Окончание доказательства теоремы

Предположим, что многочлен f разлагается в произведение неприводимых многочленов двумя способами $f = p_1 p_2 \dots p_m$ и $f = q_1 q_2 \dots q_\ell$, где $m \leq \ell$. Индукцией по m покажем, что $m = \ell$ и для некоторой перестановки $(i_1, i_2, \dots, i_m)$ чисел $\{1, 2, \dots, m\}$ каждый многочлен p_j ассоциирован с q_{i_j} при $j = 1, 2, \dots, m$. Пусть $m = 1$. Так как p_1 – неприводимый многочлен, ясно, что $\ell = 1$ и $p_1 = q_1$. Предположим, что $m > 1$ и для любого $1 \leq k < m$ утверждение доказано. Так как $p_1 | (q_1 \cdot q_2 \dots q_\ell)$, согласно предложению сл.10 p_1 ассоциирован с q_{i_1} для некоторого $1 \leq i_1 \leq m$. Пусть $p_1 = \alpha q_{i_1}$. Сокращая в равенстве $p_1 p_2 \dots p_m = q_1 q_2 \dots q_\ell$ на q_{i_1}, получим равенство $\alpha p_2 \dots p_m = \prod_{j \neq i_1} q_j$. Многочлен αp_2 является неприводимым. Положим $r_2 = \alpha p_2$ и $r_j = p_j$ для $j = 3, \dots, m$. Применяя предположение индукции к равенству $r_2 r_3 \dots r_m = \prod_{j \neq i_1} q_j$, получаем, что $m - 1 = \ell - 1$ и для некоторой перестановки $(i_2, \dots, i_m)$ чисел $\{1, 2, \dots, m\} \backslash \{i_1\}$ каждый многочлен r_j, а следовательно и p_j, ассоциирован с q_{i_j} при $j = 2, \dots, m$. Таким образом, шаг индукции доказан.
Доказательство теоремы закончено.⇑

Доказательство теоремы о разложении многочлена на неприводимые множители является примером доказательства чистого существования. Никакого алгоритма для разложения многочлена на неприводимые множители из этого доказательства извлечь нельзя.

Разложение многочлена на неприводимые множители

Пусть F – поле. Из теоремы сл.11 следует, что любой многочлен $f \in F[x]$ степени больше нуля может быть единственным образом представлен в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}, \tag{1}$$

где α — старший коэффициент многочлена f, $p_1, p_2, \dots, p_m$ – все различные неприводимые над полем F делители многочлена f, имеющие старший коэффициент 1, $k_1, k_2, \dots, k_m$ – натуральные числа. Это представление называется *разложением многочлена f на неприводимые множители над полем F*. Число k_j в равенстве (1) называется *кратностью* неприводимого многочлена p_j в разложении многочлена f на неприводимые множители. Нетрудно проверить, что $\deg(f) = \sum_{j=1}^{m} k_j \deg(p_j)$.

Наблюдение (критерий делимости многочлена на многочлен через разложение на неприводимые множители)

Многочлен f делит многочлен g тогда и только тогда, когда их разложения на неприводимые множители над одним и тем же полем связаны следующим образом: каждый неприводимый множитель многочлена f кратности k является также неприводимым множителем многочлена g кратности m и $k \leq m$.

Представление НОД через разложение многочлена на неприводимые множители

НОД ненулевых многочленов легко выразить через их разложения на неприводимые множители над одним и тем же полем. Пусть $f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} q_1^{\ell_1} \dots q_s^{\ell_s}$, $g = \beta p_1^{n_1} p_2^{n_2} \dots p_m^{n_m} q_{s+1}^{\ell_{s+1}} \dots q_t^{\ell_t}$, где $p_1, p_2, \dots, p_m$ – все общие неприводимые множители многочленов f и g. Тогда

$$(f, g) = p_1^{\min\{k_1, n_1\}} p_2^{\min\{k_2, n_2\}} \dots p_m^{\min\{k_m, n_m\}}. \tag{2}$$

В самом деле, старший коэффициент в правой части равенства (2) равен 1. Если степень неприводимого многочлена p^k делит и f и g, то согласно наблюдению сл.13 $p = p_j$ для некоторого $j = 1, 2, \dots, m$ и $k \le k_j$, $k \le n_j$. Следовательно, правая часть равенства (2) делится на любой общий делитель многочленов f и g и в то же время является их общим делителем.

