

ЛЕКЦИЯ 8

Элементарные симметрические многочлены. Основная теорема о симметрических многочленах. Лексикографический порядок. Теорема Виета. Дискриминант многочлена.

Вернемся ненадолго к теме прошлой лекции. Рассмотрим кольцо $R = K[x_1, \dots, x_n]$, где K — поле. На семинарах разбиралось, что оно не является кольцом главных идеалов и, соответственно, евклидовым кольцом. Однако несмотря на это:

Теорема. Кольцо R факториально.

Впрочем, доказывать эту теорему мы не будем.

Вернемся теперь к теме текущей лекции. Пусть K — произвольное поле.

Определение 1. Многочлен $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ называется *симметрическим*, если $f(x_{\tau(1)}, \dots, x_{\tau(n)}) = f(x_1, \dots, x_n)$ для всякой перестановки $\tau \in S_n$.

Примеры:

- 1) Многочлен $x_1x_2 + x_2x_3$ не является симметрическим, а вот многочлен $x_1x_2 + x_2x_3 + x_1x_3$ — является.
- 2) *Степенные суммы* $s_k(x_1, \dots, x_n) = x_1^k + x_2^k + \dots + x_n^k$ являются симметрическими многочленами.
- 3) *Элементарные симметрические многочлены*

$$\begin{aligned}\sigma_1(x_1, \dots, x_n) &= x_1 + x_2 + \dots + x_n; \\ \sigma_2(x_1, \dots, x_n) &= \sum_{1 \leq i < j \leq n} x_i x_j; \\ &\dots \dots \dots \\ \sigma_k(x_1, \dots, x_n) &= \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}; \\ &\dots \dots \dots \\ \sigma_n(x_1, \dots, x_n) &= x_1 x_2 \dots x_n\end{aligned}$$

являются симметрическими.

- 5) Определитель Вандермонда

$$V(x_1, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

симметрическим многочленом не является (при перестановке индексов умножается на её знак), а вот его квадрат уже является.

Основная цель этой лекции — понять, как устроены все симметрические многочлены.

Легко видеть, что все симметрические многочлены образуют подкольцо (и даже подалгебру) в $K[x_1, \dots, x_n]$. В частности, если $F(y_1, \dots, y_k)$ — произвольный многочлен и $f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)$ — симметрические многочлены, то многочлен

$$F(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) \in K[x_1, \dots, x_n]$$

также является симметрическим. Мы покажем, что всякий симметрический многочлен однозначно выражается через элементарные симметрические многочлены.

Основная теорема о симметрических многочленах. Для всякого симметрического многочлена $f(x_1, \dots, x_n)$ существует и единственен такой многочлен $F(y_1, \dots, y_n)$, что

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

Пример. $s_2(x_1, \dots, x_n) = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2 \sum_{1 \leq i < j \leq n} x_i x_j = \sigma_1^2 - 2\sigma_2$, откуда $F(y_1, \dots, y_n) = y_1^2 - 2y_2$.

Доказательство этой теоремы потребует некоторой подготовки. Начнём с того, что определим старший член многочлена от многих переменных.

Пусть M_n — множество всех одночленов от переменных x_1, \dots, x_n . Определим на M_n лексикографический порядок следующим образом:

$$ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \prec bx_1^{j_1}x_2^{j_2}\dots x_n^{j_n} \Leftrightarrow \exists k : i_1 = j_1, \dots, i_{k-1} = j_{k-1}, i_k < j_k.$$

Например, $x_1^2x_3^9 \prec x_1^2x_2$.

Свойства:

- 1) Лексикографический порядок обладает свойством транзитивности: если $u, v, w \in M_n$, $u \prec v$ и $v \prec w$, то $u \prec w$ (докажите это).
- 2) Если $u, v, w \in M_n$ и $u \prec v$, то $uw \prec vw$.

Свойство транзитивности лексикографического порядка позволяет корректно определить следующее понятие.

