

אלגברה ב2

© ארזים

26 באפריל 2017

לעיתים נסמן פונקציות מימין!

1 המשפט היסודי של תורת גלואה

המשפט מקשר בין תתי הרחבות של הרחבת גלואה L/K לבין תת חבורות של $\text{Gal}(L/K)$. אנחנו נוכיח לפי ההוכחה של ארטין.

1.1 הלמה של ארטין

הגדרה 1.1 (פעולה של חבורה על שדה) תהי G חבורה ויהי E שדה. פעולה (ימנית) של G על E היא פונקציה

$$\begin{aligned} E \times G &\rightarrow E \\ (x, g) &\mapsto x^g \end{aligned}$$

עם התכונות הבאות:

1. לכל $x \in E$ מתקיים $x^{1G} = x$.

2. לכל $x \in E$ ולכל $g, h \in G$ מתקיים $x^{gh} = (x^g)^h$.

3. לכל $x, y \in E$ ולכל $g \in G$ מתקיים $(xy)^g = x^g y^g$, $(x + y)^g = x^g + y^g$ וכן $1^g = 1$, $0^g = 0$.

הערה 1.2 פעולה של G על E משרה הומומורפיזם $\rho : G \rightarrow \text{Aut}(E)$, כאשר $\text{Aut}(E)$ הם אוטומורפיזמים של השדה. הומומורפיזם ρ שכזה משרה פעולה על ידי

$$(x, g) \mapsto x^{\rho(g)} = \rho(g)(x)$$

הגדרה 1.3 פעולה של G על E נקראת נאמנה אם $\rho : G \rightarrow \text{Aut}(E)$ שמגדיר אותה הוא חד-חד-ערכי, או באופן שקול, לכל $g \neq 1$ קיים $x \in E$ עם $x^g \neq x$.

הגדרה 1.4 אם G פועלת על E , נגדיר את שדה השבת:

$$E^G = \{x \in E \mid \forall g \in G \ x^g = x\}$$

זה שדה בגלל התכונות של פעולה.

משפט 1.5 (הלמה של ארטיין) תהי G חבורה סופית הפועלת נאמנה על שדה E . אזי $E/E^G \leq |G|$.

הוכחה: נסמן $|G| = n$. נקח $x_1, \dots, x_m \in E$ עם $m > n$. נרצה להראות כי x_1, \dots, x_m תלויים לינארית מעל $E^G = K$. נסתכל על מערכת המשוואות

$$\left\{ \sum_{i=1}^m a_i x_i^\eta = 0 \mid \eta \in G \right\}$$

זאת מערכת של n משוואות עם m נעלמים, כאשר $m > n$. לכן מרחב הפתרונות V מעל E אינו טריוויאלי. אם היה פתרון (a_i) לא טריוויאלי עם $a_i \in E^G$, אזי מהמשוואה עם $\eta = 1_G$ היינו מקבלים תלות לינארית לא טריוויאלית של x_1, \dots, x_m , ומסיימים. נוכיח שיש כזה פתרון.

יהי $(a_1, \dots, a_m) \in V$ ממשקל מינימלי (המשקל של ווקטור הוא כמות הקואורדינטות שלו שאינן 0). קיים j עבורו $a_j \neq 0$, ובלי הגבלת הכלליות נניח כי $a_j = 1$ (על ידי כפל בסקלר). יהי $\sigma \in G$. אזי

$$(a_1^\sigma, \dots, a_m^\sigma) \in V$$

שכן הפעלת σ רק משנה את סדר המשוואות:

$$\left(\sum_{i=1}^m a_i^\sigma x_i^\eta \right)^{\sigma^{-1}} = \sum_{i=1}^m a_i x_i^{\eta \sigma^{-1}} = 0$$

כעת נקבל כי

$$(a_i - a_i^\sigma) \in V$$

אבל בבירור $w(a_i - a_i^\sigma) < w(a_i)$ כי הקואורדינטה j מתאפסת. לכן נובע כי $(a_i - \sigma(a_i)) = 0$, כלומר לכל $\sigma \in G$ קיבלנו $\sigma(a_i) = a_i$. לכן $a_i \in E^G$, וסיימנו. ■

1.2 ניסוח המשפט היסודי של תורת גלואה

תזכורות

1. אם $K_1, \dots, K_n \subseteq L$ אזי $K_1 \cdots K_n = \prod K_i$ מסמן את הצירוף של K_1, \dots, K_n .
שהוא השדה הנוצר על ידי K_1, \dots, K_n בתוך L .

2. אם G חבורה, תת חבורה תסומן $H \leq G$. האינדקס שלה יסומן $[G : H]$. מסמנים $H \triangleleft G$ אם H נורמלית, ובמקרה זה G/H חבורה עם הפעולות המושרות. מסמנים $H^\sigma = \sigma^{-1}H\sigma$, והסימון $\langle H_1, H_2 \rangle$ משמעו תת החבורה הנוצרת על ידי H_1, H_2 .

3. אם N/K גלואה, $K \subseteq L \subseteq N$, הרחבת ביניים, אזי N/L גלואה.

