Cyclic Subgroup (generated by an element).

Let $(G, \circ)$ be a group and a be an element of G. Let H be the subset of G defined by $H = \{a^n : n \in \mathbb{Z}\}$. $(H, \circ)$ is a subgroup of $(G, \circ)$.

$H \rightarrow \langle a \rangle$

Note: The subgroup $\langle a \rangle$ is the smallest subgroup of the group $(G, \circ)$ containing the element a.

If $(K, \circ)$ be any subgroup of $(G, \circ)$ such that $a \in K$, then $\langle a \rangle \subset K$. ||

Proof: Since $a \in K$ and $(K, \circ)$ is a subgroup, $a^n \in K$. $\forall\, n \in \mathbb{Z}$. Therefore $\langle a \rangle \subset K$.

$\langle a \rangle \rightarrow a, a^2, a^3, \ldots a^n$

So, this proves $\langle a \rangle$ is the smallest subgroup of $(G, \circ)$ containing the element a.

$\langle \; \rangle \longrightarrow$ commutative

Note : $\langle a \rangle \longrightarrow$ commutative

Note : Let G be an additive group and $a \in G$.
The cyclic subgroup $\langle a \rangle$ is defined by

$$\langle a \rangle = \{ na : n \in \mathbb{Z} \}.$$

Eg : $G \to (\mathbb{Z}, +)$.

cyclic subgroup generated by $2 \to (2\mathbb{Z}, +)$.

Problems.

1. Find all cyclic subgroups of the group $(S, \cdot)$ where $S = \{1, i, -1, -i\}$.

$\Rightarrow$ $\langle 1 \rangle$ $\langle -1 \rangle$ $\langle i \rangle$ $\langle -i \rangle$.

$\langle 1 \rangle = \{1\}$

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

$i^1 = i$ $\quad i^2 = -1$

$i^3 = -i$, $i^4 = 1$

$\langle -1 \rangle = \{1, -1\}$

$\langle -i \rangle = \{1, i, -1, -i\}$.

2. Find all cyclic subgroups of the group $(\mathbb{Z}_5, +)$.

$\langle a \rangle$

2. Find all cyclic subgroups of $\mathbb{Z}_5$

$\Rightarrow \quad \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$

$\langle \bar{0} \rangle = \{\bar{0}\} \longrightarrow$ trivial sub.

$\langle \bar{1} \rangle = \{\bar{2}, \bar{3}, \bar{4}, \bar{0}, \bar{1}\}$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{1}, \bar{3}, \bar{0}\}$

$\langle \bar{3} \rangle = $ "

$\langle \bar{4} \rangle = $ "

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

$\langle a \rangle$

$a, a^2, a^3 \ldots$

$n = 1$

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

$\bar{2} + \bar{2} + \bar{2} = \bar{6}$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8}$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{10}$

$\mathbb{Z}_5$

4) Find all cyclic subgroups of K_4

$K_4 = \{a, b, c, e\}$

$\Rightarrow \quad \langle e \rangle = \{e\} \qquad \langle b \rangle = \{b, e\}$

$\langle a \rangle = \{a, e\} \qquad \langle c \rangle = \{c, e\}$

Cyclic Groups.

Defⁿ: A group $(G, \circ)$ is said to be a cyclic group if there exists an element a in G such that $G = \{a^n : n \in \mathbb{Z}\}$ i.e. $G = \langle a \rangle$,

'a' is the generator element

In additive notation, $G = \{na : n \in \mathbb{Z}\} = \langle a \rangle$.

Eg: $(\mathbb{Z}, +)$ — is a cyclic group generated by $\langle 1 \rangle$ and $\langle -1 \rangle$.

$(\mathbb{Z}_4, +) \to \bar{1}, \bar{3}$

$S = \{i, -1, -i, 1\}$.

Non-cyclic group $\to K_4$

Some Theorems:

Thm: Let $(G, \circ)$ be a cyclic group generated by a. Then a^{-1} is also a generator.

Thm: Every cyclic group is abelian. (commutative)

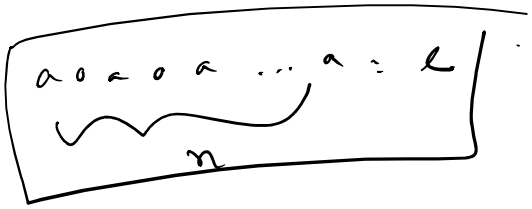
$K_4 \to$ abelian but not cyclic.

