Aufgabe F20T2A5

Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $x^8 - 2$. Sei ferner $\zeta := \exp(\frac{2\pi i}{8}) \in \mathbb{C}$. Zeigen Sie:

(a) Es gilt $\sqrt{2} \in \mathbb{Q}(\zeta)$.

(b) Die Körpererweiterung $\mathbb{Q} \subseteq L$ hat den Grad $[L : \mathbb{Q}] = 16$.

(c) Die Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ ist nicht abelsch und hat einen Normalteiler der Ordnung 4 mit $N \cong \mathbb{Z}/4\mathbb{Z}$.

Lösung:

zu (a) Es gilt $\zeta = \exp(\frac{\pi i}{4}) = \cos(\frac{1}{4}\pi) + i\sin(\frac{1}{4}\pi)$, $\zeta^{-1} = \exp(-\frac{\pi i}{4}) = \cos(\frac{1}{4}\pi) - i\sin(\frac{1}{4}\pi)$, und somit $\cos(\frac{1}{4}\pi) = \frac{1}{2}(\zeta + \zeta^{-1}) \in \mathbb{Q}(\zeta)$. Auf Grund des Additionstheorems des Kosinus gilt $0 = \cos(\frac{1}{2}\pi) = \cos(\frac{1}{4}\pi)^2 - \sin(\frac{1}{4}\pi)^2$, also $\cos(\frac{1}{4}\pi)^2 = \sin(\frac{1}{4}\pi)^2$. Es folgt $2\cos(\frac{1}{4}\pi)^2 = \cos(\frac{1}{4}\pi)^2 + \sin(\frac{1}{4}\pi)^2 = 1$, $\cos(\frac{1}{4}\pi)^2 = \frac{1}{2}$, und wegen $\cos(\alpha) > 0$ für $-\frac{1}{2}\pi < \alpha < \frac{1}{2}\pi$ folgt $\frac{1}{\sqrt{2}} = \cos(\frac{1}{4}\pi) \in \mathbb{Q}(\zeta)$. Damit ist auch der Kehrwert $\sqrt{2}$ in $\mathbb{Q}(\zeta)$ enthalten.

zu (b) Wir zeigen zunächst, dass $L = \mathbb{Q}(\sqrt[8]{2}, i)$ gilt. Die Menge der komplexen Nullstellen von $f = x^8 - 2$ ist durch $N = \{\zeta^k \sqrt[8]{2} \mid 0 \leq k < 8\}$ gegeben. Denn wegen $f(\zeta^k \sqrt[8]{2}) = (\zeta^k \sqrt[8]{2})^8 - 2 = (\zeta^8)^k \cdot 2 - 2 = 1^k \cdot 2 - 2 = 0$ sind tatsächlich alle Elemente von N Nullstellen von f. Da es sich bei ζ um eine primitive achte Einheitswurzel handelt, sind die Elemente ζ^k mit $0 \leq k < 8$ alle verschieden, und wegen $\sqrt[8]{2} \neq 0$ gilt dasselbe für $\zeta^k \sqrt[8]{2}$ mit $0 \leq k < 8$. Da andererseits ein Polynom vom Grad 8 über einem Körper nie mehr als acht Nullstellen besitzt, ist N genau die Menge der komplexen Nullstellen von f. Der Zerfällungskörper L von f über $\mathbb{Q}$ in $\mathbb{C}$ ist also durch $L = \mathbb{Q}(N)$ gegeben.

Zu zeigen bleibt $\mathbb{Q}(N) = \mathbb{Q}(\sqrt[8]{2}, i)$. Wir haben bereits in Teil (a) gesehen, dass $\cos(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}}$ und $\sin(\frac{1}{4}\pi)^2 = \cos(\frac{1}{4}\pi)^2$ gilt. Wegen $\sin(\alpha) > 0$ für $0 < \alpha < \pi$ ist somit auch $\sin(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}}$. Es folgt $\zeta = \cos(\frac{1}{4}\pi) + i\sin(\frac{1}{4}\pi) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$. Aus $\sqrt[8]{2}, i \in \mathbb{Q}(\sqrt[8]{2}, i)$ folgt $\sqrt{2} = (\sqrt[8]{2})^4 \in \mathbb{Q}(\sqrt[8]{2}, i)$ und $\zeta = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \in \mathbb{Q}(\sqrt[8]{2}, i)$. Wir erhalten weiter $\zeta^k \sqrt[8]{2} \in \mathbb{Q}(\sqrt[8]{2}, i)$ für $0 \leq k < 8$ und somit $N \subseteq \mathbb{Q}(\sqrt[8]{2}, i)$. Aus $\sqrt[8]{2} \in N \subseteq \mathbb{Q}(N)$ und $\zeta \sqrt[8]{2} \in N \subseteq \mathbb{Q}(N)$ folgt andererseits $\zeta = \frac{\sqrt[8]{2}\zeta}{\sqrt[8]{2}} \in \mathbb{Q}(N)$ und $i = \zeta^2 \in \mathbb{Q}(N)$. Insgesamt gilt also $\{\sqrt[8]{2}, i\} \subseteq \mathbb{Q}(N)$. Aus den beiden Inklusionen $\{\sqrt[8]{2}, i\} \subseteq \mathbb{Q}(N)$ und $N \subseteq \mathbb{Q}(\sqrt[8]{2}, i)$ folgt die Gleichung $\mathbb{Q}(N) = \mathbb{Q}(\sqrt[8]{2}, i)$. Insgesamt ist der Beweis von $L = \mathbb{Q}(\sqrt[8]{2}, i)$ damit abgeschlossen.

