Lösung 1

Körpererweiterungen und Galoisgruppen

1. Sei $E|K$ eine Körpererweiterung. Zeigen Sie, dass jedes Element der Galoisgruppe von $E|K$ ein K-linearer Isomorphismus des K-Vektorraumes E ist.

2. Zeigen Sie, dass $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{1, \sigma\}$, wobei σ die komplexe Konjugation auf $\mathbb{C}$ bezeichnet, d.h. $\sigma(x + iy) = x - iy$ für alle $x, y \in \mathbb{R}$.

3. Sei K ein Körper und $f \in K[X]$ ein Polynom. Zeigen Sie, dass falls E und E' zwei Zerfällungskörper von f sind, dann sind die Gruppen $\mathrm{Gal}(E|K)$ und $\mathrm{Gal}(E'|K)$ isomorph.

4. Seien K ein Körper mit $\mathrm{char}\, K \neq 2$ und $L|K$ eine Körpererweiterung vom Grad 2. Zeigen Sie, dass $|\mathrm{Gal}(L|K)| = 2$ ist.

   Lösung: Sei $\alpha \in L \setminus K$, so dass $L = K(\alpha)$. Wir wollen zeigen, dass es ein $\beta \in L$ gibt mit $\beta^2 \in K$ und $L = K(\beta)$. Sei $X^2 + sX + t \in K[X]$ das Minimalpolynom von α. Wir definieren $\beta := 2\alpha + s$. Da $\mathrm{char}\, K \neq 2$, ist $2\alpha + s \in L \setminus K$. Wir erhalten

   $$\beta^2 = (2\alpha + s)^2 = 4(\alpha^2 + s\alpha + t) + s^2 - 4t = s^2 - 4t \in K,$$

   und damit haben wir die Behauptung gezeigt. Wir setzen $b := \beta^2 \in K$.

   Sei nun $\{1, \beta\}$ eine K-Basis von L und $\varphi \in \mathrm{Gal}(L|K)$ ein Körperautomorphismus. Da φ K-linear ist (Aufgabe 1), ist φ eindeutig durch die Bilder von 1 und β bestimmt. Da $\varphi|_K = \mathrm{id}|_K$, wissen wir, dass

   $$\varphi(1) = 1 \text{ und } \varphi(\beta)^2 = \varphi(\beta^2) = \varphi(b) = b \implies \varphi(\beta) \in \{\pm b\}.$$

   Dies impliziert, dass $|\,\mathrm{Gal}(L|K)| = 2$, da $b \neq -b$ ($\mathrm{char}\, K \neq 2$).

5. Sei $f = X^4 - X - 1 \in \mathbb{Q}[X]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f. Sei $K := \mathbb{Q}(\alpha)$.

   (a) Zeigen Sie, dass das Polynom $X^4 - X - 1 \in \mathbb{F}_2[X]$ irreduzibel in $\mathbb{F}_2[X]$ ist.

   (b) Folgern Sie, dass f irreduzibel in $\mathbb{Q}[X]$ ist. *Erinnerung*: Dies impliziert, dass $\mathbb{Q}[X]/(f) \cong K$.

   (c) Schreiben Sie die folgenden Elemente als Linearkombinationen der $\mathbb{Q}$-Basiselemente $1, \alpha, \alpha^2, \alpha^3$:

   $$\alpha^{10}, \quad \frac{1}{\alpha}, \quad \frac{1}{\alpha + 1}, \quad \frac{\alpha^5}{\alpha^2 + 2}.$$

Lösung:

(a) Siehe Algebra I, Serie 6, Aufgabe 3.

(b) Eine Zerlegung von f in $\mathbb{Z}[X]$ in Polynome kleineren Grades gäbe eine Zerlegung von f aufgefasst als Polynom in $\mathbb{F}_2[X]$ (Reduktion der Koeffizienten modulo 2). Da f primitiv ist, folgt, dass es irreduzibel in $\mathbb{Z}[X]$ ist, und nach dem Gausschen Lemma ist f auch irreduzible in $\mathbb{Q}[X]$.

