lect 14 Also see notes

Finite fields, Summary

1) $\forall$ prime p, $n \geq 1$ $\exists$ field $\mathbb{F}_q$, $\mathbb{F}_p \subset \mathbb{F}_q$

$|\mathbb{F}_q| = p^n$ $\qquad \underline{\underline{q = p^n}}$ $\qquad$ p prime

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

split field $\underbrace{x^q - x}_{\text{reducible}}$ $\qquad \prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x$

$\mathbb{F}_p \xrightarrow{\simeq} F$ $\qquad D \quad -1$

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

has generators. $\qquad 1$

$\mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$ iff $k \mid n$

v.s.

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

$\underline{x}^q - x$ $\quad q = p^n$

$\underline{x^{p^k}} - \underline{x}$ $\Big]$ a divisor of $\qquad x^{p^n} = x \Rightarrow x^{(p^k)^m} = x$

$\exists \alpha$ that is a $\underline{\text{generator of } \mathbb{F}_q^*}$ $\left(\begin{array}{l} \text{note } C_m \\ \# \text{gen} = \\ \# \left(\begin{array}{l} k : \gcd(k, m) = 1 \\ 1 \leq k \leq m-1 \end{array} \right) \\ \varphi(n) \end{array} \right)$

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

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

$q = p^n$

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

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

$\forall$ such f $\quad$ $\mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_q$

p^n $\qquad$ $\mathbb{F}_{p^2} \not\subset \mathbb{F}_{p^3}$

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4}, \quad \subset \mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}, \quad \subset \mathbb{F}_{p^5} \to \mathbb{F}_{p^{10}} \ldots$$

diff such f, g $\quad$ $\underline{\mathbb{F}_p[x]/(f(x))} \simeq \mathbb{F}_p[y]/(g(y)) \simeq$

$\simeq \mathbb{F}_q$ $\quad$ $1, x, x^2, \ldots x^{n-1}$

$f(x) \mid x^q - x.$ $\qquad$ $y = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$

$\underline{\mathrm{irr}}$ root α $\quad$ $\alpha^q = \alpha$ $\qquad$ $\forall$ irr monic g

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

$\underline{g(x) \mid x^q - x}$ $\quad$ $\Rightarrow \prod\limits_{\substack{g\text{-irr,} \\ \deg n, \text{ monic}}} g(x) \mid x^q - x$

$(g_1(x), g_2(x)) = 1$ $\qquad$ nearly all of

char$(F) = p$

Frob hom (aut finite fields) $\qquad$ $F \to F$, $a \mapsto a^p$.

$\underline{\sigma : \mathbb{F}_q \to \mathbb{F}_q}$ $\quad$ $\sigma(a) = a^p$ autom.

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

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

$F \subset E$ $\quad$ $\underline{Gal(E/F)}$ - all sym of E g fix $g|_F = id_F$.

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

g $\quad$ $g(1)=1$ $\quad$ g = id on the prime subfield

$g(2)=2$ $\quad$ $\mathbb{F}_p \subset E$ or $\mathbb{Q} \subset E$

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

σ: $\quad$ $\underbrace{\{id, \sigma, \sigma^2, \dots, \sigma^{n-1}\}}$ all distinct aut of $\mathbb{F}_q$

$a^{p^n}=a$ $\forall a \in \mathbb{F}_q$ $\quad$ $|\sigma|$? less than n?

$\sigma^n(a)$ $\quad$ $\underline{d<n}$ $\sigma^d = id$ $\quad$ $d \mid n$.

$\underline{a^{p^d} = a}$ $\forall a \in \mathbb{F}_q$ $\quad$ $x^q - x$.

$\mathbb{F}_{p^d}$ $\quad$ $x^{p^d} - x$

$q = p^n > p^d$ - sol

$\mathbb{F}_q \supset \mathbb{F}_{p^d}$

__Note__ $\quad$ σ gen group C_n

$$\boxed{Aut(\mathbb{F}_q) \simeq C_n}$$

$Aut(\mathbb{F}_q) \supset \underline{\underline{C_n}}$.

