Group Theory

Lecture 3

Defn: The order of a group is defined as the number of elements in the group and it is denoted by

$|G| :=$ order of the gp G.

$|S_3| = 6$ $\quad$ $|D_4| = 8$

$|S_n| = n!$ $\quad$ $|\mathbb{R}| = \infty$

$|\mathbb{Z}| = \infty$ $\quad$ $|\mathbb{Z}/n\mathbb{Z}| = n$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

↳ In $\mathbb{Z}$, $a \equiv b \pmod n$ (equivalence relation)

if $n \mid a-b$

$\bar{0} = \{0, n, 2n, 3n, \ldots\}$.

$\bar{1} = \{1, n+1, 2n+1, 3n+1, \ldots\}$.

In $\mathbb{Z}/n\mathbb{Z}$, $\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{ab}$

$\mathbb{Z}/n\mathbb{Z}$ forms a group wrt '+' but it doesn't forms a group wrt multiplication.

$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

$\bar{2}$ doesn't have any multiplicative inverse in $\mathbb{Z}/6\mathbb{Z}$. Thus $\mathbb{Z}/6\mathbb{Z}$ doesn't form a group wrt multiplication.

$\bar{4} \cdot \bar{2} = \bar{2}$

$\bar{4} \cdot \bar{3} = \bar{0}$

$\bar{4} \cdot \bar{5} = \bar{2}$

$\bar{4} \cdot \bar{1} = \bar{4}$

$\bar{4} \cdot \bar{4} = \bar{4}$

But $\bar{5} \cdot \bar{5} = \bar{1}$

Q If you consider the non-zero elts of $(\mathbb{Z}/n\mathbb{Z})^\times$ who have multiplicative inverse then does it form a group wrt multiplication.

Defn. Let G be a group and $g \in G$. If there exists no integer $n \in \mathbb{Z}$ s.t $g^n = 1_G$ we say that g has infinite order.

If $\exists n$ s.t $g^n = 1_G$ then we say g is of finite order

$o(g)$ = order of g

$= \min\{i \mid g^i = 1_G\}$

Remark. If G is written additively i.e the operation is denoted by '+' then the identity is denoted by '0'

If G is written multiplicatively i.e the operation is denoted by '.' then the identity is denoted by '1'

Example. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \bar{5}\}$.

$\mathbb{Z}/6\mathbb{Z}$ is gp wrt $+$ and identity $\bar{0}$.

$\bar{2}+\bar{2} = \bar{4}$,

$\bar{2}+\bar{2}+\bar{2} = \bar{0}$

$\bar{3}+\bar{3} = \bar{0}$

$o(\bar{4}) = 3$ ✓

$o(\bar{2}) = 3$

$o(\bar{3}) = 2$.

$o(\bar{1}) = 6$

$o(\bar{5}) = 6$

$\bar{5} + \bar{5} = \bar{4}$

$\bar{5} + \bar{5} + \bar{5} = \bar{3}$

$\bar{5} + \bar{5} + \bar{5} + \bar{5} = \bar{2}$

$\bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \bar{1}$

what is the order of $\bar{5} + \bar{5} = \bar{4}$

Example In S_3

$o(1\,2\,3) = 3$

$o(1\,2) = 2$

Example In D_4

$o(1\,2\,3\,4) = 4$

Example. In $\mathbb{Z}$, $o(1)$ is infinite

Remark If G is a finite gp then order of every elt of G is finite.

Q Can we have an infinite gp s.t every elt of the gp has finite order?

Ans. Example Group of all roots of unity is an infinite gp with each elt having finite order.

Subgroup: A subset H of a gp G is called a subgroup if it has the following properties:

(1) if $a, b \in H$ then $a \cdot b \in H$

(2) $1 \in H$

(3) If $a \in H$ then $a^{-1} \in H$.

Examples: (1) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are subgps wrt '+'

(2) $\mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times$ are subgps wrt '.'

(3) $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$ subgp.

(4) $S^1 = \{z \in \mathbb{C} \mid |z| = 1\} \subseteq \mathbb{C}^\times$ is a subgp wrt '.'

(5) Consider the matrices

$$\mathcal{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathcal{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathcal{K} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H = \{\pm Id, \pm \mathcal{I}, \pm \mathcal{J}, \pm \mathcal{K}\} \subseteq GL_2(\mathbb{C})$$

Then H is a subgp called quaternion group.

(6) $D_4 \subseteq S_4$ is a subgp.

Q How does a subgp of $\mathbb{Z}$ look like?

Propn. Any subgp of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ where $m = 0, 1, 2, \ldots$

[Notation $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$]

Pf: Note that it is easy to see that $m\mathbb{Z}$ is a subgp of $\mathbb{Z}$.

WTS Any subgp of $\mathbb{Z}$ will be of the form $m\mathbb{Z}$.

