

## אלגברה ב' 2 - הרצאה 7

09.03.11

בפעם שעברה לקחנו  $p \in K[x]$  אי פריק והראינו ש-  $L = K[x]/(p)$  הוא שדה ו-  
 $L = K(y) = K[y]$  ואם  $y = x + p$  ואם  $K(\alpha)/K$ ,  $p(\alpha) = 0$  אז יש איזומורפיזם-  $K$  יחיד  
 $\theta : K(y) \rightarrow K(\alpha)$  כך ש-  $\theta(t) = \alpha$ .

**הגדרה.** תהי  $L/K$  הרחבה,  $\alpha \in L$ . אז נקרא אלגברי מעל  $K$  אם יש  $0 \neq f \in K[x]$   
כך ש-  $f(\alpha) = 0$ . אחרת נקרא טרנסצנדנטי.

העתקת ההצבה:  $f \mapsto f(\alpha)$  היא הומומורפיזם  $\varphi_\alpha : K[x] \rightarrow L$ .  $\alpha \in L$  אלגברי  
 $\ker \varphi_\alpha \neq \{0\}$   
תכונות:

**משפט.** תהי  $L/K$  הרחבה ויהי  $\alpha \in L$  אלגברי מעל  $K$ .

1. יש  $p \in K[x]$  מתוקן יחיד כך ש-  $\ker \varphi_\alpha = (p)$ .

**הגדרה.**  $p$  כנ"ל ייקרא הפולינום האי פריק של  $\alpha$  ונסמן  $\text{irr}(\alpha, K)$ .

2.  $p$  כנ"ל אי פריק ב-  $K[x]$ .

3. לכל  $f \in K[x]$   $f(\alpha) = 0 \Leftrightarrow p|f$ .

4.  $K(\alpha) = K[\alpha]$ .

5.  $K(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in K\}$  כאשר  $\deg p = n$ .

6.  $[K(\alpha) : K] = n = \deg p$ . ביתר דיוק,  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  בסיס של  $K(\alpha)$  מעל  $K$ .

7.  $K(\beta)$  הרחבה של  $K$  כך ש-  $p(\beta) = 0$  אז יש איזומורפיזם-  $K$  יחיד  $\rho : K(\alpha) \rightarrow K(\beta)$   
כך ש-  $p(\alpha) = \beta$ .

הוכחה.

1.  $\ker \varphi_\alpha \subset K[x]$  אידאל,  $K[x]$  ראשי לכן יש  $p \in \ker \varphi_\alpha$  כך ש-  $\ker \varphi_\alpha = (p)$ .  
ניזכר ש-  $(p) = (p') \Leftrightarrow p' = cp, c \in K^*$ . לכן, בה"כ  $p$  מתוקן יחיד.

2.  $\varphi_\alpha : K[x] \rightarrow L$  לכן  $K[x]/(p)$  איזומורפי ל-  $\text{Im } \varphi_\alpha$  תת חוג של  $L$  לכן, תחום.  
לכן  $(p)$  ראשוני כלומר  $p$  אי פריק.

3.  $f(\alpha) = 0 \Leftrightarrow f \in \ker \varphi_\alpha \Leftrightarrow f \in (p) \Leftrightarrow p|f$ .

4. לפי המשפט יש איזומורפיזם  $K$ -מ-  $\theta : K[x]/(p) \rightarrow K(\alpha)$  כך ש-  $\theta(y) = \alpha$ .

$$K(\alpha) = \theta(K[y]) = \theta(\{g(y) : g \in K[x]\}) = \{g(\alpha) : g \in K[x]\} = K[\alpha]$$

5.  $\supseteq$  ברור.  $\subseteq$ :  $K(\alpha) = K[\alpha]$  לכן כל איבר ב-  $K(\alpha)$  מהצורה  $f(\alpha)$  כך ש-  
 $a \in K[x]$ . לפי חילוק עם שארית  $f = qp + r$   $q, r \in K[x]$   $\deg r < \deg p = n$ .  
 ואז,  $f(\alpha) = q(\alpha) \underbrace{p(\alpha)}_{=0} + r(\alpha) = r(\alpha)$  לכן  $f(\alpha)$  באגף ימין.

