12/2/2021 Lecture 11 (Finite Fields, Minimal Polynomials)

Construction of Finite fields

$R_f = \mathbb{F}_p[x] \setminus f(x)$.

$\mathbb{F}_p[x]$: Polynomial ring over $\mathbb{F}_p$.

Elements of this set are equivalence classes

If $\deg(f) = d$, then there is a one-one correspondence between each element of R_f and the set of all polynomials over $\mathbb{F}_p[x]$ with degree at most $(d-1)$.

$(R_f, +, \cdot)$

$[a(x)] + [b(x)] = [a(x) + b(x)]$.

$[a(x)] \cdot [b(x)] = [a(x) \cdot b(x)]$

Assignment tomo
→ You can leave Q6.

Abelian group under addition.
Closure under multiplication,
Commutative, associative, distributive.

$a(x)$ and $b(x)$ belong to the same equivalence class if $f(x) \mid (a(x) - b(x))$.

Existance of inverse for any element.
Suppose $[a(x)]$ where $\deg(a) \leq d-1$

$$\underline{\gcd(a(x), f(x)) = 1.}$$

$\exists$ $r(x)$ and $s(x)$ s.t.

$$\boxed{a(x)\,r(x) + s(x)\,f(x) = 1.}$$

Applying mod $f(x)$ to the above equation.

$$[a(x) \cdot r(x)] + [0] = [1].$$

$$[a(x)] \cdot [r(x)] = [1].$$

$$[r(x)] = [a(x)]^{-1}.$$

Claim:- over any finite field $\mathbb{F}_p$ and any d, $\exists$ an irreducible polynomial over $\mathbb{F}_p$ of deg d.

Any finite field has a certain vector space structure and also a certain multiplicative structure.

We are going to make some deductions assuming $\mathbb{F}_q$.

Defn: The characteristic p of a finite field $\mathbb{F}_q$ is the smallest integer p s.t.

$$\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0 \text{ in } \mathbb{F}_q.$$

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = \underbrace{1+\cdots+1}_{m \text{ times}}$$

$\Downarrow$

$n > m$:

If you add 1 $(n-m)$ no. of times, you get 0.

Theorem: The characteristic p of a FF. $\mathbb{F}_q$ must be a prime number.

Proof: Suppose p is not a prime no.

$$p = a \cdot b. \quad a < p, \quad b < p$$

$$(1+1+\cdots+1) = 0.$$

$$\underbrace{(1+1\cdots+1)}_{a \text{ times}}\underbrace{(1+\cdots+1)}_{b \text{ times}} = 0.$$

$\underbrace{(1+\cdots+1)}_{a \text{ times}} = 0$

or

$\underbrace{(1+\cdots+1)}_{b \text{ times}} = 0$

} Contradicts the minimality of p satisfying the condition that

$\underbrace{1+\cdots+1}_{p \text{ times}} = 0$

$\Rightarrow$ p has to be a prime number.

$\mathbb{F}_q$.

$\{0, 1, \underbrace{2}_{1+1} \ldots \underbrace{p-1}_{\underbrace{1+\cdots+1}_{(p-1) \text{ times}}}\} = \mathbb{F}_p$.

$\mathbb{F}_p \subseteq \mathbb{F}_q$.

$\mathbb{F}_p$ is a field by itself.

Subfield:- Let $\mathbb{E}$ and $\mathbb{F}$ be fields such that $\mathbb{F} \subseteq \mathbb{E}$, then. $\mathbb{E}$ is said to be extension field of $\mathbb{F}$ and $\mathbb{F}$ is said to be

subfield of $\mathbb{E}$.

$$\mathbb{F}_p \subseteq \mathbb{F}_q.$$

$\mathbb{F}_q$ is an extension field of $\mathbb{F}_p$ and $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$.

Theorem:- If $\mathbb{E}$ is an extension field of $\mathbb{F}$, then $(\mathbb{E}, +, \mathbb{F}, \cdot)$ is a vector space.

