5.11.2020

תורת גלואה - תרגול 5

(1) יהיו $p_1,\dots,p_n \neq \pm 1$ מס' חופשיים מריבועים זרים בזוגות. אזי:

$$\dim_{\mathbb{Q}} \underbrace{\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})}_{K_n} = 2^n .$$

פתרון:

$$\mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n$$

ברור $[K_{n+1}:K_n] \le 2$, נראה:

$$\sqrt{p_{n+1}} \notin K_n .$$

$n=0$: $\sqrt{p_1} \notin \mathbb{Q}$: זהה מאוד להוכחה ש- $\sqrt{2}$ אי-רציונלי.

$n+1$:

$$\sqrt{p_{n+1}} \in K_n = K_{n-1} + \sqrt{p_n}\, K_{n-1}$$

$$\sqrt{p_{n+1}} = \alpha_0 + \sqrt{p_n}\,\alpha_1 \quad ; \quad \alpha_{0,1} \in K_{n-1}$$

$$\underbrace{p_{n+1}}_{\mathbb{Q}} = \underbrace{(\alpha_0^2 + p_n \alpha_1^2)}_{K_{n-1}} + \underbrace{2\alpha_0\alpha_1}_{K_{n-1}} \sqrt{p_n}$$

מהנחת האינדוקציה ל- n נקבל כי: $2\alpha_0\alpha_1 = 0$

$\Leftarrow \alpha_1 = 0$ $\quad \sqrt{p_{n+1}} = \alpha_0 \in K_{n-1}$ בסתירה להנחה האינדוקציה: $p_n = p_{n+1}$

$\Leftarrow \alpha_0 = 0$ $\quad \sqrt{p_{n+1}} = \alpha_1 \sqrt{p_n}$

$$\sqrt{p_{n+1}} - \sqrt{p_n} = (\alpha_1 - 1)\sqrt{p_n}$$

$$\underbrace{p_{n+1} - p_n}_{\mathbb{Q}} = (\alpha_1 - 1)\sqrt{p_n}\left(\sqrt{p_{n+1}} + \sqrt{p_n}\right) =$$

$$= \underbrace{(\alpha_1 - 1)}_{K_{n-1}}\left(\underbrace{p_n}_{\mathbb{Q}} + \sqrt{p_n p_{n+1}}\right)$$

אם $\alpha_1 = 1 \Leftarrow \sqrt{p_{n+1}} = \sqrt{p_n}$ בסתירה לכך כי p_n, p_{n+1} זרים.

לכן $\alpha_1 \neq 1 \Leftarrow \sqrt{p_n p_{n+1}} \in K_{n-1}$

בסתירה להנחת האינדוקציה כי $p_n p_{n+1}$ חופשי מריבועים וזר לכל $p_1, \dots, p_{n-1}$.

מסקנה: $\mathbb{Q} \subset K_1 \subset \dots \subset K_n$

$$[K_n : \mathbb{Q}] = 2^n.$$

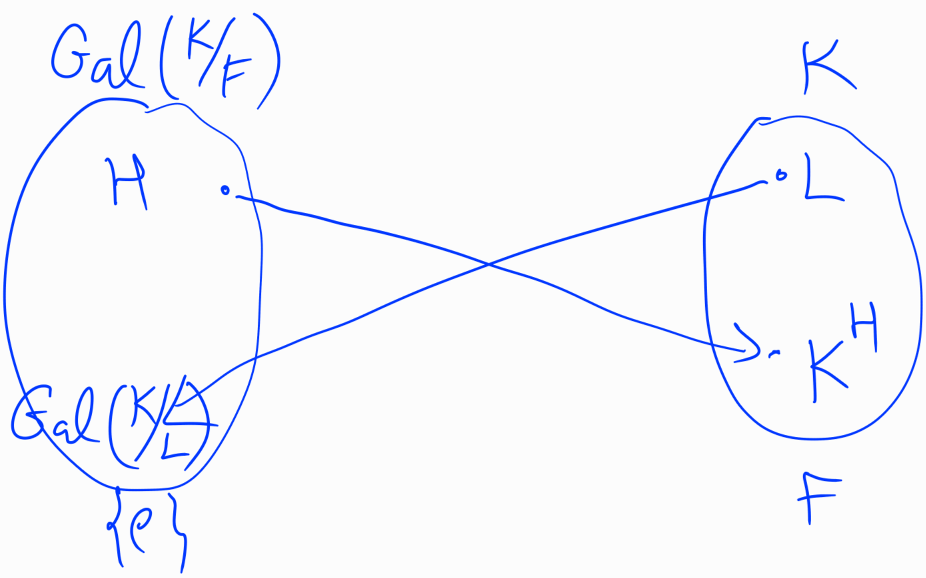
מ.ש.ל.

