Lösung 9

Galoiskorrespondenz

1. Sei K ein Körper, $f \in K[X]$ ein Polynom mit verschiedenen Nullstellen und E ein Zerfällungskörper von f. Wir schreiben $R(f) = \{z_1, \ldots, z_n\}$ und sehen $\mathrm{Gal}(E|K) \leqslant S_n$. Wir definieren die *Diskriminante von* f als
$$D(f) = \prod_{i<j}(z_i - z_j)^2.$$
   (a) Angenommen die Charakteristik von K ist nicht 2. Zeigen Sie, dass $D(f)$ ein Quadrat in K ist, genau dann, wenn $\mathrm{Gal}(E|K) \leqslant A_n$.
   (b) Zeigen Sie, dass $\mathbb{F}_4|\mathbb{F}_2$ ein Gegenbeispiel in Charakteristik 2 zu Teil (a) ist.

2. Welche der folgenden Körpererweiterungen $L|K$ sind Galois?
   (a) $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$,
   (b) $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[4]{2})$,
   (c) $K = \mathbb{Q}(X^2)$ und $L = \mathbb{Q}(X)$,
   (d) $K = \mathbb{F}_2(X^2 + X)$ und $L = \mathbb{F}_2(X)$.

3. Berechnen Sie für die folgenden Körpererweiterungen $L|K$ die Menge $\mathrm{Sub}(\mathrm{Gal}(L|K))$ und die entsprechenden Zwischenkörper.
   (a) $K = \mathbb{Q}$ und L ist der Zerfällungskörper des Polynoms $(X^2 - 2)(X^2 - 3)$,
   (b) $K = \mathbb{Q}$ und L ist der Zerfällungskörper des Polynoms $X^5 - 1$.

4. Ist die folgende Aussage wahr oder falsch? Falls die Körpererweiterungen $L|M$ und $M|K$ beide Galois sind, so ist auch $L|K$ Galois.

   Lösung: Die Aussage ist falsch. Wir betrachten z.B. die Körpererweiterungen $L = \mathbb{Q}(\sqrt[4]{2})$, $M = \mathbb{Q}(\sqrt{2})$ und $K = \mathbb{Q}$. Dann ist $M|K$ Galois als Zerfällungskörper von $f^2 - 2 \in \mathbb{Q}[X]$ und $L|M$ ist Galois als Zerfällungskörper von $f^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$. Jedoch ist $L|K$ nicht Galois, da der Zerfällungskörper von $f^4 - 2 \in \mathbb{Q}[X]$ nicht L ist, sondern $\mathbb{Q}(\sqrt[4]{2}, i)$.

Sei K ein Körper. Für jedes $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ definiert
$$\sigma\begin{pmatrix} a & b \\ c & d \end{pmatrix} P(X) := P\left(\frac{dX - b}{-cX + a}\right)$$

für $P \in K(X)$ einen Automorphismus in $\operatorname{Gal}(K(X)|K)$. Die Abbildung

$$\sigma : \operatorname{GL}_2(K) \to \operatorname{Gal}(K(X)|K)$$

ist ein Homomorphismus.

5. Sei $G := \sigma\left(\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_3^\times, b \in \mathbb{F}_3\right\}\right) \leqslant \operatorname{Gal}(\mathbb{F}_3(X)|\mathbb{F}_3)$. Finden Sie $\mathbb{F}_3(X)^G$, $\operatorname{Sub}(G)$ und alle Zwischenerweiterungen $\mathbb{F}_3(X)|\mathbb{F}_3(X)^G$.

   Lösung: Wir berechnen zunächst $\mathbb{F}_3(X)^G$. Da G 6 Elemente hat, wissen wir aus Proposition IV.9, dass der Grad der Körpererweiterung $\mathbb{F}_3(X)|\mathbb{F}_3(X)^G$ gerade 6 ist. Das Polynom $(X^3+X)^2$ hat Grad 6 und wird von G fixiert. Dieses findet man als Produkt

$$(X^3 + X)^2 = \prod_{(a,b)\in\mathbb{F}_3^\times\times\mathbb{F}_3} \sigma\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} X = \prod_{(a,b)\in\mathbb{F}_3^\times\times\mathbb{F}_3} \frac{X-b}{a}.$$

   Damit ist $\mathbb{F}_3(X)^G = \mathbb{F}_3\left((X^3+X)^2\right)$.

