21.11.13 בס״ד יח כסלו תשע״ד

אלגברה מופשטת 3 - הרצאה מס' 6.

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

קב' שדות של K — קב' חבורות של $Aut(K)$

הגבלה: במקום $\mathcal{F}, \mathcal{G}$ נרצה להסתכל על שדות הביניים:

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

שדות הביניים של K/F — תת' $\mathcal{G}$ של $Gal(K/F)$

מיון וסדר

$$K \overset{|L|}{—} L — F \qquad\qquad Gal(K/K)=1 \overset{|H|}{—} H — Gal(K/F)$$

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

אם $H_1 \le H_2 \Leftarrow |H_1| \le |H_2|$ ואם $|H_1| = |H_2|$ אז $H_1 = H_2$

$F \le L_1 \le L_2 \le K \Leftarrow |L_2| \le |L_1|$ ואם $|L_2| = |L_1|$ אז $L_1 = L_2$.

השבחנו מהמשפט: $n^K_{F\subset K} = |Gal(K/F)| \le [K:F]$

$$|F^\circ| \le |F| \quad \text{(כלו' "שקולי" מיון נגדל)}$$

נקבע הרחבה K/F.

נניח $F \le L \le K$

נאמר ש- L "נגדל" אם יש פולינום ספרבילי מעל L ש-K הוא שדה הפיצול שלו.

$K = L[\alpha_1, ..., \alpha_n]$	אם K שדה הפיצול של פול' ספרבילי f
L'	מעל L, אז K גם שדה הפיצול של f
L	מעל L' $f(x)\in L[x]$

⊛ ב״ש שדה המנורמל שדה גדול הוא גדול.

המשך אותו משפט: אם F גדול, $|F^\circ| \overset{⊛}{=} |F|$

מסקנה: אם F גדול, אז $F^{\circ *} = F$

$$\Updownarrow$$

$$[K^{Gal(K/F)} = F]$$

תזכורת: אם $H \le Gal(K/F)$

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

$$F \le K^H \le K$$

הערה: ברור ש- $F \le F^{\circ *}$

$$\downarrow$$

$$(\circ \text{ הופך הכלה}) \quad F^{\circ * \circ} \overset{⊛}{=} F^\circ$$

$$|F| \ge |F^{\circ *}|$$

הערה: לומר ש: יש פול ספרבילי מעל F שה-K הוא שדה הפיצול שלו שקול ל: $K^{Gal(K/F)}=F$

$|F| \geq |F^{\infty}|$

$\circledast\| \quad \|\circledast$

$\circledast |F^{0}| = |F^{\infty 0}|$

מכאן $|F|=|F^{\infty}|$ (כיוון שם הכלה) ולכן $F^{\infty}=F$.

הגדרה: ההרחבה E/F האלגברית נורמלית אם לכל $a\in E$, הפולינום המינימלי של a מתפצל (לגורמים לינאריים) ב-E.

(במילים אחרות: E מכיל שורש של כל פול מינימלי של איבר שלו).

הגדרה: הרחבה E/F ספרבילית אם הפולינום המינימלי של כל איבר $a\in E$ הוא ספרבילי.

(שקול לתנאי: לכל פול מינימלי הנגזרת $\neq 0$)

הערה: במאפיין 0 הכל ספרבילי

הגדרה: הרחבה נורמלית וספרבילית נקראת הרחבת גלואה.

משפט: התכונות הבאות של הרחבה סופית K/F שקולות:

(1) K/F הרחבת גלואה

(2) K הוא שדה הפיצול של פול ספרבילי מעל F.

(3) $F=K^{G}$ עבור G חבורת אוטו' כלשהי.

הוכחה:

$(1)\Rightarrow(*)$: יהי $S=\{a_1,...,a_n\}$ (קבוצת יוצרים) של K/F

$K=F(a_1,...,a_n)$

F

(נסמן ב-f_i את הפולינום המינימלי של a_i,

ונקח $f=$ מכפלת הפולינומים השונים בהשוואה $\{f_1,...,f_n\}$.

לפי "הנורמליות" כל f_i מתפצל ב-K ולכן f מתפצל.

לפי "הספרביליות" כל f_i ספרבילי ולכן f ספרבילי.

ברור ש-K הוא שדה הפיצול של f.

$(2)\Rightarrow(3)'$: מספיק ש-F עבור, הוכחנו ש- $K^{Gal(K/F)}=F$.

$F=K^{Gal(K,F)}$

כאשר: $(3)'=$:

ו- $(3)'\Rightarrow(3)$: ✓

$(3)\Rightarrow(1)$: יהי $a\in K$. יהי f הפול המינימלי של a (מעל F)

צ"ל ש-f

(נסמן ב- $a_1,...,a_t$ את השורשים השונים של f ב-K

נתבונן בפול׳ $g(x)=\prod_{i=1}^{t}(x-a_i)$

ברור ש- $g|_{K} f$.

