Глава 3.

Начала алгебры многочленов

3.1. Построение и основные свойства алгебры многочленов

Функция действительной переменной x называется многочленом, если она может быть представлена в виде

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

где $a_0, a_1, a_2, \ldots, a_n$ — какие-то действительные числа (некоторые из которых или даже все могут равняться нулю). Можно доказать, и мы это сделаем ниже в более общей ситуации, что такое представление единственно с точностью до приписывания членов с нулевыми коэффициентами, т.е. если

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n \quad \forall x \in \mathbb{R},$$

то $a_k = b_k$ при $k = 0, 1, 2, \ldots, n$.

Очевидно, что сумма и произведение многочленов, а также произведение многочлена на любое число, также являются многочленами. Это означает, что многочлены образуют подалгебру в алгебре всех функций действительной переменной (см. пример 1.8.3). Эта подалгебра называется алгеброй многочленов над $\mathbb{R}$ и обозначается $\mathbb{R}[x]$.

Если попытаться аналогичным образом трактовать многочлены над любым полем K, то возникает трудность, состоящая в том, что формально различные многочлены могут быть тождественно равны при всех значениях переменной. Например, многочлены x и x^2 над полем $\mathbb{Z}_2$ оба принимают значение 0 при $x = 0$ и 1 — при $x = 1$. В то же время хотелось бы рассматривать их как разные многочлены. Выход состоит в формальном определении, при котором многочлен фактически отождествляется с последовательностью его коэффициентов.

Рассмотрим векторное пространство K^∞ финитных последовательностей элементов поля K (см. пример 2.2.6). Условимся нумеровать члены последовательностей, начиная с нуля, и пусть e_k $(k = 0, 1, 2, \ldots)$ обозначает последовательность, k-й член которой равен 1, а все остальные члены равны 0. Последовательности $e_0, e_1, e_2, \ldots$ образуют базис пространства K^∞.

Превратим пространство K^∞ в алгебру, определив умножение базисных векторов по правилу

$$e_k e_l = e_{k+l}.$$

Из коммутативности и ассоциативности сложения целых чисел следует, что умножение базисных векторов, а, значит, и любых элементов полученной алгебры, коммутативно и ассоциативно. Элемент e_0 является ее единицей. Эта алгебра называется алгеброй многочленов над K и обозначается $K[x]$ (вместо x может использоваться любая другая буква).

Для того чтобы перейти к привычному представлению многочленов, условимся, во-первых, отождествлять элементы вида ae_0 $(a \in K)$ алгебры $K[x]$ с соответствующими элементами поля K и, во-вторых, элемент e_1 обозначим через x (здесь проявляется роль выбранной буквы x). Тогда в соответствии с определением операций в $K[x]$ мы получаем, что $e_k = x^k$ и

$$\begin{aligned}(a_0, a_1, a_2, \ldots, a_n, 0, \ldots) = a_0e_0 + a_1e_1 + a_2e_2 + \ldots + a_ne_n = \\ = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.\end{aligned}$$

Числа $a_0, a_1, a_2, \ldots$ называются коэффициентами многочлена. Последний из ненулевых коэффициентов называется старшим коэффициентом, а его номер — степенью многочлена. Степень многочлена f обозначается через $\deg f$. Степень нулевого многочлена не определена, однако иногда удобно считать, что она равна $-\infty$.

Легко видеть, что

$$\deg(f+g) \leqslant \max\{\deg f, \deg g\}, \tag{37}$$

$$\deg fg = \deg f + \deg g. \tag{38}$$

Докажем, например, последнее равенство. Пусть

$$f = a_0 + a_1 x + \ldots + a_n x^n \quad (a_n \neq 0),$$
$$g = b_0 + b_1 x + \ldots + b_m x^m \quad (b_m \neq 0).$$

Тогда при перемножении f и g получается только один член степени $n+m$, а именно, $a_n b_m x^{n+m}$, а членов большей степени не получается вообще. Так как в поле нет делителей нуля, то $a_n b_m \neq 0$ и, стало быть,

$$\deg fg = n + m = \deg f + \deg g.$$

Предыдущее рассуждение показывает, что в алгебре $K[x]$ нет делителей нуля. Из него же следует, что обратимыми элементами в этой алгебре являются только многочлены нулевой степени, т.е. ненулевые элементы поля K.

Замечание 1. Многочлен можно обозначать $f(x)$ или просто f, если из контекста ясно, какой буквой обозначается «переменная».

Замечание 2. Часто бывает удобнее располагать многочлен не по возрастающим, а по убывающим степеням x:

$$f = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n.$$

Замечание 3. В качестве K можно взять любое коммутативное ассоциативное кольцо с единицей (ср. замечание 1.9.1). В этом случае все предыдущее остается без изменений, за исключением последней части, связанной с формулой (38), где нужно дополнительно потребовать, чтобы в кольце K не было делителей нуля.

Замечание 4. Произведение финитных последовательностей $(a_0, a_1, a_2, \ldots)$ и $(b_0, b_1, b_2, \ldots)$ в кольце $K[x]$ есть последовательность $(c_0, c_1, c_2, \ldots)$, члены которой находятся по формулам

$$c_k = \sum_{l=0}^{k} a_l b_{k-l}.$$

Эти формулы имеют смысл и для любых (не обязательно финитных) последовательностей. Таким образом получается коммутативная ассоциативная алгебра с единицей, называемая алгеброй формальных степенных рядов над K и обозначаемая $K[[x]]$. Ее элементы обычно записывают как формальные бесконечные суммы вида

$$a_0 + a_1x + a_2x^2 + \ldots$$

Алгебра $K[[x]]$, как и $K[x]$, не имеет делителей нуля, но доказывается это по-другому (попробуйте это сделать!).

Каждый многочлен

$$f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \tag{39}$$

определяет функцию на K со значениями в K, значение которой в точке $c \in K$ по определению равно

$$f(c) = a_0 + a_1c + a_2c^2 + \ldots + a_nc^n.$$

Так как сумма и произведение многочленов, а также произведение многочлена на число, приводятся к каноническому виду (39) преобразованиями, использующими только свойства операций в $K[x]$, справедливые и в поле K, то мы придем к одному и тому же результату, сделав подстановку $x = c$ до или после этих преобразований. Это означает, что

$$\begin{gathered}(f+g)(c) = f(c) + g(c),\\ (fg)(c) = f(c)g(c).\\ (\lambda f)(c) = \lambda f(c),\end{gathered}$$

т. е. операции над многочленами приводят к таким же операциям над соответствующими функциями.

Как мы показали на примере в начале параграфа, разные многочлены могут определять одну и ту же функцию. Оказывается, однако, что такое возможно, только если поле K конечно.

Теорема 1. Если поле K бесконечно, то разные многочлены над K определяют разные функции.

Доказательство. Пусть многочлены $f, g \in K[x]$ определяют одну и ту же функцию. Тогда их разность $h = f - g$ определяет нулевую функцию, т. е. $h(c) = 0$ для всех $c \in K$. Предположим, что $h \neq 0$, и пусть

$$h = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \quad (a_{n-1} \neq 0).$$

Возьмем различные $x_1, x_2, \ldots, x_n \in K$ (здесь используется бесконечность поля K). Совокупность верных равенств

$$\begin{cases} a_0 + a_1x_1 + a_2x_1^2 + \ldots + a_{n-1}x_1^{n-1} = 0, \\ a_0 + a_1x_2 + a_2x_2^2 + \ldots + a_{n-1}x_2^{n-1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1x_n + a_2x_n^2 + \ldots + a_{n-1}x_n^{n-1} = 0 \end{cases}$$

рассмотрим как (квадратную) систему однородных линейных уравнений относительно $a_0, a_1, a_2, \ldots, a_{n-1}$. Определитель матрицы коэффициентов этой системы есть определитель Вандермонда $V(x_1, x_2, \ldots, x_n)$ (см. пример 2.4.5) и потому отличен от нуля. Следовательно, система имеет только нулевое решение, что противоречит нашему предположению.

Замечание 5. Если поле K конечно, то множество всех многочленов над K тем не мение бесконечно (но счетно), в то время как множество всех функций на K со значениями в K конечно. Поэтому в этом случае обязательно должны существовать разные многочлены, определяющие одну и ту же функцию.

Задача. Так называемая задача интерполяции состоит в нахождении многочлена степени $< n$, принимающего в заданных (различных) точках $x_1, x_2, \ldots, x_n \in K$ заданные значения $y_1, y_2, \ldots, y_n \in K$. (В частности, при $n = 2$ это называется линейной интерполяцией.) Доказать, что задача интерполяции имеет единственное решение при любых $x_1, x_2, \ldots, x_n$ и $y_1, y_2 \cdots, y_n$.

Деление одного многочлена на другой в обычном смысле слова в алгебре $K[x]$, как правило, невозможно. Однако возможно так называемое деление с остатком, похожее на деление с остатком в кольце целых чисел.

Теорема 2. Пусть $f, g \in K[x]$, причем $g \neq 0$. Тогда существуют такие многочлены q и r, что $f = qg + r$ и либо $r = 0$, либо $\deg r < \deg g$. Многочлены q и r определены этими условиями однозначно.

Нахождение таких многочленов q и r и называется делением с остатком f на g. При этом q называется неполным частным, а r — остатком от деления f на g. Многочлен f делится на g в алгебре $K[x]$ тогда и только тогда, когда $r = 0$.

Доказательство. 1) Докажем возможность деления с остатком. Если $\deg f < \deg g$, то можно взять $q = 0, r = f$. Если $\deg f \geqslant \deg g$, то q и r находятся обычной процедурой «деления уголком». А именно, пусть

$$f = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$
$$g = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m,$$

где $a_0, b_0 \neq 0$. Рассмотрим многочлен

$$f_1 = f - \frac{a_0}{b_0} x^{n-m} g.$$

Его степень меньше, чем степень f. Если $\deg f_1 < \deg g$, то мы можем взять

$$q = \frac{a_0}{b_0} x^{n-m}, \quad r = f_1.$$

В противном случае поступаем с многочленом f_1 так же, как с f. В конце концов мы получим такой многочлен

$$q = c_0 x^{n-m} + c_1 x^{n-m-1} + \ldots + c_{n-m},$$

что $\deg(f - qg) < \deg g$. Это и будет неполное частное от деления f на g, а многочлен $r = f - qg$ будет остатком.

2) Докажем, что многочлены q и r определены условиями теоремы однозначно. Пусть

$$f = q_1 g + r_1 = q_2 g + r_2,$$

где $\deg r_1 < \deg g$ и $\deg r_2 < \deg g$. Тогда

$$r_1 - r_2 = (q_2 - q_1) g$$

и, если $q_1 \neq q_2$, то

$$\deg(r_1 - r_2) = \deg(q_2 - q_1) + \deg g \geqslant \deg g,$$

что, очевидно, неверно. Следовательно, $q_1 = q_2$ и $r_1 = r_2$.

Особое значение имеет деление с остатком на линейный двучлен $x - c$. В этом случае остаток имеет степень < 1, т. е. является элементом поля K. Таким образом, результат деления с остатком многочлена f на $x - c$ имеет вид

$$f(x) = (x - c) q(x) + r \quad (r \in K).$$

Отсюда следует, что

$$f(c) = r,$$

т.е. остаток равен значению многочлена f в точке c. Это утверждение называется теоремой Безу.

Деление с остатком на $x-c$ осуществляется по замечательно простой схеме, называемой схемой Горнера.

А именно, пусть

$$\begin{aligned}a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n &= \\ &= (x-c)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}) + r.\end{aligned}$$

Приравнивая коэффициенты при соответствующих степенях x, получаем цепочку равенств

$$\begin{aligned}&a_0 = b_0,\\ &a_1 = b_1 - cb_0,\\ &a_2 = b_2 - cb_1,\\ &\ldots\ldots\ldots\ldots\ldots\\ &a_{n-1} = b_{n-1} - cb_{n-2},\\ &a_n = r - cb_{n-1},\end{aligned}$$

откуда находим следующие рекуррентные формулы для $b_0, b_1, \ldots\ldots, b_{n-1}$ и r:

$$\begin{aligned}&b_0 = a_0,\\ &b_1 = a_1 + cb_0,\\ &b_2 = a_2 + cb_1,\\ &\ldots\ldots\ldots\ldots\ldots\\ &b_{n-1} = a_{n-1} + cb_{n-2},\\ &r = a_n + cb_{n-1}.\end{aligned}$$

Исходные данные и результаты вычислений удобно расположить в виде таблицы:

$$\begin{array}{c|cccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ \hline c & b_0 & b_1 & b_2 & \ldots & b_{n-1} & r \end{array}$$

Каждое число во второй строке этой таблицы, начиная с b_1, находится как сумма числа, стоящего над ним, и числа, стоящего слева, умноженного на c.

В частности, это дает очень эффективный способ вычисления значений многочлена.

Пример. Найдем значение многочлена

$$f = 2x^6 - 11x^4 - 19x^3 - 7x^2 + 8x + 5$$

в точке $x = 3$. По схеме Горнера получаем:

$$\begin{array}{r|rrrrrrr} & 2 & 0 & -11 & -19 & -7 & 8 & 5 \\ \hline 3 & 2 & 6 & 7 & 2 & -1 & 5 & 20 \end{array}$$

Таким образом, $f(3) = 20$.

3.2. Общие свойства корней многочленов

Элемент c поля K называется корнем многочлена $f \in K[x]$ (или соответствующего алгебраического уравнения $f(x) = 0$), если $f(c) = 0$. Из теоремы Безу (см. предыдущий параграф) следует

Теорема 1. Элемент c поля K является корнем многочлена $f \in K[x]$ тогда и только тогда, когда f делится на $x - c$.

Этим можно воспользоваться для доказательства следующей теоремы.

Теорема 2. Число корней ненулевого многочлена не превосходит его степени.

Доказательство. Пусть c_1 — корень многочлена f. Тогда

$$f = (x - c_1)f_1 \quad (f_1 \in K[x]).$$

Пусть c_2 — корень многочлена f_1. Тогда

$$f_1 = (x - c_2)f_2 \quad (f_2 \in K[x])$$

и, значит,

$$f = (x - c_1)(x - c_2)f_2.$$

Продолжая так дальше, мы в конце концов представим многочлен f в виде

$$f = (x - c_1)(x - c_2)\ldots(x - c_m)g, \tag{40}$$

где многочлен $g \in K[x]$ не имеет корней. Числа $c_1, c_2, \ldots, c_m$ — это все корни многочлена f. В самом деле, для любого $c \in K$ имеем

$$f(c) = (c - c_1)(c - c_2)\ldots(c - c_m)g(c)$$

и, так как $g(c) \neq 0$, то $f(c) = 0$, только если $c = c_i$ для некоторого i. Таким образом, число корней многочлена f не превосходит m (оно может быть меньше m, поскольку не исключено, что среди чисел $c_1, c_2, \ldots, c_m$ есть одинаковые); но

$$m = \deg f - \deg g \leqslant \deg f.$$

Замечание 1. Эта теорема фактически уже была нами доказана другим способом в процессе доказательства теоремы 1.1. С другой стороны, из нее можно получить доказательство теоремы 1.1, не использующее теории линейных уравнений. А именно, если различные многочлены f и g над бесконечным полем K определяют одну и ту же функцию, то все элементы поля K являются корнями ненулевого многочлена $h = f - g$, что противоречит только что доказанной теореме.

Доказательство предыдущей теоремы наводит на мысль, что некоторые корни правильнее было бы считать несколько раз. Этому можно придать точный смысл.

Корень c многочлена f называется простым, если f не делится на $(x - c)^2$, и кратным — в противном случае. Кратностью корня c называется наибольшее из таких k, что f делится на $(x - c)^k$. Таким образом, простой корень — это корень кратности 1. Иногда удобно считать, что число, не являющееся корнем, — это корень кратности 0.

Очевидно, что c — корень кратности k многочлена f тогда и только тогда, когда

$$f = (x - c)^k g, \tag{41}$$

где $g(c) \neq 0$.

Теперь мы докажем уточнение теоремы 2.

Теорема 3. Число корней ненулевого многочлена с учетом их кратностей (т. е. считая каждый корень столько раз, какова его кратность) не превосходит степени многочлена, причем равенство имеет место тогда и только тогда, когда этот многочлен разлагается на линейные множители.

