§ 20. Разложение многочленов на неприводимые множители. Рациональные дроби

Б.М.Верников

Уральский федеральный университет,
Институт естественных наук и математики,
кафедра алгебры и фундаментальной информатики

Неприводимые многочлены (определение)

В арифметике немаловажную роль играет то обстоятельство, что произвольное натуральное число, отличное от 1, можно *разложить на простые множители*, т. е. представить, причем единственным образом, в виде произведения простых чисел. Аналог этого факта имеет место и в теории многочленов. Это находит многочисленные применения как в алгебре, так и за ее пределами (в частности, в математическом анализе). Прежде чем формулировать и доказывать соответствующий факт, дадим необходимое определение и докажем один вспомогательный факт.

Определение

Ненулевой многочлен f над кольцом R называется *неприводимым*, если он необратим в кольце $R[x]$ и его нельзя представить в виде произведения двух многочленов из $R[x]$, степень каждого из которых меньше степени f.

Как мы увидим ниже, неприводимые многочлены как раз и являются аналогом простых чисел.

Неприводимые многочлены (замечание)

В дальнейшем мы многократно будем использовать следующее утверждение, не упоминая его в явном виде.

Замечание о неприводимом многочлене

Если неприводимый многочлен над полем F разложим в произведение двух многочленов, то один из этих многочленов принадлежит F.

Доказательство. Пусть $f \in F[x]$ и $f = gh$. В силу неприводимости, многочлен f необратим. Случай, когда $\deg g, \deg h < \deg f$ невозможен, поскольку f неприводим. Следовательно, степень одного из многочленов g и h равна степени f. Поскольку $\deg f = \deg g + \deg h$, степень другого из них равна 0. Но тогда этот другой многочлен принадлежит F. □

Предложение о неприводимых многочленах

Если f — неприводимый многочлен над полем F и f делит произведение некоторых многочленов g и h над F, то f делит один из этих двух многочленов.

Доказательство. Положим $d = \text{НОД}(g, f)$. Тогда $f = dq$ для некоторого многочлена q. В силу неприводимости f, один из многочленов d и q принадлежит F. Если $d \in F$, то d ассоциирован с 1. Следовательно, 1 является НОД g и f, т. е. эти два многочлена взаимно просты. В силу п. 2) предложения о взаимно простых многочленах (см. §18), в этом случае f делит h. Предположим теперь, что $q \in F$. Следовательно, $d = \frac{1}{q} \cdot f$. Из построения многочлена d вытекает, что $g = ds$ для некоторого многочлена s. Следовательно, $g = \frac{s}{q} \cdot f$, т. е. f делит g. □

Теорема о разложении многочлена на неприводимые множители (1)

Перейдем к утверждению, упоминавшемуся в начале параграфа.

Теорема о разложении многочлена на неприводимые множители

Всякий ненулевой многочлен f над полем F представим в виде

$$f = \alpha g_1 g_2 \cdots g_n, \tag{1}$$

где $\alpha \in F$, а $g_1, g_2, \ldots, g_n$ — неприводимые над F многочлены со старшим коэффициентом 1. Это представление единственно с точностью до порядка следования сомножителей в правой части равенства.

Доказательство. Существование. Пусть $f \in F[x]$ и $f \neq o$. Докажем, что f представим в виде (1). Если f обратим в $F[x]$, то, в силу замечания о необратимых многочленах (см. § 18), $f \in F$. Но тогда f имеет вид (1), где $\alpha = f$, а $n = 0$. Будем далее считать, что f необратим. Если f неприводим над F, то он также представим в виде (1), где, на этот раз, $\alpha = \operatorname{lc}(f)$, $n = 1$ и $g_1 = \frac{1}{\alpha} \cdot f$. Пусть, наконец, f приводим, т. е. $f = gh$, где g и h необратимы в $F[x]$. Из замечания о необратимых многочленах (см. § 18) вытекает, что $\deg g, \deg h \geqslant 1$. Поскольку $\deg f = \deg g + \deg h$, получаем, что $\deg g, \deg h < \deg f$. Мы доказали, что если многочлен f приводим, то его можно разложить в произведение необратимых многочленов g и h, степени которых меньше степени f.

