = W$

**Proof Satz 0.5.9**

Linearität?

Für  $\alpha_1, \alpha_2 \in V, c \in K : \pi_W(c\alpha_1 + \alpha_2) = \overline{c\alpha_1 + \alpha_2} = \overline{c\alpha_1} + \bar{\alpha}_2 = c\bar{\alpha}_1 + \bar{\alpha}_2 = c\pi_W(\alpha_1) + \pi_W(\alpha_2)$

Surjektiv: Sei  $\bar{\alpha} \in V/W$ , dann ist  $\pi_W(\alpha) = \bar{\alpha}$  für  $\alpha \in V$

$\ker(\pi_W)$ ? Sei  $\alpha \in V, \alpha \in \ker(\pi_W) \iff \pi_W(\alpha) = 0_{V/W} \iff \underbrace{\alpha + W}_{\bar{\alpha}} = W \iff \alpha \in W$

**Corollary 0.5.10**

Es gilt:  $\dim W + \dim(V/W) = \dim V$

**Proof Korollar 0.5.10**

Folgt aus LAI Satz 18.2, (Dimensionssatz), Anwenden auf  $T = \pi_W$  ■

**Theorem 0.5.11 Homomorphiesatz für Vektorräume**

Seien  $V, Z$   $K$ -VR und  $T : V \rightarrow Z$  eine lineare Transformation. Es gilt:

$$V/\ker(T) \xrightarrow{\bar{T}} R_T$$

Genauer, betrachte die Abbildung  $\bar{T} : V/\ker(T) \rightarrow R_T$  definiert durch  $\bar{T}(\bar{\alpha}) := T(\alpha)$  ist wohldefiniert, linear, injektiv und surjektiv

**Proof Satz 0.5.11**

(i) Seien  $\bar{\alpha} = \bar{\alpha}'$  für  $\alpha, \alpha' \in V \implies T(\alpha) = T(\alpha')$ ?

Wir argumentieren

$$\begin{aligned} \bar{\alpha} = \bar{\alpha}' &\iff \alpha - \alpha' \in \ker(T) \\ &\iff T(\alpha - \alpha') = 0 \\ &\iff T(\alpha) - T(\alpha') = 0 \\ &\iff T(\alpha) = T(\alpha') \end{aligned}$$

$$(ii) \quad \overline{T}(c\overline{\alpha_1} + \overline{\alpha_2}) = c\overline{T}(\overline{\alpha_1}) + \overline{T}(\overline{\alpha_2}) \quad (\ddot{U}B)$$

(iii) Sei  $T(\alpha) \in R_T$  für ein geeignetes  $\alpha \in V$ . Es ist  $\overline{T}(\overline{\alpha}) = T(\alpha)$  Also  $\overline{T}$  ist surjektiv.

$$(iv) \quad \overline{\alpha} \in \ker(\overline{T}) \iff \overline{T}(\overline{\alpha}) = 0 \iff T(\alpha) = 0 \iff \alpha \in \ker(T)$$

**Erinnerung:** Seien  $W, W' \subseteq V$  so dass

$$(i) \quad V = W + W' \text{ und}$$

$$(ii) \quad W \cap W' = \{0\}.$$

Dann ist  $V$  die **direkte Summe** von  $W$  und  $W'$ , wir schreiben

$$V = W \oplus W'$$

$$\forall v \in V \exists! w \in W, w' \in W' : v = w + w'$$

### Corollary 0.5.12

Seien  $W, W'$  Unterräume, s. d.  $V = W \oplus W'$  Es gilt:

$$\frac{W \oplus W'}{W} \simeq W'$$

### Proof Korollar 0.5.12

Definiere eine Abbildung  $P_{W'} : V \rightarrow W'$  folgendermaßen: für  $v \in V$  schreibe  $v = w + w'$  für geeignete  $w \in W, w' \in W'$ , definiere

$$P_{W'}(v) := w'$$

**Beh.**  $P_{W'}$  ist surjektiv. Sei  $w' \in W'$ , dann ist  $P_{W'}(0 + w') = w'$

**Beh.**  $\ker(P_{W'}) = W$  weil  $v \in \ker(P_{W'}) \iff v = w + 0 \iff v \in W$

Satz 0.5.11 anwenden

$$\frac{W \oplus W'}{W} \simeq W'$$

■

### Corollary 0.5.13

Sei  $W \subseteq V$  ein Unterraum. Es gilt:

$$(V/W)^* \simeq W^0$$

### Proof 0.5.14 Korollar 0.5.13

Setze  $T := \pi_W$  die kanonische Projektion  $T : V \rightarrow V/W$  Betrachte  $T^t : (V/W)^* \rightarrow V^*$

Wir wollen Satz 0.4.2 anwenden, und bekommen

$$R_{T^t} = (\ker T)^0 = W^0$$

und

$$\ker T^t = (R_T)^0 = (V/W)^0 = \{0\}$$

Also ist  $T^t : (V/W)^* \xrightarrow{\sim} W^0$  linear, injektiv und surjektiv

■

**Corollary 0.5.15**

Sei  $W \subseteq V$  Es gilt

$$W^* \simeq V^*/W^0$$

**Proof 0.5.16   Korollar 0.5.14**

Betrachte  $\text{Id} : W \rightarrow V$  und dazu  $\text{Id}^t : V^* \rightarrow W^*$

Satz 0.4.2 anwenden:  $\ker(\text{Id}^t) = (R_{\text{Id}})^0 = W^0$  und  $R_{\text{Id}^t} = (\ker(\text{Id}))^0 = (\{0\})^0 = W^*$  ■



# 1 Polynomalgebren

## 1.6 Skript 6

### 1.6.1 Algebren

**Erinnerung:** Sei  $K$  ein Körper Eine  $K$ -Algebra  $\mathcal{A}$  ist ein  $K$ -Vektorraum, versehen mit Verknüpfung “Multiplikation von Vektoren”

$$\mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}, (\alpha, \beta) \mapsto \alpha\beta$$

$\forall \alpha, \beta, \gamma \in \mathcal{A}$  und  $c \in K$

$$(a) \quad \alpha(\beta\gamma) = (\alpha\beta)\gamma$$

$$(b) \quad \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \text{ und } (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$$

$$(c) \quad c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$$

Wenn es ein  $1 \in \mathcal{A}$  so dass  $1 \cdot \alpha = \alpha \cdot 1 = \alpha \quad \forall \alpha \in \mathcal{A}$  gilt, dann heißt  $\mathcal{A}$  eine Algebra mit Einheit.  
Wenn  $\alpha\beta = \beta\alpha \quad \alpha, \beta \in \mathcal{A}$ , dann ist  $\mathcal{A}$  eine kommutative Algebra

#### Example 1.6.1

$\mathcal{A} := M_{n \times n}(K)$  mit Matrixprodukt, nicht kommutativ, Einheit  $I_n$

#### Example 1.6.2

$\mathcal{A} := L(V, V)$  versehen mit  $T_1, T_2 \implies T_1 \cdot T_2 = T_1 \circ T_2$  nicht kommutative Einheit Id

#### Example 1.6.3 Potenzreihen Algebra

Sei  $K^{\mathbb{N}_0} := \{f, f : \mathbb{N}_0 \rightarrow K, f \text{ Abbildung}\}$  Für ein  $f \in K^{\mathbb{N}_0}$  werden wir auch als Folge in  $K$  schreiben,  $f = (f_n)_{n \in \mathbb{N}} = (f_0, f_1, \dots, f_n, \dots)$  wobei  $f_n := f(n)$

- Summe:  $\forall n \in \mathbb{N}_0 : (f + g)_n := f_n + g_n$
- Skalarmultiplikation:  $\forall C \in K, f \in K^{\mathbb{N}_0} (cf)_n := c(f_n)$

Damit ist  $V := (K^{\mathbb{N}_0}, +, \cdot_c)$  ist ein  $K$ -Vektorraum,  $\dim V = \infty$ .

Wir definieren nun eine weitere Verknüpfung

Produkt:  $\forall f, g \in K^{\mathbb{N}_0}$  definiere

$$(fg)_n := \sum_{i=0}^n f_i g_{n-i} \quad \forall n \in \mathbb{N}_0$$

#### Proposition 1.6.4

Setze  $\mathcal{A} := (K^{\mathbb{N}_0}, +, \cdot_c, \cdot)$  ist eine kommutative Algebra mit Einheit.

**Proof Proposition 1.6.4**

Wir prüfen hier Kommutativität, die Einheit (andere Axiome werden im ÜB vorkommen)

- Seien  $f, g \in \mathcal{A}$  zu zeigen  $fg = gf$
- Sei  $n \in \mathbb{N}_0$  berechne:

$$\begin{aligned}(gf)_n &= \sum_{i=0}^n g_i f_{n-i} \\ &= \sum_{i=0}^n g_{n-i} f_i \\ &= \sum_{i=0}^n f_i g_{n-i} \\ &= (fg)_n\end{aligned}$$

- Einheit: Zu prüfen:  $x^0 = 1 := (1, 0, 0, \dots, 0, \dots)$  ÜA  
– Ca.: Zu zeigen  $(1 \cdot g)_n = g_n$  für alle  $n \in \mathbb{N}_0$ : ■

$$\begin{aligned}(1 \cdot g)_n &= \sum_{i=0}^n 1_i g_{n-i} \\ &= 1 \cdot g_n \\ &= g_n\end{aligned}$$

Bemerke die Folgen der Gestalt:  $(1, 0, \dots, 0, \dots) = 1, (0, 1, 0, \dots, 0, \dots), (0, 0, 1, 0, \dots, 0, \dots), \dots$  unendlich viele linear unabhängige Elemente aus  $\mathcal{A}$ , deshalb ist  $\dim \mathcal{A} = \infty$ .

**Bezeichnung:**  $x = x^1 := (0, 1, 0, \dots, 0, \dots)$

**Notation:**  $n \in \mathbb{N}, x \in \mathcal{A}, x^n := \underbrace{x \cdot x \cdot \dots \cdot x}_{\mathbb{N} \ni n\text{-mal}}$

**Proposition 1.6.5**

Es ist für alle  $k \in \mathbb{N}$

$$(1) \ x^k = (0, \dots, 0, \underbrace{1}_{k\text{-te Stelle}}, 0, \dots, 0, \dots)$$

$$(2) \ X := \{x^k, k \in \mathbb{N}_0\} \text{ ist linear unabhängig}$$

- ÜB: ist  $X$  erzeugend? ist  $\text{span}(X) = \mathcal{A}$ ?
- Was ist  $\text{span } X$ ?

**Definition 1.6.6 und Bezeichnung**

$\mathcal{A} = (K^{\mathbb{N}_0}, +, \cdot_c, \cdot)$  heißt die Algebra der Potenzreihen über  $K$ .

Warum Potenzreihen:  $f \in \mathcal{A}$  schreibe

$$f = \sum_{n=0}^{\infty} f_n x^n$$

**Bezeichnung:**  $K[[x]]$

### 1.6.2 Polynomalgebra

**Definition und Notation**  $\text{span}(X) := K[x]$ , ist die Algebra der Polynome über  $K$

- $f \in K[x]$  ist ein Polynom über  $K$
- $f \in K[[x]]$ ,  $f \neq 0$ . Es gilt  $f \in K[x]$  genau dann wenn es genau ein  $n \in \mathbb{N}_0$  gibt wofür  $f_n \neq 0$ , aber  $f_k = 0$  für  $k > n$ . Wir setzen  $\deg f := n$  Grad von  $f$ . d.h. wenn  $f \neq 0$   $\deg f = n$  ist  $f = f_0x^0 + f_1x^1 + f_2x^2 + \dots + f_nx^n$ ,  $f \neq 0$
- Sei  $f \in K[[x]]$ , definiere

$$\text{support } f := \{n \in \mathbb{N}_0 : f_n \neq 0\}$$

$$(i) \text{ support } f = \emptyset \iff f = 0$$

$$(ii) \text{ support } f \text{ ist endlich} \iff f \in K[x]$$

$$(iii) \text{ Sei } f \neq 0, f \in K[x], \text{ dann ist}$$

$$\max \text{support } f = \deg f.$$

## 1.7 Skript 7

### Theorem 1.7.1

Seien  $f, g \in K[x]$ ,  $f, g \neq 0$  Es gilt:

- (i)  $fg \neq 0$
- (ii)  $\deg(fg) = \deg f + \deg g$
- (iii)  $fg$  ist normiert wenn  $f$  und  $g$  normiert sind
- (iv)  $fg$  ist Skalarpolynom  $\iff f, g$  sind Skalarpolynom
- (v) Falls  $fg \neq 0$ , gilt  $\deg(f + g) \leq \max(\deg f, \deg g)$

### Corollary 1.7.2

$K[x]$  ist eine kommutative Algebra mit Einheit.

### Corollary 1.7.3

$K[x]$  ist ein Integer Ring. Es gilt  $\forall f, g, h \in K[x]$ . Aus  $fg = fh$  folgt  $g = h$

**Beweis:**  $fg - fh = 0 \implies f(g - h) = 0 \implies (g - h) = 0 \implies g = h$  ■

### Definition 1.7.4

Sei  $f : K \rightarrow K, y \mapsto f(y)$  eine Abbildung.  $f$  ist polynomiale Funktion, falls wir zu  $f$  endlich viele Skalare aus  $K$  finden können, so dass  $f(y) = c_0 + c_1y + \dots + c_ny^n \quad \forall y \in K$ .

Satz über Existenz von Basis eines Vektorraumes gilt für alle Vektorräume, auch unendlich-dimensional, dafür benötigt man aber das Auswahlaxiom, bzw. den Satz von Zorn (Zorn's Lemma).

### Definition 1.7.5 und Notation

Sei  $\mathcal{A}$  eine  $K$ -Algebra mit Einheit. Sei  $f \in K[x]$ , und  $\alpha \in \mathcal{A}$ . Definiere

$$f(\alpha) := \sum_{i=0}^n \underbrace{f_i \alpha^i}_{\in \mathcal{A}}$$

wobei  $f = \sum_{i=0}^n f_i x^i$  und  $\alpha^0 := 1$

### Theorem 1.7.6

Seien  $\mathcal{A}$  eine  $K$ -Algebra,  $f, g \in K[x]$  und  $\alpha \in \mathcal{A}$  und  $c \in K$ . Es gelten:

$$(i) \quad (cf + g)(\alpha) \stackrel{1.7.5}{=} cf(\alpha) + g(\alpha)$$

$$(ii) \quad (fg)(\alpha) \stackrel{1.7.5}{=} f(\alpha)g(\alpha). \text{ Beweis } \ddot{U}A$$

### Example 1.7.7

Sei  $\mathcal{A} = K$  ist eine  $K$ -Algebra mit Einheit. Sei  $f \in K[x]$ , dann definiert 1.7.5 eine Polynomfunktion  $\tilde{f} : K \rightarrow K, a \mapsto f(a)$

$$f = \sum_{i=0}^n f_i x^i \quad \tilde{f} \text{ ist bestimmt durch } f_0, \dots, f_n \in K.$$

### Example 1.7.8

Sei  $\mathcal{A} = M_{2 \times 2}(K)$ . Sei  $B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \in \mathcal{A}, f \in K[x], f = 2x^0 + x^2$

$$f(B) = 2B^0 + B^2 = 2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix}$$

Wir wollen die Eigenschaften von Polynomfunktionen zusammenfassen.

### Theorem 1.7.10

Sei  $V$  der  $K$ -Vektorraum Polynomfunktionen. Wir versehen  $V$  mit punktweise Multiplikation:  $h_1, h_2 \in V$  und  $t \in K$

$$(h_1 h_2)(t) = h_1(t) h_2(t)$$

Dann ist damit die  $K$ -Algebra der Polynomfunktionen erklärt. Diese ist eine kommutative Algebra mit Einheit (die Einheit ist die Polynomfunktion  $K \rightarrow K, a \mapsto 1$ )

**Example 1.7.11**

$K = \mathbb{F}_p$  für eine Primzahl  $p$ . Betrachte  $f = (x^p - x) \in K[x] = \mathbb{F}_p[x]$   $f \neq 0$ . Aber  $\tilde{f} : \mathbb{F}_p \rightarrow \mathbb{F}_p$  die zugehörige Polynomfunktion ist die Nullabbildung.

z.B.  $p = 3$ ,  $f = x^3 - x = x^3 + 2x \in \mathbb{F}_3$   $f \neq 0$ .

Berechnen  $\tilde{f} : \mathbb{F}_3 \rightarrow \mathbb{F}_3$

$$\tilde{f}(0) = 0 = \tilde{f}(1) = 0 = \tilde{f}(2) = 0$$

**1.8 Skript 8****Definition 1.8.0 Bezeichnung**

Sei  $K[x]^\sim := \{h | h : K \rightarrow K \text{ ist eine Polynomfunktion}\}$  Also ist  $(K[x]^\sim, +, \cdot_c, \cdot)$  ist eine kommutative  $K$ -Algebra mit Einheit.

**Definition 1.8.1 Homomorphismus und Isomorphismus**

Seien  $\mathcal{A}$  und  $\mathcal{A}'$   $K$ -Algebren.

