h, g_i - примитивен $\Rightarrow a, \beta \in \mathbb{Z} \Rightarrow$ 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

Т Нека F-поле и f е неразложим полином над F и $\deg f > 1$. Тогава $\exists T$-поле: $F \subset T$ и в T $f(x)$ има корен

Доказателство

$I = (f(x)) = \{fg \mid g \in F[x]\}$

$T = F[x]/I = \{r(x) + I \mid r(x) \in F[x]\}$

$g(x) = \underbrace{f(x)q(x)}_{\in I} + r(x)$, $\deg r < \deg f$

$\Rightarrow g(x) \in r(x) + I$

Нека $f(x) = a_0x^n + \ldots + a_n$, $\deg f = n$

T- комутативен пръстен с единица

$r(x) + I \neq 0 + I \Rightarrow (r(x), f(x)) = \begin{cases} 1 \\ f \end{cases} \Rightarrow r(x) = f(x)q(x) \Rightarrow f \mid r \Rightarrow$

$\Rightarrow (r, f) = 1 = u(x)r(x) + \underbrace{v(x)f(x)}_{\in I}$, $u, v \in F[x]$ $\Rightarrow r + I = 0 + I$

$\Rightarrow u(x)r(x) \in 1 + I$

$\Rightarrow (u(x) + I)(r(x) + I) = 1 + I \Rightarrow r(x) + I$ – обратим $\Rightarrow T$ – поле

$\varphi : F \to T$ – хомоморфизъм

$\varphi(a) = a + I = \overline{a}$

$\ker \varphi = \{0\} \lhd F$

$\Rightarrow \operatorname{Im}\varphi = T_0 = \{a + I \mid a \in F\}$

$\Rightarrow \operatorname{Im}\varphi \cong F/\ker\varphi = F \Rightarrow$

$\Rightarrow F \cong T_0 \subset T \Rightarrow F \subset T$

$f(x) \in T_0[x]$

$\Rightarrow f(x) = \overline{a_0}x^n + \overline{a_1}x^{n-1} + \ldots + \overline{a_n}$

$\beta = x + I \in T$

$f(\beta) = \overline{a_0}(x+I)^n + a_1(x+I)^{n-1} + \ldots + \overline{a_n} =$

$= \overline{a_0}(x^n + I) + \overline{a_1}(x^{n-1} + I) + \ldots + \overline{a_n} =$

$= \overline{a_0}x^n + I + \overline{a_1}x^{n-1} + I + \ldots + \overline{a_n} =$

$= \overline{a_0}x^n + \overline{a_1}x^{n-1} + \ldots + \overline{a_n} + I \Rightarrow f(\beta) = f(x) + I = 0 + I = \overline{0} \Rightarrow$

$\Rightarrow f(\beta) = 0 \Rightarrow \beta$ е корен на f в T

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

$\Leftrightarrow r_1 \equiv r_2 (f) \Leftrightarrow$ $r_1(x)$ и $r_2(x)$ дават едни и същи остатъци при деление с f.

$$\Rightarrow T = \{g(x)+I\} = \{r_0 + r_1 x + \ldots + r_{n-1}x^{n-1} + I \mid r_i \in F, i=\overline{1,n}\} =$$

($\deg f = n$)

$$= \{r_0(1+I) + r_1(x+I) + \ldots + r_{n-1}(x+I)^{n-1}\}$$

$\beta = x+I$

$r_0 + r_1 x + \ldots + r_{n-1}x^{n-1} + I = r_0\overline{1} + r_1\beta + r_2\beta^2 + \ldots + r_{n-1}\beta^{n-1} \Rightarrow$

$\Rightarrow T$ може да се разглежда като породено от $1, \beta, \beta^2 \ldots \beta^{n-1}$

Следствие: Нека $f \in F[x]$, $\deg f = n > 0$. $\exists L \geq F$: в $L[x]$ полиномът се разпада на линейни множители: $f = a(x-\alpha_1)\ldots(x-\alpha_n)$

Доказателство: От твърдението за f и $F \Rightarrow \exists K_1 \geq F : f(\alpha_1) = 0, \alpha_1 \in K_1$

$\Leftrightarrow f(x) = (x-\alpha_1)g(x)$, $g \in K_1[x]$, $\deg g = n-1$.

