Musterlösung 24

Galoiserweiterungen

1. Betrachte $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{R}$.

   (a) Zeige, dass $K/\mathbb{Q}$ galoissch ist mit Galoisgruppe $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   (b) Sei $L := K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right) \subset \mathbb{R}$. Zeige, dass $L/\mathbb{Q}$ galoissch ist.

   (*c) Bestimme $[L/\mathbb{Q}]$.

   (*d) Bestimme $\mathrm{Gal}(L/\mathbb{Q})$ bis auf Isomorphie.

   Lösung: (a) Als Zerfällungskörper des Polynoms $(X^2-2)(X^2-3)$ ist $K/\mathbb{Q}$ normal. Wegen Charakteristik null ist die Erweiterung ausserdem separabel; folglich ist sie galoissch. Nach Serie 15 Aufgabe 4 (a) gilt weiter $[K/\mathbb{Q}] = 4$, darum ist $\Gamma := \mathrm{Gal}(K/\mathbb{Q})$ eine Gruppe der Ordnung 4.

   Für den Zwischenkörper $\mathbb{Q}(\sqrt{3})$ gilt $[K/\mathbb{Q}(\sqrt{3})] = [K/\mathbb{Q}]/[\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 4/2 = 2$. Also ist $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{3}))$ eine Untergruppe der Ordnung 2 von Γ. Wegen $K = \mathbb{Q}(\sqrt{3})(\sqrt{2})$ muss diese die Nullstellen $\pm\sqrt{2}$ von X^2-2 echt vertauschen. Für das nichttriviale Element $\sigma_2 \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{3}))$ gilt somit $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Dies ist also ein Element der Ordnung 2 von Γ mit $\sigma_2(\sqrt{2}) = -\sqrt{2}$ und $\sigma_2(\sqrt{3}) = \sqrt{3}$.

   Dasselbe Argument mit dem Zwischenkörper $\mathbb{Q}(\sqrt{2})$ liefert ein Element $\sigma_3 \in \Gamma$ der Ordnung 2 mit $\sigma_3(\sqrt{2}) = \sqrt{2}$ und $\sigma_3(\sqrt{3}) = -\sqrt{3}$. Das Element $\sigma_2\sigma_3 := \sigma_2 \circ \sigma_3$ fixiert dann weder $\sqrt{2}$ noch $\sqrt{3}$ und ist folglich ein weiteres nichttriviales Element von Γ. Wegen $|\Gamma| = 4$ gilt also $\Gamma = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$. Da σ_2 und σ_3 die Ordnung 2 haben, ist folglich Γ isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   (b) Jeder Homomorphismus $\varphi\colon L \to \mathbb{C}$ entsteht, indem wir zuerst einen Homomorphismus $K \to \mathbb{C}$ betrachten und diesen auf L fortsetzen durch eine geeignete Wahl einer Quadratwurzel aus $\varphi((2+\sqrt{2})(3+\sqrt{3}))$. Da $K/\mathbb{Q}$ normal ist, gilt schon $\varphi(K) = K$ und $\varphi|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Die Möglichkeiten für $\varphi((2+\sqrt{2})(3+\sqrt{3}))$ sind also nach (a) genau die vier Zahlen $(2 \pm \sqrt{2})(3 \pm \sqrt{3})$. Betrachte deren positive reelle Quadratwurzeln

$$\begin{aligned} x_1 &:= \sqrt{(2+\sqrt{2})(3+\sqrt{3})}, \\ x_2 &:= \sqrt{(2-\sqrt{2})(3+\sqrt{3})}, \\ x_3 &:= \sqrt{(2+\sqrt{2})(3-\sqrt{3})}, \\ x_4 &:= \sqrt{(2-\sqrt{2})(3-\sqrt{3})}. \end{aligned}$$

Dann ist $\varphi(x_1) = \varepsilon x_i$ für ein $\varepsilon \in \{\pm 1\}$ und $1 \leqslant i \leqslant 4$. Direkte Rechnung zeigt nun

$$(*) \qquad \begin{aligned} x_1x_2 &:= \sqrt{(2^2-2)(3+\sqrt{3})^2} &&= \sqrt{2}\cdot(3+\sqrt{3}) &&\in K^\times, \\ x_1x_3 &:= \sqrt{(2+\sqrt{2})^2(3^2-3)} &&= (2+\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} &&\in K^\times, \\ x_1x_4 &:= \sqrt{(2^2-2)(3^2-3)} &&= 2\cdot\sqrt{3} &&\in K^\times. \end{aligned}$$

In jedem Fall gilt also $K(\varepsilon x_i) = K(x_1) = L$. Daraus folgt $\varphi(L) = \varphi(K(x_1)) = \varphi(K)(\varphi(x_1)) = K(\varepsilon x_i) = L$. Da dies für jedes φ gilt, ist somit L/K normal, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ dann auch galoissch.

(c) Nehmen wir an, es sei $L = K$. Dann sind insbesondere $x_1, x_2 \in K$, und nach Konstruktion von x_1 und x_2 gilt $\sigma_2(x_1)^2 = \sigma_2(x_1^2) = x_2^2$ und folglich $\sigma_2(x_1) = \varepsilon x_2$ für ein gewisses $\varepsilon \in \{\pm 1\}$. Setze $y := x_1 \cdot \sigma_2(x_1)$. Da σ_2 die Ordnung 2 hat, gilt $\sigma_2(y) = \sigma_2(x_1)\cdot\sigma_2^2(x_1) = y$; deshalb liegt y im Fixkörper der Untergruppe $\langle\sigma_2\rangle < \Gamma$, das heisst in $\mathbb{Q}(\sqrt{3})$. Nach der obigen Rechnung $(*)$ ist andererseits $y = \varepsilon x_1x_2 = \pm\sqrt{2}\cdot(3+\sqrt{3})$. Somit ist auch $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Dies widerspricht aber der bereits etablierten Tatsache, dass $\mathbb{Q}(\sqrt{2},\sqrt{3}) \neq \mathbb{Q}(\sqrt{3})$ ist. Daher ist $L \neq K$.

