Тема 1-9: Многочлены

А. Я. Овсянников

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

Алгебра и геометрия для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Пусть F – поле. Рассмотрим множество $F[x]$ всех последовательностей с элементами из F вида $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ таких что для некоторого $m \in \mathbb{N}$ справедливы равенства $\alpha_k = 0$ при всех $k \geq m$. Две последовательности называются *равными*, если на соответствующих местах в них стоят одинаковые элементы. Определим сумму двух последовательностей из $F[x]$ поэлементно:

$$(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) + (\beta_0, \beta_1, \ldots, \beta_n, \ldots) = (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n, \ldots).$$

Произведение двух последовательностей определяется так:

$$(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \cdot (\beta_0, \beta_1, \ldots, \beta_n, \ldots) = (\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots), \quad (1)$$

$$\text{где } \gamma_n = \sum_{k+\ell=n} \alpha_k \beta_\ell.$$

Очевидно, что сумма любых двух последовательностей из $F[x]$ принадлежит $F[x]$. Легко проверить, что и произведение любых двух последовательностей из $F[x]$ также принадлежит $F[x]$.

Многочлен и его степень. Свойства сложения

Элементы из $F[x]$ будем называть *многочленами* над полем F и обозначать малыми латинскими буквами. Последовательность из нулей обозначим через o и назовем *нулевым* многочленом. Пусть $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$. Если $f \neq o$, то существует $m \in \mathbb{N}$ такое что $\alpha_m \neq 0$, $\alpha_k = 0$ для любого $k > m$. В таком случае говорят, что многочлен f имеет *степень* m, обозначаемую через $\deg(f)$. Для нулевого многочлена o полагаем $\deg(o) = -\infty$. Символ $-\infty$ по определению считается меньше любого целого числа, и для любого целого m по определению принимается, что $m + (-\infty) = -\infty + m = -\infty$. Нетрудно убедиться, что $\deg(f \cdot g) = \deg(f) + \deg(g)$, $\deg(f + g) = \max\{\deg(f), \deg(g)\}$ при $\deg(f) \neq \deg(g)$ и $\deg(f + g) \leq \deg(f), \deg(g)$ при $\deg(f) = \deg(g)$.

Непосредственно проверяются следующие свойства операций сложения многочленов:
$\forall f, g, h \in F[x] \quad f + g = g + f; \quad f + (g + h) = (f + g) + h; \quad f + o = f;$
$\forall u \in F[x]\ \exists v \in F[x]\colon u + v = o.$

Таким образом, относительно сложения $F[x]$ является абелевой группой.

Свойства умножения многочленов

Свойства умножения не столь очевидны. Докажем, что
$\forall f, g, h \in F[x] \quad f \cdot g = g \cdot f; \quad f \cdot (g \cdot h) = (f \cdot g) \cdot h; \quad f \cdot (g + h) = f \cdot g + f \cdot h.$
Первое равенство вытекает непосредственно из определения произведения (1) сл.2.
Докажем второе. Пусть $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$, $g = (\beta_0, \beta_1, \ldots, \beta_n, \ldots)$, $h = (\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots)$. Тогда $f \cdot g = (\delta_0, \delta_1, \ldots, \delta_n, \ldots)$, где $\delta_m = \sum_{k+l=m} \alpha_k \beta_l$ и $g \cdot h = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n, \ldots)$, где $\varepsilon_r = \sum_{s+t=r} \beta_s \gamma_t$. Далее, $(f \cdot g) \cdot h = (\xi_0, \xi_1, \ldots, \xi_n, \ldots)$, где

$$\xi_d = \sum_{m+t=d} \delta_m \gamma_t = \sum_{m+t=d} \left(\sum_{k+l=m} \alpha_k \beta_l \right) \gamma_t = \sum_{k+l+t=d} \alpha_k \beta_l \gamma_t.$$

Аналогично имеем $f \cdot (g \cdot h) = (\nu_0, \nu_1, \ldots, \nu_n, \ldots)$, где

$$\nu_d = \sum_{k+r=d} \alpha_k \varepsilon_r = \sum_{k+r=d} \alpha_k \left(\sum_{s+t=r} \beta_s \gamma_t \right) = \sum_{k+s+t=d} \alpha_k \beta_s \gamma_t,$$

откуда следует требуемое равенство $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.
Равенство $f \cdot (g + h) = f \cdot g + f \cdot h$ доказывается аналогично.

