D-MATH Algebra II FS 2023
Prof. Richard Pink

Musterlösung Serie 26

Symmetrische Funktionen, Resultante

1. 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

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

Konkret ergeben sich

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

2. 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 das Polynom $E := \prod_{1 \leqslant i < j \leqslant n}(X_i - X_j)$.

   (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 Satz 7.1.5 der Vorlesung ist L/L^{S_n} endlich galoissch mit Galoisgruppe S_n, und L/L^{A_n} ist endlich galoissch mit Galoisgruppe A_n. Wegen $A_n \lhd S_n$ 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

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

Also ist E invariant unter A_n, aber wegen $-1 \neq 1$ in K nicht invariant unter S_n. Folglich ist $E \in L^{A_n} \smallsetminus L^{S_n}$ und daher der Fixkörper $L^{A_n} = K(S_1, \ldots, S_n, E)$.

(b) In diesem Fall zeigt die obige Rechnung $E \in L^{S_n}$. Stattdessen nehmen wir daher das Polynom $F := \sum_{\sigma \in A_n} \prod_{i=1}^{n} X_{\sigma i}^{i-1}$. Nach Konstruktion ist F invariant unter A_n, jedoch ist es 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. Somit ist $F \in L^{A_n} \smallsetminus L^{S_n}$ und daher der Fixkörper $L^{A_n} = K(S_1, \ldots, S_n, F)$.

(Das Argument in (b) mit dem Ergebnis $L^{A_n} = K(S_1, \ldots, S_n, F)$ funktioniert übrigens in jeder Charakteristik.)

3. 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: In beiden Fällen haben die Polynome Koeffizienten in $\mathbb{Z}$, also liegt auch ihre Resultante in $\mathbb{Z}$. Da die Resultante ein Polynom über $\mathbb{Z}$ in den Koeffizienten der Polynome ist, ist die Resultante der entsprechenden Polynome über einem beliebigen algebraisch abgeschlossenen Körper K einfach das Bild in K der Resultante über $\mathbb{Z}$. Die Polynome haben daher genau dann eine gemeinsame Nullstelle in K, wenn die Charakteristik p von K die Resultante über $\mathbb{Z}$ teilt.

   (a) Die Definition der Resultante ergibt

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

   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) Wir berechnen die Resultante zuerst in $\mathbb{C}$. Dazu schreiben wir die Polynome in der Form $f_n(X) := \frac{X^n-1}{X-1}$ 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 Proposition 7.4.5 der Vorlesung 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 hat das obige Produkt bis auf Vertauschung die gleichen Zähler und Nenner. Die Resultante ist daher gleich 1. Aus der Vorbemerkung folgt, dass die zwei Polynome in keinem Körper eine gemeinsame Nullstelle besitzen.

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.

**4. 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.

5. In der Linearen Algebra wurde gezeigt: Für beliebige Elemente $a_1, \ldots, a_n$ eines kommutativen unitären Rings hat die Matrix $A = (a_i^{j-1})_{1 \leqslant i,j \leqslant n}$ die *Vandermonde-Determinante*

$$\det(A) \;=\; \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

Beweise diese Formel mit der Methode, mit der in der Vorlesung die Formel für die Resultante in Termen der Nullstellen der beteiligten Polynome gezeigt wurde.

Lösung: Wenn die Formel für die Vandermonde-Determinante für unabhängige Variablen $X_1, \ldots, X_n$ über $\mathbb{Z}$ stimmt, stimmt sie durch Einsetzen auch für beliebige Ringelemente $a_1, \ldots, a_n$. Wir interessieren uns also für das Polynom

$$V \;:=\; \begin{vmatrix} 1 & X_1 & X_1^2 & \ldots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \ldots & X_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & X_n^2 & \ldots & X_n^{n-1} \end{vmatrix} \;\in\; \mathbb{Z}[X_1, \ldots, X_n].$$

