Aufgabe F12T1A5 (6 Punkte)

Sei K der Zerfällungskörper des Polynoms $x^5 + 5 \in \mathbb{Q}[x]$. Seien $\alpha = \sqrt[5]{-5} \in \mathbb{R}$, $\zeta = e^{2\pi i/5}$. Zeigen Sie:

(a) Der Körper K wird von α und ζ über $\mathbb{Q}$ erzeugt.

(b) Die Erweiterung $\mathbb{Q} \subseteq K$ ist galoissch, und $[K : \mathbb{Q}] = 20$.

(c) Die Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist eine nichtabelsche Gruppe der Ordnung 20.

(d) Die Galoisgruppe hat einen Normalteiler der Ordnung 5.

(e) Die 2-Sylowgruppen der Galoisgruppe sind zyklisch mit der Ordnung 4.

Lösung:

zu (a) Offenbar sind durch $\zeta^k\alpha$ mit $0 \le k < 5$ fünf verschiedene Nullstellen des Polynoms $f = x^5 + 5$ gegeben. Denn für jedes k gilt $f(\zeta^k\alpha) = (\zeta^k\alpha)^5 + 5 = (\zeta^5)^k\alpha^5 + 5 = 1^k \cdot (-5) + 5 = 0$. Weil ζ eine primitive 5-te Einheitswurzel ist, gilt für $0 \le k < \ell < 5$ jeweils $\zeta^k \neq \zeta^\ell$, und wegen $\alpha \neq 0$ folgt daraus $\zeta^k\alpha \neq \zeta^\ell\alpha$. Weil f als Polynom fünften Grades nicht mehr als 5 komplexe Nullstellen haben kann, ist durch $N = \{\zeta^k\alpha \mid 0 \le k < 5\}$ somit die Menge aller komplexen Nullstellen von f gegeben. Somit ist $\mathbb{Q}(N)$ der Zerfällungskörper von f über $\mathbb{Q}$. Zu zeigen ist nun

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

„$\supseteq$“ Aus $\alpha, \zeta \in \mathbb{Q}(\alpha, \zeta)$ folgt $\zeta^k\alpha \in \mathbb{Q}(\alpha, \zeta)$ für $0 \le k < 5$, denn $\mathbb{Q}(\alpha, \zeta)$ ist als Teilkörper von $\mathbb{C}$ unter Multiplikation abgeschlossen. Es gilt also $N \subseteq \mathbb{Q}(\alpha, \zeta)$, und daraus (wiederum auf Grund der Teilkörper-Eigenschaft) folgt $\mathbb{Q}(\mathbb{N}) \subseteq \mathbb{Q}(\alpha, \zeta)$. „$\subseteq$“ Aus $\alpha, \zeta\alpha \in N \subseteq \mathbb{Q}(N)$ folgt $\zeta = \frac{\zeta\alpha}{\alpha} \in \mathbb{Q}(N)$. Es gilt also $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$, und damit erhalten wir $\mathbb{Q}(\alpha, \zeta) \subseteq \mathbb{Q}(N)$.

zu (b) Als Zerfällungskörper von f über $\mathbb{Q}$ ist die Erweiterung $K|\mathbb{Q}$ normal und insbesondere algebraisch. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist $K|\mathbb{Q}$ als algebraische Erweiterung auch separabel. Jede normale und separable Erweiterung ist nach Definition eine Galois-Erweiterung. Zum Nachweis der Gleichung $[K : \mathbb{Q}] = 20$ berechnen wir zunächst die Erweiterungsgrade $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. Das Polynom f ist nach dem Eisenstein-Kriterium (angewendet auf die Primzahl 5) über $\mathbb{Q}$ irreduzibel. Außerdem ist es normiert, und es gilt $f(\alpha) = 0$. Ingesamt ist f also das Minimalpolynom von α über $\mathbb{Q}$, und daraus folgt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad \mathrm{grad}(f) \quad = \quad 5.$$

Das Minimalpolynom von ζ über $\mathbb{Q}$ ist das fünfte Kreisteilungspolynom Φ_5, weil ζ eine primitive 5-te Einheitswurzel ist. Somit gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \mathrm{grad}(\Phi_5) = \varphi(5) = 4$. Durch Anwendung der Gradformel erhalten wir nun

$$[K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\alpha)] \cdot 5$$

und

$$[K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\zeta)] \cdot 4.$$

Somit ist sowohl 5 als auch 4 ein Teiler von $[K:\mathbb{Q}]$. Wegen $\mathrm{ggT}(4,5)=1$ folgt daraus $20 \mid [K:\mathbb{Q}]$ und insbesondere $[K:\mathbb{Q}] \geq 20$. Sei nun $h \in \mathbb{Q}(\alpha)[x]$ das Minimalpolynom von ζ über $\mathbb{Q}(\alpha)$. Wegen $\Phi_5(\zeta)=0$ und $\Phi_5 \in \mathbb{Q}(\alpha)[x]$ ist h im Polynomring $\mathbb{Q}(\alpha)[x]$ ein Teiler von Φ_5, insbesondere gilt $\mathrm{grad}(h) \leq \mathrm{grad}(\Phi_5) = 4$. Daraus folgt

$$[K:\mathbb{Q}(\alpha)] \quad = \quad [\mathbb{Q}(\alpha)(\zeta):\mathbb{Q}(\alpha)] \quad = \quad \mathrm{grad}(h) \quad \leq \quad 4 \quad ,$$

und mit der Gradformel erhalten wir $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] \leq 4 \cdot 5 = 20$. Ingesamt ist damit $[K:\mathbb{Q}]=20$ bewiesen.

zu (c) Da es sich bei $K|\mathbb{Q}$ um eine endliche Galois-Erweiterung handelt, ist die Gruppenordnung von $G = \mathrm{Gal}(K|\mathbb{Q})$ gegeben durch $|G| = [K:\mathbb{Q}] = 20$. Wäre G abelsch, dann wäre jede Untergruppe U von G ein Normalteiler. Auf Grund der Ergänzungen zum Hauptsatz der Galoistheorie würde daraus folgen, dass für jeden Zwischenkörper M von $K|\mathbb{Q}$ die Erweiterung $M|\mathbb{Q}$ normal ist.

