Aufgabe 1

Ist α eine Nullstelle von f, so auch $-\alpha$, da nur gerade Potenzen vorkommen. Daher gilt

$$X^4 - 4X^2 + 9 = (X^2 - \alpha^2)(X^2 - \beta^2) = X^4 - (\alpha^2 + \beta^2)X^2 + \alpha^2\beta^2$$

für zwei Nullstellen α und β. Durch Koeffizientenvergleich folgt $\beta = \frac{3}{\alpha}$. Durch Einsetzen verifiziert man, dass $\alpha = \sqrt{2 + \sqrt{-5}}$ eine Nullstelle von f ist. Wegen $\alpha \notin \mathbb{R}$ besitzt das Polynom keine Nullstelle in $\mathbb{Q}$. Um zu zeigen, dass f irreduzibel ist, wählen wir den Ansatz

$$X^4 - 4X^2 + 9 = (X^2 + aX + bX^2)(X^2 + cX + d) = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd$$

Daraus folgt $c = -a$ und $a(d - b) = 0$. $a = 0$ führt auf $b + d = -4$, $bd = 9$; hat keine Lösung in $\mathbb{Z}$. $a \neq 0$ führt auf $d = b \implies b^2 = 9 \implies b = \pm 3$ und $2b - a^2 = -4 \implies a^2 = 2b + 4 = 10$ oder 2, das sind aber keine Quadrate in $\mathbb{Z}$, Widerspruch. Daher ist f irreduzibel. Die Menge der Nullstellen ist dann gegeben durch $\{\pm\alpha, \pm\frac{3}{\alpha}\}$. Insbesondere ist ein Zerfällungskörper gegeben durch $L \coloneqq \mathbb{Q}(\alpha)$. Da f irreduzibel ist, ist f das Minimalpolynom zu α und die Erweiterung hat somit Grad 4. Daher ist $\sigma_i \in \mathrm{Gal}(L/Q)$ eindeutig bestimmt durch $\sigma(\alpha)$. Daher gilt

$$G \coloneqq \mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

mit $\sigma_1 \colon \alpha \mapsto \alpha$, $\sigma_2 \colon \alpha \mapsto -\alpha$, $\sigma_3 \colon \alpha \mapsto \frac{3}{\alpha}$, $\sigma_4 \colon \alpha \mapsto -\frac{3}{\alpha}$. Es gilt $\sigma_1 = \mathrm{id}$ und $\sigma_2 \circ \sigma_3 = \sigma_4 = \sigma_3 \circ \sigma_2$, $\sigma_2 \circ \sigma_4 = \sigma_3 = \sigma_4 \circ \sigma_2$ und $\sigma_3 \circ \sigma_4 = \sigma_2 = \sigma_4 \circ \sigma_3$. G ist also abelsch. Außerdem gilt $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \mathrm{id}$. Daher ist die Abbildung

$$\begin{aligned} G &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ \sigma_1 &\mapsto (0,0) \\ \sigma_2 &\mapsto (1,0) \\ \sigma_3 &\mapsto (0,1) \\ \sigma_4 &\mapsto (1,1) \end{aligned}$$

ein Gruppenisomorphismus. Alle echten Untergruppen von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ haben Ordnung 2. Die echten Untergruppen von G sind daher

$$U_1 \coloneqq \{\sigma_1, \sigma_2\}, U_2 \coloneqq \{\sigma_1, \sigma_3\}, U_3 \coloneqq \{\sigma_1, \sigma_4\}$$

. Daher erhalten wir drei Zwischenkörper.

1. Der erste Zwischenkörper ist gegeben durch

   $$K_1 = L^{U_1} = \{x \in L \colon \sigma_2(x) = x\}$$

   Es gilt $\sigma_2(\alpha^2) = \sigma_2(\alpha)\sigma_2(\alpha) = \alpha^2$. Damit ist $\mathbb{Q}(\alpha^2) \subset K_1$. Das Minimalpolynom von α^2 geht aus dem von α durch $X^2 \mapsto X$ hervor und ist folglich gegeben durch $X^2 - 4X + 9$. Damit gilt $[\mathbb{Q}(\alpha^2) \colon \mathbb{Q}] = 2$ und daher $K_1 = \mathbb{Q}(\alpha^2)$.

