Тема I: Многочлены

§ 8. Симметрические многочлены и их приложения

М.В.Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

Многочлен от переменных $x_1, x_2, \ldots, x_n$ называется *симметрическим*, если он не изменяется при перестановках переменных.

Итак, многочлен $f(x_1, x_2, \ldots, x_n)$ симметрический, если

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

для любой перестановки $\pi\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Примеры. 1) *Элементарные симметрические функции* $\sigma_k(x_1, x_2, \ldots, x_n)$:

$$\sigma_k := \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k}, \quad k = 1, 2, \ldots, n.$$

В случае надобности явно указать число переменных пишем $\sigma_k^{(n)}$. Скажем, $\sigma_1^{(3)} = x_1 + x_2 + x_3$, а $\sigma_1^{(5)} = x_1 + x_2 + x_3 + x_4 + x_5$.

2) *Степенные суммы* $s_k(x_1, x_2, \ldots, x_n) := \sum_{i=1}^{n} x_i^k$.

3) Квадрат определителя Вандермонда $V(x_1, x_2, \ldots, x_n)$.

4) По определению все многочлены нулевой степени и все многочлены от одной переменной – симметрические.

Теорема о симметрических многочленах

Симметрический многочлен над полем представи́м как многочлен над тем же полем от элементарных симметрических функций своих переменных.

Формально: для любого симметрического многочлена $f(x_1, x_2, \dots, x_n)$ над полем существует многочлен $g(y_1, y_2, \dots, y_n)$ над тем же полем, такой, что

$$f(x_1, x_2, \dots, x_n) = g(\sigma_1, \sigma_2, \dots, \sigma_n).$$

Замечание. Многочлен $g(y_1, y_2, \dots, y_n)$ определяется однозначно. Поскольку этот факт нам не понадобится, я не буду его здесь доказывать.

Доказательство. Проведем *двойную индукцию* – по *полной степени* многочлена и по числу переменных. Полная степень многочлена от нескольких переменных – это максимум сумм степеней его одночленов относительно каждой из входящих в них переменных. Например, полная степень многочлена $x_1^2x_2^4 + x_1^3x_3^5 + x_2^6x_3$ равна 8.
Для многочлена f нулевой полной степени, равно как и для многочлена f любой степени от одной переменной доказывать нечего, так как в роли многочлена g можно взять сам многочлен f. (В случае многочлена от одной переменной имеем $f(x_1) = f(\sigma_1^{(1)})$, поскольку $\sigma_1^{(1)} = x_1$.)

Пусть $f(x_1, x_2, \ldots, x_n)$ – симметрический многочлен с $n > 1$ и полной степенью $m > 0$. Рассмотрим многочлен $f(x_1, x_2, \ldots, x_{n-1}, 0)$. Он симметрический относительно $x_1, x_2, \ldots, x_{n-1}$, и по предположению индукции существует многочлен $g(y_1, y_2, \ldots, y_{n-1})$, такой, что

$$f(x_1, x_2, \ldots, x_{n-1}, 0) = g(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}). \qquad (\star)$$

Здесь полная степень обеих частей $\leqslant m$. Рассмотрим теперь многочлен

$$h(x_1, x_2, \ldots, x_n) := f(x_1, x_2, \ldots, x_n) - g(\sigma_1^{(n)}, \sigma_2^{(n)}, \ldots, \sigma_{n-1}^{(n)}).$$

Ясно, что h – симметрический многочлен. Заметим, что

$$\sigma_k^{(n)}(x_1, x_2, \ldots, x_{n-1}, 0) = \sigma_k^{(n-1)}(x_1, x_2, \ldots, x_{n-1})$$

и полные степени $\sigma_k^{(n)}$ и $\sigma_k^{(n-1)}$ равны k для всех $k = 1, 2 \ldots, n-1$. Отсюда полная степень $g(\sigma_1^{(n)}, \sigma_2^{(n)}, \ldots, \sigma_{n-1}^{(n)})$ равна полной степени $g(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)})$ и не превосходит m. Поэтому полная степень $h(x_1, x_2, \ldots, x_n)$ не превосходит m. Кроме того, имеем

$$h(x_1, x_2, \ldots, 0) = f(x_1, x_2, \ldots, x_{n-1}, 0) - g(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}) \overset{(\star)}{=} 0.$$

По следствию теоремы Безу $h(x_1, x_2, \ldots, x_n)$ делится на $x_n - 0 = x_n$.

