הגדרה

נתון $f \in F[\lambda]$. נגדיר Gal_f=חבורת גלואה של E/F כאשר E שדה הפיצול של f מעל F.

הוכחנו

I. אם $G = \mathrm{Gal}_f$ ו$\deg f = n$ אז קיים שיכון $G \hookrightarrow S_n$ ולכן $|G| \mid n!$

II. אם $g \mid f$ אי פריק ו$m = \deg g$ אז $m \mid |G|$

III. אם $E \subseteq C$ ו$E \not\subseteq \mathbb{R}$ אז $2 \mid |G|$ כי הצמדה מצמצמת לאוטומורפיזמים אי טריניאלית של E(מסדר 2)

הגדרה

K <u>הרחבה שורשית</u> של F אם $K = F[a]$ כאשר $a^m \in F$ עבור אישזהו m.

דוגמאות

1. הרחבה ציקלוטומית($F[\rho]$ כאשר ρ שורש של 1)
$\mathrm{Gal}(F[\rho]/F) \hookrightarrow \mathrm{Kulen}\, n$ כאשר ρ שורש n־פרימיטיבי של 1(=כאשר $F : \mathbb{Q}$)

2. $F[\sqrt[m]{\alpha}]$ כאשר $\alpha \in F$.
אם $\rho_m \in F$ אז $\mathrm{Gal}[F[\sqrt[m]{\alpha}] : F] = C_m = \langle\sigma\rangle$ 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 <u>מגדל שורשי</u> מF לK אם $K \subseteq E$, Galois E/F, ו$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_t = E$ 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 $\{m_0, \ldots m_{t-1}\}$.

נשים ♡: המגדל מתחיל בF ומסתיים בE, אבל אומרים שהוא מגדל מF לK 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 σ של L כך ש$\sigma(b) = \rho_n b$ ולכן $b^n \in F$.

הצדקה

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

הוכחה - LAGRANGE RESOLVEMENT

$$(\rho = \rho_n)$$

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

$$\sigma(b_j) = \rho^n \sigma^{-(n-1)}(a)\, \rho a + \rho^2 \sigma^{-1}(a) + \cdots + \rho^{n-1}\sigma^{n-2}(a) =$$

$$= \sum_{i=0}^{n-1} \rho^{ij} \sigma^{-i}(a)$$

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

נוכיח:

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

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

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

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

משפט

נניח $[E:F] = m$ Galois, $\rho_{m!} \in F$. יש מגדל שורשי מF לE מגובה $\le m$ $\iff$ $\mathrm{Gal}(E/F)$ פתירה עם כל מנה ממימד $\le m$.
כלומר:

$$F = F_0 \subset F_1 \subset \cdots \subset F^t = E$$
$$\Updownarrow$$
$$G = \mathrm{Gal}(E/F) \supset \mathrm{Gal}(E/F_1) \supset \cdots \supset \mathrm{Gal}(E/F^t) = \{e\}$$

מסקנה

נניח K/F ספרבילי, $[K:F] = m$, $\rho_{m!} \in F$ - אז קיים מגדל שורשים $\iff$ $\mathrm{Gal}(E/F)$ 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 מF לK וE סדור הGalois של K. אז קיים מגדל שורשים מF לE. לכתוב:

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

כלומר

$$K = F\left[a_0, \ldots a_{t-1}\right] \qquad a_i^{m_i} \in F_i$$

לכתוב

$$G = \mathrm{Gal}\left(E/F\right) = \left\{\sigma_1 = 1, \sigma_2, \ldots \sigma_v\right\}$$

נגדיר

$$L_1 = K$$

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

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

$$\begin{tikzcd}
E \arrow[d, dash] & \\
K\left[\rho\right] \arrow[d, dash] \arrow[dr, dash] & \\
K \arrow[d, dash] & F\left[\rho\right] \\
F \arrow[ur, dash] &
\end{tikzcd}$$

ברור: $F\left[\rho\right]/F$ הרחבה שורשית. גם הרחבה Galois עם חבורת Galois אבלית.

אם K/F בעל מגדל שורשים אז E/F בעל מגדל שורשים $\Longleftarrow$ $E/F\left[\rho\right]$ בעל מגדל שורשים $\Longleftarrow$ $\mathrm{Gal}\left(E/F\left[\rho\right]\right)$ פתירה(כי בשרשרת של החבורות כל מנה ציקלית).

$H \lhd G$ פתירה וG/H פתירה $\Longleftarrow$ G פתירה.

הוכחנו: מגדל שורשים $\Longleftarrow$ $\mathrm{Gal}\left(E/F\right)$ פתירה.

חזרה להוכחת המשפט

$\mathrm{Gal}(E/F)$ פתירה $\Longleftarrow$ קיים מגדל שורשים.

$\mathrm{Gal}(E/F[\rho])$ פתירה בגלל שהיא תח"נ של $\mathrm{Gal}(E/F)$(כל תח"נ של חבורה פתירה היא פתירה).

יש מגדל שורשים ולפי המסקנה הקודמת מ$F[\rho]$ לF יש מגדל שורשים אחד ליחיד.