

## בפעם שעברה

נניח  $E$  שדה פיצול של פולינום  $f \in F[\lambda]$ .  $[E : F] = |\text{Gal}(E/F)|$  ויש שוויון כאשר אין ל- $f$  שורש כפול ב- $E$ .  
הוכחנו עבור  $f$  אי פריק ש- $\deg f \mid [E : F]$

## הגדרה

$f \in F[\lambda]$  פולינום ספרבילי אם אין ל- $f$  שורש כפול בשדה הפיצול.

## הגדרה

נתון

$$\sum_{i=0}^t \alpha_i \lambda^i = f \in F[\lambda]$$

נגדיר

$$f' = \sum_{i=1}^t i \alpha_i \lambda^{i-1}$$

## טענה

$f$  ספרבילי  $\iff$  אין ל- $f, f'$  שורש משותף.

## הוכחה

( $\Leftarrow$ ) נניח בדרך השלילה שיש ל- $f, f'$  שורש משותף  $a$ .

$$f = (\lambda - a)g$$

$$f' = g + (\lambda - a)g'$$

$$(\lambda - a) \mid f'$$

$$(\lambda - a) \mid g \iff$$

$$(\lambda - a)^2 \mid (\lambda - a)g = f \iff$$

$$f = (\lambda - a)^2 h \text{ אם } (\implies)$$

$$f' = 2(\lambda - a)h + (\lambda - a)^2 h' = (\lambda - a)(2h + h')$$

$$\implies (\lambda - a) \mid f'$$

## מסקנה

$f$  ספרבילי  $\iff f, f'$  זרים ב  $E[\lambda]$ .

## טענה

נניח ש  $K \subseteq L$  שדות כלשהם, ו  $f, g \in K[\lambda]$ . אז  $f, g$  זרים ב  $K[\lambda] \iff f, g$  זרים ב  $L[\lambda]$ .

## הוכחה

( $\implies$ ) קל וחומר

( $\impliedby$ )  $f, g$  זרים ב  $K[\lambda] \iff \exists p, q \in K[\lambda]$  כך ש  $fp + gq = 1$ . קל וחומר  $p, q \in L[\lambda]$  זרים ב  $L[\lambda]$

## טענה

$f$  ספרבילי  $\iff f, f'$  זרים.

## מסקנה

פולינום  $f$  אי-פריק הוא לא ספרבילי  $\iff f' = 0$ .

## הוכחה

$f$  לא ספרבילי  $\iff f, f'$  אינם זרים.  
ניקח  $g = (f, f')$  לא קבוע. אבל  $g \mid f$  ו  $1 \leq \deg g \leq \deg f' < \deg f$  - בסתירה לכך ש  $f$  אי פריק!

## מסקנה

אם  $\text{char}(F) = 0$  ו  $f$  אי פריק (עם  $\deg f \geq 1$ ) אז  $f$  ספרבילי.  
באופן כללי:

$$f = \sum \alpha_i \lambda^i \quad f' = \sum i \alpha_i \lambda^{i-1}$$

$$\forall_{i \geq 1} i \alpha_i = 0 \iff f' = 0$$

אם  $\text{char}(F) \neq 0$  ו  $\alpha_i = 0$   $\iff i \cdot 1 = 0 \iff p \mid i$   
נניח  $f$  אי פריק.  $f$  אי ספרבילי  $\iff f = \sum \alpha_i \lambda^{pi}$

## תרגיל(כן או לא?)

נניח  $f = f_1 \cdots f_t \in F[\lambda]$  שדה  $E_i$  שדה פיצול של  $f_i$ .  
אי פריקים שונים וספרבילים  $f_i \in F[\lambda]$

$$G = \text{Gal}(E/F) \quad G_i = \text{Gal}(E_i/F)$$

אז  $G \cong G_1 \times \cdots \times G_t$ .

### הערות

נניח  $f = f_1 \cdots f_t \in F[\lambda]$

I. אם  $f$  ספרבילי אז כל  $f_i$  ספרבילי.

II. נניח שהי  $f$  הם אי פריקים ושונים. אם  $f_1, \dots, f_t$  ספרבילים אז  $f$  ספרבילי.

הוכחת iii: נניח  $f$  אינו ספרבילי, כלומר  $a$  שורש כפול. לכן  $a$  שורש של  $f_i, f_j$   
 $f_i, f_j$  אינם זרים. ניקח  $g = (f_i, f_j)$ . אי פריקים.

### הגדרה

$E$  הרחבה Galua של  $F$  אם  $E$  פיצול של פולינום ספרבילי  $f$ .  
כותבים  $E/F$  הוא Galua.  
הוכחנו שאם Galua  $E/F$  אז  $|\text{Gal}(E/F)| = [E : F]$ .

### הגדרה

שדה בניינים בין  $E$  ו  $F$  הוא שדה  $L$  כך ש  $F \subseteq L \subseteq E$ .

