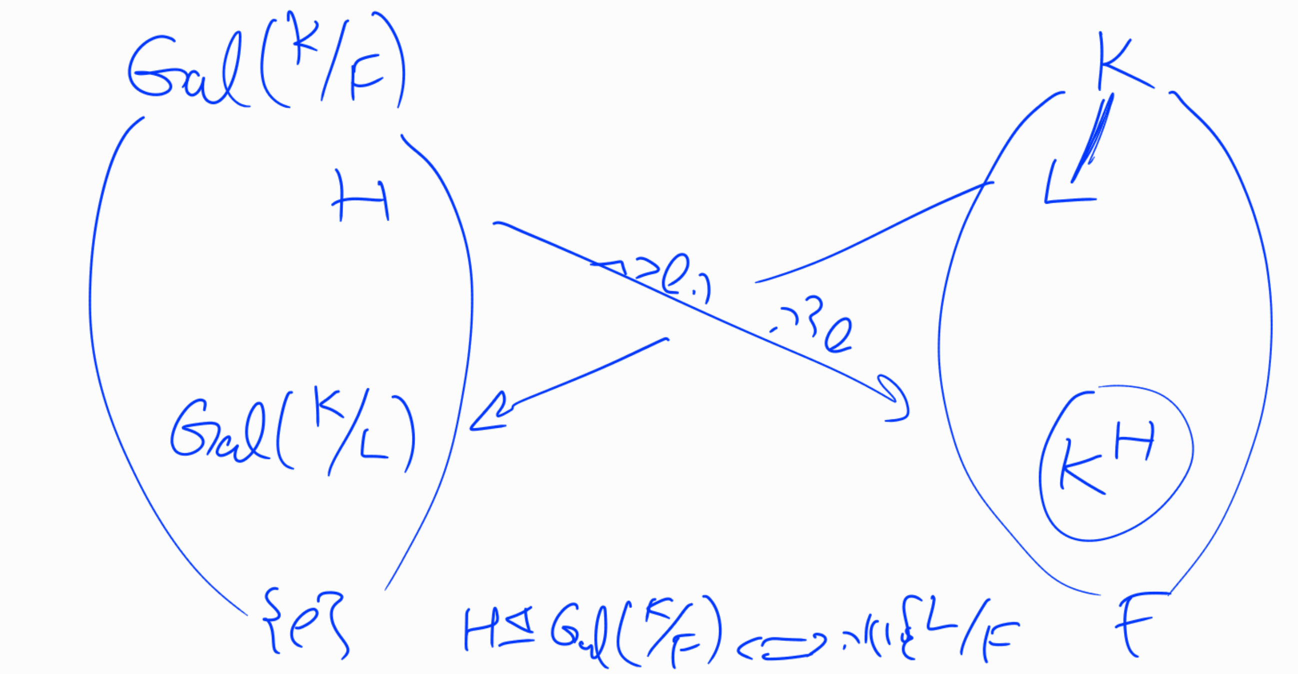
29.11.2020

תורת גלואה - תרגול 7

התאמת גלואה: (בהינתן K/F הרחבת גלואה)



$H \trianglelefteq Gal(K/F) \iff L/F$ גלואה

$$[L:F] = [Gal(K/F):H]$$

$L = K^H$

בפרט:

הרחבה מינימלית שהיא גלואה מעל F

$$\tilde{L} = K^{\bigcap_{g \in G} H^g}$$

הגרעין הנורמלי של H = $core(H)$

K גלואה

$\tilde{L}$

$L = K^H$

$K^M = E$

F

יהיו הרחבה מינימלית מעל F, E כך ש-

L/E נורמלית $\Leftarrow$ $E = K^M$

ונקבל כי: $H \trianglelefteq M$

$$\boxed{M = N_{Gal(K/F)}(H)}.$$

תרגיל: L/F נורמלית, $K_{1,2}$ שדות ביניים

מתקיים:

$$\begin{tikzcd}
 & L \arrow[d, no head] & \\
 & K_1K_2 \arrow[dl, no head] \arrow[dr, no head] & \\
K_1 \arrow[dr, no head] & & K_2 \arrow[dl, no head] \\
 & K_1\cap K_2 \arrow[d, no head] & \\
 & F &
\end{tikzcd}$$

$$\underbrace{Gal\left(L/K_1\cap K_2\right)}_{M} = \langle \underbrace{Gal(L/K_1)}_{H_1}, \underbrace{Gal(L/K_2)}_{H_2} \rangle$$

בנוסף:

$$\left[Gal(L/K_1K_2) = Gal(L/K_1) \cap Gal(L/K_2)\right]$$

פתרון:

$$\underset{L^{H_2}}{\overset{\shortparallel}{K_2}}, \underset{L^{H_1}}{\overset{\shortparallel}{K_1}} \supseteq K_1 \cap K_2 = \underset{\text{סימון}}{\underset{\uparrow}{L^M}}$$

ולכן: $H_1, H_2 \subseteq M$.