   Die Zwischenerweiterungen $\mathbb{F}_3(X)|\mathbb{F}_3(X)^G$ sind in Korrespondenz zu der Menge $\operatorname{Sub}(G)$ durch Berechnung der Fixkörper. Wir wissen, dass G sechs Elemente hat, und da G nicht kommutativ ist, ist G isomorph zu S_3. Die Untergruppen von S_3 können wir gut verstehen: es gibt die triviale Untergruppe, die ganze Gruppen, 3 zyklische Untergruppen der Ordnung 2 und eine zyklische Untergruppe der Ordnung 3 (diese ist isomorph zu A_3). Man kann sich leicht davon überzeugen, dass $H := \left\langle \sigma\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right\rangle$ Ordnung 3 hat und dass für alle $b \in \mathbb{F}_3$ die Untergruppen $H_b := \left\langle \sigma\begin{pmatrix} 2 & b \\ 0 & 1 \end{pmatrix}\right\rangle$ Ordnung 2 haben. Wir berechnen auf die gleiche Weise wie für G die Fixkörper und erhalten $\mathbb{F}_3(X)^H = \mathbb{F}_3(X^3+2X)$, $\mathbb{F}_3(X)^{H_0} = \mathbb{F}_3(X^2)$, $\mathbb{F}_3(X)^{H_1} = \mathbb{F}_3(X^2+2X)$ und $\mathbb{F}_3(X)^{H_2} = \mathbb{F}_3(X^2+X)$.

6. Zeigen Sie, dass

$$\sigma : \operatorname{GL}_2(K) \to \operatorname{Gal}(K(X)|K)$$

   einen Isomorphismus

$$\operatorname{PGL}_2(K) \cong \operatorname{Gal}(K(X)|K)$$

   induziert. Hier bezeichnet $\operatorname{PGL}_2(K)$ den Quotienten von $\operatorname{GL}_2(K)$ bezüglich

$$Z = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in K^\times\right\}.$$

   Lösung: Wir müssen zeigen, dass $Z = \ker(\sigma)$ und, dass die induzierte Abbildung auf $\operatorname{GL}_2(K)/Z$ surjektiv ist.

Sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ mit $\sigma(M) = \mathrm{id}$. Dann ist $\frac{dX-b}{-cX+a} = X$ und damit $dX - b = -cX^2 + aX$. Daraus folgt nach Koeffizientenvergleich, dass $b = c = 0$ und $a = d$, und somit $M \in Z$.

Wir wissen, dass ein Automorphismus α von $K(X)$ durch das Bild von X bestimmt ist. Seien $P, Q \in K[X]$, $Q \neq 0$ mit $\alpha(X) = \frac{P(X)}{Q(X)}$ und P, Q koprim. Wir wollen zeigen, dass P und Q Grad $\leqslant 1$ haben. Wir bemerken zunächst, dass $\alpha(X) \notin K$. Das Polynom $\alpha(X)Q(T) - P(T) \in K(\alpha(X))[T]$ hat X als Nullstelle und damit ist X algebraisch über $K(\alpha(X))$ (und nicht Null, da Q und P koprim). Wir behaupten, dass das Polynom $\alpha(X)Q(T) - P(T) \in K(\alpha(X))[T]$ irreduzibel ist. Nach Gauss' Lemma ist dieses Polynom irreduzibel in $K(\alpha(X))[T]$ genau dann, wenn es irreduzibel in $K[\alpha(X)][T] = K[T][\alpha(X)]$ ist. In $K[T][\alpha(X)]$ ist es aber als lineares Polynom in $\alpha(X)$ trivialerweise irreduzibel und die zwei Koeffizienten $Q(T)$ und $P(T)$ sind prim nach Annahme. Daraus folgt, dass $[K(X) : K(\alpha(X))] = \max(\deg(P), \deg(Q))$. Da α ein Automorphismus ist, sind $K(X)$ und $K(\alpha(X))$ isomorph und damit folgt, dass $\max(\deg(P), \deg(Q)) = 1$, was zu zeigen war.