Aufgabe F16T3A5 (15 Punkte)

Sei $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$.

(a) Zeigen Sie, dass

$$\alpha_1 = \sqrt{1+\sqrt{3}}, \quad \alpha_2 = \sqrt{1-\sqrt{3}}, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2$$

die Nullstellen von f in $\mathbb{C}$ sind.

(b) Zeigen Sie, dass $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ (als Teilkörper von $\mathbb{C}$).

(c) Zeigen Sie, dass $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$.

(d) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(\alpha_1)|\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\alpha_2)|\mathbb{Q}(\sqrt{3})$ galoissch sind.

(e) Sei K der Zerfällungskörper von f über $\mathbb{Q}$. Zeigen Sie, dass $K|\mathbb{Q}(\sqrt{3})$ galoissch ist und bestimmen Sie den Isomorphietyp der Galois-Gruppe.

Lösung:

zu (a) Für jedes $\alpha \in \mathbb{C}$ gilt die Äquivalenz

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \alpha^4 - 2\alpha^2 - 2 = 0 \quad \Leftrightarrow \quad \alpha^4 - 2\alpha^2 + 1 = 3 \quad \Leftrightarrow \quad (\alpha^2-1)^2 = 3 \quad \Leftrightarrow$$

$$(\alpha^2-1)^2 - \sqrt{3}^2 = 0 \quad \Leftrightarrow \quad (\alpha^2 - 1 - \sqrt{3})(\alpha^2 - 1 + \sqrt{3}) = 0 \quad \Leftrightarrow \quad \alpha^2 = 1+\sqrt{3} \ \vee \ \alpha^2 = 1 - \sqrt{3} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad \alpha = \pm\sqrt{1+\sqrt{3}} \ \vee \ \alpha = \pm\sqrt{1-\sqrt{3}} \quad \Leftrightarrow \quad \alpha = \pm\alpha_1 \ \vee \ \alpha = \pm\alpha_2 \quad \Leftrightarrow \quad \alpha \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}.$$

zu (b) Wegen $1+\sqrt{3} > 0$ gilt $\alpha_1 \in \mathbb{R}$ und somit $\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$. Andererseits ist $1-\sqrt{3} < 0$, also $\alpha_2 \notin \mathbb{R}$ und $\mathbb{Q}(\alpha_2)$ somit kein Teilkörper von $\mathbb{R}$. Dies zeigt, dass die Körper $\mathbb{Q}(\alpha_1)$ und $\mathbb{Q}(\alpha_2)$ nicht übereinstimmen.

zu (c) Es gilt $1 + \sqrt{3} = \alpha_1^2 \in \mathbb{Q}(\alpha_1)$, somit $\sqrt{3} \in \mathbb{Q}(\alpha_1)$ und $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_1)$. Ebenso gilt $1 - \sqrt{3} = \alpha_2^2 \in \mathbb{Q}(\alpha_2)$, woraus $\sqrt{3} \in \mathbb{Q}(\alpha_2)$ und $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_2)$ folgt. Damit ist insgesamt $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$ bewiesen. Um nun zu zeigen, dass $\mathbb{Q}(\sqrt{3})$ mit $M = \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$ übereinstimmt, bemerken wir zunächst, dass das Polynom f nach dem Eisenstein-Kriterium für $p = 2$ in $\mathbb{Q}[x]$ irreduzibel ist. Außerdem ist f normiert, und es gilt $f(\alpha_1) = 0$ nach Teil (a). Also ist f das Minimalpolynom von α_1 über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \mathrm{grad}(f) = 4$. Das Element $\sqrt{3}$ ist Nullstelle des Polynoms $x^2 - 3$, das ebenfalls nach Eisenstein (für $p = 3$) irreduzibel ist. Daraus folgt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \mathrm{grad}(x^2 - 3) = 2$. Mit dem Gradsatz erhalten wir nun

$$4 \quad = \quad [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha_1) : M] \cdot [M : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha_1) : M] \cdot [M : \mathbb{Q}(\sqrt{3})] \cdot 2.$$

Wegen $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ ist M ein echter Teilkörper von $\mathbb{Q}(\alpha_1)$, also gilt $[\mathbb{Q}(\alpha_1) : M] > 1$. Auf Grund der soeben bewiesenen Gleichung muss dann $[M : \mathbb{Q}(\sqrt{3})] = 1$, also $M = \mathbb{Q}(\sqrt{3})$ gelten.