Теорема о разложении многочлена на неприводимые множители (2)

Если какой-то из многочленов g и h приводим, представим его в виде произведения необратимых многочленов меньшей степени. Будем продолжать этот процесс до тех пор, пока среди получаемых многочленов будут встречаться приводимые. Поскольку на каждом шаге степени новых многочленов уменьшаются, через конечное число шагов этот процесс орборвется, и мы представим многочлен f как произведение неприводимых многочленов $h_1, h_2, \ldots, h_n$. Для всякого $i = 1, 2, \ldots, n$ положим $\operatorname{lc}(h_i) = \alpha_i$ и $g_i = \frac{1}{\alpha_i} \cdot h_i$. Пусть $\alpha = \alpha_1 \alpha_2 \cdots \alpha_n$. Тогда выполнено равенство (1), причем $g_1, g_2, \ldots, g_n$ — неприводимые над F многочлены со старшим коэффициентом 1.

Единственность. Пусть $f = \alpha g_1 \cdots g_n = \beta h_1 \cdots h_m$, где $\alpha, \beta \in F$, а $g_1, \ldots, g_n, h_1, \ldots, h_m$ — неприводимые над F многочлены со старшим коэффициентом 1. Ясно, что $\operatorname{lc}(\alpha g_1 \cdots g_n) = \alpha$ и $\operatorname{lc}(\beta h_1 \cdots h_m) = \beta$. Отсюда вытекает, что $\alpha = \beta$, и потому $\alpha g_1 \cdots g_n = \alpha h_1 \cdots h_m$. Разделив обе части последнего равенства на α, получим $g_1 \cdots g_n = h_1 \cdots h_m$. Многочлен g_1 делит $h_1 \cdots h_m$. В силу предложения о неприводимых многочленах g_1 делит h_i для некоторого $1 \leqslant i \leqslant m$. Не ограничивая общности, можно считать, что $i = 1$ (в противном случае можно переставить сомножители в произведении $h_1 \cdots h_m$). Итак, $h_1 = w g_1$ для некоторого многочлена w. Поскольку многочлен g_1 неприводим, он необратим, а значит $g_1 \notin F$. Следовательно, $w \in F$.

Поскольку $\operatorname{lc}(h_1) = w \cdot \operatorname{lc}(g_1) = w \cdot 1 = w$, получаем, что $w = 1$, и потому $h_1 = g_1$. Без ограничения общности будем считать, что $n \leqslant m$. Если $n = m = 1$, то все доказано. Случай, когда $n = 1$, а $m > 1$, невозможен, так как в этом случае $\deg h_1 \cdots h_m > \deg h_1 = \deg g_1$ вопреки равенству $g_1 = h_1 \cdots h_m$. Пусть теперь $n > 1$. Тогда $g_1 g_2 \cdots g_n = g_1 h_2 \cdots h_m$, откуда $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Если $g_2 \cdots g_n - h_2 \cdots h_m \neq o$, то $\deg\big(g_1(g_2 \cdots g_n - h_2 \cdots h_m)\big) \geqslant \deg g_1 > 0$ вопреки равенству $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Следовательно, $g_2 \cdots g_n = h_2 \cdots h_m$.

Рассуждая так же, как в предыдущем абзаце, получаем, что $g_2 = h_2$. Если $m = n = 2$, то все доказано. Случай, когда $n = 2$, а $m > 2$, невозможен, так как в этом случае $\deg h_2 \cdots h_m > \deg h_2 = \deg g_2$ вопреки равенству $g_2 = h_2 \cdots h_m$. Пусть теперь $n > 2$. Тогда $g_2 g_3 \cdots g_n = g_2 h_3 \cdots h_m$, откуда $g_2(g_3 \cdots g_n - h_3 \cdots h_m) = o$. Как и в предыдущем параграфе, отсюда выводится, что $g_3 \cdots g_n = h_3 \cdots h_m$. Повторяя этот процесс, мы в конце концов получим, что $g_i = h_i$ для всех $i = 1, 2, \ldots, n$. Если $n = m$, то все доказано. Если же $n < m$, то $g_1 \cdots g_n = g_1 \cdots g_n h_{n+1} \cdots h_m$. Но это невозможно, так как $\deg(g_1 \cdots g_n h_{n+1} \cdots h_m) > \deg(g_1 \cdots g_n)$. □

Кратность неприводимого множителя

В силу теоремы о разложении многочлена на неприводимые множители произвольный многочлен f над полем F единственным образом (с точностью до порядка следования сомножителей) представим в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}, \tag{2}$$

где $\alpha \in F$, а $p_1, p_2, \ldots, p_m$ — попарно различные неприводимые над полем F многочлены со старшим коэффициентом 1.

