2 Symmetric polynomials and their applications

Oleg Demchenko, St.Petersburg State University

2.1 Polynomials in several variables

A **monomial** over a field k in n variables $x_1, \ldots, x_n$ is an algebraic expression $ax_1^{i_1} \cdots x_n^{i_n}$. Its **degree** is defined as $i_1 + \cdots + i_n$. A **polynomial** over k in n variables is the sum of a finite number of monomials:

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n},$$

where only a finite number of $a_{i_1, \ldots, i_n}$ is non-zero.

Two polynomials are equal if and only if their coefficients are pairwise equal. The set of polynomials over k in variables $x_1, \ldots, x_n$ is denoted by $k[x_1, \ldots, x_n]$.

Remind that the operations on $k[x]$ can be expressed as

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i, \quad \left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} \left(\sum_{j+\ell=i} a_j b_\ell \right) x^i.$$

The operations on $k[x_1, \ldots, x_n]$ are defined in a similar manner:

$$\sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} + \sum_{i_1, \ldots, i_n = 0}^{\infty} b_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum_{i_1, \ldots, i_n = 0}^{\infty} (a_{i_1, \ldots, i_n} + b_{i_1, \ldots, i_n}) x_1^{i_1} \cdots x_n^{i_n},$$

$$\left(\sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} \right) \left(\sum_{i_1, \ldots, i_n = 0}^{\infty} b_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} \right) = \sum_{i_1, \ldots, i_n = 0}^{\infty} \left(\sum_{\substack{j_1+\ell_1=i_1 \\ \cdots \\ j_n+\ell_n=i_n}} a_{j_1, \ldots, j_n} b_{\ell_1, \ldots, \ell_n} \right) x_1^{i_1} \cdots x_n^{i_n}.$$

One can easily see that the operations are correctly defined, i.e., the results always have only a finite number of non-zero coefficients.

One can show that the operations are associative, commutative and multiplication is distributive over addition.

Definition. A polynomial is **homogeneous** of degree m if it is the sum of monomials of degree m.

Example. The polynomial $f = 2x^4y - 4x^2y^3 + y^5$ is homogeneous of degree 5.

Proposition 2.1. *A polynomial $f \in k[x_1, \ldots, x_n]$ is homogeneous of degree m if and only if*

$$f(\lambda x_1, \ldots, \lambda x_n) = \lambda^m f(x_1, \ldots, x_n)$$

for a variable λ.

Proof. If

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

then the condition $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^m f(x_1, \ldots, x_n)$ is equivalent to the condition

$$\sum_{i_1,\ldots,i_n=0}^{\infty} \lambda^{i_1+\cdots+i_n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum_{i_1,\ldots,i_n=0}^{\infty} \lambda^m a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

which is satisfied if and only if $a_{i_1,\ldots,i_n} = 0$ whenever $i_1 + \cdots + i_n \neq m$. $\square$

2.2 Symmetric polynomials

Definition. A polynomial $f(x_1, \ldots, x_n)$ is **symmetric** if for any permutation of the variables $f(x_{s_1}, \ldots, x_{s_n}) = f(x_1, \ldots, x_n)$.

Clearly, the sum and the product of symmetric polynomials are symmetric.

Example. The polynomial $f(x, y, z) = x^2 + y^2 + z^2 + 2xy + 2yz + 2xz$ is symmetric, since $f(x, y, z) = f(x, z, y) = f(y, z, x) = f(y, x, z) = f(z, x, y) = f(z, y, x)$. The polynomial $f(x, y, z) = x^2 + y^2 + z^2 + 2xz + 2yz$ is not symmetric because although $f(x, y, z) = f(y, x, z)$, but $f(x, y, z) \neq f(x, z, y)$.

The **elementary symmetric polynomial** of degree k in n variables is

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 \ldots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

In particular,

$$\begin{aligned}
\sigma_1 &= x_1 + \ldots + x_n \\
\sigma_2 &= x_1x_2 + x_2x_3 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
\sigma_n &= x_2 \cdots x_n + x_1x_3 \cdots x_n + \cdots + x_1 \cdots x_{n-1} \\
\sigma_n &= x_1 \cdots x_n
\end{aligned}$$

It is obvious that the elementary symmetric polynomials are homogeneous.

