

F17T1AS

(a) zeigen Sie: Ist p eine Primzahl,
 $n \in \mathbb{N}$, $A \in M_{n, \mathbb{F}_p}$ eine Matrix mit
irreduziblem char. Polynom $\chi_A \in \mathbb{F}_p[x]$, dann
ist A über $\mathbb{F}_{p^n}$ diagonalisierbar.

Sei $A \in M_{n, \mathbb{F}_p}$ wie angeg. Laut Vorlesung
genügt es zu zeigen:

- (i) χ_A zerfällt über $\mathbb{F}_{p^n}$ in Linearfaktoren
- (ii) Für jeden Eigenwert $\lambda \in \mathbb{F}_{p^n}$ von A gilt
 $M_g(A, \lambda) = m_a(A, \lambda)$, d.h. die geometri-

Sei Vielfachheit ist gleich der algebraischen.

zu i) Es reicht zu zeigen, dass jede Nullstelle von χ_A in einem alg. Abschluss $\mathbb{F}_p^{\text{alg}}$ von A bereits in $\mathbb{F}_{p^n}$ liegt. Sei also $\lambda \in \mathbb{F}_p^{\text{alg}}$ mit $\chi_A(\lambda) = 0$. χ_A irred. in $\mathbb{F}_p[x]$ und normiert

$$\Rightarrow \chi_A = M_{\lambda, \mathbb{F}_p}, A \in M_{n, \mathbb{F}_p} \Rightarrow \text{grad } \chi_A = n$$

$$\Rightarrow [\mathbb{F}_p(\lambda) : \mathbb{F}_p] = \text{grad } \chi_A = n$$

$$\Rightarrow \mathbb{F}_p(\lambda) = \mathbb{F}_{p^n} \Rightarrow \lambda \in \mathbb{F}_{p^n}$$

zu ii) Als irreduzibles Polynom über einem endlichen Körper ist χ_A separabel, hat also in jedem

Erw.-korp. von $\mathbb{F}_p$ nur einfache Nullstellen

$\Rightarrow \mu_a(A, \lambda) = 1$ für jeden Eigenwert $\lambda \in \mathbb{F}_{p^n}$ von A

Weil für alle Eigenwerte $1 \leq \mu_g(A, \lambda) \leq \mu_a(A, \lambda)$ gilt, folgt daraus $\mu_g(A, \lambda) = 1 = \mu_a(A, \lambda)$.

(b) Sei $A \in M_{3, \mathbb{F}_5}$ geg. durch $A = \begin{pmatrix} -1 & 3 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Zeigen Sie, dass A nicht über $\mathbb{F}_{125}$, aber über $\mathbb{F}_{25}$ diagonalisierbar ist.

$$\text{Es ist } \chi_A = x^3 + x^2 + x + 2 \quad \chi_A(1) = \bar{5} = \bar{0}$$

$$(x-1) \mid \chi_A \quad \text{Polynomdiv.} \Rightarrow \chi_A = (x-1)(x^2 + 2x + 3)$$

Sei $g = x^2 + 2x + \bar{3}$. $g(\bar{0}) = \bar{3} \neq \bar{0}$, $g(\bar{1}) = \bar{1} \neq \bar{0}$,
 $g(\bar{2}) = \bar{1} \neq \bar{0}$, $g(\bar{3}) = \bar{3} \neq \bar{0}$, $g(\bar{4}) = \bar{2} \neq \bar{0}$.
 g hat in $\mathbb{F}_5$ keine Nullst., $\text{grad}(g) = 2 \Rightarrow g$ ist irreduzibel in $\mathbb{F}_5[x]$

Da g ein normiertes irred. Polynom in $\mathbb{F}_5[x]$ vom Grad 2 ist, liegt jede Nullstelle $\lambda \in \mathbb{F}_5^{\text{alg}}$ von g bereits in $\mathbb{F}_{25}$, denn: g normiert, irred in $\mathbb{F}_5[x]$, $g(\lambda) = 0 \Rightarrow g = M_{\lambda, \mathbb{F}_5} \Rightarrow$
 $[\mathbb{F}_5(\lambda) : \mathbb{F}_5] = \text{grad}(g) = 2 \Rightarrow \mathbb{F}_5(\lambda) = \mathbb{F}_{25} \Rightarrow \lambda \in \mathbb{F}_{25}$

Also zerfallen g und χ_A über $\mathbb{F}_{25}$ in Linearfaktoren. Da g in $\mathbb{F}_5[x]$ irreduzibel ist, liegen die Nullstellen von g nicht in $\mathbb{F}_5$, sind also ungleich T . Da g als irred. Polynom über $\mathbb{F}_5$ separabel ist, sind die beiden Nullstellen von g in $\mathbb{F}_{25} \setminus \mathbb{F}_5$ verschieden. Insgesamt hat χ_A also in $\mathbb{F}_{25}$ nur einfache Nullst. $\Rightarrow$

$m_g(A, \lambda) = m_A(A, \lambda) = 1$ für jeden Eigenwert $\lambda \in \mathbb{F}_{25}$ von A . Dies zeigt, dass A über $\mathbb{F}_{25}$ diagonalisierbar ist.

