Hauptsatz über elementarsymmetrische Polynome

$$\begin{aligned}
f = x^4 + ax^3 + bx^2 + cx + d &= (x - x_1)(x - x_2)(x - x_3)(x - x_4) \\
&= x^4 - (x_1 + x_2 + x_3 + x_4)x^3 \\
&\quad + (x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4)x^2 \\
&\quad - (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)x \; + \; x_1x_2x_3x_4
\end{aligned}$$

Für das Polynom f bedeutet das ($n = 4$):

$$\begin{aligned}
e_1 = \sum_{i=1}^{n} x_i = x_1 + x_2 + x_3 + x_4 &= -a \\
e_2 = \sum_{i<j}^{n} x_ix_j = x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4 &= b \\
e_3 = \sum_{i<j<k}^{n} x_ix_jx_k = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -c \\
e_4 = x_1x_2x_3x_4 &= d
\end{aligned}$$

Die e_i sind die *elementarsymmetrischen* Polynome für $n = 4$, x_i als Variablen betrachtet, *symmetrisch*, weil jede Permutation der Indizes das Polynom in sich überführt (die Koeffizienten hängen schließlich nicht von der Nummerierung der Nullstellen ab), und *elementar* aufgrund von:

Jedes in den Variablen $x_1, \ldots, x_n$ symmetrische Polynom ist ein Polynom in den elementarsymmetrischen Polynomen, d. h.:

Sei $f(x_1, \ldots, x_n)$ ein symmetrisches Polynom, dessen Koeffizienten ganze (oder rationale, reelle, komplexe) Zahlen sind. Dann gibt es ein Polynom h mit ganzen (oder rationalen, reellen, komplexen) Koeffizienten, so dass $f(x_1, \ldots, x_n) = h(e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n))$ ist.

Beispiele

$$\begin{aligned}
x_1^2 + x_2^2 &= (x_1 + x_2)^2 - 2(x_1x_2) \\
x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) \\
x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 &= (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - 3x_1x_2x_3
\end{aligned}$$

Die Summanden eines symmetrischen Polynoms f können wir lexikographisch mit den Monomen $x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$ ordnen, die Koeffizienten spielen hierbei keine Rolle: $x_1^7x_2^5x_3 > x_1^7x_2^4x_3^2x_4^7 > x_1^7x_2^3x_4^6$
Ein Summand ist lexikographisch größer, wenn der erste Exponent von links beginnend größer ist. Ein Exponent kann auch null sein. Zu jedem Monom gibt es nur endlich viele lexikographisch kleinere Monome, falls die Exponenten begrenzt sind.

Sei nun $x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$ der lexikographisch größte Summand in f. Es wird ein symmetrisches Polynom g_1 mit gleichem größten Summand konstruiert, der dann in $f - g_1$ herausfällt. Dieses Verfahren kann für das symmetrische Polynom $f - g_1$ wiederholt werden, usw. Es entstehen stets lexikographisch kleinere Monome, bis man schließlich nach k Schritten bei 0 angelangt ist: $f - g_1 - g_2 - \ldots - g_k = 0$,
$f = g_1 + g_2 + \ldots + g_k$.

Sei für f mit $n = 3$ der größte Summand $a x_1^{m_1} x_2^{m_2} x_3^{m_3}$ mit $m_1 = 7,\ m_2 = 4,\ m_3 = 2$.

Es muss dann $m_1 \geq m_2 \geq m_3$ sein. Wäre z. B. $x_1^4 x_2^7 x_3^2$, so gäbe es eine Permutation (f ist symmetrisch, x_1 wird mit x_2 vertauscht), die ein größeres Monom $x_2^4 x_1^7 x_3^2 = x_1^7 x_2^4 x_3^2$ hervorbringt.

Der größte Summand von

$$\begin{aligned}
g_1 &= a\, e_1^{m_1-m_2}\, e_2^{m_2-m_3}\, e_3^{m_3} \\
&= a\,(x_1+x_2+x_3)^{m_1-m_2}\,(x_1x_2+x_1x_3+x_2x_3)^{m_2-m_3}\,(x_1x_2x_3)^{m_3} \\
&= a\,(x_1^7x_2^4x_3^2 + 2x_1^7x_2^3x_3^3 + x_1^7x_2^2x_3^4 + 3x_1^6x_2^5x_3^2 + 11x_1^6x_2^4x_3^3 + 11x_1^6x_2^3x_3^4 + 3x_1^6x_2^2x_3^5 \\
&\quad + 3x_1^5x_2^6x_3^2 + 18x_1^5x_2^5x_3^3 + 31x_1^5x_2^4x_3^4 + 18x_1^5x_2^3x_3^5 + 3x_1^5x_2^2x_3^6 + x_1^4x_2^7x_3^2 + 11x_1^4x_2^6x_3^3 + \ldots)
\end{aligned}$$

ist $a x_1^{m_1-m_2}(x_1x_2)^{m_2-m_3}(x_1x_2x_3)^{m_3} = a x_1^{m_1} x_2^{m_2} x_3^{m_3}$. $\square$

