Крайни полета

$|F| < \infty$, F - поле

- $\mathrm{char}\, F \neq 0 \Rightarrow \mathrm{char}\, F = p$ - просто

Св-во K, M полета, $K < M$ $\Rightarrow M$ е лин. пр-во над K

$\dim_K M = |M : K|$ - степен на разширение

Т | F - крайно $\Rightarrow |F| = p^n$, p - просто число

$\Rightarrow \mathrm{char}\, F = p$ - просто число

F_0 - простото подполе на F: $F_0 \cong \mathbb{Z}_p$

F е лин. пр-во над $\mathbb{Z}_p \Rightarrow \dim_{\mathbb{Z}_p} F = n \Rightarrow$ в базис $e_1, \dots e_n$

$F = \{a_1 e_1 + \dots + a_n e_n \mid a_i \in \mathbb{Z}_p\}$ $\quad |F| = |\{(a_1, \dots a_n)\}| = p^n$

когато $\mathrm{char}\, T = 0$

$x1 \neq s1$ за $x \neq s$, $x, s \in$

Д-во

"+": $M \times M \to M$

$a, b \to a+b$

$\alpha \in K \subset M$, $x \in M$, $y \in M$

$\alpha x \in M$ · $1x = 1$

$(\alpha+\beta)x = \alpha x + \beta x$

$\alpha(x+y) = \alpha x + \alpha y$

$(\alpha\beta)x = \alpha(\beta x)$

Св-во // Нека F - поле, $|F| = p^n$, p - просто $\Rightarrow a^{p^n} = a$, $\forall a \in F$

Д-во $|F^*| = p^n - 1$

$a \neq 0 \Rightarrow a \in F^*$

$a^{p^n - 1} = 1$

$a^{p^n} = a$, $\forall a \neq 0$

$0^{p^n} = 0$

$GF(p^n)$

Т // Ако p е просто число и $n \in \mathbb{N}$ съществува поле с p^n елемента и това поле е единствено с точност до изоморфизъм

Д-во // (Ǝ) $f = X^{p^n} - X \in \mathbb{Z}_p[X]$ // $\Rightarrow T = L$; $|L| = p^n$

T е полето на разлагане на f над $\mathbb{Z}_p$

$L = \{ \alpha \in T \mid \alpha^{p^n} - \alpha = 0 \}$

- L поле, $\mathbb{Z}_p \subset L$

$\Rightarrow L \stackrel{!}{=} T$ - полето на разлаг.

- има ли кратни корени f?

$f' = p^n X^{p^n} - 1 = -1$ ($char F = p$)

$(f, f') = 1$ няма общи корени $\Rightarrow f$ няма кратни

L - поле

$\alpha^{p^n} = \alpha$; $\beta^{p^n} = \beta \in L \subset T$

$(\alpha - \beta)^{p^n} = \alpha - \beta \in L$

$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha \cdot \beta \in L$

$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1} \in L$

$\Rightarrow L$ е поле $\mathbb{Z}_p \subset L$

($\mathbb{Z}_p \subset \mathbb{F} \Rightarrow char \mathbb{F} = p$)

(!) K - поле, $|K| = p^n \Rightarrow \operatorname{char} K = p \Rightarrow \mathbb{Z}_p \cong F_0 \subset K$

$\Rightarrow \forall a \in K: \; a^{p^n} - a = 0 \Rightarrow$ всеки елемент от K е корен

$\Rightarrow K$ е изоморфно на полето на разлагане на $F \Rightarrow$ от единственост на полето на разлагане $\; 1X^{p^n} - X \in F_0[X] = \mathbb{Z}_p[X]$

$(G, \circ)$ Абелева група

1) Ако $|a| = k \Rightarrow |a^s| = \frac{k}{(k,s)}$

2) Ако $|a| = k, |b| = s$ и $(k,s) = 1$

$\Rightarrow |ab| = k \cdot s$

3) Ако $|a| = k$ и $|b| = s \Rightarrow$ в G има елемент от ред $[k; s]$

$k = p_1^{r_1} \cdots p_l^{r_l}$; $s = p_1^{t_1} \cdots p_l^{t_s}$

p_i - различни прости числа

$r_i \geq 0$; $t_i \geq 0$

$\left| a^{\frac{k}{p_i^{r_i}}} \right| = p_i^{r_i}$ $\quad \left| b^{\frac{s}{p_i^{t_i}}} \right| = p_i^{t_i}$

