

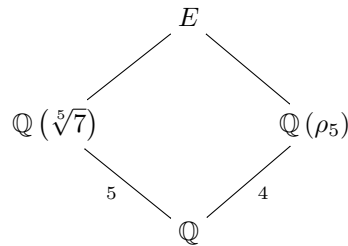
$$\mathbb{Z}_p^* = U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$$

## תרגיל

לחשב את חבורת גלואה של שדה הפיצול של  $f(x) = x^5 - 7$  מעל  $\mathbb{Q}$  (עד כדי איזומורפיזם)

## פתרון

$E/\mathbb{Q}$  שדה פיצול  $E = \mathbb{Q}(\sqrt[5]{7}, \rho_5)$  אי פריק לפי אייזנשטיין.



$$|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 20$$

$$\text{Gal}(E/\mathbb{Q}) \leq S_5$$

$$\text{Gal}(\mathbb{Q}(\rho_5)/\mathbb{Q}) \cong \mathbb{Z}_4$$

$$\text{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$$

$$\text{Gal}(\mathbb{Q}(\sqrt[5]{7})/\mathbb{Q}) = \{\text{Id}\}$$

(כי כל השורשים האחרים מרוכבים)

$20 \mid 5 \iff$  לפי קושי שקיים איבר מסדר 5 ב  $\text{Gal}(E/\mathbb{Q})$  שחייב להיות מחזור באורך 5.

הפולינום המינימלי של  $\rho_5$  נשאר אי פריק מעל  $\mathbb{Q}(\sqrt[5]{7})$ .

נטען שמתקיים  $\text{Gal}(E/\mathbb{Q}(\sqrt[5]{7})) \cong \mathbb{Z}_4$ . ניתן לבנות העתקה

$$\text{Gal}(E/\mathbb{Q}(\sqrt[5]{7})) \hookrightarrow \text{Gal}(\mathbb{Q}(\rho_5)/\mathbb{Q})$$

נבחר:

•  $\sigma$  מסדר 4 בתוך  $\text{Gal}(E/\mathbb{Q})$

•  $\tau$  מסדר 5 בתוך  $\text{Gal}(E/\mathbb{Q})$

ע"י

$$\sigma : \rho_5 \mapsto \rho_5^2, \sqrt[5]{7} \mapsto \sqrt[5]{7}$$

$$\sigma(\rho_5) = \rho_5^2 \quad \sigma^2(\rho_5) = \rho_5^4 \quad \sigma^3(\rho_5) = \rho_5^3 \quad \sigma^4(\rho_5) = \rho_5$$

$$\tau : \rho_5 \mapsto \rho_5, \sqrt[5]{7} \mapsto \rho_5 \sqrt[5]{7}$$

$G = \text{Gal}(E/\mathbb{Q})$  היא מסדר 20.

$$\langle \sigma \rangle \langle \tau \rangle = G$$

עכשיו:

$$\sigma\tau\sigma^{-1}(\rho_5) = \sigma\tau\sigma^3(\rho_5) = \sigma\tau(\rho_5^3) = \sigma(\rho_5^6) = \rho_5^6 = \rho_5$$

זוהו אומר שהאוטומורפיזם הזה קובע את  $\rho_5$ .

$$\sigma\tau\sigma^{-1}(\sqrt[5]{7}) = \sigma\tau(\sqrt[5]{7}) = \sqrt[5]{7}\sigma(\rho_5) = \rho_5^2\sqrt[5]{7}$$

$$\implies \sigma\tau\sigma^{-1} = \tau^2 \in \langle \tau \rangle \implies \langle \tau \rangle \triangleleft G$$

ולכן  $\langle \sigma \rangle \not\triangleleft G$  כי אחרת יש לנו מכפלה ישירה ואז  $\langle \sigma \rangle \simeq \mathbb{Z}_{20}$  שאינה ת"ח של  $S_5$ .

$$G = \left\langle \sigma, \tau \mid \begin{array}{l} \sigma^4 = 1, \tau^5 = 1 \\ \sigma\tau\sigma^{-1} = \tau^2 \end{array} \right\rangle : \text{אנחנו יודעים ש} G \text{ נוצרת ע"י שני יוצרים (עם יחסים):}$$

## תרגיל

נתון פולינום אי-פריק ב- $\mathbb{Q}[x]$  בעל שני שורשים מרוכבים "אמיתיים" ( $\mathbb{C} \setminus \mathbb{R}$ ) כך ש- $f(x)$  מדרגה  $p$  ראשונית.

