Aufgabe H15T3A3 (4+6+5 Punkte)

Betrachten Sie das Polynom $f = x^2 + x + \bar{1} \in \mathbb{F}_5[x]$.

(a) Zeigen Sie, dass $K = \mathbb{F}_5[x]/(f)$ ein Körper mit 25 Elementen ist.

(b) Bestimmen Sie ein Element $w \in K$ mit $w^2 = \bar{2}$.

(c) Zeigen Sie, dass die Matrix
$$A \quad = \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathcal{M}_{2\times 2,\mathbb{F}_5}$$
über K diagonalisierbar ist.

Lösung:

zu (a) Es gilt $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{3}$, $f(\bar{2}) = \bar{7} = \bar{2}$, $f(\bar{3}) = \overline{13} = \bar{3}$ und $f(\bar{4}) = \overline{21} = \bar{1}$. Das Polynom f hat also in $\mathbb{F}_5$ keine Nullstellen. Wegen $\mathrm{grad}(f) = 2$ folgt daraus, dass f irreduzibel ist. Weil $\mathbb{F}_5[x]$ als Polynomring über einem Körper ein Hauptidealring und f ein irreduzibles Element ist, ist das Hauptideal (f) ein maximales Ideal. Daraus wiederum folgt, dass der Restklassenring K ein Körper ist.

Wir zeigen nun noch, dass durch $S = \{a + bx \mid a, b \in \mathbb{F}_5\}$ ein Repräsentantensystem vom K gegeben ist; daraus ergibt sich dann $|K| = |S| = 25$. Zu überprüfen ist, dass jede Restklasse $g + (f) \in K$ mit $g \in \mathbb{F}_5[x]$ genau einen Repräsentanten aus S enthält. Dividieren wir ein vorgegebenes $g \in \mathbb{F}_5[x]$ durch f, so erhalten wir Polynome $q, r \in \mathbb{F}_5[x]$ mit $g = qf + r$ und $r = 0$ oder $\mathrm{grad}(r) < \mathrm{grad}(f) = 2$. In jedem Fall liegt r also in S, und aus $r + (f) = qf + r + (f) = g + (f)$ folgt $r \in g + (f)$. Nehmen wir nun an, dass $r_1 \in S$ ein weiteres Element in $g + (f)$ ist. Dann gilt $r + (f) = g + (f) = r_1 + (f)$, also $r_1 - r \in (f)$. Das Polynom f ist also ein Teiler von $r_1 - r$. Weil aber $r_1 - r$ beide entweder 0 oder vom Grad ≤ 1 sind und $\mathrm{grad}(f) = 2$ ist, muss $r_1 - r = 0$, also $r = r_1$ gelten. Also enthält $g + (f)$ tatsächlich genau ein Element aus S.

zu (b) Schreiben wir w in der Form $w = a + bx + (f)$ mit $a, b \in \mathbb{F}_5$, dann ist $w^2 = \bar{2}$ gleichbedeutend mit

$$(a + bx)^2 + (f) = 2 + (f) \quad \Leftrightarrow \quad a^2 + 2abx + b^2x^2 + (f) = \bar{2} + (f)$$
$$\Leftrightarrow \quad a^2 + 2abx - b^2(x+1) + (f) = \bar{2} + (f) \quad \Leftrightarrow \quad (a^2 - b^2) + (2ab - b^2)x + (f) = \bar{2} + (f)$$
$$\Leftrightarrow \quad a^2 - b^2 = \bar{2} \ \wedge \ \bar{2}ab - b^2 = \bar{0} \quad \Leftrightarrow \quad a^2 - b^2 = \bar{2} \ \wedge \ \bar{b}(\bar{2}a - b) = \bar{0}$$

Die zweite Gleichung liefert $b = 0$ oder $b = \bar{2}a$. Im Fall $b = \bar{0}$ wäre $a^2 = \bar{2}$, was aber in $\mathbb{F}_5$ nicht lösbar ist. Also bleibt nur $b = \bar{2}a$. Setzen wir dies in $a^2 - b^2 = \bar{2}$ ein, so erhalten wir $-\bar{3}\bar{a}^2 = a^2 - \bar{4}a^2 = \bar{2} \Leftrightarrow \bar{a}^2 = \bar{1} \Leftrightarrow \bar{a} \in \{\pm\bar{1}\}$. Im Fall $\bar{a} = \bar{1}$ ist $\bar{b} = 2$. Setzen wir $w = \bar{1} + \bar{2}x + (f)$, dann gilt tatsächlich $w^2 = (1 + \bar{2}x)^2 = \bar{1} + \bar{4}x + \bar{4}x^2 + (f) = \bar{1} + \bar{4}x - \bar{4}(\bar{1} + x) = \bar{1} - \bar{4} = \bar{2}$.

zu (c) Das charakteristische Polynom der Matrix A ist gegeben durch

$$\begin{aligned} \chi_A \quad &= \quad \det(xE_2 - A) \quad = \quad \det \begin{pmatrix} x - \bar{1} & -\bar{2} \\ -\bar{3} & x - \bar{4} \end{pmatrix} \quad = \quad (x - \bar{1})(x - \bar{4}) - (-\bar{2})(-\bar{3}) \\ &= \quad x^2 - \bar{5}x + \bar{4} - \bar{6} \quad = \quad x^2 - \bar{2}. \end{aligned}$$

Wie wir in Teil (b) gesehen haben, ist $w = \bar{2} + (f)$ eine Nullstelle von χ_A, und $-w$ ist wegen $(-w)^2 = (-\bar{1})^2 w^2 = \bar{2}$ eine weitere, die wegen $\bar{2}w \neq 0$ von w verschieden ist. Es gilt also $\chi_A = (x-w)(x+w)$, und die Matrix A hat in K die beiden verschiedenen Eigenwerte $\pm w$. Die algebraische Vielfachheit von $\pm w$ ist jeweils gleich 1, die geometrische Vielfachheit muss (mindstens) 1 sein. Insgesamt zerfällt χ_A also über K in Linearfaktoren, und die geometrische Vielfachheit jedes Eigenwerts ist gleich der algebraischen. Daraus folgt, dass A über K diagonalisierbar ist.