Algebra I

Musterlösung 20

Hauptsatz der Galoistheorie, Konstruktionen mit Zirkel und Lineal

---

120. Führe das Beispiel der Galoisgruppe von $X^6 - 2X^3 - 1$ über $\mathbb{Q}$ aus der Vorlesung zu Ende.

Lösung: Sei $\zeta = \frac{-1+i\sqrt{3}}{2}$ die primitive dritte Einheitswurzel im zweiten Quadranten. Sei $\alpha = 1+\sqrt{2}$ und $\beta = \sqrt[3]{\alpha} > 0$. Wegen $(1+\sqrt{2})(1-\sqrt{2}) = -1$ sind die Nullstellen des Polynoms gleich $\beta, \zeta\beta, \bar{\zeta}\beta, -\frac{1}{\beta}, -\zeta\frac{1}{\beta}, -\bar{\zeta}\frac{1}{\beta}$. Wir wollen zeigen, dass das Polynom irreduzibel über $\mathbb{Q}$ ist. Da es keine rationalen Nullstellen hat, müsste eine Zerlegung einen Faktor vom Grad 2 oder 3 haben. Wir wissen, dass nicht-reelle Nullstellen immer in komplex konjugierten Paaren auftauchen. Durch Ausprobieren aller Möglichkeiten sehen wir, dass $X^6 - 2X^3 - 1$ tatsächlich irreduzibel ist.

Sei L der Zerfällungskörper des Polynoms über $\mathbb{Q}$. Dann ist

$$L = \mathbb{Q}(\zeta, \beta) = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{1+\sqrt{2}}).$$

Offensichtlich ist $i\sqrt{3} \notin \mathbb{Q}(\beta) \subset \mathbb{R}$, und wir bekommen $[L : \mathbb{Q}] = 12 = |\operatorname{Gal}(L : \mathbb{Q})|$.

Die Erweiterung $\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}$ ist normal mit Galoisgruppe C_2, also ist

$$C_2 \cong \operatorname{Gal}(\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}) \cong \operatorname{Gal}(L : \mathbb{Q})/\operatorname{Gal}(L : \mathbb{Q}(i\sqrt{3})).$$

Weiter ist $\operatorname{Gal}(L : \mathbb{Q}(i\sqrt{3}))$ eine Untergruppe von $\operatorname{Gal}(L : \mathbb{Q})$, die Ordnung 6 hat und transitiv auf den 6 Nullstellen wirkt. Ausserdem ist jedes ihrer Elemente eindeutig durch das Bild von β bestimmt. Durch Ausprobieren erkennen wir, dass die Elemente mit $\beta \mapsto -\frac{1}{\beta}$ und $\beta \mapsto -\frac{\zeta}{\beta}$ beide Ordnung 2 haben. Daher kann $\operatorname{Gal}(L : \mathbb{Q}(i\sqrt{3}))$ nicht isomorph zu C_6 sein, ist also isomorph zu S_3. Offensichtlich enthält sie die komplexe Konjugation σ nicht, und der Fixkörper der komplexen Konjugation ist nicht normal in L. Somit ist $\operatorname{Gal}(L : \mathbb{Q})$ ein nichttriviales semidirektes Produkt von $\langle\sigma\rangle \cong C_2$ und $\operatorname{Gal}(L : \mathbb{Q}(i\sqrt{3})) \cong S_3$. Nun müssen wir die Automorphismengruppe von S_3 bestimmen. Ein Element der Automorphismengruppe permutiert offensichtlich die drei Transpositionen und ist durch eine solche Permutation eindeutig definiert, und man sieht (z.B. durch Konjugation mit geeigneten Elementen), dass alle Möglichkeiten tatsächlich existieren. Das Bild eines nichttrivialen Homomorphismus $C_2 \to S_3$ ist ausserdem eine Untergruppe, die durch eine Transposition erzeugt wird. Es gibt also bis auf Isomorphie nur ein nichttriviales semidirektes Produkt. Dieses ist isomorph zu D_6, denn wir können D_3 als so ein Produkt schreiben, z.B. als $\langle\rho^3\rangle \ltimes \langle\sigma, \rho^2\rangle$ mit σ, ρ wie in der nachfolgendne Aufgabe. Also gilt