Имеем $h(x_1, x_2, \ldots, x_n) = x_n q(x_1, \ldots, x_n)$ для некоторого $q(x_1, \ldots, x_n)$. Переставив x_i и x_n, в силу симметричности $h(x_1, x_2, \ldots, x_n)$ получим $h(x_1, x_2, \ldots, x_n) = x_i q(x_1, \ldots, x_{i-1}, x_n, x_{i+1}, \ldots, x_i)$, откуда h делится на x_i для любого i. В силу однозначности разложения в кольце многочленов отсюда следует, что h делится на $x_1 x_2 \cdots x_n = \sigma_n$.

Итак, $p(x_1, x_2, \ldots, x_n) := \dfrac{h(x_1, x_2, \ldots, x_n)}{\sigma_n}$ – многочлен, очевидно, симметрический и имеющий меньшую полную степень, чем многочлен h, полная степень которого не превосходит m. По предположению индукции существует многочлен $r(y_1, y_2, \ldots, y_n)$, такой, что

$$p(x_1, x_2, \ldots, x_n) = r(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Но тогда

$$\begin{aligned}
f(x_1, x_2, \ldots, x_n) &= h(x_1, x_2, \ldots, x_n) + g(\sigma_1, \sigma_2, \ldots, \sigma_{n-1}) \\
&= \sigma_n p(x_1, x_2, \ldots, x_n) + g(\sigma_1, \sigma_2, \ldots, \sigma_{n-1}) \\
&= \sigma_n r(\sigma_1, \sigma_2, \ldots, \sigma_n) + g(\sigma_1, \sigma_2, \ldots, \sigma_{n-1}). \qquad \square
\end{aligned}$$

Для нас важно следствие основной теоремы о симметрических многочленах, которое получается, если скомбинировать ее со следствием формул Виета: *с точностью до знака коэффициенты унитарного многочлена суть элементарные симметрические функции его корней.*

Следствие (симметрические многочлены от корней)

Любой симметрический многочлен от корней унитарного многочлена $f(x)$ над некоторым полем представи́м как многочлен над тем же полем от коэффициентов многочлена $f(x)$.

Примеры. 1) Для многочлена с действительными коэффициентами сумма k-х степеней его корней (включая комплексные!) – действительное число.

2) Квадрат определителя Вандермонда $V(x_1, x_2, \dots, x_n)$ от корней любого многочлена $f(x)$ выражается через коэффициенты многочлена $f(x)$. Это выражение называется *дискриминантом* многочлена $f(x)$. Дискриминант многочлена $f(x)$ равен 0 тогда и только тогда, когда у $f(x)$ есть кратные корни в поле разложения (*объясните, почему*). Несложно подсчитать, что для квадратного трехчлена $x^2 + px + q$ это определение приводит в точности к «школьной» формуле $p^2 - 4q$ для дискриминанта.

Мы уже формулировали основную теорему алгебры комплексных чисел: *любой многочлен положительной степени над полем $\mathbb{C}$ имеет по крайней мере один комплексный корень.*

Теперь мы ее докажем. Первым шагом будет простое наблюдение.

Лемма о модуле старшего члена

Пусть $f(x)$ – многочлен над полем $\mathbb{C}$. Тогда при всех достаточно больших по модулю значениях x модуль старшего члена многочлена $f(x)$ больше модуля суммы всех остальных его членов.

