

Aufgabe	A1	A2	A3	A4	Σ
Punkte					

Aufgabe 1. Es gilt $f = X^4 - 4X^2 + 9 = (X^2 - 2)^2 + 5$. Damit setze $\alpha := \sqrt{2 + i\sqrt{5}}$. Dann gilt

$$f(\pm\alpha) = (2 + i\sqrt{5} - 2)^2 + 5 = (i\sqrt{5})^2 + 5 = 0.$$

Damit ist $\alpha^4 - 4\alpha^2 + 9 = 0$, also insbesondere $-\alpha^4 + 2\alpha^2 = -2\alpha^2 + 9$. Damit folgt

$$f\left(\pm\frac{3}{\alpha}\right) = \left(\frac{9}{\alpha^2} - 2\right)^2 + 5 = \left(\frac{-\alpha^4 + 2\alpha^2}{\alpha^2}\right)^2 + 5 = (\alpha^2 - 2)^2 + 5 = f(\alpha) = 0.$$

Also sind die Nullstellen von f gegeben als $\{\pm\alpha, \pm 3/\alpha\}$ und damit $L = \mathbb{Q}(\alpha)$.

Z.z.: f irreduzibel. Es ist f g.d. irreduzibel über $\mathbb{Q}$, wenn f irreduzibel über $\mathbb{Z}$. Ang.: f reduzibel über $\mathbb{Z}$. Da f keine Nullstellen in $\mathbb{Z}$ hat, folgt

$$f = (X^2 + aX + b)(X^2 + cX + d) = X^4 + \underbrace{(a+c)}_{=0} X^3 + \underbrace{(b+d+ac)}_{=-4} X^2 + \underbrace{(ad+bc)}_{=0} X + \underbrace{bd}_{=9}$$

mit $a, b, c, d \in \mathbb{Z}$. Es folgt direkt $c = -a$ und $a(d - b) = 0$. Falls $a = 0$, folgt $b + d = -4$ und $bd = 9$, aber $3 + 3 = 6 \neq -4 \neq -6 = -3 - 3$. Falls $a \neq 0$ folgt $d = b$ also $b^2 = 9$ und $2b - a^2 = -4$. Also

$$a^2 = 2b + 4 = \begin{cases} 10 & b = 3 \\ -2 & b = -3 \end{cases}, \text{ aber weder } 10 \text{ noch } -3 \text{ Quadrate in } \mathbb{Z}. \text{ Also folgt } f \text{ irreduzibel.}$$

Da $\text{char}(\mathbb{Q}) = 0$ ist f also separabel und f Minimalpolynom von α , also $\#\text{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$ und $\text{Gal}(L/\mathbb{Q})$ operiert transitiv auf den Nullstellen von f . Mit $\sigma: \alpha \mapsto -\alpha$ und $\tau: \alpha \mapsto \frac{3}{\alpha}$ folgt damit $\text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$. Als Gruppe der Ordnung 4 ist $\text{Gal}(L/\mathbb{Q})$ abelsch, also $\sigma\tau = \tau\sigma$ und durch offensichtlicherweise gilt $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \text{id}$. Nach Satz von Lagrange hat $\text{Gal}(L/\mathbb{Q})$ UG der Ordnung 1, 2 oder 4. Neben der trivialen Untergruppe und $\text{Gal}(L/\mathbb{Q})$ selbst, gibt es also nur UG der Ordnung 2. Da 2 Primzahl, sind diese zyklisch. Also existieren insgesamt genau die Untergruppen

$$\begin{aligned} H_0 &:= \langle \text{id} \rangle \\ H_1 &:= \langle \sigma \rangle \\ H_2 &:= \langle \tau \rangle \\ H_3 &:= \langle \sigma\tau \rangle \\ H_4 &:= \langle \sigma, \tau \rangle \end{aligned}$$

Es ist $\sigma(\alpha^2) = \sigma(\alpha)\sigma(\alpha) = (-\alpha)(-\alpha) = \alpha^2$. Weiter ist $9 = 4\alpha^2 - \alpha^4$. Damit folgt $\frac{3}{\alpha} = \frac{4}{3}\alpha - \frac{1}{3}\alpha^3$ und $\frac{27}{\alpha^3} = \frac{7}{3}\alpha - \frac{4}{3}\alpha^3$. Damit folgt $\tau(-7\alpha + \alpha^3) = -7\left(\frac{4}{3}\alpha - \frac{1}{3}\alpha^3\right) + \frac{7}{3}\alpha - \frac{4}{3}\alpha^3 = -7\alpha + \alpha^3$ und $\sigma(\tau(\alpha - \alpha^3)) = \sigma\left(\frac{4}{3}\alpha - \frac{1}{3}\alpha^3 - \frac{7}{3}\alpha + \frac{4}{3}\alpha^3\right) = \sigma(-\alpha + \alpha^3) = \alpha - \alpha^3$. Diese Elemente sind jeweils unter den anderen Automorphismen nicht invariant. Also folgen nach dem Hauptsatz

