Делимост при полиноми

Опр. Нека F - поле, $f, g \in F[X]$, $g \neq 0$

$g \mid f$, когато $\exists\, q \in F[X] : f = q \cdot g$

(т. е. когато g и разделим - остатъкът = 0)

Св-ва

1) $g \mid 0$, $\forall g \neq 0$ $\quad (0 = g \cdot 0)$

2) Ако $\deg \alpha = 0$ (т. е. $\alpha \in (F[X])^*$) тогава $\alpha \mid f$, $\forall f \in F[X]$: $\left(f = \alpha \cdot (\alpha^{-1} f)\right)$

3) Ако $g \mid f$ и $\alpha \in (F[X])^*$ (т. е. $\deg \alpha = 0$)

$\Rightarrow \alpha g \mid f$ $\quad (f = q \cdot g \Rightarrow f = \alpha g (\alpha^{-1} q))$

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

$(h = f \cdot q_1,\ f = g q_2 \Rightarrow h = g(q_1 q_2))$

F - поле

$F[X]$

Th (деление с остатък)

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

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

$f = q \cdot g + r$

и $\deg r < \deg g$

Тв F - поле

Обратимите елементи в $F[X]$ са $f \in F[X]$ за които $\deg f = 0$

Св-ва

5) ако $g \mid f \Rightarrow g \mid f \cdot u$, $\forall u \in F[X]$

$(f = g \cdot q \Rightarrow fu = g \cdot (qu))$

6) $g \mid f_1$ и $g \mid f_2 \Rightarrow g \mid (u_1 f_1 + u_2 f_2)$

$(f_1 = g q_1;\ f_2 = g q_2 \Rightarrow u_1 f_1 + u_2 f_2 = g q_1 u_1 + g q_2 u_2 = g(q_1 u_1 + q_2 u_2))$

7) ако $g \mid f$ и $f \mid g \Rightarrow \exists \alpha \in (F[X])^* : f = \alpha g$

$g \mid f \Rightarrow \exists q_1 : f = g q_1$

$f \mid g \Rightarrow \exists q_2 : g = f q_2$

$\deg \alpha = 0$

$f = f(q_1 q_2) \Rightarrow \deg f = \deg f + \deg(q_1 q_2)$

$\Rightarrow \deg(q_1 q_2) = 0 \Rightarrow \deg q_1 = \deg q_2 = 0$

$\Rightarrow q_1, q_2 \in (F[X])^* \Rightarrow q_1 = \alpha$

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

от $g \mid f \Rightarrow f = g \cdot q \Rightarrow \underbrace{\deg f}_{\neq -\infty} = \underbrace{\deg g}_{\geq 0} + \underbrace{\deg q}_{\geq 0} \Rightarrow \deg f \geq \deg g$

Опр. | F - поле, $f, g \in F[x]$ и поне едното полином $\neq 0$

$d \in F[x]$ е НОД на f, g, когато

1) $d \mid f$ и $d \mid g$

2) Ако $d_1 \in F[x]$ такъв че $d_1 \mid f$ и $d_1 \mid g$, тогава е изпълнено че $d_1 \mid d$

НОД(f, g) | не е единствен

Ако d и p е НОД

$\Rightarrow p \mid f$ и $p \mid g \Rightarrow p \mid d$ $\Rightarrow \exists \alpha \in (F[x])^*$ (т.е. $\deg \alpha = 0$)

$d \mid f$ и $d \mid g \Rightarrow d \mid p$ $\quad d = \alpha p$

Св-во НОД$(f, 0) = \alpha f$, $\deg \alpha = 0$

Т (Безу) Нека F е поле и $f, g \in F[X]$ и $\{f \neq 0$ или $g \neq 0$. Тогава съществува d - НОД на f и g и съществуват $u, v \in F[X]$, такива, че

$$d = \text{НОД}(f,g) = uf + vg = (f,g)$$

Д-во

$M = \{tf + qg \mid t, q \in F[X]\}$, $M \neq \{0\}$ за упр. Доказвате $M \trianglelefteq F[X]$

Нека d е ненулев от M, който има най-малка степен

$\Rightarrow d = uf + vg$ $(u, v \in F[X])$

$\forall l \in M$; $l = t_1 f + q_1 g$

$\Rightarrow \exists p, r \in F[X]$: $l = p \cdot d + r$ и $\deg r < \deg d$

$\Rightarrow r = (t_1 f + q_1 g) - p(uf + vg) = (t_1 - pu)f + (q_1 - pv)g$

$\Rightarrow r \in M$ и $\deg r < \deg d \Rightarrow r = 0 \Rightarrow d \mid l$ $(\forall l \in M)$

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

Ако $d_1 \mid f$ и $d_1 \mid g$ $\Rightarrow d_1 \mid (uf+vg) \Rightarrow d_1 \mid d$

$\Rightarrow d = \text{НОД}(f,g) = uf+vg$

$M = \{fp+gq \mid p, q \in F[x]\}$

$M = (f)+(g) = (f,g)$

Забел. В th Безу е зачетн. коеф. на полиномите да бъдат от поле F.

