

אלגברה ב' 2 – תרגול 8

2.5.11

חבורת גלואה של פולינום

שאלה. מצאו את חבורת גלואה של $f = (x^3 - 3)(x^3 - 2) \in \mathbb{Q}[x]$.

תשובה. באופן כללי ל- $f \in K[x]$ פולנום מתוקן, אם $A = \{\alpha_1, \dots, \alpha_n\} \subseteq \tilde{K}$ השורשים (השונים כי פריד) של f אז $L = K(A)$, L/K גלואה, והצמצום $\sigma \mapsto \sigma|_A$ מגדיר הומומורפיזם חח"ע $\text{Gal}(L/K) \rightarrow S(A)$ ותמונתו $\text{Gal}(f, K)$ זו החבורה המבוקשת. נסמן $F = \mathbb{Q}(\zeta)$, $L_1 = F[\sqrt[3]{2}]$, $L_2 = F[\sqrt[3]{3}]$, $L_2 = F[\sqrt[3]{3}]$, $\mathbb{C} \ni \zeta^3 = 1$, $\zeta \neq 1$. אז L שדה הפיצול של f מעל $\mathbb{Q}$ (ב- $\mathbb{C}$) הוא $L = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{3}, \zeta] = L_1 L_2$. תהי $G = \text{Gal}(L/\mathbb{Q})$. מתקיים $L_1 \cap L_2 = F$: כמו שהראינו בתרגול על הרחבות פרידות, מראים ש- $\sqrt[3]{3}$ נמצא ב- $L_2 \setminus L_1$ ולכן יש לנו את השרשרת $F \subseteq L \cap L_2 \subsetneq L_2$. אבל $[L_2 : F] = 3$ (ואז נקבל ש- $[L_1 \cap L_2 : F] = 1 \vee 3$ כי $[L_1 \cap L_2 : F] = 1 \vee 3$ ואם 3 אז יש שוויון). זה נכון כי $L_2 = \mathbb{Q}[\sqrt[3]{3}, \zeta]$, אלגברי - $\mathbb{Q}$ ממעלה 3, ζ אלגברי - $\mathbb{Q}$ ממעלה 2, לכן, $[L_1 \cap L_2 : F] = 3$, $[F : \mathbb{Q}] = 2$, $[L_2 : \mathbb{Q}] = 6$.

לכן $[L_1 \cap L_2 : F] = 1$.

כעת, האם L_i/F הרחבות גלואה? (כן כי למשל L_2 זה שדה פיצול של $x^3 - 3$ מעל $\mathbb{Q}$ אז $\mathbb{Q} \subseteq F \subseteq L_2$ לכן L_2/F גלואה). ממשפט בשיעור ההעתקה $(\sigma|_{L_1}, \sigma|_{L_2})$ היא איזומורפיזם

$$H = \text{Gal}(L/F) = \text{Gal}(L_1 L_2/F) \cong \text{Gal}(L_1/F) \times_{\text{Gal}(L_1 \cap L_2/F)} \text{Gal}(L_2/F)$$

כאשר $\pi_i : G_i \rightarrow G_0$ עבור $G_1 \times_{G_0} G_2 = \{(\sigma_1, \sigma_2) \in G_1 \times G_2 : \pi_1(G_1) = \pi_2(G_2)\}$ הומומורפיזם.

כאן, $H \cong \text{Gal}(L_1/F) \times \text{Gal}(L_2/F) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, לכן, $\text{Gal}(L_1 \cap L_2/F) = \{1\}$. מהשרשרת $\mathbb{Q} \subseteq F \subseteq L$, $[F : \mathbb{Q}] = 2$, $[L : F] = 9$, כמו הגודל של H , לכן $G = \text{Gal}(L/\mathbb{Q})$ מסדר 81 וכמובן $H \triangleleft G$ כי $[G : H] = 2$. יש $\sigma \in G$ מסדר 2 (כי $\langle \sigma \rangle$ חבורת 2-סילו) אז $|H\langle \sigma \rangle| = 18$, $H \cap \langle \sigma \rangle = \{e\}$ (במקרה כזה מסמנים: $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \rtimes \mathbb{Z}_2$). כאשר $\rtimes$ מסמן מכפלה חצי ישרה, $G = H\langle \sigma \rangle$. מכיוון ש- $\sigma \in G$ נקבע ע"י $a \in \{1, 2\}$ ו- ζ_1, ζ_2 כך ש- $\zeta_1^3 = \zeta_2^3 = 1$,