Определение

Если выполнено равенство (2), то многочлены $p_1, p_2, \ldots, p_m$ называются *неприводимыми множителями* многочлена f, а число k_i (где $1 \leq i \leq m$) — *кратностью* неприводимого множителя p_i.

Поскольку степень произведения многочленов над полем равна сумме степеней сомножителей, выполнено равенство

$$\deg f = \sum_{i=1}^{m} k_i \deg p_i.$$

Производная многочлена (1)

Определение

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ — многочлен над кольцом R. Если $n > 0$, то *производной* многочлена $f(x)$ называется многочлен $n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \cdots + \alpha_1$, обозначаемый через $f'(x)$. Если $n = 0$ или $f(x) = o$, то, по определению, $f'(x) = o$.

- В случае многочленов над полем $\mathbb{R}$ производная многочлена во введенном только что смысле совпадает с производной многочлена как функции от одной переменной в смысле математического анализа.
- Отметим еще, что степень производной многочлена степени n не обязательно равна $n-1$. Рассмотрим, например, многочлен $f(x) = x^p$ над полем $\mathbb{Z}_p$, где p — произольное простое число. Тогда $f'(x) = px^{p-1} = o$, поскольку в $\mathbb{Z}_p$ выполнено равенство $px = 0$ для произвольного $x \in \mathbb{Z}_p$. Таким образом, $\deg f(x) = p$, но $\deg f'(x) = -\infty$. С другой стороны, очевидно, что
  а) для любого многочлена f над любым кольцом R выполнено неравенство $\deg f' \leq \deg f - 1$,
  б) если f — многочлен над полем характеристики 0, степень которого > 0, то $\deg f' = \deg f - 1$.

Лемма о свойствах производной

Если $f(x)$ и $g(x)$ — многочлены над кольцом R, $\alpha \in R$, а m — натуральное число такое, что $m > 1$, то:

1) $(\alpha f)' = \alpha f'$,
2) $(f + g)' = f' + g'$,
3) $(fg)' = f'g + fg'$,
4) $(f^m)' = mf^{m-1}f'$.

Доказательство. Свойства 1) и 2) непосредственно вытекают из определений суммы многочленов, умножения многочлена на константу и производной многочлена.

3) В силу свойств 1) и 2) свойство 3) достаточно доказать в случае, когда $f(x) = x^n$, а $g(x) = x^m$ для некоторых n и m. В самом деле, в этом случае

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1},$$
$$f'g = nx^{n-1} \cdot x^m = nx^{n+m-1}, \quad \text{и}$$
$$fg' = x^n \cdot mx^{m-1} = mx^{n+m-1}.$$

Следовательно, $f'g + g'f = (n+m)x^{n+m-1} = (fg)'$.

4) Докажем это свойство индукцией по m. Если $m = 2$, то, используя свойство 3), имеем $(f^m)' = (f \cdot f)' = f'f + ff' = 2ff'$. Это доказывает базу индукции. Чтобы доказать шаг индукции, предположим, что $m > 2$. Используя предположение индукции и свойство 3), имеем

$$\begin{aligned}(f^m)' = (f^{m-1}f)' = (f^{m-1})'f + f^{m-1}f' = \\ = (m-1)f^{m-2}f'f + f^{m-1}f' = \\ = (m-1)f^{m-1}f' + f^{m-1}f' = mf^{m-1}f'.\end{aligned}$$

Это завершает доказательство. □

Лемма о неприводимом многочлене и его производной

Если p — неприводимый многочлен над полем F, то $\text{НОД}(p, p') = 1$.