От твърдението за g и $K_1 \Rightarrow \exists K_2 \geq K_1 : g(\alpha_2) = 0, \alpha_2 \in K_2$

$\Leftrightarrow g(x) = (x-\alpha_2)h(x)$, $h \in K_2[x] \Rightarrow f(x) = (x-\alpha_1)(x-\alpha_2)h(x)$,

$\deg h = n-2$

...

След n стъпки получаваме, че $f = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$,

$a \in L \geq K_n \geq \ldots \geq K_1 \geq F$

D Нека $f \in F[x]$. Най-малкото възможно разширяване на F, в което влизат F и всички корени на f, наричаме поле на разлагане на полинома f над F, т.е. сечение на всички подполета на полето L от следствието, в които влизат всички корени на полинома f и F.

!Забележка: $f = x^2 - 7 \in \mathbb{Q}[x]$, $\mathbb{Q}(\sqrt{7}) \geq \mathbb{Q} \rightarrow f = (x-\sqrt{7})(x+\sqrt{7})$

$\Rightarrow \mathbb{Q}(\sqrt{7})$ е поле на разлагане на f над F.

$f = x^2 - 7 \in \mathbb{R}[x]$ - няма нужда да търсим друго

!Забележка: $f \in F[x]$

$F \cong F_1 : \varphi \begin{cases} F \to F_1 \\ a \to b \end{cases}$

$\varphi : \begin{cases} F[x] \to F_1[x] \\ f(x) \to f_1(x) \end{cases}$ - хомоморфизъм

$f, F \to K \geq F$ - ПОЛЕ НА РАЗЛАГАНЕ f НАД F; $\alpha_1 \dots \alpha_n$ - КОРЕНИ

$f_1, F_1 \to K_1 \geq F_1$ - ПОЛЕ НА РАЗЛАГАНЕ f_1 НАД F_1; $\beta_1 \dots \beta_n$ — КОРЕНИ

$\Phi: \begin{cases} K \to K_1 \\ \Phi/_F = \varphi : F \to F_1 \end{cases}$ → ИЗОМОРФИЗЪМ, ПРОДЪЛЖЕНИЕ НА φ

$\Phi(\alpha_i) = \beta_i$, $i = \overline{1,n}$

Т НЕКА $f \in F[x]$ И K Е ПОЛЕТО НА РАЗЛАГАНЕ НА f НАД F. НЕКА $F \cong F_1$, ТАКА ЧЕ $f \to f_1 \in F_1[x]$ И K_1 Е ПОЛЕТО НА РАЗЛАГАНЕ НА f_1 НАД F_1. ТОГАВА $K_1 \cong K$, Т.Е. С ТОЧНОСТ ДО ИЗОМОРФИЗЪМ СЪЩЕСТВУВА ЕДИНСТВЕНО ПОЛЕ НА РАЗЛАГАНЕ НА f НАД F.

ФОРМУЛИ НА ВИЕТ !

$f(x) \in F[x]$, $\deg f = n > 0$

$\alpha_1 \dots \alpha_n$ - КОРЕНИ НА f, $\alpha_i \in L$ - ПОЛЕ НА РАЗЛАГАНЕ НА f НАД F

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

$$\sigma_1 = \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_1}{a_0}$$

$$\sigma_2 = \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n = \frac{a_2}{a_0}$$

$$\dots$$

$$\sigma_n = \alpha_1 \dots \alpha_n = (-1)^n\frac{a_n}{a_0}$$

$$\sigma_k = (-1)^k\frac{a_k}{a_0} \to \text{ИМА } \binom{n}{k} \text{ СЪБИРАЕМИ}$$

