1. Многочлены

1.1. Многочлены от одной переменной

Определение. Многочленом $f(x)$ от переменной x называется выражение

$$a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n, \tag{1}$$

где $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ – произвольные действительные числа, причем $a_n \neq 0$.

Числа $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ — это *коэффициенты многочлена*, a_n — его *старший коэффициент*, натуральное число n — *степень* многочлена. Степень многочлена $f(x)$ будет обозначаться через $\deg f$.

В многочлене степени n все коэффициенты, кроме старшего, могут обращаться в ноль; такой многочлен иногда называют *одночленом*.

Из определения видно, что многочлен имеет конечное число коэффициентов. Однако в дальнейшем удобно использовать следующее соглашение: считать, что при $i > n$ выполнено равенство $a_i = 0$. Иными словами, мы договариваемся, что *коэффициенты многочлена образуют бесконечную последовательность, в которой лишь конечное число элементов отлично от нуля*. Определение многочлена требует, что в последовательности его коэффициентов хотя бы один был отличен от нуля. Мы откажемся от этого ограничения, и введем в рассмотрение *нулевой многочлен*, т. е. многочлен, у которого все коэффициенты равны нулю. Этот многочен будет обозначаться символом 0. Для обозначения степени нулевого многочлена вводится символ $-\infty$. По определению будем считать, что если n — произвольное неотрицательное целое число, то $-\infty < n$ и $-\infty + n = n + -\infty = -\infty$. Никаких других операций с этим символом производить не будем. Из сказанного вытекает, что для многочленов $f(x), g(x)$ неравенство $\deg f < \deg g$ выполнено в двух случаях: 1) если $f(x) = 0$, $g(x) \neq 0$; 2) $f(x), g(x) \neq 0$ и их степени сравниваются соответствующим образом.

Заметим, что степень многочлена может быть равна нулю. Многочлены нулевой степени представляются ненулевыми действительными числами.

Многочлен (1) записан по возрастанию степеней. Часто многочлен будет удобней записывать по убыванию степеней, т. е. в виде

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n,$$

где $a_0 \neq 0$. Следует обратить внимание на то, что по сравнению с (1) здесь нумерация коэффициентов изменена на обратную.

Множество всех многочленов от переменной x с действительными коэффициентами обозначается через $\mathbb{R}[x]$. Договоримся, какие многочлены будут считаться равными.

О п р е д е л е н и е. Многочлены $f(x)$ и $g(x)$ называются *равными*, если они имеют одинаковые степени и, кроме того, их коэффициенты при одинаковых степенях переменной x равны между собой.

На множестве $\mathbb{R}[x]$ можно определить операции сложения и умножения. Эти операции будут обозначаться также, как соответствующие операции на числовых множествах.

Пусть даны произвольные многочлены

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n,$$

$$g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{m-1}x^{m-1} + b_mx^m.$$

Для каждого $k \geqslant 0$ определим число (c_k) при помощи равенства

$$c_k = a_k + b_k. \tag{2}$$

Если $p = \max(m, n)$, то легко понять, что $c_k = 0$, если $k > p$.

О п р е д е л е н и е. Многочлен

$$s(x) = c_0 + c_1x + c_2x_2 + \ldots + c_{k-1}x^{k-1} + c_kx^k,$$

где коэффициенты c_i определены равенством (2), называется суммой многочленов $f(x)$, $g(x)$.

Из определения вытекает следующее неравенство

$$\deg s \leqslant \max(\deg f, \deg g).$$

Это неравенство становится равенством, если либо $\deg f \neq \deg g$, либо $\deg f = \deg g$, но $a_n \neq -b_n$; в противном случае неравенство становится строгим.

О п р е д е л е н и е. Многочлен

$$-f(x) = -a_0 - a_1x - a_2x^2 - \ldots - a_{n-1}x^{n-1} - a_nx^n$$

называется *противоположным* к многочлену (1).

Используя свойства операции сложения на множестве $\mathbb{R}$, нетрудно убедиться в том, что определенная нами операции сложения обладает свойствами ассоциативности и коммутативности, нулевой многочлен является нейтральным элементом относительно сложения и, кроме того, $f(x) + (-f(x)) = 0$.

Наличие этих свойств у операции сложения означает, что множество $\mathbb{R}[x]$ относительно этой операции является *абелевой группой*.

Чтобы ввести произведение двух многочленов, для каждого неотрицательного целого k определим число

$$d_k = \sum_{i+j=k} a_i b_j. \tag{3}$$

Ясно, что $d_{n+m} = a_n b_m \neq 0$ и $d_l = 0$, если $l > n + m$.

Определение. Многочлен

$$p(x) = d_0 + d_1 x + d_2 x_2 + \ldots + d_{m+n-1} x^{m+n-1} + d_{m+n} x^{m+n},$$

где коэффициенты d_i определены равенством (3), называется произведением многочленов $f(x)$, $g(x)$.

Какие из свойств операции умножения на $\mathbb{R}$ наследует операция умножения на $\mathbb{R}[x]$? Из определения сразу видно, что умножение на $\mathbb{R}[x]$ коммутативно. Можно убедиться (соответствующие проверки мы опускаем), что эта операция ассоциативна и дистрибутивна относительно сложения. Кроме того, многочлен 1 является нейтральным элементом относительно умножения.

Таким образом, множество $\mathbb{R}[x]$ относительно введенных нами операций сложения и умножения является *коммутативным кольцом с единицей*.

Выше было отмечено, что старший коэффициент произведения двух ненулевых многочленов равен произведению их старших коэффициентов. Поэтому произведение двух ненулевых многочленов — всегда ненулевой многочлен. Отсюда немедленно вытекает, что *кольцо* $\mathbb{R}[x]$ *не содержит делителей нуля*.

В заключение этого раздела сделаем следующее важное замечание. Наряду с полем $\mathbb{R}$ нам известны и другие поля: например, поле $\mathbb{C}$ всех комплексных чисел, поле $\mathbb{Q}$ всех рациональных чисел или поле $\mathbb{Z}_p$, состоящее из вычетов по простому модулю p. Просматривая данные выше определения, мы видим, что многочлены и операции над ними можно определить для произвольного поля, а не только для поля $\mathbb{R}$. Таким образом, можно рассматривать множество всех многочленов $F[x]$ с коэффициентами из произвольного поля F. Нетрудно понять, что определения суммы и произведения многочленов в этом более общем случае не претерпевают никаких изменений; более того, отмеченные выше свойства этих операций также сохранятся.

Начиная с этого момента, мы будем рассматривать кольцо многочленов $F[x]$ над произвольным полем F.

1.2. Теорема о делении с остатком

Пусть $f(x)$, $g(x)$ — произвольные многочлены над полем F. Будем говорить,что $g(x)$ делит $f(x)$ (обозначение $g(x) \,|\, f(x)$), если $f(x) = u(x)g(x)$, где $u(x)$ — некоторый могочлен. Например, многочлен нулевой степени делит произвольный многочлен. Нетрудно понять, однако, что не всегда один многочлен делит другой. В связи с этим важное значение имеет следующее утверждение, называемое теоремой о делении с остатком. Читателю будет полезно сравнить эту теорему с теоремой 2.1 из [3].

Теорема 1.1. *Пусть $f(x), g(x)$ — произвольные многочлены над полем F, причем $g(x)$ — ненулевой многочлен. Тогда существуют однозначно определенные многочлены $u(x)$ и $r(x)$ такие, что*

$$f(x) = u(x)g(x) + r(x), \qquad \deg r < \deg g.$$

Многочлены $u(x)$ и $r(x)$ называют соответственно *частным* и *остатком*, полученными при делении $f(x)$ на $g(x)$. Заметим, что остаток $r(x)$ может оказаться нулевым многочленом.