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

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

__Propod__ $\quad$ E/F splitting field. f

$\#$ sym $\quad$ $|Gal(E/F)| \underline{\underline{\le}} [E:F]$

= if f is separable. $\quad x^3-2$

if E not a spl. field $\quad \mathbb{Q}(\sqrt[3]{2})$

$E \supset \underline{\mathbb{Q}(\sqrt[3]{2})} \supset \mathbb{Q}$ $\quad$ $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) =$

$= \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$ $\quad g^{\mathbb{Q}}$ $\quad$ prime

$\underline{x^3-2}$

$\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ $\quad$ $g(\alpha)=\alpha \Rightarrow g(\alpha^2)=\alpha^2$

$\alpha=\sqrt[3]{2}$ $\quad$ g is id. on $\underline{\mathbb{Q}(\alpha)}$

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

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

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

"bad" extension $\quad E/F \quad |\mathrm{Gal}(E/F)| < [E:F]$

All extensions of fin fields are "good".

$G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \simeq C_n$ $\quad$ $|G| = n = [\mathbb{F}_q : \mathbb{F}_p]$

abelian $\quad S_n$

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

not abelian.

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

$6 \quad 6^n \quad q=p^n$ $\quad$ $\forall$ fin G is the Galois $\mathrm{Gal}(E/F) \simeq G$.

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

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

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

$$x^p - a = (x-b)^p = x^p - b^p$$

$\forall$ 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-th roots $\quad a_0 = b_0^p \quad a_1 = b_1^p \dots$

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

Possible $\operatorname{char} F = p \quad |F| = \infty \Rightarrow$ then may have such irr f

$F = \mathbb{F}_p(t)$ ← rat. f's

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

$x^p - t$ inseparable.

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

$\sqrt[p]{u}$

$\vdots$

$\sqrt[p^n]{t} \dots \qquad x^p - t = (x-u)^p.$

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

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

Ex

$\mathbb{F}_q \subset \mathbb{F}_{q^r}$ 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 $\mathbb{F}_{p^m} \Longleftrightarrow$ divisors of m

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

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

$\{0,1\} \quad \gamma, \gamma+1$

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

$\underline{x^2+x+1}$

4

$(x+\gamma)(x+\gamma+1)$

$\mathbb{F}_{16} \qquad \mathbb{F}_2[\alpha] / (f(\alpha))$

$x^4 + a_3 x^3 + a_2 x^2 + a_1 x + 1 \qquad a_i \in \mathbb{F}_2$

✓ $x^4 + x^3 + 1 \qquad f(1) \neq 0$

$x^4 + x^2 + 1 = (x^2+x+1)^2 \qquad a_1 + a_2 + a_3 = 1$

✓ $x^4 + x^3 + x^2 + x + 1$

✓ $x^4 + x + 1$

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

deg 4. $\mathbb{F}_{16}$

all factor in $\mathbb{F}_{16}$

all roots are distinct?

12 α's $\Leftrightarrow$ α's of $\mathbb{F}_{16} \setminus \mathbb{F}_4$.

x^2+x+1

$x \quad x+1$

$0 \quad 1$

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

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

$$\underline{\mathbb{F}_{16} \simeq \mathbb{F}_2[\alpha]/(\alpha^4+\alpha+1)}$$

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

$\underline{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3}$

$a_i \in \mathbb{F}_2$

$\mathbb{F}_{16} \circlearrowleft \sigma \qquad \sigma(a) = a^2$

$\sigma(\text{root}) = \text{root}$.

$\underline{\alpha}$, $\underline{\alpha^2}$ also a root, $\quad \sigma(\alpha^2) = \alpha^4 = \alpha+1$,

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

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

$$\alpha \xrightarrow{\sigma} \alpha^2 \xrightarrow{\sigma} \alpha+1 \xrightarrow{\sigma} \underset{\alpha^8}{\underset{\parallel}{\alpha^2+1}}$$