Wegen $L = K(x_1)$ mit $x_1^2 \in K$ ist $[L/K] = 2$. Daraus folgt schliesslich $[L/\mathbb{Q}] = [L/K]\cdot[K/\mathbb{Q}] = 2\cdot 4 = 8$.

(d) Setze $\tilde{\Gamma} := \mathrm{Gal}(L/\mathbb{Q})$. Dann ist $\mathrm{Gal}(L/K) < \tilde{\Gamma}$ eine Untergruppe der Ordnung 2; sei τ ihr nichttriviales Element. Wegen $L = K(x_i)$ mit $x_i^2 \in K$ gilt dann $\tau(x_i) = -x_i$ für jedes $1 \leqslant i \leqslant 4$. Da $K/\mathbb{Q}$ selbst galoissch ist, folgt aus Teil (e) des Hauptsatzes der Galoistheorie, dass die Untergruppe $\langle\tau\rangle$ normal in $\tilde{\Gamma}$ und die Faktorgruppe natürlich isomorph zu Γ ist.

Also existiert ein Element $\tilde{\sigma}_2 \in \tilde{\Gamma}$ mit $\tilde{\sigma}_2|_K = \sigma_2$. Nach Konstruktion von x_1 und x_2 gilt dann $\tilde{\sigma}_2(x_1)^2 = \tilde{\sigma}_2(x_1^2) = \sigma_2(x_1^2) = x_2^2$ und folglich $\tilde{\sigma}_2(x_1) = \pm x_2$. Nach etwaigem Ersetzen von $\tilde{\sigma}_2$ durch $\tau\tilde{\sigma}_2$ können wir oBdA $\tilde{\sigma}_2(x_1) = x_2$ annehmen, haben damit aber unsere Wahlmöglichkeiten erschöpft. Die Werte von $\tilde{\sigma}_2$ an den übrigen Nullstellen bestimmen wir mittels der Rechnung $(*)$ und der analogen Rechnung

$$(**) \qquad \begin{aligned} x_2x_3 &:= \sqrt{(2^2-2)(3^2-3)} &&= 2\cdot\sqrt{3} &&\in K^\times, \\ x_2x_4 &:= \sqrt{(2-\sqrt{2})^2(3^2-3)} &&= (2-\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} &&\in K^\times, \\ x_3x_4 &:= \sqrt{(2^2-2)(3-\sqrt{3})^2} &&= \sqrt{2}\cdot(3-\sqrt{3}) &&\in K^\times. \end{aligned}$$

Unter Benutzung der bereits bekannten Operation von $\tilde{\sigma}_2$ auf K erhalten wir

$$\begin{aligned} \tilde{\sigma}_2(x_1)\tilde{\sigma}_2(x_2) &= \tilde{\sigma}_2(x_1x_2) &&= \tilde{\sigma}_2\big(\sqrt{2}\cdot(3+\sqrt{3})\big) &&= -\sqrt{2}\cdot(3+\sqrt{3}) &&= -x_1x_2, \\ \tilde{\sigma}_2(x_1)\tilde{\sigma}_2(x_3) &= \tilde{\sigma}_2(x_1x_3) &&= \tilde{\sigma}_2\big((2+\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3}\big) &&= -(2-\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} &&= -x_2x_4, \\ \tilde{\sigma}_2(x_1)\tilde{\sigma}_2(x_4) &= \tilde{\sigma}_2(x_1x_4) &&= \tilde{\sigma}_2\big(2\cdot\sqrt{3}\big) &&= 2\cdot\sqrt{3} &&= +x_2x_3, \end{aligned}$$

was wegen $\tilde{\sigma}_2(x_1) = x_2$ die Werte $\tilde{\sigma}_2(x_2) = -x_1$ und $\tilde{\sigma}_2(x_3) = -x_4$ und $\tilde{\sigma}_2(x_4) = +x_3$ impliziert.

Analog finden wir ein Element $\tilde{\sigma}_3 \in \tilde{\Gamma}$ mit $\tilde{\sigma}_3|_K = \sigma_3$ und $\tilde{\sigma}_3(x_1) = x_3$, und die entsprechende Rechnung liefert uns die Werte $\tilde{\sigma}_3(x_2) = +x_4$ und $\tilde{\sigma}_3(x_3) = -x_1$ und $\tilde{\sigma}_3(x_4) = -x_2$.

Insgesamt erhalten wir so die Werte

	τ	$\tilde{\sigma}_2$	$\tilde{\sigma}_3$	$\tilde{\sigma}_2^2$	$\tilde{\sigma}_3^2$	$\tilde{\sigma}_2\tilde{\sigma}_3$	$(\tilde{\sigma}_2\tilde{\sigma}_3)^2$
x_1	$-x_1$	$+x_2$	$+x_3$	$-x_1$	$-x_1$	$-x_4$	$-x_1$
x_2	$-x_2$	$-x_1$	$+x_4$	$-x_2$	$-x_2$	$+x_3$	$-x_2$
x_3	$-x_3$	$-x_4$	$-x_1$	$-x_3$	$-x_3$	$-x_2$	$-x_3$
x_4	$-x_4$	$+x_3$	$-x_2$	$-x_4$	$-x_4$	$+x_1$	$-x_4$

Diese Tabelle impliziert $\tilde{\sigma}_2^2 = \tilde{\sigma}_3^2 = (\tilde{\sigma}_2\tilde{\sigma}_3)^2 = \tau$; insbesondere haben $\tilde{\sigma}_2$ und $\tilde{\sigma}_3$ und $\tilde{\sigma}_2\tilde{\sigma}_3$ alle die Ordnung 4. Weiter gilt $\tilde{\sigma}_2\tilde{\sigma}_3(x_1) = -x_4 = -\tilde{\sigma}_3\tilde{\sigma}_2(x_1)$. Somit ist die Gruppe Γ nichtabelsch. Da sie mit $\tilde{\sigma}_2^{\pm 1}$ und $\tilde{\sigma}_3^{\pm 1}$ und $(\tilde{\sigma}_2\tilde{\sigma}_3)^{\pm 1}$ schon 6 verschiedene Elemente der Ordnung 4 besitzt, und selbst die Ordnung 8 hat, kann sie nur eine Quaternionengruppe sein.

