Aufgabe F15T1A5 (8+8 Punkte)

Sei $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad $n \geq 1$. Sei K ein Zerfällungskörper von f. Sei $G = \mathrm{Gal}(K|\mathbb{Q})$ die zugehörige Galoisgruppe.

(a) Beweisen Sie: Falls G eine abelsche Gruppe ist, hat sie die Ordnung n.

(b) Sei $K = \mathbb{Q}(\sqrt{2}, i)$, wobei $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$ ist. Bestimmen Sie ein irreduzibles Polynom $f \in \mathbb{Q}[x]$, dessen Zerfällungskörper K ist. Beweisen Sie, dass $G = \mathrm{Gal}(K|\mathbb{Q})$ abelsch, aber nicht zyklisch ist.

Lösung:

zu (a) Die Erweiterung $K|\mathbb{Q}$ ist galoissch, denn K ist als Zerfällungskörper des Polynoms $f \in \mathbb{Q}[x]$ normal über $\mathbb{Q}$, und als algebraische Erweiterung von $\mathbb{Q}$ ist $K|\mathbb{Q}$ wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel. Daraus folgt $|G| = [K : \mathbb{Q}]$. Sei $\alpha \in K$ eine Nullstelle von f. Weil f irreduzibel ist, gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = n$. Wegen $\mathbb{Q}(\alpha) \subseteq K$ ist insgesamt also $|G| = [K : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

Nehmen wir nun an, dass einerseits G abelsch ist, andererseits aber $[K : \mathbb{Q}] = |G| > n$ gilt. Dann ist $\mathbb{Q}(\alpha)$ ein echter Teilkörper von K. Da K von den Nullstellen des Polynoms f in K erzeugt wird, muss es also eine Nullstelle $\beta \in K$ von f mit $\beta \notin \mathbb{Q}(\alpha)$ geben. Weil f über $\mathbb{Q}$ irreduzibel und α, β beides Nullstellen von f sind, existiert nach dem Fortsetzungssatz ein Element $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Ist nun τ ein Element aus $\mathrm{Gal}(K|\mathbb{Q}(\alpha))$, also $\tau \in G$ mit $\tau(\alpha) = \alpha$, dann gilt zugleich auch

$$\tau(\beta) \quad = \quad \tau(\sigma(\alpha)) \quad = \quad (\tau \circ \sigma)(\alpha) \quad = \quad (\sigma \circ \tau)(\alpha) \quad = \quad \sigma(\tau(\alpha)) \quad = \quad \sigma(\alpha) \quad = \quad \beta$$

und somit $\tau \in \mathrm{Gal}(K|\mathbb{Q}(\beta))$. Es gilt also $\mathrm{Gal}(K|\mathbb{Q}(\alpha)) \subseteq \mathrm{Gal}(K|\mathbb{Q}(\beta))$. Nach dem Hauptsatz der Galoistheorie folgt daraus $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, was aber zu $\beta \notin \mathbb{Q}(\alpha)$ im Widerspruch steht. Der Widerspruch zeigt, dass unsere Annahme falsch war.

zu (b) Zunächst bestimmen wir den Erweiterungsgrad $[K : \mathbb{Q}]$. Das Polynom $x^2 - 2$ ist normiert, in $\mathbb{Q}[x]$ irreduzibel und hat $\sqrt{2}$ als Nullstelle. Also ist $x^2 - 2$ das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Wäre das Polynom $x^2 + 1$ über $\mathbb{Q}(\sqrt{2})$ reduzibel, dann würden die beiden Nullstellen $\pm i$ des Polynoms wegen $\mathrm{grad}(x^2 + 1) = 2$ in $\mathbb{Q}(\sqrt{2})$ liegen, was aber wegen $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $\pm i \notin \mathbb{R}$ nicht der Fall ist. Das Polynom $x^2 + 1$ ist normiert, über $\mathbb{Q}(\sqrt{2})$ irreduzibel und hat i als Nullstelle. Es ist also das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$. Wir erhalten

$$[K : \mathbb{Q}(\sqrt{2})] \quad = \quad [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] \quad = \quad \mathrm{grad}(x^2 + 1) \quad = \quad 2$$

