

אלגברה ב' 2 – הרצאה 14

6.4.11

משפט. המשפט היסודי של תורת גלואה תהי L/K הרחבת גלואה וניח שהיא סופית (לפרות שיהיו חלקים מהמשפט שיהיו נכונים גם לאינסופיות). נסמן $G = \text{Gal}(L/K)$. נגדיר שתי קבוצות:

$$E \mapsto \text{Gal}(L/E) \text{ היא העתקה}$$

$$\{E \mid H \leq G \mid \text{תת חבורה } H\} \rightarrow \{E \mid K \subseteq E \subseteq L, \text{ שדה } E\}$$

ההעתקה הזאת חח"ע ועל (התאמה חח"ע) וההעתקה ההפוכה נתונה ע"י $H \mapsto L^H$.

במילים אחרות $L^{\text{Gal}(L/E)} = E$ וכן, $\text{Gal}(L/L^H) = H$.

הוכחה. שתי ההעתקות מוגדרות היטב. באמת אם ניקח שדה E אז כל האוטומורפיזמים ששומרים על E שומרים גם על K . להפך אם ניקח תת חבורה H אז שדה השבת יכיל את K . נשים לב שאם L/K הרחבת גלואה אז גם L/E הרחבת גלואה (כי היו משפטים שזאת הרחבה נורמלית ופרידה).

$\text{Gal}(L/L^H) = H$ נובע מהלמה של ארטין (שם הניסוח אפילו חזק יותר). אצלנו G ו- H סופיות.

טענה. תהי L/E גלואה. אז $L^{\text{Gal}(L/E)} = E$ (גם אם אינה סופית).

הוכחה. ההכלה $\supseteq$ ברורה: $L^{\text{Gal}(L/E)} = \{\alpha \in L : \forall \sigma \in \text{Gal}(L/E) \sigma(\alpha) = \alpha\} \supseteq E$. יהי $\alpha \in L^{\text{Gal}(L/E)}$. אז ניקח $\tilde{E}$ סגור אלגברי של E שמיל את L . כל $\sigma_0 \in \text{Isom}_E(E(\alpha), \tilde{E})$ ניתן להרחיב לאוטומורפיזם של הסגור האלגברי. בפרט אפשר לצמצם ל- L . כלומר ניתן להרחבה ל- $\sigma \in \text{Isom}_E(L, \tilde{E})$. אבל L הרחבה נורמלית לכן כל אוטומורפיזם מעליו משבית אותו ולכן $\text{Isom}_E(L, \tilde{E}) = \text{Gal}(L/E)$. לפי ההנחה $\sigma(\alpha) = \alpha$ ו- $\sigma_0(\alpha) = \alpha$ (זאת אותה ההעתקה). לכן כל אוטומורפיזם σ_0 הוא זהות על $E(\alpha)$. מכאן $[E(\alpha) : E]_S = 1$. אבל $E(\alpha)/E$ פרידה כי L/E פרידה ולכן כל הרחבה שלה פרידה, לכן $[E(\alpha) : E] = [E(\alpha) : E]_S = 1$. כלומר $E(\alpha) = E$. כלומר $\alpha \in E$. $\square$

$\square$

הערה. החלק של $\text{Gal}(L/L^H) = H$ נכון גם עבור L/K אינסופית בתנאי ש- H תת חבורה סגורה (= חיתוך של תת חבורות בעלות אינדקס סופי ב- $\text{Gal}(L/K)$).

הערה. אם L/K הרחבה סופית אז הסגור הנורמלי של M/K גם סופית. אכן, $L = K(\alpha_1, \dots, \alpha_n)$ אלגבריים מעל K . יהי M' שדה הפיצול של M/K . אז $F = \{\text{irr}(\alpha_i, K) : i = 1, \dots, n\}$ נוצר מעל K ע"י מספר סופי של איברים אלגבריים (השורשים של איברי F). לכן, M'/K סופית. כמו כן $K \subseteq L \subseteq M'$. בפרט, M/K סופית. נורמלית לכן $M \subseteq M'$ (למעשה אפילו $M = M'$). $\square$

מסקנה. להרחבה פרידה סופית L/K יש רק מספר סופי של שדות ביניים $K \subseteq E \subseteq L$ (כלומר).

