

26. 12. 2022.

Пример

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

Ако $\text{char}(K) \nmid m$, онда $mx^{m-1} \neq 0$, па је

$$\text{HЗД}(f, f') = 1.$$

Дакле, f нема вишеструких нула. Слика поље разлагања

E полинома $f(x)$ садржи m различитих корјена јединице.

Посматрамо, E^* садржи мултипликативну групу
овак корјена јединице, која је цикличка.

Дакле, у случају $\text{char}(K) \nmid m$, онда постоји

примитивни m -ти корјен јединице у неком
пречињеном пољу K . Ако је овај примитивни корјен
(генератор елемента цикличке групе) $\omega \in E$,
онда је јасно да је ω сепарисан елемент.

С групе поље, ако је p^e сликата групе која
у $\text{char}(K) = p$, онда

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

\Rightarrow постоји само један p^e -ти корјен јединице,

а то је 1.

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

ако је

$\text{char}(k) = 0$, onda postoje različitava p -ti potencija f
 sadrži sve m -te korijene jedinice.

$\text{char}(k) = p$
 p -ti potencija f

→ $p \mid m, m = p^k \cdot s$
 $x^m - 1 = x^{p^k \cdot s} - 1 = (x^s)^{p^k} - 1 = (x^s - 1)^{p^k}$
 onda razlaže se sadrži sve s -te
 korijene jedinice.

→ $p \nmid m$
 onda razlaže se sadrži sve
 m -te korijene jedinice.

Наставак:

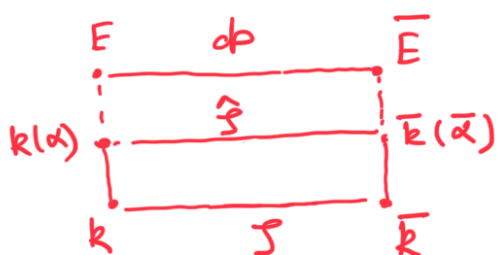
Питање за који смо одговор замишљали
 је величина групе Галоа, у неким случајевима,
 $|Gal(E/k)| = ?$

С њим 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 $\mathcal{I}: k \rightarrow \bar{k}$ изоморфизам поља, а
 $\bar{E}|\bar{k}$ поље разлагања за $\bar{f}(x) \in \bar{k}[x]$
 ($\bar{f}(x)$ добијен апсолутно – „апликацијом“
 изоморфизма \mathcal{I} на коефицијенте $f(x)$)



Онда постоји тачно $[E:k]$ изоморфизама
 $\rho: E \rightarrow \bar{E}$ који проширяју \mathcal{I}

$\hat{\mathcal{F}}_i : K(\alpha) \rightarrow K(\bar{\alpha}_i)$
 такав да $\hat{\mathcal{F}}_i|_K \equiv \mathcal{F}$ и $\hat{\mathcal{F}}_i(\alpha) = \bar{\alpha}_i$.

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

За свако италиковање $\hat{\mathcal{F}}_i : K(\alpha) \rightarrow K(\bar{\alpha}_i)$
 и полинома $f(x) \in K(\alpha)[x]$, $\bar{f}(x) \in K(\bar{\alpha}_i)(x)$, а ија
 су иста језликања E и \bar{E} , могамо применијети
 индуктивну претпоставку, што значи да има
 $\frac{[E:K]}{d}$ негових екстензија.

По значи да имамо укупно $\frac{[E:K]}{d} \cdot d$ екстензија
 италиковања \mathcal{F} , чиме је иврђење доказано.

Нормалне италиковања

$F \supset K$ је нормално италиковање тога ако је

- алгебарско
- за произвољан иредуцибилан полином $p(x) \in K[x]$
 који има једну илду γ у F , вриједи да у илду све
 илде γ у F .

иријер

$\mathbb{Q}[\sqrt[3]{2}]$ није нормално италиковање тога \mathbb{Q} , јер иредуцибилан
 полином $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ има једну илду γ у $\mathbb{Q}[\sqrt[3]{2}]$,
 док остале две илде нију у итом тољу.

Теорема

Конечно италиковање F тога K је нормално \Leftrightarrow
 F иста језликања неког полинома $p(x) \in K[x]$.

доказ:

книга Ройман.

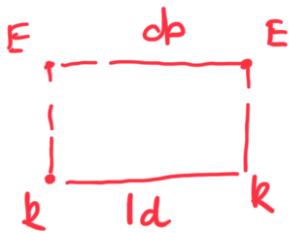
Последница

Нека је E сепарабилно проширење поља k , а $f(x)$ је нека полинома $f(x) \in k[x]$.

Онда је $|Gal(E:k)| = [E:k]$.

доказ:

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



Закључујемо да постоји $[E:k]$ изоморфизма крми проширења $Id: k \rightarrow k$.

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

Последница

Нека је E сепарабилно проширење поља k , $f(x)$ је нека полинома $f(x) \in k[x]$ (што значи да је нормално).

Онда је $n \mid |Gal(E:k)|$, где је $n = \deg(f(x))$.

доказ

Велико теорема каже да ако је E нормално и сепарабилно проширење, онда $|Gal(E:k)| = [E:k]$.

Нека је $\alpha \in E$ корјен 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 $L = K[\alpha_1, \alpha_2, \dots, \alpha_n]$ која проширене,
а F поље разлагања од $P = P_1 P_2 \dots P_n$, $P_i = \text{irr}(\alpha_i, K)$,
које садржи поље K .

Јасно је да F мора садржати L , јер садржи K и свако
 α_i , $i=1, \dots, n$. Сигурно, имамо

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

Можемо ставити 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 .

Закле, полином P се потпуно разлаже у S , али F је
његово поље разлагања, па $F \leq S$.

Закле, F је минимално нормално проширење поља
које садржи његово коначно проширење L .

Сигурно, F је јединствено.

За F кажемо да је нормално затворено проширење
 L поља K .