D-MATH | Algebra II | FS 2016
Prof. Richard Pink

Musterlösung 25

Symmetrische Funktionen, Resultante

1. Schreibe die folgenden Ausdrücke in $X_1, \ldots, X_n$ in Termen der elementarsymmetrischen Polynome:

   (a) $\sum_{i\neq j} X_i^3 X_j$.

   (b) $\sum_i X_i^4$.

   (c) $\sum_{i\neq j\neq k\neq i} X_i^2 X_j^2 X_k^2$.

   (d) $\sum_{i\neq j} X_i/X_j$.

   Lösung: (a) $\sum_{i\neq j} X_i^3 X_j = S_1^2 S_2 - S_1 S_3 - 2S_2^2 + 4S_4$.

   (b) $\sum_i X_i^4 = S_1^4 - 4S_1^2 S_2 + 2S_2^2 + 4S_1 S_3 - 4S_4$.

   (c) $\sum_{i\neq j\neq k\neq i} X_i^2 X_j^2 X_k^2 = 6(S_3^2 + 2S_1 S_5 - 2S_2 S_4 - 2S_6)$.

   (d) $\sum_{i\neq j} X_i/X_j = \frac{S_1 S_{n-1}}{S_n} - n$.

2. Seien $S_1 = X + Y + Z$ und $S_2 = XY + XZ + YZ$ und $S_3 = XYZ$ die elementarsymmetrischen Polynome in drei Variablen. Für alle $n \geqslant 1$ definiere $F_n := X^n + Y^n + Z^n$. Zeige, dass für $n \geqslant 4$ die folgende Rekursionsformel gilt:

   $$F_n = S_1 F_{n-1} - S_2 F_{n-2} + S_3 F_{n-3},$$

   und berechne F_n für alle $n = 1, \ldots, 5$.

   Lösung: Es gilt
   $X^n + Y^n + Z^n$
   $$\begin{aligned}
   &= (X+Y+Z)(X^{n-1}+Y^{n-1}+Z^{n-1}) \\
   &\quad -(XY(X^{n-2}+Y^{n-2}) + XZ(X^{n-2}+Z^{n-2}) + YZ(Y^{n-2}+Z^{n-2})) \\
   &= S_1 F_{n-1} - (XY+XZ+YZ)(X^{n-2}+Y^{n-2}+Z^{n-2}) \\
   &\quad +(XYZ^{n-2} + XZY^{n-2} + YZX^{n-2}) \\
   &= S_1 F_{n-1} - S_2 F_{n-2} + XYZ(X^{n-3}+Y^{n-3}+Y^{n-3}) \\
   &= S_1 F_{n-1} - S_2 F_{n-2} + S_3 F_{n-3}.
   \end{aligned}$$

Konkret ergeben sich

$$
\begin{aligned}
F_1 &= S_1 \\
F_2 &= S_1^2 - 2S_2 \\
F_3 &= S_1^3 - 3S_1S_2 + 3S_3 \\
F_4 &= S_1(S_1^3 - 3S_1S_2 + 3S_3) - S_2(S_1^2 - 2S_2) + S_3S_1 \\
&= S_1^4 - 4S_1^2S_2 + 4S_1S_3 + 2S_2^2 \\
F_5 &= S_1(S_1^4 - 4S_1^2S_2 + 4S_1S_3 + 2S_2^2) - S_2(S_1^3 - 3S_1S_2 + 3S_3) + S_3(S_1^2 - 2S_2) \\
&= S_1^5 - 5S_1^3S_2 + 5S_1^2S_3 + 5S_1S_2^2 - 5S_2S_3.
\end{aligned}
$$

3. Betrachte einen Körper K und eine natürliche Zahl $n \geqslant 2$. Seien $X_1, \ldots, X_n$ unabhängige Variable über K, und seien $S_1, \ldots, S_n$ ihre elementarsymmetrischen Polynome.

   (a) Zeige: Ist $\mathrm{char}(K) \neq 2$, so ist $K(X_1, \ldots, X_n)^{A_n} = K(S_1, \ldots, S_n, E)$ für $E := \prod_{1 \leqslant i < j \leqslant n}(X_i - X_j)$.

   (b) Bestimme $K(X_1, \ldots, X_n)^{A_n}$ im Fall $\mathrm{char}(K) = 2$.

   Lösung: Schreibe $L := K(X_1, \ldots, X_n)$. Nach Abschnitt 6.3 ist L/L^{S_n} endlich galoissch mit Galoisgruppe S_n, beziehungsweise L/L^{A_n} endlich galoissch mit Galoisgruppe A_n. Wegen $A_n \triangleleft S_n$ folgt mit dem Hauptsatz der Galoistheorie, dass die Erweiterung L^{A_n}/L^{S_n} galoissch und ihre Galoisgruppe isomorph zu $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ ist, also Ordnung 2 hat. Für jedes $F \in L^{A_n} \smallsetminus L^{S_n}$ gilt folglich $L^{A_n} = L^{S_n}(F)$.