- (i) Eine lineare Abbildung

$$\Phi : \mathcal{A} \rightarrow \mathcal{A}'$$

Ist eine  $K$ -Algebren **Homomorphismus**, wenn darüber hinaus gilt  $\forall a, b \in \mathcal{A}$ :

$$\Phi(ab) = \Phi(a)\Phi(b)$$

- (ii)  $\Phi$  heißt  $K$ -Algebren **Isomorphismus**, wenn  $\ker \Phi = \{0\}$

**Theorem 1.8.2**

- (i) Die Abbildung

$$\Phi : K[x] \rightarrow K[x]^\sim, f \mapsto \tilde{f}$$

ist ein surjektiver  $K$ -Algebren Homomorphismus

- (ii) Wenn  $K$  unendlich ist, ist  $\Phi$  ein  $K$ -Algebren Isomorphismus (d.h.  $K$  unendlich  $\implies \ker \Phi = \{0\}$ )

**Proof Satz 1.8.2**

$\Phi$  lineare Abbildung

- (i)  $cf + g = c\tilde{f} + \tilde{g} \quad \forall f, g \in K[x], c \in K$ . Es gilt außerdem, dass:  $\tilde{f}g = \tilde{f}\tilde{g}$ . Also ist  $\Phi$  ein  $K$ -Algebren Homomorphismus. Sei  $h \in K[x]^\sim$ , dann ist  $h$  eine Polynomfunktion, d.h.  $\exists n \in \mathbb{N}_0 : \exists c_0, \dots, c_n \in K$  so dass  $h(a) = c_0a^0 + \dots + c_na^n \quad \forall a \in K$ .

Setze  $f(x) = \sum_{i=0}^n c_i x^i \in K[x]$  Wir berechnen  $\Phi(f) = \tilde{f} \stackrel{!}{=} h$  ist  $\Phi$  surjektiv!

- (ii) Zum Beweis brauchen wir Lagrange Interpolationssatz

**Erinnerung LA I:**

Sei  $n \in \mathbb{N}$  und  $V := K[x]_{\leq n}$  der  $K$ -Vektorraum der Polynome  $f$  von  $\deg f \leq n$  oder  $f = 0$ . Wir haben  $\dim V = n + 1$ , weil z.B.  $\{x^0, \dots, x^n\}$  eine Basis bildet.

**Theorem Lagrange Interpolationssatz**

Sei  $n \in \mathbb{N}$ ,  $t_0, \dots, t_n$   $n + 1$  *verschiedene* Elemente aus  $K$ . Für jedes  $0 \leq i \leq n$ ,  $L_i \in V^*$  definiere durch  $\forall f \in V$ :

$$L_i(f) := f(t_i)$$

Dann ist  $\mathcal{L} := (L_0, L_1, \dots, L_n)$  eine Basis für  $V^*$

**Proof Lagrange Interpolationssatz**

Es genügt dafür eine Dualbasis zu  $\mathcal{L}$  zu finden, d.h. eine geordnete Basis

$$\mathcal{B} = (P_0, \dots, P_n) \text{ von } V,$$

s.d.  $L_j(P_i) = \delta_{ij} \quad \forall i, j = 0, \dots, n$

Definiere Insbesondere (Satz 22.9 LA I)  $f = \sum_{i=0}^n f(t_i)P_i$

$$P_i := \prod_{j \neq i} \left( \frac{x - t_j}{t_i - t_j} \right)$$

Prüfe dass  $L_j(P_i) = \delta_{ij} \quad \forall i, j = 0, \dots, n$  erfüllt ist

$$L_j(P_i) = \delta_{ij} \quad \blacksquare$$

Seien  $(P_0, \dots, P_n)$  LIF und  $f = \sum_{i=0}^n f(t_i)P_i$ , wenn  $\tilde{f} = 0$  dann ist  $f(t_i) = 0 \quad \forall i = 0, \dots, n$ . Aus  $f = \sum_{i=0}^n f(t_i)P_i$  folgt  $f = 0$  ■

**1.8.1 Divisionsalgorithmus****Lemma 1.8.3**

Seien  $f, d \neq 0$ ,  $f, d \in K[x]$  mit  $\deg d \leq \deg f$ . Es gibt  $g \in K[x]$ , so dass entweder ist  $f - dg = 0$  oder  $\deg(f - dg) < \deg f$ .

**Proof Lemma 1.8.3**

Schreibe  $\deg f := m \geq \deg d := n$ .

Schreibe  $f = a_m x^m + \sum_{i=0}^{m-1} a_i x^i$ ,  $d = b_n x^n + \sum_{i=0}^{n-1} b_i x^i$ , für  $a_m \in K^x, a_i \in K, b_n \in K^x, b_i \in K$

Betrachte  $\frac{a_m}{b_n} x^{m-n} d = \frac{a_m}{b_n} x^{m-n} \left( b_n x^n + \sum_{i=0}^{n-1} b_i x^i \right) = a_m x^m + \dots$

Also entweder  $\left( f - \frac{a_m}{b_n} x^{m-n} d \right) = 0$  oder  $\deg \left( f - \frac{a_m}{b_n} x^{m-n} d \right) < \deg f$ .

Also setze  $g := \frac{a_m}{b_n} x^{m-n}$  ■

**Theorem 1.8.4 Divisionsalgorithmus in  $K[x]$** 

Seien  $f, d \in K[x]$ ,  $f, d \neq 0$ , so dass  $\deg d \leq \deg f$ . Dann gibt es  $q, r \in K[x]$ , so dass

(i)  $f = dq + r$ , wobei

(ii)  $r = 0$ , oder  $\deg r < \deg d$

Ferner sind  $q, r$  eindeutig durch (i) und (ii) bestimmt.

#### Proof Satz 1.8.4

$f \neq 0$  und  $\deg d \leq \deg f$ . Lemma 1.8.3 ergibt, dass es  $g \in K[x]$  gibt, so dass  $f - dg = 0$ , oder  $\deg(f - dg) < \deg f$

Wenn  $f - dg \neq 0$  und  $\deg(f - dg) \geq \deg d$ , dann ergibt Lemma 1.8.3  $h \in K[x]$ , so dass  $(f - dg) - dh = 0$ , oder  $\deg(f - d(g + h)) < \deg(f - dg)$

Der deg Abstieg ist aber endlich, das heißt, nach er endlich vielen Schritten anhalten muss. die Prozedur ergibt  $q \in K[x]$  und ein  $r = 0$ , oder  $\deg r < d$ , und  $f = dq + r$

**Eindeutigkeit:** Sei  $f = dq_1 + r_1 = dq + r$  (wobei  $r$  und  $r_1$  (ii) erfüllen)

Es folgt daraus:  $d(q - q_1) = r_1 - r$ . Zum Widerspruch nehmen wir an, dass  $q - q_1 \neq 0$ , dann haben wir  $\deg(r_1 - r) = \deg(d(q - q_1)) = \deg d + \deg(q - q_1) \geq \deg d$ . Jedoch ist  $\deg(r_1 - r) \leq \max(\deg r_1, \deg r) < \deg d$

Also ist  $q - q_1 = 0$ , daraus folgt  $(r_1 - r) = 0$ , also  $q_1 = q$  und  $r_1 = r$  ■

#### Definition 1.8.5

Seien  $f, d \neq 0$ ,  $f, d \in K[x]$

- (i) Wir sagen  **$d$  teilt  $f$  in  $K[x]$** , oder  **$f$  ist durch  $d$  teilbar in  $K[x]$** , oder  **$f$  ist ein Vielfaches von  $d$  in  $K[x]$** , wenn  $r = 0$  in Divisionsalgorithmus (DA), d.h.

$$f = dq + 0$$

- (ii) In diesem Fall ist  $q$  der Quotient

## 1.9 Skript 9

#### Corollary 1.9.1

Seien  $f \in K[x]$ , und  $c \in K$ . Es gilt:  $(x - c)$  teilt  $f$  in  $K[x]$  genau dann, wenn  $f(c) = 0$ .

#### Proof Korollar 1.9.1

Divisionsalgorithmus  $\implies \exists! q, r \in K[x]$ , so dass  $f = (x - c)q + r$ , wobei  $r = 0$  oder  $\deg r < 1$ , i.e.  $\deg r = 0$ . Also ist  $r$  ein Skalarpolynom und  $f(c) = r$ . Insbesondere ist  $r = 0 \iff f(c) = 0$  ■

#### Definition 1.9.2

Sei  $f \in K[x]$ ,  $c \in K$ , dann ist  $c$  eine **Nullstelle von  $f$  in  $K$** , wenn  $f(c) = 0$  Abkürzung: " $c$  ist NS von  $f$  in  $K$ "

#### Corollary 1.9.3

Sei  $f \in K[x]$ ,  $\deg f =: n$ , dann hat  $f$  höchstens  $n$  Nullstellen in  $K$

**Proof Korollar 1.9.3**

Wir beweisen per Induktion nach  $n \in \mathbb{N}_0$ .

**I.A.:**  $n = 0$ :  $f = c \neq 0$ , gar keine NS,

wenn  $n = 1$ : dann ist  $f = ax + c$  für  $a \neq 0, ac \in K$  Klar gilt:  $ax + c = 0 \iff x = -\frac{c}{a}$ . Also ist  $-\frac{c}{a}$  die einzige NS.

**I. Annahme:** Die Aussage gilt für  $\forall h \in K[x] : \deg h \leq n - 1$

**I.S.:**  $\deg f = n$ , sei  $a$  eine NS von  $f$  in  $K$ . Dann  $\exists q \in K[x]$ , so dass  $f = (x - a)q$ . Also  $\deg f = \deg(x - a) + \deg q \implies \deg q = \deg f - \deg(x - a) = n - 1$ . Sei  $b \in K$ , dann ist  $f(b) = 0 \iff (b - a) = 0$  oder  $q(b) = 0$ . I. Annahme  $\implies q$  hat höchstens  $n - 1$  NS in  $K$ . Daraus folgt:  $f$  hat höchstens  $1 + n - 1 = n$  NS in  $K$

**1.9.1 Formale Ableitung**

Notation (Erinnerung): Sei  $f = c_0 + c_1x + c_2x^2 + \dots + c_nx^n$   $c_i \in K$

**Setze:**  $f^{(0)} = f = D^0 f$  (Konvention), dann  $f^{(1)} := f' = c_1 + 2c_2x + 3c_3x^2 + \dots + nc_nx^{n-1} = D^1 f$   
 $f^{(2)} := f'' = D^2 f := D^1(D^1(f))$

**Note 1.9.4**

Für  $f, g \in K[x]$  und  $c \in K$  gilt  $D^1(f + cg) = D^1(f) + cD^1(g)$ , d.h.  $D^1 : K[x] \rightarrow K[x]$  ist ein linearer Operator. In der Tat gilt  $\forall k \in \mathbb{N} : D^k := \underbrace{D \circ \dots \circ D}_{k\text{-mal}}$  ist  $D^k$  ein linearer Operator (s. ÜB 10, LA I)

**Theorem 1.9.5 Taylor's Formel**

Seien  $\text{Char}(K) = 0$ .  $n \in \mathbb{N}_0, a \in K, p \in K[x]$  und  $\deg p \leq n$ .

**Es gilt:**

$$p = \sum_{i=0}^n p^{(i)}(a) \frac{(x-a)^i}{i!} \quad (2)$$

Darüber hinaus sind die Koeffizienten  $\frac{p^{(i)}(a)}{i!}$  eindeutig

**Proof Satz 1.9.5**

Sei  $V = K[x] \leq n$ . Für  $i = 0, \dots, n$  definiere

$$l_i : V \rightarrow K, l_i \in V^*$$

durch

$$l_i(p) := p^{(i)}(a) (\in K)$$

setzte  $p_i := \frac{1}{i!}(x-a)^i \in V$

**Beh.**

Es gilt  $\forall i, j = 0, \dots, n$ .

$$l_j(p_i) = S_{ij} \quad (\text{ÜB 5})$$



Also sind

$$(l_0, \dots, l_n) \text{ und}$$

$$(p_0, \dots, p_n)$$

Dualbasen von  $V, V^*$ .

Es folgt nun aus Satz 22.8 LA I, dass

$$\forall p \in V : p = \sum_{i=0}^n l_i(p) p_i$$

■

### Note 1.9.6

(1)  $1, (x-a), \dots, (x-a)^n$  sind linear unabhängig, deshalb sind die Koeffizienten in (2) eindeutig

(2)  $\text{Char}(K) = 0$  wird vorausgesetzt, damit  $i! \neq 0 \quad \forall i = 0, \dots, n$ .

Wir wollen nun Taylor's Formel ausnutzen um die Nullstellen von Polynomen weiter zu untersuchen!

### Definition 1.9.7

Seien  $f \in K[x], f \neq 0, c \in K$  eine Nullstelle von  $f$ .

Die **Vielfachheit von  $c$**  ist die größte  $\mu \in \mathbb{N}$  wofür gilt:  $(x-c)^\mu$  teilt  $f$ .

**Bemerkung:**  $1 \leq \mu \leq \deg f$  (u.a. Korollar 1.9.3), weil:  $f = (x-c)^\mu g$  für geeignetes  $g \in K[x]$ .  
 $\deg f = \mu + \deg g$ .

### Theorem 1.9.8 Ableitungstest zur Berechnung der Vielfachheit einer Nullstelle

Seien  $\text{Char}(K) = 0, f \neq 0, \deg f \leq n$ , und  $c \in K$  eine Nullstelle von  $f$ .

**Es gilt:**  $c$  hat die Vielfachheit  $\mu$  genau dann wenn

$$\begin{cases} f^{(k)}(c) = 0 & \text{für } 0 \leq k \leq \mu - 1 \text{ und} \\ f^{(\mu)}(c) \neq 0 \end{cases}$$

### Proof Satz 1.9.8

“ $\implies$ ”  $(x-c)^\mu$  teilt  $f$ , aber  $(x-c)^{\mu+1}$  teilt  $f$  nicht.

Es gibt also  $g \neq 0$ , so dass  $f = (x-c)^\mu g$ . Bemerkung  $\deg g \leq n - \mu$  und  $g(c) \neq 0$ . Die Taylorformel liefert für  $g$

$$f = (x-c)^\mu \left( \sum_{m=0}^{n-\mu} g^{(m)}(c) \frac{(x-c)^m}{m!} \right)$$

Also:

$$f = \sum_{m=0}^{n-\mu} g^{(m)}(c) \frac{(x-c)^{\mu+m}}{m!}$$

Da die Koeffizienten von  $f$  als l. K. von  $(x-c)^k$  ( $0 \leq k \leq n$ ) eindeutig sind, ergibt der

Vergleich:

$$f = \sum_{k=0}^n f^{(k)}(c) \frac{(x-c)^k}{k!}$$

$$\sum_{m=0}^{n-\mu} g^{(m)}(c) \frac{(x-c)^{\mu+m}}{m!} = \sum_{k=0}^n f^{(k)}(c) \frac{(x-c)^k}{k!}$$

$$g^{(0)}(c) \frac{(x-c)^\mu}{0!} + \dots + g^{(n-\mu)}(c) \frac{(x-c)^n}{(n-\mu)!} = \underbrace{\frac{f^{(0)}(c)}{0!} + \dots + \frac{f^{(\mu-1)}(c)}{(\mu-1)!}}_{=0} + \dots$$

Also

$$\frac{f^{(k)}(c)}{k!} = 0$$

für  $0 \leq k \leq \mu - 1$  und

$$\frac{f^{(k)}(c)}{k!} = \frac{g^{(k-\mu)}(c)}{(k-\mu)!}$$

für  $\mu \leq k \leq n$  Insbesondere für  $k = \mu$  erhalten wir  $f^{(\mu)}(c) = g(c) \neq 0$

“ $\Leftarrow$ ” Wir haben

$$f = \sum_{k=\mu}^n f^{(k)}(c) \frac{(x-c)^k}{k!}$$

Also

$$f = (x-c)^\mu \underbrace{\left[ \frac{f^{(\mu)}(c)}{\mu!} + \frac{f^{(\mu+1)}(c)}{(\mu+1)!}(x-c) + \dots + \frac{f^{(n)}(c)}{n!}(x-c)^{n-\mu} \right]}_{:=g}$$

Also  $g(c) = \frac{f^{(\mu)}(c)}{\mu!} \neq 0$

Also gilt

$$f = (x-c)^\mu g$$

mit  $g(c) \neq 0$ , also  $(x-c)^\mu$  teilt  $f$ . Wir müssen noch zeigen  $(x-c)^{\mu+1}$  teilt  $f$  nicht!

Zum Widerspruch:

$\exists h \in K[x] : h \neq 0$  so dass  $f = (x-c)^{\mu+1}h$ , also

$$f = (x-c)^{\mu+1}h(x-c)^\mu(x-c)h = (x-c)^\mu g$$

$K[x]$  Integer  $\implies g = (x-c)h$ , also  $g(c) = 0 \perp$

■

## 1.10 Skript 10

**Definition 1.10.1**

Ein  $K$ -Unterraum  $M \subseteq K[x]$  ist ein **Ideal** wenn gilt:  $\forall f \in K[x]$  und  $g \in M$  ist  $fg \in M$ .

**Example 1.10.2**

Sei  $d \in K[x]$ , setze  $M := dK[x] = \{df : f \in K[x]\}$ . Es gilt  $dK[x]$  ist ein Ideal.

