הגדרה

שדה F הוא מושלם(Perfect) אם כל הרחבה סופית(כלומר ממימד סופי) היא ספרבילית.

משפט

I. כל שדה ממאפיין 0 הוא מושלם.

II. כל שדה סופי הוא מושלם.

הוכחה

צריך להוכיח: אם $f \in F\left[\lambda\right]$ אי פריק אז הוא ספרבילי.

I. הוכחנו כי $f' = 0 \Longleftarrow f$ קבוע.

II. ניקח $K = {}^{F[\lambda]}/_{F[\lambda]f}$.

$$|K| = |F|^{[K:F]} = |F|^{\deg f} < \infty$$

לכן K שדה פיצול של $\lambda^{|K|} - \lambda$ ספרבילי, וf מחלק אותו $\Longleftarrow$ f ספרביליל.

טענה

עבור ρ שורש n־פרימיטיבי של 1

$$(U(n) =) \qquad \text{Lulen}(n) \equiv \underbrace{\text{Gal}\left(Q\left[p\right]_G / \mathbb{Q}\right)}_{G}$$

הוכחה

הוכחנו: פולינום הציקלוטומי f_n הוא אי פריק מעל $\mathbb{Q}$(מדרגה $\varphi(n)$). לכן $|G| = |\text{Lulen}(n)|$. לכל $1 < i < n$ עבור $(i,n) = 1$ יש אוטומורפיזם σ_i של $\mathbb{Q}\left[\rho\right]$ לפי $\rho \mapsto \rho^i$. לכן אפשר להגדיר העתקה חח"ע ועל $\varphi : \underset{i \mapsto \sigma_i}{\text{Lulen} \to} G$ לפי $\psi(ij) = \sigma_{ij}$

$$\sigma_{jk} = \sigma_{ij} : \rho \to \rho^{ij} = \left(p^i\right)^j = \left(\sigma_i\left(\rho\right)\right)^j = \sigma_j \sigma_i\left(\rho\right)$$

משפט

אם ${}^{K}/_{F}$ הרחבה ספרבילית(ממימד סופי) אז קיים רק מס' סופי של שדות ביניים.

הוכחה

ניקח סגור הנורמלי E של K.
E/F Galois. מס' שדות ביניים ($E \subseteq L \subseteq F$) הוא $\infty > [K:F]! \geq [E:F] =$
$|\mathrm{Gal}\,(E/F)|$.

המשפט הראשי(השני?) של תורת Galois

I. אם E/F Galois ו$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset \{e\}$ תת חבורות אז

$$E^G = F \subseteq E^{G_1} \subset \cdots \subset E^{\{e\}} = E$$

שרשרת של שדות ביניים.

II. אם $F = F_0 \subset F_1 \subset \cdots \subset F_t = E$ אז

$$\mathrm{Gal}\,(E/F) \supset \mathrm{Gal}\,(E/F_1) \supset \cdots \supset \mathrm{Gal}\,(E/F_t) = \{e\}$$

שרשרת תת חבורות של $G = \mathrm{Gal}\,(E/F)$ אז

$$E^{G_{i+1}}/E^{G_i} \iff G_{i+1} \lhd G_i$$

הרחבת Galois $\mathrm{Gal}\left(E^{G_{i+1}}/E^{G_i}\right) \cong {}^{G_i}/_{G_{i+1}}$

הוכחה

מיידי מהמשפט המרכזי.

הגדרה

G חבורה פתירה אם"ם יש סדרה כמו i עם כל $G_{i+1} \lhd G_i$ ו${}^{G_i}/_{G_{i+1}}$ אבלי.

עובדות

I. G פתירה $\iff$ $G^{(t)} = \{e\}$ לאיזשהו t.

$$G' = G^{(1)} = \left\langle aba^{-1}b^{-1} \middle| a, b \in G \right\rangle$$

$$G^{(i+1)} = \left(G^{(i)}\right)'$$

$$G \supset G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

II. אם G פתירה(סופית)אז אפשר לעדן את הסדרה כך שכל מנה היא ציקלית מסדר ראשוני.

III. אם G חבורת־p ־ כלומר $|G| = p^t$ ־ אז G פתירה, אפילו נילפוטנטית($ {}^{G_i}/_{G_{i+1}} \leq$
$Z\left({}^{G}/_{G_{i+1}}\right)$)

המשפט היסודי של האלגברה

אם $f \in \mathbb{C}[\lambda]$ אז f מתפרק.

הוכחה

מספיק להוכיח שיש לf שורש(אינדוקציה קלה)(נניח $\deg f > 1$)

מילון תרגום לשדות: I. אין לF שורש $\iff$ יש גורם אי פריק g של f מדרגה גדולה מ1 בלי שורש $\iff$ $1 < [K:F] < \infty$ עבור $K = {}^{F[\lambda]}/_{F[\lambda]g}$

II. אם $a \in \mathbb{C}$ אז $\sqrt{a} \in \mathbb{C}$. תרגום: אם $1 < [K:F] < \infty$ אז $[K:F] \neq 2$(לפי הנוסחה הריבועית).

III. אם $f \in \mathbb{R}[\lambda]$ ו$\deg f$ אי זוגי אז יש לf שורש. תרגום: אם $[K:\mathbb{R}] < \infty$ אז הוא זוגי.(אם $[K:\mathbb{R}]$ אי זוגי אז ניקח $a \in K \backslash \mathbb{C}$ ואז $\deg a \mid [K:\mathbb{R}]$ אי זוגי $\Longleftarrow$ הפולינום המינימלי אי זוגי לכן פריק)

המשך הוכחת המשפט

$$\begin{tikzcd}
K \arrow[d, no head] \\
\mathbb{C} \arrow[d, no head] \\
\mathbb{R}
\end{tikzcd}$$

נניח $1 < [K:\mathbb{C}] < \infty$. ניקח $a \in K \backslash \mathbb{C}$. אפשר להניח $K = \mathbb{C}[a]$. ניקח f פולינום המינימלי של a מעל $\mathbb{R}$(אפשר לקחת ff' במקום f). ניקח E סגור הנורמלי מעל $\mathbb{R}$.

$$\begin{tikzcd}
 & E \arrow[dl, no head] \arrow[d, no head] \\
L \arrow[ddr, no head] & K \arrow[d, no head] \\
 & \mathbb{C} \arrow[d, no head] \\
 & \mathbb{R}
\end{tikzcd}$$

$G = \mathrm{Gal}(E/\mathbb{R})$. ניקח H=תת חבורת סילו־2 של G ו $L = E^H$:

$$[L:\mathbb{R}] = \frac{[E:\mathbb{R}]}{[E:L]} = \frac{\overbrace{|G|}^{\text{odd}}}{|H|}$$

לכן $E^H = L = \mathbb{R} \Longleftarrow [L : \mathbb{R}] = 1$.
$E^G = \mathbb{R} = E^H$ לכן $\Longleftarrow G = H$, לכן $|G|$ חזקת 2 - נגיד 2^m. לכן $|\mathrm{Gal}\,(E/\mathbb{C})| =$
2^{m-1} <u>לכן פתירה</u>. לכן קיימת שרשרת $\mathbb{C} < F_2 < F_3 < \cdots < E$ כאשר $[F_2 : \mathbb{C}] = 2$,
בסתירה לעובדה הקודמת(אין הרחבה ריבועית של $\mathbb{C}$)