Musterlösung Serie 28

Auflösung durch Radikale, Bestimmung der Galoisgruppe

1. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, dessen Grad eine Primzahl p ist und das genau zwei nicht reelle Nullstellen hat. Beweise, dass die Galoisgruppe von f gleich S_p ist.

   Lösung: Da f irreduzibel und $\mathrm{char}(\mathbb{Q}) = 0$ ist, ist das Polynom separabel. Seien $a_1, \dots, a_p$ seine Nullstellen in $\mathbb{C}$ und $L := \mathbb{Q}(a_1, \dots, a_p)$ sein Zerfällungskörper über $\mathbb{Q}$ und $G := \mathrm{Gal}(L/\mathbb{Q}) < S_p$ seine Galoisgruppe über $\mathbb{Q}$. Wir zeigen:

   (a) G enthält einen p-Zykel.

   (b) G enthält eine Transposition.

   Für (a) beachten wir zunächst, dass G transitiv auf den Nullstellen operiert, weil f irreduzibel ist. Ihre Anzahl p ist also ein Teiler der Gruppenordnung $|G|$. Da p prim ist, enthält G also ein Element der Ordnung p. Schreiben wir dieses als Produkt von disjunkten Zykeln, so ist die Länge jedes dieser Zykel ein Teiler von p, und nicht alle Zykel haben die Länge 1. Also hat einer dieser Zykel die Länge p. Da aber überhaupt nur p Ziffern vertauscht werden, gibt es in dieser Zerlegung gar keine weiteren Zykel, und das Element ist bereits ein p-Zykel. Damit ist (a) gezeigt.

   Für (b) seien ohne Beschränkung der Allgemeinheit a_1 und a_2 die beiden nicht-reellen Nullstellen von f. Da f reelle Koeffizienten hat, ist dann auch das komplex Konjugierte $\overline{a_1}$ eine Nullstelle von f. Da sie nach Voraussetzung $\neq a_1$ ist, bleibt nur die Möglichkeit $\overline{a_1} = a_2$. Daraus folgt $\overline{a_2} = a_1$; und natürlich gilt $\overline{a_i} = a_i$ für alle $3 \leqslant i \leqslant p$. Nun ist die komplexe Konjugation ein Körperautomorphismus von $\mathbb{C}$ und induziert also einen Körperautomorphismus von L, und somit ein Element von G. Die zugehörige Permutation ist die Transposition (1 2), womit (b) bewiesen ist.

   Schliesslich besagt Aufgabe 5 von Serie 4, dass jede Untergruppe von S_p mit den Eigenschaften (a) und (b) gleich S_p ist. Also ist $G = S_p$, wie gewünscht.

2. Sei $p > 11$ eine Primzahl. Zeige, dass die Gleichung $X^5 - pX + p = 0$ über $\mathbb{Q}$ nicht durch Radikale auflösbar ist.

   Lösung: Sei $f(X) = X^5 - pX + p \in \mathbb{Q}[X]$. Wir untersuchen den Graphen von f, aufgefasst als Funktion $\mathbb{R} \to \mathbb{R}$, mithilfe von Methoden aus der Analysis I. Die erste Ableitung $f'(X) = 5X^4 - p$ hat genau zwei reelle Nullstellen, nämlich $\pm\sqrt[4]{\frac{p}{5}}$. Diese Nullstellen sind einfach und sind daher die einzigen lokalen Extremalstellen von f. Ausserdem gilt $f\left(\sqrt[4]{\frac{p}{5}}\right) < 0$ und $f\left(-\sqrt[4]{\frac{p}{5}}\right) > 0$; darum hat f bei $\sqrt[4]{\frac{p}{5}}$ ein lokales Minimun und bei $-\sqrt[4]{\frac{p}{5}}$ ein lokales Maximum. Andererseits gilt $\lim_{x\to\infty} f(x) = \infty$

und $\lim_{x\to-\infty} f(x) = -\infty$, da der höchste Koeffizient von f positiv ist. Zusammen folgt daraus, dass f genau eine reelle Nullstelle in jedem der Intervalle $]-\infty, -\sqrt[4]{\frac{p}{5}}[$ und $]-\sqrt[4]{\frac{p}{5}}, \sqrt[4]{\frac{p}{5}}[$ und $]\sqrt[4]{\frac{p}{5}}, \infty[$ besitzt. Ausserdem hat es keine Nullstelle mit f' gemeinsam; darum besitzt f genau 3 reelle und 2 komplex konjugierte Nullstellen.

