

# Глава IV. Многочлены

## § 1. Построение кольца многочленов над полем

А. Я. Овсянников

Уральский федеральный университет  
Институт естественных наук и математики  
Департамент математики, механики и компьютерных наук  
Основы алгебры для направлений  
Механика и математическое моделирование и  
Прикладная математика  
(1 семестр)

Пусть  $F$  – поле. Рассмотрим множество  $F[x]$  всех последовательностей с элементами из  $F$  вида  $(\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$  таких что для некоторого  $m \in \mathbb{N}$  справедливы равенства  $\alpha_k = 0$  при всех  $k \geq m$ . Две последовательности называются **равными**, если на соответствующих местах в них стоят одинаковые элементы. Определим сумму двух последовательностей из  $F[x]$  поэлементно:

$$\begin{aligned}(\alpha_0, \alpha_1, \dots, \alpha_n, \dots) + (\beta_0, \beta_1, \dots, \beta_n, \dots) = \\ (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots, \alpha_n + \beta_n, \dots).\end{aligned}$$

Произведение двух последовательностей определяется так:

$$(\alpha_0, \alpha_1, \dots, \alpha_n, \dots) \cdot (\beta_0, \beta_1, \dots, \beta_n, \dots) = (\gamma_0, \gamma_1, \dots, \gamma_n, \dots), \quad (1)$$

$$\text{где } \gamma_n = \sum_{k+\ell=n} \alpha_k \beta_\ell = \alpha_0 \beta_n + \alpha_1 \beta_{n-1} + \dots + \alpha_{n-1} \beta_1 + \alpha_n \beta_0.$$

Очевидно, что сумма любых двух последовательностей из  $F[x]$  принадлежит  $F[x]$ .

Проверим, что и произведение двух последовательностей  $(\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$  и  $(\beta_0, \beta_1, \dots, \beta_n, \dots)$  из  $F[x]$  также принадлежит  $F[x]$ . Пусть  $\alpha_k = 0$  при всех  $k > m$  и  $\beta_k = 0$  при всех  $k > l$ . Тогда  $\gamma_k = \sum_{s+t=k} \alpha_s \beta_t = 0$  при  $k > m + l$ , так как  $s + t > m + l \implies s > m$  или  $t > l$ . Если при этом  $\alpha_m, \beta_l \neq 0$ , то  $\gamma_{m+l} = \sum_{s+t=m+l} \alpha_s \beta_t = \alpha_m \beta_l \neq 0$ , так как из  $s + t = m + l$  при  $s < m$  следует  $t > l$ , а при  $t < l$  следует  $s > m$ .

Элементы из  $F[x]$  будем называть **многочленами** над полем  $F$  и обозначать малыми латинскими буквами. Последовательность из нулей обозначим через  $o$  и назовем **нулевым** многочленом.

Пусть  $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ . Для удобства положим  $f[n] = \alpha_n$  для всех  $n = 0, 1, \dots$ . Если  $f \neq o$ , то существует  $m \in \mathbb{N}$  такое что  $f[m] \neq 0$ ,  $f[k] = 0$  для любого  $k > m$ . В таком случае говорят, что многочлен  $f$  имеет **степень**  $m$ , обозначаемую через  $\deg(f)$ . Для нулевого многочлена  $o$  полагаем  $\deg(o) = -\infty$ . Символ  $-\infty$  по определению считается меньше любого целого числа, и для любого целого  $m$  по определению принимается, что  $m + (-\infty) = -\infty + m = -\infty$ .

Из доказанного в начале этого слайда легко вывести, что  $\deg(f \cdot g) = \deg(f) + \deg(g)$ . Нетрудно убедиться, что  $\deg(f + g) = \max\{\deg(f), \deg(g)\}$  при  $\deg(f) \neq \deg(g)$  и  $\deg(f + g) \leq \deg(f), \deg(g)$  при  $\deg(f) = \deg(g)$ .

