Aufgabe H12T3A3 (8 Punkte)

Sei $f = x^4 - 2 \in \mathbb{Q}[x]$. Es sei K der Zerfällungskörper des Polynoms f in $\mathbb{C}$ über $\mathbb{Q}$. Ferner sei $\alpha \in K$ eine Nullstelle von f.

(a) Zeigen Sie, dass $[K : \mathbb{Q}] = 8$ gilt, und dass es eine Nullstelle $\beta \neq \pm\alpha$ von f in K gibt, so dass $R = \{\pm\alpha, \pm\beta\}$ die Menge aller Nullstellen von f ist.

(b) Es bezeichne S_R die Gruppe der Permutationen von R. Sei $s \in S_R$ die Permutation $R \to R$, $x \mapsto -x$. Zeigen Sie, dass die Untergruppe $C = \{\sigma \in S_R \sigma \circ s = s \circ \sigma\}$ Ordnung 8 hat.

(c) Es bezeichne $G = \mathrm{Gal}(K|\mathbb{Q})$ die Galoisgruppe von K über $\mathbb{Q}$. Zeigen Sie, dass der Gruppenhomomorphismus

$$\rho : G \longrightarrow S_R \quad , \quad \sigma \mapsto (x \mapsto \sigma(x))$$

einen Gruppenisomorphismus zwischen G und C induziert.

(d) Ist G auflösbar?

Lösung:

zu (a) Durch Einsetzen sieht man unmittelbar, dass $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$ in der Menge $R \subseteq \mathbb{C}$ der Nullstellen von f enthalten ist. Wegen $\mathrm{grad}(f) = 4$ kann es nicht mehr als vier Nullstellen geben; also gilt sogar $R = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Laut Angabe ist α in R enthalten. Gesucht wird (in Abhängigkeit von α) ein $\beta \in \mathbb{C}$ mit $\beta \neq \pm\alpha$ und $R = \{\pm\alpha, \pm\beta\}$. Ist $\alpha \in \{\pm\sqrt[4]{2}\}$, dann erfüllt offenbar $\beta = i\sqrt[4]{2}$ diese beiden Bedingungen Im Fall $\alpha \in \{\pm i\sqrt[4]{2}\}$ sind die beiden Bedingungen durch $\beta = \sqrt[4]{2}$ erfüllt.

Als nächstes zeigen wir, dass $K = \mathbb{Q}(\sqrt[4]{2}, i)$ gilt. Nach Definition des Zerfällungskörpers wird K über $\mathbb{Q}$ von der Menge der Nullstellen erzeugt, es gilt also $K = \mathbb{Q}(R)$. Zu zeigen ist

$$\mathbb{Q}(\sqrt[4]{2}, i) \quad = \quad \mathbb{Q}(R).$$

Die Inklusion „$\supseteq$“ folgt aus der Tatsache, dass mit $\sqrt[4]{2}$ und i auch die Elemente der Menge $R = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$ in $\mathbb{Q}(\sqrt[4]{2}, i)$ enthalten sind (denn $\mathbb{Q}(\sqrt[4]{2}, i)$ ist als Teilkörper von $\mathbb{C}$ unter Bildung von Negativen und Produkten abgeschlossen). Umgekehrt folgt aus $\sqrt[4]{2}, i\sqrt[4]{2} \in R \subseteq \mathbb{Q}(R)$ auch $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in \mathbb{Q}(R)$. Aus $\{\sqrt[4]{2}, i\} \subseteq \mathbb{Q}(R)$ wiederum folgt $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq \mathbb{Q}(R)$.

Nun bestimmen wir den Erweiterungsgrad $[K : \mathbb{Q}]$. Das Polynom $f = x^4 - 2$ ist nomiert, in $\mathbb{Q}[x]$ irreduzibel nach dem Eisenstein-Kriterium (angewendet auf die Primzahl $p = 2$), und es erfüllt $f(\sqrt[4]{2}) = 0$. Dies zeigt, dass f das Minimalpolyom von $\sqrt[4]{2}$ ist, und wir erhalten $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \mathrm{grad}(f) = 4$. Das Polynom $g = x^2 + 1$ ist ebenfalls normiert, und es erfüllt $g(i) = 0$. Wäre es über $\mathbb{Q}(\sqrt[4]{2})$ reduzibel, dann müssten wegen $\mathrm{grad}(g) = 2$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt[4]{2})$ liegen. Aber dies ist wegen $\pm i \in \mathbb{C} \setminus \mathbb{R}$ und $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ nicht der Fall. Also ist g in $\mathbb{Q}(\sqrt[4]{2})[x]$ irreduzibel und insgesamt das Minimalpolyom von i über $\mathbb{Q}(\sqrt[4]{2})$. Wir erhalten

$$[K : \mathbb{Q}(\sqrt[4]{2})] \quad = \quad [\mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2})] \quad = \quad \mathrm{grad}(g) \quad = \quad 2 \quad ,$$

und die Gradformel liefert $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$.

