Евклидово кольцо (ЕК)

Опр. K – евклидово кольцо

$\exists\ \varphi: K \setminus \{0\} \to \mathbb{N} \cup \{0\} = \mathbb{N}_0$

1. $\varphi(a) \le \varphi(ab)\ \ \forall a, b \in K,\ a \neq 0,\ b \neq 0$
2. $\forall a, b\ \ \exists!\ r, s: \ a = bs + r,\ \varphi(r) < \varphi(b)$ или $r = 0$

Теорема ∀ ЕК факториально

Примеры ЕК

1) $\mathbb{Z}$ $\quad \varphi(n) = |n|$
2) $\mathbb{R}[x]$ $\quad \varphi(P_n(x)) = \deg P_n(x)$

Пр. $a = 36 \quad b = 21$

$a = b \cdot 1 + 15$

$b = 15 \cdot 1 + 6$

$15 = 6 \cdot 2 + \boxed{3}$

$6 = 3 \cdot 2 + 0$

$НОД(a, b) = 3$

$15 = a - b$

$b = (a - b) \cdot 1 + 6$

$6 = 2b - a$

$a - b = (2b - a) \cdot 2 + 3$

$НОД(a, b) = 3 = 3a - 5b$

Пример $P = x^3 + x^2 + x - 3 \quad Q = x^2 - 1$

$$\begin{array}{r|l} x^3 + x^2 + x - 3 & x^2 - 1 \\ \hline -\ x^3 - x & (x + 1) \\ \hline x^2 + 2x - 3 & \\ -\ x^2 - 1 & \\ \hline 2x - 2 & \end{array}$$

$P = Q(x + 1) + 2x - 2$

$Q = (x - 1)(x + 1) + 0$

$НОД(P, Q) = \begin{cases} x - 1 \\ 2x - 2 \end{cases}$

Пример. $\mathbb{Z}_3[x]$

$$\begin{array}{r|l} x^3 + x^2 + x + 2 & 2x^2 + x + 1 \\ \hline -\ x^3 + 2x^2 + 2x & 2x + 1 \\ \hline 2x^2 + 2x + 2 & \\ -\ 2x^2 + x + 1 & \\ \hline x + 1 & \end{array}$$

$x^3 + x^2 + x + 2 = (2x + 1)(x^2 + x + 1) + x + 1$

Алгебраически замкнутое поле

$P(x)$ - многочлен

$P(x) \in K[x]$

Опр. α - корень $P(x)$

$\alpha \in K$; $P(\alpha) = 0$

Пример.

$P = x^2 - 1 \in \mathbb{Z}[x]$	$\alpha = \{\pm 1\}$
$P = x^2 - 2 \in \mathbb{Z}[x]$	$\alpha = \{\varnothing\}$
$P = x^2 - 2 \in \mathbb{R}[x]$	$\alpha = \{\pm\sqrt{2}\}$
$P = x^2 + 1 \in \mathbb{R}[x]$	$\alpha = \{\varnothing\}$
$P = x^2 + 1 \in \mathbb{C}[x]$	$\alpha = \{\pm i\}$
$P = x^2 + 1 \in \mathbb{Z}_2[x]$	$\alpha = \{1\}$

Теорема Безу

α - корень $P(x) \Leftrightarrow P(x) \vdots (x - \alpha)$

Док-во:

▲ α - корень $P(x) \Leftrightarrow P(\alpha) = 0$

$P(x) = (x - \alpha) S(x) + r(x)$, $\deg r(x) < \deg (x - \alpha) = 1$

$r(x) = 0$

$P(x) = (x - \alpha) S(x) + r$

$P(\alpha) = 0 + r = 0 \Rightarrow r = 0 \quad P(x) \vdots (x - \alpha)$ ▲

▲ $\Leftarrow \quad P(x) \vdots (x - \alpha) \Rightarrow P(x) = (x - \alpha) S(x) \Rightarrow P(\alpha) = 0$ ▲

Схема Горнера

$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \Rightarrow ((a_0 x + a_1) x + a_2) x + \ldots$

Пример.

$x^5 + 2x^4 - 3x^3 + 2x^2 + x - 3$

$=$

$(x - 1)(x^4 + 3x^3 + 2x + 3)$

	1	2	−3	2	1	−3
$x = 1$	1	3	0	2	3	0

Опр. α – корень кратности „k" многочлена $P(x)$

$P(x) \vdots (x-\alpha)^k \wedge P(x) \not\vdots (x-\alpha)^{k+1}$

Теорема. α – корень кратности k многочлена $P(x)$
α – корень кратности $k-1$ многочлена $P'(x)$

Док-во:

▲ $P(x) = (x-\alpha)^k Q(x), \quad Q(\alpha) \neq 0$

$P'(x) = k(x-\alpha)^{k-1} Q(x) + (x-\alpha)^k Q'(x) = (x-\alpha)^{k-1}\left(kQ(x) + (x-\alpha)Q'(x)\right)$

$kQ(\alpha) + (\alpha-\alpha)\underbrace{Q'(\alpha)}_{=0} \neq 0$ ▲

Теорема

$$\frac{P(x)}{НОД(P(x), P'(x))} = \text{многочлен}$$

$$\frac{(x-\alpha)^k Q(x)}{(x-\alpha)^{k-1} S(x)} \Rightarrow$$ содержит те же корни, что и $P(x)$, но кратности 1

Опр. Неприводимый многочлен кольца $K[x]$ – это простой элемент кольца (нельзя разложить в произведение мн-ов)

Свойства

1) Многочлены 1й степени неприводимые $(ax+b)$

2) $a_0x^2 + a_1x + a_2$

$\mathbb{R}[x]$ $D < 0 \Rightarrow$ неприводимый

$\mathbb{C}[x]$ нет неприводимых

$\mathbb{Z}[x]$ $\frac{p}{q}$ p – делитель a_2, q – делитель a_0

$\mathbb{Z}_p[x]$ $\mathbb{Z}_3[x]$ x^2+1 – неприводимый

$x^2+x^2+1 \quad a=1$

Теорема Эйзенштейна

$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n$ – неприв. в $\mathbb{Z}[x]$

$a_i \vdots P$, $a_n \nmid P^2$, P – простое

$x^5 + \underline{2}x^4 + \underline{4}x^3 + \underline{8}x^2 + \underline{6}x + \underline{2}$

Опр. P – алгебраически замкнуто, если неприводимые многочлены только 1й степени.

Опр. P – алгебраически замкнуто, если $\forall P(x)$ имеет корень.

Пример.

$\mathbb{Z}$ – не АЗ $(2x+1)$

$\mathbb{Q}$ – не АЗ

$\mathbb{R}$ – не АЗ (x^2+1)

Теорема. $\mathbb{C}$ – АЗ (основная теорема алгебры)

Теорема. Неприводимых мн-ов ∞ много

Док-во:

▲ 1) $\exists$ K – беск. кольцо a_i – беск. $x - a_i$ ▲

▲ 2) $\exists |K|$ – конечное.

Предположим $P_1(x), P_2(x), \dots, P_k(x)$

$Q(x) = P_1(x) \cdot P_2(x) \cdot P_3(x) \cdot \dots \cdot P_k(x) + 1 \Rightarrow Q(x) \nmid P_i(x)$

а) $Q(x)$ – неприводим – против. ↯

б) $Q(x) = \alpha(x)\beta(x)$ ▲