2. Sei L ein Zerfällungskörper des Polynoms $X^6 - 5$ über $\mathbb{Q}$. Bestimme alle Zwischenkörper von $L/\mathbb{Q}$ mitsamt Inklusionen sowie, falls sie galoissch über $\mathbb{Q}$ sind, deren Galoisgruppen über $\mathbb{Q}$.

   Lösung: Da $\mathbb{C}$ algebraisch abgeschlossen ist, können wir L als in $\mathbb{C}$ eingebettet annehmen. Sei a die positive reelle sechste Wurzel aus 5. Sei ζ eine primitive dritte Einheitswurzel in $\mathbb{C}$. Für $1 \leqslant i \leqslant 6$ sei $a_i := a \cdot (-\zeta)^{i-1}$. Dann ist $a_i^6 - 5 = a^6 \cdot (-\zeta)^{6i-6} - 5 = 0$, also sind $a_1, \ldots, a_6$ gerade die sechs verschiedenen Nullstellen von $X^6 - 5$. Somit ist $L = \mathbb{Q}(a_1, \ldots, a_6) \subset \mathbb{Q}(a, \zeta)$, und wegen $a_1 = a$ und $-\frac{a_2}{a_1} = -\frac{a\cdot(-\zeta)}{a} = \zeta$ ist sogar $L = \mathbb{Q}(a, \zeta)$.

   Für $1 \leqslant i \leqslant 6$ ist $[\mathbb{Q}(a_i)/\mathbb{Q}] = 6$, da $X^6 - 5$ nach dem Eisenstein-Kriterium irreduzibel ist. Wegen $\zeta \notin \mathbb{Q}(a) \subset \mathbb{R}$ ist zudem $[L/\mathbb{Q}(a)] = 2$, und somit $[L/\mathbb{Q}] = [L/\mathbb{Q}(a)] \cdot [\mathbb{Q}(a)/\mathbb{Q}] = 12$. Insbesondere hat auch $\mathrm{Gal}(L/\mathbb{Q})$ Ordnung 12.

   Wir fassen im Folgenden $\mathrm{Gal}(L/\mathbb{Q})$ durch die durch $a_i \mapsto i$ induzierte Einbettung als Untergruppe von S_6 auf.

   Da $L/\mathbb{Q}$ normal ist, ist die Einschränkung σ der komplexen Konjugation auf L ein Element von $\mathrm{Gal}(L/\mathbb{Q})$. Konkret entspricht σ der Permutation $(2\,6)(3\,5)$.

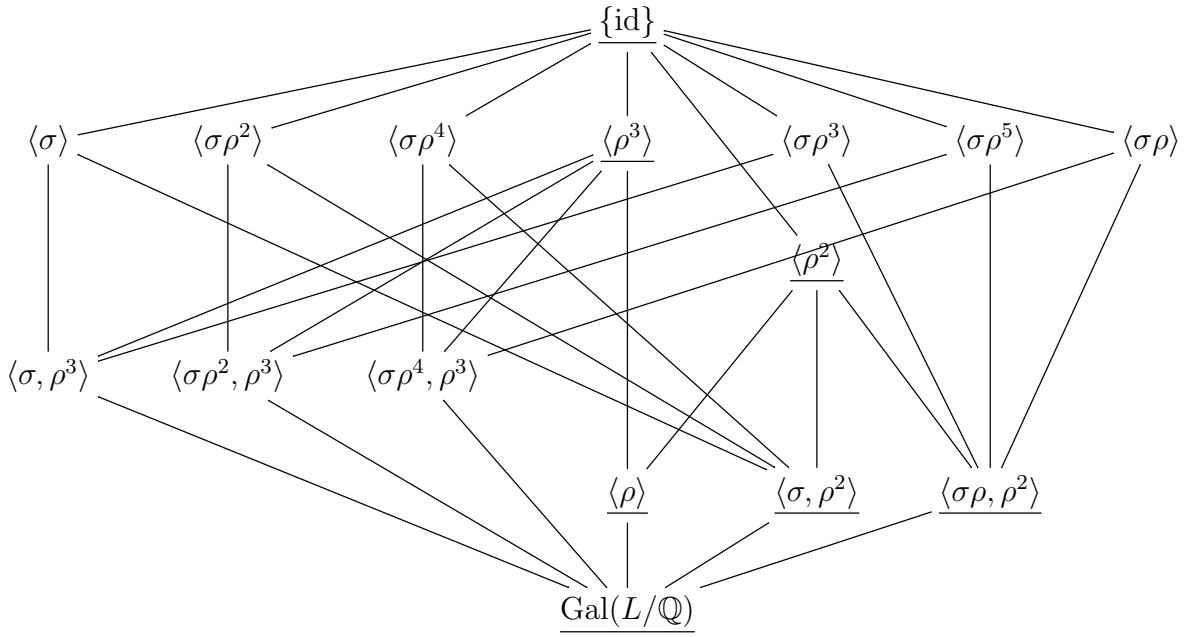
   Da $X^6 - 5$ irreduzibel ist, operiert $\mathrm{Gal}(L/\mathbb{Q})$ transitiv auf dessen Nullstellen; es existiert also ein $\rho \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\rho(a_1) = a_2$. Wegen $\sigma(a_1) = a_1$ gilt auch $(\rho\sigma)(a_1) = a_2$. Da σ die beiden Nullstellen ζ und ζ^2 des irreduziblen Polynoms $X^2 + X + 1$ vertauscht und ρ sie als $\mathbb{Q}$-Homomorphismus vertauscht oder fix lässt, können wir also (indem wir allenfalls ρ durch $\rho\sigma$ ersetzen) ohne Beschränkung der