Nun bestimmen wir den Erweiterungsgrad $[L : \mathbb{Q}]$. Das Polynom $f = x^8 - 2$ ist in $\mathbb{Q}[x]$ irreduzibel nach dem Eisenstein-Kriterium, angewendet auf die Primzahl $p = 2$. Außerdem ist es normiert und hat $\sqrt[8]{2}$ als Nullstelle. Insgesamt ist f damit das Minimalpolynom von $\sqrt[8]{2}$ über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = \mathrm{grad}(f) = 2$. Das Polynom $g = x^2 + 1$ ist normiert und hat i als Nullstelle. Wäre es über $\mathbb{Q}(\sqrt[8]{2})$ reduzibel, dann müssten wegen $\mathrm{grad}(g) = 2$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt[8]{2})$ liegen. Aber dies ist unmöglich, denn es gilt $\mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$, während die Zahlen $\pm i$ nicht reell sind. Also ist g das Minimalpolynom von i über $\mathbb{Q}(\sqrt[8]{2})$, und es folgt

$$[L : \mathbb{Q}(\sqrt[8]{2})] \quad = \quad [\mathbb{Q}(\sqrt[8]{2})(i) : \mathbb{Q}(\sqrt[8]{2})] \quad = \quad \mathrm{grad}(f) \quad = \quad 2.$$

Mit der Gradformel erhalten wir $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[8]{2})] \cdot [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 2 \cdot 8 = 16$.

zu (c) Wäre G abelsch, dann müsste jede Untergruppe von G Normalteiler sein. Insbesondere wäre $\mathrm{Gal}(L|\mathbb{Q}(\sqrt[8]{2}))$ ein Normalteiler von G, und nach den Ergänzungen zum Hauptsatz der Galoistheorie würde sich daraus ergeben, dass $\mathbb{Q}(\sqrt[8]{2})|\mathbb{Q}$ eine Galois-Erweiterung ist, insbesondere eine normale Erweiterung. Aber dies ist nicht der Fall. Denn das Polynom $f = x^8 - 2$ ist über $\mathbb{Q}$ irreduzibel und hat in $\mathbb{Q}(\sqrt[8]{2})$ eine Nullstelle. Wäre die Erweiterung normal, dann müsste f über $\mathbb{Q}(\sqrt[8]{2})$ bereits in Linearfaktoren zerfallen, also alle komplexen Nullstellen bereits in $\mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$ liegen. Aber f besitzt auch nicht-reelle Nullstellen in $\mathbb{C}$, beispielsweise $\zeta\sqrt[8]{2}$. Dies zeigt, dass G nicht-abelsch ist.

Für den Beweis der zweiten Aussage zeigen wir zunächst, dass es in G ein Element σ mit $\mathrm{ord}(\sigma) = 8$ gibt. Der erste Schritt ist die Konstruktion eines solchen Elements. Nach dem Fortsetzungssatz, angewendet auf das irreduzible Polynom $f \in \mathbb{Q}[x]$ und die beiden Nullstellen $\sqrt[8]{2}$ und $\zeta\sqrt[8]{2}$, existiert ein $\mathbb{Q}$-Homomorphismus $\tilde{\sigma} : \mathbb{Q}(\sqrt[8]{2}) \to \mathbb{C}$ mit $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$. Nochmalige Anwendung dieses Satzes, diesmal auf das über $\mathbb{Q}(\sqrt[8]{2})$ irreduzible Polynom $g = x^2 + 1$, liefert eine Fortsetzung $\sigma : L \to \mathbb{C}$ von $\tilde{\sigma}$ mit $\sigma(i) = i$. Es gilt also $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$ und $\sigma(i) = i$. Da die Erweiterung $L|\mathbb{Q}$ normal ist, handelt es sich bei σ sogar um einen $\mathbb{Q}$-Automorphismus von L, also um ein Element von G.

