# Делимост на полиноми

F - поле, $F[X]$

Th/ $f, g \in F[X]$, $g \neq 0$

$\exists! q, r \in F[X]$ :

$f = q \cdot g + r$, $\deg r < \deg g$

в $\mathbb{Z}$

Th// $a, b \in \mathbb{Z}$, $b \neq 0$

$\exists! q, r \in \mathbb{Z}$ :

$a = bq + r$ при $0 \leq r < |b|$

Обратими в $F[X]$ тези за които $\exists t \in F^*$

$h, t \in F[X]$

$ht = 1 \Rightarrow \deg ht =$

$= \deg h + \deg t = 0 \Rightarrow$

$\deg h = \deg t = 0$

$h, t \in F^*$

Обратими елементи в $\mathbb{Z} \rightarrow \pm 1$

**Опр.** $f \mid g$, когато $\exists\, h \in F[X] : \boxed{g = f \cdot h}$ | F-поле

$\Leftrightarrow g = fq + r$ за някое $\underline{0 = r}$

**Св-ва**

1) $g \mid 0$, $\forall g \neq 0$

2) $\alpha \in F^* \ (\deg \alpha = 0) \Rightarrow \alpha \mid g$

3) $g \mid f$, $\alpha \in F^* \Rightarrow \alpha g \mid f$

4) $g \mid f$ и $f \mid h \Rightarrow g \mid h$

5) $g \mid f$ и $f \mid g \Rightarrow f = \alpha g$, $\alpha \in F^*$

6) $g \mid f \Rightarrow g \mid f \cdot t$

7) $g \mid f_1$ и $g \mid f_2 \Rightarrow g \mid (t_1 f_1 + t_2 f_2)$

8) $g \mid f$ и $f \neq 0 \Rightarrow \deg g \leq \deg f$

2) $g = \alpha \cdot (\alpha^{-1} g)$

4) $f = gt$ $h = f \cdot u = gtu$

5) $f = gt$, $g = fu$

$\Rightarrow f = (gu) f \Rightarrow \deg(gu) = 0$

$\Rightarrow \deg g = \deg u = 0$, $g, u \in F^*$

8) $g \mid f \Rightarrow f = gt$

$\deg f = \deg g + \deg t$

$\geq 0$ $\geq 0$

$\deg f \geq \deg g$

$0 = \deg 0 = -\infty$

**Опр.** $f, g \in F[X]$, поне единия $\neq 0$ | F-поле

Определяме $d \in F[X]$ е най-голям общ делител

- $d \mid f$, $d \mid g$
- Ако $d_1 \mid f$ и $d_1 \mid g$, следователно $d_1 \mid d$

---

**Св-во** // Ако съществува $HOД(f, g)$ то той не е единствен и $d_1$ и $d_2$ са $HOД(f, g)$

$\Rightarrow d_1 = \alpha d_2$, където $\alpha \in F^*$ ($\deg \alpha = 0$)

$d_1$ е НОД и $d_2$ е НОД

$d_1 \mid f$, $d_1 \mid g$ $\Rightarrow d_1 \mid d_2$ $=$

$d_2 \mid f$, $d_2 \mid g$ $\Rightarrow d_2 \mid d_1 \Rightarrow d_1 = \alpha d_2$, $\alpha \in F^*$

**Т** (Безу) F-поле, $f, g \in F[X]$ и поне един $e \neq 0$ съществува $d = НОД(f,g)$ и съществуват $u, v \in F[X]$:

F-поле

Безу

$$\boxed{d = uf + vg}$$

**Дво** $M = \{tf + qg \mid t, q \in F[X]\} \neq \emptyset \neq \{0\}$

Нека $d = uf + vg$ е ненулев от $M$ с min степен

$h \in M$: $h = d\ell + r$, $\deg r < \deg d$

$tf + qg = (uf + vg)\ell + r \Rightarrow r = \underbrace{(t - u\ell)f + (q - v\ell)g}_{\in M}$

$\Rightarrow$ от min на $\deg d \Rightarrow \deg r = -\infty$ $r = 0 \Rightarrow d \mid h$

$\Rightarrow d \mid f$ и $d \mid g$ $(f = 1f + 0g \in M;\ g = 0f + 1g)$

Ако $d_1 \mid f$ и $d_1 \mid g \Rightarrow d_1 \mid (tf + qg) \Rightarrow d_1 \mid$ всеки полином от $M$

