Aufgabe F14T2A4 (3+3+3+3+4 Punkte)

Seien $a, b \in \mathbb{Q}$, und sei K der Zerfällungskörper des Polynoms

$$p \quad = \quad x^3 + ax + b \in \mathbb{Q}[x].$$

Wir nehmen an, dass p keine Nullstellen in $\mathbb{Q}$ hat. Zeigen Sie:

(a) p ist irreduzibel in $\mathbb{Q}[x]$ und hat keine mehrfachen Nullstellen in K.

(b) Die Galoisgruppe $G = \mathrm{Gal}(K|\mathbb{Q})$ ist eine Untergruppe von S_3.

(c) G hat entweder 3 oder 6 Elemente.

(d) Sei $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, wobei $\alpha_1, \alpha_2, \alpha_3 \in K$ die Nullstellen von p sind. Dann gilt für $\sigma \in G$ stets $\sigma(\delta) = \delta$ oder $\sigma(\delta) = -\delta$.

(e) Gilt $\sigma(\delta) = \delta$ für alle $\sigma \in G$, dann ist G zyklisch und hat Ordnung 3. Anderenfalls ist $G = S_3$.

Lösung:

zu (a) Da p ein Polynom vom Grad 3 ist, folgt aus der Nichtexistenz rationaler Nullstellen die Irreduzibilität in $\mathbb{Q}[x]$. Denn angenommen, $p = gh$ wäre eine Zerlegung von p in nicht-konstante Polynome $g, h \in \mathbb{Q}[x]$. Wegen $\mathrm{grad}(g) + \mathrm{grad}(h) = \mathrm{grad}(p) = 3$ wäre dann eines der Polynome g, h vom Grad 1. Dieses hätte eine rationale Nulllstelle, somit auch das Polynom p. Desweiteren ist aus der Vorlesung bekannt, dass jedes irreduzible Polynom über einem Körper der Charakteristik 0 (hier der Körper $\mathbb{Q}$) separabel ist. Dies bedeutet, dass p in keinem Erweiterungskörper von $\mathbb{Q}$ mehrfache Nullstellen besitzt, auch nicht im Körper K.

zu (b) Aus der Vorlesung ist folgender Satz bekannt: Sei $f \in K[x]$ ein Polynom mit separablem Zerfällungskörper $L \supseteq K$, sei $G = \mathrm{Gal}(L|K)$, und seien $\alpha_1, ..., \alpha_n \in L$ die verschiedenen Nullstellen von f. Dann gibt es einen Monomorphismus $\phi : G \to S_n$ von Gruppen mit $\sigma(\alpha_i) = \sigma(\alpha_{\phi(\sigma)(i)}$ für alle $\sigma \in \mathrm{Gal}(L|K)$ und $1 \leq i \leq n$.

Als algebraische Erweiterung von $\mathbb{Q}$ ist $K|\mathbb{Q}$ separabel, und weil das Polynom p nach Teil (a) keine mehrfachen Nullstellen in K besitzt, hat es in K drei verschiedene Nullstellen $\alpha_1, \alpha_2, \alpha_3$. Somit liefert uns der Satz (angewendet auf $K = \mathbb{Q}$, $L = K$, $f = p$ und $n = 3$) einen Monomorphismus $\phi : G \to S_3$ mit der angegebenen Eigenschaft, wobei $G = \mathrm{Gal}(K|\mathbb{Q})$ ist. Auf Grund der Injektivität ist G isomorph zu $\phi(G)$, einer Untergruppe S_3.

(Die Formulierung in der Aufgabenstellung, dass G eine Untergruppe von S_3 „ist“, sehe ich als ungenau an, denn selbstverständlich sind Automorphismen von K etwas anderes als Permutationen der Menge $\{1, 2, 3\}$. Allerdings haben viele Autoren die - meiner Meinung nach oft irreführende - Gewohnheit, isomorphe Strukturen direkt als „gleich“ anzusehen.)

zu (c) Auf Grund des Fortsetzungssatzes und der Irreduzibilität des Polynoms p gibt es für je zwei Nullstellen $\alpha, \beta \in K$ von p jeweils einen Automorphismus $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Insbesondere gibt es für jedes $i \in \{1, 2, 3\}$ (mindestens) einen Automorphismus $\sigma_i \in G$ mit $\sigma(\alpha_1) = \alpha_i$. Daraus folgt $|G| \geq 3$. Andererseits ist G nach Teil (b) isomorph zu einer Untergruppe von S_3, somit muss $|G|$ ein Teiler von $|S_3| = 6$ sein. Insgesamt erhalten wir damit $|G| \in \{3, 6\}$.