Aus $\sigma(\sqrt[8]{2}) = \zeta\sqrt[8]{2}$ folgt $\sigma(\sqrt[2]{8}) = \sigma((\sqrt[8]{2})^4) = \sigma(\sqrt[8]{2})^4 = (\zeta\sqrt[8]{2})^4 = \zeta^4(\sqrt[8]{2})^4 = (-1)\sqrt{2} = -\sqrt{2}$ und

$$\sigma(\zeta) \quad = \quad \sigma(\tfrac{1}{\sqrt{2}} + \tfrac{i}{\sqrt{2}}) \quad = \quad \tfrac{1}{\sigma(\sqrt{2})} + \tfrac{\sigma(i)}{\sigma(\sqrt{2})} \quad = \quad -\tfrac{1}{\sqrt{2}} - \tfrac{i}{\sqrt{2}} \quad = \quad -\zeta.$$

Wir erhalten weiter

$$\sigma^2(\sqrt[8]{2}) = \sigma(\sigma(\sqrt[8]{2})) = \sigma(\zeta\sqrt[8]{2}) = \sigma(\zeta)\sigma(\sqrt[8]{2}) = (-\zeta)(\zeta\sqrt[8]{2}) = -i\sqrt[8]{2}$$

$$\sigma^4(\sqrt[8]{2}) = \sigma^2(\sigma^2(\sqrt[8]{2})) = \sigma^2(-i\sqrt[8]{2}) = -\sigma^2(i)\sigma^2(\sqrt[8]{2}) = (-i)(-i)\sqrt[8]{2} = -\sqrt[8]{2}$$

$$\sigma^8(\sqrt[8]{2}) = \sigma^4(\sigma^4(\sqrt[8]{2})) = \sigma^4(-\sqrt[8]{2}) = -\sigma^4(\sqrt[8]{2}) = -(-\sqrt[8]{2}) = \sqrt[8]{2}.$$

Aus $\sigma^8(\sqrt[8]{2}) = \sqrt[8]{2}$ und $\sigma^8(i) = i$ folgt $\sigma^8 = \mathrm{id}$, denn wegen $L = \mathbb{Q}(\sqrt[8]{2}, i)$ ist jedes Element aus G durch die Bilder von $\sqrt[8]{2}$ und i festgelegt. Aus $\sigma^4(\sqrt[8]{2}) \neq \sqrt[8]{2}$ folgt andererseits $\sigma^4 \neq \mathrm{id}$. Damit ist $\mathrm{ord}(\sigma) = 8$ nachgewiesen.

Sei nun $N = \mathrm{Gal}(L|\mathbb{Q}(\zeta))$. Als Kreisteilungserweiterung ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine normale Erweiterung, und nach den Ergänzungen zum Hauptsatz der Galoistheorie gilt somit $N \trianglelefteq G$. Darüber hinaus gilt $G/N \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$, außerdem $|G| = |\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 16$. Es folgt

$$\frac{16}{|N|} \quad = \quad \frac{|G|}{|N|} \quad = \quad |G/N| \quad = \quad |(\mathbb{Z}/8\mathbb{Z})^\times| \quad = \quad \varphi(8) \quad = \quad 4.$$

Es folgt $|N| = \frac{16}{4} = 4$. Bekanntlich sind die einzigen Gruppen der Ordnung 4 bis auf Isomorphie durch $\mathbb{Z}/4\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})^2$ gegeben.

Nehmen wir an, es ist $N \cong (\mathbb{Z}/2\mathbb{Z})^2$. Weil es in $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ nur Elemente der Ordnung 1 und 2 gibt, gilt für jedes $\tau \in G$ jeweils $\tau^2 N = (\tau N)^2 = e_{G/N} = N$ und somit $\tau^2 \in N$. Weil auch in $N \cong (\mathbb{Z}/2\mathbb{Z})^2$ nur Elemente der Ordnung 1 und 2 existieren, folgt daraus weiter $\tau^4 = (\tau^2)^2 = \mathrm{id}_L$. Aus der Annahme folgt also, dass in G nur Elemente existieren, deren Ordnungen Teiler von 4 sind, im Widerspruch dazu, dass es in G ein Element der Ordnung 8 gibt. Somit bleibt $N \cong \mathbb{Z}/4\mathbb{Z}$ als einzige Möglichkeit.