Доказательство теоремы 1.1. Степени многочленов $f(x), g(x)$ обозначим через n и m соответственно. Докажем сначала, что требуемые многочлены $u(x)$ и $r(x)$ сущечтвуют. Удобно многочлен $g(x)$ зафиксировать, а многочлену $f(x)$ разрешить изменяться произвольным образом.

Если $n < m$, то

$$f(x) = 0 \cdot g(x) + f(x),$$

откуда видно, что $u(x) = 0$, $r(x) = f(x)$.

Пусть $n \geqslant m$. Считая, что многочлены $f(x)$ и $g(x)$ записаны по убыванию степеней, обозначим через a_0, b_0 их старшие коэффициенты.

Применим для доказательства существования многочленов $u(x)$ и $r(x)$ метод математической индукции. При $n = m$ положим

$$r(x) = f(x) - \frac{a_0}{b_0} g(x). \tag{4}$$

Поскольку степени многочленов $f(x)$ и $a_0 b_0^{-1} g(x)$ равны между собой, а их старшие коэффициенты совпадают, получаем, что $\deg r < \deg g$. Если из равенства (4) выразить многочлен $f(x)$, то станет понятно, что частное равно $a_0 b_0^{-1}$, а остаток равен $r(x)$.

Пусть $n > m$. Предположим, что для любого многочлена степени, меньшей n, частное и остаток от деления на $g(x)$ существуют. Рассмотрим многочлен

$$h(x) = f(x) - \frac{a_0}{b_0} x^{n-m} g(x). \tag{5}$$

Нетрудно понять, что $\deg h < \deg f = n$; поэтому к многочлену $h(x)$ применимо предположение индукции. Следовательно, найдутся такие многочлены $v(x)$ и $r(x)$, что

$$h(x) = v(x)g(x) + r(x), \qquad \deg r < \deg g. \tag{6}$$

Из равенств (5) и (6) легко получить, что

$$f(x) = (a_0 b_0^{-1} x^{n-m} + v(x))g(x) + r(x).$$

Таким образом, существование частного и остатка от деления $f(x)$ на $g(x)$ доказано.

Проверим единственность частного и остатка. Предположим, что существуют многочлены $u(x), v(x), r(x), s(x)$ такие, что

$$f(x) = u(x)g(x) + r(x), \qquad \deg r < \deg g, \tag{7}$$

$$f(x) = v(x)g(x) + s(x), \qquad \deg s < \deg g. \tag{8}$$

Вычитая из равенства (7) равенство (8), после очевидных преобразований приходим к равенству

$$r(x) - s(x) = (v(x) - u(x))g(x). \tag{9}$$

Допустим, что многочлены $r(x)$ и $s(x)$ различны. Тогда многочлен $r(x) - s(x)$ ненулевой, откуда следует, что $v(x) - u(x)$ также ненулевой многочлен. Так как при перемножении степени многочленов складываются, степень $(v(x) - u(x))g(x)$ не меньше, чем степень $g(x)$. С другой стороны, степени многочленов $r(x)$ и $s(x)$ строго меньше степени $g(x)$; ясно, что такому же неравенству удовлетворяет и степень разности $r(x) - s(x)$. Отсюда следует, что равенство (9) невозможно. Таким образом, предположение о том, что $r(x)$ и $s(x)$ — различные многочлены, привело к противоречию. Тем самым доказано, $r(x) = s(x)$. Поскольку кольцо многочленов не содержит делителей нуля и $g(x) \neq 0$, из равенства (9) следует, что многочлен $v(x) - u(x)$ нулевой, т. е. $u(x) = v(x)$.

Рассмотрим конкретный пример. Предположим, что требуется многочлен $f(x) = 2x^3 + x^2 + 3x - 5$ (делимое) поделить поделить с остатком на многочлен $g(x) = x^2 + x - 1$ (делитель). Имеем

$$2x^3 + x^2 + 3x - 5 = 2x(x^2 + x - 1) + (-x^2 + 5x - 5),$$

$$-x^2 + 5x - 5 = -1(x^2 + x - 1) + (6x - 6).$$

Отсюда видно, что

$$2x^3 + x^2 + 3x - 5 = (2x - 1)(x^2 + x - 1) + (6x - 6).$$

Следовательно, частное и остаток равны $2x-1$ и $6x-6$ соответственно.

Эти вычисления удобно записывать следующим образом (вспомните деление "уголком" для натуральных чисел):

$$\begin{array}{r|l} 2x^3 + x^2 + 3x - 5 & x^2 + x - 1 \\ \cline{2-2} \underline{2x^3 + 2x^2 - 2x} & 2x - 1 \\ -x^2 + 5x - 5 & \\ \underline{-x^2 - x + 1} & \\ 6x - 6 & \end{array}$$

1.3. Схема Горнера

В этом разделе мы рассмотрим простой алгоритм, при помощи которого произвольный многочлен $f(x)$ можно разделить с остатком на линейный двучлен $x-c$.

Применяя теорему о делении с остатком, имеем

$$f(x) = g(x)(x-c) + r, \tag{10}$$

где $g(x)$ — частное, а r — остаток от деления. Ясно, что $\deg g = \deg f - 1$ и r — некоторое число.

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$g(x) = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}.$$

Если многчлен $g(x)$ подставить в правую часть равенства (10), раскрыть скобки и привести подобные члены, то получится равенство

$$f(x) = b_0x^n + (b_1 - cb_0)x^{n-1} + \ldots + (b_{n-1} - cb_{n-2})x + (r - cb_{n-1}). \tag{11}$$

Сравнивая коэффициенты многочленов, стоящих в правой и левой частях равенства (11), получаем

$$\begin{array}{rcl} a_0 & = & b_0 \\ a_1 & = & b_1 - cb_0 \\ \ldots & \ldots & \ldots\ldots \\ a_{n-1} & = & b_{n-1} - cb_{n-2} \\ a_n & = & r - cb_{n-1}. \end{array} \tag{12}$$

Отсюда при помощи очевидных преобразований имеем

$$\begin{array}{rcl} b_0 & = & a_0 \\ b_1 & = & a_1 + cb_0 \\ \ldots & \ldots & \ldots\ldots \\ b_{n-1} & = & a_{n-1} + cb_{n-2} \\ r & = & a_n + cb_{n-1}. \end{array} \tag{13}$$

Равенства (13) позволяют последовательно вычислить коэффициенты частного и остаток от деления. Алгоритм, основанный на применении равенств (13), часто называют схемой Горнера.

Применим схему Горнера для деления остатком многочлена $f(x) = x^4+3x^2-2x$ на двучлен $x+2$. Обозначим через $g(x) = b_0x^3+b_1x^2+b_2x+b_3$ и r соответственно частное и остаток от деления. В силу равенств (13) имеем

$$\begin{array}{rcl} b_0 & = & a_0 = 1 \\ b_1 & = & a_1 + cb_0 = -2 \\ b_2 & = & a_2 + cb_1 = 7 \\ b_3 & = & a_3 + cb_2 = -16 \\ r & = & a_4 + cb_3 = 32. \end{array} \tag{14}$$

Эти вычисления более удобно организовать в виде следующей таблицы.

	1	0	3	−2	0
−2	1	−2	7	−16	32

Способ заполнения этой таблицы состоит в следующем. В первой строке записаны все коэффициенты многочлена $f(x)$, в начале второй строки для удобства записывается число c, равное в этом случае -2. Затем последовательно, начиная со второй клетки, заполняется вторая строка (см. равенства (14).

1.4. Отношение делимости

В разд. 1.2 было определено отношение делимости на кольце $F[x]$: многочлен $g(x)$ делит многочлен $f(x)$ ($g(x) \,|\, f(x)$), если $f(x) = u(x)g(x)$ для некоторого многочлена $u(x)$.

Свойства отношения делимости в кольце многочленов во многом аналогичны свойствам отношения делимости в кольце целых чисел (см. разд. 2.5 из [3]) . Перечислим эти свойства.