$$\operatorname{Gal}(L : \mathbb{Q}) \cong D_6.$$

Da die komplexe Konjugation ein Element der Ordnung 2 mit zwei Fixpunkten ist, muss es sich dabei um eine Spiegelung handeln. Jedes Element aus $\operatorname{Gal}(L : \mathbb{Q})$ permutiert bildet $i\sqrt{3}$ auf eine Nullstellen seines Minimalpolyonms $X^3 + 2$ über $\mathbb{Q}$ ab, analog β auf eine Nullstellen von $X^6 - 2X^3 - 1$. Das gibt insgesamt $2 \cdot 6 = 12$ Möglichkeiten. Eine jede solche bestimmt ein Element aus $\operatorname{Gal}(L : \mathbb{Q})$ eindeutig; wegen $|\operatorname{Gal}(L : \mathbb{Q})| = 12$ müssen

alle diese Möglichkeiten auch existieren. Sei ρ definiert durch $\rho(i\sqrt{3}) = -i\sqrt{3}$ und $\rho(\beta) = \bar{\zeta}\sqrt[3]{1-\sqrt{2}} = \frac{-\bar{\zeta}}{\beta}$ die Nullstelle von $X^6 - 2X^3 - 1$ im 1. Quadranten. Wir können schnell überprüfen, dass ρ Ordnung 6 hat und $\rho\sigma\rho = \sigma$ gilt, also entspricht ρ einer Drehung. Der Rest der Lösung funktioniert nun ähnlich wie in der nächsten Aufgabe.

Variante: Ein Element σ aus $\mathrm{Gal}(L : \mathbb{Q})$ ist bestimmt, wenn wir die Bilder von β und ζ kennen. Hierbei gibt es für $\sigma(\beta)$ genau sechs Möglichkeiten und für $\sigma(\zeta)$ genau zwei Möglichkeiten, da die Bilder unter σ dasselbe Minimalpolynom über $\mathbb{Q}$ haben müssen. Wegen $[L : \mathbb{Q}] = |\mathrm{Gal}(L : \mathbb{Q})| = 12$ existieren alle diese 12 Möglichkeiten auch tatsächlich.

Ist zum Beispiel $\sigma(\beta) = -\zeta\frac{1}{\beta}$, dann ist $\sigma(-\frac{1}{\beta}) = \bar{\zeta}\beta$, denn $-1 = \sigma(-1) = \sigma(\beta \cdot -\frac{1}{\beta}) = \sigma(\beta \cdot -\frac{1}{\beta}) = \sigma(\beta) \cdot \sigma(-\frac{1}{\beta}) = -\zeta\frac{1}{\beta} \cdot \bar{\zeta}\beta$.

Für $\sigma(\beta) = -\zeta\frac{1}{\beta}$ und $\sigma(\zeta) = \bar{\zeta}$ gilt

$$\beta \overset{\sigma}{\longmapsto} -\zeta\tfrac{1}{\beta} \overset{\sigma}{\longmapsto} \zeta\beta \overset{\sigma}{\longmapsto} -\tfrac{1}{\beta} \overset{\sigma}{\longmapsto} \bar{\zeta}\beta \overset{\sigma}{\longmapsto} -\bar{\zeta}\tfrac{1}{\beta} \overset{\sigma}{\longmapsto} \beta\,.$$

Somit hat σ die Ordnung 6, erzeugt also eine Untergruppe der Ordnung 6 von $\mathrm{Gal}(L : \mathbb{Q})$. Da diese Index 2 hat, ist sie normal.

