

ЛЕКЦИЯ 23

Лемма 1. Любой элемент $r \neq 0 \in \text{Quot}(A)$, где A – факториальное кольцо, представляется в виде несократимой дроби $r = \frac{a}{b}$, где $a, b \in A$ и $\text{НОД}(a, b) = 1$. Если $r = \frac{a'}{b'}$ – другое такое разложение, то $a' = \lambda a$ и $b' = \lambda b$, где λ – обратимый элемент A .

Доказательство. По определению $r = \frac{f}{g}$, где $f, g \in A \setminus \{0\}$. Если неприводимый множитель p входит и в числитель и в знаменатель, то его можно сократить. Действуем так пока НОД числителя и знаменателя не станет равным 1. Если $\frac{a}{b} = \frac{a'}{b'}$, где $\text{НОД}(a, b) = 1$ и $\text{НОД}(a', b') = 1$, то $ab' = ba'$. Тогда $b|ab'$. Так как $\text{НОД}(a, b) = 1$, $b|b'$. Аналогично получаем $b'|b$, то есть b и b' ассоциированы, значит, $b' = \lambda b$, λ – обратимый элемент A . Тогда $a' = \lambda a$. \square

Лемма 2. Любой многочлен $f(x) = r_n x^n + \dots + r_0 \in \text{Quot}(A)[x]$ можно представить в виде $r \cdot g(x)$, где $r \in \text{Quot}(A)$, $g(x) \in A[x]$ – примитивный многочлен.

Доказательство. Представим каждый ненулевой коэффициент r_i в виде несократимой дроби $r_i = \frac{a_i}{b_i}$. Тогда $a = \text{НОД}(a_i)$, $b = \text{НОК}(b_i)$. Положим $r = \frac{a}{b}$. Тогда $s_i = \frac{r_i}{r} = \frac{a_i b}{a b_i} \in A$, так как $a|a_i$, $b_i|b$. С другой стороны, допустим, что простой множитель p делит все s_i . **Случай 1:** $p|b$. Тогда существует i такое, что p входит в b_i в той же степени, что и в b . Так как $p|b_i$, получаем p не делит a_i и следовательно, не делит a . В итоге p не делит $s_i = \frac{a_i b}{a b_i}$. Противоречие. **Случай 2:** p не делит b . Так как для каждого i выполнено $p|s_i$, то $p|(a_i b)$. Поскольку b не делится на p , получаем, что для каждого i верно $p|a_i$. Но существует i такое, что степень вхождения p в a_i такая же, что и в a . При этом i степень вхождения p в $s_i = \frac{a_i b}{a b_i}$ не может быть положительной. Противоречие. \square

Замечание 1. Как следует из доказательства леммы, если $f \in A[x]$, то $r \in A$.

Замечание 2. Если $f, g \in A[x]$ примитивны и $f = rg$, где $r \in \text{Quot}(A)$, то r обратим. В самом деле, если неприводимый элемент p входит в числитель несократимого вида r , то все коэффициенты f делятся на p . А если в знаменатель, то все коэффициенты g делятся на p .

Лемма 3 (Гаусс). Произведение двух примитивных многочленов – примитивный многочлен.

Доказательство. Пусть $f = a_0 + a_1 x + \dots + a_n x^n$, $g = b_0 + b_1 x + \dots + b_m x^m$ – примитивные многочлены из $A[x]$. Пусть $fg = c_0 + c_1 x + \dots + c_{m+n} x^{m+n}$. При этом

$$c_k = \sum_{j=0}^k a_j b_{k-j}.$$

Допустим, что $p|c_i$ для всех i . Пусть j – минимальное число такое, что a_j не делится на p , а l – минимальное число такое, что b_l не делится на p . Тогда

$$c_{j+l} = a_0 c_{j+l} \dots a_{j-1} b_{l+1} + a_j b_l + a_{j+1} b_{l+1} + \dots + a_{j+l} b_0.$$

Все слагаемые делятся на p , кроме $a_j b_l$. Значит, и вся сумма не делится. Противоречие. \square

Напомним, что нашей целью является доказательство следующей теоремы.

Теорема 1. Пусть A – факториальное кольцо. Тогда кольцо $A[x]$ также факториально.

Доказательство теоремы. Докажем, что неприводимые элементы в $A[x]$ – это неприводимые элементы $p \in A$ и примитивные многочлены $f \in A[x]$, которые неприводимы в $\text{Quot}(A)[x]$. В самом деле, если многочлен степени ноль, то он приводим тогда и только тогда, когда разлагается на 2 необратимых многочлена 0 степени, то есть приводим в A . Многочлен положительной степени может разлагаться либо на произведение необратимой константы и многочлена либо на произведение двух многочленов положительной степени. Первое возможно тогда и только тогда, когда многочлен не является примитивным. Второе дает разложение f в произведение над $\text{Quot}(A)$. Таким образом, примитивный многочлен, который неприводим в $\text{Quot}(A)[x]$ является неприводимым в $A[x]$.