Доказательство. Положим $d = \text{НОД}(p, p')$. Тогда $p = dq$ и $p' = dr$ для некоторых многочленов q и r. Если $\deg q = 0$, то

$$\deg p = \deg dq = \deg d + \deg q = \deg d \leq \deg p' \leq \deg p - 1.$$

Полученное противоречие показывает, что $\deg q \neq 0$, и потому $q \notin F$. Следовательно, $d \in F$. В частности, d ассоциирован с 1. Учитывая замечание о многочленах, ассоциированных с НОД (см. § 18), мы получаем, что $\text{НОД}(p, p') = 1$. □

Предложение о неприводимых множителях многочлена и его производной

Пусть f — многочлен над полем F характеристики 0, а p — неприводимый множитель многочлена f кратности k. Если $k = 1$, то p не делит f'. Если $k > 1$, то p является неприводимым множителем многочлена f' кратности $k - 1$.

Доказательство. Обозначим через g произведение всех неприводимых множителей многочлена f, отличных от p, и старшего коэффициента многочлена f. Тогда $f = p^k g$ и НОД$(p, g) = 1$. В силу леммы о неприводимом многочлене и его производной НОД$(p, p') = 1$. Из п. 3) предложения о взаимно простых многочленах (см. § 18) вытекает теперь, что НОД$(p, p'g) = 1$. В частности, p не делит $p'g$. Если $k = 1$, то $f = pg$, и потому $f' = (pg)' = p'g + pg'$. Если бы p делил f', то p делил бы и $p'g = f' - pg'$. Следовательно, если $k = 1$, то p не делит f'. Пусть теперь $k > 1$. Тогда

$$f' = (p^k g)' = (p^k)'g + p^k g' = kp^{k-1}p'g + p^k g' = p^{k-1}(kp'g + pg').$$

Чтобы завершить доказательство, осталось проверить, что p не делит $kp'g + pg'$. Предположим, напротив, что p делит $kp'g + pg'$. Тогда, очевидно, p делит и $kp'g$, т. е. $kp'g = pa$ для некоторого многочлена a. Обозначим единицу поля F через e, чтобы не путать ее с числом 1. Тогда $pa = kep'g$. Если $ke = 0$, то $kx = kex = 0 \cdot x = 0$ для всякого $x \in F$. Но это невозможно, поскольку характеристика поля F равна 0. Таким образом, $ke \neq 0$, и потому $p'g = pb$, где $b = \frac{1}{ke} \cdot a$. Следовательно, p делит $p'g$. Но выше было показано, что это не так. □

- В частности, заключение предложения о неприводимых множителях многочлена и его производной справедливо для многочленов над полями $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.

Отделение кратных множителей

Пусть $f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ — разложение на неприводимые множители многочлена f над полем F нулевой характеристики. Из предложения о неприводимых множителях многочлена и его производной вытекает, что $\text{НОД}(f, f') = p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1}$. Многочлен

$$\frac{f}{\alpha \cdot \text{НОД}(f, f')} = p_1 p_2 \cdots p_m$$

есть произведение всех попарно различных неприводимых множителей многочлена f. Если все неприводимые множители многочлена f имеют кратность 1, то $\text{НОД}(f, f') = 1$. В противном случае, повторяя проведенные выше рассуждения применительно к многочлену $f_1 = \text{НОД}(f, f')$, можно найти произведение всех попарно различных неприводимых множителей этого многочлена, то есть произведение всех попарно различных неприводимых множителей многочлена f, имеющих кратность > 1. Сравнивая его с найденным ранее произведением всех попарно различных неприводимых множителей многочлена f, можно выделить все неприводимые множители этого многочлена, имеющие кратность 1. Далее, с помощью многочлена $f_2 = \text{НОД}(f_1, f_1')$ можно найти все неприводимые множители многочлена f, имеющие кратность 2, и т. д. Ясно, что рано или поздно этот процесс оборвется, и мы найдем кратности всех неприводимых множителей многочлена f. Описанный процесс называется *процессом отделения кратных множителей* многочлена f.

Связь неприводимости с отсутствием корней у многочленов малых степеней

Очевидно, что любой многочлен степени 1 над любым полем неприводим.

