

6.2.3. Nullstellen, Grad und die Koeffizienten des charakteristischen Polynoms

Frop. Sei $\lambda \in K$ und $A \in K^{n \times n}$ ($n \in \mathbb{N}$).

Dann ist λ genau dann ein Eigenwert von A , wenn $P_A(\lambda) = 0$ ist (d.h. λ ist Nullstelle des charakteristischen Polynoms von A).

Beweis: λ Eigenwert von $A \iff$
 $A\sigma = \lambda\sigma$ für ein $\sigma \in K^n \setminus \{0\} \iff$
 $\ker(\lambda I - A) \neq \{0\} \iff \det(\lambda I - A) = 0$
 $\iff P_A(\lambda) = 0.$ □

Aus P_A erhält man die Eigenwerte, aber P_A ist auch an sich interessant.

Frop Sei $A = (a_{ij}) \in K^{n \times n}$ ($n \in \mathbb{N}$).

Dann gilt:

$$P_A = 1 \cdot t^n - (a_{11} + \dots + a_{nn}) t^{n-1} + \dots + (-1)^n \det(A),$$

d.h. $\deg P_A = n$, der Koeff. von t^n ist $-(a_{11} + \dots + a_{nn})$ ist der Koeff. von t^{n-1} , $(-1)^n \det(A)$ ist der konstante Term.

Beweis:

$$P_A = \det(tI - A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n (t \delta_{i, \sigma(i)} - a_{i, \sigma(i)})$$

$\underbrace{\quad}_{f_\sigma}$

Ist $i = \sigma(i)$, d.h. i ist Fixpunkt von σ ,
so hat nur der Faktor $t - a_{ii}$ im Produkt den
Auswirkung auf den Faktor eine Konstante.

Die Anzahl der Faktoren in f_σ , die konstanten
ist die Anzahl der Fixpunkte von σ .

Eine Permutation hat höchstens n Fixpunkte;
die maximale Anzahl wird nur die identische
Permutation erreicht.

$$f_\sigma = (t - a_{11}) \cdot (t - a_{22}) \cdot \dots \cdot (t - a_{nn})$$

Bei allen anderen Permutationen ist die Anzahl
der Fixpunkte höchstens $n-2$, sodass

$$\deg f_\sigma \leq n-2 \text{ ist, wenn } \sigma \neq \text{id. gilt.}$$

Der Term t^n kann daher nur durch f_σ
beigesteuert werden (dieser Term hat man an f_σ mit
dem Koeffizienten 1).

Auch diese Monome t^{n-i} kann nur in f_σ vorkommen.

$$P_A(0) = \det(0 \cdot I - A) = \det(-A) = (-1)^n \det(A)$$

$\Rightarrow (-1)^n \det(A)$ der konstante Term von P_A .

□

Bei $A = (a_{ij}) \in \mathbb{K}^{n \times n}$ heißt man

$\text{tr}(A) = a_{11} + \dots + a_{nn}$ die Spur von A .

Durch P_A sind $\text{tr}(A)$ und $\det(A)$ eindeutig bestimmt.

6.2.4. Das charakteristische Polynom, die Spur und die Determinante von linearer Abbildungen.

Matrizen $A, \tilde{A} \in \mathbb{K}^{n \times n}$ heißen ähnlich, wenn $\tilde{A} = B^{-1}A \cdot B$ für eine invertierbare Matrix $B \in \mathbb{K}^{n \times n}$ erfüllt ist.

Lem. Seien $A, \tilde{A} \in \mathbb{K}^{n \times n}$ ähnliche Matrizen. Dann gilt: $P_A = P_{\tilde{A}}$, $\det(A) = \det(\tilde{A})$, $\text{tr}(A) = \text{tr}(\tilde{A})$.

[Mit anderen Worten sind P_A , $\det(A)$ und $\text{tr}(A)$ sog. charakteristische Invarianten der Ähnlichkeitseigenschaften.]

Basis: Es reicht $P_A = P_{\tilde{A}}$ zu zeigen, denn $\det(A)$ und $\text{tr}(A)$ sind in P_A "gespeichert".

Sei $\tilde{A} = B^{-1}A \cdot B$ für ein invertierbares B .

