* Suppose we generate $GF(p^m)$ by an irreducible $g(x) \in F_p[x]$. of deg m

For any <u>primitive</u> $f(x) \in F_p[x]$. of m

Since $f(x) = a_0 + a_1 x^1 + \cdots a_{m-1} x^{m-1} + x^m$

(primitive $\Rightarrow$ irreducible $\Rightarrow$ monic)

and all coefficients are in $GF(p)$.

We can view the $\{0, 1, \cdots, p-1\}$ as a subset/subfield of the $GF(p^m)$, see representation #1.

$\Rightarrow$ We can also view $f(x) \in F_{p^m}[x]$

Namely, all coefficients are now treated as an element in $GF(p^m)$ generated by $g(x) \in F_p[x]$

and all the $+$ and $\cdot$ operations

are treated as the $+, \bullet$ operations in $GF(p^m)$ generated by $g(x) \in F_p[x]$

---

* Theorem: Once we view the primitive $f(x) \in F_p[x]$ as a polynomial in $F_{p^m}[x]$, $f(x)$ is no longer irreducible (thus not primitive).

In fact, $f(x)$ can now be written as $f(x) = \prod_{i=1}^{m} (x - \beta_i)$

where $\beta_i \in GF(p^m)$ generated by $g(x)$ for all i

and all the "$+$", "$\bullet$" are defined over the $GF(p^m)$ generated by $g(x)$

* Theorem: For any primitive polynomial

* Theorem: For any primitive polynomial $f(x) \in F_p[x]$, of degree m,

the roots $\{\beta_i \in GF(p^m) ; i=1, \cdots, m\}$

are ① distinct and ② each of them is primitive element of $GF(p^m)$.

(regardless how we choose the irregular $g(x)$ to generate $GF(p^m)$)

proof: See textbook.

---

* Let β be any root $\in GF(p^m)$ a primitive polynomial $f(x) \in F_p[x]$

$\Rightarrow$ β is a primitive element of $GF(p^m)$

$$\Rightarrow GF(p^m) = \{0, 1, \beta^1, \beta^2, \cdots, \beta^{p^m-2}\}$$

* We now build the relationship between $GF(p^m)$ and the <u>primitive polynomial</u> $f(x) \in F_p[x]$.

* Since $f(x)$ is <u>monic</u>, and β is a root $\in GF(p^m)$

$$\Rightarrow \quad f(\beta) = \beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0 = 0.$$

$$\beta^l = x^l \Big|_{x=\beta} = Q_l(x) \cdot f(x) + R_l(x) \Big|_{x=\beta}$$

$\Rightarrow$ where $Q_l(x)$ and $R_l(x)$ are the quotient and remainder polynomials of x^l

$$= Q_l(\beta) f(\beta) + R_l(\beta) = R_l(\beta)$$

$$= x^l \bmod f(x) \Big|_{\beta}$$

E.g. $\quad f(x) = x^3 + x + 1 \in GF(2)[x].$

E.g. $f(x) = x^3 + x + 1 \in GF(2)[x]$.

$$\beta^5 = x^5 \bmod f(x) \Big|_{x=\beta}$$

$$= x^2 + x + 1 \Big|_{x=\beta} = \beta^2 + \beta + 1$$

If we just ignore $\beta \Longleftrightarrow x$ relabeling.

$$GF(p^m) = \{0\} \cup \{\beta^l : l = 0, \cdots, p^m - 2\}$$

$$= \{0\} \cup \{\beta^l \bmod f(\beta) : l = 0, \cdots, p^m - 2\}$$

$$= \{0\} \cup \{x^l \bmod f(x) : l = 0, \cdots, p^m - 2\}$$

Comparison: Representation #1.

$$GF(p^m) = \{a(x) \bmod g(x) : \forall a(x) \in F_p[x]\}$$

For a lot of discussion, we simply use a primitive polynomial $f(x)$ to generate $GF(p^m)$.

generate $GF(p^m)$.

NOT just an irreducible $g(x)$ to generate $GF(p^m)$

$$= \{ a(x) \bmod f(x) : \forall a(x) \in F_p[x] \}$$

Our discussion thus strengthen ↑ by

$$= \{ a(x) \bmod f(x) : a(x) = 0 \text{ or } x^l \text{ for } l = 0, \ldots, p^m - 2 \}$$

---

* In other words, "x" is a primitive element

$$ord(\text{"}x\text{"}) = ord(p) = p^m - 1$$

* $f(x) \in GF(p)[x]$ & $deg(f(x)) = m$ is a primitive polynomial iff "x" is a primitive element in the $GF(p^m)$ generated by $f(x)$

* Thus far, we discussed how to create $GF(p^m)$ from $GF(p)$ where p is a prime number

i.e. ① We find an irreducible $f(x) \in \mathbb{F}_p[x]$ and use the modulo operations in polynomial

② If $f(x)$ is also primitive, then "x" is a <u>primitive</u> element that generates the entire $GF(p^m) \setminus \{0\}$.

* This implies that $GF(p)$ is a subfield of $GF(p^m)$. Or equivalently $GF(p^m)$ is an extension field of $GF(p)$

* The same construction can be used to generate $GF(p^{m_1 \cdot m_2})$ from $GF(p^{m_1})$

i.e. find an irreducible $f(x) \in GF(p^{m_1})[x]$ and use modulo operations.

* $\Rightarrow GF(p^{m_1})$ is a sub-field of $GF(p^{m_2})$ iff $\frac{m_2}{m_1}$ is an integer.

* We call the "p" value as the <u>characteristic</u> of a field $GF(p^m)$

* Note that for any $1 \in GF(p^m)$

$$\sum_{k=1}^{p} 1 = 0$$

(Think of it as in the modulo p field.)