

אלגברה ב' 2 – הרצאה 22

18.5.11

הרחבות פתירות (הרחבות $\mathcal{C}$)

$\mathcal{C}$ – משפחה של חבורות סופיות. ביתר דיוק, קבוצת מחלקות האיזומורפיזם של חבורות סופיות. נכתוב $G \in \mathcal{C}$ אם G איזומורפית לחבורה ב- $\mathcal{C}$.

הגדרה. משפחה $\mathcal{C}$ תקרא מלאה אם היא סגורה תחת לקיחת תת חבורות, חבורות מנה, מכפלות ישירות של מספר סופי של חבורות והרחבות (כלומר אם G סופית, $N \in \mathcal{C}$, $N \triangleleft G$, $N \in \mathcal{C}$, $N \triangleleft G$, אז גם $G/N \in \mathcal{C}$). באופן שקול הסדרה הבאה מדויקת:

$$1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1$$

דוגמאות.

1. $\mathcal{C}$ – כל החבורות הסופיות.

2. $\mathcal{C}$ – חבורות p (עבור p ראשוני).

3. $\mathcal{C}$ – חבורות פתירות.

תזכורת. G פתירה אם יש $G_0 = G \triangleleft G_1 \triangleleft \dots \triangleleft G_n = \{1\}$ כאשר G_{i-1}/G_i חבורה אבלית לכל i , או באופן שקול G_{i-1}/G_i ציקלית לכל i .

דוגמא לחבורה לא מלאה: $\mathcal{C}$ – חבורות אבליות. היא איננה סגורה תחת הרחבות (ובכתיב סדרה מדויקת זה נראה כך: $1 \rightarrow A_3 \rightarrow S_3 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$). כעת נסתכל על $\mathcal{C}$ מלאה.

הגדרה. הרחבת שדות L/K נקראת הרחבת- $\mathcal{C}$ אם יש הרחבת גלואה L'/K כך ש- $\text{Gal}(L', K) \in \mathcal{C}$ וכן $K \subseteq L \subseteq L'$.

באופן שקול, L/K היא הרחבת- $\mathcal{C}$ אם L/K פרידה סופית וכן עבור $\hat{L}$ סגור גלואה של L/K מתקיים $\text{Gal}(\hat{L}/K) \in \mathcal{C}$. מקרים פרטיים: הרחבות פתירות, הרחבות p .

משפט. יהיו $K \subseteq L$, $F \subseteq M$ שדות, כאשר כל השדות מוכלים ב- $\tilde{M}$ סגור אלגברי.

1. M/K הרחבת $\mathcal{C}$ $\Leftrightarrow M/L$ הרחבת $\mathcal{C}$, L/K הרחבת $\mathcal{C}$.

2. אם L/K הרחבת $\mathcal{C}$ אז FL/F הרחבת $\mathcal{C}$.

3. אם L/K , F/K הרחבות $\mathcal{C}$ אז LF/K הרחבת $\mathcal{C}$.

הוכחה.

2. לפי הגדרת הרחבת $\mathcal{C}$, קיימת L/K גלואה כך ש- $L \subseteq L' (\subseteq \tilde{M})$ וגם $\text{Gal}(L'/K) \in \mathcal{C}$. אזי $L'F/F$ גלואה. כמו כן,

$$\text{Gal}(L'F/F) \cong \text{Gal}(L'/L' \cap F) \leq \text{Gal}(L'/K) \in \mathcal{C}$$

לכן, $\text{Gal}(L'F/F) \in \mathcal{C}$ וכמו כן $LF \subseteq L'F$ ולכן $LF \in \mathcal{C}$.

3. מהגדרת הרחבת $\mathcal{C}$ יש $F'/K, L'/K$ הרחבות גלואה כך ש- $F' \subseteq F, L' \subseteq L$ וגם $\text{Gal}(F'/K), \text{Gal}(L'/K) \in \mathcal{C}$. לכן $L'F'/K$ גלואה וכן,

$$\text{Gal}(L'F'/K) \leq \text{Gal}(L'/K) \times \text{Gal}(F'/K) \in \mathcal{C}$$

לכן, $\text{Gal}(L'F'/K) \in \mathcal{C}$, $LF \subseteq L'F'$ ולכן $LF \in \mathcal{C}$.

