Лекция 21

Определение 1. Многочлен $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ называется *симметрическим*, если для любой подстановки $\pi \in S_n$ выполнено

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

Примеры

- $f = c = const$,
- степенные суммы $s_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k$,
- элементарные симметрические многочлены $1 \leq k \leq n$

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 < i_2 < \ldots < i_k} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

- если $f_1, \ldots f_m \in F[x_1, \ldots, x_n]$ – симметрические многочлены и $g \in F[y_1, \ldots, y_m]$. Тогда

$$h(x_1, \ldots, x_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) -$$

  симметрический многочлен

Замечание 1. То, что $f(x_1, \ldots, x_n)$ симметрический равносильно тому, что коэффициенты при $x_1^{k_1} \ldots x_n^{k_n}$ и $x_1^{k_{\pi(1)}} \ldots x_n^{k_{\pi(n)}}$ одинаковы.

Теорема 1 (Теорема Виета)**.** *Пусть $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \in F[x]$ имеет $n = \deg f$ корней с учетом кратностей. То есть*

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Тогда для каждого $1 \leq k \leq n$ выполнено

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \frac{a_i}{a_0}.$$

Доказательство.

$$\begin{aligned} f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_k x^{n-k} \ldots + a_n = \\ = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) = \\ = a_0 \sum_{k=0}^{n} \sum_{i_1 < \ldots < i_k} x x \ldots (-\alpha_{i_1}) \ldots x \ldots (-\alpha_{i_k}) \ldots x = \\ = a_0 \sum_{k=0}^{n} x^{n-k} \sum_{i_1 < \ldots < i_k} (-1)^k \alpha_{i_1} \ldots \alpha_{i_k} = \\ = a_0 \sum_{k=0}^{n} x^{n-k} (-1)^k \sigma_k(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

Получаем $a_0(-1)^k \sigma_k(\alpha_1, \ldots, \alpha_n) = a_k$. □

Лемма 1. *Пусть $f(x_1, \ldots, x_n)$ – ненулевой симметрический многочлен. Тогда если*

$$LM(f) = x_1^{a_1} \ldots x_n^{a_n},$$

то $a_1 \geq a_2 \geq \ldots \geq a_n$.

Доказательство. Допустим, что $a_j > a_i$ при $i < j$. Возьмем $\pi = (i, j)$. Тогда моном

$$x_1^{a_{\pi(1)}} \ldots x_n^{a_{\pi(n)}} = x_1^{a_1} \ldots x_i^{a_j} \ldots x_j^{a_i} \ldots x_n^{a_n}$$

входит в f с тем же (а значит, ненулевым) коэффициентом. Однако этот моном больше в лексикографическом порядке, чем $x_1^{a_1} \ldots x_n^{a_n}$. Противоречие. □

Лемма 2.

$$LT(\sigma_k(x_1, \ldots x_n)) = x_1 \ldots x_k.$$

Доказательство. Заметим, что $x_1 \ldots x_k$ – единственный моном в σ_k, удовлетворяющий неравенству из леммы 1. □

Лемма 3. *Для любого набора $a_1 \geq a_2 \geq \ldots \geq a_n$ выполнено*

$$x_1^{a_1} \ldots x_n^{a_n} = LT(\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3} \ldots \sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}).$$

Доказательство.

$$\begin{aligned} LT(\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3} \ldots \sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}) = \\ = LT(\sigma_1)^{a_1-a_2} LT(\sigma_2)^{a_2-a_3} \ldots LT(\sigma_{n-1})^{a_{n-1}-a_n} LT(\sigma_n)^{a_n} = \\ = x_1^{a_1-a_2}(x_1x_2)^{a_2-a_3} \ldots (x_1 \ldots x_{n-1})^{a_{n-1}-a_n}(x_1 \ldots x_n)^{a_n} = x_1^{a_1} \ldots x_n^{a_n}. \end{aligned}$$

□

Следствие 1. *Для любого симметрического многочлена f существуют единственные $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0}$ и $c \in F$ такие, что $LT(f) = LT(c\sigma_1^{m_1} \ldots \sigma_n^{m_n})$.*

