Group Theory

Lecture 4

Cyclic group: A gp H is cyclic if H can be gen by a single elt i.e $\exists$ some $x \in H$ s.t $H = \{x^n \mid n \in \mathbb{Z}\}$

$H = \{nx \mid n \in \mathbb{Z}\}$.

Example (1) $\mathbb{Z}$ is a cyclic gp.

(2) $\mathbb{Z}/n\mathbb{Z}$ is also cyclic gp.

$\mathbb{Z}$ is gen by 1. ie $\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\}$

$= \{n(-1) \mid n \in \mathbb{Z}\}$

$$n \cdot a = \underbrace{a + a + \cdots a}_{n\text{-times}}$$

$$-n \cdot a = \underbrace{-a + (-a) + \cdots + (-a)}_{n\text{-times}}$$

We observed that every subgp of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ which is also a cyclic gp.

Q Is every subgp of a cyclic gp is cyclic?

Thm. Let $H = \langle x \rangle$ be a cyclic gp.

(1) Every subgp K of H is either (1) or $\langle x^d \rangle$ where d is the smallest (+)ve power of x in K.

(2) If $|H| = n$ then For every divisor d of n $\exists$ unique subgp of H of order d and this subgp is the cyclic gp $\langle x^{n/d} \rangle$.

Pf: (1). Let $K \neq (1)$ be a subgp of H.

Consider $P = \{n \geq 1 \mid x^n \in K\}$.

By well ordering principal P has

a smallest +ve int d.

Claim $K = \langle x^d \rangle$

Note $\langle x^d \rangle \subseteq K$.

Let $x^b \in K$. Then by division algorithm $b = dq + r$ where $0 \leq r < d$.

$\Rightarrow r = b - dq$

$\therefore x^r = x^{b-dq} = x^b \cdot (x^{-d})^q$

$\in K$,

$\because r < d$ therefore $r = 0$.

$\therefore x^b = x^{dq} \in \langle x^d \rangle$.

$\therefore K = \langle x^d \rangle$.

(2) $\because |H| = n \qquad o(x) = n$

Let $n = dd'$. Now consider $\langle x^{d'} \rangle$.

WTS $o(x^{d'}) = d$. $\qquad \langle x^{d'} \rangle = H$

Let $o(x^{d'}) = m$.

$\therefore x^{d'm} = 1$.

But $|x| = n$.

$\Rightarrow n \mid d'm \Rightarrow dd' \mid d'm$

$\Rightarrow d \mid m. \Rightarrow d = m.$

$\therefore o(x^{d'}) = d.$

WTS uniqueness.

Let H' be another subgp of order d.

$\because H'$ is cyclic $\therefore H' = \langle x^l \rangle$

$\therefore x^{ld} = 1.$

$\because o(x) = n$

$\Rightarrow n \mid ld \Rightarrow dd' \mid ld \Rightarrow d' \mid l.$

$i.e\ l = d'e'.$

$\therefore x^l = (x^{d'})^{e'} \in \langle x^{d'} \rangle = H''$

$\therefore H' \subseteq H'' \quad \therefore H' = H''.$

$i.e\ \langle x^{d'} \rangle = \langle x^l \rangle.$

Cor Let $H = \langle x \rangle$ s.t $|H| = n$.

Then $H = \langle x^a \rangle$ iff $\gcd(a, n) = 1$.

In particular, the number of gens of H is $\varphi(n)$ [where φ is Euler's φ fn.].

Remark $H = \langle x \rangle$ and $|H| = n$.

$H = \{1, x, x^2, \ldots, x^{n-1}\}$.

$x^n = 1$

$x^{n-1} = x^{-1}$

$\varphi(n)$ = # of elts $< n$ which are coprime to n.

$\varphi(p) = p - 1$

Recall S_n - Symmetric group.

Defn. The permutation $(a_1\ a_2 \cdots a_k)$ where $a_i \in [n]$ are distinct is called a k-cycle.

In S_3 - (123) is a 3-cycle.

(12) is a 2-cycle.

A two cycle is called a transposition.

Ex. Every permutation is a product of disjoint cycle. Disjoint cycles commutes with each other.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} \in S_6.$$

$$\sigma = (1\ 5)(2\ 4\ 6)$$

Remark For any $\sigma \in S_n$ the cycle decomposition of σ^{-1} is obtained by writing the number of each cycle of the cycle decomposition of σ in the reverse order.

For example $\sigma^{-1} = (5\ 1)(6\ 4\ 2)$.

Ex 1. $S_n = \langle \text{transpositions} \rangle$.

Hint! Prove that every k-cycle is a product of transpositions.

Ex2. If σ is a k-cycle then show that $o(\sigma) = k$.
and if π is a product of disjoint cycles of lengths $k_1, \ldots, k_n$ then find $o(\pi)$.