Доказательство. Перепишем равенство (40), объединив одинаковые множители:

$$f = (x - c_1)^{k_1}(x - c_2)^{k_2} \ldots (x - c_s)^{k_s} g \tag{42}$$

($c_1, c_2, \ldots, c_s$ различны). Ясно, что $c_1, c_2, \ldots, c_s$ — это все корни многочлена. Далее, выделяя в (42) множитель $(x - c_i)^{k_i}$, мы можем написать

$$f = (x - c_i)^{k_i} h_i, \quad \text{где } h_i(c_i) \neq 0.$$

Следовательно, c_i — корень кратности k_i.

Таким образом, число корней многочлена f с учетом их кратностей равно

$$k_1 + k_2 + \ldots + k_s = \deg f - \deg g,$$

откуда и вытекают все утверждения теоремы.

Замечание 2. Условно считается, что многочлен нулевой степени разлагается в произведение пустого множества линейных множителей.

Если многочлен

$$f = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

разлагается на линейные множители, то это разложение может быть записано в виде

$$f = a_0 (x - c_1)(x - c_2) \ldots (x - c_n),$$

где $c_1, c_2, \ldots, c_n$ — корни многочлена f, причем каждый из них повторен столько раз, какова его кратность. Приравнивая коэффициенты при соответствующих степенях x в этих двух представлениях многочлена f, мы получаем следующие формулы Виета:

$$\begin{gathered}
c_1 + c_2 + \ldots + c_n = -\frac{a_1}{a_0}, \\
c_1 c_2 + c_1 c_3 + \ldots + c_{n-1} c_n = \frac{a_2}{a_0}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\textstyle\sum_{i_1 < i_2 < \ldots < i_k} c_{i_1} c_{i_2} \ldots c_{i_k} = (-1)^k \frac{a_k}{a_0}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
c_1 c_2 \ldots c_n = (-1)^n \frac{a_n}{a_0}.
\end{gathered}$$

В левой части k-й формулы Виета стоит сумма всевозможных произведений k корней многочлена f. С точностью до множителя $(-1)^k$ это коэффициент при x^k в произведении $(x - c_1) \times$ $\times (x - c_2) \ldots (x - c_n)$.

Пример 1. Комплексные корни 5-й степени из 1

$$\epsilon_k = \cos \frac{2\pi k}{5} + i \sin \frac{2\pi k}{5} \quad (k = 0, 1, 2, 3, 4)$$

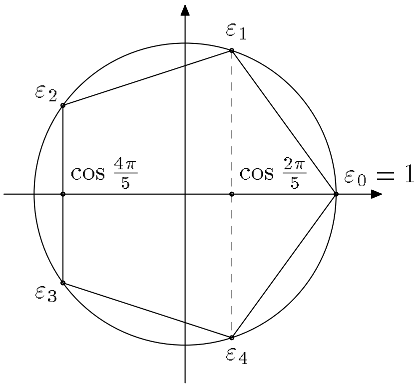

Рис. 12.

(рис. 12) суть корни многочлена $x^5 - 1$. По первой из формул Виета их сумма равна нулю. Приравнивая нулю сумму их действительных частей, получаем

$$2\cos\frac{4\pi}{5} + 2\cos\frac{2\pi}{5} + 1 = 0.$$

Пусть $\cos\frac{2\pi}{5} = x$; тогда $\cos\frac{4\pi}{5} = 2x^2 - 1$, так что

$$4x^2 + 2x - 1 = 0,$$

откуда

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}, \quad \cos\frac{4\pi}{5} = -\frac{\sqrt{5}+1}{4}.$$

Задача. Пусть n — простое число. Пользуясь задачей из §1.6 и последней из формул Виета, доказать теорему Вильсона:

$$(n-1)! \equiv -1 \pmod{n}.$$

Многочлен f называется нормированным (или приведенным), если $a_0 = 1$. Формулы Виета позволяют выразить коэффициенты нормированного многочлена через его корни (при условии, что число корней равно степени многочлена).

Пример 2. Найдем нормированный многочлен 4-й степени

$$f = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4,$$

имеющий двукратный корень 1 и простые корни 2, 3. По формулам Виета

$$\begin{aligned}
-a_1 &= 1+1+2+3 = 7,\\
a_2 &= 1\cdot 1 + 1\cdot 2 + 1\cdot 3 + 1\cdot 2 + 1\cdot 3 + 2\cdot 3 = 17,\\
-a_3 &= 1\cdot 1\cdot 2 + 1\cdot 1\cdot 3 + 1\cdot 2\cdot 3 + 1\cdot 2\cdot 3 = 17,\\
a_4 &= 1\cdot 1\cdot 1\cdot 2\cdot 3 = 6.
\end{aligned}$$

Таким образом,

$$f = x^4 - 7x^3 + 17x^2 - 17x + 6.$$

Кратность корня многочлена может быть истолкована и другим способом, отличным от данного выше определения, по крайней мере в случае $\operatorname{char} K = 0$. Для этого нужно определить дифференцирование многочленов.

Из правил дифференцирования функций действительной переменной следует, что производная многочлена есть также многочлен. Обозначим через D отображение алгебры $\mathbb{R}[x]$ в себя, сопоставляющее каждому многочлену его производную. Отображение D обладает следующими свойствами:

1) оно линейно;
2) $D(fg) = (Df)g + f(Dg)$;
3) $Dx = 1$.

Эти наблюдения позволяют определить дифференцирование многочленов над любым полем K, когда определение производной, даваемое в анализе, не имеет смысла.

Предложение 1. Существует единственное отображение $D\colon K[x] \to K[x]$, обладающее свойствами 1)–3).

Доказательство. Пусть D — такое отображение. Тогда

$$D1 = D(1\cdot 1) = (D1)\cdot 1 + 1\cdot (D1) = D1 + D1,$$

откуда $D1 = 0$. Докажем по индукции, что $Dx^n = nx^{n-1}$. При $n = 1$ это верно по предположению, а переход от $n-1$ к n делается выкладкой

$$\begin{aligned}
Dx^n = D(x^{n-1}x) = (Dx^{n-1})x + x^{n-1}(Dx) &=\\
= (n-1)x^{n-2}\cdot x + x^{n-1} &= nx^{n-1}.
\end{aligned}$$

Тем самым отображение D однозначно определено на базисных векторах $1, x, x^2, \ldots$, а значит, и на всем пространстве $K[x]$.

Обратно, построим линейное отображение $D\colon K[x] \to K[x]$, задав его на базисных векторах по формулам

$$D1 = 0, \quad Dx^n = nx^{n-1} \quad (n = 1, 2, \ldots),$$

и проверим, что оно обладает свойством 2). В силу линейности достаточно проверить это свойство для базисных векторов. Имеем:

$$D(x^m x^n) = Dx^{m+n} = (m+n)x^{m+n-1},$$
$$(Dx^m)x^n + x^m(Dx^n) = mx^{m-1}x^n + nx^m x^{n-1} = (m+n)x^{m+n-1}.$$

Многочлен Df называется производной многочлена f и обозначается, как обычно, через f'.

Сделав в многочлене $f \in K[x]$ замену $x = c + y$, где $c \in K$, мы можем представить его в виде многочлена (той же степени) от $y = x - c$ или, как говорят, разложить по степеням $x - c$:

$$f = b_0 + b_1(x-c) + b_2(x-c)^2 + \ldots + b_n(x-c)^n. \qquad (43)$$

Очевидно, что если c — корень многочлена f, то его кратность равна номеру первого отличного от нуля коэффициента этого разложения.

Предложение 2. Если $\operatorname{char} K = 0$, то коэффициенты разложения многочлена $f \in K[x]$ по степеням $x - c$ могут быть найдены по формулам

$$b_k = \frac{f^{(k)}(c)}{k!}.$$

(Здесь $f^{(k)}$, как обычно, обозначает k-ю производную многочлена f.)

Доказательство. Продифференцируем равенство (43) k раз и подставим $x = c$.

Таким образом,

$$f = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n.$$

Эта формула называется формулой Тейлора для многочленов.

Из формулы Тейлора и сделанного выше замечания следует

Теорема 4. При условии, что $\operatorname{char} K = 0$, кратность корня c многочлена $f \in K[x]$ равна наименьшему порядку производной многочлена f, не обращающейся в нуль в точке c.

Следствие. При том же условии всякий k-кратный корень многочлена f является $(k-1)$-кратным корнем его производной.

Замечание 3. В случае $\operatorname{char} K > 0$ кратность корня c может быть меньше указанного в теореме числа. Более того, такого числа может вообще не существовать. Так, например, если n — простое число, то первая, а значит, и все последующие производные многочлена $x^n \in \mathbb{Z}_n[x]$, имеющего n-кратный корень 0, являются нулевыми многочленами.

В случае $K = \mathbb{R}$ теорема 4 позволяет истолковать кратность геометрически. А именно, если кратность корня c многочлена $f \in K[x]$ равна k, то вблизи точки c многочлен f ведет себя как $b(x-c)^k$ $(b \neq 0)$. Это означает, что его график в точке c при $k = 1$ просто пересекает ось x, а при $k > 1$ имеет с ней касание k-го порядка. Кроме того, знак $f(x)$ при прохождении точки c при нечетном k меняется, а при четном k — не меняется (см. рис. 13).

Коэффициенты разложения (43), а, значит, и значения производных многочлена f в точке c (в случае $\operatorname{char} K = 0$), могут быть найдены последовательными делениями с остатком многочлена f на $x - c$. А именно, при первом делении получается остаток b_0 и неполное частное

$$f_1 = b_1 + b_2(x-c) + \ldots + b_n(x-c)^n;$$

при делении f_1 на $x - c$ получается остаток b_1 и т. д.

Пример 3. Разложим указанным способом по степеням $x-2$ многочлен

$$f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \ \in \ \mathbb{R}[x].$$

Последовательные деления с остатком на $x - 2$ будем проводить по схеме Горнера, используя строку результатов каждого

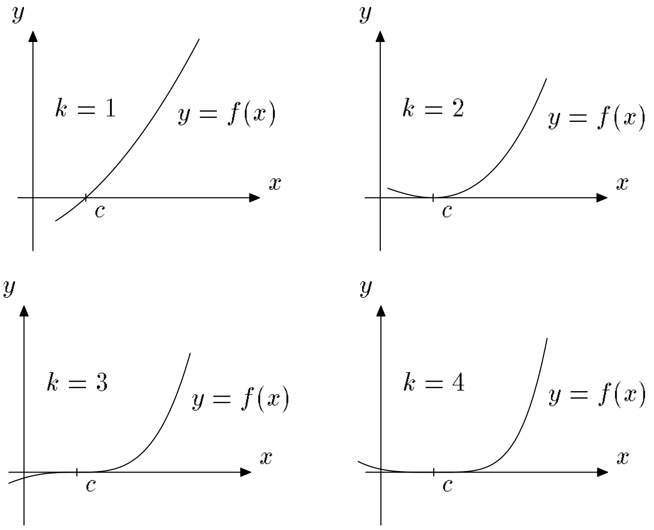

Рис. 13.

деления как строку исходных данных для следующего деления:

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0
	1	-1	-1	-2	0	
	1	1	1	0		
	1	3	7			
	1	5				
	1					

Таким образом,

$$f = 7(x-2)^3 + 5(x-2)^4 + (x-2)^5.$$

В частности, мы видим, что 2 — трехкратный корень многочлена f. Кроме того,

$$f^{\mathrm{III}}(2) = 3! \cdot 7 = 42,$$
$$f^{\mathrm{IV}}(2) = 4! \cdot 5 = 120,$$
$$f^{\mathrm{V}}(2) = 5! \cdot 1 = 120.$$

3.3. Основная теорема алгебры комплексных чисел

Оценка сверху числа корней многочлена, полученная в предыдущем параграфе, ничего не говорит о наличии хотя бы одного корня. И действительно, существуют многочлены положительной степени, не имеющие корней, например, многочлен x^2+1 над полем $\mathbb{R}$ действительных чисел. Именно это обстоятельство послужило поводом для построения поля $\mathbb{C}$ комплексных чисел. Если бы и над полем $\mathbb{C}$ существовали многочлены положительной степени, не имеющие корней, это привело бы к необходимости его дальнейшего расширения. Однако, к счастью, это не так. Это составляет содержание теоремы, которую называют основной теоремой алгебры комплексных чисел.

Теорема 1. Всякий многочлен положительной степени над полем комплексных чисел имеет корень.

Существует несколько доказательств этой теоремы. Любое из них включает элементы анализа, так как оно должно как-то использовать определение поля действительных чисел, которое не является чисто алгебраическим. Доказательство, приводимое ниже, является почти полностью аналитическим.

Нам понадобится понятие предела последовательности комплексных чисел. Перед тем как дать соответствующее определение, напомним, что модуль $|z|$ комплексного числа z есть длина вектора, изображающего это число. Отсюда следует, что $|z_1 - z_2|$ есть расстояние между точками, изображающими числа z_1 и z_2. Известные из геометрии неравенства, показывают (см. рис. 14 и 15), что

$$|z_1 + z_2| \leqslant |z_1| + |z_2|,$$
$$\big||z_1| - |z_2|\big| \leqslant |z_1 - z_2|.$$

(Равенства могут иметь место, когда соответствующий треугольник вырождается в отрезок.)

Определение. Последовательность комплексных чисел z_k $(k \in \mathbb{N})$ называется сходящейся к комплексному числу z (обозначение: $z_k \to z$), если $|z_k - z| \to 0$.

Лемма 1. Пусть $z_k = x_k + y_k i, \ \ z = x + yi$ $(x_k, y_k, x, y \in \mathbb{R})$. Тогда

$$z_k \to z \iff x_k \to x \text{ и } y_k \to y.$$

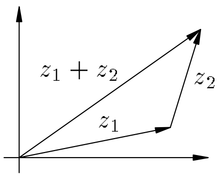

Рис. 14.

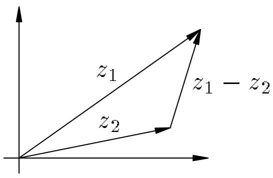

Рис. 15.

Д о к а з а т е л ь с т в о. Имеем (см. рис. 16)

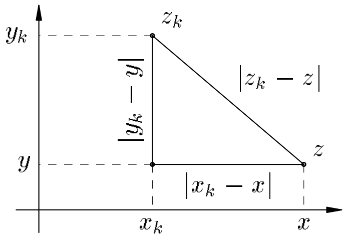

Рис. 16.

$$|z_k - z| = \sqrt{|x_k - x|^2 + |y_k - y|^2},$$

так что

$$x_k \to x \text{ и } y_k \to y \implies z_k \to z.$$

Обратная импликация вытекает из неравенств

$$|x_k - x| \leqslant |z_k - z|, \quad |y_k - y| \leqslant |z_k - z|.$$

Лемма 2. $z_k \to z$ и $w_k \to w \implies z_k + w_k \to z + w$ и $z_k w_k \to \to zw$.

Д о к а з а т е л ь с т в о. Представим комплексные числа z_k, w_k, z, w в алгебраической форме:

$$z_k = x_k + y_k i, \quad w_k = u_k + v_k i, \quad z = x + yi, \quad w = u + vi.$$

Тогда

$$z_k w_k = (x_k u_k - y_k v_k) + (x_k v_k + y_k u_k)i,$$
$$zw = (xu - yv) + (xv + yu)i.$$

По лемме 1

$$x_k \to x, \quad y_k \to y, \quad u_k \to u, \quad v_k \to v$$

и нам нужно доказать, что

$$x_k u_k - y_k v_k \to xu - yv, \quad x_k v_k + y_k u_k \to xv + yu;$$

но это следует из свойств пределов последовательностей действительных чисел, известных из анализа. Аналогично доказывается, что $z_k + w_k \to z + w$.

Следствие. Пусть $z_k \to z$ и $f \in \mathbb{C}[z]$ — любой многочлен. Тогда $f(z_k) \to f(z)$.

(Здесь мы допускаем вольность в обозначениях, обычную в анализе, когда значение переменной обозначается так же, как сама переменная.)

Лемма 3. $z_k \to z \implies |z_k| \to |z|$.