(D1) $f(x) \,|\, f(x)$;

(D2) если $f(x) \,|\, g(x)$, $g(x) \,|\, f(x)$ и $f(x), g(x) \neq 0$, то $f(x) = s \cdot g(x)$ для некоторого отличного от нуля числа s;

(D3) если $f(x) \,|\, g(x)$ и s — отличное от нуля число, то $s \cdot f(x) \,|\, g(x)$;

(D4) если $f(x) \,|\, g(x)$ и $g(x) \,|\, h(x)$, то $f(x) \,|\, h(x)$;

(D5) если $f(x) \,|\, g(x)$ и $f(x) \,|\, h(x)$, то $f(x) \,|\, u(x)g(x) + v(x)h(x)$ каковы бы ни были многочлены $u(x), v(x)$;

(D6) если $f(x) \,|\, g_i(x)$, $1 \leqslant i \leqslant k$, то $f(x) \,|\, \sum_{i=1}^{k} u_i(x)g_i(x)$ каковы бы ни были многочлены $u_i(x)$, $1 \leqslant i \leqslant k$;

(D7) если $f(x) \,|\, g(x)$ и $g(x) \neq 0$, то $\deg f \leqslant \deg g$.

Отметим, что произвольный многочлен $f(x)$ делит нулевой многочлен и если $0 \,|\, g(x)$, то $g(x) = 0$.

Введем понятие наибольшего общего делителя двух многочленов.

О п р е д е л е н и е. Многочлен $d(x)$ называется *наибольшим общим делителем* многочленов $f(x)$ и $g(x)$, если выполнены свойства:

(a) $d(x) \,|\, f(x)$ и $d(x) \,|\, g(x)$;
(b) если $c(x) \,|\, f(x)$ и $c(x) \,|\, g(x)$, то $c(x) \,|\, d(x)$.

Проверим, что любые два ненулевых многочлена $f(x)$ и $g(x)$ имеют наибольший общий делитель. Рассмотрим множество D, состоящее из ненулевых многочленов $s(x)$, представимых в виде $u(x)f(x) + v(x)g(x)$ для некоторых $u(x), v(x)$. Множество D, очевидно, непусто; ясно, что среди его элементов есть многочлен $d(x)$ наименьшей степени. Этот многочлен делит любой многочлен $s(x)$ из D. В самом деле, по теореме о делении с остатком имеем

$$s(x) = w(x)d(x) + r(x), \quad \deg r < \deg d. \tag{15}$$

Рассуждая "от противного", предположим, что $r(x)$ — ненулевой многочлен. Поскольку $s(x)$ и $d(x)$ содержатся в множестве D, имеем $d(x) = u(x)f(x) + v(x)g(x)$, $s(x) = u_1(x)f(x) + v_1(x)g(x)$ для некоторых многочленов $u(x), v(x), u_1(x), v_1(x)$. Используя равенство (15), получаем

$$r(x) = s(x) - w(x)d(x).$$

Поэтому

$$r(x) = (u_1(x) - w(x)u(x))f(x) + (v_1(x) - w(x)v(x))g(x). \tag{16}$$

Следовательно, многочлен $r(x)$ принадлежит множеству D. Поскольку $\deg r < \deg d$, мы получили противоречие с выбором многочлена $d(x)$. Это противоречие показывает, что $r(x)$ — нулевой многочлен, и потому $d(x) \,|\, s(x)$. Заметим теперь, что $f(x) = 1 \cdot f(x) + 0 \cdot g(x)$, $g(x) = 0 \cdot f(x) + 1 \cdot g(x)$; отсюда следует, $f(x), g(x)$ принадлежат множеству D. Значит, $d(x)$ является общим делителем многочленов $f(x)$ и $g(x)$.

Из свойства (D5) следует, что если $c(x) \mid f(x)$ и $c(x) \mid g(x)$, то $c(x)$ делит $d(x)$.

Следовательно, справедливо следующее утверждение.

Теорема 1.2. *Пусть $f(x)$ и $g(x)$ — ненулевые многочлены. Среди многочленов вида $f(x)u(x) + g(x)v(x)$, $(u(x), v(x) \in F[x])$ выберем ненулевой многочлен $d(x)$ наименьшей возможной степени. Тогда $d(x)$ — наибольший общий делитель многочленов $f(x)$ и $g(x)$.*

Наибольший общий делитель двух многочленов не является однозначно определенным. Легко убедиться в том, что если $d(x)$ — наибольший общий делитель двух данных многочленов, то любой наибольший общий делитель этих многочленов равен $\alpha d(x)$, где $\alpha \in F, \alpha \neq 0$. В самом деле, пусть d_1 — произвольный наибольший общий делитель данных многочленов. Тогда $d(x) \mid d_1(x)$ и $d_1(x) \mid d(x)$. Из свойства (D2) вытекает, что $d_1(x) = \alpha d(x)$. Таким образом, два наибольших общих делителя данных многочленов получаются один из другого умножением на отличное от нуля число. Отсюда немедленно вытекает, что для произвольных ненулевых многочленов $f(x)$ и $g(x)$ однозначно определен их наибольший общий делитель со старшим коэффициентом, равным единице. Этот наибольший общий делитель будет обозначаться через $(f(x), g(x))$.

Из теоремы 1.2 вытекает следующее утверждение.

Следствие 1. *Пусть $f(x)$ и $g(x)$ — ненулевые многочлены, $d(x)$ — их наибольший общий делитель. Тогда*

$$d(x) = u(x)f(x) + v(x)g(x),$$

где $u(x), v(x)$ — некоторые многочлены из $F[x]$.

При изучении кольца $\mathbb{Z}$ всех целых чисел мы убедились в важности понятия взаимно простых целых чисел. Введем аналогичное понятие для многочленов.

Определение. Многочлены $f(x)$ и $g(x)$ называются *взаимно простыми*, если $(f(x), g(x)) = 1$.

Иными словами, многочлены взаимно просты, если все их общие делители имеют нулевую степень, т. е. являются отличными от нуля числами.

Из теоремы 1.2 легко выводится признак взаимной простоты многочленов.

Теорема 1.3. *Многочлены $f(x)$ и $g(x)$ взаимно просты тогда и только тогда, когда $f(x)u(x) + g(x)v(x) = 1$ для некоторых многочленов $u(x)$ и $v(x)$.*

Доказательство. Если многочлены $f(x)$ и $g(x)$ взаимно просты, то существование таких многочленов $u(x)$ и $v(x)$, что

$$f(x)u(x) + g(x)v(x) = 1, \tag{17}$$

сразу вытекает из следствия 1.

Обратно, пусть выполнено равенство (17) и $d(x) = (f(x), g(x))$. Тогда $d(x)$ делит левую часть равенства (17), а потому $d(x) \,|\, 1$. Следовательно, $d(x) = 1$, т. е. многочлены $f(x)$ и $g(x)$ взаимно просты.

Отметим следующие полезные свойства взаимно простых многочленов:

(1) если $(f(x), g(x)) = 1$ и $(f(x), h(x)) = 1$, то $(f(x), g(x)h(x)) = 1$;

(2) если $f(x) \,|\, h(x)$, $g(x) \,|\, h(x)$ и $(f(x), g(x)) = 1$, то $f(x)g(x) \,|\, h(x)$;

(3) если $f(x) \,|\, g(x)h(x)$ и $(f(x), g(x)) = 1$, то $f(x) \,|\, h(x)$.

Доказательство свойств (1) - (3).

Пусть $(f(x), g(x)) = 1$ и $(f(x), h(x)) = 1$. Тогда

$$f(x)u(x) + g(x)v(x) = 1 \qquad f(x)t(x) + h(x)s(x) = 1.$$

Перемножив эти равенства, получим

$$f(x)(f(x)u(x)t(x)+g(x)t(x)v(x)+h(x)u(x)s(x))+(g(x)h(x))(v(x)s(x)) = 1.$$

Примение теоремы 1.3 показывает, что многочлены $f(x)$ и $g(x)h(x)$ взаимно просты. Свойство (1) доказано.

