

lect 14 Also see notes

Finite fields, Summary

1) \forall prime $p, n \geq 1 \exists$ field $\mathbb{F}_q, \mathbb{F}_p \subset \mathbb{F}_q$
 $|\mathbb{F}_q| = p^n$ $q = p^n$ \uparrow prime

\forall field $F, |F| = p^n \Rightarrow F \cong \mathbb{F}_q$ isomorphic fields

split field $\frac{x^q - x}{x}$
 reducible

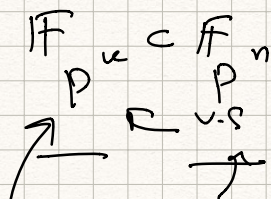
$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x$$

$$\mathbb{F}_p \cong F$$

$$\alpha \in \mathbb{F}_q \quad \downarrow \text{D}$$

$$|\mathbb{F}_q^*| = q - 1 = p^n - 1$$

\mathbb{F}_q^* - cyclic, order $q - 1$
has generators.



iff $k | n$

$$p^n = (p^k)^m = p^{km} \quad n = km$$

$\frac{x^q - x}{x}$ $q = p^n$
 $\frac{x^{p^k} - x}{x}$ a divisor of

$$x^{p^k} = x \Rightarrow x^{(p^k)^m} = x$$

$\exists \alpha$ that is a generator of \mathbb{F}_q^*

(note C_m)
 $\# \text{gen} =$

$$\mathbb{F}_p(\alpha) = \mathbb{F}_q \quad \alpha \in \mathbb{F}_q$$

$$\# \{k : \text{gcd}(k, m) = 1\}$$

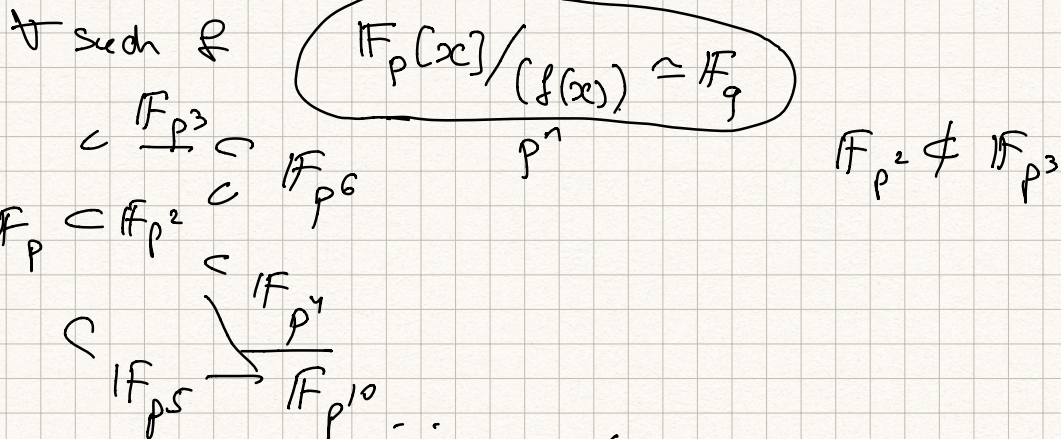
$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ basis

$$q = p^n$$

$$\varphi(n)$$

$$\text{irr}(\alpha, \mathbb{F}_p) = f(x) \quad \deg f = n$$

Cor \exists an irr. monic pol. f of $\forall \deg n / \mathbb{F}_p$.



exists such g $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[y]/(g(y)) \cong \mathbb{F}_q$