Um zu zeigen, dass A über $\mathbb{F}_{125}$ nicht diagonalisierbar ist, zeigen wir, dass χ_A über $\mathbb{F}_{125}$ nicht in Linearfaktoren zerfällt. Ang., χ_A zerfällt über $\mathbb{F}_{125}$. Dann liegen auch die Nullst. $\lambda_1, \lambda_2 \in \mathbb{F}_{125}$ von g in $\mathbb{F}_{125}$. $\Rightarrow \mathbb{F}_5(\lambda_1)$ ist Zwischentyp von $\mathbb{F}_{125} | \mathbb{F}_5$. Gradformel $\Rightarrow 3 = [\mathbb{F}_{125} : \mathbb{F}_5] = [\mathbb{F}_{125} : \mathbb{F}_5(\lambda_1)] \cdot [\mathbb{F}_5(\lambda_1) : \mathbb{F}_5]$ $g = \text{Min. Pol. (s.o.)}$ $\Rightarrow [\mathbb{F}_5(\lambda_1) : \mathbb{F}_5] = \text{grad}(g) = 2$.

in $\mathbb{F}_{125}$
 f norm
 $[\mathbb{F}_5(\lambda_1) : \mathbb{F}_5] = 2$
 und $[\mathbb{F}_{125} : \mathbb{F}_5(\lambda_1)] = 3$
 $f(x)$
 $\varphi(1)$
 $\Rightarrow 1$
 $\varphi(x) =$
 $= 0$
 matrix
 für B

einsetzen $\Rightarrow 3 = [\mathbb{F}_{25} : \mathbb{F}_5(\alpha)] \cdot 2 \nmid$ da $2 \nmid 3$



F21T3A5 (Übung: H22T3A4)

Geben Sie eine Darstellungsmatrix des Frobenius-Automorphismus von $\mathbb{F}_{25} / \mathbb{F}_5$ bzgl. einer Basis des $\mathbb{F}_5$ -Vektorraums $\mathbb{F}_{25}$ an (mit Nachweis)

Frobenius-Automorphismus von $\mathbb{F}_{25} / \mathbb{F}_5 =$
Abbildung $\varphi: \mathbb{F}_{25} \rightarrow \mathbb{F}_{25}, \alpha \mapsto \alpha^5$

Sei $f = x^2 + \bar{3} \in \mathbb{F}_5[x]$. Das Polynom hat in $\mathbb{F}_5$ keine Nullst. ($f(\bar{0}) = \bar{3} \neq \bar{0}$, $f(\bar{1}) = \bar{4} \neq \bar{0}$, $f(\bar{2}) = \bar{2} \neq \bar{0}$, $f(\bar{3}) = \bar{2} \neq \bar{0}$, $f(\bar{4}) = \bar{4} \neq \bar{0}$), ist wegen $\deg(f) = 2$ also irred. Sei α eine Nullstelle von f

nicht
lass
oren
 $\mathbb{F}_{125}$
e $\mathbb{F}_{25}$
Zwi-
formel
(2.1) J.
(s.o.)
2.

in einem alg. Abschluss $\mathbb{F}_5^{\text{alg}} \supseteq \mathbb{F}_{25}$ von $\mathbb{F}_5$.
 f normiert, irred., $f(r) = \bar{0} \Rightarrow f = m_{\gamma, \mathbb{F}_5} \Rightarrow$
 $[\mathbb{F}_5(\gamma) : \mathbb{F}_5] = \text{grad}(f) = 2 \Rightarrow \mathbb{F}_5(\gamma) = \mathbb{F}_{25}$,
und $\{1, \gamma\}$ ist eine Basis von $\mathbb{F}_{25}$ als $\mathbb{F}_5$ -Vektorraum

$$f(\gamma) = \bar{0} \Rightarrow \gamma^2 = -\bar{3} = \bar{2}$$

$$\varphi(\bar{1}) = \bar{1}^5 = \bar{1} = \underline{\bar{1}} \cdot \bar{1} + \underline{\bar{0}} \cdot \gamma$$