Таким образом, $F[x]$ является ассоциативным коммутативным кольцом с единицей (очевидно, что последовательность $(1, 0, 0, \ldots)$ является единицей относительно умножения многочленов).

Привычная запись многочленов

Последовательности вида $(\alpha_0, 0, 0, \ldots)$ складываются и умножаются, как элементы поля F: имеем $(\alpha, 0, 0, \ldots) + (\beta, 0, 0, \ldots) = (\alpha + \beta, 0, 0, \ldots)$; $(\alpha, 0, 0, \ldots) \cdot (\beta, 0, 0, \ldots) = (\alpha \cdot \beta, 0, 0, \ldots)$. Условимся отождествлять такие последовательности с их первыми элементами и называть *скалярами*. Например, нулевая последовательность o отождествляется со скаляром 0. Таким образом, $F \subset F[x]$. Нетрудно проверить, что $\alpha \cdot (\beta_0, \beta_1, \ldots) = (\alpha\beta_0, \alpha\beta_1, \ldots)$ для любого скаляра α.

Последовательность $(0, 1, 0, 0, \ldots)$ обозначим через x. Легко проверить, что $x^2 = x \cdot x = (0, 0, 1, 0, 0 \ldots)$, $x^3 = x^2 \cdot x = (0, 0, 0, 1, 0 \ldots)$, и x^m имеет 1 на $(m+1)$-й позиции, а все остальные элементы этой последовательности равны нулю.

Ясно, что выражение вида

$$f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0, \tag{2}$$

где $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$, n – натуральное число, представляет собой последовательность $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, 0, \ldots)$, в которой все члены после α_n равны 0. В дальнейшем мы будем придерживаться этой привычной записи многочленов. Скаляры $\alpha_0, \ldots, \alpha_n$ называются *коэффициентами* многочлена f. Если $\alpha_n \neq 0$, то $n = \deg(f)$ и $\alpha_n x^n$ называется *старшим членом*, а скаляр α_n – *старшим коэффициентом* многочлена f. Скаляр α_0 называется *свободным членом* многочлена f.

Теорема

Пусть $f, g \in F[x]$, $g \neq 0$. Тогда существуют такие однозначно определенные многочлены $q, r \in F[x]$, что

$$f = q \cdot g + r \text{ и } \deg(r) < \deg(g). \tag{3}$$

$\Downarrow$Если $\deg(g) = 0$, то $g \in F$ и $g \neq 0$, т.е. $f = (\frac{1}{g}f)g$ и $q = \frac{1}{g}f$, $r = 0$. Предположим, что $\deg(g) > 0$. Для доказательства существования применим индукцию по $\deg(f)$. При $\deg(f) < \deg(g)$ положим $q = 0$, $r = f$. Пусть для всех многочленов h степени меньше m, где $m \geq \deg(g)$, существуют такие многочлены q и r, что $h = qg + r$ и $\deg(r) < \deg(g)$. Рассмотрим произвольный многочлен f степени m. Имеем $f = \alpha x^m + f_1$ и $g = \beta x^k + g_1$, где $\deg(f_1) < m$, $\deg(g_1) < k$ и $\alpha \neq 0$, $\beta \neq 0$. Положим $h_1 = \frac{\alpha}{\beta}x^{m-k}$. Тогда $h_1 g = \alpha x^m + h_1 g_1$, откуда $\deg(f - h_1 g) < m$. Применяя к многочлену $f - h_1 g$ предположение индукции, констатируем существование многочленов q_1 и r таких что $f - h_1 g = q_1 g + r$ и $\deg(r) < \deg(g)$. Теперь ясно, что $f = (h_1 + q_1)g + r$, что и требуется доказать.

Докажем единственность. Предположим, что $f = q_1 g + r_1$ и $f = q_2 g + r_2$ для некоторых многочленов q_1, q_2, r_1, r_2 таких что $\deg(r_1), \deg(r_2) < \deg(g)$. Из равенства $q_1 g + r_1 = q_2 g + r_2$ получаем $(q_1 - q_2)g = r_2 - r_1$. Если $q_1 - q_2 \neq 0$, то $\deg((q_1 - q_2)g) \geq \deg(g)$, а $\deg(r_2 - r_1) < \deg(g)$ — получили противоречие. Следовательно, $q_1 - q_2 = 0$, откуда $q_1 = q_2$ и $r_1 = r_2$. Теорема доказана.⇑

В равенстве (3) сл.6 многочлен q называется *частным*, а многочлен r – *остатком* от деления (с остатком) f на g. Если $r = 0$, то говорят, что многочлен f *делится* на многочлен g; в этом случае $f = qg$. При этом говорят также, что многочлен g *делит* многочлен f; этот факт будем обозначать через $g|f$.