Für $\tau(\beta) = \beta$ und $\tau(\zeta) = \bar{\zeta}$ gilt

$$\beta - \tfrac{1}{\beta} \overset{\tau}{\longmapsto} \beta - \tfrac{1}{\beta}\,, \quad \zeta\beta - \bar{\zeta}\tfrac{1}{\beta} \overset{\tau}{\longmapsto} \bar{\zeta}\beta - \zeta\tfrac{1}{\beta}\,, \quad \bar{\zeta}\beta - \zeta\tfrac{1}{\beta} \overset{\tau}{\longmapsto} \zeta\beta - \bar{\zeta}\tfrac{1}{\beta}\,.$$

Somit hat τ die Ordnung 2.

Seien $\gamma_0 := \beta - \frac{1}{\beta}$, $\gamma_1 := \zeta\beta - \bar{\zeta}\frac{1}{\beta}$ und $\gamma_2 := \bar{\zeta}\beta - \zeta\frac{1}{\beta}$. Das Minimalpolynom von $\gamma_0, \gamma_1, \gamma_2$ ist $X^3 + 3X - 2$ mit Zerfällungskörper $M := \mathbb{Q}(\gamma_0, \gamma_1, \gamma_2)$. Da von diesen drei Zahlen genau eine reell ist, ist $\mathrm{Gal}(M : \mathbb{Q}) \cong S_3 \cong D_3$.

121. 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 $1 \leq i \leq 6$ 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 $1 \leq i \leq 6$ 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.

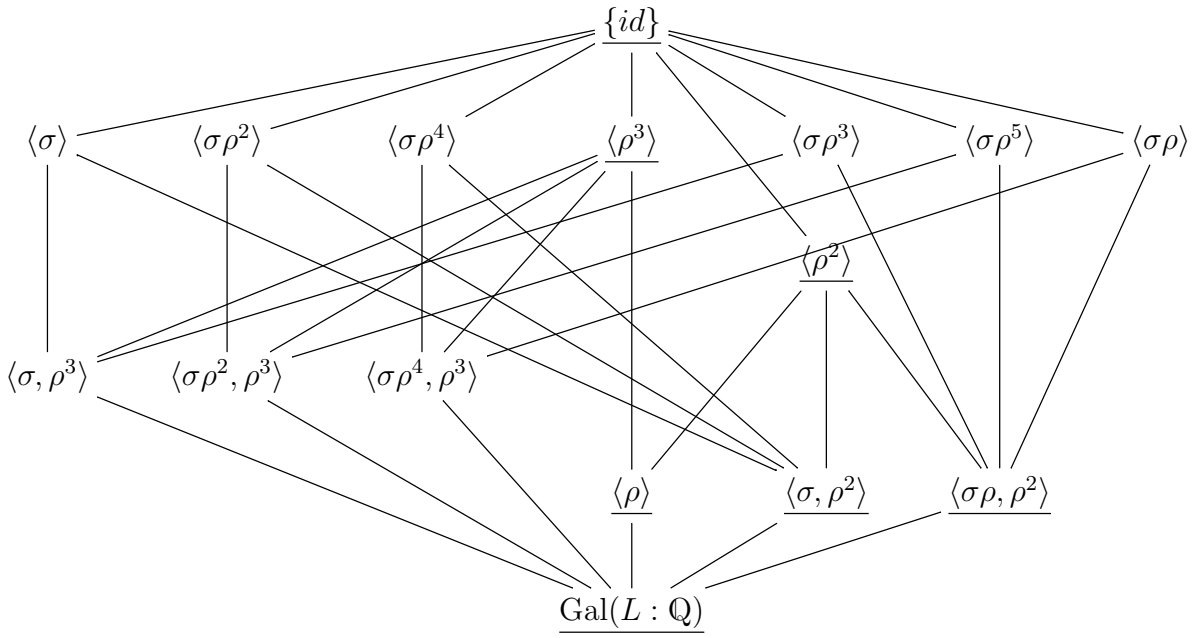
Wir fassen im Folgenden $\mathrm{Gal}(L : \mathbb{Q})$ durch die durch $a_i \mapsto i$ induzierte Einbettung als Untergruppe von S_6 auf.

