7.5 Der Satz von Cayley-Hamilton und das Minimalpolynom

Sei K ein Körper (beliebig), V ein endl.-dim. K-VR, $f \in \mathrm{End}(V)$.

Def 7.5.1: Ist $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom, so setze

$$p(f) := \sum_{i=0}^{n} a_i f^i \in \mathrm{End}(V)$$

Satz 7.5.2: Seien $p, q \in K[X]$. Dann gilt:

(a) $(p \cdot q)(f) = p(f) \circ q(f) = q(f) \circ p(f)$

(b) Ist V' ein weiterer K-VR und $g: V' \to V$ ein Isomorphismus, so gilt: $p(g^{-1} \circ f \circ g) = g^{-1} \circ p(f) \circ g$

Bew: Sei $p = \sum_i a_i X^i \quad q = \sum b_j X^j$

(a) Dann ist $p(f) \circ q(f) = \left(\sum_i a_i f^i\right) \circ \left(\sum_j b_j f^j\right) = \underbrace{\sum_{i,j} a_i b_j \underbrace{(f^i \circ f^j)}_{f^{i+j}}}_{(p \cdot q)(f)}$

(b) $p(g^{-1} \circ f \circ g) = \sum_i a_i \underbrace{(g^{-1} \circ f \circ g)^i}_{= g^{-1} \circ f^i \circ g} = g^{-1} \circ \left(\sum a_i f^i\right) \circ g = g^{-1} \circ p(f) \circ g$

$\square$

Def. 7.5.3: Ein Polynom $p \in K[x]$ annuliert f, wenn $p(f)$ die 0-Abb. ist. Ein Minimalpolynom von f ist ein normiertes Polynom $\mu_f \in K[x] \setminus \{0\}$ von minimalem Grad, das f annuliert.

Erinnerung: $p = \sum_{i=0}^{n} a_i x^i$ heißt normiert, wenn $a_n = 1$ ist.

Bsp: • $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. Sei $p(x) = x - 3$. Dann $p(A) = A - 3I_3 = 0$

• $A' = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ Sei $p'(x) = x^3$. Dann $p'(A') = 0$

Satz 7.5.4: Der Endomorphismus f besitzt genau ein Minimalpolynom μ_f.
Außerdem gilt, für beliebige Polynome $p \in K[X]$:
p annuliert f gdw p ist ein Vielfaches von μ_f, d.h.
ex. $q \in K[X]$ s.d. $p = \mu_f \cdot q$.

Bem 7.5.5: Ist V' ein weiterer K-VR und $g: V' \longrightarrow V$ ein Isomorphismus,
so gilt für $f' := g^{-1} \circ f \circ g$ so ist $\mu_{f'} = \mu_f$.

Bew. von 7.5.5:
- Reicht z.z.: Für beliebige $p \in K[X]$ gilt: $p(f) = 0 \Leftrightarrow p(f') = 0$
- Nach 7.5.2 (b) $p(f') = p(g^{-1} \circ f \circ g) = g^{-1} \circ p(f) \circ g$ $\square$

Bew von 7.5.4: Existenz:

- Sei $n = \dim V$. Dann ist $\mathrm{End}(V)$ ein n^2-dimensionaler K-VR.
Also sind $f^0, f^1, \dots, f^{n^2}$ lin. abh, d.h. es existieren
$a_0, \dots a_{n^2} \in K$, nicht alle 0, s.d. $\underbrace{a_0 f^0 + a_1 f^1 + \dots + a_{n^2} f^{n^2}}_{= p(f)} = 0$

für $p = \sum_{i=0}^{n^2} a_i x^i$

Also existiert ein Polynom, das f annuliert.

- Wähle jetzt $p' \in K[x] \setminus \{0\}$ von minimalem Grad, das f annuliert.

$$\sum_{i=0}^{m} b_i x^i \qquad (m = \deg p')$$

Dann ist $\mu_f := b_m^{-1} \cdot p'$ ein Minimalpolynom von f.

