19. 12. 2022.

Дефиниција

Нека је k потпоље поља K и $f(x) \in k[x]$.
Кажемо да се $f(x)$ разлаже над K ако је

$$f(x) = a(x - z_1) \cdot \ldots \cdot (x - z_n)$$

гдје су $z_1, \ldots, z_n \in K$ и $a \in K$ ненулти елемент.

Ако се $f(x)$ разлаже у пољу E које је проширење поља k, а не постоји поље F, $k \subseteq F \subseteq E$ тако да се $f(x)$ разлаже у пољу F, онда E називамо поље разлагања полинома $f(x)$.

Посљедица

Нека је k поље и $f(x) \in k[x]$. Онда постоји поље разлагања $f(x)$ над k.

доказ: директна посљедица Кронекерове теореме.

Лема

Нека је p прост број, а k поље. Ако је $f(x) = x^p - c \in k[x]$, онда је $f(x)$ иредуцибилан у $k[x]$ или постоји $\alpha \in k$, тако да $f(\alpha) = 0$ (односно c има p-ти коријен у k).
Стога, ако k садржи p-те коријене јединице онда је $k(\alpha)$ поље разлагања полинома $f(x)$.

доказ

На основу Кронекерове теореме, постоји проширење поља $K^{\vee} | K$ које садржи све нуле полинома $f(x)$.

Нека су α_1, α_2 нуле полинома $f(x)$. То значи

$$\alpha_1^p = c, \quad \alpha_2^p = c,$$

одакле $(\alpha_1 \alpha_2^{-1})^p = 1 \Rightarrow \alpha_1 \alpha_2^{-1} = \omega$, гдје је $\omega^p = 1$. Дакле, $\alpha_1 = \alpha_2 \omega$, гдје је ω p-ти коријен јединице.

Значи,

$$f(x) = (x - \alpha\omega_1)(x - \alpha\omega_2) \dots (x - \alpha\omega_p)$$

гдје су ω_i p-ти коријени јединице.

Ако $f(x)$ није иредуцибилан у $K[x]$, онда постоји факторизација

$$f(x) = g(x)\, h(x) \text{ у } K[x],$$

при чему $g(x)$ није константан полином и

$d = \deg(g(x)) < \deg(f(x)) = p$.

Закључујемо, $g(x) = (x - \alpha\omega_{i_1}) \dots (x - \alpha\omega_{i_d})$.

У развијеној форми $g(x)$ има неки слободан члан и нека је то $b \in K$.

Уз напомену да производ било која два p-та коријена јединице опет даје p-ти коријен јединице (p-ти коријени јединице чине групу),

онда је $b = \pm \alpha^d \cdot \omega$, гдје је ω p-ти коријен јединице.

$(\pm b) = (\alpha^q w) = \alpha = c$

Како је p прост број и $d < p$, онда је $НЗД(d, p) = 1$, што значи да постоје s и $t \in \mathbb{Z}$

$$1 = sd + tp.$$

$$c = c^{sd+tp} = c^{sd} \cdot c^{tp} = (\pm b)^{ps} \cdot c^{tp}$$

$$= \underbrace{\left[(\pm b)^s \cdot c^t\right]}_{\in k}{}^{p}$$

што значи да постоји p-ти коријен од c у k.

Уколико k садржи све p-те коријене јединице, онда је јасно да је $k(\alpha)$ минимално поље у коме се $f(x)$ потпуно раставља.

<u>Лема</u> Нека је $f(x) \in k[x]$, k поље, $\deg(f(x)) \geq 1$. Полином $f(x)$ има просте коријене (прост коријен је онај чија је вишеструкост 1) ако и само ако $НЗД(f, f') = 1$.

<u>доказ</u>

Нека је α коријен од $f(x)$ и $g(x) = \dfrac{f(x)}{x - \alpha}$

$(f(x) = (x-\alpha)\cdot g(x))$. Онда је

$$f' = (x-\alpha)\cdot g' + g(x).$$

Дакле,

α је вишеструкости веће од 1 полинома $f(x)$

$\iff \alpha$ је коријен $g(x) \iff \alpha$ је коријен f'

$\iff \alpha$ је коријен $НЗД(f, f')$.

Лема

Нека је $f(x) \in k[x]$, k поље, $\deg(f(x)) \geq 1$.

Ако је $f(x)$ иредуцибилан над $k \Rightarrow f(x)$ има просте корјене у свом пољу разлагања.

доказ

Како је $f(x)$ иредуцибилан, онда

$$НЗД(f, f') = 1 \text{ или } f \mid f'.$$

Друга могућност отпада, јер је $\deg(f'(x)) < \deg(f(x))$

Задатак

Доказати да за сваки прост број p, $x^p - 2$ је иредуцибилан у $\mathbb{Q}[x]$.

Теорема

Ако је p прост број и $n \in \mathbb{N}$, онда постоји поље са тачно p^n елемената.

доказ:

Нека је $q = p^n$. Размотримо полином $g(x) = x^q - x \in \mathbb{F}_p[x]$.

По Кронекеровој теореми, постоји поље K које садржи $\mathbb{F}_p$, тако да је $g(x)$ производ линеарних фактора у $K[x]$.

Посматрамо
$$E = \{\alpha \in K : g(\alpha) = 0\}$$

Дакле, E је скуп корјена $g(x)$.

Очигледно, $g' = q x^{q-1} - 1 = p^n x^{q-1} - 1 = -1$