2. Der zweite Zwischenkörper ist gegeben durch

   $$K_2 = L^{U_2} = \{x \in L \colon \sigma_3(x) = x\}$$

Es gilt $\sigma_3(\alpha + 3/\alpha) = \sigma_4(\alpha) + \sigma_4(3/\alpha) = 3/\alpha + \alpha$. Damit ist $\mathbb{Q}(\alpha + 3/\alpha) \subset K_2$. $X^2 - 10$ ist offensichtlich irreduzibel über $\mathbb{Q}$. Wegen

$$\begin{aligned}(\alpha + 3/\alpha)^2 &= \alpha^2 + 6 + 9/\alpha^2 \\ &= 2 + \sqrt{-5} + 6 + \frac{9}{2 + \sqrt{-5}} \\ &= 8 + \sqrt{-5} + \frac{9(2 - \sqrt{-5})}{(2 + \sqrt{-5})(2 - \sqrt{-5})} \\ &= 8 + \sqrt{-5} + \frac{9(2 - \sqrt{-5})}{2^2 + 5} && = 10\end{aligned}$$

gilt $[\mathbb{Q}(\alpha + 3/\alpha) \colon \mathbb{Q}] = 2$ und daher $K_2 = \mathbb{Q}(\alpha + 3/\alpha)$.

3. Der dritte Zwischenkörper ist gegeben durch

$$K_3 = L^{U_2} = \{x \in L \colon \sigma_4(x) = x\}$$

Es gilt $\sigma_4(\alpha - 3/\alpha) = \sigma_4(\alpha) + \sigma_4(-3/\alpha) = -3/\alpha + \alpha$. Damit ist $\mathbb{Q}(\alpha - 3/\alpha) \subset K_3$. $X^2 + 2$ ist offensichtlich irreduzibel über $\mathbb{Q}$. Wegen

$$\begin{aligned}(\alpha - 3/\alpha)^2 &= \alpha^2 - 6 + 9/\alpha^2 \\ &= 2 + \sqrt{-5} - 6 + \frac{9}{2 + \sqrt{-5}} \\ &= -4 + \sqrt{-5} + \frac{9(2 - \sqrt{-5})}{(2 + \sqrt{-5})(2 - \sqrt{-5})} \\ &= -4 + \sqrt{-5} + \frac{9(2 - \sqrt{-5})}{2^2 + 5} && = -2\end{aligned}$$

gilt $[\mathbb{Q}(\alpha - 3/\alpha) \colon \mathbb{Q}] = 2$ und daher $K_3 = \mathbb{Q}(\alpha - 3/\alpha)$.

Aufgabe 2

(a) Das Polynom $f = X^4 - 7$ (irreduzibel nach Eisenstein) hat über $\overline{Q} \subset \mathbb{C}$ die vier Nullstellen $\pm\sqrt[4]{7}, \pm i\sqrt[4]{7}$. Insbesondere besitzt es eine Nullstelle in $\mathbb{Q}(\sqrt[4]{7})$. Wegen $\mathbb{Q}(\sqrt[4]{7}) \subset \mathbb{R}$ zerfällt f aber nicht in Linearfaktoren. Daher ist die Erweiterung nicht normal und insbesondere nicht galoissch.

(b) f ist irreduzibel nach Eisenstein. Daher ist f als Polynom über $\mathbb{Q}$ separabel. Also ist $L/\mathbb{Q}$ eine endliche Galoiserweiterung und nach Korollar 4.20 kann $\mathrm{Gal}(L/\mathbb{Q})$ als Untergruppe von $\mathfrak{S}(\{\alpha_1, \ldots, \alpha_i\})$ aufgefasst werden, wenn $\{\alpha_1, \ldots, \alpha_i\}$ die Menge der Nullstellen von f bezeichnet. Da f ein Polynom 4. Grades ist gilt $i \leq 4$. Die Untergruppenordnung teilt die Ordnung der Gruppe, wegen $\#\mathfrak{S}(\{\alpha_1, \ldots, \alpha_4\}) = 24 | 24, \#\mathfrak{S}(\{\alpha_1, \ldots, \alpha_3\}) = 6 | 24$ und $\#\mathfrak{S}(\{\alpha_1, \alpha_2\}) = 2 | 24$ gilt auch $[L \colon \mathbb{Q}] = \#\,\mathrm{Gal}(L/\mathbb{Q}) | 24$.

