ЛЕКЦИЯ 20

ФОРМУЛЫ ВИЕТА

ТЕОРЕМА О СИММЕТРИЧЕСКИХ МНОГОЧЛЕНАХ

МЕТОД НЕОПРЕДЕЛЕННЫХ КОЭФФИЦИЕНТОВ

ФОРМУЛЫ ВИЕТА

Предположим, что нормализованный многочлен $f \in \mathbb{F}[x]$ степени n имеет в поле $\mathbb{F}$ или в некотором его расширении n корней $c_1, c_2, \dots, c_n$, среди которых, возможно, есть и одинаковые. Тогда справедливо разложение

$$f(x) = (x - c_1)(x - c_2) \dots (x - c_n).$$

Запишем, с другой стороны, $f(x)$ в обычном виде по степеням x:

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_k x^{n-k} + \dots + a_n,$$

а теперь перемножим все члены $x - c_i$ и приведем подобные члены. Тогда для коэффициентов $a_1, \dots, a_n$ получатся выражения через корни $c_1, \dots, c_n$:

$$\begin{aligned}
&a_1 = -(c_1 + c_2 + \dots + c_n),\\
&\dots\dots\dots\dots\dots\dots\\
&a_k = (-1)^k \sum_{i_1 < i_2 < \dots < i_k} c_{i_1} c_{i_2} \dots c_{i_k},\\
&\dots\dots\dots\dots\dots\dots\\
&a_n = (-1)^n c_1 c_2 \dots c_n.
\end{aligned}$$

Эти формулы называются *формулами Виета.*

Если бы многочлен f не был нормализованным, то есть имел бы старший коффициент $a_0 \neq 1$, то аналогичные формулы давали бы выражение для a_i/a_0.

Формулы Виета, устанавливающие явную связь между корнями и коэффициентами произвольного многочлена, замечательны тем, что их правые части не меняются при любых перестановках корней $c_1, \dots, c_n$.

Это дает нам повод ввести понятие симметрической функции.

Элемент $\pi \in S_n$ действует на функцию $\widetilde{f}(x_1, \dots, x_n)$ от n аргументов по правилу

$$\widetilde{(\pi \circ f)}(x_1, \dots, x_n) = \widetilde{f}(x_{\pi(1)}, \dots, x_{\pi(n)}).$$

Функция f называется *симметрической*, если

$$\widetilde{\pi \circ f} = \widetilde{f}$$

для всех $\pi \in S_n$.

Примером симметрических функций служат так назывемые *элементарные симметрические многочлены* σ_k:

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n} x_{i_1} x_{i_2} \dots x_{i_k}.$$

Они позволяют переписать формулы Виета в коротком виде

$$a_k = (-1)^k \sigma_k(c_1, \dots, c_n), \quad k = 1, 2, \dots, n.$$

КОЛЬЦО СИММЕТРИЧЕСКИХ МНОГОЧЛЕНОВ

Пусть $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$.

Положим

$$(\pi \circ f)(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)}).$$

Многочлен f называется *симметрическим*, если $\pi \circ f = f$ для всех $\pi \in S_n$.

Как и для функций, вводятся элементарные симметрические многочлены σ_k:

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n} x_{i_1} x_{i_2} \dots x_{i_k}.$$

Так как, далее,

$$\widetilde{\pi} : f \mapsto \pi \circ f$$

— автоморфизм кольца

$$R[x_1, \dots, x_n],$$

то любые линейные комбинации симметрических многочленов и их произведения будут снова симметрическими многочленами.

Это значит, что *множество всех симметрических многочленов образует кольцо, являющееся подкольцом кольца* $R[x_1, \dots, x_n]$.

Разберемся, как устроено это кольцо.

ОСНОВНАЯ ТЕОРЕМА О СИММЕТРИЧЕСКИХ МНОГОЧЛЕНАХ

Оказывается, что наиболее общим способом получения симметрических многочленов является следующий.

