Глава IV. Многочлены

§2. Наибольший общий делитель. Разложение на неприводимые множители

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)

Наибольший общий делитель

Пусть $f, g \in F[x]$. Многочлен d называется *наибольшим общим делителем* (НОД) многочленов f, g, если $d|f$, $d|g$, и для любого $h \in F[x]$ из $h|f$ и $h|g$ следует, что $h|d$. Из определения НОД вытекает, что если он существует для многочленов f, g, то любые два НОД ассоциированы. Для того, чтобы ненулевой НОД был определен однозначно, требуют, чтобы его старший коэффициент был равен 1.

В доказательстве утверждения на следующем слайде излагается *алгоритм Евклида* построения НОД двух многочленов.
Алгоритм назван в честь греческого математика Евклида (III век до н. э.), который впервые описал его (для натуральных чисел) в VII и X книгах «Начал». Это один из старейших численных алгоритмов, используемых в наше время.

Теорема

Для любых многочленов $f, g \in F[x]$ существует НОД d и существуют такие $u, v \in F[x]$ что

$$d = uf + vg. \tag{1}$$

⇓Если $f = 0,\ g = 0$, то 0 является общим делителем f, g и потому делит их НОД. Значит, последний равен 0. Если один из многочленов ненулевой, а другой нулевой, то их НОД равен ненулевому многочлену. Равенство (1) в обоих случаях выполняется очевидным образом.
В случае, когда f, g ненулевые, без ограничения общности предположим, что $\deg(f) \geq \deg(g)$. Применяя теорему сл.7 §1, запишем последовательность равенств:

$$\begin{gathered}
f = q_1 g + r_1,\ r_1 \neq 0,\ \deg(r_1) < \deg(g);\\
g = q_2 r_1 + r_2,\ r_2 \neq 0,\ \deg(r_2) < \deg(r_1);\\
r_1 = q_3 r_2 + r_3,\ r_3 \neq 0,\ \deg(r_3) < \deg(r_2);\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{k-1} = q_{k+1} r_k + r_{k+1},\ r_{k+1} \neq 0,\ \deg(r_{k+1}) < \deg(r_k);\\
r_k = q_{k+2} r_{k+1},\ r_{k+2} = 0.
\end{gathered} \tag{2}$$

Продолжение доказательства

Процесс (2) на сл. 3 должен завершиться получением нулевого остатка, так как степень g — натуральное число, и степени остатков $r_1, \ldots, r_k, \ldots$ убывают.

Докажем, что r_{k+1} является НОД многочленов f и g. Поднимаясь по цепочке равенств (2) снизу вверх, покажем, что $r_{k+1}|f$ и $r_{k+1}|g$. Из последнего равенства получаем, что $r_{k+1}|r_k$, из предпоследнего в силу предложения сл.10 §1 – что $r_{k+1}|r_{k-1}$. Из каждого последующего рассматриваемого равенства $r_s = q_{s+2}r_{s+1} + r_{s+2}$, получаем по упомянутому предложению, что $r_{k+1}|r_s$, так как уже доказано, что $r_{k+1}|r_{s+1}$ и $r_{k+1}|r_{s+2}$. Дойдя до второго и первого равенства, получим $r_{k+1}|g$ и $r_{k+1}|f$.

Опускаясь по цепочке равенств (2) сверху вниз, покажем, что если $h|f$ и $h|g$, то $h|r_{k+1}$. Пусть $h|f$ и $h|g$. Из первого равенства получаем $r_1 = f - q_1 g$; по предложению сл.10 §1 получаем $h|r_1$. Рассматривая следующее равенство, получаем $r_2 = g - q_2 r_1$, откуда следует в силу упомянутого предложения, что $h|r_2$. Опускаясь по цепочке равенств (2) сверху вниз, докажем, что $h|r_s$ при $s = 3, \ldots, k+1$.