Доказательство. следует из того, что

$$\big||z_k| - |z|\big| \leqslant |z_k - z|.$$

Лемма 4 (о возрастании модуля многочлена).
Если $|z_k| \to \infty$ и $f \in \mathbb{C}[z]$ — многочлен положительной степени, то $|f(z_k)| \to \infty$.

Доказательство. Пусть

$$f = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n \quad (a_0 \neq 0);$$

тогда

$$|f(z_k)| = |z_k|^n \left| a_0 + \frac{a_1}{z_k} + \ldots + \frac{a_{n-1}}{z_k^{n-1}} + \frac{a_n}{z_k^n} \right| \geqslant$$
$$\geqslant |z_k|^n \left(|a_0| - \frac{|a_1|}{|z_k|} - \ldots - \frac{|a_{n-1}|}{|z_k|^{n-1}} - \frac{|a_n|}{|z_k|^n} \right).$$

Выражение, стоящее в скобках, стремится к $|a_0|$. Следовательно, все произведение и, тем более, $|f(z_k)|$ стремится к бесконечности.

Следующая лемма является ключевой для доказательства основной теоремы.

Лемма 5 (Даламбера). Пусть $f \in \mathbb{C}[z]$ — многочлен положительной степени и $f(z_0) \neq 0$. Тогда сколь угодно близко к z_0 можно найти такое z, что $|f(z)| < |f(z_0)|$.

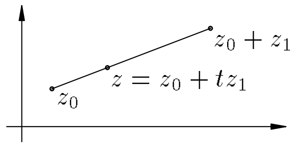

Рис. 17.

Доказательство. Разложим f по степеням $z - z_0$ и разделим на $f(z_0)$. Учитывая, что несколько первых коэффициентов разложения, следующих за свободным членом, могут оказаться равными нулю, запишем результат в виде

$$\frac{f(z)}{f(z_0)} = 1+c_p(z-z_0)^p+c_{p+1}(z-z_0)^{p+1}+\ldots+c_n(z-z_0)^n \quad (c_p \neq 0).$$

Нам нужно доказать существование такого z, что

$$\left|\frac{f(z)}{f(z_0)}\right| < 1.$$

Идея доказательства состоит в том, что если выбирать z достаточно близким к z_0, выполнение этого неравенства будет зависеть только от суммы первых двух членов предыдущего разложения.

Будем искать z в виде

$$z = z_0 + tz_1$$

(см. рис. 17), где $t \in (0,1)$, а z_1 — комплексное число, удовлетворяющее условию

$$c_p z_1^p = -1.$$

Имеем тогда:

$$\frac{f(z)}{f(z_0)} = 1 - t^p + t^{p+1}\varphi(t),$$

где φ — некоторый многочлен степени $n-p-1$ (с комплексными коэффициентами). Если C — максимум модулей коэффициентов многочлена φ, то

$$|\varphi(t)| \leqslant A = (n-p)C$$

и, следовательно,

$$\left|\frac{f(z)}{f(z_0)}\right| \leqslant 1 - t^p + At^{p+1} = 1 - t^p(1 - At) < 1$$

при $t < \dfrac{1}{A}$.

Доказательство теоремы. Пусть $f \in \mathbb{C}[z]$ — многочлен положительной степени. Положим

$$M = \inf_z |f(z)|.$$

Из определения нижней грани следует, что существует такая последовательность комплексных чисел z_k, что

$$|f(z_k)| \to M. \tag{44}$$

Если последовательность $|z_k|$ неограниченна, то из нее можно выбрать подпоследовательность, сходящуюся к бесконечности; но тогда в силу леммы 4 мы придем в противоречие с (44).

Таким образом, существует такое $C > 0$, что

$$|z_k| \leqslant C \quad \forall k.$$

Представим z_k в алгебраической форме:

$$z_k = x_k + y_k i.$$

Тогда

$$|x_k| \leqslant |z_k| \leqslant C, \quad |y_k| \leqslant |z_k| \leqslant C.$$

По теореме Больцано–Вейерштрасса из последовательности x_k можно выбрать сходящуюся подпоследовательность. Перейдя к этой подпоследовательности и изменив обозначения, можно считать, что

$$x_k \to x_0.$$

Аналогичным образом, перейдя еще раз к подпоследовательности, можно считать, что

$$y_k \to y_0.$$

Но тогда по лемме 1

$$z_k \to z_0 = x_0 + y_0 i$$

и, следовательно,

$$|f(z_k)| \to |f(z_0)| = M.$$

Если $M > 0$, то лемма Даламбера приводит нас в противоречие с определением M. Следовательно, $M = 0$, т. е. $f(z_0) = 0$.

Следствие 1. В алгебре $\mathbb{C}[x]$ всякий ненулевой многочлен разлагается на линейные множители.

В самом деле, в силу доказанной теоремы многочлен g в разложении (40) должен иметь нулевую степень, т. е. быть просто числом.

В силу теоремы 2.3 получаем отсюда

Следствие 2. Всякий многочлен степени n над $\mathbb{C}$ имеет n корней (с учетом кратностей).

3.4. Корни многочленов с действительными коэффициентами

Многочлен степени n с действительными коэффициентами может иметь $< n$ (в частности вообще не иметь) действительных корней, но, как и всякий многочлен с комплексными коэффициентами, он всегда имеет ровно n комплексных корней (с учетом кратностей). Мнимые корни многочлена с действительными коэффициентами обладают специальным свойством.

Теорема 1. Если c — мнимый корень многочлена $f \in \mathbb{R}[x]$, то $\overline{c}$ также является корнем этого многочлена, причем той же кратности, что и c.

Доказательство. Пусть

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad (a_0, a_1, \ldots, a_n \in \mathbb{R}).$$

Если $f(c) = 0$, то, поскольку комплексное сопряжение является автоморфизмом поля $\mathbb{C}$ (см. §1.5),

$$\begin{aligned} f(\overline{c}) &= a_0\overline{c}^n + a_1\overline{c}^{n-1} + \ldots + a_{n-1}\overline{c} + a_n = \\ &= \overline{a}_0\overline{c}^n + \overline{a}_1\overline{c}^{n-1} + \ldots + \overline{a}_{n-1}\overline{c} + \overline{a}_n = \overline{f(c)} = \overline{0} = 0, \end{aligned}$$

т. е. $\overline{c}$ — также корень многочлена f. Аналогично доказывается, что

$$f^{(k)}(c) = 0 \iff f^{(k)}(\overline{c}) = 0.$$

Следовательно, кратности корней c и $\overline{c}$ одинаковы.

Следствие 1. В алгебре $\mathbb{R}[x]$ всякий ненулевой многочлен разлагается на линейные множители и квадратные множители с отрицательным дискриминантом.

Доказательство. Заметим, что если c — мнимое число, то в силу (5) квадратный трехчлен

$$(x-c)(x-\overline{c}) = x^2 - (c+\overline{c})x + c\overline{c}$$

имеет действительные коэффициенты; его дискриминант, очевидно, отрицателен.

Пусть теперь

$$c_1, \ldots, c_s, c_{s+1}, \ldots, c_{s+t}, \overline{c}_{s+1}, \ldots, \overline{c}_{s+t}$$

— это все (различные) комплексные корни многочлена $f \in \mathbb{R}[x]$, причем

$$c_1, \ldots, c_s \in \mathbb{R}, \quad c_{s+1}, \ldots, c_{s+t} \notin \mathbb{R}.$$

Если кратность корня c_i равна k_i, то

$$f = a_0(x-c_1)^{k_1} \ldots (x-c_s)^{k_s}[(x-c_{s+1})(x-\overline{c}_{s+1})]^{k_{s+1}} \ldots \\ \ldots [(x-c_{s+t})(x-\overline{c}_{s+t})]^{k_{s+t}},$$

(где a_0 — старший коэффициент многочлена f). Перемножая линейные множители в квадратных скобках, получаем искомое разложение.

Пример 1.

$$\begin{aligned} & x^5 - 1 = \\ & = (x-1)\left(x - \left(\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}\right)\right)\left(x - \left(\cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5}\right)\right) \times \\ & \quad \times \left(x - \left(\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}\right)\right)\left(x - \left(\cos\frac{4\pi}{5} - i\sin\frac{4\pi}{5}\right)\right) = \\ & = (x-1)\left(x^2 - 2x\cos\frac{2\pi}{5} + 1\right)\left(x^2 - 2x\cos\frac{4\pi}{5} + 1\right) = \\ & = (x-1)\left(x^2 - \frac{\sqrt{5}-1}{2}x + 1\right)\left(x^2 + \frac{\sqrt{5}+1}{2}x + 1\right) \end{aligned}$$

(см. пример 2.1).

Пример 2. Для многочлена f из примера 2.3 разложение, о котором идет речь, имеет вид

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

Из теоремы 1 также следует, что любой многочлен $f \in \mathbb{R}[x]$ нечетной степени имеет хотя бы один действительный корень.

Впрочем, это легко доказать и по-другому. А именно, если старший коэффициент многочлена f положителен, то

$$\lim_{x\to+\infty} f(x) = +\infty, \qquad \lim_{x\to-\infty} f(x) = -\infty$$

и, значит, многочлен f принимает как положительные, так и отрицательные значения. По теореме о промежуточном значении непрерывной функции отсюда следует, что в некоторой точке он обращается в нуль.

Понятно, что представляет интерес определение точного числа действительных корней. Вычисляя значение многочлена в отдельных точках, мы можем обнаружить, что в каких-то точках a и b он принимает значения разных знаков. Отсюда следует, что в интервале (a, b) находится по меньшей мере один корень, а точнее — нечетное число корней (с учетом их кратностей). Таким образом мы можем оценить снизу число действительных корней.

Пример 3. Для многочлена

$$f = x^4 + x^2 - 4x + 1$$

находим

$$f(0) = 1 > 0, \quad f(1) = -1 < 0, \quad f(2) = 13 > 0.$$

Следовательно, f имеет корни в каждом из интервалов (0,1) и (1,2). Нетрудно показать, что $f(x) > 0$ при $x \leqslant 0$, а также при $x \geqslant 2$. Следовательно, все действительные корни многочлена f лежат в интервале (0,2). Однако, точное их число остается неясным, так как в одном из интервалов (0,1) и (1,2) может быть три корня.

Существуют методы, которые в принципе позволяют определить как общее число действительных корней любого многочлена с действительными коэффициентами, так и число его корней в любом промежутке числовой прямой. Однако их практическое применение связано с довольно большими вычислениями. Мы приведем здесь одну теорему, которая хотя и не всегда дает точный ответ, но зато не требует никаких вычислений. Она говорит не просто о числе всех действительных корней, но о числе положительных (или отрицательных) корней и является обобщением следующего тривиального утверждения: если все коэффициенты многочлена неотрицательны, то он не имеет положительных корней.

Для формулировки этой теоремы нам понадобится одно вспомогательное понятие.

Пусть имеется конечная последовательность действительных чисел

$$a_0, a_1, a_2, \ldots, a_n.$$

Говорят, что на k-м месте в этой последовательности имеется перемена знака, если $a_k \neq 0$ и знак a_k противоположен знаку последнего из предшествующих ему ненулевых членов последовательности. (Если a_k — первый из ненулевых членов последовательности, то на k-м месте перемены знака нет.)

Теорема 2 (Декарта). Число положительных корней (с учетом их кратностей) многочлена $f \in \mathbb{R}[x]$ не превосходит числа перемен знака в последовательности его коэффициентов и сравнимо с ним по модулю 2; если же все (комплексные) корни многочлена f действительны, то эти числа равны.

Обозначим через $N(f)$ число положительных корней многочлена f и через $L(f)$ — число перемен знака в последовательности его коэффициентов. Очевидно, что эти числа не изменяются при умножении f на -1; поэтому всегда можно считать, что старший коэффициент многочлена f положителен. Кроме того, если 0 является k-кратным корнем многочлена f, то при делении f на x^k эти числа также не изменяются; поэтому можно считать, что свободный член многочлена f отличен от нуля.

Лемма 1. $N(f) \equiv L(f) \pmod 2$.

Доказательство. Пусть

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad (a_0 > 0,\ a_n \neq 0).$$

Тогда $f(0) = a_n$ и $f(x) > 0$ при достаточно больших x. Когда мы двигаемся вправо по числовой прямой, то при прохождении каждого корня $f(x)$ меняет свой знак (а при прохождении k-кратного корня знак $f(x)$ умножается на $(-1)^k$, т.е. как бы меняется k раз). Поэтому $N(f)$ четно, если $a_n > 0$, и нечетно, если $a_n < 0$. То же самое можно сказать и об $L(f)$.

Лемма 2. $N(f) \leqslant N(f') + 1$.

Доказательство. По теореме Ролля между любыми двумя корнями многочлена f лежит корень его производной.

Кроме того, каждый k-кратный корень многочлена f является $(k-1)$-кратным корнем его производной (следствие теоремы 2.4). Отсюда получаем, что $N(f') \geqslant N(f) - 1$.

Лемма 3. $L(f') \leqslant L(f)$.

Доказательство очевидно.

Число отрицательных корней многочлена f равно числу положительных корней многочлена

$$\overline{f}(x) = f(-x).$$

Лемма 4. $L(f) + L(\overline{f}) \leqslant n = \deg f$.

Доказательство. Коэффициенты многочлена $\overline{f}$ получаются из коэффициентов многочлена f попеременным умножением на ± 1. Предположим вначале, что все коэффициенты $a_0, a_1, \ldots, a_n$ многочлена f отличны от нуля. Если тогда на k-м месте в последовательности $a_0, a_1, \ldots, a_n$ имеется перемена знака, то на том же месте в последовательности коэффициентов многочлена $\overline{f}$ перемены знака нет, и наоборот. Поэтому в этом случае $L(f) + L(\overline{f}) = n$. В общем случае, когда среди коэффициентов $a_0, a_1, \ldots, a_n$ могут быть нули, при их замене произвольными числами, отличными от нуля, числа $L(f)$ и $L(\overline{f})$ могут только увеличиться. Так как после этого их сумма по доказанному станет равной n, то $L(f) + L(\overline{f}) \leqslant n$.

Доказательство теоремы. Докажем неравенство $N(f) \leqslant L(f)$ индукцией по $\deg f$. Если $\deg f = 0$, то $N(f) = L(f) = 0$. Пусть $\deg f = n > 0$. Тогда $\deg f' = n - 1$. Пользуясь леммами 2 и 3 и предположением индукции, получаем:

$$N(f) \leqslant N(f') + 1 \leqslant L(f') + 1 \leqslant L(f) + 1.$$

Однако равенство $N(f) = L(f) + 1$ невозможно ввиду леммы 1. Следовательно, $N(f) \leqslant L(f)$.

Пусть теперь известно, что все корни многочлена f действительны. Мы можем считать, что 0 не является корнем. Имеем тогда в силу уже доказанного неравенства и леммы 4:

$$n = N(f) + N(\overline{f}) \leqslant L(f) + L(\overline{f}) \leqslant n,$$

откуда

$$N(f) = L(f), \quad N(\overline{f}) = L(\overline{f}).$$

Пример 4. Для многочлена f из примера 3 имеем $L(f) = 2$, так что $N(f) \leqslant 2$. Но мы уже установили, что $N(f) \geqslant 2$. Следовательно, $N(f) = 2$.

Пример 5. Многочлен $f = x^2 - x + 1$ не имеет положительных (и вообще действительных) корней, но $L(f) = 2$, так что в этом случае $N(f) < L(f)$.

Применяя теорему Декарта к многочлену

$$g(x) = f(c + x) = f(c) + \frac{f'(c)}{1!}x + \frac{f'(c)}{2!}x^2 + \ldots + \frac{f^{(n)}(c)}{n!}x^n,$$

мы получаем информацию о числе корней многочлена f в промежутке $(c, +\infty)$. В частности, если все коэффициенты многочлена g неотрицательны, то он не имеет положительных корней (тривиальной случай теоремы Декарта), а это означает, что все действительные корни многочлена f не превосходят c.