Нужно взять произвольный многочлен

$$g \in R[y_1, \ldots, y_n]$$

и подставить вместо $y_1, \ldots, y_n$ соответственно $\sigma_1, \ldots, \sigma_n$. Получившийся в результате многочлен будет, конечно, симметрическим.

Заметим еще, что одночлен

$$y_1^{i_1} \ldots y_n^{i_n},$$

входящий в g, переходит при данной подстановке в однородный многочлен от $x_1, \ldots, x_n$ степени

$$i_1 + 2i_2 + \cdots + ni_n,$$

поскольку $\deg \sigma_k = k$. Эту сумму называют обычно *весом* одночлена $y_1^{i_1} \ldots y_n^{i_n}$.

Весом многочлена $g(x_1, \ldots, x_n)$ естественно считать максимум всех весом одночленов, входящих в g.

Основное утверждение о симметрических многочленах выражает

Теорема 1. *Пусть* $f \in R[x_1, \ldots, x_n]$ *— симметрический многочлен полной степени* m *над целостным кольцом* R.

Тогда существует, и притом единственный, многочлен $g \in R[y_1, \ldots, y_n]$ *веса* m*, для которого*

$$f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n).$$

Коэффициенты многочлена g *являются целочисленными линейными комбинациями коэффициентов многочлена* f.

Доказательство. Мы уже отмечали выше, что любой многочлен $f = f(x_1, \ldots, x_n)$ можно записать в виде суммы однородных многочленов f_m различных степеней:

$$f = f_0 + f_1 + \cdots + f_k.$$

Очевидно, что эта запись единственна. Если теперь f — симметрический многочлен, то симметрическими будут и многочлены f_m, поскольку

$$\pi \circ f = \sum \pi \circ f_m,$$

а действие

$$\widetilde{\pi} : f_n \mapsto \pi \circ f_m$$

на степень m не влияет.

Таким образом, без ограничения общности симметрический многочлен f можно считать однородным.

Дальнейшие рассуждения разобьем на несколько частей.

2. Одночлен

$$u = ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$$

условимся называть *монотонным*, если

$$i_1 \geqslant i_2 \geqslant \dots \geqslant i_n.$$

Лемма 1. *Высший член симметрического многочлена (относительно лексикографического порядка) всегда монотонен.*

Доказательство. Действительно, пусть

$$HM(f) = u = ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n}.$$

Допустим, что $i_k < i_{k+1}$ при некотором $k \leqslant n-1$. Переставив в u местами переменные x_k и x_{k+1}, мы получим одночлен

$$u' = ax_1^{i_1}\dots x_k^{i_{k+1}}x_{k+1}^{i_k}\dots x_n^{i_n},$$

из-за симметричности f также входящий в f.

Но, очевидно, $u' > u$, так как показатели при $x_1, \dots, x_{k-1}$ в u и u' одинаковые, а показатель при x_k в u' больше показателя при x_k в u.

Полученное противоречие доказывает лемму. $\square$

3. Существование многочлена $g(y_1, \ldots, y_n)$.

Предположим снова, что

$$u = a x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = HM(f).$$

В силу доказанной только что леммы

$$i_k \geqslant i_{k+1}, \quad 1 \leqslant k \leqslant n-1.$$

Поэтому мы можем ввести в рассмотрение симметрический многочлен

$$f_{(1)}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3} \ldots \sigma_n^{i_n},$$

отвечающий одночлену

$$a y_1^{i_1-i_2} y_2^{i_2-i_3} \ldots y_n^{i_n}$$

веса

$$\begin{aligned}(i_1 - i_2) + 2(i_2 - i_3) + \cdots + (n-1)(i_{n-1} - i_n) + n i_n &= \\ = i_1 + i_2 + \cdots + i_n = \deg f.\end{aligned}$$