(c) Wir werden wiederholt die Tatsache benutzen, dass $\alpha^4 = \alpha + 1$.

- $\alpha^{10} = \alpha^2(\alpha^4)^2 = \alpha^2(\alpha+1)^2 = \alpha^4 + 2\alpha^3 + \alpha^2 = 2\alpha^3 + \alpha^2 + \alpha + 1.$
- Da $\alpha \cdot \alpha^3 = \alpha + 1$, bemerken wir, dass $\alpha \cdot (\alpha^3 - 1) = 1$, und somit $\alpha^{-1} = \alpha^3 - 1$.
- Aus den obigen Rechnungen erhalten wir $(\alpha+1)^{-1} = \alpha^{-4} = (\alpha^{-1})^4 = (\alpha^3-1)^4 = (\alpha^6 - 2\alpha^4 + 1)^2$. Da $\alpha^5 = \alpha^2(\alpha+1) = \alpha^2+\alpha$ und $\alpha^6 = \alpha^3+\alpha^2$ folgern wir, dass

$$\begin{aligned}(\alpha+1)^{-1} &= (\alpha^6 - 2\alpha^3 + 1)^2 = (-\alpha^3 + \alpha^2 + 1)^2 \\ &= \alpha^6 + \alpha^4 + 1 - 2\alpha^5 - 2\alpha^3 + 2\alpha^2 \\ &= \alpha^3 + \alpha^2 + \alpha + 1 + 1 - 2\alpha^2 - 2\alpha + 2\alpha^2 - 2\alpha^3 \\ &= -\alpha^3 + \alpha^2 - \alpha + 2.\end{aligned}$$

- Wir berechnen $(\alpha^2+2)^{-1}$. Seien $p, q, r, s \in \mathbb{Q}$ und wir nehmen an, dass $p + q\alpha + r\alpha^2 + s\alpha^3 = (\alpha^2+2)^{-1}$. Dann gilt

$$\begin{aligned}&(p + q\alpha + r\alpha^2 + s\alpha^3)(\alpha^2+2) = 1 \iff \\ &2p + 2q\alpha + (p+2r)\alpha^2 + (q+2s)\alpha^3 + r\alpha^4 + s\alpha^5 = 1 \iff \\ &2p + 2q\alpha + (p+2r)\alpha^2 + (q+2s)\alpha^3 + r(1+\alpha) + s(\alpha+\alpha^2) = 1 \iff \\ &(2p+r) + (r+s+2q)\alpha + (p+2r+s)\alpha^2 + (q+2s)\alpha^3 = 1 \iff \\ &2p + r = 1 \text{ und } r + s + 2q = p + 2r + s = q + 2s = 0,\end{aligned}$$

wobei die letzte Äquivalenz aus der Tatsache folgt, dass $1, \alpha, \alpha^2, \alpha^3$ eine $\mathbb{Q}$-Basis von K ist. Wir lösen das Gleichungssystem in $\mathbb{Q}$ und erhalten

$$(\alpha^2+2)^{-1} = \frac{7}{11} + \frac{2}{11}\alpha - \frac{3}{11}\alpha^2 - \frac{1}{11}\alpha^3.$$

Daraus folgt

$$\begin{aligned}\frac{\alpha^5}{\alpha^2+2} &= \left(\frac{7}{11}\alpha + \frac{2}{11}\alpha^2 - \frac{3}{11}\alpha^3 - \frac{1}{11}\alpha^4\right)(1+\alpha) \\ &= \left(-\frac{1}{11} + \frac{6}{11}\alpha + \frac{2}{11}\alpha^2 - \frac{3}{11}\alpha^3\right)(1+\alpha) \\ &= -\frac{1}{11} + \frac{5}{11}\alpha + \frac{8}{11}\alpha^2 - \frac{1}{11}\alpha^3 - \frac{3}{11}(1+\alpha) \\ &= -\frac{4}{11} + \frac{2}{11}\alpha + \frac{8}{11}\alpha^2 - \frac{1}{11}\alpha^3.\end{aligned}$$

6. Sei $g = X^3 - 2 \in \mathbb{Q}[X]$. Sei $\omega := e^{2\pi i/3}$ und $\beta := \sqrt[3]{2}$ (letzteres ist die reelle Zahl $\beta \in \mathbb{R}$ eindeutig bestimmt durch $\beta^3 = 2$).

