אלגברה ב' 2 – הרצאה 12

30.03.11

בשיעור הקודם הוכחנו את משפט האיבר הפרימיטיבי.

דוגמא. $L = \mathbb{F}_P(t,u)$ שדה פונקציות רציונליות בשני משתנים t,u. נסמן ב- $K = \mathbb{F}_p(t^p,u^p)$ למעשה אלה מנות של פולינומים בחזקות -ה- p:

$$K = \left\{ \frac{\sum_{i,j} a_{ij} t^{pi} u^{pj}}{\sum_{i,j} b_{ij} t^{pi} u^{pj}} : a_{ij}, bij \in \mathbb{F}_p \right\} \subseteq L$$

אז $K(t,u) = L$.

$$\begin{array}{ccc} & L = K(t,u) & \\ \swarrow & & \searrow \\ K(t) & & K(u) \\ \searrow & & \swarrow \\ & P & \end{array}$$

$t^p, u^p \in K$ לפי ההגדרה. כלומר $x^p - u^p \in K[x]$ לכן $[K(u) : K] \leq p$. באותו אופן, $[K(t) : K] \leq p$. נאמר גם $[K(t,u) : K] \leq p$ כי נבחר את הפולינום שיוצר את t מעל K ובפרט הוא מעל $K[u]$.
לכן, $[L : K] \leq p^2$. למעשה $[L : K] = p^2$ כי ניתן להוכיח ש- $\{t^i u^j | 0 \leq i,j < p\} \subseteq L$. מדוע? ניקח צירוף לינארי שלהם. המקדמים הם פונקציות רציונליות, נעשה מכנה משותף. כעת בגלל שאלה פולינומים במשתנים ב"ת t,u אז הם כולם חייבים להיות 0. בכל מקרה זה תרגיל.
אבל לכל $\alpha \in L$ מתקיים $\alpha^p \in K$ (אכן $\alpha = \frac{\sum a_{ij} t^i u^j}{\sum b_{ij} t^i u^j} \in K$ לכן $\alpha^p = \frac{\sum a_{ij}^p t^{pi} u^{pj}}{\sum b_{ij}^p t^{ip} u^{jp}}$ כי $(a+b)^p = a^p + b^p$ כי $\operatorname{char} K = p$ ולכן המקדמים ביניהם הם 0. אז $[K(\alpha) : K] \leq p$. בפרט, לא ייתכן $K(\alpha) = L$ (כי L ממעלה p^2). ולכן אין כאן איבר פרימטיבי.

רנצה איפיון קצת שונה של הרחבות פרידות.

סימון. עבור L_1/K, L_2/K הרחבות אלגבריות נסמן

$$\operatorname{Ism}_K(L_1, L_2) = \{\sigma : L_1 \to L_2 | K - \text{שיכון } \sigma\}$$

נסמן:

$$[L : K]_S = |\operatorname{Ism}_K(L, \tilde{K})| \in \{1, 2, 3, \ldots \infty\}$$

כאשר $\tilde{K}$ הוא סגור אלגברי של K.

$[L:K]_S$ אינו תלוי בבחירה של $\tilde{K}$ כי כל שני סגורים אלגבריים איזומורפיים מעל K ואם $\lambda\tilde{K} \to \tilde{K}'$ איזומורפיזם- K אז $\sigma \mapsto \lambda \circ \sigma$ ו- $\sigma \mapsto \lambda^{-1} \circ \sigma$ הן העתקות חח"ע ועל $\mathrm{Ism}_K(L,\tilde{K}) \to \mathrm{Ism}_K(L,\tilde{K}')$.

$$\begin{array}{ccccc} L & \xrightarrow{\sigma} & \tilde{K} & \xrightarrow{\lambda} & \tilde{K}' \\ | & & | & & | \\ K & = & K & = & K \end{array}$$

לכן בה"כ $L \subseteq \tilde{K}$ ואז $id_L \in \mathrm{Ism}_K(L,\tilde{K})$ לכן $[L:K]_S \geq 1$.

