

Moodle: jil2189VQT

H25T1A2 Sei p eine Primzahl, $n \in \mathbb{N}$,
 $q = p^n$ und $\mathbb{F}_q$ der Körper mit q Elementen.
(Achtung: $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$ falls $n > 1$)

(a) Zeigen Sie: $|GL_2(\mathbb{F}_q)| = (q-1)^2 q (q+1)$ (Ü)

Laut Vorlesung ist eine Matrix $A \in M_{2, \mathbb{F}_q}$
genau dann invertierbar, wenn die beiden
Spalten $v, w \in \mathbb{F}_q^2$ linear unabhängig

sind (wegen dem $\mathbb{F}_q^2 = 2$ gleichbedeutend: eine Basis von $\mathbb{F}_q^2$ bilden). Jedes solche System (v, w) kann gebildet werden, indem man zunächst $v \in \mathbb{F}_q^2 \setminus \{0_{\mathbb{F}_q^2}\}$ wählt und dann w so hinzufügt, dass (v, w) linear unabhängig ist. (Dies folgt aus dem Basisergänzungssatz.)

(Dieselben Aussagen gelten auch für beliebiges n an Stelle von $n=2$. Insbesondere: Ist $\{v_1, \dots, v_k\}$ ein linear unabhängiges System in $\mathbb{F}_q^n$ mit $k \leq n$, so kann dieses zu einer Basis von $(\mathbb{F}_q)^n$

ergänzt werden.)

Es genügt also, die Anzahl linear unabh. Paare (v, w) in $\mathbb{F}_q^2$ zu bestimmen

$|\mathbb{F}_q^2 \setminus \{0_{\mathbb{F}_q}\}| = q^2 - 1 \Rightarrow q^2 - 1$ Möglichkeiten für die Wahl von v

Ist $v \in \mathbb{F}_q^2 \setminus \{0\}$ vorgeg., so ist (v, w) für $w \in \mathbb{F}_q^2$ genau dann linear unabhängig, wenn $w \notin \langle v \rangle_{\mathbb{F}_q}$ gilt. $\dim \langle v \rangle_{\mathbb{F}_q} = 1 \Rightarrow |\langle v \rangle_{\mathbb{F}_q}| = q^1 = q$

$$\Rightarrow |\mathbb{F}_q^2 \setminus \langle v \rangle_{\mathbb{F}_q}| = q^2 - q \Rightarrow \text{noch } q^2 - q$$

Möglichkeiten für die Wahl von w .

Die Anzahl der linear unabh. Paare (v, w) beträgt also $(q^2-1)(q^2-q) \xrightarrow{\text{s.o.}}$

$$\begin{aligned} |GL_2(\mathbb{F}_q)| &= (q^2-1)(q^2-q) = (q^2-1) \cdot q \cdot (q-1) \\ &= (q-1) \cdot (q+1) \cdot q \cdot (q-1) = (q-1)^2 \cdot q \cdot (q+1) \quad \square \end{aligned}$$

Übung (a) Bestimmen Sie $|GL_3(\mathbb{F}_q)|$.

(b) Zeigen Sie, dass für alle $n \in \mathbb{N}$

$$|GL_n(\mathbb{F}_q)| = q^{\frac{1}{2}n(n-1)} \prod_{k=1}^n (q^k - 1) \text{ gilt.}$$

Diagonalisierbarkeit

Def. V endl.-dim. K -Vektorraum (K Körper), $\phi \in \text{End}_K(V)$

(i) $\lambda \in K$ Eigenwert von ϕ ~~==~~

$\exists v \in V \setminus \{0_v\}$ mit $\phi(v) = \lambda v$

(äquivalente Bed.: Der Eigenraum zum Wert λ geg. durch $\text{Eig}(\phi, \lambda) = \{v \in V \mid \phi(v) = \lambda v\}$ ist ungleich $\neq \{0_v\}$.)

(ii) Eigenvektor von ϕ zum Eigenwert λ
= Vektor $v \in V \setminus \{0_v\}$ mit $\phi(v) = \lambda v$
= Element der Menge $\text{Eig}(\phi, \lambda) \setminus \{0_v\}$

(iii) char. Polynom χ_A einer Matrix $A \in M_{n,K} (n \in \mathbb{N}) = \det(xE - A) \in K[x]$

$\uparrow$ Einheitsmatrix

Das char. Polynom von ϕ ist geg. durch $\chi_\phi = \chi_A$, wobei $A = M_B(\phi)$ für eine beliebige geordnete Basis B von V .

