

Proseminar Lineare Algebra SS10

# Symmetrische Polynome, Diskriminante und Resultante, Fermatscher Satz für Polynome

Natalja Shesterina

Heinrich-Heine-Universität

Betreuung: Prof. Dr. Oleg Bogopolski

## A.Symmetrische Polynome

**Definition 1.** Sei  $n \in \mathbb{N}, n > 1$ ,  $K$  ein kommutativer Ring. Dann heißt ein Polynom  $p \in K[t_1, \dots, t_n]$  symmetrisch in  $t_1, \dots, t_n$ , falls

$$p(t_{\sigma(1)}, \dots, t_{\sigma(n)}) = p(t_1, \dots, t_n)$$

für alle Permutationen  $\sigma \in S_n$  gilt.

**Bemerkung 1.** Die Menge von symmetrischen Polynomen ist ein Unterring von  $K[t_1, \dots, t_n]$ .

**Beispiel 1.** a) Betrachtet man die Polynome

$$p = X + Y - 1$$

und

$$q = X + Y^2,$$

so erhält man durch Vertauschen von  $X$  und  $Y$  die Polynome

$$\tilde{p} = Y + X - 1$$

bzw.

$$\tilde{q} = Y + X^2.$$

Dann erhält man im Fall von  $p$  also dasselbe Polynom, d.h.  $p$  ist symmetrisch in  $X$  und  $Y$ , im Fall  $q$  erhält man ein anderes Polynom,  $q$  ist nicht symmetrisch.

b) Man beachte, dass  $n$  (die Anzahl von Variablen) festgelegt werden muss. So ist

$$f = t_1 + t_2$$

symmetrisch als Polynom in  $t_1, t_2$ , aber nicht symmetrisch als Polynom in  $t_1, t_2, t_3$ , da z.B.

$$f(t_1, t_2, t_3) = t_3 + t_2 \neq f$$

ist.

**Definition 2.** Sei  $x$  eine Variable. Wir bilden ein Polynom

$$f(x) = (x - t_1) \cdots (x - t_n) = x^n - s_1 x^{(n-1)} + s_2 x^{(n-2)} - \cdots + (-1)^n s_n,$$

wobei jedes

$$s_i = s_i(t_1, \dots, t_n)$$

ein Polynom in  $t_1, \dots, t_n$  ist,

$$\begin{aligned}
s_1 &= t_1 + t_2 + \cdots + t_n \\
s_2 &= t_1t_2 + t_1t_3 + \cdots + t_1t_n + t_2t_3 + \cdots + t_{n-1}t_n \\
s_3 &= t_1t_2t_3 + t_1t_2t_4 + \cdots + t_{n-2}t_{n-1}t_n \\
&\vdots \\
s_n &= t_1t_2 \cdots t_n
\end{aligned}$$

Die Polynome  $s_1, s_2, \dots, s_n$  heißen elementarsymmetrische Polynome in  $t_1, \dots, t_n$ . Das Polynom

$$f = x^n - s_1x^{(n-1)} + s_2x^{(n-2)} - \cdots + (-1)^n s_n$$

aus dem Polynomring  $K[t_1, \dots, t_n](x)$  heißt allgemeines Polynom n-ten Grades.

**Definition 3.** Der Grad des Monoms  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$  ist  $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ , und das Gewicht dieses Monoms ist  $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$ . Der Grad bzw. das Gewicht eines Elements  $g \in K[X_1, \dots, X_n]$  ist der größte Grad bzw. das größte Gewicht eines in  $g$  auftretenden Monoms.

**Theorem 1.** Sei  $f(t) \in K[X_1, \dots, X_n]$  ein symmetrisches Polynom vom Grad  $d$ . Dann existiert ein Polynom  $g(X_1, \dots, X_n)$  mit dem Gewicht  $\leq d$ , so dass

$$f(t) = g(s_1, \dots, s_n)$$

gilt (d.h. jedes symmetrische Polynom ist eindeutig darstellbar als Polynom in den elementarsymmetrischen Polynomen  $s_1, \dots, s_n$ ).

*Beweis.* Wir beweisen die Aussage durch vollständige Induktion über  $n$ , und für fixiertes  $n$  durch vollständige Induktion über  $d$ .

Für  $n = 1$  ist die Aussage klar, weil  $s_1 = X_1$ . Sei nun  $n > 1$ . Für  $h \in K[X_1, \dots, X_n]$  bezeichne  $\bar{h}$  das Polynom  $h(X_1, X_2, \dots, X_{n-1}, 0)$  in den Variablen  $X_1, \dots, X_{n-1}$ . Man beachte, dass  $\bar{s}_1, \bar{s}_2, \dots, \bar{s}_{n-1}$  gerade die elementarsymmetrischen Polynome in  $X_1, X_2, \dots, X_{n-1}$  sind.

