

## אלגברה ב' 2 - הרצאה 6

09.03.11

היינו באמצע הוכחת המשפט:

**משפט.**  $f \in R = A[x_1, \dots, x_n]$  סימטרי מעלה  $d$  אז יש פולינום  $g \in R$  כך ש- $w(g) \leq d$  כך ש- $g(s_1, \dots, s_n) = f$

הוכחה. אנחנו באמצע אינדוקציה כפולה על  $n$  ועל  $d$ . מצאנו  $g_0 \in R_0 = A[x_1, \dots, x_{n-1}]$  כך ש- $w(g_0) \leq d$  וסימננו  $f' := f - g_0(s_1, \dots, s_{n-1})$  ממעלה  $d \geq$  ומתקיים  $x_1, \dots, x_n | f'$  ולכן המכפלה  $s_n = x_1 \dots x_n | f'$ . לכאן הגענו. לכן,  $f' = s_n f_1$  עבור איזה  $f_1 \in R$ . אז  $f_1$  סימטרי. מדוע? ניקח  $\sigma \in S_n$ ,

$$s_n \cdot f_1 = f' = \sigma(f') = \sigma(s_n)\sigma(f_1) = s_n \cdot \sigma(f_1)$$

כעת,  $s_n(f_1 - \sigma(f_1)) = 0$  ולכן  $f_1 - \sigma(f_1) = 0$  (וזה בכלל לא תחום) אלא זה ברור.  $\deg f_1 = \deg f - n \leq d - n < d$  ולכן אפשר להפעיל הנחת האינדוקציה. לפי הנחת האינדוקציה על  $d$  כיוון שהפולינום סימטרי קיים פולינום  $g_1 \in R$  כך ש- $w(g_1) \leq d - n$  ו- $f_1 = g_1(s_1, \dots, s_n)$

$$\begin{aligned} f &= f' + g_0(s_1, \dots, s_{n-1}) = \\ &= s_n g_1(s_1, \dots, s_n) + g_0(s_1, \dots, s_{n-1}) = \underbrace{x_n g_1 + g_0(s_1, \dots, s_{n-1})}_{=g} \end{aligned}$$

$$w(g) \leq d \text{ אז } w(x_n) = n, w(g_1) \leq d - n, w(g_0) \leq d$$

□

הוכחה. יהי  $g \in R$  כך ש- $g(s_1, \dots, s_n) = 0$  אז  $g = 0$ .

□

**תזכורת.** יש העתקה  $R \rightarrow R_0$  ע"י  $f \mapsto (f)_0$ ,  $f_0 = f(x_1, \dots, x_{n-1}, 0)$  זהו הומומורפיזם. אם  $g$  סימטרי אז  $(g)_0$  סימטרי.  $(s_1)_0, \dots, (s_{n-1})_0$  הם הסולינומים הסימטריים היסודיים ב- $R_0$ ,  $(s_n)_0 = 0$ .

הוכחה. באינדוקציה על  $n$ .  $n = 1$ :  $g(s_1) = g$  ולכן זה ברור. נמשיך באינדוקציה על  $\deg g$  אם  $\deg g \leq 0$  אז  $g(s_1, \dots, s_n) = g$  ולכן גם זה ברור.

$$\begin{aligned} 0 &= (g(s_1, \dots, s_n))_0 = g((s_1)_0, \dots, (s_n)_0) = \\ &= g((s_1)_0, \dots, (s_{n-1})_0, 0) = (g)_0((s_1)_0, \dots, (s_{n-1})_0) \end{aligned}$$

לפי הנחת האינדוקציה עבור  $(n-1)$ ,  $(g)_0 = 0$ , כלומר  $g(x_1, \dots, x_{n-1}, 0) = 0$ . אז  $g = x_n \cdot g_1$  עבור איזה  $g_1 \in R$ . מכאן:  $0 = g(s_1, \dots, s_n) = s_n g_1(s_1, \dots, s_n)$ . אבל  $\deg g_1 < \deg g$  ולכן לפי הנחת האינדוקציה  $g_1 = 0$  ולכן  $g = x_n g_1 = 0$ .

□

**משפט.** יהי  $f \in A[x_1, \dots, x_n]$  סימטרי אז יש  $g \in A[x_1, \dots, x_n]$  יחיד כך ש-  $f = g(s_1, \dots, s_n)$ . יתר על כן,  $w(g) \leq \deg f$ .

## הרחבות סופיות והרחבות אלגבריות

יהי  $K$  שדה.

**הגדרה.**  $K_0 \subseteq K$  היא תת שדה של  $K$ -אם היא סגורה תחת 4 הפעולות ב-  $K$  ומכילה את 0 ו-1. אז  $K_0$  הוא שדה נאמר גם ש-  $K$  הרחבה של  $K_0$  או  $K/K_0$  הרחבת שדות.