Ако разгл. $A[x]$ (A - област на цялост)

Тогава не всеки два полинома имат НОД

Пример $\mathbb{Z}[x]$

$f = 5$

$g = x$

$d \mid 5 \Rightarrow d = \pm 1$ или ± 5

Ако $d \mid 5$ $\Rightarrow$ $d \mid$ ст. коеф. на d

Ако $d \mid x$ ст. коеф. на $d \mid$ ст. коеф. на x

$d = \pm 1$

$d = \pm x$

$\Rightarrow d = \pm 1$

$M = \{5p + q \cdot x \mid p, q \in \mathbb{Z}[x]\} \lhd \mathbb{Z}[x]$

$M = (5)+(x)$ и този идеал не е главен

F-поле $f, g \in F[x]$ $f, g \neq 0$

Алгоритъм на Евклид

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

$(f, g) = (g, r_1)$

– ако $r_1 \neq 0$ → ст. 2

$r_1 = 0$ → край $g = \text{НОД}(f, g)$

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

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

Ако $r_2 = 0$ → край $d = r_1$

Ако $r_2 \neq 0$ → ст. 3

~ ~ - - `

Краен е алгоритъм!

$\deg g > \deg r_1 > \deg r_2 > \dots$ краен б. възможни стъпки

Св-во $t, m \in F[x]$

$t = qm + r$, $\deg r < \deg m$

$\Rightarrow \text{НОД}(t, m) = \text{НОД}(m, r)$

Д-во // Ако $d = (t, m)$

$d_1 = (m, r)$

$d \mid t$, $d \mid m \Rightarrow d \mid (t - qm) = r$

$\Rightarrow d \mid d_1$

$d_1 \mid m$, $d_1 \mid r$ $\Rightarrow d_1 \mid (qm + r) = t$

$\Rightarrow d_1 \mid t$, $d_1 \mid m \Rightarrow d_1 \mid d$

$\Rightarrow d_1 = d$

F - поле $F[X]$

Опр. $f, g \in F[X]$

общо кратно: $m \in F[X]$

$f \mid m$ и $g \mid m$

$\text{нок}(f,g) = [f,g]$

ако $f \mid m_1$ и $g \mid m_1 \Rightarrow m \mid m_1$

НОК не е единствено

Т-ма $f \neq 0,\ g \neq 0$

$[f,g] = \frac{fg}{(f,g)}$

$f, g \in F[X]$

нод $d = (f,g)$

$d \mid f \Rightarrow f = f_1 d$

$d \mid g \Rightarrow g = g_1 d$

$f \mid m \Rightarrow m = fq = f_1 d q$

$g \mid m \Rightarrow g_1 d \mid f_1 d q$

$\Rightarrow$

$g_1 \mid f_1 q \Rightarrow g_1 \mid q \Rightarrow m = f_1 d g_1 q_1$

$\frac{fg}{(f,g)} = f_1 g_1 d$

$m = [f,g] \Rightarrow m \mid f_1 g_1 d$

$f \mid f_1 g_1 d$

$g \mid f_1 g_1 d$

Деф $f, g \in F[x]$ f, g - взаимно прости
$d = (f, g) = 1$ (т.е. $\deg(f, g) = 0$)

Тв Ако $f, g \in F[x]$ и $(f, g) = 1$
а) ако $f \mid gh \Rightarrow f \mid h$
б) ако $f \mid h$ и $g \mid h \Rightarrow fg \mid h$

Д-во
а) $(f, g) = 1 \Rightarrow 1 = uf + vg$ $u, v \in F[x]$
$h = \underbrace{ufh}_{f \mid} + \underbrace{vgh}_{f \mid} \Rightarrow f \mid h$

б) $f \mid h \Rightarrow h = f \cdot q$
$g \mid h \Rightarrow g \mid fq \Rightarrow g \mid q \Rightarrow q = gt \Rightarrow h = fgt$
$\Rightarrow (fg) \mid h$

I/ Нека F — поле. Всеки идеал на $F[X]$ е главен.