דוגמא. יהי $L = K(\alpha)$ הרחבה אלגברית פשוטה, $\alpha \in \tilde{K}$. יהי $p = \mathrm{irr}(\alpha, K)$, נאמר $p = (x-\alpha_1)\dots(x-\alpha_n)$ כאשר $\alpha = \alpha_1, \dots, \alpha_n \in \tilde{K}$.
אם $\sigma \in \mathrm{Ism}_K(L,\tilde{K})$, אז $p(\alpha) = 0$ לכן, $p(\sigma(\alpha)) = 0$ כלומר $\sigma(\alpha) \in \{\alpha_1, \dots, \alpha_n\}$.
להפך, לכל $1 \leq i \leq n$, α_i הוא גם שורש של פולינום אי פריק וראינו שאז יש איזומורפיזם K - יחיד $\sigma_i : L = K(\alpha) \to K(\alpha_i)$ שמעתיק את α על α_i.
כל איזומורפיזם מעתיק שורש לשורש אחר ומצד שני יש רק אחד שמעתיק לשורש ספציפי.
לכן $[L:K]_S = \mathrm{Ism}_K(L,K) =$ מספר השורשים השונים.
לכן,

1. $[K(\alpha):K]_S \leq \underbrace{[K(\alpha:K]}_{=n}$.
2. $[K(\alpha):K]_S = [K(\alpha):K] \Leftrightarrow \alpha$ פריד מעל K.

אבל זה רק במקרה של הרחבה פשוטה.

משפט. תהיינה $M \subseteq L \subseteq M$ סופיות. אז:

$$[M:K]_S = [M:L]_S \cdot [L:K]_S$$

הוכחה. בה"כ $K \subseteq L \subseteq M \subseteq \tilde{K}$ (אחרת ניקח סגור אלגברי של M).
נסתכל על הצמצום:

$$\rho : \mathrm{Ism}_K(M,\tilde{K}) \to \mathrm{Ism}_K(L,\tilde{K})$$

נראה ש-:

1. הצמצום הוא על.
2. לכל $\lambda \in \mathrm{Ism}_K(L,\tilde{K})$: $\rho^{-1}(\lambda) = \rho^{-1}(id_L)$. כלומר,

$$\begin{aligned} |\{\sigma : M \to \tilde{K} | \sigma|_L = \lambda\}| = \\ = |\{\sigma : M \to \tilde{K} | \sigma|_L = id_L\}| = |\{\mathrm{Ism}_L(M,\tilde{K})\}| = \\ = [M:L]_S \end{aligned}$$

ואז המשפט ברור. מדוע? כי יש כאן העתקה על ומספר האיברים שעוברים לאותו האיבר הוא בדיוק $[M:L]_S$.

1. הוכנו שכל $\lambda \in \mathrm{Ism}_K(L, \tilde{K})$ ניתן להרחיב לאוטומורפיזם $\tilde{\lambda}$ של $\tilde{K}$. זה אפילו יותר חזק ממה שאנחנו צריכים.
   אז $\tilde{\lambda}|_M \in \mathrm{Ism}_K(M, \tilde{K})$ ו- $\rho(\tilde{\lambda}|_M) = \tilde{\lambda}|L = \lambda$.
2. יש העתקות

$$\{\sigma : M \to \tilde{K} | \sigma|_L = id_L\} \rightleftarrows \{\sigma : M \to \tilde{K} | \sigma|_L = \lambda\}$$

$$\sigma \mapsto \tilde{\lambda} \circ \sigma$$
$$\sigma \mapsto \tilde{\lambda}^{-1} \circ \sigma$$

   הפוכות זו לזו ולכן שתי הקבוצות שוות עוצמה.

□

נרחיב את הדוגמא שעשינו למקרה הכללי:

משפט. תהי L/K סופית. אז:

1. $[L : K]_S \leq [L : K]$.
2. $[L : K]_S = [L : K] \Leftrightarrow L/K$ פריזה.

הוכחה. $L = K(\alpha_1, \ldots, \alpha_n)$ כאשר $\alpha_1, \ldots, \alpha_n \in \tilde{K}$ (בה"כ $L \subseteq \tilde{K}$).
אז

$$L_0 = K \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n = L$$

כאשר $L_i = K(\alpha_1, \ldots, \alpha_i)$ מתקיים $L_i = L_{i-1}(\alpha_i)$.