Определение

Наименьшим общим кратным (НОК) многочленов f и g называется многочлен h такой, что $f|h$, $g|h$ и для любого многочлена k из того, что $f|k$, $g|k$ следует, что $h|k$.

Из определения следует, что если НОК многочленов f и g существует, то этот многочлен определяется однозначно с точностью до ассоциированности.

Предложение

Пусть f и g – многочлены. Тогда $f \cdot g = h \cdot d$, где h – некоторое НОК, а $d = (f, g)$ – НОД многочленов f, g.

$\Downarrow$Если $f = 0$ или $g = 0$, то НОК этих многочленов равен 0 и доказывать нечего. Предположим, что $f \neq 0$ и $g \neq 0$. Тогда $f = f_1 d$, $g = g_1 d$ и $(f_1, g_1) = 1$. В самом деле, $fu + gv = d$ для некоторых многочленов u, v, откуда, сократив на d, получаем $f_1 u + g_1 v = 1$. Положим $h = f_1 g_1 d = f g_1$ и докажем, что h является НОК многочленов f и g. Очевидно, что $f|h$ и $g|h$. Пусть $f|k$ и $g|k$ для некоторого многочлена k. Тогда ясно, что $k = k_1 f$ и $k = k_2 g$. Следовательно, $k_1 f_1 d = k_2 g_1 d$ и $k_1 f_1 = k_2 g_1$. Так как $(f_1, g_1) = 1$, имеем $g_1|k_1$ и поэтому $h = f g_1 | k_1 f = k$.$\Uparrow$

Обозначение НОК

Если $f \neq 0$ и $g \neq 0$, то НОК этих многочленов – ненулевой многочлен. Через $[f, g]$ будем обозначать НОК многочленов f и g, старший коэффициент которого равен единице.

Так же как и НОД, НОК ненулевых многочленов можно выразить через их разложения на неприводимые множители над одним и тем же полем. Пусть $f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} q_1^{\ell_1} \dots q_s^{\ell_s}$, $g = \beta p_1^{n_1} p_2^{n_2} \dots p_m^{n_m} q_{s+1}^{\ell_{s+1}} \dots q_t^{\ell_t}$, где $p_1, p_2, \dots, p_m$ – все общие неприводимые множители многочленов f и g. Тогда, применив рассуждения, подобные проведенным на сл.14, можно убедиться, что

$$[f, g] = p_1^{\max\{k_1, n_1\}} p_2^{\max\{k_2, n_2\}} \dots p_m^{\max\{k_m, n_m\}} q_1^{\ell_1} \dots q_s^{\ell_s} q_{s+1}^{\ell_{s+1}} \dots q_t^{\ell_t}. \qquad (3)$$

Можно доказать эту формулу и другим способом, применив предложение сл.15 и формулу (2) и используя очевидное равенство $\max\{k, n\} + \min\{k, n\} = k + n$.

Глава IV. Многочлены

§ 3. Производная многочлена

А. Я. Овсянников

Уральский федеральный университет
Институт естественных наук и математики
Департамент математики, механики и компьютерных наук

Основы алгебры для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Определение

Пусть F – поле, $f \in F[x]$. *Производной* многочлена $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0$ называется многочлен $n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \ldots + \alpha_1$, обозначаемый через f'.
В частности, если $f = \alpha_0$, то $f' = 0$.