Sei nun  $f$  wie im Theorem. Dann ist  $\bar{f}$  ein symmetrisches Polynom in  $X_1, X_2, \dots, X_{n-1}$  vom Grad höchstens  $d$ . Nach Induktionsannahme gibt es ein Polynom  $h \in K[X_1, \dots, X_{n-1}]$  vom Gewicht höchstens  $d$  mit  $\bar{f} = h(\bar{s}_1, \dots, \bar{s}_{n-1})$ . Betrachte  $\Delta(X_1, X_2, \dots, X_n) = f(X_1, X_2, \dots, X_n) - h(s_1, \dots, s_{n-1})$ . Offenbar ist  $\Delta$  symmetrisch in  $X_1, X_2, \dots, X_n$  und hat Grad höchstens  $d$ . Wegen  $\Delta(X_1, X_2, \dots, X_{n-1}, 0) = \bar{f} - h(\bar{s}_1, \dots, \bar{s}_{n-1}) = 0$  ist  $\Delta(X_1, X_2, \dots, X_n)$  durch  $X_n$  teilbar. Da  $\Delta$  symmetrisch in den  $X_i$  ist, ist  $\Delta$  durch alle  $X_i$  teilbar. Es gibt also  $r \in K[X_1, \dots, X_n]$  mit  $\Delta(X_1, X_2, \dots, X_n) = X_1 X_2 \dots X_n r(X_1, X_2, \dots, X_n)$ , also  $\Delta = s_n r$ . Da  $\Delta$  einen Grad höchstens  $d$  hat, ist der Grad von  $r$  höchstens  $d - n$ . Nach Induktionsannahme existiert somit ein  $\tilde{g} \in K[X_1, \dots, X_n]$  vom Gewicht höchstens  $d - n$  mit  $r(X_1, X_2, \dots, X_n) = \tilde{g}(s_1, s_2, \dots, s_n)$ . Aus  $f(X_1, X_2, \dots, X_n) = h(s_1, \dots, s_{n-1}) + s_n \tilde{g}(s_1, s_2, \dots, s_n)$  folgt schließlich die Behauptung. □

**Beispiel 2.** a) Sei gegeben  $n = 2$ ,

$$f = (x_1 - x_2)^2,$$

bestimme  $g_s(x_1, x_2)$  mit  $f = g_s(s_1, s_2)$ .

Offensichtlich ist  $s$  symmetrisch,

$$f = x_1^2 - 2x_1x_2 + x_2^2,$$

$$s_1 = x_1 + x_2, s_2 = x_1x_2$$

In  $f$  ist  $x_1^2$  mit Exponentialpaar  $(2, 0)$  ein Monom mit maximalem Gewicht. Somit gilt nach Theorem 1:

$$g_1(s_1, s_2) = s_1^{2-0} s_2^0 = s_1^2 = (x_1 + x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2.$$

Es gilt

$$f - g_1(s_1, s_2) = -4x_1x_2.$$

Bestimme wieder ein Monom mit maximalem Gewicht. Es ist  $x_1x_2$  mit  $(1, 1)$  als Exponentialpaar. Deswegen gilt  $g_2(s_1, s_2) = -4s_1^{1-1} s_2^1 = -4s_2$  und

$$f - g_1(s_1, s_2) - g_2(s_1, s_2) = 0.$$

Daraus folgt

$$f = s_1^2 - 4s_2, g_s = x_1^2 - 4x_2$$

b) Zu

$$f := x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$$

gebe ein Polynom  $g_s(x_1, x_2, x_3)$  mit  $f = g_s(s_1, s_2, s_3)$  an. Da  $s$  symmetrisch ist, gibt es also nach Theorem 1 ein solches Polynom  $g_s$ . Man geht, wie bei dem obigen Beispiel vor.

