H15-T3-A4

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

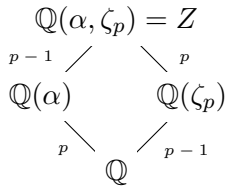
a) Zeigen Sie, dass Z ein Zerfällungskörper von $X^p - a$ ist und $[Z : \mathbb{Q}] = p(p-1)$ gilt.

b) Zeigen Sie, dass $\mathrm{Gal}(Z|\mathbb{Q})$ eine p-Sylowgruppe H besitzt, die Normaltieiler ist, und dass
$$\mathrm{Gal}(Z|\mathbb{Q})/H \simeq (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \text{ gilt.}$$

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

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

Lösungsvorschlag. Zu a). Die Nullstellen von $X^p - a$ sind bekanntlich von der Form $\zeta_p^i \alpha$, mit $i = 0, 1, \ldots, p-1$, für jede Fixierung einer vorgegebenen Nullstelle α von $X^p - a$. Somit ist klar, dass ein Zerfällungskörper $\mathrm{Zerf}(X^p - a)$ in $Z := \mathbb{Q}(\alpha, \zeta_p)$ enthalten ist, zu zeigen bleibt also nur $Z \subset \mathrm{Zerf}(X^p - a)$. Offensichtlich gilt $\zeta_p^0 \alpha = \alpha \in \mathrm{Zerf}(X^p - a)$, für ζ_p finden wir $\zeta_p = \zeta_p^{i+1}\alpha / (\zeta_p^i \alpha) \in \mathrm{Zerf}(X^p - a)$.
Zu b). Wir betrachten das folgende Diagramm von Körpererweiterungen mit entsprechenden Graden:



Es ist bekannt, dass $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ eine Galoiserweiterung ist mit $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \simeq \mathbb{Z}_p^\times$. Der Hauptsatz der Galoistheorie liefert, dass (da $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ Galois'sch ist) $\mathrm{Gal}(Z|\mathbb{Q}(\zeta_p)) \subset \mathrm{Gal}(Z|\mathbb{Q})$ ein Normalteiler ist, und dass

$$\mathrm{Gal}(Z|\mathbb{Q})/\,\mathrm{Gal}(Z|\mathbb{Q}(\zeta_p)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times.$$

Da $\mathrm{Gal}(Z|\mathbb{Q}(\zeta_p))$ die für eine p-Sylowuntergruppe von $\mathrm{Gal}(Z|\mathbb{Q})$ zu erwartende Ordnung p besitzt haben wir die gesuchte Gruppe gefunden, setze also $H := \mathrm{Gal}(Z|\mathbb{Q}(\zeta_p))$. (*Bemerkung:* Die bloße Tatsache, dass eine solche p-Sylowgruppe existiert, die Normalteiler ist, wäre auch sofort aus der in a) ermittelten Gruppenordnung $|\mathrm{Gal}(Z|\mathbb{Q})| = p(p-1)$ und den Sylowsätzen gefolgt.)
Zu c). Die Tatsache, dass $[Q(\alpha, \zeta_p) : \mathbb{Q}(\alpha)] = p - 1$ gilt, zeigt uns, dass das bekannte Minimalpolynom $X^{p-1} + \ldots + X + 1$ von ζ_p über $\mathbb{Q}$ auch, aufgefasst als Polynom in $\mathbb{Q}(\alpha)[X]$, das Minimalpolynom von ζ_p über $\mathbb{Q}(\alpha)$ ist. Dessen Nullstellen sind ζ_p^i, mit $i = 1, \ldots, p-1$. Ein Element $f \in \mathrm{Gal}(Z|\mathbb{Q}(\alpha)) = \mathrm{Aut}_{\mathbb{Q}(\alpha)}(Z)$ ist damit eindeutig bestimmt durch das Bild von $f(\zeta_p) = \zeta_p^{i_f}$ für ein $i_f \in \{1, \ldots, p-1\}$. Eine kanonische Wahl für einen Gruppenisomorphismus $\psi\colon \mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \xrightarrow{\simeq} \mathbb{Z}_p^\times$ wäre gegeben durch

$\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \ni f \mapsto i_f \in \mathbb{Z}_p^\times$. Die so definierte Abbildung ist offensichtlich bijektiv, und ein Gruppenmorphismus, da $f \circ g \mapsto i_{f\circ g} = i_f \cdot i_g$, wobei man letztere Gleichheit direkt aus der entsprechenden Definition einsehen kann:

$$f \circ g(\zeta_p) = f(\zeta_p^{i_g}) = (f(\zeta_p))^{i_g} = (\zeta_p^{i_f})^{i_g} = \zeta_p^{i_f \cdot i_g}$$

Zu d). Nachdem der Index von $\mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ in $\mathrm{Gal}(Z|\mathbb{Q})$ gleich p und mithin insbesondere nicht durch 2 teilbar ist, ist eine 2-Sylowuntergruppe von $\mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ zugleich auch eine 2-Sylowuntergruppe von $\mathrm{Gal}(Z|\mathbb{Q})$. Nach einem der Sylow-Sätze (dem ersten) wissen wir, dass $\mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ (mindestens) eine 2-Sylowuntergruppe besitzt. Wir nennen diese für den Moment S nennen und zeigen, dass S (nach der Vorüberlegung ja auch eine 2-Sylowuntergruppe von $\mathrm{Gal}(Z|\mathbb{Q})$) kein Normalteiler in $\mathrm{Gal}(Z|\mathbb{Q})$ ist. Wir wählen dazu ein beliebiges nichttriviales Element s aus S, entsprechend einem Automorphismus

$$\begin{aligned} s\colon Z &\to Z \\ \alpha &\mapsto \alpha \\ \zeta_p &\mapsto \zeta_p^i \end{aligned}$$

mit $i \neq 1$. Wir wollen ein Element $z \in \mathrm{Gal}(Z|\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(Z)$ finden, für dass zsz^{-1} sicher nicht in S liegt, wofür ein hinreichendes Kriterium wäre, dass $zsz^{-1}(\alpha) \neq \alpha$ gilt (denn dann wäre sogar bereits $zsz^{-1} \notin \mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \supset S$). Wir wählen z als den Automorphismus, der durch

$$\begin{aligned} \alpha &\overset{z}{\mapsto} \zeta_p^{p-1}\alpha \\ \zeta_p &\overset{z}{\mapsto} \zeta_p \end{aligned}$$

gegeben ist. Dann ist z^{-1} dementsprechend beschrieben durch $z^{-1}\colon \alpha \mapsto \zeta_p\alpha,\ \zeta_p \mapsto \zeta_p$, und wir erhalten:

$$\begin{aligned} zsz^{-1}\colon Z &\to Z \\ \alpha &\overset{z^{-1}}{\mapsto} \zeta_p\alpha \overset{s}{\mapsto} \zeta_p^i\alpha \overset{z}{\mapsto} \zeta_p^i\zeta_p^{p-1}\alpha = \zeta_p^{i+p-1}\alpha \\ \zeta_p &\overset{z^{-1}}{\mapsto} \zeta_p \overset{s}{\mapsto} \zeta_p^i \overset{z}{\mapsto} \zeta_p^i \end{aligned}$$

Aufgrund von $1 < i < p$ ist aber $i + p - 1 \not\equiv 0 \mod p$ und somit $zsz^{-1}(\alpha) \neq \alpha$ wie gewünscht.