# Тема I: Многочлены

# §3. Многочлены над областью с однозначным разложением

М.В.Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

# Постановка задачи

В первой лекции доказано, что кольцо многочленов над любым полем – область с однозначным разложением.

Доказательство опиралось на деление с остатком. В точности по той же схеме доказывается, что кольцо целых чисел $\mathbb{Z}$ – ООР: ведь в $\mathbb{Z}$ тоже есть деление с остатком, алгоритм Евклида и все его следствия.

Однако есть важные для приложений области целостности, для которых использованный нами подход не работает: кольцо $\mathbb{Z}[x]$ многочленов с целыми коэффициентами, кольцо $F[x,y]$ многочленов от двух переменных над полем $F$ и т.п.

Дело в том, что ключевое свойство взаимно простых многочленов над полем (*если $f$ и $g$ взаимно просты, то $uf+vg=1$ для некоторых многочленов $u$ и $v$*) для многочленов из $\mathbb{Z}[x]$ или $F[x,y]$ просто неверно.

Например, число 2 и одночлен $x$ взаимно просты в $\mathbb{Z}[x]$, но в $\mathbb{Z}[x]$ нет таких многочленов $u$ и $v$, что $2u+xv=1$, поскольку для любых $u,v\in\mathbb{Z}[x]$ свободный член многочлена $2u+xv$ – четное число.

Аналогично одночлены $x$ и $y$ взаимно просты в $F[x,y]$, но в $F[x,y]$ нет таких многочленов $u$ и $v$, что $xu+yv=1$ (*объясните, почему*).

Несмотря на описанную трудность, мы покажем, что $\mathbb{Z}[x]$, $F[x,y]$ и многие другие области являются ООР. Это следует из *теоремы переноса*:

**Теорема переноса**

*Если $D$ – область с однозначным разложением, то и кольцо многочленов $D[x]$ – область с однозначным разложением.*

Действительно, раз $\mathbb{Z}$ – ООР, то по теореме и кольцо $\mathbb{Z}[x]$ будет ООР.

Раз $F[x]$ – ООР, то по теореме и $F[x,y] = F[x][y]$ будет ООР.
Трюк в том, что кольцо многочленов от двух переменных $x$ и $y$ над полем $F$ можно мыслить как кольцо многочленов от $y$ над ООР $F[x]$:

$$2x^2 + 4xy + 7y^2 + 3x + 2y - 8 = 7y^2 + (4x+2)y + (2x^2 + 3x - 8).$$

Доказательство теоремы переноса использует «принцип чайника» и опирается на конструкцию поля частных области целостности из предыдущей лекции.

Изучим, как связаны неразложимые элементы кольца $D[x]$ и неприводимые многочлены кольца $F[x]$, где $F$ – поле частных области $D$.

# НОД в области с однозначным разложением

Пусть $D$ – ООР. Любой ненулевой элемент $a \in D$ ассоциирован с произведением вида

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \qquad (*)$$

где $p_1, p_2, \ldots, p_s$ – попарно различные неразложимые элементы, $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N} \cup \{0\}$. Если $d|a$, то из однозначности разложения в произведение неразложимых множителей следует, что

$$d \sim p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s},$$

где $0 \leq \delta_i \leq \alpha_i$ для всех $i = 1, 2, \ldots, s$. (Ведь других неразложимых множителей, кроме тех, что входят в (*), у $d$ быть не может!)
Из этого наблюдения немедленно вытекает, что для любых ненулевых $a, b \in D$ существует НОД$(a, b)$. А именно, если $a$ ассоциирован с произведением (*), а $b$ – с произведением $p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, то

$$\text{НОД}(a, b) \sim p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s},$$

где $\gamma_i = \min\{\alpha_i, \beta_i\}$ для всех $i = 1, 2, \ldots, s$.
Аналогично вычисляется НОД любого конечного подмножества в $D$.

*Содержанием* ненулевого многочлена $f \in D[x]$ называется НОД его коэффициентов. Обозначение: $c(f)$.

Многочлен $f \in D[x]$ называется *примитивным*, если $c(f) = 1$.

**Лемма Гаусса**

*Пусть $D$ – область с однозначным разложением. Для любых ненулевых многочленов $f, g \in D[x]$ содержание их произведения равно произведению их содержаний, т.е.*

$$c(fg) = c(f)c(g).$$

*Доказательство.* Если поделить каждый коэффициент многочлена на содержание этого многочлена, получится примитивный многочлен. Поэтому $f = c(f)f_0$, $g = c(g)g_0$, где $f_0$ и $g_0$ примитивны. Перемножив, получим $fg = c(f)c(g)f_0g_0$, откуда $c(fg) = c(f)c(g)c(f_0g_0)$. Поэтому достаточно доказать, что $c(f_0g_0) = 1$, т.е. что произведение двух примитивных многочленов – примитивный многочлен. Докажем это.