Let H be any subgp of $\mathbb{Z}$ and b be the smallest +ve int $\in H$.

WTS $H = b\mathbb{Z}$.

Let $n \in H$ be any elt then by division algorithm

$$n = bq + r \text{ where } 0 \le r < b. \quad q \in \mathbb{Z}.$$

$\Rightarrow r = n - bq \in H$

$\Rightarrow r = 0$ as $0 \le r < b.$

Therefore $n = bq.$

$\therefore H = b\mathbb{Z}.$

Q1 Let G be a finite gp and $x, y \in G$ s.t $|x| = n$, $|y| = m$ then can you say about $|xy| = ?$

Q2. If $|x| = n$ then what will be order of $|x^a|$ where $a \in \mathbb{Z}$?

Propn Let G be a gp and $x \in G$.
If $x^m = 1$ and $x^n = 1$ then
$x^d = 1$ where $d = \gcd(m, n)$.
In particular if $x^m = 1$ for some
$m \in \mathbb{N}$ then $|x|$ divide m.

Pf: $\because d = \gcd(m, n) \Rightarrow \exists\ r, s \in \mathbb{Z}$
s.t $d = rm + sn$

$$x^d = x^{rm+sn} = (x^m)^r (x^n)^s$$
$$= 1$$

Let $|x| = n$ i.e n is the smallest +ive
int s.t $x^n = 1$.
then $x^d = 1$ where $d = \gcd(m, n)$
Since $|x| = n$ thus $d = n \Rightarrow \underline{n \mid m}$.

Propn Let G be a gp and let $x \in G$. If $|x| = n$ then $|x^a| = \frac{n}{\gcd(n,a)}$ where a is any int.

Pf: Let $\gcd(n,a) = d$ then $n = dd'$ and $a = d \cdot b'$ with $\gcd(b', d') = 1$.

Let $y = x^a$ WTS $|y| = d'$

$$y^{d'} = (x^a)^{d'} = x^{db' \cdot d'} = (x^n)^{b'} = 1.$$

$\Rightarrow |y| \mid d'$ [By previous propn]

Let $|y| = k$. Then $y^k = 1 = x^{ak}$.

$\Rightarrow n \mid ak$ [$\because |x| = n$]

$\Rightarrow d d' \mid d b' k$

$\Rightarrow d' \mid b' k$ $\quad \gcd(d', b') = 1$

$\Rightarrow d' \mid k.$

$\therefore d' = k.$ Hence $|x^a| = d'$.

Cyclic Group:

$\mathbb{Z} = \langle 1 \rangle$; $\mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle$ and $\langle \bar{5} \rangle$.

Let G be a gp, $x \in G$. G is called a cyclic gp if G can be gen by a single elt. i.e. $\exists$ some elt $x \in G$ s.t $G = \{x^n \mid n \in \mathbb{Z}\}$.

$x^{-n} = \underbrace{(x^{-1}) \cdots (x^{-1})}_{n\text{-times}}$.

$$\mathbb{Z} = \{ n \cdot 1 \mid n \in \mathbb{Z} \}.$$

$$\mathbb{Z}/n\mathbb{Z} = \{ n \cdot \bar{1} \mid n \in \mathbb{Z} \}.$$

$$= \{ n \cdot \bar{5} \mid n \in \mathbb{Z} \}.$$

Let G be a gp and $x \in G$.

Consider $H = \{ x^n \mid n \in \mathbb{Z} \}$

$$= \{ \ldots x^{-n} \ldots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots, x^n \ldots \} \subseteq G.$$

Then H is the smallest subgp containing x. H is called cyclic subgp gen by x.

If $x^m \neq x^n$ for $m \neq n$ then H is infinite. If $x^n = x^m$ for some $n > m$ then $x^{n-m} = 1$.

Let $r = \min\{ i \geq 0 \mid x^{2^0} = 1 \}$

Then the elts $1, x, x^2, \ldots, x^{r-1}$ are all distinct and $x^r = 1$ and $H = \{1, x, \ldots, x^{r-1}\}$ with $x^r = 1$ is called cyclic gp of order r.

Example. (1) In S_3.

$x = (123) \in S_3$.

$H = \langle x \rangle$

$= \{(1), x, x^2\}$

$= \{(1), (123), (132)\}$

In S_3 consider $y = (12)$

$H' = \langle (12) \rangle$

$= \{ (1), (12) \}$

(2) In $\mathbb{Z}/6\mathbb{Z} = G_2$.

$G_2 = \langle \bar{1} \rangle = \langle \bar{5} \rangle$

$H = \langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \}$

$H' = \langle \bar{3} \rangle = \{ \bar{0}, \bar{3} \}$

$H = \langle \bar{4} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \}$

(3) Consider $GL_2(\mathbb{R})$ and

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$H = \langle A \rangle$ is infinite cyclic gp of $GL_2(\mathbb{R})$

$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$