Aufgabe H14T1A1 (8 + 8 Punkte)

Es seien $L \supseteq K$ eine endliche Galoiserweiterung und p eine Primzahl, die den Körpergrad $[L : K]$ teilt.

(a) Zeigen Sie, dass es einen Zwischenkörper $K \subseteq Z \subseteq L$ gibt, so dass

$$[L : Z] = p^m \qquad \text{und} \qquad p \nmid [Z : K]$$

für ein $m \in \mathbb{N}$ gilt.

(b) Bestimmen Sie im Fall $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_7)$ mit einer primitiven siebten Einheitswurzel ζ_7 und $p = 3$ einen solchen Zwischenkörper, indem Sie ein primitives Element α dafür angeben.

Lösung:

zu (a) Sei $G = \mathrm{Gal}(L|K)$ und U eine p-Sylowgruppe von G. Nach Definition der p-Sylowgruppen gilt dann $|U| = p^m$ für ein $m \in \mathbb{N}$ und $p \nmid (G : U)$. Sei $Z = L^U$ der Fixkörper von U. Auf Grund der Ergänzungen zum Hauptsatz der Galoistheorie gilt $[L : Z] = |U| = p^m$ und $[Z : K] = (G : U)$, also $p \nmid [Z : K]$.

zu (b) Es gilt $[L : \mathbb{Q}] = \phi(7) = 6$, wobei ϕ die Eulersche ϕ-Funktion bezeichnet. Ist Z ein Zwischenkörper mit $[Z : \mathbb{Q}] = 2$, dann gilt $3 \nmid [Z : \mathbb{Q}]$ und auf Grund der Gradformel $6 = 2 \cdot 3 = [L : Z] \cdot [Z : \mathbb{Q}] = [L : Z] \cdot 2$, also $[L : Z] = \frac{6}{2} = 3 = 3^1$; die Bedingungen aus Teil (a) wären dann also erfüllt. Laut Vorlesung gilt $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$, also ist $G = \mathrm{Gal}(L|K)$ zyklisch von Ordnung 6. Zu jedem Teiler d von 6 gibt es also genau eine Untergruppe der Ordnung d. Bezeichnen wir mit U die eindeutig bestimmte Untergruppe der Ordnung 3 von G, dann ist $Z = L^U$ wie in Teil (a) gezeigt ein Zwischenkörper mit der gewünschten Eigenschaft.

Wir bestimmen die Untergruppe U genauer. Ist $a \in \mathbb{Z}$ eine Primitivwurzel modulo 7, dann ist der Automorphismus $\sigma_a \in G$ gegeben durch $\sigma_a(\zeta_7) = \zeta_7^a$ ein Erzeuger von G. Wegen $3^2 \equiv 9 \equiv 2 \not\equiv 1 \bmod 7$, $3^3 \equiv 27 \equiv 6 \not\equiv 1 \bmod 6$ ist $a = 3$ eine solche Primitivwurzel, und es gilt $G = \langle\sigma\rangle$ für den Automorphismus σ gegeben durch $\sigma(\zeta_7) = \zeta^3$. Die Untergruppe U ist dann gegeben durch $U = \langle\sigma^2\rangle$, und es gilt $\sigma^2(\zeta_7) = (\zeta_7^3)^3 = \zeta_7^9 = \zeta_7^2$.

Um nun den Körper Z explizit zu bestimmen, suchen wir nach einem Element $\alpha \in L$, dass unter σ^2 fest bleibt. (Dieses Element ist dann zumindest im Fixkörper Z enthalten, auch wenn Z nicht unbedingt erzeugt.) Offenbar ist $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$ ein solches Element, denn es gilt

$$\sigma^2(\alpha) \quad = \quad \zeta_7^2 + (\zeta_7^2)^2 + (\zeta_7^2)^4 \quad = \quad \zeta_7^2 + \zeta_7^4 + \zeta_7^8 \quad = \quad \zeta_7 + \zeta_7^2 + \zeta_7^4 \quad = \quad \alpha.$$

Es gilt also $\mathbb{Q}(\alpha) \subseteq Z$. Bestimmen wir nun das Minimalpolynom von α über $\mathbb{Q}$. Die primitive siebte Einheitswurzel ζ_7 ist eine Nullstelle des siebten Kreisteilungspolynom, deshalb gilt $1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = 0$. Mit Hilfe dieser Relation erhalten wir

$$\alpha^2 \quad = \quad (\zeta_7 + \zeta_7^2 + \zeta_7^4)^2 \quad = \quad \zeta_7^2 + \zeta_7^4 + \zeta_7^8 + 2\zeta_7\zeta_7^2 + 2\zeta_7\zeta_7^4 + 2\zeta_7^2\zeta_7^4 \quad =$$

$$\zeta_7^2 + \zeta_7^4 + \zeta_7 + 2\zeta_7^3 + 2\zeta_7^5 + 2\zeta_7^6 \quad =$$

$$(\zeta_7 + \zeta_7^2 + 2\zeta_7^3 + \zeta_7^4 + 2\zeta_7^5 + 2\zeta_7^6) - 2(1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6) \quad =$$

$$-\zeta_7 - \zeta_7^2 - \zeta_7^4 - 2 \quad = \quad -\alpha - 2.$$

Das Element α erfüllt also die Gleichung $\alpha^2 + \alpha + 2 = 0$. Diese Gleichung ist äquivalent zu

$$\alpha^2 + \alpha + \tfrac{1}{4} = -\tfrac{7}{4} \quad \Leftrightarrow \quad (\alpha + \tfrac{1}{2})^2 - \left(\tfrac{\sqrt{-7}}{2}\right)^2 = 0$$

$$\Leftrightarrow \quad \left(\alpha - \tfrac{1}{2} - \tfrac{\sqrt{-7}}{2}\right)^2 \left(\alpha - \tfrac{1}{2} + \tfrac{\sqrt{-7}}{2}\right)^2 \quad \Leftrightarrow \quad \alpha \in \left\{\tfrac{1}{2} \pm \tfrac{\sqrt{-7}}{2}\right\}.$$

Daraus folgt $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7})$. Weil $\sqrt{-7}$ eine Nullstelle des irreduziblen Polynoms $x^2 + 7 \in \mathbb{Q}[x]$ ist (Eisenstein), gilt $[\mathbb{Q}(\sqrt{-7}) : \mathbb{Q}] = 2$. Aus $[Z : \mathbb{Q}] = (G : U) = 2 = [\mathbb{Q}(\sqrt{-7}) : \mathbb{Q}]$ und $\mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(\alpha) \subseteq Z$ folgt wiederum $Z = \mathbb{Q}(\sqrt{-7})$.