

אלגברה ב' 2 – הרצאה 13

4.4.11

בשיעור הקודם ראינו את השדה $K_n = \{\alpha \in \tilde{K} \mid \alpha^{q^n} = \alpha\}$ וזאת הרחבה יחידה ממעלה n של K .

משפט.

1. K_n/K נורמלית. K_n שדה הפיצול של $f = X^{q^n} - X$.

2. K_n/K פרידה כי f פריד ($f' = 1$).

הוכחה – תרגיל.

תורת גלואה

K שדה, $\tilde{K}$ סגור אלגברי.

הגדרה. הרחבה L/K נקראת גלואה אם היא אלגברית, נורמלית וגם פרידה.

דוגמאות.

1. כל הרחבה ריבועית מעל שדה בעל אפיון 0 (כדי שתהיה פרידה).

2. K_n/K .

3. $\tilde{K}/K$ אם K מושלם.

הגדרה. תהי L/K גלואה. קבוצת כל אוטומורפיזמים K של L היא חבורה (ביחס להרכבה). זאת נקראת חבורת גלואה של L/K ותסומן $\text{Gal}(L/K)$. בה"כ $L \subseteq \tilde{K}$ ואז

$$\text{Gal}(L\tilde{K}) = \text{Ism}_K(L, \tilde{K})$$

משפט. אם L/K גלואה סופית אז $|\text{Gal}(L/K)| = [L : K]$.

וראינו אותו אבל במילים קצת אחרות.

דוגמא. $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \varepsilon\}$ כאשר $\varepsilon(\sqrt{2}) = -\sqrt{2}$. כלומר, $\varepsilon(a, b\sqrt{2}) = a - b\sqrt{2}$. ואכן, $a, b \in \mathbb{Q}$. $f = x^2 - 2 \in \mathbb{Q}[x]$. כל $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ מעתיק שורש $\sqrt{2}$ של f לשורש של f . לכן, $\sigma(\sqrt{2}) = \pm\sqrt{2}$. למדנו שיש הומומורפיזם-יחיד $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ כך ש- $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{2}) = \sqrt{2}$.

משפט. תהי L/K הרחבה אלגברית $L \subseteq \tilde{K}$. אז קייפת הרחבה אלגברית נורמלית קטנה ביותר M/K כך ש- $L \subseteq M \subseteq \tilde{K}$. אם L/K פרידה אז M/K גלואה.

הוכחה. תהי $F = \{\text{irr}(\alpha, K) : \alpha \in K\}$ משפחה של פולינומים. יהי M שדה הפיצול של F בתוך $\tilde{K}$. אז M/K נורמלית. אם M'/K נורמלית, $L \subseteq M' \subseteq \tilde{K}$ אז כל $f \in F$ מתפצל מעל M' לכן $M \subseteq M'$.

נניח L/K פרידה, אז כל $f \in F$ פריד. נתבונן במשפחה $\{F_i\}$ של כל תת הקבוצות הסופיות של F . לכל F_i יהי $M_i \subseteq \tilde{K}$ שדה הפיצול של F_i . מכאן ברור ש- $M_i \subseteq M$. אבל M_i/K נוצר מעל K ע"י מספר סופי של איברים פרידים (שורשים של איברי F) לכן M_i/K פרידה ממשפט.

קל לראות ש- $\bigcup_i M_i$ שדה (כי כל שניים מוכלים בשדה שלישי במשפחה) לכן $M = \bigcup_i M_i$. לכן M/K פרידה כי איבר של M הוא איבר של איזהו M_i ולכן פריד. $\square$

הגדרה. M כנ"ל נקרא הסגור הנורמלי של L/K (בתוך $\tilde{K}$).

הגדרה. אם L/K פרידה אז M כנ"ל נקרא סגור גלואה של L/K .

תרגיל. תהי L/K פרידה ויהי $n \in \mathbb{N}$ כך ש- $[K(\alpha) : K] \leq n$ לכל $\alpha \in L$. אז L/K סופית וכן $[L : K] \leq n$.

הוכחה. נניח בשלילה ש- $[L : K] > n$. אז יש $\alpha_1, \dots, \alpha_{n+1} \in L$ בת"ל מעל K . לפי משפט האיבר הפרימיטיבי קיים $\alpha \in L$ כך ש- $K(\alpha_1, \dots, \alpha_{n+1}) = K(\alpha)$. לפי הנתון $[K(\alpha) : K] \leq n$ סתירה כי $\alpha_1, \dots, \alpha_{n+1} \in K(\alpha)$. $\square$

הגדרה. יהי L שדה ו- H חבורת אוטומורפיזמים של L .

$$L^H := \{\alpha \in L : \forall \sigma \in H \sigma(\alpha) = \alpha\}$$

זה תת שדה של L ונקרא לו שדה השבת בתוך L .

למה. הלמה של Artin יהי L שדה, H חבורה סופית של אוטומורפיזמים של L . יהי $E = L^H$. אז L/E הרחבת גלואה סופית ו- $\text{Gal}(L/E) = H$.

הוכחה. ניקח $\alpha \in L$. נבחר $\sigma_1, \dots, \sigma_r \in H$ כך ש- $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ הם כל האיברים השונים של $\{\sigma(\alpha) : \sigma \in H\}$. בה"כ $\sigma_1 = \text{id}$. יהי $\tau \in H$ אז $\tau(\sigma_1(\alpha)), \dots, \tau(\sigma_r(\alpha))$ הם כל האיברים השונים של $\{\sigma(\alpha) : \sigma \in H\}$ לכן שתי הסדרות הבאות שוות עד כדי הסדר: $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ ו- $\tau(\sigma_1(\alpha)), \dots, \tau(\sigma_r(\alpha))$. לכן אם נגדיר:

$$f = \prod_{i=1}^r (x - \sigma_i(\alpha)) \in L[x]$$

ולכל $\tau \in H$ נסמן τf הפולינום שמתקבל ע"י הפעלת τ על מקדמי f . אז:

$$\tau f = \prod_{i=1}^r (x - \tau(\sigma_i(\alpha))) = f$$

לכן $f \in E[x]$. מתקיים $f(\alpha) = 0$. $\text{irr}(\alpha, E) | f$.

1. ל- f אין שורשים מרובים ב- $\tilde{K}$.

2. f מתפצל מעל L .

3. $|E(\alpha) : E| = \deg \text{irr}(\alpha, E) \leq \deg f = r \leq |H|$.

לפי הסעיף הראשון ל- $\text{irr}(\alpha, E)$ אין שורשים מרובים ב- $\tilde{K}$ לכן α פריד מעל E לכן L/E פרדיה. לפי 2 $\text{irr}(\alpha, E)$ מתפצל מעל L לכן L/E נורמלית לכן L/E גלואה. לפי התרגיל $[L : E] \leq |H|$. אבל $|\text{Gal}(L/E)| = [L : E]$ ומצד שני $H \leq \text{Gal}(L/E)$ תת חבורה ולכן $H = \text{Gal}(L/E)$. $\square$