Осталось доказать, что примитивный многочлен f , приводимый в $\text{Quot}(A)[x]$ приводим и в $A[x]$. Пусть $f = gh$, где $g, h \in \text{Quot}(A)[x]$. По лемме существуют элементы r_g и r_h из $\text{Quot}(A)$ такие, что $r_g g$ и $r_h h$ примитивны. Имеем, $f = (r_g r_h)^{-1} (r_g g r_h h)$. По Лемме Гаусса $r_g g r_h h$ примитивен. По замечанию $r_g r_h$ обратим в A . Значит, $f = ((r_g r_h)^{-1} r_g g) (r_h h)$ – разложение f на необратимые множители в $A[x]$.

Существование. Пусть теперь $f \in A[x]$ – произвольный многочлен. Представим его в виде $f = rg$, где g – примитивный многочлен, и $r \in A$. Тогда r можно разложить на неприводимые в A , а g можно разложить на неприводимые в $Quot(A)[x]$. При этом разложение g можно сделать разложением на примитивные неприводимые. Таким образом мы можем разложить любой элемент $f \in A[x]$ на неприводимые в $A[x]$.

Единственность. Пусть $f = p_1 \dots p_m g_1 \dots g_k = q_1 \dots q_u h_1 \dots h_v$, где p_i, q_j – неприводимые в A , а g_i, h_j – примитивные неприводимые в $Quot(A)$. Заметим, что НОД всех коэффициентов f равен $p_1 \dots p_m$, так как $g_1 \dots g_k$ – примитивный многочлен. Аналогично этот же НОД равен $q_1 \dots q_u$. Значит, произведения $p_1 \dots p_m$ и $q_1 \dots q_u$ ассоциированы. Так как A факториально, $u = m$ и p_i и q_j попарно ассоциированы. Кольцо $Quot(A)[x]$ факториально, значит два разложения f совпадают. Отсюда $k = v$ и $g_i = r_i h_i$ для некоторого $r_i \in Quot(A)$. Как доказано ранее из того, что g_i и h_i примитивны следует, что r_i – обратимый элемент A . \square

Результант.

Пусть даны два многочлена из $F[x]$: $f(x) = a_0 x^n + \dots + a_n$, $g(x) = b_0 x^m + \dots + b_m$. Будем считать, что у них количество корней с учетом кратности равно степени:

$$f(x) = a_0 \prod_{i=1}^n (x - x_i), \quad g(x) = b_0 \prod_{j=1}^m (x - y_j).$$

Определение 1. Результантом $R(f, g)$ многочленов f и g называется число

$$a_0^m b_0^n \prod_{1 \leq i \leq n, 1 \leq j \leq m} (x_i - y_j).$$

Предложение 1 (Свойства результанта).

- (1) $R(f, g) = 0$ тогда и только тогда, когда f и g имеют общий корень (основное свойство результанта);
- (2) $R(g, f) = (-1)^{mn} R(f, g)$;
- (3)

$$R(f, g) = a_0^m \prod_{i=1}^n g(x_i) = (-1)^{mn} b_0^n \prod_{j=1}^m f(y_j).$$

Доказательство. Свойство 1) сразу следует из определения. Свойство 2) следует из того, что в определении результанта есть mn скобок $x_i - y_j$. При этом в $R(g, f)$ все они входят с противоположным знаком.

В свойстве 3) достаточно доказать только первое равенство. Второе следует из первого с помощью пункта 2). Имеем

$$a_0^m \prod_{i=1}^n g(x_i) = a_0^m \prod_{i=1}^n \left(b_0 \prod_{j=1}^m (x_i - y_j) \right) = a_0^m b_0^n \prod_{1 \leq i \leq n, 1 \leq j \leq m} (x_i - y_j) = R(f, g)$$

\square

Предложение 2.

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0 D(f).$$

Доказательство. $f(x) = a_0(x - x_1) \dots (x - x_n)$. Тогда

$$f'(x) = a_0 \sum_{i=1}^n \frac{\prod_{j \neq i} (x - x_j)}{x - x_i}.$$

Имеем

$$f'(x_i) = a_0 \prod_{j \neq i} (x_i - x_j).$$

$$\begin{aligned}
R(f, f') &= a_0^{n-1} \prod_{i=1}^n f'(x_i) = a_0^{2n-1} \prod_{i=1}^n \prod_{j \neq i} (x_i - x_j) = \\
&= a_0^{2n-1} \prod_{i < j} (x_i - x_j) \prod_{i > j} (x_i - x_j) = a_0^{2n-1} \prod_{i < j} (x_i - x_j) (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (x_i - x_j) = \\
&= (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{i < j} (x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0 D(f).
\end{aligned}$$

□

Предложение 3.

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_n & 0 & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & a_2 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & \dots & a_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & a_0 & a_1 & a_2 & \dots & a_n \\ b_0 & b_1 & b_2 & \dots & b_m & 0 & 0 & 0 & \dots & 0 \\ 0 & b_0 & b_1 & b_2 & \dots & b_m & 0 & 0 & \dots & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & \dots & b_m & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & b_0 & b_1 & b_2 & \dots & b_m \end{vmatrix}$$

(Это определитель матрицы $(m+n) \times (m+n)$.)

Данное предложение в обязательную часть программы экзамена вошло без доказательства. Доказательство будет написано в следующей лекции (она пройдёт онлайн 19 декабря в 19:00) и оно будет входить в программу досрочного экзамена.