Lösung 2

Separabilität und Berechnung von Galoisgruppen

1. Sei K ein Körper und $L|K$ eine Körpererweiterung. Zeigen Sie, dass falls $f \in K[X]$ separabel ist, dann ist f separabel in $L[X]$.

2. Welche der folgenden Polynome sind separabel?

   (a) $f(X) = X^2 + 2X + 1 \in \mathbb{Q}[X]$,

   (b) $g(X) = X^n - a \in K[X]$ für $n \geqslant 2$, K ein Körper und $a \in K$,

   (c) $h(X) = X^p - Y \in \mathbb{F}_p(Y)[X]$ für eine Primzahl p.

3. Sei $f \in K[X]$ ein irreduzibles Polynom und $L = K(\alpha)$ eine Körpererweiterung von K, wobei α eine Nullstelle von f in einem Zerfällungskörper von f ist. Angenommen es gibt eine Nullstelle β von f in L. Zeigen Sie, dass ein $\varphi \in \mathrm{Gal}(L \,|\, K)$ mit $\varphi(\alpha) = \beta$ existiert.

4. Sei $f \in K[X]$ und sei $E|K$ ein Zerfällungskörper von f. Wir wollen zeigen, dass f keine mehrfache Nullstelle in E hat, genau dann, wenn $\mathrm{ggT}_{K[X]}(f, f') = 1$.

   (a) Sei $F|K$ eine Körpererweiterung und $f, g \in K[X]$. Zeigen Sie, dass $\mathrm{ggT}_{K[X]}(f, g) = 1$, genau dann, wenn $\mathrm{ggT}_{F[X]}(f, g) = 1$.

   (b) Schreiben Sie $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $E[X]$. Verifizieren Sie, dass

   $$\prod_{i=1}^{n} f'(\alpha_i) = \pm \left(\prod_{i<j} (\alpha_i - \alpha_j) \right)^2 .$$

   (c) Folgern Sie die Aussage mithilfe der obigen Schritte.

   Lösung:

   (a) Erinnerung: Der ggT ist bis auf Assoziiertheit eindeutig. Daher gibt es einen eindeutigen monischen ggT von zwei Polynomen mit Koeffizienten in einem Körper. Bezouts Theorem impliziert, dass ein monisches Polynom $t \in k[X]$ (bzw. in $F[X]$) der ggT von f und g in $k[X]$ (bzw. in $F[X]$) ist, genau dann wenn $p, q \in k[X]$ (bzw. in $F[X]$) existieren mit $t = pf + qg$. Da $k[X] \subset F[X]$ folgt, dass $\mathrm{ggT}_{k[X]}(f, g) = \mathrm{ggT}_{F[X]}(f, g)$. Deshalb sind f, g koprim in $k[X]$ genau dann, wenn sie koprim in $F[X]$ sind.

(b) Wir können $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $E[X]$ schreiben nach der Definition von Zerfällungskörper. Es gilt die Produktregel für die Ableitung:

$$\forall p, q \in E[X],\ (pq)' = pq' + p'q.$$

Eine einfache Induktion verallgemeinert diese Aussage zu

$$\forall i \in \mathbb{Z}_{\geqslant 1},\ \forall p_1, \ldots, p_r \in E[X],\ (p_1 \cdots p_r)' = \sum_{i=1}^{r} \Big(p_i' \prod_{\substack{j \neq i \\ j=1,\ldots,r}} p_j \Big).$$

Wir wenden diese Formel auf $f = \prod_{i=1}^{n}(X - \alpha_i)$ an und erhalten

$$f' = \sum_{i=1}^{n} \Big(1 \cdot \prod_{\substack{j \neq i \\ j=1,\ldots,n}} (X - \alpha_j) \Big).$$

