Aufgabe F18T1A4 (12 Punkte)

Gegeben sei das Polynom $p = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Weiter sei $Z \subseteq \mathbb{C}$ ein Zerfällungskörper von p über $\mathbb{Q}$. Zeigen Sie:

(a) p ist irreduzibel in $\mathbb{Q}[x]$.

(b) p hat genau drei reelle Nullstellen.

(c) Die Galois-Gruppe $\mathrm{Gal}(Z|\mathbb{Q})$ enthält ein Element der Ordnung 5 und ein Element der Ordnung 2.

Lösung:

zu (a) Die Irreduzibilität von p in $\mathbb{Z}[x]$ erhält man durch Anwendung des Eisenstein-Kriteriums mit der Primzahl 2, und mit dem Gaußschen Lemma folgt draus die Irreduzibilität von p in $\mathbb{Q}$.

zu (b) Es gilt $p(0) = 2 > 0$ und $p(1) = 1-4+2 = -1 < 0$. Weil $\mathbb{R} \to \mathbb{R}$, $x \mapsto p(x)$ als Polynomfunktion stetig ist, gibt es nach dem Zwischenwertsatz ein $\beta \in]0,1[$ mit $p(\beta) = 0$. Weil p ein normiertes Polynom ungeraden Grades ist, gilt

$$\lim_{x \to -\infty} p(x) = -\infty \qquad \text{und} \qquad \lim_{x \to +\infty} p(x) = +\infty.$$

Es gibt deshalb $\alpha_1, \gamma_1 \in \mathbb{R}$ mit $\alpha_1 < 0$, $p(\alpha_1) < 0$ und $\gamma_1 > 1$, $p(\gamma_1) > 0$. Durch erneute Anwendung des Zwischenwertsatzes erhält man wegen $p(1) < 0$ und $p(\gamma_1) > 0$ eine Nullstelle $\gamma \in]1, \gamma_1[$ von p, und eine weitere Anwendung liefert wegen $p(\alpha_1) < 0$, $p(0) > 0$ eine Nullstelle $\alpha \in]\alpha_1, 0[$. Insgesamt haben wir wegen $\alpha < 0 < \beta < 1 < \gamma$ nachgewiesen, dass p mindestens drei verschiedene reelle Nulllstellen besitzt.

Bei einem reellen Polynom ungleich Null ist die Anzahl der nicht-reellen Nullstellen in $\mathbb{C}$ stets gerade, weil diese in konjugiert-komplexen Paaren auftreten. Als irreduzibles Polynom in $\mathbb{Q}[x]$ ist p separabel, besitzt wegen $\mathrm{grad}(p) = 5$ also genau fünf verschiedene komplexe Nullstellen. Weil die Anzahl der nicht-reellen Nullstellen gerade ist, kommt für die Anzahl der reellen Nullstellen nur 1, 3 oder 5 in Frage. Die erste Möglichkeit haben wir im vorherigen Absatz bereits ausgeschlossen.

Nehmen wir nun an, dass p fünf verschiedene reelle Nullstellen $\xi_1 < \xi_2 < ... < \xi_5$ besitzt. Nach dem Satz von Rolle liegt zwischen zwei Nullstellen von p jeweils eine Nullstelle von $p' = 5x^4 - 4$, es gibt dann also mindestens vier reelle Nullstellen $\delta_1, ..., \delta_4$ mit $\xi_k < \delta_k < \xi_{k+1}$ für $k = 1,2,3,4$. Aber wegen $p'(\delta) = 0 \Leftrightarrow 5\delta^4 - 4 = 0 \Leftrightarrow \delta^4 = \frac{4}{5} \Leftrightarrow \delta = \pm\sqrt[4]{5}$ hat p' nur zwei reelle Nullstellen. Somit ist auch ausgeschlossen, dass p genau fünf reelle Nullstellen hat, und folglich hat p genau drei Nullstellen in $\mathbb{R}$.

zu (c) Zunächst zeigen wir, dass es in $G = \mathrm{Gal}(Z|\mathbb{Q})$ ein Element der Ordnung 5 gibt. Da Z Zerfällungskörper eines nicht-konstanten Polynoms $p \in \mathbb{Q}[x]$ ist, ist die Erweiterung $Z|\mathbb{Q}$ normal und insbesondere algebraisch. Als algebraische Erweiterung ist $Z|\mathbb{Q}$ wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel, insgesamt also eine Galois-Erweiterung. Daraus wiederum folgt $|G| = [Z : \mathbb{Q}]$.

Sei $\alpha \in \mathbb{C}$ eine Nullstelle von p. Dann ist α nach Definition des Zerfällungskörpers in Z enthalten. Daraus folgt $\mathbb{Q}(\alpha) \subseteq Z$. Weil p normiert, nach (a) irreduzibel ist und $p(\alpha) = 0$ gilt, handelt es sich bei p um das Minimalpolynom von α über $\mathbb{Q}$. Daraus folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(p) = 5$. Mit der Gradformel erhalten wir

$$|G| \quad = \quad [Z : \mathbb{Q}] \quad = \quad [Z : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad [Z : \mathbb{Q}(\alpha)] \cdot 5.$$

Weil 5 ein Primteiler von $|G|$ ist, existiert in G eine Untergruppe der Ordnung 5. Weil 5 Primzahl ist, ist diese zyklisch. Somit existiert in G auch ein Element der Ordnung 5.

Um zu zeigen, dass G auch ein Element der Ordnung 2 besitzt, betrachten wir die komplexe Konjugation $\iota : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$. Die Einschränkung $\tau = \iota|_Z$ ist dann ein $\mathbb{Q}$-Homomorphismus $Z \to \mathbb{C}$. Weil die Erweiterung $Z|\mathbb{Q}$ normal ist, ist dies auch ein $\mathbb{Q}$-Automorphismus, also ist τ ein Element aus $\mathrm{Aut}_{\mathbb{Q}}(Z) = G$. Für jedes Element $\beta \in Z$ gilt $\tau^2(\beta) = \iota^2(\beta) = \iota(\iota(\beta)) = \iota(\bar{\beta}) = \bar{\bar{\beta}} = \beta$. Daraus folgt $\tau^2 = \mathrm{id}_Z$. Weil p nach (b) genau drei reelle Nullstellen besitzt, muss es wegen $\mathrm{grad}(p) = 5$ mindestens auch ein Paar $\gamma, \bar{\gamma}$ konjugiert-komplexer nicht-reeller Nullstellen in $\mathbb{C}$ geben. Wegen $\gamma \in Z$ und $\tau(\gamma) = \iota(\gamma) = \bar{\gamma} \neq \gamma$ ist $\tau \neq \mathrm{id}_Z$. Insgesamt ist damit gezeigt, dass es sich bei τ um ein Element der Ordnung 2 in G handelt.