Основная теорема о симметрических многочленах

Н. Н. Осипов
Сибирский федеральный университет (Красноярск)
e-mail: nnosipov@rambler.ru

§ 1. Основная теорема о симметрических многочленах

Пусть R — *область целостности*, т. е. коммутативное кольцо с единицей и без делителей нуля. Многочлен $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ называется *симметрическим*, если он не изменяется при всевозможных перестановках переменных $x_1, \ldots, x_n$. Многочлены

$$s_k = s_k(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \prod_{j=1}^{k} x_{i_j}, \quad k = 1, \ldots, n,$$

называют *элементарными симметрическими многочленами* от переменных $x_1, \ldots, x_n$. Главное утверждение о симметрических многочленах выражает следующая

Теорема. *Всякий симметрический многочлен*

$$f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$$

представляется в виде

$$f(x_1, \ldots, x_n) = F(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)),$$

где $F(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$. Это представление единственно.

Нам понадобится

Лемма. *Если лексикографически старшие члены многочленов*

$$u(x_1, \ldots, x_n) = \prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n), \quad v(x_1, \ldots, x_n) = \prod_{k=1}^{n} s_k^{m_k}(x_1, \ldots, x_n)$$

имеют одинаковые наборы показателей, то

$$(l_1, \ldots, l_n) = (m_1, \ldots, m_n).$$

Для любого невозрастающего набора показателей $(k_1, \ldots, k_n)$ найдётся многочлен $u(x_1, \ldots, x_n)$ указанного вида, лексикографически старший член которого имеет этот набор показателей.

Доказательство. Второе утверждение леммы вытекает из существования решения системы уравнений

$$l_i + \ldots + l_n = k_i, \quad i = 1, \ldots, n,$$

в целых неотрицательных числах. Первое утверждение является следствием единственности такого решения: $l_i = k_i - k_{i+1}$, $i = 1, \ldots, n-1$, и $l_n = k_n$. $\square$

Доказательство теоремы. I. Существование. Присвоим каждому одночлену

$$a \prod_{i=1}^{n} x_i^{k_i} \tag{$*$}$$

натуральный номер по следующему правилу: одночлены нулевой степени получают номер 1, затем нумеруются одночлены первой степени в порядке лексикографического возрастания последних (при этом пропорциональные одночлены получают одинаковые номера), далее аналогично поступаем с одночленами второй степени и т. д. Будем дополнительно предполагать данный симметрический многочлен $f(x_1, \ldots, x_n)$ *однородным*; утверждение теоремы докажем индукцией по номеру m лексикографически старшего члена многочлена $f(x_1, \ldots, x_n)$.

При $m = 1$ доказывать нечего. Пусть утверждение доказано для всех номеров, меньших некоторого $m > 1$, и $f(x_1, \ldots, x_n)$ — произвольный однородный симметрический многочлен, лексикографически старший член $(*)$ которого имеет номер m. Рассмотрим многочлен

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - a \prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n)$$

где набор показателей $(l_1, \ldots, l_n)$ подобран так, что лексикографически старший член произведения

$$a \prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n)$$

совпадает с $(*)$ (см. второе утверждение леммы). Нетрудно видеть, что многочлен $g(x_1, \ldots, x_n)$ — либо нулевой, либо однородный и симметрический, причем его лексикографически старший член имеет номер, меньший m. Осталось воспользоваться предположением индукции.

II. Единственность. Пусть есть ещё одно представление

$$f(x_1, \ldots, x_n) = G(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)),$$

где $G(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$. Предположим, что многочлен

$$H(y_1, \ldots, y_n) = F(y_1, \ldots, y_n) - G(y_1, \ldots, y_n)$$

оказался ненулевым, и пусть

$$U_t(y_1, \ldots, y_n), \quad t = 1, \ldots, N,$$

— все составляющие его одночлены. По первому утверждению леммы лексикографически старшие члены многочленов

$$u_t(x_1, \ldots, x_n) = U_t(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

попарно не пропорциональны. Но тогда самому старшему из них после приведения подобных в сумме

$$\sum_{t=1}^{N} u_t(x_1, \ldots, x_n) = H(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

не с чем будет сократиться — противоречие. □

Приведённое здесь доказательство является, по-видимому, стандартным для учебной литературы (см., например, книги [1], стр. 87 — 91, и [2], стр. 221 — 223). Другое доказательство дано в книге [3], стр. 259 — 261. Третье доказательство (единственности представления) есть в книге [4], стр. 422, однако оно требует погружения области целостности R в алгебраически замкнутое поле.

На практике при выражении симметрических многочленов через элементарные симметрические многочлены обычно используется *метод неопределённых коэффициентов* (см. ниже пример 3). В некоторых частных случаях возможны и другие подходы.

