14/11/13 בס״ד י״א כסלו תשע״ד

אלגברה מופשטת 3 - הרצאה מס' 5.

$$\begin{array}{c} K \\ | \\ F \hookrightarrow E \end{array}$$ ⇐ שדה הפיצול הוא יחיד.

$Gal(K/F) = \{$ אוטו' $K \to K$ שמשמרים את F איבר-איבר $\}$

$$|Gal(K/F)| = \underset{\text{הוכחנו}}{n^K_{F\le K}} \le [K:F]$$

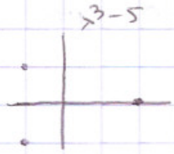
<u>דוגמה:</u> נניח $K=F[\alpha]$, כאשר α מאפס פולינום מינימלי f ב- $F[x]$.

הוכחנו למה שלפיה $|Gal(K/F)| = n^K_{F\le K} =$ מספר השורשים של f ב- K

<u>נשאל:</u> $|Gal(\mathbb{Q}[\sqrt[3]{5}]/\mathbb{Q})| = ?$

הפול' המינימלי של $\sqrt[3]{5}$ הוא x^3-5, לפול' זה יש שורש יחיד ב- $\mathbb{Q}[\sqrt[3]{5}]$ ולכן $|Gal(\mathbb{Q}[\sqrt[3]{5}]/\mathbb{Q})|=1$.

x^3-5



$$Gal(\mathbb{Q}[\rho_3, \underbrace{\sqrt[3]{5}}_{\alpha}]/\mathbb{Q}[\rho_3]) \cong \mathbb{Z}_3$$

השורשים: $\alpha, \rho\alpha, \rho^2\alpha$

האוטומורפיזמים מוגדרים ע״י:

$1: \alpha \mapsto \alpha$

$\sigma: \alpha \mapsto \rho\alpha$

$\sigma^2: \alpha \mapsto \rho^2\alpha$

$\circledast\ \sigma^2(\alpha) = \sigma(\rho\alpha) = \sigma(\rho)\sigma(\alpha) = \rho\cdot\rho\alpha = \rho^2\alpha$.

<u>משפט:</u> $|Gal(K/F)| \le [K:F]$ (כי $1 = n^K_{F\le K} \le [K:F]$)

<u>משפט:</u> אם K/F שדה הפיצול של פול' ספרבילי, $|Gal(K/F)| = [K:F]$

נניח ש- K שדה הפיצול של פול' f, כלומר $K=F[\alpha_1,\alpha_2,\dots,\alpha_n]$

כאשר α_i הם השורשים של f.

כל $\sigma \in Gal(K/F)$ משרה תמורה של השורשים, ומוגדר לפיה.

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

מספר השורשים של f ב- K.

<u>דוגמה:</u> $E=\mathbb{Q}[\rho,\alpha]$, $\alpha^3=5$, $\rho^2+\rho+1=0$.

$$\begin{tikzcd}[column sep=small] & E=\mathbb{Q}[\rho,\alpha] \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\ K=\mathbb{Q}[\rho] \arrow[dr, dash, "2"'] & & L=\mathbb{Q}[\alpha] \arrow[dl, dash, "3"] \\ & \mathbb{Q} & \end{tikzcd}$$

$Gal(K/\mathbb{Q})=\{1,\ \rho\to\rho^2\}\cong\mathbb{Z}_2$

שדה פיצול של x^2+x+1 השורשים ρ,ρ^2

נסמן ב- τ את האוטו' של E/L המוגדר ע"י $\rho\mapsto\rho^2$.

$Gal(E/K)$

$E=K[\alpha,\rho\alpha,\rho^2\alpha]$ (σ)

$Gal(E/K)\cong A_3$

E/K ש"פ של פו' ממעלה 3, המימד $=3$.

כמו, נתבונן ב- $E/\mathbb{Q}$:

השורשים של $x^3-\rho$ הם $\alpha,\rho\alpha,\rho^2\alpha$ ו- :

$$\mathbb{Q}[\alpha,\rho\alpha,\rho^2\alpha]=\mathbb{Q}[\rho,\alpha]$$

נסמן ב- σ את האוטו' המוגדר ע"י:

$\sigma:\alpha\longmapsto\rho\alpha$

$\sigma:\rho\longmapsto\rho$

$\sigma,\tau\in Gal(E/\mathbb{Q})\cong S_3$

(כי $|\,|=[E:\mathbb{Q}]=6$ ו- $Gal(\ )\le S_3$)

$\overset{1}{(\alpha},\overset{2}{\rho\alpha},\overset{3}{\rho^2\alpha})$ $\quad\sigma:\ \alpha\longmapsto\rho\alpha,\ \rho\longmapsto\rho\ \Rightarrow\ \sigma^3=1$

$(\overset{2}{\rho\alpha},\overset{3}{\rho^2\alpha})$ $\quad\tau:\ \alpha\longmapsto\alpha,\ \rho\longmapsto\rho^{-1}\ \Rightarrow\ \tau^2=1$

$$\left.\begin{array}{l}\sigma\tau:\ \alpha\longmapsto\rho\alpha,\ \ \rho\longmapsto\rho^{-1}\\ \tau\sigma:\ \alpha\longmapsto\rho^{-1}\alpha,\ \ \rho\longmapsto\rho^{-1}\end{array}\right\}\Rightarrow\tau\sigma=\sigma^{-1}\tau$$

<u>המטרה:</u> להבין את הקשר בין הרחבות ביניים של $K\supset F$ לבין תת"ח של $Gal(K/F)$

<u>הגדרה:</u> K/F הרחבה. $H\le Gal(K/F)$.