$$\begin{aligned} L^{H_0} &= L \\ L^{H_1} &= \mathbb{Q}(\alpha^2) \\ L^{H_2} &= \mathbb{Q}(-7\alpha + \alpha^3) \\ L^{H_3} &= \mathbb{Q}(\alpha - \alpha^3) \\ L^{H_4} &= \mathbb{Q} \end{aligned}$$

als Zwischenkörper von $L/\mathbb{Q}$

Aufgabe 2. Im folgenden bezeichne echte Untergruppe eine echte, nicht-triviale Untergruppe.

(a) Beh.: Die Aussage ist falsch.

Beweis. Es ist $f = X^4 - 7$ irreduzibel nach Eisenstein mit $p = 7$ und $f(\sqrt[4]{7}) = 0$, aber auch $f(i\sqrt[4]{7}) = 0$ und $i\sqrt[4]{7} \notin \mathbb{R}$, aber $\mathbb{Q}(\sqrt[4]{7}) \subseteq \mathbb{R}$, also zerfällt f über $\mathbb{Q}(\sqrt[4]{7})$ nicht in Linearfaktoren, also $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ nicht normal und damit nicht galoissch. $\square$

(b) Beh.: Die Aussage stimmt.

Beweis. Mit Euklidischem Algorithmus ist durch Rechnung zu sehen, dass $(f, f') = 1$. Also ist f separabel und damit $[L: \mathbb{Q}] \mid 4! = 24$. $\square$

(c) Beh.: Die Aussage ist falsch.

Beweis. Es ist $f = X^3 - 2$ irreduzibel nach Eisenstein mit $p = 2$ und $\text{char}(\mathbb{Q}) = 0$, also f separabel. Da $\alpha_j := \sqrt[3]{2}e^{i\frac{2\pi j}{3}}$ die 3 paarw. verschiedenen Nullstellen von f . Also folgt $L = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ und $\alpha_0 = \sqrt[3]{2} \in \mathbb{R}$, aber $L \not\subseteq \mathbb{R}$ folgt $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha_0) \subsetneq L$. Also hat $\text{Gal}(L/\mathbb{Q})$ eine echte Untergruppe. Da $[L: \mathbb{Q}] \mid 3! = 6$ folgt $\#\text{Gal}(L/\mathbb{Q}) \in \{1, 2, 3, 6\}$. Da $\{0\}$, $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ keine echten Untergruppen haben, folgt $\#\text{Gal}(L/\mathbb{Q}) = 6$ und damit $\text{Gal}(L/\mathbb{Q}) = S_3$, also nicht abelsch, insbesondere nicht zyklisch. $\square$

(d) Beh.: S_3 hat 4 echte Untergruppen.

Beweis. Es ist $\#S_3 = 6$, also haben nach Satz von Lagrange echte Untergruppen Ordnung 2 oder 3. In Zykelschreibweise ist

$$S_3 = \{(), (12), (23), (13), (123), (132)\}.$$

Es ist $\text{ord}((12)) = \text{ord}((23)) = \text{ord}((13)) = 2$ und $\text{ord}((123)) = \text{ord}((132)) = 3$.

Da Gruppen der Ordnung 2 und 3 zyklisch sind und $\langle (123) \rangle = \langle (132) \rangle$ gibt es genau eine Untergruppe der Ordnung 3 und 3 Untergruppen der Ordnung 2. $\square$

Beh.: Die Aussage stimmt.

Beweis. Falls f reduzibel existiert ein $g \in \mathbb{Q}[X]$ mit $f = g(X - \alpha)$ für $\alpha \in \mathbb{Q}$ mit $\deg(g) = 2$. Da $\alpha \in \mathbb{Q}$ ist L auch Zerfällungskörper von g über $\mathbb{Q}$ und $[L: \mathbb{Q}] \leq 2! = 2$. Also hat $L/\mathbb{Q}$ keine echten Zwischenkörper.

Sei nun f irreduzibel. Da $\text{char}(\mathbb{Q}) = 0$ ist f separabel und damit $\#\text{Gal}(L/\mathbb{Q}) \in \{1, 2, 3, 6\}$. Für $\#\text{Gal}(L/\mathbb{Q}) \in \{1, 2, 3\}$ hat diese keine echten Untergruppen, da 2 und 3 prim und $\{0\}$ die triviale Gruppe. Falls $\#\text{Gal}(L/\mathbb{Q}) = 6$ folgt $\text{Gal}(L/\mathbb{Q}) \cong S_3$. Dann folgt die Behauptung aus der Vorbemerkung. $\square$

(e) Beh.: Die Aussage stimmt.