1. לפי בדוגמא $[L_i : L_{i-1}]_S \leq [L_i : L_{i-1}]$ ולכן מנוסחאות המכפלה נובע.
2. אם L/K פריזה לפי הדוגמא $L = K(\alpha)$ $[L : K]_S = [L : K]$. נניח ש- L/K פריזה. אז יש $\alpha \in L$ שאינו פריד מעל K, לפי הדוגמא $[K(\alpha) : K]_S < [K(\alpha) : K]$ $[L : K(\alpha)]_S \leq [L : K(\alpha)]$ לפי הסעיף הקודם. לכן מנוסחאות המכפלה $[L : K]_S < [L : K]$.

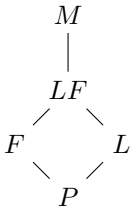
□

מסקנה. α פריד מעל $K \Leftrightarrow K(\alpha)/K$ פריזה.

הוכחה. α פריד $\Leftrightarrow [K(\alpha) : K]_S = [K(\alpha) : K] \Leftrightarrow K(\alpha)/K$ פרידה. □

משפט. יהיו $K \subseteq L, F \subseteq M$ שדות. אז:

1. $M/K \Leftrightarrow M/L$, L/K פריזות.
2. אם L/K פריזה אז LF/F פריזה.
3. $L/K, F/K$ פריזות אז LF/K פריזה.



הוכחה.

1. אם M/K סופית אז השקילות נובעת מנוסחאות המכפלה. במקרה הכללי, אם M/K פרידה, אז גם L/K פרידה מההגדרה (כי $L \subseteq M$) וגם הקלות M/L פרידה: אכן יהי $\alpha \in M$ אז ל- $irr(\alpha, K)$ אין שורשים מרובים (בסגור האלגברי) אבל $irr(\alpha, L) | \operatorname{irr}(\alpha, K)$ ב- $L[x]$. לכן גם ל- $\operatorname{irr}(\alpha, L)$ אין שורשים מרובים (בסגור האלגברי).

   להפך, אם L/K, M/L פרידות יהי $\alpha \in M$ ויהי $p = \operatorname{irr}(\alpha, L) = \sum_i a_i x^i$. יהי $L \subseteq E = K(a_0, a_1, \dots,)$, E/K הרחבה סופית, $[E : K] < \infty$ ו- $p \in E[x]$. הוא אי פריק מעל L לכן אי פריק מעל שדה קטן יותר E. לכן $p = \operatorname{irr}(\alpha, E)$. $K \subseteq E \subseteq L$, L/K פרידה, לכן, לפי הכיוון הקודם E/K פרידה (וכמובן סופית). אז $[E : K]_S = [E : K]$. α פריד מעל E (כי ל- p אין שורשים מרובים) לכן $[E(\alpha) : E]_S = [E(\alpha) : E]$ לכן $[E(\alpha) : K]_S = [E(\alpha) : K]$. וזה אומר ש- α פריד מעל K. כלומר כל איבר פריד ולכן ההרחבה פרידה.

2. בהוכחה של משפט דומה לגבי אלגבריות ראינו ש-

$$LF = \bigcup_{\text{סופית } S \subseteq L} F(S)$$

   לכן, די להוכיח: אם $\alpha_1, \dots, \alpha_n \in L$ אז $F(\alpha_1, \dots, \alpha_n)/F$ פרידה.

   אבל, $K(\alpha_1, \dots, \alpha_n)/K$ פרידה ולכן יש $\alpha \in L$ כך ש- $K(\alpha_1, \dots, \alpha_n) = K(\alpha)$. לכן $F(\alpha_1, \dots, \alpha_n 0 = F(\alpha)$. לכן די להוכיח אם $\alpha \in L$ פריד מעל K אז $\alpha \in LF$ פריד מעל F ואכן $\operatorname{irr}(\alpha, F) | \operatorname{irr}(\alpha, K)$ לכן אם ל- $\operatorname{irr}(\alpha, K)$ אין שורשים מרובים בסגור האלגברי גם ל- $\operatorname{irr}(\alpha, F)$ אין שורשים מרובים בסגור האלגברי.