Пример 6. Найдем границы действительных корней многочлена

$$f = x^5 - 5x^3 - 10x^2 + 2.$$

Пользуясь схемой Горнера, вычислим $f(3)$:

$$\begin{array}{c|rrrrrr} & 1 & 0 & -5 & -10 & 0 & 2 \\ \hline 3 & 1 & 3 & 4 & 2 & 6 & 20 \end{array}$$

Мы видим, что $f(3) = 20 > 0$. Более того, все коэффициенты неполного частного оказались положительными. Поэтому все производные многочлена f при $x = 3$ также положительны (см. пример 2.3) и, значит, все его действительные корни меньше 3. Рассмотрим теперь многочлен

$$\overline{f}(x) = -f(-x) = x^5 - 5x^3 + 10x^2 - 2.$$

Вычислим значения многочлена $\overline{f}$ и его производных при $x = 1$:

$$\begin{array}{c|rrrrrr} & 1 & 0 & -5 & 10 & 0 & -2 \\ \hline 1 & 1 & 1 & -4 & 6 & 6 & 4 \\ & 1 & 2 & -2 & 4 & 10 & \\ & 1 & 3 & 1 & 5 & & \end{array}$$

Мы видим, что

$$\overline{f}(1) = 4 > 0, \quad \overline{f}'(1) = 10 > 0, \quad \overline{f}''(1) = 2 \cdot 5 > 0.$$

Значения следующих производных также положительны, поскольку последняя строка таблицы состоит только из положительных чисел. Следовательно, все действительные корни многочлена $\overline{f}$ меньше 1, а это означает, что все действительные корни многочлена f больше -1. Таким образом, все действительные корни многочлена f лежат в интервале $(-1, 3)$.

Задача. Исследовав производную многочлена $\overline{f}$, доказать, что многочлен f из предыдущего примера имеет только один отрицательный корень.

Обратимся теперь к вопросу о приближенном вычислении корней.

Если известно, что многочлен $f \in \mathbb{R}[x]$ имеет ровно один корень в каком-то интервале, то этот корень может быть в принципе найден с любой степенью точности с помощью вычисления значений многочлена в подходящим образом подобранных точках. Поясним это на следующем примере.

Пример 7. Как мы показали (см. пример 4), многочлен f из примера 3 имеет ровно один корень в интервале (1,2). Найдем значение этого корня с точностью до 0,01. Мы видели, что $f(1) < 0$. Вычисляя $f(x)$ при $x = 1{,}1$, 1,2, 1,3, мы обнаруживаем, что

$$f(1{,}2) < 0, \quad f(1{,}3) > 0.$$

Следовательно, корень лежит в интервале $(1{,}2; 1{,}3)$. Вычисляя $f(x)$ при $x = 1{,}21$, 1,22, 1,23, 1,24, 1,25, находим, что

$$f(1{,}24) < 0, \quad f(1{,}25) > 0.$$

Следовательно, искомый корень лежит в интервале $(1{,}24; 1{,}25)$.

Конечно, существуют гораздо более совершенные методы приближенного вычисления корней. Они применимы к алгебраическим уравнениям любой степени, а некоторые из них — и к трансцендентным уравнениям. Однако изложение этих методов выходит за рамки нашего курса: они относятся скорее к вычислительной математике, чем к алгебре.

Замечание. Если многочлен имеет кратный корень, но его коэффициенты даны нам лишь приближенно, хотя бы и с любой степенью точности, то мы в принципе не можем доказать наличие этого кратного корня, так как при сколь угодно малом изменении коэффициентов многочлена он может либо рассыпаться на простые корни, либо вообще перестать существовать. Так, в случае двукратного корня мы никогда не сможем сделать выбор между ситуациями, изображенными на рис. 18а, а в случае трехкратного — между ситуациями, изображенными на рис. 18б.

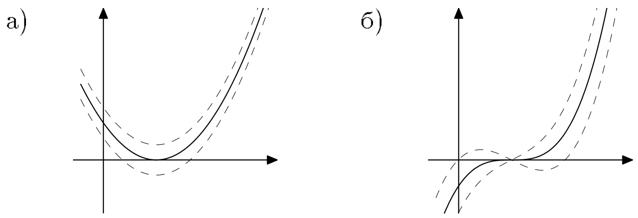

Рис. 18.

3.5. Теория делимости в евклидовых кольцах

Разложение многочленов над $\mathbb{C}$ на линейные множители и многочленов над $\mathbb{R}$ на линейные и квадратные множители аналогично разложению целых чисел на простые множители. Для многочленов над произвольным полем также имеется подобное разложение, но его множители могут иметь любую степень. Задачу отыскания такого разложения можно рассматривать как обобщение задачи отыскания корней многочлена (которой она равносильна в случае многочленов над $\mathbb{C}$). Она не имеет общего решения, пригодного для любого поля. В этом параграфе мы докажем единственность указанного разложения. Одновременно мы докажем единственность разложения целого числа на простые множители — факт широко известный, но не доказываемый в средней школе.

Для того чтобы охватить единым рассуждением оба случая, введем некоторые общие понятия.

Определение 1. Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется целостным кольцом (или областью целостности).

Так, кольцо $\mathbb{Z}$ целых чисел и кольцо $K[x]$ многочленов над любым полем K являются целостными кольцами. Более того, кольцо многочленов над любым целостным кольцом также является целостным кольцом (см. замечание 1.3).

Пусть A — целостное кольцо. Говорят, что элемент $a \in A$

делится на элемент $b \in A$ (обозначение: $a \,\vdots\, b$) или, иначе, что b делит a (обозначение: $b \mid a$), если существует такой элемент $q \in A$, что $a = qb$. Элементы a и b называются ассоциированными (обозначение: $a \sim b$), если выполняется любое из следующих эквивалентных условий:

1) $b \mid a$ и $a \mid b$;

2) $a = cb$, где c — обратимый элемент.

В следующем определении аксиоматизируется то общее, что есть у кольца многочленов над полем и кольца целых чисел — возможность деления с остатком.

Определение 2. Целостное кольцо A, не являющееся полем, называется евклидовым, если существует функция

$$N\colon A \setminus \{0\} \to \mathbb{Z}_+$$

(называемая нормой), удовлетворяющая следующим условиям:

1) $N(ab) \geqslant N(a)$, причем равенство имеет место только тогда, когда элемент b обратим;

2) для любых $a, b \in A$, где $b \neq 0$, существуют такие $q, r \in A$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Замечание 1. Условие 2) означает возможность «деления с остатком». Его единственности (т. е. однозначной определенности пары (q, r)) не требуется.

Замечание 2. Вторая часть условия 1) на самом деле может быть выведена из остальных условий. В самом деле, пусть элемент b необратим. Тогда a не делится на ab. Разделим a на ab с остатком:

$$a = q(ab) + r.$$

Так как $r = a(1 - qb)$, то

$$N(a) \leqslant N(r) < N(ab).$$

Основными для нас примерами евклидовых колец являются кольцо $\mathbb{Z}$ целых чисел и кольцо $K[x]$ многочленов над полем K. В качестве нормы в первом случае можно взять модуль целого числа, во втором — степень многочлена.

Существуют и другие евклидовы кольца.

Пример. Комплексные числа вида $c = a + bi$, где $a, b \in \mathbb{Z}$, называются целыми гауссовыми числами. Они образуют подкольцо в $\mathbb{C}$, обозначаемое через $\mathbb{Z}[i]$. Кольцо $\mathbb{Z}[i]$ является евклидовым относительно нормы

$$N(c) = |c|^2 = a^2 + b^2.$$

В самом деле, очевидно, что

$$N(cd) = N(c)N(d)$$

и, поскольку $N(1) = 1$, обратимые элементы кольца $\mathbb{Z}[i]$ — это элементы с нормой 1, т.е. ± 1 и $\pm i$. Отсюда следует, что выполнено условие 1) в определении евклидова кольца. Докажем возможность деления с остатком. Пусть $c, d \in \mathbb{Z}[i]$, $d \neq 0$. Рассмотрим целое гауссово число q, ближайшее к $\dfrac{c}{d}$. Легко видеть, что $\left|\dfrac{c}{d} - q\right| \leqslant \dfrac{1}{\sqrt{2}}$ (см. рис. 19). Положим $r = c - qd$. Тогда $c = qd + r$ и

$$N(r) = |c - qd|^2 = \left|\frac{c}{d} - q\right|^2 |d|^2 \leqslant \frac{1}{2}N(d) < N(d).$$

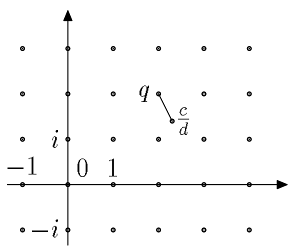

Рис. 19.

Определение 3. Наибольшим общим делителем элементов a и b целостного кольца называется их общий делитель, делящийся на все их общие делители. Он обозначается через (a, b) или НОД(a, b).

Наибольший общий делитель, если он существует, определен однозначно с точностью до ассоциированности. Однако он может не существовать. Например, элементы 2 и x в кольце $\mathbb{Z}[x]$ не имеют наибольшего общего делителя.

Теорема 1. В евклидовом кольце для любых элементов a, b существует наибольший общий делитель d и он может быть представлен в виде $d = au + bv$, где u, v — какие-то элементы кольца.

Доказательство. Если $b = 0$, то $d = a = a \cdot 1 + b \cdot 0$. Если a делится на b, то $d = b = a \cdot 0 + b \cdot 1$. В противном случае разделим с остатком a на b, затем b на полученный остаток, затем первый остаток на второй остаток и т. д. Так как нормы остатков убывают, то в конце концов деление произойдет без остатка. Получим цепочку равенств:

$$\begin{aligned}
&a = q_1 b + r_1,\\
&b = q_2 r_1 + r_2,\\
&r_1 = q_3 r_2 + r_3,\\
&\dots\dots\dots\dots\\
&r_{n-2} = q_n r_{n-1} + r_n,\\
&r_{n-1} = q_{n+1} r_n.
\end{aligned}$$

Докажем, что последний ненулевой остаток r_n и есть наибольший общий делитель элементов a и b.

Двигаясь по выписанной цепочке равенств снизу вверх, получаем последовательно

$$r_n \mid r_{n-1}, \quad r_n \mid r_{n-2}, \quad \dots, \quad r_n \mid r_1, \quad r_n \mid b, \quad r_n \mid a.$$

Таким образом, r_n — общий делитель элементов a и b.

Двигаясь по той же цепочке равенств сверху вниз, получаем последовательно

$$\begin{aligned}
&r_1 = au_1 + bv_1,\\
&r_2 = au_2 + bv_2,\\
&r_3 = au_3 + bv_3,\\
&\dots\dots\dots\dots\\
&r_n = au_n + bv_n,
\end{aligned}$$

где $u_i, v_i \quad (i = 1, \dots, n)$ — какие-то элементы кольца (например, $u_1 = 1, \ v_1 = -q_1$). Таким образом, r_n можно представить в виде $r_n = au + bv$. Отсюда, в свою очередь, следует, что r_n делится на любой общий делитель элементов a и b.

Процедура нахождения наибольшего общего делителя, использованная в этом доказательстве, называется алгоритмом Евклида. Элементы $a, b \in A$ называются взаимно простыми, если $(a, b) = 1$. В этом случае согласно доказанной теореме существуют такие $u, v \in A$, что

$$au + bv = 1.$$

Перейдем теперь к вопросу о разложении на простые множители.

Определение 4. Необратимый ненулевой элемент p целостного кольца называется простым, если он не может быть представлен в виде $p = ab$, где a и b — необратимые элементы.

Иначе говоря, элемент p простой, если всякий его делитель ассоциирован либо с 1, либо с p. Простые элементы кольца $\mathbb{Z}$ в этом смысле — это числа вида $\pm p$, где p — простое число.

Простые элементы кольца $K[x]$, где K — поле, по традиции называются неприводимыми многочленами. Таким образом, неприводимый многочлен — это такой многочлен положительной степени, который не может быть разложен в произведение двух многочленов положительной степени.

Очевидно, что всякий многочлен первой степени неприводим. Из основной теоремы алгебры комплексных чисел следует, что неприводимые многочлены над $\mathbb{C}$ — это только многочлены первой степени, а из теоремы 4.1 — что неприводимые многочлены над $\mathbb{R}$ — это многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. В следующем параграфе мы обсудим вопрос о неприводимых многочленах над $\mathbb{Q}$ и, в частности, увидим, что они могут иметь любую степень.

Пусть теперь A — любое евклидово кольцо.

Лемма 1. Если простой элемент p кольца A делит произведение $a_1 a_2 \ldots a_n$, то p делит хотя бы один из сомножителей $a_1, a_2, \ldots, a_n$.

Доказательство. Докажем это утверждение индукцией по n. При $n = 2$ предположим, что p не делит a_1. Тогда $(p, a_1) = 1$ и, значит, существуют такие $u, v \in A$, что $pu + a_1 v = 1$. Умножая это равенство на a_2, получаем

$$pua_2 + a_1 a_2 v = a_2,$$

откуда следует, что p делит a_2.

При $n > 2$ представим произведение $a_1 a_2 \ldots a_n$ в виде $a_1(a_2 \ldots a_n)$. По доказанному $p \mid a_1$ или $p \mid a_2 \ldots a_n$. Во втором случае по предположению индукции $p \mid a_i$, где i — один из индексов $2, \ldots, n$.

Теорема 2. В евклидовом кольце всякий необратимый ненулевой элемент может быть разложен на простые множители, причем это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы.

Замечание 3. Говоря о разложении на простые множители, мы не исключаем разложения, состоящего только из одного множителя.

Доказательство. Назовем необратимый ненулевой элемент $a \in A$ хорошим, если он может быть разложен на простые множители. Предположим, что существуют плохие элементы. Выберем из них элемент с наименьшей нормой. Пусть это будет элемент a. Он не может быть простым. Следовательно, $a = bc$, где b и c — необратимые элементы. Имеем $N(b) < N(a)$ и $N(c) < N(a)$ и, значит, b и c — хорошие элементы; но тогда, очевидно, и a — хороший элемент, что противоречит нашему предположению. Таким образом, всякий необратимый ненулевой элемент кольца A может быть разложен на простые множители.

Докажем теперь индукцией по n, что если

$$a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m, \tag{45}$$

где p_i, q_j — простые элементы, то $m = n$ и, после подходящей перенумерации множителей, $p_i \sim q_i$ при $i = 1, 2, \ldots, n$.

При $n = 1$ это утверждение очевидно. При $n > 1$ имеем $p_1 \mid q_1q_2 \ldots q_m$ и по лемме 1 существует такой номер i, что $p_1 \mid q_i$. Тогда $p_1 \sim q_i$. Можно считать, что $i = 1$ и $p_1 = q_1$. Сокращая равенство (45) на p_1, получаем:

$$p_2 \ldots p_n = q_2 \ldots q_m.$$

По предположению индукции отсюда следует, что $m = n$ и, после подходящей перенумерации, $p_i \sim q_i$ при $i = 2, \ldots, n$. Тем самым утверждение доказано.

Следствие 1. Пусть $a = p_1^{k_1} \ldots p_s^{k_s}$ — разложение элемента $a \in A$ на простые множители, причем $p_i \not\sim p_j$ при $i \neq j$. Тогда всякий делитель d элемента a имеет вид

$$d = cp_1^{l_1} \ldots p_s^{l_s},$$

где $0 \leqslant l_i \leqslant k_i$ $(i = 1, \ldots, s)$, а c — обратимый элемент.

Доказательство. Пусть $a = qd$. Разложим q и d на простые множители. Перемножив эти разложения, мы получим разложение a на простые множители. Сравнив его с данным разложением, получим требуемый результат.

Задача 1. Доказать, что в евклидовом кольце
а) $b \mid a,\ \ c \mid a$ и $(b, c) = 1 \implies bc \mid a$;
б) $c \mid ab$ и $(b, c) = 1 \implies c \mid a$.

Задача 2. Наименьшим общим кратным элементов a и b целостного кольца называется их общее кратное (т. е. элемент, делящийся на a и на b), делящее все их общие кратные. Оно обозначается через $[a, b]$ или НОК(a, b). Доказать, что в евклидовом кольце для любых элементов a, b существует наименьшее общее кратное $[a, b]$, причем

$$(a, b)[a, b] \sim ab.$$

Задача 3. В кольце $\mathbb{Z}[i]$ (см. пример 1) разложить на простые множители числа 2, 3 и 5 и подумать, в чем принципиальная разница между этими тремя случаями.