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$. Положим $A := \max\{|a_1|, \ldots, |a_n|\}$. По свойствам модуля имеем для любого x:

$$\left|a_1x^{n-1} + \cdots + a_n\right| \le \left|a_1x^{n-1}\right| + \cdots + |a_n| \le A\left(\left|x^{n-1}\right| + \cdots + 1\right).$$

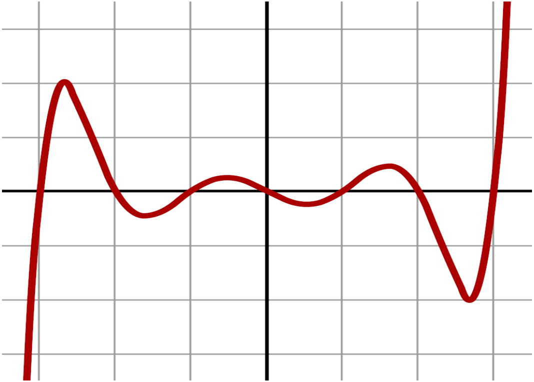
При $|x| > \frac{A}{|a_0|} + 1$, суммируя геометрическую прогрессию, получаем

$$A\left(\left|x^{n-1}\right| + \cdots + 1\right) = A\frac{|x^n| - 1}{|x| - 1} < A\frac{|x^n|}{|x| - 1} < A\frac{|x^n|}{\frac{A}{|a_0|}} = |a_0x^n|. \qquad \square$$

Следствия леммы о модуле старшего члена

Следствие 1

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ *– многочлен нечетной степени над полем* $\mathbb{R}$. *Тогда при всех достаточно больших положительных значениях* x *знак* $f(x)$ *совпадает со знаком* a_0, *а при всех достаточно больших по модулю отрицательных значениях* x *знак* $f(x)$ *противоположен знаку* a_0.



Многочлены над $\mathbb{R}$ – непрерывные функции. Поэтому, комбинируя предыдущее следствие и классический результат анализа (*теорема о промежуточном значении* aka *первая теорема Больцано–Коши*), получаем

Следствие 2

Любой многочлен нечетной степени над полем $\mathbb{R}$ имеет по крайней мере один действительный корень.

Для многочленов четной степени над $\mathbb{R}$ аналог следствия 2 не верен – пример x^2+1. Но мы докажем, что любой многочлен $f(x)$ над полем $\mathbb{R}$ имеет по крайней мере один *комплексный* корень. Пусть $\deg f = n = 2^k m$, где m нечетно. Проведем индукцию по k; следствие 2 дает базу $k=0$.

Пусть $k>1$ и $\alpha_1,\alpha_2,\dots,\alpha_n$ – корни многочлена $f(x)$ в его поле разложения; каждый корень взят столько раз, какова его кратность. Зафиксируем некоторое число $c\in\mathbb{R}$ и рассмотрим элементы $\beta_{ij} := c(\alpha_i+\alpha_j)+\alpha_i\alpha_j$, где $1\le i<j\le n$. Построим многочлен, для которого эти элементы являются корнями: $g_c(x) := \prod_{1\le i<j\le n}(x-\beta_{ij})$.

Степень $g_c(x)$ есть $\dfrac{n(n-1)}{2} = \dfrac{2^k m(2^k m-1)}{2} = 2^{k-1}\underbrace{m(2^k m-1)}_{\text{нечетно}}$.

Поэтому если показать, что коэффициенты $g_c(x)$ – действительные числа, то к $g_c(x)$ можно будет применить предположение индукции!