(iv) algebraische Vielfachheit $\mu_a(\phi, \lambda)$
eines Eigenwerts $\lambda \in K$ von ϕ
= Vielfachheit von λ als Nullstelle
von χ_ϕ

(v) geometrische Vielfachheit $\mu_g(\phi, \lambda)$
= Dimension von $\text{Eig}(\phi, \lambda)$

Def: i) Man nennt eine Matrix $A \in M_{n,k}$ diagonalisierbar, wenn sie ähnlich zu einer Diagonalmatrix ist (d.h. es gibt eine Diagonalmatrix $D \in M_{n,k}$ und ein $T \in GL_n(K)$ mit $D = T A T^{-1}$).

ii) Man nennt $\phi \in \text{End}_K(V)$ diagonalisierbar, wenn eine geordnete Basis B von V existiert, so dass $M_B(\phi)$ eine Diagonalmatrix ist.

Erkennung: Ist B eine beliebige geordnete Basis von V , dann gilt die Äquivalenz
 ϕ diagonalisierbar $\iff M_B(\phi)$ diagonalisierbar.

Diagonalisierbarkeitskriterium:

Genau dann ist $\phi \in \text{End}_K(V)$ diagonalisierbar, wenn gilt

- (i) χ_ϕ zerfällt in $K[x]$ in Linearfaktoren
- (ii) Für jeden Eigenwert λ von ϕ gilt $m_\phi(\phi, \lambda) = m_\alpha(\phi, \lambda)$.

(Erinnerung: Für jeden Eigenwert gilt
immer $1 \leq m_\phi(\phi, \lambda) \leq m_\alpha(\phi, \lambda)$.)

Übungen:

(i) zur Diagonalisierbarkeit: H16T2A3

(ii) zur Jordanschen Normalform (Beispiele)

H14T2A5, H13T1A3

(iii) zur Jordanschen Normalform (Theorie)

F20T2A1

F16T2AS Sei $A \in M_{4, \mathbb{Q}}$ gegeben durch

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

- (a) Berechnen Sie das char. Pol. $\chi_A \in \mathbb{Q}[x]$, bestimmen Sie die Eigenwerte von A und prüfen Sie, ob A diagonalisierbar ist.

$$\chi_A = \det(xE - A) = \det \begin{pmatrix} x & -1 & 0 & 0 \\ 1 & x+2 & 0 & 0 \\ 0 & 0 & x+1 & 0 \\ -2 & -2 & -2 & \boxed{x+1} \end{pmatrix}$$

Entwicklung
zur 4. Spalte

$$(x+1) \det \begin{pmatrix} x & -1 & 0 \\ 1 & x+2 & 0 \\ 0 & 0 & x+1 \end{pmatrix} = \det \begin{pmatrix} x & -1 & 0 \\ 1 & x+2 & 0 \\ 0 & 0 & x+1 \end{pmatrix}$$

Sarrus
=

$$\begin{aligned}
 & x(x+2)(x+1) + 0 + 0 - 0 - 0 - (x+1)(-1) = \\
 & x(x^2 + 3x + 2) + x + 1 = x^3 + 3x^2 + 3x + 1 \\
 & = (x+1)^3 \Rightarrow \chi_A = (x+1)^4 (*)
 \end{aligned}$$

$\Rightarrow$ einzige Nullstelle von χ_A : -1

$\rightarrow -1$ ist einziger Eigenwert von A

Diagonalisierbarkeit: Die Gleichung (*) zeigt, dass χ_A in Linearfaktoren zerfällt und $m_A(A, -1) = 4$ ist. Auf Grund des Diagonalisierbarkeitskriteriums ist A also genau dann diagonalisierbar, wenn $m_g(A, -1) = 4$ gilt.

