

## משפט שמאפיין הרחבות Galois

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

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

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

III.  $E/F$  ספרבילי<sup>1</sup> ונורמלי. (ואז ב(ii) אפשר לקחת  $G = \text{Gal}(E/F)$ )

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

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

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

### דוגמה

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

### הוכחה

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

### הגדרה

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

**הערה:** אפשר להוכיח שהוא יחיד עד כדי איזומורפיזם.

### טענה

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

<sup>1</sup> כלומר כל איבר שלו ספרבילי

## הוכחה

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

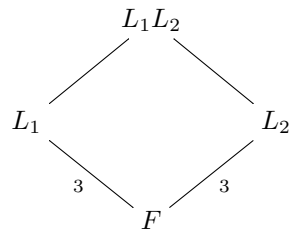
$E =$  שדה פיצול של  $f$  מעל  $F$ . אז  $E/F$  Galois. כל  $(\lambda - \sigma_j(a_i)) = f_i$  לכן  $(\lambda - \sigma_j(a_i))$  no duplicates  $\sigma_j \in \text{Gal}(E/F)$ .

$$f = \prod_{\substack{i,j \\ \text{no duplicates}}} (\lambda - \sigma_j(a_i))$$

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

## הערה

אם יש לנו תרשים



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  $[L_1L_2 : F] \mid 3$ ).

## מסקנה

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

## שאלה

האם  $E^G = F \iff G = \text{Gal}(E/F)$ ?

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

## למת Antim

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

## 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  $\sum_{i=1}^m \sigma_j(a_i) b_i = 0$  משוואות בנעלמים  $b_1, \dots, b_m$ . לכן יש מרחב פתרונות  $V$  (ממימד  $m - n$ ).  
 ניקח  $(b_1, \dots, b_m) \in V$  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  $\heartsuit$ : 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  $G = \text{Gal}(E/F)$ .

## הוכחה

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

לכן

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

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

## המשפט היסודי של תורת Galois

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

$$\begin{array}{ccc} E^H & \longleftarrow & H \\ \downarrow & & \\ L & \longrightarrow & \text{Gal}(E/L) \end{array}$$

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

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

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

הוא תת חבורה נורמלית של  $G$  ואז  $G/H \cong \text{Gal}(L/F)$ .

### הוכחה

$$E^{\text{Gal}(E/L)} = L \quad \text{I} \quad \text{צ"ל:}$$

$$\text{Gal}(E/E^H) = H \quad \text{II}$$

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

II. לפי מסקנת למת ארטיין ( $H$  במקום  $G$ ).

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

$$|H| \stackrel{\text{according to (II)}}{=} |\text{Gal}(E/E^H)| \stackrel{\text{according to old theorem}}{=} [E : E^H]$$

### הוכחת הטענה האחרונה

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

לכן

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

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

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

עכשיו נניח  $F \subset L \subset E$

$$H = \text{Gal}(E/L) \quad L = E^H$$

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

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

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

ולכן  $H \triangleleft G$ .

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

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

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

$$\begin{array}{ccc} \text{Gal}(E/F) & \rightarrow & \text{Gal}(L/F) \\ \sigma & \mapsto & \sigma|_L \end{array}$$

לכן  $L/F$  Galois. כדי לחשב  $\text{Gal}(L/F)$  יש הומומורפיזם

$$\ker \Phi = \{\sigma \in \text{Gal}(E/F) \mid \sigma|_L = 1\} = \text{Gal}(E/L)$$

$$\bar{\Phi} : \text{Gal}(E/F)/\text{Gal}(E/L) \hookrightarrow \text{Gal}(L/F)$$

## 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  $\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_t$  כאשר  $a \in F_t$ .

### מסקנה

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