Andererseits ist f irreduzibel nach dem Eisensteinkriterium mit der Primzahl $p = 5$. Also folgt aus Aufgabe 1, dass die Galoisgruppe von f gleich S_5 ist. Da diese Gruppe nicht auflösbar ist, folgt mit dem Satz von Abel-Ruffini, dass f nicht durch Radikale auflösbar ist.

3. Sei $K := \mathbb{Q}(\zeta)$ für eine Einheitswurzel $\zeta \in \mathbb{C}$ der Ordnung 7.

   (a) Beschreibe alle Zwischenkörper von $K/\mathbb{Q}$.

   (b) Gib Erzeugende in Termen von Radikalen an.

   Lösung:

   (a) Die Gruppe μ_7 der siebten Einheitswurzeln ist von ζ erzeugt. Nach Satz 7.6.4 der Vorlesung ist also $K = \mathbb{Q}(\mu_7)$ galoissch vom Grad 6 über $\mathbb{Q}$ mit der Galoisgruppe $(\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{F}_7^\times$. Als multiplikative Gruppe eines endlichen Körpers ist diese zyklisch. Da sie Ordnung 6 hat, besitzt sie genau je eine Untergruppe der Ordnung $1, 2, 3, 6$. Nach der Galoiskorrespondenz entsprechen diese eindeutigen Unterkörpern vom Grad $6, 3, 2, 1$ über $\mathbb{Q}$.

   Diese beinhalten natürlich $K = \mathbb{Q}(\zeta)$ vom Grad 6 und $\mathbb{Q}$ vom Grad 1 über $\mathbb{Q}$. Mit $a := \zeta + \zeta^{-1}$ ist nach Aufgabe 2 von Serie 27 sodann $\mathbb{Q}(a)$ ein Zwischenkörper mit $[\mathbb{Q}(\zeta)/\mathbb{Q}(a)] = 2$ und folglich $[\mathbb{Q}(a)/\mathbb{Q}] = 3$. Um den Unterkörper vom Grad 2 über $\mathbb{Q}$ zu konstruieren, suchen wir ein Element, das automatisch unter der Untergruppe vom Index 2 von $\mathbb{F}_7^\times$ invariant ist. Diese Untergruppe ist gleich $\{\overline{1}, \overline{2}, \overline{4}\}$, also ist $b := \zeta + \zeta^2 + \zeta^4$ ein solches Element. Für dieses rechnen wir

   $$b^2 \;=\; \zeta^2 + \zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6$$

   und wegen $\zeta^8 = \zeta$ erhalten wir

   $$b^2 + b + 2 \;=\; 2\zeta^2 + 2\zeta^4 + 2\zeta + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 + 2 \;=\; 0,$$

   da ζ eine Nullstelle des Kreisteilungspolynoms $\frac{X^7-1}{X-1} = X^6 + X^5 + \ldots + X + 1$ ist. Nach der Mitternachtsformel ist daher $b = (-1 \pm \sqrt{-7})/2$. Somit ist $\mathbb{Q}(b) = \mathbb{Q}(\sqrt{-7})$ der gesuchte Zwischenkörper vom Grad 2 über $\mathbb{Q}$.