Проверим свойство (2). Пусть $f(x) \,|\, h(x)$, $g(x) \,|\, h(x)$ и $(f(x), g(x)) = 1$. Поскольку $f(x)$ и $g(x)$ взаимно просты, найдутся такие многочлены $u(x)$, $v(x)$, что $f(x)u(x) + g(x)v(x) = 1$, откуда

$$f(x)h(x)u(x) + g(x)h(x)v(x) = h(x). \tag{18}$$

Поскольку $f(x) \,|\, h(x)$, имеем $f(x)g(x) \,|\, g(x)h(x)$. Аналогично, из $g(x) \,|\, h(x)$ следует $f(x)g(x) \,|\, f(x)h(x)$. Таким образом, $f(x)g(x)$ делит левую часть равенства (18), а потому делит его правую часть, равную $h(x)$.

Перейдем к доказательству свойства (3). Пусть $f(x) \mid g(x)h(x)$ и $(f(x), g(x)) = 1$. Как и раньше, взаимная простота многочленов $f(x)$ и $g(x)$ влечет выполнение равенства (18). Поскольку $f(x) \,|\, g(x)h(x)$, многочлен $f(x)$, очевидно, делит левую часть равенства (18). Следовательно, правая часть этого равенства делится на $f(x)$.

Следует отметить, что свойства отношения делимости в кольце $\mathbb{Z}$ аналогичны свойствам отношения делимости в кольце $F[x]$.

1.5. Алгоритм Евклида

В этом разделе мы изложим алгоритм Евклида, предназначенный для нахождения наибольшего общего делителя двух многочленов из кольца $F[x]$.

Пусть $f(x)$ и $g(x)$ — произвольные ненулевые многочлены из $F[x]$. Поделив первый многочлен на второй с остатком, получим

$$f(x) = u_1(x)g(x) + r_1(x), \qquad \deg r_1(x) < \deg g(x).$$

Если $\deg r_1(x) \geqslant 0$ (выпонение этого неравенства означает, что $r_1(x) \neq 0$), то поделим $g(x)$ на $r_1(x)$:

$$g(x) = u_2(x)r_1(x) + r_2(x), \qquad \deg r_2(x) < \deg r_1(x).$$

Снова, если $\deg r_2(x) \geqslant 0$, поделим $r_1(x)$ на $r_2(x)$:

$$r_1(x) = u_3(x)r_2(x) + r_3(x), \qquad \deg r_3(x) < \deg r_2(x).$$

Продолжая этот процесс, мы получим последовательность остатков

$$r_1(x), r_2(x), r_3(x), \ldots, r_i(x), \ldots$$

такую, что

$$\deg r_1(x) > \deg r_2(x) > \deg r_3(x) > \ldots \deg r_i(x) > \ldots. \tag{19}$$

Нетрудно понять, что найдется номер k, для которого $r_k(x) \neq 0$ и $r_{k+1}(x) = 0$. В самом деле, если бы указанный процесс можно было продолжать до бесконечности, то в силу неравенств (19) получилась бы бесконечная убывающая последовательность целых неотрицательных чисел. Как мы знаем, существование такой последовательности невозможно, ибо любое непустое множество целых неотрицательных чисел имеет наименьший элемент.

Итак, нами получена следующая цепочка равенств:

$$\begin{array}{rcl} f(x) & = & u_1(x)g(x) + r_1(x) \\ g(x) & = & u_2(x)r_1(x) + r_2(x) \\ r_1(x) & = & u_3(x)r_2(x) + r_3(x) \\ \ldots\ldots & \ldots & \ldots\ldots\ldots\ldots \\ r_{k-2}(x) & = & u_k(x)r_{k-1}(x) + r_k(x) \\ r_{k-1}(x) & = & u_{k+1}(x)r_k(x). \end{array} \tag{20}$$

Справедливо следующее утверждение.

Теорема 1.4. *Последний отличный от нуля остаток $r_k(x)$ является наибольшим общим делителем многочленов $f(x)$ и $g(x)$.*

Доказательство. Проверим сначала, что $r_k(x)$ делит многочлены $f(x)$ и $g(x)$. Для этого достаточно пройти по равенствам (20) снизу вверх. В самом деле, из последнего равенства имеем $r_k(x) \,|\, r_{k-1}(x)$. Поднимаясь по цепочке равенств, последовательно получаем $r_k(x) \,|\, r_{k-2}(x)$, $\ldots$, $r_k(x) \,|\, r_1(x)$, $r_k(x) \,|\, g(x)$, $r_k(x) \,|\, h(x)$.

Пусть многочлен $c(x)$ является общим делителем многочленов $f(x)$ и $g(x)$, т. е. $c(x) \,|\, f(x)$ и $c(x) \,|\, g(x)$. Убедимся, что $c(x) \,|\, r_k(x)$. Для этого

пройдем по равенствам (20) сверху вниз. Из первого равенства получаем $c(x) \mid r_1(x)$. Последовательно опускаясь вниз до предпоследнего равенства, получим $c(x) \mid r_2(x)$, $c(x) \mid r_3(x)$, $c(x) \mid r_{k-2}(x)$, $c(x) \mid r_{k-1}(x)$, и наконец, $c(x) \mid r_k(x)$.

Следовательно, $r_k(x)$ — наибольший общий делитель $f(x)$ и $g(x)$.

В качестве примера применим алгоритм Евклида для отыскания наибольшего общего делителя многочленов $f(x) = x^5 + x^4 + 1$ и $g(x) = x^4 + x^2 + 1$. Последовательно имеем

$$\begin{array}{rcl} x^5 + x^4 + 1 & = & (x+1)(x^4 + x^2 + 1) + (-x^3 - x^2 - x) \\ x^4 + x^2 + 1 & = & (-x+1)(-x^3 - x^2 - x) + (x^2 + x + 1) \\ -x^3 - x^2 - x & = & (-x)(x^2 + x + 1) \end{array} \qquad (21)$$

Последний отличный от нуля остаток равен $x^2 + x + 1$. Следовательно, $(f(x), g(x)) = x^2 + x + 1$.

Напомним, что в силу теоремы 1.2 существуют такие многочлены $u(x)$ и $v(x)$, что

$$x^2 + x + 1 = u(x)(x^5 + x^4 + 1) + v(x)(x^4 + x^2 + 1).$$

Эти многочлены легко находятся из равенств (21). В самом деле, выражая из второго равенства остаток от деления, получаем

$$x^2 + x + 1 = x^4 + x^2 + 1 - (-x+1)(-x^3 - x^2 - x).$$

В силу первого равенства имеем

$$-x^3 - x^2 - x = x^5 + x^4 + 1 - (x+1)(x^4 + x^2 + 1).$$

Поэтому

$$x^2 + x + 1 = x^4 + x^2 + 1 - (-x+1)(x^5 + x^4 + 1 - (x+1)(x^4 + x^2 + 1)) =$$

$$= x^4 + x^2 + 1 + (x-1)(x^5 + x^4 + 1) + (1 - x^2)(x^4 + x^2 + 1) =$$

$$= (x-1)(x^5 + x^4 + 1) + (2 - x^2)(x^4 + x^2 + 1).$$

1.6. Освобождение от иррациональности в знаменателе дроби

Напомним, что в некоторых простых случаях мы умеем освобождаться от иррациональности в знаменателе. Например, если даны две дроби

$$A = \frac{1}{\sqrt{3} - 1}, \qquad B = \frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 1},$$

то, умножив числитель и знаменатель первой дроби на $\sqrt{3}+1$, а числитель и знаменатель второй дроби на $\sqrt[3]{2}-1$, мы получим, что

$$A=\frac{\sqrt{3}+1}{2},\qquad B=\sqrt[3]{2}+1.$$

Здесь для преобразований были использованы формулы для разности квадратов и разности кубов.