$$\sigma = \sigma_{a, \zeta_1, \zeta_2}$$

$$\sigma(\zeta) = \zeta^a$$

$$\sigma(\sqrt[3]{2}) = \zeta_1 \sqrt[3]{2}$$

$$\sigma(\sqrt[3]{3}) = \zeta_2 \sqrt[3]{3}$$

יש 18 אפשרויות לכן אלה כולן. $\sigma_{1,\zeta,1}, \sigma_{1,1,\zeta} \in H$ עבור $\zeta \neq 1$ (כי הם משאירים את F במקום) $\sigma_{2,1,1} \in G \setminus H$. נמספר את השורשים

$$1 : \sqrt[3]{2}, \quad 2 : \zeta \sqrt[3]{2}, \quad 3 : \zeta^2 \sqrt[3]{2}, \quad 4 : \sqrt[3]{3}, \quad 5 : \zeta \sqrt[3]{3}, \quad 6 : \zeta^2 \sqrt[3]{3}$$

$$\sigma_{1,1,\zeta} = (4, 5, 6)$$

$$\sigma_{1,\zeta,1} = (1, 2, 3)$$

$$\sigma_{2,1,1} = (2, 3)(5, 6)$$

3 התמורות האלה יוצרות את $\text{Gal}(f, \mathbb{Q})$ כתת חבורות של S_6 .

שאלה. יהי p ראשוני, K שדה עם $\text{char } K = 0$ כך שכל הרחבה סופית (בפרט אלגברית) לא טריוויאלית של K היא ממעלה שמתחלקת ב- p . אז לכל הרחבה סופית של K יש $r \geq 0$ כך שזוהי הרחבה ממעלה p^r .

הערה. האם בכלל יש שדות כאלה? כן, למשל ל- $K = \mathbb{R}$ עם $p = 2$.

תשובה. הרעיון הוא לקחת הרחבה ולשכן אותה בהרחבת גלואה. תהי L/K הרחבה סופית, יש E כך ש- $K \subseteq L \subseteq E$ גלואה (ממשפט האיבר הפרימיטיבי $L = K(\alpha)$ עבור α אלגברי, ניקח את E להיות שדה פיצול של הפולינום האי פריק של α מעל K , E/K פרידה כי $\text{char } K = 0$).

בעצם, מתקיים $[L : K][E : K] = |G|$. לכן, די להוכיח כי $[E : K] = p^r$. תהי $G = \text{Gal}(E/K)$. תהי $H < G$ תת חבורה p -סילו (אם $L \subsetneq E$ אז $|G|$ אינו p -סילי כי $K \subsetneq E$ הרחבה לא טריוויאלית ומהנתון. ואז $H \neq \{1\}$. נתבונן בשרשרת $K \subseteq E^H \subseteq E$.

$$\underbrace{[E : K]}_{|G|} = \underbrace{[E : E^H]}_{|H|} [E^H : K]$$

לכן $[E^H : K] = [G : H]$. אבל $[E^H : K]$ זר ל- p (מהגדרת חבורת p -סילו $([G : H], p) = 1$) לכן מהנתון על K , $E^H = K$ ואז $|G| = |H| = p^r$.

שאלה. מצאו את חבורת גלואה של $x^4 - 7 \in \mathbb{Q}[x]$.

תשובה. בתרגיל 6 ששאלה 3 פתרנו את השאלה. אבל שם הפתרון היה טכני. חישבנו שמימד שדה הפיצול $\mathbb{Q} < L$ הוא 8. כעת, $S_4 > G = \text{Gal}(L/\mathbb{Q})$, $|G| = 8$ זו חבורת 2 - סילו של S_4 . כל חבורות p -סילו צמודות, בפרט איזומורפיות לכן $G \equiv \langle (1, 2, 3, 4), (1, 2)(3, 4) \rangle$.