3. נובע משני הסעיפים הקודמים.

□

הרחבות של שדות סופיים

נניח בחלק זה K שדה סופי, $|K| = q < \infty$ וכמו תמיד $\tilde{K}$ סגור אלגברי.

משפט.

1. $p := \operatorname{char}(K) > 0$ ($\mathbb{F}_p \subseteq K$).
2. $K^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$.
3. $\alpha^q = \alpha$ לכל $\alpha \in K$.

4. אם L/K הרחבה ממעלה $n < \infty$ אז $|L| = q^n$ בפרט $q = p^k$ כאשר $k = [K : \mathbb{F}_p]$.

הוכחה.

1. K מכיל את השדה הראשוני שלו לכן גם זה סופי (כי שונה מ- $\mathbb{Q}$).
2. K^* סופית לכן מעגלית וברור $|K^*| = q - 1$.
3. אם $\alpha = 0$ ברור. אם $\alpha \neq 0$, כלומר $\alpha \in K^*$ אז $\operatorname{ord}(\alpha) | \operatorname{ord}(K^*) = q - 1$ לכן, $\alpha^{q-1} = 1$. לבסוף $\alpha^q = \alpha$.
4. ראינו כבר. $L \cong K^n$ (איזומורפיזם של מ"ו מעל K) לכן, $|L| = q^n$.

□

משפט. יהי $n \in \mathbb{N}$ אז $K_n = \{\alpha \in \tilde{K} | \alpha^{q^n} = \alpha\} \subseteq \tilde{K}$ הוא שדה. למעשה הוא הרחבה ממעלה n של K.

הוכחה. K_n שדה: יהיו $\alpha, \beta \in K_n$ אז

$$(\alpha\beta)^{q^n} = \alpha^{q^n}\beta^{q^n} = \alpha\beta$$

$$\left(\frac{\alpha}{\beta}\right)^{q^n} = \frac{\alpha^{q^n}}{\beta^{q^n}} = \frac{\alpha}{\beta} \qquad \beta \neq 0$$

מתקיים: $(\alpha + \beta)^p = \alpha^p + \beta^p$ ובאינדוקציה $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ בפרט (q הוא חזקה של p) $(\alpha + \beta)^{q^n} = \alpha^{q^n} + \beta^{q^n} = \alpha + \beta$.
באופן דומה, אם q איזוגי $(\alpha - \beta)^{q^n} = \alpha^{q^n} + \beta^{q^n} = \alpha - \beta$. אם q זוגי אז $p = 2$ לכן $-1 = 1$ ולכן גם אז הנסוחא נכונה. לכן K_n שדה.

$K \subseteq K_n$: ברור לפי סעיף שלישי במשפט הקודם.
איברי K_n הם השורשים של הפולינום $f(x) = x^{q^n} - x$ ב- $\tilde{K}$ אבל ל- f אין שורשים מרובים ב- $\tilde{K}$ כי $f'(x) = q^n x^{q^n - 1} - 1 = -1$ לכן $1 \in \gcd(f, f')$. לכן:

$$|K_n| = \deg f = q^n$$

לכן K_n סופי ולכן מהמשפט הקודם $n = [K_n : K]$. □

טענה. K_n ההרחבה היחידה של K ממעלה n בתוך $\tilde{K}$. בפרט, $K \cong (\mathbb{F}_p)_k$ באשר $k = [K : \mathbb{F}_p]$.

הוכחה. תהי $L \subseteq \tilde{K}$ הרחבה ממעלה n של K אבל $|L| = q^n = |K_n|$ לכן די להוכיח אחת ההכלות, למשל $L \subseteq K_n$. ואכן, יהי $\alpha \in L$ אם $\alpha = 0$ אז ברור. אחרת, אם $\alpha \in K^*$ אז $\operatorname{ord}(\alpha) || L^* | = q^n - 1$ לכן $\alpha^{q^n - 1} = 1$ מכאן, $\alpha^{q^n} = \alpha$ וזאת בדיוק ההגדרה של $\alpha \in K_n$. □