

29. 04. 2013г. ВА - лекция

### Корени на полиномите

$F$  - поле  $f(x) \in F[x]$ ,  $\deg f > 0$   
 $x^2 - 2 \in \mathbb{Q}[x] \in \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$   
 $x^2 + 1 \in \mathbb{R}[x]$

Тв.  $I = (f) \trianglelefteq F[x]$   $F[x]/I$  е поле  
 $\Leftrightarrow F$  е неразложим над  $F$

Доказ.

$\Rightarrow F[x]/I$  - поле

$(\bar{g} = g + I, \bar{g} = 0 \Leftrightarrow g \in I)$

Доп. а  $f = gh \Rightarrow \bar{f} = \bar{g}\bar{h}$

$\Rightarrow \bar{g} = 0$  или  $\bar{h} = 0$ , т.е.  $g \in I$  или  $h \in I$ , но  
 това е  $\because$ , защото  $\deg g < \deg f$ ,  
 $\deg h < \deg f$

$\Leftarrow f$  - неразложим

$0 \neq \bar{g} \in F[x]/I \Rightarrow g \notin I$ , т.е.  $f \nmid g$   
 $\Rightarrow (f, g) = 1$  от Бету  $\Rightarrow \exists u, v: u \cdot f + v \cdot g = 1$   
 $\bar{u}\bar{f} + \bar{v}\bar{g} = 1$ , но  $\bar{f}$  е нулевия елемент  $\Rightarrow \bar{v}\bar{g} = 1$

Тв.  $F$  - поле,  $f \in F[x]$ ,  $\deg f > 0$ . Тогава  $F$  разложима над  $F$ ,  
 ако и само ако  $f$  има корен.

Схеми на връзки: Можем да си помислим че  $f$  е неразложим над  $F$   
 Озн.  $K = F[x]/(f)$  - поле (Тв.) Нека  $\pi: F[x] \rightarrow K = F[x]/(f)$   
 $\pi(g) = \bar{g}$

Озн.  $d = \prod |x|$

Сп.  $\exists$  разширение  $L$  на  $F$ , съдържащо всички корени на  $f \in L$   $f$  се разлага на линейни

Док.  $F \subseteq K_1 \ni d_1 \quad f(d_1) = 0 \quad f = (x - d_1)g, \quad g \in K_1[x]$

$K_1 \subseteq K_2 \ni d_2 : g(d_2) = 0 \quad g = (x - d_2)h, \quad f = (x - d_1)(x - d_2)h$

Опр Поле на разлагане на  $f$  над  $F =$  минималното поле  $\forall$  нулюлата на  $d \in F$  и корените на полинома  $f$ .

зау.  $I = (x^2 + 1) \triangleq \mathbb{R}[x]$  Док.  $\mathbb{R}[x]/I \cong \mathbb{C}$

$\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$

$g(x) \mapsto g(i)$

$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$

$\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}(\sqrt{2})$

$g(x) \mapsto g(\sqrt{2})$

$f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n = (x - d_1)(x - d_2)(x - d_3) \dots (x - d_n)$

$a_1 = -a_0(d_1 + d_2 + d_3 + \dots + d_n) \quad a_2 = a_0(d_1 d_2 + d_1 d_3 + \dots)$

$d_1 + d_2 + \dots + d_n = -\frac{a_1}{a_0}$

$a_0 x^3 + a_1 x^2 + a_2 x + a_3 = a_0(x - d_1)(x - d_2)(x - d_3)$

$d_1 + d_2 + d_3 = -\frac{a_1}{a_0}$

$d_1 d_2 + d_1 d_3 + d_2 d_3 = \frac{a_2}{a_0}$

$d_1 d_2 d_3 = -\frac{a_3}{a_0}$

$d_1 d_2 d_3 + \dots + d_{n-1} d_n = \frac{a_2}{a_0}$

$d_1 d_2 d_3 + \dots = -\frac{a_3}{a_0}$

$d_1 d_2 \dots d_n = (-1)^n \frac{a_n}{a_0}$

29.04.2013. ВА - лекция

$p$  - простое число,  $p > 2$ ,  $\mathbb{Z}_p$  - поле

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\} \quad x \in \mathbb{Z}_p \quad x^p = x \quad x \neq 0 \quad x^{p-1} = 1$$

$$f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$$

Прп.  $\lambda$  е  $k$ -кратен корен на  $f$ , ако  $f = (x-\lambda)^k g$ ,  $g(\lambda) \neq 0$ ,  $k=1$   $\lambda$ -прост корен  $f'(\lambda) \neq 0$