Schauen wir uns ein Beispiel an, f ist symmetrisch.

$$\begin{aligned}
f &= (x_1-x_2)^2 && n=2 \\
&= x_1^2 - 2x_1x_2 + x_2^2 && e_1 = x_1+x_2,\ e_2 = x_1x_2 \\
\text{größter Summand}\quad & x_1^2 \\
g_1 &= e_1^{2-0}\, e_2^0 = e_1^2 \\
&= (x_1+x_2)^2 \\
&= x_1^2 + 2x_1x_2 + x_2^2 \\
f - g_1 &= -4x_1x_2 && \text{größter Summand} \\
g_2 &= -4e_1^{1-1}\, e_2^1 = -4e_2 \\
f - g_1 - g_2 &= 0 \\
f &= g_1 + g_2 \\
&= e_1^2 - 4e_2 \\
f &= (x_1+x_2)^2 - 4x_1x_2
\end{aligned}$$

Weiteres Beispiel, f ist symmetrisch.

$$
\begin{array}{rcll}
f & = & x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 & n = 3 \\
 & & & e_1 = x_1 + x_2 + x_3,\ e_2 = x_1x_2 + x_1x_3 + x_2x_3,\ e_3 = x_1x_2x_3 \\
\text{größter Summand} & & x_1^2x_2^2 & \\
g_1 & = & e_1^{2-2}\,e_2^{2-0}\,e_3^0 = e_2^2 & \\
 & = & (x_1x_2 + x_1x_3 + x_2x_3)^2 & \\
 & = & x_1^2x_2^2 + 2x_1^2x_2x_3 + x_1^2x_3^2 + \dots & \\
f - g_1 & = & -2x_1^2x_2x_3 - 2x_1x_2^2x_3 - 2x_1x_2x_3^2 & \\
 & & -2x_1^2x_2x_3 & \text{größter Summand} \\
g_2 & = & -2e_1^{2-1}\,e_2^{1-1}\,e_3^1 = -2e_1e_3 & \\
 & = & -2(x_1 + x_2 + x_3)x_1x_2x_3 & \\
 & = & -2x_1^2x_2x_3 - 2x_1x_2^2x_3 - 2x_1x_2x_3^2 & \\
f - g_1 - g_2 & = & 0 & \\
f & = & g_1 + g_2 & \\
 & = & e_2^2 - 2e_1e_3 & \\
f & = & (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2(x_1 + x_2 + x_3)x_1x_2x_3 &
\end{array}
$$

Eindeutigkeit

Die Darstellung eines jeden in den Variablen $x_1, \dots, x_n$ symmetrischen Polynoms als Polynom in den elementarsymmetrischen Polynomen ist eindeutig.

Der indirekte Nachweis ist einfach.
Aus $f(\sigma_1, \sigma_1, \dots, \sigma_n) = g(\sigma_1, \sigma_1, \dots, \sigma_n)$ folgt $h(\sigma_1, \sigma_1, \dots, \sigma_n) = 0$.
Es kann nun gezeigt werden, dass die Einsetzung in ein von null verschiedenes Polynom ungleich null ist.
Schreibweise $n = 3$

$$\begin{aligned}
h(\sigma_1, \sigma_1, \sigma_3) &= a_1 \sigma_1^{m_1'} \sigma_2^{m_2'} \sigma_3^{m_3'} + a_2 \sigma_1^{m_1''} \sigma_2^{m_2''} \sigma_3^{m_3''} + \dots \\
&= a_1 (x_1 + x_2 + x_3)^{m_1'} (x_1x_2 + x_1x_3 + x_2x_3)^{m_2'} (x_1x_2x_3)^{m_3'} \\
&\qquad + a_2 (x_1 + x_2 + x_3)^{m_1''} (x_1x_2 + x_1x_3 + x_2x_3)^{m_2''} (x_1x_2x_3)^{m_3''} \\
&\qquad + \dots \\
&= a_1 x_1^{m_1'+m_2'+m_3'} x_2^{m_2'+m_3'} x_3^{m_3'} + \dots \quad \text{Terme lexikographisch kleiner} \\
&\qquad + a_2 x_1^{m_1''+m_2''+m_3''} x_2^{m_2''+m_3''} x_3^{m_3''} + \dots \quad \text{Terme lexikographisch kleiner} \\
&\qquad + \dots
\end{aligned}$$

Der von den blau hervorgehobenen Termen lexikographisch Größte $a_k x_1^{m_1+m_2+m_3} x_2^{m_2+m_3} x_3^{m_3}$ kann durch keinen Summanden aufgehoben werden, $h(\sigma_1, \sigma_1, \sigma_3)$ ist nicht das Null-Polynom.

