23.12.2022.

Поља

Посматрамо полином

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

$$= (x-z_1)(x-z_2)\dots(x-z_n)$$

$f(x) \in k[x]$, k поље, K поље разлагања полинома $f(x)$, $z_1, \dots, z_n \in K$.

Очигледно

$$a_{n-1} = -\sum_i z_i$$

$$a_{n-2} = \sum_{i<j} z_i z_j$$

$$\vdots$$

$$a_0 = (-1)^n z_1 z_2 \dots z_n$$

Дакле, на основу коријена ми изражавамо коефицијенте.

Да ли на основу коефицијената можемо у општем случају изразити коријене?

За $n=2,3,4$, одговор је потврдан.

За $n \geq 5$ доказујемо да не постоји општа „формула" којом је могуће изразити коријене помоћу коефицијената.

Дефиниција

[illegible]

Нека је E поље које садржи потпоље k. Аутоморфизам σ поља E кажемо да фиксира k, ако је

$$\sigma(a)=a, \ a\in k.$$

Лема

Нека је k потпоље поља K и

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in k[x],$$

а $E = k(z_1, z_2, \dots, z_n) \subseteq K$ поље разлагања полинома $f(x)$.
Нека је $\sigma: E \to E$ аутоморфизам који фиксира k.
Онда σ пермутује коријене $z_1, z_2, \dots, z_n$.

Доказ

Ако је r коријен од $f(x)$ онда

$$0 = f(r) = r^n + a_{n-1}r^{n-1} + \dots + a_1 r + a_0$$

Апликујући σ на претходну једнакост, имамо

$$0 = \sigma(r)^n + a_{n-1}\sigma(r)^{n-1} + \dots + a_1\sigma(r) + a_0$$

$$= f(\sigma(r)).$$

Дакле, $\sigma(r)$ је коријен од $f(x)$, што значи да за $Z = \{z_1, \dots, z_n\}$ коријени $f(x)$, вриједи

$$\sigma|_Z \text{ пермутација скупа } Z.$$

Непосредно да је σ функција, па је инјективно на коначном скупу Z, што значи да је и сурјективно.

Дефиниција

Нека је k потпоље поља E. Група Галоа поља E над k, коју означавамо $Gal(E|k)$ је скуп свих

над k, коју означавамо [illegible]
аутоморфизама у E који фиксирају k.

Ако је $f(x) \in k[x]$ и $E = k(z_1, \dots, z_n)$ поље разлагања $f(x)$, онда је група Галоа тог полинома заправо

$$Gal(f \mid k) = Gal(E \mid k).$$

- Лако је провјерљиво да је $Gal(E|k)$ заиста група у односу на композицију.

Лема

Нека је $E = k(z_1, \dots, z_n)$. Ако је $\sigma \in Gal(E|k)$ и $\sigma(z_i) = z_i$, $i = 1, \dots, n$, онда је $\sigma \equiv Id_E$.

доказ: тривијално.

Теорема

Ако је $f(x) \in k[x]$ степена n, онда је $Gal(E|k)$ изоморфна подгрупи групе S_n.

доказ: вјежба.

примјер

$f(x) = x^2 + 1 \in \mathbb{Q}[x]$.

Посматрајмо пресликавање $\sigma : \mathbb{Q}[i] \to \mathbb{Q}[i]$, $i^2 = -1$.

$\sigma(z) = \overline{z}$ (конјугација). Очигледно, $\sigma \in Gal(\mathbb{Q}[i] / \mathbb{Q})$.

С друге стране $Id_{\mathbb{Q}[i]} \in Gal(\mathbb{Q}[i] \mid \mathbb{Q})$.

Према претходној теореми $Gal(\mathbb{Q}[i] \mid \mathbb{Q})$ је

подгрупа S_2.
Дакле, $Gal(\mathbb{Q}[i]/\mathbb{Q}) = \{id, \sigma\} \cong C_2$
(циклична група реда 2).

Лема

Ако је k поље карактеристике 0, онда иредуцибилан полином $f(x) \in k[x]$ нема вишеструких коријена.

доказ:

Користимо тврдњу да $f(x)$ нема вишеструких нула ако и само ако НЗД $(f(x), f'(x)) = 1$
(Ротман)

Дефиниција

Нека је $E|k$ алгебарско проширење. Иредуцибилан полином $p(x)$ је сепарабилан ако нема вишеструких коријена.

Произвољан полином $f(x)$ је сепарабилан ако је сваки од његових иредуцибилних фактора сепарабилан.

Елемент $\alpha \in E$ је сепарабилан ако је испуњен један од два услова:

а) α је трансцендентан над k

б) α је алгебарски над k при чему је $irr(\alpha, k)$ сепарабилан полином.

Проширење поља E над k је сепарабилно, ако је сваки елемент $a \in E$ сепарабилан над k.
У супротном, E је несепарабилно проширење поља k.

Напомена

Последица

Нека је E проширење поља k карактеристике 0.

Онда је E сепарабилно над k.

Доказ:

Директна последица дефиниције и претходне леме.

Пример

Нека је E коначно поље са p^n елемената.

Очигледно $\mathbb{F}_p \subseteq E$.

Полином $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$

је сепарабилан.

Подсјетимо се $f'(x) = -1$, па је НЗД$(f(x), f'(x)) = 1$,

што значи да $f(x)$ нема вишеструких коријена.

С друге стране, E се састоји од нула полинома $f(x)$.

Дакле, ако је $\alpha \in E$, онда

$irr(\alpha, k) \mid x^{p^n} - x$, гдје је $\mathbb{F}_p \subseteq k \subseteq E$.

Закључујемо, E је сепарабилно проширење поља k.

! Више од тога, закључујемо да свако коначно проширење коначног поља мора бити сепарабилно.

Вјежба: Наћи пример несепарабилног проширења.

Обрадити тему: Рјешиве групе.