Известно, что простых чисел бесконечно много. Напомним рассуждение, которое это доказывает. Предположим, что $p_1, p_2, \ldots, p_n$ — это все простые числа. Тогда число $p_1, p_2, \ldots, p_n + 1$ не делится ни на одно из них, что очевидно, невозможно. Точно такое же рассуждение показывает бесконечность числа нормированных неприводимых многочленов над любым полем K. Если поле K бесконечно, то этот результат не представляет интереса, так как в этом случае имеется бесконечно много нормированных многочленов первой степени. Однако если поле K конечно, то этот результат означает, что имеются неприводимые многочлены сколь угодно высокой степени. На самом деле в этом случае имеются неприводимые многочлены любой степени.

Задача 4. Перечислить неприводимые многочлены степеней $\leqslant 4$ над полем $\mathbb{Z}_2$ и доказать, что существует ровно 6 неприводимых многочленов степени 5.

3.6. Многочлены с рациональными коэффициентами

Из однозначности разложения целого числа на простые множители вытекает

Теорема 1. Если многочлен

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

имеет рациональный корень $\frac{u}{v}$, где $u, v \in \mathbb{Z}$, $(u, v) = 1$, то $u \mid a_n$ и $v \mid a_0$.

Доказательство. Имеем:

$$0 = v^n f\left(\frac{u}{v}\right) = a_0 u^n + a_1 u^{n-1} v + \ldots + a_{n-1} u v^{n-1} + a_n v^n.$$

Все слагаемые в правой части, кроме последнего, делятся на u. Следовательно, и последнее слагаемое должно делиться на u. Но так как u и v взаимно просты, то a_n делится на u (см. задачу 5.1б). Аналогично доказывается, что a_0 делится на v.

Следствие. Если нормированный многочлен с целыми коэффициентами имеет рациональный корень, то этот корень — целый.

Очевидно, что всякий многочлен с рациональными коэффициентами пропорционален многочлену с целыми коэффициентами. Поэтому теорема 1 позволяет путем конечного числа испытаний найти все рациональные корни любого многочлена с рациональными коэффициентами. Конечно, таких корней, как правило, нет. Приводимый ниже специально подобранный пример относится к разряду тех исключений, которые подтверждают правило.

Пример 1. Рациональными корнями многочлена

$$f = 2x^4 - 7x^3 + 4x^2 - 2x - 3$$

согласно теореме 1 могут быть только

$$\pm\frac{1}{2},\ \pm 1,\ \pm\frac{3}{2},\ \pm 3.$$

Испытания дают 2 корня:

$$x_1 = 3, \quad x_2 = -\frac{1}{2}.$$

Следующая теорема может рассматриваться как обобщение теоремы 1.

Теорема 2 (Лемма Гаусса). Если многочлен с целыми коэффициентами разлагается в произведение двух многочленов с рациональными коэффициентами, то он разлагается в произведение двух пропорциональных им многочленов с целыми коэффициентами.

Иначе говоря, если $f \in \mathbb{Z}[x]$ и $f = gh$, где $g, h \in \mathbb{Q}[x]$, то существует такое $\lambda \in \mathbb{Q}^*$, что λg, $\lambda^{-1}h \in \mathbb{Z}[x]$.

Перед тем, как доказывать эту теорему, введем некоторые вспомогательные понятия.

Многочлен $f \in \mathbb{Z}[x]$ называется примитивным, если его коэффициенты взаимно просты в совокупности, т.е. не имеют общего простого делителя. Если такой делитель есть, то его можно вынести за скобки. Поэтому всякий многочлен с целыми коэффициентами, а значит, и всякий многочлен с рациональными коэффициентами, пропорционален некоторому примитивному многочлену (определенному однозначно с точностью до умножения на ± 1).

Пусть p — какое-нибудь простое число. Определим редукцию по модулю p многочлена

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

как многочлен

$$[f]_p = [a_0]_p x^n + [a_1]_p x^{n-1} + \ldots + [a_{n-1}]_p x + [a_n]_p \in \mathbb{Z}_p[x],$$

коэффициенты которого суть вычеты по модулю p коэффициентов многочлена f. Из определения операций над вычетами следует, что

$$[f+g]_p = [f]_p + [g]_p,$$
$$[fg]_p = [f]_p[g]_p$$

для любых многочленов $f, g \in \mathbb{Z}[x]$.

Доказательство теоремы. Пусть $f \in \mathbb{Z}[x]$ и $f = gh$, где $g, h \in \mathbb{Q}[x]$. Согласно предыдущему многочлены g и h пропорциональны каким-то примитивным многочленам g_1 и h_1. Имеем:

$$f = \mu g_1 h_1, \quad \mu \in \mathbb{Q}.$$

Пусть $\mu = \dfrac{u}{v}$, где $u, v \in \mathbb{Z}$, $(u, v) = 1$. Докажем, что $v = \pm 1$, откуда будет следовать утверждение теоремы. Если это не так, то пусть p — какой-нибудь простой делитель числа v. В равенстве

$$vf = ug_1h_1$$

сделаем редукцию по модулю p. Мы получим

$$0 = [u]_p[g_1]_p[h_1]_p.$$

Однако $[u]_p \neq 0$, так как u и v по предположению взаимно просты. В то же время $[g_1]_p \neq 0$ и $[h_1]_p \neq 0$, так как g_1 и h_1 — примитивные многочлены и, следовательно, все их коэффициенты не могут делиться на p. Это противоречит отсутствию делителей нуля в кольце $\mathbb{Z}_p[x]$.

Следствие. Если многочлен $f \in \mathbb{Z}[x]$ допускает разложение в произведение двух многочленов положительной степени в кольце $\mathbb{Q}[x]$, то он допускает такое разложение и в кольце $\mathbb{Z}[x]$.

Это существенно облегчает доказательство неприводимости многочленов над $\mathbb{Q}$.

Пример 2. Пусть p — простое число. Докажем неприводимость над $\mathbb{Q}$ «многочлена деления круга на p частей»

$$f = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}.$$

(Комплексными корнями этого многочлена являются все нетривиальные корни p-й степени из 1, которые вместе с 1 делят окружность $|z| = 1$ на p равных частей.) Как следует из формулы бинома Ньютона (см. §1.6), в кольце $\mathbb{Z}_p[x]$ имеет место равенство

$$x^p - 1 = (x - 1)^p,$$

так что

$$[f]_p = (x - 1)^{p-1}.$$

Если $f = gh$, где $g, h \in \mathbb{Z}[x]$ — многочлены положительной степени, то $[f]_p = [g]_p[h]_p$ и, значит,

$$[g]_p = (x - 1)^k, \quad [h]_p = (x - 1)^l \quad (k, l > 0,\ k + l = p - 1).$$

Следовательно,

$$[g(1)]_p = [g]_p(1) = 0, \quad [h(1)]_p = [h]_p(1) = 0,$$

т. е. $g(1)$ и $h(1)$ делятся на p. Но тогда $f(1) = g(1)h(1)$ делится на p^2, что не соответствует действительности, ибо $f(1) = p$.

Имеется способ, принадлежащий Кронекеру, который в принципе позволяет для любого многочлена с целыми коэффициентами определить, приводим он или неприводим над $\mathbb{Q}$. Он основывается на следующих соображениях.

Пусть $f \in \mathbb{Z}[x]$ — многочлен степени n, не имеющий целых корней. Предположим, что он разлагается в $\mathbb{Z}[x]$ в произведение двух многочленов положительной степени:

$$f = gh.$$

Тогда степень одного из них, скажем, g, не превосходит $m = \left[\frac{n}{2}\right]$.

Будем придавать x различные целые значения $x_0, x_1, \ldots, x_m$. Из равенств

$$f(x_i) = g(x_i)h(x_i)$$

следует, что $g(x_i) \mid f(x_i)$ при $i = 0, 1, \ldots, m$. Многочлен g однозначно определяется своими значениями в точках $x_0, x_1, \ldots, x_m$. Выбирая всевозможные наборы делителей $d_0, d_1, \ldots, d_m$ целых чисел $f(x_0), f(x_1), \ldots, f(x_m)$ и находя для каждого из них интерполяционный многочлен степени $\leqslant m$, принимающий в точках $x_0, x_1, \ldots, x_m$ значения $d_0, d_1, \ldots, d_m$, можно найти всех кандидатов на роль g (их будет конечное число). Тех из них, которые имеют дробные коэффициенты, следует сразу отбросить. Испытав оставшиеся многочлены, можно определить, имеются ли среди них делители многочлена f, в зависимости от чего и будет решен вопрос о приводимости последнего.

3.7. Многочлены от нескольких переменных

Функция действительных переменных $x_1, x_2, \ldots, x_n$ называется многочленом, если она может быть представлена в виде

$$f(x_1, x_2, \ldots, x_n) = \sum_{k_1, k_2, \ldots, k_n} a_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}, \qquad (46)$$

где суммирование происходит по конечному числу наборов $(k_1, k_2, \ldots, k_n)$ неотрицательных целых чисел. (Формально можно считать, что суммирование происходит по всем таким наборам, но лишь конечное число коэффициентов $a_{k_1 k_2 \ldots k_n}$ отлично от нуля.) Многочлены образуют подалгебру в алгебре всех функций от $x_1, x_2, \ldots, x_n$. Она называется алгеброй многочленов от $x_1, x_2, \ldots, x_n$ над $\mathbb{R}$ и обозначается $\mathbb{R}[x_1, x_2, \ldots, x_n]$.

Можно показать (см. теорему 6.1), что представление многочлена над $\mathbb{R}$ в виде (46) однозначно, т. е. коэффициенты многочлена определяются его значениями.

При определении алгебры многочленов от n переменных над любым полем K возникает такая же трудность, как и в случае одной переменной. Это приводит к необходимости формального определения, которое может быть дано, например, следующим образом.

Рассмотрим бесконечномерную алгебру над K с базисом

$$\{ e_{k_1 k_2 \ldots k_n} : k_1, k_2, \ldots, k_n \in \mathbb{Z}_+ \}$$

и таблицей умножения

$$e_{k_1 k_2 \ldots k_n} e_{l_1 l_2 \ldots l_n} = e_{k_1+l_1, k_2+l_2, \ldots, k_n+l_n}.$$

Очевидно, что эта алгебра коммутативна и ассоциативна и что элемент $e_{00\ldots 0}$ является ее единицей. Она называется алгеброй многочленов над K и обозначается через $K[x_1, x_2, \ldots, x_n]$.

Условимся отождествлять элементы вида $ae_{00\ldots 0}$ $(a \in K)$ с соответствующими элементами поля K и введем обозначения

$$\begin{aligned} e_{10\ldots 0} &= x_1, \\ e_{01\ldots 0} &= x_2, \\ &\ldots\ldots\ldots \\ e_{00\ldots 1} &= x_n. \end{aligned}$$

Тогда

$$e_{k_1 k_2 \ldots k_n} = x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

и любой элемент

$$\sum_{k_1, k_2, \ldots, k_n} a_{k_1 k_2 \ldots k_n} e_{k_1 k_2 \ldots k_n} \in K[x_1, x_2, \ldots, x_n]$$

записывается в обычном виде (46).

Многочлен (46) называется однородным степени d, если

$$a_{k_1 k_2 \ldots k_n} = 0 \text{ при } k_1 + k_2 + \ldots + k_n \neq d.$$

Однородные многочлены заданной степени d образуют конечномерное подпространство, так как имеется лишь конечное число наборов $(k_1, k_2, \ldots, k_n)$ целых неотрицательных чисел, удовлетворяющих условию

$$k_1 + k_2 + \ldots + k_n = d.$$

Задача. Доказать, что размерность пространства однородных многочленов степени d от n переменных равна

$$C_n^d = \frac{n(n+1)\dots(n+d-1)}{d!}$$

(число сочетаний с повторениями из n по d).

Любой многочлен однозначно представляется в виде суммы однородных многочленов степеней $0, 1, 2, \dots$, называемых его однородными компонентами. (Лишь конечное число из них отлично от нуля.)

Степенью (по совокупности переменных) ненулевого многочлена называется максимальная из степеней его ненулевых членов или, что то же, максимальная из степеней его ненулевых однородных компонент. Степень многочлена f обозначается через $\deg f$. Справедливы следующие соотношения:

$$\deg(f+g) \leqslant \deg f + \deg g,$$
$$\deg(fg) = \deg f + \deg g.$$

Первое из них очевидно, второе мы докажем чуть позже.

С другой стороны, каждый многочлен $f \in K[x_1, x_2, \dots, x_n]$ однозначно представляется в виде

$$f(x_1, x_2, \dots, x_n) = \sum_{k=0}^{\infty} f_k(x_2, \dots, x_n) x_1^k, \qquad (47)$$

где $f_0, f_1, f_2, \dots$ — какие-то многочлены от $x_2, \dots, x_n$, лишь конечное число которых отлично от нуля. Наибольший из номеров многочленов f_k, отличных от нуля, называется степенью многочлена f по x_1 и обозначается через $\deg_{x_1} f$.

Пользуясь представлением (47), можно рассматривать кольцо $K[x_1, x_2, \dots, x_n]$ как кольцо многочленов от x_1 с коэффициентами из $K[x_2, \dots, x_n]$:

$$K[x_1, x_2, \dots, x_n] = K[x_2, \dots, x_n][x_1]. \qquad (48)$$

Замечание. Мы говорим о кольцах, а не об алгебрах, так как $K[x_1, x_2, \dots, x_n]$ по определению есть алгебра над K, в то время как $K[x_2, \dots, x_n][x_1]$ есть алгебра над $K[x_2, \dots, x_n]$. Однако если рассматривать $K[x_2, \dots, x_n][x_1]$ как алгебру над K (пользуясь тем, что $K[x_2, \dots, x_n] \supset K$), то можно говорить о равенстве алгебр.

Предложение 1. Алгебра $K[x_1, x_2, \ldots, x_n]$ не имеет делителей нуля.

Доказательство. В §3.1 было фактически доказано (см. замечание 1.3), что кольцо многочленов от одной переменной над целостным кольцом также является целостным кольцом (в частности, не имеет делителей нуля). Поэтому равенство (48) позволяет доказать наше утверждение индуктивным путем, начиная с поля K.

Теперь мы в состоянии доказать соотношение (48). Разложим многочлены f и g на однородные компоненты:

$$f = f_0 + f_1 + \ldots + f_d \quad (\deg f_k = k,\ f_d \neq 0),$$
$$g = g_0 + g_1 + \ldots + g_e \quad (\deg g_k = k,\ g_e \neq 0).$$

Ясно, что при их перемножении не появится членов степени $> d + e$, а сумма всех членов степени $d + e$ будет равна $f_d g_e$. По доказанному $f_d g_e \neq 0$. Следовательно,

$$\deg fg = d + e = \deg f + \deg g.$$

Как и в случае $n = 1$, всякий многочлен от n переменных над полем K определяет функцию на K^n со значениями в K.

Теорема 1. Если поле K бесконечно, то разные многочлены от n переменных над K определяют разные функции.

Доказательство. Как и в случае многочленов от одной переменной (см. доказательство теоремы 1.1), достаточно доказать, что ненулевой многочлен определяет ненулевую функцию. Докажем это индукцией по n.

При $n = 1$ это составляет содержание теоремы 2.1. Предположим теперь, что многочлен $f \in K[x_1, x_2, \ldots, x_n]$ $(n > 1)$ определяет нулевую функцию. Представим его в виде (47) и придадим какие-то значения переменным $x_2, \ldots, x_n$. Мы получим многочлен от одной переменной x_1 с коэффициентами из K, обращающийся в нуль при любом значении x_1. По теореме 1.1 все его коэффициенты равны нулю. Таким образом, каждый из многочленов $f_k \in K[x_2, \ldots, x_n]$ обращается в нуль при любых значениях $x_2, \ldots, x_n$, т. е. определяет нулевую функцию. По предположению индукции отсюда следует, что $f_k = 0$ при любом k; но тогда и $f = 0$.