- $df \in M, dg \in M, c \in K \quad c(df) + dg = d(\underbrace{cf + g}_{\in K[x]})$
- $f \in K[x], dg \in M = f(dg) = d(\underbrace{fg}_{\in K[x]}) \in M$ .

**Definition 1.10.3**

$\langle d \rangle := dK[x]$  heißt Hauptideal mit Erzeuger  $d$

**Example 1.10.4**

$\langle 1 \rangle = K[x]$ , und  $\langle 0 \rangle = \{0\}$

**Example 1.10.5**

Seien  $d_1, \dots, d_l \in K[x]$ , setze

$$M := d_1K[x] + \dots + d_lK[x]$$

ist ein Ideal:

- $M$  ist ein Unterraum
- Sei  $p \in M, f \in K[x], p = d_1f_1 + \dots + d_lf_l \implies pf = d_1(\underbrace{f_1f}_{\in K[x]}) + \dots + d_l(\underbrace{f_lf}_{\in K[x]})$

**Definition 1.10.6**

Das Ideal  $d_1K[x] + \dots + d_lK[x] := \langle d_1, \dots, d_l \rangle$  ist ein **endlich erzeugtes Ideal** mit Erzeugern  $d_1, \dots, d_l$ .

**Definition 1.10.7**

Seien  $p_1, \dots, p_l \in K[x]$ . Ein Polynom  $d \in K[x]$  ist der **größte gemeinsame Teiler** von  $p_1, \dots, p_l$ , bezeichnet mit  $\text{ggT}(p_1, \dots, p_l)$  wenn gelten

- (1)  $\forall i : 1 \leq i \leq l : d|p_i$
- (2) wenn auch  $d_0 \in K[x]$  (1) erfüllt, dann  $d_0|d$

**Definition 1.10.8**

die Polynome  $p_1, \dots, p_l$  sind relativprim wenn  $\text{ggT}(p_1, \dots, p_l) = 1$

**Theorem 1.10.9**

Sei  $0 \neq M \subseteq K[x]$  ein Ideal. Dann  $\exists! d \in K[x]$  normiert, so dass  $M = \langle d \rangle$ . Das heißt  $K[x]$  ist ein Hauptidealring.

**Proof Satz 1.10.9**

**Existenz:** Wähle  $d \in M$  so, dass:  $d \neq 0$ ,  $\deg d$  ist minimal und  $\mathbb{C} d$  ist normiert.

**Beh.:**  $d$  erzeugt  $M$

**Begründung:** Sei  $f \in M$ , DA ergibt:  $f = dq + r$ , wobei  $q, r \in K[x]$  und entweder  $r = 0$  oder  $\deg r < \deg d$ . Aber

$$r = \underbrace{f}_{\in M} - \underbrace{dq}_{\in M} \in M$$

also muss  $r = 0$  (sonst wäre  $r \neq 0, r \in M, \deg r < \deg d$ ). Also ist  $f = dq$ . Also ist  $f \in \langle d \rangle$ , also  $M = \langle d \rangle$ .

**Eindeutigkeit:** Sei  $g \in K[x], g \neq 0$   $g$  normiert so, dass  $M = gK[x]$ . Aber  $d, g \in M$ , also  $\exists 0 \neq p, q \in K[x]$  so, dass

$$d = gp \text{ und}$$

$$g = dq,$$

es folgt,  $d = eqp$ . Daraus folgt  $\deg d = \deg d + \deg q + \deg p$ . Also sind  $\deg p = \deg q = 0, pq$  sind Skalarppolynome. Da  $g, d$  beide normiert sind, folgt  $p = q = 1$ . Also gilt  $d = g$  ■

**Corollary 1.10.10**

Sei  $0 \neq M = \langle p_1, \dots, p_l \rangle$  endlich erzeugtes Ideal von  $K[x]$  ist

(1) Der normierte Erzeuger  $d$  von  $M$  ist

$$d = \text{ggT} \langle p_1, \dots, p_l \rangle$$

(2) Insbesondere wenn  $p_1, \dots, p_l$  relativprim sind, dann ist  $\langle p_1, \dots, p_l \rangle = K[x]$

**Proof Korollar 1.10.10**

(1) Da  $\langle d \rangle = dK[x] = \langle p_1, \dots, p_l \rangle$  und  $p_i \in \langle d \rangle \quad \forall i = 1, \dots, l$  folgt  $d|p_i \quad \forall i = 1, \dots, l$ . Also  $d$  ist gT.

Sei  $d_0 \in K[x]$  so dass  $d_0|p_i \quad i = 1, \dots, l$ . Es folgt  $\exists g_i \in K[x], \forall i = 1, \dots, l$  so, dass

$$p_i = d_0 g_i$$

Nun ist  $d \in \langle p_1, \dots, p_l \rangle$ , also  $d = p_1 q_1 + \dots + p_l q_l$  für geeignete  $q_i \in K[x]$ . Also  $d = d_0 g_1 q_1 + \dots + d_0 g_l q_l = d_0 \underbrace{[g_1 q_1 + \dots + g_l q_l]}_{\in K[x]}$ . Also  $d_0|d$ . Also  $d = \text{ggT}(p_1, \dots, p_l)$  ■

(2) folgt unmittelbar aus (1)

## 1.10.5 Primzerlegung (Faktorisierung)

**Definition 1.10.11**

Sei  $f \in K[x]$  ist **reduzibel** über  $K$  (oder **reduzibel in**  $K[x]$ ) wenn es  $g, h \in K[x]$  gibt mit  $\deg g \geq 1$ ,  $\deg h \geq 1$  und  $f = gh$ . Sonst ist  $f$  **irreduzibel** über  $K$ . Wenn irreduzibel und  $\deg f \geq 1$ , nennen wir  $f$  **Primpolynom**

**Note**

$f$  reduzibel  $\implies \deg f \geq 2$

**Example 1.10.12**

$f = x^2 + 1$ ,  $f$  ist irreduzibel über  $\mathbb{R}$  (über  $\mathbb{Q}$ ) (weil  $f$  keine reelle Nullstellen hat), aber reduzibel über  $\mathbb{C}$ . Weil  $\sqrt{-1}, -\sqrt{-1} \in \mathbb{C}$  bzw.  $i, -i \in \mathbb{C}$  sind komplexe Nullstellen.

**Theorem 1.10.13**

Seien  $p, f, g \in K[x]$  und  $p$  ist Primpolynom. Aus  $p|fg \implies p|f \vee p|g$ .

**Proof Satz 1.10.13**

Setze  $d := \text{ggT}(f, p)$ .  $\mathbb{C}$  ist  $p$  normiert. Außerdem ist  $p$  irreduzibel. Es folgt die einzigen normierten Teiler von  $p$  sind 1 oder  $p$ . Insbesondere  $d = 1$  oder  $d = p$ . Aus Korollar 1.10.10 folgt außerdem, dass  $\exists p_0, f_0 \in K[x]$  so, dass  $d = p_0p + f_0f$ .

$d = p$ : dann  $d|f$ , da  $d = \text{ggT}(f, p)$

$d = 1$ : dann ist  $1 = p_0p + f_0f$ , also  $g = p(p_0g) + f_0(fg)$  Es gilt:  $p|p(p_0g)$  und  $p|fg$  (per Def.). Also  $p|g$ . ■

**Corollary 1.10.14**

Seien  $f_1, \dots, f_l \in K[x]$  sei  $p$  Primpolynom. Wenn  $p|f_1 \cdots f_l \implies \exists i \in \{1, \dots, l\}$  so, dass  $p|f_i$ .

**Proof Korollar 1.10.14**

Induktion nach  $l$ .  $l = 2$  folgt aus Satz 1.10.13. Induktionsannahme für  $l - 1$ . Induktionsschritt:  $p|(f_1 \cdots f_{l-1})f_l \implies p|(f_1 \cdots f_{l-1})$  oder  $p|f_l \implies \dots$  ■

**Theorem 1.10.15**

Sei  $f \in K[x]$ ,  $f$  normiert,  $\deg f \geq 1$ . Dann ist  $f$  ein Produkt von normierten Primpolynomen. Die Darstellung ist eindeutig (bis auf Umnummerierung).

**Proof Satz 1.10.15**

**Existenz:** Sei  $\deg f = n$ , Induktion nach  $n$

**I.A.:**  $\deg f = 1 \implies f$  irreduzibel. Es ist nichts weiter zu zeigen.

**I.S.:**  $n > 1$ , ist  $f$  irreduzibel, dann ist nichts weiter zu zeigen. Ist  $f$  reduzibel,  $f = gh$   $\deg g \geq 1, \deg h \geq 1$ , also  $\deg g < n$  und  $\deg h < n$ . Induktionsannahme gilt für  $g$  und

$$h$$

$$f = \underbrace{g}_{\text{Prod. v. Prim.}} \underbrace{h}_{\text{Prod. v. Prim.}}$$

**Eindeutigkeit:** Sei  $f = p_1 \cdots p_l = q_1 \cdots q_s$ ,  $p_i, q_i$  alle normierte Primpolynome. Außerdem  $p_l | q_1 \cdots q_s$ . Es folgt aus Kor. 1.10.14  $\exists j \in \{1, \dots, s\}$  so dass  $p_l | q_j$ . Aber  $p_l, q_j$  sind beide normierte Primpolynome, es folgt  $p_l = q_j$ . (E nach Umnummerierung  $p_l = q_s$  Betrachte

$$P := p_1 \cdots p_{l-1} = q_1 \cdots q_{s-1}$$

Aber  $\deg(P) < n$

I.A.  $\implies p_1, \dots, p_{l-1}$  sind eine Umnummerierung der  $q_1, \dots, q_{s-1}$  (insbesondere  $l = s$ ). ■

## 2 Multilinearformen und Determinanten

### 2.11 Skript 11

#### 2.11.6 Die symmetrischen Gruppen $S_n$

##### Definition 2.11.0 Notation

für  $n \in \mathbb{N}$ , setze  $\mathbb{N}_n := \{1, \dots, n\}$

##### Definition 2.11.1

Sei  $n \in \mathbb{N}$ . Eine **Permutation** auf  $\mathbb{N}_n$  ist eine Bijektion  $\alpha : \mathbb{N}_n \rightarrow \mathbb{N}_n$ . Wir setzen  $S_n := \{\alpha : \alpha \text{ ist eine Permutation auf } \mathbb{N}_n\}$ . Wir versehen  $S_n$  mit Verknüpfung:

$$\circ : S_n \times S_n \rightarrow S_n, (\alpha, \beta) \mapsto \alpha \circ \beta$$

(s. ÜB LAI (wohldefiniert))

**Bezeichnungen:**

(i)  $\alpha\beta = \alpha \circ \beta$

(ii)  $\alpha \in S_n$  schreibe

$$\alpha := \begin{pmatrix} 1 & \dots & n \\ \alpha(1) & \dots & \alpha(n) \end{pmatrix}$$

“Zwei Zeilen Darstellung” einer Permutation

(iii)  $(S_n, \circ)$  heißt die Symmetrische Gruppe auf  $n$  Elemente

Warum ist  $(S_n, \circ)$  eine Gruppe?

- Die Identitätsabbildung  $\varepsilon : \mathbb{N}_n \rightarrow \mathbb{N}_n$  definiert durch  $\varepsilon(i) = i$ .  $\varepsilon \in S_n$  ist das neutrale Element für  $(S_n, \circ)$ .
- $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ , also  $(\alpha\beta)\gamma = \alpha(\beta\gamma) \forall \alpha, \beta, \gamma \in S_n$ .
- Bijektive Abbildungen sind invertierbar, d.h.  $\forall \alpha \in S_n \exists \beta = \alpha^{-1}$  so, dass  $\alpha\beta = \beta\alpha = \varepsilon$ .

##### Example 2.11.2

Die Permutation  $\alpha \in S_n$  mit  $\alpha(1) = 3, \alpha(2) = 5, \alpha(3) = 4, \alpha(4) = 1, \alpha(5) = 2$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

##### Definition 2.11.3

(i) Sei  $\alpha \in S_5$ . Wenn es  $a_1, \dots, a_m \in \mathbb{N}_n$  (verschiedene Elemente) gibt so, dass

(i)  $\alpha(a_i) = a_{i+1} \forall 1 \leq i \leq m-1$

(ii)  $\alpha(a_m) = a_1$  und

(iii)  $\alpha(x) = x \ \forall x \notin \{a_1, \dots, a_m\}, x \in \mathbb{N}_n$

dann heißt  $\alpha$  ein  $m$ -Zyklus

**Notation:** In diesem Fall schreiben wir  $\alpha = (a_1 \ a_2 \ \dots \ a_m)$  Zyklus Notation “Ein-zeilige Bezeichnung”

(ii) Sonderbezeichnung:  $\varepsilon = (1)$

(iii) Ein 2- Zyklus heißt eine Transposition.

#### Example 2.11.4

(i)

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Zwei Zeilen Notation  $\alpha = (1 \ 4 \ 2)$

(ii)  $\alpha \in S_{10}$ ,  $\alpha = (1 \ 4 \ 2)$ . Für  $i = \{3, 5, 6, 7, 8, 9, 10\}$  gilt  $\alpha(i) = i$

#### Definition 2.11.5

(i) Sei  $i \in \mathbb{N}_n, \alpha \in S_n$  so, dass

$$\alpha(i) = i.$$

Dann heißt  $i$  ein **Fixpunkt** für  $\alpha$

(ii) Sei  $\alpha, \beta \in S_n$  sind disjunkt, wenn

$$\{x : x \in \mathbb{N}_n : \alpha(x) \neq x\} \cap \{x : x \in \mathbb{N}_n : \beta(x) \neq x\} = \emptyset$$

#### Example 2.11.6

$\sigma, \tau, \gamma \in S_4$

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1 \ 2)$$

eine Transposition

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3 \ 4)$$

eine Transposition

$$\gamma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2 \ 3)$$

eine Transposition.

$\sigma, \tau$  disjunkt

$\sigma, \gamma$  nicht disjunkt

$\tau, \gamma$  nicht disjunkt



**Lemma 2.11.7**

Seien  $\alpha_1, \dots, \alpha_k \in S_n$  paarweise disjunkt, und  $\tau \in S_n$ . Dann sind die Permutationen  $(\alpha_1 \cdots \alpha_k)$  und  $\tau$  disjunkt genau dann, wenn  $\forall i = 1, \dots, k$  ist  $\alpha_i$  und  $\tau$  disjunkt

**Theorem 2.11.8**

Jede Permutation  $\sigma \in S_n$  hat eine Darstellung als Produkt  $\sigma = \alpha_1 \cdots \alpha_m$ , wobei  $\alpha_1 \cdots \alpha_m \in S_n$  sind paarweise disjunkte Zyklen

**Proof**

Wir werden die Aussage per Induktion nach  $\Gamma(\sigma) := |\{a \in \mathbb{N}_n : \sigma(a) \neq a\}|$  ( $\Gamma(\sigma) \in \mathbb{N}_0$ )

**I.A.**  $\Gamma(\sigma) = 0$ , dann ist  $\sigma = (1)$ . passt

**I.V.** die Aussage gelte für alle Permutationen  $\beta \in S_n$  wofür  $\Gamma(\beta) < k$

**I.S.** Setze  $k := \Gamma(\sigma) > 0$ . Sei  $i_0 \in \mathbb{N}_n$  so, dass  $\sigma(i_0) \neq i_0$

**Erinnerung an Notation:** Für  $s \in \mathbb{N}$ ,  $\sigma \in S_n$ , schreibe  $\sigma^s = \underbrace{\sigma \cdots \sigma}_{s\text{-mal}} = \underbrace{\sigma \circ \cdots \circ \sigma}_{s\text{-mal}}$

Für  $s \in \mathbb{N}$  setze

$$i_s := \sigma^s(i_0)$$

Da  $\{i_s : s \in \mathbb{N}\} \subset \mathbb{N}_n$  ist die Menge endlich. Folglich gibt es  $p < q \in \mathbb{N}$  so, dass  $i_p = i_q$ , insbesondere gilt

$$\sigma^{q-p}(i_0) = i_0$$

(da  $\sigma^p(i_0) = \sigma^q(i_0) \implies \sigma^0(i_0) = \sigma^{q-p}(i_0)$ )

Also ist  $\{l \in \mathbb{N} : \sigma^l(i_0) = i_0\} \neq \emptyset$ . Sei  $\rho \geq 2$  das kleinste Element davon. Setze  $\boxed{r := \rho - 1}$ . Die Minimalität von  $\rho$  impliziert, dass  $|i_0, \dots, i_r| = \rho$  (weil  $i_j = i_l$  für  $0 \leq j < l \leq r$  dann wäre  $\sigma^{l-j}(i_0) = i_0$  also  $l - j < \rho$  - Widerspruch). Analog gilt:

$$\forall a \in \{i_0, \dots, i_r\} \text{ gilt } \sigma(a) \neq a. \quad (3)$$

Betrachte den Zyklus  $\tau := (i_0 \ \dots \ i_r)$ . d.h.

$$\tau(i_l) = \sigma(i_l) \text{ für } 0 \leq l \leq r. \quad (4)$$

Außerdem

$$\forall a \in \mathbb{N}_n \text{ gilt : } \tau(a) = a \iff a \notin \{i_0, \dots, i_r\}. \quad (5)$$

Aus (3) folgt

$$\forall a \in \mathbb{N}_n : \sigma(a) = a \implies a \notin \{i_0, \dots, i_r\} \quad (6)$$

Aus (4), (5), (6) folgt

$$\{a \in \mathbb{N}_n, \tau^{-1}\sigma(a) = a\} = \{a \in \mathbb{N}_n : \sigma(a) = a\} \cup \{i_0, \dots, i_r\} \quad (7)$$

Also  $\Gamma(\tau^{-1}\sigma) < \Gamma(\sigma)$ .