$D_4, S_3 \to$ not cyclic, not abelian.

Thm: Let G be an finite cyclic group generated by a. $o(a) = n$ if and only if $o(G) = n$.

Thm: Let G be an finite cyclic group generated by a. Then $O(G) = n$ if and only if $O(a) = n$.

$$G = \{a, a^2, \ldots a^n\}.$$



Thm: A finite group G of order n is cyclic if and only if there exists an element b in G such that $O(b) = n$.

Eg: $G \to (\mathbb{Z}_n, +) \longrightarrow |\mathbb{Z}_n| = n$.

$\bar{1} \in \mathbb{Z}_n \qquad O(\bar{1}) = n$.

So, $(\mathbb{Z}_n, +)$ is a cyclic group with $\bar{1}$ as generator.

Eg: $(S, \cdot) \qquad S = \{1, i, -i, -1\}$.

$'i' \quad O(i) = 4$, So $(S, \cdot)$ is a cyclic group with 'i' as generator.

Thm: $G \to$ finite cyc group with order $n > 1$, generated by a. Then for a positive integer r, a^r is also a generator of the group G iff $r < n$ and $g.c.d\ (r, n) = 1$.

iff $r < n$ and g.c.d $(r, n) = 1$.

Corollary: The total number of generators of a finite cyclic group of order n is $\phi(n)$.

$\phi(n) \rightarrow$ no. of positive integers less than n and prime to n.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \left(1 - \frac{1}{p_k}\right).$$

Th^{m}: Every subgroup of a cyclic group is cyclic.

Th^{m}: A cyclic group of finite order n has one and only one subgroup of order d for every positive divisor d of n.

Note: For every divisor d of n, there $\phi(d)$ distinct generators of the subgroup of order d.

Problems:

1. Find all subgroups of the group $(\mathbb{Z}, +)$.

, \ " .. , with 1 as

$\Rightarrow (\mathbb{Z}, +)$ is a cyclic group with 1 as generator. Therefore every subgroup of $(\mathbb{Z}, +)$ is cyclic.

$(m\mathbb{Z}, +)$

$(-m\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$.

$(\mathbb{Z}, +)$ $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3$

$\ldots$

$2\mathbb{Z} = \{2, 4, 6, \ldots\}$

$-2\mathbb{Z} = \{-2, -4, -6, \ldots\}$

2. Prove that the group $(\mathbb{Q}, +)$ is non cyclic. Deduce that the group $(\mathbb{R}, +)$ is non cyclic.

$\Rightarrow$ If possible let $(\mathbb{Q}, +)$ be a cyclic group generated by an element a. Then a is a non-zero element of $\mathbb{Q}$.

$na, a \in \mathbb{Q}$. $n \in \mathbb{Z}$.

But, $\frac{1}{2}a \in \mathbb{Q}$ but $\frac{1}{2}a \notin na$

$\frac{1}{2}a$ cannot be expressed as a generator of $(\mathbb{Q}, +)$.

of $(\mathbb{Q}, +)$.

This proves that $(\mathbb{Q}, +)$ is not a cyclic group.

is a subgroup of

$(\mathbb{Q}, +) \subset (\mathbb{R}, +)$

So, $(\mathbb{R}, +)$ must be non cyclic by nature.

3. Let n be a positive integer and let S be the set of n^{th} roots of unity. Show that

i) $(S, \cdot)$ is a cyclic group.

ii) Find all possible generators.

Sol^n: The elements of S are $1, \alpha, \alpha^2, \ldots \alpha^{n-1}$

$\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ . . $\omega^3 = 1$

$|S| = n$. $O(\alpha) = n$. $\alpha^n = 1$

So $(S, \cdot)$ is a cyclic group generated by α.

$\alpha^r \rightarrow$ generator

$r < n$

$g.c.d(r, n) = 1$ }.

Practice problems:

2. Let $S = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$, where $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$. Prove that S is a cyclic group under multiplication.

3. Let $S = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$. Prove that $(S, *)$ is a non-cyclic group, where $*$ is defined by $(a,b) * (c,d) = (ac, bd), (a,b), (c,d) \in S$.

4. Show that the group U_{10} is a cyclic group, but the group U_{12} is not cyclic.

5. A cyclic group G has only one generator. Prove that either $o(G) = 1$, or $o(G) = 2$.