

## Musterlösung Serie 24

### HAUPTSATZ DER GALOISTHEORIE II

---

**119.** Sei  $L$  ein Zerfällungskörper des Polynoms  $X^6 - 5$  über  $\mathbb{Q}$ .

Bestimmen Sie alle Zwischenkörper von  $L : \mathbb{Q}$  mitsamt Inklusionen sowie, falls die Körpererweiterung Galois über  $\mathbb{Q}$  ist, deren Galoisgruppe 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  $\zeta$  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  $a_1, \dots, a_6$  gerade die sechs verschiedenen Nullstellen von  $X^6 - 5$ . Somit ist  $L = \mathbb{Q}(a_1, \dots, a_6) \subset \mathbb{Q}(a, \zeta)$ , 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  $\text{Gal}(L : \mathbb{Q})$  Ordnung 12.

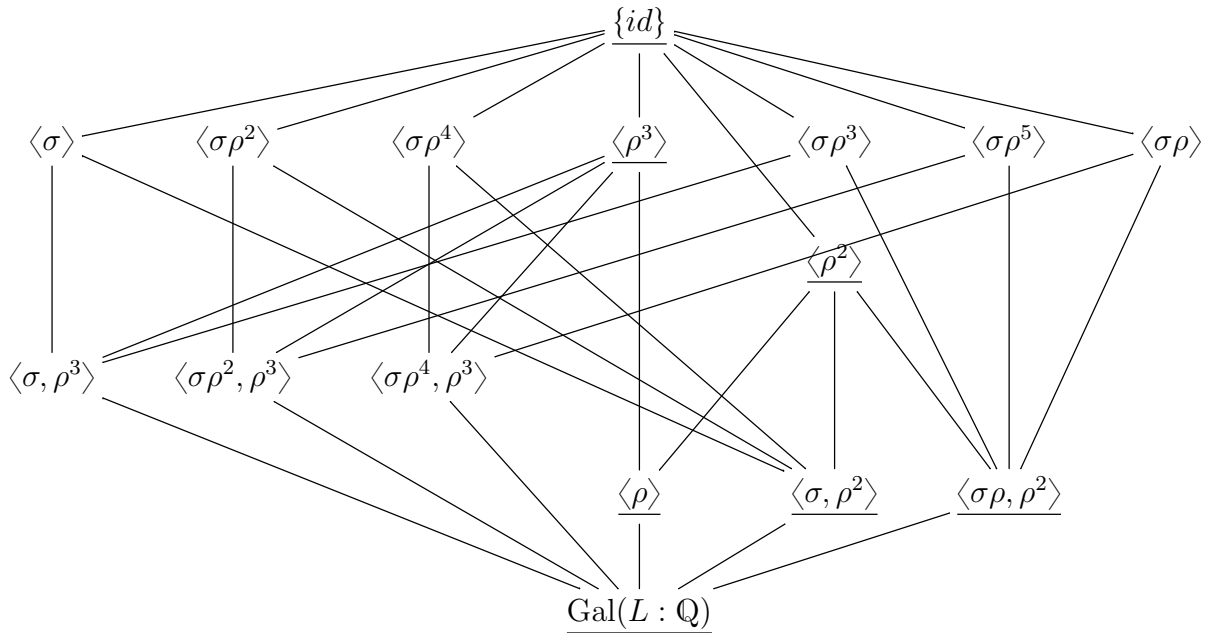
Wir fassen im Folgenden  $\text{Gal}(L : \mathbb{Q})$  durch die durch  $a_i \mapsto i$  induzierte Einbettung als Untergruppe von  $S_6$  auf.

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

Da  $X^6 - 5$  irreduzibel ist, operiert  $\text{Gal}(L : \mathbb{Q})$  transitiv auf dessen Nullstellen; es existiert also ein  $\rho \in \text{Gal}(L : \mathbb{Q})$  mit  $\rho(a_1) = a_2$ . Wegen  $\sigma(a_1) = a_1$  gilt auch  $(\rho\sigma)(a_1) = a_2$ . Da  $\sigma$  die beiden Nullstellen  $\zeta$  und  $\zeta^2$  des irreduziblen Polynoms  $X^2 + X + 1$  vertauscht und  $\rho$  sie als  $\mathbb{Q}$ -Homomorphismus vertauscht oder fix lässt, können wir also (indem wir allenfalls  $\rho$  durch  $\rho\sigma$  ersetzen) ohne Beschränkung der Allgemeinheit annehmen, dass  $\rho(\zeta) = \zeta$  ist. Dann ist  $\rho(a_i) = \rho(a \cdot (-\zeta)^{i-1}) = a \cdot (-\zeta)^i$ , also hat  $\rho$  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  $|D_6| = 12 = |\text{Gal}(L : \mathbb{Q})|$ , dass die von  $\rho$  und  $\sigma$  erzeugte Untergruppe tatsächlich isomorph zu  $D_6$  ist.

