משפט שמאפיין הרחבות Galois

התנאים הבאים שקולים עבור $[E:F]<\infty$

I. E/F Galois (E שדה פיצול של פולינום ספרבילי)

II. $F=E^G$ לאישזהו חבורת אוטומורפיזם G של E.

III. E/F ספרבילי[1] ונורמלי.(ואז ב(ii) אפשר לקחת $G=\mathrm{Gal}\left(E/F\right)$

הוכחנו כבר $(i)\Longleftarrow(ii)\Longleftarrow(iii)$. נוכיח עבור $(i)\Longleftarrow(iii)$.

תזכורת: נניח $f\in F\left[\lambda\right]$ פולינום מינימלי של $a\in E$. אזי השורשים האחרים של f הם בדיוק $\{\sigma\left(a\right)|\sigma\in\mathrm{Gal}\left(E/F\right)\}$. (אמנם יכול להיות אמנם ש$F\left[a\right]\subsetneq E$ - אבל עדיין אוטומורפיזם צריך לשלוח את a לשורש אחר)

רוצים בעצם למצוא פולינום ספרבילי בF. כותבים: $E=F\left[a_1,\dots a_t\right]$(אפשר לכתוב את זה כי E/F ממימד סופי($[E:F]<\infty$)). ניקח f_i=פולינום המינימלי של a_i. $f=\prod\limits_{\text{no duplicates}}f_i$. אז f ספרבילי(כל a_i שורש של f) $\Longleftarrow$ E שדה פיצול של f.

דוגמה

בשדה סופי E, נניח $a\in E$ וf הפולינום המינימלי של a. אז השורשים האחרים של f הם $a^p,a^{p^2},\dots$.

הוכחה

כל אוטומורפיזם הוא חזקה של Frobinious $a\mapsto a^p$.

הגדרה

נתון K/F ספרבילי נוצר סופית(כלומר $[K:F]<\infty$). <u>הסגור הנורמלי</u> הוא השדה "הקטן ביותר" $K\subset E$ כך שE/F Galois.

הערה: אפשר להוכיח שהוא יחיד עד כדי איזומורפיזם.

טענה

נניח K/F ספרבילי ממימד סופי $K=F\left[a_1,\dots a_t\right]$(כאשר כל a_i אלגברי מעל F). אז סגור הנורמלי E של K הוא $F\left[\sigma_j\left(a_i\right)\middle|\begin{array}{c}\sigma_j\in\mathrm{Gal}\left(E/F\right)\\1\le i\le t\end{array}\right]$(הבנייה של E/F נמצאת בתוך ההוכחה)

[1] כלומר כל איבר שלו ספרבילי

הוכחה

ניקח f_i הפולינום המינימלי של a_i. $f = \prod_{\text{no duplicates}} f_i$.

E=שדה פיצול של f מעל F. אז E/F Galois.

כל $\prod_{j \text{ no duplicates}} (\lambda - \sigma_j(a_i)) = f_i$, לכן $f = \prod_{\substack{i,j \\ \text{no duplicates}}} (\lambda - \sigma_j(a_i))$, $\sigma_j \in \mathrm{Gal}(E/F)$.

לכן מקבלים את שדה הפיצול E של f אחרי שמוסיפים כל $\sigma_j(a_i)$ מעל F.

הערה

אם יש לנו תרשים

$$\begin{tikzcd}
 & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash, "3"'] & & L_2 \arrow[dl, dash, "3"] \\
 & F &
\end{tikzcd}$$

מה המימד של L_1L_2 מעל F? במבט ראשון זה יכול להיות 3 או 9 - אבל זה יכול להיות גם 6(כי כל מה שאפשר ללמוד מהתרשים זה שזה $3 \mid [L_1L_2 : F]$.

מסקנה

אם K/F ספרבילי ו$K = F[a_1, \dots a_t]$ עבור כל $\deg(a_i) = 2$, E=סגור הנורמלי אז $[E : F] = 2^u$ עבור איזשהו u(בניגוד לראשוניים גדולים מ2).

שאלה

האם $E^G = F \Longrightarrow G = \mathrm{Gal}(E/F)$?

הערה: יודעים $G \subseteq \mathrm{Gal}(E/F)$ לכן $|G| \leq \mathrm{Gal}(E/F) = [E : F]$

למת Antim

אם G חבורת אוטומורפיזמים של שדה E אז $\left[E : E^G\right] \leq |G|$

הוכחה

לכתוב $G = \{\sigma_1, \dots \sigma_n\}$. ניקח איברים $a_1, \dots a_m \in E$. עבור $m > n$, טוענים $a_1, \dots a_m$ תלויים מעל E^G(זה נותן את הלמה).

עבור $1 \leq j \leq n$, ניקח $n \sum_{i=1}^{m} \sigma_j(a_i) b_i = 0$ משוואות בנעלמים $b_1, \dots b_m$. לכן יש מרחב פתרונות V(ממימד $m-n$).

ניקח $(0) \neq (b_1, \dots b_m) \in V$ עם מספר מרכיבים$\neq 0$ מינימלי. נניח $b_1 \neq 0$(לפי סידור חדש של האינדקסים).

$$\frac{1}{b_1}(b_1, \dots b_m) = \left(1, \frac{b_2}{b_1}, \dots \frac{b_m}{b_1}\right) \in V$$

לכן אפשר להניח $b_1 = 1$.