$\Rightarrow d_1 \mid d \Rightarrow d \in НОД(f,g)$

# Алгоритъм на Евклид

1) $f = g q_1 + r_1$, $\deg r_1 < \deg g$

$(f,g) = \alpha (g, r_1)$, $\alpha \in F^*$

$r_1 = 0$ ? да → край $d = g$

не → $r_1 \neq 0$ → (2)

2) $g = r_1 q_2 + r_2$, $\deg r_2 < \deg r_1$

$(g, r_1) = (r_1, r_2)$

$r_2 \stackrel{?}{=} 0$ → да $r_1 = d$

→ не (3)

3) $r_1 = r_2 q_3 + r_3$ $\deg r_3 < \deg r_1$

$f \neq 0, g \neq 0$

$d = (f,g)$ и $d_1 = (g, r_1)$

$\Rightarrow d \mid f, d \mid g \Rightarrow d \mid r_1 \Rightarrow d \mid d_1$

$d_1 \mid g, d_1 \mid r_1 \Rightarrow d_1 \mid \underbrace{g q_1 + r_1}_{f} \Rightarrow d_1 \mid d$

$\Rightarrow d = \alpha d_1$, $\alpha \in F^*$

$\deg g > \deg r_1 > \deg r_2 > \dots$

краен брой са възможните степени

F-поле

Тв // Всеки идеал в $F[X]$ е главен.

Д=бо $I \lhd F[X]$

1сл. $I = \{0\} \Rightarrow I = (0)$

2сл. $I \neq \{0\}$ Нека $d$ е ненулев полином от $I$ с най-малка степен

Нека $f \in I$ : $f = dq + r$, $\deg r < \deg d$

$\Rightarrow r = \underbrace{f}_{\in I} - \underbrace{dq}_{\in I} \in I \Rightarrow r = 0 \Rightarrow d \mid f \quad \forall f \in I$

$f \in (d)$

$\Rightarrow I \subset (d)$

Но $d \in I \Rightarrow dq \in I \Rightarrow (d) \subset I$

$\Rightarrow I = (d)$

$d = НОД(f,g)$ $M = (f) + (g) = (d)$

$M = \{ft + gh \mid t,h \in F[X]\} \lhd F[X]$

F-поле

Ако $\mathbb{Z}[X]$

$(3)+(X) = \{3b_0 + a_1X + \dots + a_nX^n$

не е главен $НОД(3,X)$

**Опр.** $f, g \in F[X]$, $f, g$ - взаимно прости, когато $1 = НОД(f,g)$ | $F$ - поле

**Тв.** // $f, g \in F[X]$, $(f,g) = 1$

а) ако $f \mid gh \Rightarrow f \mid h$ и б) $f \mid h$ и $g \mid h \Rightarrow (fg) \mid h$

**Д-во** // $(f,g) = 1 \Rightarrow \exists u, v \in F[X]$: $1 = uf + vg$

$h = ufh + vgh$, $f \mid$

$\Rightarrow f \mid h$

$f \mid h \Rightarrow h = f \cdot q$

$g \mid h \Rightarrow g \mid fq \overset{\text{от а)}}{\Rightarrow} g \mid q \Rightarrow q = gt$

$\Rightarrow h = f \cdot q = f \cdot gt \Rightarrow gf \mid h$

**Заб** $(f,g) \cdot [f,g] = f \cdot g$

**Опр.** Най-малко общо кратно $f, g$ е $m \in F[X]$: 1) $f \mid m$ и $g \mid m$ $[f,g] = m$

ако $f \mid t$ и $g \mid t \Rightarrow m \mid t$ V

F-поле

**Опр.** $f, g, h \in F[x]$ $(h \neq 0)$

$f \equiv g \pmod h$, когато $h \mid (f-g) \Leftrightarrow$ $f, g$ дават равни остатъци при деление на $h$

**Св-ва**

1) $f \equiv f \pmod h$

2) Ако $f \equiv g \pmod h \Rightarrow g \equiv f \pmod h$

"$\equiv$" релация "на еквивалентност"

3) $f \equiv g \pmod h$ и $g \equiv t \pmod h \Rightarrow f \equiv t \pmod h$

$h \mid (f-g)$ и $h \mid (g-t) \Rightarrow h \mid (f-g+g-t) \Rightarrow h \mid (f-t) \Rightarrow f \equiv t \pmod h$

