26. 12. 2022.

<u>Примјер</u>

Нека је $m \in \mathbb{N}$, а $k$ поље. Посматрамо $f(x) = x^m - 1 \in k[x]$

Ако $\mathrm{char}(k) \nmid m$, онда $m x^{m-1} \neq 0$, па је

НЗД$(f, f') = 1$.

Дакле, $f$ нема вишеструких нула. Стога поље разлагања $E$ полинома $f(x)$ садржи $m$ различитих коријена јединице.

Подсјетимо, $E^*$ садржи мултипликативну групу тих коријена јединице, која је циклична.

Дакле, у случају $\underline{\mathrm{char}(k) \nmid m}$, онда постоји примитивни $m$-ти коријен јединице у неком проширењу поља $k$. Ако је тај примитивни коријен (генераторни елемент цикличне групе) $\omega \in E$, онда је јасно да је $\omega$ сепарабилан елемент.

С друге стране, ако је $p^e$ степен простог броја и $\mathrm{char}(k) = p$, онда

$$x^{p^e} - 1 = (x-1)^{p^e}$$

$\Rightarrow$ постоји само један $p^e$-ти коријен јединице, а то је 1.

За општи случај $f(x) = x^m - 1 \in k[x]$,

ако је

$char(k)=0$, онда поље разлагања полинома $f$ садржи све $m$-те коријене јединице.

$char(k)=p$, $p$-прост број

→ $p \mid m$, $m = p^k \cdot s$

$x^m - 1 = x^{p^k \cdot s} - 1 = (x^s)^{p^k} - 1 = (x^s - 1)^{p^k}$

поље разлагања садржи све $s$-те коријене јединице.

→ $p \nmid m$

поље разлагања садржи све $m$-те коријене јединице.

Наставак:

Питање за чији смо одговор заинтересовани је величина групе Галоа, у неким случајевима, $|Gal(E|k)| = ?$

С тим у вези је следећа теорема.

Теорема

Нека је $E|k$ сепарабилно проширење које је уједно и поље разлагања за $f(x) \in k[x]$.
Нека је $\sigma : k \to \bar{k}$ изоморфизам поља, а $\bar{E}|\bar{k}$ поље разлагања за $\bar{f}(x) \in \bar{k}[x]$
($\bar{f}(x)$ добијен стандардно – „апликацијом" изоморфизма $\sigma$ на коефицијенте $f(x)$)

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash] & \bar{E} \arrow[d, dash] \\
k(\alpha) \arrow[r, dash, "\hat{\sigma}"] \arrow[d, dash] & \bar{k}(\bar{\alpha}) \arrow[d, dash] \\
k \arrow[r, dash, "\sigma"'] & \bar{k}
\end{tikzcd}$$

Онда постоји тачно $[E:k]$ изоморфизама $\phi : E \to \bar{E}$ који проширују $\sigma$

<u>доказ:</u>

Најприје уочимо да из што је $E$ поље разлагања полинома $f(x)$, говори да је $[E:k]$ коначно.

(Може се показати да је у овом случају $|E:k| \le n!$, гдје је $n = \deg(f(x))$, Кошинац страна 124)

Доказ изводимо индукцијом по $[E:k]$.

У случају $[E:k]=1$, значи да је $E=k$, па је заправо једина екстензија $\varphi$ пресликавања $\varsigma$ оно само, односно $\varphi \equiv \varsigma$.

Нека је $[E:k]>1$. Онда је $f(x)=p(x)g(x)$, гдје је $p(x)$ иредуцибилан полином степена $d>1$.

Користимо лему на почетку часа 12, конструкцију проширења $\varphi$ у односу на иредуцибилни полином $p(x)$.

Подсјетимо се, $f(x)$ је сепарабилан, па је такав и $\overline{f}(x) \in \overline{k}(x)$, односно $p(x)$ и $\overline{p}(x)$.

Дакле $p(x)$ и $\overline{p}(x)$ имају <u>тачно $d$ нула</u> у својим пољима разлагања.

$$\begin{tikzcd}
E \arrow[r, dashed] & \overline{E} \\
k(\alpha) \arrow[u, dashed] \arrow[r, dashed, "\hat{\varsigma}_i"] & \overline{k}(\overline{\alpha}_i) \arrow[u, dashed] \\
k \arrow[u, dashed] \arrow[r, "\varsigma"'] & \overline{k} \arrow[u, dashed]
\end{tikzcd}$$

$$[k[\alpha]:k] = \deg(p(x)) = d$$

$$[E:k[\alpha]] = \frac{[E:k]}{d}$$

Нека је $\alpha$ једна нула полинома $p(x)$ у пољу $E$.

