

אלגברה ב' 2 – הרצאה 24

26.5.11

הרחבות אי פרידות טהורות

בפרק זה נסמן: K שדה ו- $\tilde{K}$ סגור אלגברי.

הגדרה. תהי L/K הרחבת שדות. אז $\alpha \in L$ פריד מעל K אם $F = \{\alpha \in L : K(\alpha) \text{ פרידה מעל } K\}$ נקרא הסגור הפריד.

משפט. F הוא שדה. זוהי הרחבה הפרידה הגדולה ביותר של K בתוך L .

הוכחה. נראה כי F שדה. ברור שאם $\alpha \in F$ אז $K(\alpha) \subseteq F$ וכן $K(\alpha) \subseteq F$ וכן $K(\alpha) \subseteq F$. יהיו $\alpha, \beta \in F$ אז $K(\alpha), K(\beta) \subseteq F$ ולכן $K(\alpha, \beta) \subseteq F$ ולכן $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F$ שדה. $\square$

משפט. נניח $\text{chr } K = p > 0$ ראשוני. תהי L/K אלגברית. התנאים הבאים שקולים:

$$1. [L, K]_S = 1.$$

$$2. \text{לכל } \alpha \in L \text{ מתקיים } \text{irr}(\alpha, K) = x^{p^n} - a \text{ כאשר } n \geq 0 \text{ שלם } a \in K.$$

$$3. \text{לכל } \alpha \in L \text{ קיים } n \geq 0 \text{ שלם המקיים } \alpha^{p^n} \in K.$$

$$4. L = K(\alpha_i : i \in I) \text{ כאשר לכל } i \in I \text{ מתקיים כי קיים } n_i \geq 0 \text{ שלם המקיים } \alpha_i^{p^{n_i}} \in K.$$

$$5. \text{אם } \alpha \in L \text{ פריד מעל } K \text{ אז } \alpha \in K.$$

הגדרה. $[L : K]_S$ זה מספר האיברים ב- $\text{Ism}_K(L, \tilde{K})$.

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

(1) $\Rightarrow$ (2): יהי $f = \text{irr}(\alpha, K)$. אם $\alpha' \in K$ שורש של f אז קיים הומומורפיזם $\sigma : K(\alpha) \rightarrow K(\alpha')$ כך ש- $\sigma(\alpha) = \alpha'$. אפשר להרחיב את σ ל- $\sigma' \in \text{Ism}_K(L, \tilde{K})$ באשר $\sigma' \in \text{Ism}_K(L, \tilde{K})$ לפי ההנחה $\sigma' = 1_L$ (כי קיים איבר אחד ב- $\text{Ism}_K(L, \tilde{K})$) ולכן $\sigma'(\alpha') = \sigma(\alpha') = \alpha$ ולכן $\alpha' = \sigma'(\alpha') = \sigma(\alpha') = \alpha$ כלומר $f = (x - \alpha)^m$, $m \in \mathbb{N}$, נכתוב $m = p^n \cdot r$ כאשר $n \geq 0$ ו- $p \nmid r$. נסמן $a := \alpha^{p^n} \in L$ אז:

$$\begin{aligned} K[x] \ni f &= (x - \alpha)^{p^n r} = ((x - \alpha)^{p^n})^r = (x^{p^n} - \alpha^{p^n})^r = \\ &= (x^{p^n} - a)^r = x^{p^n r} - r a x^{p^n(r-1)} + \dots \end{aligned}$$

ובכיוון ש- $f \in K[x]$ אז $ra \in K$ (כמקדם של פולינום). כמו כן $p \nmid r$ לכן $r \neq 0$ ב- K , ולכן $a \in K$. כלומר, $x^{p^n} - a = f$ שורש שלו ולכן $\alpha^{p^n} - a = f$.