[Berechnung von $\mu_g(A, -1) = \dim \operatorname{Eig}(A, -1)$
 $= \dim \ker(A - (-1)E) = \dim \ker(A + E)$:

Forme $A + E$ mit dem Gaußverfahren auf Zeilen-
 stufenform um. Ist dann r die Anzahl der Zeilen
 ungleich null in der ZSF, dann gilt $\dim \ker(A + E)$
 $= 4 - r$]

erigt,

(A, -1)

rkeits-

lisis -

Es gilt die Äquivalenz $\mu_g(A, -1) = 4 \iff$

$\dim \ker(A - (-1)E) = 4 \iff \dim \ker(A + E) = 4$

$\iff \ker(A + E) = \mathbb{Q}^4 \iff \forall v \in \mathbb{Q}^4: (A + E)v = 0_{\mathbb{Q}^4}$

$\iff$ alle Spalten von $A + E$ sind null $\iff A + E = 0$

$\Leftrightarrow A = -E$ Es gilt aber $A \neq -E$.

Also gilt $\mu_g(A, -1) < 4$, Somit ist A nicht diagonalisierbar.

Erinnerung: Satz von Cayley-Hamilton

Für jede Matrix $A \in M_{n,K}$ ($n \in \mathbb{N}$, K Körper)

gilt $\chi_A(A) = 0_{M_{n,K}}$. (Ist $f \in K[x]$,

$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, dann ist nach

Def $f(A) = a_n A^n + a_{n-1} A^{n-1} + \dots + a_1 A + a_0 E$.)

Def. Sei $A \in M_{n,K}$. Das Minimalpolynom m_A von A ist das eindeutig bestimmte, normierte Polynom in $K[x]$ minimalen Grades mit der Eigenschaft $m_A(A) = 0_{M_{n,K}}$.

Wichtige Eigenschaft: Ist $f \in K[x]$

mit $f(A) = 0_{M_{n,K}}$, dann gilt $m_A \mid f$

(d.h. m_A ist Teiler von f) Aus dem Satz von Cayley-Hamilton folgt also $m_A \mid \chi_A$.

Beispiele: (i) $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in M_{2,\mathbb{Q}}$

$$\chi_A = \det \begin{pmatrix} x-2 & -1 \\ 0 & x-2 \end{pmatrix} = (x-2)^2$$

Wegen $M_A \mid \chi_A$ und $\text{grad } M_A \geq 1$ gilt

$$M_A = (x-2)^j \text{ für ein } j \in \{1, 2\}.$$

Ang. $j=1$. $M_A = x-2$ $M_A(A) = 0_{M_{2,\mathbb{Q}}}$

$$\Rightarrow A - 2E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Also muss $M_A = (x-2)^2$ gelten.

iii) $B = 2E = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

Hier gilt $\chi_B = (x-2)^2$, $M_B = x-2$.

(b) Bestimmen Sie einen Erzeuger
des Ideals $J_A = \{g \in \mathbb{Q}[x] \mid g(A) = 0_{M_{r, \mathbb{Q}}}\}$.

Da $\mathbb{Q}[x]$ ein Hauptidealring ist, be-
sitzt J_A ein erzeugendes Element, also
ein $r \in \mathbb{Q}[x]$ mit $J_A = (r) = \{h \cdot r \mid$
 $h \in \mathbb{Q}[x]\}$. Satz v. Cayley-Hamilton

$$\Rightarrow \chi_A(A) = 0_{M_{r, \mathbb{Q}}} \Rightarrow \chi_A \in J_A$$

$\Rightarrow J_A \neq (0)$ Also gilt $r \neq 0$ und

$r \mid \chi_A$ für jedes erzeugende Element

$r \in \mathbb{Q}[x]$ von J_A . Da sich (r) bei

Nur

norm
zeuge

$\Rightarrow$

$g=0$

Null

ist

Ang

$\Rightarrow$

$(A+E$

Also

Normierung nicht ändert, existiert ein
normiertes Polynom $r \in \mathbb{Q}[x]$ als Er-
zeugendes. $\chi_A = (x+1)^4$, $r \mid \chi_A$, r normiert

$\Rightarrow r = (x+1)^j$ für ein $j \in \{0, 1, \dots, 4\}$
 $j=0$ ist ausgeschlossen, da A keine
Nullstelle des konstanten Polynoms $1 \in \mathbb{Q}[x]$
ist

Ang $j=1 \rightarrow A$ Nullstelle von $x+1$
 $\Rightarrow A+E=0$ (siehe oben)

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

Also ist $r = (x+1)^2$ das gesuchte Polynom $\square$