במקרה זה  $K$  הוא גם מ"ו מעל  $K_0$ . מגדירים: המעלה של  $K/K_0$  היא  $\dim_{K_0} K$  סימון:  $[K : K_0]$ . זה יכול להיות גם  $\infty$ .

הערה.  $A \subseteq K$  קבוצה אז קיים התת השדה (התת חוג) הקטן ביותר של  $K$  שמכיל את  $A$ . אכן, זהו החיתוך של כל התת שדות (תת חוגים) של  $K$  שמכילים את  $A$ .

**הגדרה.** התת שדה הראשוני של שדה  $K$  זהו התת שדה הקטן ביותר של  $K$ .

פורמאלית הוא קיים. אבל מהו? נסמנו  $\mathbb{F}$ . נגדיר  $\varphi : \mathbb{Z} \rightarrow K$  ע"י

$$\varphi(n) = n1_K = \begin{cases} \underbrace{1_k + \dots + 1_k}_{n \text{ פעמים}} & n > 0 \\ \underbrace{(-1_k) + \dots + (-1_k)}_{-n \text{ פעמים}} & n < 0 \\ 0 & n = 0 \end{cases}$$

קל לראות שזה הומומורפיזם של חוגים וכן  $\varphi(\mathbb{Z}) \subseteq \mathbb{F}$  ו-  $\varphi(\mathbb{Z})$  הוא תחום כי תמונה של הומומורפיזם ולכן השדה הקטן ביותר שיכיל אותו יהיה שדה המנות של  $\varphi(\mathbb{Z})$ . לפי משפט ההומומורפיזם הראשון  $\varphi(\mathbb{Z}) \cong \mathbb{Z} / \ker \varphi$ . הינו תחום ראשי ולכן  $\ker \varphi = (p)$ . בה"כ  $p \geq 0$  (כי  $\pm 1$  הפיכים ולכן ניתן להפוך את הסימן ל-  $p$ ). נחלק לאפשרויות:

1.  $p = 0$ : אז  $\varphi(\mathbb{Z}) \cong \mathbb{Z}$  ולכן  $\mathbb{F} \cong \mathbb{Q}$ . נאמר כי  $\mathbb{Q}$  הוא השדה הראשוני של  $K$ .

2.  $p > 0$ :  $\varphi(\mathbb{Z}) = \mathbb{Z}/(p)$  תחום. לכן  $(p)$  אידיאל ראשוני ולכן  $(p)$  אידיאל מרבי ע"פ משפט עם שקילויות מהשיעור הראשון. בפרט  $\mathbb{Z}/(p)$  הוא שדה. לכן,  $\mathbb{F} = \varphi(\mathbb{Z}) = \mathbb{Z}/(p)$ . נסמן  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . במקרה זה נאמר כי  $\mathbb{F}_p$  הוא השדה הראשוני של  $K$ .

**הגדרה.**  $p$  כנ"ל נקרא האפיון של  $K$ . סימון  $\text{char}(K)$ .

**מסקנה.**  $\text{char}(K) = 0$  או  $\text{char}(K) = p$  כאשר  $p$  הוא מספר ראשוני.

**הגדרה.** שתי הרחבות  $L_1|K$  ו-  $L_2|K$  נקראות איזומורפיות (או מסומנות  $L_1 \equiv_K L_2$ ) אם יש איזומורפיזם-  $K: L_1 \rightarrow L_2$ ,  $\theta$ , כלומר, איזומורפיזם שהוא זהות על  $K$  ( $\varphi(a) = a$ ) לכל  $a \in K$ .

**הגדרה.** תהי  $L|K$  הרחבה. תהי  $S \subseteq L$  קבוצה. החוג (השדה) הנוצר ע"י  $S$  מעל  $K$  הוא תת החוג (תת השדה) הקטן ביותר של  $L$  שמכיל את  $K$  ואת  $S$ . עבור חוג נסמן  $K[S]$  ועבור שדה נסמן  $K(S)$ .

