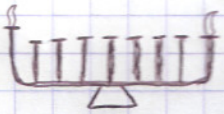
28.11.13



בס"ד כל רגל חנוכה

# אלגברה מופשטת 3 - הרצאה מס' 7.

$K/F$ הרחבת שדות.

| תת-חבורות | תת-שדות |
|---|---|
| $1$ | $K$ |
| \| | \| |
| תת-חבורות | תת-שדות |
| \| | \| |
| $Gal(K/F)$ | $F$ |

$$L \longmapsto Gal(K/L) = L^{\circ}$$

$$H^* = K^H \longleftarrow H$$

$\{x \in K : \forall \sigma \in H : \sigma(x) = x\}$

$$|L| = [K:L]$$

$$|H| \le |H^*| = |H^{*\circ}|$$

$$|L^{\circ}| = |L^{\circ *}| \le |L|$$

$|Gal(K/L)| = n^{K}_{L \hookrightarrow K} \underset{(*)}{\le} [K:L]$ (שוויון$^{(*)}$ כאשר ש- $K$ שדה פיצול של פולינום ספרבילי.

$K/F$ הרחבה גלואה = היא שדה פיצול של פול' ספרבילי.

<u>משפט:</u> $K/F$ גלואה $\Leftrightarrow$ $F = K^G$, לאיזשהי חבורת אוטו' $G$ $\Leftarrow$

$\Leftarrow$ $F = K^{Gal(K/F)}$

<u>הערה:</u> אולי יש $H < G$ כך ש- $K^G = K^H$ (נראה שלא "יתכן!).

השתמשנו שהאוטו' כ"ת: $G$ חבורת אוטו' של $K$ ($\Leftarrow$ $G \le Gal(K/\underset{F}{\overset{}{K^G}})$)

$G \le End_F(K) = M_n(F)$ כמ"ו מעל $K$

$$K \le End_F(K)$$

$$\Leftarrow \quad |G| \le [K:K^G] = |G^*|$$

<u>דוגמה:</u> $K = \mathbb{C}$, $G = \{1, \tau\}$ כאשר $\tau =$ הצמוד המרוכב.

$$F = \mathbb{C}^G = \mathbb{R}$$

$End_{\mathbb{R}}(\mathbb{C}) \cong M_2(\mathbb{R})$ ביחס לבסיס $\{1, i\}$.

השיכון של $\mathbb{C}$ לתוך $End(\mathbb{C})$ הוא לפי הכפל משמאל

$T: V \to V$
$T(b_i) = \begin{pmatrix} \vdots \end{pmatrix}$

$$x + iy \longmapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

המשך

נב' $G \subseteq End(\mathbb{C})$ : $\tau \longmapsto \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$

$id \longmapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

הצירוף שלא קיים צ"ל:

$$\begin{pmatrix}x_0 & -y_0\\ y_0 & x_0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}x_1 & -y_1\\ y_1 & x_1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = 0$$

$\in \mathbb{C}$

<u>הלמה של ארטין:</u> תהי $G$ חבורת אוטו' של שדה $K$. $(F = K^G)$.

אז $[K : K^G] \le |G|$

<u>הוכחה:</u> נסמן $n = |G|$.

נניח $n<m$ ונניח ש- $b_1, b_2, \dots, b_m \in K$. צ"ל: הם ת"ל מעל $F$.

[כלומר, קיים פתרון $x_1, \dots, x_m \in F$ (לא כולם אפס) כך ש- $\sum x_i b_i = 0$.

לכל $\sigma_j \in G$ נקבל $\forall j : \sum x_i \sigma_j(b_i) = 0$.]

נתבונן במערכת המשוואות $\forall j : \sum \sigma_j(b_i) x_i = 0$ - $m$ נעלמים $x_1, \dots, x_m$, $n$ משוואות. (מעל $K$)

מכיוון ש- $m>n$ יש פתרון לא ט' מעל $K$.

