אלגברה ב2

ארזים ©

24 במאי 2017

הוכחה: היינו באמצע הוכחת משפט גלואה. למעשה היינו באמצע הוכחת למה:

למה 0.1 יהיו $K \subseteq K_1 \subseteq K_2$ הרחבות פרידות. יהיו L_1, L_2, L סגורי גלואה של $K_1/K, K_2/K_1, K_2/K$ בהתאמה. אם $\mathrm{Gal}\left(L_1/K\right)$ פתירה וגם $\mathrm{Gal}\left(L_2/K_1\right)$ פתירה, אזי $\mathrm{Gal}\left(L/K\right)$ פתירה.

הוכחה: סימנו

$$\begin{aligned} G &= \mathrm{Gal}\left(L/K\right) \\ U_i &= \mathrm{Gal}\left(L/K_i\right) \\ H_i &= \mathrm{Gal}\left(L/L_i\right) \end{aligned}$$

כעת רוצים להראות כי G פתירה, וקיבלנו את התרשים הבא:

$$\begin{tikzcd}
 & H_2 = \bigcap_{g \in U_1} U_2^g \arrow[r, dash] \arrow[d, dash] & U_2 \arrow[r, dash] & H_1H_2 \arrow[r, dash] \arrow[d, dash] & U_1 \arrow[r, dash] & G \\
1 = \bigcap_{g \in G} U_2^g \arrow[r, dash] & H_1 \cap H_2 \arrow[rr, dash] & & H_1 = \bigcap_{g \in G} U_1^g & &
\end{tikzcd}$$

נטען שהמנה $H_1/H_1 \cap H_2$ פתירה. לפי משפט האיזומורפיזם השני,

$$H_1/H_1 \cap H_2 \cong H_1H_2/H_2 \leq U_1/H_2$$

החבורה הימנית פתירה, ולכן גם $H_1/H_1 \cap H_2$ פתירה, כתת חבורה של חבורה פתירה. נפעיל כעת הצמדה באיבר g:

$$H_1/H_1 \cap H_2 \cong H_1^g/H_1^g \cap H_2^g \cong H_1/H_1 \cap H_2^g$$

לכן לכל g גם $H_1/H_1 \cap H_2^g$ פתירה. נשתמש בכך שמכפלה ישרה של פתירות היא פתירה ולכן

$$\Gamma = \prod_{g \in G} H_1/H_1 \cap H_2^g$$

פתירה. נסתכל בהעתקה

$$\varphi : H_1 \to \Gamma$$
$$\varphi(h) = (h(H_1 \cap H_2^g))_{g\in G}$$

זה הומומורפיזם שמקיים:

$$\ker\varphi = \bigcap_{g\in G} H_1 \cap H_2^g \subseteq \bigcap_{g\in G} H_2^g \subseteq \bigcap_{g\in G} U_2^g = 1$$

וזאת משום שההרחבה L/K סגור גלואה של L_2/K, ולכן $L = \prod K_2^g$, כלומר

$$1 = \mathrm{Gal}\left(L/L\right) = \bigcap_{g\in G} \mathrm{Gal}\left(L/K_2^g\right) = \bigcap_{g\in G} U_2^g$$

לכן φ חד־חד־ערכית, כלומר H_1 איזומורפית לתת חבורה של Γ, שהיא פתירה - כלומר H_1 פתירה. אם כן, G/H_1 פתירה וכן H_1 פתירה - ולכן G פתירה. ■

כעת אנחנו מוכנים להראות שאם לפולינום f יש נוסחת שורשים אז החבורה $G = \mathrm{Gal}\left(f/K\right)$ פתירה. יש לנו מגדר של שדות

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

כאשר $K_{i+1} = K_i(\alpha_i)$ עבור $\alpha_i^{n_i} \in K_i$. כמו כן, f מתפצל מעל K_n. ראינו שדי להראות שההרחבה K_n/K פתירה (כלומר שחבורת גלואה של סגור גלואה שלה L/K היא פתירה). נשנה מעט את המגדל:

$$K = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_{n+1}'$$

באשר $K_1' = K_0(\zeta)$, עם ζ שורש יחידה פרימיטיבי מסדר $m = n_1 \cdots n_n$, ובאופן כללי $K_{i+1}' = K_i(\zeta)$ לכל $i \geq 1$. כעת, $\zeta^n = 1 \in K_0$, וכן $K_{i+1}' = K_i'(\alpha_{i-1})$ עבור $\alpha_{i-1}^{n_i} \in K_{i-1} \subseteq K_i'$. כמו כן, f מתפצל מעל K_n, ובפרט מעל $K_n \subseteq K_{n+1}'$. די להוכיח כעת כי K_{n+1}'/K פתירה. על ידי הפעלת הלמה באופן חוזר, די להוכיח למעשה שלכל i ההרחבה K_{i+1}'/K_i' פתירה.

