Lösung 8

Symmetrische Funktionen

1. Seien $E|K$ eine endliche Körpererweiterung, $G := \mathrm{Gal}(E|K)$ und wir betrachten ein Element $\alpha \in E$. Zeigen Sie, dass das Polynom

$$q(X) := \prod_{\sigma \in G/\mathrm{Stab}_G(\alpha)} (X - \sigma(\alpha)) \in E[X]$$

ein Element von $E^G[X]$ ist.

2. Seien K ein Körper und $f \in K[X]$ separabel und $\deg(f) = 5$. Sei E ein Zerfällungskörper von f. Angenommen f is durch Radikale lösbar, zeigen Sie, dass $[E : K] < 60$ gilt.

3. Seien K ein Körper, $f \in K[X]$ und E ein Zerfällungskörper von f. Angenommen $f = g \cdot h$ in $K[X]$. Seien B und C Zerfällungskörper von g und h, die in E enthalten sind. Zeigen Sie, dass $\mathrm{Gal}(E|B)$ und $\mathrm{Gal}(E|C)$ in $\mathrm{Gal}(E|K)$ kommutieren.

4. Sei V ein endlich-dimensionaler K-Vektorraum mit $|K| = \infty$. Zeigen Sie, dass V nicht die endliche Vereinigung von echten Untervektorräumen ist.

   Lösung: Angenommen $V = \bigcup_{i=1}^n V_i$, wobei V_i echte Untervektorräume von V sind. Wähle $x \in V_1$ nicht Null. Wähle $y \in V \setminus V_1$ (y existiert, da V_1 ein echter Untervektorraum ist). Da K unendlich ist, gibt es unendlich viele Vektoren der Form $v_\alpha := x + \alpha y$ mit $\alpha \in K^\times$. Da v_α nie in V_1 ist (sonst wäre $y \in V_1$), existiert ein $j \neq 1$, so dass $v_\alpha \in V_j$ für unendlich viele $\alpha \in K^\times$. Insbesondere gibt es $\alpha \neq \beta \in K^\times$ mit v_α und $v_\beta \in V_j$. Daraus folgt, dass $y \in V_j$ (da $v_\alpha - v_\beta \in V_j$), und damit auch $x \in V_j$. Da $x \in V_1$ beliebig war, folgt, dass $V_1 \subseteq \bigcup_{i=2}^n V_i$. Wir können dieses Argument iterieren und erhalten einen Widerspruch.

5. Seien E ein Körper, S eine Menge und $F(S, E)$ der Raum der Funktionen auf S mit Werten in E. Seien $\{f_1, \dots, f_n\} \subset F(S, E)$ linear unabhängig. Zeigen Sie, dass $s_1, \dots, s_n \in S$ existieren, so dass

$$\begin{pmatrix} f_1(s_1) \\ \vdots \\ f_n(s_1) \end{pmatrix}, \dots, \begin{pmatrix} f_1(s_n) \\ \vdots \\ f_n(s_n) \end{pmatrix}$$

linear unabhängig in E^n sind.

Lösung: Wir machen eine Induktion nach n. Sei $n = 1$. Dann ist f_1 linear unabhängig, genau dann, wenn f_1 nicht konstant Null ist, das heisst es existiert ein $s_1 \in S$ mit $f_1(s_1) \neq 0$ und damit ist $f_1(s_1)$ linear unabhängig in E.

Sei nun $n > 1$, und $f_1, \ldots, f_n$ linear unabhängig. Dann sind auch $f_1, \ldots, f_{n-1}$ linear unabhängig und nach Induktionsvoraussetzung existieren $s_1, \ldots, s_{n-1}$ mit

$$A := \begin{pmatrix} f_1(s_1) & \ldots & f_1(s_{n-1}) \\ \vdots & \ddots & \vdots \\ f_{n-1}(s_1) & \ldots & f_{n-1}(s_{n-1}) \end{pmatrix}$$

invertierbar. Dann ist auch A^T invertierbar und damit die Vektoren

$$\begin{pmatrix} f_1(s_1) \\ \vdots \\ f_1(s_{n-1}) \end{pmatrix}, \ldots, \begin{pmatrix} f_{n-1}(s_1) \\ \vdots \\ f_{n-1}(s_{n-1}) \end{pmatrix}$$

in E^{n-1} linear unabhängig. Die n Vektoren $\begin{pmatrix} f_1(s_1) \\ \vdots \\ f_1(s_{n-1}) \end{pmatrix}, \ldots, \begin{pmatrix} f_n(s_1) \\ \vdots \\ f_n(s_{n-1}) \end{pmatrix}$ in E^{n-1} sind nun linear abhängig. Das heisst es existieren $\alpha_1, \ldots, \alpha_n$ in E, $(\alpha_1, \ldots, \alpha_n) \neq (0, \ldots, 0)$ mit

$$\alpha_1 \begin{pmatrix} f_1(s_1) \\ \vdots \\ f_1(s_{n-1}) \end{pmatrix} + \ldots + \alpha_n \begin{pmatrix} f_n(s_1) \\ \vdots \\ f_n(s_{n-1}) \end{pmatrix} = 0.$$