נבחר פתרון שבו $|\{i \mid x_i \neq 0\}|$ מינימלי. אפשר להניח $x_1 \neq 0$,

ולחלק ב- $x_1$ כך ש- $x_1 = 1$.

$\vec{x} = (1, 0, 0, x_{i_0}, \dots x_{i_k}, \dots)$ (-הפתרון)

<u>הערה:</u> אם הפתרון הוא $(1, 0, \dots, 0)$ אז $b_1 = 0$ ולכן הם תלויים.

נסמן ב- $i_0$ אינדקס $> 1$ כך ש- $x_{i_0} \neq 0$.

נניח $x_{i_0} \notin F$. אז יש $j$ כך ש- $\sigma_j(x_{i_0}) \neq x_{i_0}$.

נגדיר $x_i' = \sigma_{j_0}(x_i)$,

אז לכל $j$: $\sum \sigma_j(b_i) x_i' = \sum \sigma_{j_0}(\sigma_{j_0}^{-1} \sigma_j(b_i) x_i) =$

$= \sigma_{j_0}\left(\sum \sigma_{j_0}^{-1} \sigma_j(b_i) x_i\right) = \sigma_{j_0}(0) = 0 \Rightarrow \vec{x_i}'$ פתרון

גם ההפרש $\vec{x_i}' - \vec{x_i}$ פתרון. הוא אינו אפס כי בקואורדינטה $i_0$

$\sigma(1,\dots,x\dots) - \sigma(1,\dots,\sigma(x)\dots) = (0,\dots,x-\sigma(x),\dots)$ $\neq 0$

מפוצל $\sigma_{j_0}(x_{i_0}) - x_{i_0} \neq 0$.

וקיבלנו סתירה (לכך שבחרנו פתרון שבו מספר האיברים $\neq 0$ מינימלי), לכן בהכרח $x_{i_0} \in F$.

אבל $\sum x_i b_i = 0$ ולכן ה-$b_i$ הם לא מעל $k^G$. סתירה.

כבר הוכחנו $|G| \le [k:k^G]$ ולכן מסתכם $[k:k^G] = |G|$

$\Rightarrow$ ($|G| = |G^*|$).

<u>מסקנה:</u> $Gal(k/k^G) = G$.

<u>הוכחה:</u> ברור ש- $G \subseteq Gal(k/k^G) = \hat{G}$. עכשיו הוכחנו

$$[k:k^G] = |G| \le |\hat{G}| = [k:k^{\hat{G}}]$$

$$[k:G^{*\circ *}] = [k:G^*] = [k:k^G]$$

$\Leftarrow$ $|G| = |\hat{G}|$ ולכן $\hat{G} = G$.

$\Leftarrow$ $G^{*\circ} = G$ תמיד

$L^{\circ *} = L \iff k/L$ גלואה

<u>המשפט המרכזי של תורת גלואה:</u> תהי $k/F$ הרחבת גלואה. (= נורמלית + ספרבילית)

$G = Gal(k/F)$. אז ההתאמות $L \longmapsto L^\circ = Gal(k/L)$,

$k^H = H^* \longleftarrow H$

<u>הופכות זו את זו</u> ⊛ ובנוסף $|Gal(k/L)| = [k:L]$, $|H| = [k:k^H]$.

ההתאמות מהוות אנטי-איזומורפיזם של סריגים. ⊛

$L^{\circ *} = L$ | $k^{Gal(k/L)} = L$

$H^{*\circ} = H$ | $Gal(k/k^H) = H$

<u>הוכחה:</u> ברור שההתאמות הפכות סדר. יהי $L$ שדה ביניים של $F \subset K$

במשפט הקודם הוכחנו ש- $k$ שדה פיצול של פול' ספרבילי מעל $F$.

ברור ש- $k$ שדה פיצול של אותו פול' מעל $L$, כלומר $k/L$ גלואה.

קיבלנו שבמקרה זה $L^{\circ *} = L$ ($k^{Gal(k/L)} = L$).

