Combinatorics

Lecture 2

- Finite fields exists.
- For any number p^r, $\exists!$ field of that order. $GF(p^r)$ or $\mathbb{F}_{p^r}$.
- $GF(p^r) \subset GF(p^s)$ iff $r \mid s$.

- Every element of $GF(p^r)$ satisfies the polynomial $X^{p^r} - X$, defined over $GF(p) = \mathbb{Z}/p\mathbb{Z}$.

$p=2$ is very interesting because the field elements are $\{0,1\}$ & hence can easily be applied in practice.

$p=2$ is usually problematic case in abstract maths, since $2=0$ in this case.

eg. • $A = \underbrace{\frac{A^t + A}{2}}_{\text{symmetric}} + \underbrace{\frac{A - A^t}{2}}_{\text{anti-symmetric}}$ $\qquad A^t = -A$

• $\langle x, y\rangle$ is given then we know that

$$\langle x+y, x+y\rangle = \langle x, x\rangle + \langle y, y\rangle + 2\langle x, y\rangle$$

$$\therefore \underset{\text{symmetric}}{\langle x, y\rangle} = \frac{\langle x+y, x+y\rangle - \langle x,x\rangle - \langle y,y\rangle}{2}$$

$\rightarrow$ $\therefore$ Any bilinear form $\langle x, y\rangle$ can be uniquely determined

$f : V \times V \to F$ $\qquad f(\alpha x + \beta y, w) = \alpha f(x,w) + \beta f(y,w)$.

$f((x,y)) = f((y,x))$ — symmetry.

$\langle \underset{\to}{x}, \underset{\to}{y}\rangle \mapsto \sum x_i y_i$.

$$Q : V \to \mathbb{R}.$$

$$Q(v) = \langle v, v\rangle.$$

$$= \sum_{i=1}^{n} v_i^2$$

If $F \subset K$ two fields & if $\alpha \in K$, α is called algebraic if it satisfies monic polynomial in $F[x]$.

If $\dim_F K < \infty$ then $\forall \alpha \in K$, look at $1, \alpha, \alpha^2, \ldots$
there has to be an eq^n of the type

$$\sum_{i=0}^{N} a_i \alpha^i = 0 \quad \text{with } a_i \in F.$$

$\Rightarrow$ α is a root of $\sum_{i=0}^{N} a_i x^i \in F[x]$.

$\Rightarrow$ α is algebraic. $\Rightarrow$ K/F is algebraic.

$\Rightarrow$ $GF(p^r) \subset GF(p^s)$ is always an algebraic ext^n

In particular $GF(p^r)$ is algebraic & hence any element $\beta \in GF(p^r)$ must satisfy a monic irreducible poly over $GF(p)$. say of deg. t.

If $\alpha \in K$ satisfies a monic irr. poly of deg l over F then $[F(\alpha) : F] = l$.
↳ deg. of field ext^n.

In finite field case, $\exists!$ field $GF(p^l)$ having deg. l over $GF(p)$.

Thm:- The polynomial $x^{p^r} - x$ factors over $GF(p)$ as the product of <u>all</u> irr. polynomials of degree s with $s \mid r$.

Pf.

$$\begin{array}{c} GF(p^r) \\ \Big| \;\} r \\ GF(p) \end{array}$$

take $f \in GF(p)[x]$ of deg. s with $s \mid r$.

$f(\beta) = 0 \Rightarrow [GF(p)[\beta] : GF(p)] = s$

$GF(p^s) \subset GF(p^r)$.
$\ni \beta \Rightarrow \beta^{p^r} - \beta = 0$.

$\Rightarrow f \mid x^{p^r} - x$.

Converse is also true.

$a^i \| b$
$\Rightarrow a^i \mid b$
& $a^{i+1} \nmid b$.

$\longrightarrow$ If F is a field then $F[x]$ is like $\mathbb{Z}$.

irr. poly $\sim$ primes in $\mathbb{Z}$.

- It is a very important fact that given a very large number, it is very difficult to find its prime factors
  ↳ in terms of time.

N - $\underbrace{1, 2, 3, \cdots, \sqrt{N}}$, ...

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

<u>Theorem</u> :- If $f(x) \in GF(p^r)[x]$ then $f(x^{p^r}) = (f(x))^{p^r}$.

$\sum a_i x^i \rightsquigarrow \sum a_i x^{ip^r}$ (Frobenius map)

<u>Pf</u>: Let $f(x) = ax^i$ then what is $(f(x))^{p^r} = a^{p^r} \cdot x^{ip^r}$

$= a x^{ip^r}$

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

$= f(x^{p^r})$.

If $f = ax^i + bx^j$ then $f^{p^r} = (ax^i + bx^j)^{p^r}$

$\binom{p^r}{i}$ is divisible by p $\forall\, 0 < i < p^r$

$= a^{p^r} x^{p^r i} + b^{p^r} x^{p^r j}$

$= a x^{ip^r} + b x^{jp^r}$

$= f(x^{p^r})$.

