Aufgabe H12T1A3 (2+3+3+3 Punkte)

(a) Bestimmen Sie den Zerfällungskörper $L \subseteq \mathbb{C}$ von $f = (x^3 - 2)(x^2 - 5) \in \mathbb{Q}[x]$.

(b) Zerlegen Sie f über L in Linearfaktoren und bestimmen Sie $[L : \mathbb{Q}]$.

(c) Bestimmen Sie ein primitives Element von L.

(d) Bestimmen Sie die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$.

Lösung:

zu (a) Die Nullstellenmenge von f ist die Vereinigung der Nullstellenmengen der beiden Faktoren $g = x^3 - 2$ und $h = x^2 - 5$. Sei $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ (eine primitive dritte Einheitswurzel), $\alpha = \sqrt[3]{2}$ und $\beta = \sqrt{5}$. Dann sind $\alpha, \zeta\alpha, \zeta^2\alpha$ die drei komplexen Nullstellen von g und $\pm\beta$ die beiden Nullstellen von h. Der Zerfällungskörper L ist also gegeben durch

$$L \quad = \quad \mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha, \beta, -\beta).$$

Wir zeigen, dass $L = \mathbb{Q}(\zeta, \alpha, \beta)$ gilt. Die Inklusion „$\subseteq$“ ist erfüllt, weil mit ζ, α, β auch die Nullstellen $\zeta\alpha$, $\zeta^2\alpha$ und $-\beta$ von f in $\mathbb{Q}(\zeta, \alpha, \beta)$ liegen. Ebenso gilt „$\supseteq$“, denn nach Definition liegt α in L, wegen $\zeta\alpha \in L$ auch $\alpha = (\zeta\alpha)/\zeta$ und mit β auch die Nullstelle $-\beta$.

zu (b) Wir haben bereits in Aufgabenteil (a) die fünf verschiedenen Nullstellen von f bestimmt, und jede Nullstelle liefert einen Linearfaktor in der Zerlegung von f. Demnach gilt

$$f \quad = \quad gh \quad = \quad (x - \alpha)(x - \zeta\alpha)(x - \zeta^2\alpha)(x - \beta)(x + \beta).$$

Nun bestimmen wir den Erweiterungsgrad $[L : \mathbb{Q}]$. Das Element α ist Nullstelle von $g \in \mathbb{Q}[x]$. Außerdem ist g normiert und nach dem Eisenstein-Kriterium (für $p = 2$) irreduzibel. Es handelt sich also um das Minimalpolynom von α über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(g) = 3$. Das Polynom $h \in \mathbb{Q}[x]$ ist normiert, irreduzibel nach Eisenstein (für $p = 5$) und hat β als Nullstelle. Also ist h das Minimalpolynom von β über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Für die Erweiterung $K|\mathbb{Q}$ mit $K = \mathbb{Q}(\alpha, \beta)$ gilt nach dem Gradsatz

$$[K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot \quad = \quad [K : \mathbb{Q}(\alpha)] \cdot 3$$

und ebenso

$$[K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\beta)] \cdot 2 \quad ,$$

also sind 2 und 3 Teiler von $[K : \mathbb{Q}]$. Wegen $\mathrm{ggT}(2, 3) = 1$ folgt daraus, dass 6 ein Teiler von $[K : \mathbb{Q}]$ ist und folglich $[K : \mathbb{Q}] \geq 6$ gilt.

Das dritte Kreisteilungspolynom $u = x^2 + x + 1$ hat ζ als Nullstelle, ist normiert und auch in $K[x]$ noch irreduzibel. Denn andernfalls würden die beiden nicht-reellen Nullstellen ζ, ζ^2 von u wegen $\mathrm{grad}(u) = 2$ in K liegen, was aber wegen $K \subseteq \mathbb{R}$ unmöglich ist. Also ist u das Minimalpolynom von ζ über K, und wir erhalten

$$[L : K] \quad = \quad [K(\zeta) : K] \quad = \quad \mathrm{grad}(u) \quad = \quad 2.$$

Es folgt $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] \geq 2 \cdot 6 = 12$.