Теорема 2 (Основная теорема о симметрических многочленах)**.** *Пусть $f \in F[x_1, \ldots, x_n]$ – ненулевой симметрический многочлен. Тогда существует единственный многочлен $g \in F[y_1, \ldots, y_n]$ такой, что*

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

Доказательство. **Доказательство существования.** По следствию существуют $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0}$ и $c \in F$ такие, что $LT(f) = LT(c\sigma_1^{m_1} \ldots \sigma_n^{m_n})$. Рассмотим $f_1 = f - c\sigma_1^{m_1} \ldots \sigma_n^{m_n}$. Старшие члены сократились. Значит, $LM(f) \succ LM(f_1)$. При этом f_1 – симметрический многочлен. Продолжим аналогично, стартуя с многочлена f_1. Получим последовательность $f, f_1, f_2, \ldots$, для которых верно, что $LM(f) \succ LM(f_1) \succ LM(f_2) \succ \ldots$ Так как не существует бесконечной убывающей цепочки мономов, данная последовательность должна прийти к нулевому многочлену. (Иначе можно продолжать эту цепочку.)

Доказательство единственности. Предположим, что

$$f(x_1, \ldots, x_n) = g_1(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = g_2(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)).$$

Положим $h = g_1 - g_2 \in F[y_1, \ldots, y_n]$. Тогда

$$h(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = 0.$$

Допустим, что $h \neq 0$. Тогда для каждых различных членов $cy_1^{l_1} \ldots y_n^{l_n}$ старшие мономы многочленов $\sigma_1^{l_1} \ldots \sigma_n^{l_n}$ не совпадают. А значит, самый старший из этих старших членов ни с кем не сократится. Противоречие. Значит, $h = 0$, то есть $g_1 = g_2$. □

Лемма 4.

$$\deg g = \deg_{x_1} f.$$

Доказательство. Самая большая степень x_1 содержится в $LM(f) = x_1^{a_1} \ldots x_n^{a_n}$. При этом в g входит $y_1^{a_1-a_2}y_2^{a_2-a_3} \ldots y_n^{a_n}$ – моном суммарной степени a_1. Отсюда $\deg g \geq \deg_{x_1} f$.

С другой стороны, если g имеет моном $y_1^{b_1} \ldots y_m^{b_m}$, то $\deg_{x_1}(\sigma_1^{b_1} \ldots \sigma_m^{b_m})$ равна $\sum b_i$. Допустим $\deg g \geq \deg_{x_1} f$. Значит, в многочлене $\sigma_1^{b_1} \ldots \sigma_m^{b_m}$ есть моном больше, чем $LM(f)$. Но тогда он должен сократиться. Как мы видели, сократиться со старшим членом многочлена $\sigma_1^{d_1} \ldots \sigma_m^{d_m}$ он не может, следовательно, он сокращается с не старшим членом одного из таких многочленов. Значит

$$LM(\sigma_1^{d_1} \ldots \sigma_m^{d_m}) \succ LM(\sigma_1^{b_1} \ldots \sigma_m^{b_m}).$$

Выберем моном с максимальным $LM(\sigma_1^{b_1} \ldots \sigma_m^{b_m})$, тогда он ни с кем не сократится. Противоречие. □

Определение 2. Пусть многочлен $f = a_0x^n + \ldots + a_n$ имеет n корней $\alpha_1, \ldots \alpha_n$ с учетом кратности. *Дискриминант* $D(f)$ многочлена $f \in F[x]$ равен

$$D(f) = a_0^{2n-2} \prod_{i<j} (x_i - x_j)^2.$$

Предложение 1 (Основное свойство дискриминанта)**.** *Пусть многочлен $f = a_0x^n + \ldots + a_n$ имеет n корней $\alpha_1, \ldots \alpha_n$ с учетом кратности. $D(f) = 0$ тогда и только тогда, когда у f есть кратные корни.*

Предложение 2. *Пусть многочлен $f = a_0x^n + \ldots + a_n$ имеет n корней $\alpha_1, \ldots \alpha_n$ с учетом кратности. $D(f)$ – многочлен от коэффициентов a_i.*