Окончание доказательства

Чтобы доказать равенство (1), нужно выразить из предпоследнего равенства в (2) $r_{k+1} = r_{k-1} - q_{k+1}r_k$, затем подставить в это равенство выражение $r_k = r_{k-2} - q_k r_{k-1}$, полученное из предыдущего равенства: $r_{k+1} = r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) = -q_{k+1}r_{k-2} + (q_{k+1}q_k + 1)r_{k-1} = u_2 r_{k-2} + v_2 r_{k-1}$. Получаем равенство $r_{k+1} = u_2 r_{k-2} + v_2 r_{k-1}$. Подставляя в это равенство выражение $r_{k-1} = r_{k-3} - q_{k-1}r_{k-2}$, полученное из 4-го снизу равенства $r_{k-3} = q_{k-1}r_{k-2} + r_{k-1}$, получим $r_{k+1} = u_2 r_{k-2} + v_2(r_{k-3} - q_{k-1}r_{k-2}) = v_2 r_{k-3} + (u_2 - v_2 q_{k+1})r_{k-2} = u_3 r_{k-3} + v_3 r_{k-2}$. Продолжая движение снизу вверх, на каждом шаге будем получать равенство $r_{k+1} = u_s r_{k-s} + v_s r_{k-s+1}$, где $s = 4, \ldots, k-1$. При $s = k-1$ получаем $r_{k+1} = u_{k-1}r_1 + v_{k-1}r_2$. Подставляя в это равенство выражение $r_2 = g - q_2 r_1$, полученное из 2-го равенства, получаем $r_{k+1} = u_{k-1}r_1 + v_{k-1}(g - q_2 r_1) = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)r_1$. Подставляем в равенство $r_{k+1} = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)r_1$ выражение $r_1 = f - q_1 g$, полученное из 1-го равенства, окончательно имеем $r_{k+1} = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)(f - q_1 g) = (u_{k-1} - v_{k-1}q_2)f + {}$ ${} + v_{k-1}(1 + q_1 q_2 - u_{k-1}q_1)g = uf + vg$, что и требовалось доказать.⇑

Если многочлены $f, g \in F[x]$ имеют ненулевой НОД, то через (f, g) обозначим НОД этих многочленов со старшим коэффициентом 1.

Равенство (1) на сл.3 дает *линейную форму* наибольшего общего делителя.

Пример нахождения НОД многочленов и его линейной формы

Приведем конкретный пример. Найти НОД многочленов

$$f = x^3 - 2x^2 + x - 2 \text{ и } g = x^2 - 3x + 2.$$

Разделив столбиком f на g с остатком, получим

$$f = (x+1)g + 2(x-2). \tag{3}$$

Разделив столбиком g на $x-2$ с остатком, получим $g = (x-1)(x-2)$, т.е.

$$g = \frac{1}{2}(x-1)(2(x-2)).$$

Алгоритм завершается. Один из НОД многочленов f, g равен $2(x-2)$, а $(f,g) = x-2$ (старший коэффициент берем равным 1). Из равенства (3) находим линейную форму:

$$x - 2 = \frac{1}{2}f - \frac{1}{2}(x+1)g.$$

Многочлены f, g называются *взаимно простыми*, если их наибольший общий делитель (f, g) равен 1. Из теоремы сл.3 получается такое

Следствие

Многочлены f, g являются взаимно простыми тогда и только тогда, когда существуют такие многочлены u, v, что выполняется равенство

$$uf + vg = 1. \tag{4}$$

Если равенство (4) имеет место, то 1 делится на любой общий делитель многочленов f, g, поэтому они взаимно просты. Обратное утверждение обеспечивается равенством (1) сл.3.

Предложение

1. Если многочлены f, g, h таковы, что f, g взаимно просты и $f|h$, $g|h$, то $(fg)|h$.
2. Если многочлены f, g, h таковы, что f, g взаимно просты и $f|gh$, то $f|h$.
3. Если многочлены f, g, h таковы, что f, h и g, h взаимно просты, то fg и h взаимно просты.

$\Downarrow$ Докажем утверждение 1. Пусть $h = fp$, $h = gq$ для некоторых многочленов p, q. Так как f, g взаимно просты, в силу следствия существуют многочлены u, v такие, что выполняется равенство $uf + vg = 1$. Умножая обе части этого равенства на h, получим $h = huf + hvg$, откуда $h = gquf + fpvg = fg(qu + pv)$, что и требуется доказать.

Докажем утверждение 2. Пусть $gh = fp$ для некоторого многочлена p. Так как f, g взаимно просты, в силу следствия существуют многочлены u, v такие, что выполняется равенство $uf + vg = 1$. Умножая обе части этого равенства на h, получим $h = huf + hvg$, откуда $h = huf + fpv = f(hu + pv)$, что и требуется доказать.

Докажем утверждение 3. Так как f, h взаимно просты, в силу следствия существуют многочлены u, v такие, что выполняется равенство $uf + vh = 1$. Умножая обе части этого равенства на g, получим $g = ufg + vhg$. От противного, предположим, что fg и h не взаимно просты. Пусть $p = (fg, h)$ и $\deg(p) > 0$. Тогда $p|h$ и $p|g$ в силу равенства $g = ufg + vgh$ и предложения сл.10 §1. Получили противоречие с условием, что g, h взаимно просты. Следовательно, fg и h взаимно просты.$\Uparrow$

Пусть F – поле.

