

18. Восемнадцатая лекция, 22 марта 2018 г.

18.1. Симметрические многочлены. Рассмотрим кольцо многочленов от n переменных $\mathbb{K}[x_1, \dots, x_n]$. Это множество конечных линейных комбинаций мономов вида $a_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$, где $a_{k_1 \dots k_n} \in K$, которые можно складывать и умножать по обычным правилам. Число $k = k_1 + \dots + k_n$ называется *степенью* монома. Степень многочлена — это максимум по степеням входящих в него мономов.

На кольце $\mathbb{K}[x_1, \dots, x_n]$ действует симметрическая группа S_n . Её действие на образующих $x_1, \dots, x_n$ задаётся перестановками переменных: $\sigma(x_i) = x_{\sigma(i)}$, и продолжается на мономы по мультипликативности: $\sigma(a x_1^{k_1} \dots x_n^{k_n}) = a x_{\sigma(1)}^{k_1} \dots x_{\sigma(n)}^{k_n}$, и далее на все многочлены по линейности.

Многочлены, инвариантные при этом действии, называются *симметрическими*.

ОПРЕДЕЛЕНИЕ 18.1. Многочлен от n переменных называется симметрическим, если он переходит в себя при любых перестановках переменных.

Группа перестановок порождается транспозициями. Поэтому можно дать следующее определение, эквивалентное предыдущему:

ОПРЕДЕЛЕНИЕ 18.2. Многочлен от n переменных называется симметрическим, если он переходит в себя при перестановке любых двух переменных.

Приведем примеры симметрических многочленов.

ПРИМЕР 18.3 (многочлены Ньютона). $s_k = x_1^k + x_2^k + \dots + x_n^k$, где $k \geq 1$.

ПРИМЕР 18.4 (элементарные симметрические многочлены). $e_1 = x_1 + \dots + x_n$, $e_2 = \sum_{i < j} x_i x_j$, $e_k = \sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}$, $e_n = x_1 x_2 \dots x_n$. В отличие от предыдущего примера, здесь k уже не превосходит n .

Элементарные симметрические многочлены возникают в формулах Виета, связывающих коэффициенты многочлена и его корни:

ТЕОРЕМА 18.5 (Виет). Пусть многочлен $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ раскладывается на линейные множители: $p(x) = a_0 (x - t_1) \dots (x - t_n)$. Тогда $a_k = (-1)^k a_0 e_k(t_1, \dots, t_n)$.

Поскольку сумма и произведение симметрических многочленов снова будут симметрическими, множество симметрических многочленов образует подалгебру в $\mathbb{K}[x_1, \dots, x_n]$. Она обозначается через $\mathbb{K}[x_1, \dots, x_n]^{S_n}$.

ПРЕДЛОЖЕНИЕ 18.6. Кольцо $\mathbb{K}[x_1, \dots, x_n]^{S_n} \subset R$ — это градуированное подкольцо: все однородные компоненты симметрического многочлена снова симметрические.

ДОКАЗАТЕЛЬСТВО. Пусть p — симметрический многочлен степени k . Тогда его старшая однородная компонента равна

$$p_k = \lim_{t \rightarrow \infty} p(tx_1, \dots, tx_n)/t^k,$$

и это снова симметрический многочлен (как предел симметрических). Для доказательства симметричности остальных однородных компонент рассмотрим многочлен $p - p_k$ и применим индукцию. $\square$

Это значит, что если $F(X_1, \dots, X_m)$ — произвольный многочлен, а $f_1, \dots, f_m$ — симметрические многочлены, то многочлен $F(f_1, \dots, f_m)$, полученный в результате подстановки f_i в F , снова будет симметрическим.

Возникает задача о нахождении *системы образующих* этой алгебры: как найти такие симметрические многочлены, через которые всякий симметрический многочлен выражался бы полиномиальным образом? Оказывается, что на эту роль подходят элементарные симметрические многочлены. Кроме того, выражение многочлена через $e_1, \dots, e_n$ оказывается единственным. Это утверждает

18.2. Основная теорема о симметрических многочленах.

ТЕОРЕМА 18.7 (Основная теорема о симметрических многочленах). *Всякий симметрический многочлен единственным образом представляется в виде многочлена от $e_1, \dots, e_n$. Иначе говоря, для любого симметрического многочлена $f(x_1, \dots, x_n)$ найдётся единственный многочлен $F(X_1, \dots, X_n)$, для которого $f(x_1, \dots, x_n) = F(e_1, \dots, e_n)$.*

ПРИМЕР 18.8. Выразим s_2 через элементарные симметрические. $s_2 = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2 \sum_{i < j} x_i x_j = e_1^2 - 2e_2$. То есть в этом случае $F(X_1, X_2) = X_1^2 - X_2$.

ДОКАЗАТЕЛЬСТВО. Определим *лексикографическое упорядочение* на мономах от n переменных. Будем говорить, что моном $x_1^{i_1} \dots x_n^{i_n}$ *старше* монома $x_1^{j_1} \dots x_n^{j_n}$, если для некоторого индекса k имеет место неравенство $i_k > j_k$, и при этом все показатели при предыдущих переменных равны: $i_1 = j_1, i_2 = j_2, \dots, i_{k-1} = j_{k-1}$. Обозначение:

$$x_1^{i_1} \dots x_n^{i_n} \succ x_1^{j_1} \dots x_n^{j_n}.$$

Таким образом можно сравнить любые два монома, т.е. это *полный* порядок. Термин «лексикографическое упорядочение» объясняется тем, что наборы $(i_1, \dots, i_n)$ и $(j_1, \dots, j_n)$ сравниваются как слова в словаре: сначала сравниваются их первые элементы, потом, в случае их равенства — вторые, и так далее.

Несложно проверить следующие свойства лексикографического упорядочения:

ПРЕДЛОЖЕНИЕ 18.9. *Для любых ненулевых мономов u, v, w верно, что:*

- (1) *если $u \succ v$ и $v \succ w$, то $u \succ w$;*
- (2) *если $u \succ v$, то $uw \succ vw$ для любого w ;*
- (3) *если $u_1 \succ v_1$ и $u_2 \succ v_2$, то $u_1 v_1 \succ u_2 v_2$.*

УПРАЖНЕНИЕ 18.10. Проверьте эти свойства.

ЗАМЕЧАНИЕ 18.11. Лексикографический порядок не согласован со степенью монома: так, например, $x_1^2 x_2 \succ x_1 x_2^3$, хотя степень второго монома равна четырём, а первого — трём.

Продолжение следует...

□

E-mail address: esmirnov@hse.ru