Für die Abschätzung des Polynomgrades nach oben sei $\tilde{g}$ das Minimalpolynom von β über $\mathbb{Q}(\alpha)$. Wegen $g(\beta) = 0$ ist $\tilde{g}$ ein Teiler von g. Es folgt

$$[K : \mathbb{Q}(\alpha)] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \quad = \quad \text{grad}(\tilde{g}) \quad \leq \quad \text{grad}(g) \quad = \quad 2$$

und $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2 \cdot 2 \cdot 3 = 12$. Damit ist insgesamt $[L : \mathbb{Q}] = 12$ bewiesen.

zu (c),(d) Zunächst bemerken wir, dass $L|\mathbb{Q}$ eine Galoiserweiterung ist. Weil L durch Adjunktion der algebraischen Elemente ζ, α, β an $\mathbb{Q}$ zu Stande kommt, handelt es sich um eine algebraische Erweiterung, und wegen $\text{char}(\mathbb{Q}) = 0$ ist diese auch separabel. Als Zerfällungskörper eines Polynoms $f \in \mathbb{Q}[x]$ über $\mathbb{Q}$ ist $L|\mathbb{Q}$ außerdem normal.

Nun bestimmen wir die Galoisgruppe $G = \text{Gal}(L|\mathbb{Q})$. Weil $L|\mathbb{Q}$ eine Galoiserweiterung ist, gilt $|G| = [L : \mathbb{Q}] = 12$. Wegen $L = \mathbb{Q}(S)$ mit $S = \{\zeta, \alpha, \beta\}$ ist jedes $\sigma \in G$ durch die Bilder $(\sigma(\zeta), \sigma(\alpha), \sigma(\beta))$ bereits eindeutig festgelegt. Weil σ ein $\mathbb{Q}$-Automorphismus ist, muss $\sigma(\zeta)$ eine Nullstelle von u, $\sigma(\alpha)$ eine Nullstelle von g und $\sigma(\beta)$ eine Nullstelle von h sein. Die Nullstellen der Polynome u, g, h wurden in den Aufgabenteilen (a) und (b) bereits bestimmt. Insgesamt ist $\sigma \mapsto (\sigma(\zeta), \sigma(\alpha), \sigma(\beta))$ damit eine injektive Abbildung $\phi : G \to T$ mit

$$T \quad = \quad \{\zeta, \zeta^2\} \times \{\alpha, \zeta\alpha, \zeta^2\alpha\} \times \{\beta, -\beta\}.$$

Wegen $|T| = 2 \cdot 3 \cdot 2 = 12 = |G|$ ist ϕ auch surjektiv. Daraus folgt, dass in G Elemente ρ, σ, τ existieren mit

$$\begin{array}{lll} \rho(\zeta) = \zeta^2 & , \quad \rho(\alpha) = \alpha & , \quad \rho(\beta) = \beta \\ \sigma(\zeta) = \zeta & , \quad \sigma(\alpha) = \zeta\alpha & , \quad \sigma(\beta) = \beta \\ \tau(\zeta) = \zeta & , \quad \tau(\alpha) = \alpha & , \quad \tau(\beta) = -\beta. \end{array}$$

