Aufgabe 1

(a) Sei $\sigma \in G_\alpha$. Dann gilt $\sigma(\alpha) = \alpha$ nach Definition der Isotropiegruppe. Insbesondere ist daher $\sigma \in \mathrm{Aut}_{K(\alpha)}(L) = \mathrm{Gal}(L/K(\alpha))$. Sei andererseits $\sigma \in \mathrm{Aut}_{K(\alpha)}(L) = \mathrm{Gal}(L/K(\alpha))$. Dann muss nach Definition von $\mathrm{Aut}_{K(\alpha)}(L)$ und wegen $\alpha \in K(\alpha)$ bereits $\sigma(\alpha) = \alpha$ gelten. Daraus folgt $\sigma \in G_\alpha$. Insgesamt erhalten wir

$$G_\alpha = \mathrm{Gal}(L/K(\alpha)) \subset G.$$

(b) Wendet man ein beliebiges $\sigma \in G$ auf die Koeffizienten von f an, so erhält man

$$f^\sigma = \sigma\left(\prod_{\alpha' \in A}(X - \alpha')\right) = \prod_{\alpha' \in A}(X - \sigma(\alpha')) = f,$$

insbesondere liegen alle Koeffizienten in $L^G = K$ und damit $f \in K[X]$. Außerdem sind alle Nullstellen α' als Elemente von A notwendigerweise verschieden.

(c) Angenommen, f wäre reduzibel.

Dann gäbe es einen Teiler $f'|f$ in $K[X]$ mit $f'(\alpha) = 0$ Dann gäbe es eine echte Teilmenge von $A' \subset A$ mit $\alpha \in A'$ derart, dass

$$f' = \prod_{\alpha' \in A'}(X - \alpha') \in K[X] = L^G[X]$$

Sei nun $\beta \in A \setminus A' \neq \emptyset$ und $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Dann gilt

$$(f')^\sigma = \prod_{\alpha' \in A}(X - \sigma(\alpha')) \neq f',$$

da $(f')^\sigma(\beta) = 0$. Wäre $f' \in K[X]$, so müsste wegen $\sigma|_K = \mathrm{id}$ aber $f' = (f')^\sigma$ gelten, Widerspruch.

Also ist f irreduzibel. Außerdem gilt $f \in K[X]$ und $f(\alpha) = 0$. Damit ist f das Minimalpolynom von α über K.

Aufgabe 2

(a) Wir folgern aus Aufgabe 3 auf Zettel 9, dass $[\mathbb{Q}(\zeta_5) \colon \mathbb{Q}(\zeta_5 + \zeta_5^{-1})] = 2$ gilt. Somit ist $\mathbb{Q}(\alpha)$ ein echter Zwischenkörper von $\mathbb{Q}(\zeta_5)$. Nach Satz 4.48 existiert ein Gruppenisomorphismus $\chi \colon G \xrightarrow{\sim} (\mathbb{Z}/5\mathbb{Z})^\times$. Wegen $\langle 2 \rangle = \{2, 4, 3, 1\} = (\mathbb{Z}/5\mathbb{Z})^\times$ und $\langle 4 \rangle = \{3, 4, 2, 1\} = (\mathbb{Z}/5\mathbb{Z})^\times$ folgt, dass $U \coloneqq \{1, 4\}$ die einzige echte Untergruppe von $(\mathbb{Z}/5\mathbb{Z})^\times$ sein kann. Insbesondere kann es nur einen echten Zwischenkörper geben. Dieser ist demnach durch $\mathbb{Q}(\alpha)$ gegeben. Nachrechnen zeigt

$$(\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 = \zeta_5^2 + 2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} - 1 = \zeta_5^0 + \zeta_5^1 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$$

nach Bemerkung 4.45 und Definition 4.43, da 5 eine Primzahl ist. Die Nullstellen von $\alpha^2 + \alpha - 1$ sind gegeben durch $-\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{-1 \pm \sqrt{5}}{2}$. Wegen $\mathrm{Re}\,\zeta_5 > 0$ folgt $\zeta_5 + \zeta_5^{-1} = \zeta_5 + \overline{\zeta_5} = 2\,\mathrm{Re}(\zeta_5) > 0$. Nun ist $\frac{\sqrt{5}-1}{2} > 0$ und $\frac{-1-\sqrt{5}}{2} < 0$, sodass α durch die beiden Bedingungen eindeutig als

$$\alpha = \frac{\sqrt{5} - 1}{2}$$

bestimmt ist.