Beweis. Sei $K \subseteq L \subseteq \overline{K}$ ein algebraischer Abschluss von K und $\alpha \in \overline{K}$ mit $\alpha^4 = a$. Es ist f irreduzibel und $f' = 4X^3 \neq 0$, da $\text{char}(K) \neq 2$, also f separabel. Sei $\zeta \in \mu_4$ mit $\langle \zeta \rangle = \mu_4$. Dann sind $\{\alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4\}$ die vier paarweise verschiedenen Nullstellen von f . Es ist $L = K(\alpha, \zeta)$. Dann ex. $\sigma, \tau \in \text{Gal}(L/K)$ mit

$$\begin{aligned}\sigma: \alpha &\mapsto \alpha & \zeta &\mapsto \zeta^2 \\ \tau: \alpha &\mapsto \alpha\zeta & \zeta &\mapsto \zeta,\end{aligned}$$

da $\sigma(\alpha\zeta^k) = \alpha\zeta^{2k}$ und $\tau(\alpha\zeta^k) = \alpha\zeta^{2k}$ Nullstellen von f in Nullstellen von f überführen. Aber es gilt

$$\sigma(\tau(\alpha)) = \sigma(\alpha\zeta) = \alpha\zeta^2 \neq \alpha\zeta = \tau(\alpha) = \tau(\sigma(\alpha)).$$

Also ist $\text{Gal}(L/K)$ nicht abelsch, insbesondere nicht zyklisch. $\square$

(f) Beh.: Die Aussage stimmt.

Beweis. Falls $[L: K] = \infty$: Dann hat $[L: \mathbb{Q}]$ maximal ∞ ZK. Falls $[L: K] = n < \infty$: Dann korrespondieren die Zwischenkörper von L/K zu Untergruppen von $\text{Gal}(L/K)$. Da $\#\text{Gal}(L/K) = n$, hat diese nur maximal 2^n paarweise verschiedene Teilmengen, insbesondere maximal 2^n paarweise verschiedene Untergruppen. $\square$

Aufgabe 3. (a) Es ist $\mu_n = \{\zeta_n^k\}_{k=0}^{n-1}$ mit $\zeta_n^k = e^{\frac{2\pi i k}{n}}$. Weiter bezeichne σ die komplexe Konjugation. Dann gilt

$$\sigma(\zeta_n^k) = e^{-\frac{2\pi i k}{n}} = e^{\frac{2\pi i}{n}(n-k)} = \zeta_n^{n-k}.$$

Beachte, dass $\zeta_n^n = \zeta_n^0 = 1$. Damit ergibt sich die Permutation

$$\pi: \{0, \dots, n-1\} \rightarrow \{0, \dots, n-1\}$$

$$k \mapsto \begin{cases} n-k & k < n \\ 0 & k = n \end{cases}.$$

Auf $\mathbb{Z}/n\mathbb{Z}$ ergibt das die Permutation

$$\tau: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

$$k \mapsto \overline{n-k}.$$

(b) Es ist $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{R} \iff \frac{2\pi i}{n} \in \{\pi i, 2\pi i\} \iff n = 1 \vee n = 2$. Also $\zeta_n \in \mathbb{C} \setminus \mathbb{R}$ für $n \geq 3$. Also $[L: L \cap \mathbb{R}] > 1$, also $L = L \cap \mathbb{C} = (L \cap \mathbb{R})(i)$ und $X^2 + 1$ irreduzibel über $L \cap \mathbb{R}$, da $\pm i \notin L \cap \mathbb{R}$. Also folgt $[L: L \cap \mathbb{R}] = [(L \cap \mathbb{R})(i): L \cap \mathbb{R}] = 2$.