Allgemeinheit annehmen, dass $\rho(\zeta) = \zeta$ ist. Dann ist $\rho(a_i) = \rho\big(a \cdot (-\zeta)^{i-1}\big) = a \cdot (-\zeta)^i$, also hat ρ die Darstellung $(1\,2\,3\,4\,5\,6)$.

Die Rechnung $\sigma\rho\sigma^{-1} = (2\,6)(3\,5)(1\,2\,3\,4\,5\,6)(2\,6)(3\,5) = (6\,5\,4\,3\,2\,1) = \rho^{-1}$ zeigt nun, dass die von ρ und σ erzeugte Untergruppe eine Surjektion auf D_6 besitzt, also mindestens Ordnung 12 hat.

Wegen $|D_6| = 12 = |\operatorname{Gal}(L/\mathbb{Q})| \geqslant |\langle\rho, \sigma\rangle|$ folgt daher $\operatorname{Gal}(L/\mathbb{Q}) = \langle\rho, \sigma\rangle \cong D_6$.

Wir machen nun eine Aufstellung aller Untergruppen von $\operatorname{Gal}(L/\mathbb{Q}) \cong D_6$ (die detaillierte Überprüfung überlassen wir dem Leser); normale Untergruppen sind unterstrichen:



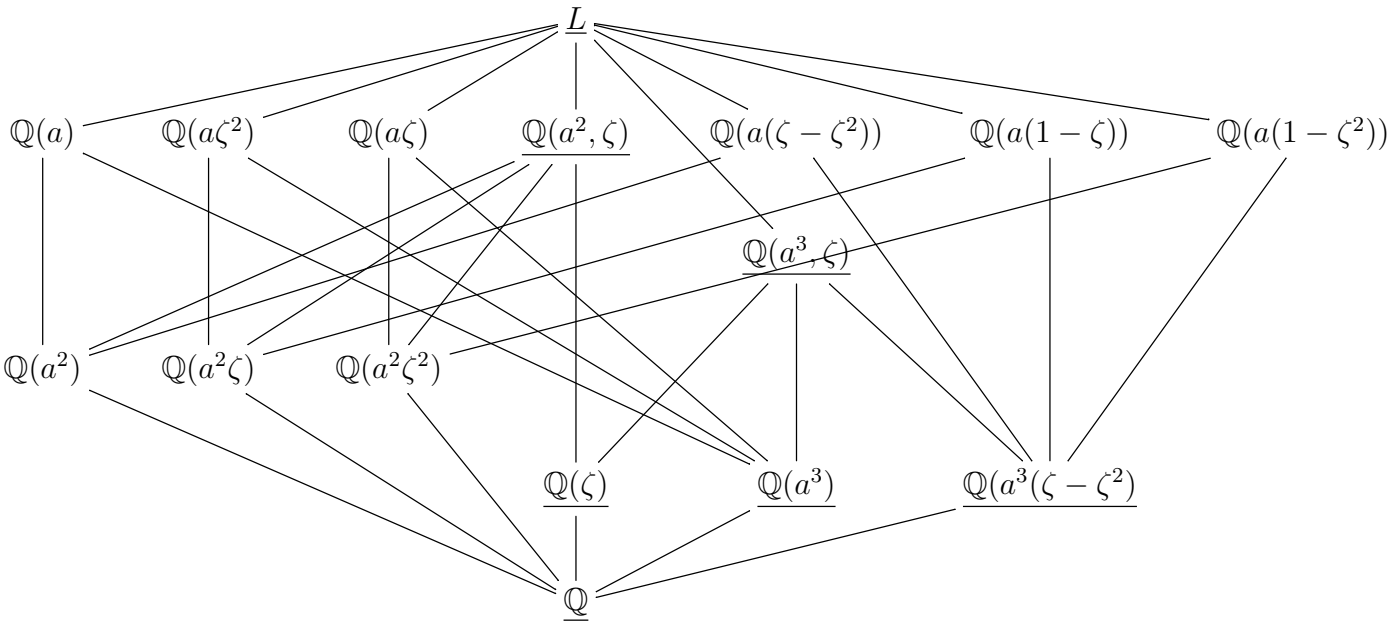
Daraus folgern wir nun die Aufstellung der Zwischenkörper; die Galois-Korrespondenz ordnet einer Untergruppe $H < \operatorname{Gal}(L/\mathbb{Q})$ den Fixkörper L^H mit dem Erweiterungsgrad $[L^H/\mathbb{Q}] = \frac{|\operatorname{Gal}(L/\mathbb{Q})|}{|H|} = \frac{12}{|H|}$ zu:

- $L^{\{\mathrm{id}\}} = L$.
- $L^{\operatorname{Gal}(L/\mathbb{Q})} = \mathbb{Q}$.
- Es ist $\sigma(a) = a$, also $\mathbb{Q}(a) \subset L^{\langle\sigma\rangle}$. Zudem ist $[\mathbb{Q}(a)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rangle|}$, also $L^{\langle\sigma\rangle} = \mathbb{Q}(a)$.
- Analog ist $(\sigma\rho^2)(a\zeta^2) = a\zeta^2$, also $\mathbb{Q}(a\zeta^2) \subset L^{\langle\sigma\rho^2\rangle}$. Zudem ist $[\mathbb{Q}(a\zeta^2)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^2\rangle|}$, also $L^{\langle\sigma\rho^2\rangle} = \mathbb{Q}(a\zeta^2)$.
- Analog ist $(\sigma\rho^4)(a\zeta) = a\zeta$, also $\mathbb{Q}(a\zeta) \subset L^{\langle\sigma\rho^4\rangle}$. Zudem ist $[\mathbb{Q}(a\zeta)/\mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^4\rangle|}$, also $L^{\langle\sigma\rho^4\rangle} = \mathbb{Q}(a\zeta)$.