הוכחה. יהי M סגור גלואה של L/K . אז M/K סופית ודי להוכיח של- M/K רק מספר סופי של שדות ביניים. לפי המשפט היסודי של תורת גלואה יש התאמה חח"ע ועל בין שדות הביניים של L/K לבין תת החבורות של חבורת גלואה $\text{Gal}(M/K)$. אבל $\text{Gal}(M/K)$ סופית לכן יש לה רק מספר סופי של תת חבורות. $\square$

משפט. תהי L/K הרחבת גלואה (לאו דווקא סופית) ניקח $K \subseteq E_1, E_2 \subseteq L$ אז

$$1. E_1 \supseteq E_2 \Leftrightarrow \text{Gal}(L/E_1) \leq \text{Gal}(L/E_2)$$

2. אם L/K סופית, $\langle \text{Gal}(L/E_1), \text{Gal}(L/E_2) \rangle = \text{Gal}(L/E_1 \cap E_2)$.
כאשר $\langle \text{Gal}(L/E_1), \text{Gal}(L/E_2) \rangle$ החבורה הקטנה ביותר שמכילה את שתי החבורות.

$$3. \text{Gal}(L/E_1 E_2) = \text{Gal}(L/E_1) \cap \text{Gal}(L/E_2)$$

הוכחה. נסמן $G = \text{Gal}(L/K)$, $G_i = \text{Gal}(L/E_i)$, $i = 1, 2$. וכן מהטענה מהמשפט היסודי $L^{G_i} = E_i$, $i = 1, 2$.

$$1. \Rightarrow: \text{מההגדרה.} \Leftarrow: \text{צ"ל } L^{G_1} \supseteq L^{G_2} \Rightarrow G_1 \leq G_2. \text{ שוב מההגדרות.}$$

$$2. \supseteq: \text{Gal}(L/E_1 \cap E_2) \geq \text{Gal}(L/E_i), i = 1, 2 \text{ ואז לפי סעיף קודם.}$$

$\subseteq$: נסמן $H := \langle \text{Gal}(L/E_1), \text{Gal}(L/E_2) \rangle$. $G_1, G_2 \leq H$, לכן לפי הסעיף הקודם $L^H \subseteq L^{G_1}, L^{G_2}$. כלומר $L^H \subseteq E_1, E_2$ לכן $L^H \subseteq E_1 \cap E_2$. לכן שוב לפי הסעיף הראשון והלמה של אקטיין (כאן משתמשים בסופיות) $H = \text{Gal}(L/L^H) \geq \text{Gal}(L/E_1 \cap E_2)$.

3. $\subseteq$: $E_i \subseteq E_1 E_2$ לכן, לפי הסעיף הראשו $\text{Gal}(L/E_1 E_2) = \text{Gal}(L/E_i)$, $i = 1, 2$ ולכן מוכלת בחיתוך.

$\supseteq$: יהי $\sigma \in \text{Gal}(L/E_1) \cap \text{Gal}(L/E_2)$. לכן $\sigma(\alpha) = \alpha$ לכל $\alpha \in E_1 \cup E_2$. אז $E_1 E_2 = \{ \frac{g(\beta)}{g(\beta)} : f, g \in E[x], g(\beta) \neq 0, \beta \in E_2 \}$ כי $\alpha \in E_1 E_2$ לכל $\sigma(\alpha) = \alpha$ לכן $\sigma \in \text{Gal}(L/E_1 E_2)$.

$\square$

למה. תהי L/K הרחבת גלואה. $K \subseteq E \subseteq L$, $\sigma \in \text{Gal}(L/K)$. אם $K \subseteq \sigma(E) \subseteq L$ אז $\text{Gal}(L/\sigma(E)) = \sigma \text{Gal}(L/E) \sigma^{-1}$.