6. לפי הקודם  $1, \alpha, \dots, \alpha^{n-1}$  פורשים את  $K(\alpha)$  מעל  $K$ . נראה שהם בת"ל: יהיו  
 $a_0, \dots, a_{n-1} \in K$  כך ש-  $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$  אז  $f(\alpha) = 0$  כאשר  
 $f = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  לפי סעיף 3 אבל  $p \nmid f$  אבל  $\deg f < \deg p$  לכן  $f = 0$ .  
 כלומר  $a_0 = \dots = a_{n-1} = 0$

7.  $\text{erutcp}$   $\rho = \theta_2 \circ \theta_1^{-1}$  והוא יחיד כי  $\theta_1, \theta_2$  יחידים.

□

**משפט.** תהי  $L/K$  הרחבה  $\alpha \in L$  טרנסצנדנטי מעל  $K$ .

1.  $K[\alpha] \cong_F K[x]$  ע"י  $f(x) \mapsto f(\alpha)$ .

2.  $K(\alpha) \cong_K K(x)$  ע"י  $\frac{f(x)}{g(x)} \mapsto \frac{f(\alpha)}{g(\alpha)}$ .

3.  $[K(\alpha) : K] = \infty$  או ביתר דיוק  $1, \alpha, \alpha^2, \dots$  בסיס של  $K[\alpha]$  מעל  $K$ .

4.  $K[\alpha] \subsetneq K(\alpha)$ .

הוכחה.

1.  $\ker \varphi_\alpha = 0$  לכן  $\varphi_\alpha : K[x] \rightarrow L$  חח"ע. ברור שהיא על, התמונה של  $\varphi_\alpha$  היא  
 $\{f(\alpha) : f \in K[x]\} = K[\alpha]$ .

2. החוגים איזומורפיים לכן גם שדות המנות שלהם.

3.  $K[\alpha] = \{f(\alpha) : f \in K[x]\} = \{a_0 + a_1\alpha + \dots + a_k\alpha^k, a_i \in K, k \in \mathbb{N}\}$ .

$1, \alpha, \alpha^2, \dots$  בת"ל: יהיו  $a_0, a_1, \dots \in K$  כמעט כולם אפס כך ש-  $\sum_{i=0}^\infty a_i \alpha^i = 0$ .  
 אז  $f(\alpha) = 0$  כאשר  $f = \sum_{i=0}^\infty a_i x^i \in K[x]$ . אבל אז  $f \in \ker \varphi_\alpha$  לכן  $f = 0$ .  
 לכן  $a_i = 0$  לכל  $i$ .

4. כי  $K[x] \subsetneq K(x)$ .

□

**מסקנה.** תהי  $L/K$  הרחבה  $\alpha \in L$  אז אלגברי מעל  $K$   $(K(\alpha) : K) < \infty \Leftrightarrow$ .

**משפט.** יהיו  $K \subseteq L \subseteq M$  שדות. אז  $[M : K] = [M : L][L : K]$ . ביתר דיוק אם  $\{x_i\}_{i \in I}$   
 בסיס של  $L$  מעל  $K$ ,  $\{y_j\}_{j \in J}$  בסיס של  $M$  מעל  $L$  אז  $\{x_i y_j\}_{(i,j) \in I \times J}$  בסיס של  $M$  מעל  $K$ .

הוכחה. פורש: יהי  $z \in M$ . אז יש  $a_j \in L$  כמעט כולם 0 כך ש-  $\sum_{j \in J} a_j y_j$  לכל  $j \in J$ .  
 יש  $b_{ij} \in K$  כמעט כולם 0 כך ש-  $a_j = \sum_{i \in I} b_{ij} x_i$ .

$$z = \sum_{j \in J} \sum_{i \in I} b_{ij} x_i y_j$$

בת"ל: יהיו  $b_{ij} \in K$  כמעט כולם 0 כך ש-  $\sum_{i \in I} b_{ij} x_i y_j = 0$  אז  $\sum_{i \in I} b_{ij} x_i = 0$  לכל  $j \in J$ .  
 בת"ל  $x_i$   $b_{ij} = 0$ .

□