תרגול 4

תורת גלואה

$f\in F[x]$, K/F <u>מפצל</u> של f

אם f מתפצל לגורמים ליניאריים מעל K.

K מינימלי כזה נקרא <u>שדה פיצול</u>.

אם f מתפצל ב-L אז:

$$F_f \cong F(\underbrace{a_1,\dots,a_n}_{\text{שורשי } f \text{ ב-} L})$$

הראינו: $[F_f:F]\le (\deg f)!$

① יהי $f(x)=x^4+ax^2+b \in F[x]$.

הוכיחו כי $[F_f:F]\le 8$.
($\mathrm{char}\, F \neq 2$)

<u>הערה:</u> אם f פריק אז:

$1,3 \qquad 1,1,2 \quad | \quad 2,2 \qquad 1,1,1,1$

$$\Downarrow$$

$$[F_f:F]\le 3! = 6$$

אם f אי-פריק אז $F(\theta)$

$$[F(\theta):F]=4$$

$$f(x)=(x-\theta)(x+\theta)\cdot\overbrace{g(x)}$$

$$f(-\theta)=f(\theta)=0$$

$$[\underbrace{F(\theta)_g}:F(\theta)]\le 2$$

כיון f זוגית

$$\Rightarrow [F_f:F]\le 4\cdot 2=8$$

מ.ש.ל.

(2) [תרגיל, מבחן קל]

$f(x)=x^5-11\in\mathbb{Q}[x]$. מצאו דרגת שדה

$\mathbb{Q}(\sqrt5)_f$.

פתרון:

$$\underbrace{x^5-11}$$

$$\begin{tikzcd}[column sep=small]
\mathbb{Q}(\sqrt[5]{11},\sqrt{5},\rho)=\mathbb{Q}(\sqrt[5]{11},\rho) \arrow[d, dash, "4\geq [\ ?"'] \arrow[drr, dash, "?\ 5"] & & \\
\mathbb{Q}(\sqrt[5]{11},\sqrt{5}) \arrow[d, dash, "2"'] \arrow[ddr, dash, "5"] & & \mathbb{Q}(\rho) \arrow[d, dash, "2"] \\
\mathbb{Q}(\sqrt[5]{11}) \arrow[dr, dash, "5"'] & & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

$$\rho := \exp\left(\frac{2\pi i}{5}\right)$$

יהיו שורשי f :

$$\sqrt[5]{11},\quad \rho\sqrt[5]{11},\quad \rho^2\sqrt[5]{11},\quad \rho^3\sqrt[5]{11},\quad \rho^4\sqrt[5]{11}$$

$$\mathbb{Q}(\sqrt{5})_f = \mathbb{Q}(\sqrt{5},\sqrt[5]{11},\rho) \quad \Leftarrow$$

$$\rho^5-1 = \cancel{(\rho-1)}\cdot\underbrace{(\rho^4+\rho^3+\rho^2+\rho+1)}_{\Phi_5}$$

פולינום אי"פ $\Leftarrow$ הפ"מ של ρ מעל $\mathbb{Q}$.

אייזנשטיין ב- $\Phi_5(x+1)$.

$$[\mathbb{Q}(\rho):\mathbb{Q}]=4$$

נותר לחשב:

$$\left[\mathbb{Q}(\rho, \sqrt[5]{11}, \sqrt{5}) : \mathbb{Q}(\sqrt[5]{11}, \sqrt{5})\right] = ?$$