Zu ergänzen ist noch, dass der lexikographisch größte Term eindeutig bestimmt ist.

Aus $a_i x_1^{m_1'+m_2'+m_3'} x_2^{m_2'+m_3'} x_3^{m_3'} = a_j x_1^{m_1''+m_2''+m_3''} x_2^{m_2''+m_3''} x_3^{m_3''}$ folgt

$$a_i = a_j,\ m_3' = m_3'',\ m_2' = m_2''\ ,\ m_1' = m_1''.$$

Diskriminante

Sei $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ ein Polynom mit den (nicht notwendig verschiedenen) Nullstellen $x_1, \ldots, x_n$. Es ist $f = (x - x_1)(x - x_2)\ldots(x - x_n)$ und $a_{n-i} = (-1)^i e_i(x_1, \ldots, x_n)$, z.B. für $n = 3$:

$$\begin{aligned} f = x^3 + a_2 x^2 + a_1 x + a_0 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - \underbrace{(x_1 + x_2 + x_3)}_{e_1} x^2 + \underbrace{(x_1x_2 + x_1x_3 + x_2x_3)}_{e_2} x - \underbrace{x_1x_2x_3}_{e_3} \end{aligned}$$

Somit gilt:

$$\begin{aligned} -(x_1 + x_2 + x_3) &= a_2 \\ x_1x_2 + x_1x_3 + x_2x_3 &= a_1 \\ -x_1x_2x_3 &= a_0 \end{aligned}$$

Die Koeffizienten einer normierten Polynomgleichung sind bis auf Vorzeichen die elementarsymmetrischen Funktionen in den Lösungen.

Die Diskriminante $D = (x_1 - x_2)^2(x_1 - x_3)^2 \ldots (x_{n-1} - x_n)^2$ (lat. discriminare unterscheiden)
ist ein Term, der genau dann null ist, wenn (mindestens) zwei Lösungen gleich sind. $D = \prod\limits_{1 \le i < j \le n} (x_i - x_j)^2$
besteht aus $\binom{n}{2}$ Faktoren und hängt wegen der Quadrate nicht von der Nummerierung der x_i ab, ist somit symmetrisch in $x_1, \ldots, x_n$, daher als Polynom in den elementarsymmetrischen Funktionen, also den Koeffizienten von f darstellbar. Beachte: D kann ohne Kenntnis der Nullstellen ausgerechnet werden.

$$\begin{aligned} f &= x^2 + px + q & & n = 2,\ e_1 = x_1 + x_2 = -p,\ e_2 = x_1x_2 = q \\ D &= (x_1 - x_2)^2 \\ &= (x_1 + x_2)^2 - 4x_1x_2 \\ &= e_1^2 - 4e_2 = p^2 - 4q \end{aligned}$$

$$\begin{aligned} D &= (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 & & n = 3 \\ &= e_1^2e_2^2 - 4e_1^3e_3 - 4e_2^3 + 18e_1e_2e_3 - 27e_3^2 & & \text{ohne Rechnung, dann folgt für} \\ f &= x^3 + px + q & & e_1 = x_1 + x_2 + x_3 = 0,\ e_2 = x_1x_2 + x_2x_3 + x_1x_3 = p \\ & & & -e_3 = -x_1x_2x_3 = q \\ D &= -4e_2^3 - 27e_3^2 = -4p^3 - 27q^2 \end{aligned}$$

Alternativ kann $D = -4p^3 - 27q^2$ direkt durch eine längere Rechnung erhalten werden.
In $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ wird jeweils $(x_i - x_j)^2$ durch $(x_i + x_j)^2 - 4x_ix_j$ ersetzt, Klammern aufgelöst, mit $x_1x_2x_3 = -q$ vereinfacht, x_i^3 durch $-px_i - q$ ersetzt, ausgeklammert und weiter mit $x_1x_2 + x_2x_3 + x_1x_3 = p$ und $x_1 + x_2 + x_3 = 0$ vereinfacht.