14/11/13 הרצאה 3 ספר תשע"ד

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

קרוי: שדה השבת של H

ברור ש- $F \le K^H \le K$, וזה שדה ביניים.

<u>התאמת גלואה:</u>

K
$|$
K_0 תת השדה הבסיסי

נסמן $\mathcal{F} = \{$ שדות הביניים של $K \}$, זה סדור עם יחס ההכלה.

$G = \{$ תת החבורות של $\begin{matrix} Aut(K) \\ '' \\ Gal(K/K_0) \end{matrix} \}$, זה סדור עם יחס ההכלה.

מגדירים התאמות $\mathcal{F} \underset{*}{\overset{\circ}{\rightleftarrows}} G$

$$F \longmapsto F^\circ = Gal(K/F)$$

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

$$\overset{''}{\{x\in K \mid \forall h\in H : h(x)=x\}}$$

<u>תכונות:</u>

(1) אם $F_1 \le F_2 (\le K)$ אז $F_2^\circ \le F_1^\circ$
אם $H_1 \le H_2 (\le Aut(K))$ אז $H_2^* \le H_1^*$
$*, \circ$ הופכות סדר הכלה.

(2) נניח $F \le K$. $F \subseteq \overset{F^{Gal(K/F)}}{\overset{''}{F^{\circ *}}}$

$H \le Aut(K)$. $H \subseteq \underset{Gal(K/K^H)}{\underset{''}{H^{*\circ}}}$

(3) מסקנה: $F^\circ \le (F^\circ)^{*\circ} \le F^\circ$ ⟸ $F^{\circ * \circ} = F^\circ$; $H^{*\circ *} = H^*$

$$F^{\circ *} \supseteq F$$

(4) $L^{\circ *} = L \iff L = H^*$ לאיזשהו H.

$H^{*\circ} = H \iff H = L^\circ$ לאיזשהו L.

<u>ניסוח מחדש:</u> (של סעיף (4))

- לכל חבורה אוטו' G של K,

$$Gal(K/K^G) = G \quad \text{(ארטין)}$$

$$\Updownarrow$$

G מהווה חבורת גלואה של K מעל $\underset{\text{משהו}}{\bullet}$ $= Gal(K/\cdot)$

- לכל תת - שדה $L \le K$,

המשך

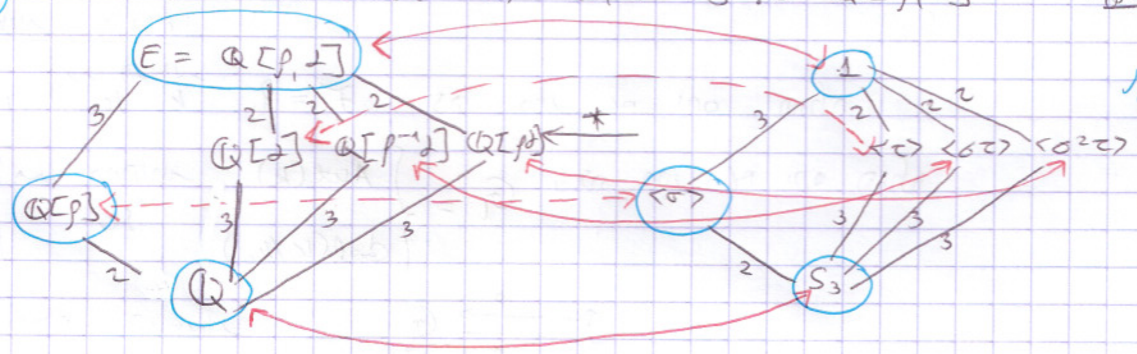
$$K \overset{Gal(K/L)}{} = L$$
$$\Updownarrow$$

L שדה שבת של תת כלשהו.

דוגמא: $E=\mathbb{Q}[\rho,\alpha]$. $Aut(E)=Gal(E/\mathbb{Q})=\langle\sigma,\tau\rangle\cong S_3$.

○ ← שדה ביניים מעל $\mathbb{Q}$

○ ← ת"ח של S_3



$\sigma:\alpha\mapsto\rho\alpha$, $\rho\mapsto\rho$	$\langle\sigma\rangle^{*}=\mathbb{Q}[\rho]$	נכתוב כל ב-E - כצירוף וקטורי מעל $\mathbb{Q}[\rho]$
$\tau:\alpha\mapsto\alpha$, $\rho\mapsto\rho^{-1}$	$E^{\sigma}=\mathbb{Q}[\rho]$	$f_0+f_1\alpha+f_2\alpha^2 \xmapsto{\sigma} f_0+\rho f_1\alpha+\rho^2 f_2\alpha^2$, $f_0,f_1,f_2\in\mathbb{Q}[\rho]$