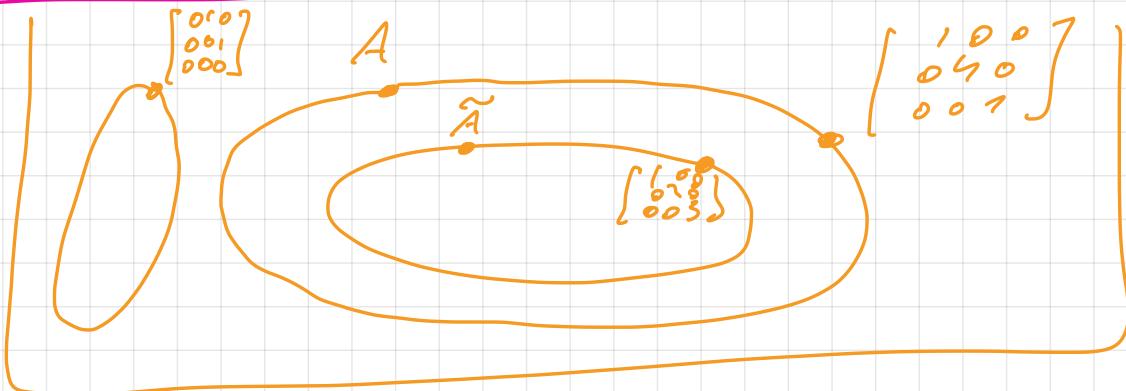
$$\begin{aligned}\Rightarrow P_{\tilde{A}} &= \det(tI - \tilde{A}^T \tilde{A}) \\ &= \det(B^{-1}(tI - A^T B)B) \\ &= \det(B^{-1}) \cdot \det(tI - A) \det(B) \\ &= \det(tI - A) = P_A.\end{aligned}$$

□

\tilde{A} kann zu $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ diagonalisiert werden.

A kann zu $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$ diagonalisiert werden.

$P_A = P_{\tilde{A}}$? Nein.



Sei $F: V \rightarrow V$ lineare Abbildung eines endlich-dim. Vektorraums V . Dann definiere wir das charakt. Polynom P_F , die Spur tr_F und die Determinante $\det(F)$ von F durch

$$P_F = P_{F_B},$$

$$\text{tr}(F) = \text{tr}(F_B)$$
 und

$$\det(F) = \det(F_B),$$

wobei B eine beliebige Basis von V ist.

Die rechten Seiten hängen nicht von B ab, da für Basen A, B von V die Matrizen F_A und F_B ähnlich sind.

6.2.5]

Der Satz von Cayley-Hamilton

Wir können Polynome, wie $f = c_0 t^0 + \dots + c_d t^d \in K[t]$ auf Matrizen $A \in K^{n \times n}$ anwenden:

$$f(A) = c_0 \underbrace{A^0}_{\mathbb{I}} + c_1 A^1 + \dots + c_d A^d$$

Bsp. $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in \mathbb{R}^{2 \times 2}$

$$P_A(t) = t^2 - 5t - 2.$$

$$\begin{aligned} P_A(A) &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^2 - 5 \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix} - 5 \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

Thm (Der Satz von Cayley-Hamilton für Matrizen).

Für jede Matrix $A \in \mathbb{K}^{n \times n}$ gilt $P_A(A) = 0$.

Beweis: $A^\# \cdot A = \det(A) \cdot \mathbb{I}$.

Wir setzen für A die Matrix $(t\mathbb{I} - A^\top)$ ein.

$$\underbrace{(t\mathbb{I} - A^\top)^\#}_{B(t)} \cdot (t\mathbb{I} - A^\top) = P_A(t) \cdot \mathbb{I}$$

$$\Downarrow \quad B(t) = (b_{ij}(t))_{ij} \in \mathbb{K}[t]^{n \times n}$$

$$B(t) \cdot (t\mathbb{I} - A^\top) = P_A(t) \cdot \mathbb{I}$$

Sei $A = (a_{ij})_{i,j=1,\dots,n}$. Komponentenweise gilt:

$$\sum_{j=1}^n b_{ij}(t) \cdot (t \delta_{jk} - a_{kj}) = P_A(t) \delta_{ik}$$

Nun setzen wir für t die Matrix A ein:

$$\sum_{j=1}^n b_{ij}(A) (A \delta_{jk} - a_{kj} \mathbb{I}) = P_A(A) \cdot \delta_{ik}$$

$$\Rightarrow \sum_{k=1}^n \sum_{j=1}^n b_{ij}(A) (A \delta_{jk} - a_{kj} I) e_k = \sum_{k=1}^n p_A(A) f_{ik} e_k$$

$$\Rightarrow \sum_{j=1}^n b_{ij}(A) \sum_{k=1}^n (A \delta_{jk} e_k - a_{kj} e_k) = p_A(A) e_i$$

$$\Rightarrow \sum_{j=1}^n b_{ij}(A) \left(A e_j - \underbrace{\sum_{k=1}^n a_{kj} e_k}_\varphi \right) = p_A(A) \cdot e_i$$

j -te Spalte von A ;
 $A e_j$ ist genau die j -te Spalte.

