Summary of finite fields & their properties

lect 14

Thm 1) For each prime p, $n \geq 1$ there exists a field $\mathbb{F}_q$ of order $q = p^n$, $\mathbb{F}_p \subset \mathbb{F}_q$.

2) $\mathbb{F}_q$ is the splitting field of polynomial $x^q - x = x^{p^n} - x$ and $\mathbb{F}_q$ consists of all roots of $x^q - x$

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

← large degree polynomial

3) Any field F of order q is isomorphic to $\mathbb{F}_q$ $\quad F \simeq \mathbb{F}_q$

4) $|\mathbb{F}_q^*| = q - 1 = p^n - 1$, $\mathbb{F}_q^*$ is a cyclic group, $\mathbb{F}_q^* \simeq C_{q-1}$

5) $\mathbb{F}_q$ is a vector space / $\mathbb{F}_p$ of dimension n.

6) $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^n}$ (a subfield) iff $k \mid n$ (k is a divisor of n)

2 × 3
$\mathbb{F}_{2^2} \not\subset \mathbb{F}_{2^3}$
not a subfield

7) if $\alpha \in \mathbb{F}_q^*$ is a generator of that cyclic group, then

$f(x) = \mathrm{irr}(\alpha, \mathbb{F}_p) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in \mathbb{F}_p$ (*)

has degree n and $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f(x))$, $f(x) \mid x^q - x$

all roots of f are $\alpha, \beta(\alpha), \beta^2(\alpha), \dots, \beta^{n-1}(\alpha)$ — n roots.

8) for any monic irreducible $g(x) = x^n + b_{n-1}x^{n-1} + \dots + a_0$, $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(g(x))$,

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

g - monic, irr / $\mathbb{F}_p$

↖ this product gives a very large degree factor of $x^q - x$

9) Frobenius homomorphism $\beta : \mathbb{F}_q \to \mathbb{F}_q$, $\beta(a) = a^p$, is an automorphism of $\mathbb{F}_q$, $\beta \in \mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p)$ $\quad \beta^2(a) = (a^p)^p = a^{p^2}$, $\beta^3(a) = a^{p^3}$, ..

$\{id, \beta, \beta^2, \dots, \beta^{n-1}\}$ - all distinct automorphisms of $\mathbb{F}_q$

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

cyclic group of order n, generated by β.

10) $$x^q - x = \prod_{\substack{g \text{ - monic,} \\ \text{irr} / \mathbb{F}_p, \\ \deg g \mid n}} g(x)$$

$q = p^n$

$x^q - x$ factors into the product of all monic polynomials that are irreducible over $\mathbb{F}_p$ of degree a divisor of n.

11) Any finite field $\mathbb{F}_q$ is perfect (p-th roots exist for all elements of $\mathbb{F}_q$).

12) Any polynomial $f \in \mathbb{F}_q[x]$ is separable. (if f is irreducible & $Df = 0$
$\Rightarrow f(x) = a_0 + a_1 x^p + \dots + a_n x^{pn}$
$\Rightarrow g(x) = \sqrt[p]{a_0} + \sqrt[p]{a_1}\, x + \dots + \sqrt[p]{a_n}\, x^n$.
$g^p(x) = g(x)^p = f(x)$
contradiction)

13) Any finite field extension $\mathbb{F}_q \subset \mathbb{F}_{q^r}$ is simple ($F \subset E$ is simple if $\exists \alpha \in E$, $E = F(\alpha)$).

Any finite field extension is of this form, $\mathbb{F}_q \subset \mathbb{F}_{q^r}$, $q = p^n$, some p, n, r

$\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \simeq C_r$ generated by σ_q,
$\sigma_q(a) = a^q$, $a \in \mathbb{F}_{q^r}$

compare $\sigma = \sigma_p$ and $\sigma_q = \sigma_p^n$ — power of σ has more fixed points, fixes a larger field

$$\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^r}$$
(σ acts on $\mathbb{F}_{q^r}$)
$\sigma|_{\mathbb{F}_p} = \mathrm{id}$ — $\mathbb{F}_{p^n}$ — $\mathbb{F}_{p^{nr}}$

$\sigma^n|_{\mathbb{F}_q} = \mathrm{id}$
$\uparrow$
$x^q = x$ for $x \in \mathbb{F}_q$.