(b) Alle ζ_5^n liegen auf dem Einheitskreis. Außerdem schließt ζ_5^n mit der reellen Achse per Definition der Polarkoordinatendarstellung den orientierten Winkel $2\pi n/5$ ein. Insbesondere ist der Winkel zwischen zwei benachbarten Einheitswurzeln stets $2\pi/5 \cong 72°$. Daher bilden die Einheitswurzeln ein regelmäßiges Fünfeck. Die Seitenlänge des Fünfecks ist nach Pythagoras gegeben durch

$$|\zeta_5 - 1| = \sqrt{(1-\cos(2\pi/5))^2 + \sin^2(2\pi/5)} = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

Aufgabe 3

(a) Mit (12345) ist auch das Inverse (54321) in H enthalten. Es gilt nach Aufgabe 4(a) auf Blatt 11 $(12)(12345)(12) = (21345)$ und damit $(12)(21345)(54321) = (12)(123) = (23)$. Weiter erhalten wir $(23)(12345)(23) = (13245)$ und $(23)(13245)(54321) = (23)(234) = (34)$. Außerdem ist $(34)(12345)(34) = (12435)$ und folglich $(34)(12435)(54321) = (34)(345) = (45)$. Wir erhalten zunächst $(23)(12)(23) = (13), (34)(13)(34) = (14)$ und $(45)(14)(45) = (15)$. Damit ist $(ij) = (1i)(1j)(1i)$ für $i, j \in \{1, 2, 3, 4, 5\}$. Jede Permutation lässt sich als Produkt von Transpositionen schreiben, daher gilt $H = \mathfrak{S}_5$.

(b) Die komplexe Konjugation wirkt trivial auf $\mathbb{R}$, insbesondere also auf den reellen Nullstellen von f. Da f genau 5 komplexe Nullstellen besitzt, gibt es genau 2 Nullstellen von f mit $\operatorname{Im} f \neq 0$. Sei σ die komplexe Konjugation. Dann ist wegen $f \in \mathbb{Q}[X]$ $f^\sigma = f$. Schreibt man f als Produkt seiner Linearfaktoren, so sind die drei Linearfaktoren mit reellem Koeffizienten invariant unter komplexer Konjugation. Das gesamte Polynom ist ebenfalls invariant unter komplexer Konjugation. Daher muss

$$(X - \overline{\beta_1})(X - \overline{\beta}_2) = (X - \beta_1)(X - \beta_2)$$

gelten. Daher ist $\beta_1 = \overline{\beta}_2$. Daher liegt die komplexe Konjugation in der Galoisgruppe G des Zerfällungskörpers L von f über $\mathbb{Q}$. G ist isomorph zu einer Untergruppe G' von $\mathfrak{S}_5$. Unter diesem Isomorphismus wird σ_c auf eine Transposition abgebildet, da genau zwei Elemente der Nullstellemenge vertauscht werden und sonst alles gleich bleibt.

