(15) Делимост при полиномите над поле, най-голям общ делител. Неразложими полиноми над поле. Разлагане на полином на неразложими множители.

Нека $f, g \in F[x]$, F - поле

Деф.: Казваме, че полином $g \neq 0$ дели полином f и означаваме с $g \mid f$, ако $\exists h \in F[x]: f = gh$. В противен случай $g \nmid f$.

Свойства:

① $af \mid bf$, $a \neq 0, a, b \in F$, $f \neq 0$

② $g \mid f \Rightarrow ag \mid bf$, $a \in F^*$, $b \in F$

③ $f \mid g, g \mid f \Rightarrow f = ag$, $a \in F^*$, където $F^* = F \setminus \{0\}$

④ $f \mid g, g \mid h \Rightarrow f \mid h$

⑤ $f \mid g_i, i = \overline{1,k} \Rightarrow f \mid g_1h_1 + g_2h_2 + \ldots + g_kh_k$

⑥ $f \mid g_1 + g_2, f \mid g_1 \Rightarrow f \mid g_2$

Деф: Нека $f, g \in F[x]$, $g \neq 0$. Казваме, че полином $d = НОД(f, g) = (f, g)$, ако d изпълнява следните две условия:

1) $d \mid f$, $d \mid g$

2) $d_1 \mid f$, $d_1 \mid g \Rightarrow d_1 \mid d$

Забележка: $d = (f, g) \Rightarrow ad = (f, g)$, $a \in F^*$

ТВ Нека $f, g \in F[x]$, $g \neq 0$. Тогава $\exists d = (f, g) \in F[x]$.

Доказателство:

$F[x]$, $I = (f, g) = \{uf + vg \mid u, v \in F[x]\} \trianglelefteq F[x]$. По

Твърдение от [14] $\Rightarrow I = (d) \trianglelefteq F[x]$ и ще покажем, че $d = (f, g)$.

$d = uf + vg \in I$ (тъждество на Безу)

1) $d \mid f$, $f \in I = (d) \Rightarrow f = df_1 \Rightarrow d \mid f$

$d \mid g$, $g \in I = (d) = g = dg_1 \Rightarrow d \mid g$

2) $\left.\begin{matrix} d_1 \mid f \\ d_1 \mid g \end{matrix}\right\} \Rightarrow d_1 \mid uf + vg \Rightarrow d_1 \mid d = uf + vg$

$\Rightarrow d = НОД(f, g)$

Алгоритъм на Евклид: $f, g \in F[x]$, $g \neq 0$

$f = gq + r$, $\deg r < \deg g$

Ако $r = 0 \Rightarrow (f, g) = g$

Ако $r \neq 0$

$g = rq_1 + r_1$

$r = r_1 q_2 + r_2$

$\cdots$

$r_{i-1} = r_i q_{i+1} + \underbrace{r_{i+1}}_{=0}$

$\Rightarrow r_i = ad$, $d = (f, g)$, a - константа $\in F^*$

<u>Деф:</u> $f_1, f_2, \ldots, f_k \in F[x]$

$(f_1, \ldots, f_k) := ((f_1, \ldots, f_{k-1}), f_k)$

<u>Деф.</u> $(f, g) = 1$ $(= a) \Rightarrow f, g$ са взаимно прости

Забележка: $(f, g) = 1 \Leftrightarrow \exists!\, u, v \in F[x] : uf + vg = 1$

Тв. Ако $\left.\begin{matrix} f \mid g_1 g_2 \\ (f,g)=1 \end{matrix}\right\} \Rightarrow f \mid g_2$.

Тв. Ако $\left.\begin{matrix} g_1 \mid f \\ g_2 \mid f \\ (g_1,g_2)=1 \end{matrix}\right\} \Rightarrow g_1 g_2 \mid f$

Деф.: НОК

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

Казваме, че $m = [f,g] = \text{НОК}(f,g)$, ако изпълнява следните две условия:

1) $f \mid m$, $g \mid m$

2) $f \mid m_1, g \mid m_1 \Rightarrow m \mid m_1$

Тв. $f,g \in F[x], f \neq 0, g \neq 0 \Rightarrow (f,g)[f,g] = afg, a \in F^*$

10.05.2016

Деф.: Нека $f \in F[x], \deg f \geq 1$

f е неразложим над полето F, ако не може да се представи като произведение на два полинома от по-ниска степен. В противен случай, f е разложим.

