Aufgabe H16T3A5 (12 Punkte)

Finden Sie zwei Polynome $f, g \in \mathbb{Q}[x]$ gleichen Grades, so dass $\mathrm{Gal}(f)$ und $\mathrm{Gal}(g)$ gleich viele Elemente haben, aber $\mathrm{Gal}(f)$ abelsch und $\mathrm{Gal}(g)$ nicht abelsch ist.

Lösung:

Sei $f = \Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ das siebte Kreisteilungspolynom und $g = (x^3 - 2)(x-1)(x-2)(x-3)$. Dann sind f und g beides Polynome vom Grad 6. Laut Vorlesung ist der Zerfällungskörper von f über $\mathbb{Q}$ der Kreisteilungskörper $\mathbb{Q}(\zeta_7)$ mit $\zeta_7 = e^{2\pi i/7}$, und $\mathbb{Q}(\zeta_7)|\mathbb{Q}$ ist eine Galois-Erweiterung. Es gilt $\mathrm{Gal}(f|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_7)|\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$, also ist $\mathrm{Gal}(f|\mathbb{Q})$ abelsch. Außerdem gilt $|\mathrm{Gal}(f|\mathbb{Q})| = |(\mathbb{Z}/7\mathbb{Z})^\times| = \varphi(7) = 6$, wobei φ die Eulersche φ-Funktion bezeichnet. Wir zeigen nun, dass $\mathrm{Gal}(g|\mathbb{Q})$ ebenfalls eine Gruppe der Ordnung 6, aber nichtabelsch ist.

Die Nullstellenmenge von g ist gegeben durch $N = \{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}, 1, 2, 3\}$, mit $\zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Es gilt

$$\mathbb{Q}(N) \quad = \quad \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \qquad ,$$

denn einerseits gilt $N \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ wegen $1, 2, 3 \in \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, und weil mit $\sqrt[3]{2}, \zeta_3$ auch $\zeta_3\sqrt[3]{2}$ und $\zeta_3^2\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{},\zeta_3)$ enthalten sind. Andererseits enthält $\mathbb{Q}(N)$ mit $\sqrt[3]{2}$ und $\zeta_3\sqrt[3]{2}$ auch $\zeta_3 = \frac{\zeta_3\sqrt[3]{2}}{\sqrt[3]{2}}$, folglich ist auch $\{\sqrt[3]{2}, \zeta_3\} \subseteq \mathbb{Q}(N)$ erfüllt. Die Gleichung zeigt, dass $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ der Zerfällungskörper von g über $\mathbb{Q}$ ist. Als Zerfällungskörper ist L normal über $\mathbb{Q}$, also insbesondere algebraisch und wegen $\mathrm{char}(\mathbb{Q})$ auch separabel über $\mathbb{Q}$. Nach Definition der Galoisgruppe eines Polynoms gilt $\mathrm{Gal}(g|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q})$.

Wir bestimmen nun den Grad der Erweiterung $L|\mathbb{Q}$. Das Polynom $h = x^3 - 2 \in \mathbb{Q}[x]$ ist auf Grund des Eisenstein-Kriteriums irreduzibel, außerdem normiert, und es gilt $h(\sqrt[3]{2}) = 0$. Also ist h das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \mathrm{grad}(h) = 3$. Das dritte Kreisteilungspolynom $k = x^2 + x + 1 \in Q[x]$ ist ebenfalls normiert, und es gilt $k(\zeta_3) = 0$. Wäre es über $\mathbb{Q}(\sqrt[3]{2})$ reduzibel, dann wären wegen $\mathrm{grad}(k) = 2$ die beiden Nullstellen ζ_3, ζ_3^2 in $\mathbb{Q}(\sqrt[3]{2})$ enthalten. Aber dies ist wegen $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ und $\zeta_3, \zeta_3^2 \notin \mathbb{R}$ unmöglich. Also ist k das Minimalpolynom von ζ_3 über $\mathbb{Q}(\sqrt[3]{2})$. Es folgt $[L : \mathbb{Q}(\sqrt[3]{2})] = [\mathbb{Q}(\sqrt[3]{2})(\zeta_3) : \mathbb{Q}(\sqrt[3]{2})] = \mathrm{grad}(k) = 2$, und mit der Gradformel erhalten wir

$$[L : \mathbb{Q}] \quad = \quad [L : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \quad = \quad 2 \cdot 3 \quad = \quad 6.$$

Da $L|\mathbb{Q}$ eine Galois-Erweiterung ist, folgt daraus $|\mathrm{Gal}(g|\mathbb{Q})| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 6$.

Nun zeigen wir noch, dass $\mathrm{Gal}(g|\mathbb{Q})$ nicht abelsch ist. Der Körper L ist nicht nur Zerfällungskörper von g, sondern auch von h. Um dies zu zeigen, bemerken wir zunächst, dass die Nullstellenmenge von h in $\mathbb{C}$ durch $M = \{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$ gegeben ist. Außerdem gilt $\mathbb{Q}(M) = \mathbb{Q}(N)$. Denn die Inklusion „$\subseteq$" ist wegen $M \subseteq N$ offensichtlich, umgekehrt gilt aber auch $N \subseteq \mathbb{Q}(M)$ wegen $N = \{1, 2, 3\} \cup M$ und $1, 2, 3 \in \mathbb{Q} \subseteq \mathbb{Q}(M)$. Aus $\mathbb{Q}(M) = \mathbb{Q}(N) = L$ folgt $\mathrm{Gal}(h|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(M)|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q})$. Als Galoisgruppe eines Polynoms vom Grad 3 ist $\mathrm{Gal}(h|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q}) = \mathrm{Gal}(g|\mathbb{Q})$ isomorph zu einer Untergruppe von S_3. Wegen $|\mathrm{Gal}(g|\mathbb{Q})| = 6 = |S_3|$ ist $\mathrm{Gal}(g|\mathbb{Q})$ also zu S_3 isomorph. Bekanntlich ist S_3 eine nichtabelsche Gruppe, also ist auch $\mathrm{Gal}(g|\mathbb{Q})$ nicht abelsch.