Für das Element ρ gilt einerseits $\rho \neq \text{id}_L$, andererseits $\rho^2(\zeta) = \rho(\rho(\zeta)) = \rho(\zeta^2) = \rho(\zeta)^2 = (\zeta^2)^2 = \zeta^4 = \zeta$ und $\rho^2(\alpha) = \alpha$, $\rho^2(\beta) = \beta$, also $\rho^2 = \text{id}_L$. Daraus folgt $\text{ord}(\rho) = 2$. Ebenso ist $\sigma \neq \text{id}_L$, aber $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\zeta\alpha) = \sigma(\zeta)\sigma(\alpha) = \zeta(\zeta\alpha) = \zeta^2\alpha$ und

$$\sigma^3(\alpha) \quad = \quad \sigma(\sigma^2(\alpha)) \quad = \quad \sigma(\zeta^2\alpha) \quad = \quad \sigma(\zeta)^2\sigma(\alpha) \quad = \quad \zeta^2(\zeta\alpha) \quad = \quad \zeta^3\alpha \quad = \quad \alpha.$$

Wegen $\sigma^3(\zeta) = \zeta$ und $\sigma^3(\beta) = \beta$ ist $\sigma^3 = \text{id}_L$ und damit insgesamt $\text{ord}(\sigma) = 3$. Also enthält die Untergruppe $\langle\rho, \sigma\rangle$ Elemente der Ordnung 2 und 3, daraus folgt $|\langle\rho, \sigma\rangle| \geq 6$. Weiter gilt $\tau \notin \langle\rho, \sigma\rangle$, denn die Elemente in $\langle\rho, \sigma\rangle$ bilden im Gegensatz zu τ das Element β auf sich selbst ab. Aus $|\langle\rho, \sigma\rangle| \geq 6$, $\langle\rho, \sigma, \tau\rangle \supsetneq \langle\rho, \sigma\rangle$ und $|G| = 12$ folgt $G = \langle\rho, \sigma, \tau\rangle$. Damit ist die Berechnung der Galoisgruppe abgeschlossen.

Zum Schluss zeigen wir, dass $\gamma = \sqrt[3]{2}\sqrt{-3} + 10\sqrt{5}$ ein erzeugendes Element der Erweiterung $L|\mathbb{Q}$ ist. Sei $G(\gamma) = \{\sigma_1(\gamma) \mid \sigma_1 \in G\}$ die Bahn von γ unter der Operation von G, und nehmen wir an, dass $\mathbb{Q}(\gamma) \subsetneq L$ gilt. Dann ist $U = \text{Gal}(L|\mathbb{Q}(\gamma))$ nach dem Hauptsatz der Galoistheorie eine nichttriviale Untergruppe von G, und wegen $\sigma_1(\gamma) = \gamma$ für alle $\sigma_1 \in U$ ist diese im Stabilisator G_γ von γ enthalten. Es folgt $|G_\gamma| > 1$ und $|G(\gamma)| = (G : G_\gamma) < |G| = 12$. Wir führen dies nun zum Widerspruch, indem wir nachweisen, dass die Bahn $G(\gamma)$ aus genau 12 verschiedenen Elementen besteht.

Zunächst zeigen wir, dass für $K_0 = \mathbb{Q}(\sqrt{5})$ und $\tilde{\gamma} = \sqrt[3]{2}\sqrt{-3}$ die Gleichung $K_0(\tilde{\gamma}) = L$ erfüllt ist. Die Inklusion „$\subseteq$“ ist gültig, weil mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ auch das Element $\sqrt{-3}$ in L liegt und wir mit $\sqrt{-3}, \sqrt[3]{2} \in L$ auch $\tilde{\gamma} \in L$ enthalten. Wegen $\sqrt{5} \in L$ gilt schließlich auch $K_0 \subseteq L$. Für den Nachweis von „$\supseteq$“ bemerken wir zunächst, dass $\sqrt{5} \in K_0 \subseteq K_0(\tilde{\gamma})$ gilt. Mit $\tilde{\gamma}$ liegt auch $\tilde{\gamma}^2 = -3\sqrt[3]{2}$ und damit $\sqrt[3]{2}$ in $K_0(\tilde{\gamma})$, und es folgt $\tilde{\gamma}/\sqrt[3]{2} = \sqrt{-3} \in K_0(\tilde{\gamma})$ und $\zeta \in K_0(\tilde{\gamma})$. Damit ist die Gleichung bewiesen.

