$f(x) = f_0 x^n + f_1 x^{n-1} + \ldots + f_n$

$\overline{f}(x) = \overline{f_0} x^n + \overline{f_1} x^{n-1} + \ldots + \overline{f_n}$

$g = f(x) \cdot \overline{f}(x) \in \mathbb{R}[x]$

$f_n \overline{f_k} + f_{n-1} \cdot \overline{f_{k+1}} + \ldots + f_k \cdot \overline{f_n}$ = КОМПЛЕКСНО СПРЕГНАТОТО СИ

$\Rightarrow \exists \alpha \in \mathbb{C} : g(\alpha) = 0 = f(\alpha) \cdot \overline{f}(\alpha)$

$\Rightarrow$ $\underbrace{f(\alpha) = 0}_{\text{корен}}$ или $\underbrace{\overline{f}(\alpha) = 0}_{(2)}$

(2) $\overline{f(\alpha)} = 0 \Rightarrow \overline{f_0 \alpha^n + \ldots + f_n} \Rightarrow \overline{f_0 \alpha^n} + \ldots + \overline{f_n} = \overline{f_0} \overline{\alpha}^n + \ldots + \overline{f_n} =$

$= f_0 \overline{\alpha}^n + \ldots + f^n = f(\overline{\alpha}) = 0 \Rightarrow \overline{\alpha}$ - корен

$\Rightarrow \alpha$ или $\overline{\alpha}$ Е КОРЕН НА $f$

---

**Сл.1** ВСИЧКИ КОРЕНИ НА ПОЛИНОМ С КОМПЛЕКСНИ КОЕФИЦИЕНТИ СА КОМПЛЕКСНИ ЧИСЛА

**Сл.2** НЕРАЗЛОЖИМИТЕ ПОЛИНОМИ НАД $\mathbb{C}$ СА САМО ПОЛИНОМИТЕ ОТ 1ВА СТЕПЕН

**Сл.3** ВСЕКИ ПОЛИНОМ СЕ РАЗЛАГА НА ЛИНЕЙНИ МНОЖИТЕЛИ — ЗА $\mathbb{R}[x]$

**Сл.4** АКО $f(x) \in \mathbb{R}[x]$, $\alpha \in \mathbb{C}$ И $f(\alpha) = 0 \Rightarrow f(\overline{\alpha}) = 0$

**Сл.5** $f(x) \in \mathbb{R}[x]$, $\alpha, \overline{\alpha}$ - КОМПЛЕКСНО-СПРЕГНАТИ КОРЕНИ $\Rightarrow$

$\Rightarrow (x-\alpha)(x+\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha\overline{\alpha}$ Е ПОЛИНОМ С $\mathbb{R}$ КОЕФИЦИЕНТИ И ДЕЛИ $f$

$x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$, $\alpha \notin \mathbb{R}$ - НЕРАЗЛОЖИМ НАД $\mathbb{R}$

**Сл.6** НЕРАЗЛОЖИМИ ПОЛИНОМИ НАД $\mathbb{R}$:

- ОТ ПЪРВА СТЕПЕН;
- ПОЛИНОМИ ОТ ВТОРИ СТЕПЕН С ОТРИЦАТЕЛНА ДИСКРИМИНАНТА

---

## Крайни полета

**D** Крайно поле - поле с краен брой елементи.

$F$ - крайно поле $|F| < \infty$

$\text{char } F = p$ - просто

$\exists!$ подполе $F_1 \subset F$ (просто): $F_1 \cong \mathbb{Z}_p \Rightarrow \mathbb{Z}_p \subset F$

($F$ е разширение на $\mathbb{Z}_p$

$F$ се разглежда като линейно пространство над $\mathbb{Z}_p$ и $F$ има краен брой елементи $\Rightarrow \dim_{\mathbb{Z}_p} F = k < \infty \Rightarrow$ има базис $e_1 \dots e_k$ на $F$ над $\mathbb{Z}_p$

$\Rightarrow \forall x \in F \rightarrow x = \alpha_1 e_1 + \dots + \alpha_k e_k \rightarrow (\alpha_1 \dots \alpha_k)$

$\Rightarrow F$ еднозначно се описва чрез $k$-орките: $F = \{\alpha_1 e_1 + \dots + \alpha_k e_k \mid \alpha_i \in \mathbb{Z}_p\}$

$\Rightarrow \forall k$-орки са $p^k \Rightarrow |F| = p^k$

$\Rightarrow$ Броят на елементите на $\forall$ крайно поле е $p^k$, $\dim F = k$, $\operatorname{char} F = p$

