Лекции по матлогу

Зайцев Вадим

2010-02-16

1 Производная, кратные корни, ф-ла Тэйлора

Опр. Пусть $f(x) = sum_{i\geq 0} a_i x^i \in K(x)$, K - поле. Тогда многочлен
$f'(x) = \sum_{j\geq 1} j a_j x^{j-1}$ назыв. производной для f(x), а отобр. $\frac{d}{dx} : f(a) \to f'(x)$ назыв.суперпроизодвной.
$(f+g)' = f' + g'$,
$(fg+' = f'g + fg'$
$f(g(x)) = f'(g(x))g'(x)$

Указание. ДОок. про ... на базисе алгебры K(x) ввиду линпйности $\frac{d}{dx}$
Теорема 1. Пусть K - поле, c $\in K$, $f(x) = (x-c)^k g(x), g(c) \neq= 0$. Если $k = 1 + ... + 1 (c raz \neq= 0$ в K...
Док-во. Имеем $f'(x) = k(x-c)^{k-1} g(x) + (x-c)^k g'(x)$. Гавнюк он. Мог бы и подождать...
Теорема 2. ПУсть $f(x) \in K(x), f = n, K$ - поле. $c \in K$. Тогда $f(x) = f(c) + \frac{f'(c)}{c!}(x-c) + \frac{f''(c)}{2!!}(x-c)^2 + \ldots + \frac{f^{(n)}}{n!}(x-c)^n$. Док-во. Обозначим через $y = x - c$, тогда $x = y + c$ иил $f(x) = \sum_{i\geq 0} a_i x^i = \sum_{i\geq 0} (y+c)^i = \sum_{i=0}^{n} r_i y^i = \sum_{i\geq 0} r_I (x-c)^{r_i}$. Тогда $f(c) = r_0$
$f'(c) = r_1$
$f''(c) = 2r_2$
$f^{(k)} = k! r_k$
$f^{(n)} = n! r_n$.
Справа должна быть хрень. Док-во тра-ля-ля.

2 НОД и Алгоритм Евклида

2.0.1 Определение

Пусть $f, g \in K[x]$, K - поля (хотя не важно). $g \neq= 0$. Многочлен $d \in K[x]$ назыв. НОД для f и g, и
1) $d \mid f$, $d \mid g$
2) $d_1 \mid f$, $d_1 \mid g \Rightarrow d_1 \mid d$.
Обозн. $d = GCD(f, g)$. Если $d_1 = GCD(f, g)$, то $d_1 \mid d$, $d \mid d_1$, значит стпень d совпадает со степенью d_1. $d = d_1 e, e \in K, e \neq= 0$. Если потребовать, чтобы с.к. $d(x) = 1$, то $d(x)$ - единственный НОД.

2.0.2 Теорема:

Пусть K - поле, $f, g \in K[x], g(x) \neq= 0$. Тогда НОД(f,g) можно найти по алгоритму Евклида:

1. $f = gq_1 + r_1$, ст $r_1 <$ степени делителя.
2. $g = r_1 q_2 | r_2$, ст $r_2 <$ ст r_3.
3. $r_1 = r_2 q_3 | r_3$, ст $r_3 <$ ст r_4.
4. ...
5. $r_{k-1} = r_k q_{k+1} + r_2 \Rightarrow r_k = GCD(x, y)$

2.0.3 Док-во

Пусть $f = gq + r$. Тогда $GCD(f, g) = GCD(g, r)$, т.к. совпадают мно-ва общих делителей. Отсюда по алгоритму Евклида мы получаем $GCD(f, g) = GCD(f, r_1) = GCD(r_1, r_2) = ... = GCD(r_{k-1}, r_k) = k_k$. Теорема доказана.

2.1 Линейные дифоантовые уравнения.

$(*) fu + gv = h$
Здесь $f, g, h \in K[x]$ - данные многочлены, u, v - неизвестные многочлены в K[x].

2.1.1 Теорема

Ур-ие (*) разрешима в $K[x] \Leftrightarrow d = GCD(f, g) \mid h$.

Доказательство. $\Rightarrow$) имеем $f = df_1, g = dg_1, f_1, g_1 \in K[x]$. Тогда $h = fu+gv = df_1u+dg_1v = d\underbrace{\in K[x]}(f_1u + g_1v), d \mid h$
$\Leftarrow) I = \{fu + gv \mid u, v \in K[x]\}$. Надо доказать, что $h \in I$. Отметим следующие сво-ва I:
1) $h_1, h_2 \in I \Rightarrow h_1 - h_2 \in I$
2) $h_1 \in I, g(x) \in K[x] \Rightarrow h_1 g \in I$ x в K[x] - любой.
$h_1 = fu_1gv_1$
$h_2 = fu_2 + gv_2 \Rightarrow h_1 - h_2 = f(u_1 - u_2) + g(v_1 - v_2)$
$h_1 q = f(u, q) + g(v, q)$.
Ввиду алгоритма Евклида
$f = gr_1 +_1$
$g = r_1q_2 + r2$
...
$- - -$
$r_{k-1} = r_kq_{k+1}$
. Получаем: $f - gr_q = r_1 \in I$
$g - r_1q_2 = r_2 \in I$
$r_1 - r_2q_3r_3 \in I$
...
$r_{k-2} - r_{k-1}q_k = r_k \in I$.
Можно считать, что $d = r_k \cdot e, e \in K, e \neq= 0, d \in I. h = dh_1 \in I$, значит наше уравнение разрешимо

2.2 Сво-ва взаимно-простых многочленов

Опр. могочлены f,g из K[x] назыв. взаимно-простыми, если их НОД =1.
Обозн $f \perp g$.

