תרגול 10 - תורת גלואה

$Tr(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$, $N \dots$ ✗

$Tr_{F(\alpha)/F}(\alpha) \longleftrightarrow -a_{n-1}$

K/F

$Tr_{K/F} = \sum_{\sigma : K \hookrightarrow \bar{F}}$, ...

$f \in F[x]$, K שדה פיצול, G חבורת גלואה:

$$disc(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

$\alpha_0, \dots, \alpha_{n-1}$

$$\left(f \text{ ספרבילי} \iff disc(f) \neq 0 \right)$$

טענה: $disc(f) \in F$

$\forall \sigma \in Gal(K/F)$,

$$\sigma(disc(f)) = \prod (\pm(\alpha_i - \alpha_j))^2 = disc(f)$$

$\Rightarrow disc(f) \in K^G = F$

טענה:

$G \hookrightarrow A_n \iff disc(f) \in (F^\times)^2$

בפעולה על השורשים

(לא קשה להראות: $\displaystyle \prod_{i<j}(\alpha_i - \alpha_j) = \sqrt{disc(f)} \ldots$)

[illegible] הדיסקרימיננטה

$\displaystyle \sqrt{disc(f)} = \prod_{i<j} (\alpha_i - \alpha_j) =$ ונדרמונדה

$$= \det A = \begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ & & \vdots & \\ 1 & \alpha_{n-1} & \cdots & \alpha_{n-1}^{n-1} \end{pmatrix}$$

$A_{ij} = \alpha_i^j$ $\qquad 0 \le i \le n-1$, $0 \le j \le n-1$

$disc(f) = \det A^t A$

$$A^tA = \left(\alpha_j^i\right)_{ij}\left(\alpha_j^k\right)_{jk} =$$

$$= \Bigg(\underbrace{\sum_{j=0}^{n-1}\alpha_j^{i+k}}_{\pi_{i+k}}\Bigg)_{ik} = \left(\pi_{i+j}\right)_{ij}$$

$$\pi_d = \sum_{j=0}^{n-1}\alpha_j^d = Tr_{F(\alpha_0)/F}\left(\alpha_0^d\right)$$

$$Tr_{F(\alpha_0)/F}\left(\alpha_0^i\alpha_0^j\right)$$

A^tA היא המייצגת של התבנית הבילינארית

$$Tr_{F(\alpha_0)/F} : F(\alpha_0) \longrightarrow F$$

$$1, \alpha_0, \dots, \alpha_0^{n-1}$$

$$\pi_1 = Tr_{F(\alpha)/F} = -a_{n-1}$$

$$\pi_2 = \sum \alpha_i^2 = \left(\sum\alpha_i\right)^2 - 2\overbrace{\sum_{i<j}\alpha_i\alpha_j}^{a_{n-2}}$$

$$\underbrace{\prod(x-\alpha_i)}$$

<u>תרגיל:</u> חשבו $\mathrm{disc}(f)$ עבור:

$$f(x) = x^3 + ax + b$$ (טרינום)

(כל פולינום ממעלה 3 שקול לפולינום כזה:
$$\tilde{x} = x - \frac{a_2}{3} \rightsquigarrow f(\tilde{x}) = \dots$$)

<u>פתרון:</u>

$$\mathrm{disc}(f) = \det \underbrace{A^t A}$$

$$\begin{pmatrix} \pi_0 & \pi_1 & \pi_2 \\ \pi_1 & \pi_2 & \pi_3 \\ \pi_2 & \pi_3 & \pi_4 \end{pmatrix}$$

$$\pi_0 = \sum_{j=0}^{2} \alpha_j^0 = 3$$

$$\pi_1 = \sum_{j=0}^{2} \alpha_j = 0$$

$$\pi_2 = \sum_{j=0}^{2} \alpha_j^2 = \cancel{tr^2}^{\,0} - 2\Big(\underbrace{\alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2}_{a}\Big) =$$

$$= -2a$$

$$\pi_3 = \sum_{j=0}^{3} \alpha_j^3 = -a \cancel{\sum_{j=0}^{3} \alpha_j} - 3b = -3b$$

$$x^3 = -ax - b$$

$$\pi_4 = \sum_{j=0}^{4} \alpha_j^4 = -a \underbrace{\sum_{j=0}^{3} \alpha_j^2}_{-2a} - b \underbrace{\cancel{\sum_{j=0}^{3} \alpha_j}}_{0} = 2a^2$$

סה"כ:

$$|A^t A| = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} =$$

$$= 3\begin{vmatrix} -2a & -3b \\ -3b & 2a^2 \end{vmatrix} - 2a \begin{vmatrix} 0 & -2a \\ -2a & -3b \end{vmatrix} =$$

$$= 3\cdot(-4a^3 - 9b^2) + (2a)^3 = \boxed{-4a^3 - 27b^2}$$

לכן, אם $f(x) = x^3 + ax + b$ אי ספרבילי $\Leftarrow$

$$G_f \cong A_3 \iff -4a^3 - 27b^2 \in (\mathbb{F}^\times)^2$$

ואחרת, S_3.

דוגמאות:

① $f(x) = x^3 - 3x + 1$ אי"פ מעל $\mathbb{Q}$ (למה?)

$$\mathrm{disc}(f) = -4\cdot(-3)^3 - 27\cdot 1^2 = 81 = 9^2$$

$$\Leftarrow \quad G_f \cong A_3$$

$\mathbb{Q}[x]/\langle x^3-3x+1\rangle$ -> <u>נורמלי</u> f

② $f(x) = x^3 - 2x - 2$ אי"פ מעל $\mathbb{Q}$,

$$\mathrm{disc}(f) = -4\cdot(-2)^3 - 27\cdot(-2)^2 = 32 - 108 = -76 = 4\cdot(-19)$$

$$G_f \cong S_3 \rightsquigarrow \mathbb{Q}(\sqrt{-19}) \subset \mathbb{Q}_f$$

כי $\sqrt{\mathrm{disc}(f)}$ = מכפלת הפרשי השורשים $\in$ שדה פיצול,

לכן תת-שדה הביניים הריבועי היחיד של $\mathbb{Q}_f$.