הוכחה. $K = \sigma(K) \subseteq \sigma(E) \subseteq \sigma(L) = L$.

$$\begin{aligned} \text{Gal}(L/\sigma(E)) &= \{ \tau \in \text{Aut}(L) : \forall \alpha \in E \tau(\sigma(\alpha)) = \sigma(\alpha) \} = \\ &= \{ \tau \in \text{Aut}(L) : \forall \alpha \in E \sigma^{-1} \tau \sigma(\alpha) = \alpha \} = \\ &= \{ \tau \in \text{Aut}(L) : \sigma^{-1} \tau \sigma \in \text{Gal}(L/E) \} = \\ &= \{ \tau \in \text{Aut}(L) : \tau \in \sigma \text{Gal}(L/E) \sigma^{-1} \} = \\ &= \sigma \text{Gal}(L/E) \sigma^{-1} \end{aligned}$$

$\square$

משפט. תהי L/K גלואה, $K \subseteq E \subseteq L$ אזי

1. E/K נורמלית (ולכן גלואה) $\Leftrightarrow \text{Gal}(L/E) \triangleleft \text{Gal}(L/K)$ (תת חבורה נורמלית).

2. אם E/K נורמלית אז ההעתקת הצמצום $\sigma \mapsto \sigma|_E$ שהיא העתקה $\text{Gal}(L/K) \rightarrow \text{Gal}(E/K)$ היא אפימורפיזם של חבורות. הגרעין הוא $\text{Gal}(L/E)$ ולכן (מפשט האיזומורפיזם הראשון) מתקיים:

$$\text{Gal}(L/K)/\text{Gal}(L/E) \cong \text{Gal}(E/K)$$

הוכחה. נניח בה"כ $K \subseteq E \subseteq L \subseteq \tilde{K}$ הסגור האלגברי של K . נעבוד בתוכו.

1. E/K נורמלית $\Leftrightarrow \sigma_0(E) = E \Leftrightarrow \sigma_0 \in \text{Ism}_K(E, \tilde{K})$ לכל $\sigma_0 \in \text{Gal}(E/K)$ (לפי ההגדרה) $\Leftrightarrow \sigma_0 \in \text{Ism}_K(K, \tilde{K}) = \text{Gal}(L/K)$ לכל E (כאשר σ למעשה הרחבה של σ_0) $\Leftrightarrow \text{Gal}(L/\sigma(E)) = \text{Gal}(L/E)$ לכל $\sigma \in \text{Gal}(L/K)$ (לפי הלמה הקודמת) $\Leftrightarrow \sigma \in \text{Gal}(L/K)$ לכל $\sigma \text{ Gal}(L/E)\sigma^{-1} = \text{Gal}(L/E)$ $\Leftrightarrow \text{Gal}(L/E) \triangleleft \text{Gal}(L/K) \Leftrightarrow \sigma \in \text{Gal}(L/K)$.

2. רוצים להוכיח $(\sigma_1\sigma_2)|_E = \sigma_1|_E\sigma_2|_E$ כלומר $(\sigma_1\sigma_2)|_E(\alpha) = \sigma_1|_E(\sigma_2|_E(\alpha))$ לכל $\alpha \in E$.

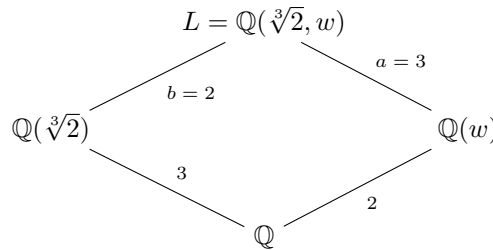
זה שקול לשאלה האם לכל $\alpha \in E$ $(\sigma_1 \circ \sigma_2)(\alpha) = \sigma_1(\sigma_2(\alpha))$ וזה אכן נכון. לכן $\sigma \mapsto \sigma|_E$ הומומורפיזם. הוא על כי כל $\sigma_0 \in \text{Gal}(E/K) = \text{Ism}_K(E, \tilde{K})$ ניתן להרחבה לאוטומורפיזם φ על $\tilde{K}$ וצמצומו ל- L הוא $\sigma \in \text{Ism}_K(L, \tilde{K})$. הגרעין הוא $\{\sigma \in \text{Gal}(L/K) : \sigma|_E = id|_E\} = \text{Gal}(L/E)$ מכאן נותר רק להפעיל את משפט האיזומורפיזם הראשון.