Проверим следующие свойства операций сложения многочленов:

$$\forall f, g, h \in F[x] \quad f + g = g + f; \quad f + (g + h) = (f + g) + h; \quad f + o = f;$$

$$\forall u \in F[x] \quad \exists v \in F[x]: u + v = o.$$

Покажем, что  $f + g = g + f$ . Для любого  $n \geq 0$  справедливы равенства  $(f + g)[n] = f[n] + g[n] = g[n] + f[n] = (g + f)[n]$ , откуда следует  $f + g = g + f$ .

Аналогично проверяется, что  $f + (g + h) = (f + g) + h$  и  $f + o = f$ .

Для любого  $u \in F[x]$  рассмотрим  $v \in F[x]$ , определенный условиями  $v[n] = -u[n]$  для всех  $n \geq 0$ . Тогда  $(u + v)[n] = 0$  при всех  $n \geq 0$ , т.е.  $u + v = o$  и  $v = -u$ .

Таким образом, относительно сложения многочленов  $F[x]$  является абелевой группой.

Покажем, что отображение  $\varphi : F \rightarrow F[x]$ , определенное условием  $\varphi(\gamma_0) = (\gamma_0, 0, 0, \dots)$ , является изоморфизмом поля  $F$  на подполе кольца  $F[x]$ . Ясно, что  $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$ . Равенство  $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$  следует из того, что  $\varphi(\alpha)\varphi(\beta)[0] = \alpha\beta$  и  $\varphi(\alpha)\varphi(\beta)[n] = 0$  при всех  $n > 0$ . Так как  $\varphi(0) = o$ ,  $\varphi(-\alpha) = -\varphi(\alpha)$  для любого  $\alpha \in F$  и  $\varphi(1)$  – единица кольца  $F[x]$ , множество всех скаляров  $\{\varphi(\gamma) | \gamma \in F\}$  является подполем кольца  $F[x]$  и  $\varphi$  является изоморфизмом поля  $F$  на это подполе.

Свойства умножения не столь очевидны. Докажем, что

$$\forall f, g, h \in F[x] \quad f \cdot g = g \cdot f; \quad f \cdot (g \cdot h) = (f \cdot g) \cdot h;$$

$f \cdot (g + h) = f \cdot g + f \cdot h$ . Первое равенство вытекает непосредственно из определения произведения (1) сл.2.

Докажем второе. Пусть  $f, g, h \in F[x]$ . Тогда  $(f \cdot g)[m] = \sum_{k+s=m} f[k]g[s]$  и

$$(g \cdot h)[r] = \sum_{s+t=r} g[s]h[t]. \text{ Далее, } ((f \cdot g) \cdot h)[d] = \sum_{m+t=d} (f \cdot g)[m]h[t] =$$

$$\sum_{m+t=d} \left( \sum_{k+s=m} f[k]g[s] \right) h[t] = \sum_{k+s+t=d} f[k]g[s]h[t]. \text{ Аналогично}$$

$$\text{имеем } (f \cdot (g \cdot h))[d] = \sum_{k+r=d} f[k](g \cdot h)[r] =$$

$$\sum_{k+r=d} f[k] \left( \sum_{s+t=r} g[s]h[t] \right) = \sum_{k+s+t=d} f[k]g[s]h[t], \text{ откуда следует}$$

требуемое равенство  $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ .

Докажем равенство  $f \cdot (g + h) = f \cdot g + f \cdot h$ :

$$(f \cdot (g + h))[m] = \sum_{k+s=m} f[k](g[s] + h[s]) = \sum_{k+s=m} (f[k]g[s] + f[k]h[s]) =$$

$$\sum_{k+s=m} f[k]g[s] + \sum_{k+s=m} f[k]h[s] = (f \cdot g)[m] + (f \cdot h)[m] = (f \cdot g + f \cdot h)[m].$$

Таким образом,  $F[x]$  является ассоциативным коммутативным кольцом с единицей (напомним, что  $\varphi(1)$  является единицей относительно умножения многочленов). Из условия  $\deg(f \cdot g) = \deg(f) + \deg(g)$  следует, что кольцо  $F[x]$  не имеет делителей нуля, т.е. оно является областью целостности.

