Aufgabe F12T3A2 (6 Punkte)

Sei $p \neq 2$ eine Primzahl, $\zeta = \exp(2\pi i/p) \in \mathbb{C}$ und $\sqrt[p]{p} \in \mathbb{R}_{>0}$. Weiter sei L der Zerfällungskörper des Polynoms $f = x^p - p$ in $\mathbb{C}$ und M der Zerfällungskörper des Polynoms $g = x^{p^2} - 1$ in $\mathbb{C}$. Zeigen Sie:

(a) $L = \mathbb{Q}(\zeta, \sqrt[p]{p})$

(b) $[L : \mathbb{Q}] = [M : \mathbb{Q}]$

(c) Die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$ ist nicht abelsch.

(d) Die Körper L und M sind nicht isomorph.

Lösung:

zu (a) Sei $\alpha = \sqrt[p]{p}$. Für $0 \leq j < p$ gilt $f(\zeta^j\alpha) = (\zeta^j\alpha)^p - p = (\zeta^p)^j\alpha^p - p = 1^j \cdot p - p = 0$. Außerdem sind die komplexen Zahlen $\zeta^j\alpha$ alle verschieden, denn weil ζ eine primitive p-te Einheitswurzel ist, gilt $\zeta^j \neq \zeta^k$ für $0 \leq j < k < p$. Durch $N = \{\zeta^j\alpha \mid 0 \leq j < p\}$ ist also eine p-elementige Nullstellenmenge von f gegeben. Weil ein Polynom vom Grad p nicht mehr als p komplexe Nullstellen hat, ist N schon die gesamte Nullstellenmenge von f. Nach Definition des Zerfällungskörpers gilt also $L = \mathbb{Q}(N)$. Zu zeigen bleibt

$$\mathbb{Q}(N) \quad = \quad \mathbb{Q}(\zeta, \alpha).$$

„$\subseteq$“ Mit ζ und α ist auch $\zeta^j\alpha$ für $0 \leq j < p$ in $\mathbb{Q}(\zeta, \alpha)$ enthalten, denn $\mathbb{Q}(\zeta, \alpha)$ ist als Teilkörper von $\mathbb{C}$ unter Multiplikation abgeschlossen. Es gilt also $N \subseteq \mathbb{Q}(\zeta, \alpha)$, und daraus folgt $\mathbb{Q}(N) \subseteq \mathbb{Q}(\zeta, \alpha)$.
„$\supseteq$“ Mit $\alpha, \zeta\alpha \in N \subseteq \mathbb{Q}(N)$ gilt auch $\zeta = \frac{\zeta\alpha}{\alpha} \in \mathbb{Q}(N)$. Es gilt also $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$, und daraus folgt $\mathbb{Q}(\alpha, \zeta) \subseteq \mathbb{Q}(N)$.

zu (b) Die Nullstellen des Polynoms g sind genau die p^2-ten Einheitswurzeln in $\mathbb{C}$. Der Körper M entsteht durch Adjunktion dieser Einheitswurzeln und ist somit der p^2-te Kreisteilungskörper. Laut Vorlesung ist der Erweiterungsgrad dieses Körpers über $\mathbb{Q}$ durch $[M : \mathbb{Q}] = \varphi(p^2) = p(p-1)$ gegeben, wobei φ die Eulersche φ-Funktion bezeichnet.

Bestimmen wir nun den Erweiterungsgrad $[L : \mathbb{Q}]$. Auf Grund des Eisenstein-Kriteriums, angewendet auf die Primzahl p, ist das Polynom f über $\mathbb{Q}$ irreduzibel. Außerdem ist es normiert, und es gilt $f(\alpha) = 0$. Insgesamt ist f damit das Minimalpolynom von α über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = p$. Laut Vorlesung ist das p-te Kreisteilungspolynom $\Phi_p \in \mathbb{Q}[x]$ normiert und irreduzibel, und es gilt $\Phi_p(\zeta) = 0$. Also ist Φ_p das Minimalpolynom von ζ über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \mathrm{grad}(\Phi_p) = \varphi(p) = p - 1$. Der Gradsatz liefert nun

$$[L : \mathbb{Q}] \quad = \quad [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad [L : \mathbb{Q}(\alpha)] \cdot p$$

und

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

Dies zeigt, dass der Erweiterungsgrad $[L : \mathbb{Q}]$ sowohl durch p als auch durch $p-1$ teilbar ist. Es gilt $\mathrm{ggT}(p, p-1) = 1$, denn jeder gemeinsame Teiler von p und $p-1$ ist auch ein Teiler von $p+(-1)(p-1) = 1$. Aus $p \mid [L : \mathbb{Q}]$ und $(p-1) \mid [L : \mathbb{Q}]$ folgt deshalb, dass auch $p(p-1)$ ein Teiler von $[L : \mathbb{Q}]$ ist. Insbesondere gilt $[L : \mathbb{Q}] \geq p(p-1)$. Um zu sehen, dass auch „$\leq$“ gilt, betrachten wir das Minimalpolynom $h \in \mathbb{Q}(\alpha)[x]$ von ζ über $\mathbb{Q}(\alpha)$. Wegen $\Phi_p(\zeta) = 0$ und $\Phi_p \in \mathbb{Q}(\alpha)[x]$ ist Φ_p ein Vielfaches von h in $\mathbb{Q}(\alpha)[x]$. Es gilt also

