

18. Восемнадцатая лекция, 9 апреля 2019 г.

18.1. Симметрические многочлены. Рассмотрим кольцо многочленов от n переменных $\mathbb{K}[x_1, \dots, x_n]$, где $\mathbb{K}$ — поле нулевой характеристики. Это множество конечных линейных комбинаций мономов вида $a_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$, где $a_{k_1 \dots k_n} \in \mathbb{K}$, 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: $\sigma(ax_1^{k_1} \dots x_n^{k_n}) = x_{\sigma(1)}^{k_1} \dots x_{\sigma(n)}^{k_n}$, 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 $a_k = (-1)^k a_0 e_k(t_1, \dots, t_n)$.

ПРИМЕР 18.6 (полные симметрические многочлены). $h_1 = x_1 + \dots + x_n$, $h_2 = \sum_{i < j} x_i x_j$, $\dots$, $h_k = \sum_{i_1 \leq \dots \leq i_k} x_{i_1} x_{i_2} \dots x_{i_k}$. Здесь n уже будет произвольным.

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 Λ_n . Кроме того, эта подалгебра градуированная: если многочлен является симметрическим, то каждая его однородная компонента данной степени — снова симметрический многочлен.

Это значит, что если $F(y_1, \dots, y_m)$ — 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 многочлена $f(x_1, \dots, x_n) \in \Lambda_n$ найдётся единственный многочлен $F(y_1, \dots, y_n) \in \mathbb{K}[y_1, \dots, y_n]$, 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 $F(y_1, y_2) = y_1^2 - y_2$.

ДОКАЗАТЕЛЬСТВО. Оно будет конструктивным: мы приведем алгоритм нахождения такого многочлена F .

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. (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 $u \succ v$ и $u' \succ v'$, то $uu' \succ vv'$.

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 четырем, а первого — трем.

ОПРЕДЕЛЕНИЕ 18.12. *Старшим членом* многочлена $P(x_1, \dots, x_n)$ (обозначение: $\text{ht } P$) называется самый старший при лексикографическом упорядочении из входящих в него мономов.

ПРИМЕР 18.13. $\text{ht}(2x_1 x_3^3 + x_1 x_2^2 x_3 - x_2 x_3^2 + 5x_1^2 x_2 - 4x_2) = 5x_1^2 x_2$.

ЛЕММА 18.14. *Старший член произведения многочленов равен произведению их старших членов.*

ДОКАЗАТЕЛЬСТВО. Это следует из свойств лексикографического порядка (предложение 18.9). $\square$

Следующая лемма уже относится к симметрическим многочленам.

ЛЕММА 18.15. Пусть $f \in \Lambda_n$ — симметрический многочлен. Тогда его старший член $\text{ht } f = u = ax_1^{k_1} \dots x_n^{k_n}$ удовлетворяет неравенствам $k_1 \geq k_2 \geq \dots \geq k_n$.

ДОКАЗАТЕЛЬСТВО. Предположим противное: пусть $k_i < k_{i+1}$ для некоторого i . Тогда, по определению симметрического многочлена, f должен содержать и моном $ax_1^{k_1} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_n^{k_n}$. Но этот моном лексикографически старше, чем u . Противоречие. $\square$

ОПРЕДЕЛЕНИЕ 18.16. Будем называть мономы вида $ax_1^{k_1} \dots x_n^{k_n}$, для которых $k_1 \geq k_2 \geq \dots \geq k_n$, *ступенчатыми*.

ЛЕММА 18.17. Пусть $u = x_1^{k_1} \dots x_n^{k_n}$ — ступенчатый моном. Тогда существуют и однозначно определены числа $\ell_1, \dots, \ell_n$, что старший член многочлена $e_1^{\ell_1} \dots e_n^{\ell_n}$ совпадает с u .

ДОКАЗАТЕЛЬСТВО. Старший член многочлена e_k равен $x_1 \dots x_k$. Поэтому старший член многочлена $e_1^{\ell_1} \dots e_n^{\ell_n}$ равен

$$x_1^{\ell_1} (x_1 x_2)^{\ell_2} \dots (x_1 \dots x_n)^{\ell_n} = x_1^{\ell_1 + \dots + \ell_n} x_2^{\ell_2 + \dots + \ell_n} \dots x_n^{\ell_n}.$$

Получаем систему уравнений на ℓ_i :

$$\begin{aligned}\ell_1 + \ell_2 + \dots + \ell_n &= k_1; \\ \ell_2 + \dots + \ell_n &= k_2; \\ &\dots \\ \ell_n &= k_n.\end{aligned}$$

Она имеет единственное решение: $\ell_i = k_i - k_{i+1}$. Лемма доказана.