$\Rightarrow$ 1. Spalte der Darstellungsmatrix ist $\begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}$

$$\varphi(\gamma) = \gamma^5 = (\gamma^2)^2 \cdot \gamma = \bar{2}^2 \cdot \gamma = \bar{4} \gamma$$

$= \bar{0} \cdot \bar{1} + \bar{4} \cdot \gamma \Rightarrow$ 2. Spalte der Darstellungsmatrix ist $\begin{pmatrix} \bar{0} \\ \bar{4} \end{pmatrix}$ insgesamt: $M_B(\varphi) = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{4} \end{pmatrix}$

für $B = (\bar{1}, \gamma)$. □

Def normale Körpererweiterung = Erweiterung
L/K von Körpern mit der Eigenschaft, dass
jedes über K irreduzible Polynom, das in L eine
Nullstelle besitzt, über L in Linearfaktoren
zerfällt

- Jede Ers. von Grad 2 ist normal.
- Die Ers. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal.

(denn: Das Pol. $x^3 - 2 \in \mathbb{Q}[x]$ ist über $\mathbb{Q}$ irred.,
hat in $\mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle, zerfällt aber über
 $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren.)

Nullstelle besitzt, über L in Linearfaktoren

- Eine endliche Erz. L/K ist genau dann normal, wenn L Zerfällungskörper eines Polynoms $f \in K[X]$ über K ist.

Def Sei $f \in K[X]$ ein irred. Polynom und L/K eine Körpererweiterung.

- f separabel $\Leftrightarrow f$ hat in jeder Erz. von K nur einfache Nullst $\Leftrightarrow \text{ggT}(f, f') = 1$
- X ist separabel über $K \Leftrightarrow X$ ist algebraisch über K , und das Min. pol. $\mu_{X,K}$ ist separabel
- L/K ist separabel $\Leftrightarrow$ Jedes $\alpha \in L$ ist separabel über K .

• Ist $\text{char}(K) = 0$ oder ist K endlich, dann ist jede alg. Erweiterung von K separabel.

• Ist p eine Primzahl und $\mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$, dann ist $\mathbb{F}_p(t) \mid \mathbb{F}_p(t^p)$ eine algebraische, aber nicht separable Erweiterung
$$(M_{t, \mathbb{F}_p(t^p)} = x^p - t^p = (x-t)^p)$$

• Satz vom primitiven Element:

Jede endliche, separable Erweiterung L/K ist einfach, d.h. es gibt ein $\gamma \in L$ mit $L = K(\gamma)$.

tionenkörper über $\mathbb{F}_p$, dann ist $\mathbb{F}_p(t) \mid \mathbb{F}_p(t^p)$ eine algebraische, aber nicht separable Erweiterung.

F13T2A4 Sei $K = \mathbb{F}_5(\sqrt[4]{3})$, d.h.

$K = \mathbb{F}_5(\alpha)$, wobei $\alpha \in \mathbb{F}_5^{\text{alg}}$ ein Element mit $\alpha^4 = \bar{3}$ bezeichnet. Zeigen Sie, dass $K \mid \mathbb{F}_5$ galois'sch ist (also normal und separabel); bestimmen Sie alle Zwischenkörper von $K \mid \mathbb{F}_5$ mit allen Inklusionen und bestimmen Sie die Anzahl der Elemente $\beta \in K$ mit $K = \mathbb{F}_5(\beta)$. Als Nullstelle des Polynoms $f = x^4 - \bar{3}$ ist α algebraisch über $\mathbb{F}_5 \Rightarrow K = \mathbb{F}_5(\alpha) \mid \mathbb{F}_5$ ist algebraische Erweiterung. Da $\mathbb{F}_5$ ein endlicher Körper ist, ist sie somit auch separabel. Sei $n = \text{grad } \mu_{\alpha, \mathbb{F}_5} \Rightarrow [\mathbb{F}_5(\alpha) : \mathbb{F}_5] = n \Rightarrow K = \mathbb{F}_5^n$.

Nullstelle besitzt, über L in Linearfaktoren

Laut VI. ist $\mathbb{F}_5$ der Zerfällungskörper des Polynoms $x^{5^n} - x$ über $\mathbb{F}_5$ und die Erweiterung $\mathbb{F}_5 \mid \mathbb{F}_5$ somit normal. (alternativ: Ist $E \mid F$ eine Körpererw. und E, F beide endlich, dann ist $E \mid F$ lt. VI. normal.)

A
in
Da
se