אלגברה מופשטת- תרגול מס' 5

<u>תרגיל:</u> K/F הרחבה אלגברית.

$F\le L\le K$, L חוג.

<u>הוכיחו:</u> L שדה.

<u>הוכחה:</u> יהי $l\in L$, l אלגברי מעל F נובע מהגדר הרחבה סופית.

יהי $f_l(x)\in F[x]$ הפולינום המינימלי של l מעל F.

<u>נסמן:</u> $f_l = a_0 + a_1x + \dots + a_nx^n$

$$f_l(l) = a_0 + a_1 l + \dots + a_n l = 0$$

$a_0 \neq 0$ כי f_l אי-פריק

$$\Downarrow$$

$$l(\underbrace{a_1 + a_2 l + \dots + a_n l^{n-1}}_{\in L \text{ כי סגור של איברים מ-}L}) = -a_0$$

ו-

$$l\cdot(\underbrace{-\frac{a_1}{a_0} - \frac{a_2}{a_0} l - \dots - \frac{a_n}{a_0} l^{n-1}}_{\in L}) = 1$$

$\Leftarrow$ לכן, כל $l\in L$ הפיך ו-L שדה.

<u>תרגיל:</u> מצאו את שדה הפיצול של x^5-2 מעל $\mathbb{Q}$ ואת מימדו (מעל $\mathbb{Q}$).

⊛ <u>הגדרה:</u> יהיו ρ_n שורשי היחידה ה-n-ים של 1. $\left(\sqrt[n]{1} = e^{i\cdot\frac{2\pi}{n}}\right)$

הפולינום הציקלוטומי של ρ_n הוא הפולינום המינימלי של ρ_n מעל $\mathbb{Q}$

נסמן אותו ב- $\Phi_n(x)$.

<u>משפט:</u> הפולינום הציקלוטומי של ρ_n

$$\Phi_n(x) = \prod_{\substack{1\le k\le n \\ (k,n)=1}} (x-\rho_n^k)$$

ו- $\Phi_n(x)\in\mathbb{Z}[x]$

בפרט, לכל p ראשוני נקבל $\Phi_p(x) = 1+x+\dots+x^{n-1}$

<u>תזכורת:</u>

⊛ שדה פיצול של $f\in F[x]$ הוא השדה הקטן ביותר המכיל את כל שורשי $f(x)$.

(מימד שדה הפיצול של פולינום מדרגה $n \le n!$)

<u>מחזרה לתרגיל:</u> השורשים של x^5-2 הם:

<u>מסק'</u>

נסמן $\alpha = \sqrt[5]{2}$,

$\{\alpha, \alpha\rho_5, \dots, \alpha\rho_5^4\}$

שדה הפיצול הוא: $E = \mathbb{Q}[\alpha, \alpha\rho_5, \dots, \alpha\rho_5^4] = \mathbb{Q}[\alpha, \rho_5]$

$$\begin{tikzcd}[column sep=small]
 & E & \\
\mathbb{Q}[\sqrt[5]{2}] \arrow[ur, dash, "4"] & & \mathbb{Q}[\rho_5] \arrow[ul, dash, "5"'] \\
 & \mathbb{Q} \arrow[ul, dash, "5"] \arrow[ur, dash, "4"'] &
\end{tikzcd}$$

$f_\alpha = x^5 - 2$ $\Phi_5(x) = 1 + x + \dots + x^4$

f_α אי-פריק (איזנשטיין) ומתאפס ב-α

ומימד ההרחבה הוא 20.

<u>תרגיל:</u> בנה שדה עם 4 איברים.

<u>פתרון:</u> מספיק למצוא פולינום f אי-פריק מדרגה 2 מעל $\mathbb{Z}_2$.

$$\mathbb{Z}_2[x]/\langle f\rangle = \{a + bt \mid a, b \in \mathbb{Z}_2\} \quad \text{כאשר } \deg f = 2$$

יש רק 4 פולינומים מתוקנים מדרגה 2:

$$\text{פריקים}\left[\begin{array}{l} x^2 \\ x^2+1 \\ x^2+x \end{array}\right.$$

<u>x^2+x+1</u>

לכן $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ שדה מסדר 4.

