петък 28.05
от 15:00 ч.
лекция

Поле на разлагане

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$

$i^2 = -1$ — $\mathbb{R} \subset \mathbb{C}$
— $i \in \mathbb{C}$, $i^2 = -1$

$a \cdot 1 + 0i$

$X^2 + 1 =$

$\mathbb{C}$ е лин. пр-во над $\mathbb{R}$ с базис $1, i$

$x^3 = 5$

$\mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} \mid a, b, c \in \mathbb{Q}\}$

$\mathbb{Q}$, $x^3 = 5$ $\sqrt[3]{5}$, $\sqrt[3]{25}$

$\sqrt[3]{5} \in \mathbb{R}$

$\mathbb{Q}(\sqrt[3]{5})$ лин. пр-во над $\mathbb{Q}$ с базис $1, \sqrt[3]{5}, \sqrt[3]{25}$

I // F-поле и $g \in F[X]$, $\deg g \geq 1$, g - неразложим

$K = F[X]/(g(x))$. Тогава:

1) K е поле, $\exists$ подполе $F_0 < K$: $F_0 \cong K$

2) K е лин. пр-во над F, $\dim_F K = \deg(g)$

$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ - базис

3) α е корен на g ($\alpha \in K$) $\Rightarrow f$ - разложим в K

Д-во // g - неразложим, $I = (g)$

$I <_{max} F[X]$ Нека $t \notin I$

$t + I \neq 0 + I$, $(t, g) = 1$

$1 = ug + vt$, $u, v \in F[X]$

$vt = 1 - ug \in 1 + (g) = 1 + I$

$(v + I)(t + I) = 1 + I \Rightarrow (t + I)^{-1} = (v + I)$

$\Rightarrow$ всеки ненулев ел. е обратим

$\Rightarrow K = F[X]/(g)$

$F_0 = \{\alpha + I \mid \alpha \in F\}$ $F \subset F[X]$

$\varphi: F \to F_0$: $\varphi(\alpha) = \alpha + I$

φ е изоморфизъм

$\ker \varphi = \{\alpha \mid \alpha + I = I\} = \{0\}$

$\Rightarrow F \cong F_0 < K$

K и F - поле

$t, f \in F[X]$ $t + I, f + I \in K$

$(t + I) + (f + I) = (t + f) + I$

$\alpha \in F \cong F_0$

$(\alpha + I)(t + I) = \alpha t + I \in K$

F_0

K лин. пр-во над F

$K = F[X]/(g) = \{f+\bar{I} \mid f \in F[X]\} = \{r(x)+\bar{I} \mid \deg r \le n-1\}$

$t+\bar{I} = f+I \iff t-f \in \bar{I} \iff g \mid (t-f) \iff t \equiv f \pmod g$

$\iff t, f$ равни остатъци при делене на g

Ако $\deg g = n$

$K = \{r_0 + r_1 x + \dots + r_{n-1}x^{n-1} + \bar{I} \mid r_i \in F\}$

$\beta \in F$ - const

Нека $x+\bar{I} = \alpha$

$F_0 = \{\beta+\bar{I} \mid \beta \in F[X], \deg \beta \le 0\}$

$F_0 \cong F$

$r_0 + r_1 x + \dots + r_{n-1}x^{n-1} + \bar{I} = (r_0+\bar{I}) + (r_1+\bar{I})\underbrace{(x+\bar{I})}_{\alpha} + \dots + (r_{n-1}+\bar{I})(x+\bar{I})^{n-1}$

$= r_0 \cdot (1+\bar{I}) + r_1 \cdot \alpha + \dots + r_{n-1}\alpha^{n-1}$

$K \subset l(1, \alpha, \dots, \alpha^{n-1})$

Ако $\beta_0 \dots \beta_{n-1} \in F$

$\beta_0 + \beta_1\alpha + \dots + \beta_{n-1}\alpha^{n-1} = 0+\bar{I}$

$(\beta_0 + \beta_1 x + \dots + \beta_{n-1}x^{n-1}) + \bar{I} = 0+\bar{I}$

$1, \alpha, \dots, \alpha^{n-1}$ лин. независ.