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, wegen $|D_6| = 12 = |\operatorname{Gal}(L:\mathbb{Q})|$, dass die von ρ und σ erzeugte Untergruppe tatsächlich isomorph zu D_6 ist.

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:



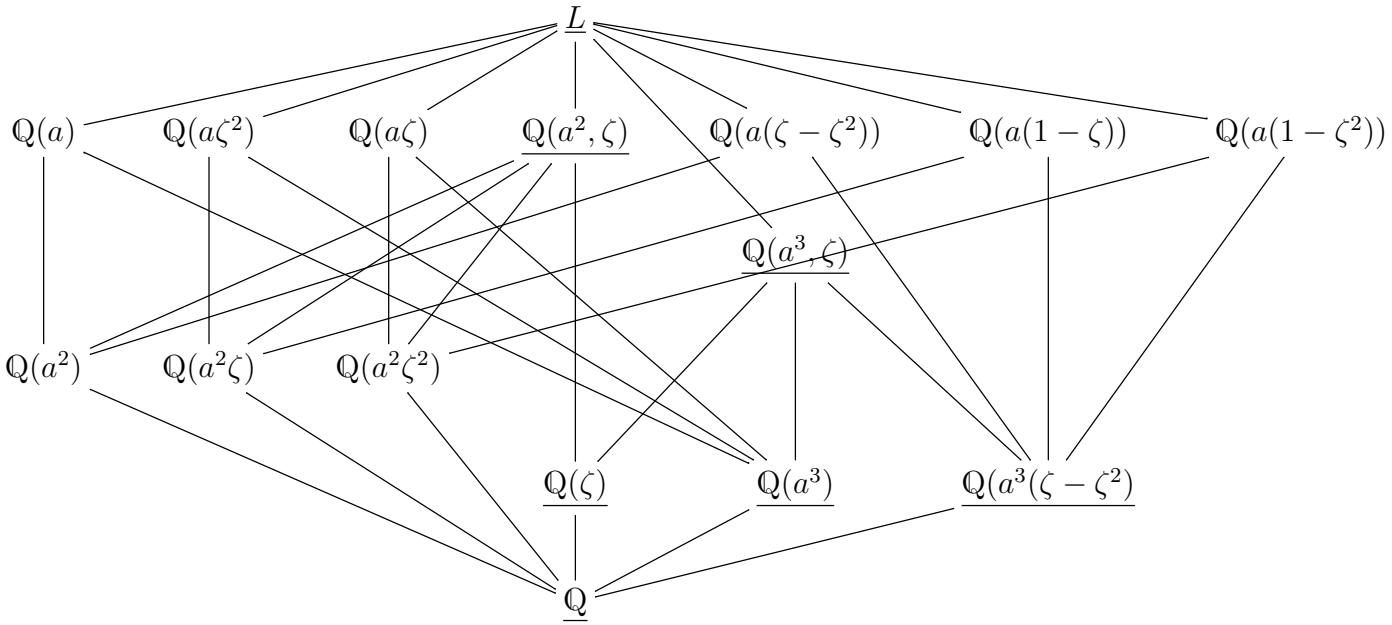
Daraus folgern wir nun die Aufstellung der Zwischenkörper; die Galois-Korrespondenz ordnet einer Untergruppe $H < \operatorname{Gal}(L:\mathbb{Q})$ den Fixkörper L^H mit dem Erweiterungsgrad $[L^H:\mathbb{Q}] = \frac{|\operatorname{Gal}(L:\mathbb{Q})|}{|H|} = \frac{12}{|H|}$ zu:

- $L^{\{\}} = L$.
- $L^{\operatorname{Gal}(L:\mathbb{Q})} = \mathbb{Q}$.
- 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 $(\sigma\rho^3)^2 = id_L$; 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 $(\sigma\rho^5)^2 = id_L$; 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 $(\sigma\rho)^2 = id_L$; 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:

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

122. 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 $\gamma\Delta\gamma^{-1} = \Delta'$. Dann ist $\gamma(E) = E'$. 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 $\gamma(E) = E'$. Daher ist $\gamma\Delta\gamma^{-1} = \Delta'$.