**Тв** Ако $F$ - крайно поле, то $\exists$ $p$ - просто и $k \in \mathbb{N}$ : $|F| = p^k$

$GF(p^k)$ - крайно поле с $(p^k)$ елемента - то е $\exists!$ с точност до изоморфизъм

**Т** За $\forall k \in \mathbb{N}$ и $p$ - просто $\exists$ поле $F$ : $|F| = p^k$

Ако $|F| = p^k \rightarrow |F^*| = p^k - 1$ - мултипликативна група (без 0)

$\alpha \in F^*$ : $m$ - min число : $\alpha^m = 1$ : $m \mid (p^k - 1)$

$\alpha^{p^k - 1} = 1 \Rightarrow \alpha$ - корен на $x^{p^k - 1} - 1 \;/\; x^{p^k} - x$

Доказателство:

Разглеждаме $g(x) = x^{p^k} - x$ над $\mathbb{Z}_p$ и нека $T$ е полето на разлагане на $g(x)$ над $\mathbb{Z}_p$.

$F_1 = \{\alpha \in T \mid \alpha^{p^k} - \alpha = 0\} \subset T$ (множество от корените на полинома)

т.е. $(\alpha^{p^k} = \alpha)$ ; $\beta^{p^k} = \beta$

От въпроса за char на поле: Ако $\operatorname{char} F = p$ и $a, b \in F$, то

$(a+b)^p = a^p + b^p \Rightarrow (a+b)^{p^s} = a^{p^s} + b^{p^s}$

$(\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k} = \alpha + \beta \Rightarrow \alpha + \beta \in F_1$

$(\alpha-\beta)^{p^k} = \alpha^{p^k} + (-\beta)^{p^k} = \alpha - \beta \in F_1$

$(\alpha\beta)^{p^k} = \alpha^{p^k} \beta^{p^k} = \alpha\beta \in F_1$

$\alpha \neq 0 \; (\alpha^{-1})^{p^k} = (\alpha^{p^k})^{-1} = \alpha^{-1} \in F_1$

$\Rightarrow F_1 < T$

Има ли кратни корени?

$g'(x) = p^k x^{p^k - 1} - 1 = -1$ в $\mathbb{Z}_p[x]$

$g$ и $g'$ нямат общ корен $\Rightarrow$ няма кратни корени $\Rightarrow$ броят на корените е $\deg g(x) = p^k \Rightarrow |F_1| = p^k \Rightarrow \exists$ поле $F_1$ : $|F_1| = p^k$

**Т** Ако $F$ крайно поле и $|F|=p^k$, то за $\forall \alpha \in F \Rightarrow \alpha^{p^k}=\alpha$

**Т** (от 17 въпрос)

$F$ - поле и $f(x) \in F[x]$ - неразложим.

$T=F[x]/(f(x))$ е поле и $F \subset T$ и $\dim_F T = \deg f(x)$

Пример: $4=2^2 \Rightarrow \dim_{\mathbb{Z}_2} F = 2 \Rightarrow \deg f(x)=2$

↳ char $\Rightarrow \mathbb{Z}_2$

$\Rightarrow$ Търсим неразложим полином $f(x)$ с коефициент от $\mathbb{Z}_2$ и $\deg f=2$

$x^2+ax+b \Rightarrow f(\bar{0})=1 \Rightarrow \bar{b}=\bar{1}$

$f(\bar{1})=\bar{1} \Rightarrow \bar{a}=\bar{1}$

↳ не $\bar{0}$, защото е неразложим

$\Rightarrow f(x)=x^2+x+1$

Идеалът $I=(x^2+x+1)=\{t(x)(x^2+x+1) \mid t(x) \in \mathbb{Z}_2[x]\}$

$r_1(x)+I=r_2(x)+I \Leftrightarrow r_1-r_2=I \Leftrightarrow f(x) \mid r_1(x)-r_2(x)$

Възможните остатъци при делене на $x^2+x+1$: $\bar{0}, \bar{1}, x, x+\bar{1}$

$T=\mathbb{Z}_2[x]/(f(x))=\{\underbrace{\bar{0}+I, \bar{1}+I}_{\mathbb{Z}_2}, x+I, x+\bar{1}+I\}$

$\alpha=x+I \Rightarrow \alpha+\bar{1}=(x+\bar{1})+(\bar{1}+I)=x+\bar{1}+I \Rightarrow T=\{\bar{0}, \bar{1}, \alpha, \alpha+\bar{1}\}$

Освен това, $\alpha^2=(x+I)^2=x^2+I \overset{+I}{=} x^2+x+1+x+1=x+1+\bar{1}=\alpha+1$