1. $\Leftarrow$ לפי הגדרת הרחבת $\mathcal{C}$, קיימת M'/K גלואה כך ש- $M \subseteq M'$ וכן $\text{Gal}(M'/K) \in \mathcal{C}$. בפרט, $L \subseteq M$ ולכן L/K הרחבת $\mathcal{C}$.

$$\text{Gal}(M'/L) \leq \text{Gal}(M'/K) \in \mathcal{C}$$

ולכן $\text{Gal}(M'/L) \in \mathcal{C}$ וכיוון שגם $M \subseteq M'$ אז M/L הרחבת $\mathcal{C}$.

$\Rightarrow$ ניתן להניח בה"כ כי L/K גלואה (אחרת נחליף את L בסגור האלגברי של L/K , ואז $M \subseteq ML'$, נקבל (מההגדרות) כי L'/K הרחבת $\mathcal{C}$, ולפי שני נקבל ML'/L' הרחבת $\mathcal{C}$. מכאן נוכיח כי ML'/K הרחבת $\mathcal{C}$, ומהצד הראשון של הסעיף נקבל M/K הרחבת $\mathcal{C}$. כלומר, אנ נחליף את L ב- L', M ב- ML' . כך L/K תהא הרחבת גלואה ואז נסיק את רצוננו. ולכן נוכל להניח מראש כי L/K הרחבת גלואה.

יהיו $1 = \sigma_1, \sigma_2, \dots, \sigma_m$ כך אברי $\text{Isom}_k(M, \tilde{M})$. נסמן $\hat{M} := \sigma(M) \cdots \sigma_m(M)$. כיוון ש- M/L הרחבת $\mathcal{C}$ גם $\sigma_i(M)|\sigma_i(L)$ הרחבות $\mathcal{C}$. אבל, L/K גלואה ולכן $\sigma_i(L) = L$ לכל i . לפי הסעיף השני (ובעזרת אינדוקציה על m) נקבל כי $\hat{M}/L$ הרחבת $\mathcal{C}$. $M/L, L/K$ פרידות וסופיות, לכן M/K פרידה וסופית. לכן, יש $\alpha \in M$ כך ש- $M = K(\alpha)$. כמו כן, $\sigma_1(\alpha), \dots, \sigma_m(\alpha)$ הם כל שורשי $\text{irr}(\alpha, K)$. לכן מתקיים:

$$\hat{M} = \sigma(M) \cdots \sigma_m(M) = K(\sigma(\alpha)) \cdots K(\sigma(\alpha)) = K(\sigma_1(\alpha), \dots, \sigma_m(\alpha))$$

כלומר $\hat{M}$ הוא שדה הפיצול של $\text{irr}(\alpha, K)$ מעל K . לכן $\hat{M}/K$ נורמלית, ולכן $\hat{M}/K$ הרחבת גלואה (כי $\hat{M}/L$ פרידה בצירוף של הרחבות פרידות $\sigma_i(M)|L$ ואז גם $\hat{M}/K$ פרידה).

לכן, קיבלנו $\hat{M}/K$ גלואה, $L/K, \hat{M}/L$ הרחבות $\mathcal{C}$. לפי הסדרה המדויקת הבאה:

$$1 \rightarrow \underbrace{\text{Gal}(\hat{N}/L)}_{\in \mathcal{C}} \rightarrow \text{Gal}(\hat{M}/K) \rightarrow \underbrace{\text{Gal}(L/K)}_{\in \mathcal{C}} \rightarrow 1$$

נקבל כי $\text{Gal}(\hat{M}/K) \in \mathcal{C}$ וכיוון ש- $M \subseteq M'$ אז M/K הרחבת $\mathcal{C}$.

□

כעת נדבר על שדות עם אפיון 0 ונסתכל על $\mathcal{C}$ בתור החבורות הפתירות.

הגדרה. L/K נקראית רדיקלית אם קיימים $\alpha \in L, n \in \mathbb{N}$ כך ש- $L = K(\alpha)$ וגם $\alpha^n \in K$.

תרגיל. אם L/K רציונלית אז L/K פתירה.

הוכחה. עבור r_n שורש יחידה n , $K \subseteq L \subseteq K(\alpha, r_n)$. לכן די להראות כי $K(r_n, \alpha)/K$ פתירה. כמו כן $K \subseteq K(r_n) \subseteq K(\alpha, r_n)$, לכן די להראות כי $K(r_n)/K$ פתירה. מתקיים $K(r_n, \alpha)/K(r_n)$ פתירות. (כתת חבורה של $\mathbb{Z}/n\mathbb{Z}$) ולכן פתירה וכן

□

$K(r_n, \alpha)/K(r_n)$ מעגלית ולכן פתירה.