Sei α eine Nullstelle von f. Dann ist $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] = 5$. Dann gilt $\#G = [L \colon \mathbb{Q}] = [L \colon \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) \colon \mathbb{Q}] = [L \colon \mathbb{Q}(\alpha)] \cdot 5$ und $\#G | \#\mathfrak{S}_5 = 120 = 2^3 \cdot 3 \cdot 5$. Also taucht der Primfaktor 5 in der Primfaktorzerlegung von $\#G' = \#G$ genau einmal auf, es existiert also eine 5-Sylowgruppe der Ordnung 5 in G'. Diese ist zyklisch von der Ordnung 5 und enthält daher ein Element σ der Ordnung 5. In Zykel-Schreibweise erhalten wir $\sigma = (1, \sigma(1), \sigma^2(1), \sigma^3(1), \sigma^4(1))$. In der Tat, die Länge dieses Zyklus muss genau $\operatorname{ord}(\sigma) = 5$ sein. Alle Einträge des Zyklus müssen notwendigerweise verschieden sein, also ist $\sigma(i) \forall i \in \{1, \dots, 5\}$ bestimmt. Folglich ist σ durch diesen Zyklus vollständig beschrieben.

Insgesamt folgt, dass G' sowohl eine Transposition als auch einen Fünferzykel enthält. Nach Teilaufgabe (a) ist damit bereits $G \cong G' = \mathfrak{S}_5$.

(c) Wir identifizieren f mir der induzierte Polynomfunktion auf $\mathbb{R}$, die nach Ana 1 insbesondere stetig ist. Es gilt

$$
\begin{aligned}
2 \cdot (-2)^5 - 10 \cdot (-2) + 5 &= -39 < 0. \\
2 \cdot (-1)^5 - 10 \cdot (-1) + 5 &= 13 > 0. \\
2 \cdot 1^5 - 10 \cdot 1 + 5 &= -3 < 0 \\
2 \cdot 2^5 - 10 \cdot 2 + 5 &= 49 > 0
\end{aligned}
$$

Nach dem Zwischenwertsatz besitzt f daher eine reelle Nullstelle zwischen -2 und -1, eine reelle Nullstelle zwischen -1 und 1 sowie eine reelle Nullstelle zwischen 1 und 2.

Wir betrachten die Ableitung $f'(x) = 10x^4 - 10$ und die zweite Ableitung $f''(x) = 40x^3$. Es gilt $f'(x) = 0 \implies 10x^4 = 10 \implies x^4 = 1 \implies x = \pm 1$. Wegen $f''(1) = 40$ sowie $f''(-1) = -40$ besitzt f einen Hochpunkt bei -1, einen Tiefpunkt bei 1 und sonst keine Extremstellen. Eine Funktion mit zwei Extremstellen kann höchstens drei Nullstellen besitzen, zusammen mit den Zwischenwertsatzargumenten hat f also genau drei reelle Nullstellen.

Der ggT aller Koeffizienten von f in $\mathbb{Z}$ ist 1, insbesondere ist also f primitiv. Nach dem Eisensteinkriterium mit $p = 5$ folgt wegen $5|10, 5|5, 5^2 \not| 5$ und $5 \not| 2$ die Irreduzibilität von f. Mit Teilaufgabe (b) folgt, dass die Galoisgruppe der Gleichung $f(x) = 0$ gleich $\mathfrak{S}_5$ ist. $\mathfrak{S}_5$ ist aber nicht auflösbar. Also ist $f(x) = 0$ nicht durch Radikale auflösbar.

Aufgabe 4

Behauptung: Jede Gruppe H der Ordnung 6 ist auflösbar.

Beweis. Es gilt $\#H = 6 = 2 \cdot 3$. Nach Satz 5.29 existiert eine 3-Sylow-Gruppe H' der Ordnung 3 in H. Da 3 eine Primzahl ist, ist H' nach Satz 5.39 auflösbar. Die Anzahl s der 3-Sylowgruppen erfüllt $s|6$ und $s = 1 \mod 3$. Da 4 kein Teiler von 6 ist, gilt $s = 1$. Alle zu H' konjugierten Untergruppen haben ebenfalls die Ordnung 3 und sind damit 3-Sylowgruppen. Da es aber nur eine 3-Sylowgruppe gibt, muss $gH'g^{-1} = H' \forall g \in H$ gelten und H' ist ein Normalteiler. Wir betrachten daher $H'' = H/H'$. H'' hat die Ordnung $6/3 = 2$. Da 2 und 3 Primzahlen sind, müssen H' und H'' nach Satz 5.39 auflösbar sein. Nach Satz 5.48 ist das äquivalent dazu, dass H auflösbar ist. □

Behauptung: Jede Gruppe H der Ordnung 10 ist auflösbar.

