Lecture 13 & 14: 30/8/2022 & 1/09/2022

Note Title 9/2/2022

Ex: Let $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \,\middle|\, a \in \mathbb{R},\ a \neq 0 \right\}$.

Then, for $\begin{pmatrix} a & a \\ a & a \end{pmatrix}, \begin{pmatrix} b & b \\ b & b \end{pmatrix} \in G$, we have

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \cdot \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \in G \quad [\because ab \neq 0]$$

$\therefore$ G is closed under matrix multiplication.

$e = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity and if $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$,

then $A^{-1} = \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$.

Hence, G is a group.

Also, G is commutative. #

Note Title 9/2/2022

<u>The quaternion group Q_8:</u>

$$SL_2(\mathbb{C}) = \left\{ \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix} \,\middle|\, z_1, z_2, z_3, z_4 \in \mathbb{C} \text{ and } z_1 z_4 - z_2 z_3 = 1 \right\}.$$

Let
$$Q_8 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}$$

$$= \{ I, -I, A, -A, B, -B, C, -C \}, \text{ where}$$

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note Title 9/2/2022

We have $A^2 = B^2 = C^2 = -I$

$\therefore \; o(A) = o(B) = o(C) = 4 = o(-A) = o(-B) = o(-C)$.

Also, $AB = C = -BA$

$BC = A = -CB$

$CA = B = -AC$.

Q_8 is a subgroup of $SL_2(\mathbb{C})$, which is not commutative.

#

§ Orders of elements in a group:

Note Title — 9/2/2022

Let G be a group.

(1) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall\, a, b \in G$

(2) $o(a) = o(a^{-1}) \quad \forall\, a \in G$

(3) $o(x) = o(yxy^{-1}) \quad \forall\, x, y \in G$

(4) $o(a) = n$ and $a^m = e \Rightarrow n \mid m$.

Proof of (4): We write $m = n\cdot q + r$, where $0 \le r < n$.

Then, $a^m = e \Rightarrow a^{n\cdot q + r} = e \Rightarrow (a^n)^q \cdot a^r = e \Rightarrow a^r = e$

Since $o(a) = n$ and $0 \le r < n$, so $r = 0$. Hence, $m = n\cdot q$, that is, $n \mid m$.

Theorem 1: Let G be a group, and $a \in G$.

(1) If $o(a) = \infty$, then $o(a^k) = \infty \ \forall\ k \neq 0$.

(2) If $o(a)$ is finite, then for any $k \neq 0$, $o(a^k) = \dfrac{o(a)}{\gcd(o(a), k)}$.

Proof: (1) Easy.

(2) Since $o(a^k) = o(a^{-k})$, so it is enough to consider $k \geq 1$.

Let $o(a) = n$, $d = \gcd(n, k)$, $o(a^k) = m$.

Then, $n = dn_1$ and $k = dk_1$ with $\gcd(n_1, k_1) = 1$.

We need to prove that $m = \dfrac{n}{d}$.

We have $(a^k)^{n/d} = a^{kn/d} = (a^n)^{k/d} = e$

$\therefore \quad m = o(a^k)$ divides $\frac{n}{d}$. Thus, $m \mid \frac{n}{d} \quad \rightarrow (*)$

Next, we prove that $\frac{n}{d} \mid m$.

We have $(a^k)^m = e \Rightarrow a^{km} = e \Rightarrow o(a) = n \mid km$

$\Rightarrow dn_1 \mid dk_1 m \Rightarrow n_1 \mid k_1 m \Rightarrow n_1 \mid m \quad [\because \gcd(n_1, k_1) = 1]$.

But $n_1 = \frac{n}{d}$, and hence $\frac{n}{d} \mid m \longrightarrow (**)$

From $(*)$ and $(**)$, we have $m = \frac{n}{d}$.

$$\therefore \quad o(a^k) = \frac{o(a)}{\gcd(o(a), k)}.$$

#

§ Generators of cyclic groups.