Eindeutigkeit:

- Annahme, p und p' sind zwei verschiedene Minimalpolynome von f.
Insbes: $p = \sum_{i=0}^{m} a_i x^i$ und $p' = \sum_{i=0}^{m} a_i' x^i$ mit $a_m = a_m' = 1$

Setze $q := p - p'$.
  - $q \neq 0$ da $p \neq p'$
  - $\deg q < m$ (da sich der x^m-Koeff. weghebt.)
  - $q(f) = p(f) - p'(f) = 0 - 0 = 0$

Widerspruch zu: p, p' haben minimalen Grad.

Außerdem-Teil: Sei p gegeben. Zu zeigen:

$$p(f)=0 \iff p \text{ ist Vielfaches von } \mu_f$$

- „$\Leftarrow$": Sei $p = q \cdot \mu_f$

  Dann $p(f) = q(f) \circ \underbrace{\mu_f(f)}_{=0} = 0$.

- „$\Rightarrow$": • Ann: p ist ein Gegenbeispiel, d.h.

  $p(f)=0$ aber p ist kein Vielfaches von μ_f.

  - Wir nehmen zusätzlich an, dass p ein Gegenbsp. von minimalem Grad ist.
  - $p = \sum_{i=0}^{m} a_i x^i \qquad m = \deg p.$ $\qquad$ Sei $m_0 := \deg \mu_f$
  - Habe $m \geq m_0$
  - Setze $q := p - \mu_f \cdot a_m \cdot x^{m-m_0} \in K[x]$
  - Der x^m-Koeff von q hebt sich weg.

  $$\left(\mu_f = x^{m_0} + \sum_{j=0}^{m_0-1} b_j x^j \right.$$

  $$\left. \Rightarrow \mu_f \cdot a_m \cdot x^{m-m_0} = a_m \cdot \underbrace{x^{m-m_0} \cdot x^{m_0}}_{x_m} + \text{Rest} \right)$$

  - Also $\deg q < \deg p$.
  - Außerdem: $q(f) = \underbrace{p(f)}_{=0} - \underbrace{\mu_f(f)}_{=0} \circ a_m \cdot f^{m-m_0} = 0$
  - Beh: q ist kein Vielfaches von μ_f.

    Sonst: Wenn $q = \mu_f \cdot q'$ für ein $q' \in K[x]$ wäre:

    Dann wäre $p = \underbrace{q}_{=\mu_f \cdot q'} + \mu_f \cdot a_m \cdot x^{m-m_0}$

    $$= \mu_f \cdot (q' + a_m \cdot x^{m-m_0}),$$

    also wäre p ein Vielfaches von μ_f. ↯

  - q ist also ein Gegenbsp von kleinerem Grad. Widerspruch zur Annahme, dass p ein Gegenbsp von minimalem Grad war. $\square$

Satz 7.5.6: Ist K $\overbrace{\text{alg. abg.}}^{\text{algebraisch abgeschlossen}}$, so ist $\mu_f = (x-\lambda_1)^{r_1} \cdots (x-\lambda_s)^{r_s}$, wobei $\lambda_1, \dots, \lambda_s$ die EW von f sind und r_i die Größe des größten Jordanblocks von f $\underbrace{\text{zum Eigenwert } \lambda_i}_{\text{d.h. mit } \lambda_i \text{ auf der Diagonalen}}$.

D.h.: r_i ist der Nilpotenzgrad von $f|_{Hau_{\lambda_i}(f)} - \lambda_i \cdot id$

Bew: Nach 7.5.5 ist $\mu_f = \mu_A$, wobei A die JNF von f ist.

Sei $p = (x-\lambda_1)^{r_1} \cdots (x-\lambda_s)^{r_s}$

Zu zeigen: (i) $p(A) = 0$

(ii) Es existiert kein $p' \in K[x] \setminus \{0\}$ von kleinerem Grad als p mit $p'(A) = 0$.

(i) • Da $K^n = Hau_{\lambda_1}(A) \oplus \dots \oplus Hau_{\lambda_s}(A)$ reicht es zu zeigen:

$$p(A)|_{Hau_{\lambda_i}(A)} = 0 \quad \text{für alle } i$$

• Sei i gegeben. Habe: $p(x) = q(x) \cdot (x-\lambda_i)^{r_i}$, für q = Produkt der restl. Faktoren.

$$p(A) = q(A) \circ \underbrace{(A - \lambda_i \cdot id)^{r_i}}_{\text{bildet ganz } Hau_{\lambda_i}(A) \text{ auf } 0 \text{ ab.}}$$

Also bildet auch $p(A)$ ganz $Hau_{\lambda_i}(A)$ auf 0 ab.