zu (b) Wir betrachten die Operation der Gruppe S_R auf sich selbst durch Konjugation, die wir mit $\cdot : S_R \times S_R \to S_R$ bezeichnen. Bezüglich dieser Operation ist C genau der Stabilisator $(S_R)_s$ von s in S_R, denn für jedes $\sigma \in S_r$ gilt die Äquivalenz

$$\sigma \in (S_R)_s \quad \Leftrightarrow \quad \sigma \cdot s = s \quad \Leftrightarrow \quad \sigma \circ s \circ \sigma^{-1} = s \quad \Leftrightarrow \quad \sigma \circ s = s \circ \sigma \quad \Leftrightarrow \quad \sigma \in C.$$

Die Bahn $S_R(s)$ von s unter dieser Operation ist genau die Konjugationsklasse. Aus der Vorlesung ist bekannt, dass in den symmetrischen Gruppen S_n die Konjugationsklassen genau die Teilmengen eines festen Zerlegungstyps sind, und da es sich bei R um eine vierelemente Menge handelt, können wir S_R mit S_4 identifizieren. Nun ist s in S_R eine Doppeltransposition, da s die Elemente $\alpha, -\alpha$ und $\beta, -\beta$ jeweils miteinander vertauscht. In S_4 gibt es bekanntlich genau 3 Doppeltranspositionen, also gilt dasselbe für S_R. Es folgt $(S_R : (S_R)_s) = |S_R(s)| = 3$. Mit dem Satz von Lagrange und dem allgemeinen Zusammenhang $|G(x)| = (G : G_x)$ zwischen Bahnlänge und Stabilisator erhalten wir

$$|C| \quad = \quad |(S_R)_s| \quad = \quad \frac{|S_R|}{(S_R : (S_R)_s)} \quad = \quad \frac{|S_4|}{(S_R : (S_R)_s)} \quad = \quad \frac{24}{3} \quad = \quad 8.$$

zu (c) Wegen $K = \mathbb{Q}(R)$ ist jedes $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ durch die Bilder der Elemente aus R bereits eindeutig festgelegt. Daraus folgt, dass die Abbildung $\rho : G \to S_R$, $\sigma \mapsto \sigma|_R$ injektiv ist. Darüber hinaus ist das Bild $\rho(G)$ in C enthalten, denn für alle $\sigma \in G$ und $\gamma \in R$ gilt

$$(\sigma \circ s)(\gamma) \quad = \quad \sigma(-\gamma) \quad = \quad -\sigma(\gamma) \quad = \quad (s \circ \sigma)(\gamma)$$

und somit $\sigma \in G$. Also handelt es sich bei ρ um eine injektive Abbildung $G \to C$. Die Mengen G und C sind gleichmächtig, denn nach Teil (b) gilt $|C| = 8$, und das es sich bei $K|\mathbb{Q}$ um eine Galois-Erweiterung handelt, ist auch $|G| = [K : \mathbb{Q}] = 8$. Eine injektive Abbildung zwischen zwei gleichmächtigen Mengen ist auch surjektiv. Dies zeigt insgesamt, dass durch ρ eine Bijektion zwischen G und C gegeben ist.

Für alle $\sigma, \tau \in G$ gilt jeweils $\sigma(R) \subseteq R$ und $\tau(R) \subseteq R$, denn σ und τ sind $\mathbb{Q}$-Automorphismen von K, und diese bilden jede Nullstelle von $f \in \mathbb{Q}[x]$ auf eine Nullstelle von f ab. Daraus folgt $\rho(\sigma) \circ \rho(\tau) = (\sigma|_R) \circ (\tau|_R) = (\sigma \circ \tau)|_R = \rho(\sigma \circ \tau)$. Damit ist genzeigt, dass ρ auch ein Gruppenhomomorphismus ist, auf Grund der Bijektivität also insgesamt ein Isomorphismus von Gruppen.

zu (d) Aus der Vorlesung ist bekannt, dass jede Gruppe von Primzahlpotenzordnung auflösbar ist. Wegen $|G| = 8 = 2^3$ ist G also auflösbar.