חבורת גלואה

$$Gal(K/F) = \{\sigma : K \to K \mid \sigma|_F = id_F\} \qquad \begin{array}{c} K \\ | \\ F \end{array}$$

$$|Gal(K/F)| \le [K:F]$$

יש שוויון עבור K שדה פיצול של פולינום ספרבילי



כאשר $K = F_f$ שדה פיצול:

(1) $F_f = F(a_1, \dots, a_n)$ $\quad (f \in F[x]) \quad (Gal_f)$

$$Gal(K/F) \curvearrowright \{a_1, \dots, a_n\}$$

קב' שורשי הפולינום f

(2) זוהי פעולה נאמנה: אם $\sigma(a_i) = a_i \Rightarrow \sigma = id_K$.

$$Gal(K/F) \hookrightarrow S_n$$

(2) יהי K שדה פיצול של f מעל F,
כאשר f אי"פ. אזי הפעולה:

$Gal(K/F) \curvearrowright \{a_1, \dots, a_n\}$ טרנזיטיבית.

להפך אם הפעולה טרנזיטיבית אז f אי"פ.

!f- ספרבילי

פתרון:

$$\begin{tikzcd} & K \arrow[dl, dash] \arrow[dr, dash] & \\ F(\theta_1) \arrow[rr, "\sim"] & & F(\theta_2) \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$$F(\theta_1) \cong \frac{F[x]}{\langle f(x) \rangle} \cong F(\theta_2)$$

לכן עבור הלמה נשתמש להרחיב לאוטומורפיזם:

$\sigma(\theta_1) = \theta_2$, $\sigma : K \to K$.

כעת נניח כי הפעולה גלואה על השורשים טרנזיטיבית —.

$r > 1$ $\qquad f = g_1 g_2 \cdots g_r$ $\qquad$ אי-פריקים (מעל F)

$$\begin{matrix} g_1 & g_2 \\ \uparrow & \uparrow \\ \theta_1 & \theta_2 \end{matrix}$$

לכן הידוע, קיים אוט $\sigma : K \to K$, $\sigma(\theta_1) = \theta_2$

$$0=\sum c_i\theta_1^i \xrightarrow{\sigma} 0=\sum c_i \underbrace{\sigma(\theta_1)}_{\theta_2}{}^i$$

מכאן של θ_1,θ_2 בדיוק אותם פולינומים (מעל F)

מינימליים אותם, כלומר אז פ״מ: $g_1=g_2$

בסתירה לספרביליות של f.

מ.ש.ל.

③ חשבו את חבורת גלואה של $f(x)=x^3+x+1$

מעל $\mathbb{Q}$.

$$\begin{array}{c} \mathbb{Q}_f \\ \big| \\ \mathbb{Q} \end{array} \Big] G$$

פתרון: ל-f אין שורש רציונלי ("q/r")

והוא מדרגה 3 $\Leftarrow$ f אי״פ.

$$G \curvearrowright \{\alpha_1,\alpha_2,\alpha_3\}$$

שורשי f

נאמנה וטרנזיטיבית.

$$G \hookrightarrow S_3$$

והפעולה טרנזיטיבית ולכן $[G:Stab_G(\alpha_1)]=3$

כלומר, $3 \mid |G|$.

נמצא איבר מסדר 2 ב-G.

$$f'(x) = 3x^2 + 1 > 0$$

לכן ל-f יש רק שורש ממשי אחד, נקרא α_1.

לכן: $\bar{\alpha}_2 = \alpha_3$.

נסמן, הצמדה מרוכבת τ משרה אוטומורפיזם של $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)/\mathbb{Q}$, שמקיים:

$$\tau = (2\ 3)$$

יש איבר מסדר 2 ב-G $\Leftarrow$ $2 \mid |G|$

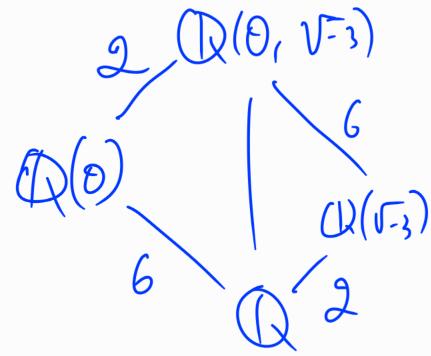
לכן $|G| = 6$ $\Leftarrow$ $G \cong S_3$. מש"ל.

(4) חשבו ת' חבורת גלואה של $f(x) = x^6 - 3 \in \mathbb{Q}[x]$.