The elementary symmetric polynomials arise naturally from the formula:

$$(x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^i \sigma_i x^{n-i} + \cdots + (-1)^n \sigma_n.$$

It implies

Theorem 2.2 (Vieta's formulas)**.** *Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with n (not necessarily distinct) roots $x_1, \ldots, x_n$. Then $\sigma_k(x_1, \ldots, x_n) = (-1)^k \frac{a_{n-k}}{a_n}$.*

When $n = 2$ the theorem gives the well-known formulas about the sum and product of the roots x_1, x_2 of the quadratic equation $a_2 x^2 + a_1 x + a_0 = 0$:

$$x_1 + x_2 = -\frac{a_1}{a_2}, \qquad x_1 x_2 = \frac{a_0}{a_2}.$$

We introduce an order on the monomials: the monomial $u = a x_1^{i_1} \cdots x_n^{i_n}$ is less than the monomial $v = b x_1^{j_1} \cdots x_n^{j_n}$ (this is denoted by $u \prec v$), if there is an index $1 \leq t \leq n$ such that $i_1 = j_1, \ldots, i_{t-1} = j_{t-1}$ and $i_t > j_t$. This order is called the **lexicographic order**. One can see that for any two different monomials u, v in a given polynomial either $u \succ v$ or $u \prec v$.

The largest monomial of the polynomial f with respect to the lexicographic order is called its **leading monomial** and denoted by $\mathrm{LT}(f)$.

Example. A polynomial with monomials going in the lexicographic order

$$f = 2x_1^2x_2^2x_3 + 3x_1^2x_2x_3^3 - x_1x_2^4x_3^2 + x_1x_2^4x_3,$$

with $\mathrm{LT}(f) = 2x_1^2x_2^2x_3$.

Lemma 2.3. *The leading monomial of the product of two polynomials is equal to the product of their leading monomials.*

Proof. It suffices to show that if u, v are monomials and $u \succ v, u' \succ v'$, then $uu' \succ vv'$. Let $u = ax_1^{i_1}\cdots x_n^{i_n}, u' = a'x_1^{i'_1}\cdots x_n^{i'_n}$ and $v = bx_1^{j_1}\cdots x_n^{j_n}, v' = b'x_1^{j'_1}\cdots x_n^{j'_n}$. Then for some indices $1 \le t, t' \le n$ one has $i_1 = j_1, \ldots, i_{t-1} = j_{t-1}, i_t > j_t$ and $i'_1 = j'_1, \ldots, i'_{t'-1} = j'_{t'-1}, i'_{t'} > j'_{t'}$. Suppose that t and t' are not equal, for example $t' > t$. Then $i_1 + i'_1 = j_1 + j'_1, \ldots, i_{t-1} + i'_{t-1} = j_{t-1} + j'_{t-1}$ и $i_t + i'_t > j_t + i'_t = j_t + j'_t$. If $t = t'$, then $i_1 + i'_1 = j_1 + j'_1, \ldots, i_{t-1} + i'_{t-1} = j_{t-1} + j'_{t-1}$ and $i_t + i'_t = i_t + i'_{t'} > j_t + j'_{t'} = j_t + j'_t$. ☐

Lemma 2.4. *If $u = ax_1^{i_1}\cdots x_n^{i_n}$ is the leading monomial of a symmetric polynomial f, then $i_1 \ge \cdots \ge i_n$.*

Proof. Assume the contrary. Then $i_k < i_{k+1}$ for some $1 \le k < n$. Swap of the variables x_k and x_{k+1} in f does not change f which implies that the monomial $u' = ax_1^{i_1}\cdots x_k^{i_{k+1}}x_{k+1}^{i_k}\cdots x_n^{i_n}$ is in f and thus $u' \prec u$. But obviously $u' \succ u$, a contradiction. ☐

Theorem 2.5 (Fundamental theorem of symmetric polynomials)**.** *Any symmetric polynomial in n variables over k can be represented as a polynomial in $\sigma_1, \ldots, \sigma_n$ with coefficients from k and this representation is unique.*

Proof. Any polynomial can be uniquely split into the sum of homogeneous polynomials of different degrees. If the polynomial is symmetric, then due to uniqueness of such expansion its homogeneous components are also symmetric. Therefore the theorem may be proved for symmetric homogeneous polynomials.

Let f be a symmetric homogeneous polynomial with $\mathrm{LT}(f) = ax_1^{i_1}\cdots x_n^{i_n}$. Lemma 2.4 implies that $i_1 \ge \cdots \ge i_n$. Consider the symmetric polynomial $g = a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3}\cdots\sigma_n^{i_n}$. Since $\mathrm{LT}(\sigma_i) = x_1\cdots x_i$, one can see that $\mathrm{LT}(g) = ax_1^{i_1-i_2}(x_1x_2)^{i_2-i_3}\cdots(x_1\cdots x_n)^{i_n} = \mathrm{LT}(f)$ by Lemma 2.3. Thus $\mathrm{LT}(f) > \mathrm{LT}(f_1)$, where $f_1 = f - g$.