Aber der Zwischenkörper $M = \mathbb{Q}(\alpha)$ liefert keine normale Erweiterung $M|\mathbb{Q}$. Denn das Polynom f ist irreduzibel über $\mathbb{Q}$ und besitzt mit α in M eine Nullstelle. Wäre $M|\mathbb{Q}$ normal, dann müsste f über $\mathbb{Q}(\alpha)$ in Linearfaktoren zerfallen. Dies würde bedeuten, dass alle komplexen Nullstellen von f schon in $\mathbb{Q}(\alpha)$ liegen. Aber dies ist nicht der Fall, denn wegen $\alpha \in \mathbb{R}$ gilt einerseits $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, und andererseits folgt aus $\zeta \in \mathbb{C}$ und $0 \neq \alpha \in \mathbb{R}$, dass $\zeta\alpha$ nicht in $\mathbb{R}$ und somit erst recht nicht in $\mathbb{Q}(\alpha)$ liegt. Also ist G nicht abelsch.

zu (d) Wir beweisen die Existenz eines geeigneten Normalteilers über den Hauptsatz der Galoistheorie. Der Körper $\mathbb{Q}(\zeta)$ ist ein Zwischenkörper von $K|\mathbb{Q}$, und wie wir bereits in Teil (b) gezeigt haben, gilt $[\mathbb{Q}(\zeta):\mathbb{Q}] = \mathrm{grad}(\Phi_5) = 4$. Bezeichnen wir die zugehörige Untergruppe von G mit $U = \mathrm{Gal}(K|\mathbb{Q}(\zeta))$, dann gilt $(G:U) = [\mathbb{Q}(\zeta):\mathbb{Q}] = 4$ und $|U| = \frac{|G|}{(G:U)} = \frac{20}{4} = 5$. Aus der Vorlesung ist bekannt, dass Kreisteilungserweiterungen stets normale Erweiterungen sind, insbesondere also auch $\mathbb{Q}(\zeta)|\mathbb{Q}$. Aus den Ergänzungen zum Hauptsatz der Galoistheorie folgt, dass U ein Normalteiler von G ist. Insgesamt handelt es sich bei U also um einen Normalteiler von G der Ordnung 5.

zu (e) Sei $V = \mathrm{Gal}(K|\mathbb{Q}(\alpha))$. Wegen $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ gilt $(G:V) = 5$ und somit $|V| = \frac{|G|}{(G:V)} = \frac{20}{5} = 4$. Weil 4 die größte 2-Potenz ist, die $|G|$ teilt, handelt es sich bei V um eine 2-Sylowgruppe von G. Wir konstruieren nun mit dem Fortsetzungssatz in V ein Element der Ordnung 4. Das Polynom Φ_5 ist nicht nur über $\mathbb{Q}$, sondern auch über $\mathbb{Q}(\alpha)$ irreduzibel. Denn anderernfalls wäre das Minimalpolynom $g \in \mathbb{Q}(\alpha)[x]$ von ζ über $\mathbb{Q}(\alpha)$ ein echter Teiler von Φ_5 in $\mathbb{Q}(\alpha)[x]$, und insbesondere wäre $\mathrm{grad}(g) < \mathrm{grad}(\Phi_5) = 4$. Daraus würde

$$[K:\mathbb{Q}(\alpha)] \quad = \quad [\mathbb{Q}(\alpha)(\zeta):\mathbb{Q}(\alpha)] \quad = \quad \mathrm{grad}(g) \quad < \quad 4$$

folgen, und mit der Gradformel würden wir $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)] \cdot [K:\mathbb{Q}(\alpha)] = [K:\mathbb{Q}(\zeta)] \cdot 5 < 4 \cdot 5 = 20$ erhalten, im Widerspruch zum Ergebnis von Teil (b). Also ist Φ_5 tatsächlich über $\mathbb{Q}(\alpha)$ irreduzibel. Weil ζ und ζ^2 beides Nullstellen von Φ_5 sind, existiert nach dem Fortsetzungssatz in $V = \mathrm{Gal}(K|\mathbb{Q}(\alpha))$ ein Element σ mit $\sigma(\zeta) = \zeta^2$. Wegen $\sigma^2(\zeta) = \sigma(\sigma(\zeta)) = \sigma(\zeta^2) = \sigma(\zeta)^2 = (\zeta^2)^2 = \zeta^4 \neq \zeta$ ist $\sigma^2 \neq \mathrm{id}_K$. Die Ordnung von σ ist also kein Teiler von 2. Andererseits ist $\mathrm{ord}(\sigma)$ wegen $\sigma \in V$ und $|V| = 4$ ein Teiler von 4. Damit ist $\mathrm{ord}(\sigma) = 4$ nachgewiesen, und folglich ist die 2-Sylowgruppe V zyklisch. Da nach dem Zweiten Sylowsatz je zwei 2-Sylowgruppen in G zueinander konjugiert und damit isomorph sind, ist auch jede andere 2-Sylowgruppe von G zyklisch.