26.04.2016

(14) Пръстенът на полиномите на една променлива. Теорема за деление с частно и остатък. Правило на Хорнер. Принципи за сравняване на коефициентите.

Полиноми на една променлива

Нека A - комутативен пръстен с 1

$B = \{ f(a_0, a_1, \dots, a_i, \dots) \mid a \in A \}$

$g = (b_0, b_1, \dots, b_j, \dots)$

$f+g := (a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots)$

$fg := (d_0, d_1, \dots, d_n, \dots)$, $d_n := \sum_{i+j=n} a_i b_j$

$(a_0 b_0, a_1 b_0 + a_0 b_1, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$

$(B, +, \cdot)$ - комутативен пръстен с 1, (директна проверка на аксиомите)

Нека проверим **асоциативен закон** на умножението:

$h = (c_0, c_1, \dots, c_k, \dots)$

$(\forall f, g, h \in B \Rightarrow (fg)h = f(gh))$

$gh = (t_0, t_1, \dots, t_s, \dots)$, $t_s = \sum_{j+k=s} b_j c_k$

$(fg)h = (u_0, u_1, \dots, u_m, \dots)$

$f(gh) = (v_0, v_1, \dots, v_m, \dots)$

$u_m = v_m$, $\forall m$

$u_m = \sum_{n+k=m} d_n c_k = \sum_{n+k=m} \left(\sum_{i+j=n} a_i b_j \right) c_k \overset{A}{=\!=} \sum_{i+j+k=m} a_i b_j c_k$

$v_m = \sum_{i+s=m} a_i t_s = \sum_{i+s=m} a_i \left(\sum_{j+k=s} b_j c_k \right) \overset{A}{=\!=} \sum_{i+j+k=m} a_i b_j c_k$

//.

$B(0, 0, \dots, 0, \dots) = 0$

$(1, 0, \dots, 0, \dots) = 1, \quad (a, 0, \dots, 0) = a$

$A_0 = \{(a, 0, \dots, 0, \dots) \mid a \in A\} \leq B$

$\begin{cases} A \to A_0 \\ a \to (a, 0, \dots, 0, \dots) \end{cases} : \varphi$

φ - биекция

φ - хомоморфизъм на пръстени

$\Big\} \varphi \cong \Rightarrow A \cong A_0$

↓

$\varphi(a+b) = \varphi(a) + \varphi(b)$

$\varphi(ab) = \varphi(a)\varphi(b)$

$\Rightarrow (a, 0, \dots, 0, \dots) = a$

$x \overset{def}{=} (0, 1, 0, \dots, 0) \Rightarrow x^2 = (0, 0, 1, 0, \dots, 0) \Rightarrow$

$\Rightarrow x^n = (0, 0, \dots, 0, \underbrace{1}_{n+1 \text{ позиция}}, 0, \dots 0)$

$ax^n = (a, 0, \dots, 0)(0, 0, \dots, 0, \underbrace{1}_{n+1 \text{ поз.}}, 0, \dots, 0) = (0, \dots, 0, \underbrace{a}_{n+1 \text{ поз.}}, 0, \dots 0)$

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

$+ (0, 0, \dots, 0, \underbrace{a_n}_{n+1 \text{ поз.}}, 0, \dots 0) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = f(x)$

Тъй като интуитивно въведената дефиниция на полином се различава от позната от училищния курс, то: -3-

$B = \{ f(x) = b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n \mid b_i \in A, n \in \mathbb{N} \}$

$\parallel$ (на променливата x)

$A[x]$ - пръстенът на полиномите с коефициенти от A

~~$A(x)$~~ (полиномиален пръстен над A)

$f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in A[x]$

a_0 - старши коефициент, $a_0 \neq 0$

$a_0 = 1$ - унитарен полином

a_i - коефициенти

a_n - свободен коефициент

$n = \deg f$ - степен на полином

$f = a \neq 0 = \text{const}, \deg f = 0$

! $\deg 0 := -\infty$

$\deg(f+g) \leq \max(\deg f, \deg g)$

$\deg(fg) = \deg f + \deg g$, A - област (комутативен пръстен с 1 без делители на 0)

пример:

$\mathbb{Z}_6$: $(\bar{2}x^7 + \dots)(\bar{3}x^4 + \dots) = \bar{0}x^{11}$

$(-3x^6 + \dots) + (3x^6 + \dots)$

A - комутативен пръстен с 1 $\longrightarrow$ $A[x]$ - комутативен пръстен с 1

A - област $\longrightarrow$ $A[x]$ - област

! F - поле $\longrightarrow$ $F[x]$ - област

$A[x]$ функция

полином $\rightarrow f \longrightarrow f : a \in A \rightarrow f(a) := a_0 a^n + \dots + a_n \in A$

$f = g \longrightarrow f = g$

! $f = g \not\longleftarrow f = g$

пример:

$x^p \neq x \longrightarrow x^p = x$, $\forall x \in \mathbb{Z}_p$ (следствие от малката теорема на Ферма: $x^p \equiv x \pmod p$)

Нека $F[x]$, F - поле

Th|| (деление с частно и остатък)

Нека $f, g \in F[x]$, $g \neq 0$. Тогава $\exists!$ q (частно), r (остатък), $q, r \in F[x]$: $f = gq + r$, $\deg r < \deg g$

Доказателство:

$\exists$) Индукция по $\deg f = n$, $f = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, $g = b_0 x^s + b_1 x^{s-1} + \ldots + b_s$

база: $g = const \neq 0$

$f = g(g^{-1} f) + 0$

$q \quad r$

$\deg f < \deg g$

$f = g \cdot 0 + f$

$q \quad r$

ИП: $(a_0 x^n + \ldots + a_n) - (x^{n-s} a_0 b_0^{-1}) = g = f_1$, $\deg f \leq n-1$