המקדמים של g הם פולינומים סימטריים במספרים $a_1,\dots,a_t$:

$$g(x)=\sum_{k=0}^{t}(-1)^k\cdot\Big(\sum_{1\le i_1\le\dots\le i_k} a_{i_1}\cdot\dots\cdot a_{i_k}\Big)\cdot x^{t-k}$$

יהי $\sigma\in G$. המספרים $\sigma(a_1),\dots,\sigma(a_t)$ הם שורשים של f ולכן

$\{\sigma(a_1),\dots,\sigma(a_t)\}=\{a_1,\dots,a_t\}$ ומכאן ש- σ שומר כל

מקדם של g .

במילים אחרות, $g\in K^{\sigma}[x]$.

$\Leftarrow$ $g\in K^{G}[x]=F[x]$.

אבל f אי-פריק ולכן $g=f$ $\Leftarrow$ $t=\deg g=\deg f$

לכן f מתפצל וספרבילי.

<u>מסקנה:</u> K/F הרחבת גלואה (1) $\Leftrightarrow$ $K^{Gal(K/F)}=F$ (3)' $\Leftrightarrow$ $|Gal(K/F)|=[K:F]$ (2) ⊛

⊛<u>הערה:</u> הכיוון היחידי שטרם הוכחנו הוא:

$$K^{Gal(K/F)}=F \Leftarrow |Gal(K/F)|=[K:F]$$

$$(F^{\circ *}=F \Leftarrow |F^{\circ}|=|F|)$$

מכיוון ש- $F^{\circ *}$ הוא שדה שמכיל, אז לפי $(2)\Leftarrow(3)$ במשפט,

$F^{\circ *}$ שדה סגור ולכן $|F^{\circ *}|=|F^{\circ *\circ}|$

וכן שמירה מעגלית $|F^{\circ *\circ}|=|F^{\circ}|$ ומההנחה מעגלית $|F^{\circ}|=|F|$

קיבלנו כנדרש $|F^{\circ *}|=|F|$

<u>סיכום של סוף המשפט</u>

לכל $H\le Gal(K/F)$

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

(H^{*} שדה סגור לפי המשפט,
$((2)\Leftarrow(3))$

$H=L^{\circ}$

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

לכל שדה L ,

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

$L\subseteq L^{\circ *}$

מסקנה

<u>דוגמה:</u> $K=\mathbb{Q}[\sqrt[3]{2}]$ אם $F=\mathbb{Q}$;

$$F^\circ = 1$$

$$1 = |F^\circ| < |F| = 3$$

⇐ כי לא הרחבה שלווה, מכיוון איבר $\sqrt[3]{2}$ שהפול המינימלי שלו

לא מתפצל לגורמים ליניאריים (⇐ הרחבה לא נורמלית)

<u>למה:</u> נניח $F = K^G$

$G \subseteq End_F(K)$ תת קבוצה של K.

(אוטומ' G)

[$End_F(K)$ מרחב וקטורי מעל K: $(aT)(x) = a \cdot T(x)$]

$End_F(K) = Hom(K,K) \cong M_n(F)$	
$\sigma \in End_F(K)$	$\sigma \in Gal(K/F)$
$\sigma(a+b) = \sigma(a)+\sigma(b)$	בנוסף
$\sigma(\alpha a) = \alpha\sigma(a)$	$\sigma(ab) = \sigma(a)\sigma(b)$
	$\sigma(\alpha) = \alpha$
	לכל $\alpha \in F$

טענה: אם $\sigma_1, \dots, \sigma_n \in G$ שונים ו-:

$a_1, \dots, a_n \in K$ עם

$$\forall x \in K: \sum a_i \sigma_i(x) = 0$$

אז $a_1 = \dots = a_n = 0$

<u>הוכחה:</u> אחרת נבחר צירוף ליניארי לא טריוויאלי קצר ביותר.

כלומר $\sum a_i \sigma_i = 0$ ~~אפשר לחלק ב-a_1~~ ולהרכיב ב-σ_1^{-1} משמאל ומימין.

(כלומר, אפשר להניח $\sigma_1 = 1$. לכן $\sigma_2 \neq 1$.

לכן יש $t \in K$ כך ש- $\sigma_2(t) \neq t$.

$$\sum a_i \sigma_i(t)\sigma_i(x) = 0 \xleftarrow{x \mapsto tx} \sum a_i \sigma_i(x) = 0$$

$$\xleftarrow{t}$$

$$\sum a_i t \sigma_i(x) = 0$$

$$\sum a_i(\sigma_i(t) - t)\sigma_i = 0$$

זה צירוף ליניארי יותר קצר מהנתון, בסתירה להנחה.

$$\Leftarrow) \quad |G| \leq [K : K^G]$$

$$|G| \leq |G^*|$$ (זוכרים את זה..)

=