   (b) Die Zwischenkörper $\mathbb{Q}(\zeta)$ und $\mathbb{Q}$ und $\mathbb{Q}(\sqrt{-7})$ sind bereits durch Radikale beschrieben. Es bleibt, dies noch für den Zwischenkörper $\mathbb{Q}(a)$ zu tun. Mit etwas Probieren finden wir

   $$\begin{aligned} a^3 + a^2 - 2a - 1 &= (\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}) + (\zeta^2 + 2 + \zeta^{-2}) - 2(\zeta + \zeta^{-1}) - 1 \\ &= \zeta^3 + \zeta + \zeta^{-1} + \zeta^{-3} + \zeta^2 + 1 + \zeta^{-2} \\ &= 0. \end{aligned}$$

Jetzt können wir die Lösungsformeln für Gleichungen dritten Grades verwenden. Zuerst bringen wir den quadratischen Term zum Verschwinden durch kubische Ergänzung. Die Substution $a = (c-1)/3$ führt zu $\mathbb{Q}(a) = \mathbb{Q}(c)$ mit $c^3 - 21c - 7 = 0$. Nach Spezialfall 7.8.6 der Vorlesung erhalten wir daher

$$c \;=\; \sqrt[3]{\tfrac{7}{2} - \sqrt{-7^3 + \left(\tfrac{7}{2}\right)^2}} \;+\; \sqrt[3]{\tfrac{7}{2} + \sqrt{-7^3 + \left(\tfrac{7}{2}\right)^2}}.$$

4. Seien $\varepsilon, \delta \in \{\pm 1\}$. Zeige, dass jedes Polynom $f \in \mathbb{Q}[X] \smallsetminus \{0\}$ vom Grad $n \leqslant 9$ mit der Eigenschaft $f(X) = \varepsilon X^n f(\delta X^{-1})$ auflösbar durch Radikale ist.

   Lösung: Die Voraussetzung impliziert, dass der konstante Koeffizient von f gleich $\pm$ dem höchsten Koeffizienten ist; insbesondere ist er ungleich Null. Also ist jede Nullstelle $\alpha \in \mathbb{C}$ von f ungleich Null. Weiter ist die Abbildung $\varphi\colon \alpha \mapsto \delta\alpha^{-1}$ eine Permutation der Menge der Nullstellen mit $\varphi^2 = \mathrm{id}$, welche zudem die Multiplizität der Nullstellen erhält.

   Zuerst betrachten wir den Fall, dass φ eine Nullstelle $\alpha \in \overline{\mathbb{Q}}$ auf sich abbildet. Diese erfüllt dann die Gleichung $\alpha^2 = \delta$. Im Fall $\delta = 1$ ist also $\alpha \in \{\pm 1\}$ und somit $f(X) = (X - \alpha) \cdot g(X)$ für ein Polynom $g \in \mathbb{Q}[X]$ vom Grad $n - 1$. Dieses erfüllt

$$g(X) = \frac{f(X)}{X - \alpha} = \frac{\varepsilon X^n f(X^{-1})}{-\alpha X(X^{-1} - \alpha)} = -\frac{\varepsilon}{\alpha} \cdot X^{n-1} g(X^{-1}),$$

   also die entsprechende Eigenschaft. Da f und g denselben Zerfällungskörper haben, genügt es, die Aussage für g anstatt f zu beweisen. Im Fall $\delta = -1$ ist $\{\alpha, \overline{\alpha}\} = \{\pm i\}$, und beides sind Nullstellen von f. Somit ist $f(X) = (X^2 + 1) \cdot g(X)$ für ein Polynom $g \in \mathbb{Q}[X]$ vom Grad $n - 2$. Dieses erfüllt

$$g(X) = \frac{f(X)}{X^2 + 1} = \frac{\varepsilon X^n f(-X^{-1})}{X^2(X^{-2} + 1)} = \varepsilon X^{n-2} g(-X^{-1}),$$

   also wieder die entsprechende Eigenschaft. Ist $K \subset \mathbb{C}$ der Zerfällungskörper von g, so ist $K(i) \subset \mathbb{C}$ der Zerfällungskörper von f. Somit ist letzterer auflösbar über $\mathbb{Q}$, wenn ersterer es ist, und es genügt wieder, die Aussage für g anstatt f zu beweisen.

