תורת גלואה - תרגול 2

1. $f(x)=x^4+1$ אי מעל $\mathbb{Q}$ פריק
לכל p ראשוני, f <u>פריק</u> ב-$\mathbb{F}_p$.

<u>פתרון:</u>

$$x^4+1=(x^2+ax+b)(x^2+cx+d)$$

$$\begin{cases} a+c=0 & (3) \\ ac+b+d=0 & (2) \\ ad+bc=0 & (1) \\ bd=1 & (0) \end{cases}$$

$$\boxed{\begin{cases} b+\frac{1}{b}=a^2 & (\mathrm{I}) \\ \frac{a}{b}=ba & (\mathrm{II}) \end{cases}}$$

$a,b\in\mathbb{F}_p$:
$(b\in\mathbb{F}_p^\times)$

<u>$a=0$</u> : $b^2+1=0$ $(\sqrt{-1}\in\mathbb{F}_p)$

<u>$a\neq 0$</u>: <u>$b=1$</u> : $\sqrt{2}\in\mathbb{F}_p$

<u>$b=-1$</u> : $\sqrt{-2}\in\mathbb{F}_p$

עלינו להוכיח כי לכל p, אחד מבין:

$$-1,\ 2,\ -2$$

הם שאריות ריבועיות. (קיים a כך ש- $a^2 = \dots$)
([illegible])

רמז לשאלה 5 בשיעורי הבית: ט היוצרים הם שורשים של הפולינום $x^{\exp(G)} - 1$ ...

$$\langle g \rangle = \mathbb{F}_p^\times$$

$$\mathbb{F}_p^\times \cong \underbrace{\mathbb{Z}/(p-1)}$$

$$\underline{\{a \in \mathbb{F}_p^\times \mid \exists b : a = b^2\} = (\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/\left(\tfrac{p-1}{2}\right)}$$

$$\left(\cong \ker\left(\mathbb{Z}/(p-1) \longrightarrow \mathbb{Z}/2\right)\right)$$

מסקנה: $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$.

נניח של $-1, 2, -2$ כשלושה קוסטים ב- $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$. אם גם -1 וגם 2 לא ריבועיים, אז שניהם מייצגים את הקוסט הלא-טריוויאלי של $\underbrace{\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2}$, ולכן $-1 \cdot 2 = -2 \overset{!}{=}$ ריבועי.

מ.ש.ל.

הערה: ב- תרגול – פולינומים מעל $\mathbb{Z}$ קודם **שדה**
מודולו p (ראו p, אין **כללי** שדה $\rightarrow \mathbb{Q}$.
(כמו מתרגיל 4.)

הרחבת שדות: K/F

$\alpha \in K \setminus F$, $F \subseteq \underbrace{F(\alpha)}_{\text{מכיל } \alpha \text{ ו- } F} \subseteq K$

אם α אלגברי: $F[x] \ni \underbrace{p_\alpha(x)}_{\text{קיים פולינום מינימלי}}$

מתקיים:
$$\frac{F[x]}{\langle p_\alpha(x) \rangle} \cong F(\alpha)$$

טענה: f פ"מ של α מעל F אם:

1. $f \in F[x]$
2. $f(\alpha) = 0$
3. f אי"פ אז $\deg f = [F(\alpha):F]$.

חישובים בשדה הרחבה

2. יהי: $\alpha \in K \setminus \mathbb{Q}$ המקיים:

$$\alpha^3 + 2\alpha + 2 = 0$$

חשבו את $\frac{1}{\alpha^2+1}$ כצ״ל של $1, \alpha, \alpha^2$ מעל $\mathbb{Q}$.

פתרון: $f = x^3 + 2x + 2$ פ״מ של α

נרצה לגלות: f

$$1 = p \cdot \overbrace{(x^2+1)}^{g} + q \cdot \overbrace{(x^3+2x+2)}^{f}$$

אלג׳ אוקלידס:

$$\begin{array}{r|l} x^3+2x+2 & x^2+1 \\ -\;(x^3+x) & x \\ \hline x+2 & \end{array}$$

$$f = x \cdot g + x + 2$$

$$f - x \cdot g = x + 2$$

$$\begin{array}{r|l} x^3+2x+2 & x+2 \\ -\;(x^3+2x^2) & x^2-2x+2 \\ \hline -2x^2+2x+2 & \\ -\;(-2x^2-4x) & \\ \hline 2x+2 & \\ -\;(2x+4) & \\ \hline -2 & \end{array}$$

$$f = (x^2+2x+2) \cdot (x+2) - 2$$

$$f = (x^2+2x+2)\cdot(f - x\cdot g) - 2$$

מודולו f:

$$0 = (x^2+2x+2)\cdot(-x)\cdot g - 2$$

לכן: ההופכי של g מודולו f,

$$-\frac{1}{2}(x^3+2x^2+2x)$$

צ"ל: להציג את $\frac{1}{\alpha^2+1}$ כצ"ל של $1,\alpha,\alpha^2$:

$$\frac{1}{\alpha^2+1} = -\alpha - \alpha^2 - \frac{1}{2}\alpha^3$$

$$(\alpha^3 = -2\alpha - 2)$$

$$= -\alpha - \alpha^2 - \frac{1}{2}(-2\alpha-2) =$$

$$= \underline{-\alpha^2+1}.$$

מ.ש.ל.

<u>חישוב פולינום מינימלי:</u>

3. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ (כזכור: הראינו כי $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.)

$\alpha = \sqrt{2}+\sqrt{3}$, נחשב פ"מ, מעל $\mathbb{Q}$.

פתרון:

$$\overbrace{(\sqrt{2}+\sqrt{3})}^{\alpha}{}^2 = 5+2\sqrt{6}$$

$$\Rightarrow (\alpha^2-5)^2 = (2\sqrt{6})^2 \Rightarrow \alpha^4 - 10\alpha^2 + 25 = 24$$

$$\Rightarrow \underline{\alpha^4 - 10\alpha^2 + 1 = 0}$$

? $\sqrt[4]{3} + \sqrt[7]{2}$, ...

סילה – ההצגה הרגולרית:

שהראנו:

$$F \subset K \subset L$$

בסיסים $\{b_i\}$ $\{c_j\}$

$\{b_ic_j\}$ בסיס ל- L/F $\Leftarrow$

בנוסף, $\underbrace{\{\overset{e_1}{1}, \overset{e_2}{\sqrt{2}}, \overset{e_3}{\sqrt{3}}, \overset{e_4}{\sqrt{6}}\}}$ בסיס ל- $\mathbb{Q}(\sqrt{2},\sqrt{3})$ מעל $\mathbb{Q}$.

$$T_\alpha = \begin{bmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{array}{cc} \alpha\cdot 1 & \alpha\cdot\sqrt{2} \end{array}$$

פ"מ של α = פ"מ של T_α