(c) Die Diskriminante von $X^3 - 2$ ist gegeben durch $-27 \cdot b^2 = -108 \neq x^2 \forall x \in \mathbb{Q}$. Daher ist $\mathrm{Gal}(L/K) \cong \mathfrak{S}_3$ und damit nicht zyklisch.

(d) Für die Galoisgruppe G eines Polynoms dritten Grades gilt entweder $G \cong \mathfrak{S}_3$ oder $G \cong \mathfrak{A}_3$. Im zweiten Fall hat die Gruppe nur 3 Elemente und somit weniger als 4 echte Untergruppen. Echte Untergruppen von $\mathfrak{S}_3$ haben die Ordnung 2 oder 3, da sie die Gruppenordnung teilen müssen. Da jede Transposition selbstinvers sind, erhalten wir durch $\{e, (12)\}, \{3, (23)\}, \{e, (31)\}$ drei Untergruppen. Außerdem ist $\mathfrak{A}_3$ ebenfalls eine Untergruppe von $\mathfrak{S}_3$. Es gilt nun $(123)^2 = (132)$ und $(132)^2 = (123)$. Zu jedem Element $\pi \in \mathfrak{A}_3$ existieren zwei Transpositionen τ_1, τ_2 mit $\tau_1 \circ \tau_2 = \pi$. Genauso gilt $\forall tau_1 \neq \tau_2 \in \mathfrak{S}_3 \setminus \mathfrak{A}_3 \colon \tau_1\tau_2 \in \mathfrak{A}_3 \setminus \{e\}$. Eine Transposition τ und ein Element $\pi \in \mathfrak{A}_3$ erzeugen daher stets eine weitere Transposition, da $\exists \tau' \colon \pi = \tau'\tau$ und daher $\pi\tau = \tau'\tau\tau = \tau'$. Folglich kann es keine weiteren Untergruppen der Ordnung zwei oder drei geben. Die Anzahl der echten Untergruppen ist also durch 4 nach oben beschränkt. Nach dem Hauptsatz der Galoistheorie ist damit die Anzahl der echten Zwischenkörper auch kleiner als 4.

(e) Sei $K = \mathbb{F}_5$ und sei α eine Nullstelle von $X^4 - a$. Dann ist wegen $(2^i\alpha)^4 = (2^4)^i\alpha^4 = a$ die Menge der Nullstellen gerade $\{2^i\alpha,\ i \in \{1, 2, 3, 4\}\}$, da diese Menge bereits vier verschiedene Nullstellen enthält. Der Zerfällungskörper von $X^4 - a$ ist daher gegeben durch $\coloneqq \mathbb{F}_5(\alpha)$ und jedes $\sigma \in \mathrm{Gal}(L/K)$ ist eindeutig bestimmt durch $\sigma(\alpha)$. Daher gilt

$$\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_4\}$$

mit $\sigma_i \colon \alpha \mapsto 2^i\alpha$. Also ist $\mathrm{Gal}(L/K)$ zyklisch mit Erzeuger σ_1:

$$\sigma_i(\alpha) = 2^i\alpha = (\sigma_1)^i(\alpha).$$

Also ist die Aussage falsch.

(f) Ist $[L \colon K] < \infty$, so ist die Menge aller Untergruppen von $\mathrm{Gal}(L/K)$ ist eine Teilmenge der Potenzmenge, deren Kardinalität durch $2^{\#\,\mathrm{Gal}(L/K)} = 2^{[L \colon K]}$ gegeben ist. Nach dem Hauptsatz der Galoistheorie damit die Anzahl der Zwischenkörper auch höchstens $2^{[L \colon K]}$. Ist L/K eine unendliche Erweiterung, so stellt $2^{[L \colon K]} = \infty$ keine Schranke dar und die Aussage ist ebenfalls wahr.