ИП $\Rightarrow \exists q_1, r_1 : f_1 = g q_1 + r_1$, $\deg r_1 < \deg g$

$f = f_1 + a_0 b_0^{-1} x^{n-s} g = g q_1 + r_1 + a_0 b_0^{-1} x^{n-s} g =$

$= (\underbrace{q_1 + a_0 b_0^{-1} x^{n-s}}_{q}) g$, $\deg r < \deg g$

!) $f = gq_1 + r_1 = gq_2 + r_2$, $\deg r_i < \deg g$, $i = 1,2$

$g(q_1 - q_2) = r_2 - r_1$, $q_1 \neq q_2$

$\deg(g(q_1 - q_2)) \underset{F}{=} \deg g + \deg(q_1 - q_2) \geq \deg g > \deg(r_2 - r_1)$

$\Rightarrow$ (1) $\Rightarrow q_1 = q_2$, $r_1 = r_2$

Забележка: Ако A - област, b_0 - обратим елемент, $b_0 = 1$, но ако A - комутативен пръстен с 1, не е обратим

$\mathbb{Z}_6$: $\bar{3}x^3 = (\bar{3}x^2 - \bar{1})(x + \bar{2}) + (x + \bar{2})$

$\bar{3}x^3 = (\bar{3}x^2 - \bar{1})(x + \bar{4}) + (x + \bar{4})$ $\Rightarrow$ няма еднозначност

Приложение на Th (деление с частно и остатък):

$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, $g = x - \alpha$; $a_i, \alpha \in F$

$q = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}$

$f = gq + r$, $\deg r < 1 \Rightarrow r \in F$

$a_0x^n + a_1x^{n-1} + \ldots + a_n = (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + \underbrace{r}$

$a_0 = b_0$

$a_1 = b_1 - \alpha b_0$

$a_2 = b_2 - \alpha b_1$

$\ldots$

$a_{n-1} = b_{n-1} - \alpha b_{n-2}$

$a_n = r - \alpha b_{n-1}$

Хорнер $\longrightarrow$

$b_0 = a_0$

$b_1 = a_1 + \alpha b_0$

$b_2 = a_2 + \alpha b_1$

$\ldots$

$b_{n-1} = a_{n-1} + \alpha b_{n-2}$

$r = a_n + \alpha b_{n-1}$

	a_0	a_1	$\ldots$	a_{n-1}	a_n
α	$a_0 = b_0$	b_1	$\ldots$	b_{n-1}	r

схема на Хорнер

$f = g(x - \alpha) \Leftrightarrow r = 0$

(ТВ) $\mathbb{K}$ - област, $g = x - \alpha \in \mathbb{K}[x]$

$f \in \mathbb{K}[x]: f = gq + r$

$\Rightarrow f = g(x-\alpha) \Leftrightarrow r = 0$

Th|| Всеки идеал в пръстена $F[x]$ е главен идеал, породен от полинома от най-ниска степен, принадлежащ на множеството I.

Доказателство: $F[x]$, $\{0\} \trianglelefteq F[x]$, Нека $I \neq \{0\}$ и нека $f \in I$, $\deg f = n$ - възможно най-ниската степен на елемент от I.

Ще докажем, че $I = (f) = \{f.h \mid h \in F[x]\}$

Нека $g \in I \Rightarrow g = fq + r$, $\deg r < \deg f = n$

$\underbrace{g}_{\in I}$ $\underbrace{f}_{\in I}$

$r = g - fq \in I \Rightarrow r = 0 \Rightarrow g = fq \in (f) \Rightarrow$

$\Rightarrow I \subseteq (f)$ (1)

Обратно, нека $t \in (f) \Rightarrow t = \underbrace{f}_{\in I} . \underbrace{s}_{\in F[x]} \Rightarrow t \in I \Rightarrow (f) \subseteq I$ (2)

От (1), (2) $\Rightarrow I = (f)$

$\mathbb{K}$ - област, $f = (x-\alpha)q \Leftrightarrow f(\alpha) = r = 0$

ТВ|| Нека $f \in \mathbb{K}[x]$, $\deg f = n$, $\exists \alpha_i \in \mathbb{K}$, $\alpha_i \neq \alpha_j$, $f(\alpha_i) = 0$.
$i = \overline{1, n+1}$ $i \neq j$

Тогава $f = 0$.

Доказателство:

$f = (x-\alpha_1) q_1(x) \longrightarrow f(\alpha_2) \overset{\mathbb{K} \text{ област}}{=} (\alpha_2 - \alpha_1) q_1(\alpha_2) = 0 \Rightarrow q_1(\alpha_2) = 0$ $\neq 0$, защото сме в област

$\Rightarrow q_1 = (x-\alpha_2)\,q_2(x) \Rightarrow q_1(\alpha_3) = (\alpha_3-\alpha_2)\,q_2(\alpha_3) = 0$ ...

$f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_{n+1})\,q_{n+1}(x)$

$\deg f = n > n+1$

$\Rightarrow f = 0$

Ако K **не е област**:

$\mathbb{Z}_{16}$: $x^2 = 0$

$\bar{0}, \bar{4}, \bar{8}, \overline{12}$ - 4 корена, но полиномът е от втора степен

Следствие (Принцип за сравнение на коефициентите)

Нека $f, g \in \underset{\text{обл}}{K}[x]$, $\alpha_i \in K$, $\alpha_i \neq \alpha_j$ $\quad i = \overline{1,n+1}$ $\quad i \neq j$

$\deg f = \deg g = n$

$f(\alpha_i) = g(\alpha_i)$, $i = \overline{1,n+1} \Rightarrow f = g$

Доказателство:

$f - g$ и приложим предното твърдение $\Rightarrow f = g$