Das größte Monom in  $f$  ist  $x_1^2x_2^2$ , das zugehörige Exponentialtripel ist  $(2, 2, 0)$ . Daher definiert man

$$h_1 = g_1(s_1, s_2, s_3) = s_1^{2-2} s_2^{2-0} s_3^0 = s_2^2 = (x_1x_2 + x_1x_3 + x_2x_3)^2 = x_1^2x_2^2 + \dots + 2x_1^2x_2x_3 + \dots$$

Es ist

$$g - h_1 = -2x_1^2x_2x_3 + \dots$$

Das größte Monom in  $f - h_1$  ist  $x_1^2x_2x_3$ , und das zugehörige Exponentialtripel ist  $(2, 1, 1)$ . Daher setzt man

$$h_2 = s_1^{2-1} s_2^{1-1} s_3^1 = s_1s_3 = (x_1 + x_2 + x_3)x_1x_2x_3 = x_1^2x_2x_3 + \dots$$

Man sieht, dass  $f - h_1 = -2h_2$  ist. Daher gilt

$$f = h_1 - 2h_2 = s_2^2 - 2s_1s_3.$$

Das gesuchte Polynom  $g_s$  ist also  $g_s = x_2^2 - 2x_1x_3$ .

c) (Als Übung)

Zu  $f = (x_2 - x_1)^2(x_3 - x_1)^2(x_3 - x_2)^2$ ,  $n = 3$  gebe ein Polynom  $g_s(x_1, x_2, x_3)$  mit  $g_s(s_1, s_2, s_3)$  an.

Die Lösung:  $f = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2$  und  $g_s = x_1^2x_2^2 - 4x_1^3x_3 - 4x_2^3 + 18x_1x_2x_3 - 27x_3^2$

## B. Die Diskriminante

**Definition 4.** Sei  $K$  ein Körper und  $f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in K[x]$  ein Polynom. Ferner seien  $\alpha_1, \dots, \alpha_n$  die Nullstellen von  $f$ . Dann nennen wir

$$D(f) := a_0^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2$$

die Diskriminante von  $f$ .

**Satz 1.** Sei Grad  $f = n$ . Dann kann man ein Polynom  $g$  über  $K$  in  $n$  Unbestimmten berechnen mit

$$D(f) = a_0^{2n-2} g\left(\frac{-a_1}{a_0}, \frac{a_2}{a_0}, \dots, \frac{(-1)^n a_n}{a_0}\right).$$

*Beweis.* Ersetzen wir  $\alpha_1, \dots, \alpha_n$  in der Definition von  $D(f)$  durch Unbestimmte  $x_1, \dots, x_n$ , so erhält man ein Polynom  $D(x_1, \dots, x_n)$  aus  $K[x_1, \dots, x_n]$ . Ist  $\sigma \in S_n$  eine beliebige Permutation, so liefert  $\{i, j\} \mapsto \{\sigma(i), \sigma(j)\}$  eine Permutation der Menge  $\{\{i, j\} : i \neq j \wedge i, j \in \{1, \dots, n\}\}$ . Jedem solchen Paar entspricht genau ein Term  $(x_i - x_j)^2$  mit  $i < j$ . Daher entsprechen diese Terme umkehrbar eindeutig den Termen  $(x_{\sigma(i)} - x_{\sigma(j)})^2$ , denn das Vorzeichen spielt wegen des Quadrats keine Rolle. Damit ist

$$d(x_1, \dots, x_n) := \prod_{i < j} (x_i - x_j)^2 = \prod_{i < j} (x_{\sigma(i)} - x_{\sigma(j)})^2 = d(x_{\sigma(1)}, \dots, x_{\sigma(n)}),$$

$d$  ist ein symmetrisches Polynom. Nach dem Theorem 1 gibt es ein Polynom  $g \in K[x_1, \dots, x_n]$ , das wir effektiv berechnen können, mit  $d(x_1, \dots, x_n) = g(s_1, \dots, s_n)$ . Nun ist

$$\prod (x - \alpha_j) = \frac{1}{a_0} f = x^n + \frac{a_1}{a_0} x^{n-1} + \dots + \frac{a_n}{a_0}.$$

Nach Definition der elementarsymmetrischen Polynome folgt:

$$s_j(\alpha_1, \dots, \alpha_n) = (-1)^j \frac{a_j}{a_0}.$$

Dies ergibt

$$D(f) = a_0^{2n-2} g\left(\frac{-a_1}{a_0}, \frac{a_2}{a_0}, \dots, \frac{(-1)^j a_j}{a_0}\right).$$

□

**Beispiel 3.** Mit Hilfe der Ergebnissen aus dem Beispiel 2:

$$(x_2 - x_1)^2 = s_1^2 - 4s_2$$

und

$$(x_1 - x_2)^2 (x_3 - x_1)^2 (x_3 - x_2)^2 = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18s_1 s_2 s_3 - 27s_3^2$$

berechne die Diskriminanten vom Polynom zweiten und dritten Grades aus  $K[x]$ .