$$\Rightarrow \sum_{j=1}^n b_{ij}(A) \cdot 0 = p_A(A) \cdot e_i$$

$$\Rightarrow p_A(A) \cdot e_i = 0 \quad \text{für alle } i=1, \dots, n$$

\Rightarrow Alle Spalten von $p_A(A)$ sind 0

$$\Rightarrow p_A(A) = 0$$

□

Bsp.

$$(2 - \sqrt{2})^\mathbb{Z} = ?$$

$\mathbb{Q}[\sqrt{2}] = \text{lin}_{\mathbb{Q}} \underbrace{(1, \sqrt{2})}_\text{Basis, BS.} \leftarrow 2\text{-dim. Vektorraum über } \mathbb{Q}$

$$F(u) = \sqrt{2} \cdot u \leftarrow \text{lineare Transformation von } \mathbb{Q}[\sqrt{2}].$$

Ans Basis \mathcal{B}

$$F(1) = \sqrt{2}$$

$$F(\sqrt{2}) = 2$$

$$F_{\mathcal{B}} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \underset{\textcircled{1}}{\textcircled{2}} =: A$$

$$p_A(t) = t^2 - 2 \Rightarrow$$

$$A^2 - 2I = 0$$

$$(2I - A)^2 = \begin{bmatrix} 2 & -2 \\ -1 & 2 \end{bmatrix}^2 = \begin{bmatrix} 2704 & -3824 \\ -1912 & 2704 \end{bmatrix}$$

$$= 2704I - 1912A$$

$$(2-\sqrt{2})^7 = 2704 - 1912\sqrt{2}.$$

Bem Was beschreibt Cayley-Hamilton aus der Perspektive der Ringe? Jedes $A \in K^{n \times n}$ erzeugt den Ring $K[A] := \{f(A) : f \in K[t]\}$.

Die Einz dieses Rings ist $I = A^0$? Dies ist ein kommutativer Ring, denn $A^i \cdot A^j = A^{i+j} \cdot A^i$.

Pl. man hat z.B. Gleichungen wie

$$(A - I)(A + I) = A^2 - I \quad \text{in diesem Ring.}$$

Aber gleichzeitig ist $K[A]$ auch ein Vektorraum über K . Es ergibt sich dann die Frage:

Was ist $\dim_K K[A]$? Die Dimension ist in jedem Fall endlich, denn $K[A]$ ist UVR von $K^{n \times n}$ und $\dim K^{n \times n} = n^2$. Das ergibt die Abschätzung

$\dim_K K[A] \leq n^2$. Aber es gibt eine bessere Abschätzung.

Nehmen wir zuerst an, das $A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$, für welches $P_A(t) = t^2 - 2$ ist ($K = \mathbb{Q}$).

$K[A]$ ist erzeugt durch $A^0, A^1, A^2, A^3, \dots$

Was passiert hier mit den Potenzen?

$$A^0 = I$$

$$A^2: A^2 - 2I = 0, A^2 = 2I$$

$$A^4 = A^2 \cdot A = 2I \cdot A = 2A$$

$$\in \text{lin}(I, A)$$

$$A^8 = A^4 \cdot A = 2A^2 = 4I \in \text{lin}(I, A)$$

$$\text{aus. } \Rightarrow K[A] = \text{lin}(I, A).$$

Wie würde es für ein allgemeines A aussehen,
 $A \in \mathbb{K}^{n \times n}$? Es gilt: $\dim_{\mathbb{K}} [\mathbb{K}[A]] \leq n$.

Sei $p_A(t) = t^n + c_1 t^{n-1} + \dots + c_n t^0$
 $c_1, \dots, c_n \in \mathbb{K}$.

Cayley-Hamilton

$$\Rightarrow p_A(A) = A^n + c_1 A^{n-1} + \dots + c_n A^0 = 0.$$

$$[\mathbb{K}[A]] = \lim_{\mathbb{K}} \{A^i : i \in \mathbb{N}_0\}$$

A^0, \dots, A^{n-1} nehmen wir mit.

$$A^n = -c_1 A^{n-1} - \dots - c_n A^0 \in \text{lin}(A^0, \dots, A^{n-1})$$

$$A^{n+1} = A^n \cdot A$$

$$= (-c_1 A^{n-1} - \dots - c_n A^0) \cdot A$$

$$= \underbrace{-c_1 A^n - \dots - c_n A^1}_{\in \text{lin}(A^0, \dots, A^{n-1})} \in \text{lin}(A^0, \dots, A^{n-1})$$

$$\in \text{lin}(A^0, \dots, A^{n-1})$$

iterative Matrix umgewandelt.