При $n > 1$ члены многочлена от n переменных нельзя, вообще говоря однозначно упорядочить по их степеням, поскольку может быть несколько членов одинаковой степени. Между тем какое-то упорядочение иногда бывает полезно. В этих случаях обычно используют лексикографическое упорядочение (т. е. подобное упорядочению слов в словаре), при котором вначале сравниваются показатели при x_1, затем, если они равны, — показатели при x_2 и т. д. Если одночлен u лексикографически старше одночлена v, то мы будем писать $u \succ v$. Согласно определению это означает, что первая из переменных, которая входит в u и v с разными показателями, входит в u с бóльшим показателем, чем в v.

Предложение 2. Отношение лексикографического упорядочения одночленов обладает следующими свойствами:

1) если $u \succ v$ и $v \succ w$, то $u \succ w$ (транзитивность);
2) если $u \succ v$, то $uw \succ vw$ для любого одночлена w;
3) если $u_1 \succ v_1$ и $u_2 \succ v_2$, то $u_1u_2 \succ v_1v_2$.

Первое из этих свойств, собственно, и дает основание называть отношение «$\succ$» упорядочением.

Доказательство. 1) Пусть первая переменная, которая не входит во все одночлены u, v, w с одним и тем же показателем, входит в них с показателями k, l, m соответственно. Тогда

$$k \geqslant l \geqslant m,$$

причем хотя бы в одном из двух случаев имеет место строгое неравенство. Следовательно, $k > m$, а это и означает, что $u \succ w$.

2) При умножении на w к показателям, с которыми каждая из переменных входит в u и v, добавляется одно и то же число, и знак неравенства (или равенства) между этими показателями не меняется, а только эти неравенства и имеют значение при сравнении одночленов.

3) Пользуясь предыдущим свойством, получаем:

$$u_1u_2 \succ v_1u_2 \succ v_1v_2.$$

Пример. Следующий многочлен расположен по лексикографическому убыванию членов:

$$x_1^2x_2 + x_1x_2^2x_3 + 2x_1x_3^2 + x_2x_3^3 - x_2x_3^2 + 3.$$

Обратите внимание на то, что член $x_1x_2^2x_3$ лексикографически младше $x_1^2x_2$, хотя его степень больше.

Среди ненулевых членов любого ненулевого многочлена $f \in K[x_1, x_2, \ldots, x_n]$ имеется единственный, который лексикографически старше всех остальных. Он называется старшим членом многочлена f.

Предложение 3. Старший член произведения ненулевых многочленов равен произведению их старших членов.

Доказательство. Достаточно доказать это утверждение для двух многочленов. Пусть f_1, f_2 — ненулевые многочлены, u_1, u_2 — их старшие члены, v_1, v_2 — какие-то их члены. Если $v_1 \neq u_1$ или $v_2 \neq u_2$, то в силу предложения 2

$$u_1u_2 \succ v_1v_2.$$

Следовательно, после приведения подобных членов в произведении f_1f_2 произведение u_1u_2 сохранится в качестве ненулевого члена, который старше всех остальных.

3.8. Симметрические многочлены

Определение. Многочлен $f \in K[x_1, x_2, \ldots, x_n]$ называется симметрическим, если он не изменяется при любых перестановках переменных.

Так как любая перестановка может быть осуществлена путем последовательных перестановок двух элементов, то многочлен является симметрическим, если он не изменяется при перестановке любых двух переменных.

Очевидно, что каждая однородная компонента симметрического многочлена также является симметрическим многочленом.

Пример 1. Степенные суммы

$$s_k = x_1^k + x_2^k + \ldots + x_n^k \quad (k = 1, 2, \ldots),$$

очевидно, являются симметрическими многочленами.

Пример 2. Следующие симметрические многочлены называются элементарными симметрическими многочленами:

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_k = \sum_{i_1<i_2<\ldots<i_k} x_{i_1}x_{i_2}\ldots x_{i_k},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_n = x_1x_2\ldots x_n.$$

Пример 3. Определитель Вандермонда

$$V(x_1, x_2, \ldots, x_n) = \prod_{i>j}(x_i - x_j)$$

(см. пример 2.4.5), представляющий собой произведение разностей всевозможных пар переменных, при перестановках переменных может только умножиться на ± 1 за счет того, что в некоторых случаях уменьшаемое и вычитаемое поменяются ролями. Число таких случаев равно числу инверсий в соответствующей перестановке. Следовательно,

$$V(x_{k_1}, x_{k_2}, \ldots, x_{k_n}) = \mathrm{sgn}(k_1, k_2, \ldots, k_n)V(x_1, x_2, \ldots, x_n).$$

Таким образом, сам определитель Вандермонда не является симметрическим многочленом, но таковым является его квадрат

$$V(x_1, x_2, \ldots, x_n)^2 = \prod_{i>j}(x_i - x_j)^2.$$

Пример 4. При любых перестановках переменных x_1, x_2, x_3, x_4 многочлены

$$h_1 = x_1x_2 + x_3x_4,\ \ h_2 = x_1x_3 + x_2x_4,\ \ h_3 = x_1x_4 + x_2x_3$$

переставляются между собой. Поэтому любой симметрический многочлен от них будет симметрическим многочленом от x_1, x_2, x_3, x_4. В частности, таковым является их произведение

$$h_1h_2h_3 = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3).$$

Задача 1. Доказать, что многочлен

$$(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$$

является симметрическим.

Симметрические многочлены находят применение к алгебраическим уравнениям с одним неизвестным благодаря формулам Виета (см. §3.2), которые выражают элементарные симметрические многочлены от корней алгебраического уравнения через его коэффициенты (при условии, что число корней уравнения в рассматриваемом поле равно его степени). Ясно, что только симметрические многочлены от корней уравнения однозначно определены: значение любого другого многочлена, вообще говоря, зависит от нумерации корней. С другой стороны, мы покажем, что любой симметрический многочлен от корней алгебраического уравнения может быть выражен через коэффициенты этого уравнения.

Пример 5. Многочлен $s_2 = x_1^2 + x_2^2 + \ldots + x_n^2$ является симметрическим. Легко видеть, что

$$s_2 = \sigma_1^2 - 2\sigma_2. \tag{49}$$

Поэтому сумма квадратов корней алгебраического уравнения

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$$

равна $a_1^2 - 2a_2$.

Очевидно, что сумма и произведение симметрических многочленов, а также произведение симметрического многочлена на число, являются симметрическими многочленами. Иными словами, симметрические многочлены образуют подалгебру в алгебре всех многочленов.

Следовательно, если $F \in K[X_1, X_2, \ldots, X_m]$ — произвольный многочлен от m переменных и $f_1, f_2, \ldots, f_m \in K[x_1, x_2, \ldots, x_n]$ — какие-то симметрические многочлены, то $F(f_1, f_2, \ldots, f_m)$ — также симметрический многочлен от $x_1, x_2, \ldots, x_n$. Естественно поставить вопрос, нельзя ли найти такие симметрические многочлены $f_1, f_2, \ldots, f_m$, чтобы всякий симметрический многочлен можно было выразить через них указанным способом. Оказывается, что в качестве таких многочленов можно взять элементарные симметрические многочлены $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Теорема 1. Всякий симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов.

Доказательству теоремы предпошлем две леммы.

Лемма 1. Пусть $u = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ — старший член симметрического многочлена f. Тогда

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n. \tag{50}$$

Доказательство. Предположим, что $k_i < k_{i+1}$ для некоторого i. Наряду с членом u многочлен f должен содержать член

$$u' = ax_1^{k_1}\ldots x_i^{k_{i+1}}x_{i+1}^{k_i}\ldots x_n^{k_n},$$

получающийся из u перестановкой x_i и x_{i+1}. Легко видеть, что $u' \succ u$. Это противоречит тому, что u — старший член многочлена f.

Лемма 2. Для любого одночлена $u = x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, показатели которого удовлетворяют неравенствам (50), существуют такие неотрицательные целые числа $l_1, l_2, \ldots, l_n$, что старший член многочлена $\sigma_1^{l_1}\sigma_2^{l_2}\ldots\sigma_n^{l_n}$ совпадает с u. Числа $l_1, l_2, \ldots, l_n$ определены этим условием однозначно.

Доказательство. Старший член многочлена σ_k равен $x_1x_2\ldots x_k$. В силу предложения 3 старший член многочлена $\sigma_1^{l_1}\sigma_2^{l_2}\ldots\sigma_n^{l_n}$ равен

$$x_1^{l_1}(x_1x_2)^{l_2}\ldots(x_1x_2\ldots x_n)^{l_n} = x_1^{l_1+l_2+\ldots+l_n}x_2^{l_2+\ldots+l_n}\ldots x_n^{l_n}.$$

Приравнивая его одночлену u, получаем систему линейных уравнений

$$\begin{cases} l_1 + l_2 + \ldots + l_n = k_1, \\ l_2 + \ldots + l_n = k_2, \\ \ldots\ldots\ldots\ldots \\ l_n = k_n, \end{cases}$$

которая, очевидно, имеет единственное решение

$$l_i = k_i - k_{i+1}\ (i = 1, 2, \ldots, n-1), \quad l_n = k_n. \tag{51}$$

Из условия леммы следует, что определенные таким образом числа $l_1, l_2, \ldots, l_n$ неотрицательны.

Замечание 1. Уравнение $l_1+l_2+\ldots+l_n = k_1$ показывает, что степень одночлена $X_1^{l_1}X_2^{l_2}\ldots X_n^{l_n}$ по совокупности переменных равна степени одночлена u по x_1.

Доказательство теоремы. Пусть $f \in K[x_1, x_2, \ldots, x_n]$ — симметрический многочлен. Нам нужно найти такой многочлен $F \in K[X_1, X_2, \ldots, X_n]$, что

$$F(\sigma_1, \sigma_2, \ldots, \sigma_n) = f.$$

Если $f = 0$, то можно взять $F = 0$. В противном случае пусть $u_1 = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ — старший член многочлена f. По лемме 1 выполняются неравенства (50). По лемме 2 существует такой одночлен $F_1 \in K[X_1, X_2, \ldots, X_n]$, что старший член многочлена $F_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ равен u_1. Рассмотрим симметрический многочлен

$$f_1 = f - F_1(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Если $f_1 = 0$, то можно взять $F = F_1$. В противном случае пусть u_2 — старший член многочлена f_1. Ясно, что он младше, чем u_1. Существует такой одночлен $F_2 \in K[X_1, X_2, \ldots, X_n]$, что старший член многочлена $F_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$ равен u_2. Рассмотрим симметрический многочлен

$$f_2 = f_1 - F_2(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Если $f_2 = 0$, то можно взять $F = F_1 + F_2$. В противном случае, продолжая процесс, получаем последовательность симметрических многочленов $f, f_1, f_2, \ldots$, старшие члены которых удовлетворяют неравенствам

$$u_1 \succ u_2 \succ \ldots$$

По лемме 1 показатель при любой переменной в любом из одночленов u_m не превосходит показателя при x_1 в этом одночлене, а он, в свою очередь, не превосходит k_1. Поэтому для наборов показателей одночленов u_m имеется лишь конечное число возможностей, так что описанный выше процесс должен оборваться. Это означает, что $f_M = 0$ для некоторого M. В качестве F можно тогда взять $F_1 + F_2 + \ldots + F_M$.

Докажем теперь, что многочлен F определен однозначно. Предположим, что F и G — такие многочлены, что

$$F(\sigma_1, \sigma_2, \ldots, \sigma_n) = G(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Рассмотрим их разность $H = F - G$. Тогда

$$H(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0.$$

Нам нужно доказать, что $H = 0$. Предположим, что это не так, и пусть $H_1, H_2, \ldots, H_s$ — все ненулевые члены многочлена H. Обозначим через w_i $(i = 1, 2, \ldots, s)$ старший член многочлена

$$H_i(\sigma_1, \sigma_2, \ldots, \sigma_n) \in K[x_1, x_2, \ldots, x_n].$$

В силу леммы 2 среди одночленов $w_1, w_2, \ldots, w_s$ нет пропорциональных. Выберем из них старший. Пусть это будет w_1. По построению одночлен w_1 старше всех остальных членов многочлена $H_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ и всех членов многочленов $H_i(\sigma_1, \sigma_2, \ldots, \sigma_n)$ $(i = 2, \ldots, s)$. Поэтому после приведения подобных членов в сумме

$$H_1(\sigma_1, \sigma_2, \ldots, \sigma_n) + H_2(\sigma_1, \sigma_2, \ldots, \sigma_n) + \ldots + \\ + H_s(\sigma_1, \sigma_2, \ldots, \sigma_n) = H(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

член w_1 сохранится, так что эта сумма не будет равна нулю, что противоречит нашему предположению.

Замечание 2. Согласно замечанию 1 для любого m

$$\deg F_m = \deg_{x_1} u_m \leqslant \deg_{x_1} u_1 = \deg_{x_1} f (= k_1).$$

Следовательно,

$$\deg F = \deg_{x_1} f. \tag{52}$$

Следуя доказательству этой теоремы, можно в принципе найти выражение любого конкретного симметрического многочлена через $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Пример 6. Выразим через $\sigma_1, \sigma_2, \ldots, \sigma_n$ многочлен

$$f = s_3 = x_1^3 + x_2^3 + \ldots + x_n^3.$$

Представим вычисления в виде таблицы.

m	u_m	$F_m(\sigma_1, \sigma_2, \ldots, \sigma_n)$	f_m
1	x_1^3	$\sigma_1^3 = \sum\limits_i x_i^3 + 3\sum\limits_{i\neq j} x_i^2 x_j + {}$ $+ 6\sum\limits_{i<j<k} x_i x_j x_k$	$-3\sum\limits_{i\neq j} x_i^2 x_j -$ $-6\sum\limits_{i<j<k} x_i x_j x_k$
2	$-3x_1^2 x_2$	$-3\sigma_1\sigma_2 = -3\sum\limits_{i\neq j} x_i^2 x_j -$ $- 9\sum\limits_{i<j<k} x_i x_j x_k$	$3\sum\limits_{i<j<k} x_i x_j x_k$
3	$3x_1x_2x_3$	$3\sigma_3 = 3\sum\limits_{i<j<k} x_i x_j x_k$	0

Таким образом,

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \tag{53}$$

На практике для однородных симметрических многочленов удобнее применять другой способ, который мы поясним на следующем ниже примере.

Пример 7. Выразим через $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ многочлен

$$f = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$$

из примера 4. В обозначениях доказательства теоремы, имеем $u_1 = x_1^3 x_2 x_3 x_4$. Не производя вычислений, можно найти с точностью до коэффициентов возможных кандидатов на роль одночленов $u_2, u_3, \ldots$ Во-первых, их показатели должны удовлетворять неравенствам леммы 1. Во-вторых, поскольку f — однородный многочлен степени 6, сумма их показателей должна равняться 6. В-третьих, они должны быть младше u_1. Выпишем в таблицу все наборы показателей одночленов, удовлетворяющих этим условиям, в порядке лексикографического убывания, начиная с набора показателей u_1. Справа выпишем соответствующие произведения элементарных симметрических многочленов, найденные по формулам (51).

$$\begin{array}{cccc|l} 3 & 1 & 1 & 1 & \sigma_1^2\sigma_4 \\ 2 & 2 & 2 & 0 & \sigma_3^2 \\ 2 & 2 & 1 & 1 & \sigma_2\sigma_4 \end{array}$$

Итак, мы можем утверждать, что

$$f = \sigma_1^2\sigma_4 + a\sigma_3^2 + b\sigma_2\sigma_4.$$

Для того чтобы найти коэффициенты a и b, будем придавать в этом равенстве переменным x_1, x_2, x_3, x_4 какие-нибудь выбранные значения. Представим вычисления в виде таблицы, в правом столбце которой будем выписывать получаемые уравнения.

x_1	x_2	x_3	x_4	σ_1	σ_2	σ_3	σ_4	f	
1	1	1	0	3	3	1	0	1	$a = 1$
1	1	-1	-1	0	-2	0	1	8	$-2b = 8$

Таким образом, $a = 1$ и $b = -4$, так что

$$f = \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4.$$

В случае неоднородного симметрического многочлена этот способ можно применить к каждой его однородной компоненте и полученные выражения сложить.