Алгоритм деления многочленов столбиком

Доказательство теоремы сл.6 служит основой для *алгоритма деления столбиком многочлена на многочлен*. Этот алгоритм состоит в следующем. Пусть $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0$, $g = \beta_m x^m + \beta_{m-1} x^{m-1} + \ldots + \beta_1 x + \beta_0$, и пусть $\alpha_n, \beta_m \neq 0$ и $n \geq m > 0$. Положим $q = 0$. Шаг алгоритма делается так. Многочлен f заменяется на многочлен $f_1 = f - \frac{\alpha_n}{\beta_m} x^{n-m} g$, а многочлен q – на многочлен $q + \frac{\alpha_n}{\beta_m} x^{n-m}$. Шаги повторяются до тех пор, пока $\deg(f_1) \geq m$. Так как степень f_1 на каждом шаге уменьшается на m, алгоритм закончит работу. При этом частное будет равно q, а остаток – последнему значению f_1.

Пример деления столбиком

Рассмотрим конкретный пример. Вычисления записываются так же, как при делении многозначных чисел.

$$
\begin{array}{l|l}
x^3 - 2x^2 + 3x + 1 & \underline{x^2 - x + 2} \\
- & x - 1 \\
\underline{x^3 - x^2 + 2x} & \\
\quad -x^2 + x + 1 & \\
\quad - & \\
\quad \underline{-x^2 + x - 2} & \\
\qquad 3 &
\end{array}
$$

Таким образом, $x^3 - 2x^2 + 3x + 1 = (x - 1)(x^2 - x + 2) + 3$ и частное равно $x - 1$, остаток равен 3.

Следующее утверждение проверяется непосредственно.

Предложение

Пусть $f, g, g_1, g_2, h \in F[x]$. Тогда если $f|g$, то $f|(gh)$ и если $f|g_1$, $f|g_2$, то $f|(g_1 + g_2)$ и $f|(g_1 - g_2)$.

Многочлены f и g называются *ассоциированными*, если существует ненулевой элемент $\gamma \in F$ такой, что $f = \gamma g$. Легко проверить, что многочлены f и g ассоциированы тогда и только тогда, когда $f|g$ и $g|f$, а также что отношение ассоциированности является отношением эквивалентности на множестве $F[x]$. Каждый класс эквивалентности по этому отношению, содержащий ненулевой многочлен, содержит единственный многочлен со старшим коэффициентом 1. Поэтому справедливо

Наблюдение

Для любого ненулевого многочлена существует единственный ассоциированный с ним многочлен со старшим коэффициентом 1.

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 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.

Теорема

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

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

$\Downarrow$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 (4) 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.6, запишем последовательность равенств:

$$\begin{gathered} f = q_1 g + r_1,\ r_1 \neq 0,\ \deg(r_1) < \deg(g); \\ g = q_2 r_1 + r_2,\ r_2 \neq 0,\ \deg(r_2) < \deg(r_1); \\ r_1 = q_3 r_2 + r_3,\ r_3 \neq 0,\ \deg(r_3) < \deg(r_2); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{k-1} = q_{k+1} r_k + r_{k+1},\ r_{k+1} \neq 0,\ \deg(r_{k+1}) < \deg(r_k); \\ r_k = q_{k+2} r_{k+1}. \end{gathered} \tag{5}$$

Процесс (5) на сл. 12 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 (5) 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 – 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 предложению сл.10, 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 (5) 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 получаем $h|r_1$. Рассматривая следующее равенство, получаем $r_2 = g - q_2 r_1$, откуда следует в силу предложения сл.10, что $h|r_2$. Опускаясь по цепочке равенств (5) сверху вниз, докажем, что $h|r_s$ при $s = 3, \ldots, k+1$.

Окончание доказательства

Чтобы доказать равенство (4), нужно выразить из предпоследнего равенства в (5) $r_{k+1} = r_{k-1} - q_{k+1}r_k$, 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 $r_{k+1} = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)(f - q_1 g) = -v_{k-1}q_2 f + v_{k-1}(1 + q_1 q_2)g = uf + vg$, 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 (4) на сл.12 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

$$f = (x+1)g + 2(x-2). \tag{6}$$

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. НОД многочленов f, g равен $2(x-2)$, а $(f,g) = x-2$ (старший коэффициент берем равным 1). Из равенства (6) 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.12 получается такое

Следствие

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

$$uf + vg = 1. \tag{7}$$

Если равенство (7) имеет место, то 1 делится на любой общий делитель многочленов f, g, поэтому они взаимно просты. Обратное утверждение обеспечивается равенством (4) сл.12.

