

## הגדרה

נתון  $f \in F[\lambda]$ . נגדיר  $\text{Gal}_f = \text{חבורת גלואה של } E/F \text{ כאשר } E \text{ שדה הפיצול של } f \text{ מעל } F$ .

## הוכחנו

- I. אם  $G = \text{Gal}_f$  ו  $\deg f = n$  אז קיים שיכון  $G \hookrightarrow S_n$  ולכן  $|G| \mid n!$
- II. אם  $f = g \mid f$  אי פריק ו  $\deg g = m$  אז  $|G| \mid m$
- III. אם  $E \subseteq C$  ו  $E \not\subseteq \mathbb{R}$  אז  $|G| \mid 2$  כי הצמדה מצמצמת לאוטומורפיזמים אי טריניאלית של  $E$  (מסדר 2)

## הגדרה

$K$  הרחבה שורשית של  $F$  אם  $K = F[a]$  כאשר  $a^m \in F$  עבור אישהו  $m$ .

## דוגמאות

1. הרחבה ציקלוטומית ( $F[\rho]$  כאשר  $\rho$  שורש של 1)  $\text{Gal}(F[\rho]/F) \hookrightarrow \text{Kulen } n$  כאשר  $\rho$  שורש  $n$ -פרימיטיבי של 1 (=כאשר  $F = \mathbb{Q}$ )
2.  $\alpha \in F$  כאשר  $F[\sqrt[m]{\alpha}]$ . אם  $\rho_m \in F$  אז  $C_m = \langle \sigma \rangle = \text{Gal}(F[\sqrt[m]{\alpha}]/F)$  כאשר  $\sigma(\sqrt[m]{\alpha}) = \rho \sqrt[m]{\alpha}$  [זה נכון עבור  $m$  ראשוני או  $F = \mathbb{Q}$  כאשר  $\alpha \in \mathbb{Q}$  אינו ריבועי]

## הגדרה

נניח  $F \subseteq K$ . אומרים שקיים מגדל שורשי מ  $F$  ל  $K$  אם  $K \subseteq E$ , Galois  $E/F$ , ו  $F = F_0 \subset \dots \subset F_t = E$  כאשר כל  $F_{i+1}/F_i$  הרחבה שורשית  $F_{i+1} = F_i[a_i]$  כאשר  $a_i^{m_i} \in F_i$ . נגיד הגובה של המגדל הוא מקסימום  $\{m_0, \dots, m_{t-1}\}$ .

**נשים:**  $\heartsuit$  המגדל מתחיל ב  $F$  ומסתיים ב  $E$ , אבל אומרים שהוא מגדל מ  $F$  ל  $K$  כאשר  $F \subseteq K \subseteq E$ .

## למה מרכזית

נניח  $L = F[a]$ ,  $a^n \in F$  ו  $\rho_n \in F$ . אז קיים  $b \in F$  ואוטומורפיזם  $\sigma$  של  $L$  כך ש  $\sigma(b) = \rho_n b$  ולכן  $b^n \in F$ .

## הצדקה

$$\sigma(b) = \rho_n b \implies \sigma(b^n) = \rho_n^n b^n = b^n \therefore b^n \in L^{(\sigma)} = F$$

## הוכחה - LAGRANGE RESOLVEMENT

$$(\rho = \rho_n)$$

$$b = \underbrace{a}_{=\rho^n \sigma^{-n}(a)} + \rho \sigma^{-1}(a) + \rho^2 \sigma^{-2}(a) + \dots + \rho^{n-1}$$

$$\begin{aligned} \sigma(b_j) &= \rho^n \sigma^{-(n-1)}(a) \rho a + \rho^2 \sigma^{-1}(a) + \dots + \rho^{n-1} \sigma^{n-2}(a) = \\ &= \sum_{i=0}^{n-1} \rho^{ij} \sigma^{-i}(a) \end{aligned}$$