Ако $f \equiv f_1 \pmod h$
$g \equiv g_1 \pmod h$ $\Rightarrow$

4) $f \pm t \equiv f_1 \pm t \pmod h$

5) $f \pm g \equiv f_1 \pm g_1 \pmod h$

6) $ft \equiv f_1 t \pmod h$

7) $fg \equiv f_1 g_1 \pmod h$

8) $f^k \equiv f_1^k \pmod{} \; k \in \mathbb{N}$

$(f+g)-(f_1+g_1)=(f-f_1)+(g-g_1)$ ($h \mid$, $h \mid$)

$ft - f_1 t = (f-f_1)t$

(I) $fg - f_1 g_1 =$

$= fg - f_1 g + f_1 g - f_1 g_1 =$

$= (f-f_1)g + f_1(g-g_1)$ ($h \mid$, $h \mid$)

$F = \mathbb{Z}_2$, $g = x^4 + x^3 + \bar{1} \in \mathbb{Z}_2[x]$

$x^{10} \equiv t \pmod{g}$

$t$ - min ciężar

$x^{10} - t = g \cdot q \quad x^{10} = gq + t$

$\mathbb{Z}_2$: $\bar{-1} = \bar{1}$

$x^{10} : (x^4 + x^3 + \bar{1}) = x^6 + x^5 + x^4 + x^3 + x$

$x^{10} + x^9 + x^6$

$x^9 + x^6$

$x^9 + x^8 + x^5$

$x^8 + x^6 + x^5$

$x^8 + x^7 + x^4$

$x^7 + x^6 + x^5 + x^4$

$x^7 + x^6 + x^3$

$x^5 + x^4 + x^3$

$x^5 + x^4 + x$

$x^3 + x$

$x^{10} \equiv x^3 + x \pmod{g}$

$g = x^4 + x^3 + \bar{1} \in \mathbb{Z}_2[x]$ $\quad h \in \mathbb{Z}_2[x]$ ?

$(\underbrace{x^7 + x^2 + \bar{1}}_{f}) \cdot h \equiv 1 \pmod{g} \Rightarrow 1 = fh + gt$ $\quad \boxed{\text{NWD}(f,g) = 1}$

$x^7 + x^2 + 1 \;\big|\; x^4 + x^3 + \bar{1}$

$x^7 + x^6 + x^3 \qquad x^3 + x^2 + x + \bar{1}$

$x^6 + x^3 + x^2 + 1$

$x^6 + x^5 + x^2$

$x^5 + x^3 + 1$

$x^5 + x^4 + x$

$x^4 + x^3 + x + 1$

$x^4 + x^3 \quad + 1$

$x$

$f = g \cdot \underbrace{(x^3 + x^2 + x + 1)}_{q} + \underbrace{x}_{r}$

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

$x^4 + x^3 + \bar{1} \;\big|\; x$

$1 = g + (x^3 + x^2)/x = g + (x^3 + x^2) \cdot (f + g \cdot q)$

$= \underbrace{(x^3 + x^2)}_{h} f + g \underbrace{(1 + (x^3 + x^2)\,q)}_{t}$

$h \equiv x^3 + x^2 \pmod{x^4 + x^3 + 1}$

**Опр.** // $K$ - комутативен пр. с 1 и без делители на 0

$f \in K[X]$, $\deg f \geq 1$

$f$ е **неразложим над $K$**, ако не може да се представи като произведение на два полинома с по-ниски степени

Ако $f = g \cdot h \Rightarrow \deg g = \deg f$ или $\deg h = \deg f$ $\Leftrightarrow \deg g = 0$ или $\deg h = 0$

$\deg f = \deg g + \deg h$

**Пример** // Всички полиноми с $\deg = 1$ са неразложими.

**Пр**// $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$x^2+1$ неразложим над $\mathbb{R}$

$x^2+1$ разложим над $\mathbb{C}$ $\quad x^2+1 = (x+i)(x-i)$

$x^3 - 5 \in \mathbb{Q}[X]$ неразлож.

$x^3 - 5 \in \mathbb{R}[X]$ $\quad \left(x - \sqrt[3]{5}\right)\left(x^2 + \sqrt[3]{5}x + \sqrt[3]{25}\right)$

$x^2 + x + \bar{1} \in \mathbb{Z}_2[X]$

$x^2 + x + \bar{1} = x(x+\bar{1}) + \bar{1}$.