Aufgabe 3

(a) Wir betrachten O.B.d.A. den algebraischen Abschluss von $\mathbb{Q}$ in den komplexen Zahlen, $\overline{Q} \subset \mathbb{C}$. Nach Analysis 2 hat die Gleichung $\zeta^n = 1$ genau die Lösungen $e^{\frac{2\pi ik}{n}}$ mit $1 \leq k \leq n$. Wegen $e^{\frac{2\pi ik}{n}} = (e^{\frac{2\pi i}{n}})^k$ ist $e^{\frac{2\pi i}{n}}$ eine primitive Einheitswurzel. Setze daher $\zeta_n = e^{\frac{2\pi i}{n}}$. Dann erhalten wir einen Gruppenisomorphismus

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\to \mu_n \\ k &\mapsto \zeta_n^k = e^{\frac{2\pi ik}{n}} \end{aligned}$$

Es gilt $\overline{e^{\frac{2\pi ik}{n}}} = e^{\frac{2\pi i(-k)}{n}} = e^{\frac{2\pi i(n-k)}{n}}$. Also induziert die komplexe Konjugation eine Permutation π_C von $\mathbb{Z}/N\mathbb{Z}$ via $\zeta_n^k \mapsto \zeta_n^{\pi_C(k)}$ mit $\pi_C(n) = n$ und $\pi_C(k) = \pi_C(n-k) \forall k \in \{1, \ldots, n-1\}$.

(b) Da L gerade der Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist, kann die Galoisgruppe $\mathrm{Gal}(L/L \cap \mathbb{R})$ mit einer Untergruppe der $\mathfrak{S}_n$ identifiziert werden, wobei $\pi \in \mathfrak{S}_n$ auf μ_n via $\zeta_n^k \mapsto \zeta_n^{\pi(k)}$ operiert.

Außerdem gilt

$$\begin{aligned}\zeta_n^k + \zeta_n^{-k} &= e^{\frac{2\pi i k}{n}} + e^{\frac{2\pi i (n-k)}{n}} \\ &= \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) + \cos(\frac{2\pi(-k)}{n}) + i\sin(\frac{2\pi(-k)}{n}) \\ &= 2\cos(\frac{2\pi k}{n}) \in \mathbb{R}\end{aligned}$$

Sei also $\sigma \in \mathrm{Gal}(L/L\cap\mathbb{R})$. Dann muss gelten

$$\begin{aligned}\sigma(\zeta_n + \zeta_n^{-1}) &= \zeta_n + \zeta_n^{-1} \\ \sigma(\zeta_n) + \sigma(\zeta_n)^{-1} &= \zeta_n + \zeta_n^{-1}\end{aligned}$$

Sei π die zu σ gehörige Permutation

$$\begin{aligned}\zeta_n^{\pi(1)} + \zeta_n^{-\pi(1)} &= \zeta_n + \zeta_n^{-1} \\ 2\cos(\frac{2\pi\pi(1)}{n}) &= 2\cos(\frac{2\pi}{n})\end{aligned}$$

Für $\pi(1) \in \{1,\dots,n\}$ gibt es hier aufgrund der Symmetrie von $\cos(x)$ bezüglich $x = 1$ zwei Möglichkeiten

$$\pi(1) \in \{1, n-1\}$$

Da es sich bei ζ_n um eine primitive Einheitswurzel handelt gilt $L = \mathbb{Q}(\zeta_n)$ und π ist durch $\pi(1)$ bereits eindeutig bestimmt, es gilt dann $\zeta_n^{\pi(k)} = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = \zeta_n^{k\pi(1)}$. Wegen $\pi_C(1) = n-1$ handelt es sich bei einem Automorphismus $\sigma \in \mathrm{Gal}(L/L\cap\mathbb{R})$ entweder um die Identität oder die komplexe Konjugation, es gilt also

