Aufgabe H15T3A4 (5+5+5+3 Punkte)

Es sei $p \geq 3$ eine Primzahl und $a \in \mathbb{Q}$ eine rationale Zahl, so dass $x^p - a$ über $\mathbb{Q}$ irreduzibel ist. Ferner sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel, $\alpha \in \mathbb{C}$ eine beliebige Nullstelle von $x^p - a$ und $Z = \mathbb{Q}(\alpha, \zeta)$.

(a) Zeigen Sie, dass Z ein Zerfällungskörper von $x^p - a$ ist und $[Z : \mathbb{Q}] = p(p-1)$ gilt.

(b) Zeigen Sie, dass $\mathrm{Gal}(Z|\mathbb{Q})$ eine p-Sylowsgruppe H besitzt, die ein Normalteiler ist, und dass

$$\mathrm{Gal}(Z|\mathbb{Q})/H \quad \cong \quad (\mathbb{Z}/p\mathbb{Z})^\times \quad = \quad \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \qquad \text{gilt.}$$

(c) Bestimmen Sie einen Gruppenisomorphismus $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times$.

(d) Zeigen Sie, dass $\mathrm{Gal}(Z|\mathbb{Q})$ mehr als eine 2-Sylowgruppe besitzt.

Lösung:

zu (a) Die p komplexen Nullstellen von $f = x^p - a$ sind gegeben durch $\zeta^i\alpha$ mit $0 \leq i < p$, denn es gilt jeweils $f(\zeta^i\alpha) = (\zeta^i\alpha)^p - a = \zeta^{ip}\alpha^p - a = 1 \cdot a - a = 0$, und weil ζ eine primitive p-te Einheitswurzel ist, sind die Elemente $\zeta^i\alpha$ mit $0 \leq i < p$ auch verschieden voneinander. Um zu zeigen, dass $Z = \mathbb{Q}(\alpha, \zeta)$ gilt, müssen wir also die Gleichung

$$\mathbb{Q}(\alpha, \zeta) \quad = \quad \mathbb{Q}(\{\zeta^i\alpha \mid 0 \leq i < p\})$$

überprüfen. Die Inklusion „$\supseteq$“ ist erfüllt, weil sich jedes der Elemente $\zeta^i\alpha 4$, $0 \leq i < p$ als Produkt von ζ und α schreiben lässt. Die Inklusion „$\subseteq$“ gilt wegen $\alpha = \zeta^0\alpha$ und $\zeta = \frac{\zeta^1\alpha}{\zeta^0\alpha}$.

Nun beweisen wir die Gleichung $[Z : \mathbb{Q}] = p(p-1)$. Das Polynom $f = x^p - a$ ist laut Angabe irreduzibel, außerdem normiert, und es besitzt α als Nullstelle. Also handelt es sich um das Minimalpolynom von α über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = p$. Sei nun g das Minimalpolynom von ζ über $\mathbb{Q}(\alpha)$. Das p-te Kreisteilungspolynom Φ_p ist in $\mathbb{Q}(\alpha)[x]$ enthalten, und es gilt $\Phi_p(\zeta) = 0$. Daraus folgt, dass Φ_p ein Vielfaches von g ist. Wir erhalten $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] = \mathrm{grad}(g) \leq \mathrm{grad}(\Phi_p) = p - 1$ und mit der Gradformel

$$[Z : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad \leq \quad (p-1)p.$$

Weil $\mathbb{Q}(\alpha)$ ein Zwischenkörper von $Z|\mathbb{Q}$ ist, gilt nach der Gradformel auch $[Z : \mathbb{Q}] = [Z : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [Z : \mathbb{Q}(\alpha)] \cdot p$, also ist p ein Teiler von $[Z : \mathbb{Q}]$. Bekanntlich gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p) = p - 1$, und auch $\mathbb{Q}(\zeta)$ ist ein Zwischenkörper von $Z|\mathbb{Q}$. Es gilt also $[Z : \mathbb{Q}] = [Z : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = [Z : \mathbb{Q}(\zeta)](p-1)$, somit ist auch $p - 1$ ein Teiler von $[Z : \mathbb{Q}]$. Weil die Zahlen p und $p - 1$ teilerfremd sind, folgt daraus, dass $p(p-1)$ ein Teiler von $[Z : \mathbb{Q}]$ ist. Insbesondere gilt $[Z : \mathbb{Q}] \geq p(p-1)$, so dass wir insgesamt $[Z : \mathbb{Q}] = p(p-1)$ erhalten.

zu (b) Die Untergruppe $H = \mathrm{Gal}(Z|\mathbb{Q}(\zeta))$ von $G = \mathrm{Gal}(Z|\mathbb{Q})$ hat die Ordnung

$$[Z : \mathbb{Q}(\zeta)] \quad = \quad \frac{[Z : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \quad = \quad \frac{p(p-1)}{p-1} \quad = \quad p.$$

Wegen $p \nmid (p-1)$ ist p^1 die maximale p-Potenz, die die Gruppenordnung $|G|$ teilt. Also ist H eine p-Sylowgruppe von G. Außerdem ist bekannt, dass $\mathbb{Q}(\zeta)|\mathbb{Q}$ als Kreisteilungserweiterung normal ist. Deshalb ist H ein Normalteiler von G.