Всички полиноми от 1 ви ст. са $x$, $x+\bar{1}$

над $\mathbb{Z}_2$

**Св-во 1** Нека $g$ - неразложим $h \in F[X]$

$$(g,h) = \begin{cases} \stackrel{\sim}{1}, & \text{когато } g \nmid h \\ g, & \text{когато } g \mid h \end{cases}$$

**Св-во 2** $g$ неразложим $F$-поле

$f_1, f_2 \in F[X]$

$\Rightarrow$ Ако $g \mid f_1 f_2 \Rightarrow g \mid f_1$ или $g \mid f_2$

**Д-во** Ако $g \nmid f_1 \Rightarrow (g, f_1) = 1$

$\Rightarrow$ от $g \mid f_1 f_2 \Rightarrow g \mid f_2$

**Св-во 3** $g$ - неразложим

$g \mid fh$ и $g \nmid f \Rightarrow g \mid h$ ✓

**I** Нека $F$ - поле, $g$ - неразложим и $g \nmid h$ $g, h \in F[X]$

сравнението $h \cdot u \equiv 1 \pmod g$ има реш. $u \in F[X]$

**Д-во** // $g$ - неразложим и $g \nmid h \Rightarrow (g,h) = 1$

(безу) $uh + vg = 1 \Rightarrow g \mid (uh - 1) \Rightarrow uh \equiv 1 (g)$

Нека $f = g_1 \cdots g_k$ ; $f = t_1 \cdots t_s$ — неразложими

$g_k \mid t_1 \cdots t_s \Rightarrow g_k$ дели поне едно от $t_1, \ldots, t_s$

Преномерираме $g_k \mid t_s \Rightarrow$ но $t_s$ - неразлож.

$t_s = \alpha_k g_k$ $(\deg t_s = \deg g_k)$ $\alpha_k \in F^*$ $(\deg \alpha_k = 0)$

$g_1 \cdots g_{k-1} \cdot g_k = t_1 \cdots t_{s-1} \cdot \alpha_k \cdot g_k$

$g_1 \cdots g_{k-1} = t_1 \cdots t_{s-1} \underbrace{\alpha_k}_{ст=0}$ Ако $k \leq s$

Продължавам се $! = t_1 \cdots t_{s-k} \alpha_k \alpha_{k-1} \cdots \alpha_1$

Не е възможно $s-k \geq 1$ | степента от лявата страна е 0 от дясната $\geq 1$

$\Rightarrow s = k$

$1 = \alpha_k \alpha_{k-1} \cdots \alpha_1$

$Z_2[x]$ Неразложимые полиномы

$Z_2 = \{\bar{0}, \bar{1}\}$

① $x$, $x+\bar{1}$

② $f = x^2 + ax + b$ — неразложим

$x \nmid f \Rightarrow b = \bar{1}$

$x^2+\bar{1}$ разложим

$x+\bar{1} \nmid f$ $(x+\bar{1})^2 = x^2 + \bar{1}$

$x^2+x+\bar{1}$

Неразложим е $\boxed{x^2+x+\bar{1}}$

③ $f = x^3 + ax^2 + bx + c$

$x \nmid f \Rightarrow c = \bar{1}$

$x+1 \nmid f$

$x+1 = x-1$

| | $\bar{1}$ | $a$ | $b$ | $\bar{1}$ |
|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{1}+a$ | $\bar{1}+a+b$ | $a+b$ |

$\Rightarrow a+b \neq 0$

$a+b = \bar{1}$

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

$x^3+x+\bar{1}$

Неразложимые

④ $f = x^4 + ax^3 + bx^2 + cx + d$

$x \nmid f \Rightarrow d \neq \bar{0} \Rightarrow d = \bar{1}$

| | $\bar{1}$ | $a$ | $b$ | $c$ | $\bar{1}$ |
|---|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{1}+a$ | $\bar{1}+a+b$ | $\bar{1}+a+b+c$ | $a+b+c \neq \bar{0}$ |

$x-1 \nmid f$ $a+b+c = \bar{1}$

$(x^2+x+\bar{1})^2 \neq f$

$x^4+x^2+\bar{1} \neq f$

| $a$ | $b$ | $c$ | |
|---|---|---|---|
| $\bar{1}$ | $\bar{0}$ | $\bar{0}$ | $f_1 = x^4 + x^3 + \bar{1}$ |
| $\bar{0}$ | $\bar{1}$ | $\bar{0}$ | $f_2 = x^4 + x^2 + \bar{1}$ разлож |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $f_3 = x^4 + x + \bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{1}$ | $f_4 = x^4 + x^3 + x^2 + x + \bar{1}$ |