Сейчас на примерах мы рассмотрим более общую ситуацию. Пусть дана дробь

$$C=\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}.$$

Видно, что применение формул сокращенного умножения здесь к цели не приведет. Поэтому поступим следующим образом. Рассмотрим два многочлена: x^3-2 и x^2+x+3. Ниже при помощи алгоритма Евклида мы убедимся, что эти многочлены взаимно просты. Поэтому найдутся такие многочлены $u(x)$ и $v(x)$, что

$$u(x)(x^3-2)+v(x)(x^2+x+3)=1. \tag{22}$$

Подставив в равенство (22) вместо x число $\sqrt[3]{2}$, получим

$$v(\sqrt[3]{2})(\sqrt[3]{4}+\sqrt[3]{2}+3)=1.$$

Следовательно, умножение числителя и знаменателя дроби C на число $v(\sqrt[3]{2})$ позволяет освободиться от иррациональности в знаменателе дроби C.

Реализуем намеченный план решения задачи. Применяя алгоритм Евклида к многочленам x^3-2 и x^2+x+3, получим

$$x^3-2=(x-1)(x^2+x+3)+(-2x+1),$$

$$x^2+x+3=\left(-\frac{1}{2}x-\frac{3}{4}\right)(-2x+1)+\frac{15}{4}.$$

Отсюда находим

$$\left(-\frac{1}{2}x-\frac{3}{4}\right)(x^3-2)+\left(-\frac{1}{2}x^2-\frac{1}{4}x+\frac{7}{4}\right)(x^2+x+3)=\frac{15}{4}. \tag{23}$$

Если теперь в равенство (23) вместо x подставить $\sqrt[3]{2}$, а затем обе части умножить на 4, то получится числовое равенство

$$(-2\sqrt[3]{4}-\sqrt[3]{2}+7)(\sqrt[3]{4}+\sqrt[3]{2}+3)=15.$$

Отсюда вытекает, что в результате умножения числителя и знаменателя дроби C на $-2\sqrt[3]{4} - \sqrt[3]{2} + 7$, получим

$$C = -\frac{2\sqrt[3]{4} + \sqrt[3]{2} - 7}{15}.$$

В качестве второго примера освободимся от иррациональности в знаменателе дроби

$$D = \frac{1}{\sqrt[4]{9} + \sqrt[4]{3} + 1}.$$

Для этого алгоритм Евклида нужно применить к многочленам $x^4 - 3$ и $x^2 + x + 1$. Последовательно имеем

$$x^4 - 3 = (x^2 - x)(x^2 + x + 1) + (x - 3),$$

$$x^2 + x + 1 = (x + 4)(x - 3) + 13.$$

Из этих равенств получаем

$$-(x + 4)(x^4 - 3) + (x^3 + 3x^2 - 4x + 1)(x^2 + x + 1) = 13. \qquad (24)$$

Подставив в равенство (24) число $\sqrt[4]{3}$ вместо x получаем числовое равенство

$$(\sqrt[4]{27} + 3\sqrt[4]{9} - 4\sqrt[4]{3} + 1)(\sqrt[4]{9} + \sqrt[4]{3} + 1) = 13.$$

Следовательно, после освобождения от иррациональности в знаменателе дроби D получим

$$D = \frac{\sqrt[4]{27} + 3\sqrt[4]{9} - 4\sqrt[4]{3} + 1}{13}.$$

1.7. Корни многочлена

Пусть $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ — произвольный многочлен над полем F. Для произвольного $c \in F$ выражение

$$f(c) = a_0c^n + a_1c^{n-1} + a_2c^{n-2} + \ldots + a_{n-1}c + a_n$$

является элементом поля F и называется значением многочлена $f(x)$ при $x = c$.

Теорема 1.5. *Значение многочлена $f(x)$ при $x = c$ совпадает с остатком от деления $f(x)$ на $x - c$.*

Доказательство. По теореме о делении с остатком имеем $f(x) = (x - c)u(x) + r$. Подставив в это равенство вместо x элемент c, получим $f(c) = r$.

Если $f(c) = 0$, то c называют корнем многочлена $f(x)$.

Из теоремы 1.5 легко получить следующее утверждение.

Следствие 1. *Элемент $c \in F$ является корнем многочлена $f(x)$ тогда и только тогда, когда $x - c$ делит $f(x)$.*

В самом деле, $x - c$ делит $f(x)$ тогда и только тогда, когда остаток от деления $f(x)$ на $x - c$ равен нулю.

Это утверждение часто называют теоремой Безу.

Заметим, что если c — корень многочлена $f(x)$, то $f(x)$ может делится не только на $x - c$, но и на $(x - c)^j$, где $j > 1$. Пусть k — наибольшее натуральное число со свойством: $f(x)$ делится $(x - c)^k$. В этом случае говорят, что c — *корень кратности* k многочлена $f(x)$. По-другому это свойство можно сформулировать следующим образом:

$$f(x) = (x - c)^k u(x),$$

причем $u(x)$ не делится на $x - c$.

Корень кратности 1 часто называют простым корнем, кратности 2 — двойным корнем, а корень кратности 3 — тройным корнем.

Возникает вопрос: сколько корней может иметь многочлен степени n. Частичный ответ на этот вопрос дает следующее утверждение.

Теорема 1.6. *Пусть $f(x)$ — произвольный многочлен степени $n \geqslant 1$. Тогда $f(x)$ имеет не более чем n корней с учетом их кратности.*

Доказательство. Применим индукцию по степени многочлена.

Если $n = 1$, то $f(x)$ — многочлен первой степени, имеющий только один корень.

Пусть $n > 1$. Предположим, что для всех многочленов, степень которых меньше чем n, утверждение выполнено. Если многочлен $f(x)$ не имеет корней, то доказываемое утверждение очевидно выполнено. Пусть $f(x)$ имеет корень c_1. Тогда $f(x) = (x - c_1)g(x)$. Многочлен $g(x)$ имеет степень $n - 1$ и потому по предположению индукции число его корней не превосходит $n - 1$. Следовательно, $f(x)$ имеет не более чем n корней.

Из теоремы 1.6 вытекает следующее важное утверждение.

Теорема 1.7. *Пусть $f(x)$ и $g(x)$ — многочлены, степени которых не превосходят n. Если $c_1, c_2, \ldots, c_n, c_{n+1}$ — попарно различные числа и $f(c_k) = g(c_k)$ при всех $k \in \{1, 2, \ldots, n, n + 1\}$, то многочлены $f(x)$ и $g(x)$ равны.*

Доказательство. Рассмотрим многочлен

$$h(x) = f(x) - g(x)$$

и предположим, рассуждая "от противного", что этот многочлен не является нулевым. Тогда $0 \leqslant \deg h \leqslant n$ и $h(c_k) = 0$, где $1 \leqslant k \leqslant n+1$. Таким образом, ненулевой многочлен $h(x)$ имеет $n+1$ различных корней, хотя его степень не превосходит n. Существование такого многочлена противоречит теореме 1.6.

Теорема 1.7 утверждает, что многочлен степени n однозначно определяется своими значениями в $n+1$ различных точках.

Пусть $f(x)$ — многочлен степени n, c_1, c_2, …, c_n, c_{n+1} — попарно различные числа. Для каждого $k \in \{1, 2, \ldots, n, n+1\}$ рассмотрим многочлен

$$\varphi_k(x) = \frac{(x-c_1)\ldots(x-c_{k-1})(x-c_{k+1})\ldots(x-c_{n+1})}{(c_k-c_1)\ldots(c_k-c_{k-1})(c_k-c_{k+1})\ldots(c_k-c_{n+1})}.$$

Легко проверить, что

$$\varphi_k(c_j) = \begin{cases} 0, & \text{если } j \neq k, \\ 1, & \text{если } j = k. \end{cases} \tag{25}$$

В самом деле, из определения многочлена $\varphi_k(x)$ видно, что числа c_1, c_2, …, c_{k-1}, c_{k+1}, …, c_n, c_{n+1} являются его корнями, а при подстановке числа c_k в этот многочлен получается дробь, у которой числитель равен знаменателю.

