

## 6. ШЕСТАЯ ЛЕКЦИЯ, 11 ОКТЯБРЯ 2022 Г.

**6.1. Многочлены с рациональными коэффициентами: корни и признак неприводимости.** Приведем полезный критерий для поиска рациональных корней многочленов с целыми коэффициентами.

**Предложение 6.1.** Пусть несократимая дробь  $p/q$  — корень многочлена  $a_n x^n + \dots + a_1 x + a_0$ , где  $a_i \in \mathbb{Z}$ . Тогда  $a_n : q$  и  $a_0 : p$ .

*Доказательство.* Подставим  $p/q$  в многочлен и домножим его на  $q^n$ . Получим следующее равенство (в целых числах):

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Все слагаемые в нем, кроме последнего, делятся на  $p$ , поэтому и  $a_0 q^n : p$ . Но  $p$  и  $q$  взаимно просты, то есть  $a_0 : p$ . Аналогично  $a_n : q$ .  $\square$

В частности, если  $a_n = 1$ , мы получаем следующий результат: рациональный корень приведенного многочлена (т.е. многочлена со старшим коэффициентом 1), если он есть, обязательно будет целым числом.

В отличие от многочленов над  $\mathbb{R}$  и тем более  $\mathbb{C}$ , неприводимые многочлены над  $\mathbb{Q}$  (или, что почти то же самое, над  $\mathbb{Z}$ ) устроены сложно, и доказательство неприводимости того или иного многочлена может быть непростой задачей. Приведем одно достаточное условие, которое иногда позволяет убедиться в неприводимости многочлена с целыми коэффициентами.

**Теорема 6.2** (признак Эйзенштейна). Пусть  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  — приведенный многочлен с целыми коэффициентами, и для некоторого простого  $p$  верно, что все коэффициенты  $f(x)$ , кроме старшего, делятся на  $p$ , а свободный член  $a_0$  не делится на  $p^2$ . Тогда  $f(x)$  неприводим над  $\mathbb{Q}$ .

*Доказательство.* Предположим противное: что  $f(x) = g(x)h(x)$  приводим. Аналогично доказательству леммы Гаусса рассмотрим редукцию по модулю  $p$ :

$$\bar{f}(x) = x^n = \bar{g}(x) \cdot \bar{h}(x).$$

Значит,  $\bar{g}(x) = x^m$  и  $\bar{h}(x) = x^{n-m}$  для некоторого  $m$ , где  $0 < m < n$ . Поэтому свободные члены  $g(x)$  и  $h(x)$  делятся на  $p$ . Но отсюда следует, что  $a_0$  делится на  $p^2$  — противоречие.  $\square$

Иногда для применения признака Эйзенштейна бывает полезно сделать в многочлене замену переменной.

**Пример 6.3.** Рассмотрим циклотомический многочлен

$$\Phi_p(x) = x^{p-1} + \dots + x + 1 = \frac{x^p - 1}{x - 1},$$

где  $p$  — простое число. Докажем, что он будет неприводим. Для этого сделаем замену переменной  $y = x - 1$ . Тогда

$$\Phi_p(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \dots + \binom{p}{p-2}y + p.$$

Все коэффициенты этого многочлена  $\binom{p}{k}$  кратны  $p$ , а свободный член равен  $p$  — в частности, он не делится на  $p^2$ . Поэтому  $\Phi_p(y)$ , а значит и  $\Phi_p(x)$ , неприводим по признаку Эйзенштейна.

Этот пример, в частности, показывает, что признак Эйзенштейна не является необходимым условием: коэффициенты многочлена  $\Phi_p(x)$  не удовлетворяют условию ни для какого  $p$ , а он, тем не менее, неприводим.

**6.2. Симметрические многочлены.** В учебнике алгебры для восьмого класса есть следующая задача (как там написано, «повышенной сложности»):

**Задача 6.1.** Пусть  $x_1, x_2$  — корни квадратного уравнения  $x^2 + px + q = 0$ . Найдите  $x_1^3 + x_2^3$ .

Конечно, можно вычислить корни уравнения по известной формуле, посчитать их кубы и сложить. Но это долго и велик шанс ошибиться, так что лучше поступить иначе: заметить, что по теореме Виета (доказанной в том же учебнике несколькими страницами раньше)  $x_1 + x_2 = -p$ ,  $x_1 x_2 = q$ . Далее,  $x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1^2 x_2 - 3x_1 x_2^2 = (x_1 + x_2)^3 - 3x_1 x_2 (x_1 + x_2) = -p^3 + 3pq$ . Это и есть ответ.

При решении этой задачи мы воспользовались тем, что многочлен  $x_1^3 + x_2^3$ , а также  $p$  и  $q$  — это *симметрические* многочлены от  $x_1, x_2$ .

**6.3. Симметрические многочлены.** Пусть  $\mathbb{K}$  — некоторое поле нулевой характеристики (т.е. содержащее поле  $\mathbb{Q}$ ). Например, можно считать, что  $\mathbb{K} = \mathbb{R}$  или  $\mathbb{C}$ .