   Durch Induktion über den Grad können wir uns damit auf den Fall reduzieren, dass die Abbildung $\varphi\colon \alpha \mapsto \delta\alpha^{-1}$ keine Nullstelle festlässt. Dann ist n gerade, und die komplexen Nullstellen sind Paare $\alpha_k \neq \delta\alpha_k^{-1}$ für $1 \leqslant k \leqslant m := n/2$. Die Rechnung

$$\frac{f(X)}{X^m} \;=\; \prod_{k=1}^{m} \frac{(X - \alpha_k)(X - \delta\alpha_k^{-1})}{X} \;=\; \prod_{k=1}^{m} \Big(X + \delta X^{-1} - \alpha_k - \delta\alpha_k^{-1}\Big)$$

   zeigt nun, dass $f(X) = X^m \cdot h(X + \delta X^{-1})$ ist für ein Polynom h vom Grad m. Da f Koeffizienten in $\mathbb{Q}$ hat, gilt dies auch für h. Wegen $n \leqslant 9$ ist jetzt aber $m \leqslant 4$

und folglich h auflösbar durch Radikale. Die Nullstellen von f ergeben sich dann aus den Nullstellen β_k von h durch Lösen der Gleichung $X + \delta X^{-1} = \beta_k$, welche zu der quadratischen Gleichung $X^2 - \beta_k X + \delta = 0$ äquivalent ist. Sie sind somit durch Radikale über dem Zerfällungskörper von h ausdrückbar, und deshalb ist auch f durch Radikale auflösbar.

5. Sei $f(X) \in \mathbb{R}[X]$ ein separables normiertes Polynom vom Grad 3 mit der Diskriminante Δ. Zeige:

   (a) Es gilt $\Delta > 0$, falls alle Nullstellen von f reell sind, andernfalls $\Delta < 0$.

   (b) Falls f genau eine reelle Nullstelle hat, so enthält die Lösungsformel dafür nur reelle Quadrat- und dritte Wurzeln.

   (c) Im Gegensatz dazu erfordert die Lösungsformel ausgerechnet dann eine dritte Wurzel aus einer nicht-reellen komplexen Zahl, wenn f drei reelle Nullstellen hat (*"Casus irreducibilis"*).

   *(d) Versuche zu erklären, wieso der Umstand aus (c) unvermeidbar ist, also weshalb die Nullstellen von f, selbst wenn sie reell sind, im Allgemeinen nicht mit reellen Radikalen ausgedrückt werden können.

   Lösung: (a) Seien x_1, x_2, x_3 die Nullstellen von f. Falls x_1, x_2, x_3 reell sind, so ist

$$\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 > 0.$$

   Hat f andererseits nicht-reelle Nullstellen, so ist genau eine Nullstelle reell, und die anderen beiden sind zueinander komplex konjugiert. Sei ohne Beschränkung der Allgemeinheit x_1 die reelle Nullstelle. Dann ist $x_3 = \bar{x}_2$ und folglich

$$\begin{aligned} \Delta &= (x_1 - x_2)^2 (x_1 - \overline{x_2})^2 (x_2 - \overline{x_2})^2 \\ &= \underbrace{\big((x_1 - x_2)\overline{(x_1 - x_2)}\big)^2}_{|x_1 - x_2|^4} \cdot \underbrace{(x_2 - \overline{x_2})^2}_{-4\,\mathrm{Im}(x_2)^2} < 0. \end{aligned}$$

   (b) und (c): Verwende die Notationen aus der Vorlesung. Laut Vorlesung ist die Lösungsformel für kubische Gleichungen gegeben durch

$$y_i = \zeta^i \cdot \sqrt[3]{q - \sqrt{-\frac{\Delta}{4 \cdot 27}}} + \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{-\frac{\Delta}{4 \cdot 27}}}.$$

   Wir sehen, dass unter der dritten Wurzel genau dann eine reelle Zahl steht, wenn $\Delta < 0$ gilt. Dies ist mit (a) genau dann der Fall, wenn f genau eine reelle Nullstelle hat.