Рассмотрим многочлен

$$g(x) = f(c_1)\varphi_1(x) + f(c_2)\varphi_2(x) + \ldots + f(c_n)\varphi_n(x) + f(c_{n+1})\varphi_{n+1}(x). \tag{26}$$

Степень многочлена $g(x)$ не превосходит числа n, поскольку степень каждого многочлена $\varphi_k(x)$ равна n. Кроме того, из равенства (25) вытекает, что при вычислении $g(c_k)$ в правой части равенства (26) останется только одно слагаемое, равное $f(c_k)$ (все остальные слагаемые обратятся в ноль). Следовательно, многочлены $f(x)$ и $g(x)$ совпадают в $n+1$ различных точках и их степени не превосходят n. Применяя теорему 1.7, получаем, что многочлены $f(x)$ и $g(x)$ равны, и потому справедлива формула

$$f(x) = f(c_1)\varphi_1(x) + f(c_2)\varphi_2(x) + \ldots + f(c_n)\varphi_n(x) + f(c_{n+1})\varphi_{n+1}(x). \tag{27}$$

Эта формула называется *интерполяционной формулой Лагранжа*. Она позволяет восстановить многочлен степени не превосходящей n, если известны его значения в $n+1$ различных точках.

Пусть $f(x)$ — произвольный многочлен над полем F. Определим отображение $\tilde{f} : F \to F$ при помощи правила: $\tilde{f}(c) = f(c)$ для каждого $c \in F$. Такое отображение называется полиномиальным отображением, соответствующим многочлену $f(x)$.

Очевидно, что из равенства $f(x) = g(x)$ вытекает равенство $\tilde{f} = \tilde{g}$. Возникает вопрос: верно ли обратное утверждение? Ответ на этот вопрос утвердителен в случае бесконечного поля F. В самом деле, пусть поле F бесконечно, а степени многочленов $f(x)$ и $g(x)$ не превосходят n. Если c_1, c_2,..., c_{n+1} — попарно различные элементы поля F (такие элементы существуют в силу бесконечности поля), то

$$f(c_i) = \tilde{f}(c_i) = \tilde{g}(c_i) = g(c_i),$$

где $1 \leqslant i \leqslant n+1$. Применяя теорему 1.7, получим,что $f(x) = g(x)$.

Пусть $f(x)$ — произвольный многочлен. Определим многочлен $f'(x)$, называемый производной многочлена $f(x)$.

Если $f(x)$ — многочлен нулевой степени, то $f'(x) = 0$. Если же

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

где $n \geqslant 1$, то

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + a_{n-1}.$$

Из этого определения можно вывести следующие равенства.

1. $(f(x) + g(x))' = f'(x) + g'(x)$,
2. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$,
3. $(f^n(x))' = nf^{n-1}(x)f'(x)$.

Производная многочлена применяется для решения вопроса о том, является ли данный корень многочлена его кратным корнем. А именно, справедливо следующее утверждение.

Теорема 1.8. *Пусть c — корень многочлена $f(x)$. Элемент c является корнем кратности k многочлена $f(x)$ в том и только том случае, когда c — корень кратности $k-1$ его производной $f'(x)$.*

Доказательство. Пусть $f(x) = (x-c)^k g(x)$, где $k \geqslant 2$ и $g(x)$ не делится на $x - c$. Тогда с использованием равенств 1 — 3 получаем

$$f'(x) = k(x-c)^{k-1}g(x) + (x-c)^k g'(x) = (x-c)^{k-1}(kg(x) + (x-c)g'(x)).$$

Так как многочлен $kg(x) + (x-c)g'(x)$ не делится на $x-c$, отсюда видно, что c — корень кратности $k-1$ производной $f'(x)$.

Обратно, пусть c — корень многочлена $f(x)$, одновременно являющийся корнем кратности $k-1$ его производной. Предположим, что c является корнем кратности m многочлена $f(x)$. Только что мы убедились, что c — корень кратности $m-1$ производной $f'(x)$. Следовательно, $m - 1 = k - 1$, откуда $m = k$.

Установим равенства, связывающие корни многочлена с его коэффициентами. Пусть $f(x)$ — многочлен степени $n \geqslant 1$, имеющий в поле F корни $x_1, x_2, \ldots, x_n$. Тогда

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n = a_0(x-x_1)(x-x_2)\ldots(x-x_{n-1})(x-x_n). \quad (28)$$

1.8. Рациональные корни многочлена с целыми коэффициентами

Отыскание рациональных корней многочлена с целыми коэффициентами основано на следующем утверждении.

Теорема 1.9. *Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ — произвольный многочлен с целыми коэффициентами. Если несократимая дробь p/q является его корнем, то $p \,|\, a_n$, $q \,|\, a_0$ и $p - mq \,|\, f(m)$ для любого целого m.*

Доказательство. Учитывая, что p/q — корень $f(x)$, имеем

$$q^n f\left(\frac{p}{q}\right) = a_0p^n + a_1p^{n-1}q + \ldots + a_{n-1}pq^{n-1} + a_nq^n = 0.$$

Убедимся, что $p \,|\, a_n$. Поскольку p делит каждое из целых чисел a_0p^n, $a_1p^{n-1}q, \ldots, a_{n-1}pq^{n-1}$ и число 0, имеем $p \,|\, a_nq^n$. Дробь p/q несократима, т. е. p и q взаимно просты. Отсюда следует взаимная простота чисел p и q^n. Таким образом, $p \,|\, a_n$.

Аналогично проверяется, что $q \,|\, a_0$.

Докажем, что $p - mq \,|\, f(m)$ для любого целого m. Рассмотрим многочлен

$$q^n f\left(\frac{x}{q}\right) = a_0x^n + a_1qx^{n-1} + \ldots + a_{n-1}q^{n-1}x + a_nq^n.$$

Ясно, что многочлен $q^n f(x/q)$ имеет целые коэффициенты и число p является его корнем. Поэтому

$$q^n f\left(\frac{x}{q}\right) = (x-p)u(x).$$

Ссылка на схему Горнера показывает, что многочлен $u(x)$ имеет целые коэффициенты. Подставив в последнее равенство $x = mq$, получим

$$q^n f(m) = (mq-p)u(mq).$$

Понятно, что $u(mq)$ — целое число. Следовательно, $mq-p$ делит $q^n f(m)$. Теперь заметим, что числа $mq - p$ и q взаимно просты (проверьте это утверждение самостоятельно). Отсюда вытекает взаимная простота чисел $mq-p$ и q^n. Следовательно, $mq-p$ делит $f(m)$. Числа $p-mq$ и $mq-p$ взаимно противоположны, и потому $p - mq$ также делит $f(m)$.

1.9. Неприводимые многочлены

В разд. 1.4 было отмечено, что имеется аналогия между некоторыми свойствами колец $\mathbb{Z}$ и $F[x]$. В этом разделе будут рассмотрены многочлены, играющие в кольце $F[x]$ ту же роль, что и простые числа в кольце $\mathbb{Z}$.

Определение. Многочлен $p(x) \in F[x]$ называется *неприводимым над полем* F, если $\deg p \geqslant 1$ и для любого делителя $q(x)$ многочлена $p(x)$ либо $\deg q = 0$, либо $\deg q = \deg p$.

