Aufgabe H15T1A5 (4+4+6+6 Punkte)

Sei $\zeta_5 \in \mathbb{C}$ eine primitive fünfte Einheitswurzel, $\zeta_7 \in \mathbb{C}$ eine primitive siebte Einheitswurzel und $u = \zeta_7 + \zeta_7^{-1}$. Zeigen Sie:

(a) $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] = 2$,

(b) $[\mathbb{Q}(u) : \mathbb{Q}] = 3$,

(c) $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = 12$.

(d) Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(u, \zeta_5)|\mathbb{Q})$ ist isomorph zu $\mathbb{Z}/12\mathbb{Z}$.

Lösung:

zu (a) Sei f das Minimalpolynom von ζ_7 über $\mathbb{Q}(u)$ und $g = x^2 - ux + 1 \in \mathbb{Q}(u)[x]$. Es gilt

$$g(\zeta_7) \quad = \quad \zeta_7^2 - u\zeta_7 + 1 \quad = \quad \zeta_7^2 - (\zeta_7 + \zeta_7^{-1})\zeta_7 + 1 \quad = \quad \zeta_7^2 - \zeta_7^2 - 1 + 1 \quad = \quad 0 \quad ,$$

also ist f ein Teiler von g. Nehmen wir an, dass f ein echter Teiler von g ist. Dann wäre g über $\mathbb{Q}(u)[x]$ reduzibel und die Nullstelle ζ_7 von g in $\mathbb{Q}(u)$ enthalten. Aber das ist unmöglich, denn wegen $|\zeta_7| = 1$ gilt $\zeta_7^{-1} = \bar{\zeta}_7$ und $u = \zeta_7 + \zeta_7^{-1} = \zeta_7 + \bar{\zeta}_7 \in \mathbb{R}$, also $\mathbb{Q}(u) \subseteq \mathbb{R}$. Andererseits ist ζ_7 nicht in $\mathbb{R}$ enthalten, denn es gilt $\zeta_7 = e^{2\pi ik/7} = \cos(\frac{2\pi k}{7}) + i\sin(\frac{2\pi k}{7})$ mit einer zu 7 teilerfremden Zahl $k \in \mathbb{Z}$. Wäre $\zeta_7 \in \mathbb{R}$, dann würde $\sin(\frac{2\pi k}{7}) = 0$ und $\frac{2\pi k}{7} \in \pi\mathbb{Z}$ folgen, also $\frac{2k}{7} \in \mathbb{Z}$, was aber wegen $7 \nmid (2k)$ nicht der Fall ist. Also muss $f = g$ gelten, und wir erhalten

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] \quad = \quad [\mathbb{Q}(u, \zeta_7) : \mathbb{Q}(u)] \quad = \quad \mathrm{grad}(f) \quad = \quad \mathrm{grad}(g) \quad = \quad 2.$$

zu (b) Aus der Vorlesung ist bekannt, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt, wobei $\zeta_n \in \mathbb{C}^\times$ eine primitive n-te Einheitswurzel und φ die Eulersche φ-Funktion bezeichnet. Insbesondere gilt $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \varphi(7) = 6$. Mit der Gradformel erhalten wir

$$[\mathbb{Q}(u) : \mathbb{Q}] \quad = \quad \frac{[\mathbb{Q}(\zeta_7) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)]} \quad = \quad \frac{6}{2} \quad = \quad 3.$$

zu (c) Sei h das Minimalpolynom von ζ_5 über $\mathbb{Q}(u)$ und $\Phi_5 \in \mathbb{Q}[x]$ das fünfte Kreisteilungspolynom. Wegen $\Phi_5(\zeta_5) = 0$ und $\Phi_5 \in \mathbb{Q}(u)[x]$ ist h ein Teiler von Φ_5. Es folgt

$$[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(u)] \quad = \quad \mathrm{grad}(h) \quad \leq \quad \mathrm{grad}(\Phi_5) \quad = \quad \varphi(5) \quad = \quad 4$$

und $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] \leq 4 \cdot 3 = 12$ auf Grund der Gradformel und Aufgabenteil (b). Andererseits zeigt die Gleichung

$$[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(u)] \cdot 3 \quad ,$$

dass $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$ von 3 geteilt wird. Ebenso ist wegen

$$[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(\zeta_5)] \cdot [\mathbb{Q}(\zeta_5) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}(\zeta_5)] \cdot 4$$

die Zahl 4 ein Teiler von $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$. Wegen $\mathrm{ggT}(3, 4) = 1$ folgt insgesamt $12 \mid [\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$ und insbesondere $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] \geq 12$. Zusammen mit der bereits gezeigten Ungleichung von oben erhalten wir schließlich die Gleichung $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = 12$.

zu (d) Aus der Vorlesung ist folgendes bekannt: Ist $L|K$ eine Galois-Erweiterung und M ein Zwischenkörper von $L|K$ derart, dass $M|K$ normal ist, dann ist durch $\mathrm{Gal}(L|K) \to \mathrm{Gal}(M|K)$, $\sigma \mapsto \sigma|_M$ ein surjektiver Gruppenhomorphismus definiert. Die Galoisgruppe $\mathrm{Gal}(M|K)$ ist also isomorph zu einer Faktorgruppe von $\mathrm{Gal}(L|K)$.