Множество всех обратимых элементов кольца  $F[x]$  есть

$$\{\varphi(\gamma) \mid \gamma \in F \setminus \{0\}\}.$$

Условимся отождествлять последовательности  $\varphi(\alpha)$  с их первыми элементами и называть *скалярами*. Например, нулевая последовательность  $\varphi(0) = o$  отождествляется со скаляром 0.

Таким образом,  $F \subset F[x]$ . Нетрудно проверить, что  $\alpha \cdot (\beta_0, \beta_1, \dots) = (\alpha\beta_0, \alpha\beta_1, \dots)$  для любого скаляра  $\alpha$ .

Последовательность  $(0, 1, 0, 0, \dots)$  обозначим через  $x$ . Легко проверить, что  $x^2 = x \cdot x = (0, 0, 1, 0, 0, \dots)$ ,  $x^3 = x^2 \cdot x = (0, 0, 0, 1, 0, \dots)$ , и  $x^m$  имеет 1 на  $(m + 1)$ -й позиции, а все остальные элементы этой последовательности равны нулю.

Ясно, что выражение вида

$$f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0, \quad (2)$$

где  $\alpha_0, \alpha_1, \dots, \alpha_n \in F$ ,  $n$  – натуральное число, представляет собой последовательность  $f = (\alpha_0, \alpha_1, \dots, \alpha_n, 0, \dots)$ , в которой все члены после  $\alpha_n$  равны 0. В дальнейшем мы будем придерживаться этой привычной записи многочленов. Скаляры  $\alpha_0, \dots, \alpha_n$  называются *коэффициентами* многочлена  $f$ . Если  $\alpha_n \neq 0$ , то  $n = \deg(f)$  и  $\alpha_n x^n$  называется *старшим членом*, а скаляр  $\alpha_n$  – *старшим коэффициентом* многочлена  $f$ . Скаляр  $\alpha_0$  называется *свободным членом* многочлена  $f$ .

## Теорема

Пусть  $f, g \in F[x]$ ,  $g \neq 0$ . Тогда существуют такие однозначно определенные многочлены  $q, r \in F[x]$ , что

$$f = q \cdot g + r \text{ и } \deg(r) < \deg(g). \quad (3)$$

↓ Если  $\deg(g) = 0$ , то  $g \in F$  и  $g \neq 0$ , т.е.  $f = (\frac{1}{g}f)g$  и  $q = \frac{1}{g}f$ ,  $r = 0$ .

Предположим, что  $\deg(g) > 0$ . Для доказательства существования применим индукцию по  $\deg(f)$ . При  $\deg(f) < \deg(g)$  положим  $q = 0$ ,  $r = f$ . Пусть для всех многочленов  $h$  степени меньше  $m$ , где  $m \geq \deg(g)$ , существуют такие многочлены  $q$  и  $r$ , что  $h = qg + r$  и  $\deg(r) < \deg(g)$ .

Рассмотрим произвольный многочлен  $f$  степени  $m$ . Имеем  $f = \alpha x^m + f_1$  и  $g = \beta x^k + g_1$ , где  $\deg(f_1) < m$ ,  $\deg(g_1) < k$  и  $\alpha \neq 0$ ,  $\beta \neq 0$ . Положим  $h_1 = \frac{\alpha}{\beta} x^{m-k}$ . Тогда  $h_1 g = \alpha x^m + h_1 g_1$ , откуда  $\deg(f - h_1 g) < m$ .

Применяя к многочлену  $f - h_1 g$  предположение индукции, констатируем существование многочленов  $q_1$  и  $r$  таких что  $f - h_1 g = q_1 g + r$  и  $\deg(r) < \deg(g)$ . Теперь ясно, что  $f = (h_1 + q_1)g + r$ , что и требуется доказать.