   (d) Nehmen wir an, dass eine allgemeine Lösungsformel für den Fall (c) existiert, welche nur reelle Wurzeln enthält. Dann gilt diese Formel insbesondere dann, wenn

f irreduzibel über einem gegebenen Unterkörper $K \subset \mathbb{R}$ ist, was wir also nun annehmen. Die Formel bedeutet, dass ein Radikalturm

$$K \subset K_0 := K(\sqrt{\Delta}) \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$$

existiert mit $x_1, x_2, x_3 \in K_n$. Dabei können wir ohne Beschränkung der Allgemeinheit annehmen, dass jedes $K_i = K_{i-1}(\sqrt[p_i]{\alpha_i})$ ist für eine Primzahl p_i und ein $\alpha_i \in K_{i-1}$. Sei m minimal, sodass eine der Nullstellen x_ν in K_m liegt. Da f irreduzibel über K ist, gilt $x_\nu \notin K_0$ und somit $m \geqslant 1$. Da dann keine der drei Nullstellen von f in K_{m-1} liegt, ist f wegen $\deg f = 3$ irreduzibel über K_{m-1}. Wegen $[K_m/K_{m-1}]$ prim und $K_{m-1}(x_\nu) \subset K_m$ folgt dann $K_{m-1}(x_\nu) = K_m$, das heisst, K_m ist ein Stammkörper von f über K_{m-1}. Aber wir wissen bereits, dass $K_0(x_\nu) = K(\sqrt{\Delta}, x_\nu)$ alle drei Nullstellen von f enthält. Daher gilt das Gleiche für K_m, und somit ist K_m ein Zerfällungskörper von f über K_{m-1}. Er ist also galoissch vom Grad 3 über K_{m-1}. Nach Konstruktion gilt nun aber $K_m = K_{m-1}(\sqrt[3]{\alpha_m})$ mit $\alpha_m \in K_{m-1}$, wobei $X^3 - \alpha_m \in K_{m-1}[X]$ irreduzibel ist und somit insbesondere $\alpha_m \neq 0$. Da K_m normal über K_{m-1} ist, muss er also auch die anderen beiden Nullstellen von $X^3 - \alpha_m$ enthalten, das heisst, die beiden nicht reellen dritten Wurzeln aus α_m, im Widerspruch zu $K_m \subset \mathbb{R}$.

6. Betrachte ein Polynom der Form $f(X) = X^4 + aX^3 + bX^2 + cX + d$ über einem Körper K der Charakteristik 0. Ziel dieser Aufgabe ist es, explizite Lösungsformeln für die Nullstellen von f in Termen der vier Grundrechenarten sowie von zweiten und dritten Wurzeln zu finden. Schreibe dafür

$$f(X) = (X - a_1)(X - a_2)(X - a_3)(X - a_4)$$

über einem Zerfällungskörper $L = K(a_1, a_2, a_3, a_4)$ von f und setze

$$\left\{ \begin{array}{lcl} b_1 & := & a_1a_2 + a_3a_4 \\ b_2 & := & a_1a_3 + a_2a_4 \\ b_3 & := & a_1a_4 + a_2a_3 \end{array} \right\} \qquad \text{sowie} \qquad \left\{ \begin{array}{lcl} c_1 & := & a_1 + a_2 - a_3 - a_4 \\ c_2 & := & a_1 - a_2 + a_3 - a_4 \\ c_3 & := & a_1 - a_2 - a_3 + a_4 \end{array} \right\}.$$

   (a) Zeige, dass nach einer Substitution der Form $X = Y + \alpha$ für ein geeignetes $\alpha \in K$ der Koeffizient von Y^3 verschwindet. Im folgenden nehmen wir daher $a = 0$ an, damit die Formeln einfacher werden.

   (b) Berechne das Polynom $g(Y) := (Y - b_1)(Y - b_2)(Y - b_3)$ durch eine explizite Formel in $\mathbb{Q}[b, c, d][Y]$.

   (c) Gib Lösungsformeln für b_1, b_2, b_3 an aus der Theorie der kubischen Gleichung.

