Aufgabe H16T2A4 (2+6+6+2 Punkte)

Sei $p > 2$ eine Primzahl. Wir betrachten den Körper $K = \mathbb{Q}(\zeta_p, \alpha_p) \subseteq \mathbb{C}$ mit $\alpha_p = \sqrt[p]{p} \in \mathbb{R}$ und $\zeta_p = e^{2\pi i/p}$. Zeigen Sie:

(a) Die Körpererweiterung $K|\mathbb{Q}$ ist galoissch.

(b) $[K : \mathbb{Q}] = p(p-1)$

(c) Die Teilerweiterung $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ ist nicht normal, und daher ist die Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ nicht abelsch.

(d) $\mathrm{Gal}(K|\mathbb{Q})$ hat einen Normalteiler der Ordnung p.

Lösung:

zu (a) Als Nullstellen der Polynome $f = x^p - p$ und $g = \Phi_p = x^{p-1} + x^{p-2} + ... + x + 1$ (p-tes Kreisteilungspolynom) aus $\mathbb{Q}[x]$ sind α_p und ζ_p algebraisch über $\mathbb{Q}$. Dies zeigt, dass $K|\mathbb{Q}$ eine algebraische Erweiterung ist. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist jede algebraische Erweiterung von $\mathbb{Q}$ auch separabel.

Um zu zeigen, dass $K|\mathbb{Q}$ auch normal ist, überprüfen wir, dass K der Zerfällungskörper von f über $\mathbb{Q}$ ist. Die Menge der komplexen Nullstellen von f ist gegeben durch $N = \{\zeta_p^i \alpha_p \mid 0 \le i \le p-1\}$. Zu überprüfen ist also $K = \mathbb{Q}(N)$. Dafür wiederum genügt es, $N \subseteq K$ und $\{\alpha_p, \zeta_p\} \subseteq \mathbb{Q}(N)$ zu überprüfen. Die erste Inklusion ist erfüllt, denn nach Definition liegen α_p und ζ_p in $K = \mathbb{Q}(\zeta_p, \alpha_p)$. Da K abgeschlossen unter Multiplikation ist, sind damit auch Elemente der Form $\zeta_p^i \alpha_p$ mit $0 \le i \le p-1$ in K enthalten. Zum Nachweis der zweiten Inklusion genügt es zu bemerken, dass mit α_p und $\zeta_p \alpha_p$ auch das Element $\zeta_p = \frac{\zeta_p \alpha_p}{\alpha_p}$ in $\mathbb{Q}(N)$ liegt und somit $\{\alpha_p, \zeta_p\} \subseteq \mathbb{Q}(N)$ gilt. Als normale und separable Erweiterung ist $K|\mathbb{Q}$ insgesamt eine Galois-Erweiterung.

zu (b) Das Polynom f ist normiert, irreduzibel auf Grund des Eisenstein-Kriteriums, und es gilt $f(\alpha_p) = 0$. Daraus folgt $f = \mu_{\mathbb{Q},\alpha_p}$ und $[\mathbb{Q}(\alpha_p) : \mathbb{Q}] = \mathrm{grad}(f) = p$. Wegen

$$[K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\alpha_p)] \cdot [\mathbb{Q}(\alpha_p) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\alpha_p)] \cdot p$$

ist p also ein Teiler von $[K : \mathbb{Q}]$. Auch das Polynom g ist normiert, es gilt $g(\zeta_p) = 0$, und aus der Vorlesung ist bekannt, dass g als Kreisteilungspolynom in $\mathbb{Q}[x]$ irreduzibel ist. Also ist $g = \mu_{\mathbb{Q},\zeta_p}$ und $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \mathrm{grad}(g) = p - 1$. Die Gleichung $[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_p)] \cdot [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_p)] \cdot (p-1)$ zeigt, dass auch $p - 1$ ein Teiler von $[K : \mathbb{Q}]$ ist. Da p und $p - 1$ teilerfremd sind, folgt daraus insgesamt, dass $[K : \mathbb{Q}]$ von $p(p-1)$ geteilt wird. Insbesondere gilt $[K : \mathbb{Q}] \ge p(p-1)$.

Sei $h \in \mathbb{Q}(\alpha_p)[x]$ das Minimalpolynom von ζ_p über $\mathbb{Q}(\alpha_p)$. Wegen $g \in \mathbb{Q}(\alpha_p)[x]$ und $g(\zeta_p) = 0$ folgt $h \mid g$ auf Grund der Definition des Minimalpolynoms. Wir erhalten $[K : \mathbb{Q}(\alpha_p)] = [\mathbb{Q}(\alpha_p)(\zeta_p) : \mathbb{Q}(\alpha_p)] = \mathrm{grad}(h) \le \mathrm{grad}(g) = p - 1$ und $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_p)] \cdot [\mathbb{Q}(\alpha_p) : \mathbb{Q}] \le (p-1)p$. Insgesamt ist damit $[K : \mathbb{Q}] = p(p-1)$ nachgewiesen.

zu (c) Das Polynom f ist irreduzibel, und es besitzt wegen $f(\alpha_p) = 0$ in $\mathbb{Q}(\alpha_p)$ eine Nullstelle. Wäre $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ normal, dann müsste f über $\mathbb{Q}(\alpha_p)$ in Linearfaktoren zerfallen. Insbesondere wäre dann auch die Nullstelle $\zeta_p\alpha_p$ in $\mathbb{Q}(\alpha_p)$ enthalten. Aber das ist unmöglich, denn wegen $p > 2$ gilt einerseits $\zeta_p\alpha_p \notin \mathbb{R}$, andererseits $\mathbb{Q}(\alpha_p) \subseteq \mathbb{R}$. Dies zeigt, dass $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ nicht normal ist.

Laut Vorlesung ist ein Zwischenkörper M der Galois-Erweiterung $K|\mathbb{Q}$ genau dann normal über $\mathbb{Q}$, wenn die Untergruppe $U = \mathrm{Gal}(K|M)$ ein Normalteiler von $G = \mathrm{Gal}(K|\mathbb{Q})$ ist. Da $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ nicht normal ist, ist $\mathrm{Gal}(K|\mathbb{Q}(\alpha_p))$ also kein Normalteiler von G. Dies zeigt, dass G nicht abelsch ist, denn dann wären laut Vorlesung sämtliche Untergruppen von G Normalteiler.

zu (d) Aus der Vorlesung ist bekannt, dass $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ als Kreisteilungserweiterung galoissch und somit auch normal ist. Also handelt es sich bei $V = \mathrm{Gal}(K|\mathbb{Q}(\zeta_p))$ um einen Normalteiler von G. Auf Grund der Gradformel gilt

$$[K : \mathbb{Q}(\zeta_p)] \quad = \quad \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]} \quad = \quad \frac{p(p-1)}{p-1} \quad = \quad p.$$

Mit $K|\mathbb{Q}$ ist auch $K|\mathbb{Q}(\zeta_p)$ eine Galois-Erweiterung, und folglich ist $|V| = [K : \mathbb{Q}(\zeta_p)] = p$.