$\beta_i = 0 \iff g \mid (\beta_0 + \beta_1 x + \dots + \beta_{n-1}x^{n-1})$

$\alpha = X + \overline{I}$ $\quad \overline{I} = (g)$

$F \cong F_0 < K = F[X]/(g)$

g с коэф. из F_0

$g = g_0 + g_1 X + \dots + g_n X^n \in F$, $\deg g = n$

$g = (g_0 + \overline{I}) + (g_1 + \overline{I})X + \dots + (g_n + \overline{I})X^n$

$g(\alpha) = g(X + \overline{I}) = (g_0 + \overline{I}) + (g_1 + \overline{I})(X + \overline{I}) + \dots + (g_n + \overline{I})(X + \overline{I})^n =$

$= (g_0 + \overline{I}) + (g_1 X + \overline{I}) + \dots + (g_n X^n + \overline{I}) =$

$= (g_0 + g_1 X + \dots + g_n X^n) + \overline{I} = g + \overline{I} = 0 + \overline{I}$

$\Rightarrow g(\alpha) = 0 + \overline{I} \in K$

α корень $\Rightarrow (x - \alpha) \mid g$ (в поле K)

Пр. 1

$\mathbb{C}$ лин.-пр.-во с базисом $1, i$

i

$\overline{I}$

$\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$

$(a_1 + b_1 X + \overline{I})(a_2 + b_2 X + \overline{I}) =$

$= (a_1 + b_1 X)(a_2 + b_2 X) + \overline{I}$

$= a_1 a_2 + (a_1 b_2 + a_2 b_1) X + b_1 b_2 X^2 + \overline{I}$

$(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) X + \overline{I}$

$X^2 + 1 + \overline{I} = \overline{I} \Rightarrow X^2 + \overline{I} = -1 + \overline{I}$

$i = X + \overline{I}$

$F < K$ поле (F подполе на K) (K разширение на F)

4 елемента $\mathbb{Z}_2$ $\quad 4 = 2^2$

Неразложим $\in \mathbb{Z}_2[X]$ $\quad \deg g = 2$ $\quad g = X^2 + X + \bar{1} \in \mathbb{Z}_2[X]$

$K = \mathbb{Z}_2[X]/(g)$, $\bar{I} = (g)$, $\alpha = X + \bar{I} = X + (g)$

$K = \{ \underbrace{\bar{0} + \bar{I}}_{=\bar{0}}, \underbrace{\bar{1} + \bar{I}}_{=1}, \underbrace{X + \bar{I}}_{\alpha}, \underbrace{X + \bar{1} + \bar{I}}_{X+\bar{I}+\bar{1}+\bar{I}} \} = \{ \bar{0}, \bar{1}, \alpha, \alpha + \bar{1} \}$

$F_0 \cong \mathbb{Z}_2$

Базис $\bar{1}, \alpha$

Лин. нр.-во над $\mathbb{Z}_2$

α корен на $g \in K[X] \Rightarrow \boxed{\alpha^2 + \alpha + \bar{1} = \bar{0}} \Rightarrow \alpha^2 = -(\alpha + \bar{1}) = \alpha + \bar{1}$

$\operatorname{char} \mathbb{Z}_2 = \operatorname{char} K = 2$ $\quad (\beta = -\beta, \forall \beta \in K)$

$\alpha^2 = \alpha + 1$ $\quad \alpha^3 = \alpha \cdot \alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 1$

$\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha^3 \cdot \alpha = \alpha$

$\alpha + 1 = \alpha^2$

	1	α	α^2	0
1	1	α	α^2	0
α	α	α^2	1	0
α^2	α^2	1	α	0
0	0	0	0	0

Т | F - поле, $g \in F[X]$, $\deg g \geq 1$

а) $\exists$ поле K в което g има корен

б) $\exists$ поле $T : (F \subset T)$ в което g се разлага на множители от степен 1 (в което се съдържат всички корени на g)

Д-во

а) Ако g - неразложим. $\Rightarrow$ прилагаме предишната

Ако g разложим $g = g_1 g_2 \cdots g_s$ неразлож. и прилагаме предп. за g_1

б) индукция по $\deg g$

$n = 1$ g - неразложим $g = ax + b$ $(a \neq 0)$

$g = a\left(x - \frac{-b}{a}\right) = a(x - c)$ $\quad c = -\frac{b}{a} \in F$ корен

Предполагаме ее е вярна за полином от $\deg \leq n-1$

$\deg g = n$ от $\cdot A \Rightarrow \exists K \supset F : g(\alpha) = 0$ | $\alpha \in K$ корен

$\Rightarrow (X - \alpha) \mid g(X)$ $(\text{като } \in K[X]) \Rightarrow g(X) = (X-\alpha) \cdot g_1(X)$, $\deg g_1 = n-1$

Прилагаме инд. за $g_1(X)$ ....