(4) $\Rightarrow$ (3) $\Rightarrow$ (2): ברור.
 (5) $\Rightarrow$ (2): יהי $f = \text{irr}(\alpha, K) = x^{p^n} - a$. לכן $f' = p^n x^{p^n-1} \neq 0$ אם ורק אם $n \neq 0$.
 כלומר $f = x - a \in K$. לכן $\alpha = a$.
 (1) $\Rightarrow$ (4): יהי $\sigma \in \text{Ism}_K(L, \bar{K})$. צ"ל $\sigma = 1_L$. די להוכיח כי $\sigma(\alpha_i) = \alpha_i$ לכל $i \in I$.
 נכי איברי L הם פונקציות רציונליות ב- $\{\alpha_i : i \in I\}$ עם מקדמים ב- K . $\{\alpha_i\}_{i \in I}$ הם שורשים של פולינום, כאשר α_i שורש של $f_i = x^{p^{n_i}} - a_i$ (עבור $a_i \in K$), לכן גם $\sigma(\alpha_i)$ שורש שלו. אולם, $f_i = x^{p^{n_i}} - a_i = (x - \alpha)^{p^{n_i}}$, כלומר ל- f יש שורש יחיד, α_i ולכן $\sigma(\alpha_i) = \alpha_i$.
 (3) $\Rightarrow$ (5): אפשר לכתוב $\text{irr}(\alpha, K) = g(x^{p^n})$ עבור איזשהו $g \in K[x]$ כך שאין $h \in K[x]$ המקיים $g(x) = h(x^p)$. אז אי פריק (אחרת $g(x^p)$ פריק). ל- g אין שורשים מרובים. α^{p^n} שורש של g , לכן α^{p^n} פריד מעל K ולכן מההנחה $\alpha^{p^n} \in K$. $\square$

הגדרה. נניח $\text{chr } K = p > 0$. L/K אלגברית נקראת אי פרידה טהורה אם היא מקיימת אחד מהתנאים הנ"ל.

דוגמא. יהיו t, u משתנים בלתי תלויים מעל F_p . אזי $F_p(t, u)/F_p(t^p, u^p)$ אי פרידה טהורה (הסעיף הרביעי).

משפט. תהי L/K אלגברית ויהי $K \subseteq F \subseteq L$ הסגור הפריד של K בתוך K . אזי L/F אי פרידה טהורה.

הוכחה. לפי הסעיף החמישי $\alpha \in L$ פריד מעל F . אז F/K פרידה ולכן α פריד מעל K ולכן $\alpha \in K$. $\square$

טענה. תהי L/K אלגברית, פרידה וגם פרידה טהורה. אזי $L = K$.

הוכחה. יהי $\alpha \in L$ אזי α פריד מעל K (כי L/K פרידה) ולכן $\alpha \in K$ (מסעיף חמישי). $\square$

משפט. יהיו $L \subseteq L, F \subseteq M$ שדות.

1. M/K אי פרידה טהורה $\Leftrightarrow L/K, M/L$ אי פרידות טהורות.

2. אם L/K אי פרידה טהורה אז LF/F אי פרידה טהורה.

3. אם $F/K, L/K$ אי פרידות טהורות אז LF/K אי פרידה טהורה.

הוכחה. הסעיף השלישי נובע מהשניים הקודמים ולכן נוכיח את השניים הראשונים.

1. $[M : L]_S \cdot [L : K]_S = [M : K]_S$ מכאן ומסעיף הראשון בהגדרת אי פרידות טהורה הכל נובע.

2. לפי הסעיף הרביעי של אי פרידות טהורה $L = K(\alpha_i : i \in I)$ כאשר $\alpha_i^{p^{n_i}} \in K$ לכל $i \in I$. לכן $LF = F(\alpha_i : i \in I)$ וכן לכל $i \in I$ $\alpha_i^{p^{n_i}} \in F \supseteq K$. $\square$

משפט. נניח $p = \text{chr } K > 0$ סופית. אז:

1. אם L/K אי פרידה טהורה אז $[L : K] \in \mathbb{N}$ חזקה של p .

2. $\frac{[L:K]}{[L:K]_S} \in \mathbb{N}$ חזקה של p .

הוכחה.

1. יש מגדל $L = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L$ כך ש- L_i/L_{i-1} פשוטה. לפי כפלות המעלה בה"כ L/K פשוטה. לכן $L = K(\alpha)$ אז $\text{irr}(\alpha) = x^{p^n} - a$ ולכן $[L : K] = p^n$.