$\Rightarrow \alpha^2=\alpha+1 \Rightarrow$ можем да попълним таблиците за събиране и умножение

| $*$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
| $\alpha$ | $0$ | $\alpha$ | $\alpha+1$ | $1$ |
| $\alpha+1$ | $0$ | $\alpha+1$ | $1$ | $\alpha$ |

| $+$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
| $1$ | $1$ | $0$ | $\alpha+1$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\alpha+1$ | $0$ | $1$ |
| $\alpha+1$ | $\alpha+1$ | $\alpha$ | $1$ | $0$ |

**Т** Мултипликативната група на крайно поле е циклична.

Доказателство: $|F|=p^k$, $|F^*|=p^k-1$

Нека $\alpha$ е елементът с max ред от $F^*$, $\beta \in F^*$, $|\alpha|=m$, $|\beta|=r$

$\Rightarrow \exists$ елемент $\gamma: |\gamma|=\text{НОК}(m,r)$

но $m$ - max ред $\Rightarrow \text{НОК}(m,r) \leq m \Rightarrow r \mid m \Rightarrow$ за $\forall \beta \in F^*$: $|\beta| \mid |\alpha| \Rightarrow \beta^m=1$ за $\forall \beta \in F^* \Rightarrow$ корен на $x^m-1$

$\Rightarrow \deg(x^m-1)=m \geq p^k-1$, освен това $m=|\alpha| \Rightarrow m=p^k-1 \Rightarrow F^*=\langle \alpha \rangle$

**Т** Нека $F_1, F_2$: (char $F_1$ = char $F_2$) $|F_1| = p^k$, $|F_2| = p^s$

$F$ е подполе на $F_2 \Leftrightarrow k | s$

Пример: $GF(16)$? $16 = 2^4$

$f(x)$ - неразложим, $\deg f = 4$ над $\mathbb{Z}_2[x]$

$f = x^4 + ax^3 + bx^2 + cx + d$

$f(\bar{0}) = f(\bar{1}) = \bar{1}$ // за да няма корени

$x^4+x^3+x^2+x+1$
$x^4+x^3+1$
$x^4+x+1$
~~$x^4+x^2+1$~~

Това са неразложим полиноми без корени, тоест тези без множител от първа степен $\Rightarrow$ със сигурност в някой от тях е скрит $(x^2+x+1)^2$, Това е $x^4+x^2+1$

$\Rightarrow$ него го нахаме.

$I = (f) \rightarrow \{a + bx + cx^2 + dx^3 + I\} = F$

$\alpha = x + I$, $\alpha^2 = x^2 + I$, $\alpha^3 = x^3 + I \rightarrow \{a + b\alpha + c\alpha^2 + d\alpha^3\} = F \Rightarrow$

$\Rightarrow$ базис $1, \alpha, \alpha^2, \alpha^3$ - базис на $F$

$\alpha^4 = x^4 + I = \underbrace{x^4 + x^3 + x^2 + x + 1}_{f} + x^3 + x^2 + x + 1 + I = x^3 + x^2 + x + 1 + I =$

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

$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1 \Rightarrow \alpha^5 = 1$

Можем да напишем таблиците.

Нека по друг начин разглеждаме втория полином.

$g(x) = x^4 + x^3 + 1$

$J$

$I = \mathbb{Z}_2[x] / (g) = \{a + bx + cx^2 + dx^3 + J\}$

$\beta = x + J$

$\beta^4 = x^4 + J = x^4 + x^3 + 1 + x^3 + 1 + J = x^3 + 1 + J = \beta^3 + 1$

| | 1 | $\beta$ | $\beta^2$ | $\beta^3$ | $\beta^4$ | $\beta^5$ | $\beta^6$ | $\beta^7$ | $\beta^8$ | $\beta^9$ | $\beta^{10}$ | $\beta^{11}$ | $\beta^{12}$ | $\beta^{13}$ | $\beta^{14}$ | $\beta^{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| $\beta^1$ | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| $\beta^2$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| $\beta^3$ | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |

По-лесно представяне на крайните полета е:

$\frac{\beta^2 + \beta^7 + \beta^{11}}{\beta^3 + \beta^{12}} = \frac{\beta^8}{\beta^5} = \beta^3$

$(0\ 0\ 1\ 0) + (1\ 1\ 1\ 0) + (1\ 0\ 1\ 1) = (0\ 1\ 1\ 1)$

В криптографията често се използват крайни полета. Ползват се алгебрични методи чрез въвеждане на крайни полета