<u>Cor.</u> If $f(\alpha) = 0$ $\alpha \in GF(p^r)$ $f \in GF(p)[x]$

then $f(\alpha^p) = 0$, $f(\alpha^{p^2}) = 0$, ..., $f(\alpha^{p^i}) = 0$, ...

since $f(\alpha^{p^i}) = (f(\alpha))^{p^i} = 0$

<u>Thm</u>: Let $f \in GF(p)[x]$. $\underset{\neq 0}{\alpha} \in GF(p^r)$; $o(\alpha)$ in $GF(p^r)^*$ be n for some n $n \mid p^r - 1$.

s.t. $f(\alpha) = 0$. $\Rightarrow (n, p) = 1$.

(since $(n,p)=1$, p invertible element in $\mathbb{Z}/n\mathbb{Z} \Rightarrow p^{r+1}=1 \pmod n$ for some r.
$\overset{\shortparallel}{O(\alpha)}$ $\quad r = O(p)$ in $\mathbb{Z}/n\mathbb{Z}^*$)

then $\overset{\alpha^{p^{r+1}}}{\overset{\shortparallel}{\alpha}}, \alpha^{p}, \alpha^{p^2}, \ldots \alpha^{p^r}$ are all <u>distinct</u> roots of $f(x)$.

$\alpha^n = 1$ & $p^{r+1} \equiv 1 \pmod n \Rightarrow \alpha^{p^{r+1}} = \alpha^{kn+1} = \alpha$.

<u>pf.</u> By cor. above, we know that α^{p^k} is a root $\forall k$

If $\alpha^{p^i} = \alpha^{p^j} = \alpha^{p^i - p^j} = 1$.

$\Rightarrow \quad n \mid p^i - p^j \Rightarrow p^i \equiv p^j \pmod n$

$\Rightarrow p^{i-j} \equiv 1 \pmod n$.

$\Rightarrow r+1 \mid i-j$ can not happen!

QED.

$\Rightarrow \quad f(x) = \prod_{i=1}^{r} (x - \alpha^{p^i}) \cdot g$ if $O(p)$ in $\mathbb{Z}/n\mathbb{Z}^*$ is $r+1$.

$\Rightarrow$ If f is monic & irreducible then $g \equiv 1$.

& $f = \prod_{i=1}^{r} (x - \alpha^{p^i})$. This is the monic irr. polynomial satisfied by α.

---

(1). Start with $\underset{\ne 0}{\alpha}$ is $GF(p^r)$ (2) Let $O(\alpha) = n$ in $GF(p^r)^*$.

(3) Let $r+1$ be s.t. $p^{r+1} = 1 \pmod n$ & it is the least such.

(let $O(p) = r+1$ in $(\mathbb{Z}/n\mathbb{Z})^*$)

4. Then the irr. poly satisfied by α over $GF(p)$ is

$$\prod_{i=1}^{r} (x - \alpha^{p^i}).$$

<u>$x^{p^n} - x$.</u>

example :- $p=2$. $r=4$. $GF(16)$.

α s.t. $O(\alpha) = 15 = 2^4-1$ a generator of $GF(16)^*$.

$$p^{r+1} \equiv 1 \pmod n).$$

$$\overset{p^1}{2}, \overset{p^2}{4}, \overset{p^3}{8}, 16.$$

$(X-\alpha)(X-\alpha^p)(X-\alpha^{p^2})(X-\alpha^{p^3})$ is the irr. poly of α.

GF(16). Fact. • X^4+X^3+1 is irr. over $GF(2) = \{0,1\}$

(can not have linear factor)

aX^2+bX+C. $\cancel{a}=1, b, c \in \{0,1\}$.

X^2+X+1

$\underline{X^2+X}$, X^2+1, X^2.

$x(x+1)$ $(x+1)(x-1)$,

$X^4+X^3+1 \neq (X^2+X+1)^2 = X^4+X^2+1$ since squaring is a Frobenius map

$GF(16)^* = GF(16) - \{0\}$

$\alpha^4+\alpha^3+1 = 0 \Rightarrow \langle\alpha\rangle = GF(16)^*$

$\alpha, \alpha^2, \alpha^4, \alpha^8$ roots of irr. poly of α.

$(1, 2, 4, 8)$

every $\overset{\neq 0}{\beta} \in GF(16)$,

$\beta = \alpha^i$ for some $i \Rightarrow O(\beta) =$

$\langle x \rangle$.

$o(x^i) = ?$

$\frac{o(x)}{(o(x), i)}$

$\longrightarrow$ $GF(16)^* = \{1, \alpha, \alpha^2, \cdots \underset{\beta}{\alpha^i} \cdots \alpha^{14}\}$

$$(\underset{\alpha^i}{X-\beta})(X-\underset{\alpha^{ip}}{\beta^p}) \cdots (X-\underset{\alpha^{ip^r}}{\beta^{p^r}})$$

$\{0,1,2,\ldots,14\} = \bigsqcup S_i$ s.t. $\prod_{i=S_i} X-\alpha^i$ is irr. over $GF(2)$.