2. יהי F הסגור הפריד של K בתוך L (לכן $K \subseteq F \subseteq L$). אזי F/K פרידה ולכן $[F : K]_S = [F : K]$. L/F אי פרידה טהורה ולכן $[L : F]_S = 1$. מכאן,

$$\frac{[L : K]}{[L : K]_S} = \frac{[L : F] \cdot [F : K]}{[L : F]_S [F : K]_S} = \frac{[L : F] [F : K]}{1 \cdot [F : K]} = [L : F]$$

ו- $[L : F]$ חזקה של p מסעיף קודם.

□

הגדרה. תהי L/K סופית. אז $[L : K]_i = \frac{[L : K]}{[L : K]_S}$ נקראת מעלת אי פרידות של L/K .

מתקיים $[L : K] = [L : K]_S [L : K]_i$.

מסקנה. הרחבה סופית L/K היא פרידה $\Leftrightarrow [L : K]_i = 1$.

מסקנה. אם $K \subseteq L \subseteq M$ הרחבה סופית, אז $[M : K]_i = [M : L]_i [L : K]_i$.

משפט. יהי $\text{chr } K = p > 0$, תהי L/K נורמלית ויהי F הסגור הפריד של K בתוך L . תהי H חבורת האוטומורפיזמים של L מעל J ויהי $E = L^H$ (שדה השבת שלה). אזי E/K אי פרידה טהורה וכן L/E פרידה. כמו כן מתקיים $EF = L$, $E \cap F = K$.

הוכחה. בה"כ ניתן להניח $L \subseteq \tilde{K}$. ראשית נראה E/K אי פרידה טהורה. יהי $\sigma \in \text{Isom}_K(E, \tilde{K})$. אפשר להרחיב אותו לשיכון K - $\tilde{K}$ $\sigma' : L \rightarrow \tilde{K}$. $\sigma' \in H$ כלומר $\sigma'(L) = L$ לכן σ' משביתה את E (מהגדרת E) כלומר $\sigma = 1_E$ ולכן מקריטריון הראשון לאי פריקות טהורה E/K אי פרידה טהורה.

כעת נראה L/E פרידה. יהי $\alpha \in L$. אז α אלגברי מעל K ולכן גם מעל E . אם $\sigma \in H$ אז גם $\sigma(\alpha)$ שורש של $\text{irr}(\alpha, E)$ לכן $\Sigma := \{\sigma(\alpha) : \sigma \in H\}$ סופית. יהיו $\sigma_1, \dots, \sigma_r \in H$ $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ הם כל האיברים השונים של Σ . נניח בה"כ $\sigma_1 = 1_L$ (כי קיים i המקיים $\sigma_i = 1_L$ מהגדרת H).

אם $\tau \in H$ אז $\tau \sigma_1(\alpha), \dots, \tau \sigma_r(\alpha) \in \Sigma$ שונים זה מזה. לכן $\tau \sigma_1(\alpha), \dots, \tau \sigma_r(\alpha)$ של $\sigma_1, \dots, \sigma_r$.

יהי $\tau(f) = \prod_{i=1}^r (x - \tau \sigma_i(\alpha)) = f$ אם $\tau \in H$. אז $L[x] \ni f = \prod_{i=1}^r (x - \sigma_i(\alpha))$ לכן $f \in E[x]$ (מהגדרת E). α שורש של f ואין ל- f שורשים מרובים. כיוון ש- f אי פרידה L/E גם ל- $\text{irr}(\alpha, E)$ אין שורשים מרובים. לכן α פריד מעל E ולכן L/E פרידה. כעת נוכיח את שתי הזהויות:

L/E פרידה ולכן גם L/EF פרידה. L/F אי פרידה טהורה ולכן L/EF אי פרידה טהורה. לכן $L = EF$.

באותו אופן F/K פרידה, לכן גם $F \cap E/K$ פרידה. E/K אי פרידה טהורה ולכן $F \cap E/K$ אי פרידה טהורה ולכן $F \cap E = K$. □