Auswerten an α_k liefert

$$f'(\alpha_k) = \prod_{\substack{j \neq k \\ j=1,\ldots,n}} (\alpha_k - \alpha_j),$$

woraus folgt, dass

$$\begin{aligned}
\prod_{k=1}^{n} f'(\alpha_k) &= \prod_{k=1}^{n} \prod_{\substack{j \neq k \\ j=1,\ldots,n}} (\alpha_k - \alpha_j) = \prod_{k=1}^{n} \Big(\prod_{\substack{j>k \\ j=1,\ldots,n}} (\alpha_k - \alpha_j) \prod_{\substack{j<k \\ j=1,\ldots,n}} (-1)(\alpha_j - \alpha_k) \Big) \\
&= \prod_{j=1}^{n} \Big(\prod_{\substack{k>j \\ k=1,\ldots,n}} (\alpha_j - \alpha_k) \Big) \prod_{k=1}^{n} (-1)^{k-1} \Big(\prod_{\substack{j<k \\ j=1,\ldots,n}} (\alpha_j - \alpha_k) \Big) \\
&= (-1)^{\binom{n}{2}} \Big(\prod_{1 \leqslant j < k \leqslant n}^{n} (\alpha_k - \alpha_j) \Big)^2.
\end{aligned}$$

(c) Aus (a) folgt, dass f und f' koprim in $k[X]$ sind genau dann, wenn sie koprim in $E[X]$ sind. Da $E[X]$ ein faktorieller Ring ist und $f = \prod_{i=1}^{n}(X - \alpha_i)$ in irreduzible Polynome faktorisiert, ist f koprim zu f' in $E[X]$ genau dann, wenn für jedes $i = 1, \ldots, n$ das Polynom $X - \alpha_i$ das Polynom f' nicht teilt. Dies ist äquivalent dazu, dass keines der α_i eine Nullstelle von f' ist, was bedeutet, dass $\prod_{i=1}^{n} f'(\alpha_i) \neq 0$. Dies ist äquivalent dazu, dass die α_i alle verschieden sind. Also sind f und f' koprim genau dann, wenn f keine mehrfachen Nullstellen hat.

5. Sei p eine Primzahl. Betrachten Sie das Polynom $\varphi_p := \frac{X^p - 1}{X - 1} \in \mathbb{Q}[X]$ und sei $\zeta := e^{\frac{2\pi i}{p}}$. Sei E ein Zerfällungskörper von φ_p.

(a) Zeigen Sie, dass φ_p irreduzibel in $\mathbb{Q}[X]$ ist und folgern Sie, dass φ_p das Minimalpolynom von ζ ist.

(b) Zeigen Sie, dass $E = \mathbb{Q}(\zeta)$.

(c) Zeigen Sie, dass $\mathrm{Gal}(E \mid \mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$.

Lösung:

(a) Siehe Algebra 1, Serie 13, Aufgabe 6 (f).

(b) Eine komplexe Nullstelle x von $X^p - 1$ muss Absolutbetrag 1 haben (da $|x|^p = |x^p| = |1| = 1$), und damit ist x von der Form $x = e^{\alpha i}$ für $\alpha \in \mathbb{R}$. Die Bedingung $x^p = 1$ liefert $\alpha = 2\pi i \frac{k}{p}$ für ein $k \in \mathbb{Z}$. Da $e^{2\pi i} = 1$ können wir $k \in \{0, 1, \ldots, p-1\}$ betrachten. Wir sehen, dass

$$X^p - 1 = \prod_{k=0}^{p-1}(X - \zeta^k), \text{ und damit } \varphi_p = \prod_{k=1}^{p-1}(X - \zeta^k).$$

Da $\mathbb{Q}(\zeta)$ alle Potenzen von ζ enthält folgern wir, dass $E = \mathbb{Q}(\zeta)$.

(c) Aus Teil (b) folgt, dass ein Automorphismus σ von E über $\mathbb{Q}$ eindeutig durch das Bild von ζ bestimmt ist. Da $\mathrm{Gal}(E|\mathbb{Q})$ Nullstellen von φ_p auf Nullstellen von φ_p sendet, wissen wir, dass $\sigma(\zeta) \in \{\zeta^k,\ k \in \{1, 2, \ldots, p-1\}\}$. Wir definieren eine Abbildung

$$\xi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(E|\mathbb{Q}),\ k + p\mathbb{Z} \mapsto (\zeta \mapsto \zeta^k).$$

