Глава пятая

ЦЕЛЫЕ РАЦИОНАЛЬНЫЕ ФУНКЦИИ

Содержание. Простые теоремы о многочленах от одной и нескольких переменных с коэффициентами из коммутативного кольца $\mathfrak{o}$.

§ 27. Дифференцирование

В этом параграфе мы определяем производные целой рациональной функции для произвольного кольца многочленов без использования непрерывности.

Пусть $f(x)=\sum a_i x^i$ — произвольный многочлен кольца $\mathfrak{o}[x]$. Построим в кольце многочленов $\mathfrak{o}[x, h]$ многочлен $f(x+h)=\sum a_i (x+h)^i$ и разложим его по степеням h:

$$f(x+h)=f(x)+hf_1(x)+h^2f_2(x)+\ldots,$$

или

$$f(x+h)\equiv f(x)+hf_1(x)\pmod{h^2}.$$

Коэффициент $f_1(x)$ при первой степени h (определенный однозначно) называется *производной* многочлена $f(x)$ и обозначается через $f'(x)$. Очевидно, можно получить $f'(x)$ и таким способом: разделить разность $f(x+h)-f(x)$ на содержащийся в ней множитель h и в полученном многочлене положить $h=0$. Отсюда легко следует, что когда $\mathfrak{o}$ — поле вещественных чисел, такое определение производной согласуется с обычным определением *производной в дифференциальном исчислении* как предела $\lim\limits_{h\to 0}\frac{f(x+h)-f(x)}{h}$. Поэтому только что определенную производную обозначают также через $\frac{df}{dx}$, или через $\frac{d}{dx}f(x)$, или, если f содержит, кроме x, и другие переменные, через $\frac{\partial f}{\partial x}$.

Имеют место следующие *правила дифференцирования*:

$$(f+g)'=f'+g' \qquad \text{(производная суммы)}, \tag{1}$$

$$(fg)'=f'g+fg' \qquad \text{(производная произведения)}. \tag{2}$$

Доказательство формулы (1):

$$f(x+h)+g(x+h)\equiv f(x)+hf'(x)+g(x)+hg'(x)\pmod{h^2}.$$

Доказательство формулы (2):

$$f(x+h)\,g(x+h) \equiv \{f(x)+hf'(x)\}\,\{g(x)+hg'(x)\} \equiv$$
$$\equiv f(x)\,g(x)+h\,\{f'(x)\,g(x)+f(x)\,g'(x)\} \pmod{h^2}.$$

Точно так же доказываются более общие утверждения:

$$(f_1+\ldots+f_n)' = f_1'+\ldots+f_n', \tag{3}$$
$$(f_1f_2\ldots f_n)' = f_1'f_2\ldots f_n+f_1f_2'\ldots f_n+\ldots+f_1f_2\ldots f_n'. \tag{4}$$

Из (4) следует далее, что

$$(ax^n)' = nax^{n-1}. \tag{5}$$

Из (3) и (5) получается равенство

$$\left(\sum_0^n a_kx^k\right)' = \sum_1^n ka_kx^{k-1}.$$

С помощью этой формулы можно было бы формально определить все описанные выше производные.

Задача 1. Пусть $F(z_1, \ldots, z_m)$ — некоторый многочлен и $F_\nu = \partial F/\partial z_\nu$. Доказать формулу

$$\frac{d}{dx}F(f_1(x), \ldots, f_m(x)) = \sum_1^m F_\nu(f_1, \ldots, f_m)\frac{df_\nu}{dx}.$$

Задача 2. Для однородных многочленов r-й степени $f(x_1, \ldots, x_n)$ из равенства

$$f(hx_1, \ldots, hx_n) = h^rf(x_1, \ldots, x_n)$$

вывести «эйлерово дифференциальное соотношение» (тождество Эйлера):

$$\sum_\nu \frac{\partial f}{\partial x_\nu}x_\nu = rf.$$

Задача 3. Дать алгебраическое определение производной рациональной функции $f(x)/g(x)$ с коэффициентами из поля и доказать известные формулы для производных суммы, произведения и частного.

§ 28. Корни

Пусть $\mathfrak{o}$ — целостное кольцо с единицей.

Элемент α из $\mathfrak{o}$ называется *корнем* многочлена $f(x)$ из $\mathfrak{o}[x]$, если $f(\alpha)=0$. Имеет место следующая теорема:

Если α — корень многочлена $f(x)$, то $f(x)$ делится на $x-\alpha$.

Доказательство. Деление $f(x)$ на $x-\alpha$ дает равенство

$$f(x) = q(x)(x-\alpha)+r,$$

где r — некоторая константа. Подставим в это равенство $x=\alpha$:

$$0 = r,$$

откуда

$$f(x) = q(x)(x-\alpha).$$

Если $\alpha_1, \ldots, \alpha_k$ — различные корни многочлена $f(x)$, то $f(x)$ делится на произведение $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)$.

Доказательство. Для $k=1$ теорема уже доказана. Если считать ее доказанной для $k-1$, то будет иметь место равенство:

$$f(x) = (x-\alpha_1)\ldots(x-\alpha_{k-1})\,g(x).$$

Подстановка $x=\alpha_k$ дает

$$0 = (\alpha_k-\alpha_1)\ldots(\alpha_k-\alpha_{k-1})\,g(\alpha_k);$$

следовательно, так как в $\mathfrak{o}$ нет делителей нуля и $\alpha_k \neq \alpha_1, \ldots$ $\ldots, \alpha_k \neq \alpha_{k-1}$, имеем

$$g(\alpha_k) = 0,$$

откуда в силу предыдущей теоремы

$$g(x) = (x-\alpha_k)\,h(x),$$
$$f(x) = (x-\alpha_1)\ldots(x-\alpha_{k-1})(x-\alpha_k)\,h(x),$$

а это и требовалось доказать.

Следствие. *Отличный от нуля многочлен степени n имеет в целостном кольце не более n корней.*

Эта теорема верна также и в целостных кольцах без единицы, потому что такие кольца могут быть погружены в поле. Однако эта теорема неверна в кольцах с делителями нуля; например, в кольце классов вычетов по модулю 16 многочлен x^2 имеет в качестве корней классы, представляемые числами 0, 4, 8, 12; существуют даже кольца, в которых многочлен такого же вида имеет бесконечно много корней (§ 11, задача 3).

Если $f(x)$ делится на $(x-\alpha)^k$, но не делится на $(x-\alpha)^{k+1}$, то элемент α называют *k-кратным корнем* многочлена $f(x)$. Имеет место теорема:

k-кратный корень многочлена $f(x)$ является не менее, чем $(k-1)$-кратным корнем производной $f'(x)$.

Доказательство. Из $f(x) = (x-\alpha)^k g(x)$ следует, что

$$f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x),$$

откуда $f'(x)$ делится на $(x-\alpha)^{k-1}$.

Точно так же доказывается утверждение: *простой* (т. е. 1-кратный) *корень многочлена $f(x)$ не является корнем производной $f'(x)$.*

Перейдем теперь к некоторым теоремам о корнях многочленов от многих переменных.

Если $f(x_1, \ldots, x_n)$ — ненулевой многочлен, а каждая из переменных $x_1, \ldots, x_n$ может принимать бесконечное множество значений из кольца $\mathfrak{o}$ или любого целостного кольца, содержащего $\mathfrak{o}$,

то существует по крайней мере один набор значений $x_1=\alpha_1, \ldots, x_n=\alpha_n$, *для которого* $f(\alpha_1, \ldots, \alpha_n)\neq 0$.

Доказательство. Многочлен $f(x_1, \ldots, x_n)$ как многочлен от x_n (с коэффициентами из целостного кольца $\mathfrak{o}[x_1, \ldots, x_{n-1}]$) имеет не более конечного числа корней; следовательно, в бесконечном множестве значений, которое можно подставлять вместо элемента x_n, существует такой элемент α_n, что

$$f(x_1, \ldots, x_{n-1}, \alpha_n)\neq 0.$$

Рассмотрим это выражение как многочлен от x_{n-1}; тогда существует значение α_{n-1}, для которого

$$f(x_1, \ldots, x_{n-2}, \alpha_{n-1}, \alpha_n)\neq 0,$$

и т. д.

Следствие. *Если для всех значений переменных* x_i *из некоторого бесконечного целостного кольца многочлен* $f(x_1, \ldots, x_n)$ *принимает значение нуль, то он сам является нулевым.*

Здесь следует напомнить о том, что в алгебре обращение в нуль многочлена от $x_1, \ldots, x_n$ означает равенство нулю всех его коэффициентов и не определяется через равенство нулю всех его значений на всевозможных конкретных наборах значений переменных $x_1, \ldots, x_n$. Поэтому последняя из сформулированных теорем не является тавтологией.

Задача 1. Распространить последнюю теорему на конечные системы многочленов $f_i(x_1, \ldots, x_n)$, ни один из которых не равен нулю.