**טוענים:** קיים  $0 \leq j < n$  כך ש  $b_j \notin F$

**נוכיח:**

$$\sum \rho^{jk} b_j = \sum_{i=0}^{n-1} \sigma^{-i}(a_j) \sum_{j=0}^{n-1} \rho^{j(k+j)} = \dots$$

$$\sum_{j=0}^{n-1} \rho^{j(k+j)} = 0 \text{ אלא אם } i = -k \text{ ואז הוא } n \text{ . נמשך את החישוב:}$$

$$\dots = \sigma^{-(-k)}(a) n = n \sigma^k(a)$$

**נובע:** אם כל  $b_j \in F$  אז  $\forall_k n \sigma^k(a) \in F \iff a \in F$  . לכן איזוהו  $b_j \notin F$ .

### משפט

נניח  $[E:F] = m$  Galois,  $\rho_m! \in F$  . יש מגדל שורשי  $F$  מ  $E$  לגובה  $m \leq$   $\iff$   $\text{Gal}(E/F)$  פתירה עם כל מנה ממימד  $\leq m$  .  
 כלומר:

$$\begin{aligned} F &= F_0 \subset F_1 \subset \dots \subset F^t = E \\ &\quad \updownarrow \\ G &= \text{Gal}(E/F) \supset \text{Gal}(E/F_1) \supset \dots \supset \text{Gal}(E/F^t) = \{e\} \end{aligned}$$

### מסקנה

נניח  $K/F$  ספרבילי,  $[K:F] = m$ ,  $\rho_m! \in F$  - אז קיים מגדל שורשים  $\iff \text{Gal}(E/F)$  פתירה כאשר  $E$  סגור הנורמלי של  $K$ .

### מסקנה

אותו דבר בלי הנחה ש  $\rho_m! \in F$ .

### הוכחה

#### למה $(K/F)$ ספרבילי

נניח יש מגדל שורשים מ  $F$  ל  $K$  ו  $E$  סדור Galois של  $K$ . אז קיים מגדל שורשים מ  $F$  ל  $E$ . לכתוב:

$$F = F_0 \subset F_1 = F_0[a_0] \subset F_2 = F_1[a_1] \subset \dots \subset K = F_{t-1}[a_{t-1}]$$

כלומר

$$K = F[a_0, \dots, a_{t-1}] \quad a_i^{m_i} \in F_i$$

לכתוב

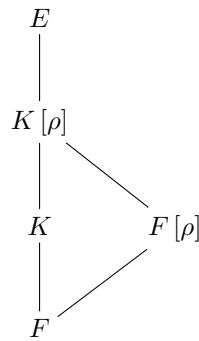
$$G = \text{Gal}(E/F) = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_v\}$$

נגדיר

$$L_1 = K$$

$$L_{10} \subset L_{10}[\sigma_2(a_0)] \subset L_{12}[\sigma_2(a_1)] \subset \dots \subset L_{1,t-1}[\sigma_2(a_{t-1})] = L_2$$

כלומר כל  $L_{1,j+1} = L_{1,j}[\sigma_2(a_j)]$



ברור:  $F[\rho]/F$  הרחבה שורשית. גם הרחבה Galois עם חבורת Galois אבליה. אם  $K/F$  בעל מגדל שורשים אז  $E/F$  בעל מגדל שורשים  $\iff E/F[\rho]$  בעל מגדל שורשים  $\iff \text{Gal}(E/F[\rho])$  פתירה(נכי בשרשרת של החבורות כל מנה ציקלית).  $H \triangleleft G$  פתירה ו  $G/H$  פתירה  $\iff G$  פתירה.

**הוכחנו:** מגדל שורשים  $\iff \text{Gal}(E/F)$  פתירה.

### חזרה להוכחת המשפט

$\text{Gal}(E/F)$  פתירה  $\iff$  קיים מגדל שורשים.  
 $\text{Gal}(E/F[\rho])$  פתירה בגלל שהיא תח"נ של  $\text{Gal}(E/F)$  (כל תח"נ של חבורה פתירה היא פתירה).  
יש מגדל שורשים ולפי המסקנה הקודמת מ' $F[\rho]$  ל' $F$  יש מגדל שורשים אחד ליחיד.