zu (d) Jeder Automorphismus liefert eine Permutation der Nullstellen. Somit ist intuitiv „klar“, dass jeder Automorphismus bis auf Vorzeichen die Differenzen $\alpha_i - \alpha_j$ lediglich vertauscht. Das einzige Problem besteht darin, dies auf formale Weise auszudrücken. Ein möglicher Weg ist der folgende: Sei $\mathcal{S}$ die Menge der zweielementigen Teilmengen von $\{1, 2, 3\}$, also

$$\mathcal{S} \quad = \quad \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

Setzen wir für jedes $T = \{i, j\} \in \mathcal{S}$ jeweils $\alpha_T = (\alpha_i - \alpha_j)^2$, dann gilt $\delta = \prod_{T \in \mathcal{S}} \alpha_T$. Sei nun $\sigma \in G$ und $\tilde{\sigma} = \phi(\sigma) \in S_3$ die zugehörige Permutation. Nach Definition gilt $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ für $1 \leq i \leq 3$ und somit für jedes $T = \{i, j\} \in \mathcal{S}$ jeweils

$$\sigma(\alpha_T) \quad = \quad \sigma((\alpha_i - \alpha_j)^2) \quad = \quad (\sigma(\alpha_i) - \sigma(\alpha_j))^2 \quad = \quad (\alpha_{\tilde{\sigma}(i)} - \alpha_{\tilde{\sigma}(j)})^2 \quad = \quad \alpha_{\tilde{\sigma}(T)}$$

mit $\tilde{\sigma}(T) = \{\tilde{\sigma}(i), \tilde{\sigma}(j)\}$, wobei im zweiten Schritt die Automorphismus-Eigenschaft von σ verwendet wurde. Auf Grund der Bijektivität von $\tilde{\sigma}$ durchläuft mit T auch $\sigma(T)$ die gesamte Menge $\mathcal{S}$. Daraus folgt

$$\sigma(\delta)^2 \quad = \quad \sigma(\delta^2) \quad = \quad \sigma\left(\prod_{T \in \mathcal{S}} \alpha_T\right) \quad = \quad \prod_{T \in \mathcal{S}} \alpha_{\tilde{\sigma}(T)} \quad = \quad \prod_{T \in \mathcal{S}} \alpha_T \quad = \quad \delta^2.$$

Aus $\sigma(\delta)^2 = \delta^2$ wiederum folgt $\sigma(\delta) = \delta$ oder $\sigma(\delta) = -\delta$.

zu (e) Aus Teil (c) ist bereits bekannt, dass $|G| \in \{3, 6\}$ gilt. Ist $\sigma(\delta) = \delta$ für alle $\sigma \in G$, dann ist $\phi(G)$ eine echte Untergruppe von S_3. Denn andernfalls gäbe es ein Element $\sigma \in G$ mit $\tilde{\sigma} = \phi(\sigma) = (1\ \ 2)$, und es würde

$$\begin{aligned} \sigma(\delta) \quad &= \quad \sigma\left((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\right) \quad = \quad (\alpha_{\tilde{\sigma}(1)} - \alpha_{\tilde{\sigma}(2)})(\alpha_{\tilde{\sigma}(1)} - \alpha_{\tilde{\sigma}(3)}(\alpha_{\tilde{\sigma}(2)} - \alpha_{\tilde{\sigma}(3)}) \\ &= \quad (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \quad = \quad -\delta \end{aligned}$$

gelten. Da die drei Nullstellen $\alpha_1, \alpha_2, \alpha_3$ aber verschieden sind, ist $\delta \neq 0$, und somit steht $\sigma(\delta) = -\delta$ im Widerspruch zu $\sigma(\delta) = \delta$. Es gilt also $|G| = |\phi(G)| < |S_3| = 6$, und damit ist $|G| = 3$ die einzige Möglichkeit. Als Gruppe von Primzahlordnung ist G auch zyklisch.

Nehmen wir nun an, dass ein $\sigma \in G$ mit $\sigma(\delta) = -\delta$ existiert. Dann muss $\mathrm{ord}(\sigma) = 2$ gelten, denn im Fall $\mathrm{ord}(\sigma) = 3$ würde sich der Widerspruch

$$\delta \quad = \quad \mathrm{id}_K(\delta) \quad = \quad \sigma^3(\delta) \quad = \quad (-1)^3(\delta) \quad = \quad -\delta$$

ergeben, und ebenso ist $\mathrm{ord}(\sigma) = 1$ ausgeschlossen. Durch $\mathrm{ord}(\sigma) = 2$ ist aber $|G| = 3$ ausgeschlossen. Also muss $|G| = 6$ gelten. Die Gruppe G ist somit isomorph zu einer sechselementigen Untergruppe von S_3, wegen $|S_3| = 6$ also zu S_3 selbst.