$\mathrm{grad}(h) \leq \mathrm{grad}(\Phi_p) = p-1$. Daraus folgt $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)] = \mathrm{grad}(h) \leq p-1$, und eine erneute Anwendung der Gradformel liefert $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq (p-1)p$. Insgesamt ist damit $[L : \mathbb{Q}] = p(p-1) = [M : \mathbb{Q}]$ bewiesen.

zu (c) Wäre $G = \mathrm{Gal}(L|\mathbb{Q})$ abelsch, dann wären alle Untergruppen von G Normalteiler. Auf Grund der Ergänzungen zum Hauptsatz der Galoistheorie würde daraus folgen, dass jeder Zwischenkörper von $L|\mathbb{Q}$ normal über $\mathbb{Q}$ ist. Aber $\mathbb{Q}(\alpha)|\mathbb{Q}$ ist keine normale Teilerweiterung von $L|\mathbb{Q}$. Wie wir bereits festgestellt haben, ist das Polynom f über $\mathbb{Q}$ irreduzibel, und es besitzt mit α eine Nullstelle in $\mathbb{Q}(\alpha)$. Wäre $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal, dann müsste f über $\mathbb{Q}(\alpha)$ in Linearfaktoren zerfallen. Die gesamte Menge N der komplexen Nullstellen von f wäre dann in $\mathbb{Q}(\alpha)$ enthalten. Aber dies ist nicht der Fall, denn wegen $p > 2$ ist ζ nicht-reell, und wegen $\alpha \in \mathbb{R} \setminus \{0\}$ ist damit auch $\zeta\alpha$ nicht-reell (denn aus $\zeta\alpha \in \mathbb{R}$ würde $\zeta = (\zeta\alpha)\alpha^{-1} \in \mathbb{R}$ folgen, Widerspruch). Andererseits gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ wegen $\alpha \in \mathbb{R}$. Dies zeigt, dass die Nullstelle $\zeta\alpha \in N$ von f nicht im Körper $\mathbb{Q}(\alpha)$ liegt. Also ist die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal, und die Gruppe G ist nicht abelsch.

zu (d) Jeder Isomorphismus zwischen Erweiterungskörpern von $\mathbb{Q}$ ist ein $\mathbb{Q}$-Isomorphismus, denn ein solcher Isomorphismus muss 1 auf 1 abbilden, und aus den Homomorphismus-Eigenschaften folgt dann unmittelbar, dass jede rationale Zahl r auf sich selbst abgebildet wird. Wären L und M isomorph, dann gäbe es also einen $\mathbb{Q}$-Isomorphismus $\phi : L \to M$. Durch die Abbildung

$$\tilde{\phi} : \mathrm{Gal}(L|\mathbb{Q}) \to \mathrm{Gal}(M|\mathbb{Q}) \quad , \quad \sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$$

ist ein dann Isomorphismus von Gruppen definiert. Denn für jedes $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ ist das Element $\phi \circ \sigma \circ \phi^{-1}$ als Komposition von $\mathbb{Q}$-Isomorphismen ebenfalls ein $\mathbb{Q}$-Isomorphismus, außerdem ein Körperhomomorphismus $M \to M$, insgesamt also ein Element von $\mathrm{Gal}(M|\mathbb{Q})$. Für alle $\sigma, \tau \in \mathrm{Gal}(L|\mathbb{Q})$ gilt

$$\tilde{\phi}(\sigma \circ \tau) \quad = \quad \varphi \circ (\sigma \circ \tau) \circ \varphi^{-1} \quad = \quad (\varphi \circ \sigma \circ \varphi^{-1}) \circ (\varphi \circ \tau \circ \varphi^{-1}) \quad = \quad \tilde{\phi}(\sigma) \circ \tilde{\phi}(\tau) \quad ,$$

also ist die Abbildung $\tilde{\phi}$ ein Homomorphismus von Gruppen. Darüber hinaus ist die Abbildung bijektiv, denn $\sigma \mapsto \varphi^{-1} \circ \sigma \circ \varphi$ ist offenbar eine Umkehrabbildung von $\tilde{\phi}$. Also wären die Gruppen $\mathrm{Gal}(L|\mathbb{Q})$ und $\mathrm{Gal}(M|\mathbb{Q})$ isomorph. Aber nach Teil (c) ist $\mathrm{Gal}(L|\mathbb{Q})$ nicht abelsch; andererseits ist aus der Vorlesung bekannt, dass $\mathrm{Gal}(M|\mathbb{Q}) = (\mathbb{Z}/p^2\mathbb{Z})^\times$ gilt, weil M der p^2-te Kreisteilungskörper ist, und $\mathrm{Gal}(M|\mathbb{Q})$ somit abelsch ist (denn $(\mathbb{Z}/n\mathbb{Z})^\times$ ist für jedes $n \in \mathbb{N}$ eine abelsche Gruppe). Da eine nicht-abelsche Gruppe nicht zu einer abelschen Gruppe isomorph sein kann, erhalten wir einen Widerspruch. Die Annahme, dass L und M isomorph sind, war also falsch.