Перейдём к доказательству теоремы. Пусть $f(x_1, \dots, x_n)$ — симметрический многочлен. Докажем существование такого многочлена $F(y_1, \dots, y_n)$, что $f = F(e_1, \dots, e_n)$. Пусть $\text{ht } f = u = ax_1^{k_1} \dots x_n^{k_n}$. Согласно предыдущей лемме, существует такой многочлен $F_1(y_1, \dots, y_n)$, что $\text{ht } F(e_1, \dots, e_n) = u$. Рассмотрим разность этих многочленов:

$$f_1(x_1, \dots, x_n) = f - F(e_1, \dots, e_n).$$

Если $f_1 = 0$, то всё доказано. Если нет, то пусть $u_2 = \text{ht } f_1$. Ясно, что $u_2 \prec u_1$. Применим к u_2 ту же процедуру: найдём многочлен от $\sigma_1, \dots, \sigma_n$ со старшим членом u_2 и вычтем его из f_1 , получим многочлен со старшим членом u_3 , и так далее. Мы получим убывающую последовательность мономов

$$u_1 \succ u_2 \succ u_3 \succ \dots$$

Все эти мономы являются старшими членами симметрических многочленов, т.е. являются ступенчатыми. Но существует лишь конечное число ступенчатых мономов, лексикографически младших u_1 : действительно, показатели при всех x_i во всех таких мономах не превосходят показателя при x_1 в мономе u_1 , т.е. k_1 . Таких мономов имеется конечное число. Поэтому процесс оборвётся: на каком-то шаге $u_N = 0$. Тем самым мы получим выражение многочлена f через элементарные симметрические.

Докажем единственность такого выражения. Предположим противное: пусть найдутся такие многочлены $F(y_1, \dots, y_n)$ и $G(y_1, \dots, y_n)$, что $F(e_1, \dots, e_n) = G(e_1, \dots, e_n)$. Положим $H(y_1, \dots, y_n) = F - G$; получаем, что $H(e_1, \dots, e_n) = 0$.

Покажем, что $H = 0$. Пусть $H_1(y_1, \dots, y_n), \dots, H_s(y_1, \dots, y_n)$ — все ненулевые мономы, входящие в H . Пусть $w_i(x_1, \dots, x_n) = \text{ht } H_i(e_1, \dots, e_n)$ — старшие члены многочленов, которые получаются при подстановке e_k в H_i . Согласно лемме 18.17, среди w_i нет пропорциональных. Выберем среди них старший моном. Пусть это будет w_1 . По построению, w_1 старше всех остальных мономов, входящих в $H_1(e_1, \dots, e_n)$, и всех мономов, входящих в $H_i(e_1, \dots, e_n)$. Поэтому после приведения подобных слагаемых в сумме

$$H(e_1, \dots, e_n) = H_1(e_1, \dots, e_n) + \dots + H_n(e_1, \dots, e_n)$$

член w_1 сохранится, т.к. ему не с кем будет сократиться. Противоречие. Значит, $e_1, \dots, e_n$ алгебраически независимы. $\square$

$\square$

19. Девятнадцатая лекция, 9 апреля 2019 г.

19.1. Результат. Рассмотрим два многочлена от одной переменной (над произвольным полем K), степени n и m соответственно:

$$\begin{aligned}f(x) &= a_n x^n + \dots + a_1 x + a_0; \\ g(x) &= b_m x^m + \dots + b_1 x + b_0.\end{aligned}$$

Наша ближайшая задача — определить, имеют ли эти многочлены общий сомножитель.

Сначала дадим на этот вопрос «малоинформативный» ответ. Предположим, что общий множитель у f и g есть: $f = f_1 h$, $g = g_1 h$, где $\deg h > 0$. Это значит, что у них имеется общее кратное степени строго меньшей, чем $m + n$. Это кратное есть $f_1 g_1 h$. При этом «дополнительные множители», на которые надо домножить f и g для того, чтобы его получить, равны g_1 и f_1 соответственно, и их степени не превосходят $m-1$ и $n-1$. Напротив, если у f и g нет общих множителей, то их наименьшее общее кратное имеет степень $m + n$, и нельзя найти такие многочлены p и q , где $\deg p < m$, $\deg q < n$, что $fp + gq = 0$.

