H15-T1-A4

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

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

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

c) Das Polynom $P(X)$ hat genau eine reelle Nullstelle.

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

Lösungsvorschlag. Zu a). Es gilt $P(0) = 2 = P(1) = P(2)$ in $\mathbb{F}_3$, insbesondere hat $P(X)$ keine Nullstelle in $\mathbb{F}_3$ und ist (da von Grad 3) damit irreduzibel in $\mathbb{F}_3[X]$.
Zu b). Aus Teil a) wissen wir, dass $P(X)$ irreduzibel in $\mathbb{F}_3[X]$ ist. Da der Grad von $P(X)$ bei der Reduktion modulo 3 nicht abnimmt, wissen wir also, dass $P(X)$ irreduzibel in $\mathbb{Z}[X]$ ist, und damit, nach Satz von Gauß, auch in $\mathbb{Q}[X]$.
Zu c). Betrachten wir die Ableitung $P'(X) = 3X^2 - 1$: Diese hat Nullstellen bei $\pm 1/\sqrt{3}$. Wir lesen ab, dass $P(X)$ auf den Intervallen $(-\infty, -1/\sqrt{3})$ und $(1/\sqrt{3}, \infty)$ streng monoton steigt und auf $(-1/\sqrt{3}, 1/\sqrt{3})$ fällt. Es ist aber offensichtlich $|X^3| < |X| < 1$ für $X \in (-1/\sqrt{3}, 1/\sqrt{3})$ und somit $P(X) > 0$ auf $(-1/\sqrt{3}, 1/\sqrt{3})$. Mithin kann $P(X)$ nur eine reelle Nullstelle in $(-\infty, -1/\sqrt{3})$ besitzen (und eine solche besitzt es sicherlich, beispielsweise nach dem Mittelwertsatz mit $P(-2) = -4 < 0$ oder aufgrund der Tatsache, dass Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ stets in konjugierten Paaren auftreten).
Zu d). Bezeichne $\mathrm{Gal}(P) := \mathrm{Gal}_{\mathbb{Q}}(P) := \mathrm{Gal}(L|\mathbb{Q}) := \mathrm{Aut}_{\mathbb{Q}}(L)$ die Galoisgruppe von P über $\mathbb{Q}$. Wir wissen bereits, dass $|\mathrm{Gal}(P)| \geq \deg(P) = 3$ gelten muss – da $\mathrm{Gal}(P)$ isomorph zu einer Untergruppe von S_3 ist, ist somit klar, dass $\mathrm{Gal}(P)$ entweder (isomorph zu) A_3 oder S_3 ist. Nach Teil c) wissen wir, dass P ein paar konjugierter Nullstellen in $\mathbb{C}\setminus\mathbb{R}$ bestitzt. Somit liefert die komplexe Konjugation einen nichttrivialen $\mathbb{Q}$-Automorphismus

$$\mathrm{Id} \neq \sigma\colon L \to L, \quad z \mapsto \overline{z},$$

wobei wir mit $\overline{z}$ das komplex Konjugierte zu z meinen. Bekanntlich gilt dabei aber $\sigma^2 = \mathrm{Id}$, womit $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L) = \mathrm{Gal}(P)$ ein Element der Ordnung 2 ist. Da ein solches in A_3 nicht existiert, muss also $\mathrm{Gal}(P) \simeq S_3$ gelten.