משפט 1.6 (המשפט היסודי של תורת גלואה) תהי N/K הרחבת גלואה סופית, ותהי $G = \text{Gal}(N/K)$. אזי ההתאמות הבאות בין תתי הרחבות של N/K ותתי חבורות של G הן הופכיות זו לזו:

$$H \leq G \mapsto N^H \\ \text{Gal}(N/E) \leftrightarrow K \subseteq E \subseteq N$$

יתר על כן, אם E, E_1, E_2 הן תתי הרחבות המתאימות לחבורות H, H_1, H_2 , אז מתקיים 1. היפוך הכלה:

$$E_2 \subseteq E_1 \iff H_1 \leq H_2$$

2. שמירת אינדקסים:

$$[G : H] = [E : K]$$

3. החלפת חיתוכים ויצירה:

$$E = E_1 \cap E_2 \iff H = \langle H_1, H_2 \rangle \\ E = E_1 E_2 \iff H = H_1 \cap H_2$$

4. לכל $\sigma \in G$ מתקיים

$$H_1 = H_2^\sigma \iff E_1 = E_2^\sigma$$

5. שמירת נורמליות:

$$H \triangleleft G \iff E/K \text{ is Galois}$$

6. אם E/K גלואה, אזי העתקת הצמצום

$$\text{res} : \text{Gal}(N/K) \rightarrow \text{Gal}(E/K)$$

היא על, וגרעינה הוא בדיוק $\text{Gal}(N/E)$. בפרט, ממשפט האיזומורפיזם הראשון:

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

במילים אחרות, המשפט אומר שיש אנטי-איזומורפיזם (הופך סדר) בין סריג הרחבות הביניים לבין סריג תת החבורות של G .

1.3 הוכחת המשפט היסודי של תורת גלואה

הוכחה: נתחיל בלהראות שההעתקה

$$H \mapsto N^H \mapsto \text{Gal}(N/N^H)$$

היא הזהות. כלומר, נרצה להראות $H = \text{Gal}(N/N^H)$. ברור שמתקיים $H \leq \text{Gal}(N/N^H)$, שכן N^H מוגדר להיות כל אותם איברים שאותם H שומרת. בכיוון השני, הלמה של ארטין אומרת לנו שמתקיים

$$|\text{Gal}(N/N^H)| \leq |H|$$

ולכן נקבל שוויון $H = \text{Gal}(N/N^H)$. בכיוון השני, נראה שההעתקה

$$E \mapsto \text{Gal}(N/E) \mapsto N^{\text{Gal}(N/E)}$$

היא הזהות. כלומר, נרצה להראות $E = N^{\text{Gal}(N/E)}$. ברור שמתקיים $E \subseteq N^{\text{Gal}(N/E)}$, שכן $\text{Gal}(N/E)$ מוגדרת להיות כל אותם שיכונים ששומרים את E . בכיוון השני, ממה שכבר הראינו נקבל כי

$$\text{Gal}(N/N^{\text{Gal}(N/E)}) = \text{Gal}(N/E)$$

ועל כן נקבל

$$\begin{aligned} [N : N^{\text{Gal}(N/E)}] &= [N : E] = [N : N^{\text{Gal}(N/E)}] [N^{\text{Gal}(N/E)} : E] \\ 1 &= [N^{\text{Gal}(N/E)} : E] \end{aligned}$$

ולכן נקבל שוויון $E = N^{\text{Gal}(N/E)}$

נעבור להוכיח את התכונות. יהיו E, E_1, E_2 תת הרחבות של N/K , שמתאימות לחבורות $H = \text{Gal}(N/E), H_1 = \text{Gal}(N/E_1), H_2 = \text{Gal}(N/E_2)$

1. נוכיח כי $E_2 \subseteq E_1 \iff H_1 \leq H_2$.
 נניח כי $H_1 \leq H_2$. אזי $E_1 = N^{H_1} \subseteq N^{H_2} = E_2$, כי אם איבר מסויים מושבת תחת H_2 , בפרט הוא מושבת תחת H_1 , שהיא קטנה יותר.
 נניח כי $E_2 \subseteq E_1$. אזי $H_2 = \text{Gal}(N/E_2) \leq \text{Gal}(N/E_1) = H_1$, כי אם העתקה מסויימת משביתה את E_1 , בפרט היא משביתה את E_2 , שהוא קטן יותר.