   (d) Berechne c_1^2, c_2^2, c_3^2 durch explizite Formeln in $\mathbb{Q}[b, c, d, b_1, b_2, b_3]$.

   (e) Berechne a_1, a_2, a_3, a_4 durch explizite Formeln in $\mathbb{Q}[b, c, d, b_1, b_2, b_3, c_1, c_2, c_3]$.

   Nehmen wir jetzt zusätzlich an, dass f die Galoisgruppe S_4 hat. Zeige dann:

(f) Das Polynom $g(Y) \in K[Y]$ hat die Galoisgruppe S_3.

(g) Der zu der Kleinschen Vierergruppe $H < S_4$ gehörende Zwischenkörper ist $K(b_1, b_2, b_3)$.

Lösung:

(a) Die Substitution $X = Y - \frac{a}{4}$ liefert

$$\begin{aligned} f(Y - \tfrac{a}{4}) &= (Y - \tfrac{a}{4})^4 + a(Y - \tfrac{a}{4})^3 + b(Y - \tfrac{a}{4})^2 + c(Y - \tfrac{a}{4}) + d \\ &= Y^4 + (b - \tfrac{3}{8}a^2)Y^2 + (c - \tfrac{1}{2}ab + \tfrac{1}{8}a^3)Y + (d - \tfrac{1}{4}ac + \tfrac{1}{16}a^2b - \tfrac{3}{256}a^4) \end{aligned}$$

(b) Seien S_1, S_2, S_3, S_4 die elementarsymmetrischen Polynome in a_1, a_2, a_3, a_4. Aus Abschnitt 7.3 der Vorlesung folgen die Gleichungen

$$S_1 = -a = 0, \quad S_2 = b, \quad S_3 = -c, \quad S_4 = d.$$

Seien nun T_1, T_2, T_3 die elementarsymmetrischen Polynome in b_1, b_2, b_3. Aus der Definition von b_1, b_2, b_3 berechnen wir

$$T_1 = S_2 = b, \quad T_2 = S_1 \cdot S_3 - 4S_4 = -4d$$

Das Polynom T_3 ist etwas schwieriger. Wir rechnen

$$T_3 = \frac{1}{6} \sum_{i \neq j \neq k \neq i} a_i^2 a_j^2 a_k^2 + a_1 a_2 a_3 a_4 \sum_i a_i^2 = S_3^2 + (S_1^2 - 4S_2)S_4 = c^2 - 4bd$$

wobei wir Aufgabe 7 von Serie 25 und Beispiel 7.3.10 der Vorlesung verwendet haben. Es folgt

$$g(Y) = Y^3 - T_1 Y^2 + T_2 Y - T_3 = Y^3 - bY^2 - 4dY + 4bd - c^2.$$

(c) Aus Spezialfall 7.8.6 der Vorlesung wissen wir, dass wir durch $Y = Z + \frac{b}{3}$ das Polynom $g(Y)$ in die Form $Z^3 + 3pZ - 2q$ transformieren können für gewisse $p, q \in K$. Explizit rechnen wir

$$p = -\frac{b^2 + 12d}{9}, \quad q = \frac{b^3}{27} - \frac{4bd}{3} + \frac{c^2}{2}$$

Dann hat $g(Z)$ die Nullstellen

$$z_i \ := \ \zeta^i \cdot \sqrt[3]{q - \sqrt{p^3 + q^2}} \ + \ \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{p^3 + q^2}} \ \in \ \overline{K}$$

für $i = 1, 2, 3$ mit $\zeta := \frac{-1+\sqrt{-3}}{2}$ und einer geeigneten Wahl der Wurzeln in $\overline{K}$. Es gilt dann $b_i = z_i + \frac{b}{3}$ für $i = 1, 2, 3$.