Так как высшими членами элементарных симметрических многочленов $\sigma_1, \sigma_2, \ldots, \sigma_n$ являются, очевидно,

$$x_1,\ x_1x_2, \ldots,\ x_1x_2 \ldots x_n,$$

то высшим членом в $a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3} \ldots \sigma_n^{i_n}$ будет

$$ax_1^{i_1-i_2}(x_1x_2)^{i_2-i_3}\dots(x_1x_2\dots x_{n-1})^{i_{n-1}-i_n}(x_1x_2\dots x_n)^{i_n} = \\ = ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n},$$

то есть в точности $u = HM(f)$. Значит, он сокращается, в $f_{(1)}$ не входит и

$$HM(f) > HM(f_{(1)}).$$

Отметим еще, что коэффициенты многочлена $f_{(1)}$ имеют вид $c - qa$, где c, a — коэффициенты многочлена f, $q \in \mathbb{Z}$.

Пусть

$$v = bx_1^{j_1}x_2^{j_2}\dots x_n^{j_n} = HM(f_{(1)}), \quad b \in R.$$

Снова имеем

$$j_1 \geqslant j_2 \geqslant \dots \geqslant j_n,$$

и по изложенным выше соображениям, для симметрического многочлена

$$f_{(2)}(x_1,\dots,x_n) = f_{(1)}(x_1,\dots,x_n) - b\sigma_1^{j_1-j_2}\sigma_2^{j_2-j_3}\dots\sigma_n^{j_n}$$

получаем

$$HM(f_{(1)}) > HM(f_{(2)}).$$

Кроме того, коэффициенты многочлена $f_{(2)}$ имеют вид $c_1 - q_1b$, где $q_1 \in \mathbb{Z}$, а c, b — коэффициенты многочлена $f_{(1)}$.

Продолжая этот процесс, мы придем к последовательности однородных симметрических многочленов

$$f_{(k)} = f - a\sigma_1^{i_1-i_2}\dots\sigma_n^{i_n} - b\sigma_1^{j_1-j_2}\dots\sigma_n^{j_n} - \dots$$

степени

$$\deg f_{(k)} = \deg f,$$

для которых

$$HM(f) > HM(f_{(1)}) > HM(f_{(2)}) > \dots > HM(f_{(k)}) > \dots,$$

причем коэффициенты у $f_{(k)}$ будут линейными комбинациями коэффициентов многочлена f.

Так как одночленов фиксированной степени (тем более, монотонных) конечное число, то цепочка неравенств должна оборваться, то есть $f_{(k)} = 0$ при некотором k.

Получаем требуемое выражение

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

где

$$g(y_1, \dots, y_n) = ay_1^{i_1-i_2}y_2^{i_2-i_3}\dots y_n^{i_n} + by_1^{j_1-j_2}y_2^{j_2-j_3}\dots y_n^{j_n} + \dots$$

4. Единственность.

В случае существования двух различных представлений

$$f = g_1(\sigma_1, \ldots, \sigma_n) = g_2(\sigma_1, \ldots, \sigma_n)$$

мы имели бы отличный от нуля многочлен

$$g(y_1, \ldots, y_n) = g_1(y_1, \ldots, y_n) - g_2(y_1, \ldots, y_n)$$

веса $\deg f$, для которого $g(\sigma_1, \ldots, \sigma_n) = 0$.

Если $ay_1^{k_1} y_2^{k_2} \ldots y_n^{k_n}$ — одночлен, входящий в g, то, как мы видели,

$$\begin{aligned} HM(a\sigma_1^{k_1} \ldots \sigma_n^{k_n}) = ax_1^{k_1}(x_1x_2)^{k_2} \ldots (x_1 \ldots x_n)^{k_n} = \\ = ax_1^{k_1+k_2+\cdots+k_n} x_2^{k_2+\cdots+k_n} \ldots x_n^{k_n}. \end{aligned}$$

Ясно поэтому, что различным одночленам, входящим в g, отвечают разные высшие члены. Среди них один будет самым высшим, и, значит,

$$HM(g(\sigma_1, \ldots, \sigma_n)) \neq 0$$

вопреки предположению. $\square$

МЕТОД НЕОПРЕДЕЛЕННЫХ КОЭФФИЦИЕНТОВ

Существует несколько различных доказательств основной теоремы о симметрических многочленах, а соответственно, и методов выражения заданного симметрического многочлена f через элементарные симметрические. Чтобы описать один из таких употребительных методов, введем новый тип симметрических многочленов.

