

H22-T3-A4

Sei $K = \mathbb{Z}[X]/(X^5 + 2, X^4 + X^3 + X^2 + X + 1)$.

- Beweisen Sie, dass $3 \in (X^5 + 2, X^4 + X^3 + X^2 + X + 1)$ gilt.
- Zeigen Sie, dass K ein Körper ist.
- Beweisen Sie, dass K eine Galoiserweiterung seines Primkörpers \mathbb{F}_3 ist und bestimmen Sie die Galoisgruppe von $K|\mathbb{F}_3$.
- Sei x die Restklasse von X in K . Zeigen Sie, dass $\{x, x^3, x^9, x^{27}\}$ eine \mathbb{F}_3 -Basis von K ist und bestimmen Sie die Darstellungsmatrizen der Elemente der Galoisgruppe $\text{Gal}(K|\mathbb{F}_3)$ bzgl. dieser Basis.

Lösungsvorschlag. Zu a) Es ist $\Phi_5 = X^4 + X^3 + X^2 + X + 1$ und bekanntlich gilt

$$X^5 - 1 = (X - 1) \cdot \Phi_5,$$

sodass wir erhalten:

$$3 = (X^5 + 2) - (X^5 - 1) = (X^5 + 2) - (X - 1) \cdot \Phi_5 \in (X^5 + 2, \Phi_5).$$

Zu b) Wegen der Darstellung der 3 aus Teilaufgabe a) gilt

$$(X^5 + 2, \Phi_5) = (3, \Phi_5).$$

Dann folgt:

$$K = \mathbb{Z}[X]/(3, \Phi_5) \cong \mathbb{F}_3[X]/(\Phi_5).$$

Es genügt zu zeigen, dass $(\Phi_5) \subset \mathbb{F}_3[X]$ ein maximales Ideal ist. Da $\mathbb{F}_3[X]$ ein Hauptidealbereich ist, ist das genau dann der Fall, wenn Φ_5 über \mathbb{F}_3 irreduzibel ist. Man überprüft schnell, dass Φ_5 keine Nullstellen in \mathbb{F}_3 hat, sodass wir nur noch (oBdA normierte) Teiler von Grad 2 ausschließen müssen. Seien also $X^2 + aX + b, X^2 + cX + d \in \mathbb{F}_3[X]$ mit

$$(X^2 + aX + b) \cdot (X^2 + cX + d) = \Phi_5.$$

Ein Koeffizientenvergleich von

$$X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd = X^4 + X^3 + X^2 + X + 1$$

ergibt

$$a + c = 1, \tag{1}$$

$$b + d + ac = 1, \tag{2}$$

$$ad + bc = 1, \tag{3}$$

$$bd = 1. \tag{4}$$

Aus (4) folgt $b = d = 1$ oder $b = d = -1$. Letzteres eingesetzt in (3) ergibt einen Widerspruch zu (1). Setzen wir $b = d = 1$ in (2) ein, erhalten wir $ac = -1$, was $a = 1 = -c$ oder $a = -1 = -c$ liefert. Beides ist ein Widerspruch zu (1), sodass es keine Teiler von Grad 2 gibt und $\Phi_5 \in \mathbb{F}_3[X]$ irreduzibel ist.

Zu c) Es ist $K = \mathbb{F}_3(x)$ und Φ_5 das Minimalpolynom von x über \mathbb{F}_3 , sodass gilt

$$[K : \mathbb{F}_3] = \deg(\Phi_5) = 4.$$

Außerdem gilt für x^{3^i} mit $i = 1, 2, 3$

$$\Phi_5(x^{3^i}) = (x^4)^{3^i} + (x^3)^{3^i} + (x^2)^{3^i} + x^{3^i} + 1 = (x^4 + x^3 + x^2 + x + 1)^{3^i} = \Phi_5(x)^{3^i} = 0.$$

Die Elemente x, x^3, x^9, x^{27} sind paarweise verschieden, wie die Rechnung in Teilaufgabe d) zeigt. Wir sehen damit also, dass K der Zerfällungskörper des separablen Polynoms Φ_5 über \mathbb{F}_3 ist, daher ist $K|\mathbb{F}_3$ galoisch und die Galoisautomorphismen sind gegeben durch die Abbildungsvorschriften $x \mapsto x, x \mapsto x^3, x \mapsto x^9$ und $x \mapsto x^{27}$. Bekanntlich ist die Galoisgruppe endlicher Körper zyklisch mit Erzeuger $\sigma : x \mapsto x^3$, d.h. $\text{Gal}(K|\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$. Zu d) Offensichtlich ist $\{1, x, x^2, x^3\}$ eine \mathbb{F}_3 -Basis von K . Da x eine Nullstelle ist von Φ_5 , ist x ebenfalls eine Nullstelle von $X^5 - 1$, d.h. in K gilt $x^5 = 1$. Damit erhalten wir

$$x^9 = x^5 \cdot x^4 = -(x^3 + x^2 + x + 1)$$

und

$$x^{27} = (x^5)^5 \cdot x^2 = x^2.$$

Man erkennt damit leicht, dass $\{x, x^3, x^9, x^{27}\} = \{x, x^2, x^3, -(x^3 + x^2 + x + 1)\}$ ebenfalls eine \mathbb{F}_3 -Basis von K ist.

Um die Darstellungsmatrix M_σ von σ zu bestimmen, berechnen wir

- $\sigma(x) = x^3 = 0 \cdot x + 1 \cdot x^3 + 0 \cdot x^9 + 0 \cdot x^{27}$
- $\sigma(x^3) = (x^3)^3 = x^9 = 0 \cdot x + 0 \cdot x^3 + 1 \cdot x^9 + 0 \cdot x^{27}$
- $\sigma(x^9) = (x^3)^9 = x^{27} = 0 \cdot x + 0 \cdot x^3 + 0 \cdot x^9 + 1 \cdot x^{27}$
- $\sigma(x^{27}) = (x^3)^{27} = x^{81} = x = 1 \cdot x + 0 \cdot x^3 + 0 \cdot x^9 + 0 \cdot x^{27}$

und erhalten damit

$$M_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Da nach c) $\text{Gal}(K|\mathbb{F}_3)$ von σ erzeugt wird, ergeben sich damit die übrigen Darstellungsmatrizen

$$M_\sigma^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, M_\sigma^3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad M_\sigma^4 = E_4.$$