Beweis. Es gilt $\#H = 10 = 2 \cdot 5$. Nach Satz 5.29 existiert eine 5-Sylow-Gruppe H' der Ordnung 5 in H. Da 5 eine Primzahl ist, ist H' nach Satz 5.39 auflösbar. Die Anzahl s der 5-Sylowgruppen erfüllt $s|10$ und $s = 1 \mod 5$. Da 6 kein Teiler von 10 ist, gilt $s = 1$. Alle zu H' konjugierten Untergruppen haben ebenfalls die Ordnung 5 und sind damit 5-Sylowgruppen. Da es aber nur eine 5-Sylowgruppe gibt, muss $gH'g^{-1} = H' \forall g \in H$ gelten und H' ist ein Normalteiler. Wir betrachten daher $H'' = H/H'$. H'' hat die Ordnung $10/5 = 2$. Da 2 und 5 Primzahlen sind, müssen H' und H'' nach Satz 5.39 auflösbar sein. Nach Satz 5.48 ist das äquivalent dazu, dass H auflösbar ist. □

(a) Es gilt $\#G = 42 = 7 \cdot 3 \cdot 2$. Nach Satz 5.29 existiert eine 7-Sylow-Gruppe G' der Ordnung 7 in G. Da 7 eine Primzahl ist, ist G' nach Satz 5.39 auflösbar. Die Anzahl s der 7-Sylowgruppen erfüllt $s|42$ und $s = 1 \mod 7$. Jeder Teiler von 42, der nicht durch 7 teilbar ist, lässt sich als Produkt von 2 und 3 schreiben. Daher kommen für s nur Zahlen ≤ 6 infrage $\implies s = 1$. Alle zu G' konjugierten Untergruppen haben ebenfalls die Ordnung 7 und sind damit 7-Sylowgruppen. Da es aber nur eine 7-Sylowgruppe gibt, muss $gG'g^{-1} = G' \forall g \in G$ gelten und G' ist ein Normalteiler. Wir betrachten daher $G'' = G/G'$. G'' hat die Ordnung $42/7 = 6$. Daher ist G'' auch auflösbar. Nach Satz 5.48 ist das äquivalent dazu, dass G auflösbar ist.

(b) Es gilt $\#G = 30 = 5 \cdot 3 \cdot 2$. Nach Satz 5.29 existiert eine 5-Sylowgruppe G' der Ordnung 5 in G. Da 5 eine Primzahl ist, ist G' nach Satz 5.39 auflösbar. Die Anzahl s_5 der 5-Sylowgruppen erfüllt $s_5 | 30$ und $s_5 = 1 \mod 5$. Jeder Teiler von 30, der nicht durch 5 teilbar ist, lässt sich als Produkt von 2 und 3 schreiben. Daher kommen für s_5 nur Zahlen ≤ 6 infrage $\implies s_5 \in \{1, 6\}$.

Sollte $s_5 = 1$ gelten, so besitzen alle zu G' konjugierten Untergruppen ebenfalls die Ordnung 5 und sind damit 5-Sylowgruppen. Da es aber nur eine 5-Sylowgruppe gibt, muss $gG'g^{-1} = G' \forall g \in G$ gelten und G' ist ein Normalteiler. Wir betrachten daher $G'' = G/G'$. G'' hat die Ordnung $30/5 = 6$. Daher ist G'' auch auflösbar. Nach Satz 5.48 ist das äquivalent dazu, dass G auflösbar ist.