תהי $H \le G$. לפי המסקנה מהלמה של ארטין $G^{*\circ} = G$ ($Gal(k/k^G) = G$).

השוויון $|H| = [k:k^H]$ הוא מסקנה של הלמה של ארטין.

השיוויון הקודם הוכחנו שכאשר $k/L$ גלואה, $L = k^H$ כאשר $H = Gal(k/L)$

ולכן $|Gal(k/L)| = [k:k^H] = [k:L]$.

**מסקנות:**

$$\begin{tikzcd}[column sep=small] & K \arrow[d, dash] & \\ & \cdot \arrow[dl, dash] \arrow[dr, dash] & \\ K^{H_1} \arrow[dr, dash] & & K^{H_2} \arrow[dl, dash] \\ & F & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & 1 \arrow[d, dash] & \\ & \cdot \arrow[dl, dash] \arrow[dr, dash] & \\ H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & \cdot \arrow[d, dash] & \\ & G & \end{tikzcd}$$

$$K^{\langle H_1, H_2\rangle} = K^{H_1} \cap K^{H_2}$$

$$K^{H_1\cap H_2} = K^{H_1}\cdot K^{H_2}$$

$$\begin{tikzcd}[column sep=small] & K \arrow[d, dash] & \\ & \cdot \arrow[dl, dash] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\ & \cdot \arrow[d, dash] & \\ & F & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & 1 \arrow[d, dash] & \\ & \cdot \arrow[dl, dash] \arrow[dr, dash] & \\ \cdot \arrow[dr, dash] & & \cdot \arrow[dl, dash] \\ & \cdot \arrow[d, dash] & \\ & G & \end{tikzcd}$$

$$\mathrm{Gal}(K/L_1\cap L_2) = \langle \mathrm{Gal}(K/L_1), \mathrm{Gal}(K/L_2)\rangle$$

$$\mathrm{Gal}(K/L_1L_2) = \mathrm{Gal}(K/L_1) \cap \mathrm{Gal}(K/L_2)$$

__דוגמה:__ $F=\mathbb{Q}$. נתבונן בפולינום $f(x)=x^4-7$.

נסמן $\alpha=\sqrt[4]{7}$. שורשי הפולינום הם $\alpha, i\alpha, -\alpha, -i\alpha$.

$\Leftarrow$ שדה הפיצול הוא $K=\mathbb{Q}[i,\alpha]=\mathbb{Q}[\alpha, i\alpha, -\alpha, -i\alpha]$

$\mathbb{Q} \underset{4}{\subseteq} \mathbb{Q}[\alpha] \underset{2}{\subseteq} \mathbb{Q}[\alpha, i] \Leftarrow [K:F]=8$.

$K/F$ הרחבת גלואה כי זה ש״פ של $f$ והוא ספרבילי.

$G=\mathrm{Gal}(K/F)\le S_4$ מסדר 8.

$$\begin{array}{l} \mathbb{R} \not\supseteq \mathbb{Q}[i,\alpha] \\ \qquad | \, 2 \\ \mathbb{R} \supseteq \mathbb{Q}[\alpha] \\ \mathbb{Q}[i] \quad | \, 4 \\ \quad {}^{2}\diagdown\ \mathbb{Q} \end{array}$$

נחפש אוטומורפיזמים: $\tau: \begin{array}{l}\alpha \mapsto \alpha \\ i \mapsto -i\end{array}$

לכל אוטו׳ $\mu$, $\mu(\alpha)\in\{\alpha, i\alpha, -\alpha, -i\alpha\}$

$\mu(i)\in\{i, -i\}$

המשך

לכן יש לכל היותר $4\cdot 2=8$ אוטו׳, אבל כבר ראינו את

האוטו׳, ולכן כל בחירה של $\mu(\alpha), \mu(i)$ מותרת.

$$\delta: \alpha \longmapsto i\alpha$$
$$i \longrightarrow i$$

קל לחשוב ש- $G=\langle \delta, \tau\rangle \cong ?$