Aufgabe H17T2A4 (15 Punkte)

Sei L der Zerfällungskörper von $x^{12} - 729 \in \mathbb{Q}[x]$ in $\mathbb{C}$ und ζ die primitive 12-te Einheitswurzel $\exp(2\pi i/12) = \frac{1}{2}(\sqrt{3} + i) \in \mathbb{C}$.

(a) Zeigen Sie: $\sqrt{3} \in \mathbb{Q}(\zeta)$ und $L = \mathbb{Q}(\zeta)$

(b) Zeigen Sie, dass $\mathrm{Gal}(L|\mathbb{Q})$ eine abelsche Gruppe der Ordnung 4 ist, die genau drei Elemente der Ordnung zwei enthält.

(c) Beschreiben Sie alle echten Zwischenkörper der Erweiterung $L|\mathbb{Q}$, indem Sie für jeden echten Zwischenkörper ein primitives Element angeben.

Lösung:

zu (a) Weil ζ eine Einheitswurzel in $\mathbb{C}^\times$ ist, gilt $\zeta\bar{\zeta} = |\zeta|^2 = 1$ und somit $\bar{\zeta} = \zeta^{-1} \in \mathbb{Q}(\zeta)$. Aus $\zeta, \bar{\zeta} \in \mathbb{Q}(\zeta)$ folgt $\zeta + \bar{\zeta} = \frac{1}{2}(\sqrt{3} + i) + \frac{1}{2}(\sqrt{3} - i) = \sqrt{3} \in \mathbb{Q}(\zeta)$.

Die Gleichung $729 = 27^2 = 3^6$ zeigt, dass $\sqrt{3}$ eine Nullstelle von $f = x^{12} - 729$ ist, denn es gilt $f(\sqrt{3}) = (\sqrt{3})^{12} - 729 = 3^6 - 3^6 = 0$. Weil ζ eine zwölfte Einheitswurzel ist, sind die Elemente ζ^k mit $0 \le k < 12$ verschieden, und wegen $\sqrt{3} \neq 0$ ist $N = \{\zeta^k\sqrt{3} \mid 0 \le k < 12\}$ eine 12-elementige Menge. Jedes Element aus N ist wegen

$$f(\zeta^k\sqrt{3}) = (\zeta^k\sqrt{3})^{12} - 729 \quad = \quad (\zeta^{12})^k(\sqrt{3})^{12} - 729 \quad = \quad 1^k \cdot (\sqrt{3})^{12} - 729 \quad = \quad f(\sqrt{3}) \quad = \quad 0$$

eine Nullstelle von f. Da f als Polynom vom Grad 12 nicht mehr als zwölf komplexe Nullstellen besitzt, ist N genau die Nullstellenmenge von f. Es gilt also $L = \mathbb{Q}(N)$ nach Definition des Zerfällungskörpers. Zu zeigen bleibt

$$\mathbb{Q}(\zeta) \quad = \quad \mathbb{Q}(N).$$

Die Inklusion „$\subseteq$“ ist erfüllt, weil mit $\sqrt{3}, \zeta\sqrt{3} \in \mathbb{Q}(N)$ auch $\zeta = \frac{\zeta\sqrt{3}}{\sqrt{3}}$ in $\mathbb{Q}(N)$ liegt. Für die Inklusion „$\supseteq$“ verwenden wir, dass (wie oben gezeigt) $\sqrt{3}$ in $\mathbb{Q}(\zeta)$ liegt. Zusammen mit $\zeta \in \mathbb{Q}(\zeta)$ folgt daraus $\zeta^k\sqrt{3} \in \mathbb{Q}(\zeta)$ für $0 \le k < 12$ und somit $N \subseteq \mathbb{Q}(\zeta)$.

zu (b) Wegen $L = \mathbb{Q}(\zeta)$ ist L der zwölfte Kreisteilungskörper. Laut Vorlesung gilt deshalb $\mathrm{Gal}(L|\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $|\mathrm{Gal}(L|\mathbb{Q})| = |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$. Mit $(\mathbb{Z}/12\mathbb{Z})^\times$ ist auch die Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ abelsch. In der Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gibt es genau drei Elemente der Ordnung 2, nämlich $(\bar{1}, \bar{0})$, $(\bar{0}, \bar{1})$ und $(\bar{1}, \bar{1})$. (Das einzige verbleibende Element in das Neutralelement $(\bar{0}, \bar{0})$.) Also gibt es auch in $\mathrm{Gal}(L|\mathbb{Q})$ genau drei Elemente der Ordnung 2.

zu (c) Zunächst überprüfen wir, dass $L|\mathbb{Q}$ eine Galois-Erweiterung ist. Als Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist L normal über $\mathbb{Q}$, damit auch algebraisch. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist jede algebraische Erweiterung separabel. Dies zeigt, dass $L|\mathbb{Q}$ insgesamt eine Galois-Erweiterung ist, und das somit der Hauptsatz der Galoistheorie auf $L|\mathbb{Q}$ angewendet werden kann.

