H10-T3-A5

Sei $P := X^4 + X + 2 \in \mathbb{F}_3[X]$ und $K = \mathbb{F}_3[X]/(P)$. Weiter sei a das Bild von X in K.

a) Zeigen Sie, dass K ein Körper mit 81 Elementen ist.

b) Bestimmen Sie explizit alle Teilkörper von K. Hierbei heiße "explizit": Die Angabe einer $\mathbb{F}_3$-Basís, wobei die Basiselemente Polynome in a vom Grad ≤ 3 sind. [Hinweis: Betrachten Sie $a^{10} \in K$.]

Lösungsvorschlag. Zu a). Offenbar genügt es hier, zu zeigen, dass P irreduzibel über $\mathbb{F}_3$ ist. Dazu beobachten wir, dass $P(0) = 2, P(1) = 1, P(2) = 2 \neq 0$ gilt, so dass P keine Nullstelle in $\mathbb{F}_3$ besitzt. Eine Zerlegung in irreduzible Faktoren über $\mathbb{F}_3$ müsste also aus zwei irreduziblen Faktoren von Grad 2 bestehen. Durch Auflisten aller Möglichkeiten und Testen auf Nullstellen in $\mathbb{F}_3$ ermitteln wir die (normierten) irreduziblen Polynome von Grad 3 über $\mathbb{F}_3$:

- X^2, $X^2 + X$, $X^2 + 2X$ – nicht irreduzibel, da 0 Nullstelle ist.
- $X^2 + 1$ – irreduzibel.
- $X^2 + 2$ – nicht irreduzibel (z.B. 1 ist Nullstelle).
- $X^2 + X + 1$ – nicht irreduzibel (z.B. 1 ist Nullstelle).
- $X^2 + 2X + 1 = (X + 1)^2$ – nicht irreduzibel.
- $X^2 + X + 2$ – irreduzibel.
- $X^2 + 2X + 2$ – irreduzibel.

Nun müssen wir lediglich noch überprüfen, ob eines dieser drei irreduziblen Polynome P teilt. Dazu berechnen wir

- $P \equiv 1 + X + 2 = X \neq 0 \not\equiv X^2 + 1$ – also teilt $X^2 + 1$ nicht P,
- $P \equiv (-X - 2)^2 + X + 2 = X^2 + X + 1 + X + 2 = X^2 + 2X \equiv X + 1 \not\equiv 0 \mod X^2 + X + 2$ – also teilt $X^2 + X + 2$ nicht P, und
- $P \equiv (-2X-2)^2+X+2 = X^2+2X+1+X+2 = X^2 \equiv X+1 \not\equiv 0 \mod X^2+2X+2$ – also teilt auch $X^2 + 2X + 2$ nicht P.

Somit ist P in der Tat irreduzibel in $\mathbb{F}_3[X]$ und $K = \mathbb{F}_3[X]/(P)$ damit ein Körper mit $|\mathbb{F}_3|^{\deg(P)} = 81$ Elementen.
Zu b). Nach Definition von K ist $K = \mathbb{F}_3(a)$. Aus der Theorie endlicher Körper wissen wir, dass die Galoisgruppe $G = \mathrm{Gal}(K|\mathbb{F}_3)$ zyklisch ist, also $G \simeq \mathbb{Z}_4$. Neben den trivilen Zwischenerweiterungen $\mathbb{F}_3$ (mit $\mathbb{F}_3$-Basis $\{1\}$) und K (mit der $\mathbb{F}_3$-Basis $\{1, a, a^2, a^3\}$) gibt es also genau eine echte Zwischenerweiterung Z, gegeben durch K^U, wenn $U \simeq \{0, 2\} \subset \mathbb{Z}_4$ die einzige echte Untergruppe von $G \simeq \mathbb{Z}_4$ ist. Weiter wissen wir, dass $Z^\times \subset K^\times$

zyklisch von Ordnung 8 sein muss, also die eindeutige Untergruppe der Ordnung 8 von $K^\times$. Wegen $[Z : \mathbb{F}_3] = 2$ genügt es aber wiederum, ein beliebiges Element $z \in Z \setminus \mathbb{F}_3$ zu finden, damit gilt $Z = \mathbb{F}_3(z)$, womit dann $\{1, z\}$ eine $\mathbb{F}_3$-Basis von Z ist. Anders gesagt möchten wir also ein $z \in Z^\times \setminus \mathbb{F}_3^\times$ finden – dazu können wir nun den Hinweis verwenden und $z := a^{10} \in K^\times$ betrachten. Wegen $|K^\times| = 80$ gilt $z^8 = 1$, das heißt $z \in Z^\times$. Wir rechnen außerdem noch nach

$$z = a^{10} = (a^4)^2 \cdot a^2 = (-a-2)^2 \cdot a^2 = (a^2+a+1)a^2 = a^4 + a^3 + a^2 = a^3 + a^2 - a - 2,$$

also $z \notin \mathbb{F}_3$. Also $Z = \mathbb{F}_3(z)$ mit $\mathbb{F}_3$-Basis $\{1, z = a^3 + a^2 - a - 2\}$.