# Musterlösung Serie 24

## Galoiserweiterungen, Galoisgruppen

1. 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 $\gamma$ 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 $\varphi$ 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 ${}^{\gamma}\Delta = \Delta'$.

2. Sei $L/K$ eine endliche Galoiserweiterung mit Zwischenkörpern $K_1$ und $K_2$ und den entsprechenden Galoisgruppen $\Gamma_i := \mathrm{Gal}(L/K_i) \leqslant \Gamma := \mathrm{Gal}(L/K)$. Zeige:

   (a) $K_1K_2 = L^{\Gamma_1 \cap \Gamma_2}$,

   (b) $K_1 \cap K_2 = L^{\langle \Gamma_1, \Gamma_2 \rangle}$, wobei $\langle \Gamma_1, \Gamma_2 \rangle$ die von $\Gamma_1$ und $\Gamma_2$ erzeugte Untergruppe von $\Gamma$ bezeichnet.

   (c) Gilt $K_1K_2 = L$ und $K_1 \cap K_2 = K$ und sind $K_1/K$ und $K_2/K$ beide galoissch, so ist $\mathrm{Gal}(L/K) \cong \Gamma_1 \times \Gamma_2$.

   *Lösung*: (a) Die Gruppe $\Gamma_1 \cap \Gamma_2$ operiert trivial auf $K_1$ und $K_2$ und daher auch auf dem Zwischenkörper $K_1K_2$, mit anderen Worten gilt $K_1K_2 \subset L^{\Gamma_1 \cap \Gamma_2}$. Andererseits ist $\mathrm{Gal}(L/K_1K_2) < \mathrm{Gal}(L/K_i) = \Gamma_i$ für $i = 1, 2$, also gilt $\mathrm{Gal}(L/K_1K_2) < \Gamma_1 \cap \Gamma_2$. Nach dem Hauptsatz der Galoistheorie folgt daraus $K_1K_2 \supset L^{\Gamma_1 \cap \Gamma_2}$.

   (b) Jede der Untergruppen $\Gamma_1$ und $\Gamma_2$ operiert trivial auf $K_1 \cap K_2$, also tut dies auch die Untergruppe $\langle \Gamma_1, \Gamma_2 \rangle$, mit anderen Worten gilt $K_1 \cap K_2 \subset L^{\langle \Gamma_1, \Gamma_2 \rangle}$. Auf der anderen Seite gilt $L^{\langle \Gamma_1, \Gamma_2 \rangle} \subset L^{\Gamma_i} = K_i$ für $i = 1, 2$, und daher $K_1 \cap K_2 \supset L^{\langle \Gamma_1, \Gamma_2 \rangle}$.

   (c) Wir benutzen verschiedene Teile des Hauptsatzes der Galoistheorie. Zuerst ist jedes $K_i/K$ galoissch und daher $\Gamma_i \lhd \Gamma$. Insbesondere ist $\langle \Gamma_1, \Gamma_2 \rangle = \Gamma_1\Gamma_2$. Nach Annahme und (b) gilt nun aber $K = K_1 \cap K_2 = L^{\Gamma_1\Gamma_2}$, und daraus folgt $\Gamma_1\Gamma_2 = \Gamma$. Schliesslich gilt nach Annahme und (a) auch $L = K_1K_2 = L^{\Gamma_1 \cap \Gamma_2}$, und daher $\Gamma_1 \cap \Gamma_2 = 1$. Nach Abschnitt 5.5 der Vorlesung folgt daraus, dass $\Gamma_1 \times \Gamma_2 \to \Gamma$, $(\gamma_1, \gamma_2) \mapsto \gamma_1\gamma_2$ ein Gruppenisomorphismus ist.

3. Sei $f \in K[X]$ irreduzibel und separabel und sei $L$ ein Zerfällungskörper von $f$ über $K$. Zeige: Ist $\mathrm{Gal}(L/K)$ abelsch, so ist $L = K(a)$ für eine beliebige Nullstelle $a \in L$ von $f$.

   *Lösung*: Als Zerfällungskörper eines separablen Polynoms ist $L/K$ galoissch. Da $f$ irreduzibel ist, operiert $\mathrm{Gal}(L/K)$ transitiv auf der Menge der Nullstellen von $f$ nach Proposition 7.2.5 der Vorlesung.

   Für jede Nullstelle $a$ von $f$ ist $L/K(a)$ galoissch, und $\mathrm{Gal}(L/K(a))$ ist die Untergruppe aller $\gamma \in \mathrm{Gal}(L/K)$ mit $\gamma|_{K(a)} = \mathrm{id}_{K(a)}$, oder äquivalent $\gamma(a) = a$. Für jede zweite Nullstelle $a'$ von $f$ wähle ein $\delta \in \mathrm{Gal}(L/K)$ mit $\delta(a) = a'$. Da $\mathrm{Gal}(L/K)$ abelsch ist, gilt für jedes $\gamma \in \mathrm{Gal}(L/K(a))$ dann $\gamma \circ \delta = \delta \circ \gamma$ und folglich $\gamma(a') = \gamma(\delta(a)) = \delta(\gamma(a)) = \delta(a) = a'$. Variieren wir $a'$, so sehen wir also, dass $\gamma$ jede Nullstelle von $f$ auf sich abbildet. Da $L$ aber von diesen Nullstellen über $K$ erzeugt wird, ist $\gamma$ auf ganz $L$ die Identität. Also ist $\mathrm{Gal}(L/K(a))$ die triviale Untergruppe von $\mathrm{Gal}(L/K)$. Wegen $|\mathrm{Gal}(L/K(a))| = [L/K(a)]$ folgt also $[L/K(a)] = 1$ und somit $L = K(a)$.

