

## 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  $\text{Gal}(L_1/K)$  פתירה וגם  $\text{Gal}(L_2/K_1)$  פתירה, אזי  $\text{Gal}(L/K)$  פתירה.

**הוכחה:** סימנו

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

קעת רוצים להראות כי  $G$  פתירה, וקיבלנו את התרשים הבא:

$$\begin{array}{ccccccc} H_2 = \bigcap_{g \in U_1} U_2^g & \text{---} & U_2 & \text{---} & H_1 H_2 & \text{---} & U_1 \text{ --- } G \\ & & & & \downarrow & & \\ 1 = \bigcap_{g \in G} U_2^g & \text{---} & H_1 \cap H_2 & \text{---} & H_1 = \bigcap_{g \in G} U_1^g & & \end{array}$$

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

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

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

$$\begin{aligned}\varphi: H_1 &\rightarrow \Gamma \\ \varphi(h) &= (h(H_1 \cap H_2^g))_{g \in G}\end{aligned}$$

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

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

לכן  $\varphi$  חד-חד-ערכית, כלומר  $H_1$  איזומורפית לתת חבורה של  $\Gamma$ , 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  $G = \text{Gal}(f/K)$  פתירה. יש לנו מגדר של שדות

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

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:

$$K = K'_0 \subseteq K'_1 \subseteq \dots \subseteq K'_{n+1}$$

באשר  $K'_1 = K_0(\zeta)$ , עם  $\zeta$  שורש יחידה פרימיטיבי מסדר  $m = n_1 \dots n_n$ , 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  $\alpha_{i-1}^{n_{i-1}} \in K_{i-1} \subseteq K'_i$ . כמו כן,  $f$  מתפצל מעל  $K_n$ , ובפרט מעל  $K'_n \subseteq K_n$ . 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

$$\text{Gal}(K'_1/K) \leq (\mathbb{Z}/m\mathbb{Z})^*$$

ולכן אבלית, ובפרט פתירה. גם  $K'_{i+1}/K'_i$  היא מעגלית, כי  $K'_i \subseteq \mu_m \subseteq \mu_{n_{i-1}}$  וכן  $K'_{i+1} = K'_i[\alpha_{i-1}]$  עם  $\alpha_{i-1}^{n_{i-1}} \in K'_i$ . 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 טרנסנדנטי. הרחבת שדות שבה יש איבר אחד לפחות שהוא נעלה נקראת הרחבה נעלה.

משיקולי עוצמות פשוטים, חייבים למשל להיות ממשיים נעלים.

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

$$\sum_{0 \leq i_1, \dots, i_n \leq N} a_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} = 0$$

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

**הערה 1.3** בלתי תלויה אלגברית מעל  $K$  אם ורק אם  $\{\alpha_1^{i_1} \cdots \alpha_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{Z}\}$  בלתי תלויה לינארית מעל  $K$ .

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

במצב הזה יש איזומורפיזם:

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

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 תלויה 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 -  $\alpha$  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  $\bigcup B_i \in \mathcal{F}$ . ניקח  $\alpha_1, \dots, \alpha_n \in \bigcup B_i$  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  $\alpha_j \in B_i$  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

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

נקבץ לפי חזקות של  $\alpha$  ונקבל

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

ומכאן נובע כי  $\tilde{c}_{i_n} (b_1, \dots, b_{n-1}) = 0$  כי  $\alpha$  נעלה. מכאן  $\tilde{c}_{i_n} = 0$  ולכן כל  $c_{i_1, \dots, i_n}$  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.  $\alpha$  אלגברי מעל  $K(B)$ .

2. קיים פולינום  $f \in K[x_1, \dots, x_m, y]$  וקיימים  $\beta_1, \dots, \beta_m \in B$  כך שמתקיים  $f(\beta_1, \dots, \beta_m, \alpha) = 0$  אבל  $f(\beta_1, \dots, \beta_m, y) \neq 0$ .

**הוכחה:** ראינו את  $1 \Rightarrow 2$  בסוף הוכחת המשפט הקודם. כעת נוכיח  $2 \Rightarrow 1$ .  $\alpha$  אלגברי מעל  $K(B)$ , ולכן יש  $g(y) \in K(B)[Y]$  כך שמתקיים  $g(\alpha) = 0$  וכן  $g(y) \neq 0$  נכתוב את  $g$  מפורשות:

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

נכפול במכנה משותף

$$d(\beta_1, \dots, \beta_m) = \prod_i d_i(\beta_1, \dots, \beta_m)$$

ונגדיר כך את

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

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

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

■

כנדרש.