Задача 2 (Определитель Вандермонда) [1]. Доказать, что

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}(x_i-x_j).$$

§ 29. Интерполяционные формулы

Вернемся к случаю многочленов от одной переменной; в качестве кольца коэффициентов теперь будет рассматриваться некоторое *поле*. Согласно доказанным выше теоремам два многочлена степеней $\leqslant n$, значения которых совпадают в $n+1$ различных точках, оказываются равными, потому что их разность — многочлен степени, не большей n, — имеет в этом случае $n+1$ корень. Следовательно, существует самое большее один многочлен, который в заданных $n+1$ различных точках $\alpha_0, \ldots, \alpha_n$ принимает заданные значения $f(\alpha_i)$. С другой стороны, всегда существует

[1]) Добавлена при переводе, так как используется в дальнейшем. *Прим. ред.*

многочлен степени $\leqslant n$, который в этих точках принимает нужные значения, — это многочлен

$$f(x)=\sum_{i=0}^{n}\frac{f(\alpha_i)(x-\alpha_0)\ldots(x-\alpha_{i-1})(x-\alpha_{i+1})\ldots(x-\alpha_n)}{(\alpha_i-\alpha_0)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})(\alpha_i-\alpha_n)}. \tag{1}$$

Итак, *существует один и только один многочлен степени* $\leqslant n$, *который при заданных* $n+1$ *различных значениях* $\alpha_0, \alpha_1, \ldots, \alpha_n$ *переменной принимает заданные значения* $f(\alpha_i)$; этот многочлен задается формулой (1). Формула (1) называется *интерполяционной формулой Лагранжа.*

Многочлен с нужными свойствами можно получить и с помощью *интерполяционной формулы Ньютона*:

$$f(x)=\lambda_0+\lambda_1(x-\alpha_0)+\lambda_2(x-\alpha_0)(x-\alpha_1)+\ldots$$
$$\ldots+\lambda_n(x-\alpha_0)(x-\alpha_1)\ldots(x-\alpha_{n-1}), \tag{2}$$

где коэффициенты $\lambda_0, \ldots, \lambda_n$ определяются последовательно путем подстановки значений аргумента $x=\alpha_0, \ldots, x=\alpha_n$.

Проводить вычисления лучше всего так: подставим в (2) сначала $x=\alpha_0$; получим

$$f(\alpha_0)=\lambda_0.$$

Вычтем это из (2) и разделим на $x-\alpha_0$; получится

$$\frac{f(x)-f(\alpha_0)}{x-\alpha_0}=\lambda_1+\lambda_2(x-\alpha_1)+\ldots+\lambda_n(x-\alpha_1)\ldots(x-\alpha_{n-1}). \tag{3}$$

Обозначим левую часть через $f(\alpha_0, x)$. Подставим в (3) $x=\alpha_1$; получится

$$f(\alpha_0, \alpha_1)=\lambda_1.$$

Вычтем теперь это из (3) и разделим на $x-\alpha_1$; тогда

$$\frac{f(\alpha_0, x)-f(\alpha_0, \alpha_1)}{x-\alpha_1}=\lambda_2+\lambda_3(x-\alpha_2)+\ldots+\lambda_n(x-\alpha_2)\ldots(x-\alpha_{n-1}).$$

Обозначим левую часть через $f(\alpha_0, \alpha_1, x)$. Подставим теперь $x=\alpha_2$; получится

$$f(\alpha_0, \alpha_1, \alpha_2)=\lambda_2.$$

Эти вычисления можно продолжить. В общем случае положим (определение с помощью индукции)

$$f(\alpha_0, \ldots, \alpha_k, x)=\frac{f(\alpha_0, \ldots, \alpha_{k-1}, x)-f(\alpha_0, \ldots, \alpha_{k-1}, \alpha_k)}{x-\alpha_k} \tag{4}$$

и, как и выше, получим

$$f(\alpha_0, \ldots, \alpha_{k-1}, x)=\lambda_k+\lambda_{k+1}(x-\alpha_k)+\ldots+\lambda_n(x-\alpha_k)\ldots(x-\alpha_{n-1}),$$
$$f(\alpha_0, \ldots, \alpha_k)=\lambda_k. \tag{5}$$

Константу $f(\alpha_0, \ldots, \alpha_k)$ называют k-м *разностным отношением* функции $f(x)$ в точках $\alpha_0, \ldots, \alpha_k$. В силу (4)

$$\left.\begin{aligned} f(\alpha_0, \alpha_1) &= \frac{f(\alpha_1)-f(\alpha_0)}{\alpha_1-\alpha_0}, \\ f(\alpha_0, \alpha_1, \alpha_2) &= \frac{f(\alpha_0, \alpha_2)-f(\alpha_0, \alpha_1)}{\alpha_2-\alpha_1}, \\ f(\alpha_0, \ldots, \alpha_n) &= \frac{f(\alpha_0, \ldots, \alpha_{n-2}, \alpha_n)-f(\alpha_0, \ldots, \alpha_{n-2}, \alpha_{n-1})}{\alpha_n-\alpha_{n-1}}. \end{aligned}\right\} \quad (6)$$

k-е разностное отношение может быть определено и как коэффициент при x^k в многочлене $\varphi_k(x)$ степени $\leqslant k$, который в точках $\alpha_0, \ldots, \alpha_k$ принимает значения $f(\alpha_0), \ldots, f(\alpha_k)$. Действительно, этот многочлен задается с помощью интерполяционной формулы Ньютона

$$\varphi_k(x) = \lambda_0 + \lambda_1(x-\alpha_0) + \ldots + \lambda_k(x-\alpha_0)\ldots(x-\alpha_{k-1}),$$

а коэффициент при x^k здесь равен в точности $\lambda_k = f(\alpha_0, \ldots, \alpha_k)$.

Из последнего определения следует, что k-е разностное отношение не зависит от нумерации точек $\alpha_0, \ldots, \alpha_k$. Это свойство следующим образом используется на практике: если $\alpha_0, \ldots, \alpha_n$, — например, рациональные числа, расположенные в естественном порядке, то разностные отношения вычисляются всякий раз для следующих друг за другом чисел α_ν, а потому формула (6) с помощью перестановки чисел α_ν превращается в формулу

$$f(\alpha_0, \alpha_1, \ldots, \alpha_k) = \frac{f(\alpha_1, \ldots, \alpha_k)-f(\alpha_0, \ldots, \alpha_{k-1})}{\alpha_k-\alpha_0}. \quad (7)$$

Поэтому конечные разности можно расположить в некоторую схему по следующему принципу:

$$\begin{array}{llll} f(\alpha_0) & & & \\ & f(\alpha_0, \alpha_1) & & \\ f(\alpha_1) & & f(\alpha_0, \alpha_1, \alpha_2) & \\ & f(\alpha_1, \alpha_2) & & \ldots \\ f(\alpha_2) & & f(\alpha_1, \alpha_2, \alpha_3) & \\ & f(\alpha_2, \alpha_3) & \ldots & \\ f(\alpha_3) & \ldots & & \\ \ldots & & & \end{array}$$

Каждый последующий столбец получается по формуле (7) путем составления первых разностных отношений предыдущего столбца. Эту схему можно как угодно расширить, вводя все новые и новые исходные точки. Если $f(x)$ — многочлен n-й степени, то в $(n+1)$-м столбце всюду стоит одна и та же константа,

а именно коэффициент λ_n при x^n. В $(n+2)$-м столбце в этом случае стоят нули.

Арифметические прогрессии высших порядков. Будем считать, что основное в наших рассмотрениях поле содержит кольцо целых чисел и что точки $\alpha_0, \alpha_1, \alpha_2, \ldots$ являются последовательными целыми числами, скажем, $0, 1, 2, \ldots$ Если в этом случае составить описанную выше схему разностных отношений, то знаменатели $\alpha_k - \alpha_1, \alpha_{k+1} - \alpha_1, \ldots,$ которые согласно (7) появляются при вычислении $(k+1)$-го столбца, будут все равны k. Если второй столбец умножить на 1, третий — на 2, четвертый — на $2 \cdot 3$ и, вообще, $(k+1)$-й столбец на $k!$, то вместо прежней схемы разностных отношений получится *схема разностей*

$$\begin{array}{lll} b_0 & & \\ & \Delta b_0 & \\ b_1 & & \Delta^2 b_0 \\ & \Delta b_1 & \qquad \ldots, \\ b_2 & & \Delta^2 b_1 \\ & \Delta b_2 & \ldots \\ b_3 & \ldots & \\ \ldots & & \end{array} \tag{8}$$

где $f(a_\nu) = b_\nu$; символ Δb_ν означает $b_{\nu+1} - b_\nu$; символ $\Delta^2 b_\nu$ означает $\Delta\Delta b_\nu = \Delta b_{\nu+1} - \Delta b_\nu$ и т. д. Если $b_0, b_1, \ldots$ — значения некоторого многочлена n-й степени, то согласно сказанному выше n-е разности будут равны одной и той же константе, а $(n+1)$-е разности все равны нулю. Сам многочлен будет задаваться формулой (2) с коэффициентами

$$\lambda_k = \frac{\Delta^k b_0}{k!}. \tag{9}$$

Оказывается, имеет место и обратное утверждение:

Если $(n+1)$-е разности последовательности $b_0, b_1, b_2, \ldots$ равны нулю, то $b_0, b_1, \ldots$ являются значениями многочлена n-й степени $f(x)$, который задается формулами (2) *и* (9).

Действительно, построим с помощью многочлена $f(x)$ схему разностей и сравним ее с заданной схемой (8); обязательно совпадут начальные элементы $b_0, \Delta b_0, \Delta^2 b_0, \ldots, \Delta^n b_0$ каждого из столбцов, а $(n+1)$-й столбец в обоих случаях будет нулевым. Отсюда последовательно получается, что элементы n-х столбцов, а затем $(n-1)$-х столбцов и т. д. и, наконец, первых столбцов обеих схем совпадают.