(ii) Annahme, so ein p' existiert. O.E. sei p' normiert.

Schreibe $p' = (x-\lambda_1')^{r_1'} \cdots (x-\lambda_{s'}')^{r_{s'}'}$

Da $\underset{\underset{r_1' + \dots + r_{s'}'}{||}}{\deg p'} < \underset{\underset{r_1 + \dots + r_s}{||}}{\deg p}$ existiert mindestens ein i, so dass $(x-\lambda_i)^{r_i}$ nicht als Faktor von p' auftaucht, und auch nicht $(x-\lambda_i)^{r''}$ für $r'' > r_i$

Betrachte $p'(A)|_{Hau_{\lambda_i}(A)}$:

• $(A - \lambda_j')^{r_j'}|_{Hau_{\lambda_i}(A)}$ ist ein Automorphismus von $Hau_{\lambda_i}(A)$ falls $\lambda_j' \neq \lambda_i$

- Falls $\lambda_j' = \lambda_i$: $r_j' < r_i$ nach Wahl von i

  r_i ist der Nilpot-Grad von $(A - \lambda_i id)|_{Hau_{\lambda_i}(A)}$

  also ist $(A - \lambda_j')^{r_j'}|_{Hau_{\lambda_i}(A)} \in End_{\lambda_i}(A)$ nicht die 0-Abb.

- $p'(A)|_{Hau_{\lambda_i}(A)}$ ist also eine Verknüpfung von Automorphismen und einer Abb., die nicht die 0-Abb ist, also auch insgesamt nicht die 0-Abb.
- Also ist auch $p'(A) \neq 0$. $\square$

(K muss nicht alg. abg sein.)

Satz 7.5.7 (Satz von Cayley-Hamilton): $\chi_f(f) = 0$

Insbesondere ist χ_f ein Vielfaches von μ_f, d.h. ex. $q \in K[x]$ s.d. $\chi_f = q \cdot \mu_f$.

Bew: (1) Falls K alg. abg ist:

$$\mu_f = \prod_{i=1}^{s} (x - \underbrace{\lambda_i}_{\text{EW}})^{r_i}$$

r_i: Größe des größten λ_i - Jordanblockes

$$\chi_f = \prod_{i=1}^{s} (\underbrace{\lambda_i}_{\text{EW}} - x)^{d_i}$$

$d_i = \dim Hau_{\lambda_i}(f)$

$= \text{Summe der Größen aller } \lambda_i\text{-Jordanblöcke}$

$\geq r_i$

$$\chi_f = \mu_f \cdot \left(\pm \prod_{i=1}^{s} (x - \lambda_i)^{d_i - r_i} \right)$$

Insbes folgt $\chi_f(f) = 0$ (nach 7.5.4)

(2) Allgemeiner Fall:

- Sei K beliebig. Sei $K' \supseteq K$ ein Körper, der K enthält und alg. abg. ist. (Ex. nach 7.3.6)

- Wähle einen Isomorphismus $g: K^n \to V$ $(n = \dim V)$ $\circlearrowleft_A$ $\circlearrowleft_f$
- Sei $A = g^{-1} \circ f \circ g$
- Wir werden zeigen: $\chi_A(A) = 0$, und damit: χ_A ist Vielfaches von μ_A.

  Daraus folgt dann auch $\chi_f(f) = 0$, da $\chi_f = \chi_A$ und $\mu_f = \mu_A$
- Fasse A als Matrix in $(K')^{n \times n}$ auf.

  Jetzt gilt $\chi_A(A) = 0$ nach (1). □

<u>Def. 7.5.8:</u> Sei $p = x^d + \sum_{i=0}^{d-1} a_i x^i \in K[x]$ ein normiertes Polynom. Die <u>Begleitmatrix</u> zu p ist

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & \ddots & & 0 & -a_1 \\ & \ddots & \ddots & & \vdots \\ & 0 & \ddots & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix} \in K^{d \times d}$$

<u>Satz 7.5.9:</u> Ist A die Begleitmatrix zu einem normierten Polynom $p \in K[x]$, so ist $\mu_A = p$ und $\chi_A = \pm p$.