נסתכל על פולינום $f \in K[x]$ ונסתכל על המשוואה $f(x) = 0$. נאמר שהמשוואה פתירה אם יש שורש $\alpha \in \bar{K}$ שאפשר למצוא בעזרת איברי K , פעולות $+, \cdot, ^{-1}, \sqrt[n]{}$ כאשר $n \in \mathbb{N}$.

הגדרה. עבור $f \in K[x]$ אי פריק, המשוואה $f(x) = 0$ פתירה אם:

1. קיימת סדרה (מגדל) של שדות

$$K = K_0 \leq K_1 \leq \dots \leq K_k = L$$

כאשר K_i/K_{i-1} רדיקלית לכל i .

2. ל- f יש שורש ב- L .

משפט. יהי $f \in K[x]$ אי פריק. יהי $\alpha \in \bar{K}$ שורש של f . אזי $f(x) = 0$ פתירה $\Leftrightarrow K(\alpha)/K$ פתירה.

הוכחה. $\Leftarrow$: לפי התרגיל K_i/K_{i-1} פתירה לכל i . לפי המשפט הקודם L/K פתירה $K(\alpha) \leq L$ ולכן $K(\alpha)/K$ פתירה (נזכור כי $\mathcal{C}$ היא חבורת כל הפתירות). $\Rightarrow$: יש F/K גלואה סופית כך ש- $K(\alpha) \subseteq F$, $G = \text{Gal}(F/K)$ פתירה, כלומר קיימת סדרה $G = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{k-1} \triangleleft G_k = 1$ כאשר G_{i-1}/G_i מעגליות לכל i . לכל i נסמן $F_i = F^{G_i}$, ונסמן $n = [F : K] = |G|$. מתקיים $K = F_0 \leq F_1 \leq \dots \leq F_k = F$ וכן $F_2 \leq \dots \leq F_k = F$, $\text{Gal}(F/K_i) = G_i$ לכל i , לכן F_i/F_{i-1} גלואה וכן $\text{Gal}(F_i/F_{i-1}) = G_{i-1}K_i$ מעגלית מסדר n . יהי $E = K(r_1, \dots, r_n)$ אז

$$K = K(r_1) \subseteq K(r_1, r_2) \subseteq \dots \subseteq EF_k = EF$$

לכל i מתקיים EF_i/EF_{i-1} הרחבת גלואה והחבורה שלה היא תת חבורה של $\text{Gal}(F_i/F_{i-1})$, לכן מעגלית מסדר $n_i \geq n$. כיוון ש- $r_{n_i} \in E \subseteq EF_{i-1}$ אז קיים α_i המקיים $EF_i = EF_{i-1}(\alpha_i)$ וגם $\alpha_i^{n_i} \in EF_{i-1}$. $K(r_1, \dots, r_t)/K(r_1, r_{t-1})$ מתקבלת ע"י צירוף שורש יחידה ולכן גם היא רדיקלית. כמו כן $\alpha \in F \subseteq EF$ ולכן $f(x) = 0$ פתירה. □

מסקנה. $f(x) = 0$ פתירה $\text{Gal}(f, K)$ חבורה פתירה.

הוכחה. $\text{Gal}(f, K) = \text{Gal}(L/K)$ עבור סגור אלגברי של $K(\alpha)/K$.

□

מסקנה. אם $\text{Gal}(f, K) = S_n$ או $\text{Gal}(f, K) = A_n$ עבור $n \geq 5$ אז המשוואה $f(x) = 0$ איננה פתירה. בפרט $t_1, \dots, t_n$ משתנים בלתי תלויים מעל שדה K_0 עבור $f(x) = x^n + t_1x^{n-1} + \dots + t_n \in K_0(t_0, \dots, t_n)[x]$ אינה פתירה אם $n \geq 5$.

בנייה בעזרת סרגל ומחוגה

מסקנה. נקודה $(a, b) \in \mathbb{R}^2$ ניתנת לבנייה מתוך נתונים פתיחה $\rho \Leftrightarrow Q(\rho) =$ קיימת סדרה $K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$ כך ש- $[K_i : K_{i-1}] = 2$ $a, b \in K_m$.

מסקנה. תנאי הכרחי לכך ש- (a, b) ניתנת לבנייה מתוך הוא $[K(a, b) : K]$ חזקה של 2 כאשר $K = Q(\rho)$.

הוכחה. $[K(a, b) : K][K_m : K] = 2^m$. □