Lösung: Sei  $f = a_0x^2 + a_1x + a_2$ . Dann nach Theorem 1 und Satz 1 gilt:

$$\text{für } n = 2: D(f) = a_0^2 \left( \frac{a_1^2}{a_0} - 4 \frac{a_2}{a_0} \right) = a_1^2 - 4a_0a_2.$$

Sei nun  $n = 3$  und  $f = a_0x^3 + a_1x^2 + a_2x + a_3$ . Dann ist

$$D(f) = a_0^4 \left( \frac{a_1^2 a_2}{a_0^2} - 4 \frac{(-a_1^3)(-a_3)}{a_0^3 a_0} - 4 \frac{a_2^3}{a_0^3} + 18 \frac{(-a_1)a_2(-a_3)}{a_0 a_0 a_0} - 27 \frac{a_3^2}{a_0^2} \right) = a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_0 a_2^3 + 18a_0 a_1 a_2 a_3 - 27a_0^2 a_3^2.$$

**Insbesondere:** für  $a_0 = 1$  und  $a_1 = 0$  folgt für das Polynom  $f(x) = x^3 + a_2x + a_3$   
 $D(f) = -4a_2^3 - 27a_3^2$ .

**Beispiel 4.** Berechne die Diskriminante für  $f = 2x^2 + 5x + 8$ .

Lösung:  $D(f) = a_1^2 - 4a_0a_2$  für  $f = a_0x^2 + a_1x + a_2$  liefert  $D(f) = 25 - 4 \cdot 2 \cdot 8 = -39$   
(d.h.  $f$  hat 2 verschiedene Nullstellen in  $\mathbb{C} \setminus \mathbb{R}$ ).

## C. Fermatscher Satz für Polynome

**Theorem 2.** (Mason-Stothers): Seien  $a(t), b(t)$  und  $c(t)$  teilerfremde, nicht-konstante Polynome mit  $a + b = c$ . Dann ist

$$\max(\text{grad}\{a, b, c\}) \leq N_0(abc) - 1,$$

wobei  $N_0(c)$  die Anzahl der verschiedenen Nullstellen von  $c$  ist.

*Beweis.* Dividiere Polynome  $a, b$  durch  $c$ , und definiere  $f := \frac{a}{c}, g := \frac{b}{c}$ , dann ergibt sich, dass  $f + g = 1$ , wobei  $f, g$  rationale Funktionen sind.

Durch Differenzieren, erhalten wir  $f' + g' = 0$ , schreiben das als

$$\frac{f'f}{f} + \frac{g'g}{g} = 0,$$

so dass

$$\frac{b}{a} = \frac{g}{f} = \frac{-f'}{g'}.$$

Wir definieren:

$$a(t) = c_1 \prod (t - \alpha_i)^{m_i}$$

$$b(t) = c_2 \prod (t - \beta_j)^{n_j}$$

$$c(t) = c_3 \prod (t - \gamma_k)^{r_k}$$

Dann bekommen wir

$$\frac{b}{a} = \frac{-f'}{g'} = - \frac{\sum \frac{m_i}{t - \alpha_i} - \sum \frac{r_k}{t - \gamma_k}}{\sum \frac{n_j}{t - \beta_j} - \sum \frac{r_k}{t - \gamma_k}}.$$

Ein gemeinsamer Nenner für  $f'/f$  und  $g'/g$  ist das Produkt

$$N_0 = \prod (t - \alpha_i) \prod (t - \beta_j) \prod (t - \gamma_k),$$



**Satz 3.** Seien  $f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m$  und  $g(x) = b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n$  Polynome. Dann:

1) Es existieren Polynome  $G(x)$  und  $F(x)$ , so dass  $\text{grad}(G) < m, \text{grad}(F) < n$  ist und

$$\text{res}(f, g) = fG + gF$$

gilt.

2)  $\text{res}(f, g) = 0 \iff f, g$  einen gemeinsamen Faktor haben, der von  $x$  abhängt oder  $a_0 = b_0 = 0$  ist.

3)  $\text{res}(f, g)$  ist als eine Funktion von  $a_0, \dots, a_n$  homogen von Grad  $m$  und ist als eine Funktion von  $b_0, \dots, b_n$  homogen von Grad  $n$ .