2.2.1 Теорема

1) $f \perp g \Leftarrow \exists u, v \in K[x] : fu + gv = 1$.
2) $f \perp g_1, f \perp g_2 \Rightarrow f \perp (g_1g_2)$
3) $d_1|f, d_2|f, d_1 \perp d_2 \Rightarrow (d_1d_2)|f$
4) $p|(fg), p \perp f \Rightarrow p|g$.

Доказательство. 1) Верно ввиду критерия разрешимости ур-ия $fu + gv = h$.
2) Ввиду (1) $\exists u_1, v_1, u_2, v_2 \in K[x]$:
$fu_1|g_1v_1, fu_2 + g_2v_2 = 1$, пермножим эти равенства:
$f[...] + (g_1g_2)(v_1v_2) = 1$
Ввиду (1) получаем, что $f \perp g_1g_2$.
3) Условие делимости: $f = d_1f_1 = d_2f_2$. Ввиду (1) $d_1u + d_2v = 1$, где $u, v \in K[x]$ (некоторы многочлены). Умножим на f: $f = fd_1u + fd_2v = d_1d_2[f_2u + f_1v]. \Rightarrow d_1d_2 \mid f$.
4) Имеем $pu + fv = 1, u, v \in K[x]$. Умножим на g: $pug + (fg)v = g. \quad p[ug + hv] = g(fg = ph), \quad p \mid g$.

2.3 Однозначность разложения мно-на на множители

2.3.1 Опр.

Мно-н $p(x) \in K[x]$ назыв. неразложимым в K[x] (на множители), если $deg(p) \geq 1, p = uv, u, v \in K[x] \Rightarrow (deg(u) = 0||deg(v) = 0)$.

2.3.2 Опр.

Многочлены f, g назыв. ассоциировнными, если $f = eg, e \in K, e \neq= 0$. Обозн.: $f \sim g$.
Упр. ассоциир. - отно. эквив.

2.3.3 Теорема

Пусть K - поле, тогда любой мно-н ст >=1 имеет в K[x] разложение в про-ие неразложимы в K[x] множ-ей, причём это разложене единственно с точно. до порядка мно-лей и ассоциированности.

Доказательство. 1. Существование. Пусть $f(x0 \in K[x], deg(f) \geq 1$, если f неразложим в K[x], то доказывать нечего. Если f разложим, то тогда $f = f_1 f_2, deg(f_i) < deg(f), i = 1, 2$. Если f_1, f_2)- неразложимы, то получено требованное разложение, если какой-либо из них разложим, то $f_i = f_{11} f_{12}, deg(f_{1g}) < deg(f_1)$.
Степени понижаются, поэтмоу процесс разложения обязательно оборвётся на про-ие неразложимых множителей.

2. Единственность. Если p - нераложим, то $p \mid fg$, то $p \mid f$ или $p \mid g$. Докажем это:
Пусть $p \not| f$. Есл $d = GCD(p, f)$, то $d \mid p$. Если $d = 1$, то $p \perp f$, и $p \mid g$ по сво-ву взаимно простых,наверное.
Если $d \sim p, d = pe, r \in K, e \neq 0$.. Но $d \mid f$ и тгда $p \mid f$, что протеворечить предположение в начале пункта.
Лемма 2:
p - неразложимы, $p \mid (f_1 f_2 ... f_k) \Rightarrow \exists i : p \mid f_i$.
Док-во индукцией по к
k=1 - очевидно
к-1=>: $p \mid \underbrace{f}(f_1 ... f_{k-1}) \underbrace{g} f_k$.
По лемме(1) $p \mid f_1 ... f_{k-1}$.
$f = p_1 p_2 .. p_r = q_1 q_2 ... q_3$
p_i, q_j неразложим в $K[x], r \leq s$.
Тогда$p_1 \mid q_1 ... q_s$. По лемме 2 сущ. $i : p_1 \mid q_i$. Перенумеруем, $p_1 \mid q_1$. Но q_1 перенумеруем, $q_1 = e_1 p_1, e_1 \in K, e_1 \neq 0$. $p_1 p_2 ... p_s = e_1 p_1 q_2 ... q_s = p_1(e_1 q_2 ... q_s)$.
Можно сократить, $p_2 ... p_r = e_1 q_2 ... q_s$, Аналогично можно скоратить далее $p_2 ... p_r$. В итоге $q = \underbrace{\in K} e_1 e_2 .. e_r q_{r+1} ... r_s$.
Если s>r, то ст$(e_1 ... e_r q_{r+1} ... q_s) \geq 1$. Противоречие. Значит, r=s и $p_i \sim q_i$ после подходящей перенумерации.

2.3.4 Зам

Если в целостном кольце (ассоциативном, коммутативном, с 1, без делителей нуля) есть ещё “деление с остатком”, то есть алгоритм Евклида для нахождения НОД. Есть критерий разрешимости линейных диофантовых ур-ий, сво-ва взаимно-простых эле-ов и однозначность разложения на множители.