Тем самым, имеет место следующее предложение:

ПРЕДЛОЖЕНИЕ 19.1. *Многочлены $f(x)$ и $g(x)$, где $\deg f = n$, $\deg g = n$, имеют общий множитель тогда и только тогда, когда найдутся такие многочлены $p(x)$ и $q(x)$, не равные одновременно нулю, где $\deg p(x) \leq m-1$, $\deg q(x) \leq n-1$, что $f(x)p(x) + g(x)q(x) = 0$.*

Попробуем интерпретировать это условие как-то ещё. Выпишем многочлены $p(x)$ и $q(x)$:

$$\begin{aligned} p(x) &= p_{m-1}x^{m-1} + \dots + p_1x + p_0; \\ q(x) &= q_{n-1}x^{n-1} + \dots + q_1x + q_0. \end{aligned}$$

Запишем в явном виде условие из предложения 19.1:

$$\begin{aligned} f(x)p(x) + g(x)q(x) &= (a_n p_{m-1} + b_m q_{n-1})x^{m+n-1} + \\ &+ (a_{n-1}p_{m-1} + a_n p_{m-2} + b_{m-1}q_{n-1} + b_m q_{n-2})x^{m+n-2} + \dots + a_0 p_0 + b_0 q_0 = 0. \end{aligned}$$

Условие равенства многочлена степени $m+n-1$ нулю — это система из $m+n$ линейных однородных уравнений на неизвестные $p_{m-1}, \dots, p_0, q_{n-1}, q_0$. Искомые многочлены $p(x)$ и $q(x)$ существуют тогда и только тогда, когда у этой системы есть ненулевое решение, т.е. когда матрица системы вырождена. Определитель этой матрицы называется *результантом* многочленов $f(x)$ и $g(x)$ и обозначается $\text{Res}(f, g)$. Выпишем его явно:

$$\text{Res}(f, g) = \begin{vmatrix} a_n & & & & b_m & & & \\ a_{n-1} & a_n & & & b_{m-1} & b_m & & \\ \vdots & a_{n-1} & \ddots & & \vdots & b_{m-1} & \ddots & \\ a_0 & \vdots & \ddots & a_n & b_0 & \vdots & \ddots & b_m \\ & a_0 & & a_{n-1} & & b_0 & & b_{m-1} \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{vmatrix}$$

Мы доказали следующую теорему.

ТЕОРЕМА 19.2. *Многочлены $f(x)$ и $g(x)$ имеют общий множитель тогда и только тогда, когда их результат $\text{Res}(f, g)$ равен нулю.*

СЛЕДСТВИЕ 19.3. *Пусть многочлены $f(x)$ и $g(x)$ имеют общий корень. Тогда $\text{Res}(f, g) = 0$.*

19.2. Другие формулы для результата. Предположим, что многочлены $f(x)$ и $g(x)$ раскладываются на линейные множители:

$$\begin{aligned} f(x) &= a_n(x - t_1) \dots (x - t_n); \\ g(x) &= b_m(x - u_1) \dots (x - u_m). \end{aligned}$$

Коэффициенты a_k и b_k выражаются через корни этих многочленов:

$$a_k = a_n(-1)^{n-k} e_{n-k}(t_1, \dots, t_n), \quad b_k = b_m(-1)^{m-k} \tilde{e}_{m-k}(u_1, \dots, u_m), \quad (*)$$

где e и $\tilde{e}$ — элементарные симметрические многочлены от n и m переменных соответственно. Также полезно заметить, что $\text{Res}(f, g)$ является однородным многочленом от a_i степени m и от b_j степени n .

ПРЕДЛОЖЕНИЕ 19.4. $\text{Res}(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (t_i - u_j) = a_n^m \prod_{i=1}^n g(t_i) = (-1)^{mn} b_m^n \prod_{j=1}^m f(u_j)$.

ДОКАЗАТЕЛЬСТВО. Последние два равенства очевидно следуют из вида разложения $f(x)$ и $g(x)$ на линейные множители. Докажем первое равенство.

Во-первых, из равенств (*) следует, что $\text{Res}(f, g)$ как многочлен от a_n, b_m, t_i, u_j делится на $a_n^m b_m^n$. Кроме того, $\text{Res}(f, g)$ обращается в нуль, если многочлены f и g имеют общий корень, т.е. если $t_i = u_j$ при каких-то i, j . Поэтому $\text{Res}(f, g)$ делится на любую из разностей $t_i - u_j$, а значит, и на их произведение. Мы доказали, что $\text{Res}(f, g)$ делится на $a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (t_i - u_j)$.

Далее, заметим, что оба эти выражения имеют степень m как многочлены от $a_0, \dots, a_n$: про результат это, как было сказано выше, следует из его явного вида, а про правую часть это верно в силу того, что она равна $(-1)^{mn} b_m^n \prod_{j=1}^m f(u_j)$, а каждый из сомножителей $f(u_j)$ линеен как многочлен от a_i . По тем же соображениям они оба имеют степень n как многочлены от $b_0, \dots, b_m$. Следовательно, эти выражения получаются друг от друга домножением на элемент основного поля $\mathbb{K}$.

Для завершения доказательства заметим, что оба эти выражения как многочлены от a_i и b_j содержат одночлен $a_n^m b_0^n$ с коэффициентом 1. Поэтому они равны. $\square$