Д-во Нека $I \lhd F[X]$

I сл. $I = \{0\} = (0)$

II сл. $I \neq \{0\} \Rightarrow$ Нека $d \in I$, $d \neq 0$ и d е от най-нисък степен от I

$d \in I \Rightarrow (d) \subset I$ *

Дко $f \in I$ произволен $f = dq + r$, $\deg r < \deg d$

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

$\Rightarrow f \in (d) \Rightarrow I \subset (d)$ *

Т.е. $I = (d)$

Нод $(f, g) = d$ $\boxed{(f) + (g) = (d)}$

Опр. $f, g, h \in F[x]$ (F – поле)

$f \equiv g \pmod h$, когато $h \mid (f-g)$

---

① $f \equiv g \pmod h \iff$ когато f, g дават равни остатъци при деление на h

② $f \equiv f \ (h)$

③ $f \equiv g \ (h) \Rightarrow g \equiv f \ (h)$

④ $f \equiv g \ (h)$ и $g \equiv t \ (h) \Rightarrow f \equiv t \ (h)$

$h \mid (f-g)$

$h \mid (g-t)$

$\Downarrow$

$h \mid (f-g)+(g-t)$

$h \mid (f-t)$

„$\equiv$" $\pmod h$ е релация на еквивалентност

Св-ва F-поле, $F[x]$

$\left.\begin{array}{l} f \equiv f_1 \pmod h \\ g \equiv g_1 \pmod h \end{array}\right\} \Rightarrow$

① $f \pm t \equiv f_1 \pm t \pmod h$

② $f \pm g \equiv f_1 \pm g_1 \pmod h$

③ $ft \equiv f_1 t \pmod h$

④ $fg \equiv f_1 g_1 \pmod h$

⑤ $f^s \equiv f_1^s \pmod h$ $s \in \mathbb{N}$

② $(f+g)-(f_1+g_1) =$

$= \underbrace{(f-f_1)}_{h} + \underbrace{(g-g_1)}_{h} \Rightarrow h \mid (f+g)-(f_1+g_1)$

④ $fg - f_1 g_1 = \underline{fg - f_1 g} + \underline{f_1 g - f_1 g_1} = \underbrace{(f-f_1)}_{h} g + f_1 \underbrace{(g-g_1)}_{h}$

$\Rightarrow h \mid (fg - f_1 g_1)$

⑤ следует из ④ $\quad f^s - f_1^s = (f-f_1)\left(\sum_{i=0}^{s-1} f^i f_1^{s-i}\right)$

зад $\mathbb{Z}_2[X]$ $f = x^4 + x^3 + 1 \in \mathbb{Z}_2[X]$

g - min степен : $x^{10} \equiv g \pmod f$

$$
\begin{array}{r}
+\,x^{10} \\
x^{10} + x^9 + x^6 \\
\hline
x^9 + x^6 \\
+\,x^9 + x^8 + x^5 \\
\hline
x^8 + x^6 + x^5 \\
x^8 + x^7 + x^4 \\
\hline
x^7 + x^6 + x^5 + x^4 \\
x^3 + x^6 + x^3 \\
\hline
x^5 + x^4 + x^3 \\
x^5 + x^4 + x \\
\hline
x^3 + x
\end{array}
\qquad
\begin{array}{l|l}
x^4 + x^3 + 1 & \\
\hline
x^6 + x^5 + x^4 + x^3 + x &
\end{array}
$$

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

$\mathbb{Z}_2[x]$ $f = x^4 + x^3 + \bar{1}$

Търсим се $h \in \mathbb{Z}_2[x]$

$(x^7 + x^2 + \bar{1}) \cdot h \equiv \bar{1} \pmod f$

g

① Търсим $HOД(f, x^7 + x^2 + 1)$

$x^7 + x^2 + 1 \quad | \; x^4 + x^3 + 1$

$x^7 + x^6 + x^3 \quad \overline{x^3 + x^2 + x + 1}$

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

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

$x^5 + x^3 + 1$

$x^5 + x^4 + x$

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

$x^4 + x^3 + 1$

x

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

$f = x(x^3 + x^2) + 1$

$x = 1 \cdot x + 0$

$\Rightarrow HOД(f, g) = 1$

$1 = f + x(x^3 + x^2) =$

$= f + (g + f(x^3 + x^2 + x + 1))(x^3 + x^2) =$

x

$1 = f + g(x^3 + x^2) + f(x^3 + x^2 + x + 1)(x^3 + x^2)$

$g(x^3 + x^2) \equiv \bar{1} \pmod f$

$h \equiv x^3 + x^2$