Betrachte beliebige Indizes $1 \leqslant i < j \leqslant n$. Wenn wir die Variable X_j gleich X_i setzen, wird die j-te Zeile der Matrix gleich der i-ten Zeile und folglich die Determinante zu Null. Also hat V, als Polynom in X_j betrachtet, die Nullstelle X_i, und ist folglich durch $X_j - X_i$ teilbar. Da die Polynome $X_j - X_i$ für alle $1 \leqslant i < j \leqslant n$ paarweise teilerfremd sind, ist V somit auch schon durch $\prod_{i<j}(X_j - X_i)$ teilbar, das heisst, es gilt $V = c \cdot \prod_{i<j}(X_j - X_i)$ für ein Polynom $c \in \mathbb{Z}[X_1, \ldots, X_n]$.

Für jedes j ist die j-te Spalte der Matrix homogen vom Grad $j-1$ in den Variablen $X_1, \ldots, X_n$, also ist V homogen vom Grad $\sum_{j=1}^{n}(j-1) = \frac{n(n-1)}{2}$. Dies ist aber auch schon der Grad von $\prod_{i<j}(X_j - X_i)$. Folglich muss c den Grad 0 haben; somit ist $c \in \mathbb{Z}$.

In der Vorlesung haben wir c bestimmt, indem wir konkrete Werte eingesetzt haben, für die die Determinante einfach zu berechnen war. Im vorliegenden Fall scheint es keine geeigneten Werte zu geben, daher wählen wir eine andere Methode, nämlich Koeffizientenvergleich. Nach Definition ist

$$V \;=\; \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot X_{\sigma 2}^{1} \cdots X_{\sigma n}^{n-1}.$$

Also ist der Koeffizient von $X_2^1 \cdots X_n^{n-1}$ in V gleich $+1$. Wir behaupten das gleiche für das Polynom $\prod_{1 \leqslant i < j \leqslant n}(X_j - X_i)$. Beim Ausmultiplizieren entsteht nur dann der Term X_n^{n-1}, wenn wir aus allen Faktoren der Form $(X_n - X_i)$ den Term X_n auswählen. Übrig bleibt dann das Produkt $\prod_{1 \leqslant i < j \leqslant n-1}(X_j - X_i)$, für welches wir genauso argumentieren können mit X_{n-1}^{n-2}, und so weiter. Insgesamt zeigt dies, dass beim Ausmultiplizieren nur dann das Monom $X_2^1 \cdots X_n^{n-1}$ entsteht, wenn wir aus jedem Faktor $X_j - X_i$ mit $i < j$ das X_j auswählen. Der Koeffizient von $X_2^1 \cdots X_n^{n-1}$ ist also ebenfalls gleich $+1$. Durch Koeffizientenvergleich folgt somit $c = 1$, und wir sind fertig.

6. Sei R ein Ring, und betrachte das Polynom $f(X) = X^m + aX + b \in R[X]$ mit $m \geqslant 2$. Verifiziere die folgende Formel für die Diskriminante von f:

$$\operatorname{Disc}_f = (-1)^{m(m-1)/2}[(1-m)^{m-1}a^m + m^m b^{m-1}].$$

Lösung: Da f normiert ist, gilt $\operatorname{Disc}_f = (-1)^{m(m-1)/2} \det(\operatorname{Sylv}_{f,f'})$, wobei $\operatorname{Sylv}_{f,f'}$ die Sylvestermatrix von f und seiner Ableitung f' bezeichnet. Wir berechnen dies

mit $f(X) = X^m + aX + b$ und $f'(X) = mX^{m-1} + a$:

$$\mathrm{Sylv}_{f,f'} = \begin{pmatrix} 1 & 0 & \cdots & 0 & a & b & & 0 \\ & \ddots & \cdots & \cdots & \cdots & \ddots & \ddots & \\ 0 & & 1 & 0 & \cdots & 0 & a & b \\ m & \cdots & \cdots & 0 & a & & & 0 \\ & \ddots & & \cdots & \cdots & \ddots & & \\ 0 & & & m & \cdots & 0 & a & \\ & & & & m & \cdots & 0 & a \end{pmatrix}$$