(d) Unter Ausnutzung der Formel $a_1^2+a_2^2+a_3^2+a_4^2 = S_1^2-2S_2$ aus Beispiel 7.3.10 und den Identitäten aus (b) zeigt eine direkte Rechnung:

$$\begin{aligned} c_1^2 &= S_1^2 - 2S_2 + 2b_1 - 2b_2 - 2b_3 = -2b + 2b_1 - 2b_2 - 2b_3, \\ c_2^2 &= S_1^2 - 2S_2 - 2b_1 + 2b_2 - 2b_3 = -2b - 2b_1 + 2b_2 - 2b_3, \\ c_3^2 &= S_1^2 - 2S_2 - 2b_1 - 2b_2 + 2b_3 = -2b - 2b_1 - 2b_2 + 2b_3. \end{aligned}$$

(e) Wir lösen das lineare Gleichungssystem

$$\begin{aligned} c_1 &= a_1 + a_2 - a_3 - a_4 \\ c_2 &= a_1 - a_2 + a_3 - a_4 \\ c_3 &= a_1 - a_2 - a_3 + a_4 \\ S_1 = 0 &= a_1 + a_2 + a_3 + a_4 \end{aligned}$$

und finden

$$\begin{aligned} a_1 &= \tfrac{1}{4}(c_1 + c_2 + c_3) \\ a_2 &= \tfrac{1}{4}(c_1 - c_2 - c_3) \\ a_3 &= \tfrac{1}{4}(-c_1 + c_2 - c_3) \\ a_4 &= \tfrac{1}{4}(-c_1 - c_2 + c_3) \end{aligned}$$

(f) Der Isomorphismus $\mathrm{Gal}(L/K) \cong S_4$ ist charakterisiert durch die Formel $\gamma(a_i) = a_{\gamma i}$ für jedes $1 \leqslant i \leqslant 4$. Die Anwendung eines solchen γ auf b_1, b_2, b_3 ergibt einen Homomorphismus $\varphi\colon S_4 \to S_3$, dessen Bild die Galoisgruppe von $g(Y)$ ist. Wir wenden die Permutationen $\gamma_1 := (1\ 4)$, $\gamma_2 := (1\ 2)$ und $\gamma_3 := (1\ 3)$ von a_1, a_2, a_3, a_4 auf b_1, b_2, b_3 an und erhalten

$$\begin{aligned} &\gamma_1(b_1) = b_2, \quad \gamma_1(b_2) = b_1, \quad \gamma_1(b_3) = b_3, \\ &\gamma_2(b_1) = b_1, \quad \gamma_2(b_2) = b_3, \quad \gamma_2(b_3) = b_2, \\ &\gamma_3(b_1) = b_3, \quad \gamma_2(b_2) = b_2, \quad \gamma_3(b_3) = b_1. \end{aligned}$$

Daher enthält das Bild von φ die Transpositionen $(1\ 2)$, $(2\ 3)$ und $(1\ 3)$ und ist daher gleich ganz S_3. Wir folgern, dass somit das Polynom $g(Y)$ als Galoisgruppe S_3 besitzt.

(g) Der Kern des Homomorphismus φ aus (f) ist die Kleinsche Vierergruppe $H = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \lhd S_4$, also gilt $S_4/H \cong \mathrm{Gal}(K(b_1, b_2, b_3)/K)$. Aus der Galoiskorrespondenz folgt, dass der zu H gehörende Zwischenkörper gleich $K(b_1, b_2, b_3)$ ist. (Vergleiche dazu Aufgabe 1 von Serie 27.)

7. Bestimme die Galoisgruppen der folgenden Polynome über $\mathbb{Q}$:

(a) $f(X) = X^5 + X^3 - 2X + 5$

(b) $g(X) = X^4 - 2X^3 + 2X + 3$

(c) $h(X) = X^4 + 3X^3 + 3X + 1$

Lösung: Nach Satz 7.9.4 der Vorlesung sagt uns die Faktorisierung eines Polynoms modulo einer Primzahl p, wenn sie separabel ist, dass die Galoisgruppe eine Permutation enthält, deren Zykellängen genau die Grade der irreduziblen Faktoren modulo p sind.

