Combinatorics

29/9/21.

Lecture 4. Factoring $x^n - 1$ over $GF(p^r)$.

Review :- Galois Theory.

Algebraic field extensions.

$F \subset E$ two fields. $\{\theta : E \to E \mid \theta$ is field auto. & $\theta(\alpha) = \alpha \ \forall \alpha \in F\}$

$\mathrm{Perm}(E) \supset Gal(E/F) \to$ group

If extension is normal & separable, then this group "describes" the field extension very well.

$\{F \subset K \subset E \mid K$ a field$\} \longleftrightarrow \{e \subseteq H \subseteq G \mid H$ a subgroup$\}$

$\downarrow$ field theory $\qquad\qquad \downarrow$ group theory

$K \longmapsto Gal(K/F)$

the fixed field of H $= E^H = \{\alpha \mid \theta(\alpha) = \alpha \ \forall \theta \in H\} \longleftarrow H$

E^H is normal & separable. $\longleftrightarrow$ H is normal

$|Gal(E/F)| = [E:F]$.

$\boxed{\text{In general } |Gal(E/F)| \leq [E:F]}$

---×---×---×---

Apply this to finite fields.

Thm: $\forall$ p-prime, $r \in \mathbb{N}$, $\exists!$ $GF(p^r)$.

& $GF(p^r) \subset GF(p^s)$ iff $r \mid s$.

Frobenius map: $\alpha \to \alpha^p$. $\quad \alpha^{p-1} \equiv 1 \pmod p$ in $\mathbb{Z}$.

$\Rightarrow$ Fixed field

$(\alpha+\beta)^p = \alpha^p + \beta^p$

$(\alpha\beta)^p = \alpha^p \beta^p$

$\Rightarrow$ Frobenius is a field homo. of $GF(p^r)$ whose fixed field contains $\mathbb{Z}/p\mathbb{Z}$

Since $X^p = X$ has at most p roots, the fixed field of the Frobenius is precisely $GF(p) = \mathbb{Z}/p\mathbb{Z}$.

$\Rightarrow \quad \text{Frob} \in \text{Gal}(GF(p^r)/GF(p))$.

We know that every $x \in GF(p^r)$ satisfies $\boxed{X^{p^r} = X}$.

$$(\text{Frob})^2(x) = (\text{Frob}(\text{Frob}))(x) = \text{Frob}(x^p) = x^{p^2}.$$

$$\vdots$$

$$(\text{Frob})^s(x) = x^{p^s} \quad \forall s.$$

$\Rightarrow$ the order of Frob in $\text{Gal}(GF(p^r)/GF(p)) = r$.

$$= [GF(p^r) : GF(p)].$$

$\therefore$ $GF(p^r)/GF(p)$ is Galois & its Galois group is cyclic, a gen. given by Frob.

—— x —— x —— x ——

$$\text{Gal}(\overline{GF(p)}/GF(p)) \ni \text{Frob}$$

$$\overline{GF(p)} \circlearrowleft \text{Frob}$$

$$GF(p^r) \circlearrowleft \text{Frob}$$

$$GF(p) \qquad x \mapsto x^p$$

$GF(p^r)$ — r — $GF(p)$ — p.

$\text{Gal}(GF(p^r)/GF(p)) \subset S_{p^r}$.

—— x —— x —— x ——

Q. Factor $X^{p^r} - X$ (or $\underline{\underline{X^{p^r-1} - 1}}$) over $GF(p)$.

__Idea.__ Its splitting field is $GF(p^r)$; $GF(p^r)^*$ is cyclic, say generated by α.

$\therefore$ If $X^{p^r} - X = f_1 \cdot f_2 \cdots f_\ell \qquad f_i \in GF(p)[X]$ irr.

$$f_1 = (X - \alpha_{1,1})(X - \alpha_{2,1}) \cdots (X - \alpha_{k_1,1})$$

$$= (X - \alpha^{i_1})(X - \alpha^{i_2}) \cdots (X - \alpha^{i_{k_1}})$$

$$= X^{k_1} - \underline{\underline{\left(\sum_{t=1}^{k_1} \alpha^{i_t}\right)}} X^{k_1 - 1} + \cdots + (-1)^{k_1}\left(\prod \alpha^{i_1}\alpha^{i_2}\cdots\alpha^{i_{k_1}}\right)$$

$$\prod \alpha^{i_t} = \alpha^{\sum i_t}$$

$$\Uparrow$$

$$GF(p)[X].$$

$x_1, x_2, \ldots, x_n$

$x_1, x_2, \ldots, x_n$.