הראו ש- $\text{Gal}(E/\mathbb{Q}) \simeq S_p$  כאשר  $E$  שדה הפיצול של  $f(x)$ .

## פתרון

$\text{Gal}(E/\mathbb{Q}) \leq S_p$  (כפועלת של שורשי  $f(x)$ ). יודעים גם ש- $|\text{Gal}(E/\mathbb{Q})|$  מתחלק ב- $p$  כי אם  $\alpha \in E$  שורש של  $f(x)$  אזי  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p \iff |\text{Gal}(E/\mathbb{Q})| \iff [E : \mathbb{Q}] = p$ . זה גורר שקיים מחזור מאורך  $p$  בחבורה.

מספיק להראות שהחבורה  $\text{Gal}(E/\mathbb{Q})$  מכילה חילוף. הצמדה מרוכבת מחליפה בין שני השורשים המרוכבים ולכן כוללת חילוף על השורשים. לכן קיים חילוף ב- $\text{Gal}(E/\mathbb{Q})$  (כי חילוף+מחזור מאורך  $p$  יוצרים את  $S_p$ ).

## הגדרה

הרחבה  $E/F$  נקראת פשוטה אם  $E = F(\alpha)$  ו- $\alpha$  נקרא איבר פרימיטיבי.

<sup>1</sup>אפשר גם לכתוב  $E = F[a]$  במקרה הזה זה לא באמת משפיע.

## משפט(לא לשימוש כרגע)

כל הרחבה ספרבילית סופית היא פשוטה.

### תרגיל

כל הרחבה סופית של שדה סופי היא הרחבה פשוטה.

### פתרון

$E/F, E^* = \langle a \rangle$  (שכן  $E^*$  ת"ח סופית כפלית של שדה ולכן צקלית). לכן  $E = F[a]$ .

### שאלה

מהי דרגת הפולינום של  $a$  מהשאלה הקודמת כאשר  $F = \mathbb{Z}_p$ ?

### פתרון

$|E| = p^t$ , ולכן  $\deg m_a = t$ :

$$\begin{array}{ccc} F(a) & \implies & \deg m_a = t \\ \left| \begin{array}{c} t \\ \deg M_a \end{array} \right. & & \\ \mathbb{Z}_p & & \end{array}$$

### מסקנה

קיים פולינום אי־פריק מכל דרגה מעל  $\mathbb{Z}_p$ .

### תרגיל

בתרגיל הקודם קיבלנו פולינום אי־פריק מדרגה  $t$  עם שורש  $a$ , כך ש  $a$  פרימיטיבי. מיהם שאר השורשים?

### תשובה

זה  $\phi : x \mapsto x^p$  אוטומורפיזם של שדה הפיצול. הוא מעביר את  $a$  לשורש אחר של  $a$ :

$$a, a^p, a^{p^2}, \dots, a^{p^{t-1}}$$

$\phi$  יוצר את חבורת גלואה שהיא מסדר  $t$ , ולכן  $\text{Id}(a), \phi(a), \phi^2(a), \dots, \phi^{t-1}(a)$  ולכן שונים



## תרגיל

הוכיחו או הפריכו:

$$E = \mathbb{Z}_p(a) \implies E^* = \langle a \rangle$$

## פתרון

נפריך ע"י דוגמה:  $\Phi_5 = x^4 + x^3 + x^2 + x + 1$  מעל  $\mathbb{Z}_2$ . (בדקו אי-פריק). דרגת ההרחבה היא 4.

$$E = \mathbb{Z}_2(\rho_5) \quad |E| = 16$$

אבל  $\rho_5$  לא יכול להיות היוצר של  $E^*$ , כי  $\rho_5^5 = 1$  כלומר  $\rho_5$  מסדר 5.