Например, многочлен $p(x) = x^2 - 3$ принадлежит кольцу $\mathbb{Q}[x]$. Легко убедиться в том, что этот многочлен неприводим над полем $\mathbb{Q}$. В самом деле, пусть $p(x)$ имеет делитель первой степени. Можно считать, что старший коэффициент делителя равен 1. Следовательно, $x - c \,|\, p(x)$ для некоторого $c \in \mathbb{Q}$. Поскольку

$$x^2 - 3 = (x + c)(x - c) + (c^2 - 3),$$

имеем $c^2 - 3 = 0$. Отсюда $c = \pm\sqrt{3} \notin \mathbb{Q}$.

Этот многочлен принадлежит, очевидно, и кольцу $\mathbb{R}[x]$. Так как $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$, получаем, что данный многочлен приводим над полем $\mathbb{R}$.

Из рассмотренного примера видно, что неприводимость многочлена — это свойство, зависящее от того, над каким полем рассматривается многочлен.

Лемма 1. *Пусть $p(x)$ — неприводимый многочлен над полем F. Тогда для любого ненулевого многочлена $f(x) \in F[x]$ либо $p(x) \,|\, f(x)$, либо $(p(x), f(x)) = 1$.*

Доказательство. Пусть $(p(x), f(x)) = d(x)$. Тогда $d(x) \mid p(x)$ и, следовательно, либо $\deg d(x) = 0$, либо $\deg d(x) = \deg p(x)$. В первом случае $d(x) = 1$, откуда вытекает взаимная простота многочленом $p(x)$ и $f(x)$. Рассмотрим второй случай. Поскольку $d(x) \mid p(x)$ и $\deg d(x) = \deg p(x)$, имеем $p(x) = sd(x)$ для некоторого $s \in F$. Учитывая, что $d(x) \,|\, f(x)$, получаем $sd(x) \,|\, f(x)$, т. е. $p(x) \,|\, f(x)$.

Лемма 2. *Пусть $p(x)$ и $q(x)$ — неприводимые над F многочлены, причем $p(x) \,|\, q(x)$. Тогда $q(x) = ap(x)$ для некоторого $a \in F$. В частности, если старшие коэффициенты многочленов $p(x)$ и $q(x)$ совпадают, то $q(x) = p(x)$.*

Доказательство. Поскольку $p(x) \mid q(x)$ и $q(x)$ — неприводимый многочлен, имеем $\deg p = 0$ или $\deg p = \deg q$. Но $p(x)$ — неприводимый многочлен, поэтому $\deg p \geqslant 1$. Следовательно, выполнено равенство

$\deg p = \deg q$. Из этого равенства вытекает, что частное от деления $q(x)$ на $p(x)$ является многочленом нулевой степени, т. е. $q(x) = ap(x)$, $a \in F$.

Заметим, что многочлены $p(x)$ и $ap(x)$ одновременно являются неприводимыми. Это свойство легко следует из утверждения: множества делителей этих многочленов совпадают.

Лемма 3. *Любой многочлен $f(x \in F[x]$ ненулевой степени имеет неприводимый делитель.*

Доказательство. Рассмотрим множество D, состоящее из всех делителей многочлена $f(x)$, имеющих ненулевую степень. Пусть $p(x)$ — многочлен наименьшей степени из D. Убедимся, что $p(x)$ неприводим. Пусть $g(x) \mid p(x)$ и $\deg g \geqslant 1$. Тогда $g(x)$ принадлежит D и потому $\deg p \leqslant \deg g$. С другой стороны из соотношения $g(x) \mid p(x)$ вытекает, что $\deg g \leqslant \deg p$. Следовательно, $\deg g = \deg p$. Таким образом, всякий делитель многочлена $p(x)$ либо имеет нулевую степень, либо его степень равна степени многочлена $p(x)$. Это означает, что многочлен $p(x)$ неприводим.

Теорема 1.10. *Пусть $f(x \in F[x])$ — произвольный многочлен степени не ниже первой. Тогда*

$$f(x) = a_0 p_1(x) p_2(x) \dots p_{s-1}(x) p_s(x),$$

где a_0 — старший коэффициент многочлена $f(x)$, а $p_1(x)$, $p_2(x)$,. . . ,$p_{s-1}(x)$, $p_s(x)$ — неприводимые над полем F многочлены, старшие коэффициенты которых равны 1.

Указанное представление единственно с точностью до перестановки сомножителей.

Доказательство. Заметим, что утверждение выполнено в том случае, когда $f(x)$ — неприводимый многочлен.

Доказательство для приводимых многочленов проведем при помощи метода математической индукции. Пусть $n = deg f$.

Если $n = 1$, то $f(x) = a_0(x - c)$. Многочлен $x - c$ очевидно неприводим. Кроме того, это представление единственно, поскольку из равенства $a_0(x - c) = b_0(x - d)$ сразу следует, что $a_0 = b_0$ и $c = d$.

Пусть $n > 1$ и для всех многочленов, степень которых меньше чем n, утверждение выполнено. Рассмотрим произвольный многочлен $f(x)$ степени n. В силу леммы 3 многочлен $f(x)$ имеет неприводимый над F делитель $p_1(x)$ со старшим коэффициентом, равным единице. Поэтому

$$f(x) = p_1(x) g(x),$$

причем степень $g(x)$ меньше чем n. К многочлену $g(x)$ применимо предположение индукции; следовательно,

$$g(x) = a_0 p_2(x) \dots p_{s-1}(x) p_s(x),$$

где a_0 — старший коэффициент $g(x)$, а $p_2(x), \dots, p_{s-1}(x)p_s(x)$ — неприводимые многочлены со старшими коэффициентами, равными 1. Таким образом,

$$f(x) = a_0 p_1(x) p_2(x) \dots p_{s-1}(x) p_s(x). \tag{29}$$

Проверим единственность разложения. Предположим, что наряду с равенством (29) имеет место равенство

$$f(x) = a_0 q_1(x) q_2(x) \dots q_{t-1}(x) q_t(x), \tag{30}$$

где q_1, $q_2(x)$,..., $q_{t-1}(x)$, $q_t(x)$ — неприводимые над полем F многочлены, старшие коэффициенты которых равны 1. Поскольку $p_1(x) \mid f(x)$, многочлен $p_1(x)$ не является взаимно простым с произведением, стоящим в правой части равенства (30). Отсюда вытекает, что $p_1(x)$ не взаимно прост с одним из многочленов q_1, $q_2(x)$,..., $q_{t-1}(x)$, $q_t(x)$. Без ограничения общности можно считать, что этим многочленом является $q_1(x)$. В силу леммы 1 имеем $p_1(x) \mid q_1(x)$. Применяя лемму 2 и учитывая, что старшие коэффициенты многочленов $p_1(x)$ и $q_1(x)$ равны между собой, получаем, что $p_1(x) = q_1(x)$.

Пусть $g(x)$ — частное от деления $f(x)$ на $p_1(x)$. С учетом равенств (29) и (30) получаем

$$g(x) = a_0 p_2(x) \dots p_{s-1}(x) p_s(x) = a_0 q_2(x) \dots q_{t-1}(x) q_t(x). \tag{31}$$

Поскольку $\deg g < \deg f$, к многочлену $g(x)$ применимо предположение индукции. Отсюда вытекает, что $s - 1 = t - 1$, т. е. $s = t$. Кроме того, два представления многочлена $g(x)$, указанные в равенстве (31), различаются только порядком сомножителей. С учетом равенств (29) и (30) аналогичным свойством обладают два представления многочлена $f(x)$.

1.10. Основная теорема и следствия из нее

Пусть $f(x)$ — многочлен с коэффициентами из поля F, причем $\deg f \geqslant 2$. Возникает вопрос: обязательно ли этот многочлен имеет хотя бы один корень из поля F? Вообще говоря, это не так. В самом деле, многочлен $f(x) = x^2+1$ лежит в кольце $\mathbb{R}[x]$, однако действительных корней не имеет. С другой стороны, этот многочлен имеет два комплексных корня: i и $-i$. Из этого примера вытекает, что многочлен, не имеющий корней в данном поле F, может иметь корни в более широком поле K.