zu (d) Wir haben bereits in Teil (c) gezeigt, dass $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$ gilt. Da auch α_2 eine Nullstelle von f ist, erhalten wir ebenso $[\mathbb{Q}(\alpha_2) : \mathbb{Q}] = 4$. Mit dem Gradsatz folgt

$$[\mathbb{Q}(\alpha_i) : \mathbb{Q}(\sqrt{3})] \quad = \quad \frac{[\mathbb{Q}(\alpha_i) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]} \quad = \quad \frac{4}{2} \quad = \quad 2$$

für $i = 1, 2$. Aus der Vorlesung ist bekannt, dass jede Erweiterung vom Grad 2 normal ist. Als endliche Erweiterung ist $\mathbb{Q}(\alpha_i)|\mathbb{Q}(\sqrt{3})$ algebraisch und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel. Insgesamt handelt es sich bei $\mathbb{Q}(\alpha_i)|\mathbb{Q}(\sqrt{3})$ für $i = 1, 2$ also um Galois-Erweiterungen.

zu (e) Als Zerfällungskörper von f über $\mathbb{Q}$ ist K auch Zerfällungskörper von f über $\mathbb{Q}(\sqrt{3})$. Dies zeigt, dass die Erweiterung $K|\mathbb{Q}(\sqrt{3})$ normal ist. Wegen $\mathrm{char}\ \mathbb{Q}(\sqrt{3}) = 0$ ist sie auch separabel, insgesamt also eine Galois-Erweiterung.

Weil $\alpha_1, ..., \alpha_4$ die Nullstellen von f sind, gilt $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ nach Definition des Zerfällungskörpers von f über $\mathbb{Q}$. Wegen $\alpha_3 = -\alpha_1$ und $\alpha_4 = -\alpha_2$ folgt $K = \mathbb{Q}(\alpha_1, \alpha_2)$. Seien $g \in \mathbb{Q}(\sqrt{3})[x]$ und $h \in \mathbb{Q}(\alpha_1)[x]$ die Minimalpolynome von α_2 über $\mathbb{Q}(\sqrt{3})$ bzw. $\mathbb{Q}(\alpha_1)$. Wegen $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_1)$ ist das Polynom g auch in $\mathbb{Q}(\alpha_1)[x]$ enthalten und wegen $g(\alpha_2) = 0$ somit ein Vielfaches von h. Aus $\mathrm{grad}(g) = [\mathbb{Q}(\sqrt{3}, \alpha_2) : \mathbb{Q}(\sqrt{3})] = 2$ folgt $\mathrm{grad}(h) \leq 2$. Wäre $\mathrm{grad}(h) = 1$, dann würde $\alpha_2 \in \mathbb{Q}(\alpha_1)$ und $\mathbb{Q}(\alpha_2) \subseteq \mathbb{Q}(\alpha_1)$ folgen. Zusammen mit

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha_2) : \mathbb{Q}] \quad = \quad 4$$

würde daraus $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$ folgen, im Widerspruch zu Aufgabenteil (b). So aber erhalten wir

$$[K : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \quad =$$

$$\mathrm{grad}(h) \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \quad = \quad 2 \cdot 4 \quad = \quad 8$$

und

$$[K : \mathbb{Q}(\sqrt{3})] \quad = \quad \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]} \quad = \quad \frac{8}{2} \quad = \quad 4.$$

Sei nun $G = \mathrm{Gal}(K|\mathbb{Q}(\sqrt{3}))$. Dann gilt $|G| = [K : \mathbb{Q}(\sqrt{3})] = 4$. Weil die Zahl 4 ein Primzahlquadrat ist, handelt es sich bei G um eine abelsche Gruppe. Nach dem Hauptsatz über endliche abelsche Gruppen ist G isomorph zu einem direkten Produkt zyklischer Gruppen, es gilt also $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im Fall $G \cong \mathbb{Z}/4\mathbb{Z}$ wäre G zyklisch. Weil die 4 nur einen einzigen nichttrivialen Teiler besitzt (nämlich 2), hätte G dann nur eine einzige Untergruppe $U \neq \{\mathrm{id}\}, G$. Nach dem Hauptsatz der Galoistheorie hätte die Erweiterung $K|\mathbb{Q}(\sqrt{3})$ damit genau einen echten Zwischenkörper. Aber wie wir gesehen haben, sind $\mathbb{Q}(\alpha_1), \mathbb{Q}(\alpha_2)$ beides Zwischenkörper der Erweiterung, wegen

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \quad < \quad [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 4 \quad < \quad [K : \mathbb{Q}] = 8$$

für $i = 1, 2$ sogar echte Zwischenkörper. Nach Teil (b) sind diese beiden Zwischenkörper voneinander verschieden. Also muss $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gelten.