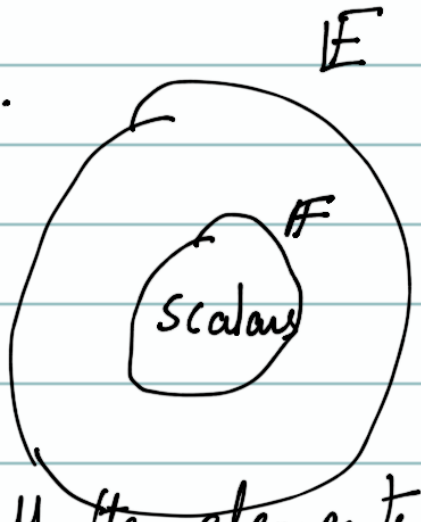
$\mathbb{E}$: extension field. $\mathbb{F}$: field. $\cdot$ is multiplication in $\mathbb{E}$. $+$ is addition in $\mathbb{E}$.

$a \in \mathbb{E}, \; b \in \mathbb{E}, \; a+b \in \mathbb{E}$.

$c \in \mathbb{F}, \; a \in \mathbb{E}, \; a.c \in \mathbb{E}$

Abelian group under vector addition

scalar multiplication.



All the elements in $\mathbb{E}$ are vectors

$\mathbb{F}_{2^4} \simeq \mathbb{F}_p[x] \,|\, f(x)$. $\quad f(x) = x^4 + x + 1$

$\mathbb{F}_p \rightarrow [0], [1], \ldots [p-1]$.

$\mathbb{F}_p[x] \,|\, f(x)$ forms a vector space over $\mathbb{F}_p$.

$[0], [1]$.

$\mathbb{E} : \mathbb{F}_p[x] \,|\, f(x)$. $\qquad \mathbb{E}$

$\mathbb{F} : [0], [1] \qquad\qquad \mathbb{F}$.

$\mathbb{F}_q$ $\quad (\mathbb{F}_q, +, \mathbb{F}_p, \cdot)$ is a vector space.

$\mathbb{F}_p$.

Let $\{ r_1, r_2, \ldots, r_m \}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$.

What is the size of $\mathbb{F}_q$? $= p^m$.

We started off with $\mathbb{F}_q \rightarrow$ There should exist an $\mathbb{F}_p$ sitting inside $\mathbb{F}_q$ which has prime no. of elements.

$\mathbb{F}_q$ is a vector space of $\mathbb{F}_p$.

Three facts put together imply that
$q = p^m$ for some $m > 0$.

$$x = \sum_{i=1}^{m} a_i r_i \qquad r_i \in \mathbb{F}_q, \quad a_i \in \mathbb{F}_p.$$

Example: $\left(\mathbb{F}_2[x] \,\middle|\, (x^4 + x + 1), +, \cdot \right)$.

Basis and the subfield of interest are all in terms of equivalence classes.

Another equivalent description of elements of the above finite field.

Analogy is from complex numbers.

$$\mathbb{C} = \mathbb{R}[x] \,\middle|\, (x^2+1) \qquad a + bi,\ a, b \in \mathbb{R}.$$

where i is a soln to $x^2 + 1 = 0$.

$\mathbb{R}$

Introducing an imaginary element "i".

$\{1, i\}$ basis elements.

$\mathbb{F}_q = \mathbb{F}_2[x] \big/ (x^4 + x + 1) \Rightarrow \mathbb{F}_2^4 = \mathbb{F}_{16}$.

Let "α" be an imaginary element which satisfies the condition

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

$\alpha \in \mathbb{F}_q$; $\alpha^2, \alpha^3 \in \mathbb{F}_q$.

Basis of $\mathbb{F}_q$ over $\mathbb{F}_2$ is $\{1, \alpha, \alpha^2, \alpha^3\}$

$$\alpha \equiv [x].$$

Give me an example of $\mathbb{F}_9 = \mathbb{F}_3^2$

$$\mathbb{F}_3[x] \big/ (x^2 + 1)$$

Let $\alpha^2 + 1 = 0$, where α is your imaginary element in $\mathbb{F}_9$.

$\{1, \alpha\}$ basis.