(1) Let G be a finite group. Then, G is cyclic if and only if G has an element of order equal to $|G|$.

(2) Let G be a cyclic group of order n. Let 'a' be a generator. Then, $G = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$.

By Theorem 1, we have $o(a^k) = n \iff \gcd(n, k) = 1$.

Thus, the set of generators of $G = \{a^k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}$

Hence, a cyclic group of order n, there are $\varphi(n)$ number of generators.

(3) Generators of $(\mathbb{Z}_n, +)$:

We know that 1 is a generator of $(\mathbb{Z}_n, +)$.

$\therefore$ The set of generators $= \{ k \mid 1 \leq k \leq n, \gcd(n,k) = 1 \}$

$= U(n)$.

Ex: The generators of $(\mathbb{Z}_{10}, +)$ are $1, 3, 7, 9$.

Ex: $\mu_n = \{ \zeta_n^k \mid 1 \leq k \leq n \} = \{ \zeta_n^k \mid 0 \leq k < n \}$

where $\zeta_n = e^{2\pi i/n}$

A generator of μ_n is called a primitive n-th root of unity.

There are $\varphi(n)$ number of primitive nth root of unity.

Generators of infinite cyclic groups:

In $(\mathbb{Z}, +)$, the generators are 1 and -1.

- If G is an infinite cyclic group, then G has exactly two generators.

__Proof__: Let G be an infinite cyclic group, and let a be a generator of G. Then,

$$G = \langle a \rangle = \{ \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots \}.$$

Let 'b' be any other generator of G.

Then, $b = a^k$ and $a = b^m$ for some $k, m \in \mathbb{Z}$.

Now, $a = b^k = (a^m)^k \Rightarrow a^{mk-1} = e$

Since $o(a) = \infty$, so $mk - 1 = 0 \Rightarrow m = \pm 1,\ k = \pm 1$.

$\therefore\ b = a$ or $b = a^{-1}$.

This completes the proof.

—— x ——

§ Subgroups of cyclic groups:

<u>Theorem</u>: Let G be a cyclic group (finite or infinite). If H is a subgroup of G, then H is also cyclic.

<u>Proof</u>: Let $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$

If $H = \{e\}$, then H is cyclic.

So, let $\{e\} \subsetneq H \leq G$. Then, $\exists\, h \in H$ such that $h \neq e$.

$\therefore\ h = a^k$ for some $k \neq 0$.

Since $H \leq G$, so $h^{-1} \in H \Rightarrow a^{-k} \in H$.

Thus, $a^k, a^{-k} \in H$ for some $k \neq 0$. $\longrightarrow$ (*).

Let $M = \{n \in \mathbb{N} \mid a^n \in H\}$ Due to (*), $M \neq \phi$.

By Well-ordering principle, M has a least element, say k_0.

<u>Claim:</u> $H = \langle a^{k_0} \rangle$.

We have $a^{k_0} \in H$, and hence $(a^{k_0})^m \in H \quad \forall\, m \in \mathbb{Z}$.

$$\Rightarrow \langle a^{k_0} \rangle \subseteq H.$$

We next prove that $H \subseteq \langle a^{k_0} \rangle$.

Let $x \in H$. Then, $x = a^m$ for some $m \in \mathbb{Z}$.

By division algorithm, we write $m = q \cdot k_0 + r$, $0 \leq r < k_0$.

Now, $x = a^m = (a^{k_0})^q \cdot a^r \Rightarrow a^r = x \cdot (a^{k_0})^{-q} \in H$.

Since k_0 is the least +ve integer with $a^{k_0} \in H$, so

$0 \leq r < k_0 \Rightarrow r = 0 \quad \therefore\; m = q k_0$

Thus, $x = a^m = (a^{k_0})^q \in \langle a^k \rangle \Rightarrow H \subseteq \langle a^{k_0} \rangle$.

This proves that $H = \langle a^{k_0} \rangle$, and hence H is cyclic.

This completes the proof.

#