Sei nun $V = \mathrm{Gal}(L|K_0)$. Wegen $K_0(\tilde{\gamma}) = L$ gilt $\sigma_1(\tilde{\gamma}) \neq \tilde{\gamma}$ für alle $\sigma_1 \in V \backslash \{\mathrm{id}_L\}$ (denn aus $\sigma_1(\tilde{\gamma}) = \tilde{\gamma}$ folgt bereits $\sigma_1 = \mathrm{id}_L$, weil jedes Element der Galoisgruppe durch das Bild von $\tilde{\gamma}$ festliegt). Der Stabilisator $V_{\tilde{\gamma}}$ ist also trivial, und folglich besteht $V(\tilde{\gamma})$ aus mindestens sechs verschiedenen Elementen. Durch Anwendung der Automorphismen $\rho, \sigma \in V$ sieht man, dass diese durch

$$V(\tilde{\gamma}) \quad = \quad \{\tilde{\gamma} = \sqrt[3]{2}\sqrt{-3} \ , \ -\sqrt[3]{2}\sqrt{-3} \ , \ \sqrt[3]{2}\zeta\sqrt{-3} \ , \ -\sqrt[3]{2}\zeta\sqrt{-3} \ , \ \sqrt[3]{2}\zeta^2\sqrt{-3} \ , \ -\sqrt[3]{2}\zeta^2\sqrt{-3}\}$$

gegeben sind. Mit $V(\tilde{\gamma})$ enthält auch

$$\begin{aligned} V(\gamma) \quad = \quad & \{\sqrt[3]{2}\sqrt{-3} + 10\sqrt{5} \ , \ -\sqrt[3]{2}\sqrt{-3} + 10\sqrt{5} \ , \ \sqrt[3]{2}\zeta\sqrt{-3} + 10\sqrt{5} \ , \\ & -\sqrt[3]{2}\zeta\sqrt{-3} + 10\sqrt{5} \ , \ \sqrt[3]{2}\zeta^2\sqrt{-3} + 10\sqrt{5} \ , \ -\sqrt[3]{2}\zeta^2\sqrt{-3} + 10\sqrt{5}\} \end{aligned}$$

genau sechs verschiedene Elemente. Berücksichtigt man nun noch die Operation von τ, so erhalten für die Bahn von γ unter G die Gleichung $G(\gamma) = V(\gamma) \cup B$ mit

$$\begin{aligned} B \quad = \quad & \{\sqrt[3]{2}\sqrt{-3} - 10\sqrt{5} \ , \ -\sqrt[3]{2}\sqrt{-3} - 10\sqrt{5} \ , \ \sqrt[3]{2}\zeta\sqrt{-3} - 10\sqrt{5} \ , \\ & -\sqrt[3]{2}\zeta\sqrt{-3} - 10\sqrt{5} \ , \ \sqrt[3]{2}\zeta^2\sqrt{-3} - 10\sqrt{5} \ , \ -\sqrt[3]{2}\zeta^2\sqrt{-3} - 10\sqrt{5}\}. \end{aligned}$$

Dabei sind die Menge $V(\gamma)$ und B disjunkt. Denn alle Elemente in $V(\tilde{\gamma})$ sind vom Betrag $\sqrt[3]{2}\sqrt{3}$, und damit kann der Realteil der Elemente in $V(\gamma)$ durch $\geq 10\sqrt{5} - \sqrt[3]{2}\sqrt{3} \geq 20 - 2 \cdot 3 \geq 14$ abgeschätzt werden. Für den Realteil der Elemente aus B dagegen gilt die obere Abschätzung $\leq -10\sqrt{5} + \sqrt[3]{2}\sqrt{3} \leq -20 + 2 \cdot 3 \leq -14$. Insgesamt erhalten wir damit $|G(\gamma)| = |V(\gamma)| + |B| = 6 + 6 = 12$ wie gewünscht.