$g = (X - c_1)(X - c_2) \cdots (X - c_n) \cdot c_0$ $\quad \checkmark$

Опр. $g \in F[X]$, $\deg \geq 1$. Нека T е поле
- $F < T$
- в T се съдържат всички корени на g

Ако T е „минималното" поле с това свойство тогава T е поле на разлагане на g над F.

Ако U - поле, $U \subsetneq T$ и $F \subset U \subsetneq T$ (произв.)
$\Rightarrow \exists$ корен на g, който не е от U

поле на разлагане
на x^2+1 над $\mathbb{R}$ е $\mathbb{C}$

На x^2+1 над $\mathbb{Q}$ е $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$

$\mathbb{Q}[X]$ $x^3-5=g$ $\mathbb{Q}(\sqrt[3]{5})$
$x^3-5 = (x-\sqrt[3]{5})(x^2+\sqrt[3]{5}x+\sqrt[3]{25})$

Тв/ F-поле и $g \in F[X]$, $\deg g \geq 1$
$\Rightarrow$ съществува поле на разлагане на g над F.

Д-во $\exists\, T \supseteq F$, T съдържа всички корени на g

$T_0 = \bigcap L$, L : $\begin{cases} F \subset L \subset T \\ L \text{ съдържа всички корени на } g \end{cases}$

$\Rightarrow T_0$ е полето на разлагане на g над F

Т/ F-поле, $g \in F[X]$, $\deg g \geq 1$
Ако T_1 и T_2 са полета на разлагане на g над F, тогава $T_1 \cong T_2$

без док-во

I (формули на Виет) Нека $g \in F[X]$, $\deg g \geq 1$

Нека $T \supseteq F$ поле на разлагане, $\alpha_1, \dots, \alpha_n$ корени на g

$$g = g_0 X^n + g_1 X^{n-1} + \dots + g_n \quad (\deg g = n,\ g_0 \neq 0)$$

$$\alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{g_1}{g_0}$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n = \frac{g_2}{g_0}$$

$$\vdots$$

$$\sum_{i_1 < i_2 < \dots < i_k} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} = (-1)^k \frac{g_k}{g_0}$$

$$\vdots$$

$$\alpha_1\alpha_2\dots\alpha_n = (-1)^n \frac{g_n}{g_0}$$

"k" формула

$\binom{n}{k}$ събираеми

Т - поле на разлагане $(x-\alpha) \mid g(x)$

$\Rightarrow g(x) = a(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n) = g_0 x^n + g_1 x^{n-1} + \ldots + g_n$

коеф. пред	$a = g_0$
пред x^{n-1}	$a\,(-\alpha_1-\alpha_2-\ldots-\alpha_n) = g_1 \Rightarrow \alpha_1+\ldots+\alpha_n = -\frac{g_1}{g_0}$
пред x^{n-2}	$a(\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_1\alpha_n) = g_2 \Rightarrow \alpha_1\alpha_2+\ldots+\alpha_1\alpha_n = \frac{g_2}{g_0}$
$\vdots$	
пред x^{n-k}	$a(-1)^k \sum_{i_1<\ldots<i_k} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k} = g_k \Rightarrow \sum \alpha_{i_1}\ldots\alpha_{i_k} = (-1)^k \frac{g_k}{g_0}$
- - -	
св. коеф	$a(-1)^n \alpha_1\ldots\alpha_n = g_n \Rightarrow \alpha_1\ldots\alpha_n = (-1)^n \frac{g_n}{g_0}$

$ax^2+bx+c=0$

$\alpha_1+\alpha_2=-\frac{b}{a}$

$\alpha_1\alpha_2=\frac{c}{a}$

$ax^3+bx^2+cx+d=0$

$\alpha_1+\alpha_2+\alpha_3=-\frac{b}{a}$

$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=\frac{c}{a}$

$\alpha_1\alpha_2\alpha_3=-\frac{d}{a}$

$ax^4+bx^3+cx^2+dx+e=0$

$\alpha_1+\alpha_2+\alpha_3+\alpha_4=-\frac{b}{a}$

$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4=\frac{c}{a}$

$\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_3\alpha_4=-\frac{d}{a}$

$\alpha_1\alpha_2\alpha_3\alpha_4=\frac{e}{a}$