За произвољну нулу $\overline{\alpha}_i$ полинома $\overline{p}(x)$, $\overline{\alpha}_i \in \overline{E}$, $i=1,2,\dots,d$, одређен је изоморфизам

$\hat{\varsigma}_i : k(\alpha) \to \overline{k}(\overline{\alpha}_i)$, $i=1,2,\dots,d$

$\sigma_i : k(\alpha) \to k(\alpha_i)$ ...

такав да $\hat{\sigma}_i|_k \equiv \sigma$ и $\hat{\sigma}_i(\alpha) = \bar{\alpha}_i$.

Уочавамо да је $[E : k(\alpha)] = \frac{[E:k]}{d} < [E:k]$

За свако пресликавање $\hat{\sigma}_i : k(\alpha) \to \bar{k}(\bar{\alpha}_i)$ и полиноме $f(x) \in k(\alpha)[x]$, $\bar{f}(x) \in \bar{k}(\bar{\alpha}_i)(x)$, а чија су поља разлагања $E$ и $\bar{E}$, можемо примијенити индуктивну претпоставку, што значи да има $\frac{[E:k]}{d}$ њетових екстензија.

То значи да имамо укупно $\frac{[E:k]}{d} \cdot d$ екстензија пресликавања $\sigma$, чиме је тврђење доказано.

## Нормална проширења

$F \geq K$ је <u>нормално проширење</u> поља ако је

- алгебарско
- за произвољан иредуцибилан полином $p(x) \in k[x]$ који има једну нулу у $F$, вриједи да су му све нуле у $F$.

<u>Примјер</u>

$\mathbb{Q}[\sqrt[3]{2}]$ није нормално проширење поља $\mathbb{Q}$, јер иредуцибилан полином $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ има једну нулу у $\mathbb{Q}[\sqrt[3]{2}]$, док остале двије нису у том пољу.

<u>Теорема</u>

Коначно проширење $F$ поља $K$ је нормално $\iff$ $F$ поље разлагања неког полинома $p(x) \in k[x]$.

<u>доказ:</u>

књига Ротман.

## Последица

Нека је $E$ сепарабилно проширење поља $k$, а уједно и поље разлагања $f(x) \in k[x]$.
Онда је $|Gal(E:k)| = [E:k]$.

**доказ:**

Из претходне теореме закључујемо да је $E$ нормално проширење поља $k$, док из теореме слиједи

$$\begin{tikzcd} E \arrow[r, dashed, "\varphi"] & E \\ k \arrow[u, dash, dashed] \arrow[r, "Id"] & k \arrow[u, dash] \end{tikzcd}$$

закључујемо да постоји $[E:k]$ изоморфизама који проширују $Id: k \to k$.

|| Дакле, $|Gal(E:k)| = [E:k]$ у случају да је $E$ нормално и сепарабилно проширење поља $k$. ||

## Последица

Нека је $E$ сепарабилно проширење поља $k$, уједно и поље разлагања иредуцибилног полинома $f(x) \in k[x]$ (што значи да је нормално).
Онда је $n \mid |Gal(E|k)|$, гдје је $n = deg(f(x))$.

**доказ**

Већ смо истакли да ако је $E$ нормално и сепарабилно проширење, онда $|Gal(E:k)| = [E:k]$.
Нека је $\alpha \in E$ коријен од $f(x)$. Како је $f(x)$ иредуцибилан и $[k(\alpha):k] = n$, онда је

$$[E:k] = [E:k(\alpha)] \cdot [k(\alpha):k] = n \cdot [E:k(\alpha)].$$

## Појам нормалног затворења

Нека је $L = K[\alpha_1, \alpha_2, \dots, \alpha_n]$ коначно проширење, а $F$ поље разлагања од $p = p_1 p_2 \cdots p_n$, $p_i = \operatorname{Irr}(\alpha_i, K)$, које садржи поље $K$.
Јасно је да $F$ мора садржати $L$, јер садржи $K$ и свако $\alpha_i$, $i = 1, \dots, n$. Стога, имамо

$$K \leq L \leq F.$$

Претпоставимо да је $S$ нормално проширење поља $K$ које садржи $L$.
Како $S$ садржи $\alpha_1, \alpha_2, \dots, \alpha_n$, а то су нуле полинома $p_1, p_2, \dots, p_n$, онда због чињенице да је $S$ нормално, $S$ мора садржати све нуле сваког од тих полинома, односно полинома $p$.
Дакле, полином $p$ се потпуно разлаже у $S$, али $F$ је његово поље разлагања, па $F \leq S$.

Дакле, $F$ је минимално нормално проширење поља које садржи његово коначно проширење $L$.
Стога, $F$ је јединствено.
За $F$ кажемо да је нормално затворење проширења $L$ поља $K$.