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

better call β, use α below for small else $\beta, \beta+1$

$\{0,1\}$ $\quad \subset \quad \{0, 1, \alpha, \alpha+1\}$

x^2+x+1 ← unique monic irrep deg 2 / $\mathbb{F}_2$

$\text{irr}(\alpha, \mathbb{F}_2) = x^2+x+1$ "$+ = -$" in char 2.

$x^2+x+1 = (x+\alpha)(x+\alpha+1)$ — irr in $\mathbb{F}_2$; factors in $\mathbb{F}_4$

α here is different from α below relabel this $\alpha+1 = \beta$

$|\mathbb{F}_{16}| = 16$, $|\mathbb{F}_4| = 4$ — 12 el's in $\mathbb{F}_{16}$ not in $\mathbb{F}_4$

each of these elements have degree 4, roots of irreps of deg 4 / $\mathbb{F}_2$

Find irreds of deg 4 / $\mathbb{F}_2$

$a_i \in \mathbb{F}_2$

$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ $\quad a_0 \neq 0 \Rightarrow a_0 = 1$

$x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ $\Rightarrow$ $1 + a_3 + a_2 + a_1 + 1 = 1$ since $x=1$ not a root

$a_1 + a_2 + a_3 = 1$.

$x^4 + x^3 + x^2 + x + 1$ — irr

$x^4 + x^3 + 1$ — irr

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

$x^4 + x + 1$ — irr

3 monic irreps / $\mathbb{F}_2$ of degree 4

$(*)$ $\left\{ \begin{array}{l} x^4+x^3+x^2+x+1 \\ x^4+x^3+1 \\ x^4+x+1 \end{array} \right\}$ each one factors fully in $\mathbb{F}_{16}$,

Remark f - irrep, deg 4 / $\mathbb{F}_2$ $\Rightarrow$ $\mathbb{F}_2[x]/(f(x)) \simeq \mathbb{F}_{16}$ no choice — such field is unique up to isomorphism.

for each such f get a concrete realization of $\mathbb{F}_{16}$ as such quotient (3 realizations)

Choose $f(x) = x^4+x+1$ $\quad \mathbb{F}_{16} \simeq \mathbb{F}[\alpha]/(\alpha^4+\alpha+1)$ $\quad$ basis $\{1, \alpha, \alpha^2, \alpha^3\}$

$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ $\quad a_i \in \mathbb{F}_2$ ← all el's of $\mathbb{F}_{16}$.

$\mathbb{F}_{16} \circlearrowleft \delta$ automorphism (Frobenius) acts on $\mathbb{F}_{16}$, $\quad \delta^4 = 1$ (identity)

- takes roots of f to roots of f $\Rightarrow$ permutes the roots (4 roots since irr, separable)

α root of f $\Rightarrow$ α^2 is a root, $\quad \alpha^4 = \alpha+1$ is a root, $\quad (\alpha^4)$

$\alpha^8 = (\alpha+1)^2 = \alpha^2+1$ is a root $\quad$ check that $\alpha^{16} = \alpha$ $\quad (\alpha^8)$

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

factors fully in $\mathbb{F}_{16}$, irr in $\mathbb{F}_2$

$\alpha^2+1 \xleftarrow{\delta} \alpha+1$

$\downarrow$ $\qquad \uparrow \delta$

$\alpha \xrightarrow[\delta]{} \alpha^2$ $\quad (\alpha^{16})$

This "explains" 6 out of 16 elements of $\mathbb{F}_{16}$:

$\{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+1\}$

↑ in prime field $\mathbb{F}_2$

what about the remaining 10 elements?

Principle: Galois groups permute roots of polynomials with coefficients in base field F $\quad \text{Gal}(E/F)$.

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

12 elements in $\mathbb{F}_{16} \setminus \mathbb{F}_4$.

split into 3 groups of 4 elements each

each group contains 4 roots of one of the three monic irreps / $\mathbb{F}_2$ deg 4, see (*) page 3.