Aus der Vorlesung ist bekannt: Ist $L|K$ eine Galois-Erweiterung und M ein Zwischenkörper mit der Eigenschaft, dass $M|K$ normal ist, dann ist durch $\sigma \mapsto \sigma|_M$ ein Epimorphismus $\mathrm{Gal}(L|K) \to \mathrm{Gal}(M|K)$ definiert, dessen Kern die Untergruppe $\mathrm{Gal}(L|M)$ von $\mathrm{Gal}(L|K)$ ist. Der Homomorphiesatz liefert dann einen Isomorphismus

$$\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \quad \cong \quad \mathrm{Gal}(M|K).$$

Wenden wir dies auf $K = \mathbb{Q}$, $L = Z$ und $M = \mathbb{Q}(\zeta)$ an, so erhalten wir einen Isomorphismus $G/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Außerdem ist aus der Vorlesung bekannt, dass ein Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ existiert, der $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ auf die Restklasse $a + p\mathbb{Z}$ abbildet, falls $a \in \mathbb{Z}$ die Gleichung $\sigma(\zeta) = \zeta^a$ erfüllt. Insgesamt erhalten wir so einen Isomorphismus $G/H \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

zu (c) Wir definieren eine Abbildung $\phi : \mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ durch $\phi(\sigma) = \sigma|_{\mathbb{Q}(\zeta)}$. Weil die Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ normal ist, handelt es sich bei $\sigma|_{\mathbb{Q}(\zeta)}$ für jedes $\sigma \in \mathrm{Gal}(Z|\mathbb{Q}(\alpha)$ tatsächlich um einen $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\zeta)$, also um ein Element der Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$. Weil die Einschränkung von Abbildungen verträglich mit der Komposition ist, handelt es sich bei ϕ um einen Gruppenhomomorphismus. Dieser ist surjektiv, denn auf Grund des Fortsetzungssatzes kann jedes vorgegebene $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ auf Z fortgesetzt werden, es gibt also ein $\sigma \in \mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ mit $\phi(\sigma) = \sigma|_{\mathbb{Q}(\zeta)} = \tau$. Zum Nachweis der Injektivität sei $\sigma \in \mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ ein Element mit $\phi(\sigma) = \mathrm{id}_{\mathbb{Q}(\zeta)}$, also $\sigma|_{\mathbb{Q}(\zeta)} = \mathrm{id}_{\mathbb{Q}(\zeta)}$. Dann gilt $\sigma(\alpha) = \alpha$ und $\sigma(\zeta) = \zeta$, also stimmt σ auf Z mit id_Z überein. Insgesamt haben wir damit gezeigt, dass ϕ ein Isomorphismus ist. Durch Komposition mit dem bereits in Teil (b) verwendeten Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ erhalten wir insgesamt einen Isomorphismus $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

zu (d) Nehmen wir an, dass $P \leq G$ die einzige 2-Sylowgruppe von G ist. Sei $M = Z^P$ der zugehörige Fixkörper. Sei 2^r die höchste Zweierpotenz, die $p-1$ teilt; dann ist dies wegen $2 \nmid p$ zugleich die höchste Zweierpotenz, die $|G|$ teilt, und es gilt $|P| = 2^r$ nach Definition der 2-Sylowgruppen. Wegen

$$|\mathrm{Gal}(Z|\mathbb{Q}(\alpha))| \quad = \quad [Z : \mathbb{Q}(\alpha)] \quad = \quad \frac{[Z : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \quad = \quad \frac{p(p-1)}{p} \quad = \quad p-1$$

ist 2^r ein Teiler von $|\mathrm{Gal}(Z|\mathbb{Q}(\alpha))|$. Da 2^r eine Primzahlpotenz ist, existiert eine Untergruppe Q von $\mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ der Ordnung 2^r. Weil P in G die einzige 2-Sylowgruppe ist, folgt $\mathrm{Gal}(Z|M) = \mathrm{Gal}(Z|Z^P) = P = Q \subseteq \mathrm{Gal}(Z|\mathbb{Q}(\alpha))$, und der Hauptsatz der Galoistheorie liefert $\mathbb{Q}(\alpha) \subseteq M$.

Wegen $f(\zeta\alpha) = 0$ ist f auch Minimalpolynom von $\zeta\alpha$, und es folgt $[\mathbb{Q}(\zeta\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = p$. Genau wie im vorherigen Absatz können wir daraus $\mathrm{Gal}(Z|M) \subseteq \mathrm{Gal}(Z|\mathbb{Q}(\zeta\alpha))$ und $\mathbb{Q}(\zeta\alpha) \subseteq M$ schließen. Insgesamt enthält M also die Elemente α und $\zeta\alpha$, damit auch $\zeta = \frac{\zeta\alpha}{\alpha}$. Aus $\zeta, \alpha \in M$ folgt $Z = \mathbb{Q}(\alpha, \zeta) \subseteq M$, also $M = Z$. Durch Anwendung des Hauptsatzes der Galoistheorie erhalten wir $P = \mathrm{Gal}(Z|M) = \mathrm{Gal}(Z|Z) = \{\mathrm{id}_Z\}$. Aber dies steht zu $|P| = 2^r$ im Widerspruch, denn $p-1$ ist gerade und somit $r \geq 1$. Also muss es in G mehr als eine 2-Sylowgruppe geben.