Die Aussage $\dim [\mathbb{K}[A]] \leq n$ ist nicht immer
 mit Gleichheit erfüllt, z.B. bei $A = I$
 ist $\dim [\mathbb{K}[A]] = 1$.

Bem:

Es gibt eine verdeckte Werte Gleichungssysteme
 zu lösen, die wie folgt geht:

Man formuliert das System der
 die Fixpunktbedingung $F(x) = x$
 mit $F: \mathbb{R}^n \rightarrow \mathbb{R}^n$.

$x^{(0)} \in \mathbb{R}^n$ beliebig wählen

$x^{(k)} = F(x^{(k-1)})$ für alle $k \in \mathbb{N}$ setzen.

Wenn die Folge aus $x^{(k)}$'s konvergiert und F stetig ist, dann hat man

$$\begin{array}{ccc} x^{(k)} & = & F(x^{(k-1)}) \\ \downarrow k \rightarrow \infty & & \downarrow \\ x^* & = & F(x^*) \end{array} .$$

In der Lineare Algebra betrachten wir lineare Gleichungen: $Ax = b$ mit $A \in \mathbb{R}^{n \times n}$, $b \in \mathbb{R}^n$.

$$b - Ax = \underbrace{\quad}_{0}$$

$$b + (I-A)x = x$$

Wir können $F(x) = b + (I-A)x$ nutzen.

$x^{(0)}$

$$x^{(1)} = F(x^{(0)}) = b + (I-A) \cdot x^{(0)}$$

$$\begin{aligned} x^{(2)} &= b + (I-A)(b + (I-A)x^{(0)}) \\ &= b + (I-A) \cdot b + (I-A)^2 \cdot x^{(0)} \\ &\quad \underbrace{\qquad}_{\stackrel{\wedge}{[K(A)]}} \quad \underbrace{\qquad}_{\stackrel{\wedge}{[K(A)]}} \end{aligned}$$

Thm (Cayley-Hamilton in der Formulierung mit linearen Abbildungen).

Sei $F: V \rightarrow V$ lineare Abbildung auf einem endlich-dim. VR V . Dann gilt:

$$P_F(F) = 0,$$

wobei $P_F(F)$ genau so wie im Fall von Matrizen eingesetzt wird.

Beweis: Übungsaufgabe.

6.3 Diagonalisierbarkeit

6.3.1

Sei $f \in K[t]$ vom Grad $\deg f \geq 1$.

Wir sagen, dass f in $K[t]$ in Linearfaktoren zerfällt, wenn man f als

$$f = c \cdot (t - \mu_1) \cdots (t - \mu_n)$$

mit $c \in K \setminus \{0\}$ und $\mu_1, \dots, \mu_n \in K$ darstellen kann.

Bsp.

$$\underbrace{3t^2 - 6t + 3}_{\in \mathbb{Q}[t]} \in \mathbb{Q}[t]$$

$$3(t^2 - 2t + 1) = 3 \cdot (t-1) \cdot (t-1)$$

zerfällt in linare Faktoren

$t^2 - 2 \in \mathbb{Q}[t]$ zerfällt nicht in linare Faktoren
als Polynom aus dem
Ring $\mathbb{Q}[t]$

$t^2 - 2 \in \mathbb{R}[t]$ zerfällt in linare Faktoren
als Element aus $\mathbb{R}[t]$

$$t^2 - 2 = (t - \sqrt{2}) \cdot (t + \sqrt{2}).$$

$t^2 + 1 \in \mathbb{R}[t]$ zerfällt nur in lin. Fakt. im $\mathbb{R}[t]$

$$\underbrace{t^2 + 1}_{\text{zerfällt in Lin. Fakt. in diesem Ring.}} = (t - i)(t + i) \in \mathbb{C}[t]$$

Thm Sei $F: V \rightarrow V$ lineare Abbildung auf einem VR V der Dimension $n \in \mathbb{N}$. Dann gilt:

(i) Ist F diagonalisierbar, so zerfällt P_F in linare Faktoren.

(ii) Ist P_F Produkt von Linearfaktoren

$P_F = (t - \mu_1) \cdots (t - \mu_n)$ mit paarweise
verschiedenen $\mu_1, \dots, \mu_n \in K$, so ist

F diagonalisierbar.