Nach dem Hauptsatz der Galoistheorie ist durch $U \mapsto L^U$ eine Bijektion zwischen der Menge der Untergruppen von $G = \mathrm{Gal}(L|\mathbb{Q})$ und der Menge der Zwischenkörper von $L|\mathbb{Q}$ gegeben, wobei L^U jeweils den Fixkörper von U bezeichnet. Dabei ist L^U genau dann ein echter Zwischenkörper von $L|\mathbb{Q}$, wenn $\{\mathrm{id}\} \subsetneq U \subsetneq G$ gilt. Wegen $|G| = 4$, und weil $1, 2, 4$ die einzigen Teiler von 4 sind, ist dies wiederum äquivalent zu $|U| = 2$. Die Anzahl der echten Zwischenkörper von $L|\mathbb{Q}$ ist also gleich der Anzahl der Untergruppen der Ordnung 2 von G und wegen $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ auch gleich der Anzahl der Untergruppen der Ordnung 2 von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Weil 2 eine Primzahl ist, ist jede solche Untergruppe zyklisch, wird also von einem Element der Ordnung 2 erzeugt. Dies zeigt, dass $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ genau drei Untergruppen der Ordnung 2 besitzt, nämlich $\langle(\bar{1}, \bar{0})\rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\}$, $\langle(\bar{0}, \bar{1})\rangle = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}$ und $\langle(\bar{1}, \bar{1})\rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$. Also ist auch die Anzahl der Zwischenkörper von $L|\mathbb{Q}$ gleich 3.

Zwei dieser Zwischenkörper können wir direkt angeben. Das Polynom $g = x^2 - 3$ ist normiert, nach dem Eisenstein-Kriterium irreduzibel, und es gilt $g(\sqrt{3}) = 0$. Also ist g das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \mathrm{grad}(g) = 2$. Weil $L|\mathbb{Q}$ galoissch ist, gilt $[L : \mathbb{Q}] = |G| = 4$. Wegen $1 < [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] < [L : \mathbb{Q}]$ ist $\mathbb{Q}(\sqrt{3})$ ein echter Zwischenkörper von $L|\mathbb{Q}$. Ebenso ist $h = x^2 + 1$ normiert und erfüllt $h(i) = 0$. Wäre h reduzibel in $\mathbb{Q}[x]$, dann müssten wegen $\mathrm{grad}(h) = 2$ die Nullstellen $\pm i$ in $\mathbb{Q}$ liegen. Aber die ist offenbar nicht der Fall. Also ist h das Minimalpolynom von i über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(i) : \mathbb{Q}] = \mathrm{grad}(h) = 2$. Also ist auch $\mathbb{Q}(i)$ ein echter Zwischenkörper von $L|\mathbb{Q}$. Wegen $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ und $\mathbb{Q}(i) \not\subseteq \mathbb{R}$ gilt $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(i)$.

Mit $\sqrt{3}$ und i liegt auch $i\sqrt{3}$ in L, und somit ist auch $\mathbb{Q}(i\sqrt{3})$ ein Zwischenkörper von $L|\mathbb{Q}$. Das Polynom $k = x^2 + 3$ ist normiert, nach dem Eisenstein-Kriterium irreduzibel, und es gilt $k(i\sqrt{3}) = 0$. Also ist k das Minimalpolynom von $i\sqrt{3}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = \mathrm{grad}(k) = 2$. Somit ist auch $\mathbb{Q}(i\sqrt{3})$ ein echter Zwischenkörper von $L|\mathbb{Q}$. Wegen $\mathbb{Q}(i\sqrt{3}) \not\subseteq \mathbb{R}$ gilt $\mathbb{Q}(i\sqrt{3}) \neq \mathbb{Q}(\sqrt{3})$. Wäre $\mathbb{Q}(i) = \mathbb{Q}(i\sqrt{3})$, dann würde mit i und $i\sqrt{3}$ auch das Element $\sqrt{3} = \frac{i\sqrt{3}}{i}$ in $\mathbb{Q}(i)$ liegen. Es würde dann $\zeta = \frac{1}{2}(\sqrt{3} + i) \in \mathbb{Q}(i)$ und $L = \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i)$ folgen, insgesamt also $L = \mathbb{Q}(i)$ und $[L : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$, was zu $[L : \mathbb{Q}] = 4$ im Widerspruch steht. Dies zeigt, dass auch $\mathbb{Q}(i) \neq \mathbb{Q}(i\sqrt{3})$ gilt. Ingesamt haben wir damit alle echten Zwischenkörper von $L|\mathbb{Q}$ gefunden, nämlich $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$ und $\mathbb{Q}(i\sqrt{3})$.