<u>תרגיל:</u> יהי $f(x)\in F[x]$ ספרבילי מעל $F \subseteq \mathbb{R}$.

ל-f יש n שורשים $= \underbrace{r}_{\text{ממשיים}} + \underbrace{2s}_{\text{מרוכבים}}$.

הוכיחו כי s זוגי $\iff \mathrm{disc}(f) > 0$.

(לכן.) (אי-זוגי $\iff$ <0)

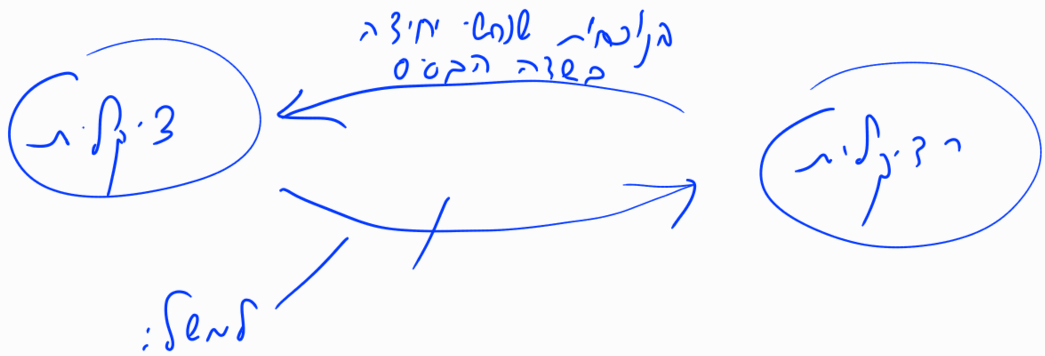
הרחבה רדיקלית

K/F **רדיקלית** $\Leftarrow$ $K=F(\alpha)$ כך ש- $\alpha^{[K:F]}\in F$.

הערה: אם K/F גלואה רדיקלית מדרגה n $\Leftarrow$ $\rho_n\in K$

(הוכחה: $X^n-\alpha^n$ פיצ׳ של α, מתפצל ב-K, ... מינימלי שלו, שורשים שונים, נותן ρ_n.)

K/F **ציקלית**: הרחבה גלואה בעלת חבורת גלואה ציקלית.



$\mathbb{Q}(\sqrt[3]{2})$ · רדיקלית $\not\Rightarrow$ ציקלית:

$\mathbb{Q}(\rho_7)/\mathbb{Q}$

$Gal\cong\mathbb{Z}/6$

$\rho_7^7=1\in\mathbb{Q}$ אך לא הרחבה רדיקלית:

אחרת, לפי הטענה הקודמת

$\rho_6\in\underbrace{\mathbb{Q}(\rho_7)}_{\text{מכיל תת-שדה ריבועי:}}$

$\wr$

$\mathbb{Q}(\sqrt{-3})$ $\qquad$ $\mathbb{Q}(\sqrt{-7})$

רדיקלית $\Rightarrow$ ציקלית:

(בתנאים שורש יחידה מסדר ממד ההרחבה בשדה הבסיס)

X^n-a^n

$\Downarrow$

$\alpha,\rho_n\alpha,\ldots,\rho_n^{n-1}\alpha\in K = F(\alpha)$

הרחבה רדיקלית + ציקלית ממעלה $n=p$ גלואה $\Leftarrow$ שורש יחידה בשדה הבסיס;

$F(\alpha): K/F$

$Gal(K/F) = \langle \sigma \rangle \quad , \quad \alpha^p \in F$

$$\begin{cases} \sigma(\alpha) = \rho_p \alpha \\ \sigma(\rho_p) = \rho_p^{r} \end{cases}$$

$$\sigma^i(\alpha) = \rho^{r^{i-1}+r^{i-2}+\dots+1}\alpha \Rightarrow \underset{\alpha}{\underset{\parallel}{\sigma^p(\alpha)}} = \rho_p^{r^{p-1}+\dots+1}\alpha$$

$$\Rightarrow \rho_p^{r^{p-1}+\dots+1} = 1 \Rightarrow p \mid r^{p-1}+\dots+1 \underset{(r-1)}{\mid} r^p - 1$$

$$r \equiv r^p \equiv 1 \pmod p$$

$$\Rightarrow \sigma(\rho_p) = \rho_p^{r} = \rho_p^{1+kp} = \rho_p \Rightarrow \rho_p \in K^{\sigma} = F.$$

רדיקלית + ציקלית ממעלה $\neq p$ לא חייבת להכיל $\underbrace{\text{שורש יחידה}}_{}$; (מסדר = מעלה)

ציקלית ממעלה 9 $\qquad Q(\rho_{27}) / Q(\rho_3)$

רדיקלית $\qquad \rho_{27}^{9} = \rho_3 \in Q(\rho_3)$

(מעלה.) $\qquad \rho_9 \notin Q(\rho_3)$

שאלות נוספות:

(1) K/F ציקלית עם שורשי יחידה מסדר המציין בשדה

הפוך $\overset{?}{\Leftarrow}$ רדיקלית

(2) K/F ציקלית ממעלה p $\overset{?}{\Leftarrow}$ רדיקלית

(במציין [illegible].)