Доказательство. $\prod_{i<j}(x_i - x_j)^2$ – симметрический многочлен. И его степень по x_1 равна $2n-2$. Применяя теорему Виета, получаем утверждение предложения. □

Пусть A – область целостности. Рассмотрим множество пар $\{(a,b)|a,b \in A, b \neq 0\}$. Введем отношение эквивалентности: $(a,b) \sim (a',b')$, если $ab' = ba'$. Докажем, что это отношение эквивалентности. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a,b) \sim (a',b') \sim (a'',b'')$. Тогда $ab' = ba'$ и $a'b'' = b'a''$. Перемножим эти 2 равенства, получим $ab''a'b' = ba''a'b'$. Если $a'b' \neq 0$, то на него можно сократить. То есть $ab''a'b' - ba''a'b' = (ab'' - ba'')a'b' = 0$, следовательно $ab'' - ba'' = 0$. Если же $a'b' = 0$, то либо $a' = 0$, либо $b' = 0$. Но по условию $b' \neq 0$. Значит, $a' = 0$. Тогда $ab' = ba' = 0$, значит, $a = 0$. Аналогично, $a'b'' = b'a'' = 0$, значит, $a'' = 0$. Получается, что $ab'' = ba'' = 0$.

Определение 3. Классы эквивалентности по данному отношению назовем дробями и класс пары (a,b) будем обозначать $\frac{a}{b}$. При этом $\frac{a}{b} = \frac{a'}{b'}$ тогда и тольк тогда, когда $ab' = ba'$.

Определение 4. Рассмотрим множество частных $Quot(A)$ дробей $\{\frac{a}{b}, a,b \in A, b \neq 0\}$ с операциями

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Докажем корректность операций. Пусть $\frac{a}{b} = \frac{a'}{b'}$, тогда $\frac{a'}{b'} + \frac{c}{d} = \frac{a'd+b'c}{b'd}$. Нужно доказать, что $\frac{a'd+b'c}{b'd} = \frac{ad+bc}{bd}$. В самом деле

$$(a'd + b'c)bd - (ad + bc)b'd = a'bd^2 + b'bcd - abd^2 - b'bcd = (a'b - b'a)d^2 = 0.$$

Аналогично, докажем, что $\frac{a'}{b'} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{c}{d}$.

$$a'cbd - acb'd = (a'b - ba')cd = 0.$$

Теорема 3. *Множество частных $Quot(A)$ с введенными операциями сложения и умножения является полем. (Далее будем называть его полем частных.)*

Доказательство. Коммутативность, ассоциативность сложения и дистрибудивность доказываются приведением к общему знаменателю, а затем применяются тождества к числителю. Нулевой элемент $\frac{0}{1} = \frac{0}{b}$. Противоположный элемент $-\left(\frac{a}{b}\right) = \frac{-a}{b}$. Коммутативность и ассоциативность умножения следует из применения соответствующих свойств к числителю и знаменателю. Единичный элемент $\frac{1}{1}$. Если $a \neq 0$, то $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. □

Теорема 4. *Множество элементов $\frac{a}{1} \in Quot(A)$ образуют подкольцо в $Quot(A)$, изоморфное A. При этом каждый элемент $Quot(A)$ является отношением двух элементов из этого кольца.*

Доказательство. Рассмотрим отображение $\varphi\colon A \to Quot(A)$, $\varphi(a) = \frac{a}{1}$. Легко проверить, что φ – инъективный гомоморфизм. Тогда образ этого гомоморфизма – кольцо, изоморфное A. При этом $\frac{a}{b} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1}$. Если отождествить по φ элементы a и $\frac{a}{1}$, то $\frac{a}{b} = ab^{-1}$, то есть дробь имеет смысл деления. □

Пример 1. *1) Если $A = \mathbb{Z}$, то $Quot(A) = \mathbb{Q}$.*

1) Если $A = F[x]$, то $Quot(A) = F(x)$ – поле рациональных дробей от 1 переменной с коэффициентами в F.