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 $p = (fg, h)$. Тогда $p|h$ и $p|g$ в силу равенства $g = ufg + vgh$ и предложения сл.10. Получили противоречие с условием, что g, h взаимно просты. Следовательно,fg и h взаимно просты.$\Uparrow$

Неприводимые многочлены

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 $\deg(h) = \deg(f)$.

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

Все многочлены первой степени неприводимы над любым полем.

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 этого утверждения и утверждения 2 предложения сл.16 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 сл.18 получаем, что $p|q_1$ или $p|q_2$, откудв в силу неприводимости p, q_1, q_2 следует требуемое. Предположим, что утверждение уже доказано для всех $2 \leq k < m$ 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 сл.18 $p|q_1$ 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 $2 \leq j \leq m$, 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.

Доказательство единственности на следующем слайде.

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.19 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. Обозначим его снова через p_2. Применяя предположение индукции к равенству $p_2 \dots p_m = \prod_{j \neq i_1} q_j$, 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 p_j ассоциирован с q_{i_j} при $j = 2, \dots, m$. Таким образом, шаг индукции доказан.

Доказательство теоремы закончено.⇑

Разложение многочлена на неприводимые множители

Пусть F – поле. Из теоремы сл.20 следует, что любой многочлен $f \in F[x]$ степени больше нуля может быть единственным образом представлен в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}, \tag{8}$$

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. Это представление называется *разложением многочлена f на неприводимые множители*. Число k_j в равенстве (8) называется *кратностью* неприводимого многочлена p_j в разложении многочлена f на неприводимые множители. Легко понять, что $\deg(f) = \sum_{j=1}^{m} k_j \deg(p_j)$.

НОД ненулевых многочленов легко выразить через их разложения на неприводимые множители. 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 легко понять, что

$$(f, g) = p_1^{\min\{k_1, n_1\}} p_2^{\min\{k_2, n_2\}} \dots p_m^{\min\{k_m, n_m\}}. \tag{9}$$

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'.

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

$$(f+g)' = f' + g'; \quad (\alpha f)' = \alpha f' \text{ для любого } \alpha \in F. \tag{10}$$

Докажем, что имеет место обычная формула дифференцирования произведения

$$(fg)' = f'g + fg'. \tag{11}$$

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

$$(x^m x^n)' = x^m(x^n)' + (x^m)'x^n. \tag{12}$$

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 (10) и (12) $(f\cdot g)' = \left(\sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k\beta_\ell x^{k+\ell}\right)' = \sum\limits_{k=0}^{n}\sum\limits_{\ell=0}^{m} \alpha_k\beta_\ell (x^{k+\ell})' =$

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

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

$\left(\sum\limits_{k=0}^{n} \alpha_k x^k\right)' \sum\limits_{\ell=0}^{m} \beta_\ell x^\ell + \sum\limits_{k=0}^{n} \alpha_k x^k \left(\sum\limits_{\ell=0}^{m} \beta_\ell x^\ell\right)' = f'g + fg'$. Таким образом, равенство (12) доказано.

Из формулы (11) по индукции выведем формулу для производной степени многочлена

$$(f^m)' = mf^{m-1}f'. \tag{13}$$

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 (13) 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.

Напомним, что через $\mathrm{char}(F)$ обозначается характеристика поля F (см. сл.13 т.1-4).

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 $k - 1$.

$\Downarrow$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.16, 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.$\Uparrow$

Отделение кратных множителей

Пусть F – поле, $\mathrm{char}(F) = 0$. Рассмотрим многочлен f, разложенный на неприводимые множители согласно равенству (8) сл.22. Из предложения сл.26 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, частное $f/(f, f') = p_1 p_2 \dots p_m$ 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. $f = (x^2 + 1)^2(x^2 + x + 1)^2$.

Определение

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

НОК ненулевых многочленов легко выразить через их разложения на неприводимые множители. 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 легко понять, что

$$[f, g] = p_1^{\max\{k_1, n_1\}} p_2^{\max\{k_2, n_2\}} \dots p_m^{\max\{k_m, n_m\}} q_1^{\ell_1} \dots q_s^{\ell_s} q_{s+1}^{\ell_{s+1}} \dots q_t^{\ell_t}. \qquad (14)$$