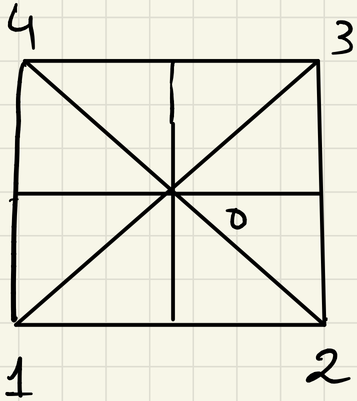
# Group Theory

Lecture 3

10/01/2022




(1) There are four rotations about the centre O through the angles $0°, 90°, 180°, 270°$

(2) The Two reflections along two diagonals and two reflections along horizontal & vertical bisector.

$$D_4 = \Big\{ (1), \overset{a}{(1\,2\,3\,4)}, \overset{a^2}{(1\,3)(2\,4)}, \overset{a^3}{(1\,4\,3\,2)}, \overset{b}{(2\,4)}, \underset{ba^2}{(1\,3)}, \underset{ba}{(1\,4)(2\,3)}, \underset{ba^3}{(1\,2)(3\,4)} \Big\}.$$

$$D_4 = \langle a, b \mid a^4 = (1), b^2 = (1), ab = ba^3 \rangle$$

# Dihedral Group:

A dihedral group is the gp of symmetries of a regular n-gon including both rotation & reflection. It is denoted by $D_n$ and has $2n$ elts among which there are $n$ rotations and $n$-reflections.

$$D_n = \langle a, b \mid a^n = 1,\ b^2 = 1,\ ba = a^{-1}b \rangle.$$

---

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

$a \equiv b \pmod{n}$. i.e $n \mid b-a$.

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

$\bar{0} = \{6n \mid n \in \mathbb{Z}\}$.

$\bar{1} = \{6n+1 \mid n \in \mathbb{Z}\}$.

$\mathbb{Z}/n\mathbb{Z}$ is a group wrt '+', with $\bar{0}$ as identity

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{4} + \bar{5} = \bar{3}.$$

Q Does $(\mathbb{Z}/6\mathbb{Z})^{\times}$ form a group wrt multiplication?

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

It is not a group wrt multiplication!

**Example** $\left(\mathbb{Z}/5\mathbb{Z}\right)^{\times}$ wrt $\cdot$

$$\left(\mathbb{Z}/5\mathbb{Z}\right)^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

what is the inverse of $\bar{4}$ $\quad \bar{4}\cdot\bar{4} = \bar{1}$

what is the inver of $\bar{2}$ $\quad \bar{2}\cdot\bar{3} = \bar{1}$

$\left(\mathbb{Z}/5\mathbb{Z}\right)^{\times}$ is group wrt multiplicatio.

**Ex.** Identify $n$ for which $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ forms a gp wrt multiplication.

**Defn** The order of a group is defined as the number of elts in the group.

**Example.** (1) $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are groups with infinite order

(2) $S_n$ is a gp of order $n!$

(3) $D_n$ is a gp of order $2n$

(4) $\mathbb{Z}/n\mathbb{Z}$ is a gp of order $n$.

**Defn.** Let $G$ be a gp and $g \in G$.

If $\nexists$ no integer in $\mathbb{Z}$ s.t $g^n = 1$ we say that $g$ has infinite order.

If $\exists\, n \in \mathbb{Z}$, s.t $g^n = 1$ then we say $g$ is of finite order and (denoted by $|g|$).

$$o(g) := \text{order of } g$$
$$:= \min \{ i \in \mathbb{N} \mid g^i = 1 \}.$$

Example (1) In $S_3$, $(1\,2\,3) \in S_3$.

we see that $o(1\,2\,3) = 3$.

$(1\,2) \in S_3$, then $o(1\,2) = 2$.

(2) $\mathbb{Z}/6\mathbb{Z}$, $o(\bar{2}) = 3$.

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

(3) $(\mathbb{Z}, +)$. $1 \in \mathbb{Z}$.

Here order of 1 is infinite.

Remark Let $G$ be a gp of finite order. Then all the elts of the gp should have finite order.

Q. Let $G$ be a group of infinite order. Is it true that every elt of $G$ will have infinite order?

Ans. Consider all the roots of unity is an infinite group but every elt has finite order.

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

(1) $1 \in H$

(2) If $a, b \in H$ then $ab \in H$

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

Equivalently if $H \neq \emptyset$ and $a, b \in H$ then $ab^{-1} \in H$.

Example (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 '$\cdot$'

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

(4) $D_n \subset S_n$ is a subgp.

Q. How does the subgps of $(\mathbb{Z}, +)$ looks like?