und $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Als nächtes beweisen wir die Gleichung $K = \mathbb{Q}(\sqrt{2} + i)$. Die Inklusion „$\supseteq$“ ist erfüllt, denn aus $\sqrt{2}, i \in K$ folgt $\sqrt{2} + i \in K$. Zum Nachweis von „$\subseteq$“ müssen wir zeigen, dass $\sqrt{2}$ und i in $L = \mathbb{Q}(\sqrt{2} + i)$ enthalten sind. Aus $\sqrt{2} + i \in L$ folgt $(\sqrt{2} + i)^2 = 2 + 2i\sqrt{2} + (-1) = 1 + 2i\sqrt{2} \in L$ und $i\sqrt{2} \in L$. Es folgt $i\sqrt{2}(\sqrt{2} + i) = 2i - \sqrt{2} \in L$ und $(i + \sqrt{2}) + (2i - \sqrt{2}) = 3i \in L$, somit auch $i \in L$ und $(\sqrt{2} - i) + i = \sqrt{2} \in L$.

Nun bestimmen wir ein Polynom $f \in \mathbb{Q}[x]$, dass $\alpha = i + \sqrt{2}$ als Nullstelle besitzt. Es gilt

$$\alpha = i + \sqrt{2} \quad \Rightarrow \quad \alpha - i = \sqrt{2} \quad \Rightarrow \quad (\alpha - i)^2 = 2 \quad \Rightarrow \quad \alpha^2 - 2i\alpha + (-1) = 2$$

$$\Rightarrow \quad \alpha^2 - 3 = 2i\alpha \quad \Rightarrow \quad (\alpha^2 - 3)^2 = -4\alpha^2 \quad \Rightarrow \quad \alpha^4 - 6\alpha^2 + 9 = -4\alpha^2 \quad \Rightarrow \quad \alpha^4 - 2\alpha^2 + 9 = 0.$$

Also ist α eine Nullstelle von $f = x^4 - 2x^2 + 9$. Außerdem ist f irreduzibel. Wäre f nämlich reduzibel, dann wäre das Minimalpolynom $g \in \mathbb{Q}[x]$ von α über $\mathbb{Q}$ ein echter Teiler von f. Es würde dann

$$[K : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad \text{grad}(g) \quad < \quad \text{grad}(f) \quad = \quad 4$$

folgen, im Widerspruch zu $[K : \mathbb{Q}] = 4$. Nun zeigen wir noch, dass K ein Zerfällungskörper von f über $\mathbb{Q}$ ist. Der Körper K wird von den Nullstellen von f über $\mathbb{Q}$ erzeugt, da er bereits von α erzeugt wird. Außerdem gilt

$$(x - \sqrt{2} - i)(x - \sqrt{2} + i)(x + \sqrt{2} - i)(x + \sqrt{2} + i) \quad = \quad ((x - \sqrt{2})^2 - (-1))((x + \sqrt{2})^2 - (-1))$$

$$= \quad (x^2 - 2\sqrt{2}x + 3)(x^2 + 2\sqrt{2}x + 3) \quad = \quad x^4 - 2x^2 + 9.$$

Wegen $\pm\sqrt{2} \pm i \in K$ zerfällt f über K also in Linearfaktoren. Damit sind die Eigenschaften eines Zerfällungskörpers vollständig nachgewiesen.

Die Körpererweiterung $K|\mathbb{Q}$ ist normal, weil K Zerfällungskörper eines Polynoms f über $\mathbb{Q}$ ist. Als algebraische Erweiterung von $\mathbb{Q}$ ist sie wegen $\text{char}(\mathbb{Q}) = 0$ außerdem separabel. Insgesamt ist $K|\mathbb{Q}$ also eine Galois-Erweiterung, und für die Galoisgruppe $G = \text{Gal}(K|\mathbb{Q})$ gilt somit $|G| = [K : \mathbb{Q}] = 4$. Weil die Ordnung von G ein Primzahlquadrat ist, handelt es sich bei G um eine abelsche Gruppe. Wäre G auch zyklisch, dann gäbe es zu jedem Teiler d der Gruppenordnung genau eine Untergruppe U mit $(G : U) = d$. Insbesondere gäbe es genau eine Untergruppe U mit $(G : U) = 2$. Nach dem Hauptsatz der Galoistheorie würde daraus folgen, dass die Erweiterung $K|\mathbb{Q}$ genau einen quadratischen Zwischenkörper besitzt. Aber $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ sind beides Zwischenkörper der Erweiterung, und wegen $i \notin \mathbb{Q}(\sqrt{2})$ stimme diese auch nicht überein. Also ist G nicht zyklisch.