Aufgabe H15T1A4 (2+2+4+4 Punkte)

Sei f das Polynom $x^3 - x + 2 \in \mathbb{Z}[x]$. Zeigen Sie die folgenden Behauptungen:

(a) Das Bild von f in $\mathbb{F}_3[x]$ ist irreduzibel.

(b) Das Polynom f ist irreduzibel in $\mathbb{Q}[x]$.

(c) Das Polynom f hat genau eine reelle Nullstelle.

(d) Die Galoisgruppe des Zerfällungskörpers von f über $\mathbb{Q}$ ist isomorph zu S_3.

Lösung:

zu (a) Sei $\bar{f}$ das Bild von f in $\mathbb{F}_3[x]$. Es gilt $\bar{f}(\bar{0}) = \bar{2}$, $\bar{f}(\bar{1}) = \bar{1}^3 - \bar{1} + \bar{2} = \bar{2}$ und $\bar{f}(\bar{2}) = \bar{2}^3 - \bar{2} + \bar{2} = \bar{8} = \bar{2}$. Also hat $\bar{f}$ in $\mathbb{F}_3$ keine Nullstellen. Wegen $\operatorname{grad}(\bar{f}) = 3$ folgt daraus, dass $\bar{f}$ in $\mathbb{F}_3[x]$ irreduzibel ist.

zu (b) Aus der Irreduzibilität von $\bar{f}$ in $\mathbb{F}_3[x]$ folgt nach dem Reduktionskriterium die Irreduzibilität von f in $\mathbb{Z}[x]$. Das Gaußsche Lemma zeigt, dass f auch in $\mathbb{Q}[x]$ irreduzibel ist.

zu (c) Wegen $f \in \mathbb{R}[x]$ treten alle nicht-reellen Nullstellen von f in konjugiert-komplexen Paaren auf. Daraus folgt, dass f entweder genau eine oder genau drei reelle Nullstellen besitzt. Um zu zeigen, dass es nur eine reelle Nullstelle gibt, untersuchen wir das Monotonieverhalten von f. Es gilt $f'(x) = 3x^2 - 1$, die einzigen beiden Nullstellen der Ableitung sind $\pm\frac{1}{\sqrt{3}}$. Dabei gilt

$$f(-\tfrac{1}{\sqrt{3}}) = -\tfrac{1}{3\sqrt{3}} + \tfrac{1}{\sqrt{3}} + 2 > 2 > 0 \qquad \text{und} \qquad f(\tfrac{1}{\sqrt{3}}) = \tfrac{1}{3\sqrt{3}} - \tfrac{1}{\sqrt{3}} + 2 > (-1) + 2 > 0.$$

Auf dem Intervall $]-\infty, -\frac{1}{\sqrt{3}}[$ gilt $f'(x) > 0$, also ist f dort streng monoton wachsend. Also kann es dort nicht mehr als eine Nullstelle geben. Auf dem Intervall $]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}[$ gilt $f'(x) < 0$, deshalb ist f dort streng monoton fallend. Wegen $f(-\frac{1}{\sqrt{3}}) > 0$ und $f(\frac{1}{\sqrt{3}}) > 0$ gibt es dort keine Nullstelle. Schließlich gilt $f'(x) > 0$ auf dem Intervall $]\frac{1}{\sqrt{3}}, +\infty[$, also ist f dort wieder streng monoton wachsend. Wegen $f(\frac{1}{\sqrt{3}}) > 0$ existiert hier ebenfalls keine Nullstelle. Damit ist insgesamt gezeigt, dass f auf ganz $\mathbb{R}$ nicht mehr als eine Nullstelle besitzt.

zu (d) Sei $G = \operatorname{Gal}(f|K)$ die Galoisgruppe des Zerfällungskörpers $K \subseteq \mathbb{C}$ von f über $\mathbb{Q}$. Weil f als irreduzibles Polynom in $\mathbb{Q}[x]$ wegen $\operatorname{char}(\mathbb{Q}) = 0$ separabel ist, besitzt es drei *verschiedene* Nullstellen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. Nach Teil (c) ist genau eine dieser Nullstellen reell; nach eventueller Umnummerierung können wir also $\alpha_1 \in \mathbb{R}$ und $\alpha_2, \alpha_3 \in \mathbb{C} \setminus \mathbb{R}$ annehmen, wobei α_2, α_3 komplex-konjugiert zueinander sind, also $\bar{\alpha}_2 = \alpha_3$ gilt. Nach Definition des Zerfällungskörpers gilt $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

Außerdem liefert die Nummerierung der Nullstellen laut Vorlesung einen Isomorphismus von G auf eine Untergruppe $\tilde{G}$ von S_3. Auf Grund der Irreduzibilität von f ist $\tilde{G}$ eine *transitive* Untergruppe von S_3. Laut Vorlesung folgt daraus wiederum, dass die Ordnung $|\tilde{G}|$ von 3 geteilt wird.

Schränkt man die komplexe Konjugation auf $\mathbb{C}$ auf K ein, so erhält man einen $\mathbb{Q}$-Homomorphismus $\iota : K \to \mathbb{C}$. Weil K als Zerfällungskörper von f normal über $\mathbb{Q}$ ist, handelt es sich bei ι um eine $\mathbb{Q}$-Automorphismus von K, es gilt also $\iota \in G$. Wegen $\alpha_1 \in \mathbb{R}$ und $\bar{\alpha}_2 = \alpha_3$ gilt $\iota(\alpha_1) = \alpha_1$, $\iota(\alpha_2) = \alpha_3$ und $\iota(\alpha_3) = \alpha_2$. Das Bild von ι in S_3 ist also die Transposition (2 3). Dies zeigt, dass $\tilde{G}$ ein Element der Ordnung 2 enthält; also ist neben 3 auch 2 ein Teiler von $|\tilde{G}|$. Weil 2 und 3 teilerfremd sind, ist auch $6 = 2 \cdot 3$ ein Teiler von $|\tilde{G}|$, insbesondere gilt $|\tilde{G}| \leq 6 = |S_3|$. Zusammen mit $\tilde{G} \subseteq S_3$ folgt daraus $\tilde{G} = S_3$. Wegen $G \cong \tilde{G}$ ist G also isomorph zu S_3.