Now consider the leading monomial of the symmetric polynomial f_1 and apply the same procedure to it. As a result, we obtain a chain of polynomials $f_i = f_{i-1} - g_{i-1}, i \ge 1$, where g_{i-1} is a polynomial in $\sigma_1, \ldots, \sigma_n$. In this chain $\mathrm{LT}(f) > \mathrm{LT}(f_1) > \mathrm{LT}(f_2) > \cdots$, and clearly that it stops at some point, i.e. $f_s = 0$ for some s. Then $f = g + g_1 + \cdots + g_{s-1}$, which gives the required representation. ☐

2.3 Problems

Problem 2.6. *Express $f = x_1^3 + x_2^3 + x_3^3$ and $f' = x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3$ as polynomials in $\sigma_1, \sigma_2, \sigma_3$*

Solution. We follow the proof of Theorem 2.5. Since $\mathrm{LT}(f) = x_1^3$, we consider

$$\begin{aligned} f_1 = f - \sigma_1^3 &= x_1^3 + x_2^3 + x_3^3 - (x_1 + x_2 + x_3)^3 \\ &= x_1^3 + x_2^3 + x_3^3 - (x_1^3 + x_2^3 + x_3^3 + 3(x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) + 6x_1x_2x_3) \\ &= -3(x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) - 6x_1x_2x_3. \end{aligned}$$

Further, $\mathrm{LT}(f_1) = -3x_1^2x_2$ and we put

$$
\begin{aligned}
f_2 &= f_1 + 3\sigma_1\sigma_2 = \\
&- 3(x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) - 6x_1x_2x_3 + 3(x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_1x_3) \\
&= 3x_1x_2x_3 = 3\sigma_3.
\end{aligned}
$$

Thus $f = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Similarly, $\mathrm{LT}(f') = x_1^3x_2^3$, then

$$
\begin{aligned}
f_1' = f' - \sigma_2^3 &= x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 - (x_1x_2 + x_1x_3 + x_2x_3)^3 \\
&= x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 - \big(x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 \\
&\qquad + 3(x_1^3x_2^2x_3 + x_1^3x_2x_3^2 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 + x_1x_2^3x_3^2 + x_1x_2^2x_3^3) + 6x_1^2x_2^2x_3^2\big) \\
&= -3(x_1^3x_2^2x_3 + x_1^3x_2x_3^2 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 + x_1x_2^3x_3^2 + x_1x_2^2x_3^3) - 6x_1^2x_2^2x_3^2.
\end{aligned}
$$

Since $\mathrm{LT}(f_1') = -3x_1^3x_2^2x_3$, we put

$$
\begin{aligned}
f_2' &= f_1' + 3\sigma_1\sigma_2\sigma_3 = -3(x_1^3x_2^2x_3 + x_1^3x_2x_3^2 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 + x_1x_2^3x_3^2 + x_1x_2^2x_3^3) - 6x_1^2x_2^2x_3^2 \\
&\qquad + 3(x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_1x_3)x_1x_2x_3 \\
&= 3x_1^2x_2^2x_3^2 = 3\sigma_3^2,
\end{aligned}
$$

whence $f' = \sigma_2^3 - 3\sigma_1\sigma_2\sigma_3 + 3\sigma_3^2$. □

Problem 2.7. *Express $f = (x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2)$ as a polynomial in $\sigma_1, \sigma_2, \sigma_3$*

Solution. The polynomials $g, g_1, \ldots$ in $\sigma_1, \sigma_2, \sigma_3$ from the proof of Theorem 2.5 have the leading monomials not greater than $\mathrm{LT}(f) = x_1^4x_2^2$. Therefore they can be associated to one of these monomials (Lemma 2.4 is taken into account) which are the leading monomials of the following polynomials in $\sigma_1, \sigma_2, \sigma_3$:

1	$x_1^4x_2^2$	$\sigma_1^2\sigma_2^2$
2	$x_1^4x_2x_3$	$\sigma_1^3\sigma_3$
3	$x_1^3x_2^3$	σ_2^3
4	$x_1^3x_2^2x_3$	$\sigma_1\sigma_2\sigma_3$
5	$x_1^2x_2^2x_3^2$	σ_3^2

Therefore $f = A\sigma_1^2\sigma_2^2 + B\sigma_1^3\sigma_3 + C\sigma_2^3 + D\sigma_1\sigma_2\sigma_3 + E\sigma_3^2$. First notice that $A = 1$ as $\mathrm{LT}(f) = \mathrm{LT}(\sigma_1^2\sigma_2^2)$. Pick up 4 combinations of x_1, x_2, x_3 and the corresponding values of $\sigma_1, \sigma_2, \sigma_3$ and f:

x_1	x_2	x_3	σ_1	σ_2	σ_3	f
1	1	0	2	1	0	2
2	-1	-1	0	-3	2	50
1	-2	-2	-3	0	4	200
1	-1	-1	-1	-1	1	8

Then we have

$$
\begin{cases}
4 + C = 2 \\
-27C + 4E = 50 \\
-108B + 16E = 200 \\
1 - B - C + D + E = 8
\end{cases}.
$$