$m_i = \max\{r_i, t_i\}$

$\Rightarrow \exists \, |c_i| = p_i^{m_i} \quad i = 1, \ldots l$

$\Rightarrow |c_1 \cdot \ldots \cdot c_l| = p_1^{m_1} \cdots p_l^{m_l}$

$p_1^{m_1} \cdots p_l^{m_l} = \text{НОК}[k, s]$

Т/ F - крайно поле $\Rightarrow F^*$ е циклична група

Д-во $|F| = p^n$, $|F^*| = p^n - 1 \Rightarrow |\alpha| \mid p^n - 1$, $\forall \alpha \neq 0, \alpha \in F$

Нека $\beta \in F^*$ и β има max ред $|\beta| = m \Rightarrow \boxed{m \mid p^n - 1}$ (1)

$\Rightarrow |\alpha| \leq |\beta| = m$, $\forall \alpha \in F^*$

Допускаме, $\exists \alpha \in F^*$: $|\alpha| \nmid |\beta| \Rightarrow [|\alpha|, |\beta|] > |\beta|$

$\Rightarrow \in F^*$ $\exists \gamma$: $|\gamma| = НОК[|\alpha|, |\beta|] > m \Rightarrow$ противоречие

$\Rightarrow \forall \alpha \in F^*$: $|\alpha| \mid |\beta|$: $|\alpha| \neq m \Rightarrow \alpha^m = 1$

$\forall \alpha \in F^*$: α е корен на $x^m - 1 = 0$

$\Rightarrow |F^*| \leq m \Rightarrow \boxed{p^n - 1 \leq m}$ (2)

$\Rightarrow m = p^n - 1 \Rightarrow |\beta| = p^n - 1 = |F^*| \Rightarrow F^* = \langle \beta \rangle$

примитивен елемент в полето $GF(p^n)$ — елемент, който поражда F^* - мултипл. група

Т/ Нека F - поле, $|F| = p^n$

1) Ако $L < F$ (подполе) $\Rightarrow |L| = p^s$ и $\underline{s \mid n}$.

2) Ако $s \mid n \Rightarrow \exists$ подполе на F с p^s елемента

Д-во

1) $L \leq F$, $|L| = p^s$ ($\operatorname{char} F = \operatorname{char} L = p$) $s \leqslant n$

$L^* < F^*$ (групи), $|L^*| = p^s - 1$, $|F^*| = p^n - 1 \Rightarrow (p^s-1) \mid (p^n-1) \Rightarrow \underline{s \mid n}$

$L < F \Rightarrow F$ елем. пр-во над $L \Rightarrow \dim_L F = t$

$\Rightarrow F \tilde{=} \{(\alpha_1, \ldots, \alpha_t) \mid \alpha_i \in L\} \Rightarrow |F| = |L|^t = \left| n = st \right| \Rightarrow$

$\Rightarrow p^n = (p^s)^t \Big| \Rightarrow s \mid n$

---

2) $s \mid n \Rightarrow (p^s-1) \mid (p^n-1)$ в F^* има единствена подгрупа

$H < F^* : |H| = p^s - 1 \Rightarrow T = H \cup \{0\} = \{\alpha \mid \alpha^{p^s} = \alpha\}$

T - поле на разлагане $x^{p^s} - x$ над $T < F$

$g = x^n + a_{n-1}x^{n-1} + \dots + a_1 \in \mathbb{Z}_p[x]$ — неразложимый?