$1, x, x^2, \dots, x^{n-1}$

$$f(x) \mid x^q - x.$$

$$y = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$$

irr \uparrow α \uparrow $\alpha^q = \alpha$

\forall irr monic g

$$g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$$

$$\frac{g(x) \mid x^q - x}{(g_1(x), g_2(x)) = 1}$$

$$\Rightarrow \prod g(x) \mid x^q - x$$

g - irr, $\deg n$, monic \nwarrow nearly all

Frobenius (aut finite fields)

$$\sigma: \mathbb{F}_q \rightarrow \mathbb{F}_q \quad \sigma(a) = a^p \text{ auto.}$$

$$\sigma^2(a) = (a^p)^p = a^{p^2} \quad \sigma^3(a) = a^{p^3}$$

$\text{char}(\mathbb{F}) = p$

$$\mathbb{F} \rightarrow \mathbb{F}$$

$$a \mapsto a^p$$

$$\sigma \in \text{Aut}(\mathbb{F}_q) = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$$

$F \subseteq E$ $\text{Gal}(E/F)$ - all sym of E g
 fix $g|_F = \text{id}_F$.

$\text{Aut}(E) = \text{Gal}(E/F_0)$

$g(1)=1$
 $g(2)=2$
 $g = \text{id}$ on \mathbb{Q} prime subfield
 $\mathbb{F}_p \subseteq E$ on $\mathbb{Q} \subseteq E$

$g(a)=a \forall a$ in prime subfield $F_0 \subseteq E$

$\zeta: \{ \text{id}, \zeta, \zeta^2, \dots, \zeta^{n-1} \}$ all distinct
 aut of \mathbb{F}_q

$a^{p^n} = a \forall a \in \mathbb{F}_q$ $|\mathbb{Z}|? \text{ less than } n?$
 $\zeta^n(a)$ $a^{p^d} = a \forall a \in \mathbb{F}_q$ $d \leq n$ $\zeta^d = \text{id}$ $d | n$.

$\mathbb{F}_q \supset \mathbb{F}_{p^d}$ $q = p^n > p^d$ - sol
 $\mathbb{F}_q \supset \mathbb{F}_{p^d}$ x^{q-x}
 x^{p^d-x}

Note ζ gen group C_n

$\text{Aut}(\mathbb{F}_q) \cong C_n$ $\text{Aut}(\mathbb{F}_q) \cong C_n$

$\text{Aut}(\mathbb{F}_q) = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$

$\text{Sym}(\mathbb{F}_q/\mathbb{F}_p) = \text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$

Proped E/F splitting field. f

$\# \text{ sym} \mid \text{Gal}(E/F) \mid \leq [E:F]$

= if f is separable.

if E is a spl. field

$$\mathbb{Q}(\sqrt[3]{2})$$

$$x^3 - 2$$

$$E \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$$

$$\uparrow = \text{Aut}(\mathbb{Q}(\sqrt[3]{2}))$$

$$\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$$

$$\alpha = \sqrt[3]{2}$$

$$\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) =$$

$g \in$

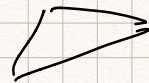
$$x^3 - 2$$

\uparrow prime

$$g(\alpha) = \alpha \Rightarrow g(\alpha^2) = \alpha^2$$

g is id. on $\mathbb{Q}(\alpha)$

$$\text{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$$



$$[E:\mathbb{Q}] = 6 = |\text{Gal}(E/\mathbb{Q})|$$

$$\text{Gal}(E/\mathbb{Q}) = S_3$$

"bad" extensions E/F $|\text{Gal}(E/F)| < [E:F]$

All extensions of \mathbb{R} fields are "good".

$$G = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong C_n$$

$$|G| = n = [\mathbb{F}_q:\mathbb{F}_p]$$

\uparrow
abelian

$$\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong C_n$$

$$\text{Gal}(E/\mathbb{Q}) = S_3$$

not abelian.