Предложение о неприводимых многочленах малых степеней

Многочлен $f(x)$ степени 2 или 3 над произвольным полем F неприводим над F тогда и только тогда, когда он не имеет корней в F.

Доказательство. Необходимость. Произвольный многочлен степени > 1, который имеет корень, приводим в силу следствия из теоремы Безу (см. § 19).

Достаточность. Предположим, что $2 \leqslant \deg f \leqslant 3$ и f приводим над F. Тогда $f = gh$ для некоторых необратимых многочленов g и h над F. В силу замечания о необратимых многочленах (см. § 18) многочлены g и h имеют степень > 0. Поскольку $\deg g + \deg h = \deg f \leqslant 3$, хотя бы один из многочленов g и h линеен. Без ограничения общности можно считать, что $\deg g = 1$ и $\operatorname{lc} g = 1$ (если $\operatorname{lc} g = \alpha \neq 1$, мы можем заменить g на $\frac{1}{\alpha} \cdot g$, а h на αh). Иными словами, $g = x - a$ для некоторого $a \in F$. Но тогда $f = (x - a)h$ и a является корнем многочлена f, лежащим в F. □

Аналог этого предложения для многочленов степени > 3 места не имеет. Например, многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим над полями $\mathbb{R}$ и $\mathbb{Q}$, но не имеет действительных (и, в частности, рациональных) корней.

Рациональные дроби (1)

Определение

Рациональной дробью над полем F называется функция вида $\frac{f}{g}$, где $f, g \in F[x]$ и $g \neq o$. Рациональная дробь $\frac{f}{g}$ называется *правильной*, если $\deg f < \deg g$ и $f \neq o$. Рациональная дробь $\frac{f}{g}$ называется *простейшей*, если существуют многочлен p, неприводимый над полем F, и натуральное число n такие, что $g = p^n$ и $\deg f < \deg p$.

Очевидно, что всякая простейшая дробь является правильной.

Теорема о рациональных дробях

Любая правильная рациональная дробь над произвольным полем может быть представлена, причем единственным образом, в виде суммы простейших дробей.

- Возможность представить произвольную правильную рациональную дробь над полем $\mathbb{R}$ в виде суммы простейших дробей играет важную роль в курсе математического анализа при вычислении интегралов от дробно-рациональных функций.

Доказательство. Существование. Пусть $\frac{f}{g}$ — правильная рациональная дробь. Без ограничения общности можно считать, что $\mathrm{lc}(g) = 1$ (в противном случае можно разделить каждый из многочленов f и g на $\mathrm{lc}(g)$). Пусть $g = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ — разложение многочлена g на неприводимые множители. Доказательство того, что дробь $\frac{f}{g}$ может быть представлена в виде суммы простейших дробей разобьем на два шага. На первом шаге мы докажем, что дробь $\frac{f}{g}$ может быть представлена как сумма правильных рациональных дробей, у каждой из которых знаменатель есть степень неприводимого многочлена. На втором шаге будет доказано, что правильная рациональная дробь, у которой знаменатель есть степень неприводимого многочлена, можно представить как сумму простейших дробей.

Шаг 1. Докажем индукцией по n, что

$$\frac{f}{g} = \frac{f_1}{p_1^{k_1}} + \frac{f_2}{p_2^{k_2}} + \cdots + \frac{f_n}{p_n^{k_n}} \tag{3}$$

для некоторых многочленов $f_1, f_2, \ldots, f_n$ таких, что $\deg f_i < \deg p_i^{k_i}$ для всех $i = 1, 2, \ldots, n$.

База индукции очевидна: если $n = 1$, то равенство (3) выполнено при $f_1 = f$.