$I = (g) \Rightarrow T = \mathbb{Z}_p[x]/I$ е поле

$T = \{ r(x) + I \mid r(x) \in \mathbb{Z}_p[x] \} = \{ r_0 + r_1 x + \dots + r_{n-1}x^{n-1} + I \mid r_i \in \mathbb{Z}_p \}$

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

имат равни остатъци при деление с g

$1+I, x+I, x^2+I, \dots, x^{n-1}+I$ базис

$x + I = \alpha$

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

$T = \{ r_0 \cdot 1 + r_1\alpha + r_2\alpha^2 + \dots + r_{n-1}\alpha^{n-1} \mid r_i \in \mathbb{Z}_p \}$

$g(\alpha) = 0 = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1 \Rightarrow \alpha^n = -(a_{n-1}\alpha^{n-1} + \dots + a_1)$

- $|T| = p^n$

$\mathbb{Z}_5[x]$ $g(x) = x^3 + \bar{2}x^2 + x + \bar{3} \in \mathbb{Z}_5[x]$

неразложим $I = (g) \lhd \mathbb{Z}_5[x]$

$\mathbb{Z}_5[x]/I = T$; - T - поле

; - $|T| = 5^3 = 125$

$x + \bar{I} = \alpha$

$1, \alpha, \alpha^2$ базис на T

$T = \{ a + bx + cx^2 + \bar{I} \mid a, b, c \in \mathbb{Z}_5 \} =$

$= \{ a \cdot 1 + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_5 \}$

$\bar{2} + \bar{3}\alpha + \alpha^2 = y_1$, $y_2 = \bar{4} - 2\alpha + 3\alpha^2$

$y_1 y_2$: $(2 + 3x + x^2 + \bar{I})(4 - 2x + 3x^2 + \bar{I})$

$3x^4 + 2x^3 + 4x^2 - 2x + 3 \mid x^3 + 2x^2 + x + 3$

$3x^4 + x^3 + 3x^2 + 4x$ — $\bar{3}x + \bar{1}$

$x^3 + x^2 - x + 3$

$x^3 + 2x^2 + x + 3$

$-x^2 - 2x = r(x)$

$y_1 y_2 = 4\alpha^2 + 3\alpha$

	$\bar{1}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\mathbb{Z}_5$
$\bar{1}$	1	3	4	$\bar{2} \neq \bar{0}$	
$\bar{2}$	$\bar{1}$	4	4	$\bar{1} \neq \bar{0}$	
$\bar{3}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{1} \neq \bar{0}$	
$\bar{4}$	$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{3} \neq \bar{0}$	

Няма корен

Няма ненул. от степен 1, $\deg g = 3$

$\Rightarrow g$ - неразл.

$\Rightarrow (2 + 3x + x^2)(4 - 2x + 3x^2) \equiv ?$

$\bar{3} - \bar{4}x + x^2 + \bar{2}x - x^2 + \bar{4}x^3$

$+ \bar{4}x^2 - \bar{2}x^3 + \bar{3}x^4$

$= \bar{3} - \bar{2}x + \bar{4}x^2 + \bar{2}x^3 + \bar{3}x^4$

$g = x^3 + 2x^2 + x + 3 \in \mathbb{Z}_5[x]$

$(2\alpha^2 + 3\alpha + 4)^{-1} = \beta$

$t = \bar{2}x^2 + \bar{3}x + \bar{4}$

$(g, t) = 1$

$\bar{3} = t - r_1(\bar{3}x + \bar{3})$

$\bar{3} = t - (g - t(\bar{3}x - \bar{1}))(\bar{3}x + \bar{3})$

$\bar{3} = t(1 + (3x-1)(3x+3)) - g(3x+3)$

$\bar{3} = t(\bar{4}x^2 + x + \bar{3}) - g(\bar{3}x + \bar{3}) \mid \cdot \bar{2}$

