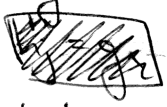
Ако допуснем, че $(g_1, h_i) = 1$, $\forall i \Rightarrow g_1 \nmid h_1 \dots h_s \Rightarrow \exists h_j : g_1 \mid h_j$

Преназначаване: 

$h_j = h'_1 \Rightarrow g_1 \mid h'_1 \Rightarrow h'_1 = \alpha_1 g_1$, $\alpha_1 \in F^*$

... // Аналогично правим и другите

$\Rightarrow g_1 \dots g_t = h'_1 \dots h'_s \Rightarrow g_2 \dots g_t = h'_2 \dots h'_s$

Не е възможно s и t да са различни, защото от едната страна бихме останали полиноми, а от другата – константи $\Rightarrow s = t$

$\Rightarrow g_i = \alpha_i h'_i \Rightarrow 1 = \alpha_1 \dots \alpha_t$

Разлагане на полиноми над $\mathbb{Z}$ и $\mathbb{Q}$

$f(x) \in \mathbb{Q}[x]$

$f = a_0 + a_1 x + \dots + a_s x^s$

$a_i = b_i / c_i$, $b_i, c_i \in \mathbb{Z}$

$НОК(c_0 \dots c_s) = c \in \mathbb{Z}$

$$f = \frac{1}{c}\left(\underbrace{\frac{b_0}{c_0}}_{l_0} \cdot c + \underbrace{\frac{b_1}{c_1}}_{l_1} c x + \dots + \underbrace{\frac{b_s}{c_s}}_{l_s} c x^s\right) \longrightarrow l_i \in \mathbb{Z}$$

$НОД(l_0 \dots l_s) = l$

$$f = \frac{l}{c}\left(\underbrace{\frac{l_0}{l}}_{h_0} + \underbrace{\frac{l_1}{l}}_{h_1} x + \dots + \underbrace{\frac{l_s}{l}}_{h_s} x^s\right) \Rightarrow h_i \in \mathbb{Z}$$

$$f = \frac{l}{c}(h_0 + h_1 x + \dots + h_s x^s), \quad НОД(h_0 \dots h_s) = 1$$

D → примитивен полином – полином с $\mathbb{Z}$ коефициенти $h_0 \dots h_s$: $НОД(h_0 \dots h_s) = 1$

Св-во: Всеки полином над $\mathbb{Q}$ може да се представи като рационална константа, умножена с примитивен полином.

($\forall f \in \mathbb{Q}[x] \Rightarrow f = \alpha g$, $\alpha \in \mathbb{Q}$, $g \in \mathbb{Z}[x]$)

Л Лема на Гаус

Произведението на два примитивни полинома с цели коефициенти е примитивен полином

$f(x) \in \mathbb{Z}[x]$, $f = a_0 + a_1x + \ldots + a_sx^s$

$n \in \mathbb{Z}$

$\varphi: \mathbb{Z}[x] \to \mathbb{Z}_n[x] \Rightarrow \varphi(f) = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_s}x^s$, $\overline{a_i} \in \mathbb{Z}_n$

↳ хомоморфизъм

Доказателство:

Нека f и g - примитивни

$h = f \cdot g$; $f = f_0 + f_1x + \ldots + f_ex^e$; $g = g_0 + g_1x + \ldots + g_mx^m$

Допускаме, че $\exists p : p \mid$ всички коефициенти на h.

↳ просто

$\varphi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

$\varphi(fg) = \varphi(h) = 0$

f - примитивен $\Rightarrow \exists k : p \nmid f_k$

g - примитивен $\Rightarrow \exists t : p \nmid g_t$

$\Rightarrow \varphi(h) = 0 = \underbrace{\varphi(g)}_{\neq 0} \underbrace{\varphi(f)}_{\neq 0} \Rightarrow 0 = \overline{f_k} \cdot \overline{g_t} \Rightarrow$ $\mathbb{Z}_p$ - поле $\Rightarrow$ няма делители на $\emptyset$, $\neq \emptyset$