(a) Wir zerlegen $f(X) = X^5 + X^3 - 2X + 5$ in irreduzible Faktoren modulo kleinen Primzahlen:

$$\begin{aligned} f &\equiv X^5 + X^3 + 1 \bmod (2) && \rightsquigarrow \text{5-Zykel} \\ f &\equiv X^5 + X^3 - 2X + 2 \bmod (3) && \rightsquigarrow \text{5-Zykel} \\ f &\equiv X(X+1)(X+4)(X^2+2) \bmod (5) && \rightsquigarrow \text{2-Zykel} \end{aligned}$$

Somit enthält die Galoisgruppe von f einen 2-Zykel und einen 5-Zykel und ist daher gleich S_5 nach Aufgabe 5 von Serie 4.

(b) Wir zerlegen $g(X) = X^4 - 2X^3 + 2X + 3$ in irreduzible Faktoren modulo kleinen Primzahlen:

$$\begin{aligned} g &\equiv (X+1)^4 \bmod (2) && \text{Keine Aussage, da inseparabel} \\ g &\equiv X(X^3 + X^2 + 2) \bmod (3) && \rightsquigarrow \text{3-Zykel} \\ g &\equiv X^4 + 3X^3 + 2X + 3 \bmod (5) && \rightsquigarrow \text{4-Zykel} \end{aligned}$$

Damit enthält die Galoisgruppe von g bereits 12 Elemente und eine ungerade Permutation, ist also gleich S_4.

(c) Wir zerlegen $h(X) = X^4 + 3X^3 + 3X + 1$ in irreduzible Faktoren modulo kleinen Primzahlen:

$$\begin{aligned} h &\equiv (X+1)^2(X^2+X+1) \bmod (2) && \text{Keine Aussage, da inseparabel} \\ h &\equiv (X^2+X+2)(X^2+2X+2) \bmod (3) && \rightsquigarrow \text{Produkt zweier 2-Zykel} \\ h &\equiv X^4 + 3X^3 + 3X + 1 \bmod (5) && \rightsquigarrow \text{4-Zykel} \\ h &\equiv X^4 + 3X^3 + 3X + 1 \bmod (7) && \rightsquigarrow \text{4-Zykel} \\ h &\equiv (X^2+4X+7)(X^2+10X+8) \bmod (11) && \rightsquigarrow \text{Produkt zweier 2-Zykel} \\ h &\equiv (X+2)(X+7)(X^2+7X+1) \bmod (13) && \rightsquigarrow \text{2-Zykel} \end{aligned}$$

Auch die nächsten Primzahlen liefern keine weiteren Informationen.

Wir können aber bereits folgern, dass die Galoisgruppe $G < S_4$ eine D_4 enthält. Denn jeder 4-Zykel in G liegt in einer 2-Sylowgruppe $P < G$. Da G auch eine Transposition enthält, und diese in einer 2-Sylowgruppe von G liegt,

enthält auch P schon einen 2-Zykel. Da aber das Quadrat eines 4-Zykels ein Produkt zweier disjunkter 2-Zykel ist, kann P nicht schon von dem 4-Zykel erzeugt sein. Also hat P mindestens die Ordnung 8. Wegen $|S_4| = 8 \cdot 3$ ist P somit schon eine 2-Sylowgruppe von S_4 und daher isomorph zur D_4.

Nun sehen wir weiter, dass das Polynom h palindromisch vom Grad 4 ist wie in der obigen Aufgabe 4. Genauer ist für jede Nullstelle $\alpha \in \mathbb{C}$ auch α^{-1} eine Nullstelle. Damit enthält die Erweiterung $\mathbb{Q}(\alpha)$ vom Grad $\leqslant 4$ schon die zwei Nullstellen $\alpha^{\pm 1}$. Adjungieren der letzten beiden Nullstellen erfordert dann höchstens eine weitere Erweiterung vom Grad 2. Dies zeigt, dass der Grad eines Zerfällungskörpers $\leqslant 8$ ist. Also ist auch $|G| \leqslant 8$, und es bleibt nur noch die Möglichkeit $G = D_4$.