Aufgabe H16T1A5 (12 Punkte)

Sei f ein separables Polynom über $\mathbb{Q}$, welches in der Form $f(x) = h(x^2)$ mit $h \in \mathbb{Q}[x]$ und $n = \text{grad}(h) \geq 2$ geschrieben werden kann. Zeigen Sie, dass die Galoisgruppe (eines Zerfällungskörpers) von f nicht die volle symmetrische Gruppe S_{2n} der Nullstellen sein kann.

Lösung:

Sei $L \subseteq \mathbb{C}$ ein Zerfällungskörper von f über $\mathbb{Q}$. Wegen $f(x) = h(x^2)$ gilt $\text{grad}(f) = 2\text{grad}(h) = 2n$. Da f separabel ist, besitzt f genau $2n$ verschiedene Nullstellen $\alpha_1, ..., \alpha_{2n} \in \mathbb{C}$. Ist $\alpha \in \mathbb{C}$ eine beliebige Nullstelle von f, dann ist wegen $f(-\alpha) = h((-\alpha)^2) = h(\alpha^2) = f(\alpha)$ auch $-\alpha$ eine Nullstelle von f. Nach Umnummerierung können wir daher voraussetzen, dass $\alpha_{2k} = -\alpha_{2k-1}$ für $1 \leq k \leq n$ erfüllt ist.

Sei $G = \text{Gal}(L|\mathbb{Q}) = \text{Gal}(f|\mathbb{Q})$. Laut Vorlesung existiert ein Monomorphismus $\phi : G \to S_{2n}$ von Gruppen mit $\sigma(\alpha_i) = \alpha_{\phi(\sigma)(i)}$ für $1 \leq i \leq 2n$. Nehmen wir nun an, dass $\phi(G) = S_{2n}$ gilt. Dann existiert auch ein $\sigma \in G$ mit $\phi(\sigma) = (1\ 2\ 3)$. Für dieses Element gilt dann $\sigma(\alpha_1) = \alpha_{\phi(\sigma)(1)} = \alpha_{(1\ 2\ 3)(1)} = \alpha_2$, und ebenso erhält man $\sigma(\alpha_2) = \alpha_3$ und $\sigma(\alpha_3) = \alpha_1$. Andererseits gilt aber $\alpha_2 = -\alpha_1$, und daraus folgt $\sigma(\alpha_2) = \sigma(-\alpha_1) = -\sigma(\alpha_1) = -\alpha_2 = \alpha_1$, im Widerspruch zu $\sigma(\alpha_2) = \alpha_3$. Dies zeigt, dass die Annahme $\phi(G) = S_{2n}$ falsch war.

Hinweis:
Laut Vorlesung ist ein irreduzibles Polynom $f \in K[x]$ über einem Körper K *separabel* genau dann, wenn $\text{ggT}(f, f') = 1$ gilt. Dies ist äquivalent dazu, dass f in jedem Erweiterungskörper von K nur einfache Nullstellen besitzt. Für *reduzible* Polynome f wird die Eigenschaft „separabel“ je nach Lehrbuch unterschiedlich definiert. Einige Autoren bezeichnen auch ein reduzibles Polynom f als separabel, wenn $\text{ggT}(f, f') = 1$ ist. In anderen Quellen ist ein reduzibles Polynom separabel, wenn alle irreduziblen Faktoren separabel sind. Die beiden Definitionen sind nicht äquivalent, denn beispielsweise ist das Polynoom $(x + 1)^2$ in $\mathbb{Q}[x]$ nach der zweiten Definition separabel, nach der ersten aber nicht.

Bei der Lösung dieser Aufgabe wurde von der ersten Definition ausgegangen. Legt man die zweite Definition zu Grunde, muss die Lösung geringfügig abgeändert werden: Die Anzahl der verschiedenen Nullstellen von f ist dann nicht notwendigerweise gleich $2n$, sondern gleich $2m$ für ein $m \leq n$. Im Fall $m < n$ ist sofort klar, dass die Galoisgruppe nicht mit S_{2n} übereinstimmt, da die Gruppenordnung höchstens $(2m)!$ ist. Im Fall $m = n$ bleibt die Argumentation der Originalfassung gültig.