Aufgabe H13T3A1 (6 Punkte)

Sei $r \geq 1$. Die komplexen Zahlen $\alpha_1, ..., \alpha_r$ seien alle algebraisch vom Grad 2 über $\mathbb{Q}$. Setze $K = \mathbb{Q}(\alpha_1, ..., \alpha_r)$. Zeigen Sie, dass K eine Galoiserweiterung von $\mathbb{Q}$ ist. Sei $G = \text{Gal}(K|\mathbb{Q})$ und C_2 eine Gruppe der Ordnung 2. Geben Sie einen natürlichen injektiven Gruppenhomomorphismus $G \to C_2^r$ an.

Lösung:

Für $1 \leq i \leq r$ sei $f_i \in \mathbb{Q}[x]$ jeweils das Minimalpolynom von α_i über $\mathbb{Q}$. Für jedes i gilt jeweils $\text{grad}(f_i) = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 2$. Da f_i als irreduzibles Polynom über $\mathbb{Q}$ wegen $\text{char}(\mathbb{Q}) = 0$ separabel ist, besitzt f_i in $\mathbb{C}$ genau eine von α_i verschiedene Nullstelle, die wir mit β_i bezeichnen. Wir definieren $P_i = \text{Per}(\{\alpha_i, \beta_i\})$ für $1 \leq i \leq r$. Wegen $|\{\alpha_i, \beta_i\}| = 2$ gilt $|P_i| = |S_2| = 2$.

Sei $i \in \{1, ..., r\}$ und $\sigma \in G$. Da das Bild jeder Nullstelle von f_i unter σ wiederum eine Nullstelle von f_i ist, gilt $\sigma(\{\alpha_i, \beta_i\}) \subseteq \{\alpha_i, \beta_i\}$. Als Körperhomomorphismus ist σ injektiv, somit auch die Einschränkung $\sigma_i : \sigma|_{\{\alpha_i, \beta_i\}}$ als Abbildung $\{\alpha_i, \beta_i\} \to \{\alpha_i, \beta_i\}$. Weil die Menge $\{\alpha_i, \beta_i\}$ endlich ist, ist σ_i auch surjektiv, insgesamt gilt also $\sigma_i \in P_i$.

Als Gruppen der Primzahlordnung 2 sind P_i und C_2 beide zyklisch von Ordnung 2 und somit isomorph zueinander. Für $1 \leq i \leq r$ sei $\tau_i : P_i \to C_2$ jeweils ein Isomorphismus. Wir definieren nun eine Abbildung $\phi : G \to C_2^r$ durch

$$\phi(\sigma) \quad = \quad (\tau_1(\sigma_1), ..., \tau_r(\sigma_r)).$$

Wir müssen überprüfen, dass ϕ ein Gruppenhomomorphismus und außerdem injektiv ist. Für beliebige $\rho, \sigma \in G$ gilt offenbar $(\rho \circ \sigma)_i = \rho_i \circ \sigma_i$ für $1 \leq i \leq r$, also

$$\phi(\sigma\rho) \quad = \quad (\tau_1((\sigma\rho)_1), ..., \tau_r((\sigma\rho)_r)) \quad = \quad (\tau_1(\sigma_1\rho_1), ..., \tau_r(\sigma_r\rho_r)) \quad =$$
$$(\tau_1(\sigma_1)\tau_1(\rho_1), ..., \tau_r(\sigma_r)\tau_r(\rho_r)) \quad = \quad (\tau_1(\rho_1), ..., \tau_r(\rho_r)) \cdot (\tau_1(\sigma_1), ..., \tau_r(\sigma_r)) \quad = \quad \phi(\sigma) \cdot \phi(\rho).$$

Damit ist die Homomorphismus-Eigenschaft nachgewiesen. Zum Nachweis der Injektivität sei $\sigma \in G$ mit $\phi(\sigma) = e_{C_2^r} = (e_{C_2}, ..., e_{C_2})$ vorgegeben, wobei e_H jeweils das Neutralelement einer Gruppe H bezeichnet. Dann folgt $\tau_i(\sigma_i) = e_{C_2}$ für $1 \leq i \leq r$. Da τ_i ein Isomorphismus ist, erhalten wir $\sigma|_{\{\alpha_i, \beta_i\}} = \sigma_i = e_{P_i} = \text{id}_{\{\alpha_i, \beta_i\}}$ und somit $\sigma(\alpha_i) = \sigma_i(\alpha_i) = \alpha_i$ für $1 \leq i \leq r$. Wegen $K = \mathbb{Q}(\alpha_1, ..., \alpha_r)$ ist jedes Element aus G durch die Bilder von $\alpha_1, ..., \alpha_r$ bereits eindeutig festgelegt. Also muss $\sigma = \text{id}_K$ gelten.