Теорема Безу. (напомнить)

Кратность корня.

$f(t) = (t-\alpha)^k g(t)$, где

$g(\alpha) \neq 0$

k — кратность.

Простой корень

Кратный корень.

Следствие. $f = \prod (t-\alpha_i)^{k_i} \cdot g$

g не имеет корней,

Следствие Число корней посчитанных с кратностями $\leq \deg f$.

$\square$

Деление многочленов с остатком

Теорема $\Bbbk$ - поле.

$f, g \in \Bbbk[t]$ $g \neq 0$

$\Rightarrow \exists!\ h, r \in \Bbbk[t]$

такие, что

$f = g \cdot h + r$, $\underline{\deg r < \deg g}$.

Доказательство.

$f = a_n t^n + \dots + a_0$

$g = b_m t^m + \dots + b_0$ Можно считать, что $n \geq m$.

По индукции. (по $\deg(f) = n$.)

$$f_1 = f - \frac{a_n}{b_m} \cdot g \cdot t^{n-m}$$

$\deg f_1 \leq n.$

Коэфф t^n $\quad a_n - \frac{a_n}{b_m} \cdot b_m = 0$

$\Longrightarrow \deg f_1 \leq n-1.$

По предположению индукции

$$f_1 = g \cdot h_1 + r_1$$

$$\deg r_1 < \deg g$$

$$f = \frac{a_n}{b_m} g \cdot t^{n-m} + gh + r$$

$$= g\underbrace{\left(\frac{a_n}{b_m} t^{n-m} + h\right)} + r$$

Однозначность.

$$f = gh + r = gh' + r'$$

$$g(h-h') = r' - r.$$

$$\deg(r'-r) < \deg g$$

С др. стороны,

$$\deg g(h-h') \geq \deg g.$$

$\square$

Делимость в кольцах

A коммутативное ассоциативное кольцо с 1 без делителей 0.

(целостное кольцо).

Говорят, что $f \in A$ делится на $g \in A$, $g \neq 0$, если $f = g \cdot h$ $(\exists h \in A)$

Обозначение: $g \mid f$ (g делит f)

или $f \equiv 0 \mod g$

Свойства. (1) $g \mid f_1$, $g \mid f_2$ $\Longrightarrow$ $g \mid (f_1 \pm f_2)$

(2) $g \mid f_1, g \mid f_2 \Longrightarrow g \mid f_1 \cdot f_2$

(3) $g \mid f, h \mid g \Longrightarrow h \mid f$

(4) $f \mid g,\ g \mid f \Longrightarrow$

$f = g \cdot u$ и обратим

__Неразложимый элемент.__

$f \in A$ неразложим (простой) если $g \mid f \Longrightarrow$ или

g обратим или $g = f \cdot u$ и обратим.

__Пример.__ (1) $A = \mathbb{Z}$

неразложимые = простые числа.

(2) $A = \mathbb{R}[t]$

Неприводимые многочлены.

R — кольцо без делителей 0 (комм., ассоциативное с 1)

$f = f_1 \cdot f_2 \Rightarrow$

или $\deg(f_1) = 0$ или $\deg(f_2) = 0$.

Примеры. • Многочлены степени 1 неприводим.

• Неприводимый многочлен степени > 1 не имеет корней. Обратное не верно,

Пример. $x^2 + 1$ над $\mathbb{R}[x]$ неприводим

$(x^2+1)^4$. неприводим.

Теорема $R = k[t]$

k – поле.

$\Rightarrow \forall f$

$\exists\ f = f_1^{k_1} \cdots f_r^{k_r}$

разложение в произведение неприводимых. Это разложение единственно с точностью до порядка и умножения на обратимые элементы (константы).

Доказательство

Наибольший общий делитель

$НОД(f,g) = h$ т.ч.

(1) $h \mid f$, $h \mid g$

(2) если $h_1 \mid f$ и $h_1 \mid g$

$\Longrightarrow h_1 \mid h$.

Если НОД существует $\Longrightarrow$ он единственен с точностью до умножения на обратимый

Теорема. $R = k[t]$ k-поле

$\forall f, g \in k[t]$ $\exists$ НОД

$НОД(f,g) = u \cdot f + v \cdot g$

$\exists u, v \in k[t]$.

<u>Доказательство.</u> (алгоритм Евклида). Можно считать, что $g \neq 0$, $g \nmid f$.

$$f = g \cdot q_1 + r_1 \qquad \deg r_1 < \deg g$$

$$g = r_1 \cdot q_2 + r_2 \qquad \deg r_2 < \deg r_1$$

$$r_1 = r_2 \cdot q_3 + r_3 \qquad \deg r_3 < \deg r_2$$

$$\ldots$$

$$r_k = r_{k+1} q_{k+2} + r_{k+2} \qquad \ldots$$

$$\ldots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} \cdot r_n$$

$\Longrightarrow r_n \mid r_{n-1},\ r_n \mid r_{n-2}, \ldots$

$r_n \mid g,\ r_n \mid h.$

$$r_1 = u_1 f + v_1 \cdot g = f - q_1 \cdot g$$

$$r_2 = g - r_1 q_2 = u_2 f + v_2 g$$

$$\ldots$$

$$r_n = u_n \cdot f + v_n g. \Longrightarrow \text{НОД}. \ \square$$

Теорема. $\mathbb{K}$ – поле.

$\Rightarrow$ $\forall$ многочл. f степени ≥ 1

$f = f_1^{k_1} \ldots f_n^{k_n}$, f_i неприводимы.

Разложение единственно с точностью до порядка множителей.

Существование Индукция по степени.

Единственность

Лемма p неприводим. $p \mid g \cdot h \Rightarrow p \mid g$ или $p \mid h$.

__Доказательство__. Пусть

$p \nmid q \Rightarrow НОД(p,q)=1$

$1 = p \cdot u + q \cdot v$

$h = p \cdot u \cdot h + q \cdot h \cdot v \Rightarrow$

$p \mid h$ $\square$

__Факториальное кольцо.__

Целостное кольцо, в котором выполнена теорема

т.е. $\forall f \in R$

$\exists$ разложение на неразложимые (простые)

и оно единственно с точностью ...

Евклидова кольца

$\exists N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ т.ч.

(a) $N(f \cdot g) \geq N(f)$

"=" $\Longleftrightarrow$ g – обратим

(b) $\forall f, g \quad g \neq 0$

$\exists \quad f = q \cdot g + r$ $\quad r = 0$ или $N(r) < N(g)$.

<u>Теорема</u>: В евклидовом кольце $\exists$ НОД

$\text{НОД}(f, g) = f \cdot u + g \cdot v$.

<u>Теорема</u>: Евклидово кольцо факториально.

Дифференцирования

R алгебра коммутативная ассоциативная

$\partial : R \to R$ дифференцирование если

(1) k-линейно.

(2) $\partial(f \cdot g) = f \cdot \partial(g) + \partial(f) \cdot g$.

Свойства

(a) $\partial(1) = 0$

(b) $\partial(f^n) = \underline{\underline{(n-1)}}\, f^{n-1} \cdot \partial(f)$.

пояснить

Теорема k — поле $\Longrightarrow$

$\exists!\ \partial : k[t] \to k[t]$ т.ч.

$$\partial(t) = 1.$$

Доказательство

Единственность $f = \sum a_i t^i$

$$\partial(f) = \sum i \cdot a_i t^{i-1}$$

Существование Определим этой формулой

Проверка правила Лейбница

(1) Для одночленов

(2) по линейности для всех. $\square$