Aufgabe F15T3A4 (4+6+6 Punkte)

Im Folgenden ist $L|K$ eine Körpererweiterung und ein Element $\alpha \in L$ gegeben. Bestimmen Sie jeweils das Minimalpolynom von α über dem Grundkörper K (mit Nachweis!).

(a) $K = \mathbb{Q}$, $L = \mathbb{C}$ und $\alpha = \sqrt{2} + \sqrt{3}$

(b) $K = \mathbb{F}_3$, $L = \mathbb{F}_3^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_3$ und α eine Nullstelle von $x^6 + 1$

(c) $K = \mathbb{Q}(\zeta + \zeta^{-1})$, $L = \mathbb{Q}(\zeta)$ und $\alpha = \zeta$ eine primitive p-te Einheitswurzel, wobei $p \geq 3$ eine Primzahl bezeichne

Lösung:

zu (a) Zunächst zeigen wir, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ gilt, wobei wir $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ als bekannt voraussetzen. Zunächst beweisen wir die Gleichung $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Die Inklusion „$\subseteq$“ ist wegen $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ offensichtlich. Für die Umkehrung bemerken wir

$$\alpha^2 \quad = \quad (\sqrt{2} + \sqrt{3})^2 \quad = \quad 2 + 2\sqrt{6} + 3 \quad = \quad 5 + 2\sqrt{6} \quad \in \quad \mathbb{Q}(\alpha)$$

und $\sqrt{6} \in \mathbb{Q}(\alpha)$. Daraus wiederum folgt $\sqrt{6}\alpha = \sqrt{6}(\sqrt{2} + \sqrt{3}) = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha)$, schließlich $(2\sqrt{3} + 3\sqrt{2}) - 2\alpha = \sqrt{2} \in \mathbb{Q}(\alpha)$ und $\alpha - \sqrt{2} = \sqrt{3} \in \mathbb{Q}(\alpha)$. Damit ist auch „$\supseteq$“ bewiesen.

Das Polynom $f = x^2 - 2 \in \mathbb{Q}[x]$ ist normiert, nach dem Eisenstein-Kriterium irreduzibel und hat $\sqrt{2}$ als Nullstelle. Also ist f das Minimalpolynom von $\sqrt{2}$, und es folgt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \mathrm{grad}(f) = 2$. Ebenso zeigt man $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Das Polynom $g = x^2 - 3$ ist normiert und hat $\sqrt{3}$ als Nullstelle. Wäre es über dem Körper $\mathbb{Q}(\sqrt{2})$ reduzibel, dann würden wegen $\mathrm{grad}(g) = 2$ die beiden Nullstellen $\pm\sqrt{3}$ des Polynoms in $\mathbb{Q}(\sqrt{2})$ liegen. Daraus würde dann $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})$ folgen, und zusammen mit $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ würde sich $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$ ergeben, im Widerspruch zur oben erwähnten Voraussetzung. Also ist g über $\mathbb{Q}(\sqrt{2})$ irreduzibel, insgesamt das Minimalpolynom von $\sqrt{3}$ über diesem Körper. Es folgt $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ und insgesamt mit der Gradformel

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \quad = \quad 2 \cdot 2 \quad = \quad 4.$$

Im nächsten Schritt bestimmen wir ein Polynom $h \in \mathbb{Q}[x]$ mit α als Nullstelle. Es gilt

$$\alpha = \sqrt{2} + \sqrt{3} \quad \Rightarrow \quad \alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \quad \Rightarrow \quad (\alpha^2 - 5)^2 = 24 \quad \Rightarrow \quad \alpha^4 - 10\alpha^2 + 25 = 24$$
$$\Rightarrow \quad \alpha^4 - 10\alpha^2 + 1 = 0.$$

Setzen wir also $h = x^4 - 10x^2 + 1$, dann folgt $h(\alpha) = 0$. Bezeichnen wir das Minimalpolynom von α über $\mathbb{Q}$ mit h_1, dann ist h_1 auf Grund der Gleichung $h(\alpha) = 0$ ein normierter Teiler von h. Zusammen mit

$$\mathrm{grad}(h_1) \quad = \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad 4 \quad = \quad \mathrm{grad}(h)$$

folgt $h = h_1$, also ist h das gesuchte Minimalpolynom.

zu (b) Da $\mathbb{F}_3$ ein Körper der Charakteristik 3 ist, gilt

$$(\alpha^2+1)^3 \quad = \quad (\alpha^2)^3+1^3 \quad = \quad \alpha^6+1 \quad = \quad 0$$

und somit $\alpha^2+1=0$. Das Element α ist also eine Nullstelle des normierten Polynoms $f=x^2+1\in\mathbb{F}_3[x]$. Wäre f reduzibel, dann müsste f wegen $\mathrm{grad}(f)=2$ in $\mathbb{F}_3$ eine Nullstelle besitzen. Aber wegen $f(0)=1$, $f(1)=2$ und $f(3)=10=1$ ist dies nicht der Fall. Also ist f das Minimalpolynom von α über $\mathbb{F}_3$.

zu (c) Um ein Polynom $f\in K[x]$ mit $f(\zeta)=0$ zu finden, versuchen wir ζ^2 als K-Linearkombination von $\{1,\zeta\}$ darzustellen. Tatsächlich gilt $\zeta^2=(\zeta+\zeta^{-1})\zeta+(-1)\cdot 1$, also $\zeta^2-(\zeta+\zeta^{-1})\zeta+1=0$. Somit ist $\alpha=\zeta$ eine Nullstelle des normierten Polynoms $f=x^2-(\zeta+\zeta^{-1})x+1\in K[x]$. Wäre f über K reduzibel, dann müsste wegen $\mathrm{grad}(f)=2$ die Nullstelle ζ in K liegen. Als primitive p-te Einheitswurzel hat ζ die Form

$$\zeta \quad = \quad \exp\left(\frac{2\pi i k}{p}\right) \quad = \quad \cos\left(\frac{2\pi k}{p}\right)+i\sin\left(\frac{2\pi k}{p}\right) \quad ,$$

mit einem $k\in\mathbb{Z}$ und $p\nmid k$, und es gilt

$$\zeta^{-1} \quad = \quad \exp\left(-\frac{2\pi i k}{p}\right) \quad = \quad \cos\left(-\frac{2\pi k}{p}\right)+i\sin\left(-\frac{2\pi k}{p}\right) \quad = \quad \cos\left(\frac{2\pi k}{p}\right)-i\sin\left(\frac{2\pi k}{p}\right).$$

Wegen $\zeta+\zeta^{-1}=2\cos(\frac{2\pi k}{p})\in\mathbb{R}$ folgt daraus $K\subseteq\mathbb{R}$ und $\zeta\in\mathbb{R}$. Andererseits ist $\frac{2\pi k}{p}$ kein ganzzahliges Vielfaches von π, woraus $\sin(\frac{2\pi k}{p})\neq 0$ und $\zeta\notin\mathbb{R}$ folgt. Der Widerspruch zeigt, dass f über K irreduzibel, insgesamt also das Minimalpolynom von α über K ist.