15.04.2013г. ВА - лекция

Полиноми на една променлива

A - комутативен пръстен с 1 (напр. $A = \mathbb{Z}$)

$B = \{(a_0, a_1, a_2, \dots) \mid a_i \in A\}$ - краен брой $\neq 0$

$f = (a_0, a_1, a_2 \dots)$ $g = (b_0, b_1, b_2 \dots)$

Деф. $f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$

$f.g = (c_0, c_1, c_2, 0 \dots 0)$

$c_n = \sum_{i+j=n} a_i b_j$

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

c_3

с тези две деф. операции, полученото множество става комутативен пръстен.

Озн. $A_0 = \{(a, 0, 0, \dots) \mid a \in A\}$ - подпръстен на B

$A \to A_0$
$A \to (a, 0, 0, \dots)$ → биекция
} изоморфизъм

Всъщност в себе си като подпръстен а

$A \subseteq B$ $a \equiv (a, 0, 0, \dots)$

Озн. $x = (0, 1, 0, 0, \dots)$

$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$x = (0, 1, 0, 0, \dots)$

$x^2 = (0, 0, 1, 0, \dots)$

$x^n = (0, 0, \dots, 1, 0, \dots 0)$

$n+1$ позиция

$a.x = (0, a, 0, \dots 0)$

$\vdots$

$a x^n = (0, \dots, 0, 0, 0, \underset{\downarrow}{a}, 0, \dots)$

(n+1) позиция

$f = (a_0, a_1, a_2, \dots, a_n, 0, 0, 0\dots) = (a_0, 0, 0, \dots, 0, \dots) +$
$+ (0, a_1, 0, \dots, 0, \dots) +$
$+ (0, 0, a_2, \dots 0, \dots) + \dots +$
$+ \dots +$
$+ (0, 0, 0, \dots, a_n, 0, \dots) =$
$= a_0 + a_1 x + a_2 x^2 + \dots + \underset{\neq 0}{a_n} x^n$

$B = A[x]$ ако се напише някъ F е полином в $A[x]$, то F е полином с коефициенти от A

$f = f(x)$

$x = 5 \quad f(5)$

$5 = (5, 0, 0, \dots, 0)$

$x = (0, 1, 0, \dots, 0)$

$\deg f = n$ (степен на полином)

$a \in A,\ a \neq 0 \quad \deg a = 0$

$\deg 0 = -\infty$

нулевия полином има степен $-\infty$

Пример:

$\mathbb{Z}_6$

$\bar{2} \cdot x^3 \cdot \bar{3} x^7 = \bar{6} x^{10} = \bar{0}$

$\deg(fg) = \deg f + \deg g$

Ако f и g са цели $g \neq 0$

то $\exists !\ q, r \in \mathbb{Z}$:

$f = gq + r, \ 0 \leq r < |g|$

Тh за деление с остатък.

F - поле, $f, g \in F[x]$, $g \neq 0$

Тогава $\exists$ еднозначно определени полиноми $q, r \in F[x]$:

$f = gq + r$, $\deg r < \deg g$

Док. Нека $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $g = b_0x^m + b_1x^{m-1} + \ldots + b_m$, $b_0 \neq 0$

Съществуване:

при $m > n$

$f = \underset{q}{0} \cdot g + \underset{r}{f}$

$g \neq 0$ пример $g = 5$

$f = 5 \cdot \underset{q}{\frac{1}{5} f} + \underset{r}{0}$

Индукция по $n = \deg f$

$n = 0$, $n > 0$

Разглеждаме $f_1 = f - b_0^{-1} a_0 x^{n-m} g$

$\deg f_1 < \deg f = n$

инд. предп. : $\exists\, q_1, r_1 \in F[x]$:

$f_1 = g \cdot q_1 + r_1$, $\deg r_1 < \deg g$

ще представим f като произведение на $g \cdot q + r_1 + 0$

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

$= g \underbrace{(q_1 + b_0^{-1} a_0 x^{n-m})}_{q} + \underset{r_1}{r_1}$

Единственост: $f = gq_1 + r_1, \quad \deg r_1 < \deg g$

$f = gq_2 + r_2, \quad \deg r_1 < \deg g$

$0 = g(q_1 - q_2) + r_1 - r_2$

$r_2 - r_1 = g(q_1 - q_2)$

$q_1 - q_2 \neq 0 \Rightarrow \deg(q_1 - q_2) \geq \deg g > \deg(r_2 - r_1)$

$q_1 - q_2 = 0 \Rightarrow q_2 - r_1 = 0$

$$
\begin{array}{l|l}
3x^3 - 2x + 4 & 2x^2 + x + 1 \\
\hline
-\ 3x^3 - \frac{3}{2}x^2 + \frac{3}{2}x & \underbrace{\frac{3}{2}x - \frac{3}{4}}_{q} \\
\hline
-\frac{3}{2}x^2 - \frac{7}{2}x + \frac{8}{2} & \\
-\ \frac{3}{2}x^2 - \frac{3}{4}x - \frac{3}{4} & \\
\hline
\underbrace{-\frac{11}{4}x + \frac{19}{4}}_{r} &
\end{array}
$$

$$3x^2 - 2x + 4 = (2x^2 + x + 1)\underbrace{\left(\frac{3}{2}x - \frac{3}{4}\right)}_{q} \underbrace{- \frac{11}{4}x + \frac{19}{4}}_{r}$$

Следствие: Ако F-поле $\Rightarrow$ в $F[x]$ всеки идеал е главен

Док. $I \trianglelefteq F[x]$. Ако $I = (0)$ ✓

Нека $I \neq (0)$ и $0 \neq g \in I$, g - с най-ниска степен

Ще док., че $I = (g)$. Очев. $(g) \subseteq I$

$\Leftarrow$ нека $f \in I$ $\quad f = g.q + r, \quad \deg r < \deg g$

$r = \underbrace{f}_{\in I} - \underbrace{g}_{\in I}.q \in I \Rightarrow r = 0 \Rightarrow f = g.q \in (g)$

Следствие: Нека K е поле $f \in K[x]$ и $\alpha \in K : f(\alpha) = 0$

Тогава $f(x) = (x-\alpha)\, q(x)$, $q(x) \in K[x]$

$f(x) = (x-\alpha)\, q(x) + r$, $r \in K$

$x \to \alpha$

$0 = f(\alpha) = r$

Следствие:* F - поле, $f \in F[x]$ е полином. Ако $f \neq 0$, $\deg f = n$, то f не може да има $> n$ различни корена.

Док. Доп., че $\exists\ \alpha_1, \alpha_2, \dots, \alpha_{n+1}$, 2×2 разл. и $f(\alpha_i) = 0$

$f(x) = (x-\alpha_1)\, q_1(x)$ $\quad 0 = f(\alpha_2) = \underbrace{(\alpha_2-\alpha_1)}_{\neq 0}\, q_1(\alpha_2) \Rightarrow q_1(\alpha_2) = 0$

от предното сл.

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

$f(x) = (x-\alpha_1)(x-\alpha_2)\, q_2(x)$

Следствие** (принцип за сравняване на коефициентите)

F - поле, $g, h \in F[x]$, $\deg g \leq n$, $\deg h \leq n$

Ако $\exists$ 2×2 различни елемента $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in F$:

$g(\alpha_i) = h(\alpha_i)$, то $g = h$

Док. Прил. предното сл. за полинома $f = g - h$

$* \Leftrightarrow **$