Da die ersten $n - 1$ Vektoren linear unabhängig sind, ist $\alpha_n \neq 0$ und wir können annehmen, dass $\alpha_n = -1$. Dann ist

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = (A^T)^{-1} \begin{pmatrix} f_n(s_1) \\ \vdots \\ f_n(s_{n-1}) \end{pmatrix},$$

und damit sind $\alpha_1, \ldots, \alpha_{n-1}$ eindeutig durch A und $f_n(s_1), \ldots, f_n(s_{n-1})$ bestimmt.

Da $f_1, \ldots, f_n$ linear unabhängig sind existiert ein $s_n \in S$ mit

$$\alpha_1 f_1(s_n) + \ldots + \alpha_{n-1} f_{n-1}(s_n) - f_n(s_n) \neq 0.$$

Wir behaupten nun, dass $e_1 := \begin{pmatrix} f_1(s_1) \\ \vdots \\ f_1(s_n) \end{pmatrix}, \ldots, e_n := \begin{pmatrix} f_n(s_1) \\ \vdots \\ f_n(s_n) \end{pmatrix}$ linear unabhängig in E^n sind. Angenommen es existieren $\beta_1, \ldots, \beta_n \in E$, nicht alle β_i gleich Null, mit

$$\beta_1 e_1 + \ldots + \beta_n e_n = 0.$$

Insbesondere gilt dies für die ersten $n-1$ Zeilen, und aus dem gleichen Argument wie oben, folgt $\beta_n \neq 0$. Nach Normierung können wir annehmen, dass $\beta_n = -1$, und damit auch $\alpha_i = \beta_i$ für alle i, da die α_i durch A und $f_n(s_1), \ldots, f_n(s_{n-1})$ bestimmt sind. Nun gilt in der letzten Zeile, dass

$$0 = \beta_1 f_1(s_n) + \ldots + \beta_{n-1} f_{n-1}(s_n) - f_n(s_n) = \alpha_1 f_1(s_n) + \ldots + \alpha_{n-1} f_{n-1}(s_n) - f_n(s_n) \neq 0,$$

was ein Widerspruch ist nach Wahl von s_n. Damit sind $e_1, \ldots, e_n$ linear unabhängig und damit auch $\begin{pmatrix} f_1(s_1) \\ \vdots \\ f_n(s_1) \end{pmatrix}, \ldots, \begin{pmatrix} f_1(s_n) \\ \vdots \\ f_n(s_n) \end{pmatrix}$, was zu zeigen war.

6. Sei K ein Körper, $E = K(y_1, \ldots, y_n)$, $F = K(\varepsilon_0, \ldots, \varepsilon_{n-1})$, wobei $\varepsilon_0, \ldots, \varepsilon_{n-1}$ die elementarsymmetrischen Polynome in $y_1, \ldots, y_n$ sind. Zeigen Sie mit Hilfe von Theorem II.17, dass

$$E^{S_n} = F.$$

Folgern Sie daraus, dass jede symmetrische rationale Funktion eine rationale Funktion in den elementarsymmetrischen Polynomen ist.

Hinweis: Siehe den Beweis des Satzes von Abel-Ruffini.

Lösung: Wir haben im Beweis des Satzes von Abel-Ruffini bereits gesehen, dass E der Zerfällungskörper des Polynoms $f(X) = \prod_{i=1}^{n}(X - y_i)$ ist und, dass $G := \mathrm{Gal}(E|F) \cong S_n$. Aus Theorem II.17,(2), folgt, dass $|G| = [E : F]$ und aus Proposition IV.9, dass $|G| = [E : E^G]$, und somit

$$[E : F] = [E : E^G].$$

Da $F \subseteq E^G$ gilt $[E : F] = [E : E^G][E^G : F]$, und damit $[E^G : F] = 1$, also $F = E^G$. Zusammen ergibt sich $E^{S_n} = F$.

Aber $g(y_1, \ldots, y_n)/h(y_1, \ldots, y_n) \in E^{S_n}$ genau dann, wenn es invariant unter Permutation der Variablen ist, das heisst eine symmetrische Funktion ist.