מתקיים:

$$K[S] = \{f(s_1, \dots, s_m) | f \in K[x_1, \dots, x_m], m \in \mathbb{N}, s_1, \dots, s_m \in S\}$$

$$k(s) = \left\{ \frac{f(s_1, \dots, s_m)}{g(s_1, \dots, s_m)} | f, g \in K[x_1, \dots, x_m], m \in \mathbb{N}, s_1, \dots, s_m \in S, G(s_1, \dots, s_n) \neq 0 \right\}$$

אם  $S = \{\alpha_1, \dots, \alpha_r\}$  אז נכתוב  $K[\alpha_1, \dots, \alpha_r], K(\alpha_1, \dots, \alpha_r)$  במקום  $K[S], K(S)$ .  
 אם  $|S| = n$  אז ניתן לקבוע את  $m$  בהגדרת  $K(S)$  ו-  $K[S]$  ל-  $n$ .  
 בפרט  $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} | f, g \in K[x], g(\alpha) \neq 0 \right\}, K[\alpha] = \{f(\alpha) | f \in K[x]\}$   
 אומרים כי  $L|K$  נוצרת סופית אם יש  $\alpha_1, \dots, \alpha_n \in L$  כך שמתקיים  $L = K(\alpha_1, \dots, \alpha_n)$ .  
 אומרים כי  $L|K$  פשוטה אם יש  $\alpha \in L$  כך ש-  $L = K(\alpha)$ .

**דוגמאות.** 1.  $\mathbb{Q}(\pi, e) | \mathbb{Q}$  נוצרת סופית.

2.  $\mathbb{C} | \mathbb{R}(\sqrt{-1})$  פשוטה כי  $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ .

**משפט.** יהי  $p \in K[x]$  אי פריק.

1. יהי  $L = K[x]/(p)$  ויהי  $Y := X + (p)$  אזי  $L = K[Y] = K(Y)$  ו-  $p(Y) = 0$ .

2. אם  $K(\alpha)$  הרחבה פשוטה של  $K$  כך ש-  $p(\alpha) = 0$  אז קיים הומומורפיזם-יחיד  $\theta : K(y) \rightarrow K(\alpha)$  שמעתיק את  $y$  על  $\alpha$ . הוא איזומורפיזם- $K$ .

הערה.  $X$  הוא הפולינום  $x$ , כלומר, הפולינום  $0 + x + 0 \cdot x^2 + 0 \cdot x^3 + \dots$ .

1.  $p$  אי-פריק והחוג הוא ראשי לכן  $(p)$  מרבי ולכן  $L$  שדה.

$$K \rightarrow K[x] \rightarrow K[x]/(p) = L$$

הוא הומומורפיזם של חוגים עם יחידה (כלומר בין השאר מעתיק יחידה ליחידה). הוא גם חח"ע.

הערה. כל הומומורפיזם  $\varphi : K \rightarrow R$  של חוגים עם יחידה שונה מאפס הוא חח"ע כי גרעינו הוא אידאל שאינו כל  $K$  כי  $\varphi(1) = 1 \neq 0$  ולכן הוא  $(0)$ .

נזהה את  $K$  עם תמונתו ב-  $L$  ואת  $L$  כ-  $K$ . כומבן  $K \subseteq K[y] \subseteq L$  ו-  $K(y) \subseteq L$  אם  $g = \sum_{i=0}^{\infty} a_i x^i \in K[x]$  אז

$$g(y) = \sum_{i=0}^{\infty} a_i (Y)^i = \sum_{i=0}^{\infty} a_i (X + (p))^i = \sum_{i=0}^{\infty} a_i x^i + (p) = g + (p)$$

לכן נקבל

$$L = K[x]/(p) = \{g + (p) | g \in K[x]\} = \{g(y) | g \in K[x]\} = K[y]$$

לכן,  $K[y] = K(y) = L$  ואז  $p(y) = p + (p) = 0$ .

2. היחידות: אם  $\theta$  כזה אז לכל  $g = \sum_{i=0}^{\infty} a_i x^i$  מתקיים  $\theta(g(y)) = \theta(\sum_{i=0}^{\infty} a_i y^i) = \sum_{i=0}^{\infty} \theta(a_i) (\theta(y))^i = \sum_{i=0}^{\infty} a_i \alpha^i$ .  
מכאן היחידות כי:

$$L = K[y] = \{g(y) | g \in K[x]\}$$

ההצגה:  $x \mapsto \alpha$  מגדיר הומומורפיזם  $K[x] \rightarrow K(\alpha)$  ע"י  $\varphi(f) = f(\alpha)$ . בפרט  $\varphi(x) = \alpha$ .  $\varphi(p) = p(\alpha) = 0$  ולכן  $p \in \ker \varphi$  ואז  $(p) \subseteq \ker \varphi$  לפי משפט האיזומורפיזם הראשון  $\varphi$  משקה הומומורפיזם  $K(\alpha) \xrightarrow{\theta} K[x]/(p)$  כך ש- $\theta(y) = \alpha$  שדה ולכן  $\theta$  חח"ע.  
התמונה שלו היא שדה שמכיל את  $K$  (כי  $\theta$  מעתיק את  $K$  זהותית לעצמו) ואת  $\alpha$  ולכן  $\theta$  על.  
לכן  $\varphi$  איזומורפיזם.

□