Приведенный выше способ доказательства одновременно показывает, как, начиная с последнего столбца, можно получить все элементы схемы (8), когда заданы начальные элементы $\Delta^k b_0 = k!\lambda_k$ $(k = 0, 1, \ldots, n)$ всех столбцов. Нижеследующий пример

($n=3$, $a_0=0$, $\Delta a_0=1$, $\Delta^2 a_0=6$, $\Delta^3 a_0=6$), возможно, пояснит сказанное:

$$
\begin{array}{ccccl}
0 & & & & \\
 & 1 & & & \lambda_0=0, \\
1 & & 6 & & \\
 & 7 & & 6 & \\
8 & & 12 & & \lambda_1=1, \\
 & 19 & & 6 & \\
27 & & 18 & & \\
 & 37 & & 6 & \lambda_2=\frac{6}{2}=3, \\
64 & & 24 & & \\
 & 61 & & & \lambda_3=\frac{6}{6}=1, \\
125 & & & &
\end{array}
$$

$$
f(x)=\lambda_0+\lambda_1 x+\lambda_2 x(x-1)+\lambda_3 x(x-1)(x-2)=
$$
$$
=x+3x(x-1)+x(x-1)(x-2)=x^3.
$$

Будем подразумевать под *арифметической прогрессией нулевого порядка* произвольную последовательность одинаковых чисел b, b, b, ..., а под *арифметической прогрессией n-го порядка* — такую последовательность чисел, у которой последовательность разностей является арифметической прогрессией $(n-1)$-го порядка. Очевидно, что первый столбец в схеме (8) является арифметической прогрессией n-го порядка, потому что $(n+2)$-й столбец состоит из одних нулей. Тем самым доказанное выше мы можем сформулировать так:

Значения многочлена $f(x)$ степени n в точках 0, 1, 2, 3, ... *составляют арифметическую прогрессию n-го порядка, и каждая арифметическая прогрессия n-го порядка состоит из значений в заданных точках некоторого многочлена не выше n-й степени.* Сам многочлен $f(x)$ находится из формул (2) и (9). Общий член b_x арифметической прогрессии n-го порядка определяется по формуле

$$
b_x=f(x)=
$$
$$
=b_0+(\Delta b_0)x+\frac{\Delta^2 b_0}{2}x(x-1)+\ldots+\frac{\Delta^n b_0}{n!}x(x-1)\ldots(x-n+1).
$$

Схема разностей (8) находит свое практическое применение в интерполировании и интегрировании функций, которые задаются числовыми (эмпирически построенными) таблицами. Если b_0, b_1, b_2, ... — значения некоторой функции $\varphi(x)$ при равноотстоящих значениях аргумента α_0, α_0+h, α_0+2h, ..., то практика показывает, что для достаточно гладких функций и для небольших зна-

чений h разности второго, третьего, четвертого или, в худшем случае, пятого порядка практически равны нулю; поэтому в нескольких непосредственно следующих друг за другом интервалах функция достаточно точно заменяется многочленом степени не выше четвертой. Для целей численного интерполирования или интегрирования данную функцию можно заменить многочленом, принимающим заданные значения в следующих друг за другом точках, число которых колеблется от 2 до 5. Интерполирование осуществляется с помощью формулы (2). Как правило, при этом оказывается возможным ограничиться разностями первого и второго порядка, т. е. линейными или квадратичными многочленами. При вычислении элементов $\Delta^k a_\nu$ в разностных отношениях функции встречаются не только множители $k!$, но и степени длины интервала h; тем самым вместо (9) получается формула

$$\lambda_k = \frac{\Delta^k a_0}{k! h^k}.$$

Если значения аргумента $\alpha_0, \alpha_1, \ldots$ не являются равноудаленными друг от друга, то вместо разностей $\Delta^k a_\nu$ нужно составлять разностные отношения (7). По поводу дальнейших подробностей теории, оценок погрешностей и т. д. мы отсылаем читателя к соответствующей учебной литературе [1]).

Задача 1. Частичные суммы $s_m = \sum_{\nu=0}^{m-1} a_\nu$ арифметической прогрессии n-го порядка (где предполагается, что $s_0 = 0$) составляют арифметическую прогрессию $(n+1)$-го порядка. Отсюда получается формула для суммы

$$s_m = ma_0 + \binom{m}{2} \Delta a_0 + \ldots + \binom{m}{n+1} \Delta^n a_0.$$

Задача 2. Получить формулы для сумм $\sum_{\nu=0}^{m-1} \nu$, $\sum_{\nu=0}^{m} \nu^2$, $\sum_{\nu=0}^{m-1} \nu^3$.

§ 30. Разложение на множители

В § 18 мы уже видели, что в кольце многочленов $K[x]$ над *полем* K выполняется теорема об однозначном разложении на простые множители. Сейчас мы докажем более общую основную теорему:

Если $\mathfrak{S}$ — целостное кольцо с единицей и в $\mathfrak{S}$ имеет место теорема об однозначном разложении на простые множители, то и в кольце многочленов $\mathfrak{S}[x]$ эта теорема оказывается выполненной.

Приводимое здесь доказательство восходит к Гауссу.

---

[1]) См., например, Ковалевский (Kowalewski G.). Interpolation und genäherte Quadratur. — Leipzig, 1930.

Пусть $f(x)=\sum_0^n a_i x^i$ — произвольный ненулевой многочлен из $\mathfrak{S}[x]$. Наибольший общий делитель d коэффициентов $a_0, \ldots, a_n$ в кольце $\mathfrak{S}$ (ср. § 18, задача 7) назовем *содержанием* многочлена $f(x)$. Если вынести d за скобки, то получится равенство

$$f(x)=dg(x),$$

в котором $g(x)$ является многочленом с содержанием 1. Многочлен $g(x)$ и скаляр d определены однозначно с точностью до обратимых множителей.

Лемма 1. *Произведение двух многочленов с содержанием* 1 *вновь является многочленом с содержанием* 1.

Доказательство. Пусть

$$f(x)=a_0+a_1x+\ldots$$

и

$$g(x)=b_0+b_1x+\ldots$$

— данные многочлены с содержанием 1. Допустим, что наибольший общий делитель коэффициентов многочлена $f(x)g(x)$ равен d и необратим. Если p — произвольный простой делитель элемента d, то p должен быть делителем всех коэффициентов произведения $f(x)g(x)$. Пусть a_r — первый из коэффициентов многочлена $f(x)$, который не делится на p, и b_s — коэффициент многочлена $g(x)$ с аналогичным свойством.

Коэффициент при x^{r+s} в произведении $f(x)g(x)$ выглядит так:

$$a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\ldots+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\ldots$$

Эта сумма должна делиться на p. Все ее слагаемые, за исключением первого, должны делиться на p. Следовательно, a_rb_s также должно делиться на p, так что a_r или b_s должно делиться на p, что противоречит предположению.

Пусть Σ — поле частных кольца $\mathfrak{S}$ (§ 13). Тогда каждый многочлен кольца $\Sigma[x]$ разлагается на простые множители однозначно (§ 18). Чтобы перейти от разложения в $\Sigma[x]$ к разложению в $\mathfrak{S}[x]$, воспользуемся следующей процедурой: каждый многочлен $\varphi(x)$ кольца $\Sigma[x]$ можно представить в виде $\frac{F(x)}{b}$ (где $F(x)$ принадлежит кольцу $\mathfrak{S}[x]$, а b — кольцу $\mathfrak{S}$), причем b является произведением знаменателей коэффициентов многочлена $\varphi(x)$. Многочлен же $F(x)$ можно записать в виде произведения его содержания на многочлен с содержанием 1:

$$F(x)=af(x)$$

и

$$\varphi(x)=\frac{a}{b}f(x). \tag{1}$$

Мы утверждаем теперь следующее:

Лемма 2. *Указанный в равенстве* (1) *многочлен* $f(x)$ *с содержанием* 1 *определяется многочленом* $\varphi(x)$ *однозначно с точностью до обратимых в* $\mathfrak{S}$ *элементов. Обратно, многочлен* $\varphi(x)$ *определяется многочленом* $f(x)$ *однозначно с точностью до обратимых в* $\Sigma[x]$ *элементов. Если таким способом сопоставить каждому* $\varphi(x)$ *из* $\Sigma[x]$ *многочлен* $f(x)$ *с содержанием* 1, *то произведению двух многочленов* $\varphi(x)\psi(x)$ *будет соответствовать с точностью до обратимых множителей произведение соответствующих многочленов с содержанием* 1 (*и обратно*). *Если многочлен* $\varphi(x)$ *неразложим в* $\Sigma[x]$, *то и многочлен* $f(x)$ *неразложим в* $\mathfrak{S}[x]$ (*и обратно*).

Доказательство. Пусть даны два различных представления многочлена $\varphi(x)$:

$$\varphi(x)=\frac{a}{b}f(x)=\frac{c}{d}g(x).$$

Тогда

$$adf(x)=cbg(x). \tag{2}$$

Содержание левой части равно ad, а содержание правой равно cb, следовательно,

$$ad=\varepsilon cb,$$

где ε — обратимый элемент кольца $\mathfrak{S}$. Подставим это в (2) и сократим на cb:

$$\varepsilon f(x)=g(x).$$

Таким образом, многочлены $f(x)$ и $g(x)$ отличаются друг от друга обратимым в $\mathfrak{S}$ множителем.