Т.е. ако $f = gh \Rightarrow \deg g = \deg f$ или ~~$\deg h = \deg f$~~

Свойство: Ако f е неразложим $\Rightarrow$ делителите на f са αf; α, $\alpha \in F^* = F \setminus \{0\}$

Пример: • x^2+1 е неразложим над $\mathbb{R}$, но разложим над $\mathbb{C}$

• x^2-2 е неразложим над $\mathbb{Q}$, но разложим

над $\mathbb{R}$

Свойство: Нека g е неразложим полином над F

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

Свойство: Всички полиноми с $\deg = 1 \to$ неразложими

Th|| Нека F е поле.

Всеки полином от степен по-голяма или равна на 1, може да се представи като произведение на неразложими полиноми и това представяне е единствено в следния смисъл:

ако $f = g_1 \cdot \ldots \cdot g_t = h_1 \cdot \ldots \cdot h_s$, където g_i, h_j са неразложими, то $t = s$, $\exists$ пермутация на $h_1 \ldots h_s \to$

$\to h_1' \ldots h_s'$, $g_i = \alpha_i h_i$, $\alpha \in F^*$, $\alpha_1 \cdot \alpha_2 \ldots \alpha_s = 1$

Доказателство: ($\exists$ индукция по $\deg f$)

база: $\deg f = 1 \Rightarrow f$ - неразложим (ОК)

~~инд. стъпка~~ ИП: Нека е в сила за всеки полином от $\deg f < n$

инд. стъпка: Нека $\deg f = n$

- ако f е неразложим $\Rightarrow$ ОК
- ако f не е неразложим (т.е. е разложим)

$\Rightarrow \exists g, h: f = g \cdot h$, $\deg g < \deg f$, $\deg h < \deg f$

по инд. предположение (ИП) за g и h:

$\exists\, g_1, \dots, g_s : g = g_1, \dots, g_s$, g_i – неразл.

$\exists\, h_1, \dots, h_t : h = h_1, \dots, h_t$, h_j – неразл.

$f = g_1 \dots g_s h_1 \dots h_t$

(!) Нека $\left.\begin{matrix} f = g_1 \dots g_t \\ f = h_1 \dots h_s \end{matrix}\right\} g_i, h_i$ неразл.

$g_1 \dots g_t = h_1 \dots h_s$

$g_1 \mid h_1 \dots h_s$

$\Rightarrow (g_1, h_i) = \begin{cases} 1, & g_1 \nmid h_i \\ g_1, & g_1 \mid h_i \end{cases}$

Ако допуснем, че $(g_1, h_i) = 1$, $\forall i = 1, \dots, s$.

$\Rightarrow g_1 \nmid h_1 \dots h_s$ (↯)

$\Rightarrow \exists h_j : g_1 \mid h_j$, пренареждане: $h_j = h_1'$

$g_1 \mid h_1'$, но и h_1' е неразл.

$\Rightarrow h_1' = \alpha_1 \cdot g_1$, $\alpha_1 \in F^*$

$g_1 g_2 \dots g_t = \underbrace{h_1' h_2'}_{\alpha_1 g_1} \dots h_s'$

$\Downarrow$

$g_2 \dots g_t = \alpha_1 h_2' \dots h_s'$

Не е възможно $s \neq t$, защото от едната страна биха останали само полиноми, а от другата само константи, което не е възможно $\Rightarrow s = t$

$$g_i = \alpha_i h_i$$

$$\vdots$$

$$1 = \alpha_1 \dots \alpha_t$$

Аналог на Th. за представяне на числа като произведение на прости числа.