$$\mathbb{Z} \quad \mathbb{Z}^n \quad q \neq p^n$$

$\forall \mathbb{R}$ G is the

$$\text{Galois } \text{Gal}(E/F) \cong G.$$

Any f. field \mathbb{F}_q is perfect (p-th roots exist)

$$\mathbb{F}_q^* = C_{q-1} = C_{p^n-1} \cong (p, p^n-1)$$

$$\forall a \in \mathbb{F}_q \exists b \quad b^p = a \quad b = \sqrt[p]{a}$$

$$\underbrace{x^p - a = (x-b)^p = x^p - b^p}$$

* pol. $f \in \mathbb{F}_q[x]$ is separable

no irreducibles of the form

$$f(x) = a_0 + a_1 x^p + a_2 x^{p^2} + \dots + a_n x^{p^n} =$$

$$\exists p\text{-th roots } a_0 = b_0^p \quad a_1 = b_1^p, \dots$$

$$= (b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n)^p$$

Possible char $F = p \quad |F| = \infty \Rightarrow \mathbb{F}_p$ may have such irr. f

$$F = \mathbb{F}_p(t) \subset \text{rad. f's}$$

$$\frac{g(t)}{h(t)} = \frac{g(t) \cancel{r(t)}}{h(t) \cancel{r(t)}}$$

$x^p - t$ inseparable.

$$u = \sqrt[p]{t} \quad \mathbb{F}_p(u) \supset \mathbb{F}_p(t)$$

$$x^p - t = (x-u)^p$$

$$\begin{matrix} \sqrt[p]{u} \\ \vdots \\ \sqrt[p]{t} \end{matrix}$$

$\mathbb{F}_p \subset \mathbb{F}_q$ simple extension Ex

$\mathbb{F}_q = \mathbb{F}_p(\alpha)$ for some α

$\mathbb{F}_q \subset \mathbb{F}_{q^r}$
simple

$F \subset E$ simple if $\exists \alpha \in E$ s.t. $E = F(\alpha)$

Prop Any finite field extension is

of the form $\mathbb{F}_q \subset \mathbb{F}_{q^r}$

Subfields of $\mathbb{F}_{p^m} \leftrightarrow$ divisors of m

$d|m$ $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^m}$

$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$ irr

$\{0,1\}$ $x, x+1$

irr(x, \mathbb{F}_2) = x^2+x+1

$$\frac{x^2+x+1}{4}$$

$$\frac{(x+x)(x+x+1)}{4}$$

$\mathbb{F}_{16} \quad \mathbb{F}_2[x]/(f(x))$

$$x^4 + a_3 x^3 + a_2 x^2 + a_1 x + 1$$

$$a_i \in \mathbb{F}_2$$

$$\checkmark x^4 + x^3 + 1$$

$$f(1) \neq 0$$

$$\checkmark x^4 + x^2 + 1$$

$$a_1 + a_2 + a_3 = 1$$

$$\checkmark x^4 + x^3 + x^2 + x + 1$$

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

$$\checkmark x^4 + x + 1$$

$$\left\{ \begin{array}{l} x^4 + x^3 + x^2 + x + 1 \\ x^4 + x^2 + 1 \\ x^4 + x + 1 \end{array} \right\}$$

deg 4.

\mathbb{F}_{16}

all factors in \mathbb{F}_{16}

all roots are distinct?

12 cl's \leftrightarrow cl's of

\uparrow
 $g(x)$ $\mathbb{F}_{16} \cong \mathbb{F}_2(x) / (g(x))$

$\mathbb{F}_{16} \setminus \mathbb{F}_4$
 $x^2 + 2x + 1$

$x \quad x+1$
 $0 \quad 1$

$f(x) = x^4 + x + 1$

$\mathbb{F}_{16} \cong \mathbb{F}_2[x] / (x^4 + x + 1)$

$\mathbb{F}_{16} \cong \mathbb{F}_2 \quad \iota(a) = a^2$

$(1, \alpha, \alpha^2, \alpha^3)$

$a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3$

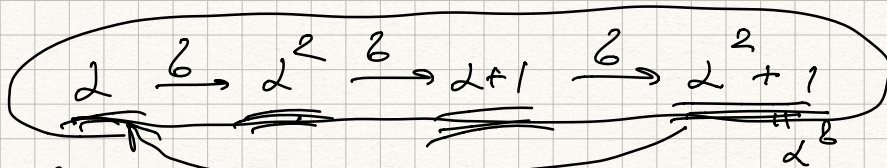
\uparrow $a_i \in \mathbb{F}_2$

$\iota(\text{root}) = \text{root}$

α^2 also a root, $\iota(\alpha^2) = \alpha^4 = \alpha + 1$

$\iota(\alpha^4) = \alpha^8 = (\alpha + 1)^2 = \alpha^2 + 1$ root

$x^4 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha + 1)(x + \alpha^2 + 1)$