# Лемма Гаусса (2)

Пусть $f_0 = a_0 + a_1 x + \cdots + a_n x^n$, $g_0 = b_0 + b_1 x + \cdots + b_k x^k$.
Если допустить, что многочлен $f_0 g_0$ не является примитивным, то есть неразложимый элемент $p \in D$, который делит все коэффициенты $f_0 g_0$.
Поскольку $f_0$ и $g_0$ примитивны, $p$ не делит какие-то коэффициенты в каждом из этих многочленов. Рассмотрим наименьшие $i, j$ для которых $p \nmid a_i$ и $p \nmid b_j$. Коэффициент при $x^{i+j}$ в произведении $f_0 g_0$ имеет вид

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0.$$

В соответствии с выбором $i, j$ элемент $p$ делит все слагаемые за исключением $a_i b_j$, которое $p$ не делит в силу того, что $D$ – ООР.
Стало быть, $p$ не делит один из коэффициентов многочлена $f_0 g_0$, противоречие. $\square$

**Следствие 1**

*Пусть $f, g \in D[x]$ и $g$ примитивен. Если $g|af$ для $a \in D \setminus \{0\}$, то $g|f$.*

*Доказательство.* Имеем $af = gh$ для некоторого $h \in D[x]$, откуда $c(af) = c(gh)$. Ясно, что $c(af) = ac(f)$, а по лемме Гаусса $c(gh) = c(h)$. Итак, $ac(f) = c(h)$. Пусть $h = c(h)h_0$, где $h_0$ примитивен. Тогда $af = gh = c(h)h_0g = ac(f)h_0g$. Сократив, имеем $f = c(f)h_0g$, т.е. $g|f$. □

Пусть $F$ – поле частных области $D$.

**Следствие 2**

*Если примитивные многочлены $f, g \in D[x]$ ассоциированы в $F[x]$, то они ассоциированы и в $D[x]$.*

*Доказательство.* Если $f, g \in D[x]$ ассоциированы в $F[x]$, то $f = \frac{a}{b}g$ для некоторых $a, b \in D \setminus \{0\}$. Отсюда $bf = ag$. По следствию 1 из примитивности $g$ следует, что $g|f$, а из примитивности $f$ – что $f|g$. □

**Следствие 3**

*Если многочлен $f \in D[x]$ неприводим над $D$, то он неприводим и над $F$.*

*Доказательство.* От противного. Пусть $f$ приводим над $F$, т.е. $f = gh$ для некоторых многочленов ненулевой степени $g, h \in F[x]$. Коэффициенты многочленов $g$ и $h$ суть некоторые дроби. Умножив равенство $f = gh$ на произведение $a$ знаменателей этих дробей, получим $af = g_1 h_1$, где $g_1$ и $h_1$ – многочлены из $D[x]$. Представим эти многочлены как $g_1 = c(g_1)g_0$, $h_1 = c(h_1)h_0$, где многочлены $g_0$ и $h_0$ примитивны. Тогда

$$af = c(g_1)c(h_1)g_0 h_0,$$

откуда $g_0 | af$ и $h_0 | af$. По следствию 1 примитивность $g_0$ и $h_0$ влечет $g_0 | f$ и $h_0 | f$, что противоречит неприводимости многочлена $f$ над $D$. □

Мы готовы к доказательству теоремы переноса. Напомним ее:

**Теорема переноса**

*Если $D$ – область с однозначным разложением, то и кольцо многочленов $D[x]$ – область с однозначным разложением.*

*Существование*. Пусть $f$ – ненулевой и необратимый многочлен из $D[x]$. Представим его как $f = c(f)f_0$, где $f_0$ примитивен. Элемент $c(f) \in D$ можно разложить в произведение неразложимых элементов области $D$, а примитивный многочлен $f_0$ можно разложить в произведение примитивных неприводимых многочленов индукцией по степени.

*Единственность*. Пусть $f = p_1 \cdots p_k f_1 \cdots f_s$ и $f = q_1 \cdots q_\ell g_1 \cdots g_t$ – два таких разложения многочлена $f$, что $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ – неразложимые элементы области $D$, а $f_1, \ldots, f_s, g_1, \ldots, g_t$ – примитивные неприводимые многочлены из $D[x]$. По лемме Гаусса $c(f) = p_1 \cdots p_k = q_1 \cdots q_\ell$. Поскольку $D$ – ООР, отсюда следует, что $k = \ell$ и что после подходящей перенумерации $p_i \sim q_i$ для каждого $i = 1, \ldots, k$.

Далее, $f_1 \cdots f_s = g_1 \cdots g_t$. По следствию 3 многочлены $f_1, \ldots, f_s, g_1, \ldots, g_t$ неприводимы над $F$, но кольцо многочленов над полем – ООР (теорема предыдущей лекции). Отсюда следует, что $s = t$ и что после подходящей перенумерации многочлены $f_j$ и $g_j$ ассоциированы в кольце $F[x]$ для каждого $j = 1, \ldots, s$. По следствию 2 $f_j$ и $g_j$ ассоциированы и в $D[x]$. □

**Следствие**

*Для любого $n \in \mathbb{N}$ и любого поля $F$ кольца $\mathbb{Z}[x_1, \ldots, x_n]$ и $F[x_1, \ldots, x_n]$ – области с однозначным разложением.*