Th |  $\text{char } F = 0$   $\lambda$  е  $k$ -кратен корен на  $f \Leftrightarrow f(\lambda) = f'(\lambda) = \dots = f^{(k-1)}(\lambda) = 0$ , но  $f^{(k)}(\lambda) \neq 0$

Док.  $\Rightarrow$   $f = (x-\lambda)^k g$ ,  $g(\lambda) \neq 0$ . Умножаваме по  $k$ .

$$f = (x-\lambda)^k g, \quad g(\lambda) \neq 0$$

$$f' = k(x-\lambda)^{k-1} g + (x-\lambda)^k g'$$

Док.  $f'(\lambda) = g(\lambda) \neq 0$

Нека  $k > 1$

$$\Rightarrow f = (x-\lambda)^k g, \quad g(\lambda) \neq 0$$

$$f' = k(x-\lambda)^{k-1} g + (x-\lambda)^k g' = (x-\lambda)^{k-1} [kg + (x-\lambda)g']$$

$$h(\lambda) = kg(\lambda) \neq 0 \quad (\text{char } F = 0)$$

$0 \neq f' = (x-\lambda)^{k-1} h$ ,  $h(\lambda) \neq 0 \Rightarrow \lambda$  е  $(k-1)$ -кратен корен на  $f'$

и т.н.  $\Rightarrow \lambda$  е  $k$ -кратен корен на  $f$  по  $(k-1)$ -кратен корен на  $f'$ .

Th  $\Leftarrow$  Доказ.  $f(\lambda) = f'(\lambda) = \dots = f^{(k-1)}(\lambda) = 0$ ,  $f^{(k)}(\lambda) \neq 0$

Нека  $\lambda$  е  $e$ -кратен:  $f(x) = (x-\lambda)^e g(x)$ ,  $g(\lambda) \neq 0$ .

Укажеме  $e$  и  $k$ , че  $e = k$

Док. че  $e < k \Rightarrow e \leq k-1 \Rightarrow f^{(e)}(\lambda) = 0$  при  $e \leq k-1$  с аса  $e$  и  $k < e \Rightarrow k \leq e-1$  от  $f^{(k)}(\lambda) = 0 \Rightarrow \lambda$  е  $k$ -кратен корен = поне  $e$ -кратен (не е прост)

ТВ Если полином  $f$  и  $f'$  имеют общий корень  $\alpha \Rightarrow f$  имеет корень  $\alpha$

Сл Если полином  $f$  и  $f'$  имеют общий корень  $\alpha$ , то  $f$  имеет корень  $\alpha$

Доказательство  
Пусть  $f(x) = K_1(x-\alpha)^m \cdot g(x)$  и  $f'(x) = K_2(x-\alpha)^n \cdot h(x)$   
где  $g(\alpha) \neq 0$  и  $h(\alpha) \neq 0$   
Тогда  $f' = K_2(x-\alpha)^n \cdot h(x) = m \cdot K_1(x-\alpha)^{m-1} \cdot g(x) + K_1(x-\alpha)^m \cdot g'(x)$   
Сравним коэффициенты при  $(x-\alpha)^{n-1}$  в  $f'$  и  $f'$ .  
В  $f'$  коэффициент равен  $K_2 \cdot h(\alpha)$ .  
В  $f'$  коэффициент равен  $m \cdot K_1 \cdot g(\alpha)$ .  
Так как  $h(\alpha) \neq 0$  и  $g(\alpha) \neq 0$ , то  $K_2 \cdot h(\alpha) = m \cdot K_1 \cdot g(\alpha)$ .  
Отсюда  $K_2 = \frac{m \cdot K_1 \cdot g(\alpha)}{h(\alpha)}$ .  
Подставим это в  $f'$ :  
 $f'(x) = \frac{m \cdot K_1 \cdot g(\alpha)}{h(\alpha)} (x-\alpha)^n \cdot h(x) = m \cdot K_1 (x-\alpha)^n \cdot \frac{g(x) \cdot h(x)}{h(\alpha)}$   
Сравним коэффициенты при  $(x-\alpha)^{n-1}$  в  $f'$  и  $f'$ .  
В  $f'$  коэффициент равен  $m \cdot K_1 \cdot \frac{g(\alpha) \cdot h(\alpha)}{h(\alpha)} = m \cdot K_1 \cdot g(\alpha)$ .  
В  $f'$  коэффициент равен  $m \cdot K_1 \cdot g(\alpha)$ .  
Таким образом, равенство выполняется.