Для произведения двух многочленов

$$\varphi(x)=\frac{a}{b}f(x),$$

$$\psi(x)=\frac{c}{d}g(x)$$

мы немедленно получаем

$$\varphi(x)\psi(x)=\frac{ac}{bd}f(x)g(x),$$

и согласно лемме 1 произведение $f(x)g(x)$ вновь является многочленом с содержанием 1. Следовательно, произведению $\varphi(x)\psi(x)$ соответствует произведение $f(x)g(x)$.

Наконец, если $\varphi(x)$ — неразложимый многочлен, то таким же будет и $f(x)$, потому что любое разложение $f(x)=g(x)h(x)$ сразу же приводит к разложению

$$\varphi(x)=\frac{a}{b}f(x)=\frac{a}{b}g(x)h(x).$$

Обратное утверждение получается точно так же.

Лемма 2 доказана.

С помощью леммы 2 однозначность разложения многочленов немедленно переносится на соответствующие многочлены с содержанием 1. Итак: *многочлены с содержанием 1 разлагаются на простые множители однозначно с точностью до обратимых элементов, причем эти простые множители снова являются многочленами с содержанием 1.*

Рассмотрим теперь разложение на множители произвольного многочлена в $\mathfrak{S}[x]$. Неразложимые многочлены обязательно являются или неразложимыми константами или неразложимыми многочленами с содержанием 1, потому что любой другой многочлен разложим в произведение своего содержания и многочлена с содержанием 1. Следовательно, чтобы разложить какой-либо многочлен $f(x)$, нужно сначала разложить $f(x)$ в произведение его содержания и многочлена с содержанием 1, а потом каждый из этих сомножителей разлагать на простые множители. В силу предпосылок основной теоремы разложение содержания осуществить можно, и притом однозначно с точностью до обратимых элементов; разложение же на простые множители многочлена с содержанием 1 также возможно в силу доказанного выше. Тем самым основная теорема доказана.

Попутно мы получили следующий важный результат:

Если многочлен $F(x)$ из $\mathfrak{S}[x]$ разложим в $\Sigma[x]$, то он разложим уже в $\mathfrak{S}[x]$.

Действительно, в силу того, что $F(x) = df(x)$, многочлену $F(x)$ соответствует некоторый многочлен $f(x)$ с содержанием 1, а согласно лемме 2 разложение многочлена $F(x)$ в $\Sigma[x]$ приводит к разложению многочлена $f(x)$ в $\mathfrak{S}[x]$, но если $f(x)$ неразложим, то неразложим и $F(x)$.

Например, любой многочлен с целыми рациональными коэффициентами, который разлагается над рациональными числами, оказывается разложимым уже над целыми числами. Итак: *если целочисленный многочлен неразложим над целыми числами, то он неразложим и над рациональными числами.*

С помощью индукции из основной теоремы получается следующий результат:

Если $\mathfrak{S}$ — целостное кольцо с единицей и в $\mathfrak{S}$ имеет место теорема об однозначном разложении на множители, то она справедлива и в кольце многочленов $\mathfrak{S}[x_1, \ldots, x_n]$.

Отсюда, среди прочего, получается однозначность разложения для целочисленных многочленов (от произвольного числа переменных), для многочленов с коэффициентами из произвольного поля и т. д.

Понятие многочлена с содержанием 1, фигурирующее в приведенных выше леммах Гаусса, в особенности используется при исследовании колец многочленов от большого числа переменных.

Если K — поле, то многочлен f из $\mathsf{K}[x_1, \ldots, x_n]$ называется *многочленом с содержанием* 1 *относительно* $x_1, \ldots, x_{n-1}$, если его содержание как многочлена с коэффициентами из целостного кольца $\mathsf{K}[x_1, \ldots, x_{n-1}]$ равно 1, т. е. если он не имеет делителей, отличных от констант и зависящих лишь от $x_1, \ldots, x_{n-1}$.

Задача 1. Обратимыми элементами кольца $\mathfrak{S}[x]$ являются лишь обратимые элементы кольца $\mathfrak{S}$.

Задача 2. Доказать, что в разложении на множители произвольного однородного многочлена участвуют лишь однородные многочлены.

Задача 3. Доказать, что определитель

$$\Delta = \begin{vmatrix} x_{11} & \ldots & x_{1n} \\ \cdot & \cdot & \cdot \\ x_{n1} & \ldots & x_{nn} \end{vmatrix}$$

неразложим в кольце многочленов $\mathfrak{S}[x_{11}, \ldots, x_{nn}]$. (Фиксировать произвольную переменную, скажем, x_{11}, и показать, что многочлен Δ имеет содержание 1 относительно остальных переменных.)

Задача 4. Указать способ, который позволил бы выяснить, обладает ли произвольно заданный целочисленный многочлен делителями первой степени или нет.

Задача 5. Доказать неразложимость многочлена

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

в кольце многочленов от одной переменной x с целыми коэффициентами. Разложим ли этот многочлен над полем рациональных чисел? Разложим ли он над кольцом целых гауссовых чисел?

§ 31. Признаки неразложимости

Пусть $\mathfrak{S}$ — целостное кольцо с единицей, в котором имеет место теорема об однозначном разложении на множители, и пусть

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

— произвольный многочлен из кольца $\mathfrak{S}[x]$. Нижеследующая теорема позволяет во многих случаях выяснить вопрос о неразложимости $f(x)$:

Теорема Эйзенштейна. *Если в $\mathfrak{S}$ существует простой элемент p, для которого*

$$a_n \not\equiv 0 \ (p),$$
$$a_i \equiv 0 \ (p) \text{ для всех } i < n,$$
$$a_0 \not\equiv 0 \ (p^2),$$

то многочлен $f(x)$ неразложим в кольце $\mathfrak{S}[x]$ с точностью до постоянных множителей; другими словами, многочлен $f(x)$ неразложим в кольце $\Sigma[x]$, где Σ — поле частных кольца $\mathfrak{S}$.

Доказательство. Если $f(x)$ разложим, то

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

$$g(x) = \sum_0^r b_\nu x^\nu,$$

$$h(x) = \sum_0^s c_\nu x^\nu,$$

$$r > 0, \quad s > 0, \quad r + s = n,$$

и тогда

$$a_0 = b_0 c_0, \quad a_0 \equiv 0\ (p).$$

Отсюда либо $b_0 \equiv 0\ (p)$, либо $c_0 \equiv 0\ (p)$. Пусть, скажем, $b_0 \equiv 0\ (p)$. Тогда $c_0 \not\equiv 0\ (p)$, так как иначе

$$a_0 = b_0 c_0 \equiv 0\ (p^2).$$

Не все коэффициенты многочлена $g(x)$ делятся на p, потому что в противном случае произведение $f(x) = g(x)\,h(x)$ делилось бы на p и все коэффициенты, в частности a_n, делились бы на p, что противоречит условию. Пусть b_i — первый коэффициент в $g(x)$, который не делится на p $(0 < i \leqslant r < n)$. Тогда

$$\begin{aligned} a_i &= b_i c_0 + b_{i-1} c_1 + \ldots + b_0 c_i, \\ a_i &\equiv 0\ (p), \\ b_{i-1} &\equiv 0\ (p), \\ &\ldots\ldots\ldots \\ b_0 &\equiv 0\ (p), \end{aligned}$$

и, следовательно,

$$\begin{aligned} b_i c_0 &\equiv 0\ (p), \\ c_0 &\not\equiv 0\ (p), \\ b_i &\equiv 0\ (p), \end{aligned}$$

что противоречит условию.

Таким образом, многочлен $f(x)$ является неразложимым с точностью до постоянных множителей.

Пример 1. Многочлен $x^m - p$ (p — простое число) в кольце целочисленных многочленов (и тем самым в кольце многочленов с рациональными коэффициентами) неразложим. Следовательно, $\sqrt[m]{p}$ ($m > 1$, p — простое число) — иррациональное число.

Пример 2. Многочлен $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ при простом числе p является левой частью «уравнения деления круга». Поставим и здесь вопрос о разложимости над целыми (или, что по существу то же самое, над рациональными) числами. Признак Эйзенштейна применить непосредственно здесь нельзя, но можно поступить следующим образом. Если бы многочлен $f(x)$ был разложим, то таким же был бы и многочлен $f(x+1)$. Имеем

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

Все коэффициенты, кроме коэффициента при x^p, делятся на p, потому что в формуле для биномиального коэффициента

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$$

при $i < p$ числитель делится на p, а знаменатель нет. Кроме того, постоянный член $\binom{p}{p-1}$ не делится на p^2. Следовательно, $f(x+1)$ — неразложимый многочлен, а потому неразложим и $f(x)$.

Пример 3. То же самое преобразование приводит многочлен $f(x) = x^2 + 1$ к виду

$$f(x+1) = x^2 + 2x + 2$$

и тем самым приводит к решению вопроса о разложимости.

Задача 1. Показать иррациональность числа $\sqrt[m]{p_1 p_2 \ldots p_r}$, где $p_1, \ldots, p_r$ — различные простые целые числа и $m > 1$.

Задача 2. Показать неразложимость многочлена

$$x^2 + y^2 - 1$$

в кольце $\mathsf{P}[x, y]$, где P является произвольным полем, в котором $+1 \neq -1$.

Задача 3. Показать неразложимость многочленов

$$x^4 + 1, \quad x^6 + x^3 + 1$$

в кольце целочисленных многочленов.

