Note Title

Ex: (1) $F_4 = \{0, 1, \alpha, \alpha^2 = 1+\alpha\}$ $\alpha^3 = 1$

Some field $G = \{a, b, c, d\}$

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

×	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	d

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

×	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

} in F_4

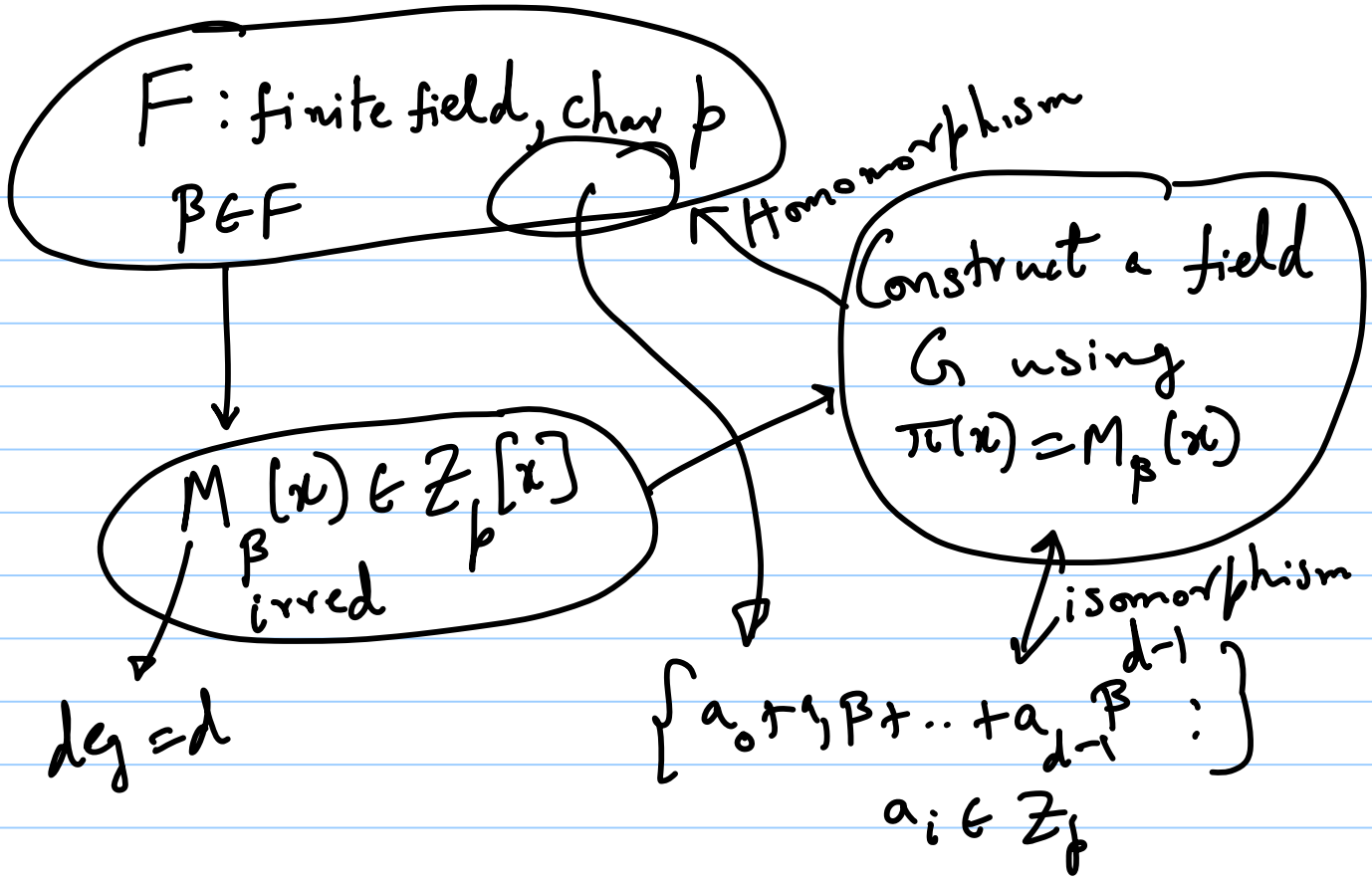
Isomorphism

G		F_4
a	$\longrightarrow$	0
b	$\xrightarrow{f}$	1
c	$\longrightarrow$	α
d	$\longrightarrow$	α^2

$\forall \alpha, \beta \in G$

$f(\alpha \underset{G}{+} \beta) = f(\alpha) \underset{F_4}{+} f(\beta)$

$f(\alpha\beta) = f(\alpha) f(\beta)$


F : finite field, char p
β ∈ F
Homomorphism
Construct a field
G using
π(x) = M_β(x)
M_β(x) ∈ Z_p[x]
irred
deg = d
isomorphism
{a_0 + a_1 β + .. + a_{d-1} β^{d-1} :
a_i ∈ Z_p}