Это формальное определение совпадает с определением, даваемом в математическом анализе для многочленов из $\mathbb{R}[x]$. Из него очевидным образом следует, что

$$(f+g)' = f' + g'; \quad (\alpha f)' = \alpha f' \text{ для любого } \alpha \in F. \tag{1}$$

Докажем, что имеет место обычная формула дифференцирования произведения

$$(fg)' = f'g + fg'. \tag{2}$$

Доказательство формулы дифференцирования произведения

Сначала заметим, что $(x^m x^n)' = (x^{m+n})' = (m+n)x^{m+n-1}$ и $x^m(x^n)' + (x^m)'x^n = x^m n x^{n-1} + m x^{m-1} x^n = (m+n)x^{m+n-1}$, т.е. $(x^m x^n)' = x^m(x^n)' + (x^m)'x^n$ для любых натуральных m, n. Если $m = 0$ и $n > 0$ или $m > 0$ и $n = 0$, то также $(x^m x^n)' = (m+n)x^{m+n-1}$. Таким образом, для любых неотрицательных целых чисел m, n справедливо

$$(x^m x^n)' = x^m(x^n)' + (x^m)'x^n. \tag{3}$$

Далее, пусть $f = \sum\limits_{k=0}^{n} \alpha_k x^k$ и $g = \sum\limits_{\ell=0}^{m} \beta_\ell x^\ell$. Тогда $f \cdot g = \sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell x^{k+\ell}$ и согласно (1) и (3) $(f \cdot g)' = \left(\sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell x^{k+\ell}\right)' = \sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell (x^{k+\ell})' =$

$\sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell ((x^k)'x^\ell + x^k(x^\ell)') = \sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell (x^k)'x^\ell + \sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k \beta_\ell x^k (x^\ell)' =$

$\sum\limits_{k=0}^{n} \alpha_k (x^k)' \sum\limits_{\ell=0}^{m} \beta_\ell x^\ell + \sum\limits_{k=0}^{n} \alpha_k x^k \sum\limits_{\ell=0}^{m} \beta_\ell (x^\ell)' =$

$\left(\sum\limits_{k=0}^{n} \alpha_k x^k\right)' \sum\limits_{\ell=0}^{m} \beta_\ell x^\ell + \sum\limits_{k=0}^{n} \alpha_k x^k \left(\sum\limits_{\ell=0}^{m} \beta_\ell x^\ell\right)' = f'g + fg'$. Таким образом, равенство (2) доказано.

Производная степени многочлена

Из формулы (2) по индукции выведем формулу для производной степени многочлена

$$(f^m)' = mf^{m-1}f'. \tag{4}$$

База индукции. При $m = 1$ формула получается из соглашения $f^0 = 1$.
При $m = 2$ имеем $(f^2)' = (f \cdot f)' = f'f + ff' = 2ff'$.
Шаг индукции. Предположим, что для всех $2 < m \leq n$ формула (4) справедлива. Имеем $(f^{n+1})' = (f \cdot f^n)' = f'f^n + f(f^n)' =$
$f'f^n + f(nf^{n-1}f') = f^nf' + nf^nf' = (n+1)f^nf'$. Таким образом,
$(f^{n+1})' = (n+1)f^nf'$. Шаг индукции доказан.

Пусть f – многочлен степени n над полем F, $n \geq 1$ и пусть $\alpha \in F$. Очевидно, что имеет место равенство (называемое *разложением многочлена по степеням $x - \alpha$*)

$$f(x) = \lambda_0 + \lambda_1(x-\alpha) + \lambda_2(x-\alpha)^2 + \ldots + \lambda_n(x-\alpha)^n \qquad (5)$$