В своей основе теорема Эйзенштейна опирается на то, что равенство

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

превращается в сравнение по модулю p^2:

$$f(x) \equiv g(x)\, h(x),$$

а это последнее приводит к противоречию. В многочисленных других случаях оказывается в равной степени возможным доказать неразложимость переходом от равенств в данном кольце к сравнениям по модулю некоторого элемента q в кольце $\mathfrak{S}$ и выяснением, является ли данный многочлен разложимым по модулю q. В частности, если $\mathfrak{S}$ — кольцо целых чисел $\mathbb{Z}$, то в кольце классов вычетов по модулю целого числа q есть лишь конечное число многочленов заданной степени; поэтому есть лишь конечное число возможностей разложения многочлена $f(x)$ по модулю q, которые легко проверить. Если окажется, что $f(x)$ неразложим по модулю q, то $f(x)$ был неразложим и в кольце $\mathbb{Z}[x]$, но в противном случае можно доказать неразложимость, если извлечь из разложимости многочлена по модулю q некоторую дополнительную информацию, причем, если в качестве q взять какое-либо простое число, то можно воспользоваться теоремой об однозначном разложении многочленов по модулю этого простого числа (§ 18, задача 3).

Пример 4. $\mathfrak{S} = \mathbb{Z}$; $f(x) = x^5 - x^2 + 1$. Если многочлен $f(x)$ разложим mod (2), то один из сомножителей должен быть линейным или квадратичным. По модулю 2 есть лишь два линейных многочлена

$$x, \quad x + 1$$

и лишь один неразложимый квадратичный многочлен

$$x^2 + x + 1.$$

Процесс деления показывает, что $x^5 - x^2 + 1$ не делится ни на один из этих многочленов (по модулю 2). Это непосредственно усматривается из соотношений

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

Следовательно, $f(x)$ — неразложимый многочлен.

§ 32. Разложение на множители в конечное число шагов

Мы рассмотрели теоретическую возможность разложения каждого многочлена кольца $\Sigma[x_1, \ldots, x_n]$ над полем Σ на простые множители и в некоторых случаях указали средство выяснения того, возможно такое разложение или нет. Однако у нас нет метода, который позволял бы в любом случае решить вопрос о разложении многочлена в конечное число шагов. Один из этих методов, который пригоден по крайней мере в случае, когда Σ — поле рациональных чисел, мы сейчас изложим.

Согласно § 30 любой многочлен с рациональными коэффициентами можно считать многочленом с целыми коэффициентами и искать целочисленное разложение последнего. В кольце $\mathbb{Z}$ целых чисел разложение на простые множители проводится, очевидно, с помощью конечного числа проб; кроме того, в этом кольце есть лишь конечное множество обратимых элементов ($+1$ и -1), а потому лишь конечное число возможных разложений. В кольце многочленов $\mathbb{Z}[x_1, \ldots, x_n]$ число обратимых элементов тоже конечно: эти элементы суть $+1$ и -1. Индукцией по числу переменных n все сводится к следующей задаче:

Пусть в кольце $\mathfrak{S}$ разложение на множители осуществляется в конечное число шагов, и пусть в $\mathfrak{S}$ существует лишь конечное множество обратимых элементов. Найти метод разложения произвольного многочлена из кольца $\mathfrak{S}(x)$ на простые множители.

Решение этой задачи было дано Кронекером.

Пусть $f(x)$ — многочлен n-й степени из $\mathfrak{S}[x]$. Если $f(x)$ разложим, то один из сомножителей будет иметь степень $\leqslant n/2$; следовательно, если s — наибольшее целое число, не превосходящее $n/2$, то мы должны проверить, имеет ли $f(x)$ какой-либо делитель $g(x)$ степени $\leqslant s$.

Найдем значения $f(a_0), f(a_1), \ldots, f(a_s)$ многочлена $f(x)$ в $s+1$ произвольно выбранных целочисленных точках $a_0, a_1, \ldots, a_s$. Если теперь $f(x)$ делится на $g(x)$, то обязательно $f(a_0)$ делится на $g(a_0)$, $f(a_1)$ делится на $g(a_1)$ и т. д. Но так как каждое целое число $f(a_i)$ в кольце $\mathfrak{S}$ имеет лишь конечное число делителей, для $g(a_i)$ имеется лишь конечное число возможных значений, которые, согласно условию, можно перебрать. Согласно теоремам из § 29 для каждой возможной комбинации значений $g(a_0), g(a_1), \ldots, g(a_s)$ существует ровно один многочлен $g(x)$, причем $g(x)$ всегда может быть указан в явном виде. Тем самым мы нашли конечное множество многочленов $g(x)$, которые могут быть делителями данного многочлена. По поводу каждого конкретного многочлена $g(x)$ с помощью алгоритма деления можно выяснить, является ли он в действительности делителем многочлена $f(x)$ или нет. Если ни один из многочленов $g(x)$ не окажется делителем многочлена $f(x)$ (мы опускаем случаи обратимых делителей), то $f(x)$ неразложим; в противном же случае находим некоторое разложение и к каждому из полученных множителей можно применить ту же процедуру и т. д.

В целочисленном случае ($\mathfrak{S}=\mathbb{Z}$) описанный метод можно сильно сократить. Сначала нужно рассмотреть разложение данного многочлена по модулю 2 и, возможно, по модулю 3, чтобы понять, какие степени могли бы иметь его делители $g(x)$ и каковы классы вычетов коэффициентов по модулю 2 и по модулю 3. Такие наблюдения значительно сократят число возможных претендентов на роль делителей вида $g(x)$. Затем, применяя интерполяционную формулу Ньютона, можно заметить, что последний коэффициент λ_s какого бы то ни было делителя является старшим коэффициентом многочлена $f(x)$, а это вновь уменьшает число возможностей. Наконец, часто используется прием, при котором берется более $s+1$ точек a_i. Здесь нужно определить возможные значения $g(a_i)$, делящие те $f(a_i)$, которые содержат наименьшее число простых делителей; остальные точки также можно использовать для того, чтобы ограничить число возможностей. Для этого при вычислении каждого многочлена $g(x)$ нужно сначала выяснить, являются ли его значения в неучтенных еще точках a_i делителями соответствующих чисел $f(a_i)$ или нет.

Задача 1. Разложить многочлен

$$f(x)=x^5+x^4+x^2+x+2$$

в кольце $\mathbb{Z}[x]$ на простые множители

Задача 2. Разложить многочлен

$$f(x, y, z)=-x^3-y^3-z^3+x^2(y+z)+y^2(x+z)+z^2(x+y)-2xyz$$

в кольце $\mathbb{Z}[x, y, z]$ на простые множители.

§ 33. Симметрические функции

Пусть $\mathfrak{o}$ — произвольное коммутативное кольцо с единицей. Многочлен кольца $\mathfrak{o}[x_1, \ldots, x_n]$ называется (целой рациональной) *симметрической функцией* переменных $x_1, \ldots, x_n$, если он переходит в себя при любой перестановке переменных $x_1, \ldots, x_n$. Например, сумма, произведение, сумма степеней этих переменных — симметрические функции.

С помощью новой переменной z построим многочлен

$$f(z) = (z - x_1)(z - x_2)\ldots(z - x_n) = \\ = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots + (-1)^n \sigma_n; \qquad (1)$$

тогда коэффициенты этого многочлена при степенях z таковы:

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n,$$
$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_n = x_1x_2x_3 \ldots x_n.$$

Очевидно, это — симметрические функции, так как левая часть равенства (1), как и его правая часть, не меняются при перестановках переменных x_i. Функции $\sigma_1, \ldots, \sigma_n$ называются *элементарными симметрическими функциями от* $x_1, \ldots, x_n$.

Каждый многочлен $\varphi(\sigma_1, \ldots, \sigma_n)$ дает симметрическую функцию от $x_1, \ldots, x_n$, если вместо σ подставить соответствующие выражения через переменные x. При этом слагаемое вида $c\sigma_1^{\mu_1} \ldots \sigma_n^{\mu_n}$ в выражении для $\varphi(\sigma_1, \ldots, \sigma_n)$ окажется однородным многочленом от x_i степени $\mu_1 + 2\mu_2 + \ldots + n\mu_n$, так как каждый многочлен σ_i является однородным многочленом степени i. Сумму $\mu_1 + 2\mu_2 + \ldots + n\mu_n$ мы называем *весом* слагаемого $c\sigma_1^{\mu_1} \ldots \sigma_n^{\mu_n}$, а под *весом* многочлена $\varphi(\sigma_1, \ldots, \sigma_n)$ подразумевается наибольший вес из входящих в него слагаемых. Многочлены $\varphi(\sigma_1, \ldots, \sigma_n)$ веса k дают тем самым симметрические многочлены от x_i степени $\leqslant k$.

Так называемая основная теорема о симметрических функциях гласит:

Каждая целая рациональная симметрическая функция из кольца $\mathfrak{o}[x_1, \ldots, x_n]$ *может быть записана в виде многочлена* $\varphi(\sigma_1, \ldots, \sigma_n)$.

Доказательство. Упорядочим заданный симметрический многочлен *словарно* (как в словаре), т. е. таким образом, чтобы слагаемое $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ предшествовало слагаемому $x_1^{\beta_1} \ldots x_n^{\beta_n}$ в том случае, если первая ненулевая разность $\alpha_i - \beta_i$ положительна.