Sei nun $\zeta_{35} \in \mathbb{C}^\times$ eine primitive 35-te Einheitswurzel, $L = \mathbb{Q}(\zeta_{35})$, $M = \mathbb{Q}(u, \zeta_5)$ und $K = \mathbb{Q}$. Weil ζ_{35}^7 eine primitive 5-te und ζ_{35}^5 eine primitive 7-te Einheitswurzel ist, gilt $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{35}^7) \subseteq L$, $\mathbb{Q}(\zeta_7) = \mathbb{Q}(\zeta_{35}^5) \subseteq L$, also insbesondere $\zeta_5 \in L$ und $u = \zeta_7 + \zeta_7^{-1} \in L$. Damit ist $M \subseteq L$ nachgewiesen, und offensichtlich gilt $K \subseteq M$. Die Galoisgruppe $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/35\mathbb{Z})^\times$ ist abelsch. Daraus folgt, dass $\mathrm{Gal}(L|M)$ Normalteiler von $\mathrm{Gal}(L|K)$ und die Erweiterung $M|K$ somit normal ist. Wie oben bemerkt, ist $\mathrm{Gal}(M|K)$ damit isomorph zu einer Faktorgruppe von $\mathrm{Gal}(L|K)$ und als solche ebenfalls abelsch.

Wegen $[M : K] = 12$ ist $\mathrm{Gal}(M|K)$ also eine abelsche Gruppe der Ordnung 12. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen folgt daraus $\mathrm{Gal}(M|K) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$ oder $\mathrm{Gal}(M|K) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Der zweite Fall kann ausgeschlossen werden, sobald wir in $\mathrm{Gal}(M|K)$ ein Element nachgewiesen haben, dessen Ordnung ein Vielfaches von 4 ist. Denn wegen $6(\bar{a}, \bar{b}, \bar{c}) = (\bar{0}, \bar{0}, \bar{0})$ für alle $\bar{a} \in \mathbb{Z}/3\mathbb{Z}$ und $\bar{b}, \bar{c} \in \mathbb{Z}/2\mathbb{Z}$ sind alle Elementordnungen in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ Teiler von 6.

Weil das Kreisteilungspolynom Φ_5 in $K[x]$ irreduzibel und ζ_5, ζ_5^2 Nullstellen von Φ_5 sind, gibt es nach dem Fortsetzungssatz einen K-Homomorphismus $K(\zeta_5) \to \mathbb{C}$, der ζ_5 auf ζ_5^2 abbildet. Dieser kann zu einem $\mathbb{Q}$-Homomorphismus $\sigma : M \to \mathbb{C}$ fortgesetzt werden. Weil $M|K$ eine Galois-Erweiterung ist, handelt es sich bei σ um einen K-Automorphismus von M, also ein Element von $\mathrm{Gal}(M|K)$. Es gilt $\sigma(\zeta_5) = \zeta_5^2 \neq \sigma_5$, $\sigma^2(\zeta_5) = \sigma(\zeta_5^2) = \sigma(\zeta_5)^2 = (\zeta_5^2)^2 = \zeta_5^4 \neq \zeta_5$ und $\sigma^4(\zeta_5) = \sigma^2(\zeta_5^4) = \sigma^2(\zeta_5)^4 = (\zeta_5^4)^4 = \zeta_5^{16} = \zeta_5$. Für $k, \ell \in \mathbb{Z}$ mit $0 \leq \ell < 4$ folgt daraus $\sigma^{4k}(\zeta_5) = \zeta_5$ und weiter

$$\sigma^{4k+\ell}(\zeta_5) \quad = \quad \sigma^\ell(\sigma^{4k}(\zeta_5)) \quad = \quad \sigma^\ell(\zeta_5) \quad ,$$

wobei $\sigma^\ell(\zeta_5) \neq \zeta_5$ für $\ell = 1, 2, 3$ ist. Für $m \in \mathbb{Z}$ ist $\sigma^m = \mathrm{id}$ also nur dann möglich, wenn m ein Vielfaches von 4 ist. Also muss $\mathrm{ord}(\sigma)$, das kleinste $m \in \mathbb{N}$ mit $\sigma^m = \mathrm{id}$, ein Vielfaches von 4 sein.