I.V. anwenden auf  $\tau^{-1}\sigma$ .

$$\tau^{-1}\sigma = \alpha_1 \cdots \alpha_m \implies \sigma = \tau \cdot \alpha_1 \cdots \alpha_m$$

$\forall i = 1, \dots, m$   $\alpha_i$  Zyklus ■

## 2.12 Skript 12

**Example 2.12.0**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1 \ 3 \ 4) (2 \ 5)$$

$$\sigma \in S_5$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (1 \ 3 \ 4)$$

**Theorem 2.12.1**

Jede Permutation  $\sigma \in S_n, n \geq 2$  ist Produkt von Transpositionen.

**Bemerke:**  $n = 1 \ S_1 = \{(1)\}$ .

**Proof Satz 2.12.1**

Das neutrale Element  $(1) = (1 \ 2) (2 \ 1)$ .

Sei nun  $\sigma \neq (1), \sigma \in S_n$  wegen Satz 2.11.8 genügt es zu zeigen dass ein Zyklus ein Produkt von Transpositionen, also  $\exists \sigma = (i_1 \ \dots \ i_r)$  mit  $r \geq 2$ .

Wenn  $r = 2$ , passt.

Jetzt  $r > 2$ .

$$\text{Beh.: } (i_1 \ i_2 \ \dots \ i_r) = (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots (i_1 \ i_3) (i_1 \ i_2).$$

**Bew.:** Wir berechnen

$$\underbrace{\left( (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots (i_1 \ i_3) \underbrace{(i_1 \ i_2)}_{=i_r} \right)}_{=i_r} (i_r) = (i_1 \ i_r) (i_r)$$

Für  $i_s$  mit  $1 \leq s < r$  gilt:

$$\begin{aligned} & (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots (i_1 \ i_s) (i_s) \\ &= (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots (i_1 \ i_{s+1}) \underbrace{(i_1 \ i_s) (i_s)}_{=i_1} \\ &= (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots \underbrace{(i_1 \ i_{s+1}) (i_1)}_{=i_{s+1}} \\ &= (i_1 \ i_r) (i_1 \ i_{r-1}) \cdots (i_1 \ i_{s+2}) i_{s+1} \\ &= i_{s+1} \end{aligned}$$

**Example 2.12.2**

$$(1 \ 2 \ 3) \in S_4$$

$$(1 \ 2 \ 3) = (1 \ 3) (1 \ 2)$$

aber auch gilt

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix}$$

$\implies$  Parität eindeutig.

Wir werden zeigen, dass die Parität der Darstellung eindeutig ist! Dafür brauchen wir

### Definition 2.12.3

Sei  $b \in S_n$  und  $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$  eine Abbildung. Wir definieren  $\sigma f : \mathbb{Z}^n \rightarrow \mathbb{Z}$  folgend:

$$(\sigma f)(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

### Example 2.12.4

$f : \mathbb{Z}^3 \rightarrow \mathbb{Z}$  definiert durch

$$f(x_1, x_2, x_3) := x_1 x_2 + x_3, \sigma \in S_3 \quad \sigma := \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}.$$

$$\sigma f : \mathbb{Z}^3 \rightarrow \mathbb{Z}, \sigma f(x_1, x_2, x_3) = f(x_2, x_3, x_1) = x_2 x_3 + x_1$$

### Lemma 2.12.5

Sei  $\sigma, \tau \in S_n, f, g : \mathbb{Z}^n \rightarrow \mathbb{Z}$  ( $f, g$  Abbildungen).

Es gelten:

$$(i) \quad \sigma(\tau f) = (\sigma\tau)f$$

$$(ii) \quad \sigma(fg) = (\sigma f)(\sigma g).$$

**Bew.:** ÜA.

### Theorem 2.12.6 Eindeutigkeit der Parität

Es gibt eine wohldefinierte Abbildung

$$\text{sign} : S_n \rightarrow \{1, -1\}$$

so, dass:

$$(a) \quad \text{Für jede Transposition } \tau \in S_n \text{ gilt } \text{sign}(\tau) = -1$$

$$(b) \quad \text{Für alle } \sigma, \tau \in S_n \text{ gilt}$$

$$\text{sign}(\sigma\tau) = \text{sign}(\sigma) \text{sign}(\tau)$$

Diese Abbildung ist eindeutig. Darüber hinaus gilt  $\forall \sigma \in S_n : \text{sign}(\sigma) = 1$  genau dann, wenn  $\sigma$  ist Produkt von  $m$  Transpositionen mit  $m$  gerade, und

$$\text{sign}(\sigma) = -1$$

genau dann, wenn  $\sigma$  ist Produkt von  $m$  Transpositionen mit  $m$  ungerade.

**Proof Satz 2.12.6**

Sei  $\Delta : \mathbb{Z}^n \rightarrow \mathbb{Z}$  die Abbildung

$$\Delta(x_1, \dots, x_n) := \prod_{1 \leq i < j \leq n} (x_j - x_i) \quad (8)$$

**Beh.:** Für eine Transposition  $\tau \in S_n$  gilt

$$\tau \Delta = -\Delta$$

**Bew.:** In der Tat, sei  $\tau = (rs)$   $r < s$ . Aus Lemma 2.12.5 (ii) folgt

$$\tau \Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} \tau(x_j - x_i) \quad (9)$$

- Offensichtlich, wenn  $i, j \notin \{r, s\}$  ist

$$\tau(x_j - x_i) = (x_{\tau(j)} - x_{\tau(i)}) = (x_j - x_i)$$

- Für den Faktor  $(x_s - x_r)$  gilt

$$\tau(x_s - x_r) = (x_r - x_s) = -(x_s - x_r)$$

- Die anderen Faktoren können wir paaren wie folgt:

$$\begin{aligned} (x_k - x_s)(x_k - x_r) & \text{ wenn } k > s \\ (x_s - x_k)(x_k - x_r) & \text{ wenn } r < k < s \\ (x_s - x_k)(x_r - x_k) & \text{ wenn } k < r \end{aligned}$$

Jedes Produkt ist von  $\tau$  unberührt. Alles zusammen ein Vergleich der Faktoren in (8) bzw. (9) ergibt

$$\tau \Delta = -\Delta \quad \blacksquare$$

Sei  $\sigma \in S_n$  wegen Satz 2.12.1 schreibe  $\sigma = \tau_1 \cdots \tau_m$  als Produkt von Transpositionen. Aus Lemma 2.12.5 (i) folgt

$$\sigma \Delta = (\tau_1 \cdots \tau_m) \Delta = \tau_1 (\tau_2 (\cdots (\tau_m \Delta)))$$

Ferner folgt aus der Behauptung, dass

$$\tau_1 (\tau_2 (\cdots (\tau_m \Delta))) = (-1)^m \Delta$$

Wir sehen also: entweder

$$\begin{aligned} \sigma \Delta &= \Delta \quad \text{genau dann, wenn } m \text{ gerade} \\ \sigma \Delta &= -\Delta \quad \text{genau dann, wenn } m \text{ ungerade} \end{aligned}$$

Für  $\sigma \in S_n$  setze

$$\text{sign}(\sigma) = 1$$

wenn  $\sigma \Delta = \Delta$ .

$\sigma \in S_n$  setze

$$\text{sign}(\sigma) = -1$$

wenn  $\sigma \Delta = -\Delta$  ■

**Definition 2.12.7**

Wir nennen  $\sigma$  genau dann gerade, wenn  $\text{sign}(\sigma) = 1$ , bzw, wir nennen  $\sigma$  genau dann ungerade, wenn  $\text{sign}(\sigma) = -1$

Betrachte folgende Untermenge von  $S_n$ .

$$A_n := \{\sigma : \sigma \text{ ist eine gerade Permutation}\}$$

**Corollary 2.12.9**

$A_n$  ist eine Untergruppe und

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

**Proof Korollar 2.12.9**

$(1) \in A_n$ .

- Seien  $\sigma, \tau \in A_n$  zu zeigen  $\sigma\tau \in A_n$ :

Wir berechnen:

$$\text{sign}(\sigma\tau) \stackrel{\text{Satz 2.12.6 b)}}{=} \text{sign}(\sigma) \text{sign}(\tau) = 1 \cdot 1 = 1$$

- Sei  $\sigma \in A_n$

$$\sigma = \tau_1 \cdots \tau_m$$

wobei  $m$  gerade ist.

Wir berechnen:

$$\sigma^{-1} = \tau_m^{-1} \cdots \tau_1^{-1}$$

Nun ist die Inverse von einer Transposition wieder eine Transposition (weil  $\tau = (i_1 \ i_2) \implies \tau^{-1} (i_2 \ i_1), i_1, i_2 \in \mathbb{N}_n$ )

2. Beweis

$$\sigma = \tau_1 \cdots \tau_m$$

$m$  gerade.

$$1 = \text{sign}(1) = \text{sign}(\sigma\sigma^{-1}) = \text{sign}(\sigma) \text{sign}(\sigma^{-1}) = \text{sign}(\sigma^{-1})$$

Wir wissen

$$S_n = A_n \uplus U \quad (X \uplus Y = X \cup Y, X \uplus Y \implies |X \cap Y| = 0)$$

wobei  $U = \{\sigma : \sigma \text{ ist ungerade}\}$

$$|S_n| = |A_n| + |U|$$

Wir zeigen  $|A_n| = |U|$ : Betrachte die Abbildung

$$A_n \rightarrow U, \sigma \mapsto \underbrace{\begin{pmatrix} 1 & 2 \end{pmatrix}}_{\text{sign}\begin{pmatrix} 1 & 2 \end{pmatrix} = -1} \sigma$$

Diese Abbildung ist bijektiv, also

$$|A_n| = |U|.$$

■

**Definition 2.12.10**

Wir nennen  $A_n$  die alternierende Gruppe.

**2.13 Skript 13****2.13.7 Multilinear Formen**

Sei  $K$  ein Körper und  $U$  und  $V$   $K$ -Vektorräume

$$\beta : U \times V \rightarrow K, (x, y) \mapsto \beta(x, y)$$

Die Abbildung  $\beta$  ist eine bilineare Funktionale (Form) falls gelten.

$$\forall x, x_1, x_2 \in U, \forall y, y_1, y_2 \in V, \forall c_1, c_2, d_1, d_2 \in K$$

$$(1) \quad \beta(c_1x_1 + c_2x_2, y) = c_1\beta(x_1, y) + c_2\beta(x_2, y)$$

$$(2) \quad \beta(x, d_1y_1 + d_2y_2) = d_1\beta(x, y_1) + d_2\beta(x, y_2)$$

**Example 2.13.2**

Betrachte

$$V \times V^* \rightarrow K, (x, f) \mapsto [x, f] := f(x)$$

ist bilinear

**Definition Notation**

$L^{(2)}(U \times V, K)$  = der  $K$ -Vektorraum der bilinearen Formen auf  $U \times V$  versehen mit den Verknüpfungen

$$\underbrace{(c_1\beta_1 + c_2\beta_2)}_{\in L^{(2)}} \underbrace{(x, y)}_{\in U \times V} := c_1\beta_1(x, y) + c_2\beta_2(x, y)$$

wie üblich ■

**Definition 2.13.3**

Seien  $m \in \mathbb{N}$ ,  $V_1, \dots, V_m$   $K$ -VR. Eine Abbildung

$$\mu : V_1 \times \dots \times V_m \rightarrow K$$

ist eine  **$m$ -lineare Funktionale** ( **$m$ -lineare Form** oder **multilineare Funktionale vom Grad  $m$** ) Wenn  $\forall i \in \{1, \dots, m\}$  gilt  $\forall \alpha_i, \gamma_i \in V_i, c \in K$

$$\mu(\alpha_1, \dots, c\alpha_i + \gamma_i, \dots, \alpha_m) = c\mu(\alpha_1, \dots, \alpha_i, \dots, \alpha_m) + \mu(\alpha_1, \dots, \gamma_i, \dots, \alpha_m)$$

**Definition Notation**

$L^{(m)}(V_1 \times \dots \times V_m, K)$  =  $K$ -VR der  $m$ -linearen Formen.

**Note 2.13.4**

Ansatz wie oben, wenn  $\mu$  multilinear ist, dann gilt

$$\mu(\alpha_1, \dots, \alpha_i, \dots, \alpha_m) = 0$$

falls  $\alpha_i = 0$

**2.13.8 Alternierende Multilineare Formen auf  $K^n$** **Definition 2.13.5**

Sei  $n \in \mathbb{N}$  und  $V = K^n$  Eine  $n$ -lineare Form auf

$$\delta : \underbrace{K^n \times \dots \times K^n}_{n\text{-mal}} \rightarrow K$$

ist **alternierend**, wenn:  $i, j \in \{1, \dots, n\}$  mit  $i \neq j$  existieren mit  $Z_i = Z_j$ , dann  $\delta(z_1, \dots, z_n) = 0$  (für  $z_1, \dots, z_n \in K^n$ )

**Definition Konvention**

:  $\delta$  wird auch als Abbildung auf  $K^{n \times n} = \text{Mat}_{n \times n}(K)$   $\delta(A) = \delta(z_1, \dots, z_n)$

$A \in M_{n \times n}(K)$  wobei

$$A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$$

**Lemma 2.13.6**

Sei  $\delta$  alternierend. Es gilt

$$(i) \ z_1, \dots, z_n \text{ sind linear abhängig} \implies \delta(z_1, \dots, z_n) = 0$$

$$(ii) \ \delta(z_1, \dots, z_i, \dots, z_j, \dots, z_n) = -\delta(z_1, \dots, z_j, \dots, z_i, \dots, z_n)$$

(iii) Allgemeiner gilt

$$\delta(z_{\pi(1)}, \dots, z_{\pi(n)}) = \text{sign}(\pi) \delta(z_1, \dots, z_n)$$

mit  $\pi \in S_n$

**Proof Lemma 2.13.6**

(i) ☞ nehmen wir an lineare Abhängigkeit

$$\implies z_n = \sum_{i=1}^{n-1} c_i z_i$$

für  $c_1, \dots, c_{n-1} \in K$ . Wir berechnen

$$\delta \left( z_1, \dots, z_{n-1}, \sum_{i=1}^{n-1} c_i z_i \right) = \sum_{i=1}^{n-1} c_i \delta(z_1, \dots, z_{n-1}, z_n) = 0$$

(ii) wir berechnen

$$\begin{aligned}
 0 &= \delta(z_1, \dots, z_i + z_j, \dots, z_j + z_i, \dots, z_n) \\
 &= \delta(z_1, \dots, z_i, \dots, z_j + z_i, \dots, z_n) + \delta(z_1, \dots, z_j, \dots, z_j + z_i, \dots, z_n) \\
 &= \delta(z_1, \dots, z_i, \dots, z_j, \dots, z_n) + \underbrace{\delta(z_1, \dots, z_i, \dots, z_i, \dots, z_n)}_{=0} \\
 &\quad + \underbrace{\delta(z_1, \dots, z_j, \dots, z_j, \dots, z_n)}_{=0} + \delta(z_1, \dots, z_j, \dots, z_i, \dots, z_n) \\
 &= \delta(z_1, \dots, z_i, \dots, z_j, \dots, z_n) + \delta(z_1, \dots, z_j, \dots, z_i, \dots, z_n)
 \end{aligned}$$

■

### Note 2.13.7

- (1)  $\text{Char}(K) \neq 2$  dann gilt: Sei  $\delta$  eine  $m$ -lineare Form auf  $K^n$  so, dass Lemma 2.13.6 (ii) gilt, dann ist  $\delta$  alternierend.
- (2)  $\text{Char}(K) = 2$   $\delta : \mathbb{F}_2 \rightarrow \mathbb{F}_2, \delta((a, b), (c, d)) := ac + bd$  ist ein Gegenbeispiel!

