14.10.25

Кольцо многочленов

$(a_0, a_1, a_2, \dots, a_n, \dots) \quad \forall a_i \in A$

$(a_0, a_1, a_2, \dots, a_n, \dots) = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + \dots =$

$= a_0(1, 0, 0, \dots) + a_1(0, 1, 0, \dots) + \dots$

$$\boxed{\begin{aligned}(1, 0, 0, \dots) &= 1\\ (0, 1, 0, \dots) &= X\end{aligned}}$$

$X \cdot X = (0, 1, 0, \dots) \cdot (0, 1, 0, \dots) = (0, 0, 1, 0, \dots)$

$C_0 = 0 \cdot 0 = 0 \quad C_1 = a_0 a_1 + a_1 a_0 = 0 \quad C_2 = a_{02} + a_1 \cdot a_1 + a_2 \cdot a_0 = 1$

$X \cdot X^2 = (0, 1, 0, \dots) \cdot (0, 0, 1, 0, \dots) = (0, 0, 0, 1, 0, \dots)$

$C_0 = a_0 b_0 = 0 \quad C_1 = a_0 b_1 + a_1 b_0 = 0$

$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$

$C_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 1$

$(a_0, a_1, a_2, \dots, a_n, \dots) = a_0(1, 0, 0, \dots) + a_1(0, 1, 0, \dots) + \dots =$

$= a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \dots \qquad a_i \in A$

$A[x]$ — Кольцо многочленов над кольцом A

Св-ва многочленов:

1) $\deg P(x) = \deg(a_0, a_1, a_2, \dots) = \max i \quad a_i \neq 0$
2) $\deg(P(x) + Q(x)) \leq \max(\deg P(x), \deg Q(x))$
3) $\deg(P(x) \cdot Q(x)) \leq \deg P(x) + \deg Q(x)$

$(\alpha X^n + \dots)(\beta X^k + \dots) = \alpha\beta X^{n+k}$

$\alpha \neq 0 \qquad \beta \neq 0 \qquad \alpha\beta \overset{?}{=} 0$

$\Leftarrow$ α, β — делители нуля

$\mathbb{Z}_4[x] \qquad 2x^2 \cdot 2x^2 = 0$

4) $\deg(P(x) \cdot Q(x)) = \deg P(x) + \deg Q(x) \Leftrightarrow$ кольцо целостное

Теорема. A – целостное кольцо $\Rightarrow$
$\Rightarrow A[x]$ – целостное кольцо

Теорема K – коммут. кольцо с 1 $\Rightarrow L \subseteq K$

$\exists\, \varphi : L[x] \to K :$
1) $\forall a \in L \quad \varphi(a) = a$
2) $\varphi(x) = x\ ,\ x \in K$

$L[x] \quad a_0 + a_1 x + \ldots + a_n x^n$

$$\varphi(a_0 + a_1 x + \ldots + a_n x^n) = \varphi(a_0) + \varphi(a_1 x) + \varphi(a_2 x^2) + \ldots +$$
$$+ \varphi(a_n x^n) = \varphi(a_0) + \varphi(a_1)\cdot\varphi(x) + \varphi(a_2)\cdot\varphi(x)\cdot\varphi(x) + \ldots +$$
$$+ \varphi(a_n)\cdot(\varphi(x))^n = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$$

t – алгебраическое число над кольцом A

$\varphi(t) = 0 \iff a_0 + a_1 t + \ldots + a_n t^n = 0$

t – трансцендентное число над кольцом A

$\varphi(t) \neq 0$

Пример

$\mathbb{Z} \Rightarrow \mathbb{Z}[x]$

$2 :\ x - 2 \qquad n :\ x - n \quad \Rightarrow$ все t – алгебраические

$\frac{2}{3} :\ 3x - 2 \qquad \frac{p}{q}$ – алг. над $\mathbb{Z} \qquad qx - p$

Поле рациональных дробей

$\frac{P_n(x)}{Q_k(x)} \qquad P_n(x),\ Q_k(x) \in A[x]$

Факториальные кольца

K – целостное кольцо

Опр. $a \mid b$ $(a \vdots b) \Leftrightarrow \exists c: ac = b$

Опр. $a \mid b$, $b \mid a \Rightarrow a, b$ – ассоциированные

Опр. a – простой элемент $K \Leftrightarrow a$ необратим и не разлагается в произв. необратимых.

Пример

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Z}[x]$
простые	$\pm 2; \pm 3; \pm 5$	нет	
ассоц.	$1, -1$ $2, -2$ $\ldots$ $n, -n$	$\frac{p}{q}^{\neq 0}, \frac{a}{b}^{\neq 0}$	

Св-ва

1) $a \mid b$, $b \mid c \Rightarrow a \mid c$
2) $a \mid b$, $a \mid c \Rightarrow c \mid (b+a)$
3) ?

Опр. K – факториальное кольцо

$\forall a \neq 0$, $a \in K$ $\qquad u \in K$ – обратим

$a = u \cdot p_1 \cdot p_2 \cdots p_s$ $\qquad p_i \in K$ – простые

$a = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_r$, $\qquad v \in K$ – обратим

$q_i \in K$ – простые

то $s = r$

$p_1 = \alpha_1 q_1$; $p_2 = \alpha_2 q_2$; $\ldots$ α_i – обратим.

Пример.

$\mathbb{Z}$, $A[x]$ — факториальные

Опр. $НОД(a, b) = n$

1) $n \mid a$, $n \mid b$

2) $k \mid a$, $k \mid b \Rightarrow k \mid n$

Опр. $НОК(a, b) = m$

1) $a \mid m$, $b \mid m$

2) $a \mid k$, $b \mid k \Rightarrow m \mid k$

Теорема

$$a = u \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \qquad b = v \cdot p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$$

$$НОД(a, b) = w \cdot p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_s^{\min(\alpha_s, \beta_s)}$$

$$НОК(a, b) = t \cdot p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_s^{\max(\alpha_s, \beta_s)}$$

$$НОД(a, b) \cdot НОК(a, b) = u \cdot a \cdot b$$

Алгоритм Евклида

$НОД(a, b) = ?$

$a = b \cdot s_1 + r_1$

$b = r_1 s_2 + r_2$

$r_1 = r_2 s_3 + r_3$

$r_2 = r_3 s_4 + r_4$

$\ldots\ldots$

НОД(a, b)

$r_k = r_{k+1} s_{k+2} + \boxed{r_{k+2}}$

$r_{k+1} = \boxed{r_{k+2}} s_{k+3} + 0$

Теорема

$\forall a, b \ \exists u, v \Rightarrow ua + vb = НОД(a, b)$