Коэффициенты многочлена $g_c(x) := \prod_{1\leq i<j\leq n}(x-\beta_{ij})$ не меняются при перестановках $\beta_{ij} = c(\alpha_i+\alpha_j)+\alpha_i\alpha_j$. Если совершить произвольную перестановку корней $\alpha_1, \alpha_2, \dots, \alpha_n$, то и с элементами β_{ij} произойдет некоторая перестановка. Поэтому коэффициенты многочлена $g_c(x)$ не меняются при перестановках α_i. Значит, эти коэффициенты выражаются как многочлены с действительными коэффициентами от элементарных симметрических функций от α_i, а последние с точностью до знака суть коэффициенты многочлена $f(x) \in \mathbb{R}[x]$. Итак, имеем $g_c(x) \in \mathbb{R}[x]$, и по предположению индукции $\beta_{ij} \in \mathbb{C}$ для какой-то пары (i,j).

Пар (i,j) конечное число, а чисел $c \in \mathbb{R}$ бесконечно много. По принципу Дирихле найдутся два разных действительных числа c и d, которым отвечает одна и та же пара (i,j). Значит, для каких-то $u, v \in \mathbb{C}$ имеем

$$\begin{cases} c(\alpha_i+\alpha_j)+\alpha_i\alpha_j = & u, \\ d(\alpha_i+\alpha_j)+\alpha_i\alpha_j = & v. \end{cases}$$

Отсюда $\alpha_i+\alpha_j = \dfrac{u-v}{c-d}$ и $c\dfrac{u-v}{c-d}+\alpha_i\left(\dfrac{u-v}{c-d}-\alpha_i\right) = u$.

Получили для α_i квадратное уравнение с комплексными коэффициентами. Решение такого уравнения – комплексное число. Таким образом, у многочлена $f(x)$ есть комплексный корень.

Чтобы завершить доказательство основной теоремы, нужно рассмотреть произвольный многочлен $h(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{C}[x]$. Положим $\overline{h}(x) := \overline{b_n}x^n + \overline{b_{n-1}}x^{n-1} + \cdots + \overline{b_0}$ и рассмотрим многочлен $f(x) := h(x)\overline{h}(x)$. Все коэффициенты многочлена $f(x)$ действительны. В самом деле, коэффициент $b_0\overline{b_k} + b_1\overline{b_{k-1}} + \cdots + b_{k-1}\overline{b_1} + b_k\overline{b_0}$ при x^k равен своему сопряженному $\overline{b_0}b_k + \overline{b_1}b_{k-1} + \cdots + \overline{b_{k-1}}b_1 + \overline{b_k}b_0$.

По доказанному у $f(x)$ есть хотя бы один комплексный корень α. Имеем $f(\alpha) = h(\alpha)\overline{h}(\alpha) = 0$, откуда либо $h(\alpha) = 0$, либо $\overline{h}(\alpha) = 0$. В первом случае α – корень $h(x)$, и все доказано, а во втором

$$h(\overline{\alpha}) = b_n\overline{\alpha}^n + b_{n-1}\overline{\alpha}^{n-1} + \cdots + b_0 =$$
$$= \overline{\overline{b_n}\alpha^n + \overline{b_{n-1}}\alpha^{n-1} + \cdots + \overline{b_0}} = \overline{\overline{h}(\alpha)} = 0.$$

Таким образом, во втором случае $\overline{\alpha}$ – корень $h(x)$. □

Приведенное доказательство принадлежит Гауссу (1815). Оно основано на идеях Эйлера и Лагранжа.

Следствия основной теоремы

Напомним два следствия основной теоремы алгебры комплексных чисел.

Следствие (разложение многочленов над $\mathbb{C}$)

Любой многочлен степени $n > 0$ над полем $\mathbb{C}$ однозначно представи́м как произведение n линейных двучленов.

Следствие (разложение многочленов над $\mathbb{R}$)

Любой многочлен степени $n > 0$ над полем $\mathbb{R}$ однозначно представи́м как произведение $k \leq \lfloor\frac{n}{2}\rfloor$ квадратных трехчленов с отрицательными дискриминантами и $n - 2k$ линейных двучленов.