Пример 1. *Степенные суммы*

$$p_k = p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k, \quad k = 1, 2, \ldots,$$

можно выразить через элементарные симметрические многочлены, используя следующую *рекуррентную формулу Ньютона*:

$$p_l - p_{l-1}s_1 + p_{l-2}s_2 - \ldots + (-1)^{l-1}p_1 s_{l-1} + (-1)^l l s_l = 0. \qquad (**)$$

Здесь $l = 1, 2, \ldots$ и $s_k = 0$ при $k > n$.

Будем называть формулу $(**)$ (l,n)-*формулой*. Очевидно, $(1,n)$-формула верна.

I. Докажем, что (n,n)-формула верна. Для этого рассмотрим многочлен

$$f(X)=\prod_{i=1}^{n}(X-x_i)=$$
$$=X^n-s_1X^{n-1}+\ldots+(-1)^{n-1}s_{n-1}X+(-1)^n s_n\in R[x_1,\ldots,x_n][X].$$

Ясно, что

$$f(x_i)=0,\quad i=1,\,\ldots,\,n.$$

Сложив эти n равенств, получим (n,n)-формулу.

II. Докажем, что (l,n)-формула верна при $l>n$. Для этого достаточно положить в (l,l)-формуле $x_{n+1}=\ldots=x_l=0$, и она превратится в (l,n)-формулу.

III. Пусть $l<n$. Докажем, что из $(l,n-1)$-формулы и $(l-1,n-1)$-формулы следует (l,n)-формула. Обозначим через s_k^* и p_k^* элементарные симметрические многочлены и степенные суммы от переменных $x_1,\ldots,x_{n-1}$. (l,n)-формулу можно записать так:

$$(p_l^*+x_n^l)-(p_{l-1}^*+x_n^{l-1})(s_1^*+x_n)+(p_{l-2}^*+x_n^{l-2})(s_2^*+x_ns_1^*)-\ldots+$$
$$+(-1)^{l-1}(p_1^*+x_n)(s_{l-1}^*+x_ns_{l-2}^*)+(-1)^l((l-1)+1)(s_l^*+x_ns_{l-1}^*)=0.$$

Частично раскрывая скобки в левой части, получим

$$\Big[p_l^*-p_{l-1}^*(s_1^*+x_n)+p_{l-2}^*(s_2^*+x_ns_1^*)-\ldots+$$
$$+(-1)^{l-1}p_1^*(s_{l-1}^*+x_ns_{l-2}^*)+(-1)^l(l-1)(s_l^*+x_ns_{l-1}^*)\Big]+$$
$$+\Big[x_n^l-x_n^{l-1}(s_1^*+x_n)+x_n^{l-2}(s_2^*+x_ns_1^*)-\ldots+$$
$$+(-1)^{l-1}x_n(s_{l-1}^*+x_ns_{l-2}^*)+\boxed{(-1)^l(s_l^*}+x_ns_{l-1}^*)\Big]=0$$

Выражение во вторых квадратных скобках — «телескопическое», оно равно $(-1)^l s_l^*$. Добавляя это к выражению в первых квадратных скобках, мы получим ровно то, что будет, если от левой части $(l,n-1)$-формулы отнять левую часть $(l-1,n-1)$-формулы, предварительно умноженную на x_n.

IV. Теперь для доказательства (l,n)-формулы при $l<n$ можно применить метод индукции (база индукции — $(1,n)$-формулы и (n,n)-формулы).

Другое доказательство формулы Ньютона см., например, в книге [2], стр. 225 — 226. Оно же переизлагается в статье [5], где есть и ссылки на другие доказательства.

Так, например, имеем

$$p_1=s_1,\quad p_2=s_1^2-2s_2,\quad p_3=s_1^3-3s_1s_2+3s_3$$

и т. д.

Если R — кольцо целых чисел, то из формулы Ньютона вытекает возможность выразить элементарные симметрические многочлены через первые n степенных сумм, однако коэффициенты соответствующих выражений уже будут дробными. Например:

$$s_1=p_1,\quad s_2=\frac{p_1^2-p_2}{2},\quad s_3=\frac{p_1^3-3p_1p_2+2p_3}{6}$$

и т. д. Как следствие, любой симметрический многочлен $f(x_1, \ldots, x_n)$ с рациональными коэффициентами можно представить в виде некоторого многочлена (также с рациональными коэффициентами) от степенных сумм $p_1, \ldots, p_n$. Нетрудно показать, что такое представление единственно. Это следует из теоремы и связано с тем, что степенные суммы $p_1, \ldots, p_n$ выражаются через элементарные симметрические многочлены «треугольно»:

$$p_k = (-1)^{k-1} k s_k + \Phi_k(s_1, \ldots, s_{k-1}), \quad k = 1, \ldots, n,$$

где Φ_k — многочлены с целыми коэффициентами.

