תרגול 13 - שלמות

- יש בדיוק שדה מסדר $q = p^n$ לכל p ראשוני, $n \geq 1$.
- השדה הזה יחיד ($\cong$) - שדה פיצול של $x^q - x$ (מעל $\mathbb{F}_p$)
- שדות סופיים הם אלמנטים - כל ההרחבות הן סופיות-נורמליות.
- $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n = \langle \Phi \rangle$

$$\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$
$$x \longmapsto x^p$$

① $f \in \mathbb{F}_p[x]$ אי"פ, $q = p^n$

$$\deg f \mid n \iff f \mid x^q - x$$

$\mathbb{F}_p[x]/\langle f \rangle \hookrightarrow \mathbb{F}_q \iff$ f אי"פ $\iff$ ל f שו' $\alpha \in \mathbb{F}_q$ מ"מ $0 = \alpha^q - \alpha$

② נזכר: $x^q - x = \prod_{d \mid n} \left(\prod_{\substack{f \text{ אי"פ} \\ \text{מתוקן} \\ \text{מדרגה } d}} f(x) \right)$

שורה תחתונה:

$$q = \sum_{d \mid n} d \cdot \underbrace{I_p(d)}_{\substack{\#\text{ הפולינומים ההי"פ} \\ \text{האי-פריקים מעל } \mathbb{F}_p \\ \text{מדרגה } d}}$$

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{יש ריבוע שמחלק את } n \\ (-1)^{\text{מס' הגורמים הראשוניים}} & \text{אחרת} \end{cases}$$

$$I_p(n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$$

דוגמה:

$$I_p(2) = \frac{1}{2}\left(\underbrace{\mu(1)}_{1} \cdot p^2 + \underbrace{\mu(2)}_{-1} p\right) = \frac{p^2 - p}{2}$$

מס' הפולינומים ההי"פ האי-פריקים מדרגה 2 מעל $\mathbb{F}_p$.

תרגיל: מצא דוגמה לחוג F_9/F_3 שאינו שדה. כמה איברים יש ב- $F_9^\times$? מצא את כל הסדרים האפשריים.

כמו כן: איברים ב- F_9 $\longleftrightarrow$ 6

$\cup$

איברים ב- $F_9^\times$ $\longleftrightarrow$ $\varphi(9-1) = 4$

$[F_9 : F_3] = 2 \Rightarrow$ ה-6 איברים האחרים נמצאים בשדה ביניים

(כי $\deg f_i = 3$) פירוק לגורמים אי-פריקים של

$$X^9 - X = (X^3 - X) \cdot \underbrace{f_1 \cdot f_2 \cdot f_3}_{X^6 + X^4 + X^2 + 1}$$

* $X^2 + 1$

* $\begin{cases} X^2 + X - 1 \\ X^2 - X - 1 \end{cases}$

$\alpha^2 + 1 = 0$

$\alpha^2 = -1$

$\alpha^4 = 1 \Rightarrow o(\alpha) = 4$

$\alpha \in \mathbb{F}_9^*$ יוצר!

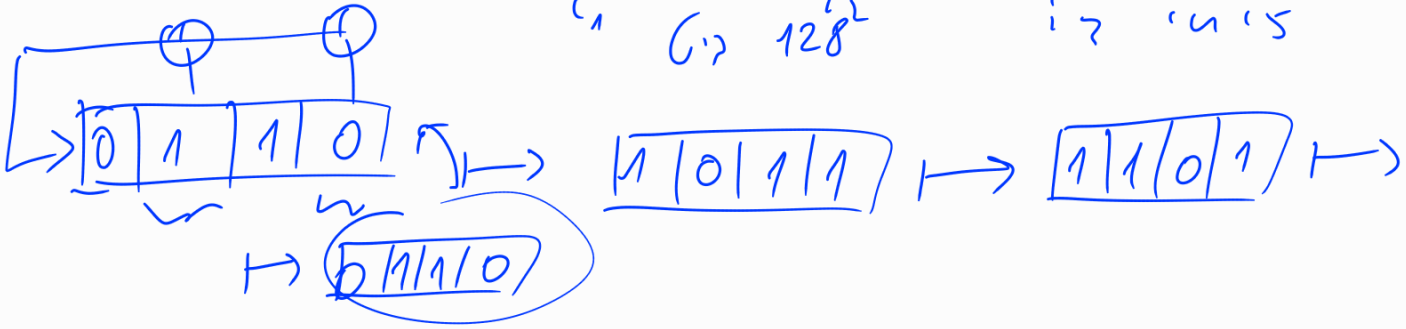
הגדרה: יהי $f(x) \in \mathbb{F}_q[x]$ פולינום הפיך. הסדר של f הוא המספר הטבעי הקטן ביותר e כך ש-$f(x) \mid x^e - 1$.