Другой способ  
Пусть  $\alpha$  - общий корень  $f$  и  $f'$ . Тогда  $f(\alpha) = 0$  и  $f'(\alpha) = 0$ .  
Рассмотрим разложение  $f(x) = (x-\alpha)^m \cdot g(x)$ , где  $g(\alpha) \neq 0$ .  
Тогда  $f'(x) = m(x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x)$ .  
Подставим  $x = \alpha$ :  
 $f'(\alpha) = m(\alpha-\alpha)^{m-1} \cdot g(\alpha) + (\alpha-\alpha)^m \cdot g'(\alpha) = m \cdot 0^{m-1} \cdot g(\alpha) + 0 \cdot g'(\alpha) = 0$ .  
Так как  $g(\alpha) \neq 0$ , то  $m \cdot 0^{m-1} = 0$ .  
Если  $m = 1$ , то  $0^0 = 1$ , и  $1 \cdot g(\alpha) = 0$ , что противоречит  $g(\alpha) \neq 0$ .  
Следовательно,  $m \geq 2$ .  
Таким образом,  $\alpha$  является корнем  $f$ .

Случай 1  
Если  $f(x) = K_1(x-\alpha)^m$ , то  $f'(x) = m \cdot K_1(x-\alpha)^{m-1}$ .  
Если  $\alpha$  - корень  $f$  и  $f'$ , то  $f'(\alpha) = 0$ .  
Тогда  $m \cdot K_1(\alpha-\alpha)^{m-1} = 0$ .  
Если  $m = 1$ , то  $K_1 = 0$ , что противоречит  $f(x) = K_1(x-\alpha)^m$ .  
Следовательно,  $m \geq 2$ .  
Таким образом,  $\alpha$  является корнем  $f$ .

Случай 2  
Если  $f(x) = K_1(x-\alpha)^m \cdot g(x)$ , то  $f'(x) = m \cdot K_1(x-\alpha)^{m-1} \cdot g(x) + K_1(x-\alpha)^m \cdot g'(x)$ .  
Если  $\alpha$  - корень  $f$  и  $f'$ , то  $f'(\alpha) = 0$ .  
Тогда  $m \cdot K_1(\alpha-\alpha)^{m-1} \cdot g(\alpha) + K_1(\alpha-\alpha)^m \cdot g'(\alpha) = 0$ .  
Так как  $g(\alpha) \neq 0$  и  $g'(\alpha) \neq 0$ , то  $m \cdot K_1(\alpha-\alpha)^{m-1} \cdot g(\alpha) = -K_1(\alpha-\alpha)^m \cdot g'(\alpha)$ .  
Отсюда  $m \cdot (\alpha-\alpha)^{m-1} \cdot g(\alpha) = -(\alpha-\alpha)^m \cdot g'(\alpha)$ .  
Таким образом,  $\alpha$  является корнем  $f$ .

Случай 3  
Если  $f(x) = K_1(x-\alpha)^m \cdot g(x)$ , то  $f'(x) = m \cdot K_1(x-\alpha)^{m-1} \cdot g(x) + K_1(x-\alpha)^m \cdot g'(x)$ .  
Если  $\alpha$  - корень  $f$  и  $f'$ , то  $f'(\alpha) = 0$ .  
Тогда  $m \cdot K_1(\alpha-\alpha)^{m-1} \cdot g(\alpha) + K_1(\alpha-\alpha)^m \cdot g'(\alpha) = 0$ .  
Таким образом,  $\alpha$  является корнем  $f$ .

Случай 4  
Если  $f(x) = K_1(x-\alpha)^m \cdot g(x)$ , то  $f'(x) = m \cdot K_1(x-\alpha)^{m-1} \cdot g(x) + K_1(x-\alpha)^m \cdot g'(x)$ .  
Если  $\alpha$  - корень  $f$  и  $f'$ , то  $f'(\alpha) = 0$ .  
Тогда  $m \cdot K_1(\alpha-\alpha)^{m-1} \cdot g(\alpha) + K_1(\alpha-\alpha)^m \cdot g'(\alpha) = 0$ .  
Таким образом,  $\alpha$  является корнем  $f$ .

Случай 5  
Если  $f(x) = K_1(x-\alpha)^m \cdot g(x)$ , то  $f'(x) = m \cdot K_1(x-\alpha)^{m-1} \cdot g(x) + K_1(x-\alpha)^m \cdot g'(x)$ .  
Если  $\alpha$  - корень  $f$  и  $f'$ , то  $f'(\alpha) = 0$ .  
Тогда  $m \cdot K_1(\alpha-\alpha)^{m-1} \cdot g(\alpha) + K_1(\alpha-\alpha)^m \cdot g'(\alpha) = 0$ .  
Таким образом,  $\alpha$  является корнем  $f$ .