4) Seien  $\alpha_1, \dots, \alpha_n$  Nullstellen von  $f(x)$  und seien  $\beta_1, \dots, \beta_m$  Nullstellen von  $g(x)$ . Dann gilt

$$\text{res}(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^m f(\beta_j) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

*Beweis.* von 4). Sei  $y$  eine Unbekannte. Dann ist  $g(x) - y = b_0x^m + \dots + b_{m-1}x + (b_m - y)$  und so ist  $\text{res}(f(x), g(x) - y)$  ein Polynom von  $y$  (siehe Definition von Resultant). Wir bezeichnen

$$R(y) = \text{res}(f(x), g(x) - y).$$

Setzen wir  $y_i = g(\alpha_i)$ , wobei  $\alpha_i$  eine Nullstelle von  $f(x)$  ist,  $i = 1, \dots, n$ . Dann gilt

$$R(y_i) = \text{res}(f(x), g(x) - g(\alpha_i)).$$

Die Polynome  $f(x)$  und  $g(x) - g(\alpha_i)$  haben eine gemeinsame Nullstelle  $x = \alpha_i$ , also sie haben einen gemeinsamen Faktor  $x - \alpha_i$ . Aus 2) folgt dann  $R(y_i) = 0$ . Dann ist  $(y - y_i)$  ein Teiler von  $R(y)$ .

**Fall 1.** Sei  $y_1, \dots, y_n$  verschieden. Dann ist  $\prod_{i=1}^n (y - y_i)$  ein Teiler von  $R(y)$ . Wenn man die Definition von  $R(y)$  mit Achtung analysiert, stellt man fest, dass Polynom  $R(y)$  Grad  $n$  und die Hauptkoeffiziente  $(-1)^n a_0^m$  hat. Deswegen gilt

$$R(y) = (-1)^n a_0^m \prod_{i=1}^n (y - y_i).$$

Setzen wir  $y = 0$ , erhalten wir

$$\text{res}(f(x), g(x)) = R(0) = a_0^m \prod_{i=1}^n y_i = a_0^m \prod_{i=1}^n g(\alpha_i). \quad (0.1)$$

**Fall 2.** Sei  $y_1, \dots, y_n$  nicht unbedingt verschieden, Wir skizzieren eine Idee. Betrachten wir  $\alpha'_1, \dots, \alpha'_n$ , so dass  $\alpha'_i$  nah zu  $\alpha_i$  ist und  $y'_1, \dots, y'_n$  verschieden sind (hier, wie oben,  $y'_i = g(\alpha'_i)$ ).

Dann sind die Koeffizienten von  $\Phi(x) = a_0 \prod_{i=1}^n (x - \alpha'_i)$  nah zu Koeffizienten von  $f(x) = a_0 \prod_{i=1}^n (x - \alpha_i)$  und so ist  $\text{res}(\Phi(x), g(x))$  nah zu  $\text{res}(f(x), g(x))$ . Nach Fall 1 gilt  $\text{res}(\Phi(x), g(x)) = a_0^m \prod_{i=1}^n g(\alpha'_i)$ . Streben wir  $\alpha'_i \rightarrow \alpha_i$ , erhalten wir

$$\text{res}(f(x), g(x)) = a_0^m \prod_{i=1}^n g(\alpha_i).$$

□

**Satz 4.** *Es sei  $f \in K[x]$  ein normiertes Polynom vom Grad  $m > 0$  und  $f'$  seine Ableitung. Dann besteht zwischen der Diskriminante  $D(f)$  und der Resultante  $\text{res}(f, f')$  die folgende Beziehung:*

$$D(f) = (-1)^{m(m-1)/2} \text{res}(f, f').$$

*Beweis.* Angenommen, dass  $f$  über  $K[x]$  vollständig in Linearfaktoren zerfällt. Es gelte also  $f = \prod_{i=1}^m (x - \alpha_i)$ . Dann folgt aus dem Satz 3

$$\text{res}(f, f') = \prod_{i=1}^m f'(\alpha_i).$$

Aufgrund der Produktregel ergibt sich

$$f' = \sum_{i=1}^m (x - \alpha_1) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots (x - \alpha_m)$$

und somit gilt

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_m).$$

Dies bedeutet aber

$$\text{res}(f, f') = \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{m(m-1)/2} \prod_{i < j} (\alpha_i - \alpha_j)^2 = (-1)^{m(m-1)/2} D(f).$$

□

**Beispiel 5.** *Sei  $f = x^3 + px + q$  gegeben, berechne  $D(f)$ . Nach dem Satz 4 gilt:*

$$\text{res}(f', f) = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 0 & 0 & -2p & -3q \\ 0 & 0 & 3 & 0 & p \end{vmatrix}$$

*Nun liefert Entwicklung nach Laplace:*

$$D(f) = \text{res}(f, f') = -4p^3 - 27q^2.$$