פתרון: f אי"פ (לפי קריטריון אייזנשטיין).

$$\theta = \sqrt[6]{3}, \quad \rho_6\theta, \rho_6^2\theta, \dots, \rho_6^5\theta$$

$$\rho_6 = \exp\left(\frac{2\pi i}{6}\right) = \frac{1}{2} + \underbrace{i\frac{\sqrt{3}}{2}}_{\sqrt{-3}/2}$$



נבחר $\theta \in \mathbb{R}$, אזי $\sqrt{-3} \notin \mathbb{Q}(\theta)$ ולכן:

$$[\mathbb{Q}_f : \mathbb{Q}] = 12.$$

נעבור לפעולת חבורת גלואה:

$$G \curvearrowright \{1, 2, 3, 4, 5, 6\}$$

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \updownarrow & \updownarrow & \updownarrow & & & \updownarrow \\ \theta & \rho\theta & \rho^2\theta & \cdots & & \rho^5\theta \end{array}$$

$|G| = 12$, G טרנזיטיבית, $G \hookrightarrow S_6$

נמצא איברים מסוימים ב-G:

(I) הצמדה מרוכבת τ:

$\tau(\theta) = \theta$ $\qquad 1$

$\tau(\rho) = \rho^{-1} = \rho^5$

$\tau(\rho\theta) = \rho^5\theta$ $\qquad 2 \longleftrightarrow 6$

$\tau(\rho^2\theta) = \rho^4\theta$ $\qquad 3 \longleftrightarrow 5$

$\tau(\rho^3\theta) = \rho^3\theta$ $\qquad 4$

-1

$$\tau = (2\ 6)(3\ 5)$$

(II) נחשב איבר נוסף – "גאומטרי" הינה הקונקרטית

$\mathcal{G}$ G :

$$\sigma : \mathbb{Q}(\theta,\rho) \longrightarrow \mathbb{Q}(\theta,\rho)$$

$$\theta \longmapsto \rho\theta$$

$$\rho \longmapsto \rho$$

$$\mathbb{Q}(\theta,\rho) \cong \frac{\mathbb{Q}[x,y]}{\langle x^6-3,\ \underbrace{y^2-y+1}_{\text{הפ"מ של } \rho}\rangle}$$

$$\begin{cases} \rho = \frac{1}{2} + i\frac{\sqrt{3}}{2} \\ \rho + \rho^{-1} = 1 \Rightarrow \rho^2 - \rho + 1 = 0 \end{cases}$$

כך מאפשר להגדיר את $\mathcal{G}$ $\mathbb{Q}(\theta,\rho)$:

$$\sigma : \frac{\mathbb{Q}[x,y]}{\langle x^6-3,\ y^2-y+1\rangle} \xrightarrow{\sim} \frac{\mathbb{Q}[x,y]}{\langle x^6-3,\ y^2-y+1\rangle}$$

$$\begin{cases} x \longmapsto yx \\ y \longmapsto y \end{cases}$$

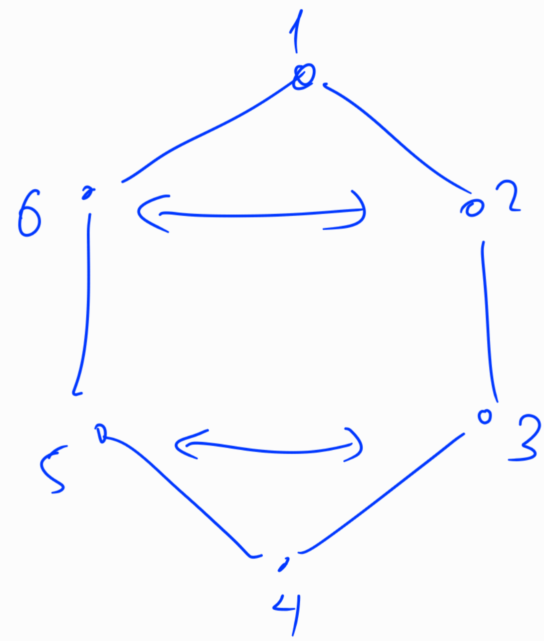
אז מה המשמעות של זה על השורשים?

$$(1\ 2\ 3\ 4\ 5\ 6)$$

$$\theta \mapsto \rho\theta \mapsto \rho^2\theta \mapsto \cdots$$

$$S_6$$

$$G \cong D_6$$



מ.ש.ל.

<u>תרגילים:</u>

חשבו חבורת גלואה של:

(1) $f(x) = x^6 + 3$ (מעל $\mathbb{Q}$)

(2) הוכיחו כי:

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) / \mathbb{Q}\right) \cong \mathbb{Z}_2^n$$