Ex: $F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ $\alpha^4 = 1+\alpha$, $\alpha^{15} = 1$

$\{0, 1, \alpha^5, \alpha^{10}\} \cong F_4$

0
1
α
α^2
α^3
$\alpha^4 = 1+\alpha$
$\alpha^5 = \alpha+\alpha^2$
$\alpha^{10} = \alpha^2+\alpha+1$

$M_{\alpha^5}(x) = x^2+x+1$

$\pi(x) = x^2+x+1$

$F_4 = \{0, 1, \gamma, 1+\gamma = \gamma^2\}$

$\gamma^3 = 1$

Property: $\beta \in F_{p^m}$: primitive

$$\Downarrow$$

$$\deg M_\beta(x) = m$$

Fact: Two fields with p^m elements are isomorphic to each other.

Pf: F & G : two fields with p^m elements

F: β is primitive, $M_\beta(x)$: irreducible, deg-m $\in Z_p[x]$ factor of $x^{p^m} - x$

$$M_\beta(x) \mid (x^{p^m} - x) = \prod_{\gamma \in G} (x - \gamma) \Rightarrow \exists\, \gamma' \in G \text{ s.t.}$$

$$M_{\gamma'}(x) = M_\beta(x)$$

$G \xleftrightarrow{\text{iso}}$ Field with $\xleftrightarrow{\text{iso}} F$

$\pi(x) = M_{\gamma'}(x) = M_\beta(x)$

QED

Fact: $x^{p^m} - x$ = Product of all monic irreducible polynomials over $\mathbb{Z}_p[x]$ of degree d s.t. $d \mid m$

Ex: $p=2$, $m=4$

$$x^{16} + x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

$p=2$, $m=3$

$$x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$$

Pf: (1) $\pi(x)$: irred, deg d s.t. $d \mid m$

if $\pi(x) = x$, $x \mid (x^{p^m} - x)$ ✓ we are done.

Assume $\pi(x) \neq x$.

$\pi(x) \mid x(x^{p^d - 1} - 1) \Rightarrow$

$\pi(x) \mid (x^{p^d - 1} - 1)$

We can show $x^{p^d - 1} - 1 \mid x^{p^m - 1} - 1$ whenever $d \mid m$.

$\left(x^d - 1 \mid x^m - 1 \text{ iff } d \mid m \right)$

(2) if $\pi(x) \mid x^{p^m} - x$, then we have to show $d \mid m$.

$\pi(x) \neq x$

$\Rightarrow \pi(x) \mid x^{p^m-1} - 1$. $\exists\, \alpha \in F_{p^m}$ s.t. $\operatorname{ord}(\alpha) = p^d - 1$

$\pi(x)$ $\downarrow$ $\deg = d$ $\qquad$ $x^{p^m-1} - 1$ $\Rightarrow$ $p^d - 1 \mid p^m - 1$

$\downarrow$

$d \mid m$

$N(m)$: # of monic irred poly of deg m over $\mathbb{Z}_p[x]$

$$p^m = \sum_{d|m} d\,N(d)$$

↓ Mobius inversion

can show $N(m) \geq 1$

Property?: $\beta \in F_{p^m}$

$C_\beta = \text{Conjugates of } \beta = \{\beta, \beta^p, \beta^{p^2}, \ldots\}$

will be distinct roots of $M_\beta(x)$.

Let $|C_\beta| = d$.

$$\prod_{\alpha \in C_\beta} (x - \alpha) = M_\beta(x)$$

Pf: $f_0 + f_1 x + \cdots + f_d x^d = f(x) = \prod_{\alpha \in C_\beta} (x-\alpha) = (x-\beta)(x-\beta^p)(x-\beta^{p^2}) \cdots (x-\beta^{p^{d-1}})$

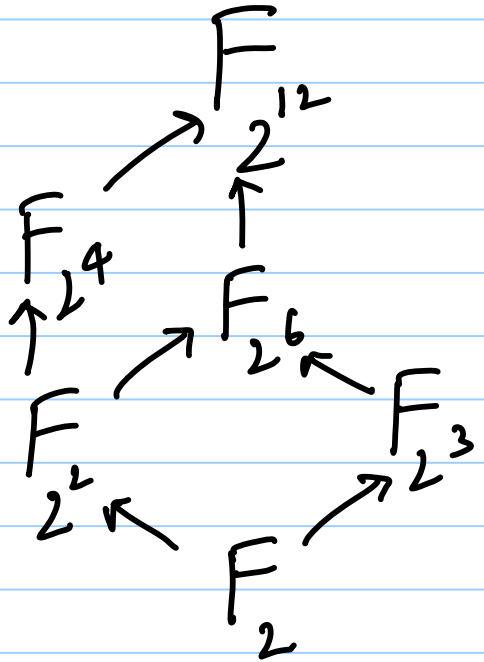
We need to show $f_i \in Z_p$.