נגדיר: $H = \langle H_1, H_2 \rangle$ אזי:

$$L^H \subseteq L^{H_1} \cap L^{H_2} = K_1 \cap K_2 = L^M \Rightarrow M \subseteq H$$

סה"כ: $\underline{\underline{M=H}}$. כנדרש.

תרגיל: מצאו את תתי-שדות הביניים הריבועיים

בתוך: $\mathbb{Q}(\rho_p)$ כאשר: $\rho_p = \exp\left(\frac{2\pi i}{p}\right)$.

($p>2$ ראשוני)

פתרון:

הרחבה גלואה

עם חבורת גלואה $\cong U_p \cong \mathbb{Z}_{p-1}$

ידוע

$$\begin{array}{c} \mathbb{Q}(\rho_p) \\ | \\ \mathbb{Q} \end{array}$$

$\rho_p \longmapsto \rho_p^k$

כאשר k יוצר את U_p

$\cong (2\mathbb{Z}_{p-1})$

מסוים, יש ת"ח יחידה מאינדקס 2 ולכן יש תת-שדה ביניים ריבועי יחיד.

ת"ח מאינדקס 2 של U_p = ת"ח הריבועים U_p^2.

נחפש איבר ב-$\mathbb{Q}(\rho_p)$ שנקבע ע"י U_p^2.

$$\left\{ \sigma : \rho_p \longmapsto \rho_p^k \;\middle|\; k \text{ ריבוע מוד } p \right\}$$

$$\theta = \sum_{k \text{ ריבוע מוד } p} \rho_p^k$$

תחת U_p^2, θ נשלח לעצמו.

$$\theta \longmapsto \sum_{\substack{k \text{ ריבועי} \\ p \text{ מוד} \\ 0 \neq}} (\rho_p^m)^k = \sum_{\substack{k' \text{ ריבועי} \\ p \text{ מוד} \\ 0 \neq}} \rho_p^{k'}$$

$m \in U_p^2$

דוגמה:

$\mathbb{Q}(\rho_5)$

$\langle 2 \rangle = U_5$, $\{1,4\} = U_5^2$

$\theta = \rho_5 + \rho_5^4$

$\sigma(\theta) = \rho_5^4 + (\rho_5^4)^4 = \rho_5^4 + \rho_5 = \theta$

העלאה בחזקת 4:

לכן $\theta \in \mathbb{Q}(\rho_p)^{U_p^2}$.

$$(1+\theta)^2 = \Big(\sum_{\substack{a \text{ ריבועי} \\ p \text{ מוד}}} \rho_p^a\Big)^2 = \Big(\sum_{a \in \mathbb{Z}_p} \rho_p^{a^2}\Big)^2 =$$

$$= \sum_{a,b \in \mathbb{Z}_p} \rho_p^{a^2+b^2} = \sum_{a,b \in \mathbb{Z}_p} \rho_p^{\overbrace{(a+ib)}^{s}\overbrace{(a-ib)}^{t}} =$$

נניח מעתה:

$p \equiv 1 \pmod 4 \Rightarrow \exists$:

$i \in \mathbb{Z}_p$ כך ש- $i^2 = -1$

(כי יש איבר מסדר 4 ב- U_p ...)

$$= \sum_{s,t \in \mathbb{Z}_p} \rho_p^{st} = \underbrace{\sum_{\substack{s \in \mathbb{Z}_p \\ (t=0)}} 1}_{\boxed{p}} + \boxed{\sum_{\substack{s \in \mathbb{Z}_p \\ t \in \mathbb{Z}_p^*}} \rho_p^{ts}}$$

גנון מוקדם:

$$\mathbb{Z}_p^2 \longrightarrow \mathbb{Z}_p^2$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \longmapsto \begin{pmatrix} s \\ t \end{pmatrix} \begin{matrix} = a+ib \\ = a-ib \end{matrix}$$

(המטריצה הרלוונטית:

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

$$\det = -2i \neq 0$$

$$\overset{?}{=} \sum_{t \in \mathbb{Z}_p^*} \Bigg(\underbrace{\sum_{s \in \mathbb{Z}_p} \left(\rho_p^t\right)^s}_{1 + \rho_p^t + \rho_p^{2t} + \dots + \rho_p^{(p-1)t}} \Bigg)$$

$$= \frac{\rho_p^{pt} - 1}{\rho_p^t - 1} = 0$$

נניח: עבור $p \equiv 1 \pmod 4$,

$$(1+\theta)^2 = p$$

ולכן

$$\mathbb{Q}(\rho_p)^{U_p^2} = \mathbb{Q}(\theta) = \underline{\mathbb{Q}(\sqrt{p})}$$

מה קורה כאשר $p \equiv 3 \pmod 4$? תרגיל עליכם.