$$\mathrm{Gal}(L/L\cap\mathbb{R}) = \{\mathrm{id}, C\},$$

wobei C die komplexe Konjugation bezeichne. Daher erhalten wir $[L\colon L\cap\mathbb{R}] = \#\,\mathrm{Gal}(L/L\cap\mathbb{R}) = 2$. Sei $\alpha := \frac{\zeta_n+\zeta_n^{-1}}{2} = \cos(\frac{2\pi}{n})$. Dann gilt $\zeta_n = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = \alpha + i\sin(\frac{2\pi}{n})$. Es gilt

$$\begin{aligned}(\zeta_n - \alpha)^2 &= -\sin^2(\frac{2\pi}{n}) \\ &= -(1-\cos^2(\frac{2\pi}{n})) \\ &= \alpha^2 - 1\end{aligned}$$

Daher gilt

$$(\zeta_n - \alpha)^2 - \alpha^2 + 1 = 0,$$

es folgt $[L\colon \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = [\mathbb{Q}(\zeta_n)\colon \mathbb{Q}(\alpha)] \le 2$. Wegen $\alpha \in L\cap\mathbb{R}$ ist aber $\mathbb{Q}(\alpha) \subset L\cap\mathbb{R}$. Also gilt $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}(\alpha)] \ge [L\colon L\cap\mathbb{R}] = 2$ und insgesamt $[L\colon \mathbb{Q}(\alpha)] = 2$. Daher ist auch $[L\cap\mathbb{R}\colon \mathbb{Q}] = [\mathbb{Q}(\alpha)\colon \mathbb{Q}]$ und, weil es sich um endliche Erweiterungen handelt, ist $L\cap\mathbb{R}$ isomorph zu $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-VR. Wegen $\mathbb{Q}(\alpha) \subset L\cap\mathbb{R}$ ist bereits $L\cap\mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Aufgabe 4

(a) Nach der universellen Eigenschaft des Polynomrings existiert genau ein Ringhomomorphismus

$$\begin{aligned}\sigma'_a\colon K[Y] &\to L\\ Y &\mapsto Y+a\\ k &\mapsto k \forall k \in K\end{aligned}$$

Diese Abbildung ist als Isomorphismus auf den Unterring $K[Y] \subset K(Y) = L$ injektiv. Nach der universellen Eigenschaft des Quotientenkörpers existiert dann genau ein injektiver Körperhomomorphismus $\sigma_a\colon Q(K[Y]) = K(Y) \to L$ mit $\sigma_a|_{K[Y]} = \sigma'_a$.

(b) Es gilt $\sigma_0 = \mathrm{id}$. Wegen $\sigma_a \circ \sigma_b(Y) = \sigma_a(Y+b) = Y+b+a = Y+(a+b) = \sigma_{a+b}$ erhalten wir einen Isomorphismus $\Phi\colon (K,+) \to (\mathrm{Aut}_K(L), \circ), a \mapsto \sigma_a$. Angenommen, $L^G \neq 0$. Dann existiert ein $0 \neq f \in K(X)$ mit $f(Y+a) = \sigma_a(f(Y)) = f(Y) \forall a \in K$. Wir betrachten die rationale Funktion $h \in L(X)$ mit $h(X) \coloneqq f(Y+X) - f(Y)$. Diese rationale Funktion besitzt wegen $f(Y+a) = f(Y)$ unendlich Nullstellen in K. Eine rationale Funktion hat aber nur endlich viele Nullstellen, Widerspruch.