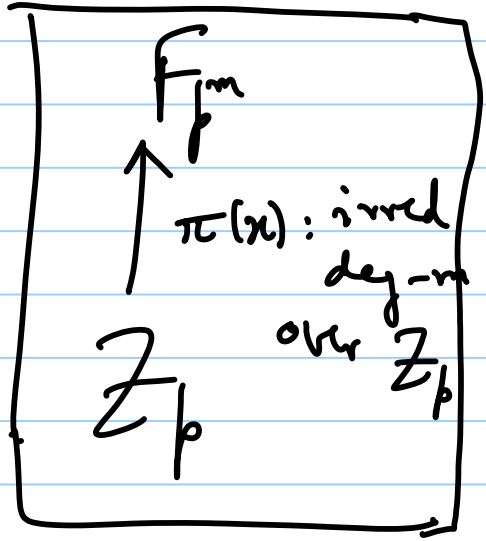
$f_i^p = f_i$ → raise both sides to power p

$\left(F_{p^m}: \text{if } \exists\, \alpha \text{ s.t. } \alpha^{p^d} = \alpha, \text{ then } \alpha \in F_{p^d} \subseteq F_{p^m}\right)$

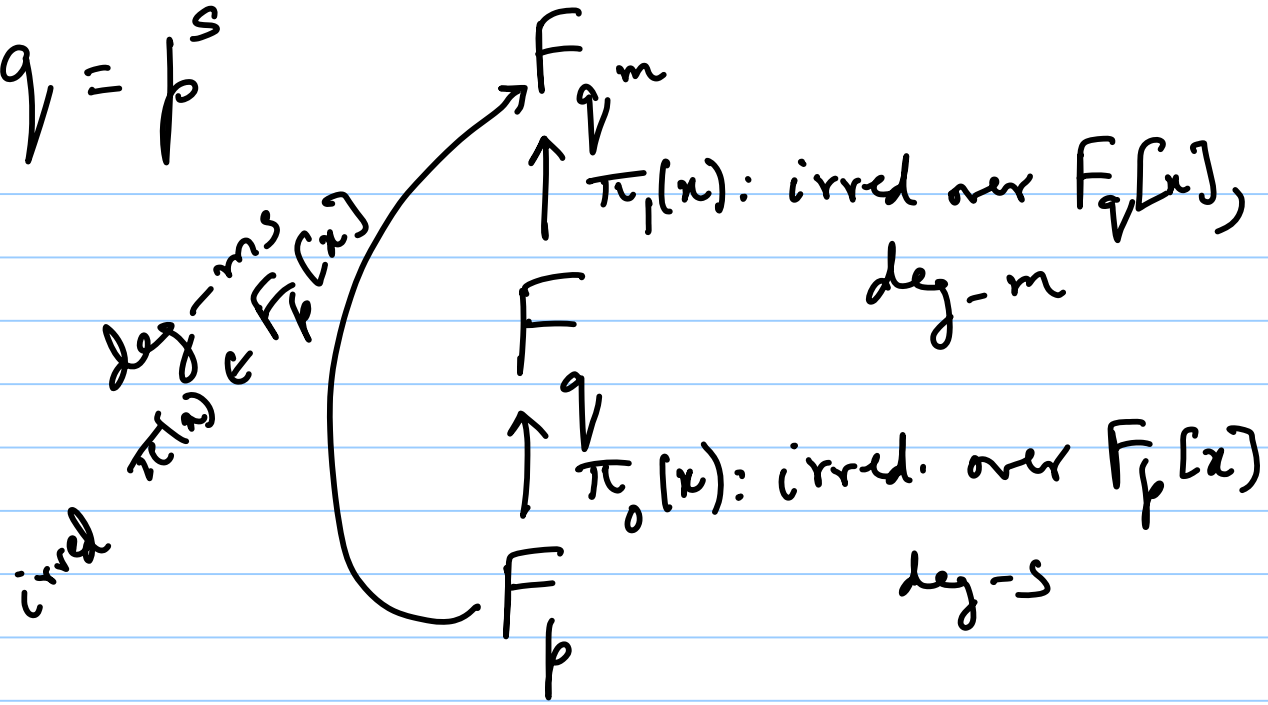
$(d \mid m) \hookleftarrow$

Sub field: $F_{p^d} \subseteq F_{p^m}$ iff $d \mid m$





$q = p^s$



$p=2$, $m = 2, 3, 9, \ldots$