Gelte nun $s_5 = 6$. Dann operiert G vermöge der Konjugation auf der Menge der 5-Sylowgruppen $S_1, \ldots, S_6$. Da 5 prim ist, erzeugt jedes $e \neq x \in S_i$ bereits die Sylowgruppe. Da die Gruppen verschieden sind, muss daher $S_i \cap S_j = \{e\} \forall i \neq j$ sein. Jedes Element einer 5-Sylowgruppe hat Ordnung 5^r nach Lemma 5.33(ii), aber auch Ordnung ≤ 5, da wir sonst durch $\{a^i, i = 0, \ldots, 5\}$ 6 verschiedene Elemente erhalten, die alle in der Untergruppe liegen müssen. Also hat jedes Element (außer e) einer solchen Sylowgruppe Ordnung 5. Da die Sylowgruppen bis auf das neutrale Element disjunkt sind, gilt

$$\# \bigcup_{i=1}^{6} S_i \setminus \{e\} = 6 \cdot 4 = 24$$

und es gibt mindestens 24 Elemente der Ordnung 5.

Nach Satz 5.29 existiert eine 3-Sylowgruppe H' der Ordnung 3 in G. Da 3 eine Primzahl ist, ist H' nach Satz 5.39 auflösbar. Die Anzahl s_3 der 3-Sylowgruppen erfüllt $s_3 | 30$ und $s_3 = 1 \mod 3$. Jeder Teiler von 30, der nicht durch 3 teilbar ist, lässt sich als Produkt von 2 und 5 schreiben. Daher kommen für s_3 nur Zahlen ≤ 10 infrage $\implies s_3 \in \{1, 10\}$.

Sollte $s_3 = 1$ gelten, so besitzen alle zu H' konjugierten Untergruppen ebenfalls die Ordnung 3 und sind damit 3-Sylowgruppen. Da es aber nur eine 3-Sylowgruppe gibt, muss $gH'g^{-1} = H' \forall g \in G$ gelten und H' ist ein Normalteiler. Wir betrachten daher $H'' = G/H'$. H'' hat die Ordnung $30/3 = 10$. Daher ist H'' auch auflösbar. Nach Satz 5.48 ist das äquivalent dazu, dass G auflösbar ist.

Gelte nun $s_3 = 10$. Dann operiert G vermöge der Konjugation auf der Menge der 3-Sylowgruppen $T_1, \ldots, T_6$. Da 3 prim ist, erzeugt jedes $e \neq x \in T_i$ bereits die Sylowgruppe. Da die Gruppen verschieden sind, muss daher $T_i \cap T_j = \{e\} \forall i \neq j$ sein. Jedes Element einer 3-Sylowgruppe hat Ordnung 3^r nach Lemma 5.33(ii), aber auch Ordnung ≤ 3, da wir sonst durch $\{a^i, i = 0, \ldots, 3\}$ 4 verschiedene Elemente erhalten, die alle in der Untergruppe liegen müssen. Also hat jedes Element (außer e) einer solchen Sylowgruppe Ordnung 3. Da die Sylowgruppen bis auf das neutrale Element disjunkt sind, gilt

$$\# \bigcup_{i=1}^{1} 0T_i \setminus \{e\} = 10 \cdot 2 = 20$$

und es gibt mindestens 20 Elemente der Ordnung 3.

Gilt also $s_3 = 1$ oder $s_5 = 1$, so ist G auflösbar. Gilt $s_3 \neq 1$ und $s_5 \neq 1$, so erhalten wir mindestens 24 Elemente der Ordnung 5 und 20 Elemente der Ordnung 3. G hat aber nur 30 Elemente, Widerspruch. Also kann dieser Fall nicht eintreten und G ist stets auflösbar.

(c) Wegen $(g,h) \cdot (e \times H) \cdot (g^{-1}, h^{-1}) = gg^{-1} \times hHh^{-1} \subset (e \times H)$ ist $e \times H \triangleleft G \times H$. Weiter folgern wir

$$(G \times H)/(e \times H) = \{g \times H : g \in G\} \cong G$$

Offensichtlich ist außerdem $(e \times H) \cong H$. Mit H und G sind demnach auch $e \times H$ und $(G \times H)/(e \times H)$ auflösbar. Nach Satz 5.48 folgt bereits die Auflösbarkeit von $G \times H$.