סדר של פולינום אי-פריק = סדר של שורש כלשהו של הפולינום.

Linear feedback shift register (LFSR):

$1 + x^{i_1} + x^{i_2} + x^{i_3} + x^{i_4} + x^{i_5}$

XOR = $\oplus$



סדרת הפלט של ה-LFSR מהווה סדרה מחזורית מעל $\mathbb{F}_2$ $\Leftarrow$ כל מחזור של ה-LFSR יכיל מספר אי-זוגי של אפסים ($2^n - 1$)

מסקנה – $1 + x^i + x^j$ מעל $\mathbb{F}_2$ שאינו שלו (מספר אי-זוגי של מונים.)

תרגיל: הוכיחו שקיים $a \in \mathbb{F}_{11}$ כך ש- $\mathbb{F}_{11}[x] / \langle x^5 - a \rangle$ הינו שדה.

פתרון: יהי $K = \mathbb{F}_{11^5}$.

מספיק להראות כי קיים $\theta \in K$ (יוצר) כך ש- $\theta^5 \in \mathbb{F}_{11}$.

$$\left(\theta^{50} = 1 \iff \beta^{10} = 1 \iff \beta \in \mathbb{F}_{11}^{\times} \right)$$

$\#$ יוצרים של ההרחבה $K/\mathbb{F}_{11}$: $11^5 - 11$

$\#$ איברים מסדר 50 ב- $K^{\times}$: ?

$$K^\times \cong \mathbb{Z}_{11^5-1}$$

$$\Big|$$

$$\mathbb{F}_{11}^\times \cong \mathbb{Z}_{10} \quad (=11-1)$$

נשים לב:

$$5 \mid 11^4 + 11^3 + 11^2 + 11 + 1$$

$$\Rightarrow 50 \mid |K^\times| .$$

$\Rightarrow$ קיים $K^\times$ (שהוא ציקלי!) מסדר $\varphi(50)$ כאשר

$$\varphi(50) = \varphi(2 \cdot 5^2) = 2 \cdot 5 - 5 = \underline{\underline{20}}$$

לכן קיים $\theta \in K^\times$ מסדר 50, כלומר $\theta^{10} \neq 1$ אבל

$$\theta^{10} = 1 \text{ , כלומר } \mathbb{F}_{11}[\theta] = K$$

$$(\theta^5)^{10} = 1 \rightarrow \theta^5 \in \mathbb{F}_{11}$$

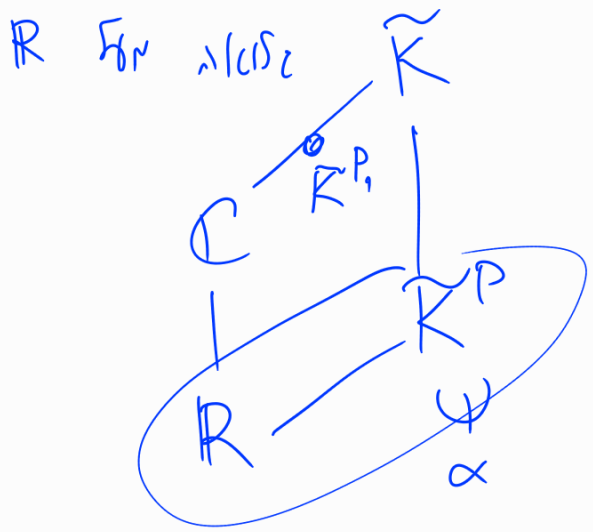
$\square$

הוכחת המשפט של הילברט:

לכל פולינום קיים קבוצת מפת $\mathbb{C}$ יש שורש.

הוכחה: (אוקיון)

נניח בשלילה:



נסמן: $P \leq G = Gal\left(\tilde{K}/\mathbb{R}\right)$ סילו-2 כלשהי.

$$\left[\tilde{K}^P : \mathbb{R}\right] = \left[G : P\right] = \text{אי זוגי}$$

לכן נובע, כי כל הרחבה אי-זוגית של שדה $\mathbb{R}$ שווה (נוסף על $\alpha \in \mathbb{R} \setminus \tilde{K}^P$ גם α עצמו וכו' ...)

$\Leftarrow \left[G : P\right] = 1 \iff G = P$ משפט-2.

למשפט-2 יש גם אינטרפטציה גיאומטרית יפה

2^n P
2^{n-1} P_0
2^{n-2} P_1
$\vdots$
1

$P_0 = Gal\left(\tilde{K}/\mathbb{C}\right)$, אותו

P_1 הוא שדה P_0 אותו

אי זוגי 2.

$\Leftarrow \left[\tilde{K}^{P_1} : \mathbb{C}\right] = 2$, כך שהוא שדה מרוכב

(מנוסחת הפונקציות).