! ЗАБЕЛЕЖКА: НЕКА L - ПОЛЕ, $L > F$, $\sigma_1 \dots \sigma_n \in L \Rightarrow$

$\Rightarrow f(x) = x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} - \dots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n$ - ИМА КОРЕНИ, ЗА КОИТО ВАЖАТ σ_i

D $f(x) \in F[x]$, $f \neq \text{const}$, $K \geq F$, $\alpha \in K$. КАЗВАМЕ, ЧЕ $\alpha \in K$ - КРАТЕН КОРЕН НА $f(x)$, АКО $f(x) = (x-\alpha)^k g(x)$, $g(x) \in K[x]$, $g(\alpha) \neq 0$.

ПРИ $k = 1$ - (ПРОСТ/ЕДНОКРАТЕН) КОРЕН.

Т НЕКА $f(x) \in F[x]$, $\text{char}F = 0$. ТОГАВА α Е k-КРАТЕН КОРЕН НА $f(x)$ ТОЧНО ТОГАВА, КОГАТО:

$f(\alpha) = f'(\alpha) = \dots = f^{(k-1)}(\alpha) = 0$, $f^{(k)}(\alpha) \neq 0$

! В КРАЙНА ХАРАКТЕРИСТИКА ПРОИЗВОДНИТЕ НЕВИНАГИ СЕ ПОЛУЧАВАТ ПРАВИЛНО

Доказателство:

$\Rightarrow$) Нека $f \in F[x]$, f има k-кратен корен $\alpha \in K \geq F$

$f = (x-\alpha)^k g(x)$, $g(\alpha) \neq 0$, $g \in K[x]$

Индукция по k

$k=1 \Rightarrow f(x) = (x-\alpha) g(x)$, $g(\alpha) \neq 0$, [redacted]

$f'(x) = g(x) + (x-\alpha) g'(x) \Rightarrow f'(\alpha) = g(\alpha) \neq 0$

ИП: α - s-кратен, $s<k$

$f(x) = (x-\alpha)^k g(x)$, $g(\alpha) \neq 0$

$f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x) = (x-\alpha)^{k-1} g_1(x)$

$g_1(x) = kg(x) + (x-\alpha) g'(x)$

$g_1(\alpha) = kg(\alpha) \neq 0$

$\uparrow$

$\mathrm{char} F = 0$

$f'(x)$ има $(k-1)$-кратен корен и $g_1(\alpha) \neq 0 \Rightarrow$ от индукционното предположение $\Rightarrow f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) \neq 0$, $f^{(k)}(\alpha) \neq 0$.

$\Leftarrow$) Нека $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha)$, $f^{(k)} \neq 0$

Нека f има ℓ-кратен корен $\alpha \in K$

[redacted]

$k < \ell \Rightarrow f^{(k)} \neq 0$, $f^{(k)}(\alpha) = 0$ (от ℓ-кратен) $\Rightarrow \ell \leq k$

$\ell < k \Rightarrow f^{(\ell)} \neq 0$, $f^{(\ell)}(\alpha) = 0$ (от k-кратен) $\Rightarrow k \leq \ell$

$\Big\} \ell = k$

Т Един полином $f \in F[x]$ има кратен корен $\alpha \Leftrightarrow \Rightarrow$ α е общ корен за f и f'.

Т Уилсън

Нека p-просто. $(p-1)! \equiv (-1) \pmod p$

Доказателство: $\mathbb{Z}_p[x] \to f(x) = x^{p-1} - 1$; $x^{p-1} \equiv 1 \pmod p$ $(p \nmid x)$

$f(x) = x^{p-1} - 1 = 0 \Rightarrow \overline{1}, \overline{2}, \ldots, \overline{p-1}$ - корени на f

$\Rightarrow x^{p-1} - \overline{1} = (x-\overline{1})(x-\overline{2}) \ldots (x-\overline{p-1})$

$\alpha_1 \ldots \alpha_{p-1} = \overline{(p-1)!} = (-1)^{\overline{p-1}} \cdot \frac{\overline{1}}{\overline{-1}} = (\overline{-1})^p$