ЛЕКЦИЯ 21

ТЕОРЕМА О СИММЕТРИЧЕСКИХ МНОГОЧЛЕНАХ

МЕТОД НЕОПРЕДЕЛЕННЫХ КОЭФФИЦИЕНТОВ

ОСНОВНАЯ ТЕОРЕМА АЛГЕБРЫ — ФОРМУЛИРОВКА

КОЛЬЦО СИММЕТРИЧЕСКИХ МНОГОЧЛЕНОВ

Пусть $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$.

Положим

$$(\pi \circ f)(X_1, \ldots, X_n) = f(X_{\pi(1)}, \ldots, X_{\pi(n)}).$$

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

Как и для функций, вводятся элементарные симметрические многочлены s_k:

$$s_k(X_1, \ldots, X_n) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} X_{i_1} X_{i_2} \ldots X_{i_k}.$$

Так как, далее,

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

— автоморфизм кольца

$$R[X_1, \ldots, X_n],$$

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* $R[X_1, \ldots, X_n]$.

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 $s_1, \ldots, s_n$. 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 $\deg s_k = k$. 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

$$f(X_1, \ldots, X_n) = g(s_1, \ldots, s_n).$$

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 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. □

3. Существование многочлена $g(Y_1, \ldots, Y_n)$.

Предположим снова, что

$$u = aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} = HM(f).$$

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

$$f_{(1)}(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - as_1^{i_1-i_2} s_2^{i_2-i_3} \ldots s_n^{i_n},$$

отвечающий одночлену

$$aY_1^{i_1-i_2} Y_2^{i_2-i_3} \ldots Y_n^{i_n}$$

веса

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

Так как высшими членами элементарных симметрических многочленов $s_1, s_2, \ldots, s_n$ являются, очевидно,

$$X_1,\ X_1X_2, \ldots,\ X_1X_2 \ldots X_n,$$

то высшим членом в $as_1^{i_1-i_2} s_2^{i_2-i_3} \ldots s_n^{i_n}$ 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

$$f_{(2)}(X_1, \dots, X_n) = f_{(1)}(X_1, \dots, X_n) - bs_1^{j_1-j_2}s_2^{j_2-j_3}\dots s_n^{j_n}$$

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

$$f_{(k)} = f - as_1^{i_1-i_2} \dots s_n^{i_n} - bs_1^{j_1-j_2} \dots s_n^{j_n} - \dots$$

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

$$f(X_1, \dots, X_n) = g(s_1, \dots, s_n),$$

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

$$f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$$

мы имели бы отличный от нуля многочлен

$$g(Y_1, \ldots, Y_n) = g_1(Y_1, \ldots, Y_n) - g_2(Y_1, \ldots, Y_n)$$

вкса $\deg f$, для которого $g(s_1, \ldots, s_n) = 0$.

Если $aY_1^{k_1}Y_2^{k_2}\ldots Y_n^{k_n}$ — одночлен, входящий в g, то, как мы видели,

$$HM(as_1^{k_1}\ldots s_n^{k_n}) = aX_1^{k_1}(X_1X_2)^{k_2}\ldots(X_1\ldots X_n)^{k_n} = \\ = aX_1^{k_1+k_2+\cdots+k_n}X_2^{k_2+\cdots+k_n}\ldots X_n^{k_n}.$$

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

$$HM(g(s_1, \ldots, s_n)) \neq 0$$

вопреки предположению. □

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

$$v = X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$$

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

Например,

$$s_k(X_1, X_2, \dots, X_n) = S(X_1 X_2 \dots X_k)$$

— k-й элементарный симметрический многочлен.

Далее,

$$p_k(X_1, X_2, \dots, X_n) = S(X_1^k) = X_1^k + X_2^k + \dots + X_n^k$$

— 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

$$g_v = g_v(X_1, \dots, X_n) = s_1^{i_1 - i_2} s_2^{i_2 - i_3} \dots s_n^{i_n},$$

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 $v = X_1^3$, $S(v) = p_3(X_1, \ldots, X_n)$, $n \geqslant 3$, $g_v = s_1^3$.

Тогда еще возможности для мономов — это $s_1 s_2$ (соответствует $X_1^2 X_2$) и s_3 (соответствует $X_1 X_2 X_3$).