נכתוב את טבלת הכפל שלו:

	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	0	0	0	0
$\bar{1}$	0	1	x	x+1
$\bar{x}$	0	x	x+1	1
$\overline{x+1}$	0	x+1	1	$\bar{x}$

<u>שים ♡:</u> $\bar{x} := x + \langle x^2+x+1\rangle$

21.11.13 תכנה זה כמו אשמה

$(\bar{x}^2 \equiv \overline{x+1})$

$x^2-(x+1) = x^2+x+1 \in \langle x^2+x+1 \rangle$

$\bar{x}\cdot(\overline{x+1}) = x^2+$

<u>הערה</u>: לכל $n\in\mathbb{N}$ ולכל p ראשוני קיים שדה סופי מסדר p^n.

כי: קיים פולינום מדרגה n, אי-פריק מעל $\mathbb{Z}_p$.

<u>תרגיל</u>: מצאו את שדה הפיצול של x^4-x מעל $\mathbb{Z}_2$.

$$x^4-x = x(x^3-1) = x\underbrace{(x-1)}_{\text{השורשים}}\underbrace{(x^2+x+1)}_{f}$$

השורשים הם 0,1 כבר ב- $\mathbb{Z}_2$

וזאת שדה הפיצול של f כבר חישבנו.

<u>תרגיל / משפט</u>: נניח $|K|=p^n$ (p ראשוני).

אז K הוא שדה פיצול של הפולינום:

$p(x) = x^{p^n}-x$ (מעל $\mathbb{Z}_p$).

<u>הוכחה</u>: $K^*=K\setminus\{0\}$ חבורה כפלית, $|K^*|=(p^n-1)$

לכן לגרנז' לכל $k\in K^*$, $k^{p^n-1}=1$

$x^{p^n-1}-1$

כלומר: לכל איבר $k\in K^*$ מאפס את הפולינום:

נכפול ב- x, כדי להוסיף את השורש 0, ונקבל

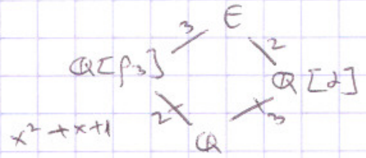
$x^{p^n}-x$

פולינום עם p^n שורשים.

כלומר K שדה פיצול של $x^{p^n}-x$

תזכורת לדוגמא משיעור שעבר: $x^3-2\in\mathbb{Q}[x]$ אי-פריק מעל $\mathbb{Q}$,

השורשים $\alpha, \rho_3\alpha, \rho_3^2\alpha$



$Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) \cong Gal(\mathbb{Q}[\rho_2\alpha]/\mathbb{Q}) \cong Gal(\mathbb{Q}[\rho_3^2\alpha]/\mathbb{Q}) =$

$=\{id\}$

נסמן: $K = \mathbb{Q}[\alpha, \rho_2]$

(נזכיר ש- $Gal(K/\mathbb{Q}) \le S_3$ כי ההרחבה עם שלשה

שורשים של x^3-2 וכל אוטומורפיזם הוא תמורה של השורשים)

נוכיח ש- $Gal(K/\mathbb{Q}) = S_3$

$$\begin{array}{c} K \\ 2 | \\ \mathbb{Q}[\alpha] \\ 3 | \\ \mathbb{Q} \end{array}$$

← קיים אוטו' π_1 שמחליף בין ρ_3 ו- ρ_3^2 מעל $\mathbb{Q}[\alpha]$.

והוא גם מעל $\mathbb{Q}$ חילוף ב- S_3

$$\begin{array}{ccc} \alpha & \rho_3\alpha & \rho_3^2\alpha \\ | & \times & \\ \alpha & \rho_3\alpha & \rho_3^2\alpha \end{array}$$

$$\begin{array}{c} K \\ 3 | \\ \mathbb{Q}[\rho_3] \\ 2 | \\ \mathbb{Q} \end{array}$$

⇐ קיים אוטו' π_2 של K מעל $\mathbb{Q}[\rho_3]$ ~~...~~ מעביר את α ל- ρ_3

ו! $\pi_1 \ne \pi_2$ ⇐ $Gal(K/F) = S_3$