для некоторых однозначно определенных элементов $\lambda_j \in F$ $(j = 1, 2, \ldots, n)$. Чтобы найти значения λ_j, подставим в (5) вместо x элемент α, получим $\lambda_0 = f(\alpha)$. Затем продифференцируем равенство (5), получим

$$f'(x) = \lambda_1 + 2\lambda_2(x-\alpha) + \ldots + n\lambda_n(x-\alpha)^{n-1}. \qquad (6)$$

Подставим в (6) вместо x элемент α, получим $\lambda_1 = f'(\alpha)$. Продолжая таким образом, получим (продифференцировав k раз) $f^{(k)}(x) =$ $= k!\lambda_k + (k+1)!\lambda_{k+1}(x-\alpha) + \ldots + n(n-1)\cdots(n-k+1)\lambda_n(x-\alpha)^{n-k}$, откуда, подставив вместо x элемент α, будем иметь $k!\lambda_k = f^{(k)}(\alpha)$ и $\lambda_k = \frac{1}{k!}f^{(k)}(\alpha)$. Теперь из (5) получается

Формула Тейлора для многочлена

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

Напомним, что через $\mathrm{char}(F)$ обозначается характеристика поля F (см. сл.8 §4 гл.III).

Предложение

Пусть F – поле, $\mathrm{char}(F) = 0$ и $f \in F[x]$, p — неприводимый множитель многочлена f кратности k. Если $k = 1$, то p не делит f'. Если $k > 1$, то p – неприводимый множитель многочлена f' кратности $k - 1$.

⇓Пусть $f = p^k g$, где $(p, g) = 1$.
Если $k = 1$, то $f' = (pg)' = p'g + pg'$. Так как $\deg(p') = \deg(p) - 1$, по определению неприводимого многочлена $(p, p') = 1$. Из $(p, g) = 1$, в силу утверждения 3 предложения сл.7 §2, следует, что $(p, p'g) = 1$.
Следовательно, p не делит f'.
Пусть $k > 1$. Тогда $k \neq 0$ в поле F, и
$f' = (p^k g)' = kp^{k-1}p'g + p^k g' = p^{k-1}(kp'g + pg')$. Поскольку p не делит $kp'g + pg'$, утверждение доказано.⇑

Отделение кратных множителей

Пусть F – поле, $\mathrm{char}(F) = 0$. Рассмотрим многочлен f, разложенный на неприводимые множители согласно равенству (5) сл.13 §2:

$$f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m},$$

где α — старший коэффициент многочлена f, $p_1, p_2, \dots, p_m$ – все различные неприводимые над полем F делители многочлена f, имеющие старший коэффициент 1, $k_1, k_2, \dots, k_m$ – натуральные числа.
Из предложения сл.7 следует, что $(f, f') = p_1^{k_1-1} p_2^{k_2-1} \dots p_m^{k_m-1}$ (мы считаем, что многочлен в нулевой степени равен 1). Следовательно, многочлен $\frac{1}{\alpha} f/(f, f') = p_1 p_2 \dots p_m$ есть произведение первых степеней всех неприводимых множителей многочлена f. Применяя эти рассуждения к многочлену $f_1 = (f, f')$ в случае, когда его степень больше нуля, получим произведение первых степеней тех неприводимых множителей многочлена f, которые имеют кратности больше 1. Продолжая таким образом, получим произведения первых степеней тех неприводимых множителей многочлена f, которые имеют кратности больше s. Эта процедура называется *отделением кратных множителей многочлена* f.

Пример отделения кратных множителей

Отделить кратные множители многочлена
$f = x^8 + 2x^7 + 5x^6 + 6x^5 + 8x^4 + 6x^3 + 5x^2 + 2x + 1$.

