H18-T1-A4

Seien $p > 0$ eine Primzahl, $\mathbb{Q} \subseteq K$ eine Körpererweiterung vom Grad p, $\alpha \in K$ ein Element mit $K = \mathbb{Q}(\alpha)$, $\alpha_1 := \alpha, \ldots, \alpha_p \in \mathbb{C}$ die Konjugierten von α über $\mathbb{Q}$ und letztlich $E := \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ die normale Hülle von $K/\mathbb{Q}$.

a) Zeigen Sie, z.B. durch Betrachten der Operation der Galoisgruppe auf den Nullstellen, dass die Galoisgruppe $\mathrm{Gal}(E/\mathbb{Q})$ eine zyklische Untergruppe der Ordnung p enthält.

b) Zeigen Sie: Gilt $\alpha_2 \in K$, so folgt $K = E$.

Lösungsvorschlag. Zu a). Nach Gradsatz ist $[E : \mathbb{Q}] = [E : K] \cdot [K : \mathbb{Q}] = [E : K] \cdot p$ und mit $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$ folgt $p \mid |\mathrm{Gal}(E/\mathbb{Q})|$. Nach Satz von Cauchy existiert dann eine Untergruppe $U \subseteq \mathrm{Gal}(E/\mathbb{Q})$ mit $|U| = p$. Diese ist zyklisch, denn für $\sigma \in U \setminus \{\mathrm{Id}\}$ (und damit $\mathrm{ord}(\sigma) > 1$) gilt nach Lagrange $\mathrm{ord}(\sigma) \mid p$, also $\mathrm{ord}(\sigma) = p$ und damit $U = \langle\sigma\rangle$.
Zu b). Bekanntlich kann man mithilfe des injektiven Gruppenhomomorphismus

$$\begin{aligned} \varphi : \mathrm{Gal}(E/\mathbb{Q}) &\longrightarrow S_{|\{\alpha_1,\ldots,\alpha_p\}|} \\ g &\longmapsto g|_{\{\alpha_1,\ldots,\alpha_p\}} \end{aligned}$$

$\mathrm{Gal}(E/\mathbb{Q})$ als Untergruppe der S_p auffassen.
Es ist also σ mit $\langle\sigma\rangle = U$ (aus Teilaufgabe a)) ein p-Zykel, der $\alpha_1, \ldots, \alpha_p$ permutiert. Es existiert ein $k \in \{1, \ldots, p-1\}$ mit $\sigma^k(\alpha_1) = \alpha_2$ und wegen $\sigma^k \in U$ ist wie in Teilaufgabe a) $\mathrm{ord}(\sigma^k) = p$ und damit σ^k ebenfalls ein p-Zykel.
Dann können wir schreiben $\rho := \sigma^k = (\alpha_1, \alpha_2, x_3, \ldots, x_p)$ mit $x_3, \ldots, x_p \in \{\alpha_3, \ldots, \alpha_p\}$ und $x_i \neq x_j$ für $i \neq j$. Setze oBdA $x_i = \alpha_i$, dann ist $\rho = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p)$. Eine kurze Induktion über $n \in \{3, \ldots, p\}$ zeigt die Aussage:

(IA) n=3: Wegen $\alpha_2 \in \mathbb{Q}(\alpha_1)$, also $\alpha_2 = f(\alpha_1)$ mit $f(X) \in \mathbb{Q}[X]$, ist $\alpha_3 = \rho(\alpha_2) = \rho(f(\alpha_1)) = f(\rho(\alpha_1)) = f(\alpha_2) \in \mathbb{Q}(\alpha_2) \subseteq \mathbb{Q}(\alpha_1)$.

(IV) Für festes $n-1$ ist $\alpha_{n-1} \in \mathbb{Q}(\alpha_1)$, also $\alpha_{n-1} = f(\alpha_1)$ mit $f(X) \in \mathbb{Q}[X]$.

(IS) $n-1 \to n : \alpha_n = \rho(\alpha_{n-1}) = \rho(f(\alpha_1)) = f(\rho(\alpha_1)) = f(\alpha_2) \in \mathbb{Q}(\alpha_2) \subseteq \mathbb{Q}(\alpha_1)$

Also ist $\alpha_n \in \mathbb{Q}(\alpha_1) = K$ für $2 \leq n \leq p$ und damit $E = K$.

Alternative Lösung: Zu a). Dem Hinweis aus Teilaufgabe a) folgend, betrachten wir die wohldefinierte Gruppenwirkung von $G = \mathrm{Gal}(E/\mathbb{Q})$ auf der Nullstellenmenge $N = \{\alpha_1, \ldots, \alpha_p\}$:

$$\begin{aligned} G \times N &\longrightarrow N \\ (g, \alpha_i) &\longmapsto g(\alpha_i) \end{aligned}$$

Sei $f(X) \in \mathbb{Q}[X]$ das Minimalpolynom von α_1, dann ist $G = \mathrm{Gal}_{\mathbb{Q}}(f)$; bekanntlich operiert G genau dann transitiv auf den Nullstellen von f, wenn f irreduzibel ist. Es gilt für $\alpha_i \in N$ also $G \cdot \alpha_i = N$. Wegen $|G \cdot \alpha_i| = [G : G_{\alpha_i}]$ ist $p = |N| = |G \cdot \alpha_i|$ ein Teiler von G und weiter folgert man wie oben.
Zu b).Wir betrachten die Standgruppen der Gruppenwirkung aus a) etwas genauer. Es ist $G_{\alpha_1} \subseteq G_{\alpha_2}$, denn für $g \in G_{\alpha_1}$ ist $g(\alpha_1) = \alpha_1$ und mit $\alpha_2 \in \mathbb{Q}(\alpha_1)$ folgt $g(\alpha_2) = \alpha_2$, also $g \in G_{\alpha_2}$. Da die Gruppenwirkung transitiv ist, sind die Standgruppen insbesondere gleichmächtig und somit $G_{\alpha_1} = G_{\alpha_2}$.
Sei also $M = \{G_{\alpha_1}, \ldots, G_{\alpha_p}\}$ die Menge der Standgruppen mit $|M| < p$ und U die zyklische Untergruppe aus a). Wir definieren nun eine zweite Gruppenwirkung durch Konjugation:

$$\begin{aligned} U \times M &\longrightarrow M \\ (g, G_{\alpha_i}) &\longmapsto g G_{\alpha_i} g^{-1} \end{aligned}$$

Zur Wohldefiniertheit sei bemerkt, dass $gG_{\alpha_i}g^{-1} = G_{g(\alpha_i)}$ wieder in M liegt. Da U transitiv auf den Nullstellen operiert, ist auch diese Gruppenwirkung transitiv. Es gilt (analog zu a)) $|M| \mid |U| = p$ und daher muss $|M| = 1$ gelten, also $G_{\alpha_1} = G_{\alpha_i}$ für $2 \leq i \leq p$. Wegen $G_{\alpha_i} = \mathrm{Gal}(E/\mathbb{Q}(\alpha_i))$ ist also $\mathrm{Gal}(E/\mathbb{Q}(\alpha_1)) = \mathrm{Gal}(E/\mathbb{Q}(\alpha_i))$ für $2 \leq i \leq p$ und mit dem Hauptsatz der Galoistheorie folgt $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_i)$ für $2 \leq i \leq p$. Es folgt $\alpha_i \in \mathbb{Q}(\alpha_1)$ und damit $E = K$.