Докажем единственность. Предположим, что  $f = q_1g + r_1$  и  $f = q_2g + r_2$  для некоторых многочленов  $q_1, q_2, r_1, r_2$  таких что  $\deg(r_1), \deg(r_2) < \deg(g)$ . Из равенства  $q_1g + r_1 = q_2g + r_2$  получаем  $(q_1 - q_2)g = r_2 - r_1$ . Если  $q_1 - q_2 \neq 0$ , то  $\deg((q_1 - q_2)g) \geq \deg(g)$ , а  $\deg(r_2 - r_1) < \deg(g)$  — получили противоречие. Следовательно,  $q_1 - q_2 = 0$ , откуда  $q_1 = q_2$  и  $r_1 = r_2$ . Теорема доказана.  $\uparrow$

В равенстве (3) сл.б многочлен  $q$  называется *частным*, а многочлен  $r$  — *остатком* от деления (с остатком)  $f$  на  $g$ . Если  $r = 0$ , то говорят, что многочлен  $f$  *делится* на многочлен  $g$ ; в этом случае  $f = qg$ . При этом говорят также, что многочлен  $g$  *делит* многочлен  $f$ ; этот факт будем обозначать через  $g|f$ .

Доказательство теоремы сл.б служит основой для *алгоритма деления столбиком многочлена на многочлен*. Этот алгоритм состоит в следующем. Пусть  $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$ ,  $g = \beta_m x^m + \beta_{m-1} x^{m-1} + \dots + \beta_1 x + \beta_0$ , и пусть  $\alpha_n, \beta_m \neq 0$  и  $n \geq m > 0$ . Положим  $q = 0$ . Шаг алгоритма делается так. Многочлен  $f$  заменяется на многочлен  $f_1 = f - \frac{\alpha_n}{\beta_m} x^{n-m} g$ , а многочлен  $q$  – на многочлен  $q + \frac{\alpha_n}{\beta_m} x^{n-m}$ . Шаги повторяются до тех пор, пока  $\deg(f_1) \geq m$ . Так как степень  $f_1$  на каждом шаге уменьшается по крайней мере на 1, алгоритм закончит работу. При этом частное будет равно  $q$ , а остаток – последнему значению  $f_1$ .



Следующее утверждение проверяется непосредственно.

## Предложение

Пусть  $f, g, g_1, g_2, h \in F[x]$ . Тогда если  $f|g$ , то  $f|(gh)$  и если  $f|g_1, f|g_2$ , то  $f|(g_1 + g_2)$  и  $f|(g_1 - g_2)$ .

Многочлены  $f$  и  $g$  называются *ассоциированными*, если существует ненулевой элемент  $\gamma \in F$  такой, что  $f = \gamma g$ . Легко проверить, что многочлены  $f$  и  $g$  ассоциированы тогда и только тогда, когда  $f|g$  и  $g|f$ . Покажем, что отношение ассоциированности является отношением эквивалентности на множестве  $F[x]$ . Очевидно, что оно рефлексивно ( $\gamma = 1$ ) и симметрично ( $\gamma \neq 0$ , из  $f = \gamma g$  следует  $g = \gamma^{-1}f$ ). Оно транзитивно, так как из  $f = \gamma g$  и  $g = \beta h$  следует  $f = \gamma\beta h$  и  $\gamma\beta \neq 0$ , поскольку поле  $F$  не содержит делителей нуля. Каждый класс эквивалентности по этому отношению, содержащий ненулевой многочлен, содержит единственный многочлен со старшим коэффициентом 1. Поэтому справедливо

## Наблюдение

Для любого ненулевого многочлена существует единственный ассоциированный с ним многочлен со старшим коэффициентом 1.

При построении кольца многочленов вместо поля  $F$  можно было взять любое кольцо  $K$ . Кольцо многочленов  $K[x]$  наследует следующие свойства кольца  $K$ : коммутативность, ассоциативность, наличие единицы, отсутствие делителей нуля.

В частности, можно построить кольцо многочленов от нескольких переменных  $x_1, x_2, \dots, x_n$  над полем  $F$ , рассматривая последовательно  $F[x_1]$ ,  $(F[x_1])[x_2] = F[x_1, x_2]$ ,  $(F[x_1, x_2])[x_3] = F[x_1, x_2, x_3]$ ,  $\dots$ ,  $(F[x_1, \dots, x_{n-1}])[x_n] = F[x_1, \dots, x_n]$ . Это кольцо будет областью целостности.

Можно построить и кольцо многочленов над кольцом матриц  $F^{n \times n}[x]$  над полем  $F$ . Это ассоциативное кольцо с единицей.

С указанными кольцами мы будем иметь дело в конце этой главы.