Aufgabe H18T1A4 (12 Punkte)

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

Lösung:

zu (a) Die Operation der Galoisgruppe zu betrachten, scheint mir hier unnötig kompliziert zu sein. Zunächst bemerken wir, dass $E|\mathbb{Q}$ eine Galois-Erweiterung ist. Denn laut Angabe ist $E|\mathbb{Q}$ (als normale Hülle) eine normale Erweiterung. Als normale Erweiterung ist $E|\mathbb{Q}$ insbesondere algebraisch und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel. Weil $E|\mathbb{Q}$ also galoissch ist, ist die Ordnung der Galoisgruppe $G = \mathrm{Gal}(E|\mathbb{Q})$ gegeben durch $|G| = [E : \mathbb{Q}]$. Weil K ein Zwischenkörper von $E|\mathbb{Q}$ ist, liefert die Gradformel sowie die Angabe $[K : \mathbb{Q}] = p$ die Gleichung

$$|G| \quad = \quad [E : \mathbb{Q}] \quad = \quad [E : K] \cdot [K : \mathbb{Q}] \quad = \quad [E : K] \cdot p.$$

Die Gruppenordnung $|G|$ wird also von der Primzahl p geteilt. Aus dem Satz von Cauchy folgt nun, dass in G ein Element σ mit $\mathrm{ord}(\sigma) = p$ existiert. Die von σ erzeugte Untergruppe $\langle\sigma\rangle$ ist dann eine zyklische Untergruppe der Ordnung p von G.

Variante:
Wenn man dem Hinweis in der Aufgabenstellung folgen möchte, kann man auch folgendermaßen vorgehen. Zunächst zeigt man auch hier, dass eine Galois-Erweiterung vorliegt. (Ob dieser Nachweis tatsächlich erbracht werden soll, geht aus der Aufgabenstellung nicht klar hervor.) Ist allgemein $\beta \in \mathbb{C}$ über $\mathbb{Q}$ algebraisch, dann sind die Konjugierten von β nach Definition die Nullstellen des Minimalpolynoms $\mu_{\mathbb{Q},\beta}$ in $\mathbb{C}$. Setzen wir also $f = \mu_{\mathbb{Q},\alpha}$, dann sind $\alpha_1 = \alpha, ..., \alpha_p$ genau die komplexen Nullstellen von f. Somit ist E der Zerfällungskörper von f über $\mathbb{Q}$, und die Galoisgruppe $G = \mathrm{Gal}(E|\mathbb{Q})$ stimmt mit der Galoisgruppe $\mathrm{Gal}(f|\mathbb{Q})$ des Polynoms f über $\mathbb{Q}$ überein.

Nun ist f als Minimalpolynom über $\mathbb{Q}$ irreduzibel. Daraus folgt, dass G auf der Menge $N = \{\alpha_1, ..., \alpha_p\}$ der Nullstellen transitiv operiert, denn für beliebige Nullstellen $\beta, \gamma \in \mathbb{C}$ von f existiert auf Grund des Fortsetzungssatzes ein Element $\sigma \in G$ mit $\sigma(\beta) = \gamma$. Bezeichnet G_α den Stabilisator und $G(\alpha)$ die Bahn des Elements α unter der Operation von G, dann gilt $G(\alpha) = N$ auf Grund der Transitivität, und außerdem $|G| = |G_\alpha|(G : G_\alpha) = |N|(G : G_\alpha) = p(G : G_\alpha)$. Also ist p ein Teiler von $|G|$, und wie in der ersten Lösung folgert man daraus die Existenz einer zyklischen Untergruppe der Ordnung p in G.

zu (b) Nach Teil (a) gibt es in $G = \mathrm{Gal}(E|\mathbb{Q})$ eine zyklische Untergruppe U der Ordnung p. Sei σ ein Erzeuger dieser Untergruppe. Wir beweisen die Gleichung $K = E$ unter der Voraussetzung $\alpha_2 \in G$, indem wir die Operation von U auf der Menge $N = \{\alpha_1, ..., \alpha_p\}$ der Konjugierten von α betrachten. Bezeichnen wir mit $U(\alpha)$ die Bahn und U_α den Stabilisator dieser Operation, dann gilt $p = |U(\alpha)| \cdot |U_\alpha|$. Weil p eine Primzahl ist, folgt $|U(\alpha_j)| \in \{1, p\}$ für $1 \leq j \leq p$. Nehmen wir zunächst an, es gilt $|U(\alpha_j)| = 1$ und somit $U(\alpha_j) = \alpha_j$ für alle j. Dann folgt $\tau(\alpha_j) = \alpha_j$ für $1 \leq j \leq p$ und alle $\tau \in U$. Weil jedes Element der Galoisgruppe wegen $E = \mathbb{Q}(\alpha_1, ..., \alpha_p)$ durch die Bilder von $\alpha_1, ..., \alpha_p$ eindeutig festgelegt ist, würde dies $\tau = \mathrm{id}_E$ für alle $\tau \in U$ bedeuten, also $U = \{\mathrm{id}_E\}$. Aber dies ist wegen $|U| = p$ unmöglich.

Es gibt also ein $j \in \{1, ..., p\}$ mit $|U(\alpha_j)| = p$, also $U(\alpha_j) = N$. Dann operiert U also transitiv auf N. Insbesondere gibt es ein $\tau \in U$ mit $\tau(\alpha_1) = \alpha_2$. Wegen $\tau \neq \mathrm{id}_E$ gilt $U = \langle \tau \rangle$, denn als Gruppe von Primzahlordnung besitzt U nur die Untergruppen $\{\mathrm{id}_E\}$ und U. Aus $K = \mathbb{Q}(\alpha_1)$, $\alpha_2 \in K$ und $\tau(\alpha_1) = \alpha_2$ folgt $\tau(K) \subseteq K$ und damit auch $\tau^m(K) \subseteq K$ für alle $m \in \mathbb{Z}$. Weil $U = \langle \tau \rangle$ auf N transitiv operiert, existiert für jedes $j \in \{1, ..., p\}$ ein $m_j \in \mathbb{Z}$ mit $\tau^{m_j}(\alpha_1) = \alpha_j$. Wegen $\tau^{m_j}(K) \subseteq K$ erhalten wir jeweils $\alpha_j = \tau^{m_j}(\alpha_1) \in K$, für $1 \leq j \leq p$. Aus $\alpha_1, ..., \alpha_p \in K$ folgt $E = \mathbb{Q}(\alpha_1, ..., \alpha_p) \subseteq K$; weil andererseits K in E liegt, gilt damit insgesamt $K = E$.