- Es ist $\sigma(a^2) = \rho^3(a^2) = a^2$, also $\mathbb{Q}(a^2) \subset L^{\langle \sigma, \rho^3 \rangle}$. Zudem ist a^2 eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2)/\mathbb{Q}] = 3 = \frac{12}{|\langle \sigma, \rho^3 \rangle|}$ und somit $L^{\langle \sigma, \rho^3 \rangle} = \mathbb{Q}(a^2)$.
- Analog ist $(\sigma\rho^2)(a^2\zeta) = \rho^3(a^2\zeta) = a^2\zeta$, also $\mathbb{Q}(a^2\zeta) \subset L^{\langle \sigma\rho^2, \rho^3 \rangle}$. Zudem ist $a^2\zeta$ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2\zeta)/\mathbb{Q}] = 3 = \frac{12}{|\langle \sigma\rho^2, \rho^3 \rangle|}$ und somit $L^{\langle \sigma\rho^2, \rho^3 \rangle} = \mathbb{Q}(a^2\zeta)$.
- Analog ist $(\sigma\rho^4)(a^2\zeta^2) = \rho^3(a^2\zeta^2) = a^2\zeta^2$, also $\mathbb{Q}(a^2\zeta^2) \subset L^{\langle \sigma\rho^4, \rho^3 \rangle}$. Zudem ist $a^2\zeta^2$ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 5$, also $[\mathbb{Q}(a^2\zeta^2)/\mathbb{Q}] = 3 = \frac{12}{|\langle \sigma\rho^4, \rho^3 \rangle|}$ und somit $L^{\langle \sigma\rho^4, \rho^3 \rangle} = \mathbb{Q}(a^2\zeta^2)$.
- Es ist $\rho(\zeta) = \zeta$, also $\mathbb{Q}(\zeta) \subset L^{\langle \rho \rangle}$. Zudem ist $[\mathbb{Q}(\zeta)/\mathbb{Q}] = 2 = \frac{12}{|\langle \rho \rangle|}$, also $\mathbb{Q}(\zeta) = L^{\langle \rho \rangle}$.
- Es ist $\sigma(a^3) = \rho^2(a^3) = a^3$, also $\mathbb{Q}(a^3) \subset L^{\langle \sigma, \rho^2 \rangle}$. Zudem ist a^3 eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^2 - 5$, also ist $[\mathbb{Q}(a^3)/\mathbb{Q}] = 2 = \frac{12}{|\langle \sigma, \rho^2 \rangle|}$ und somit $\mathbb{Q}(a^3) = L^{\langle \sigma, \rho^2 \rangle}$.
- Es ist $\rho^2(a^3) = a^3$ und $\rho^2(\zeta) = \zeta$, also $\mathbb{Q}(a^3, \zeta) \subset L^{\langle \rho^2 \rangle}$. Wegen $\zeta \notin \mathbb{Q}(a^3) \subset \mathbb{R}$ ist $[\mathbb{Q}(a^3, \zeta)/\mathbb{Q}] = [\mathbb{Q}(a^3, \zeta)/\mathbb{Q}(a^3)][\mathbb{Q}(a^3)/\mathbb{Q}] = 4$, also $[\mathbb{Q}(a^3, \zeta)/\mathbb{Q}] = \frac{12}{|\langle \rho^2 \rangle|}$ und somit $L^{\langle \rho^2 \rangle} = \mathbb{Q}(a^3, \zeta)$.
- Analog ist $\rho^3(a^2) = a^2$ und $\rho^3(\zeta) = \zeta$, also $\mathbb{Q}(a^2, \zeta) \subset L^{\langle \rho^3 \rangle}$. Wegen $\zeta \notin \mathbb{Q}(a^2) \subset \mathbb{R}$ ist $[\mathbb{Q}(a^2, \zeta)/\mathbb{Q}] = [\mathbb{Q}(a^2, \zeta)/\mathbb{Q}(a^2)][\mathbb{Q}(a^2)/\mathbb{Q}] = 6$, also $[\mathbb{Q}(a^2, \zeta)/\mathbb{Q}] = \frac{12}{|\langle \rho^3 \rangle|}$ und somit $L^{\langle \rho^3 \rangle} = \mathbb{Q}(a^2, \zeta)$.
- Es gilt $(\sigma\rho^3)(a\zeta) = -a\zeta^2$ und somit $(\sigma\rho^3)(a(\zeta - \zeta^2)) = a(\zeta - \zeta^2)$ wegen $(\sigma\rho^3)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(\zeta - \zeta^2)) \subset L^{\langle \sigma\rho^3 \rangle}$. Zudem ist $a(\zeta - \zeta^2)$ eine Nullstelle des Polynoms $X^6 + 135$, und dieses ist irreduzibel über $\mathbb{Q}$ nach dem Eisensteinkriterium bezüglich der Primzahl 5. Also ist $[\mathbb{Q}(a(\zeta - \zeta^2))/\mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho^3 \rangle|}$ und somit $L^{\langle \sigma\rho^3 \rangle} = \mathbb{Q}(a(\zeta - \zeta^2))$.
- Analog gilt $(\sigma\rho^5)(a) = -a\zeta$ und somit $(\sigma\rho^5)(a(1 - \zeta)) = a(1 - \zeta)$ wegen $(\sigma\rho^5)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(1 - \zeta)) \subset L^{\langle \sigma\rho^5 \rangle}$. Zudem ist $a(1 - \zeta)$ eine Nullstelle des Polynoms $X^6 + 135$. Also ist $[\mathbb{Q}(a(1 - \zeta))/\mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho^5 \rangle|}$ und somit $L^{\langle \sigma\rho^5 \rangle} = \mathbb{Q}(a(1 - \zeta))$.
- Analog gilt $(\sigma\rho)(a) = -a\zeta^2$ und somit $(\sigma\rho)(a(1 - \zeta^2)) = a(1 - \zeta^2)$ wegen $(\sigma\rho)^2 = \mathrm{id}_L$; also ist $\mathbb{Q}(a(1 - \zeta^2)) \subset L^{\langle \sigma\rho \rangle}$. Zudem ist $a(1 - \zeta^2)$ eine Nullstelle des Polynoms $X^6 + 135$. Also ist $[\mathbb{Q}(a(1 - \zeta^2))/\mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho \rangle|}$ und somit $L^{\langle \sigma\rho \rangle} = \mathbb{Q}(a(1 - \zeta^2))$.
- Es ist $L^{\langle \sigma\rho, \rho^2 \rangle} = L^{\langle \sigma\rho \rangle} \cap L^{\langle \rho^2 \rangle} = \mathbb{Q}(a^3, \zeta) \cap \mathbb{Q}(a(1 - \zeta^2)) \ni (a(1 - \zeta^2))^3 = 3a^3(\zeta - \zeta^2)$. Wegen $[L^{\langle \sigma\rho, \rho^2 \rangle}/\mathbb{Q}] = \frac{12}{|\langle \sigma\rho, \rho^2 \rangle|} = 2$ und $a^3(\zeta - \zeta^2) \notin \mathbb{Q} \subset \mathbb{R}$ gilt also $L^{\langle \sigma\rho, \rho^2 \rangle} = \mathbb{Q}(a^3(\zeta - \zeta^2))$.