Für jedes $1 \leqslant k \leqslant m-1$ subtrahieren wir das m-fache der k-ten Zeile von der $k+m-1$-ten Zeile. So erhalten wir eine obere Blockdreiecksmatrix mit einer $(m-1) \times (m-1)$-Einheitsmatrix in der oberen linken Ecke und der Nullmatrix unter ihr. Also können wir die ersten $m-1$ Spalten und Zeilen streichen und erhalten

$$\det(\mathrm{Sylv}_{f,f'}) = \det \begin{pmatrix} (1-m)a & -mb & & & & 0 \\ & \ddots & & \ddots & & \\ 0 & & & & (1-m)a & -mb \\ m & 0 & \cdots & \cdots & 0 & a \end{pmatrix}.$$

Durch Entwicklung dieser Determinante nach der letzten Zeile erhalten wir

$$\det(\mathrm{Sylv}_{f,f'}) = m(mb)^{m-1} + a((1-m)a)^{m-1}$$

und berechnen

$$\begin{aligned} \mathrm{Disc}_f &= (-1)^{m(m-1)/2} \det(\mathrm{Sylv}_{f,f'}) \\ &= (-1)^{m(m-1)/2}[m(mb)^{m-1} + a((1-m)a)^{m-1}] \\ &= (-1)^{m(m-1)/2}[(1-m)^{m-1}a^m + m^m b^{m-1}]. \end{aligned}$$

7. Bestimme für jedes der folgenden ganzzahligen Polynome f, ob es separabel in $\mathbb{Q}[X]$ ist, sowie für welche Primzahlen f mod (p) separabel in $\mathbb{F}_p[X]$ ist.

   (a) $f(X) = X^5 + 5X + 5$,

   (b) $f(X) = X^4 - 5X^3 + 6X^2 + 4X - 8$.

   (c) $f(X) = X^5 + 2X^3 + 4$,

   Wie geht es schneller: mit der Diskriminante oder durch Berechnung des grössten gemeinsamen Teilers des Polynoms f und seiner Ableitung f' ?

   Lösung: Nach Proposition 6.5.7 der Vorlesung ist ein Polynom f über einem Körper K genau dann separabel, wenn f und f' teilerfremd sind. Nach Folge 7.4.8 der Vorlesung ist dies auch äquivalent dazu, dass die Diskriminante $\mathrm{Disc}_f \neq 0$ ist. Es genügt also, entweder $\mathrm{ggT}(f, f')$ oder Disc_f zu berechnen. Letzteres benötigt die Determinante der Sylvestermatrix $\mathrm{Sylv}_{f,f'}$. Für $n = \deg(f)$ ist dies eine Matrix der Grösse $(2n-1) \times (2n-1)$, deren Determinante im Allgemeinen relativ aufwendig zu berechnen ist. Die Methode mit dem ggT ist daher oft einfacher.

   (a) Nach Aufgabe 6 hat das Polynom $f(X) = X^5 + 5X + 5$ die Diskriminante

   $$\mathrm{Disc}_f \;=\; (-1)^{5(5-1)/2}[(1-5)^{5-1}5^5 + 5^5 5^{5-1}] \;=\; 4^4 \cdot 5^5 + 5^5 \cdot 5^4 \;=\; 5^5 \cdot 881 \;\neq\; 0.$$

   Folglich ist f separabel in $\mathbb{Q}[X]$. Da 5 und 881 Primzahlen sind, ist f mod (p) in $\mathbb{F}_p[X]$ genau dann separabel, wenn $p \neq 5, 881$ ist.