$1 = t(\bar{3}x^2 + \bar{2}x + \bar{1}) - g(x + \bar{1})$

$(2\alpha^2 + 3\alpha + 4)^{-1} = \bar{3}\alpha^2 + \bar{2}\alpha + \bar{1}$

$x^3 + \bar{2}x^2 + \bar{3}x + \bar{3} \mid \bar{2}x^2 + \bar{3}x + \bar{4}$

$x^3 + \bar{4}x^2$

$\bar{3}x - \bar{1}$

$-\bar{2}x^2 + x + \bar{3}$

$-\bar{2}x^2 - \bar{3}x - \bar{4}$

$\bar{4}x + \bar{2}$

$g = t(3x-1) + r_1$

$\bar{2}x^2 + \bar{3}x + \bar{4} \mid \bar{4}x + \bar{2}$

$2x^2 + 1x$

$\bar{3}x + 3$

$2x + 4$

$2x + 1$

3

$\underbrace{2x^2 + 3x + 4}_{t} = \underbrace{(4x+2)}_{z}(3x+3) + 3$

$(3x-1)(3x+3) = 4x^2 + 4x - 3x - 3$

$|T| = p^n$, $T^* = \langle \beta \rangle$ β - примитивен за T

Ако g - неразложим полином, който има за корен β

$\Rightarrow g$ - примитивен полином

$T = \mathbb{Z}_p[X]/(g) = \{ r_0 + r_1\beta + \dots + r_n\beta^{n-1} \mid r_i \in \mathbb{Z}_p \}$ $\Big/$ базис $1, \beta, \dots, \beta^{n-1}$

всички елем-та $\{1, \beta, \beta^2, \dots, \beta^{p^n-2}\} = T^*$
ненулеви

Проверка за примит. полином

1) $\deg g = n$

2) g - неразложим

3) $g \nmid (X^k - 1)$, $k < p^n - 1$

Забел. $|T^*| = p^n - 1$

$\varphi(p^n-1)$ броя на примит. елем. в полето

$\frac{\varphi(p^n-1)}{n}$ броя на примитивните полиноми от ст. n над $\mathbb{Z}_p$

$GF(16) = GF(2^4)$

неразложимый над $\mathbb{Z}_2$

$\deg f = 4$

$g_1 = x^4 + x^3 + \bar{1}$ // $F = \mathbb{Z}_2[x]/(x^4 + x^3 + \bar{1})$; $\alpha = x + \bar{1}$

$1, \alpha, \alpha^2, \alpha^3$

$x^4 + x^3 + \bar{1} = g_1$

$x^4 + x + \bar{1} = g_2$

$x^4 + x^3 + x^2 + x + \bar{1} = g_3$

$g_3 \mid (x^5 - \bar{1})$

$|F| = 16 \quad |F^*| = 15$

$\alpha \in F^*: |\alpha| = \{1, 3, 5, 15\}$

g_1, g_2 примитивны

	$1\ \alpha\ \alpha^2\ \alpha^3$
1	$(\bar{1}, \bar{0}, \bar{0}, \bar{0})$
α	$(0, \bar{1}, 0, 0)$
α^2	$(0, 0, \bar{1}, 0)$
α^3	$(0, 0, 0, \bar{1})$
α^4	$1, 0, 0, 1$
α^5	$1\ 1\ 0\ 1$
α^6	$1\ 1\ 1\ 1$
α^7	$1\ 1\ 1\ 0$
α^8	$0\ 1\ 1\ 1$
α^9	$1\ 0\ 1\ 0$
α^{10}	$0\ 1\ 0\ 1$
α^{11}	$1\ 0\ 1\ 1$

$\alpha^{12}(1, 1, 0, 0)$

$\alpha^{13}(0\ 1\ 1\ 0)$

$\alpha^{14}(0\ 0\ 1\ 1)$

$\alpha^{15} = 1$

$\alpha^6 + \alpha^8 = 1$

$\alpha^4 \alpha^9 =$

α^{4+15-9}

$\frac{\alpha^4}{\alpha^9} = \alpha^{10}$

$= \alpha^{10} = (0101)$

$= \alpha + \alpha^3$

$\alpha^4 + \alpha^3 + \bar{1} = 0 \Rightarrow \alpha^4 = \alpha^3 + \bar{1}$

$\alpha^5 = \alpha^4 + \alpha = \alpha^3 + 1 + \alpha$

$\alpha^6 = \alpha^3 + 1 + \alpha + \alpha^2$

$\alpha^7 = (1 + \alpha^3) + \alpha + \alpha^2 + \alpha^3$

$\alpha^8 = \alpha + \alpha^2 + \alpha^3$

$\alpha^9 = \alpha^2 + \alpha^3 + 1 + \alpha^3$

$\alpha^{10} = \alpha^3 + \alpha$

$\alpha^{11} = 1 + \alpha^3 + \alpha^2$

$\alpha^{12} = \alpha + 1 + \alpha^3 + \alpha^3$

$\alpha^{13} = \alpha^2 + \alpha$

$\alpha^{14} = \alpha^3 + \alpha^2$

$\alpha^{15} = 1 + \alpha^3 + \alpha^3$