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 6.4.** 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 6.5.** Многочлен от  $n$  переменных называется симметрическим, если он переходит в себя при перестановке любых двух переменных.

Приведем примеры симметрических многочленов.

**Пример 6.6** (многочлены Ньютона).  $s_k = x_1^k + x_2^k + \dots + x_n^k$ , где  $k \geq 1$ .

**Пример 6.7** (элементарные симметрические многочлены).  $\sigma_1 = x_1 + \dots + x_n$ ,  $\sigma_2 = \sum_{i < j} x_i x_j$ ,  $\sigma_k = \sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}$ ,  $\sigma_n = x_1 x_2 \dots x_n$ . 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 6.8** (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  $a_k = (-1)^k a_0 \sigma_k(t_1, \dots, t_n)$ .

Поскольку сумма и произведение симметрических многочленов снова будут симметрическими, множество симметрических многочленов образует подкольцо в  $\mathbb{K}[x_1, \dots, x_n]$ . Оно обозначается через  $\mathbb{K}[x_1, \dots, x_n]^{S_n}$ . Кроме того, это подкольцо градуированное: если многочлен является симметрическим, то каждая его однородная компонента данной степени — снова симметрический многочлен.

Это значит, что если  $g(y_1, \dots, y_m)$  — произвольный многочлен, а  $f_1, \dots, f_m$  — симметрические многочлены, то многочлен  $g(f_1, \dots, f_m)$ , полученный в результате подстановки  $f_i$  в  $g$ , 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  $\sigma_1, \dots, \sigma_n$  оказывается единственным. Это утверждает

#### 6.4. Основная теорема о симметрических многочленах.

**Теорема 6.9** (Основная теорема о симметрических многочленах). *Всякий симметрический многочлен единственным образом представляется в виде многочлена от  $\sigma_1, \dots, \sigma_n$ . Иначе говоря, для любого симметрического многочлена  $f(x_1, \dots, x_n)$  найдётся единственный многочлен  $g(y_1, \dots, y_n)$ , для которого  $f(x_1, \dots, x_n) = g(\sigma_1, \dots, \sigma_n)$ .*

**Пример 6.10.** Выразим  $s_2$  через элементарные симметрические.  $s_2 = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2 \sum_{i < j} x_i x_j = \sigma_1^2 - 2\sigma_2$ . То есть в этом случае  $g(y_1, y_2) = y_1^2 - y_2$ .

*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 6.11.** (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 6.12.** Проверьте эти свойства.

*Замечание 6.13.* 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 — трем.

**Определение 6.14.** *Старшим членом* многочлена  $f(x_1, \dots, x_n)$  (обозначение:  $\text{ht } f$ ) называется самый старший при лексикографическом упорядочении из входящих в него мономов.

**Пример 6.15.**  $\text{ht}(2x_1 x_3^3 + x_1 x_2^2 x_3 - x_2 x_3^2 + 5x_1^2 x_2 - 4x_2) = 5x_1^2 x_2$ .

**Лемма 6.16.** *Старший член произведения многочленов равен произведению их старших членов.*

*Доказательство.* Это следует из свойств лексикографического порядка (предложение 6.11).  $\square$

Следующая лемма уже относится к симметрическим многочленам.

**Лемма 6.17.** Пусть  $f$  — 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.  $\square$

**Лемма 6.18.** Пусть  $u = x_1^{k_1} \dots x_n^{k_n}$ . Тогда существуют и однозначно определены числа  $\ell_1, \dots, \ell_n$ , что старший член многочлена  $\sigma_1^{\ell_1} \dots \sigma_n^{\ell_n}$  совпадает с  $u$ .

*Доказательство.* Старший член многочлена  $\sigma_k$  равен  $x_1 \dots x_k$ . Поэтому старший член многочлена  $\sigma_1^{\ell_1} \dots \sigma_n^{\ell_n}$  равен

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

Получаем систему уравнений на  $\ell_i$ :

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

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

Перейдём к доказательству теоремы. Пусть  $f(x_1, \dots, x_n)$  — симметрический многочлен. Докажем существование такого многочлена  $g(y_1, \dots, y_n)$ , что  $f = g(\sigma_1, \dots, \sigma_n)$ . Пусть  $\text{ht } f = u = ax_1^{k_1} \dots x_n^{k_n}$ . Согласно предыдущей лемме, существует такой многочлен  $g_1(y_1, \dots, y_n)$ , что  $\text{ht } g_1(\sigma_1, \dots, \sigma_n) = u$ . Рассмотрим разность этих многочленов:

$$f_1(x_1, \dots, x_n) = f - g_1(\sigma_1, \dots, \sigma_n).$$

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. удовлетворяют условию леммы 6.17. Значит, все показатели при всех  $x_i$  во всех  $u_j$  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.

Единственность такого представления будет доказана на следующей лекции.  $\square$