123. Zeige oder widerlege: Es existiert eine Körpererweiterung mit genau $50'000$ echten Zwischenkörpern.

Lösung: Für jede natürliche Zahl n existiert eine zyklische Körpererweiterung vom Grad n, zum Beispiel eine Erweiterung $\mathbb{F}_{p^n} : \mathbb{F}_p$ vom Grad n für p prim, oder die Erweiterung $\mathbb{C}(X) : \mathbb{C}(X^n)$. Nach dem Hauptsatz der Galoistheorie ist die Anzahl der Zwischenkörper dann gleich der Anzahl der Untergruppen einer zyklischen Gruppe der Ordnung n, also gleich der Anzahl der Teiler von n. Für die echten Zwischenkörper sind die Teiler 1 und n wegzulassen, also suchen wir eine ganze Zahl $n > 1$ mit genau $50'002$ Teilern. Ein Beispiel hierfür ist $n = r^{50'001}$ für eine Primzahl r, oder $k = r_1 r_2^{25'000}$ für Primzahlen r_1, r_2, oder $k = r_1 r_2^{22} r_3^{1086}$ für Primzahlen r_1, r_2, r_3.

124. In dieser Aufgabe beweisen wir den Fundamentalsatz der Algebra mit Hilfe der Galoistheorie. Sei $K : \mathbb{R}$ eine endliche Körpererweiterung.

(a) Nimm an, $K : \mathbb{R}$ sei galoissch. Zeige, dass ein Körperturm $K = K_n : \ldots : K_0 : \mathbb{R}$ existiert, sodass $[K_0 : \mathbb{R}]$ ungerade ist und für jedes $0 \leq i \leq n-1$ die Erweiterung $K_{i+1} : K_i$ den Grad 2 hat.

(b) Zeige, dass $\mathbb{R}$ keine nichttriviale Erweiterung von ungeradem Grad hat.

(c) Zeige, dass jede Erweiterung von $\mathbb{R}$ vom Grad 2 isomorph zu $\mathbb{C}$ ist.

(d) Zeige, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 hat.

(e) Folgere, dass K entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

Lösung: (a) Set $G := \mathrm{Gal}(K : \mathbb{R})$. Write $|G| = 2^n m$, where m is an odd natural number. By Sylow, there exists a subgroup $G_0 < G$ of order $|G_0| = 2^n$. By the Galois correspondence, there is then an intermediate field K_0 such that

$$[K_0 : \mathbb{R}] = [G : G_0] = m = \text{odd}.$$

Now repeat the process with the subgroup G_0. Since G_0 is a p-group for $p = 2$, there exists a chain of normal subgroups $1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0$ such that each G_l has order 2^{n-l}. By the

Galois correspondence, it corresponds to a chain of intermediate fields $K = K_n \supset \ldots \supset K_0$ with $[K_{i+1} : K_i] = 2$.

(b) Suppose that $[K : \mathbb{R}]$ is odd. Take any element $\alpha \in K$ and let $f \in \mathbb{R}[X]$ be its minimal polynomial over $\mathbb{R}$. Then $\deg(f) = [\mathbb{R}(\alpha) : \mathbb{R}]$ divides $[K : \mathbb{R}]$ and is therefore also odd. By the Intermediate Value Theorem f then has a zero $\beta \in \mathbb{R}$. Thus $(X - \beta)$ divides f in $\mathbb{R}[X]$; but since f is already irreducible over $\mathbb{R}$ by assumption, we must have $f(X) = X - \beta$. Thus $\alpha = \beta \in \mathbb{R}$. This shows that every element of K already lies in $\mathbb{R}$; hence $K = \mathbb{R}$.

