L11.1

Monday, October 10, 2022 9:57 AM

* Let us study a bit more on the properties of finite-field polynomials

---

* Def'n: Let $\alpha \in GF(p^m)$. A <u>minimal</u> polynomial of α is the ② smallest degree monic (non-zero) polynomial $f(x) \in \mathbb{F}_p[x]$ such that ① $f(\alpha) = 0$ in $GF(p^m)$

Theorem: $\forall \alpha \in GF(p^m)$, its <u>minimal polynomial</u> $f(x)$ exists and it is unique.

Furthermore, $f(x)$ must also satisfy the following properties (in addition to ①, ②

③ $\deg(f(x)) \leq m$

④ for all $\tilde{f}(x) \in \mathbb{F}_p[x]$,

④ for all $f(x) \in F_p[x]$,
$\tilde{f}(\alpha) = 0$ in $GF(p^m)$ implies
$f(x) \mid \tilde{f}(x)$ in $F_p[x]$

⑤ $f(x)$ is irreducible in $F_p[x]$.

Some remarks (partial proof)

* $\tilde{f}(x) = Q(x) \cdot f(x) + r(x)$

$\Rightarrow \tilde{f}(\alpha) = Q(\alpha) \cdot 0 + r(\alpha) = 0$

because $f(x)$ is "minimal"

$\Rightarrow r(\alpha) = 0 \Rightarrow r(x) = 0$ is zero-polynomial

$\Rightarrow$ uniqueness of $f(x)$ & ④

* If $f(x) = a(x) \cdot b(x)$

then $f(\alpha) = a(\alpha) \cdot b(\alpha) = 0$.

$\Rightarrow$ either $a(\alpha) = 0$ or $b(\alpha) = 0$.

contradicts "minimal deg."

Relationship to Primitive Polynomials.

If $\alpha \in GF(p^m)$ is also <u>primitive</u> then, the minimal polymomial of α is exactly the primitive polynomial $g(x)$ that generate $GF(p^m)$

Q: Any further relationship between α and its minimal polynomial?

Conjugates: $\beta \in GF(p^m)$, the conjugates of β w.r.t. $GF(p)$ are

$$\beta, \beta^{p}, \beta^{p^2}, \ldots\ldots$$

i.e. apply $(\ )^p$ iteratively

The <u>congugacy class</u> of $\beta \in GF(p^m)$ with respect to $GF(\ )$ is with respect to [illegible] is

$$\{ \beta^{p^i} \in GF(p^m) : i = 0, 1, 2, \cdots \}$$

Fact #1: (Proof sketches)

The conjugacy class is finite

proof: because $GF(p^m)$ is finite.

Fact #2: First repeated element is

$$\beta \longrightarrow \beta^{p^1} \longrightarrow \beta^{p^2} \cdots\cdots \beta^{p^{d-1}}$$

totally d of them

Fact #3: $d \mid m$

$$\because \beta^{p^m} = \beta \quad \text{and} \quad \beta^{p^d} = \beta$$

$$\Rightarrow \left(\beta^{p^d}\right)^{p^{m-d}} = \beta$$

$$\Rightarrow \beta^{p^{m-d}} = \beta$$ repeated applying this relationship

$$\Rightarrow d \mid m$$

this relationship

$\Rightarrow d \mid m$

Roots theorem

Let $\alpha \in GF(p^m)$ and $f(x) \in \mathbb{F}_p[x]$ is the <u>minimal polynomial</u> of α.

Then the roots of $f(x)$ in $GF(p^m)$ are exactly the conjingacy class of $f(x)$. i.e. $\{\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \cdots \alpha^{p^{d-1}}\}$

and $f(x)$ can thus be written as

$$f(x) = \prod_{i=0}^{d-1} (x - \alpha^{p^i}) \quad \text{in } GF(p^m)$$

Theorem: For $\forall\ m, r > 0$ integers. and $\forall\ f(x) \in \mathbb{F}_{p^m}[x]$

$$= f_0 + f_1 x^1 + \cdots + f_L x^L$$

We have

$$(f(x))^{p^r} = f_0^{p^r} + f_1^{p^r} x^{p^r} + \cdots + f_L^{p^r} x^{p^r \cdot L}$$

$$(f(x))^{p^r} = f_0^{p^r} + f_1^{p^r} x^{p^r} + \cdots + f_L^{p^r} x^{p^r \cdot L}$$

proof: By induction.

$L=1$: $(f_0 + f_1 x)^{p^r}$

$$= \sum_{k=0}^{p^r} \binom{p^r}{k} \cdot f_0^{k} \cdot (f_1 x)^{p^r - k}$$

$$= f_0^{p^r} + f_1^{p^r} x^{p^r} + \sum_{k=1}^{p^r-1} \binom{p^r}{k} \cdot f_0^{k} \cdot (f_1 x)^{p^r-k}$$

Observation #1: $p \mid \binom{p^r}{l}$ is true for all r

<u>for all $l = 1, \ldots p^r - 1$</u>

$\boxed{\text{pf: } p \text{ is a prime}}$

$$\Rightarrow \quad p \mid \binom{p^r}{l}$$

<u>Observation #2:</u> $\binom{p^r}{k}$ is not an element in $GF(p^m)$, instead it is shorthand for counting how

is shorthand for counting how many "terms" in the summation.

$$\binom{p^r}{k} f_0^k (f_1 x^1)^{p^r-k}$$

$$= \sum_{l=1}^{\binom{p^r}{k}} f_0^k \cdot (f_1 x^1)^{p^r-k}$$

$$= \sum_{l=1}^{\binom{p^r}{k}/p} \cdot \sum_{l'=1}^{p} f_0^k \cdot (f_1 x^1)^{p^r-k}$$

$$= \sum_{l=1}^{\binom{p^r}{k}/p} 0 = 0.$$

$$\Rightarrow (f_0 + f_1 x^1)^{p^r} = f_0^{p^r} + (f_1 x^1)^{p^r}$$

For $L \geq 2$.

$$(f_{L-1}(x) + f_L \cdot x^L)^{p^r}$$

$\big\downarrow$ By the same two observations

$$= (f_{L-1}(x))^{p^r} + (f_L \cdot x^L)^{p^r}$$

$$= \sum_{\ell=0}^{L} \left(f_\ell x^\ell\right)^{p^r} = \left(\sum_{\ell=0}^{L} f_\ell x^\ell\right)^{p^r}$$

#