$x^4+x+1 \rightsquigarrow^{\text{roots}} \{\alpha, \alpha^2, \alpha+1, \alpha^2+1\}$ permuted by Frobenius δ

$\alpha \quad \alpha^2 \quad \alpha^4 \quad \alpha^8$

$\delta(y) = y^2$, $y \in \mathbb{F}_{16}$

$0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1$ already accounted for.

take the "next" one

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

write $\beta, \beta^2, \beta^3 \ldots$ in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$

to find $\operatorname{irr}(\beta, \mathbb{F}_2)$:

	1	β	β^2	β^3
1	1	0	1	⋮
α	0	1	1	
α^2	0	1	1	
α^3	0	0	0	

already done!

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

$\alpha^4 + \alpha + 1 = 0$

$\Downarrow \alpha^4 = \alpha + 1$

$\beta^2 + \beta + 1 = 0$ (add 3 columns to get $\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$)

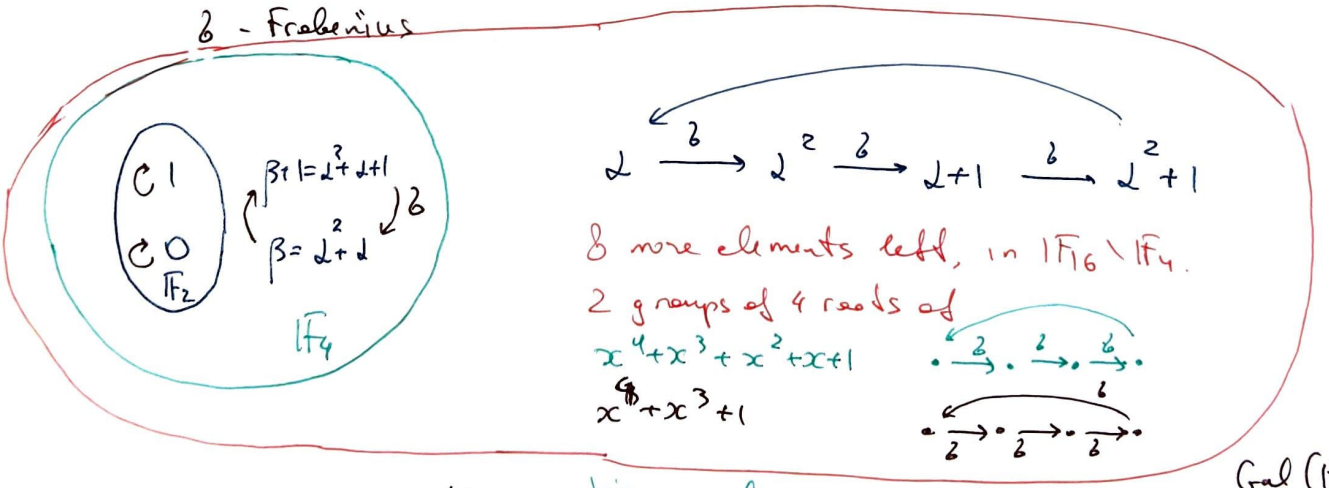
Got lucky: $\Rightarrow \operatorname{irr}(\beta, \mathbb{F}_2) = x^2 + x + 1$

$\mathbb{F}_2(\beta) \subset \mathbb{F}_{16}$ is the subfield $\mathbb{F}_4$

$\mathbb{F}_4 = \{0, 1, \beta, \beta+1\}$ $\{1, \beta\}$-basis of $\mathbb{F}_4/\mathbb{F}_2$

Execise: find the other 2 groups of 4 elements, their irreducible pols and how δ acts on them

δ - Frobenius



C_4 has subgroups H: (bigger subgroup →)

$H = \{1\}$ $\quad$ $H = \{1, \delta^2\}$ $\quad$ $H = \{1, \delta, \delta^2, \delta^3\} = C_4$

$\mathbb{F}_{16}^H = \mathbb{F}_{16}$ $\quad$ $\mathbb{F}_{16}^{\delta^2} = \mathbb{F}_4$ $\quad$ $\mathbb{F}_{16}^{C_4} = \mathbb{F}_2$

entire field $\quad$ $\delta^2 = \mathrm{id}$ on $\mathbb{F}_4$

(→ smaller subfield)

$\operatorname{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) = \operatorname{Aut}(\mathbb{F}_{16}) \simeq C_4 \simeq \{1, \delta, \delta^2, \delta^3\}$.

Fixed field $H \subset \operatorname{Gal}(E/F)$

$E^H = \{a \in H \mid ha = a \ \forall h \in H\}$

bigger subgroup ↔ smaller subfield