Note Title

Abstract: $F_{p^m} = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_i \in F_p\}$

Construction: $F_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} : a_i \in F_p\}$

$+$: poly addition

$\pi(\alpha)$: deg-m irreducible poly over F_p

$a(\alpha), b(\alpha) \in F_{p^m}$ $\quad \overbrace{a(\alpha) \times b(\alpha)}^{\text{in } F_{p^m}} = a(\alpha)\, b(\alpha) \bmod \pi(\alpha)$

Ex:

$$F_9 = \{\underbrace{0, 1, 2}_{\mathbb{Z}_3}, \alpha, 2\alpha, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$$

$$\pi(\alpha) = \alpha^2 + 1$$

$$(\alpha+1) \times (2\alpha+2) = 2\alpha^2 + \alpha + 2$$

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

$F^*_{p^m}$: $p^m - 1$ elements

$\beta \in F^*_{p^m}$. $\exists$ minimal r s.t

$\beta, \beta^2, \beta^3, \dots, \beta^r = 1$

M :

Multiplicative order of β:
minimal r s.t. $\beta^r = 1$

① $r \mid |F_{p^m}^*| = p^m - 1 \Rightarrow \beta^{p^m-1} = 1$

Subgroup generated by β: $\{\beta, \beta^2, \ldots, \beta^{r-1}, \beta^r = 1\}$
of $F_{p^m}^*$

② if $\beta^a = 1$, then $r \mid a$.

<u>Pf</u>: Divide a by r: $a = qr + q'$, $0 \le q' < r$

$$1 = \beta^{a} = \beta^{(qr+q')} = \beta^{qr} \cdot \beta^{q'} = \beta^{q'}$$

$$0 \le q' < r$$

$$\Downarrow$$

$$q' = 0 \quad \text{QED}$$

$$\operatorname{ord}(\beta^{2}) = ?$$

<u>Fact</u>: $\exists\ \beta \in F_{p^m}^*$ s.t. order$(\beta) = p^m - 1$.

$$F_{p^m} = \{0, \beta, \beta^2, \dots, \beta^{p^m-2}, 1\} \rightarrow \text{Useful for mult.}$$

$$F_{p^m} = \{a_1\alpha_1 + a_2\alpha_2 + \dots + a_m\alpha_m : a_i \in F_p\} \rightarrow \text{Useful for addition}$$

<u>Pf</u>: Pick $\beta \in F_{p^m}^*$ s.t. order$(\beta) = r \geq$ order(β')
$\forall\ \beta' \in F_{p^m}^*$

..

- $r \leq p^m - 1$ ✓

Claim: $\beta' \in F^*_{p^m}$ with $\text{order}(\beta') = r'$. Then, $r' | r$.

Pf: π : prime number that divides r

$$r = \pi^a r_1 \quad \underbrace{(r_1, \pi)}_{\text{gcd}} = 1$$

$$r' = \pi^b r_2 \quad (r_2, \pi) = 1$$

Claim': $b \leq a$

Pf: $\text{order}\left((\beta')^{r_2} (\beta)^{\pi^a}\right) = \pi^b r_1 \leq r = \pi^a r_1$

QED

$x^r - 1$: roots are all elements of $\mathbb{F}_{p^m}^*$

$\Rightarrow \quad r \geq p^m - 1$

QED

Primitive element of $\mathbb{F}_{p^m}$: $\beta \in \mathbb{F}_{p^m}$ s.t.

$\operatorname{order}(\beta) = p^m - 1$

Ex: $F_2 = \{0, \overset{*}{1}\}$ $F_3 = \{0, 1, \overset{*}{2}\}$

$F_5 = \{0, 1, \overset{*}{2}, \overset{*}{3}, 4\}$

$2, 2^2 = 4, 2^3 = 3, 2^4 = 1$

F_p : ways to find primitive element

$m=1$: base field

$m>1$: extension field

Ex: $F_4 = \{0, 1, \underset{*}{\alpha}, \underset{*}{1+\alpha}\}$ $\quad \alpha^2 = \alpha + 1$

mod 2 addition

$$F_9 = \{0, 1, 2, \alpha, 2\alpha, \overset{*}{\alpha+1}, \overset{*}{\alpha+2}, 2\alpha+1, 2\alpha+2\}$$

mod 3 addition, $\alpha^2 + 1 = 0$

$$(\alpha+1)^4 = 1 + 4\alpha + 4\alpha^3 + \alpha^4$$

$$= 2$$