Определение 2. *Старшим членом* ненулевого многочлена $f(x_1, \dots, x_n)$ называется наибольший в лексикографическом порядке встречающийся в нём одночлен. Обозначение: $L(f)$.

Примеры:

- 1) $L(s_k) = x_1^k$;
- 2) $L(\sigma_k) = x_1x_2\dots x_k$.

Лемма о старшем члене. Пусть $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ — произвольные ненулевые многочлены. Тогда $L(fg) = L(f)L(g)$.

Доказательство. Пусть u — какой-то одночлен многочлена f и v — какой-то одночлен многочлена g . По определению старшего члена имеем

$$(1) \quad u \preceq L(f), \quad v \preceq L(g).$$

Тогда $uv \preceq uL(g) \preceq L(f)L(g)$, т.е. $uv \preceq L(f)L(g)$. Более того, легко видеть, что $uv \prec L(f)L(g)$ тогда и только тогда, когда хотя бы одно из «неравенств» (1) является строгим. Отсюда следует, что после раскрытия скобок в произведении fg одночлен $L(f)L(g)$ будет старше всех остальных возникающих одночленов. Ясно, что после приведения подобных членов этот одночлен сохранится и будет по-прежнему старше всех остальных одночленов, поэтому $L(f)L(g) = L(fg)$. \square

Лемма 1. Если $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ — старший член некоторого симметрического многочлена $f(x_1, \dots, x_n)$, то $k_1 \geq k_2 \geq \dots \geq k_n$.

Доказательство. От противного. Пусть $k_i < k_{i+1}$ для некоторого $i \in \{1, \dots, n-1\}$. Тогда, будучи симметрическим, многочлен f содержит одночлен $ax_1^{k_1}\dots x_{i-1}^{k_{i-1}}x_i^{k_{i+1}}x_{i+1}^{k_i}x_{i+2}^{k_{i+2}}\dots x_n^{k_n}$, который старше $L(f)$. Противоречие. \square

Лемма 2. Пусть k_1, \dots, k_n — целые неотрицательные числа. Если $k_1 \geq k_2 \geq \dots \geq k_n$, то существуют и единственны такие целые неотрицательные числа l_1, l_2, \dots, l_n , что

$$x_1^{k_1}x_2^{k_2}\dots x_n^{k_n} = L(\sigma_1(x_1, \dots, x_n)^{l_1}\sigma_2(x_1, \dots, x_n)^{l_2}\dots\sigma_n(x_1, \dots, x_n)^{l_n}).$$

Доказательство. С учётом леммы о старшем члене требуемое условие означает, что искомые числа l_1, \dots, l_n удовлетворяют системе

$$\begin{cases} l_1 + l_2 + \dots + l_n = k_1; \\ \quad l_2 + \dots + l_n = k_2; \\ \quad \quad \dots \dots \dots \\ \quad \quad \quad l_n = k_n, \end{cases}$$

из которой они легко находятся:

$$\begin{aligned} l_i &= k_i - k_{i+1} \quad \text{при } 1 \leq i \leq n-1; \\ l_n &= k_n. \end{aligned}$$

\square

Доказательство основной теоремы о симметрических многочленах. Пусть $f(x_1, \dots, x_n)$ — произвольный симметрический многочлен.