$\overline{g_t} \neq 0 \quad \overline{f_k} \neq 0$

$\Rightarrow h$ е примитивен полином

Т8 Нека h - примитивен полином. $\alpha \in \mathbb{Q} : \alpha \cdot h \in \mathbb{Z}[x]$. Тогава $\alpha \in \mathbb{Z}$

Доказателство:

$\alpha = a/b$, $a, b \in \mathbb{Z}$, $(a, b) = 1$

$\alpha h = \alpha(h_0 + h_1x + \ldots + h_sx^s) \in \mathbb{Z}[x]$

$\alpha h_i \in \mathbb{Z} \Rightarrow \frac{ah_i}{b} \in \mathbb{Z} \Rightarrow b \mid h_i$, $i = \overline{0,s} \Rightarrow b \mid НОД(h_0 \ldots h_s) \Rightarrow$ т.к. h - примитивен

↳ $НОД(h_0 \ldots h_s) = 1 \Rightarrow b \mid 1 \Rightarrow b = \pm 1 \Rightarrow \alpha = \frac{a}{b} = \pm a \in \mathbb{Z}$

Т Нека $f(x) \in \mathbb{Z}[x]$, $\deg f \geq 1$. f е неразложим над $\mathbb{Z} \Leftrightarrow f$ е неразложим над $\mathbb{Q}$.

Доказателство:

Нека f е неразложим над $\mathbb{Z}$. Допускаме, че f е неразложим над $\mathbb{Q}$.

$\Rightarrow \exists h, g \in \mathbb{Q}[x] : f = hg \to \deg f > \deg h$, $\deg f > \deg g$

Представяне h и g:

$h = \alpha h_1(x)$, $h_1 \in \mathbb{Z}[x]$ - примитивен

$g = \beta g_1(x)$, $g_1 \in \mathbb{Z}[x]$ - примитивен, $\alpha, \beta \in \mathbb{Q}$

$\Rightarrow f = \alpha\beta g_1h_1$

$f \in \mathbb{Z}[x]$, $\alpha\beta \in \mathbb{Q}$

hg_i - ПРИМИТИВЕН $\Rightarrow \alpha\beta \in \mathbb{Z} \Rightarrow$ ИМАМЕ РАЗЛАГАНЕ НА f НАД $\mathbb{Z}$

$\Rightarrow$ ↯ $\Rightarrow f$ - НЕРАЗЛОЖИМ НАД $\mathbb{Q}$

Т Критерий на Айзенщайн

Нека $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Z}[x]$

Ако $\exists p$ - просто:

1) $p \nmid a_0$
2) $p \mid a_i,\ i = \overline{1,n}$
3) $p^2 \nmid a_n$,

то f е неразложим

Доказателство:

Допускаме, че е разложим над $\mathbb{Z}$.

$f(x) = g(x)h(x)$. $\deg g < n$, $\deg h < n$

$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

$\varphi(f) = \overline{a_0}x^n = \varphi(g)\varphi(h)$

$\hookrightarrow$ имат само неразложими множители

$\varphi(g) = a_{1\bullet}x^s$

$\varphi(h) = \beta_1 x^t$, $s + t = n$

$\Rightarrow p \mid g_i,\ i = \overline{0,s}$, $p \mid h_i,\ i = \overline{0,t}$

$\Rightarrow a_n = g_0h_0$

$p \mid h_0, p \mid g_0 \Rightarrow p^2 \mid a_n \Rightarrow$ ↯ $\Rightarrow f$ е неразложим

Следствие: Над полето на рационалните числа има неразложими полиноми от произволна степен.

Корени на полиноми

$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in F[x]$, F - поле

D α е корен на f, когато $f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$.

$f(x) = q(x)(x-\alpha) + r(x) = q(x)(x-\alpha) + \beta$

$\deg r < \deg(x-\alpha) = 1 \Rightarrow r = \text{const}$

$f(\alpha) = q(\alpha)(\alpha-\alpha) + \beta \Rightarrow f(\alpha) = \beta \Rightarrow$

$\Rightarrow \alpha$ е корен $\Leftrightarrow (x-\alpha) \mid f(x)$ ← Свойство