(c) If $[K : \mathbb{R}] = 2$, we have $K = \mathbb{R}(\alpha)$ for some element $\alpha \in K \setminus \mathbb{R}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{R}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. As this is irreducible over $\mathbb{R}$, we must have $\alpha^2 < 0$, because otherwise it would have a real zero. Let β be the positive real square root of $|\alpha^2|$. Then $K = \mathbb{R}(\alpha) = \mathbb{R}(\frac{\alpha}{\beta})$ with $(\frac{\alpha}{\beta})^2 = \frac{\alpha^2}{\beta^2} = -1$. Thus $K \cong \mathbb{C}$ over $\mathbb{R}$ with $\frac{\alpha}{\beta} \leftrightsquigarrow i$.

(d) If $[K : \mathbb{C}] = 2$, we have $K = \mathbb{C}(\alpha)$ for some element $\alpha \in K \setminus \mathbb{C}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{C}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. But every complex number has a square root in $\mathbb{C}$; so this polynomial is reducible over $\mathbb{C}$; contradiction.

(e) Suppose first that $K : \mathbb{R}$ is Galois, and let $K = K_n : \ldots : K_0 : \mathbb{R}$ be as in (a). Then $K_0 = \mathbb{R}$ by (b). If $n = 0$, it follows that $K = \mathbb{R}$. Otherwise (c) implies that $K_1 \cong \mathbb{C}$, and (d) implies by induction that $K_i = K_1$ for all $1 \leq i \leq n$. Thus $K = K_n \cong \mathbb{C}$.

For general K let L be a Galois closure of $K : \mathbb{R}$. Then the preceding case shows that $L \cong \mathbb{R}$ or $\mathbb{C}$; hence the same follows for K.

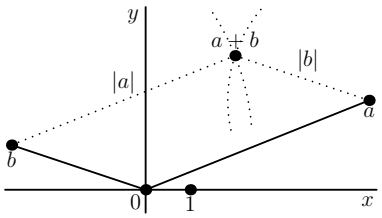
125. Diese Aufgabe ist eher informell, die auftretenden Begriffe werden später in der Vorlesung formal definiert werden. Wir identifizieren die Ebene mit $\mathbb{C}$ und nehmen die Punkte 0 und 1 als gegeben (d.h. bereits konstruiert) an.

Zeige: Die Menge aller Zahlen (*bzw.* Punkte), die mit Zirkel und Lineal konstruierbar sind, bilden einen Unterkörper von $\mathbb{C}$, der abgeschlossen ist unter komplexer Konjugation und Quadratwurzelbildung.

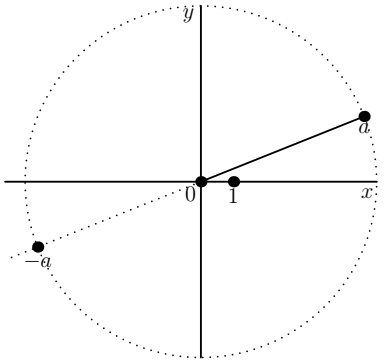
Erinnerung: Mit Zirkel und Lineal sind folgende Punkte, Geraden und Kreise konstruierbar.

- Sind A und B zwei verschiedene konstruierbare Punkte, so ist auch die Gerade durch A und B konstruierbar.
- Sind M, A und B konstruierbare Punkte mit $A \neq B$, so ist auch der Kreis mit Mittelpunkt M und Radius $\overline{AB}$ konstruierbar.
- Sind g_1 und g_2 zwei verschiedene konstruierbare Geraden, so ist auch der Schnittpunkt von g_1 und g_2 konstruierbar (falls er existiert).
- Ist g eine konstruierbare Geraden und k ein konstruierbarer Kreis, so sind auch die Schnittpunkte von g mit k konstruierbar (falls solche existieren).
- Sind k_1 und k_2 konstruierbare Kreise, so sind auch die Schnittpunkte von k_1 und k_2 konstruierbar (falls solche existieren).