Вместе со слагаемым $ax_1^{\alpha_1}\ldots x_n^{\alpha_n}$ в выражение для данного многочлена входят также все слагаемые, показатели которых являются (в своем наборе) некоторой перестановкой показателей α_i; эти слагаемые мы записывать не будем, а воспользуемся записью $a\sum x_1^{\alpha_1}\ldots x_n^{\alpha_n}$, в которую фактически входит лишь первое в словарном упорядочении слагаемое во всей сумме слагаемых. Для такого слагаемого $\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_n$.

Пусть степень данного симметрического многочлена равна k, а первое в словарном упорядочении слагаемое есть $ax_1^{\alpha_1}\ldots x_n^{\alpha_n}$. Составим произведение элементарных симметрических функций, в котором (после раскрытия скобок и приведения в словарный порядок) первое слагаемое будет таким же: $ax_1^{\alpha_1}\ldots x_n^{\alpha_n}$. Это произведение найти легко; вот оно:

$$a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n}.$$

Вычтем это произведение из данного многочлена, упорядочим разность словарно, найдем в ней старшее слагаемое и т. д.

Такая процедура должна будет в конце концов оборваться. Действительно, вычитаемое произведение имеет вес

$$\alpha_1-\alpha_2+2\alpha_2-2\alpha_3+3\alpha_3-\ldots-(n-1)\alpha_n+n\alpha_n=$$
$$=\alpha_1+\alpha_2+\alpha_3+\ldots+\alpha_n\leqslant k;$$

поэтому, расписанное как многочлен от переменных x, это произведение приобретает степень $\leqslant k$. Следовательно, степень данной симметрической функции при вычитании, описанном выше, не возрастает. Но при заданной степени k существует лишь конечное множество произведений степеней $x_1^{\alpha_1}\ldots x_n^{\alpha_n}$. Так как при каждом вычитании такое произведение исчезает, а остаются лишь следующие за ним в словарном упорядочении, процедура после конечного числа шагов должна оборваться: просто не остается больше слагаемых.

Такое доказательство одновременно дает средство выражения данной симметрической функции через элементарные функции σ_i. Если данная функция имеет степень k, то найденное выражение $\varphi(\sigma_1, \ldots, \sigma_n)$ будет иметь вес k.

Кроме того, из доказательства следует предложение: однородные симметрические функции степени k могут быть выражены «изобарически» через функции σ_i, т. е. так, что слагаемые в полученной сумме все будут иметь вес k.

Покажем теперь, что любая симметрическая функция выражается в виде целой рациональной функции от $\sigma_1, \ldots, \sigma_n$ единственным способом. Точнее:

Если $\varphi_1(y_1, \ldots, y_n)$ *и* $\varphi_2(y_1, \ldots, y_n)$ — *два многочлена от переменных* $y_1, \ldots, y_n$ *и*

$$\varphi_1(y_1, \ldots, y_n) \neq \varphi_2(y_1, \ldots, y_n),$$

то и

$$\varphi_1(\sigma_1, \ldots, \sigma_n) \neq \varphi_2(\sigma_1, \ldots, \sigma_n).$$

Рассмотрение разности $\varphi_1 - \varphi_2 = \varphi$ показывает, что достаточно доказать утверждение: из $\varphi(y_1, \ldots, y_n) \neq 0$ следует $\varphi(\sigma_1, \ldots, \sigma_n) \neq 0$.

Доказательство. Каждое слагаемое в $\varphi(y_1, \ldots, y_n)$ можно записать в виде

$$ay_1^{\alpha_1-\alpha_2}y_2^{\alpha_2-\alpha_3} \ldots y_n^{\alpha_n}.$$

Среди всех систем $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, которые соответствуют коэффициенту $a \neq 0$, существует первая в словарном упорядочении. Заменим y_i на σ_i и выразим эти последние через x_i; тогда получится первое в словарном смысле слагаемое в $\varphi(\sigma_1, \ldots, \sigma_n)$:

$$ax_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Это слагаемое нельзя ни с чем сократить, так что и в самом деле

$$\varphi(\sigma_1, \ldots, \sigma_n) \neq 0.$$

Мы доказали:

Каждый симметрический многочлен из кольца $\mathfrak{o}[x_1, \ldots, x_n]$ *можно и притом единственным способом представить в виде многочлена от* $\sigma_1, \ldots, \sigma_n$; *вес этого многочлена равен степени заданного многочлена.*

Все целые рациональные соотношения между симметрическими функциями сохраняются, если x_i перестают быть переменными и становятся какими-то элементами из $\mathfrak{o}$, например, корнями разлагающегося на линейные множители в $\mathfrak{o}[z]$ многочлена $f(z)$. Из доказанного, таким образом, следует, что каждая симметрическая функция корней многочлена $f(z)$ выражается через коэффициенты этого многочлена.

Задача 1. Для произвольного n выразить суммы степеней $\sum x_i$, $\sum x_i^2$, $\sum x_i^3$ через элементарные симметрические функции.

Задача 2. Пусть $\sum x_i^\rho = s_\rho$. Доказать формулы

$$s_\rho - s_{\rho-1}\sigma_1 + s_{\rho-2}\sigma_2 - \ldots + (-1)^{\rho-1} s_1\sigma_{\rho-1} + (-1)^\rho \rho\sigma_\rho = 0 \quad \text{для} \quad \rho \leqslant n$$

$$s_\rho - s_{\rho-1}\sigma_1 + \ldots + (-1)^n s_{\rho-n}\sigma_n = 0 \quad \text{для} \quad \rho > n,$$

и с их помощью выразить суммы степеней s_1, s_2, s_3, s_4, s_5 через элементарные симметрические функции.

Важной симметрической функцией является квадрат произведения разностей:

$$D=\prod_{i<k}(x_i-x_k)^2.$$

Выражение для D как многочлена от

$$a_1=-\sigma_1,\quad a_2=\sigma_2,\ \ldots,\ a_n=(-1)^n\sigma_n$$

называется *дискриминантом* многочлена

$$f(z)=z^n+a_1z^{n-1}+\ldots+a_n.$$

Обращение в нуль дискриминанта для частных значений $a_1, \ldots, a_n$ означает, что $f(z)$ имеет кратные линейные множители.

Если многочлен $f(z)$ представить в более общем виде с произвольным старшим коэффициентом a_0:

$$f(z)=a_0z^n+a_1z^{n-1}+\ldots+a_n,$$

то получится

$$\sigma_1=-\frac{a_1}{a_0},\quad \sigma_2=\frac{a_2}{a_0},\quad \ldots,\quad \sigma_n=(-1)^n\frac{a_n}{a_0}.$$

Дискриминантом многочлена $f(z)$ в этом случае называют произведение разностей, умноженное на a_0^{2n-2}:

$$D=a_0^{2n-2}\prod_{i<k}(x_i-x_k)^2.$$

В § 35 мы увидим, что D представляет собой многочлен от $a_0, a_1, \ldots, a_n$.

Применяя описанный выше общий метод, мы получим дискриминанты

для $a_0x^2+a_1x+a_2$:

$$D=a_1^2-4a_0a_2;$$

для $a_0x^3+a_1x^2+a_2x+a_3$:

$$D=a_1^2a_2^2-4a_0a_2^3-4a_1^3a_3-27a_0^2a_3^2+18a_0a_1a_2a_3.$$

Задача 3. Дискриминант остается инвариантным при замене всех x_i на x_i+h. Вывести отсюда дифференциальное соотношение

$$na_0+(n-1)a_1\frac{\partial D}{\partial a_2}+\ldots+a_{n-1}\frac{\partial D}{\partial a_n}=0.$$

§ 34. Результант двух многочленов

Пусть K — произвольное поле и

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m,$$

— два многочлена из $K[x]$. Найдем необходимое и достаточное условие для того, чтобы эти два многочлена имели отличный от константы общий множитель $\varphi(x)$.

С самого начала мы не исключаем возможность того, что $a_0=0$ или $b_0=0$, т. е. степень $f(x)$ может в действительности быть меньше n, а степень $g(x)$ — меньше m. Если многочлен $f(x)$ записан в указанном виде и начинается с (возможно нулевого) слагаемого a_0x^n, то число n называют *формальной степенью многочлена,* а a_0 — *формальным старшим коэффициентом.* Мы будем предполагать, что по крайней мере один из старших коэффициентов a_0, b_0 отличен от нуля.

В этом предположении мы прежде всего покажем следующее: $f(x)$ и $g(x)$ имеют общий множитель, отличный от константы, тогда и только тогда, когда имеет место равенство вида:

$$h(x)f(x)=k(x)g(x), \tag{1}$$

где $h(x)$ имеет степень, не бо́льшую $m-1$, а $k(x)$ — степень, не бо́льшую $n-1$, причем хотя бы один из многочленов h, k не является тождественным нулем.

Действительно, если выполнено (1), то при разложении обеих частей этого равенства на простые множители слева и справа должно стоять одно и то же. Мы можем предположить, что $f(x)$ в действительности имеет степень n (и $a_0\neq 0$); в противном случае мы могли бы поменять ролями $f(x)$ и $g(x)$. Все простые множители многочлена $f(x)$ должны быть и в правой части равенства (1), причем с тем же самым числом повторений. В один лишь многочлен $k(x)$ все эти множители входить в тех же степенях, что и в $f(x)$, не могут, потому что степень $k(x)$ не превосходит $n-1$. Следовательно, некоторый простой множитель многочлена $f(x)$ входит в $g(x)$, что и требовалось.