בתרגיל האחרון ראינו: $\sqrt{5} \in \mathbb{Q}(\rho)$

$$\begin{array}{c} \mathbb{Q}(\rho) \\ {\scriptstyle 2}\,| \\ \mathbb{R} \supseteq \mathbb{Q}(\sqrt{5}) \\ {\scriptstyle 2}\,| \\ \mathbb{Q} \end{array}$$

$$(x-\rho)(x-\underset{\substack{\shortparallel \\ \rho^{-1}}}{\bar{\rho}}) \overset{?}{\in} \mathbb{Q}(\sqrt{5})[x]$$

$$= x^2 - \underbrace{(\rho+\rho^{-1})}_{\theta} x + 1$$

$$\theta^2 = (\rho+\rho^{-1})^2 = \rho^2 + \rho^{-2} + 2$$

$$\left[\rho^4+\rho^3+\rho^2+\rho+1=0 \implies \underline{\underline{\rho^2}}+\underline{\underline{\rho}}+1+\underline{\underline{\rho^{-1}}}+\underline{\underline{\rho^{-2}}}=0\right]$$

$$\theta^2 + \theta = (\rho^2+\rho^{-2}+2) + (\rho+\rho^{-1}) = 1$$

$$\theta^2+\theta-1=0 \implies \theta = \frac{-1+\sqrt{5}}{2}$$

ולכן,

$$\mathbb{Q}(\rho+\rho^{-1}) = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{5})$$

כעת:

$$\mathbb{Q}(\sqrt[5]{11}, \sqrt{5}, \rho) = \mathbb{Q}(\sqrt[5]{11}, \rho)$$

$$[\mathbb{Q}(\sqrt[5]{11}, \rho) : \mathbb{Q}(\rho)] = 5 \implies$$

$$\Rightarrow \underline{[\mathbb{Q}(\sqrt[5]{11}, \rho) : \mathbb{Q}(\sqrt{5})] = 10}$$

(3) חשבו יוצרים וממד לשדה פיצול של

$K = \mathbb{F}_p(t)$ מעל $f(x) = x^p - t$

$$\mathbb{F}_p(t) = \left\{ \frac{u(t)}{v(t)} \;\middle|\; u, v \in \mathbb{F}_p[t],\ v \neq 0 \right\}$$

פתרון: נבחר גורם א"פ של f (אולי f עצמו) ונספח שורש ל-K:

$$\begin{array}{c} K(\theta) \\ | \\ K \end{array}$$

נשים לב:

$$X^p - t = X^p - \theta^p = (X - \theta)^p$$

$\downarrow$

$$(a+b)^p = a^p + b^p \pmod p$$

[השתמשו בבינום של ניוטון ושימו לב כי כל המקדמים הבינומים מתחלקים ב-p]

מכאן:

$$u(x)^p = u(x^p)$$

לכל פולינום

מסקנה:

$$K_f = K(\theta)$$

$$[K_f : K] = [K(\theta) : K] \underset{\substack{\uparrow \\ f \text{ אי"פ}}}{=} p$$

תג"י $\mathbb{F}_p[t]$ וניתן להפעיל עליו מבחן הפולינומים

$\mathbb{F}_p[t] \rhd \langle t \rangle \Leftarrow$ קריטריון אייזנשטיין.

מ.ש.ל.

4 יהיו K,L שדות סופיים מאותו גודל.

אזי $K \cong L$.

פתרון:

$|K| = |L| = p^n$.

נשים לב כי K הוא שדה פיצול של $x^{p^n} - x$ מעל $\mathbb{F}_p$. באותה מידה זה יהיה נכון גם לגבי L, ומיחידות שדה הפיצול $\Leftarrow K \cong L$.

$$K \overset{?}{=} (\mathbb{F}_p)_{x^{p^n} - x}$$

נגדיר $f(x) = x^{p^n} - x$

הכל־ ,

מעל K.

ל־ f יש p^n שורשים.

$$f(a)=0 \Leftarrow a^{p^n-1}=1 \Leftarrow a \in K^*$$

סדר החבורה
הכפלית – p^n-1

בנוסף: $f(0)=0$.

הראינו כי איברי K הם כל בדיוק שורשי f.

$$f(x)=\prod_{\alpha\in K}(x-\alpha)$$

מסקנה: $K=(\mathbb{F}_p)_f$, וכן גם L,

ולכן: $K\cong L$. נשל.