Шаг индукции. Пусть $n > 1$. Положим $g_1 = p_1^{k_1}$ и $g_2 = p_2^{k_2} \cdots p_n^{k_n}$. Многочлены g_1 и g_2 взаимно просты. В силу следствия о взаимно простых многочленах (см. § 18) существуют многочлены u и v такие, что $ug_1 + vg_2 = 1$. Следовательно, $f = fug_1 + fvg_2$. Разделим fu на g_2 с остатком: $fu = qg_2 + r$, где $\deg r < \deg g_2$. Имеем:
$f = fug_1 + fvg_2 = (qg_2 + r)g_1 + fvg_2 = rg_1 + (qg_1 + fv)g_2$, откуда

$$f - rg_1 = (qg_1 + fv)g_2. \tag{4}$$

Положим $f_1 = qg_1 + fv$ и $f_2 = r$. Тогда $f = f_2 g_1 + f_1 g_2$, откуда

$$\frac{f}{g} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}.$$

По предположению индукции дробь $\frac{f_2}{g_2}$ представима как сумма правильных рациональных дробей, у каждой из которых знаменатель есть степень неприводимого многочлена. Для того, чтобы завершить шаг 1, осталось проверить, что дробь $\frac{f_1}{g_1}$ является правильной, т. е. что $\deg f_1 < \deg g_1$. Последнее неравенство равносильно тому, что $\deg f_1 + \deg g_2 < \deg g_1 + \deg g_2$. Учитывая (4) получаем, что

$$\begin{aligned}\deg f_1 + \deg g_2 = \deg(f_1 g_2) = \deg(qg_1 + fv)g_2 = \\ = \deg(f - rg_1) \leqslant \max\{\deg f, \deg(rg_1)\}.\end{aligned}$$

Итак, для завершения шага 1 достаточно установить, что $\deg f < \deg g_1 + \deg g_2$ и $\deg(rg_1) < \deg g_1 + \deg g_2$. Оба этих неравенства проверяются легко: $\deg f < \deg g = \deg(g_1 g_2) = \deg g_1 + \deg g_2$ и $\deg(rg_1) = \deg r + \deg g_1 < \deg g_2 + \deg g_1$.

Шаг 2. Осталось доказать, что каждое из слагаемых, стоящих в правой части равенства (3), представимо в виде суммы простейших дробей. Иными словами, мы можем далее считать, что $g = p^k$, где p — неприводимый многочлен. Если $k = 1$, то $\frac{f}{g}$ — простейшая дробь, и все доказано. Пусть теперь $k > 1$. Разделим f на p^{k-1} с остатком: $f = a_1 p^{k-1} + b_1$, где $\deg b_1 < \deg p^{k-1}$. Из последнего неравенства вытекает, что $\deg b_1 < \deg(a_1 p^{k-1})$, и потому $\deg f = \deg(a_1 p^{k-1} + b_1) = \deg(a_1 p^{k-1})$. Если $\deg a_1 \geqslant \deg p$, то

$$\deg f = \deg(a_1 p^{k-1}) = \deg a_1 + \deg p^{k-1} = \deg a_1 + (k-1)\deg p \geqslant$$
$$\geqslant \deg p + (k-1)\deg p = k \deg p = \deg p^k = \deg g$$

вопреки неравенству $\deg f < \deg g$. Следовательно, $\deg a_1 < \deg p$.

Далее, разделим b_1 на p^{k-2} с остатком: $b_1 = a_2 p^{k-2} + b_2$, где $\deg b_2 < \deg p^{k-2}$. Из последнего неравенства вытекает, что $\deg b_2 < \deg(a_2 p^{k-2})$, и потому $\deg b_1 = \deg(a_2 p^{k-2} + b_2) = \deg(a_2 p^{k-2})$. Если $\deg a_2 \geqslant \deg p$, то

$$\deg b_1 = \deg(a_2 p^{k-2}) = \deg a_2 + \deg p^{k-2} = \deg a_2 + (k-2)\deg p \geqslant$$
$$\geqslant \deg p + (k-2)\deg p = (k-1)\deg p = \deg p^{k-1}$$

вопреки неравенству $\deg b_1 < \deg p^{k-1}$. Следовательно, $\deg a_2 < \deg p$.