$\sum_{i<j} x_i x_j$, $\sum_{i<j<k} x_i x_j x_k$

$\Rightarrow$ every coeff of f_i is invariant under Frobenius map.

$$\boxed{\mathrm{Frob}(f_1) = \prod_{t=1}^{k_1}(X - \mathrm{Frob}(\alpha^{i_t}))}$$

$\theta : F \to F$. field homo.

$\Downarrow$

$\theta : F[X] \to F[X]$

$\sum a_i x^i \mapsto \sum \theta(a_i) x^i$

$\Downarrow$

$\Rightarrow$ α^{i_j} is a root of f_1 then so is $\alpha^{p i_1}$.

order ~~powers~~ so that $i_1 \lneq i_2 < \cdots < i_t$

look at $\alpha^{i_1}, \alpha^{p i_1}, \ldots \alpha^{p^r i_1}$ with $(\alpha^{i_1})^{p^{r+1}} = \alpha^{i_1}$

$o(\alpha) = p^r - 1$

$o(\alpha^{i_1}) \mid o(\alpha)$ & $\therefore$ is coprime to p. $\Rightarrow \exists\, r$ s.t. $p^{r+1} \equiv 1 \mod n$.

$\overset{\parallel}{n}$ $g_1 = (X - \alpha^{i_1})(X - \alpha^{p i_1}) \cdots (X - \alpha^{p^r i_1})$ invariant under Frob.

$\cap$

$GF(p)[X]$. $\Rightarrow g_1 = f_1$. Ily we can find all roots f_i $\forall$ $1 \le i \le l$.

---x---x---x---

<u>Algorithm</u> Start with any number i from 0 to $p^r - 1$.

$\downarrow$

α^i α - gen. of $GF(p^r)^*$

what is the order α^i in $\mathbb{Z}/p^r - 1 = \langle \alpha \rangle$.

$$= \frac{p^r - 1}{(i, p^r - 1)} = n.$$

Let s be the first integer s.t. $p^{s+1} \equiv 1 \pmod n$

$(\alpha^i, \alpha^{pi}, \alpha^{p^2 i}, \ldots \alpha^{p^s i})$ are all the roots of the irr. poly of α^i in $GF(p^r)$.

To factor $x^{p^r - 1} - 1$ we partition the set $\{0, 1, \ldots, p^r - 1\}$ as $(i, pi, p^2 i, \ldots, p^s i)$ s.t. $p^{s+1} \equiv 1 \mod \left(\frac{p^r - 1}{(i, p^r - 1)}\right)$

$\hookrightarrow$ reduce mod $(p^r - 1)$

Explicit computation over $GF(16)$ $p = 2$, $r = 4$.

<u>ex. 1</u> $S = \{0, 1, \ldots, 15\}$

$S = \{0\} \sqcup \{1,2,4,8\} \sqcup \{7,14,13,11\} \sqcup \{3,6,12,9\}$
$(x+1)$ α^7 $\sqcup \{5,10\}.$

$\Rightarrow$ $\boxed{x^{15}-1}$ is a product of 1 poly of deg 1
3 poly of deg 4
1 poly of deg 2.

ex.2 $\boxed{x^{63}-1}$ $\{0,1,\dots,63\}$

over $GF(2) = \mathbb{Z}/2\mathbb{Z}$

is a product of nine irr. poly of deg 6
two poly of deg 3
one poly of deg 2
& one poly of deg 1

Def^n :- A cyclotomic coset is a subset of $\{0,1,\dots,p^r-1\}$ such that it is generated by its least element in the following way $\{s, ps, p^2s, \dots, p^ts\}$ with $p^{t+1} \equiv 1 \left(\text{mod } \frac{p^r-1}{(s,p^r-1)}\right)$

$1\left(\text{mod } \frac{p^r-1}{(s,p^r-1)}\right)$

——— x ——— x ——— x ———

Q. What happens when we want to factor x^n-1 for $n \neq p^r-1$ for some r.

Assume that $(n,p)=1$. $\Rightarrow \exists\, r$ s.t. $p^{r+1} \equiv 1 \pmod n$

$$\Rightarrow n \mid p^{r+1}-1.$$

$$\Rightarrow (x^n-1) \mid (x^{p^{r+1}-1}-1)$$

Same technique can be applied. (Exercise - Find out how).

—— x —— x —— x ——