## 2.14 Skript 14

Sei  $\delta$  eine alternierende lineare Form auf  $K^n$  (laut Def 2.13.5 auch als  $\delta : M_{n \times n}(K) \rightarrow K$  auffassen).  
Sei  $A \in M_{n \times n}(K)$

$$A = \begin{pmatrix} z_1 \\ \dots \\ \vdots \\ \dots \\ z_n \end{pmatrix}$$

### Lemma 2.14.1

Sei  $e$  eine elementare Zeilenumformung Es gelten

- (i)  $\delta(e(A)) = -\delta(A)$ , wenn  $e$  von Typ 1 ist.
- (ii)  $\delta(e(A)) = c\delta(A)$ , wenn  $e$  von Typ 2 ist.
- (iii)  $\delta(e(A)) = \delta(A)$ , wenn  $e$  von Typ 3 ist.
- (iv) Allgemeiner gilt:  $\forall c \in K : \delta(cA) = c^n \delta(A)$

### Proof Lemma 2.14.1

Wir berechnen  $\delta(e(A))$ :

- (i)  $\delta(z_1 + cz_2, z_2, \dots, z_n) = \delta(z_1, z_2, \dots, z_n) + c\delta(z_2, z_2, z_3, z_4, \dots, z_n) = \delta(z_1, \dots, z_n)$
- (ii) Folgt aus Lemma 2.13.6
- (iii) Folgt aus  $n$ -Linearität
- (iv)  $\delta(cz_1, \dots, cz_n) = c\delta(z_1, cz_2, \dots, cz_n) = c^2\delta(z_1, z_2, cz_3, \dots, cz_n) = \dots = c^n\delta(z_1, \dots, z_n)$



**Lemma 2.14.2**

Für jede Matrix  $A \in M_{n \times n}(K)$  gibt es  $\Delta_A \in K^x$ ,  $\Delta_A$  hängt nur von  $A$  ab, so dass

$$\delta(A) = \Delta_A \delta(\text{r. z. s. F.}(A))$$

**Proof Lemma 2.14.2**

$\Delta_A$  ergibt sich durch wiederholte Anwendung von Lemma 2.14.1. Wir bekommen  $\Delta_A$  ist ein Produkt der Gestalt

$$(-1)^l c_1 \cdots c_k$$

für geeignete  $l, k \in \mathbb{N}_0$  und  $c_1, \dots, c_k \in K^x$  ■

**Note 2.14.3**

(Erinnerung: Skript 7 LA I Bemerkung 7.3)

Für  $A \in M_{n \times n}(K)$  Dann gilt: Entweder

**Fall 1:** r. Z. S. F.  $(A)$  hat eine Null Zeile, oder

**Fall 2:** r. Z. S. F.  $(A) = I_n$ .

Also erhalten wir auch hier eine Dichotomie:  
Entweder

**Fall 1:**  $\delta(A) = \Delta_A \cdot 0 = 0$ , oder

**Fall 2:**  $\delta(A) = \Delta_A \delta(I_n)$

**Corollary 2.14.4**

$\delta \neq 0$  genau dann, wenn  $\delta(I_n) \neq 0$

**Proof Korollar 2.14.4**

“ $\Leftarrow$ ”: klar

“ $\Rightarrow$ ”:  $\delta(I_n) = 0 \Rightarrow \delta(A) = 0$  in **Fall 1** und **Fall 2** in Bemerkung 2.14.3

**Corollary 2.14.5**

Wir nehmen an, dass  $\delta \neq 0$ . Sei  $A \in M_{n \times n}(K)$   
Es gilt:  $\delta(A) \neq 0$  genau dann, wenn  $A$  invertierbar ist.

**Proof Korollar 2.14.5**

Folgt aus Lemma 2.14.2 und Korollar 2.14.4: weil  $A$  invertierbar  $\Leftrightarrow$  r. Z. S. F.  $(A) = I_n$  (Skript 9 LA I, Satz 9.8) ■

**Definition 2.14.6 Definition und Notation**

$\mathbb{A} := \text{alt}^{(n)}(K^n) :=$  der Unterraum von  $L^{(n)}(K^n \times \cdots \times K^n, K)$  von  **$n$ -linear** alternierenden Formen auf  $K^n$

$$\mathbb{A} = \{\delta : \delta n\text{-linear alt. auf } K^n\} \subseteq L^{(n)}(K^n \times \cdots \times K^n, K)$$

**Corollary 2.14.8**

Seien  $\delta_1, \delta_2 \in \mathbb{A}$ . Es gilt:  $\delta_1 = \delta_2$  genau dann, wenn

$$\delta_1(I_n) = \delta_2(I_n)$$

(oder  $\delta_1(e_1, \dots, e_n) = \delta_2(e_1, \dots, e_n)$ )

**Proof Korollar 2.14.8**

Sei  $\delta_1(I_n) = \delta_2(I_n)$ , so dass

$$(\delta_1 - \delta_2)(I_n) = \delta_1(I_n) - \delta_2(I_n) = 0$$

Es folgt nun aus Kor. 2.14.4, dass

$$\delta_1 - \delta_2 = 0$$

also

$$\delta_1 = \delta_2$$

■

**Corollary 2.14.9**

$$\dim(\mathbb{A}) \leq 1$$

**Proof Korollar 2.14.9**

$\dim(\mathbb{A}) = 0$ , passt

Ansonsten  $\delta_1 \neq 0, \delta_1 \in \mathbb{A}$ , wir nehmen  $\delta_1$  fest.

Sei  $\delta_2 \in \mathbb{A}$ , Sei  $A \in M_{n \times n}(K)$  wie im Fall 2 von Bemerkung 2.14.3. Wir berechnen

$$\delta(A) = \triangle_A \delta_2(I_n) = \triangle_A \frac{\delta_2(I_n)}{\delta_1(I_n)} \delta_1(I_n) \quad (*)$$

Setze  $d := \frac{\delta_2(I_n)}{\delta_1(I_n)} \in K$

Es folgt:

$$\delta_2(A) = d(\triangle_A \delta_1(I_n)) = d\delta_1(A), d \in K$$

■

Wir werden nun zeigen, dass es  $\delta \in \mathbb{A}$  gibt mit  $\delta(I_n) = 1$  wegen Korollar 2.14.8 ist dann diese  $\delta$  notwendig eindeutig. Sobald wir  $\delta$  gefunden haben, wissen wir

$$\dim(\mathbb{A}) = 1$$

**Ziel:** zu zeigen  $\exists \delta \in \mathbb{A}$  so, dass  $\delta(I_n) = 1$ .

**Formelberechnung:**

Sei  $\boxed{\delta \in \mathbb{A}}$  und  $A \in M_{n \times n}(K)$  schreiben

$$A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$$

$$a_{ij} \in K \forall i, j$$

$$A = \begin{pmatrix} z_1 \\ \dots \\ \vdots \\ \dots \\ z_n \end{pmatrix}$$

wobei,  $\forall i : 1 \leq i \leq n$ ,  $z_i$  die  $i$ -te Zeile der Matrix  $A$ .

Sei  $e_1, \dots, e_n$  die Standard Basis von  $K^n$ . Wir schreiben  $\forall i : 1 \leq i \leq n$

$$z_i := \sum_{j_i=1}^n a_{ij_i} e_{j_i}$$

(die eindeutige Darstellung von  $z_i$  in der Standardbasis). Wir berechnen:

$$\delta(A) = \delta \left( \sum_{j_1=1}^n a_{1j_1} e_{j_1}, \dots, \sum_{j_n=1}^n a_{nj_n} e_{j_n} \right) = \sum_{j_1, \dots, j_n=1}^n a_{1j_1} \cdots a_{nj_n} \quad (**)$$

Prüfen!!

Für jeden Summand in  $(**)$  betrachte die Abbildung

$$\{1, \dots, n\} \rightarrow \{1, \dots, n\}, i \mapsto j_i$$

- Wenn solch eine Abbildung **nicht** injektiv ist, dann gibt es eine Wiederholung in  $(j_1, \dots, j_n)$  und entsprechend ist der Summand = 0 (weil  $\delta$  alternierend ist!)
- Die Abbildung (für einen gegebenen Summand in  $(**)$ ) ist injektiv, dann ist sie eine Permutation  $\pi \in S_n$  und damit im Summand in  $(**)$  erhalten wir:

$$\delta(e_{j_1}, \dots, e_{j_n}) = \delta(e_{\pi(1)}, \dots, e_{\pi(n)}) \stackrel{\text{Lem. 2.13.6}}{=} \text{sign}(\pi) \delta(e_1, \dots, e_n).$$

Also können wir nun  $(**)$  umschreiben:

$$\begin{aligned} (**) &= \sum_{\pi \in S_n} \text{sign}(\pi) a_{1\pi(1)} \cdots a_{n\pi(n)} \delta(I_n) \\ &= \delta(I_n) \sum_{\pi \in S_n} \text{sign}(\pi) a_{1\pi(1)} \cdots a_{n\pi(n)} \end{aligned}$$

Wir sehen also dass wenn wir  $\delta(I_n) = 1$  setzen, dann bekommen wir

$$\delta(A) = \text{sign}(\pi) \prod_{i=1}^n a_{i\pi(i)} \text{det}$$

Wir müssen nur noch prüfen, dass **det** eine  $n$ -lineare alternierende Form definiert!

### Definition Notation

$$A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$$

$$\delta : K^n \times \cdots \times K^n$$

$$\delta(z_1, \dots, z_n)$$

$$\delta(z_1 + dz'_1, z_2, \dots, z_n) \quad d \in K$$

$$A' = \begin{pmatrix} z'_1 \\ \vdots \\ z'_n \end{pmatrix}$$

**Theorem 2.14.10**

Die Formel (det) definiert eine  $n$ -lineare alternierende Form  $\delta$  mit  $\delta(I_n) = 1$ .

**Proof Satz 2.14.10**

☞  $n \geq 2$ .

- $n$ -linear?

$z_1 + dz'_1 = [a_{11} + da'_{11} \cdots a_{1n} + da'_{1n}]$ . Also müssen wir berechnen

$$\begin{aligned} & \text{sign}(\pi) \left( (a_{1\pi(1)} + da'_{1\pi(1)}) a_{2\pi(1)} \cdots a_{n\pi(n)} \right) \\ &= \text{sign}(\pi) \left( (a_{1\pi(1)} \cdots a_{n\pi(n)}) + d \left( a'_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)} \right) \right) \end{aligned}$$

usw. ÜB

- alternierend? Sei  $z_1 = z_2$ , zu zeigen  $\delta(A) = 0$   $z_1 = z_2$  i.e.  $a_{1j} = a_{2j} \quad \forall i \leq j \leq n$ , i.e.  $a_{i\pi(j)} = a_{2\pi(j)} \quad \forall \pi \in S_n$ . Wir berechnen  $\delta(A)$  (Wie in der Formel (det)) (mithilfe der Angabe  $S_n = A_n \cup A_n(1 \ 2)$ )  $(1 \ 2) \in S_n$

$$\begin{aligned} \delta(A) &= \underbrace{\sum_{\pi \in A_n} \text{sign}(\pi) (a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)})}_I \\ &\quad + \underbrace{\sum_{\pi \in A_n} \underbrace{\text{sign}(\pi(1 \ 2))}_{=-1} \left( a_{1\pi(1 \ 2)(1)} a_{2\pi(1 \ 2)(2)} \cdots a_{n\pi(1 \ 2)(n)} \right)}_{II} \\ &= I + II \\ &= 0 \end{aligned}$$

- zu zeigen  $\delta(I_n) = 1$ . Sei  $A$  diagonal, also  $i \neq j \implies a_{ij} = 0$ . Die  $\forall i, j = 1, \dots, n$  einzige  $\pi \in S_n$ , wofür der Summand in der (det) Formel  $\neq 0$ , ist  $\pi(i) = i \quad \forall i = 1, \dots, n$  also  $\pi = (1) \in S_n$  also  $\delta(A) = a_{11} \cdots a_{nn}$  Insbesondere  $\delta(I_n)$

**Definition Bezeichnung**

$\delta(A)$  die  $\delta$  (det) erfüllt werden wird  $\det(A)$  genannt

**Corollary 2.14.11**

$\dim(\mathbb{A}) = 1$ . Insbesondere gilt:  $\forall \delta \in \text{alt}^{(n)}(K^n)$  und  $A \in M_{n \times n}(K)$  gilt  $\delta(A) = \det(A) \delta(I_n)$

**Proof Korollar 2.14.11**

$\det \in \mathbb{A}$ ,  $\det \neq 0 \forall \delta \in \mathbb{A} : \exists d \in K$  so teilt  $\delta = d \det$  i.e.  $\forall A \in M_{n \times n}(K)$

$$\delta(A) = d \det(A),$$

Insbesondere  $A = I_n$ , i.e.

$$\delta(I_n) = d \det(I_n)$$

$$\delta(I_n) = d$$

i.e.  $\delta(A) = \delta(I_n) \det(A)$

**2.15 Skript 15****Corollary 2.15.1**

Für alle  $\delta \in A$ ,  $\delta \neq 0 \forall A \in M_{n \times n}(K)$  gilt:  $\delta(A) = \det(A) \delta(I_n)$

**Note 2.15.2**

Sei  $R$  kommutativer Ring 1,  $\delta \in \text{alt}^{(n)}(R^n)$  können analog definieren! Der Hauptsatz 2.14.10 gilt:  $A \in M_{n \times n}(R)$ ,  $A = (a_{ij})_{i,j}$ , definiere

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} \cdots a_{n\pi(n)} \underbrace{\det(I_n)}_{=1}$$

**Example 2.15.3**

Setze  $R := K[x]$  und

$$A = \begin{pmatrix} x & 0 & -x \\ 0 & 1 & 0 \\ 1 & 0 & x^3 \end{pmatrix}$$

$$\det(A) = x^4 + x^2$$

■

**Theorem 2.15.4**

Sei  $A \in M_{n \times n}(R)$ . Es gilt:

$$\det(A) = \det(A^t)$$

**Proof Satz 2.15.4**

Betrachte:

$$\prod_{i=1}^n a_i \pi(i) = \prod_{i=1, j=\pi(i)}^n a_{ij} = \prod_{j=1, i=\pi^{-1}(j)}^n a_{ij} = \prod_{j=1}^n a_{\pi^{-1}(j)j} = \prod_{j=1}^n a_{j\pi^{-1}(j)}^t$$

Daraus folgt:

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi \prod_{i=1}^n a_{i\pi(i)} = \sum_{\pi^{-1} \in S_n} \text{sign } (\pi^{-1}) \prod_{j=1}^n a_{j\pi^{-1}(j)}^t = \det(A^t) \quad \blacksquare$$

### Theorem 2.15.5

$\forall A, B \in M_{n \times n}(R)$  gilt:

$$\det(AB) = \det(A) \cdot \det(B)$$

### Proof Satz 2.15.5

Sei  $B$  fest und  $A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ . Definiere

$$\delta_B(A) := \det(AB) = \delta_B(z_1, \dots, z_n) = \det(z_1 B, \dots, z_n B)$$

(Bmk 7.6 L.A.I)

**Beh.:**  $\delta_B$  ist  $n$ -linear und alternierend (ÜB).

Also

$$\delta_B \in \text{alt}^{(n)}(R^n)$$

$$\text{Korollar 2.15.1} \implies \delta_B(A) = \det(A) \delta_B(I_n) = \det(A) \det(B) \quad \blacksquare$$

### Corollary 2.15.6

Sei  $A$  invertierbar. Es gilt

$$\det(A^{-1}) = (\det(A))^{-1}$$

### Definition Notation (Erinnerung)

Sei  $A \in M_{n \times n}(R)$ ,  $i, j \in \{1, \dots, n\}$ . Wir  $A[i|j]$  (entfernen von  $A$  die  $i$ -te Zeile und  $j$ -te Spalte).

$$D_{ij}(A) := \det(A[i|j])$$

### Theorem 2.15.7

Sei  $j, 1 \leq j \leq n$  fest. Setze

$$\delta(A) := \sum_{i=1}^n (-1)^{i+j} a_{ij} D_{ij}(A)$$

Dann ist  $\delta \in \text{alt}^{(n)}(R^n)$  und  $\delta(I_n) = 1$

### Proof Satz 2.15.7

Siehe Skript 15 S.2, S.3

**Details** und gegebenenfalls die Plenumsübung \blacksquare

**Corollary 2.15.8**

Sei  $A \in M_{n \times n}(R)$ . Für jedes  $1 \leq j \leq n$  gilt:

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} D_{ij}(A)$$

**2.16 Skript 16**

$$A \in M_{n \times n}(R)$$

**Note 2.16.1 Erinnerung**

$$C_{ij} = (-1)^{i+j} D_{ij}$$

der  $ij$ -te Kofaktor von  $A$ .