Рассмотрим теперь многочлен $f(x)$ с комплексными коэффициентами и зададимся аналогичным вопросом: обязательно ли $f(x)$ имеет комплексный корень? Казалось бы, следует поискать многочлен с комплексными коэффициентами, не имеющий комплексных корней. Однако, такого многочлена не существует, ибо справедливо следующее утверждение.

Теорема 1.11. *Пусть $f(x)$ — многочлен с комплексными коэффициентами, причем $\deg f \geqslant 1$. Тогда $f(x)$ имеет хотя бы один комплексный корень.*

Эта теорема была доказана К. Ф. Гауссом в 1799 году. С тех пор получено много различных доказательств этой теоремы. Однако все эти доказательства содержат соображения, связанные с понятием непрерывности. Мы не будем приводить доказательство теоремы 1.11. Часто эту теорему называют основной теоремой о многочленах с комплексными коэффициентами.

Из теоремы 1.11 легко получается следующее утверждение.

Теорема 1.12. *Любой многочлен с комплексными коэффициентами степени не ниже первой разлагается в произведение многочленов первой степени с комплексными коэффициентами.*

Доказательство. Пусть $f(x)$ — многочлен с комплексными коэффициентами, причем $n = \deg f \geqslant 1$.

Если $n = 1$, то $f(x)$ — многочлен первой степени и утверждение очевидно выполняется.

Пусть $n > 1$. Предположим, что для всех многочленов степени меньшей, чем n, утверждение выполнено, т. е. любой такой многочлен разлагается на линейные множители. Из теоремы 1.11 вытекает, что существует комплексное число c_1, являющееся корнем многочлена $f(x)$. Тогда

$$f(x) = (x - c_1)g(x). \tag{32}$$

Ясно, что старшие коэффициенты многочленов $f(x)$ и $g(x)$ совпадают и $\deg g = n - 1$. К многочлену $g(x)$ применимо предположение индукции, поэтому

$$g(x) = a_0(x - c_2)(x - c_3)\dots(x - c_n), \tag{33}$$

где a_0 — старший коэффициент многочлена $f(x)$. Подставляя выражение для $g(x)$ из равенства (33) в равенство (34), получим

$$f(x) = a_0(x - c_1)(x - c_2)\dots(x - c_n).$$

Тем самым, теорема 1.12 доказана.

Из теоремы 1.12 вытекает, что *в кольце* $\mathbb{C}[x]$ *только многочлены первой степени являются неприводимыми.*

Заметим, что поле F называют *алгебраически замкнутым*, если любой многочлен из $F[x]$, отличный от константы, в кольце $F[x]$ разлагается на множители первой степени. Таким образом, поле $\mathbb{C}$ всех комплексных чисел алгебраически замкнуто.

В отличие от поля $\mathbb{C}$ поле $\mathbb{R}$ всех действительных чисел алгебраически замкнутым не является. Например, произвольный многочлен второй степени с отрицательным дискриминантом не разлагается в произведение многочленов первой степени с действительными коэффициентами. Возникает вопрос: на какие множители наименьшей степени можно разложить произвольный многочлен с действительными коэффициентами в кольце $\mathbb{R}[x]$?

Ответ на этот вопрос дает следующее утверждение.

Теорема 1.13. *Любой многочлен с действительными коэффициентами степени не ниже первой в кольце* $\mathbb{R}[x]$ *разлагается в произведение многочленов первой степени и многочленов второй степени с отрицательным дискриминантом.*

Для доказательства этой теоремы нам понадобится несколько вспомогательных утверждений.

Лемма 1. *Пусть* $f(x)$ *— многочлен с действительными коэффициентами. Если комплексное число* c *является корнем* $f(x)$*, то и сопряженное к* c *число* $\overline{c}$ *также является корнем этого многочлена.*

Доказательство. Поскольку c — корень многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

имеем

$$a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c + a_n = 0.$$

Из свойств операции сопряжения вытекает, что равенство не изменится при замене всех чисел на сопряженные к ним. Так как применение операции сопряжения к действительным числам a_0, a_1, …, a_{n-1}, a_n и 0 не изменяет эти числа, получаем

$$a_0\overline{c}^n + a_1\overline{c}^{n-1} + \ldots + a_{n-1}\overline{c} + a_n = 0,$$

т. е. $f(\overline{c}) = 0$.

Замнтим, что если корень c не является действительным числом, то многочлен $f(x)$ делится на многочлен

$$\varphi(x) = (x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}, \tag{34}$$

имеющий, очевидно, действительные коэффициенты. Кроме того, дискриминант квадратного трехчлена $\varphi(x)$, равный $(c-\overline{c})^2$, является квадратом чисто мнимого числа, и потому отрицателен.

Лемма 2. *Пусть $f(x)$ — многочлен с действительными коэффициентами. Если комплексное число c является корнем $f(x)$ кратности k, то и сопряженное к c число $\overline{c}$ также является корнем той же кратности.*

Доказательство. Пусть c — комплексный (но не действительный) корень многочлена $f(x)$, имеющий кратность k. Предположим, что $\overline{c}$ является корнем кратности l данного многочлена. Без ограничения общности можно считать, что $l \leqslant k$. Поскольку c и $\overline{c}$ — корни многочлена $f(x)$ кратности не ниже l, этот многочлен делится на многочлен $\varphi^l(x) = (x-c)^l(x-\overline{c})^l$, имеющий действительные коэффициенты. Если $g(x)$ — частное от деления $f(x)$ на $\varphi^l(x)$, то

$$f(x) = \varphi^l(x)g(x) = (x-c)^l(x-\overline{c})^l g(x). \tag{35}$$

Из теоремы о делении с остатком вытекает, что $g(x)$ имеет действительные коэффициенты. Поскольку число $\overline{c}$ — корень кратности l многочлена $f(x)$, это число не является корнем многочлена $g(x)$. Применение леммы 1 к многочлену $g(x)$, получаем, что c также не является корнем $g(x)$. Из равенства (35) вытекает, что c является корнем многочлена $f(x)$ кратности l, т. е. $k = l$.

Лемма 2 показывает, что комплексные корни многочлена с действительными коэффициентами разбиваются на пары взаимно сопряженных корней.

Перейдем к доказательству теоремы 1.13. Теорема, очевидно, выполнена для многочленов первой степени. Пусть $n > 1$. Предположим, что теорема выполнена для всех многочленов степени меньшей, чем n, и проверим ее выполнимость для многочлена $f(x)$ степени n. В силу основной теоремы многочлен $f(x)$ имеет комплексный корень c. Возможны два случая.

1. Корень c является действительным числом. Тогда

$$f(x) = (x-c)g(x),$$

причем $g(x)$ имеет действительные коэффициенты. Ясно, что к $g(x)$ применимо предположение индукции. Следовательно, теорема выполнена и для $f(x)$.

2. Корень c не является действительным числом. В этом случае

$$f(x) = \varphi(x)h(x),$$

где $\varphi(x) = (x - c)(x - \overline{c})$ — многочлен с действительными коэффициентами. Понятно, что $h(x)$ имеет действительные коэффициенты и $\deg h < \deg f$. Поэтому к $h(x)$ применимо предположение индукции. Отсюда, как и выше, вытекает, что теорема выполнена для $f(x)$.

Из теоремы 1.13 следует, что *в кольце* $\mathbb{R}[x]$ *неприводимыми являются только многочлены первой степени и многочлены второй степени с отри цательным дискриминантом.*

Список литературы

[1] *Кострикин А.И.* Введение в алгебру. М., Наука, 1977.

[2] *Курант Р., Роббинс Г.* Что такое математика: Элементарный очерк идей и методов. М., Просвещение, 1967.

[3] *Расин В.В.* Лекции по алгебре. Натуральные и целые числа. Неравенства. Отображения множеств. Числовые функции. Екатеринбург: УрГУ, 2000.

Содержание