### הערה

אם  $F \subseteq L \subseteq E$ ,  $\text{Gal}(E/L) \leq \text{Gal}(E/F)$ . קל וחומר

### דוגמה

$f = \lambda^4 - 2$ , שדה  $E$ .  
הפיצול של  $F$  מעל  $\mathbb{Q}[\sqrt[4]{2}, i] = \mathbb{Q}[\sqrt[4]{2}, i]$ , ו  $[E : \mathbb{Q}] = 8$ .  
 $\{1, \tau\} = \text{Gal}(E/\mathbb{Q}[\sqrt[4]{2}])$  צמוד מרוכב  $\tau$ .  
 $\text{Gal}(E/\mathbb{Q}[i])$  (ת"ל  $\lambda^4 - 2$  אי פריק מעל  $\mathbb{Q}[i]$ )  
 $0 \leq 4 \leq 3$ ,  $i^4 \sqrt[4]{2}$  שורשים 4  
 $\text{Gal}(E/\mathbb{Q}[i]) = 4$  נתון על ידי  $\langle \sigma \rangle$  כאשר  
 $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$

הוכחנו:  $\sigma, \sigma^2, \sigma^3, \sigma^4 = 1$  - שונים! לכן

$$G = \langle \sigma, \tau \rangle = \left\{ \sigma^i \tau^j \mid \begin{array}{l} 0 \leq i \leq 3 \\ 0 \leq j \leq 1 \end{array} \right\}$$

$$\tau \circ \tau^{-1} = \tau \circ \sigma$$

**נשים** ♡:  $\frac{|G|}{|\langle \sigma \rangle|} = 2 \iff \langle \sigma \rangle \triangleleft G \iff \tau \sigma \tau^{-1} \in \langle \sigma \rangle \iff \tau \sigma \tau^{-1} = \sigma^j$  כלומר  $\tau \sigma \tau^{-1} = \sigma^j$  לאיזשהו  $j$ .

לכן:

$$\tau \sigma \tau^{-1} \left( \sqrt[4]{2} \right) = \tau \sigma \left( \sqrt[4]{2} \right) = \tau \left( i \sqrt[4]{2} \right) = \tau(i) \tau \left( \sqrt[4]{2} \right) = -i \sqrt[4]{2} = \sigma^3 \left( \sqrt[4]{2} \right)$$

$$\tau \sigma \tau^{-1} = \sigma^3 \iff \text{לכן}$$

$$G \cong D_4$$

### איך לבדוק אם פולינום אי פריק?

האם  $x^4 + 7$  פריק מעל  $\mathbb{Q}$ ? לא! מה עם  $x^4 + 6$ ? גם לא!

אבל מה לגבי  $x^4 + 4$ ? לכאורה נראה שגם הוא אי פריק מעל  $\mathbb{Q}$ , אבל:

$$\begin{aligned} x^4 + 4 &= (x^2 - 2i)(x^2 + 2i) = (x - (1 + i))(x + (1 + i))(x - (1 - i))(x + (1 - i)) = \\ &= (x^2 - 2ix + 2)(x^2 + 2ix + 2) \end{aligned}$$

לעומת זאת, עבור  $x^4 + 9$  נקבל פירוק ב  $\mathbb{R}$  - אבל לא ב  $\mathbb{Q}$ ! למעשה יש משפט ש  $x^4 + p^2$  פריק אם  $p = 2$ . בעצם, השיטה היא קודם כל לפרק אותו מעל  $\mathbb{R}$ , ואז לראות אם אפשר להפוך את זה לפירוק מעל  $\mathbb{Q}$ .

### הגדרה

נניח  $H < \text{Gal}(E/F)$

$$E^H = \{a \in E \mid \sigma(a) = a \forall \sigma \in H\}$$

### הערה

$E^H$  שדה ביניים.

$$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$$

$$\sigma(ab) = \sigma(a)\sigma(b) = ab \iff \sigma(b) = b \text{ ו} \sigma(a) = a \text{ אם } \sigma(b) = b \text{ ו} \sigma(a) = a$$

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

## טענה

נניח  $E/F$  הרחבה Galua, אזי  $E^{\text{Gal}(E/F)} = F$ .

## הוכחה

יודעים ש  $[E : F] = |\text{Gal}(E/F)|$ .  
נגדיר  $L = E^{\text{Gal}(E/F)}$ .

$E/L$  הרחבה Galua (שדה פיצול של אותו פולינום ספרבילי)

$$[E : L] = |\text{Gal}(E/L)|$$

ו  $\text{Gal}(E/L) = \text{Gal}(E/F)$  לפי הגדרת  $L$  !!! לכן  $[E : L] = [E : F]$ , אבל  $F \subseteq L \subseteq E$ , לכן  $L = F$ .

## שדות סופיים

רוצים לדעת מה השדות הסופיים.

## דוגמה

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$$

## באופן כללי

אם  $F \leq E$  שדות, אז  $E$  שדה וקטורי מעל  $E$  עם בסיס  $l_1, \dots, l_t$ . אם שניהם סופיים,  $F \cong \mathbb{F}_p$  הוא שדה המאפיין. כל איבר כותבים באופן יחיד:

$$\sum_{i=1}^t \alpha_i l_i$$

מספר הבחירות הוא  $p \cdots p = p^t$ , לכן  $|E| = p^t$  כאשר  $t = [E : \mathbb{F}_p]$ .