**Lemma 2.16.2 Hilfslemma**

$\forall k, j = 1, \dots, n$

$$k \neq j \implies \sum_{i=1}^n A_{ik} C_{ij} = 0$$

**Proof Hilfslemma 2.16.2**

Ersetze die  $j$ -te Spalte von  $A$  durch ihre  $k$ -te Spalte, nenne die so erhaltene Matrix  $B$ , weil  $B$  zwei Wiederholte Spalten hat, ist  $\det B = 0$ . Nun ist

$$B[i|j] = A[i|j]$$

Also berechnen wir

$$\begin{aligned} 0 &= \det B \\ &= \sum_{i=1}^n (-1)^{i+j} B_{ij} \det B[i|j] \\ &= \sum_{i=1}^n (-1)^{i+j} A_{ik} \det A[i|j] \\ &= \sum_{i=1}^n A_{ik} C_{ij} \end{aligned}$$

■

Wir fassen zusammen:

**Corollary 2.16.3**

(a)

$$\det A = \sum_{i=1}^n A_{ij} C_{ij}$$

(b)

$$\sum_{i=1}^n A_{ik} C_{ij} = \begin{cases} \det A & j = k \\ 0 & j \neq k \end{cases} \quad (*)$$

■

**Definition 2.16.4 Notation (Erinnerung)**

Sei  $A \in M_{n \times n}(R)$ ,  $i, j \in \{1, \dots, n\}$ . Wir  $A[i|j]$  (entfernen von  $A$  die  $i$ -te Zeile und  $j$ -te Spalte)..

$$D_{ij}(A) := \det(A[i|j])$$

**Note Erinnerung**

$$(\operatorname{adj} A)_{ij} := C_{ji} = (-1)^{-1} \det A[j|i]$$

**Corollary 2.16.5**

$$(\operatorname{adj} A)(A) = \det(A) I_n \quad (**)$$

**Proof Korollar 2.16.5**

Matrixprodukt + (\*)

■

Wir zeigen jetzt umgekehrt:

**Lemma 2.16.6**

$$A(\operatorname{adj} A) = \det(A) I_n$$

**Proof Lemma 2.16.6**

gleich

**Proof Lemma 2.16.6**

Es gilt

$$A^t[i|j] = A[j|i]^t$$

$\forall i, j = 1, \dots, n$  Satz 2.15.4  $\implies ij$ -te Kofaktor von  $A^t = ji$ -te Kofaktor. Also

$$\operatorname{adj}(A^t) = \operatorname{adj}(A)^t \quad (***)$$

Nun impliziert (\*\*) für  $A^t$ :

$$(\operatorname{adj} A^t) A^t = (\det A^t) I_n = (\det A) I_n$$

zusammen mit (\*\*\*) erhalten wir

$$(\operatorname{adj} A)^t A^t = [A(\operatorname{adj} A)]^t = (\det A) I_n = A(\operatorname{adj} A).$$

■



**Corollary 2.16.7**

$$A (\operatorname{adj} A) = \det(A) I_n$$

und

$$(\operatorname{adj} A) A = \det(A) I_n \quad (\dagger)$$

Insbesondere wenn  $A$ ,  $\det A \neq 0$ , folgt  $A^{-1} = \det(A)^{-1} \operatorname{adj}(A)$  ■

**Theorem 2.16.8**

$A \in M_{n \times n}(R)$  ist über  $R$  invertierbar genau dann, wenn  $\det(A) \in R^\times$  (eine Einheit in  $R$ ). Insbesondere wenn  $R = K$  ein Körper ist, dann ist  $A$  invertierbar genau dann wenn  $\det(A) \neq 0$ . Wenn  $R = K[x]$ , dann ist  $A$  invertierbar genau dann wenn  $\det(A) \in K^\times$ . Ist  $A$  invertierbar, so ist

$$A^{-1} = (\det A)^{-1} \operatorname{adj}(A)$$

**Proof Satz 2.16.8**

aus  $(\dagger)$  sehen wir:  $\det A$  invertierbar  $\implies A$  invertierbar mit

$$A^{-1} = (\det A)^{-1} \operatorname{adj}(A)$$

umgekehrt:  $A$  invertierbar über

$$\begin{aligned} R &\implies AA^{-1} = I_n \\ &\implies \det(AA^{-1}) = 1 \\ &\implies \det(A) \det(A^{-1}) = 1 \\ &\implies \det(A) \in R^\times \end{aligned}$$

Wir berechnen  $(K[x])^\times$  seien  $f, g \in K[x]$

$$fg = 1 \implies \deg f + \deg g = 0 \implies \deg f = \deg g = 0$$

Also die Einheiten von  $K[x]$  sind die Skalarpolynome  $\neq 0$ , i.e.  $K^\times$  ■

**Example 2.16.9**

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$\det(A) = a_{11}a_{22} - a_{21}a_{12}$$

$$\operatorname{adj}(A) = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_{2 \times 2}(\mathbb{Z})$$

$$\det(A) = -1 \notin \mathbb{Z}^\times,$$

$A$  ist nicht invertierbar über  $\mathbb{Z}$ .  $-2 \in \mathbb{Q}^\times$ ,  $A^{-1} = -\frac{1}{2} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$

**Example 2.16.10**

$$R = \mathbb{R}[x]$$

$$A = \begin{pmatrix} x^2 + x & x + 1 \\ x - 1 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} x^2 - 1 & x + 2 \\ x^2 - 2x + 3 & x \end{pmatrix}$$

$$\det(A) = x + 1,$$

$A$  ist **nicht** invertierbar

$$\det(B) = -6$$

$B$  invertierbar

**Lemma 2.16.11**

*Ähnliche Matrizen haben gleiche Determinanten.*

**Proof Lemma 2.16.11**

Seien  $A, B \in M_{n \times n}(K)$  ähnlich, d.h.  $\exists P$  invertierbar so, dass

$$B = P^{-1}AP$$

Berechne:

$$\begin{aligned} \det B &= \det(P^{-1}AP) \\ &= \det(P^{-1}) \det(A) \det(P) \\ &= \det(P)^{-1} \det(A) \det(P) \\ &= \det A \end{aligned}$$

■

**Definition 2.16.12**

Sei  $K$  ein Körper  $V$  ein  $K$ -Vektorraum,  $\dim V = n$ , und

$$T : V \rightarrow V$$

ein linearer Operator iwr definieren

$$\det(T) := \det([T]_{\mathcal{B}})$$

wobei  $\mathcal{B}$  eine beliebige geordnete Basis für  $V$  ist.

**Theorem 2.16.13 Cramer's Regel**

Sei  $A \in M_{n \times n}(K)$  mit  $\det(A) \neq 0$  und

$$Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^{n \times 1}$$

Betrachte das LGS:

$$(S)AX = Y$$

wobei

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Dann können wir die eindeutige Lösung von (S)

$$X = A^{-1}Y$$

so beschreiben:  $\forall j = 1, \dots, n \ x_j = \det(B_j) (\det(A))^{-1}$  wobei  $B_j$  die  $n \times n$  Matrix ist, die man erhält, wenn man die  $j$ -te Spalte von  $A$  durch  $Y$  ersetzt.

### Proof Satz 2.16.13

Multiplizieren mit  $\text{adj}(A)$  ergibt

$$\underbrace{(\text{adj}(A)A)}_{\det(A)I_n} X = \text{adj}(A)Y$$

$$\xrightarrow{\text{Kor. 2.16.7}} \det(A)X = \text{adj}(A)Y$$

Also

$$\det(A)x_j = \sum_{i=1}^n (\text{adj } A)_{ji} y_i$$

Also gilt  $\forall j = 1, \dots, n$  (laut Definition 2.16.4

$$\begin{aligned} \det(A)x_j &= \sum_{i=1}^n (-1)^{i+j} \det(A[i|j]) y_i \\ &= \sum_{i=1}^n (-1)^{i+j} y_i \det A[i|j] \\ &= \sum_{i=1}^n (-1)^{i+j} y_j \det B_j[i|j] \\ &\stackrel{\text{Kor 2.15.8}}{=} \det B_j \end{aligned}$$

### 3 Normalformen

#### 3.17 Skript 17

##### 3.17.9 Eigenwerte und Eigenvektoren

Sei  $V$  ein  $n$ -dim  $K$ -VR über

###### Definition 3.17.1

Sei  $T \in \mathcal{L}(V, V)$  und  $c \in K$ .

- (a)  $c$  ist ein Eigenwert für  $T$ , falls  $\exists \alpha \in V, \alpha \neq 0$  so, dass

$$T(\alpha) = c\alpha$$

- (b) sei  $\alpha \in V$  so, dass

$$T(\alpha) = c\alpha$$

Dann ist  $\alpha$  ein **Eigenvektor**

- (c)  $W_c := \{\alpha \in V, T(\alpha)\}$  der **Eigenraum** zu  $c$

###### Note 3.17.2

$$W_c = \ker(cI - T)$$

weil

$$W_c = \{\alpha : c\alpha - T(\alpha) = 0\}$$

###### Theorem 3.17.3

Wir folgern aus Satz 2.16.8 und Bem. 3.17.2 und Def. 3.17.1:  
Sei  $T \in \mathcal{L}(V, V)$ ,  $c \in K$ . Folgende Aussagen sind äquivalent:

- (i)  $c$  ist ein Eigenwert von  $T$
- (ii)  $(cI - T)$  ist **nicht** invertierbar
- (iii)  $\det(cI - T) = 0$

###### Proof Satz 3.17.3

“(i)  $\implies$  (ii)”: wenn  $c$  Eigenwert von  $T$ , dann existiert ein  $\alpha \in V$  mit  $\alpha \neq 0$ , so dass  $(cI - T)(\alpha) = 0$ , somit Kern nicht trivial, also  $(cI - T)$  nicht invertierbar

“(ii)  $\implies$  (iii)”: ...

“(iii)  $\implies$  (i)”:  $\det(cI - T) = 0$  bedeutet  $(cI - T)$  nicht invertierbar, also Kern trivial, also existiert kein  $\alpha \in V$ , ... vllt. auch einfacher mit Widerspruch ■

**Theorem 3.17.4**

$\det(cI - T)$  ist ein normiertes Polynom von Grad  $n$ . Die Eigenwerte von  $T$  sind also seine NS in  $K$ . Insbesondere hat  $T$  **höchstens**  $n$  Eigenwerte in  $K$

**Proof Satz 3.17.4**

Sei  $\mathcal{B}$  eine geordnete Basis für  $V$ ,  $A := [T]_{\mathcal{B}}$ . Es ist  $xI_n - A = [xI - T]_{\mathcal{B}}$

$$\begin{aligned} B &:= xI_n - A \\ &= \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & x & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & x \end{pmatrix} - A \\ &= \begin{pmatrix} x - a_{11} & \dots & -a_{1n} \\ -a_{21} & \ddots & \vdots \\ \vdots & & x - a_{nn} \end{pmatrix} \end{aligned}$$

wobei  $A_{ij} = a_{ij}$ . Also  $b_{ii} = (x - a_{ii})$ ,  $\deg b_{ii} = 1$ . Die Einträge von  $B$  sind 0 Polynome, Polynome von Grad 0 oder 1. Berechne

$$\det B = \sum_{\tau \in S_n} \text{sign } \tau b_{1\tau(1)} \cdots b_{n\tau(n)}$$

$$\deg(b_{1\tau(1)} \cdots b_{n\tau(n)}) = |\{i \in \{1, \dots, n\} : \tau(i) = i\}|$$

Also ist

$$\prod_{i=1}^n (x - a_{ii})$$

der **einzige** Term von Grad  $n$ , und somit ist der **Hauptterm!** Also

$$\deg(\det B) = n$$

und ist normiert ■

**Definition 3.17.5**

Sei  $A \in M_{n \times n}(K)$  und  $c \in K$ ,  $c$  ist ein **Eigenwert von**  $A$  falls  $\det(cI - A) = 0$ .

**Definition 3.17.6**

$f(x) := \det(xI_n - A)$  für  $A \in M_{n \times n}(K)$  heißt das **Charakteristische** Polynom von  $A$

**Lemma 3.17.7**

*Ähnliche Matrizen haben das gleiche charakteristische Polynom*

**Proof Lemma 3.17.7**

$$B = P^{-1}AP$$

$$\begin{aligned}\det(xI - B) &= \det(xI - P^{-1}AP) \\ &= \det\left(P^{-1}(xI - A)P\right) \\ &= \det P^{-1} \det(xI - A) \det(P) \\ &= \det(xI - A)\end{aligned}$$

■

**Definition 3.17.8**

Sei  $V$  endlich dimensional,  $T \in \mathcal{L}(V, V)$

$$\text{CharPol}(T) = \text{CharPol}([T]_{\mathcal{B}})$$

für irgendeine geordnete Basis  $\mathcal{B}$  von  $V$

**Example 3.17.9**

(1)

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M_{2 \times 2}(\mathbb{R}), \det(xI - A) = x^2 + 1$$

hat keine reelle NS, also hat  $A$  keine reelle Eigenwerte

(2)

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{pmatrix} \in M_{3 \times 3}(\mathbb{R})$$

$$|xI - A| = x^3 - 5x^2 + 8x - 4 = (x - 1)(x - 2)^2$$

Eigenwerte  $c = 1, c = 2$

Berechne Eigenvektoren

- $c = 1 \ker(A - I) := W_1$

$$(A - I) = \begin{pmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 1 & -1 \end{pmatrix}$$

$\implies \text{Rang}(A) = 2, \dim W_1 = 1$  Wir wollen eine Basis für  $W_1$  finden, löse

$$(A - I) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Hier  $\alpha_1 = (1, 0, 2) \neq 0$  ist eine Lösung, und  $\{\alpha_1\}$  ist eine Basis für  $W_1$

- $c = 2 \ W_2?$

$$(A - 2I) = \begin{pmatrix} 1 & 1 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & -2 \end{pmatrix}$$

hat  $\text{Rang}(A) = 2 \implies \dim W_2 = 1$  Lösung wie oben  $\alpha_2 = (1, 1, 2) \neq 0$  und  $\{\alpha_2\}$  eine Basis

**Lemma 3.17.10**

Sei  $T \in \mathcal{L}(V, V)$  seien  $c_i$  für  $i = 1, \dots, k$  Eigenwerte von  $T$  (in  $K$ ) und  $\forall i \neq j, i, j \in \{1, \dots, k\} : c_i \neq c_j$ . Sei  $v_i \neq 0, v_i \in V$  Eigenvektor zum Eigenwert  $c_i$ . Dann ist  $\{v_1, \dots, v_k\}$  linear Unabhängig

**Proof Lemma 3.17.10**

Wir führen Induktion nach  $k$

**I.A.**  $k = 2$ : wenn  $v_2 = cv_1$  dann ist  $v_2 \in W_{c_1}$ , dann ist  $v_2$  Eigenvektor zu  $c_1 \perp$

**I.V.** Für  $k - 1$

**I.S.** Seien  $v_1, \dots, v_k$  linear abhängig

**Bem.:** Sei  $v \in V, v \neq 0$  kann  $v$  **nicht** Eigenvektor sein zu verschiedenen Eigenwerten!  
 ☹

$$v_k = \sum_{i=1}^{k-1} v_i$$

Wir berechnen

$$\begin{aligned} T(v_k) &= c_k v_k = c_k \sum_{i=1}^{k-1} v_i \\ &= T(v_k) = \sum_{i=1}^{k-1} T(v_i) = \sum_{i=1}^{k-1} c_i v_i \\ &\implies c_k \sum_{i=1}^{k-1} v_i = \sum_{i=1}^{k-1} c_i v_i \\ &\implies \sum_{i=1}^{k-1} (c_k - c_i) v_i = 0. \end{aligned}$$

Aus I.V. folgt  $c_k - c_i = 0 \forall i = 1, \dots, k - 1$

**Corollary 3.17.11**

Sei  $\dim V = n, T \in \mathcal{L}(V, V)$ . Wir nehmen an, dass  $T$   **$n$  verschiedene** Eigenwerte  $d_1, \dots, d_n \in K$  hat. Dann hat  $V$  eine Basis  $\mathcal{D}$  bestehend aus Eigenvektoren für  $T$ . ■

**Definition 3.17.12**

Sei  $\dim V = n, T \in \mathcal{L}(V, V)$ .  $T$  ist **diagonalisierbar** über  $K$ , falls  $V$  eine Basis, bestehend aus Eigenvektoren von  $T$  hat.