Пример 2. Вычислим *кубические резольвенты Феррари и Эйлера* для уравнения 4-й степени

$$x^4 + ax^3 + bx^2 + cx + d = 0,$$

корни которого обозначим x_1, x_2, x_3, x_4.

I. Корнями резольвенты Феррари являются

$$z_1 = x_1x_2 + x_3x_4, \quad z_2 = x_1x_3 + x_2x_4, \quad z_3 = x_1x_4 + x_2x_3.$$

Нетрудно видеть, что

$$\begin{aligned} &z_1 + z_2 + z_3 = s_2 = b, \\ &z_1z_2 + z_1z_3 + z_2z_3 = s_1s_3 - 4s_4 = ac - 4d, \\ &z_1z_2z_3 = s_1^2 s_4 - 4s_2s_4 + s_3^2 = a^2d - 4bd + c^2. \end{aligned}$$

Следовательно, резольвента Феррари выглядит так:

$$z^3 - bz^2 + (ac - 4d)z - (a^2d - 4bd + c^2) = 0.$$

Метод Феррари состоит в том, чтобы записать данное уравнение в виде

$$(x^2 + ax/2 + z/2)^2 + \ldots = 0,$$

где $z = z_i$ — один из корней резольвенты Феррари. В частности, для уравнения

$$x^4 + (\alpha + \gamma)x^3 + (\alpha\gamma + \beta + \delta)x^2 + (\alpha\delta + \beta\gamma)x + \beta\delta = 0,$$

которое приводится к виду

$$(x^2 + \alpha x + \beta)(x^2 + \gamma x + \delta) = 0,$$

одним из корней кубической резольвенты будет $\beta + \delta$.

II. Корни резольвенты Эйлера — это

$$\begin{aligned} w_1 &= (x_1 + x_2 - x_3 - x_4)^2, \\ w_2 &= (x_1 - x_2 - x_3 + x_4)^2, \\ w_3 &= (x_1 - x_2 + x_3 - x_4)^2. \end{aligned}$$

Имеем

$$\begin{aligned}
&w_1 + w_2 + w_3 = 3s_1^2 - 8s_2 = 3a^2 - 8b,\\
&w_1w_2 + w_1w_3 + w_2w_3 = 3s_1^4 - 16s_1^2s_2 + 16s_1s_3 + 16s_2^2 - 64s_4 =\\
&= 3a^4 - 16a^2b + 16ac + 16b^2 - 64d,\\
&w_1w_2w_3 = (s_1^3 - 4s_1s_2 + 8s_3)^2 = (a^3 - 4ab + 8c)^2,
\end{aligned}$$

и резольвента Эйлера такова:

$$w^3 - (3a^2 - 8b)w^2 + (3a^4 - 16a^2b + 16ac + 16b^2 - 64d)w - (a^3 - 4ab + 8c)^2 = 0.$$

§2. Дискриминант и результант

Не будем изобретать велосипед, а просто возьмём учебник [2], где на стр. 226 — 231 есть всё, что нужно знать про *дискриминант* и *результант*.

Пример 3. Вычислим дискриминант $D(f)$ кубического многочлена

$$f(x) = x^3 + ax + b.$$

По определению имеем

$$D(f) = [(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2,$$

где x_1, x_2, x_3 — корни $f(x)$. Следовательно,

$$D(f) = x_1^4x_2^2 + \ldots = s_1^2s_2^2 + As_1^3s_3 + Bs_2^3 + Cs_1s_2s_3 + Ds_3^2.$$

Составив и затем решив систему линейных уравнений, найдём

$$A = -4, \quad B = -4, \quad C = 18, \quad D = -27.$$

Таким образом,

$$D(f) = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2 = -4a^3 - 27b^2,$$

поскольку $s_1 = x_1 + x_2 + x_3 = 0$.

Список литературы

[1] *Винберг Э.Б.* Алгебра многочленов. М.: Просвещение, 1980.

[2] *Кострикин А.И.* Введение в алгебру. Ч. I. Основы алгебры. М.: Физико-математическая литература, 2000.

[3] *Кострикин А.И.* Введение в алгебру. М.: Наука, 1977.

[4] *Ляпин Е.С., Евсеев А.Е.* Алгебра и теория чисел. Ч. II. М: Просвещение, 1978.

[5] *Райхштейн З.Б.* Тождества Ньютона и математическая индукция // Математическое просвещение. Третья серия. Вып. 4. М.: МЦНМО, 2000. С. 204 — 205.