<u>Bew:</u> Sei $d := \deg p$.

- <u>Beh:</u> Ex kein Polynom q vom Grad $< d$ mit $q(A) = 0$.

  <u>Bew:</u> Sei $q = \sum_{i=0}^{d'} b_i x^i$ $\quad d' < d$

  Annahme: $q(A) = 0$. Insbes:

  Betrachte $(q(A))\, e_1 = 0$

  $$\| $$

  $$\sum_{i=0}^{d'} b_i \underbrace{A^i e_1}_{\text{Wende } (*) \text{ an.}}$$

  $$\left.\begin{aligned} A e_1 &= e_2 \\ A e_2 &= e_3 \\ &\vdots \\ A e_{d-1} &= e_d \end{aligned}\right\} \text{Insbes: Für } i \leq d-1 \quad A^i e_1 = e_{1+i} \quad (*)$$

  $$A e_d = -a_0 e_1 - \dots - a_{d-1} e_d$$

  Erhalte Widerspruch dazu, dass $e_1, \dots, e_d$ lin. unabh. sind.
- Also hat das Minimalpolynom von A mind. Grad d.

  Nach 7.5.7 folgt: $\deg \mu_A = d$ und $\chi_A = \pm \mu_A$
- Rest: Übung. □

Satz 7.5.10: Sei $v \in V$. Setze $v_i := f^i(v)$ (insbes.: $v_0 := f^0(v) = v$)

und $U := \langle v_i \mid i \in \mathbb{N} \rangle_K$. Dann:

(a) U ist der kleinste f-invariante UVR von V, der v enthält.

(d.h. für jeden f-invar. UVR $U' \subseteq V$, der v enthält, gilt: $U \subseteq U'$).

Wir nehmen jetzt an, dass $\dim U =: d < \infty$

(b) $v_0, \ldots, v_{d-1}$ ist eine Basis von U

(c) Die Matrix von $f|_U$ bezgl. der Basis $v_0, \ldots, v_{d-1}$ ist die Begleitmatrix zu $\mu(f|_U)$. Insbes ist $\deg \mu_{f|_U} = d$.

<u>Bew</u>: (a) U ist f-invar, da für $\underset{\substack{\shortparallel \\ \sum a_i v_i}}{u} \in U$ gilt: $f(u) = \sum a_i \underbrace{f(v_i)}_{= v_{i+1} \in U}$

U kleinster f-invariante UVR: klar.

(b) Ann: $v_0, \ldots, v_{d-1}$ l. abh.

Also ex. $m \leq d-1$ s.d. $v_m = \sum_{i=0}^{m-1} b_i v_i$

$v_m \in \langle v_0, \ldots, v_{m-1} \rangle_K$

<u>Beh</u>: $v_i \in \langle v_0, \ldots, v_{m-1} \rangle_K$ für alle i (also $U = \langle v_0, \ldots, v_{m-1} \rangle_K$ $\Rightarrow \dim U = m$ ↯)

Bew per Induktion: • Für $i \leq m$: ✓

• Sei $i > m$:

da $v_{i-1} \in \langle v_0, \ldots, v_{m-1} \rangle_K$

$$v_i = f(v_{i-1}) = f\left(\sum_{j=0}^{m-1} c_j v_j\right)$$

$$= \sum_{j=0}^{m-1} c_j \underbrace{f(v_j)}_{v_{j+1} \in \langle v_0, \ldots, v_{m-1} \rangle_K \text{ da } j+1 \leq m}$$

(c) $f(v_0) = v_1$, $f(v_1) = v_2$, $\ldots$, $f(v_{d-2}) = v_{d-1}$

$f(v_{d-1}) = \sum_{i=0}^{d-1} a_i v_i$

d.h. die Matrix dazu ist
$$\begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix}$$

Das ist die Begleitmatrix zu
$$p(x) = x^d - \sum_{i=0}^{d-1} a_i x^i.$$

$\square$