21. 12. 2022.

Лема Нека је $f(x) \in k[x]$, k поље и E поље разлагања $f(x)$ над k.
Нека је $\varphi : k \to \bar{k}$ изоморфизам поља, а $\bar{E}$ поље разлагања полинома $\bar{f}(x) \in \bar{k}[x]$ ($\bar{f}(x)$ добија се пресликавањем одговарајућих коефицијената полинома $f(x)$ преко пресликавања φ)
Онда постоји $\Phi : E \to \bar{E}$ изоморфизам тако да
$\Phi|_k = \varphi$.

$$\begin{tikzcd}
E \arrow[r, dash, "\Phi"] & \bar{E} \\
k(z) \arrow[u, dash] \arrow[r, dash, dashed, "\bar{\varphi}"] & \bar{k}(\bar{z}) \arrow[u, dash] \\
k \arrow[u, dash] \arrow[r, dash, "\varphi"'] & \bar{k} \arrow[u, dash]
\end{tikzcd}$$

доказ
Индукцијом по $d = [E:k]$.
Ако је $d = 1$, онда је $f(x)$ производ линеарних полинома у $k[x]$, па је такав и $\bar{f}(x)$ у $\bar{k}[x]$. У том случају, закључујемо да је $\bar{E} = \bar{k}$ и тиме $\Phi \equiv \varphi$.

За индуктивни корак, нека је z коријен од $f(x)$ у E, а није у k.
Нека је $p(x) = irr(z,k)$. Пошто $z \notin k \Rightarrow deg(p) > 1$ и $[k(z):k] = deg(p(x))$.
Нека је $\varphi(p) = \bar{p}$. Јасно је да је $\bar{p}$ иредуцибилан у $\bar{k}[x]$.
Нека је $\bar{z}$ произвољна нула од $\bar{p}(x)$ у $\bar{E}$. Наравно,

$\bar z \notin \bar k$.

По претходној леми, постоји

$$\bar\sigma : k(z) \to \bar k(\bar z)$$

изоморфизам, такав да $\bar\sigma(z) = \bar z$, $\bar\sigma|_k \equiv \sigma$.

E је поље разлагања $f(x)$ над $k(z)[x]$, а на исти начин $\bar E$ је поље разлагања $\bar f(x)$ над $\bar k(\bar z)[x]$.

Међутим $[E : k(z)] < [E : k]$, па по индуктивној претпоставци, постоји $\varphi : E \to \bar E$ изоморфизам тако да $\varphi|_{k(z)} = \bar\sigma \Rightarrow \varphi|_k = \sigma$.

Теорема

Ако је k поље и $f(x) \in k[x]$, онда су свака два поља разлагања $f(x)$ над k изоморфна.

доказ

Нека су E и $\bar E$ два поља разлагања $f(x)$ над k.
Ако је $\sigma \equiv \mathrm{Id}\ (k \to k)$, онда по претходној леми постоји изоморфизам $\bar\sigma : E \to \bar E$, тако да

$$\bar\sigma|_k \equiv \mathrm{Id}.$$

Последица

Свака два поља E и $\bar E$, тако да $|E| = |\bar E| = p^n$, p-прост број, $n \in \mathbb{N}$, су изоморфна.

доказ

Поља E и $\bar E$ садрже $\mathbb{F}_p$, а из једне од претходних лема знамо да су E и $\bar E$ поља разлагања полинома $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

полином $f(x) = x \ldots - x \ldots$

$$\begin{tikzcd}
E \arrow[r, dashed, "\varphi"] & \overline{E} \\
\mathbb{F}_p \arrow[u, dashed] \arrow[r, "\mathrm{Id}"] & \mathbb{F}_p \arrow[u, dashed]
\end{tikzcd}$$

φ - изоморфизам $E \to \overline{E}$, $\varphi|_{\mathbb{F}_p} \equiv \mathrm{Id}$.

Лема Ако је F коначно поље са q елемената, онда за свако $a \in F$, $a^q = a$.

доказ: вјежба.

Лема Ако је F коначно поље са q елемената и K подпоље од F, онда се полином $x^q - x \in K[x]$ разлаже у F.

$$x^q - x = \prod_{a \in F} (x - a)$$

односно F је поље разлагања $x^q - x \in K[x]$.

Напомена

$$\underbrace{x^{p^n} - x}_{g(x)} \in \mathbb{F}_p[x], \quad p\text{-прост број}, \; n \in \mathbb{N}.$$

НЗД$(g(x), g'(x)) = 1$, јер

$$g'(x) = \underbrace{p^n \cdot x^{p^n - 1}}_{\equiv 0 \text{ у } \mathbb{F}_p} - 1 = -1.$$

То значи да у све нуле $g(x)$ једноструке (просте).

Доказано је раније

$$E = \{a \in K \mid g(a) = 0\}, \quad (K\text{- Кронекерово поље})$$

$|E| = p^n$

је поље и $|E| = p$.

Лема

Нека је $\mathbb{F}_q$ коначно поље са $q = p^n$ елемената.
Онда свако потпоље поља $\mathbb{F}_q$ има p^m елемената, при чему $m \mid n$.
Такође, ако је $m \mid n$, онда постоји тачно једно потпоље поља $\mathbb{F}_q$ са p^m елемената.

доказ

Ако је K потпоље од $\mathbb{F}_q \Rightarrow [\mathbb{F}_q : K] = s \Rightarrow$
$|\mathbb{F}_q| = |K|^s \Rightarrow |K| = p^m$ и $m \cdot s = n$.

Обрнуто, ако је $m \mid n \Rightarrow p^m - 1 \mid p^n - 1$

$\Rightarrow x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ у $\mathbb{F}_p[x]$

Дакле, сваки корјен $x^{p^m} - x$ припада $\mathbb{F}_q$, односно $\mathbb{F}_q$ садржи поље разлагања полинома $x^{p^m} - x$, а њих елемената има тачно p^m.
Ако би постојала два таква поља, онда $x^{p^m} - x$ би имао више од p^m нула, што је немогуће.

Лема

Нека је F_q коначно поље, а F_r његово коначно проширење.
Онда је $F_r = F_q[\alpha]$, за неко $\alpha \in F_r$.

доказ

F_r је коначно проширење и постоји $\langle \alpha \rangle = F_r^*$.
Јасно, $F_q(\alpha) \subseteq F_r$, а са друге стране
$F_q(\alpha)$ садржи нулу и све степене од $\alpha \Rightarrow F_q(\alpha) = F_r$.

Како је α алгебарски, онда $F_2(\alpha) = F_2[\alpha] = F_r$.

Последица

Нека је F_2 коначно поље и $n \in \mathbb{N}$. Постоји иредуцибилни полином у $\mathbb{F}_2[x]$ степена n.

Доказ

Знамо да постоји $\mathbb{F}_r$ тако да $|\mathbb{F}_r| = 2^n$.

и сходно томе $[\mathbb{F}_r : \mathbb{F}_2] = n$.

Према претходној леми $\mathbb{F}_r = \mathbb{F}_2[\alpha]$.

С друге стране $f(x) = Irr(\alpha, \mathbb{F}_2)$, знамо

$$\mathbb{F}_2[x] / (f(x)) \cong \mathbb{F}_2[\alpha]$$

$$\Rightarrow deg(f(x)) = (\mathbb{F}_2[\alpha] : \mathbb{F}_2) = n.$$