Basis:

(i) Sei F diagonalisierbar. Dann gibt es eine Basis \mathcal{B} von V , für die $F_{\mathcal{B}}$ diagonal ist, d.h.

$$F_{\mathcal{B}} = \begin{bmatrix} \mu_1 & & \\ & \ddots & 0 \\ 0 & \cdots & \mu_n \end{bmatrix}$$

mit $\mu_1, \dots, \mu_n \in K$. \Rightarrow

$$P_F(t) = P_{F_{\mathcal{B}}}(t) = \det(tI - F_{\mathcal{B}})$$

$$= \det \begin{bmatrix} t - \mu_1 & & \\ & \ddots & 0 \\ 0 & \cdots & t - \mu_n \end{bmatrix} = (t - \mu_1) \cdots (t - \mu_n)$$

(ii) Ist $P_F = (t - \mu_1) \cdots (t - \mu_n)$ mit paarweise verschiedenen $\mu_1, \dots, \mu_n \in K$, so sind μ_1, \dots, μ_n n verschiedene Nullstellen

von P_F und damit n verschiedene Eigenwerte von F . Wir wissen, dass die jeweiligen n Eigenvektoren zu μ_1, \dots, μ_n linear unabhängig sind und somit eine Basis von V bilden. $\Rightarrow F$ diagonalisierbar.

wurde hier implizit benutzt.



$$F(x) = \lambda x \Leftrightarrow F_{\mathcal{B}} \cdot x_{\mathcal{B}} = \lambda \cdot x_{\mathcal{B}}$$

Eigenwertaufgabe
für $F: V \rightarrow V$

Eigenwert angebe
für $F_{\mathcal{B}} \in K$

6.3.2

Vielfachheit von Nullstellen des
charakteristischen Polynoms.

Prop

Sei $\lambda \in \mathbb{K}$ Nullstelle eines Polynoms

$f \in \mathbb{K}[t]$ mit $\deg f \geq 1$. Dann existiert
eine eindeutige Zahl $r \in \mathbb{N}$ mit

$$f(t) = (t - \lambda)^r \cdot g(t),$$

wobei $g \in \mathbb{K}[t]$ ein Polynom ist,
das $g(\lambda) \neq 0$ erfüllt.

Beweis: Aufgabe.

Die Zahl r aus der vorigen Proposition nennt
man die (algebraische) Vielfachheit der
Nullstelle λ von f .

Prop

Sind $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ paarweise verschiedene
Nullstellen eines Polynoms $f \in \mathbb{K}[t]$ mit $\deg f \geq 1$,
so kann f eindeutig als

$$f = (t - \lambda_1)^{r_1} \cdot \dots \cdot (t - \lambda_k)^{r_k} \cdot g$$

mit $r_1, \dots, r_k \in \mathbb{N}$, $g \in \mathbb{K}[t]$ und $g(\lambda_i) \neq 0$

:

$$g(\lambda_k) \neq 0.$$

Insgesamt, wenn $\lambda_1, \dots, \lambda_k$ alle Nullstellen
von f in \mathbb{K} sind, ist das die eindeutige
Darstellung von f bis auf die Numerierung
der Nullst. □

Beweis: Aufgabe.

Bem.

Wie findet man alle Nullstellen eines Polynoms?

\mathbb{K} endlich \Rightarrow man kann im Prinzip alle
Elemente aus \mathbb{K} durchprobieren.
Es ist nicht immer zulässig.

In der Kryptographie hat man standard
körper mit $|\mathbb{K}| \approx 10^{80}$.

$$K = \mathbb{Q} : \quad at^2 + bt + c = 0 \quad (a, b, c \in \mathbb{Z}).$$

Sei $\frac{u}{v}$ Nullstelle dieses Polynoms

mit $u \in \mathbb{Z}$, $v \in \mathbb{N}$ und $\gcd(u, v) = 1$.

$$\Rightarrow a \cdot \left(\frac{u}{v}\right)^2 + b \cdot \frac{u}{v} + c = 0$$

$$\Rightarrow a \cdot u^2 + b \cdot u \cdot v + c v^2 = 0$$

$$\Rightarrow \begin{cases} cv^2 \equiv 0 \pmod{u} \\ au^2 \equiv 0 \pmod{v} \end{cases}$$

$$\Rightarrow \begin{cases} cv^2 \text{ durch } u \text{ teilbar} \\ au^2 \text{ durch } v \text{ teilbar} \end{cases}$$

$$\Rightarrow \begin{cases} c \text{ ist durch } u \text{ teilbar} \\ a \text{ ist durch } v \text{ teilbar.} \end{cases}$$

\Rightarrow + Teiler a ist zudem auch für den Nenner v

\pm Teiler von c ist zudem auch für den Zähler u .