Es ist

$$\zeta_n + \zeta_n^{-1} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) + \cos\left(-\frac{2\pi}{n}\right) + i \sin\left(-\frac{2\pi}{n}\right) = 2 \cos\left(\frac{2\pi}{n}\right) \in \mathbb{R}.$$

Also folgt $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \in L \cap \mathbb{R}$. Betrachte nun $f = X^2 - (\zeta_n + \zeta_n^{-1})X + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Es ist $f(\zeta_n) = 0$, also folgt $[L: \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$. Da $[L: L \cap \mathbb{R}] = 2$ folgt

$$2 \geq [L: \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = \underbrace{[L: L \cap \mathbb{R}]}_{=2} [L \cap \mathbb{R}: \mathbb{Q}(\zeta_n + \zeta_n^{-1})],$$

und damit $L \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Aufgabe 4. (a) Sei $a \in K$. Dann definiere

$$\sigma_a: L \rightarrow L$$

$$f \mapsto f(Y + a).$$

Dann ist $\sigma_a|_K = \text{id}$ und $\sigma_a(Y) = Y + a$. Es ist $\sigma_{-a} \circ \sigma = \text{id} = \sigma \circ \sigma_{-a}$, also σ_a bijektiv. Nachrechnen ergibt, dass σ_a K -Homomorphismus ist. Also $\sigma_a \in \text{Aut}_K(L)$. Das zeigt die Existenz.

Seien nun $\sigma, \tau \in \text{Aut}_K(L)$ mit $\sigma(Y) = Y + a = \tau(Y)$. Dann sei $f \in K(Y)$. Dann gilt wegen $\sigma|_K = \text{id} = \tau|_K$:

$$\sigma(f) = f(Y + a) = \tau(f).$$

Das zeigt die Eindeutigkeit.

(b) Setze $\phi: K \rightarrow G, a \mapsto \sigma_a$. Es ist ϕ wohldefiniert nach (a) und

$$\phi(a) = \phi(b) \implies \sigma_a(Y) = \sigma_b(Y) \implies Y + a = Y + b \implies a = b,$$

also ϕ injektiv. Nach Konstruktion von G ist ϕ surjektiv. Es gilt außerdem für $a, b \in K$:

$$\phi(a+b)(Y) = Y + a + b = \sigma_a(Y) + b = \sigma_a(Y + b) = \sigma_a(\sigma_b(Y)) = \sigma_a \circ \sigma_b(Y).$$

Nach (a) ist $\phi(a+b)$ damit eindeutig festgelegt und es folgt $\phi(a+b) = \phi(a)\phi(b)$, also ϕ Gruppeniso. Da $G = \text{Bild}(\phi)$ folgt G Untergruppe von $\text{Aut}_K(L)$.

Zeige letzte Behauptung per Kontraposition. Sei also $K \subsetneq L^G$. Dann ex. ein $f \in L^H \setminus K$ mit $g, h \in K[Y], g \neq 0$ und $f = \frac{g}{h}$.

Falls $\forall a \in K: h(a) = 0$, folgt wegen $g \neq 0 \# K \leq \deg(h) < \infty$, also K endlich.

Sonst ex. ein $a \in K$ mit $h(a) \neq 0$. Dann setze $d := f(a) \in K$. Betrachte nun $p := f - d \in K(Y)$. Es ist $f \in L^G$, denn $\forall r \in K$ ist $\sigma_r(p) = \sigma_r(f) - d = f - d = p$. Es ist außerdem $p(a) = f(a) - d = d - d = 0$ und damit $\forall r \in K: p(a+r) = p(a) = 0$. Da $f \notin K$ ist $p = f - d \notin K$ und damit $p \neq 0$. Weiter existieren $\tilde{g}, \tilde{h} \in K[Y]$ mit $f = \frac{\tilde{g}}{\tilde{h}}$ und damit $\forall r \in K: \tilde{g}(a+r) = \tilde{g}(a) = 0$. Also folgt, da $p \neq 0$ und damit $\tilde{g} \neq 0: \# K \leq \deg(\tilde{g}) < \infty$. Also ist K endlich.

(c) Es ist zunächst $K(Z) \subseteq L^H$, denn für $f \in K(Z)$ und $a \in \mathbb{F}_p$ ist

$$\begin{aligned} \sigma_a(f(Y^p - Y)) &= f(\sigma_a(Y^p - Y)) \\ &= f((Y + a)^p - Y - a) \\ &\stackrel{\text{char}(K)=p>0}{=} f(Y^p + a^p - Y - a) \\ &\stackrel{\text{Fermat}}{=} f(Y^p - Y). \end{aligned}$$

Weiter ist $\mathbb{F}_p$ endlich und nach (a) ist damit $\#H = \#\mathbb{F}_p = p$. Damit ist L/L^H galoissch mit $[L : L^H] = \#H = p$. Betrachte nun weiter

$$f = X^p - X - (Y^p - Y) \in K(Z)[X].$$

Dann ist $\deg(f) = p$ und $f(Y) = 0$. Also folgt $[L : K(Z)] \leq p$. Damit gilt wegen $K(Z) \subseteq L^H$:

$$p \geq [L : K(Z)] = [L : L^H][L^H : K(Z)] = p[L^H : K(Z)].$$

Also folgt $L^H = K(Z)$.