Diese Abbildung ist wohl-definiert, da $\zeta^{\ell p} = 1$ für alle $\ell \in \mathbb{Z}$. Um zu zeigen, dass ξ ein Gruppenhomomorphismus ist, seien $k_1, k_2 \in \mathbb{Z}$, $(k_1 + p\mathbb{Z}) \cdot (k_2 + p\mathbb{Z}) := k_1k_2 + p\mathbb{Z}$. Dann gilt

$$\xi(k_1k_2 + p\mathbb{Z})(\zeta) = \zeta^{k_1k_2},$$

und

$$(\xi(k_1 + p\mathbb{Z}) \circ \xi(k_2 + p\mathbb{Z}))(\zeta) = (\xi(k_1 + p\mathbb{Z}))(\zeta^{k_2}) \overset{(*)}{=} (\zeta^{k_1})^{k_2} = \zeta^{k_1k_2},$$

wobei wir in $(*)$ die Tatsache benutzt haben, dass $\xi(k_1+p\mathbb{Z})$ ein Körperhomomorphismus ist mit $\zeta \mapsto \zeta^{k_1}$. Daraus folgt, dass ξ ein Gruppenhomomorphismus ist. xi ist surjektiv nach den Überlegungen von oben und injektiv, da

$$\ker(\xi) = \{k + p\mathbb{Z} : \xi(k + p\mathbb{Z}) = \mathrm{id}_E\} = \{k + p\mathbb{Z} : \zeta^k = \zeta\} = \{1 + p\mathbb{Z}\}.$$

Damit ist gezeigt, dass $\mathrm{Gal}(E|\mathbb{Q})$ isomorph zu $(\mathbb{Z}/p\mathbb{Z})^\times$ ist.

6. Sei $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) Zeigen Sie, dass $[E : \mathbb{Q}] = 4$.

(b) Zeigen Sie, dass $\mathrm{Gal}(E \,|\, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lösung:

(a) Man überprüft zuerst, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Daraus folgt, dass $E|\mathbb{Q}(\sqrt{2})$ keine triviale Körpererweiterung ist. Da $E|\mathbb{Q}(\sqrt{2})$ erzeugt ist von $\sqrt{3}$, welches eine Nullstelle von $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ ist, folgern wir, dass $[E : \mathbb{Q}(\sqrt{2})] = 2$. Die Multiplizität der Grade von Körpererweiterungen gibt

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

(b) Da E der Zerfällungskörper des separablen irreduciblen Polynoms $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ ist, wissen wir, dass $2|\,\mathrm{Gal}(E|\mathbb{Q}(\sqrt{2}))$. Ein Automorphismus $\sigma \in \mathrm{Gal}(E|\mathbb{Q}(\sqrt{2}))$ ist eindeutig durch das Bild von $\sqrt{3}$ bestimmt, welches entweder $\sqrt{3}$ oder $-\sqrt{3}$ ist. Daraus folgt, dass $\mathrm{Gal}(E|\mathbb{Q}(\sqrt{2}))$ genau 2 Elemente enthält: die Identität id und $\sigma_3 : \sqrt{3} \mapsto -\sqrt{3}$ (und $\sigma_3(\sqrt{2}) = \sqrt{2}$ nach der Definition von $\mathrm{Gal}(E|\mathbb{Q}(\sqrt{2}))$). Auf ähnliche Weise sieht man, dass $\mathrm{Gal}(E|\mathbb{Q}(\sqrt{3})) = \{\mathrm{id}, \sigma_2\}$, wobei $\sigma_2(\sqrt{2}) = -\sqrt{2}$ (und $\sigma_2(\sqrt{3}) = \sqrt{3}$).

Alle obigen Automorphismen von E sind alle auch Elemente von $\mathrm{Gal}(E|\mathbb{Q})$, welches somit die vier verschiedenen Automorphismen $\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3$ enthält. Andererseits ist $\sigma \in \mathrm{Gal}(E|\mathbb{Q})$ eindeutig durch die Bilder von $\sqrt{2}$ und $\sqrt{3}$ bestimmt, welche jeweils nur auf zwei Elemente geschickt werden können, woraus folgt, dass es höchstens vier Möglichkeiten gibt. Daraus folgt, dass $\mathrm{Gal}(E|\mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3\}$. Die einzigen zwei Gruppen der Ordnung vier bis auf Isomorphie sind $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Nun haben σ_2 und σ_3 beide Ordnung 2, aber in $\mathbb{Z}/4\mathbb{Z}$ gibt es nur ein Element der Ordnung 2. Damit folgt, dass $\mathrm{Gal}(E|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.