   (a) Für jedes $\sigma \in S_n$ gilt

   $$
   {}^{\sigma}E = \prod_{1 \leqslant \sigma(i) < \sigma(j) \leqslant n} (X_{\sigma(i)} - X_{\sigma(j)}) = \mathrm{sgn}(\sigma) \prod_{1 \leqslant i < j \leqslant n} (X_i - X_j) = \mathrm{sgn}(\sigma) E.
   $$

   Also ist E invariant unter A_n, aber nicht unter S_n. Folglich ist der Fixkörper $L^{A_n} = K(S_1, \ldots, S_n, E)$.

   (b) Setze $F := \sum_{\sigma \in A_n} \prod_{i=1}^{n} X_{\sigma i}^{i-1}$; nach Konstruktion ist $F \in L^{A_n}$. Jedoch ist das Polynom nicht invariant unter S_n, da zum Beispiel der Term $X_2 X_3^2 X_4^3 \ldots X_n^{n-1}$ als Summand auftaucht, der Term $X_3 X_2^2 X_4^3 \ldots X_n^{n-1}$ aber nicht. Folglich ist der Fixkörper $L^{A_n} = K(S_1, \ldots, S_n, F)$.

   Übrigens folgt aus der Vandermondeschen Determinante, dass $F - {}^{\tau}F = -E$ ist für jede Transposition $\tau \in S_n$. Weil nur die Hälfte aller Terme genommen werden, funktioniert das auch in Charakteristik 2.

4. Bestimme die Resultante folgender ganzzahliger Polynome bis aufs Vorzeichen:

   (a) $X^3 - X + 1$ und $X^2 + X + 3$.

   (b) $X^{n-1} + X^{n-2} + \cdots + 1$ und $X^{m-1} + X^{m-2} \cdots + 1$ für teilerfremde n und m.

Für welche p haben sie gemeinsame Nullstellen in einem algebraisch abgeschlossenen Körper der Charakteristik p?

Lösung: (a) Die Resultante ist

$$\det\begin{pmatrix} 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 3 & 0 & 0 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix} = 55.$$

Die zwei Polynome haben also genau dann eine gemeinsame Nullstelle in einem algebraisch abgeschlossenen Körper der Charakteristik p, wenn $p \in \{5, 11\}$ ist.

(b) Die fraglichen Polynome sind $f_n(X) := \frac{X^n-1}{X-1}$ und $f_m(X) := \frac{X^m-1}{X-1}$. Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel; dann hat f_n die paarweise verschiedenen Nullstellen ζ^i für $i = 1\ldots, n-1$. Mit der Formel aus der zweiten Proposition in Abschnitt 6.4 ergibt sich

$$\mathrm{Res}_{f_n,f_m} \;=\; \prod_{i=1}^{n-1} f_m(\zeta^i) \;=\; \prod_{i=1}^{n-1} \frac{\zeta^{im}-1}{\zeta^i-1}.$$

Da n und m teilerfremd sind, durchläuft im genau wie i alle nichttrivialen Kongruenzklassen modulo n. Deshalb sind die Zähler im obigen Produkt gleich den Nennern geeignet vertauscht. Die Resultante ist daher gleich 1.

Aliter: Nach Definition ist die Resultante eine ganze Zahl. Nehmen wir an, sie habe einen Primteiler p. Dann haben die Polynome eine gemeinsame Nullstelle ζ in einem algebraisch abgeschlossenen Körper der Charakteristik p. Für diese gilt $\zeta^m = 1$ und $\zeta^n = 1$. Wegen $\mathrm{ggT}(m,n) \sim 1$ existieren $u, v \in \mathbb{Z}$ mit $um+vn = 1$; also gilt sogar $\zeta = \zeta^{um+vn} = 1$. Daraus folgt aber $f_n(\zeta) = f_n(1) = n$ und $f_m(\zeta) = m$. Wegen $p \nmid \mathrm{ggT}(m,n)$ sind diese Werte nicht beide null, was der Annahme, ζ sei eine gemeinsame Nullstelle, widerspricht. Folglich ist die Resultante eine ganze Zahl ohne Primteiler und somit gleich ± 1.

**5. Betrachte den Polynomring $R := \mathbb{Z}[A_0, \ldots, A_m, B_0, \ldots, B_m]$ und eine weitere Variable X. Betrachte die Polynome $F(X) = \sum_{i=0}^m A_i X^i$ und $G(X) = \sum_{j=0}^n B_j X^j$ in $R[X]$, und sei $H \in R$ deren Resultante bezüglich X. Zeige, dass H ein irreduzibles Element von R ist.