<u>תרגיל:</u> בנו הרחבה גלואה לפולינום $f = x^6+3$

$$K = \mathbb{Q}(\underbrace{\sqrt[6]{3}}_{\theta}, \rho_6)$$

$$(\sqrt{-3})$$

$$G_f \cong D_6$$

$$\boxed{\sigma: \begin{matrix}\theta \longmapsto \rho\theta \\ \rho \longmapsto \rho\end{matrix} \quad , \quad \tau: \begin{matrix}\theta \longmapsto \theta \\ \rho \longmapsto \rho^{-1}\end{matrix}}$$

נמצא הרחבות ממ׳-שני ריבועיות $\Longleftrightarrow$ תת"ח מאינדקס 2

$$\varphi: D_6 \longrightarrow \mathbb{Z}_2$$

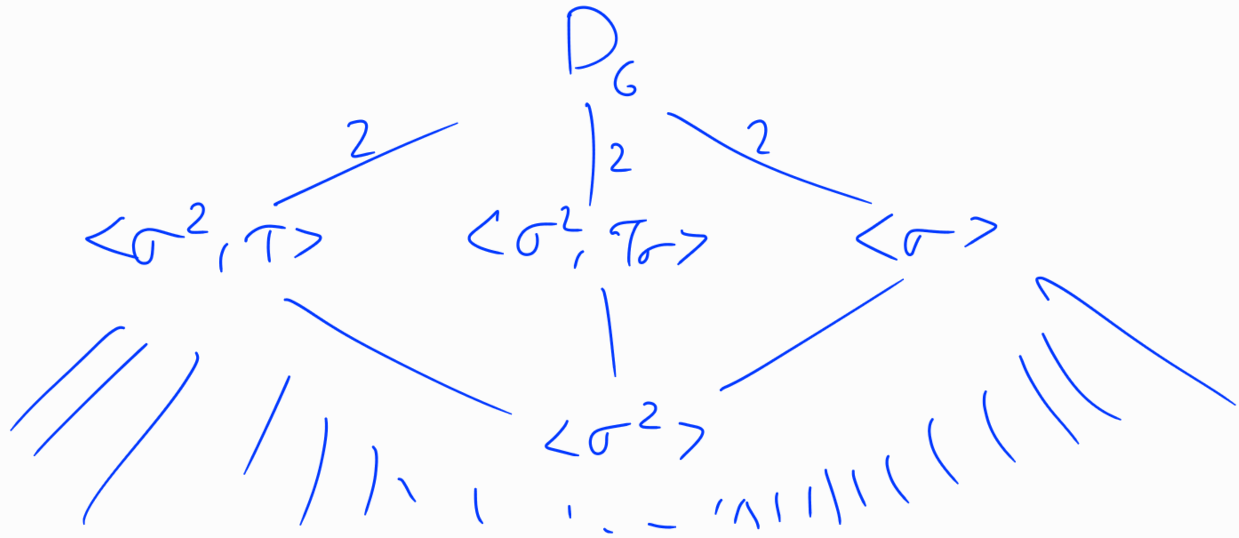
$$\sigma^2 \in \mathrm{Ker}\,\varphi$$

כל תת"ח מאינדקס 2 מכילה את $\langle\sigma^2\rangle$:

$$D_6/\langle\sigma^2\rangle \cong \frac{\langle \tau,\sigma \mid \tau^2=1,\ \sigma^6=1,\ \tau\sigma\tau=\sigma^{-1}\rangle}{\langle\sigma^2\rangle} =$$

$$= \langle \tau,\sigma \mid \tau^2=\sigma^2=1,\ \tau\sigma=\sigma\tau\rangle$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$



(I) $K^{\langle\sigma\rangle} \ni \rho \implies K^{\langle\sigma\rangle} = \mathbb{Q}(\rho_6) = \mathbb{Q}(\sqrt{-3})$

(II) $K^{\langle\sigma^2,\tau\rangle}$

$\sigma^2: \theta \mapsto \rho^2\theta$ $\quad\quad$ $\tau: \theta \mapsto \theta$

$\rho \mapsto \rho$ $\quad\quad$ $\rho \mapsto \rho^{-1}$

$\theta, \rho\theta, \rho^2\theta, \ldots, \rho^5\theta$

$0 \quad 1 \quad 2 \quad\quad 5$

$\sigma^2: (0\ 2\ 4)(1\ 3\ 5)$

$\tau: (1\ 5)(2\ 4)$ $\implies \theta, \rho^2\theta, \rho^4\theta$

$K^{\langle\sigma^2,\tau\rangle} \ni \theta\cdot\rho^2\theta\cdot\theta\rho^4 = \theta^3 =$

$= \sqrt{3}$

$K^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}(\sqrt{3})$

כעת נמצא את השדה הריבועי השלישי...

$$(1+\theta)^2 = p$$

$$1+\theta = \sqrt{p}$$

$$\sqrt{p} \in \mathbb{Q}(\rho_p)$$

$$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\rho_p)$$