נשים לב שמתקיים

$$\mathrm{Gal}\left(K_1'/K\right) \leq \left(\mathbb{Z}/m\mathbb{Z}\right)^*$$

ולכן אבלית, ובפרט פתירה. גם K_{i+1}'/K_i' היא מעגלית, כי $\mu_{n_{i-1}} \subseteq \mu_m \subseteq K_i'$ וכן $K_{i+1}' = K_i'[\alpha_{i-1}]$ עם $\alpha_{i-1}^{n_i} \in K_i'$. בפרט, החבורה פתירה, וסיימנו. ■

1 הרחבות נעלות (טרנסנדנטליות)

הגדרה 1.1 תהי L/K הרחבת שדות. $\alpha \in L$ אלגברי מעל K אם יש פולינום $0 \neq f \in K[x]$ שמקיים $f(\alpha) = 0$. איבר שאינו כזה נקרא נעלה מעל K, או טרנסנדנטלי. הרחבת שדות שבה יש איבר אחד לפחות שהוא נעלה נקראת <u>החרבה נעלה</u>.

משיקולי עוצמות פשוטים, חייבים למשל להיות ממשיים נעלים.

הגדרה 1.2 תהי L/K הרחבת שדות, ותהי $A \subseteq L$. נאמר כי A בלתי תלוייה אלגברית מעל K אם לכל צירוף

$$\sum_{0 \leq i_1, \ldots, i_n \leq N} a_{i_1, \ldots, i_n} \alpha_i^{i_1} \cdots \alpha_n^{i_n} = 0$$

עבור איזשהם $a_{i_1, \ldots, i_n} \in K$ ואיזשהם $\alpha_i \in A$ שונים, מתקיים בהכרח $a_{i_1, \ldots, i_n} = 0$ לכל $0 \leq i_1, \ldots, i_n \leq N$. במילים אחרות, אם יש פולינום f בכמה משתנים כך שמתקיים $f(\alpha_1, \ldots, \alpha_n) = 0$ אזי f הוא פולינום האפס.

הערה 1.3 A בלתי תלוייה אלגברית מעל K אם ורק אם $\left\{\alpha_1^{i_1} \cdots \alpha_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{Z}\right\}$ בלתי תלוייה לינארית מעל K.

הגדרה 1.4 אם $L = K(A)$, A בלתי תלוייה אלגברית, נאמר כי L/K הרחבה נעלה בטוהרה.

במצב הזה יש איזומורפיזם:

$$\varphi : K(X_a \mid a \in A) \to L$$

על ידי

$$\varphi\left(\frac{f(x_a \mid a \in A)}{g(x_a \mid a \in A)}\right) = \frac{f(a \mid a \in A)}{g(a \mid a \in A)}$$

למשל אם $A = \{\alpha_1, \alpha_2\}$ אזי

$$\varphi\left(\frac{f(x, y)}{g(x, y)}\right) = \frac{f(\alpha_1, \alpha_2)}{g(\alpha_1, \alpha_2)}$$

1.1 בסיס נעלות

הגדרה 1.5 תהי L/K הרחבה של שדות, ותהי $A \subseteq L$ קבוצה. נאמר כי A בסיס נעלות של L/K אם A בלתי תלוייה אלגברית וכן $L/K(A)$ אלגברית. במצב זה $K(A)/K$ היא כמובן נעלה בטוהרה.

דוגמא יהי $\alpha \in \mathbb{C}$ נעלה. נתבונן בהרחבה $\mathbb{Q}(\alpha)/\mathbb{Q}$. אזי $\{\alpha\}$ הוא בסיס נעלות, אבל גם למשל $\{\alpha^5 + 3\}$ בסיס נעלות - α ממעלה חמש מעל $\mathbb{Q}(\alpha^5 + 3)$.

משפט 1.6 לכל L/K יש בסיס נעלות. יתר על כן, אם $A \subseteq L$ בלתי תלוייה אלגברית, אזי יש בסיס נעלות המכיל את A.