Замечание 3. Изложенная теория без всяких изменений переносится на более общий случай, когда K — произвольное коммутативное ассоциативное кольцо с единицей. Так, в случае $K = \mathbb{Z}$ получается следующий результат: всякий симметрический многочлен с целыми коэффициентами представляется в виде многочлена с целыми коэффициентами от элементарных симметрических многочленов.

Доказанная теорема в сочетании с формулами Виета позволяет найти любой симметрический многочлен от корней заданного алгебраического уравнения. А именно, пусть $f \in K[x_1, x_2, \ldots, x_n]$ — симметрический многочлен и $F \in K[X_1, X_2, \ldots, X_n]$ — такой многочлен, что

$$f = F(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Пусть далее, $c_1, c_2, \ldots, c_n$ — корни алгебраического уравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \quad (a_0 \neq 0).$$

Тогда

$$f(c_1, c_2, \ldots, c_n) = F\left(-\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, (-1)^n\frac{a_n}{a_0}\right). \tag{54}$$

Замечание 4. Пусть $\deg_{x_1} f = k$. Тогда $\deg F = k$ (см. замечание 2) и, домножив равенство (54) на a_0^k, мы получим в правой части однородный многочлен степени k от $a_0, a_1, a_2, \ldots, a_n$.

Пример 8. Пусть c_1, c_2, c_3, c_4 — корни уравнения

$$x^4 + px^2 + qx + r = 0. \tag{55}$$

Найдем уравнение 3-й степени, корнями которого являются числа

$$d_1 = c_1c_2 + c_3c_4, \quad d_2 = c_1c_3 + c_2c_4, \quad d_3 = c_1c_4 + c_2c_3.$$

Запишем его в виде

$$y^3 + a_1y^2 + a_2y + a_3 = 0.$$

Согласно формулам Виета

$$\begin{aligned} a_1 &= -(d_1 + d_2 + d_3), \\ a_2 &= d_1d_2 + d_1d_3 + d_2d_3, \\ a_3 &= -d_1d_2d_3. \end{aligned}$$

Имеем $d_i = h_i(c_1, c_2, c_3, c_4)$, где h_1, h_2, h_3 — многочлены из примера 4. Находим:

$$h_1 + h_2 + h_3 = \sigma_2,$$

$$h_1h_2 + h_1h_3 + h_2h_3 = \sum_{\substack{i\neq j,k \\ j<k}} x_i^2x_jx_k = \sigma_1\sigma_3 - 4\sigma_4,$$

$$h_1h_2h_3 = \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4.$$

(Последнее равенство есть результат примера 7.) По формулам Виета

$$\begin{aligned} \sigma_1(c_1, c_2, c_3, c_4) &= 0, \\ \sigma_2(c_1, c_2, c_3, c_4) &= p, \\ \sigma_3(c_1, c_2, c_3, c_4) &= -q, \\ \sigma_4(c_1, c_2, c_3, c_4) &= r. \end{aligned}$$

Следовательно,

$$a_1 = -p, \quad a_2 = -4r, \quad a_3 = q^2 - 4pr,$$

т. е. искомое уравнение имеет вид

$$y^3 - py^2 - 4ry + (4pr - q^2) = 0. \tag{56}$$

Задача 2. В обозначениях предыдущего примера, доказать, что

$$(c_1 + c_2 - c_3 - c_4)^2 = 4(d_1 - p),$$
$$(c_1 - c_2 + c_3 - c_4)^2 = 4(d_2 - p),$$
$$(c_1 - c_2 - c_3 + c_4)^2 = 4(d_3 - p)$$

и, кроме того,

$$(c_1 + c_2 - c_3 - c_4)(c_1 - c_2 + c_3 - c_4)(c_1 - c_2 - c_3 + c_4) = -8q \tag{57}$$

(см. задачу 1).

Пользуясь результатами этой задачи, можно свести решение уравнения (55) к решению уравнения (56) (при условии, что $\operatorname{char} K \neq 2$). А именно, складывая с подходящими знаками равенства

$$c_1 + c_2 + c_3 + c_4 = 0,$$
$$c_1 + c_2 - c_3 - c_4 = 2\sqrt{d_1 - p},$$
$$c_1 - c_2 + c_3 - c_4 = 2\sqrt{d_2 - p},$$
$$c_1 - c_2 - c_3 + c_4 = 2\sqrt{d_3 - p},$$

получаем

$$c_{1,2,3,4} = \frac{1}{2}\left(\pm\sqrt{d_1 - p} \pm \sqrt{d_2 - p} \pm \sqrt{d_3 - p}\right),$$

где число минусов должно быть четно. Исходные значения квадратных корней здесь следует выбирать таким образом, чтобы их произведение равнялось $-q$ (см. формулу (57)).

Уравнение (56) называется кубической резольвентой уравнения (55).

3.9. Кубические уравнения

При решении квадратных уравнений ключевую роль играет дискриминант. По его обращению в нуль можно судить о наличии кратного корня, а по его знаку (в случае поля действительных чисел) — о числе действительных корней.

Выясним смысл дискриминанта $D(\varphi)$ квадратного трехчлена

$$\varphi = a_0x^2 + a_1x + a_2 \ \in \ \mathbb{C}[x].$$

Пусть c_1, c_2 — корни этого трехчлена. Тогда

$$D(\varphi) = a_1^2 - 4a_0a_2 = a_0^2\left[\left(\frac{a_1}{a_0}\right)^2 - \frac{4a_2}{a_0}\right] = \\ = a_0^2[(c_1+c_2)^2 - 4c_1c_2] = a_0^2(c_1-c_2)^2.$$

В случае, когда $a_0, a_1, a_2 \in \mathbb{R}$, полученная формула хорошо объясняет ту связь между дискриминантом и свойствами корней, о которой говорилось выше. А именно, имеются следующие три возможности:

1) $c_1, c_2 \in \mathbb{R}$, $c_1 \neq c_2$; тогда $c_1 - c_2$ — отличное от нуля действительное число и $D(\varphi) > 0$;

2) $c_1 = c_2 \in \mathbb{R}$; тогда $c_1 - c_2 = 0$ и $D(\varphi) = 0$;

3) $c_1 = \overline{c}_2 \notin \mathbb{R}$; тогда $c_1 - c_2$ —отличное от нуля чисто мнимое число и $D(\varphi) < 0$.

Что еще более важно, эта формула подсказывает, как можно определить дискриминант любого многочлена

$$\varphi = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x] \quad (a_0 \neq 0).$$

Предположим вначале, что многочлен φ имеет n корней $c_1, c_2, \ldots, c_n \in K$. Определим тогда его дискриминант $D(\varphi)$ по формуле

$$D(\varphi) = a_0^{2n-2}\prod_{i>j}(c_i - c_j)^2. \tag{58}$$

(Показатель при a_0 не так важен; почему мы выбрали его именно таким, будет ясно из дальнейшего.)

Иными словами, $D(\varphi)$ есть умноженное на a_0^{2n-2} значение симметрического многочлена (см. пример 8.3)

$$f = \prod_{i>j}(x_i - x_j)^2$$

от корней φ. Описанная в §3.8 процедура позволяет выразить $D(\varphi)$ через коэффициенты φ. Так как

$$\deg_{x_1} f = 2n - 2,$$

то в силу замечания 8.4 это выражение будет представлять собой некоторый однородный многочлен Δ степени $2n-2$ от $a_0, a_1, \ldots, a_n$:

$$D(\varphi) = \Delta(a_0, a_1, \ldots, a_n). \tag{59}$$

Для нахождения многочлена Δ нет необходимости знать, что многочлен φ имеет n корней в K. Это позволяет определить дискриминант любого многочлена φ по формуле (59).

Замечание 1. Так как f имеет целые коэффициенты, то и Δ имеет целые коэффициенты (см. замечание 8.3).

Замечание 2. Как можно доказать, для любого многочлена $\varphi \in K[x]$ степени n существует расширение L поля K, в котором φ имеет n корней. (Например, если $K = \mathbb{R}$, то можно взять $L = \mathbb{C}$.) Так как описанная выше процедура вычисления дискриминанта не зависит от того, над каким полем рассматривается многочлен φ (лишь бы его коэффициенты лежали в этом поле), то для $D(\varphi)$ будет справедлива формула (58), если в качестве $c_1, c_2, \ldots, c_n$ взять корни многочлена φ в поле L.

Из определения (58) дискриминанта ясно, что многочлен $\varphi \in \mathbb{C}[x]$ имеет кратные корни тогда и только тогда, когда $D(\varphi) = 0$. Это показывает, что наличие кратных корней является исключительным обстоятельством: если выбрать коэффициенты многочлена наудачу, то вероятность того, что он будет иметь кратные корни, равна нулю.

Пусть теперь φ — кубический многочлен с действительными коэффициентами и c_1, c_2, c_3 — его комплексные корни. Тогда

$$D(\varphi) = a_0^4(c_1 - c_2)^2(c_1 - c_3)^2(c_2 - c_3)^2.$$

Имеются следующие три возможности (с точностью до перенумерации корней):

1) c_1, c_2, c_3 — различные действительные числа; тогда $D(\varphi) > 0$;
2) $c_1, c_2, c_3 \in \mathbb{R}$, $c_2 = c_3$; тогда $D(\varphi) = 0$;
3) $c_1 \in \mathbb{R}$, $c_2 = \overline{c_3} \notin \mathbb{R}$; тогда

$$D(\varphi) = a_0^4[(c_1 - c_2)(c_1 - \overline{c_2})]^2(c_2 - \overline{c_2})^2 = \\ = a_0^4|c_1 - c_2|^4(c_2 - \overline{c_2})^2 < 0.$$

Таким образом, мы приходим к тому же выводу, что и в случае квадратного трехчлена: все корни многочлена φ действительны тогда и только тогда, когда $D(\varphi) \geqslant 0$.

Задача. Доказать, что если φ — многочлен любой степени с действительными коэффициентами, не имеющий кратных комплексных корней, то

$$\operatorname{sgn} D(\varphi) = (-1)^t,$$

где t — число пар комплексно сопряженных мнимых корней многочлена φ.

Мы найдем теперь явное выражение дискриминанта кубического многочлена через его коэффициенты, но перед этим сделаем некоторые общие замечания, позволяющие упростить вычисления.

Любой многочлен можно нормировать, разделив на старший коэффициент, что не изменит его корней. Далее, любой нормированный многочлен

$$\varphi = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$

над полем нулевой характеристики (или, более общо, над полем, характеристика которого не делит n) с помощью замены

$$x = y - \frac{a_1}{n}$$

приводится к многочлену

$$\psi = y^n + b_2 y^{n-2} + \ldots + b_{n-1} y + b_n,$$

в котором коэффициент при y^{n-1} равен нулю. Многочлен такого вида называется неполным. При $n = 2$ именно таким способом получается формула решения квадратного уравнения. При $n > 2$ эта замена не решает дела, но, во всяком случае, может упростить задачу.

Найдем дискриминант неполного кубического многочлена

$$\varphi = x^3 + px + q. \tag{60}$$

Следуя способу, изложенному в примере 8.7, будем искать выражение симметрического многочлена

$$f = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$$

через элементарные симметрические многочлены $\sigma_1, \sigma_2, \sigma_3$. Многочлен f является однородным степени 6, и его старший член равен $x_1^4 x_2^2$. Выпишем наборы показателей старших членов симметрических многочленов, которые могут встретиться в процессе, описанном в доказательстве теоремы 1, и соответствующие им произведения элементарных симметрических многочленов:

$$\begin{array}{ccc|l} 4 & 2 & 0 & \sigma_1^2\sigma_2^2 \\ 4 & 1 & 1 & \sigma_1^3\sigma_3 \\ 3 & 3 & 0 & \sigma_2^3 \\ 3 & 2 & 1 & \sigma_1\sigma_2\sigma_3 \\ 2 & 2 & 2 & \sigma_3^2 \end{array}$$

Мы видим, что

$$f = \sigma_1^2\sigma_2^2 + a\sigma_1^3\sigma_3 + b\sigma_2^3 + c\sigma_1\sigma_2\sigma_3 + d\sigma_3^2. \qquad (61)$$

Для вычисления $D(\varphi)$ мы должны будем сделать в выражении (61) подстановку

$$\sigma_1 = 0, \quad \sigma_2 = p, \quad \sigma_3 = -q.$$

Поэтому коэффициенты a и c не будут влиять на окончательный результат, и мы можем их не находить.

Для нахождения b и d будем в равенстве (60) придавать переменным x_1, x_2, x_3 значения, указанные в следующей таблице, в правом столбце которой выписаны получаемые при этом уравнения.

x_1	x_2	x_3	σ_1	σ_2	σ_3	f	
1	-1	0	0	-1	0	4	$-b = 4$
2	-1	-1	0	-3	2	0	$-27b + 4d = 0$

Таким образом, $b = -4$, $d = -27$ и

$$D(\varphi) = -4p^3 - 27q^2. \qquad (62)$$

Пример 1. Найдем число действительных корней многочлена

$$\varphi = x^3 - 0{,}3x^2 - 4{,}3x + 3{,}9.$$

С помощью замены

$$y = x - 0{,}1$$

приводим его к неполному многочлену (коэффициенты которого могут быть найдены по схеме Горнера как в примере 2.3)

$$\psi = y^3 - 4{,}33y + 3{,}468.$$

Теперь находим:

$$D(\varphi) = D(\psi) = 4 \cdot 4{,}33^3 - 27 \cdot 3{,}468^2 = 0{,}013 > 0.$$

Следовательно, многочлен φ имеет 3 различных действительных корня.

Замечание 3. Дискриминант кубического многочлена общего вида
$$\varphi = a_0x^3 + a_1x^2 + a_2x + a_3$$
равен
$$D(\varphi) = a_1^2a_2^2 - 4a_1^3a_3 - 4a_0a_2^3 + 18a_0a_1a_2a_3 - 27a_0^2a_3^2.$$

Изложим теперь способ решения кубического уравнения.

Предположим, что основное поле K содержит нетривиальный (т.е. отличный от 1) кубический корень из единицы, скажем, w. Тогда $1, w, w^{-1}$ — это все кубические корни из единицы, и по формуле Виета получаем
$$w + w^{-1} = -1. \tag{63}$$

Рассмотрим линейные многочлены
$$h_1 = x_1 + wx_2 + w^{-1}x_3, \quad h_2 = x_1 + w^{-1}x_2 + wx_3.$$
При перестановке x_2 и x_3 они меняются местами, а при перестановке x_1 и x_2 многочлен h_1 переходит в wh_2, а h_2 — в $w^{-1}h_1$. Отсюда следует, что многочлены
$$f = h_1^3 + h_2^3, \quad g = h_1h_2$$
являются симметрическими. Выражая их через элементарные симметрические многочлены, получаем:
$$f = 2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3, \quad g = \sigma_1^2 - 3\sigma_2.$$

Пусть теперь c_1, c_2, c_3 — корни многочлена (60). Положим
$$d_1 = c_1 + wc_2 + w^{-1}c_3, \quad d_2 = c_1 + w^{-1}c_2 + wc_3.$$
Из предыдущего следует, что
$$d_1^3 + d_2^3 = -27q, \quad d_1d_2 = -3p$$
и, значит,
$$d_1^3d_2^3 = -27p^3.$$
Таким образом, d_1^3 и d_2^3 — это корни квадратного уравнения
$$x^2 + 27qx - 27p^3 = 0.$$

Решая его, находим:

$$d_1^3 = 27\left(-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}\right), \tag{64}$$

$$d_2^3 = 27\left(-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}\right). \tag{65}$$

Заметим, что выражение, стоящее под знаком радикала, лишь множителем $-\frac{1}{108}$ отличается от дискриминанта многочлена (60).

Складывая равенства

$$c_1 + c_2 + c_3 = 0,$$
$$c_1 + wc_2 + w^{-1}c_3 = d_1,$$
$$c_1 + w^{-1}c_2 + wc_3 = d_2,$$

с учетом соотношения (63) получаем:

$$c_1 = \frac{1}{3}(d_1 + d_2).$$

Поскольку нумерация корней может быть произвольной, эта формула на самом деле дает все три корня, если в качестве d_1 и d_2 выбирать всевозможные значения кубических корней из выражений (64) и (65), связанные полученным выше соотношением

$$d_1 d_2 = -3p. \tag{66}$$

Таким образом, мы приходим к следующей окончательной формуле

$$c_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

называемой формулой Кардано.

