Глава 5

Кольцо многочленов

§ 5.1. Кольцо многочленов от одной переменной

Эта глава посвящена многочленам. Под многочленом (от одной переменной) с действительными коэффициентами обычно понимается функция $f : \mathbb{R} \to \mathbb{R}$ вида $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, где $a_i \in \mathbb{R}$. Однако если рассматривать многочлены над произвольным полем (или даже кольцом), то в случае конечного поля (кольца) определение многочлена как отображения не слишком удачно. Действительно, многочлены x и x^2 над полем $F = \mathbb{Z}_2$ порядка 2, очевидно, совпадают как отображения, так как $0^2 = 0$ и $1^2 = 1$. Поскольку удобнее считать их различными, мы дадим более абстрактное определение многочлена, а потом покажем, что в случае бесконечного поля данное нами определение не отличается от определения многочлена как функции. Для краткости обозначим через $\mathbb{N}_0$ множество $\mathbb{N} \cup \{0\}$ целых неотрицательных чисел.

Определение 5.1.1. Пусть $k \in \mathbb{N}_0$. *Многочленом* (или *полиномом*) f от переменной x над кольцом R называется выражение

$$f(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 x^0 + a_1 x^1 + \ldots + a_k x^k + \ldots,$$

где коэффициенты a_k лежат в кольце R и лишь конечное их число отлично от 0. Ненулевой коэффициент многочлена f с наибольшим индексом называется *старшим коэффициентом* многочлена, а сам этот индекс называется *степенью* многочлена f и обозначается через $\deg f$. Коэффициент многочлена с индексом нуль называется *свободным* коэффициентом. Множество всех многочленов от переменной x над кольцом R обозначается через $R[x]$.

Замечание. Если договориться, что одночлены, т. е. выражения вида $a_k x^k$, с нулевыми коэффициентами при записи многочлена могут быть опущены, то многочлен степени n можно записать в виде $f(x) = a_0 x^0 + a_1 x^1 + \ldots + a_n x^n$. Кроме того, многочлены нулевой степени естественным образом отождествляются с элементами кольца R $(a_0 x^0 = a_0)$. Используя это отождествление, мы приходим к привычной форме записи многочлена $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Отметим также, что нулевой многочлен $0 = \sum_{k=0}^{\infty} 0x^k$ не является многочленом степени 0. Его степень считается неопределённой. Иногда для удобства (об этом ниже) полагают, что $\deg 0 = -\infty$.

Определение 5.1.2. Многочлены $f(x) = \sum_{k=0}^{\infty} a_kx^k$ и $g(x) = \sum_{k=0}^{\infty} b_kx^k$ *равны*, если для любого $k \in \mathbb{N}_0$ имеет место равенство $a_k = b_k$.

Замечание. В силу данного определения многочлены x и x^2 над полем $\mathbb{Z}_2$ должны рассматриваться как различные.

Определение 5.1.3. Пусть R — кольцо и многочлены

$$f(x) = \sum_{k=0}^{\infty} a_kx^k,\ g(x) = \sum_{k=0}^{\infty} b_kx^k \in R[x].$$

Многочлены

$$h(x) = \sum_{k=0}^{\infty} c_kx^k \text{ и } p(x) = \sum_{k=0}^{\infty} d_kx^k \in R[x]$$

называются соответственно *суммой* и *произведением* многочленов f и g, если для любого $k \in \mathbb{N}_0$ выполняется $c_k = a_k + b_k$ и $d_k = \sum_{i+j=k} a_ib_j$. Обозначения: $h = f + g$ и $p = fg$.

Замечание. Данное определение корректно, поскольку $h = f + g$ и $p = fg$ имеют лишь конечное число отличных от нуля коэффициентов, а значит, являются многочленами.

Теорема 5.1.1. *Пусть R — кольцо. Тогда имеют место следующие утверждения.*

1. *$R[x]$ — кольцо относительно операций сложения и умножения многочленов.*

2. *Если R — коммутативное кольцо, то $R[x]$ — коммутативное кольцо.*

3. *Если R — кольцо с единицей, то $R[x]$ — кольцо с единицей.*

Доказательство. Доказательство теоремы представляет собой последовательную проверку аксиом кольца, а также свойств коммутативности и существования единицы. Например, если $f(x) = \sum_{k=0}^{\infty} a_kx^k$, $g(x) = \sum_{k=0}^{\infty} b_kx^k$, $h(x) = \sum_{k=0}^{\infty} c_kx^k$, то закон правой дистрибутивности $fh + gh = (f + g)h$ следует из равенств

$$\sum_{i+j=k} a_ic_j + \sum_{i+j=k} b_ic_j = \sum_{i+j=k} (a_i + b_i)c_j \text{ для } k \in \mathbb{N}_0,$$

которые, в свою очередь, легко выводятся из соответствующих аксиом кольца R. $\square$

Замечание. Отождествление элементов кольца R с многочленами нулевой степени в $R[x]$ (и нуля с нулевым многочленом) позволяет считать, что R — подкольцо кольца $R[x]$.