Bemerkung: An einigen Stellen hätte man auch ausnutzen können, dass mehrere der Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$ zu einander konjugiert sind. Sind nämlich zwei Untergruppen H, H' unter φ konjugiert, so ist $L^{H'} = \varphi(L^H)$.

Insgesamt ergibt sich die folgende Aufstellung:



Dabei ist ein Zwischenkörper unterstrichen, wenn die entsprechende Untergruppe von $\mathrm{Gal}(L/\mathbb{Q})$ normal ist. Nach dem Hauptsatz der Galoistheorie ist das genau dann der Fall, wenn der Zwischenkörper galoissch über $\mathbb{Q}$ ist, und dann gilt weiter $\mathrm{Gal}(L^H/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/H$. Daraus ergeben sich die folgenden Galoisgruppen:

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(a^2,\zeta)/\mathbb{Q}) &\cong D_3,\\
\mathrm{Gal}(\mathbb{Q}(a^3,\zeta)/\mathbb{Q}) &\cong (\mathbb{Z}/2\mathbb{Z})^2,\\
\mathrm{Gal}(\mathbb{Q}(a^3)/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(a^3(\zeta-\zeta^2))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.
\end{aligned}$$

3. (a) 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.

   (*b) Finde für jede Primzahl p ein Polynom wie in (a).

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

i. G enthält einen p-Zykel, d.h. ein Element der Form $(i_1\ i_2\ \ldots\ i_p)$ für irgendeine Anordnung $i_1, \ldots, i_p$ von $1, \ldots, p$.

ii. G enthält eine Transposition, d.h. ein Element $(i\ j)$ für $1 \leqslant i < j \leqslant p$.

Für i. wissen wir aus der Vorlesung, dass G transitiv auf den Nullstellen operiert, weil f irreduzibel ist. Ihre Anzahl p ist also ein Teiler der Gruppenordnung $|G|$. Somit enthält G 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 i. gezeigt.

Für ii. seien ohne Beschränkung der Allgemeinheit a_1 und a_2 die beiden nichtreellen Nullstellen von f. Da die Koeffizienten von f reell sind, 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 $3 \leqslant i \leqslant p$. Die komplexe Konjugation ist ein Körperautomorphismus von $\mathbb{C}$ und induziert also einen Körperautomorphismus von L, und somit ein Element von G. Als Permutation dargestellt ist es die Transposition (1 2), womit ii. bewiesen ist.

Aus Aufgabe 4 der Übungsserie 11 der Vorlesung Algebra I des Herbstsemesters ist bekannt, daß jede Untergruppe von S_p mit den obigen Eigenschaften i. und ii. gleich S_p ist. Daraus folgt die gewünschte Behauptung.

(b) Wir konstruieren ein solches Polynom, indem wir mit einem geeigneten Polynom vom Grad p beginnen, welches genau zwei nichtreelle Nullstellen hat, und seine Koeffizienten nur wenig abändern, so dass diese Eigenschaft erhalten bleibt und das Polynom irreduzibel über $\mathbb{Q}$ wird. Die Irreduzibilität garantieren wir mit dem Eisensteinkriterium bei irgendeiner Primzahl, zum Beispiel bei 2.

Für jedes $t \in \mathbb{R}$ setzen wir

$$f_t(x) := (x^2 + 1) \prod_{j=1}^{p-2} (x - j) + t.$$

Behauptung: Es existiert ein $\varepsilon > 0$, sodass f_t für jedes t mit $|t| < \varepsilon$ in $\mathbb{C}$ genau $p - 2$ verschiedene reelle, sowie 2 komplex konjugierte nicht-reelle Nullstellen hat.

