תורת גלואה - תרגול 1

תזכורות מקורסים קודמים:

- F - שדה.
- $F[x]$ - חוג שלמות, חוג ראשי
- [ראינו: מקסימלי הינו מהצורה $\langle f(x)\rangle$ כאשר $f \neq 0$ אי-פריק]
- $F[x_1,\dots,x_n]$ - חוג שלמות, חוג פריקות יחידה.

מסקנה: אם $f \in F[x]$ אי-פריק אז $F[x]/\langle f\rangle$ הינו שדה.

$$F \hookrightarrow \underbrace{F[x]/\langle f\rangle}_{\text{מ"ו מעל } F}$$

תרגיל. נניח כי $\deg f = d$, אזי:

$$\dim_F F[x]/\langle f\rangle = d.$$

הוכחה: תרגיל (רעיון: $\{\bar{1}, \bar{x}, \dots, \bar{x}^{d-1}\}$ מהווה בסיס מעל F.)

תרגיל: חשבו: $\dim_{\mathbb{Q}} \mathbb{Q}[x]/\langle f,g\rangle$

נסמן:

$$f = x^4 - 1$$
$$g = x^3 + 2x^2 + x + 2$$

פתרון:

$$x - 2$$

$$x^4 - 1 \;\big|\; x^3 + 2x^2 + x + 2$$

$$-\quad x^4 + 2x^3 + x^2 + 2x$$

$$-2x^3 - x^2 - 2x - 1$$

$$-\quad -2x^3 - 4x^2 - 2x - 4$$

$$3x^2 + 3$$

$$\langle f, g\rangle = \langle g, 3x^2+3\rangle = \langle g, x^2+1\rangle$$

$$f = (x-2)\cdot g + 3x^2 + 3$$

נחלק את g ב- x^2+1:

$$x + 2$$

$$x^3 + 2x^2 + x + 2 \;\big|\; x^2 + 1$$

$$-\quad x^3 + x$$

$$2x^2 + 2$$

$$-\quad 2x^2 + 2$$

$$0$$

$\langle f, g\rangle = \langle x^2+1\rangle$ **מסקנה:**

$$\frac{\mathbb{Q}[x]}{\langle f,g\rangle} = \frac{\mathbb{Q}[x]}{\langle x^2+1\rangle} \quad \left(= \mathbb{Q}[i]\right)$$ ולכן

ולכן ממדו מעל $\mathbb{Q}$ הינו 2. מ.ש.ל.

$\boxed{\text{דרכי לבדיקה שבדו עלינו להבין פולינומים א״פ}}$

דוגמה: כל פולינום לינארי הוא א״פ:

$$f(x) = ax+b \quad (a\neq 0)$$

$$\left.\begin{aligned} \frac{F[x]}{\langle f(x)\rangle} &\longrightarrow F \\ x &\longmapsto -a^{-1}b \end{aligned}\right\}$$

תרגיל: יהי f פולינום מדרגה >1, מעל שדה F.

(i) אם ל-f יש שורש ב-F אז f פריק.

(ii) אם f פריק, $\deg f \le 3$ אז יש לו שורש ב-F.

פתרון:

(i) נניח כי $f(\alpha)=0$, $\alpha\in F$.

נחלק (עם שארית) את f ב- $x-\alpha$:

$$(*)\quad f(x)=q(x)\cdot(x-\alpha)+\underbrace{r(x)}_{\deg r<1}$$

לכן $r(x)=\beta$ קבוע.

כעת, נציב $x=\alpha$ ב-$(*)$:

$$0=f(\alpha)=q(\alpha)\cdot\underbrace{(\alpha-\alpha)}_{0}+\beta$$

לכן: $\beta=0$. כלומר:

$$f(x)=q(x)\cdot(x-\alpha)$$

לכן f פריק.

(ii) אם $\deg f\le 3$ ו- f פריק:

$$f=g_1\cdot g_2$$

לפחות אחד מבין g_1,g_2 לינארי:

$$g_1=x-\alpha$$

לכן α שורש של f, כנדרש.

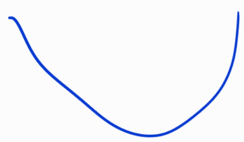
מ.ש.ל.

עבור דרגה גדולה יותר - קיום שורש <u>אינו</u>
שקול לפריקות הפולינום:

<u>תרגיל</u>: $f(x)=x^4+1$, אין לו שורשים
מעל $\mathbb{R}$, מצאו את פירוקו לגורמים אי מעל $\mathbb{R}$.