Упражнение 5.1.1. *Докажите теорему* 5.1.1 *полностью.*

Предложение 5.1.1. *Пусть R — кольцо и $f, g \in R[x]$, $f, g \neq 0$. Тогда имеют место следующие утверждения.*

1. $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$.

2. $\deg fg \leqslant \deg f + \deg g$, *причём если R — кольцо без делителей нуля, то* $\deg fg = \deg f + \deg g$ *и $R[x]$ — кольцо без делителей нуля.*

Замечание. Отметим, что если один из многочленов в формулировке предложения нулевой, то утверждение п. 2 предложения остаётся в силе, если считать, что $\deg 0 = -\infty$.

Следствие. *Если R — поле, то множество $R[x]^*$ всех обратимых элементов кольца $R[x]$ — это множество всех многочленов нулевой степени.*

Упражнение 5.1.2. *Докажите предложение* 5.1.1 *и следствие из него. Приведите пример кольца R, для многочленов над которым формула* $\deg fg = \deg f + \deg g$ *неверна.*

В дальнейшем мы будем рассматривать многочлены над некоторым полем F. Как уже отмечалось, множество многочленов $F[x]$ относительно операций сложения и умножения на скаляр образует векторное пространство. Следовательно, $F[x]$ — алгебра над полем F. Отметим, что эта алгебра всегда бесконечномерна.

§ 5.2. Делимость в кольце многочленов

В силу следствия из предложения 5.1.1 многочлен ненулевой степени не имеет обратного по умножению в кольце $F[x]$. Поэтому деление в привычном смысле в кольце многочленов невозможно. Однако, как и в кольце целых чисел, в кольце многочленов можно естественным образом определить деление с остатком.

Теорема 5.2.1 (о делении с остатком)**.** *Пусть F — поле, f, g — многочлены из $F[x]$ и $g \neq 0$. Тогда существуют многочлены $q, r \in F[x]$ такие, что $f = qg + r$ и либо $r = 0$, либо* $\deg r < \deg g$. *Многочлены q и r, удовлетворяющие этим условиям, определены однозначно.*

Доказательство. Начнём с доказательства существования. Если $\deg f < \deg g$, то, полагая $q = 0$, $r = f$, получим требуемое. Таким образом, мы можем считать, что $\deg f = n \geqslant \deg g = m$. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0$ и $b(x) = b_m x^m + \ldots + b_1 x + b_0$. Используем индукцию по n. Поскольку для $n = 0$ утверждение очевидно (речь идет о делении в поле F), база индукции установлена. Следовательно, мы можем полагать, что $n > 0$ и для всех многочленов степени, меньшей n, утверждение уже доказано. Рассмотрим многочлен $f_1 = f - \frac{a_n}{b_m} x^{n-m} g$. Его степень меньше n, следовательно, существуют такие многочлены q_1 и r, что $f_1 = q_1 g + r$ и либо $r = 0$, либо $\deg r < \deg g$. Тогда $f = \frac{a_n}{b_m} x^{n-m} g + f_1 = (\frac{a_n}{b_m} x^{n-m} + q_1) g + r$, и многочлены $q = \frac{a_n}{b_m} x^{n-m} + q_1$ и r — искомые.

Пусть $f = qg + r = q'g + r'$. Тогда $r - r' = (q' - q)g$. Если $q' - q$ — ненулевой многочлен, то в силу п. 2 предложения 5.1.1 степень многочлена, стоящего в правой части равенства, больше или равна $\deg g$. С другой стороны, степень многочлена, стоящего в левой части, в силу п. 1 того же предложения и условия на степени многочленов r, r' меньше $\deg g$. Полученное противоречие показывает, что $q' = q$, а значит, и $r = r'$. $\square$

Определение 5.2.1. Многочлены q и r, определённые в теореме, называются соответственно (*неполным*) *частным* и *остатком* при делении f на g.