Обратно, если $\varphi(x)$ — отличный от константы общий множитель $f(x)$ и $g(x)$, то нужно лишь положить

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

и получится (1).

Чтобы подробнее изучить равенство (1), положим

$$h(x)=c_0x^{m-1}+c_1x^{m-2}+\ldots+c_{m-1},$$
$$k(x)=d_0x^{n-1}+d_1x^{n-2}+\ldots+d_{n-1}.$$

Раскрывая скобки в равенстве (1) и сравнивая коэффициенты при одинаковых степенях x^{n+m-1}, x^{n+m-2}, ..., x, 1 слева и справа,

мы приходим к системе уравнений для коэффициентов c_j, и d_j:

$$\begin{aligned}
c_0a_0 &= d_0b_0,\\
c_0a_1+c_1a_0 &= d_0b_1+d_1b_0,\\
c_0a_2+c_1a_1+c_2a_0 &= d_0b_2+d_1b_1+d_2b_0,\\
&\cdots\cdots\cdots\cdots\\
c_{m-2}a_n+c_{m-1}a_{n-1} &= d_{n-2}b_m+d_{n-1}b_{m-1},\\
c_{m-1}a_n &= d_{n-1}b_m.
\end{aligned} \tag{2}$$

Это $n+m$ однородных линейных уравнений относительно $n+m$ величин c_i, d_j. От этих величин требуется, чтобы они не обращались в нуль одновременно. Условием для этого является равенство нулю определителя. Чтобы в определителе не было знака минус, мы перенесем выражения, стоящие в правых частях, налево и в качестве неизвестных рассмотрим величины c_i, $-d_j$. Если после этого еще поменять ролями строки и столбцы определителя (транспонирование относительно главной диагонали), то получится определитель вида

$$R=\begin{vmatrix}
a_0 & a_1 & \dots & a_n & & & \\
 & a_0 & a_1 & \dots & a_n & & \\
 & & \cdots & \cdots & \cdots & & \\
 & & & a_0 & a_1 & \dots & a_n\\
b_0 & b_1 & \dots & b_m & & & \\
 & b_0 & b_1 & \dots & b_m & & \\
 & & \cdots & \cdots & \cdots & & \\
 & & & b_0 & b_1 & \dots & b_m
\end{vmatrix}\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{matrix}$$

(Всюду там, где ничего не написано, подразумеваются нули.)

Этот определитель называется *результантом* многочленов $f(x)$, $g(x)$. Следует отметить, что он является однородным многочленом степени m по переменным a_i и степени n по переменным b_j; далее, его старший член — произведение элементов главной диагонали — равен $a_0^m b_m^n$ и, наконец, результант равен нулю не только тогда, когда f, g имеют общий множитель, но и тогда, когда (вопреки сделанному в начале предположению) $a_0=b_0=0$.

Суммируем все сказанное:

Результант двух многочленов $f(x)$, $g(x)$ является целой рациональной формой от коэффициентов вида (3). Если результант равен нулю, то либо многочлены f, g обладают отличным от константы общим множителем, либо в обоих многочленах равен нулю старший коэффициент. Верно и обратное.

Метод исключения, которому мы здесь следовали, принадлежит Эйлеру; вид (3) результанта известен в основном благодаря исследованиям Сильвестра.

В приведенной формулировке теоремы исключительный случай $a_0 = b_0 = 0$ можно опустить, если вместо того, чтобы говорить о двух многочленах от одной переменной, повести речь о двух однородных многочленах от двух переменных:

$$F(x) = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n,$$
$$G(x) = b_0 x_1^m + b_1 x_1^{m-1} x_2 + \ldots + b_m x_2^m.$$

Исходные многочлены f, g и числа m, n определяют формы F, G совершенно однозначно и наоборот. Каждому разложению на множители многочлена f:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = (p_0 x^r + \ldots + p_r)(q_0 x^s + \ldots + q_s)$$

соответствует разложение формы F:

$$F(x) = a_0 x_1^n + \ldots + a_n x_2^n = (p_0 x_1^r + \ldots + p_r x_2^r)(q_0 x_1^s + \ldots + q_s x_2^s)$$

и аналогичное верно для g и G. Тем самым каждому общему множителю многочленов f и g соответствует общий множитель форм F и G. Обратно, каждое разложение для F или для G, в котором мы полагаем $x_1 = x$, $x_2 = 1$, дает разложение для f или соответственно для g и каждый общий множитель форм F и G дает общий множитель многочленов f и g. Но может оказаться, что некоторый общий множитель форм F и G будет лишь чистой степенью переменной x_2; тогда соответствующий общий множитель многочленов f и g будет константой. Случай, когда F и G делятся на некоторую степень x_2, как раз является случаем равенств $a_0 = b_0 = 0$, и поэтому сформулированные выше два случая в теореме объединяются в единое высказывание: *если результант равен нулю, то F и G имеют отличный от константы однородный общий множитель, и наоборот.*

Выведем теперь важное тождество. Пусть коэффициенты a_μ, b_ν многочленов $f(x)$, $g(x)$ будут неизвестными. Положим

$$\begin{aligned}
x^{m-1} f(x) &= a_0 x^{n+m-1} + a_1 x^{n+m-2} + \ldots + a_n x^{m-1},\\
x^{m-2} f(x) &= \qquad\qquad a_0 x^{n+m-2} + \ldots + a_n x^{m-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
f(x) &= \qquad\qquad\qquad\qquad a_0 x^n + \ldots + a_n,\\
x^{n-1} g(x) &= b_0 x^{n+m-1} + b_1 x^{n+m-2} + \ldots + b_m x^{n-1},\\
x^{n-1} g(x) &= \qquad\qquad b_0 x^{n+m-2} + \ldots + b_m x^{n-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
g(x) &= \qquad\qquad\qquad\qquad b_0 x^m + \ldots + b_m.
\end{aligned}$$

Определитель этой системы уравнений в точности равен R. Исключим справа $x^{n+m-1}, \ldots, x$, для чего осуществим умножения на ми-

норы последнего столбца и соответствующее сложение[1]); тогда получится тождество вида[2])

$$Af + Bg = R, \tag{4}$$

где A и B — целочисленные многочлены от переменных a_μ, b_ν, x.

Задача 1. В терминах определителей дать критерий того, что $f(x)$ и $g(x)$ имеют общие множители степени, не меньшей k.

Задача 2. Для любых двух многочленов второй степени справедливо равенство

$$4R = (2a_0b_2 - a_1b_1 + 2a_2b_0)^2 - (4a_0a_2 - a_1^2)(4b_0b_2 - b_1^2).$$

§ 35. Результант как симметрическая функция корней

Предположим теперь, что оба многочлена $f(x)$ и $g(x)$ полностью разлагаются на линейные множители:

$$f(x) = a_0(x - x_1)(x - x_2)\ldots(x - x_n),$$
$$g(x) = b_0(x - y_1)(x - y_2)\ldots(x - y_m).$$

Тогда коэффициенты a_μ многочлена $f(x)$ являются произведениями a_0 и элементарных симметрических функций корней $x_1, \ldots, x_n$; равным образом, коэффициенты b_ν являются произведениями b_0 и элементарных симметрических функций корней y_k. Результант R является однородным степени m по a_μ и однородным степени n по b_ν; следовательно, результант R равен произведению $a_0^m b_0^n$ на некоторую симметрическую функцию от x_i и y_k.

Пусть корни x_i и y_k рассматриваются сначала как переменные. Многочлен R обращается в нуль при $x_i = y_k$, так как в этом случае многочлены $f(x)$ и $g(x)$ имеют общий линейный множитель. Поэтому R делится на $x_i - y_k$ (§ 28). Так как линейные формы $x_i - y_k$ попарно взаимно просты, результант R делится на произведение

$$S = a_0^m b_0^n \prod_i \prod_k (x_i - y_k). \tag{1}$$

Это произведение можно преобразовать двумя способами. Первый получается из равенства

$$g(x) = b_0 \prod_k (x - y_k)$$

подстановкой $x = x_i$ и составлением произведения

$$\prod_i g(x_i) = b_0^n \prod_i \prod_k (x_i - y_k);$$

---

[1]) См. задачу 9 в § 25. — *Прим. ред.*

[2]) Для форм F и G соответствующее тождество таково:

$$AF + BG = x_2^{n+m-1} R.$$

таким образом,

$$S = a_0^m \prod_i g(x_i). \tag{2}$$

Второй способ получается из равенства

$$f(x) = a_0 \prod_i (x - x_i) = (-1)^n a_0 \prod (x_i - x)$$

и точно так же приводит к

$$S = (-1)^{nm} b_0^n \prod_k f(y_k). \tag{3}$$

Из (2) усматривается, что S является целым и однородным степени n по переменным b, а из (3) видно, что S является целым и однородным степени m по переменным a. Результант R имеет, однако, те же степени по тем же переменным и делится на S; следовательно, R и S совпадают с точностью до некоторого целочисленного множителя. Сравнение слагаемых, которые содержат наивысшую степень элемента b_m, дает слагаемое $+a_0^m b_m^n$ как в R, так и в S; поэтому целочисленный множитель равен 1 и

$$R = S.$$

Таким образом, для R получены три представления (1), (2) и (3). В силу теоремы единственности из § 33 равенство (2) выполняется тождественно по b_ν, а (3) тождественно по a_μ, т. е. (2) имеет место и тогда, когда $g(x)$ не разлагается на линейные множители, а (3) справедливо и тогда, когда на линейные множители не разлагается $f(x)$.