**Note 3.17.13**

$d_1, \dots, d_n \in K$   $n$ -verschiedene Eigenwerte von  $T$ ,  $\mathcal{D}$  die geordnete Basis wie im Korollar 3.17.11, dann ist

$$[T]_{\mathcal{D}} = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

## 3.18 Skript 18

**Corollary 3.18.1** Verallgemeinerung Lemma 3.17.10

$\dim V = n$ ,  $T \in \mathcal{L}(V, V)$ ,  $d_1, \dots, d_k \in K$  verschiedene Eigenwerte von  $T$  für  $i \in \{1, \dots, k\}$  Sei

$$\mathcal{B}_i \subseteq W_{d_i}$$

linear unabhängig. Dann ist  $\mathcal{B} = \bigcup_{i \in I} \mathcal{B}_i$

**Proof** Korollar 3.18.1

$$L := \{v_1, \dots, v_l\} \subseteq \mathcal{B}$$

Betrachte

$$\sum_{j=1}^l c_j v_j$$

Setze

$$L_i := L \cap \mathcal{B}_i$$

und setze

$$\alpha_i := \sum_{v_j \in L_i} c_j v_j \in W_{d_i} \quad (*)$$

(Konvention falls  $L_i = \emptyset$ , setze  $\alpha_i = 0$ ). Also wenn

$$0 = \sum_{j=1}^l c_j v_j \implies \sum_{i=1}^k \alpha_i = 0$$

**Beh.:** Wenn

$$\sum_{i=1}^k \alpha_i = 0$$

dann ist  $\alpha_i = 0 \quad \forall i = 1, \dots, k$

**Bew. der Beh.** sonst

$$\alpha_i \neq 0,$$

Eigenvektoren zu verschiedenen Eigenwerten und linear abhängig. Widerspruch zu 3.17.10 zurück  
in (\*)  $\alpha_1 = 0 \implies$

$$\sum_{v_j \in L_i} c_j v_j = 0$$

aber  $v_j$  sind per Annahme linear unabhängig. Also  $c_j = 0 \quad \forall j = 1, \dots, k$  ■



**Theorem 3.18.2 Verallgemeinerung von Korollar 3.17.11**

Sei  $\dim V = n$ ,  $T \in \mathcal{L}(V, V)$ ,  $d_1, \dots, d_k \in K$  die verschiedenen Eigenwerte von  $T$  in  $K$ .  
Es gilt:  $T$  ist diagonalisierbar über  $K$  genau dann, wenn

$$\sum_{j=1}^k \dim W_{d_j} = n$$

**Proof Satz 3.18.2**

“ $\Leftarrow$ ”: Sei  $\mathcal{B}_j$  eine Basis für  $W_{d_j}$  für jedes  $j = 1, \dots, k$  setze

$$B = \bigcup_{j=1}^k \mathcal{B}_j$$

Korollar 3.18.1  $\implies$   $\mathcal{B}$  linear unabhängig

“ $\implies$ ”: Sei  $\mathcal{B}$  eine Basis für  $V$  von Eigenvektoren von  $T$ . Setze  $\mathcal{B}_j = \mathcal{B} \cap W_{d_j}$ . Also ist

$$\mathcal{B} = \bigcup_{j=1}^k \mathcal{B}_j$$

$$|\mathcal{B}| = n$$

Setze

$$l_j = |\mathcal{B}_j|$$

also

$$n = \sum_{j=1}^k l_j$$

**Beh.:**  $l_j = \dim W_{d_j}$  Es ist klar, dass

$$l_j \leq \dim W_{d_j}$$

Wenn  $l_i < \dim W_{d_i}$ , dann  $\exists \beta \in W_{d_i}$  so, dass

$$\mathcal{B}'_i = \mathcal{B}_i \cup \{\beta\}$$

linear unabhängig ist. Aber dann

$$\mathcal{B}' = \mathcal{B} \cup \{\beta\}$$

linear unabhängig! Aber  $|\mathcal{B}'| = n + 1 \perp$  ■

Sei  $\mathcal{D}$  die Basis

$$[T]_{\mathcal{D}} = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_1 & \\ & & & \ddots \end{pmatrix}$$

Wobei  $\forall i = 1, \dots, k$ ,  $d_i$  erscheint  $l_i := \dim W_{d_i}$  mal

Mit diesem Ansatz

$$\text{CharPol}(T) = \text{CharPol}([T]_{\mathcal{D}}) = \prod_{i=1}^k (x - d_i)^{l_i} \quad (\dagger)$$

Umgekehrt, sei  $T \in \mathcal{L}(V, V)$ ,  $\text{CharPol}(T)$  genau so, wie in  $(\dagger)$  ist, dann ist  $T$  diagonalisierbar (wegen Satz 3.18.2) wir haben bewiesen

### Theorem 3.18.3

Sei  $\dim V = n, T \in \mathcal{L}(V, V)$ . Es gilt:  $T$  ist diagonalisierbar genau dann wenn  $\text{CharPol}(T) = \prod_{i=1}^k (x - d_i)^{l_i}$ .

**Terminologie:**  $\dim W_d$  wird auch als  $d \in K$  Eigenwert **geometrische Vielfachheit** der Eigenwerte  $d$  genannt

$T$  ist diagonalisierbar (über  $K$ ) genau dann wenn  $\text{CharPol}(T)$  als Produkt von lin. Faktoren über  $K$  erfüllt **und** die algebraische Vielfachheit jeder Nullstelle ist gleich geometrischer Vielfachheit jeder Eigenwerte

### Theorem 3.18.4

Sei  $\dim V = n, T \in \mathcal{L}(V, V), d \in K$ . Eigenwerte von  $T$  mit Vielfachheit  $\mu$ . Es gilt:  $l := \dim(W_d) \leq \mu$

### Proof Satz 3.18.4

Sei  $(\alpha_1, \dots, \alpha_l)$  eine Basis für  $W_d$ , ergänze  $\mathcal{B} = (\alpha_1, \dots, \alpha_l, \alpha_{l+1}, \dots, \alpha_n)$  zur Basis von  $V$ . Berechne

$$A := [T]_{\mathcal{B}} = \begin{pmatrix} d & 0 & & \\ & \ddots & & B \\ 0 & & d & \\ & 0 & & C \end{pmatrix}$$

$$\det(xI - A) = \det \begin{pmatrix} x-d & 0 & & \\ & \ddots & & -B \\ 0 & & x-d & \\ & 0 & & xI - C \end{pmatrix} \stackrel{\text{ÜB}}{=} (x-d)^l \det(xI - C)$$

Dies impliziert  $l \leq \mu$  ■

### Example 3.18.5

$$A = \begin{pmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{pmatrix}$$

über  $\mathbb{R}$   $\text{CharPol} = (x-1)(x-2)^2$

$$d_1 = 1$$

$$A = \begin{pmatrix} 4 & -6 & -6 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{pmatrix}$$

$$\text{Rang}(A - I) = 2$$

$$d_2 = 2$$

$$A = \begin{pmatrix} 3 & -6 & -6 \\ -2 & 3 & 2 \\ 3 & -6 & -6 \end{pmatrix}$$

$\text{Rang}(A - 2I) = 1$  Also  $\dim W_{d_1} = 1$ ,  $\dim W_{d_2} = 2$ , also  $\dim W_{d_1} + \dim W_{d_2} = 3$ , also  $T$  diagonal und

$$[T]_{\mathcal{D}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \blacksquare$$

### 3.19 Skript 19

#### 3.19.10 Annihilator Ideal

$\dim V = n, T \in \mathcal{L}(V, V), V$   $K$ -Vektorraum

##### Proposition 3.19.1

Es gelten

- (1)  $\mathcal{A}(T) := \{p \in K[x]; p(T) = 0\}$  ist ein Ideal
- (2)  $\mathcal{A}(T) \neq \{0\}$

##### Proof Proposition 3.19.1

(1)  $(p + q)(T) = p(T) + q(T)$  und  $\forall p, q \in K[x] \ (pq)(T) = p(T)q(T)$  (1) folgt.

(2) Betrachte die  $n^2 + 1$  Elemente in  $\mathcal{L}(V, V)$ .

$$I, T, T^2, \dots, T^{n^2} \in \mathcal{L}(V, V)$$

Aber  $\dim \mathcal{L}(V, V) = n^2$  Also sind die linear abhängig  
i.e.  $\exists c_0, \dots, c_{n^2} \in K$ .

$$c_0 I + c_1 T + \dots + c_{n^2} T^{n^2} = 0$$

und die  $c_i$  sind **nicht** alle gleich 0. Also das Polynom

$$c_0 + c_1 x + \dots + c_{n^2} x^{n^2} = g(x) \neq 0$$

$$g(x) \in \mathcal{A}(T) \quad \blacksquare$$

**Definition 3.19.2**

$\mathcal{A}(T)$  ist **annihilator Ideal**. Der (eindeutig bestimmte normierte Erzeuger von  $\mathcal{A}(T)$  ist das **minimal Polynom von  $T$**  und wird mit  $\text{MinPol } T$  bezeichnet.

**Note 3.19.3**

- (1)  $\deg(\text{MinPol}(T)) \leq n^2$
- (2)  $p = \text{MinPol}(T)$  ist Charakterisiert durch
  - (a)  $p \in K[x]$
  - (b)  $p(T) = 0$
  - (c)  $\forall q \in K[x] : \deg q < \deg p \implies q(T) \neq 0$

**Definition 3.19.4**

für ein  $A \in \text{Mat}_{n \times n}(K)$  sind  $\mathcal{A}(A)$  und  $\text{MinPol}(A)$  analog definiert

**Note 3.19.5**

- (1) Sei  $\mathcal{B}$  eine geordnete Basis von  $V$  und  $f \in K[x]$ . Es gilt  $[f(T)]_{\mathcal{B}} = f([T]_{\mathcal{B}})$  Insbesondere für  $A = [T]_{\mathcal{B}}$  gilt

$$f(T) = 0 \iff f(A) = 0$$

- (2) Es folgt: ähnliche Matrizen haben das gleiche minimale Polynom!

**Theorem 3.19.6**

Sei  $T \in \mathcal{L}(V, V)$  (oder  $A \in \text{Mat}_{n \times n}(K)$ ). Es gilt:  $\text{CharPol}(T)$  und  $\text{MinPol}(T)$  haben, bis auf Vielfachheit, dieselben Nullstellen in  $K$

**Proof Satz 3.19.6**

Sei  $p := \text{MinPol}(T)$  und  $c \in K$ . Zu zeigen  $p(c) = 0 \iff c$  ist Eigenwert von  $T$

“ $\implies$ ”:  $p(c) = 0 \implies p = (x - c)q$ .

$$\deg q < \deg p$$

Also ist  $q(T) \neq 0$ . Also wähle  $\beta \in V$  so, dass  $\alpha := q(T)(\beta) \neq 0$  Es gilt  $0 = p(T)(\beta) = (T - cI)(qT)(\beta) = (T - cI)(\alpha)$  Also ist  $\alpha$  Eigenvektor und  $c$  Eigenwert

“ $\impliedby$ ”: Sei  $T(\alpha) = c\alpha$ ,  $\alpha \neq 0$ ,  $\alpha \in V$ ,  $c \in K$  Nun gilt:  $p(T)(\alpha) \stackrel{\text{ÜB}}{=} p(c)\alpha = 0$ . Da aber  $p(T) = 0$  und  $\alpha \neq 0$ , folgt  $p(c) = 0$  ■

**Proposition 3.19.7**

Sei  $T$  diagonalisierbar. Dann zerfällt das  $\text{MinPol}(T)$  (über  $K$ ) in verschiedene lineare Faktoren

**Proof Proposition 3.19.7**

Sei  $T$  diagonalisierbar und  $c_1, \dots, c_k \in K$  die verschiedenen Eigenwerte. Setze  $p := \text{MinPol } T$ . Wegen Satz 3.19.6 ist  $\deg p \geq k$ . Betrachte  $q(x) := (x - c_1) \cdots (x - c_k)$ . Wir berechnen:

$$(T - c_1 I) \cdots (T - c_k I)(\alpha) = 0$$

für  $\alpha$  Eigenvektor  $\in V$  (weil  $\alpha$  Eigenvektor zum Eigenwert  $c_i$ , für geeignetes  $i$ ). Da es eine Basis gibt bestehend aus Eigenvektoren für  $T$ . Also  $q(T)$  verschwindet auf dieser Basis der Eigenvektoren. Das impliziert

$$q(T) = 0$$

Also  $q(x) \in \text{Annihilator}(T)$ . Es folgt nun aus Bemerkung 3.19.3  $\deg q = k \leq \deg p$  und  $q$  ist normiert, folgt  $q(x) = p(x)$

**Example 3.19.8**

Wir berechnen  $\text{MinPol } A := p$  für  $A$  im Beispiel 3.17.9 (ii)

$$\text{CharPol}(A) = (x - 1)(x - 2)^2$$

$A$  ist **nicht** diagonalisierbar. Also hier können wir **nicht** Proposition 3.19.7 anwenden. Aber wir können Satz 3.17.6 anwenden. Also  $p$  die Nullstellen 1 und 2 hat. Wir probieren Polynome der Form

$$(x - 1)^k (x - 2)^l$$

mit  $k \geq 1, l \geq 1, 2 \leq k + l \leq 3^2 = 9$  Wir probieren  $k = l = 1$

$$(A - I)(A - 2I) = \begin{pmatrix} 2 & 0 & -1 \\ 2 & 0 & -1 \\ 4 & 0 & -2 \end{pmatrix}$$

Also ist  $\deg(p) \geq 3$ . Nun probieren wir:

$$(x - 1)^2 (x - 2) \text{ oder}$$

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

Wir berechnen:

$$(A - I)(A - 2I)^2 = 0$$

Also ist  $p(x) = (x - 1)(x - 2)^2 \implies \text{MinPol } A = \text{CharPol } A$ . ■

## 3.20 Skript 20

**Theorem 3.20.1 von Cayley Hamilton**

Sei  $\dim V = n, L \in \mathcal{L}(V, V)$

$$f := \text{CharPol}(L).$$

Es gilt  $f(L) = 0$ . Insbesondere teilt  $\text{MinPol}(L)$  das  $\text{CharPol}(L)$

**Proof Satz von Cayley Hamilton 3.20.1**

Sei  $\mathcal{K}$  die Algebra der Polynome in  $L$  und  $\mathcal{B} = (\alpha_1, \dots, \alpha_n)$  für  $V$ . Setze

$$A := [L]_{\mathcal{B}}$$

d.h.

$$L(\alpha_i) = \sum_{j=1}^n A_{ji} \alpha_j$$

$$\forall i \leq i \leq n$$

- Wir schreiben diese um, als

$$\sum_{j=1}^n (\delta_{ij} L - A_{ji} I) (\alpha_j) = 0 \quad \forall 1 \leq i \leq n \quad (1)$$

Sei  $B$  die  $n \times n$  Matrix mit den Koeffizienten in  $\mathcal{K}$  definiert durch

$$B_{ij} = \delta_{ij} L - A_{ji} I$$

**Beh.:**

$$\det B = f(L) \text{ und}$$

$$\det B = 0$$

- Wir haben  $f(x) = \det(xI - A) = \det(xI - A)^t$ . Wir berechnen

$$(xI - A)_{ij}^t = \delta_{ij} x - A_{ji}$$

Also gilt:

$$(xI - A)_{ij}^t(L) = \delta_{ij} L - A_{ji} I = B_{ij}$$

Außerdem gilt:

$$\begin{aligned} f(L) &= [\det(xI - A)](L) \\ &= [\det(xI - A)^t](L) \\ &= \det((xI - A)^t(L)) \\ &= \det B. \end{aligned}$$

- Wir zeigen  $\det B = 0$ . Dafür genügt es zu zeigen, dass

$$(\det B)(\alpha_k) = 0 \quad k = 1, \dots, n$$

Wegen (1) gelten  $B_{ij}$  und  $\alpha_j$ :

$$\sum_{j=1}^n B_{ij}(\alpha_j) = 0 \quad \forall 1 \leq i \leq n \quad (2)$$

- Setze  $\tilde{B} = \text{adj } B$  Aus (2) folgt, für alle  $k$  und  $i$

$$\tilde{B}_{ki} \left( \sum_{j=1}^n B_{ij} \alpha_j \right) = 0 = \sum_{j=1}^n \tilde{B}_{ki} B_{ij} \alpha_j$$

Wir summieren über  $i$  und bekommen

$$0 = \sum_{i=1}^n \sum_{j=1}^n \tilde{B}_{ki} B_{ij} \alpha_j = \sum_{j=1}^n \underbrace{\left( \sum_{i=1}^n \tilde{B}_{ki} B_{ij} \right)}_{kj\text{-te Koef von } \tilde{B}B} (\alpha_j)$$

### 3.20.1 Trigonalisierbarkeit

Sei  $V$  endlich dimensional  $K$ -VR

#### Definition 3.20.2

$T \in \mathcal{L}(V, V)$  ist trigonalisierbar falls es eine Basis  $\mathcal{B}$  für  $V$  gibt so dass  $[T]_{\mathcal{B}}$  eine obere  $\Delta$ -Matrix ist (d.h.  $a_{ij} = 0$  für  $i > j$ )

#### Theorem 3.20.3

Es gilt:  $T$  ist trigonalisierbar  $\iff \text{CharPol}(T)$  zerfällt in linear-Faktoren über  $K$ , (d.h.  $\text{CharPol}(T) = (x - c_1)^{n_1} \cdots (x - c_k)^{n_k}$  mit  $c_i \in K$ )

#### Proof Satz 3.20.3

“ $\implies$ ”  $[T]_{\mathcal{B}} = A$   $\Delta$ -Matrix  $\implies \det(xI - A) = \prod_{i=1}^n (x - a_{ii})$ .