orbit of G

$\iota(\alpha^8) = \alpha^{16}$

$x^{16} - x$

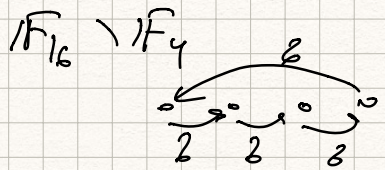
$0, 1,$

E

Principle Galois groups permute roots of polyn. w/ all roots in base field F
 $\text{Gal}(E/F)$

$$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$$

0, 1 ~~2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15~~



$$\beta = \alpha^2 + \alpha$$

β, β^2, \dots

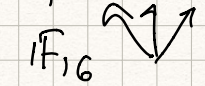
	1	β	β^2	β^3	\dots
1	1	0	1		
α	0	1	1		
α^2	0	1	1		
α^3	0	0	0		

$$\beta^4 = (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\beta^3 =$$

$$\beta^2 + \beta + 1 = 0 \text{ in } \mathbb{F}_{16}$$

$$\text{irr}(\beta, \mathbb{F}_2) = x^2 + x + 1$$



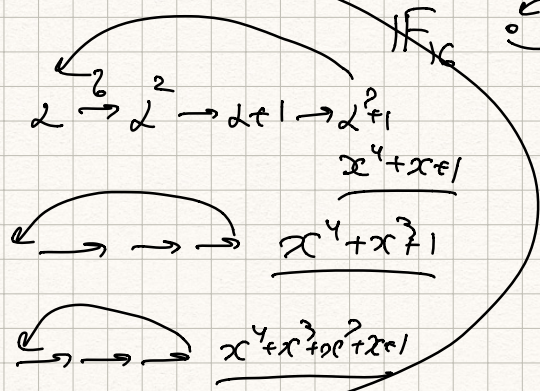
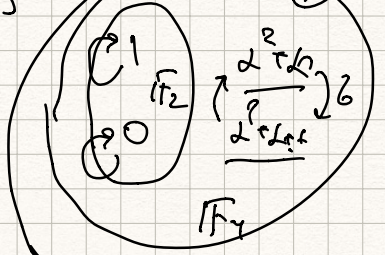
$$\mathbb{F}_2(\beta) = \mathbb{F}_4 \subset \mathbb{F}_{16}$$

$$\mathbb{F}_4 = \{0, 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

$$\underline{G} \quad C_4 = G$$

$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$ ← fixed by $b^4 = \text{id}$

↑ fixed by b
 ↑ fixed by b^2
 b^2 fixes all el's



$$h(x) \rightarrow \mathbb{F}_2[x] / (h(x))$$

3 models.

$$\frac{\mathbb{F}_x}{\mathbb{F}_{16} \supset \mathbb{F}_4}$$

$$F \subset E \quad G = \text{Gal}(E/F)$$

$$H \subset G \quad E^H = \{ \text{all } a \in E : h(a) = a \forall h \in H \}$$

Claim E^H is a subfield of E .

$$E, \quad H \subset \text{Aut}(E) \quad E^H \subset E.$$

$$\mathbb{F}_p \subset \mathbb{F}_q \quad G = \text{Gal}(\mathbb{F}_q / \mathbb{F}_p) = \underline{\text{Aut}(\mathbb{F}_q)}$$