4. Sei $L$ ein Zerfällungskörper des Polynoms $X^4 + 1$ 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 $L$ in $\mathbb{C}$ realisieren. Betrachte also die primitive 8-te Einheitswurzel $\zeta := e^{\pi i/4} = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$. Dann hat das Polynom $X^4 + 1$ genau die 4 verschiedenen Nullstellen $\zeta^{\pm 1}$ und $\zeta^{\pm 3}$ und den Zerfällungskörper $L = \mathbb{Q}(\zeta)$. Wegen $\zeta^2 = i$ ist dann $L = \mathbb{Q}(i, \sqrt{2})$ und enthält die beiden Unterkörper $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$, die beide vom Grad 2 über $\mathbb{Q}$ sind. Da diese einander nicht enthalten, folgt $[L/\mathbb{Q}(\sqrt{2})] = 2$ und somit $[L/\mathbb{Q}] = 4$.

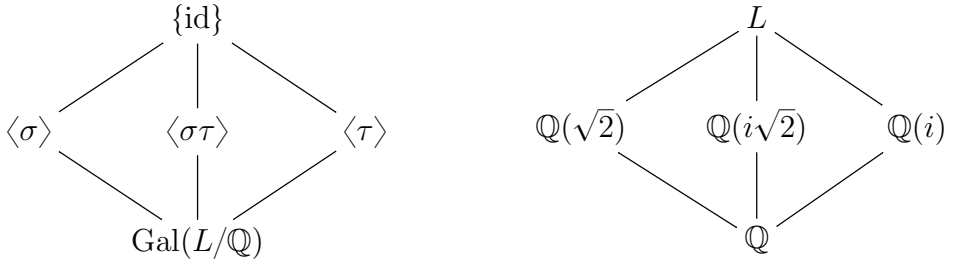
   Als normale Erweiterung von Körpern der Charakteristik Null ist $L/\mathbb{Q}$ galoissch. Ihre Galoisgruppe $\Gamma := \mathrm{Gal}(L/\mathbb{Q})$ hat daher die Ordnung 4. Wegen $L = \mathbb{Q}(\zeta)$ ist jedes Element davon schon durch das Bild von $\zeta$ bestimmt. Also operiert $\Gamma$ transitiv auf der Menge der Nullstellen $\{\zeta^{\pm 1}, \zeta^{\pm 3}\}$. Betrachte Elemente $\sigma, \tau \in \Gamma$ mit $\sigma(\zeta) = \zeta^{-1}$ und $\tau(\zeta) = \zeta^5$. Wegen $(-1)^2 \equiv 5^2 \equiv 1 \bmod (8)$ gilt dann $\sigma^2(\zeta) = \tau^2(\zeta) = \zeta$ und folglich $\sigma^2 = \tau^2 = 1$. Somit ist $\Gamma$ ein Produkt zweier zyklischer Gruppen der Ordnung 2 und besitzt neben der trivialen Untergruppe und sich selbst nur noch die drei Untergruppen $\langle\sigma\rangle$ und $\langle\tau\rangle$ und $\langle\sigma\tau\rangle$ der Ordnung 2.

   In der Galoiskorrespondenz entspricht die triviale Untergruppe dem grössten Zwischenkörper $L$ und die ganze Gruppe $\Gamma$ dem kleinsten Zwischenkörper $\mathbb{Q}$. Die drei Untergruppen vom Index 2 entsprechen Zwischenkörpern vom Grad 2 über $\mathbb{Q}$. Zwei solche kennen wir bereits.

   - Wegen $\tau(i) = \tau(\zeta^2) = \zeta^{10} = \zeta^2 = i$ operiert $\tau$ trivial auf dem Zwischenkörper $\mathbb{Q}(i)$. Also gilt $\mathbb{Q}(i) \subset L^{\langle\tau\rangle}$. Da diese Körper aber denselben Grad 2 über $\mathbb{Q}$ haben, müssen sie gleich sein. Somit entspricht die Untergruppe $\langle\tau\rangle$ dem Zwischenkörper $\mathbb{Q}(i)$.

- Wegen $\zeta^{-1} = \frac{1-i}{\sqrt{2}}$ gilt $\zeta + \zeta^{-1} = \sqrt{2}$ und folglich $\sigma(\sqrt{2}) = \sqrt{2}$. Wie oben folgt daraus, dass die Untergruppe $\langle\sigma\rangle$ dem Zwischenkörper $\mathbb{Q}(\sqrt{2})$ entspricht.
- Wegen $\sigma\tau(\zeta) = \zeta^{-5} = \zeta^3$ und $(\zeta^3)^3 = \zeta^9 = \zeta$ vertauscht $\sigma\tau$ die beiden Nullstellen $\zeta, \zeta^3$. Somit ist $\zeta + \zeta^3$ invariant unter $\sigma\tau$. Wegen $\zeta^3 = \frac{-1+i}{\sqrt{2}}$ gilt aber $\zeta + \zeta^3 = i\sqrt{2}$, was wieder eine quadratische Erweiterung von $\mathbb{Q}$ erzeugt. Wie oben entspricht die Untergruppe $\langle\sigma\tau\rangle$ also dem Zwischenkörper $\mathbb{Q}(i\sqrt{2})$.

Insgesamt ergibt sich die folgende Aufstellung aller Untergruppen von $\Gamma$ und ihrer entsprechenden Zwischenkörper:




Da $\Gamma$ abelsch ist, ist jede Untergruppe normal und folglich jeder Zwischenkörper galoissch über $\mathbb{Q}$. Die Galoisgruppe der Zwischenkörper vom Grad 2 über $\mathbb{Q}$ ist dabei eine Gruppe der Ordnung 2 und somit zyklisch.

*5. 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 ist.)

*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.