Решение. Вычислим $f' = 8x^7 + 14x^6 + 30x^5 + 30x^4 + 32x^3 + 18x^2 + 10x + 2$ и с помощью алгоритма Евклида найдем $(f, f') = x^4 + x^3 + 2x^2 + x + 1$. При вычислениях можно заменять многочлены на ассоциированные, в частности, вместо производной взять многочлен $\frac{1}{2}f'$. Разделив столбиком f на (f, f'), найдем частное $x^4 + x^3 + 2x^2 + x + 1$. Таким образом, $f = (x^4 + x^3 + 2x^2 + x + 1)^2$, а произведение первых степеней всех неприводимых множителей многочлена f есть $x^4 + x^3 + 2x^2 + x + 1$, и каждый неприводимый множитель имеет кратность 2. Легко заметить, что $x^4 + x^3 + 2x^2 + x + 1 = x^4 + x^3 + x^2 + x^2 + x + 1 = (x^2 + 1)(x^2 + x + 1)$, т.е. $f = (x^2 + 1)^2(x^2 + x + 1)^2$.

Глава IV. Многочлены

§4. Корни многочленов. Неприводимые многочлены над полями $\mathbb{C}$, $\mathbb{R}$

А. Я. Овсянников

Уральский федеральный университет
Институт естественных наук и математики
Департамент математики, механики и компьютерных наук

Основы алгебры для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0$ – многочлен над полем F. Этот многочлен можно рассматривать как функцию из F в F, сопоставляющую каждому элементу $\beta \in F$ элемент из F, который называется *значением* многочлена $f(x)$ на элементе β: $f(\beta) = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \ldots + \alpha_1 \beta + \alpha_0$.

Определение

Элемент $\beta \in F$ называется *корнем* многочлена $f(x)$, если $f(\beta) = 0$.

Теорема Безу

Пусть $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ – многочлен над полем F и $\alpha \in F$. Тогда $f(x) = q(x)(x - \alpha) + f(\alpha)$, где $q(x) = b_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-1}$, и $b_0 = a_0,\ b_k = a_k + \alpha b_{k-1}$ при всех $k = 1, \ldots, n-1, f(\alpha) = a_n + \alpha b_{n-1}$. (1)

⇓Разделим $f(x)$ на $x - \alpha$ с остатком: $f(x) =$ $= (b_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-1})(x - \alpha) + r$, $\deg(r) \leq 0$, и $r = f(\alpha)$. Из $a_0 x^n + a_1 x^{n-1} + \ldots + a_n = (b_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-1})(x - \alpha) + f(\alpha)$ следует $a_0 x^n + a_1 x^{n-1} + \ldots + a_k x^{n-k} + \ldots + a_n =$ $b_0 x^n + (b_1 - \alpha b_0) x^{n-1} + \ldots + (b_k - \alpha b_{k-1}) x^{n-k} + \ldots + f(\alpha) - \alpha b_{n-1}$ и $a_0 = b_0,\ a_1 = b_1 - \alpha b_0, \ldots, a_k = b_k - \alpha b_{k-1}, \ldots, a_n = f(\alpha) - \alpha b_{n-1}$. Отсюда получаются все равенства (1).⇑

Следствие из теоремы Безу. Связь неприводимости с наличием корней у многочлена

Следствие

Скаляр β будет корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = q(x)(x - \beta)$.

Пусть F – поле. В силу следствия получаем, что если многочлен f из $F[x]$ имеет корень в поле F, то он является неприводимым над полем F тогда и только тогда, когда $\deg(f) = 1$.

Предложение

Пусть $f \in F[x]$, $\deg(f) = 2$ или $\deg(f) = 3$. Многочлен f является неприводимым над полем F тогда и только тогда, когда он не имеет корней в поле F.

$\Downarrow$В силу сказанного выше неприводимый над полем F многочлен степени выше первой не может иметь корней в поле F. Если многочлен f имеет степень 2 или 3, то отсутствие корней, равносильное тому, что многочлен не имеет делителей первой степени, влечет за собой неприводимость, так как при разложении f в произведение двух многочленов gh, где $\deg(g) < \deg(f)$ и $\deg(h) < \deg(f)$, степень по крайней мере одного из сомножителей должна быть равна 1.$\Uparrow$