הוכחה: אם L/K אלגברית, אזי $A=\emptyset$ הוא בסיס נעלות. לכן נניח שההרחבה לא אלגברית. נסתכל באוסף $\mathcal{F}$ של הקבוצות $B \subseteq L$ כך שהן בלתי תלויות אלגברית ומכילות את A. נסדר את $\mathcal{F}$ לפי הכלה.

$\mathcal{F}$ לא ריקה, כי $A \in \mathcal{F}$ (אם לא נתנו לנו A נגדיר $A=\emptyset$). אם יש לנו שרשרת $\{B_i\} \subseteq \mathcal{F}$, כלומר לכל $i \neq j$ $B_i \subseteq B_j$ או להיפך, אז נראה כי $\bigcup B_i \in \mathcal{F}$ וחסם עליון של השרשרת - לכן מהלמה של צורן יש איבר מקסימלי $B \in \mathcal{F}$. נראה שאכן $\bigcup B_i \in \mathcal{F}$ - ברור שהוא מכיל את A. ניקח $\alpha_1, \ldots, \alpha_n \in \bigcup B_i$, ונראה שהם בלתי תלויים אלגברית. ניקח $\alpha_j \in B_{i_j}$, ומתכונת השרשרת יש i עבורו $B_{i_j} \subseteq B_i$ לכל j, ולכן $\alpha_j \in B_{i_j}$ לכל j, כלומר הם בלתי תלויים אלגברית.

B בלתי תלוייה אלגברית ומכילה את A. אילו $L/K(B)$ אלגברית, סיימנו. אחרת, יש $\alpha \in L$ נעלה מעל $K(B)$. לכן, נובע כי $B \cup \{\alpha\}$ בלתי תלוייה אלגברית - אכן, אחרת היה סכום

$$\sum c_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_{n-1}^{i_{n-1}} \alpha^{i_n} = 0$$

נקבץ לפי חזקות של α ונקבל

$$\sum \tilde{c}_{i_n}\left(b_1, \ldots, b_{n-1}\right) \alpha^{i_n} = 0$$

ומכאן נובע כי $\tilde{c}_{i_n}\left(b_1, \ldots, b_{n-1}\right) = 0$ כי α נעלה. מכאן $\tilde{c}_{i_n} = 0$, ולכן כל $c_{i_1,\ldots,i_n}$ הוא אפס. אם כן $B \cup \{\alpha\}$ בלתי תלוייה אלגברית. כמובן, זו סתירה למקסימליות של B מתוך $\mathcal{F}$, ולכן סיימנו. ■

כעת נרצה להראות שעוצמה של בסיס נעלות היא תכונה שמורה של L/K.

למה 1.7 תהי L/K הרחבת שדות, $\alpha \in L$, $B \subseteq L$ בלתי תלוייה אלגברית. התנאים הבאים שקולים:

1. α אלגברי מעל $K(B)$.
2. קיים פולינום $f \in K\left[x_1, \ldots, x_m, y\right]$ וקיימים $\beta_1, \ldots, \beta_m \in B$ כך שמתקיים $f\left(\beta_1, \ldots, \beta_m, y\right) \neq 0$ אבל $f\left(\beta_1, \ldots, \beta_m, \alpha\right) = 0$.

הוכחה: ראינו את $1 \Rightarrow 2$ בסוף הוכחת המשפט הקודם. כעת נוכיח $2 \Rightarrow 1$.

α אלגברי מעל $K(B)$, ולכן יש $g(y) \in K(B)[Y]$ כך שמתקיים $g(y) \neq 0$ וכן $g(\alpha) = 0$. נכתוב את g מפורשות:

$$g(y) = \sum \frac{c_i\left(\beta_1, \ldots, \beta_m\right)}{d_i\left(\beta_1, \ldots, \beta_m\right)} y^i$$

נכפול במכנה משותף

$$d\left(\beta_1, \ldots, \beta_m\right) = \prod_i d_i\left(\beta_1, \ldots, \beta_m\right)$$

ונגדיר כך את

$$f(x_1,\ldots,x_m,y)=d(x_1,\ldots,x_m)\sum_i \frac{c_i(x_1,\ldots,x_m)}{d_i(x_1,\ldots,x_m)}y^i\in K[x_1,\ldots,x_m,y]$$

פולינום זה אינו אפס שכן $d(x_1,\ldots,x_m)\neq 0$. כמו כן

$$f(\beta_1,\ldots,\beta_m,\alpha)=d(\beta_1,\ldots,\beta_m)\,g(\alpha)=0$$

כנדרש. ■