16.01.14

בס״ד ט״ו שבט תשע״ד

אלגברה מופשטת 3 - תרגול מס׳ 11

$E=F_{p^n}$, $char(E)=p$

$\varphi: F_{p^n} \longrightarrow F_{p^n}$

$a \longmapsto a^p$

<u>טענה</u>: φ אוטומורפיזם (שמשאיר את $\mathbb{Z}_p$)

$\varphi(ab)=$

$\varphi(a+b)=(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^k b^{p-k}$

$\varphi\in Gal(E/\mathbb{Z}_p)$ $\quad k\in\mathbb{Z}_p^{\times}$ $\quad (a^{p-1}=1)\rightarrow a^p=a$

מה יכול להיות הסדר של φ ?

$\varphi^k=id \Rightarrow \forall a\,(\varphi^k(a)=a)$

$\Rightarrow \forall a\,(\varphi^{p^k}(a)=a)$

$\forall a\,(a^{p^k}-a=0)$

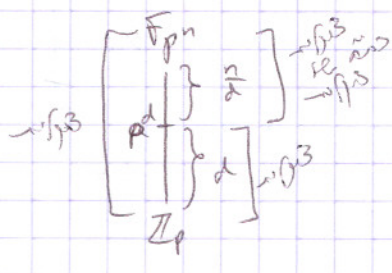
אם $k<n$ אזי לפולינום יש p^k שורשים לכל היותר $\quad p^k<p^n$

$\Downarrow$

φ יוצר את $Gal(E/\mathbb{Z}_p)$

F_{p^n}
$|\; n \quad (x^{p^n}-x)$
$\mathbb{Z}_p$

כל הרחבה של שדה סופי היא ציקלית



<u>תרגיל</u>: מצאו את חבורת גלואה של שדה הפיצול של $f=x^3-2$ מעל $\mathbb{Z}_{11}$ ומעל $\mathbb{Z}_7$

<u>פתרון</u>:

מעל $\mathbb{Z}_{11}$ ל-f יש שורש יחיד (בדוק!) - 7 ,

$f=(x-7)(\_\_$ פולינום ממעלה 2 $\_\_)$

ואין לו שורשים

$G=\mathbb{Z}_2$

מעל $\mathbb{Z}_7$ אין ל-f שורשים ולכן הוא אי-פריק

שורש α של f ב- $\mathbb{Z}_7$

$F = \mathbb{Z}_7[\alpha]$

$| 3$

$\mathbb{Z}_7$

מגודל 343 ל-3,7 $\mathbb{Z}^*_{p^n}$

ניקח $b \in F$ כך ש- $F^* = \langle b \rangle$

$b^{342} = 1$

$(b^{114})^3 = 1$

$\rho_3 \in F$

$\Leftarrow$ $\alpha, \alpha\rho_3, \alpha\rho_3^2 \in F$

$\Leftarrow$ F מכיל את הפולינום המינימלי לכן הוא C_3.

נראה איזומורפיזם

$$k_1 = \mathbb{Z}_2[x] / \underbrace{\langle x^3+x^2+1 \rangle}_{f_1} \xrightarrow{\varphi} \mathbb{Z}_2[x] / \underbrace{\langle x^3+x+1 \rangle}_{f_2}$$

$\cong \; F_8 \; \cong$

$F_8 = \mathbb{Z}_2[\alpha]$, $\langle \rho_7 \rangle$ $| 3$, $\mathbb{Z}_2$

$F_8 = \mathbb{Z}_2[\beta]$, $\langle \rho_7 \rangle^3$, $\mathbb{Z}_2$

	000
	001
β	010
β^2	101
β^4	110
	011
	101
	111

$\alpha = 010$

$\psi : k_1 \to k_2$

$\alpha \mapsto \beta + 1$

$\psi(a + b\alpha + c\alpha^2) = a + b\psi(\alpha) + c\psi(\alpha)^2$

ההוכחה של הפיצול של $x^4-4, x^4+4 \in \mathbb{Q}[x]$ איזומורפיים.

Gal → $\mathbb{Z}_2 \times \mathbb{Z}_2$; Gal → $\mathbb{Z}_2$