Определение

Многочлен $f \in F[x]$ называется *неприводимым над полем F*, если $\deg(f) \geq 1$ и для любых многочленов $g, h \in F[x]$ из равенства $f = gh$ следует $\deg(g) = \deg(f)$ или $\deg(h) = \deg(f)$.

Многочлен может быть неприводим над одним полем и приводим над другим (расширением первого). Например, $x^2 + 1 = (x + i)(x - i)$ неприводим над $\mathbb{R}$ и приводим над $\mathbb{C}$.

Все многочлены первой степени неприводимы над любым полем.

Из определения следует, что любой делитель неприводимого многочлена либо ассоциирован с ним, либо является ненулевым скаляром.

Предложение

Пусть $p \in F[x]$ –неприводимый многочлен. Для любого $f \in F[x]$ либо $p|f$, либо $(p, f) = 1$.

$\Downarrow$Предположим, что $p \not| f$. Пусть $q = (p, f)$. Тогда q не ассоциирован с p и $q|p$, откуда следует $\deg(q) = 0$, т.е. $q = 1$.$\Uparrow$

Из предложения сл.9 и утверждения 2 предложения сл.7 вытекает

Следствие

Если неприводимый многочлен p делит произведение fg некоторых многочленов f, g, то p делит f или p делит g.

Предложение

Если неприводимый многочлен p делит произведение $q_1 \dots q_m$ некоторых неприводимых многочленов $q_1, \dots, q_m$, то p ассоциирован по крайней мере с одним многочленом q_j $(j = 1, \dots, m)$.

$\Downarrow$ Проведем индукцию по m. При $m = 2$ из следствия получаем, что $p|q_1$ или $p|q_2$, откуда в силу неприводимости p, q_1, q_2 следует требуемое. Предположим, что утверждение уже доказано для всех $2 \le k < m$ и неприводимый многочлен p делит произведение $q_1 \dots q_m$ некоторых неприводимых многочленов $q_1, \dots, q_m$. Так как $p|q_1 \cdot (q_2 \dots q_m)$, согласно следствию $p|q_1$ или $p|(q_2 \dots q_m)$. В первом случае p ассоциирован с q_1, а во втором по предположению индукции p ассоциирован с q_j для некоторого $2 \le j \le m$, что и требуется доказать.$\Uparrow$

Теорема о неприводимом разложении многочлена

Теорема

Пусть F – поле. Любой многочлен из $F[x]$ степени больше 0 либо является неприводимым, либо разлагается в произведение неприводимых многочленов, причем это разложение определяется однозначно с точностью до замены неприводимых множителей ассоциированными многочленами и перестановки сомножителей.

$\Downarrow$ Пусть $f \in F[x]$ – многочлен. Докажем существование разложения индукцией по $\deg(f)$. База индукции: $\deg(f) = 1$. Тогда f – неприводимый многочлен. Шаг индукции. Пусть для всех многочленов степени меньше $\deg(f)$ утверждение доказано. Если многочлен f не является неприводимым, то $f = gh$ для некоторых многочленов $g, h \in F[x]$, причем $\deg(g) < \deg(f)$ и $\deg(h) < \deg(f)$. По предположению индукции каждый из многочленов g, h либо неприводим, либо разлагается в произведение неприводимых многочленов, поэтому f также разлагается в произведение неприводимых многочленов.

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

$$f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}, \tag{5}$$

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 (5) 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

$$(f, g) = p_1^{\min\{k_1, n_1\}} p_2^{\min\{k_2, n_2\}} \dots p_m^{\min\{k_m, n_m\}}. \tag{6}$$

В самом деле, старший коэффициент в правой части равенства (6) 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 (6) 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 и его выражение через разложения на неприводимые множители

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

$$[f, g] = p_1^{\max\{k_1, n_1\}} p_2^{\max\{k_2, n_2\}} \dots p_m^{\max\{k_m, n_m\}} q_1^{\ell_1} \dots q_s^{\ell_s} q_{s+1}^{\ell_{s+1}} \dots q_t^{\ell_t}. \qquad (7)$$

Можно доказать эту формулу и другим способом, применив предложение сл.15 и формулу (6) и используя очевидное равенство $\max\{k, n\} + \min\{k, n\} = k + n$.