   (a) Zeigen Sie, dass $E = \mathbb{Q}(\omega, \beta)$ ein Zerfällungskörper von g ist.

   (b) Zeigen Sie, dass $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

   (c) Zeigen Sie, dass $[E : \mathbb{Q}] > 3$.

   Folgern Sie daraus, dass $\mathrm{Gal}(E|\mathbb{Q}) \cong S_3$.

   Lösung:

   (a) Die Nullstellen von $X^3 - 2$ in $\mathbb{C}$ sind

   $$\sqrt[3]{2},\ \sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2.$$

   Daraus folgt, dass $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = E$ ein Zerfällungskörper von g ist.

   (b) Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ hat Grad 3, da $X^3 - 2$ das Minimalpolynomial von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist ($X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel nach Eisenstein mit $p = 2$).

   (c) Die Körpererweiterung $E|\mathbb{Q}$ enthält die Zwischenkörper $\mathbb{Q}(\omega)$ und $\mathbb{Q}(\beta)$. Aus (b) wissen wir, dass $\mathbb{Q}(\beta)|\mathbb{Q}$ Grad 3 hat. Die Körpererweiterung $\mathbb{Q}(\omega)|\mathbb{Q}$ hat Grad 2, da $X^2 + X + 1 \in \mathbb{Q}[X]$ das Minimalpolynom von ω über $\mathbb{Q}$ ist ($X^2 + X + 1 \in \mathbb{Q}[X]$ ist irreduzibel, siehe Algebra I, Serie 13, Aufgabe 6 (f) mit $p = 3$). Wir wissen bereits, dass $[E : \mathbb{Q}] \geqslant 3$. Aus der Multiplizität der Grade von Körpererweiterungen, muss sowohl 3 als auch 2 $[E : \mathbb{Q}]$ teilen, woraus folgt, dass $[E : \mathbb{Q}] \geqslant 6 > 3$.

   Wir wissen bereits, dass $\mathrm{Gal}(E|\mathbb{Q})$ als Untergruppe von S_3 aufgefasst werden kann (durch die Wirkung der Galoisgruppe auf die Nullstellen von $X^3 - 2$). Um nun zu zeigen, dass $\mathrm{Gal}(E|\mathbb{Q}) \cong S_3$, genügt es zu zeigen, dass $|\mathrm{Gal}(E|\mathbb{Q})| \geqslant 6 = 3!$. Moreover $[E : \mathbb{Q}(\sqrt[3]{2})] \leqslant 2$ da $X^2 + X + 1 \in \mathbb{Q}(\sqrt[3]{2})[X]$ ein Polynom vom Grad 2 ist, das ω als Nullstelle hat. Dann gilt

   $$6 \leqslant [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leqslant 2 \cdot 3 = 6,$$

   und damit $[E : \mathbb{Q}] = 6$. Die Multiplizität des Grades und (b) implizieren, dass

   $$[E : \mathbb{Q}(\sqrt[3]{2})] = 2 \text{ und } [E : \mathbb{Q}(\omega)] = 3.$$

   Aus Theorem II.17 folgt, dass 2 die Ordnung von $\mathrm{Gal}(E|\mathbb{Q}(\sqrt[3]{2}))$ teilt und dass 3 die Ordnung von $\mathrm{Gal}(E|\mathbb{Q}(\omega))$ teilt. Da diese beiden Galoisgruppen Untergruppen von $\mathrm{Gal}(E|\mathbb{Q})$ sind, folgern wir, dass 6 die Ordnung von $\mathrm{Gal}(E|\mathbb{Q})$ teilt. Zusammen mit der ersten Überlegung können wir nun schliessen, dass $\mathrm{Gal}(E|\mathbb{Q}) \cong S_3$.