2. נוכיח כי $[G : H] = [E : K]$ מתקיים

$$[G : H] = \frac{|G|}{|H|} = \frac{|\text{Gal}(N/K)|}{|\text{Gal}(N/E)|} = \frac{[N : K]}{[N : E]} = \frac{[N : E][E : K]}{[N : E]} = [E : K]$$

3. נוכיח כי $E = E_1 E_2 \iff H = H_1 \cap H_2$, $E = E_1 \cap E_2 \iff H = \langle H_1, H_2 \rangle$
 (זה נובע מתכונה כללית של סריגים - העתקה חד-חד-ערכית ועל בין קבוצות סדורות חלקית שהופכת סדר חייבת להעביר מקסימום למינימום ולהיפך).
 מתקיים:

$$\begin{aligned} E = N^H &= N^{\langle H_1, H_2 \rangle} = \{x \in N \mid \forall \sigma \in \langle H_1, H_2 \rangle \ x^\sigma = x\} = \\ &= \{x \in N \mid \forall \sigma \in H_1, \tau \in H_2 \ x^\sigma = x^\tau = x\} = \\ &= \{x \in N \mid \forall \sigma \in H_1 \ x^\sigma = x\} \cap \{x \in N \mid \forall \sigma \in H_2 \ x^\sigma = x\} = \\ &= N^{H_1} \cap N^{H_2} = E_1 \cap E_2 \end{aligned}$$

ובנוסף:

$$\begin{aligned} H = \text{Gal}(N/E) &= \text{Gal}(N/E_1 E_2) = \{\sigma \in G \mid \sigma|_{E_1 E_2} = \text{id}\} = \\ &= \{\sigma \in G \mid \sigma|_{E_1} = \text{id}, \sigma|_{E_2} = \text{id}\} = \\ &= \{\sigma \in G \mid \sigma|_{E_1} = \text{id}\} \cap \{\sigma \in G \mid \sigma|_{E_2} = \text{id}\} = \\ &= \text{Gal}(N/E_1) \cap \text{Gal}(N/E_2) = H_1 \cap H_2 \end{aligned}$$

4. נוכיח כי $H_1 = H_2^\sigma \iff E_1 = E_2^\sigma$ מתקיים:

$$\begin{aligned} H_1 = \text{Gal}(N/E_1) &= \text{Gal}(N/E_2^\sigma) = \{\tau \in G \mid \forall x \in E_2 \ (x^\sigma)^\tau = x^\sigma\} = \\ &= \{\tau \in G \mid \forall x \in E_2 \ x^{\sigma\tau\sigma^{-1}} = x\} = \\ &= \{\tau \in G \mid \sigma\tau\sigma^{-1} \in \text{Gal}(N/E_2) = H_2\} = \\ &= \sigma^{-1} H_2 \sigma = H_2^\sigma \end{aligned}$$

ובנוסף:

$$\begin{aligned}
 E_1 = N^{H_1} = N^{H_2^\sigma} &= \{x \in N \mid \forall \tau \in H_2 \ x^{\tau^\sigma} = x\} = \\
 &= \{x \in N \mid \forall \tau \in H_2 \ x^{\sigma^{-1}\tau\sigma} = x\} = \\
 &= \{x \in N \mid \forall \tau \in H_2 \ x^{\sigma^{-1}\tau} = x^{\sigma^{-1}}\} = \\
 &= \{x \in N \mid x^{\sigma^{-1}} \in E_2\} = \\
 &= E_2^\sigma
 \end{aligned}$$

5. נוכיח כי E/K is Galois $\iff H \triangleleft G$.
 זה נובע ישירות מהסעיף הקודם - אם H נורמלית, $H^\sigma = H$ לכל σ , ולכן $E^\sigma = E$ לכל σ , כלומר E/K נורמלית. היא תמיד פרידה (הוכחנו כבר), ולכן היא גלואה.

6. נוכיח כי במצב של הסעיף הקודם, העתקת הצמצום

$$\begin{aligned}
 \text{res} : \text{Gal}(N/K) &\rightarrow \text{Gal}(E/K) \\
 \sigma &\mapsto \sigma|_E
 \end{aligned}$$

היא על, וגרעינה הוא $\text{Gal}(N/E)$ (האיזומורפיזם $\text{Gal}(E/K)/\text{Gal}(N/E) \cong \text{Gal}(E/K)$ נובע ממשפט האיזומורפיזם הראשון כמו שאמרנו בעת הניסוח).
 ראינו בעבר שאפשר להרים אוטומורפיזם לאוטומורפיזם, ולכן ברור שההעתקה על. נבדוק מה הגרעין:

$$\ker(\text{res}) = \{\sigma \in G \mid \sigma|_E = \text{id}\} = \text{Gal}(N/E)$$

■

דוגמא יהי $p > 0$ ראשוני ויהי $\zeta \in \mathbb{C}$ שורש יחידה מסדר p . אזי $\mathbb{Q}(\zeta)/\mathbb{Q}$ גלואה, וכן

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

הוכחה: ζ מאפס את $x^{p-1} = (x-1)(1+x+\dots+x^{p-1})$. ידוע כי $x^{p-1} = 1+x+\dots+x^{p-1}$ אי פריק (מתרגיל הבית), ולכן

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$$

כל שאר שורשי f הם חזקות של ζ , ולכן $\mathbb{Q}(\zeta)$ הוא שדה הפיצול של f , כלומר ההרחבה היא גלואה. כעת נגדיר העתקה

$$\begin{aligned}
 \varphi : \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) &\rightarrow \mathbb{Z}/(p-1)\mathbb{Z} \\
 \varphi(g) = k &\iff \zeta^g = \zeta^k
 \end{aligned}$$



אזי φ הומומורפיזם חד-חד-ערכי ועל (תרגיל - להשתכנע).