□

דוגמא. יהי L שדה פיצול של $f = x^2 - 2$ מעל $\mathbb{Q}$ (f א"פ לפי קריטריון איזנשטיין). אז $L/\mathbb{Q}$ הרחבת גלואה. מתקיים:

$$f = (x - \sqrt[3]{2})(x - \sqrt[3]{2}w)(x - \sqrt[3]{2}w^2)$$

כאשר w שורש שלישי של 1. (כלומר $w^3 = 1, w \neq 1$ ולמשל $w = e^{2\pi i/3}$). לכן w שורש של $x^3 - 1 = (x - 1)(x^2 + x + 1)$ לכן $\text{irr}(w, \mathbb{Q}) = x^2 + x + 1$. לכן מתקיים $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2) = \mathbb{Q}(\sqrt[3]{2}, w)$.

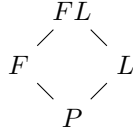


אנו יודעים $a \leq 3$ כי יש פולינום מסדר 3 ב- $\mathbb{Q}(w)$ ש- $\sqrt[3]{2}$ שורש שלו. מאותה סיבה $b \leq 2$ ולכן משיקולי גדלים (2, 3) זרים $a = 3, b = 2$. לכן $[L : \mathbb{Q}] = 6$. לכן

$$\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \text{ או } S_3$$

אולם $\text{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) \leq \text{Gal}(L/\mathbb{Q})$ בעלת סדר 2 איננה נורמלית כי $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ אינה נורמלית (אחרת f היה מתפצל מעל $\mathbb{Q}(\sqrt[3]{2})$) לכן $\text{Gal}(L/\mathbb{Q}) \not\cong \mathbb{Z}_6$ ואז $\text{Gal}(L/\mathbb{Q}) \cong S_3$.
 חוץ מזה גם $\text{Gal}(L/\mathbb{Q}(w)) \cong A_3$.

משפט. תהי L/K הרחבת גלואה, F/K הרחבה כך ש- F, L מוכלים בשדה משותף. אזי:



1. FL/F גלואה.

2. קיים איזומורפיזם $\text{Gal}(FL/F) \rightarrow \text{Gal}(L, F \cap L)$ ע"י $\sigma \mapsto \sigma|_L$.

הוכחה.

1. ראינו כבר.

2. בה"כ נניח $F \cap L = L$ (אחרת נחליף את $L \cap F$ ב- K). יהי C סגור אלגברי של FL ויהי $\tilde{K}$ הסגור האלגברי של K בתוך C . $\tilde{K} = \{\alpha \in C : \alpha \text{ אלגברי מעל } K\}$.
 בפרט $L \subseteq \tilde{K}$. יהי $\sigma \in \text{Gal}(FL/F)$ אזי $\sigma|_F = id|_F$ כמו כן $K \subseteq F$ ולכן $\sigma|_K = id|_K$.

$$\sigma(L) \subseteq \sigma(FL) = FL \subseteq C$$

אולם $\sigma(L)$ הרבחה אלגברית של $\sigma(K) = K$ כי L/K אלגברית, לכן $\sigma(L) \subseteq \tilde{K}$.
 אולם L/K נורמלית לכן $\sigma(L) = L$. לכן $\sigma|_L \in \text{Gal}(L, K)$. קל לראות כי זה הומומורפיזם ומתקיים:

$$\begin{aligned} \ker &= \{\sigma \in \text{Gal}(FL/F) : \sigma|_F = id|_F, \sigma|_L = id|_L\} = \\ &= \{\sigma|_{FL} : \sigma|_F = id|_F, \sigma|_L = id|_L\} = \{1\} \end{aligned}$$

□