Определение 5.2.2. Многочлен $g \neq 0$ *делит* многочлен f, если найдётся многочлен q такой, что $f = qg$. В этом случае g называется *делителем* многочлена f, а f — *кратным* многочлена g. Запись $g \mid f$ означает, что g *делит* f, а запись $f \,\vdots\, g$ означает, что f *делится на* g.

Замечание. Тот факт, что g не делит f, будем кратко обозначать так: $g \nmid f$.

Предложение 5.2.1 (свойства делимости многочленов)**.** *В кольце $F[x]$ выполняются следующие утверждения.*

1. *Если $g \mid f$ и $g \mid h$, то $g \mid (f + h)$.*
2. *Если $g \mid f$, то для каждого $h \in F[x]$ выполняется $g \mid (fh)$.*
3. *Если $\deg g = 0$, то для каждого $h \in F[x]$ выполняется $g \mid h$.*
4. *Если $\deg h = 0$ и $g \mid f$, то $(hg) \mid f$.*

Упражнение 5.2.1. *Доказать предложение* 5.2.1, *используя определение делимости.*

Определение 5.2.3. Пусть $f, g \in F[x]$. *Наибольшим общим дели-*

телем многочленов f и g называется многочлен $d \in F[x]$, удовлетворяющий следующим условиям:

1) $d \mid f$ и $d \mid g$;

2) если $d' \in F[x]$ таков, что $d' \mid f$ и $d' \mid g$, то $d' \mid d$.

Обозначение: $d = (f, g)$.

Замечание. Из свойств 2 и 4 делимости многочленов следует, что если d — наибольший общий делитель многочленов f и g, то многочлен w также является наибольшим общим делителем многочленов f и g тогда и только тогда, когда $w = ud$, где u — многочлен нулевой степени. Иными словами, наибольший общий делитель определяется с точностью до скаляра из поля F. Поэтому запись вида $(f, g) = (u, v)$ ниже означает, что наибольшие делители соответствующих многочленов равны с точностью до ненулевого скаляра.

Теорема 5.2.2 (алгоритм Евклида)**.** *Пусть $f, g \in F[x]$ и $g \neq 0$. Тогда существует наибольший общий делитель этих многочленов $d = (f, g)$ и он может быть представлен в виде $d = fu + gv$, где $u, v \in F[x]$. Более того, если степени f и g больше 0, то многочлены u и v можно выбрать так, что $\deg u < \deg g$ и $\deg v < \deg f$.*

Доказательство. Доказательство теоремы основано на следующем несложном утверждении.

Лемма. *Пусть r — остаток от деления f на g. Тогда множество общих делителей многочленов f и g совпадает с множеством общих делителей многочленов g и r. В частности, $(f, g) = (g, r)$.*

Доказательство. Если $h \mid g$ и $h \mid r$, то в силу свойств 1 и 2 делимости многочленов h делит $f = qg + r$. Обратно, если $h \mid f$ и $h \mid g$, то $h \mid r$, так как $r = f - qg$. Таким образом, множества общих делителей совпадают, а значит, совпадают и наибольшие по делимости элементы этих множеств. $\square$

Вернёмся к доказательству теоремы. Если f делится на g, то $d = g = f \cdot 0 + g \cdot 1$ и теорема доказана. В противном случае разделим с остатком f на g, затем g на полученный остаток, затем первый остаток на второй и т. д. Поскольку степени остатков убывают, на некотором шаге произойдёт деление без остатка. Получим цепочку равенств:

$$f = q_1 g + r_1,$$

$$\begin{aligned} &g = q_2 r_1 + r_2,\\ &\dots\dots\dots\dots\dots\\ &r_{n-2} = q_n r_{n-1} + r_n,\\ &r_{n-1} = q_{n+1} r_n, \end{aligned} \tag{1}$$

где $r_i \neq 0$ для каждого $i = 1, \dots, n$.

Имеем $r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \dots = (r_1, r_2) = (g, r_1) = = (f, g)$. Таким образом, наибольшим общим делителем многочленов f и g оказывается многочлен r_n — последний ненулевой остаток в этой цепочке.

Проходя по цепочке сверху вниз, мы последовательно получаем, что

$$\begin{aligned} &r_1 = fu_1 + gv_1,\\ &r_2 = fu_2 + gv_2,\\ &\dots\dots\dots\dots\dots\\ &r_{n-1} = fu_{n-1} + gv_{n-1}\\ &r_n = fu_n + gv_n, \end{aligned} \tag{2}$$

где u_i, v_i $(i = 1, \dots, n)$ — некоторые многочлены из $F[x]$ (например, $u_1 = 1$, $v_1 = -q_1$). Таким образом, $d = r_n$ можно представить в виде суммы $fu + gv$.