Замечание 4. Формула Кардано имеет смысл, если извлекаются входящие в нее квадратные и кубические корни. В частности, если мы решаем по этой формуле кубическое уравнение с действительными коэффициентами, то нам, вообще говоря, придется работать с комплексными числами, даже если нас интересуют только действительные корни. Именно так обстоит дело в случае положительного дискриминанта, когда все три корня действительны: в этом случае число, стоящее под знаком квадратного радикала, отрицательно.

Пример 2. Найдем корни многочлена ψ из примера 1. Имеем:

$$\frac{p^3}{27}+\frac{q^2}{4}=-\frac{1}{108}D(\psi)\approx -0{,}0000120,$$

так что под знаком одного из кубических радикалов в формуле Кардано будет стоять число

$$-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}\approx -1{,}734+0{,}00347i\approx$$
$$\approx 1{,}73400[\cos(\pi-0{,}00200)+i\sin(\pi-0{,}00200)].$$

Под знаком другого кубического радикала будет стоять комплексно сопряженное число. Условие (66) означает в данном случае, что при извлечении кубических корней следует комбинировать их комплексно сопряженные значения. При сложении комплексно сопряженных чисел получается их удвоенная действительная часть. Таким образом,

$$c_1\approx 2\sqrt[3]{1{,}73400}\cos\frac{\pi-0{,}00200}{3}\approx 1{,}20278,$$
$$c_2\approx 2\sqrt[3]{1{,}73400}\cos\frac{\pi+0{,}00200}{3}\approx 1{,}20001,$$
$$c_3\approx -2\sqrt[3]{1{,}73400}\cos\frac{0{,}00200}{3}\approx -2{,}40277.$$

3.10. Поле рациональных дробей

Таким же образом, как кольцо целых чисел расширяется до поля рациональных чисел, любое целостное кольцо можно расширить до поля.

Пусть A — целостное кольцо. Рассмотрим множество пар (a,b), где $a,b\in A,\ b\neq 0$, и определим в нем отношение эквивалентности по правилу

$$(a_1,b_1)\sim(a_2,b_2)\iff a_1b_2=a_2b_1.$$

Рефлексивность и симметричность этого отношения очевидны; докажем его транзитивность. Если $(a_1,b_1)\sim(a_2,b_2)$ и

$(a_2, b_2) \sim (a_3, b_3)$, то

$$a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_1 b_2,$$

откуда после сокращения на b_2 получаем:

$$a_1 b_3 = a_3 b_1,$$

т. е. $(a_1, b_1) \sim (a_3, b_3)$.

Из данного определения следует, что

$$(a, b) \sim (ac, bc) \tag{67}$$

для любого $c \neq 0$. С другой стороны, как показывает следующая ниже цепочка эквивалентностей, любая эквивалентность $(a_1, b_1) \sim (a_2, b_2)$ является следствием эквивалентностей типа (67):

$$(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2.)$$

(Мы сначала умножили оба члена пары (a_1, b_1) на b_2, а затем сократили оба члена получившейся пары на b_1.)

Определим теперь сложение и умножение пар по правилам:

$$(a_1, b_1) + (a_2, b_2) = (a_1 b_2 + a_2 b_1, b_1 b_2),$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Докажем, что определенное выше отношение эквивалентности согласовано с этими операциями. В силу предыдущего достаточно показать, что при умножении обоих членов одной из пар (a_1, b_1) и (a_2, b_2) на элемент $c \neq 0$ сумма и произведение этих пар заменятся эквивалентными им парами; но очевидно, что при такой операции оба члена суммы и произведения умножатся на тот же элемент c.

Класс эквивалентности, содержащий пару (a, b), условимся записывать как «дробь» $\frac{a}{b}$ (пока это просто символ, не подразумевающий фактического деления). Ввиду доказанного выше операции сложения и умножения пар определяют операции сложения и умножения дробей, осуществляемые по обычным правилам:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \qquad \frac{a_1}{b_1} \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

Докажем, что относительно этих операций дроби образуют поле.

Любое конечное множество дробей можно привести к общему знаменателю, а сложение дробей с одинаковыми знаменателями сводится к сложению их числителей. Поэтому сложение дробей коммутативно и ассоциативно. Дробь $\frac{0}{1}$ ($=\frac{0}{b}$ при любом $b \neq 0$) служит нулем для операции сложения дробей, а дробь $\frac{-a}{b}$ противоположна дроби $\frac{a}{b}$. Таким образом, дроби образуют абелеву группу относительно сложения.

Коммутативность и ассоциативность умножения очевидны. Следующая цепочка равенств доказывает дистрибутивность умножения дробей относительно сложения:

$$\left(\frac{a_1}{b}+\frac{a_2}{b}\right)\frac{a_3}{b_3}=\frac{(a_1+a_2)a_3}{bb_3}=\frac{a_1a_3+a_2a_3}{bb_3}=\frac{a_1}{b}\frac{a_3}{b_3}+\frac{a_2}{b}\frac{a_3}{b_3}.$$

Дробь $\frac{1}{1}$ служит единицей для операции умножения дробей, а при $a \neq 0$ дробь $\frac{b}{a}$ обратна дроби $\frac{a}{b}$.

Построенное поле называется полем отношений (или полем дробей) кольца A и обозначается через $\operatorname{Quot} A$.

Сложение и умножение дробей вида $\frac{a}{1}$ сводятся к соответствующим операциям над их числителями. Кроме того, $\frac{a}{1}=\frac{b}{1}$ только при $a=b$. Следовательно, дроби такого вида образуют подкольцо, изоморфное A. Условившись отождествлять дробь вида $\frac{a}{1}$ с элементом a кольца A, мы получим вложение кольца A в поле $\operatorname{Quot} A$. Далее, поскольку

$$\frac{a}{b}\,\frac{b}{1}=\frac{a}{1},$$

дробь $\frac{a}{b}$ равна отношению элементов a и b кольца A в поле $\operatorname{Quot} A$. Таким образом, обозначение $\frac{a}{b}$ можно теперь понимать содержательным образом.

В силу (67) дробь не изменится, если ее числитель и знаменатель умножить или разделить (если это возможно) на один и тот же элемент кольца A. Если A — евклидово кольцо, то путем сокращения числителя и знаменателя на их наибольший общий делитель любая дробь приводится к виду $\frac{a}{b}$, где $(a,b)=1$. Такой вид дроби называется несократимым. (Допуская вольность речи, обычно говорят просто о несократимой дроби.) Несократимый вид дроби определен однозначно с точностью до умножения числителя и знаменателя на один и тот же обратимый элемент.

Поле отношений кольца $\mathbb{Z}$ целых чисел есть поле $\mathbb{Q}$ рациональных чисел. Поле отношений кольца $K[x]$ многочленов над полем K называется полем рациональных дробей (или рациональных функций) над полем K и обозначается через $K(x)$.

Каждая рациональная дробь определяет функцию на K со значениями в K, определенную там, где ее знаменатель (в несократимой записи) не обращается в нуль. А именно, значением дроби $\frac{f}{g}$ $(f, g \in K[x])$ в точке $c \in K$ называется число $\frac{f(c)}{g(c)}$. Легко видеть, что операции сложения и умножения дробей соответствуют таким же операциям над определяемыми ими функциями в их общей области определения.

Задача 1. Доказать, что если рациональные дроби $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ над бесконечным полем K определяют функции, совпадающие в их общей области определения, то $\frac{f_1}{g_1} = \frac{f_2}{g_2}$.

Рациональная дробь $\frac{f}{g}$ называется правильной, если $\deg f < \deg g$. Очевидно, что сумма и произведение правильных дробей являются правильными дробями.

Предложение 1. Всякая рациональная дробь единственным образом представляется в виде суммы многочлена и правильной дроби.

Доказательство. Пусть $f, g \in K[x]$, $g \neq 0$. Разделим f на g с остатком в кольце $K[x]$:

$$f = qg + r \quad (q, r \in K[x],\ \deg r < \deg g). \tag{68}$$

Тогда

$$\frac{f}{g} = q + \frac{r}{g}, \tag{69}$$

причем $\frac{r}{g}$ — правильная дробь. Обратно, из равенства (69) следует равенство (68), так что единственность искомого представления рациональной дроби вытекает из однозначности деления с остатком в кольце многочленов.

Изложим теперь теорию, используемую в математическом анализе при интегрировании рациональных функций.

Определение. Рациональная дробь $\frac{f}{g}$ над полем K называется простейшей, если $g = p^k$, где $p \in K[x]$ — неприводимый многочлен, и $\deg f < \deg p$.

В частности, всякая дробь вида

$$\frac{a}{(x-c)^k} \quad (a, c \in K)$$

является простейшей. В случае $K = \mathbb{C}$ дробями такого вида исчерпываются все простейшие дроби. В случае $K = \mathbb{R}$ имеются еще простейшие дроби вида

$$\frac{ax+b}{(x^2+px+q)^k} \quad (a, b, p, q \in \mathbb{R}),$$

где $p^2 - 4q < 0$.

Теорема 1. Всякая правильная рациональная дробь $\frac{f}{g}$ разлагается в сумму простейших дробей. Более точно, если $g = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ — разложение многочлена g на неприводимые множители, то дробь $\frac{f}{g}$ единственным образом разлагается в сумму простейших дробей со знаменателями

$$p_1, p_1^2, \ldots, p_1^{k_1}, p_2, p_2^2, \ldots, p_2^{k_2}, \ldots, p_s, p_s^2, \ldots, p_s^{k_s}.$$

Доказательство. Возможность указанного разложения докажем индукцией по числу неприводимых множителей многочлена g. Если g — неприводимый многочлен, то сама дробь $\frac{f}{g}$ является простейшей. Если $g = p^k$, где p — неприводимый многочлен, то разделим f на p с остатком:

$$f = qp + r, \quad \deg r < \deg p.$$

Мы тогда получим:

$$\frac{f}{g} = \frac{q}{p^{k-1}} + \frac{r}{p^k}.$$

Второе из слагаемых является простейшей дробью, а первое может быть разложено в сумму простейших дробей со знаменателями $p, p^2, \ldots, p^{k-1}$ по предположению индукции.

Пусть теперь $s \geqslant 2$. Так как многочлены $p_1^{k_1}$ и $h = p_2^{k_2} \ldots p_s^{k_s}$ взаимно просты, то существуют такие многочлены u и v, что

$$f = up_1^{k_1} + vh. \tag{70}$$

Мы можем добиться того, чтобы

$$\deg u < \deg h. \tag{71}$$

В самом деле, если это не так, разделим u на h с остатком:

$$u = qh + r, \quad \deg r < \deg h.$$

Равенство (70) может быть тогда переписано в виде

$$f = rp_1^{k_1} + (v + qp_1^{k_1})h = u_1 p_1^{k_1} + v_1 h,$$

где $u_1 = r,\ v_1 = v + qp_1^{k_1}$ и $\deg u_1 < \deg h$.

В предположении, что выполнено (71), разделим равенство (70) на g. Мы тогда получим:

$$\frac{f}{g} = \frac{u}{h} + \frac{v}{p_1^{k_1}}.$$

В силу (71) первое из слагаемых является правильной дробью. По предположению индукции оно может быть разложено в сумму простейших дробей со знаменателями

$$p_2, p_2^2, \ldots, p_2^{k_2}, \ldots, p_s, p_s^2, \ldots, p_s^{k_s}.$$

Второе слагаемое является правильной дробью как разность правильных дробей и по доказанному выше может быть разложено в сумму простейших дробей со знаменателями

$$p_1, p_1^2, \ldots, p_1^{k_1}.$$

Это и дает нужное разложение дроби $\dfrac{f}{g}$.

Докажем теперь единственность такого разложения. Если имеются два таких разложения, то, вычитая одно из другого, получаем равенство вида

$$\frac{u_{11}}{p_1} + \frac{u_{12}}{p_1^2} + \ldots + \frac{u_{1k_1}}{p_1^{k_1}} + \frac{u_{21}}{p_2} + \frac{u_{22}}{p_2^2} + \ldots + \frac{u_{2k_2}}{p_2^{k_2}} + \\ + \frac{u_{s1}}{p_s} + \frac{u_{s2}}{p_s^2} + \ldots + \frac{u_{sk_s}}{p_s^{k_s}} = 0,$$

где $\deg u_{ij} < \deg p_i$. Нам нужно доказать, что все многочлены u_{ij} равны нулю. Предположим, что это не так. Пусть, например, среди многочленов $u_{11}, u_{12}, \dots, u_{1k_1}$ имеются ненулевые, и пусть u_{1k} $(k \leqslant k_1)$ — последний из них. Умножив тогда предыдущее равенство на $p_1^k p_2^{k_2} \dots p_s^{k_s}$, мы получим в левой части сумму многочленов, все слагаемые которой, кроме $u_{1k} p_2^{k_2} \dots p_s^{k_s}$, делятся на p_1. Следовательно, и это слагаемое должно делиться на p_1, но это невозможно, так как $\deg u_{1k} < \deg p_1$.

Пример 1. Предположим, что

$$g = (x - c_1)(x - c_2) \dots (x - c_n),$$

где $c_1, c_2, \dots, c_n$ различны. Тогда

$$\frac{f}{g} = \frac{a_1}{x - c_1} + \frac{a_2}{x - c_2} + \dots + \frac{a_n}{x - c_n},$$

где $a_1, a_2, \dots, a_n \in K$. Для нахождения a_i умножим обе части предыдущего равенства на g и положим $x = c_i$. Мы получим тогда:

$$f(c_i) = a_i(c_i - c_1) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_i - c_n) = a_i g'(c_i),$$

откуда

$$a_i = \frac{f(c_i)}{g'(c_i)}.$$

Итак,

$$\frac{f}{g} = \sum_{i=1}^{n} \frac{f(c_i)}{g'(c_i)(x - c_i)} \tag{72}$$

(при условии, что $\deg f < \deg g$). Интересно отметить, что, умножив обе части этого равенства на g, мы получим интерполяционную формулу Лагранжа

$$f = \sum_{i=1}^{n} b_i \frac{(x - c_1) \dots (x - c_{i-1})(x - c_{i+1}) \dots (x - c_n)}{(c_i - c_1) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_1 - c_n)},$$

задающую многочлен f степени $< n$, принимающий в точках $c_1, c_2, \dots, c_n$ значения $b_1, b_2, \dots, b_n$.

Задача 2. Доказать равенство

$$\frac{1}{x^n - 1} = \frac{1}{n} \sum_{i=0}^{n-1} \frac{\varepsilon_i}{x - \varepsilon_i},$$

где $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ — комплексные корни n-й степени из единицы.

Задача 3. Разложить в сумму простейших дробей над полем $\mathbb{Z}_p$ (p — простое) дробь $\dfrac{1}{x^p - x}$.

Пример 2. Метод неопределенных коэффициентов, использованный в предыдущем примере, разумно применять и в более общей ситуации. Разложим, например, в сумму простейших дробей над $\mathbb{R}$ рациональную дробь

$$\frac{x}{(x+1)(x^2+1)^2}.$$

Имеем согласно теореме:

$$\frac{x}{(x+1)(x^2+1)^2} = \frac{a}{x+1} + \frac{bx+c}{x^2+1} + \frac{dx+e}{(x^2+1)^2},$$

где a, b, c, d, e — какие-то действительные числа. Для их нахождения умножим предыдущее равенство на $(x+1)(x^2+1)^2$:

$$x = a(x^2+1)^2 + (bx+c)(x+1)(x^2+1) + (dx+e)(x+1).$$

Положив в этом равенстве последовательно $x = -1$ и $x = i$, получим:

$$-1 = 4a, \quad i = (di+e)(i+1) = (e-d) + (d+e)i,$$

откуда

$$a = -\frac{1}{4}, \quad d = e = \frac{1}{2}.$$

Далее, сравнив свободные члены и коэффициенты при x^4, получим:

$$0 = a + c + e, \quad 0 = a + b,$$

откуда

$$b = \frac{1}{4}, \quad c = -\frac{1}{4}.$$

Таким образом,

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