Отсюда легко следует и неразложимость результанта как многочлена от $a_0, \ldots, b_m$, причем неразложимость не только в смысле целочисленных многочленов, а *неразложимость абсолютная*, т. е. неразложимость в кольце многочленов над любым полем. Действительно, если бы R разлагался на два множителя A, B, то A и B можно было бы вновь рассматривать как симметрические функции корней [1]). Так как R делится на $x_1 - y_1$, то A или B — пусть A — делится на эту же разность. Но как симметрическая функция, многочлен A должен (если он делится на $x_1 - y_1$) делиться и на все остальные $x_i - y_k$, а потому и на произведение

$$\prod_i \prod_k (x_i - y_k).$$

Так как

$$R = a_0^m b_0^n \prod \prod (x_i - y_k),$$

---

[1]) В этом месте неявно используется теорема о существовании корня произвольного многочлена в надлежащем расширении поля коэффициентов, о которой речь впереди (§ 39). — *Прим ред.*

для другого множителя B остается лишь одна возможность: $B = a_0^p b_0^q$. Но R как многочлен от a и b делится либо на a_0, либо на b_0; поэтому для B остается возможным лишь равенство $B = 1$. Тем самым неразложимость многочлена R доказана.

Другое доказательство дается в книге Маколей (Macaulay F S). Algebraic theory of modular systems — Cambride, 1916, § 3.

Существует интересная связь между результантом двух многочленов и дискриминантом многочлена. Именно, построим результант $R(f, f')$ для данного многочлена

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = a_0 (x - x_1)(x - x_2) \ldots (x - x_n)$$

и его производной $f'(x)$; тогда согласно (2)

$$R(f, f') = a_0^{n-1} \prod_i f'(x_i). \tag{4}$$

По формуле производной произведения имеем

$$f'(x) = \sum_i a_0 (x - x_1) \ldots (x - x_{i-1})(x - x_{i+1}) \ldots (x - x_n),$$

$$f'(x_i) = a_0 (x_i - x_1) \ldots (x_i - x_{i-1})(x_i - x_{i+1}) \ldots (x_i - x_n).$$

Подставим это в (4); тогда получится равенство

$$R(f, f') = a_0^{2n-1} \prod_{i \neq k} (x_i - x_k),$$

или, если через D обозначить дискриминант многочлена $f(x)$,

$$R(f, f') = \pm a_0 D. \tag{5}$$

Если записать $R(f, f')$ как определитель из § 34, то из первого столбца можно будет вынести множитель a_0; тем самым D становится многочленом от $a_0, \ldots, a_n$. Равенство (5) выполняется, конечно, тождественно по $a_0, \ldots, a_n$ и не зависит от того, разлагается ли $f(x)$ на линейные множители или нет

Задача 1. Результант многочленов f и g является изобарическим веса mn по коэффициентам a и b (§ 33)

Задача 2. Если $y_1, \ldots, y_{n-1}$ являются корнями производной $f'(x)$, то

$$D = n^n a_0^{n-1} \prod_k f(y_k).$$

Задача 3. Дискриминант D обращается в нуль тогда и только тогда, когда $f(x)$ и $f'(x)$ имеют общий множитель. Если такой множитель существует, то в разложении многочлена $f(x)$ на простые множители существует либо кратный множитель, либо множитель с тождественно равной нулю производной.

§ 36. Разложение рациональных функций на простейшие дроби

Разложение рациональных функций на простейшие дроби опирается на следующую теорему о целых рациональных функциях:

Если $g(x)$ и $h(x)$ — два взаимно простых многочлена над полем **K**, *если a — степень многочлена $g(x)$, b — степень многочлена $h(x)$ и если $f(x)$ — произвольный многочлен, степень которого меньше $a+b$, то имеет место тождество*

$$f(x) = r(x)\,g(x) + s(x)\,h(x), \tag{1}$$

в котором $r(x)$ имеет степень, меньшую b, а $s(x)$ имеет степень, меньшую a.

Доказательство. По условию, наибольший общий делитель многочленов $g(x)$ и $h(x)$ равен 1; поэтому справедливо тождество

$$1 = c(x)\,g(x) + d(x)\,h(x).$$

Если это умножить на $f(x)$, то получится

$$f(x) = f(x)\,c(x)\,g(x) + f(x)\,d(x)\,h(x). \tag{2}$$

Чтобы сделать степень $f(x)\,c(x)$ меньшей b, разделим этот многочлен на $h(x)$:

$$f(x)\,c(x) = q(x)\,h(x) + r(x), \tag{3}$$

где степень многочлена $r(x)$ меньше степени многочлена $h(x)$ и, следовательно, меньше b. Подставим (3) в (2):

$$f(x) = r(x)\,g(x) + \{f(x)\,d(x) + q(x)\,g(x)\}\,h(x) = r(x)\,g(x) + s(x)\,h(x).$$

При этом степень левой части и первого слагаемого справа меньше $a+b$; следовательно, и последнее слагаемое справа имеет степень, меньшую $a+b$, так что степень многочлена $s(x)$ меньше a. Тем самым сформулированная выше теорема доказана.

Разделим тождество (1) на $g(x)\,h(x)$; тогда получится разложение дроби $\frac{f(x)}{g(x)\,h(x)}$ на две дроби:

$$\frac{f(x)}{g(x)\,h(x)} = \frac{r(x)}{h(x)} + \frac{s(x)}{g(x)}.$$

В левой части, по условию, степень числителя меньше степени знаменателя. В каждой из дробей справа имеет место то же самое. Если в одной из этих дробей вновь можно разложить знаменатель в произведение двух взаимно простых многочленов, то эту дробь можно будет в свою очередь разложить в сумму двух других дробей. Так можно продолжать до тех пор, пока знаменатели не превратятся в степени простых многочленов. Это доказывает теорему о разложении рациональных функций на простейшие дроби:

Каждая дробь $f(x)/k(x)$, знаменатель которой имеет степень, бо́льшую степени числителя, является суммой простейших дробей, знаменатели которых являются степенями простых многочленов, на которые разлагается знаменатель $k(x)$.

Получаемые таким способом дроби $r(x)/q(x)$ со знаменателями $q(x)=p(x)^t$ можно разлагать дальше. Действительно, если многочлен $p(x)$ имеет степень l, то $q(x)$ имеет степень lt и числитель $r(x)$, степень которого меньше lt, можно сначала разделить на $p(x)^{t-1}$, получив некоторый остаток степени, меньшей $l(t-1)$; затем этот остаток поделить на $p(x)^{t-2}$, получив остаток степени, меньшей $l(t-2)$, и т. д.:

$$\begin{aligned} r(x) &= s_1(x)\,p(x)^{t-1}+r_1(x),\\ r_1(x) &= s_2(x)\,p(x)^{t-2}+r_2(x),\\ &\cdots\cdots\cdots\cdots\cdots\\ r_{t-2}(x) &= s_{t-1}(x)\,p(x)+r_{t-1}(x),\\ r_{t-1}(x) &= s_t(x). \end{aligned}$$

При этом частные $s_1, \ldots, s_k$ имеют степень, меньшую l. Из всех этих равенств в совокупности следует, что

$$r(x)=s_1(x)\,p(x)^{t-1}+s_2(x)\,p(x)^{t-2}+\ldots+s_{t-1}(x)\,p(x)+s_t(x),$$

$$\frac{r(x)}{p(x)^t}=\frac{s_1(x)}{p(x)}+\frac{s_2(x)}{p(x)^2}+\ldots+\frac{s_{t-1}(x)}{p(x)^{t-1}}+\frac{s_t(x)}{p(x)^t}. \tag{4}$$

Так получается вторая формулировка теоремы о разложении в сумму элементарных дробей.

Пусть $f(x)/k(x)$ — дробь, числитель которой имеет степень, меньшую степени знаменателя, и знаменатель которой разлагается на простые множители следующим образом:

$$k(x)=p_1(x)^{t_1}p_2(x)^{t_2}\ldots p_h(x)^{t_h};$$

тогда $f(x)/k(x)$ является суммой простейших дробей, знаменатели которых представляют собой степени $p_\nu(x)^{\mu_\nu}$ $(\mu_\nu \leqslant t_\nu)$, а числители которых имеют степень, меньшую степени входящего в знаменатель неразложимого многочлена $p_\nu(x)$.

Если, в частности, все простые множители $p_\nu(x)$ линейны, то все числители являются константами. В этом важном частном случае разложение в сумму простейших дробей осуществляется очень простым способом: нужно всякий раз отделять дробь с наибольшей возможной степенью знаменателя, и степень знаменателя тем самым будет понижаться. Действительно, запишем знаменатель в виде $k(x)=(x-a)^t g(x)$, где $g(x)$ не делится на $x-a$; тогда

$$\frac{f(x)}{k(x)}=\frac{f(x)}{(x-a)^t g(x)}=\frac{b}{(x-a)^t}+\frac{f(x)-bg(x)}{(x-a)^t g(x)}, \tag{5}$$

где константу b всегда можно определить так, чтобы числитель второй дроби обращался в нуль при $x=a$ и, следовательно, делился на $x-a$:

$$f(a)-bg(a)=0,$$
$$f(x)-bg(x)=(x-a)f_1(x).$$

Вторую дробь в (5) можно теперь сократить на $x-a$ и, продолжая тем же способом, прийти к полному разложению на простейшие дроби.