σ

orbit of G

$\sigma(\alpha^8) = \alpha^{16} \qquad x^{16}-x$

$0, 1,$

E

Principle Galois groups permute roots of polyn. with coeff in base field F

$\mathrm{Gal}(E/F)$

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

$0, 1 \qquad \gamma, \gamma+1$

$\mathbb{F}_{16} \setminus \mathbb{F}_4$

$\sigma \quad \sigma \quad \sigma \quad \sigma$

$\beta = \underline{\alpha^2 + \alpha}$

$1, \beta, \beta^2, \ldots$

	1	β	β^2	$\beta^3 \ldots$
1	1	0	1	
α	0	1	1	
α^2	0	1	1	
α^3	0	0	0	

$\mathbb{F}_{16}$

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

$\beta^3 =$

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

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

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

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

$\underline{\sigma} \qquad C_4 = G$

$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16} \leftarrow$ fixed by $\sigma^4 = id$

fixed by σ — fixed by σ^2

σ^2 fixes all el's

$1 \quad 0 \quad \mathbb{F}_2$

$\alpha^2 + \alpha \rightleftarrows_{\sigma} \alpha^2 + \alpha + 1$

$\mathbb{F}_4$

$\mathbb{F}_{16}$

$\alpha \xrightarrow{\sigma} \alpha^2 \to \alpha + 1 \to \alpha^2 + 1$

$\underline{x^4 + x + 1}$

$\underline{x^4 + x^3 + 1}$

$\underline{x^4 + x^3 + x^2 + x + 1}$

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

3 models.

$\underline{\underline{Ex}}$

$F_{16} \supset \mathbb{F}_4$

$\underline{\underline{?}}.$

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

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

Claim E^H is a subfield of E.

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

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

σ – automorphism / homomorphism

$1, \sigma, \sigma^2, \sigma^3 \ldots \in G$

$\text{finite} \quad F \xrightarrow{\sigma} F$ injective $\Downarrow$ bijective

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

$1 \mapsto 1$

$2 \mapsto 2$

$\vdots$

If g aut of something g^n aut.

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

$= \sigma(a^p) = (a^p)^p = a^{(p^2)} \quad g^2 = gg \quad T \xrightarrow{g} T \xrightarrow{g} T$, $\; g^2$

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

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

$G = \mathrm{Gal}(E/F) \quad [E:F] < \infty$

fin. deg $\quad \forall \alpha \in E$ alg. $/F$.

fin. irr. pol. of $\alpha \quad \mathrm{irr}(\alpha, F)$

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

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

$$\begin{tikzcd} & E \arrow[loop right] & \\ F(\alpha) \arrow[ur, dash] \arrow[rr, squiggly, "g"] & & F(\beta) \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\beta \in E$, β root of f

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

$\exists$ an isom $g \quad g : F(\alpha) \to F(\beta)$

$$\begin{tikzcd} E \arrow[r, dashed, "g"] & E \\ F(\alpha) \arrow[u, dash] \arrow[r, "g"] \arrow[dr, dash] & F(\beta) \arrow[u, dash] \\ & F \arrow[u, dash] \end{tikzcd}$$

if E spl. field f

$\alpha, \beta, \gamma \ldots$

α root of f, g - symm. of E

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

at most n roots in E

$\alpha \xrightarrow{g} \beta = g(\alpha)$. $\quad E \quad \deg f = n$

$\alpha_1 \ldots \alpha_i \, \alpha_n$

if

G permutes $\alpha_1 \ldots \alpha_n$ $\quad E = F(\alpha_1 \ldots \alpha_n)$

$G \subset S_n$

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

α of $x^4 + x + 1 = f(x)$

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

$\underline{\underline{\alpha}} \quad \underline{\alpha_2}, \underline{\alpha_3}, \underline{\alpha_4}$. at most 4 symmetries

$\alpha_2 = h_2(\alpha)$ $\qquad$ $\alpha \xrightarrow{g} \beta \in \{\alpha, \alpha_2, \alpha_3, \alpha_4\}$

$\alpha_3 = h_3(\alpha)$ $\qquad$ $\alpha_2 = h_2(\alpha) \mapsto h_2(\beta)$

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

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

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

$|G| = [E:F]$ best-case scenario.

otherwise $<$.

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

only 1 triv. aut

$1 < 3$

$x^3 - 2$

fin fields

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

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

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