Продолжая этот процесс, получаем цепочку равенств $b_2 = a_3 p^{k-3} + b_3$, $\ldots$, $b_{k-2} = a_{k-1} p + b_{k-1}$, где $\deg b_3 < \deg p^{k-3}$, $\ldots$, $\deg b_{k-1} < \deg p$ и $\deg a_3, \ldots, \deg a_{k-1} < \deg p$. Учитывая, что

$$f = a_1 p^{k-1} + b_1 = a_1 p^{k-1} + a_2 p^{k-2} + b_2 = \cdots =$$
$$= a_1 p^{k-1} + a_2 p^{k-2} + \cdots + a_{k-1} p + b_{k-1},$$

имеем:

$$\frac{f}{g} = \frac{a_1 p^{k-1} + a_2 p^{k-2} + \cdots + a_{k-1} p + b_{k-1}}{p^k} = \frac{a_1}{p} + \frac{a_2}{p^2} + \cdots + \frac{a_{k-1}}{p^{k-1}} + \frac{b_{k-1}}{p^k}.$$

Поскольку $\deg a_1, \deg a_2, \ldots, \deg a_{k-1}, \deg b_{k-1} < \deg p$, мы представили $\frac{f}{g}$ как сумму простейших дробей.

Единственность. Предположим, что дробь $\frac{f}{g}$ двумя разными способами представлена в виде суммы простейших дробей:

$$\frac{f}{g} = \frac{a_1}{p_1^{k_1}} + \cdots + \frac{a_m}{p_m^{k_m}} \quad \text{и} \quad \frac{f}{g} = \frac{b_1}{q_1^{\ell_1}} + \cdots + \frac{b_n}{q_n^{\ell_n}} \tag{5}$$

(имеется в виду, что некоторые из многочленов $p_1, \ldots, p_m$, равно как и некоторые из многочленов $q_1, \ldots, q_n$ могут совпадать). Разумеется, все слагаемые в правых частях двух последних равенств можно считать ненулевыми. Тогда

$$\frac{a_1}{p_1^{k_1}} + \cdots + \frac{a_m}{p_m^{k_m}} = \frac{b_1}{q_1^{\ell_1}} + \cdots + \frac{b_n}{q_n^{\ell_n}}. \tag{6}$$

Если левая и правая части равенства (6) содержат одно и то же слагаемое, вычеркнем его из обеих частей равенства. Проделаем это для всех пар одинаковых слагаемых. Если после этого получится равенство $0 = 0$, значит исходно мы имели два совпадающих разложения дроби $\frac{f}{g}$ в сумму простейших дробей. В этом случае доказательство завершено.

Предположим, что в результате описанного выше процесса в равенстве (6) будут вычеркнуты не все слагаемые. Перенеся все оставшиеся слагаемые в левую часть равенства и изменив обозначения, мы получим равенство вида

$$\frac{s_1}{t_1} + \cdots + \frac{s_r}{t_r} = 0. \tag{7}$$

Все слагаемые в левой части этого равенства являются простейшими дробями. В частности, $t_1 = p^k$ для некоторого неприводимого многочлена p и некоторого числа k. Если $r = 1$, то единственное слагаемое в левой части равенства (7), совпадающее, с точностью до знака, с одним из слагаемых равенства (6), равно нулю. Но это противоречит нашей договоренности о том, что все слагаемые в правых частях равенств (5) являются ненулевыми. Следовательно, $r > 1$. Без ограничения общности можно считать, что, для всякого $i = 2, \ldots, r$, либо $t_i = p^\ell$, где $\ell < k$, либо t_i — степень неприводимого многочлена, отличного от p (если это не так, то слагаемые в левой части равенства (7) можно поменять местами). Обозначим через Q общий знаменатель всех дробей, стоящих в левой части равенства (7), у которых знаменатель имеет второй из указанных только что видов. Из п. 3) предложения о взаимно простых многочленах (см. § 18) вытекает, что многочлены p и Q взаимно просты.

Умножим обе части равенства (7) на $p^{k-1}Q$. Получим равенство вида $\frac{s_1 Q}{p} + R = 0$, где R — некоторый многочлен. Следовательно, $s_1 Q = -pR$. Таким образом, многочлен p делит $s_1 Q$. Напомним, что p взаимно прост с Q. По п. 2) предложения о взаимно простых многочленах (см. § 18) отсюда вытекает, что p делит s_1. Но это невозможно, так как дробь $\frac{s_1}{p^k}$ является простейшей, и потому $\deg s_1 < \deg p$. □