Auf der nächsten Seite ist eine Aufstellung aller Untergruppen von  $\text{Gal}(L : \mathbb{Q}) \cong D_6$  (die detaillierte Überprüfung lassen wir hier weg); normale Untergruppen sind unterstrichen:



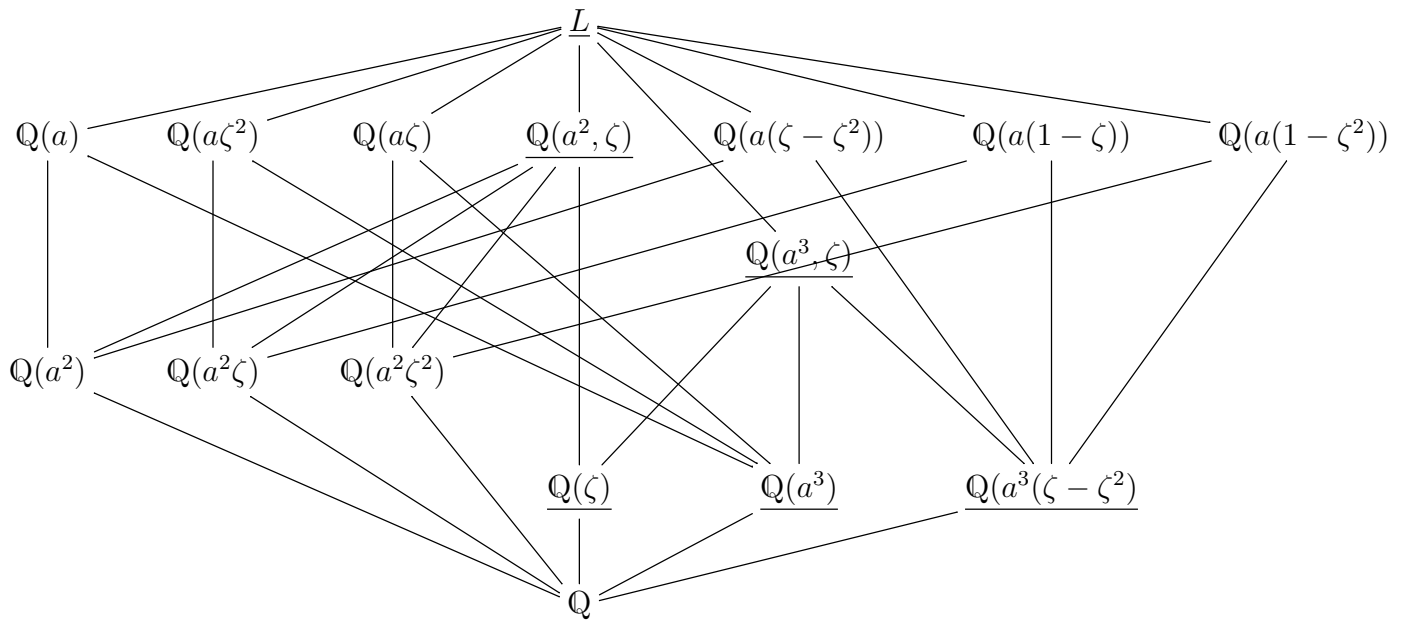
Daraus folgern wir nun die Aufstellung der Zwischenkörper; die Galois-Korrespondenz ordnet einer Untergruppe  $H < \text{Gal}(L : \mathbb{Q})$  den Fixkörper  $L^H$  mit dem Erweiterungsgrad  $[L^H : \mathbb{Q}] = \frac{|\text{Gal}(L:\mathbb{Q})|}{|H|} = \frac{12}{|H|}$  zu:

- $L^{\{ \}} = L$ .
- $L^{\text{Gal}(L:\mathbb{Q})} = \mathbb{Q}$ .
- 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  $\text{Gal}(L : \mathbb{Q})$  zu einander konjugiert sind. Sind nämlich zwei Untergruppen  $H, H'$  unter  $\varphi$  konjugiert, so ist  $L^{H'} = \varphi(L^H)$ .

Insgesamt ergibt sich die folgende Aufstellung:



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

$$\text{Gal}(\mathbb{Q}(a^2, \zeta) : \mathbb{Q}) \cong D_3,$$

$$\text{Gal}(\mathbb{Q}(a^3, \zeta) : \mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

$$\text{Gal}(\mathbb{Q}(a^3) : \mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(a^3(\zeta - \zeta^2)) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$