

אלגברה ב' 2 - הרצאה 11

28.03.11

משפט. יהי K שדה ותהי $A \leq K^*$ תת חבורה סופית. אז A מעגלית (ציקלית).

הוכחה. A חילופית סופית לכן $A = \prod_{p \text{ ראשוניים}} A_p$ כאשר A_p חבורת p -סילו של A .
אם נוכיח שכל A_p מעגלית אז ידוע שמכפלה ישרה של מעגליות היא מעגלית. לכן בה"כ
 $A = A_p$ חבורת p -סילו. נניח $|A| = p^r$.
יהי $\alpha \in A$. אז $\text{ord}(\alpha) | p^r$ לכן $\text{ord}(\alpha) = p^i$, $i \leq r$. יהי $p^s = \max\{\text{ord}(\alpha) : \alpha \in A\}$.
כלומר $s \leq r$ צ"ל $s = r$ אם $\text{ord}(\alpha) = p^i$ אז $\alpha^{p^r} = (\alpha^{p^i})^{p^{r-i}} = 1$. כלומר, α שורש של
הפולינום $f = x^{p^r} - 1$.
אבל ל- f לכל היותר p^s שורשים ב- K ואילו $|A| = p^r \geq p^s$ לכן $s = r$. $\square$

תזכורת. K שדה. ל- $f \in K[x]$, $f \neq 0$ אין שורשים מרובים (ב- $\tilde{K}$) $\Leftrightarrow f, f' \neq 0$.
אם f אי פריק אז אין שורשים מרובים (ב- $\tilde{K}$) $\Leftrightarrow f' \neq 0$.

הגדרה. $f \in K[x]$ הוא פריד (ספרבילי) אם כל שורשיו ב- $\tilde{K}$ פשוטים.

הגדרה. α פריד מעל K אם α אלגברי מעל K ו- $\text{irr}(\alpha, K)$ פריד.

הגדרה. הרחבה L/K נקראת פרידה אם כל $\alpha \in L$ פריד מעל K .

הגדרה. K נקרא מושלם אם כל הרחבה אלגברית היא פרידה.

משפט. אם $\text{char } K = 0$ או K סופי אז K מושלם.

את החלק של $\text{char } K = 0$ כבר הוכחנו.

את החלק K סופי נוכיח בהמשך.

דוגמא. $F_p(t)$ אינו מושלם כאשר t טרנסנדנטי. $f(x) = x^p - t$ אי פריק (לפי איזנשטיין)
ויש לו שורש יחיד (מרובה).

משפט. (איבר פרימיטיבי)

תהי L/K פרידה סופית. אז יש $\alpha \in L$ כך ש- $L = K(\alpha)$.

הוכחה. אם K סופי אז L מ"ו ממימד סופי (נאמר n) מעל K , לכן $L \cong K^n$ כמרחבים
וקטוריים, בפרט L סופי. לכן L^* מעגלית. כלומר $L = \langle \alpha \rangle$ עבור איזהו $\alpha \in L$. אז

$$K(\alpha) = L, \text{ לכן, } L^* = \langle \alpha \rangle \subseteq K(\alpha) \subseteq L$$

נניח כי K אינסופי. כידוע $L = K(\alpha_1, \dots, \alpha_k)$ כאשר $\alpha_1, \dots, \alpha_k$ אלגבריים. נוכיח
באינדוקציה על k .

בסיס: $k = 1$ אין מה להוכיח.

$k = 2$:

טענה. יהיו $a, b \in L$. אז יש $c \in K$ כך ש- $K(a, b) = K(a - cb)$.

הוכחה. ואכן, בה"כ $K \subseteq L \subseteq \tilde{K}$.

$$f = \text{irr}(a, K) = (x - a)(x - a_1) \dots (x - a_m) \quad a_1, \dots, a_m \in \tilde{K}$$

$$g = \text{irr}(b, K) = (x - b)(x - b_1) \dots (x - b_n) \quad b_1, \dots, b_n \in \tilde{K}$$

כאשר $a, a_1, \dots, a_m$ שונים וגם $b, b_1, \dots, b_n$ שונים.

$$S = \left\{ \frac{a_i - a}{b_j - b} : \begin{matrix} i = 1, \dots, m \\ j = 1, \dots, n \end{matrix} \right\} \subseteq \tilde{K}$$

קבוצה זו סופית. לכן יש $c \in K, c \notin S$ כך ש- $c \neq 0$. נגדיר $\gamma = a - cb$. אז $K(\gamma) \subseteq K(a, b)$. לכן $c \notin S$. לכן $c \neq \frac{a_i - a}{b_j - b}$ לכל i, j . לכן $cb_j - cb \neq a_i - a$. לכן, $\gamma = a - cb \neq a_i - cb_j$. אז $h(x) = f(\gamma + cx) \in K(\gamma)[x]$ לכל i, j .

$$h(b) = f(\gamma + cb) = f(a) = 0$$

$$h(b_j) = f(\gamma + cb_j) \neq 0$$

כי השורשים הם רק a_i ואילו $\gamma + cb_j$ בהכרח לא כזה. מדוע זה שונה מ- a ? כי $\gamma + cb_j \neq 0$ (השוויון מתקיים רק עבור $c = 0$).

לכן אם ניקח $h, g \in K(\gamma)[x]$ נקבל $\gcd(h, g) \mid x - b$. לכן $x - b \in K(\gamma)[x]$. בפרט $b \in K(\gamma)$. כעת $a = cb + \gamma \in K(\gamma)$. לכן $K(a, b) \subseteq K(\gamma)$ ולכן $K(a, b) = K(\gamma)$. $\square$

מעבר האינדוקציה:

$$K(\alpha_1, \dots, \alpha_k) = K(\alpha_1, \dots, \alpha_{k-2})(\alpha_{k-1}, \alpha_k)$$

α_{k-1}, α_k פרידים מעל K אבל $\text{irr}(\alpha_k, K(\alpha_1, \dots, \alpha_{k-2})) \mid \text{irr}(\alpha_k, K)$ לכן פריד ולכן α_k פריד מעל $K(\alpha_1, \dots, \alpha_{k-1})$. כנ"ל עבור α_{k-1} . אז,

$$K(\alpha_1, \dots, \alpha_{k-2})(\alpha_{k-1}, \alpha_k) = K(\alpha_1, \dots, \alpha_{k-2}, \alpha) = K(\alpha)$$

$\square$