“ $\impliedby$ ” Wir beweisen per Induktion über  $\dim V = n$  eine Basis  $\mathcal{B} = (\alpha_1, \dots, \alpha_n)$  aufbauen wofür  $[T]_{\mathcal{B}}$  eine  $\Delta$ -Matrix ist. Da  $T$  mindestens ein Eigenwert  $c_1 \in K$  hat, sei  $\alpha \neq 0$  ein Eigenvektor  $\{\alpha\}$  linear unabhängig  $\xrightarrow{\text{Basis Ergänzung}} (\alpha, \beta_2, \dots, \beta_n)$  für  $V$ , Matrixdarstellung von  $T$  in dieser Basis

$$\left( \begin{array}{c|ccc} c_1 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ 0 & a_{n2} & \dots & a_{nn} \end{array} \right) \quad (*)$$

$$\Gamma \in M_{(n-1) \times (n-1)}(K)$$

Setze  $W = \text{span} \{\beta_2, \dots, \beta_n\}$  definiere  $G \in \mathcal{L}(W, W)$

$$Gw = \Gamma w \text{ für alle } w \in W$$

Wir sehen aus (\*)  $\text{CharPol}(T) = (x - c_1) \text{CharPol}(G)$

Eindeutigkeit der Faktoren in  $K[x]$ , folgt  $\text{CharPol}(G)$  Produkt von linearen Faktoren. I.A. liefert nun eine geordnete Basis  $(\alpha_1, \dots, \alpha_n)$  so, dass die Matrixdarstellung von  $G$  eine obere  $\Delta$ -Matrix ist ■

### 3.21 Skript 21

#### 3.21.12 Invariante Unterräume

##### Definition 3.21.1

Sei  $W \subseteq V$  ein Unterraum und  $T \in \mathcal{L}(V, V)$ . Dann ist  $W$  **T-invariant** falls  $T(W) \subseteq W$

##### Example 3.21.2

- (0)  $\{0\}$ , und  $V$  sind  $T$ -invariant für alle  $T \in \mathcal{L}(V, V)$ .
- (1) Sei  $D$  der Ableitung Operator auf  $V := K[x]$  und  $W = K[x] \leq d$ . Dann ist  $W$   $T$ -invariant
- (2) Sei  $U \subset \mathcal{L}(V, V)$  so, dass  $TU = UT$ , setze
  - (a)  $W = \text{Bild}(U)$
  - (b)  $N = \ker(U)$

Dann sind  $W$  und  $N$   $T$ -invariant

##### Proof

- (a) Sei  $\alpha \in \text{Bild}(U)$ ,  $\exists \beta$  so, dass  $\alpha = U(\beta)$ .

$$T(\alpha) = T(U(\beta)) = U(T(\beta)) \in \text{Bild } U$$

- (b) Sei  $\alpha \in N$ , berechne  $U(T(\alpha)) = T(U(\alpha)) = T(0) = 0 \implies T(\alpha) \in N$  ■

- (3)  $W \subseteq V$  ist  $T$ -invariant  $\implies W$  ist  $g(T)$ -invariant für alle  $g(x) \in K[x]$  ÜB
- (4) Für alle  $g \in K[x]$  gilt

$$g(T)T = Tg(T) \quad (\ddot{\mathbf{U}}\mathbf{A})$$

Insbesondere gilt  $g(T) = cI - T$ . Daraus folgt wegen (2)  $\ker(T - cI)$   $T$ -invariant, d.h. der Eigenraum zum Eigenwert  $c \in K$  ist  $T$ -invariant.

- **Der Operator  $T_w$ :** sei  $T \in \mathcal{L}(V, V)$ ,  $W \subseteq V$  ist  $T$ -invariant. setze

$$T|_W := T_w$$

$$T_w : W \rightarrow W,$$



also ist

$$T_W \in \mathcal{L}(W, W)$$

† Matrix Darstellung für  $T_W$ : Sei  $W \subseteq V$   $T$ -invariant mit  $\dim W = r$ . Sei  $\mathcal{B}' = (\alpha_1, \dots, \alpha_r)$  eine geordnete Basis für  $W$ . Ergänze  $\mathcal{B}'$  zu einer Basis  $\mathcal{B} = (\alpha_1, \dots, \alpha_r, \alpha_{r+1}, \dots, \alpha_n)$  für  $V$ . Betrachte  $A = [T]_{\mathcal{B}}$  Wir haben die Gleichungen

$$T(\alpha_j) = \sum_{i=1}^n A_{ij} \alpha_i$$

Da  $W$   $T$ -invariant ist, sind  $T(\alpha_j) \in W$  für  $j \leq r$  Also

$$T(\alpha_j) = \sum_{i=1}^r A_{ij} \alpha_i$$

Das heißt  $A_{ij} = 0$  für  $j \leq r$  und  $i > r$  Also sieht  $A$  so aus

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

wobei  $B : r \times r$ ,  $C : r \times (n - r)$ ,  $D : (n - r) \times (n - r)$  und  $B = [T_W]_{\mathcal{B}'}$ .

### Lemma 3.21.3

Sei  $T \in \mathcal{L}(V, V)$   $W \subseteq V$ ,  $T$ -invariant. Es gelten:

- (a)  $\text{CharPol } T_W$  teilt  $\text{CharPol } T$
- (b)  $\text{MinPol } T_W$  teilt  $\text{MinPol } T$

### Proof Lemma 3.21.3

Seien  $\mathcal{B}'$  und  $\mathcal{B}$  so gewählt wie in (†), in  $A$  und  $B$  wie in (†) ÜB  $\implies$

(i)

$$\underbrace{\det(xI - A)}_{\text{CharPol } T} = \underbrace{\det(xI - B)}_{\text{CharPol } T} \det(xI - D) \quad \blacksquare$$

(ii)

$$A^k = \begin{pmatrix} B^k & C_k \\ 0 & D^k \end{pmatrix}$$

wobei  $C_k$  eine  $r \times (n - r)$ -Matrix für  $k \in \mathbb{N}_0$ .

Es folgt daraus, dass ein Polynom  $q \in \text{Annihilator}(A)$  ist  $q$  auch  $\in \text{Annihilator}(B)$ . Also teilt  $\text{MinPol } B$  das  $\text{MinPol } A$ .  $\blacksquare$

**Lemma 3.22.1**

Sei  $W \subseteq V$  ein Unterraum, sei  $\mathcal{B}'$  eine geordnete Basis für  $W$ , und

$$\mathcal{B}' \cup \mathcal{B}''$$

eine ergänzende Basis für  $V$ . Dann gelten

(i)  $\overline{\mathcal{B}''}$  ist eine Basis für  $V/W$

(ii) Umgekehrt, wenn  $(\overline{\beta_{r+1}}, \dots, \overline{\beta_n})$  eine geordnete Basis für  $V/W$  ist, dann ist

$$\mathcal{B}' \cup \{\beta_{r+1}, \dots, \beta_n\}$$

ist eine Basis für  $V$ . ■

**Note**

Sei  $W \subseteq V$   $T$ -invariant. Dann ist die Abbildung

$$\overline{T} : V/W \rightarrow V/W$$

so definiert

$$\overline{T}(\overline{\alpha}) := \overline{T(\alpha)}$$

ist wohldefiniert und ist linear. Also ist  $\overline{T} \in \mathcal{L}(V/W, V/W)$ .

**Proof**

“wohldefiniert”: Zu zeigen  $\overline{\alpha_1} = \overline{\alpha_2} \implies \overline{T(\alpha_1)} = \overline{T(\alpha_2)}$

**Bew.:**  $\alpha_1 - \alpha_2 \in W \implies T(\alpha_1 - \alpha_2) \in W \implies T(\alpha_1) - T(\alpha_2) \in W \implies \overline{T(\alpha_1)} = \overline{T(\alpha_2)}$  ■

**Theorem 3.22.2**

Sei  $W \subseteq V$   $T$ -invariant  $\mathcal{B}'$  geordnete Basis für  $W$ , ergänzt

$$\mathcal{B} = \mathcal{B}' \cup \mathcal{B}''$$

von  $V$ . Es gilt

$$A = [T]_{\mathcal{B}} = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

wobei  $D = [\overline{T}]_{\overline{\mathcal{B}''}}$  und  $B = [T_W]_{\mathcal{B}'}$ .

**Proof 3.22.3 Satz 3.22.2**

$$T(\alpha_i) = \sum_{j=1}^n A_{ji} \alpha_j \quad \text{für } 1 \leq i \leq n \quad (*)$$

$$A = \left( \begin{array}{c|c|c|c} B & A_{1,r+1} & & \\ \hline & \vdots & & \\ & A_{r,r+1} & & \\ & \vdots & & \\ & A_{n,r+1} & & \end{array} \right)$$

$$T(\alpha_i) = \sum_{j=1}^r A_{ji} \alpha_j \quad \text{für } 1 \leq i \leq r \quad \sum_{j=r+1}^n A_{ji} \alpha_j \quad \text{für } r+1 \leq i \leq n \quad (**)$$

Also ist

$$\overline{T(\alpha_i)} = \sum_{j=r+1}^n A_{ji} \overline{\alpha_j} = \overline{T}(\overline{\alpha_j})$$

für  $r+1 \leq i \leq n$  ■

### Corollary 3.22.4

$$\text{CharPol } T = (\text{CharPol } T_W) (\text{CharPol } \overline{T})$$

Ziel ist es Korollar 3.22.6 zu beweisen

Hintergrund: in Satz 3.20.3 hatten wir bewiesen  $V$  end. dim. VR,  $T \in \mathcal{L}(V, V)$ .

$T$  ist **trigonalisierbar** genau dann, wenn  $\text{CharPol } T$  im Produkt von linearen Faktoren über  $K$  zerfällt.

**Kor. 3.22.6** gibt uns dieselbe Charakterisierung mithilfe von

**MinPol**  $T$

anstatt

**CharPol**  $T$

### Corollary 3.22.6

Sei  $K$  Körper,  $T \in \mathcal{L}(V, V)$ ,  $V$  endlich dimensionaler Vektorraum. Dann ist  $T$  trigonalisierbar genau dann, wenn  $\text{MinPol } T$  im Produkt von linearen Faktoren über  $K$  zerfällt.

### Proposition

Sei  $K$  Körper,  $V$  endl.  $K$ -VR,  $T \in \mathcal{L}(V, V)$

**Es gilt:**  $\text{CharPol } T$  zerfällt im Produkt von linearen Faktoren über  $K$  genau dann, wenn  $\text{MinPol } T$  zerfällt im Produkt von linearen Faktoren über  $K$ .

Für den Beweis der Proposition brauchen wir ein Konzept und Aussage, die wir erst in der Vorlesung Algebra I im Wintersemester 2024 beweisen werden.

### Definition 3.22.7

Sei  $K$  ein Körper und  $p \in K[x]$ ,  $\deg p = n$ ,  $n \in \mathbb{N}$ . Eine Körpererweiterung

$$Z|K$$

ist ein **Zerfällungskörper** für  $p$ , wenn  $p(x)$  zerfällt im Produkt von linearen Faktoren über  $Z$ .

Das heißt  $\exists l_i \in \mathbb{N}$ ,  $c_i \in \mathbb{Z}$  und  $l \in \mathbb{N}$  so, dass

$$p(x) = \prod_{i=1}^l (x - c_i)^{l_i} \quad (*)$$

Das heißt,  $c_1, \dots, c_l$  sind Nullstellen von  $p$  und

$$\sum_{i=1}^l l_i = n$$

### Theorem

Sei  $K$  ein Körper,  $p \in K[x]$ ,  $\deg p \in \mathbb{N}$ . Dann gibt es ein Zerfällungskörper  $Z|K$  für  $p$ .

### Proof

VL Algebra I

### Proof Proposition

Sei  $Z|K$  ein Zerfällungskörper von

$$\text{CharPol}_K T.$$

Dann sind die NS von  $\text{CharPol}_Z T$  die  $c_1, \dots, c_l$  wie in der Faktorisierung (\*). Wir haben aber bewiesen, dass  $\text{MinPol}_Z T$  und  $\text{CharPol}_Z T$  dieselbe Nullstelle in  $Z$  haben. Insbesondere ist  $Z$  auch ein Zerfällungskörper für  $\text{MinPol}_Z T$ . Das heißt wiederum, dass  $\text{MinPol}_Z T$  in Produkt von linearen Faktoren und umgekehrt zerfällt: wenn  $\text{MinPol}_Z T$  in Produkt von linearen Faktoren in  $Z$  zerfällt, dann ist  $Z$  Zerfällungskörper für  $\text{CharPol}_Z T$ , also zerfällt  $\text{CharPol}_Z T$  in Produkt von linearen Faktoren wie in (\*).

Aber

$$\text{CharPol}_Z T = \text{CharPol}_K T$$

$$\text{MinPol}_Z T = \text{MinPol}_K T$$

### Corollary 3.22.8 Charakterisierung von Trigonalisierbarkeit

Sei  $K$  ein Körper,  $V$  ednl dim.  $K$ -VR, und  $T \in \mathcal{L}(V, V)$ . Es gilt:  $T$  ist trigonalisierbar über  $K$  genau dann, wenn  $\text{CharPol} T$  zerfällt über  $K$  genau dann wenn  $\text{MinPol} T$  zerfällt über  $K$

### 3.23 Skript 23

#### 3.23.13 Direkte Summe und Primzerlegung

##### Lemma 3.23.1

Sei  $V$   $K$ -VR,  $W_1, \dots, W_k$  Unterräume von  $V$ . Die folgende Aussagen sind äquivalent.

(i)  $W_1, \dots, W_k$  sind unabhängig, d.h. sei  $\alpha_i \in W_i$  für  $1 \leq i \leq k$  so, dass

$$\sum_{i=1}^k \alpha_i = 0,$$

dann ist  $\alpha_i = 0 \forall i = 1, \dots, k$ .

(ii)

$$W_j \cap (W_1, \dots, W_j) = \{0\} \text{ für } 2 \leq j \leq k$$

(iii) Ist  $\mathcal{B}_i$  eine Basis für  $W_i$ , dann ist

$$\mathcal{B} = \bigcup_{i=1}^k \mathcal{B}_i$$

eine Basis für  $W_1 + \dots + W_k$  ■

##### Definition Notation und Terminologie

Wir schreiben  $V = W_1 + \dots + W_k$ , wenn  $V$ , die **Summe** von Unterräumen  $W_i$  ist, und wir schreiben

$$V = W_1 \oplus \dots \oplus W_k$$

wenn die Unterräume  $W_1, \dots, W_k$  die Bedingungen von Lemma 3.23.1 erfüllen und sagen  $V$  ist die **direkte Summe**.

T

##### Theorem 3.23.2 Primzerlegung von $V$ bezüglich Primfaktorisierung MinPol T

Sei  $V$  endl dim über  $K$ ,  $T \in \mathcal{L}(V, V)$ . Setze  $\text{MinPol } T = p = p_1^{r_1} \dots p_k^{r_k}$  die Primfaktorisierung in  $K[x]$  (wobei  $p_i$  verschiedene normierte irreduzible Polynome in  $K[x]$  sind und  $r_i \in \mathbb{N}$ ) Setze  $W_i = \ker p_i(T)^{r_i}$  für  $1 \leq i \leq k$ . Dann sind  $W_i$ , für  $1 \leq i \leq k$ ,  $T$ -invariante Unterräume, und darüber hinaus gelten

(i)  $V = W_1 \oplus \dots \oplus W_k$

(ii)  $\text{MinPol } T_{W_i} = p_i^{r_i}$  für  $1 \leq i \leq k$ .

##### Proposition 3.23.3

Sei  $V$  endl dim  $K$ -VR  $T \in \mathcal{L}(V, V)$ .  $\text{MinPol } T = m = m_1 m_2$  mit  $\text{ggT}(m_1, m_2) = 1$  Setze  $V_i = \ker m_i(T)$  für  $i = 1, 2$ . Es gelten:  $V_1, V_2$  sind  $T$ -invariant und  $V = V_1 \oplus V_2$  und  $\text{MinPol } T_{V_i} = m_i$

für  $i = 1, 2$

### Proof Proposition 3.23.3

Da  $m_1, m_2$  relativprim sind  $\exists q_1, \dots, q_2 \in K[x]$  so, dass

$$1 = m_1 q_1 + m_2 q_2$$

oder

$$I = m_1(T)q_1(T) + m_2(T)q_2(T) \quad (*)$$

**Beh 1:**  $V_1 = I_m m_2(T)$  und  $V_2 = I_m m_1(T)$

**Bew.:**  $0 = m(T) = m_1(T)m_2(T)$ , also  $I_m m_2(T) \subseteq \ker m_1(T)$  umgekehrt  $v \in \ker m_1(T)$ , gilt wegen  $(*)$

$$v = \underbrace{q_1(T)m_1(T)(v)}_{=0} + \underbrace{m_2(T)(q_2(T)(v))}_{\in I_m m_2(T)}$$

**Beh. 2**  $V = V_1 \oplus V_2$

**Bew.:**

(1) Summe:

Sei  $v \in V$ , wegen  $(*)$  schreibe

$$v = \underbrace{m_1(T)q_1(T)(v)}_{\in I_m m_1} + \underbrace{m_2(T)q_2(T)(v)}_{\in I_m m_2(T)}$$

(2) direkt:

Sei  $v \in V_1 \cap V_2$ , wegen  $(*)$  gilt  $v = \underbrace{q_1(T)m_1(T)(v)}_{=0} + \underbrace{q_2(T)m_2(T)(v)}_{=0}$ . Sei nun ...

Da  $V_i = \ker m_i(T)$  für  $i = 1, 2$  ist es klar, dass  $m_i(T_{V_i}) = 0$ , d.h.

$$\tilde{m}_1|_{m_1} \text{ und } \tilde{m}_2|_{m_2} \quad (**)$$

**Beh. 3:**  $\tilde{m}_1 \tilde{m}_2$  annihiliert  $T$  **Bew.:** Seien  $v_1 \in V_1$  und  $v_2 \in V_2$ ,  $v = v_1 + v_2 \in V$ , rechne

$$\begin{aligned} \tilde{m}_1(T)\tilde{m}_2(T)(v_1 + v_2) &= \tilde{m}_1(T) [\tilde{m}_2(T)(v_2) + \tilde{m}_2(T)(v_1)] \\ &= \tilde{m}_1(T) \left[ 0 + \underbrace{\tilde{m}_2(T)(v_1)}_{\in V_1 \text{ weil Bsp 3.20.2 (4)}} \right] \\ &= 0 \end{aligned}$$

Da  $\tilde{m}_2 \tilde{m}_1$  annihiliert  $T \implies m_1 m_2 | \tilde{m}_1 \tilde{m}_2$ . Aber  $m_1, m_2$  sind normiert folgt nun aus  $(**)$ , dass  $\tilde{m}_1 = m_1$  und  $\tilde{m}_2 = m_2$  ■