(c) Angenommen, es gäbe ein Polynom $f \in K[Y]$ mit $\deg f < p$ und $f(Y+a) = f(Y) \forall a \in \mathbb{F}_p$. Betrachte dann $h \in L[X]$ mit $h(X) \coloneqq f(Y+X) - f(Y)$. Es gilt $\deg h < p$ wegen $\deg f < p$, allerdings besitzt h p Nullstellen, nämlich alle Elemente von $\mathbb{F}_p$, Widerspruch. Das Polynom $f(Y) = Y^p - Y$ erfüllt $f(Y+a) = (Y+a)^p - (Y+a) = Y^p + a^p - a - Y = Y^p - Y = f(Y)$ Angenommen, es gäbe noch ein weiteres normiertes Polynom f' vom Grad p mit dieser Eigenschaft, dann folgte $(f-f')(Y+a) = f(Y+a) - f'(Y+a) = (f-f')(Y)$ mit $\deg(f-f') < p$, Widerspruch. Jedes Polynom vom Grad $\leq p$ mit der Eigenschaft $f(Y+a) = f(Y) \forall a \in \mathbb{F}_p$ ist also ein Polynom in Z. Diese Aussage beweisen wir per Induktion für Polynome vom Grad $\leq np$ für beliebiges $n \in \mathbb{N}$ (also für alle). Wir nehmen also an, jedes $f \in K[Y]$ mit $\deg f \leq kp$ lässt sich darstellen als Polynom in Z $f(Y) = \tilde{f}(Y^p - Y)$. Sei also $g \in K[Y]$ mit $\deg g \leq (k+1)p$ und $g(Y+a) = g(Y)$. Da $K[Y]$ ein euklidischer Ring ist, erhalten wir $g(Y) = f(Y) \cdot (Y^p - Y) + q(Y)$ mit $\deg f \leq kp$ und $\deg q < p$. Nach Induktionsvoraussetzung erhalten wir daraus $g(Y) = \tilde{f}(Y^p - Y) \cdot (Y^p - Y) + q(Y) = \tilde{g}(Y^p - Y) + q(Y)$. Es gilt allerdings $g(Y+a) = \tilde{g}((Y+a)^p - (Y+a)) + q(Y+a) = \tilde{g}(Y^p - Y) + q(Y+a) \overset{!}{=} \tilde{g}(Y^p - Y) + q(Y)$. Daraus erhalten wir die Forderung $q(Y) = q(Y+a)$ mit $\deg q < p$, woraus wir sofort $q(Y) = 0$ folgern können. Es folgt $g(Y) = \tilde{g}(Y^p - Y) = \tilde{g}(Z)$. Nun betrachten wir ein Element $(f(Y), g(Y)) \in K(Y)$. Wir wählen einen Vertreter mit jeweils eindeutiger Zerlegung in irreduzible Polynome $f(Y) = \prod_{i=1}^r f_i(Y)$ und $g(Y) = \prod_{j=1}^r g_j(Y)$ derart, dass $\forall i,j\colon f_i \neq g_j$. Dann gilt $(f(Y+a), g(Y+a)) \sim (f(Y), g(Y))$ genau dann, wenn

$$\begin{aligned}f(Y+a)g(Y) &= f(y)g(Y+a)\\ \prod_{i=1}^r f_i(Y+a) \prod_{j=1}^r g_j(Y) &= \prod_{i=1}^r f_i(Y) \prod_{j=1}^r g_j(Y+a)\end{aligned}$$

Durch $Y \mapsto Y+a$ bleibt die Irreduzibilität der Faktoren erhalten. Die Gleichheit gilt, wenn $\prod_{i=1}^r f_i(Y+a) = \prod_{i=1}^r f_i(Y)$ und $\prod_{j=1}^r g_j(Y+a) = \prod_{j=1}^r g_j(Y)$. Ist dies allerdings nicht erfüllt, so müssen i,j existieren mit $f_i(Y+a) = g_j(Y+a)$. Daraus folgt aber sofort $f_i(Y) = g_j(Y)$, was wir ausgeschlossen hatten. Daher erhalten wir $f(Y+a) = f(Y)$ und $g(Y+a) = g(Y)$, somit ist

aber $(f(Y), g(Y)) \sim (\tilde{f}(Z), \tilde{g}(Z))$ für geeignetes $\tilde{f}, \tilde{g}$. Es gilt also für jedes Element $x \in K(Y)$ mit $\sigma_a(x) = x \forall a \in \mathbb{F}_p$ die Eigenschaft $x \in K(Z)$, was zu zeigen war.