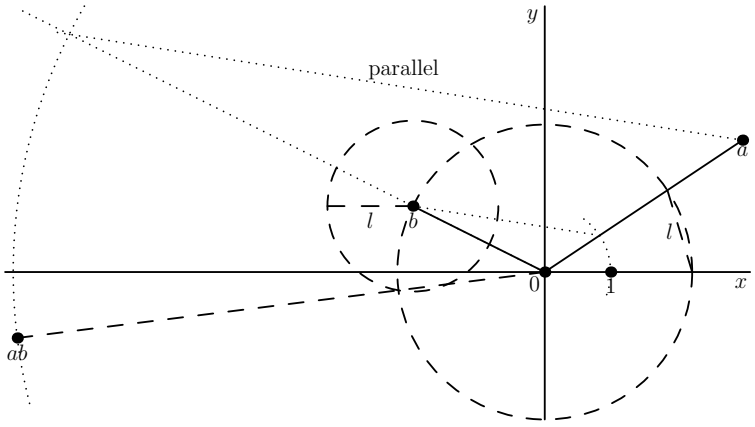
Lösung: Nach Definition sind 0 und 1 konstruierbar. Falls a und b konstruierbar sind, so ist auch $a + b$ konstruierbar:



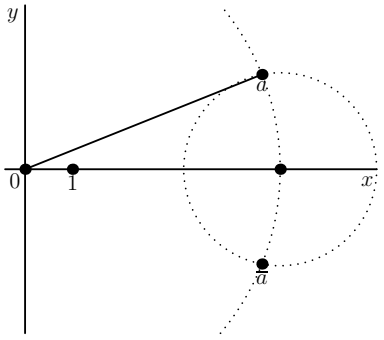
Falls a konstruierbar ist, so ist auch $-a$ konstruierbar:



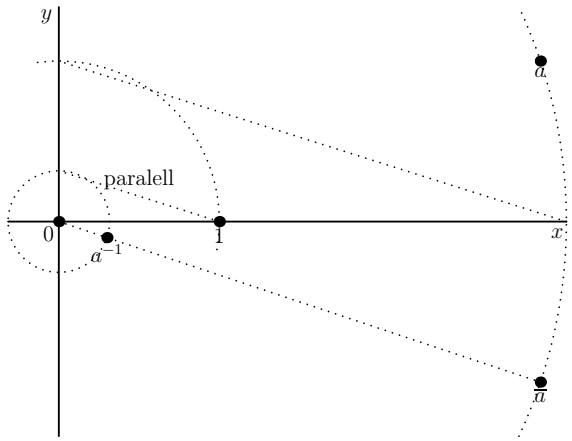
Falls a und b konstruierbar sind, so ist auch ab konstruierbar: Hier setzen wir voraus, dass bekannt ist, dass man zu einer gegebenen Geraden (hier: die durch b und den Punkt $a/|a|$) eine Parallele durch einen gegebenen Punkt (hier: a) konstruieren kann. In der Zeichnung werden die gestrichelten Linien benutzt, um den richtigen Winkel für ab zu bekommen, und die gepunkteten für die Länge. Für die Länge benutzen wir den Strahlensatz.



Falls a konstruierbar ist, so ist auch a^{-1} konstruierbar: Hier benutzen wir zuerst: Falls a konstruierbar ist, so ist auch $\overline{a}$ konstruierbar:



Und nun zu a^{-1}: Wir benutzen wieder den Strahlensatz.



Somit ist die Menge der Konstruierbaren Punkte ein Körper, der abgeschlossen unter komplexer Konjugation ist.

Es bleibt zu zeigen: Falls a konstruierbar ist, so ist auch $\pm\sqrt{a}$ konstruierbar: Das $\pm$ soll darauf hinweisen, dass in den komplexen Zahlen keine klare Definition einer Quadratwurzel existiert; man könnte den hier konstruierten Punkt als $\sqrt{2}$ oder $-\sqrt{2}$ bezeichnen. Hier sind wieder die gestrichelten Linien für den Winkel und die gepunkteten für den Betrag. Wir benutzen den Satz von Thales und, dass ein rechtwinkeliges Dreieck, in dem die Höhe die Hypothenuse in Abschnitte der Länge r und 1 unterteilt, Höhe $\sqrt{r}$ hat.