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha\}$$

Multiplicative structure of a finite field

$\mathbb{F}_q$, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

Defn:- The order of an element $\beta \in \mathbb{F}_q^*$ is the smallest nonzero integer n s.t

$$\beta^n = 1.$$

$$\underbrace{\beta \cdot \cdots \cdot \beta}_{n \text{ times}} = \underbrace{\beta \cdot \cdots \cdot \beta}_{m \text{ times}}$$

$$\beta^{n-m} = 1$$

Theorem:- Every FF contains an element α of order $= (q-1)$. In terms of α, $\mathbb{F}_q$ has the following simple representation.

$$\mathbb{F}_q = \{0\} \cup \{ \alpha^i \mid 0 \le i \le (q-2) \}$$

$\alpha^{q-1} = 1$ and $q-1$ is the smallest integer which satisfies this property.

Such an element α is called as primitive element of $\mathbb{F}_q$. It need not be unique.

$\alpha^{m_1} = \alpha^{m_2}$ for some m_1, m_2

$0 \le i \le q-2$

$\alpha^{m_1 - m_2} = 1 \quad 0 \le m_1 - m_2 \le q-2$

↳ Cannot happen.

$\alpha^0, \alpha^1, \ldots, \alpha^{q-2}$ are all distinct elements.

There are $(q-1)$ such elements.

<u>Example:-</u> $\left(\mathbb{F}_2[x]/(x^4+x+1), +, \cdot\right)$

Assume α satisfies $\alpha^4 + \alpha + 1 = 0$.

What is order of α.

$\alpha^5 = \alpha + \alpha^2$

$\alpha^6 = \alpha^2 + \alpha^3$

$\alpha^7 = \alpha^3 + 1 + \alpha$.

$\alpha^8 = 1 + \alpha^2$

$\alpha^9 = \alpha + \alpha^3$

$\alpha^{10} = \alpha^2 + 1 + \alpha$

$\alpha^{11} = \alpha^3 + \alpha + \alpha^2$

$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$

$\alpha^{13} = 1 + \alpha^2 + \alpha^3$

$\alpha^{14} = 1 + \alpha^3$

$\alpha^{15} = 1$

$O(\alpha) = 15$

α is the primitive element of $\mathbb{F}_{16}$

$\alpha^2, \alpha^7, \alpha^8 \qquad (\alpha^3)^5 = 1$

Defn: We define minimal polynomial $m_\beta(x)$ of an element $\beta \in F_q$ to be the smallest degree monic polynomial over F_p of which β is a zero.

$$m_\beta(\beta) = 0.$$

$m_\beta(x)$ is monic

Coeff of m_β are in F_p which is a subfield of F_q

$x - \beta$

Minimal polynomial corresponding to the primitive element is called as primitive polynomial.

Lemma: $m_\beta(x)$ is irreducible polynomial over F_p.

Proof: Suppose $m_\beta(x)$ is not irreducible.

$m_\beta(x) = g(x)\, h(x)$ — $\deg(g(x)) < d$ & $\deg(h(x)) < d$.

$m_\beta(\beta) = g(\beta)\, h(\beta) = 0. \Rightarrow g(\beta) = 0$ or $h(\beta) = 0$

Lemma: Let $\mathbb{F}_q$ be the FF with $\mathbb{F}_q$ - 1 and $\mathbb{F}_p$ $q = p^m$.

$$\deg\left(m_\beta(x)\right) \leq m.$$

Proof: Consider the sequence of elements

$1, \beta, \beta^2, \ldots, \beta^m$ ← Collection of $(m+1)$ elements.

$\mathbb{F}_q = p^m$.

$\mathbb{F}_p$ → In particular, any basis will have m elements

⇓

Any $(m+1)$ elements are linearly dependent.

$\{1, \beta, \beta^2, \ldots, \beta^m\}$ → linearly dependent set with coeffs from $\mathbb{F}_p$.

$$\sum_{i=1}^{m} a_i \beta^i = 0. \leftarrow \text{Say } f(x) = \sum_{i=1}^{m} a_i x^i$$

$f(\beta) = 0$ & $\deg(f(x)) \leq m$

$$\Rightarrow \deg\left(m_\beta(x)\right) \leq \deg\left(f(x)\right) \leq m.$$