Beweis: Das Polynom f_0 hat die komplexen Nullstellen $z_k := k$ für $1 \leqslant k \leqslant p - 2$, sowie $z_{p-1}, z_p := \pm i$. Setze $G_k := \{z \in \mathbb{C} \mid |z - z_k| < \frac{1}{3}\}$ und $G := \bigcup_{k=1}^{n} G_k$. Da ∂G keine Nullstelle von f_0 enthält und f_0 eine stetige Funktion darstellt, ist $\varepsilon := \min_{z \in \partial G} |f_0(z)| > 0$. Für jedes $t \in \mathbb{R}$ mit $|t| < \varepsilon$ und jedes $1 \leqslant k \leqslant p$ gilt nun

$$\forall z \in \partial G_k : |f_t(z) - f_0(z)| < |f_t(z)| + |f_0(z)|.$$

Nach dem Satz von Rouché haben also f_t und f_0 gleich viele Nullstellen in G_k, also genau eine. Die beiden Nullstellen von f_t in G_{p-1} und G_p sind nicht-reell und komplex konjugiert. Die Nullstellen von f_t in $G_1, \ldots, G_{p-2}$ sind alle reell; wäre nämlich $z \in G_k$ eine nicht-reelle Nullstelle von f_t, so müsste dies auch für $\overline{z} \in G_k$ gelten, im Widerspruch dazu, dass f_t genau eine Nullstelle in G_k hat. $\square$

Sei nun ε wie oben, wähle $k \in \mathbb{Z}^{>0}$ mit $t := \frac{2}{(2k)^p} < \varepsilon$, und setze

$$f(x) \;:=\; f_t(x/2k) \cdot (2k)^p \;=\; (x^2 + 4k^2) \prod_{j=1}^{p-2} (x - 2kj) + 2 \;\in\; \mathbb{Z}[X].$$

Nach obiger Behauptung hat f_t und somit auch f genau $p-2$ relle, sowie 2 komplex konjugierte nicht-reelle Nullstellen. Ausserdem ist f irreduzibel nach dem Eisensteinkriterium bezüglich der Primzahl 2.

4. Sei L/K eine endliche Galoiserweiterung und seien E, E' zwei Zwischenkörper. Zeige, dass E und E' genau dann isomorph über K sind, wenn $\mathrm{Gal}(L/E)$ und $\mathrm{Gal}(L/E')$ in $\mathrm{Gal}(L/K)$ konjugiert sind.

   Lösung: Wir setzen $\Gamma := \mathrm{Gal}(L/K)$ und $\Delta := \mathrm{Gal}(L/E)$ und $\Delta' := \mathrm{Gal}(L/E')$.

   "$\Leftarrow$": Sei $\gamma \in \Gamma$ mit ${}^{\gamma}\Delta = \Delta'$. Nach Teil (c) des Hauptsatzes der Galoistheorie ist dann $\gamma(E) = E'$. Also induziert γ einen Isomorphismus $E \xrightarrow{\sim} E'$ über K.

   "$\Rightarrow$": Sei $\varphi\colon E \xrightarrow{\sim} E'$ ein Isomorphismus über K. Da L/E algebraisch ist, besitzt φ eine Fortsetzung zu einem Homomorphismus $\psi\colon L \to \overline{L}$ über K in einen algebraischen Abschluss $\overline{L}$ von L. Da L/K normal ist, erfüllt dieser $\psi(L) = L$, entspricht also einem $\gamma \in \mathrm{Gal}(L/K)$ mit $\gamma|_E = \varphi$. Für dieses gilt insbesondere $\gamma(E) = E'$. Nach Teil (c) des Hauptsatzes der Galoistheorie ist daher ${}^{\gamma}\Delta = \Delta'$.

*5. Sei K ein Körper und sei f ein irreduzibles separables normiertes Polynom in $K[X]$ von geradem Grad $2d$, das *palindromisch* ist, das heisst, die Form

$$f(X) = X^{2d} + a_1 X^{2d-1} + \cdots + a_{d-1} X^{d+1} + a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + 1$$

hat für gewisse $a_1, \ldots, a_d \in K$. Sei L ein Zerfällungskörper von f über K und sei $G := \mathrm{Gal}(L/K)$. Zeige:

   (a) Für jede Nullstelle a von f ist $\frac{1}{a}$ auch eine Nullstelle.

   (b) Die Gruppe G besitzt eine Einbettung in die Untergruppe der symmetrischen Gruppe $S_{2d} = \mathrm{Sym}(\{\pm 1, \ldots, \pm d\})$, die definiert ist durch

$$W_{2,d} := \big\{ \sigma \in S_{2d} \;\big|\; \forall i \in \{1, \ldots, d\} \exists j \in \{1, \ldots, d\} \colon \sigma(\{\pm i\}) = (\{\pm j\}) \big\}.$$

   (c) Es gilt $|G| \leqslant 2^d d!$.

   (d) Im Fall $2d \leqslant 8$ ist G auflösbar.

   Lösung: (a) We can write $f(X) = a_d X^d + \sum_{i=0}^{d-1} a_i (X^{2d-i} + X^i)$, with $a_0 := 1$. Let $Z_P \subset L$ be the set of roots of f. Since $f(0) = 1$, this set does not contain 0. For any $x \in Z_f$ we have $f(x) = 0$ and therefore

$$\begin{aligned} f\left(\frac{1}{x}\right) &= a_d x^{-d} + \sum_{i=0}^{d-1} a_i (x^{-(2d-i)} + x^{-i}) = \frac{1}{x^{2d}} \left(a_d x^{-d} + \sum_{i=0}^{d} a_i (x^i + x^{2d-i}) \right) \\ &= \frac{1}{x^{2d}} f(x) = 0. \end{aligned}$$

Thus the set Z_f is invariant under the inversion map $L^\times \to L^\times$, $x \mapsto \frac{1}{x}$.