Для определенности будем брать в качестве кольца R или кольцо $\mathbb{Z}$, или поле $\mathbb{R}$. Пусть

$$v = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

— какой-то одночлен. Обозначим через $S(v)$ сумму одночленов, получающихся из одночлена v всеми перестановками всех независимых переменных.

Например,

$$\sigma_k(x_1, x_2, \ldots, x_n) = S(x_1 x_2 \ldots x_k)$$

— k-й элементарный симметрический многочлен.

Далее,

$$p_k(x_1, x_2, \ldots, x_n) = S(x_1^k) = x_1^k + x_2^k + \cdots + x_n^k$$

— так называемая k-я степенная сумма.

Понятно, что всегда $S(v)$ — однородный симметрический многочлен той же полной степени, что и одночлен v.

По смыслу ясно, что любой симметрический многочлен f над R является линейной комбинацией многочленов типа $S(v)$:

$$f = \sum a_v S(v).$$

Таким образом, задача сводится к выражению $S(v)$ через элементарные симметрические многочлены.

С каждым монотонным одночленом

$$v = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

ассоциируется симметрический многочлен

$$g_v = g_v(x_1, \dots, x_n) = \sigma_1^{i_1 - i_2} \sigma_2^{i_2 - i_3} \dots \sigma_n^{i_n},$$

высшим членом которого как раз и является v.

В связи со схемой доказательства основной теоремы о симметрических многочленах вырисовывается следующий метод выражения $S(v)$ через элементарные симметрические многочлены.

Пусть $\deg v = m$. Берутся все монотонные разбиения

$$m = j_1 + j_2 + \dots + j_n, \quad j_1 \geqslant j_2 \geqslant \dots \geqslant j_n \geqslant 0,$$

целого числа m такие, что

$$w = x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} < v.$$

Рассматривается множество M_v всех таких одночленов w.

Мы уже знаем, что

$$S(v) = g_v + \sum_{w \in M_v} n_w g_w,$$

где n_w — какие-то целые числа. Неопределенные коэффициенты n_w (отсюда и название — *метод неопределенных коэффициентов*) находятся путем последовательных подстановок в это неопределенное равенство вместо $x_1, \ldots, x_n$ каких-то целых значений, обычно нулей и единиц.

Значения g_u, g_w и $S(v)$ при этом известны, и для n_w получается заведомо совместная система линейных уравнений.

Пример 1. Пусть $v = x_1^3$, $S(v) = p_3(x_1, \ldots, x_n)$, $n \geqslant 3$, $g_v = \sigma_1^3$.

Тогда еще возможности для мономов — это $\sigma_1\sigma_2$ (соответствует $x_1^2 x_2$) и σ_3 (соответствует $x_1 x_2 x_3$).

Наше уравнение принимает вид

$$p_3 = \sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3.$$

Подставим сначала $x_1 = x_2 = 1$, $x_i = 0$ при $i > 2$, получим

$$p_3 = 2, \quad \sigma_1 = 2, \quad \sigma_2 = 1, \quad \sigma_3 = 0.$$

Если же

$$x_1 = x_2 = x_3 = 1, \quad x_i = 0 \text{ при } i > 3,$$

то

$$p_3 = 3, \quad \sigma_1 = 3, \quad \sigma_2 = 3, \quad \sigma_3 = 1.$$

Находим, что $a = -3$, $b = 3$, то есть

$$p_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$