Finite fields

Note Title

F : finite field

$|F| = p^m$, p : prime

In F, $\underset{\downarrow\ \text{characteristic}}{p} = \overbrace{1+1+\cdots+1}^{p\ \text{times}} = 0$

"Addition" F : m-D vector space over $\mathbb{Z}_p$

$\downarrow$ vector representation

$$F = \{0, 1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}.$$

primitive element

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

→ Roots of $x^{p^m-1} - 1$ in F are all <u>nonzero</u> elements of F.

$$x^{p^m-1} - 1 = (x-1)(x-\beta)\ldots(x-\beta^{p^m-2})$$

$$x^{p^m} - x = \prod_{\alpha \in F} (x - \alpha)$$

F : field $\quad p(x) \in F[x]$

$\downarrow$

$p(x)$: factors into irreducibles in a unique way over $G[x]$, G : extension of F.

Specific construction:

$\pi(x)$: deg-m, irreducible over $\mathbb{Z}_p$

$$\mathbb{F}_{p^m} = \{a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} : a_i \in \mathbb{Z}_p\}$$

$+$: mod p

$\times$: mod $\pi(x)$

Minimal polynomial

$\beta \in \underline{\underline{F}}$, finite field $|F| = p^m$

The minimal poly of β over $\mathbb{Z}_p$ is the monic least degree poly in $\mathbb{Z}_p[x]$ with β as a root.

$\longrightarrow$ makes sense because β is a root of

$$x^{p^m} - x \in \mathbb{Z}_p[x]$$

Notation: $M_\beta(x)$

<u>Properties</u>: (1) If $f(x) \in \mathbb{Z}_p[x]$ and $f(\beta) = 0$, then

$$M_\beta(x) \mid f(x)$$

Pf: Use division

(2) $\deg M_\beta(x) \leq m$

Pf: $1, \beta, \beta^2, \ldots, \beta^{m-1}, \beta^m \in F$ are lin. dep. over $\mathbb{Z}_p \Rightarrow \exists\, a_0, a_1, \ldots, a_m \in \mathbb{Z}_p$

s.t. $a_0 + a_1\beta + a_2\beta^2 + \cdots + a_m\beta^m = 0$ & ΣD

(3) $M_\beta(x)$:

$$M_\beta(\beta^p) = 0$$

<u>Pf:</u> $\rightarrow (x+y)^p = x^p + y^p$ for $x, y \in F$.

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdot \cdots i} = ap = 0$$ in F

$a_i \in \mathbb{Z}_p$ $\quad \rightarrow \overbrace{(a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m)}^{a(x)}{}^p$

$$= a_0^p + a_1^p x^p + a_2^p x^{2p} + \cdots + a_m^p x^{pm} = a(x^p)$$

$a(x) \in \mathbb{Z}_p[x]$ $\quad (a(x))^p = a(x^p) \longrightarrow$ set $a(x) = M_\beta(x)$

$$(M_\beta(x))^p = M_\beta(x^p)$$

$$\vdots$$

$$\downarrow$$

$$(a(x))^{p^i} = a(x^{p^i})$$

put $x = \beta$

$$M_\beta(\beta^p) = 0$$

<u>More generally</u>,

$$a(x) \in \mathbb{Z}_p[x]$$

if $\alpha \in F$ is a root of $a(x)$, then

$\ldots, \alpha^{p^2}, \alpha^p$ is also a root.

Conjugates: $\alpha \in F$

$\alpha^p, \alpha^{p^2}, \ldots$ are conjugates of

α over $\mathbb{Z}_p$