<u>פתרון</u>: ל- f אין שורש ממשי:

$f' = 4x^3 \Rightarrow x=0$ נק' המינימום



$f(0)=1>0$ אין

נמצא את הפירוק של f לגורמים אי מעל $\mathbb{R}$.
נמצא את שורשי f מעל $\mathbb{C}$

$$f(x)\cdot(x^4-1)=x^8-1$$

$$f(x)=\frac{x^8-1}{x^4-1}$$

שורשי x^8-1:

$$\left\{e^{\frac{2\pi i k}{8}} \;\middle|\; k=0,\dots,7\right\}$$

שורשי f:

$$\left\{e^{\frac{2\pi i k}{8}} \;\middle|\; k=1,3,5,7\right\}$$

לפינק;

$$f(x)=\left(x-e^{\frac{\pi i}{4}}\right)\left(x-e^{\frac{3\pi i}{4}}\right)\left(x-e^{\frac{5\pi i}{4}}\right)\left(x-e^{\frac{7\pi i}{4}}\right)$$

$$=\left(x-e^{\frac{\pi i}{4}}\right)\left(x-e^{\frac{7\pi i}{4}}\right) \qquad \vdots$$

$$= x^2-\underbrace{\left(e^{\frac{\pi i}{4}}+e^{\frac{7\pi i}{4}}\right)}x+1$$

$$\underbrace{\cos\frac{\pi}{4}}_{\sqrt{2}/2}+\underbrace{\cos\frac{7\pi}{4}}_{\sqrt{2}/2}=\sqrt{2}$$

ומקבלים:

$$f(x)=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$$

תרגיל: האם $f=x^3-x+1$ אי"פ מעל $\mathbb{F}_5$? מעל $\mathbb{F}_3$?

פרקו לגורמים אי"פ.

פתרון: מכיוון שהפולינום מדרגה 3, מספיק
לבדוק האם יש שורשים:

$\underline{\mathbb{F}_3}$: $f(0)=f(1)=f(2)=1\neq 0$

$\underline{\mathbb{F}_5}$: $\dots$ $f(3)=0$

$$f(x)=(x-3)\cdot\underbrace{(x^2+3x+3)}_{\substack{\text{אין שורשים} \Leftarrow \text{א"פ} \\ \deg=2}}$$

מ.ש.ל.

תרגיל: אם $f(x)=a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}[x]$

ו- q/r שורש (כתיב מצומצם) רציונלי

אז f מקיים: $q|a_0$, $r|a_n$.

הוכחה:

$$0=f(q/r)=\sum_{i=0}^{n}a_i\left(q/r\right)^i$$

נכפול ב- r^n:

$$0=\underbrace{\overset{q|a_0}{a_0r^n}+\overbrace{a_1qr^{n-1}+\dots+}^{\text{מתחלק ב-}q}}_{\text{מתחלק ב-}r}\underbrace{a_nq^n}_{r|a_n}$$

מ.ש.ל.

<u>תרגיל:</u> הראו ש- $f = x^3 - x - 5$ אי פריק מעל $\mathbb{Q}$.

<u>פתרון:</u> $\deg f = 3 \Rightarrow$ אי פריק אם״ם אין לו שורשים רציונליים:

לפי המבחן הרציונלי אם q/r שורש אז:

$q \mid c,\ r \mid 1 \Rightarrow \{\pm 5\}$

בודקים, הם לא שורשים ולכן f אי פריק. מ.ש.ל.

<u>שיטת הרדוקציה:</u>

[יהי $f \in \mathbb{Z}[x]$ פולינום מתוקן. אם f אי פריק מודולו p (ב-$\mathbb{F}_p$) אז f אי פריק מעל $\mathbb{Z}$. (ולכן מעל $\mathbb{Q}$, לפי הלמה של גאוס.)]

<u>קריטריון אייזנשטיין:</u> נניח כי $f \in \mathbb{Z}[x]$

$$f = a_0 + a_1x + \dots + a_nx^n$$

נניח כי p ראשוני המקיים:

(I) $p \mid a_0, \dots, a_{n-1}$, $p \nmid a_n$

(II) $p^2 \nmid a_0$

יהי f פול' מעל $\mathbb{Z}$.

תרגיל: $f(x)=x^4+4x^3+6x^2+8x+15$ א"פ?

(**למה** - $f(x)\in\mathbb{Z}[x]$ א"פ $\Longleftrightarrow$ $f(x+m)$ א"פ $(m\in\mathbb{Z})$)

נציב ב- -1:

$$
\begin{aligned}
f(x-1) &= (x-1)^4+4(x-1)^3+6(x-1)^2+8(x-1)+15 = \\
&= x^4-4x^3+6x^2-4x+1 \\
&+ \quad 4x^3-12x^2+12x-4 \\
&+ \quad 6x^2-12x+6 \\
&+ \quad 8x+7 \\
\hline
& x^4+4x+10
\end{aligned}
$$

פולינום אייזנשטיין עבור $p=2$.

מ.ש.ל.