   Aliter: Nach dem Eisensteinkriterium für $p = 5$ ist das Polynom irreduzibel in $\mathbb{Q}[X]$ und wegen $\mathrm{char}(\mathbb{Q}) = 0$ folglich separabel in $\mathbb{Q}[X]$. Offenbar ist ausserdem $f(X) \equiv X^5$ mod (5) und daher nicht separabel in $\mathbb{F}_5[X]$. Für andere Primzahlen kann man $\mathrm{ggT}(f, f')$ in $\mathbb{F}_p[X]$ berechnen wie in (c).

   (b) Wir berechnen $\mathrm{ggT}(f, f')$ in $\mathbb{Q}[X]$ mit dem euklidischen Algorithmus. Dass der ggT sich nicht ändert, wenn wir die Polynome mit Elementen von $\mathbb{Q}^\times$ multiplizieren, benutzen wir während der Rechnung dazu, dass die Koeffizienten ganzzahlig bleiben.

   $$\begin{aligned}
   \mathrm{ggT}(f, f') &= \mathrm{ggT}(X^4 - 5X^3 + 6X^2 + 4X - 8, 4X^3 - 15X^2 + 12X + 4) \\
   &\sim \mathrm{ggT}(4X^3 - 15X^2 + 12X + 4, X^2 - 4X + 4) \\
   &\sim \mathrm{ggT}(X^2 - 4X + 4, 0) \\
   &\sim X^2 - 4X + 4 \;=\; (X-2)^2.
   \end{aligned}$$

   Folglich ist 2 eine doppelte Nullstelle von $\mathrm{ggT}(f, f')$ und damit eine dreifache Nullstelle von $f(X) = X^4 - 5X^3 + 6X^2 + 4X - 8$. Also ist f nicht separabel in $\mathbb{Q}[X]$, und a fortiori auch nicht in $\mathbb{F}_p[X]$.

(c) Wir berechnen den ggT von f und f' in $\mathbb{Q}[X]$ wiederum mit Hilfe des euklidischen Algorithmus.

$$\begin{aligned}
\mathrm{ggT}(f, f') &= \mathrm{ggT}(X^5 + 2X^3 + 4, 5X^4 + 6X^2) \\
&\sim \mathrm{ggT}(5X^2 + 6, X^3 + 5) \\
&\sim \mathrm{ggT}(5X^2 + 6, 6X - 25) \\
&\sim \mathrm{ggT}(6X - 25, 125X + 36) \\
&\sim \mathrm{ggT}(6X - 25, 3341) \ \sim \ 1.
\end{aligned}$$

Folglich sind f und f' teilerfremd und f ist separabel in $\mathbb{Q}[X]$.

Modulo p: In der obigen Rechnung wurde mit Produkten der Primzahlen 2, 3 und 5 erweitert. Diese Fälle müssen wir deshalb getrennt betrachten. Für alle übrigen Primzahlen gilt die obige Rechnung genauso modulo (p). Wegen $3341 = 13 \cdot 257$ mit 257 prim ist also $f \bmod (p)$ separabel für alle $p \notin \{2, 3, 5, 13, 257\}$ und inseparabel für $p \in \{13, 257\}$.

Für $p = 2$ ist $f(X) \equiv X^5 \bmod (2)$ mit der fünffachen Nullstelle 0; also ist $f \bmod (2)$ inseparabel.

Für $p = 3$ ist $f'(X) = 5X^4 + 6X^2 \equiv 2X^4 \bmod (3)$ mit der vierfachen Nullstelle 0, es gilt jedoch $f(0) = 4 \not\equiv 0 \bmod (3)$. Somit ist $f \bmod (3)$ separabel.

Für $p = 5$ gilt $f'(X) = 5X^4 + 6X^2 \equiv X^2 \bmod (5)$ mit der zweifachen Nullstelle 0, es gilt jedoch $f(0) = 4 \not\equiv 0 \bmod (5)$. Somit ist $f \bmod (5)$ separabel.

Insgesamt ist also $f \bmod (p)$ separabel genau dann, wenn $p \notin \{2, 13, 257\}$ ist.