The solution of this system is $B=-2, C=-2, D=4, E=-1$, whence $f=\sigma_1^2\sigma_2^2-2\sigma_1^3\sigma_3-2\sigma_2^3+4\sigma_1\sigma_2\sigma_3-\sigma_3^2$. □

Problem 2.8. *Find a cubic polynomial whose roots are the cubes of the roots of the polynomial* x^3-x-1

Solution. Let x_1, x_2, x_3 are the roots of x^3-x-1. Then $\sigma_1=0, \sigma_2=-1, \sigma_3=1$. Now express the elementary symmetric polynomials in x_1^3, x_2^3, x_3^3 via $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{aligned} x_1^3+x_2^3+x_3^3 &= \sigma_1^3-3\sigma_1\sigma_2+3\sigma_3=3 \\ x_1^3x_2^3+x_1^3x_3^3+x_2^3x_3^3 &= \sigma_2^3-3\sigma_1\sigma_2\sigma_3+3\sigma_3^2=2 \\ x_1^3x_2^3x_3^3 &= \sigma_3^3=1 \end{aligned}$$

Then the polynomial y^3-3y^2+2y-1 has the roots x_1^3, x_2^3, x_3^3. □

Problem 2.9. *Solve the system in* $\mathbb{C}$

$$\begin{cases} x+y+z=0 \\ x^2+y^2+z^2=0 \\ x^3+y^3+z^3=24 \end{cases}.$$

Solution. First, change variable to $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{cases} \sigma_1=0 \\ \sigma_1^2-2\sigma_2=0 \\ \sigma_1^3-3\sigma_1\sigma_2+3\sigma_3=24 \end{cases}.$$

Then $\sigma_1=0, \sigma_2=0, \sigma_3=8$. Thus x, y, z are the roots of the cubic equation $t^3-8=0$, whence $\{x, y, z\}=\{2, -1-\sqrt{3}i, -1+\sqrt{3}i\}$. □

Problem 2.10. *Solve the system in* $\mathbb{C}$

$$\begin{cases} x^2+y^2+z^2=6 \\ x^3+y^3+z^3-xyz=-4 \\ xy+yz+xz=-3 \end{cases}.$$

2.4 Discriminant

The **discriminant** of a polynomial $f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ with roots $x_1, \ldots, x_n$ is

$$D(f)=(-1)^{n(n-1)/2}a_n^{2n-2}\prod_{i\neq j}(x_i-x_j)=a_n^{2n-2}\prod_{i<j}(x_i-x_j)^2$$

Proposition 2.11. *A polynomial has multiple roots if and only if its discriminant is* 0.

Let $n = 2$. Then $D(f) = a_2^2(x_1 - x_2)^2 = a_2^2(x_1^2 + x_2^2 - 2x_1x_2) = a_2^2(\sigma_1^2 - 4\sigma_2) = a_2^2((-\frac{a_1}{a_2})^2 - 4\frac{a_0}{a_2}) = a_1^2 - 4a_0a_2$.

Let $n = 3$. Then $D(f) = a_3^4(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$. Assume that $a_3 = 1, a_2 = 0, a_1 = p, a_3 = q$, i.e., $f = x^3 + px + q$. Since $\mathrm{LT}(f) = x_1^4x_2^2$, the leading monomial of the monomials in $\sigma_1, \ldots, \sigma_n$ in the representation of f can be associated to one of the following: $x_1^4x_2^2, x_1^4x_2x_3, x_1^3x_2^3, x_1^3x_2^2x_3, x_1^2x_2^2x_3^2$, which are the leading monomials of $\sigma_1^2\sigma_2^2, \sigma_1^3\sigma_3, \sigma_2^3, \sigma_1\sigma_2\sigma_3, \sigma_3^2$, respectively.

Our assumption $a_2 = 0$ implies $\sigma_1 = 0$ and thus $D(f) = A\sigma_2^3 + B\sigma_3^2$ for some $A, B \in \mathbb{Z}$. In order to determine A and B, first take $p = -1, q = 0$ and get $f_1 = x^3 - x$ with roots $\pm1, 0$. Then $D(f_1) = (1 - (-1))^2(1 - 0)^2(0 - (-1))^2 = 4$. Since $\sigma_2 = -1, \sigma_3 = 0$, one gets $A = -4$. Now take $p = 0, q = -1$ and get $f_2 = x^3 - 1$ with roots $1, \omega, \omega^2$ where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then $D(f_2) = (1-\omega)^2(1-\omega^2)^2(\omega-\omega^2)^2 = (1-\omega-\omega^2+1)^2(\sqrt{3}i)^2 = (-3)^2(-3) = -27$. Since $\sigma_2 = 0, \sigma_3 = 1$, one gets $B = -27$. Thus $D(f) = -4p^3 - 27q^2$.