Сначала докажем существование искомого многочлена $F(y_1, \dots, y_n)$. Если $f(x_1, \dots, x_n)$ — нулевой многочлен, то можно взять $F(y_1, \dots, y_n) = 0$. Далее считаем, что $f(x_1, \dots, x_n) \neq 0$. Пусть $L(f) = ax_1^{k_1} \dots x_n^{k_n}$, $a \neq 0$. Тогда $k_1 \geq k_2 \geq \dots \geq k_n$ в силу леммы 1. По лемме 2 найдётся одночлен от элементарных симметрических многочленов $a\sigma_1^{l_1} \dots \sigma_n^{l_n}$, старший член которого совпадает с $L(f)$. Положим $f_1 := f - a\sigma_1^{l_1} \dots \sigma_n^{l_n}$. Если $f_1 = 0$, то $f = a\sigma_1^{l_1} \dots \sigma_n^{l_n}$ и искомым многочленом будет $F(y_1, \dots, y_n) = ay_1^{l_1} \dots y_n^{l_n}$. Если же $f_1 \neq 0$, то $L(f_1) \prec L(f)$. Повторим ту же процедуру: вычтя из f_1 подходящий одночлен от $\sigma_1, \dots, \sigma_n$, мы получим новый многочлен f_2 со следующим свойством: либо $f_2 = 0$ (и тогда мы получаем выражение f через элементарные симметрические многочлены), либо $L(f_2) \prec L(f_1)$. Многократно повторяя эту процедуру, мы получим последовательность многочленов f, f_1, f_2, \dots со свойством $L(f) \succ L(f_1) \succ L(f_2) \succ \dots$. Покажем, что процесс закончится, т. е. найдётся такое m , что $f_m = 0$ (и тогда мы получим представление f в виде многочлена от $\sigma_1, \dots, \sigma_n$). Для этого заметим, что переменная x_1 входит в старший член каждого из многочленов f_1, f_2, \dots в степени, не превышающей k_1 . Но в силу леммы 1 одночленов с таким условием имеется лишь конечное число, поэтому процесс не может продолжаться бесконечно.

Теперь докажем единственность многочлена $F(y_1, \dots, y_n)$. Предположим, что

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

для двух различных многочленов $F(y_1, \dots, y_n), G(y_1, \dots, y_n) \in K[y_1, \dots, y_n]$. Тогда многочлен

$$H(y_1, \dots, y_n) := F(y_1, \dots, y_n) - G(y_1, \dots, y_n)$$

является ненулевым, но $H(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) = 0$. Покажем, что такое невозможно. Пусть H_1, \dots, H_s — все ненулевые одночлены в H . Обозначим через w_i старший член многочлена

$$H_i(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \in K[x_1, \dots, x_n].$$

В силу леммы 2 среди одночленов w_1, \dots, w_s нет пропорциональных. Выберем из них старший в лексикографическом порядке. Он не может сократиться ни с одним членом в выражении

$$H_1(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) + \dots + H_s(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)),$$

поэтому $H(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \neq 0$, и мы пришли к противоречию. \square

На практике многочлен $F(y_1, \dots, y_n)$ можно искать, повторяя описанный в доказательстве алгоритм, однако он может потребовать много вычислений. Более эффективным для нахождения многочлена $F(y_1, \dots, y_n)$ является метод неопределённых коэффициентов, который планируется разобрать на семинарах.

Теорема Виета. Пусть $\alpha_1, \dots, \alpha_n$ — корни многочлена $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Тогда

$$\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k}, \quad k = 1, \dots, n.$$

Доказательство. Достаточно приравнять коэффициенты при x^{n-k} в левой и правой частях равенства

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

\square

Из теоремы Виета и основной теоремы о симметрических многочленах следует, что мы можем выразить значение любого симметрического многочлена от корней данного многочлена через коэффициенты, не находя самих корней.

Определение 3. Дискриминантом многочлена $h(x) = a_nx^n + \dots + a_1x + a_0$ с корнями $\alpha_1, \dots, \alpha_n$ называется выражение

$$D(h) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Замечание 1. Дискриминант $D(h)$ является симметрическим многочленом от $\alpha_1, \dots, \alpha_n$, а значит, в соответствии с вышесказанным он является многочленом от коэффициентов a_n, a_{n-1}, \dots, a_0 .

Замечание 2. Непосредственно из определения следует, что $D(h) = 0$ тогда и только тогда, когда многочлен h имеет кратный корень.

СПИСОК ЛИТЕРАТУРЫ

- [1] Э.Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 3, § 8)
- [2] А.И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 6, § 2)
- [3] Сборник задач по алгебре под редакцией А.И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 6, §§ 31,32)