17/03/18

• Cyclic Groups :-

① $\langle G = \{ \dots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots \}, \times \rangle$

$\langle G = \{ (\frac{1}{2})^n : n \in \mathbb{Z} \}, \times \rangle$

OR

$\langle G = \{ (2)^n : n \in \mathbb{Z} \}, \times \rangle$

② $\langle \mathbb{Z}, + \rangle$

$1^n = n$, $n \in \mathbb{Z}^+$	$(-1)^n = -n$, $n \in \mathbb{Z}^+$
$1^0 = 0$	$1^0 = 0$
$1^{-n} = -n$, $n \in \mathbb{Z}^+$	$(-1)^{-n} = n$, $n \in \mathbb{Z}^+$

$\langle \mathbb{Z} = \{ (1)^n / (-1)^n : n \in \mathbb{Z} \}, + \rangle$

③ $\langle R, + \rangle$ ✗ not possible

⇒ A group $\langle G, * \rangle$ is said to be a cyclic group if there exists an element $a \in G$ such that $G = \{ a^n : a \in \mathbb{Z} \}$. Such a group is denoted by →

$G = \langle a \rangle$ [G generated by a]

Here,

a → generator of group G.

• **Proposition** :- Let G be a cyclic group generated by a, i.e $G = \langle a \rangle$. Then a^{-1} is also a generator of G.

Proof :- Let, H is a group where a^{-1} is generator.

$H = \langle a^{-1} \rangle$.

Let, $p \in G$. Then $p = a^K$ for some $K \in \mathbb{Z}$.

$\therefore p = a^K = (a^{-1})^{-K}$

$= (a^{-1})^{\ell} \in H$ [where, $\ell = -K \in \mathbb{Z}$]

$\therefore G \subseteq H$ — (1)

Let, $q \in H$. Then, $q = (a^{-1})^m$ for some $m \in \mathbb{Z}$.

$\therefore q = (a^{-1})^m = a^{-m}$

$= a^n \in G$ [where, $n = -m \in \mathbb{Z}$]

$\therefore H \subseteq G$ — (2)

From (1) & (2) $\longrightarrow$

$\boxed{H = G.}$

• **Proposition** :- Every cyclic group is abelian.

Proof:- Let, G is a cyclic group generated by a.

$G = \langle a \rangle$.

Then, $p = a^m$, $q = a^n$, ~~where~~ for some $m, n \in \mathbb{Z}$

Then, $pq = a^m . a^n = a^{m+n}$

$= a^{n+m} = a^n . a^m = qp$

Since, p & q had been chosen arbitrarily, the result follows.

• Proposition :- Let $G = \langle a \rangle$. Then, $o(G) = n$, iff $o(a) = n$.

$- \langle G = \{1, -1, i, -i\}, \times \rangle$

$G = \langle i \rangle$

$i^4 = 1$

$o(i) = 4$

$o(G) = 4$ [total no. of elements in G is order of G]

Proof :- Let, $o(a) = n$

$a^n = e$

$\therefore a, a^2, a^3, \ldots, a^{n-1}, a^n (= e)$ are all distinct.

$\therefore \{a, a^2, \ldots, a^{n-1}, a^n\} \subseteq G$ —— (1)

Let, $p = a^m \in G$. for some $m \in \mathbb{Z}^+$.

Then, by division algorithm $\longrightarrow$

$m = nq + r$, $0 \le r \le (n-1)$.

$\therefore a^m = a^{nq+r}$

$= (a^n)^q \cdot a^r = a^r$ [$\because a^n = e$]

i.e $a^m \in \{a, a^2, a^3, \ldots, a^{n-1}, e\}$

$\therefore G \subseteq \{a, a^2, \ldots, a^{n-1}, e\}$ — (2)

from (1) & (2) $\longrightarrow$

$\{a, a^2, a^3, \ldots, e\} = G$

$\therefore o(G) = n$.

» Conversely, let $o(G) = n$.

Therefore G has n elements.

~~Given, a is a generator of G~~.

Let, $o(a) = K$

i.e, $\{a, a^2, \ldots, a^{K-1}, a^K (=e)\}$ are all distinct

& $K \leq n$. [By closure property].

Then, by the foregoing argument, $\longrightarrow$

$o(G) = K$ which is a contradiction:

$\therefore o(a) = n \quad \therefore K = n$. .

- Proposition :- A subgroup of a cyclic group is cyclic.

Proof: Let G is a cyclic group generated by a.

$G = \langle a \rangle$

and $H \leq G$.

» case 1 :- If $H = \{e\}$, then the proposition is obvious as $e^n = e$.

» case 2 :- Let H is a proper subgroup of G and $x (\neq e) \in H \subset G$. i.e,

$x = a^K$ for some $k \in \mathbb{Z}$.

Since, H is a subgroup, $x^{-1} \in H$ i.e.

$x^{-1} = a^{-K} \in H$

$\therefore H$ contain some integral power of a.

Then, by Well-ordering principle in $\mathbb{Z}$, we can find a least positive $m \in \mathbb{Z}$, since that

$a^m \in H$.

Let, $p \in H \subset G$. Then $p = a^l$ for some $l \in \mathbb{Z}$.

By division algorithm $\longrightarrow$

$l = mq + r \quad , \; 0 \le r \le (m-1)$

$\therefore a^l = a^{mq+r}$

$= a^{mq} \cdot a^r = (a^m)^q \cdot a^r$

$\Rightarrow a^r = a^l \cdot a^{-mq}$ [$\because$ abelian group]

$\Rightarrow a^r = a^{l-mq} \in H$

(This is a contradiction and $a^r \notin H$.)

~~Because, $r \le m-1$~~

where, $r = 0$; otherwise this is a contradiction that, m is least element, such that

$a^m \in H$.

$\therefore l = mq$

$\Rightarrow p = a^l = a^{mq} = (a^m)^q \quad , q \in \mathbb{Z}$

Since, p has been chosen arbitrarily, it proves that any element in H can be expressed as $(a^m)^n$ for some $n \in \mathbb{Z}$.

$\therefore H$ is a cyclic group generated by a^m.

(Proved).

• <u>Proposition</u> :- A cyclic group of prime order has no proper non-trivial sub-group.

<u>Proof</u>:- Let, $o(G) = p$ and $G = \langle a \rangle$.

$\therefore a^p = e$. [e = identity in G]

Let H is a proper non-trivial cyclic sub-group of G such that, $H = \langle a^m \rangle$, where m is the least positive integer such that $a^m \in H$.

Now, $e = a^p \in H$

Then, $a^p = (a^m)^n$ for some, $n \in \mathbb{Z}$.

$\Rightarrow p = m \cdot n$

which is a contradiction to the fact that p is prime.

Hence, no such H exists.

$\therefore$