Наше уравнение принимает вид

$$p_3 = s_1^3 + a s_1 s_2 + b s_3.$$

Подставим сначала $X_1 = X_2 = 1$, $X_i = 0$ при $i > 2$, получим

$$p_3 = 2, \quad s_1 = 2, \quad s_2 = 1, \quad s_3 = 0.$$

Если же

$$X_1 = X_2 = X_3 = 1, \quad X_i = 0 \text{ при } i > 3,$$

то

$$p_3 = 3, \quad s_1 = 3, \quad s_2 = 3, \quad s_3 = 1.$$

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

$$p_3 = s_1^3 - 3 s_1 s_2 + 3 s_3.$$

АЛГЕБРАИЧЕСКАЯ ЗАМКНУТОСТЬ ПОЛЯ $\mathbb{C}$

Пусть F — поле и f — произвольный многочлен над F.

Определение 1. Поле F называется *алгебраически замкнутым*, если каждый многочлен из кольца $F[X]$ разлагается на линейные множители.

То же самое можно выразить другими словами: *поле F алгебраически замкнуто, если неприводимыми над F являются лишь линейные многочлены.*

Если любой многочлен $f \in F[X]$ обладает по крайней мере одним корнем, то поле F алгебраически замкнуто.

Доказательство. Действительно, тогда

$$f(X) = (X - a)h(X), \quad a \in F, \quad h \in F[X],$$

но по условию для многочлена $h[X]$ в F также существует хотя бы один корень, то есть

$$h(X) = (X - b)r(X), \quad b \in F,\ r \in F[X].$$

Подолжая этот процесс, мы придем в конце концов к полному разложению f на линейные множители. Так как f — произвольный многочлен, то поле F алгебраически замкнуто. $\square$

Хотя и справедливо утверждение о том, что *для всякого поля F существует расширение $\widetilde{F} \supset F$, являющееся алгебраически замкнутым полем* (*теорема Штейница*), на первых порах все же трудно воспринять не только конструкцию алгебраически замкнутого расширения, но и саму идею такого расширения. Тем более приятно, что мы фактически располагаем ярким и очень важным примером алгебраически замкнутого поля, как об этом гласит так называемая *основная теорема алгебры.*

Именно, справедлива

Теорема 2. *Поле комплексных чисел $\mathbb{C}$ алгебраически замкнуто.*

Если формулировать ее иначе, то получим:

Произвольный многочлен $f(X)$ степени $n \geqslant 1$ с комплексными или вещественными коэффициентами имеет ровно n комплексных корней, считаемых со своими кратностями.

Громкий титул основной теоремы алгебры эта теорема приобрела еще в те времена, когда решение алгебраических уравнений было одним из главных занятий алгебраистов.

Впервые строгое доказательство основной теоремы алгебры было предложение Гауссом в 1779 году. С тех пор появилось много вариантов доказательств, различающихся между собой, так сказать, степенью алгебраичности. Необходимость опираться а свойства непрерывности полей $\mathbb{R}$ и $\mathbb{C}$ возникает в этих доказательствах в той или иной степени.

Сейчас мы приведем доказательство, основанное на элементарных сведениях из математического анализа и восходящее к идеям Даламбера, Эйлера, Гаусса, Коши, Аргана. Именно последнему (1814 год) принадлежит наиболее прозрачное изложение, которому с тех пор следуют почти все учебники по алгебре.

Его неалгебраичность начинается с двух вспомогательных утверждений, которые можно найти в любом курсе анализа.

(1) *Каждый комплексный многочлен*

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n, \quad n \geqslant 0,$$

является непрерывной функцией в любой точке плоскости $\mathbb{C}$.

Другими словами, для любой окрестности точки $f(z_0)$ — $V = V(f(z_0))$ найдется такая окрестность точки z_0 — $U = U(z_0)$, что для всех $z \in U$ выполняется $f(z) \in V$.

(2) *Каждая непрерывная функция* $f : K \to \mathbb{R}$ *на компакте* $K \subset \mathbb{R}^2$ *достигает своего минимума* (напомним, что компакт — это замкнутое ограниченное подмножество плоскости).

Компактом у нас будет круг $|z| \leqslant r$ некоторого достаточно большого радиуса r, который мы определим далее.