σ - automorphism / homomorphism

$$1, \underline{\sigma}, \underline{\sigma^2}, \underline{\sigma^3}, \dots \in G$$

$$\text{Aut}(\mathbb{F}_p) = \text{id}$$

$$1 \mapsto 1$$

$$\sigma \mapsto ?$$

\vdots

$$\sigma^2 \quad \sigma^2(a) = \sigma(\sigma(a))$$

$$= \sigma(a^p) = (a^p)^p = a^{p^2}$$

$$\underline{(a^n)^m = a^{nm}}$$

$$= a^p \cdot p = a^{p^2}$$

$$g^2 = g \circ g$$

If g out of something

g^n out.

$$\tau \xrightarrow{\sigma} \tau \xrightarrow{\sigma} \tau$$

$\searrow \sigma$

$$G = \text{Gal}(E/F)$$

$$[E:F] < \infty$$

\uparrow
fn. deg

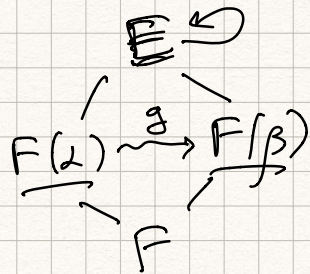
$\forall \alpha \in E$ alg. / F .

fn. irr. pol. of α

$\text{irr}(\alpha, F)$

$$f(\alpha) = 0 \quad f = a_0 + a_1 x + \dots + a_n x^n$$

$$F(\alpha) = F[\alpha] = F[x] / (f(x)) \quad |, \alpha, \dots, \alpha^{n-1}$$



$\beta \in E, \beta$ root of f

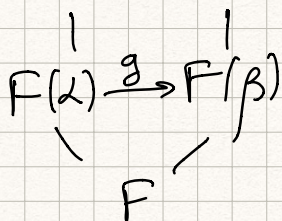
$$g(\alpha) = \beta \quad g(\alpha^k) = \beta^k \dots$$

\exists an isom g

$$g: F(\alpha) \rightarrow F(\beta)$$

$$E \xrightarrow{g} E$$

if E spl. field of f



$\alpha, \beta, \gamma, \dots$

α root of f, g -symm. of E

$\Rightarrow g(\alpha)$ also a root of f .

$$\alpha \xrightarrow{g} \beta = g(\alpha)$$

at most n roots in E

$E \quad \deg f = n$

$\alpha_1 \dots \alpha_i \dots \alpha_n$

G permutes $\alpha_1, \dots, \alpha_n$

$$E = F(\alpha_1, \dots, \alpha_n)$$

$$G \subset S_n$$

$$\mathbb{F}_p \subset \mathbb{F}_q$$

α of $x^4 + x + 1 = f(x)$

$\mathbb{F}_2(\alpha)$ - already contains all other roots of f

$\underline{\alpha} = \underline{\alpha_1}, \underline{\alpha_2}, \underline{\alpha_3}, \underline{\alpha_4}$ at most 4 symmetries

$$\alpha_2 = h_2(\alpha)$$

$$\alpha_3 = h_3(\alpha)$$

$$\alpha \mapsto \beta \in \{\alpha, \alpha_2, \alpha_3, \alpha_4\}$$

$$\alpha_2 = h_2(\alpha) \mapsto h_2(\beta)$$

$$\alpha_3 = h_3(\alpha) \mapsto h_3(\beta) \dots$$

at most 4 symmetries of $\mathbb{F}_2[\alpha]$

$$\mathbb{F}_p \subset \mathbb{F}_{p^n}$$

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = C_n$$

$$|G| = [E:F]$$

best-case scenario.

otherwise $<$.

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

only div. out

$$1 < 3$$

\mathbb{F}_q fields

$$\mathbb{F}_q \subset \mathbb{F}_{q^r}$$

$$r^3 - 2$$

$$\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) = C_r$$

$$\text{order} = r = [\mathbb{F}_{q^r} : \mathbb{F}_q]$$