(b) The inversion map is its own inverse and has only two fixed points ± 1. Since f is irreducible of degree > 1, none of its roots lies in $\mathbb{Q}$; in particular $\pm 1 \notin Z_f$. We can therefore write $Z_f = \{x_1, x_1^{-1}, \ldots, x_d, x_d^{-1}\}$ with pairwise distinct entries. For any $\sigma \in G$ and any $i \in \{1, \ldots, d\}$ we then have $\sigma(x_i) \in \{x_j, x_j^{-1}\}$ and hence $\sigma(\{x_i, x_i^{-1}\}) = \{x_j, x_j^{-1}\}$ for some $j \in \{1, \ldots, d\}$. Via the evident bijection $\varepsilon i \mapsto x_i^\varepsilon$ between $\{\pm 1, \ldots, \pm d\}$ and $Z_p = \{x_1^{\pm 1}, \ldots, x_d^{\pm 1}\}$, we deduce that the image of the embedding $G \hookrightarrow S_{2d}$ lies inside $W_{2,d}$.

(c) In view of (b) this amounts to checking that $|W_{2,d}| \leqslant 2^d d!$. For this abbreviate $A_i := \{i, -i\}$ for all $1 \leqslant i \leqslant d$. By definition $W_{2,d}$ acts on the set $\{A_1, \ldots, A_d\}$. This action corresponds to a homomorphism $\pi\colon W_{2,d} \to S_d$, $\sigma \mapsto \pi_\sigma$, which is characterized by the formula $\sigma(A_i) = A_{\pi_\sigma i}$ for all i. The kernel of this homomorphism consists of all $\sigma \in S_{2d}$ with $\sigma(A_i) = A_i$ for all $1 \leqslant i \leqslant d$. It is therefore isomorphic to a product of d copies of the group S_2 and hence of order $|S_2|^d = 2^d$. By Lagrange $|W_{2,d}|$ is therefore 2^d times the order of the image of π. Being a subgroup of S_d, this image has order $\leqslant |S_d| = d!$, and the desired bound follows.

(More precisely, let H be the subgroup of all $\sigma \in W_{2,d}$ satisfying $\sigma(\{1, \ldots, d\}) = \{1, \ldots, d\}$. Each such σ must satisfy $\sigma(-i) = -\sigma i$ for all $1 \leqslant i \leqslant d$, so it is completely determined by its restriction to $\{1, \ldots, d\}$, and this restriction is precisely π_σ. Thus π induces an isomorphism $H \xrightarrow{\sim} S_d$. Since the kernel of π is a normal subgroup isomorphic to $S_2^d \cong \{\pm 1\}^d$, we deduce that $W_{2,d}$ is a semidirect product of the form

$$W_{2,d} \;\cong\; \mathrm{Kern}(\pi) \rtimes H \;\cong\; \{\pm 1\}^d \rtimes S_d.$$

In particular we have $|W_{2,d}| = 2^d d!$.)

(d) The kernel of the above homomorphism π is abelian and hence solvable. For $d \leqslant 4$ the group S_d is also solvable. Since subgroups and extensions of solvable groups are solvable, it follows that $W_{2,d}$ is solvable. From (b) it then follows that G is solvable, as desired.

*6. In der Vorlesung wurde der Hauptsatz der Galoistheorie unter Verwendung des Satzes vom primitiven Element bewiesen. Man kann auch umgekehrt vorgehen, wenn man den Hauptsatz der Galoistheorie anders beweist, wie zum Beispiel in Miles Reids Vorlesungsnotizen, Abschnitt 4.3
`http://homepages.warwick.ac.uk/~masda/MA3D5/Galois.pdf`

Dann zeigt man wie in der Vorlesung, dass jede endliche separable Erweiterung nur endlich viele Zwischenkörper hat.

Folgere daraus direkt den Satz vom primitiven Element für jede endliche separable Erweiterung von unendlichen Körpern. (Hinweis: Zeige, dass ein Vektorraum über einem unendlichen Körper keine Vereinigung endlich vieler echter Unterräume sein kann.)

Lösung: Wir zeigen zuerst die Behauptung aus dem Hinweis. Für einen Widerspruchsbeweis nehmen wir an, es gebe einen K-Vektorraum V und echte Unterräume V_i mit $\bigcup_{i=1}^{n} V_i = V$. Unter allen Gegenbeispielen wählen wir eines mit n minimal. Wegen $0 \in V$ ist dann jedenfalls $n \geqslant 1$. Wegen der Minimalität existiert ein $v \in V \smallsetminus \bigcup_{i=1}^{n-1} V_i$, das folglich in V_n liegen muss. Betrachte weiter ein $w \in V \smallsetminus V_n$. Nach Annahme gibt es für jedes $x \in K$ ein i mit $v + xw \in V_i$. Wegen $|K| = \infty$ gibt es folglich ein i_0 und $x_0 \neq y_0 \in K$, sodass $v + x_0 w$ und $v + y_0 w$ in V_{i_0} liegen. Dann muss V_{i_0} auch die Differenz $v + x_0 - (v + y_0 w) = (x_0 - y_0)w$, deren skalares Vielfaches w und $v = v + x_0 w - x_0 w$ enthalten. Das ist ein Widerspruch zur Wahl von v.

Sei nun L/K eine endliche separable Körpererweiterung. Dann ist L die Vereinigung der Zwischenkörper $K(x)$ für alle $x \in L$. Da L/K nur endlich viele Zwischenkörper hat, ist diese Vereinigung in Wirklichkeit schon endlich. Nach der obigen Behauptung muss folglich einer dieser Unterkörper $K(x)$ gleich L sein.