נשים ♡: אם $\sigma \in G$ ו$(b_1, \dots b_m) \in V$ אז $(\sigma(b_1), \dots \sigma(b_m)) \in V$. סיבה:

$$\sum \sigma_j(a_i) \sigma(b_i) = \sigma\left(\sum_i \sigma^{-1}\sigma_j(a_i) b_i\right) = \sigma(0) = 0$$

לכן

$$(\sigma(1), \sigma(b_2), \dots \sigma(b_n)) = (1, \sigma(b_2), \dots \sigma(b_n)) \in V$$

$$(1, b_2, \dots b_n) \in V$$

$$\implies (0, \sigma(b_2) - b_2, \dots \sigma(b_n) - b_n) \in V$$

וקיבלנו שיש לנו עוד מרכיב שווה לאפס - אבל הנחנו מינימליות של מרכיבים שונים מאפס, ולפי ההנחה הזו $\forall_i \sigma(b_i) = b_i$, וזה נכון לכל $\sigma \in G$, לכן $\forall_i b_i \in E^G$.

מסקנה

אם $E^G = F$ אז $G = \mathrm{Gal}(E/F)$.

הוכחה

$$[E:F] \overset{\text{Antin Lemma}}{\leq} |G| \leq |\mathrm{Gal}(E/F)| = [E:F]$$

לכן

$$|G| = |\mathrm{Gal}(E/F)|$$

$$\implies G = \mathrm{Gal}(E/F)$$

המשפט היסודי של תורת Galois

נניח E/F Galois, $[E:F]<\infty$. יש התאמה חח"ע בין תת חבורות של $G=\mathrm{Gal}\left(E/F\right)$ ושדות ביניים $F\subseteq L\subseteq E$ ($H<G$) לפי

$$\begin{tikzcd} E^H \arrow[d] & H \arrow[l] \\ L \arrow[r] & \mathrm{Gal}\left(E/L\right) \end{tikzcd}$$

$$E^{H_1}\supseteq E^{H_2} \iff H_1\subseteq H_2$$

$$|H|=\left[E:E^H\right] \qquad \left|\frac{G}{H}\right|=\left[E^H:F\right]$$

$$H:=\mathrm{Gal}\left(E/L\right) \iff \text{Galois}$$

הוא תת חבורה נורמלית של G ואז $\mathrm{Gal}\left(l/F\right)\cong {}^{G}/_{H}$.

הוכחה

צ"ל:

I. $E^{\mathrm{Gal}(E/L)}=L$

II. $\mathrm{Gal}\left(E/E^H\right)=H$

I. E/L Galois כי E/F Galois. ניקח L במקום F במשפט I.

II. לפי מסקנת למת ארטין(H במקום G).

$$\Longleftarrow \text{Galois } E/E^H$$

$$|H| \overset{\text{according to } (II)}{=} \left|\mathrm{Gal}\left(E/E^H\right)\right| \overset{\text{accoring to old theorem}}{=} \left[E:E^H\right]$$

הוכחת הטענה האחרונה

$$\sigma\tau\sigma^{-}\left(\sigma\left(a\right)\right)=\sigma\tau\left(a\right)$$

לכן

$$\sigma\tau\sigma^{-1}\left(\sigma\left(a\right)\right)=\sigma\left(a\right) \iff \tau\left(a\right)=a$$

$$\sigma\left(E^H\right)=E^{\sigma H\sigma^{-1}}$$

(ניקח כל $\tau\in H$)
(הוכחנו לכל $\sigma\in$)

עכשיו נניח $F \subset L \subset E$

$$H = \mathrm{Gal}\left(E/L\right) \qquad L = E^H$$

אם L/F הרחבה נורמלית, אז $\sigma\left(L\right) = L$

$$\therefore E^{\sigma H \sigma^{-1}} = \sigma\left(E^H\right) = \sigma\left(L\right) = L = E^H$$

$$\therefore \forall_{\sigma \in G} \sigma H \sigma^{-1} = H$$

ולכן $H \lhd G$.

אם $H \lhd G$ אז $\sigma H \sigma^{-1} = H$ ולכן

$$L = E^H = E^{\sigma H \sigma^{-1}} = \sigma\left(E^H\right) = \sigma\left(L\right)$$

לכן הפולינום המינימלי של כל איבר של L מתפצל מעל L, ולכן F נורמלי.

לכן L/F Galois. כדי לחשב $\mathrm{Gal}\left(L/F\right)$ יש הומומורפיזם $\begin{array}{ccc} \mathrm{Gal}\left(E/F\right) & \to & \mathrm{Gal}\left(L/F\right) \\ \sigma & \mapsto & \sigma|_L \end{array}$.

$$\ker \Phi = \{\sigma \in \mathrm{Gal}\left(E/F\right) | \, \sigma|_L = 1\} = \mathrm{Gal}\left(E/L\right)$$

$$\bar{\Phi} : {}^{\mathrm{Gal}(E/F)}/_{\mathrm{Gal}(E/L)} \hookrightarrow \mathrm{Gal}\left(L/F\right)$$

נושא חדש - בניית מספרים באופן גיאומטרי

נקודות בעלות בנייה הן נקודות במישור המרוכב שאפשר לבנות אותן באמצעות מחוגה וסרגל.

תרגיל

עבור כל נקודה בעלת בנייה $a \in \mathbb{R}$ יש שרשרת של הרחבות ריבועיות $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_t$ כאשר $a \in F_t$.

מסקנה

אם a בעל בנייה, אז $\deg(a)$ חזקה של 2, כי הוא מחלק 2^t.