Пусть в представлении $d = fu + gv$ степень u больше или равна степени g. Поделим с остатком u на g: $u = qg + r$. Подставляя в исходное равенство, имеем $d = f(qg + r) + gv = fr + gv'$. В получившемся новом представлении $\deg r < \deg g$. Если $\deg f \leqslant \deg v'$, то $\deg fr < \deg gv'$. Кроме того, поскольку в случае, когда g делит f, теорема уже доказана, мы можем полагать, что $\deg d < \deg g \leqslant \deg gv'$. С другой стороны, $gv' = d - fr$, следовательно, $\deg gv' = \deg(d - fr) \leqslant \max\{\deg d, \deg fr\}$; противоречие. Таким образом, $\deg v' < \deg f$. □

Замечание. Практический метод поиска наибольшего общего делителя основан на цепочке равенств (1). Его принято называть *алгоритмом Евклида*. Мы договоримся считать, что старший коэффициент наибольшего общего делителя (f, g) многочленов f и g равен единице. Тогда (f, g) уже единственным образом определяется по f и g.

Определение 5.2.4. Многочлены $f, g \in F[x]$ называются *взаимно простыми*, если $(f, g) = 1$.

Теорема 5.2.3 (критерий взаимной простоты многочленов)**.** *Многочлены $f, g \in F[x]$ взаимно просты тогда и только тогда, когда существуют многочлены $u, v \in F[x]$ такие, что $1 = fu + gv$.*

Доказательство. Если $(f, g) = 1$, то u, v, удовлетворяющие условию, существуют по теореме 5.2.2. Обратно, если существуют многочлены u, v такие, что $1 = fu + gv$, то любой общий делитель d многочленов f, g делит $fu + gv = 1$. Следовательно, d — многочлен нулевой степени. □

Предложение 5.2.2 (свойства взаимно простых многочленов)**.** *Пусть $f, g, h \in F[x]$. Тогда выполняются следующие утверждения.*

1. *Если $(f, g) = (f, h) = 1$, то $(f, gh) = 1$.*
2. *Если $(f, g) = 1$ и $f \mid (gh)$, то $f \mid h$.*
3. *Если $(f, g) = 1$, $f \mid h$ и $g \mid h$, то $(fg) \mid h$.*

Доказательство. Докажем первое утверждение. Поскольку $(f, g) = 1$, существуют $a, b \in F[x]$ такие, что $fa + gb = 1$. Тогда $h = h(fa) + h(gb)$. Кроме того, существуют $c, d \in F[x]$ такие, что $fc + hd = 1$. Подставим в последнее равенство выражение для h. Получим $fc + (hfa + hgb)d = f(c + had) + (gh)cd = 1$. Полагая $u = c + ha$ и $v = cd$, имеем $fu + (gh)v = 1$. Следовательно, по теореме 5.2.3 многочлены f и gh взаимно просты.

Второй и третий пункт предложения доказываются схожим образом с использованием критерия взаимной простоты. □

Упражнение 5.2.2. *Докажите* пп. 2 *и* 3 *предложения* 5.2.2.

Аналогия между кольцом многочленов и кольцом целых чисел, которую мы имеем в виду на протяжении этого параграфа, приводит к понятию *неразложимого* многочлена, соответствующего понятию простого числа.

Определение 5.2.5. Многочлен $f \in F[x]$ степени, большей нуля, называется *неразложимым*, если из равенства $f = uv$, где $u, v \in F[x]$, следует, что либо $\deg u = 0$, либо $\deg v = 0$. В противном случае многочлен f *разложим*.

Замечание. К многочленам нулевой степени понятие разложимости не применяется, так же как в случае кольца целых чисел единица не считается ни простым, ни составным числом. Кроме того, очевидно, что многочлен первой степени всегда неразложим.

Пример. Многочлен $x^2 + 1$ неразложим в $\mathbb{Q}[x]$ и $\mathbb{R}[x]$, но разложим в $\mathbb{C}[x]$: $x^2 + 1 = (x + i)(x - i)$. Многочлен $x^2 - 2$ неразложим в $\mathbb{Q}[x]$, но разложим в $\mathbb{R}[x]$: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. Таким образом, ответ на вопрос о разложимости многочлена зависит от того, над каким полем задан многочлен.