G $\quad a \in G$. $\quad a \circ f = f \circ a$

$\langle a \rangle = \{ e, a, a^2, \ldots, a^n = e \}$

Centralizer of 'a' in a group G :—

$C(a) = \{ g \in G : ag = ga \}$, $a \in G$.

$e \in C(a)$, $a^{-1} \in C(a)$, $a \in C(a)$

If G is abelian, $C(a) = G$.

$G = D_4$, $\quad Z(D_4) = \{ R_0, R_{180} \}$

$C(H) = \{ R_0, R_{180}, H, V \} = C(V)$

$C(D) = \{ R_0, R_{180}, D, D' \} = C(D')$

$C(R_0) = D_4 = C(R_{180})$

$C(R_{90}) = \{ R_0, R_{180}, R_{90}, R_{270} \}$

$= \langle R_{90} \rangle \qquad = C(R_{270})$

for G,

$Z(G) \subseteq C(a)$, $\forall a \in G$.

for abelian group G,

$G = Z(G) = C(a)$, $\forall a \in G$.

Prop :— $C(a)$ forms a subgroup of G, where $a \in G$.

$\because \quad e \in C(a)$, $C(a)$ is nonempty.

Let $b, c \in C(a)$

$\Rightarrow ab = ba$ and $ac = ca$.

$\Rightarrow c^{-1}a = ac^{-1}$

$(bc^{-1})a = b(c^{-1}a)$

$= b(ac^{-1}) = (ba)c^{-1} = (ab)c^{-1}$

$= a(bc^{-1})$

$\Rightarrow bc^{-1} \in C(a)$, for $b, c \in C(a)$

$\therefore C(a)$ is a subgroup of G.

cyclic group

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

$|G| = |a| = n$.

$\langle a \rangle = G$., cyclic.

Let G is finite group and $|G| = n$.

if $\exists\ a \in G$ s.t. $|a| = n$. Then

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

as if $a^i = a^j$, $1 \le i < j \le n$

$\Rightarrow a^{j-i} = e$

$\Rightarrow |a| \mid j - i$

$\Rightarrow n \mid j-1$ contradiction.

Then $G = \{a, a^2, \ldots, a^n = e\} = \langle a \rangle$.

G is cyclic group generated by a.

Ex:— i) $G = \{1, -1, i, -i\}$. $|G| = 4$

$|i| = 4$. $G = \langle i \rangle = \{i, i^2, i^3, i^4\}$

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

ii) $(\mathbb{Z}_n, +) = \langle 1 \rangle = \langle n-1 \rangle$

$|\mathbb{Z}_n| = n$ finite cyclic group.

Let G is infinite group. G is cyclic if $\exists\ a \in G$ s.t. $G = \{a^n : n \in \mathbb{Z}\}$

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

Ex:- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

Prop:- If $|G| > 2$ and G be a cyclic group. Then G has even number of generators.

$\Rightarrow$ Case I:- Let G be finite cyclic grp. $|G| > 2$. $G = \langle a \rangle$, $a \in G$

Then a^{-1} is also a generator of G.

$a \neq a^{-1}$ as if $a = a^{-1} \Rightarrow a^2 = e$

$\Rightarrow G \neq \langle a \rangle$ [$\because |G| > 2$]

$\therefore$ generators of G occur in pair. G has even no of generators.

Case II:- If G is infinite cyclic grp. If $G = \langle a \rangle$. Then G has only two generators a and a^{-1}.

Why ?.!

Let α, β be two generators of G.

$\therefore \alpha = \beta^i$, $\beta = \alpha^j$, $i, j \in \mathbb{Z}$.

$\therefore \alpha = \beta^i = (\alpha^j)^i = \alpha^{ij}$

$\Rightarrow \quad \alpha^{ij-1} = e$

$\therefore \quad ij = 1$ otherwise order of α is finite.

$\Rightarrow \quad i = 1 = j \quad , \quad i = -1 = j$.

$\therefore$ G has two generators α and α^{-1}.

Ex :→

1) $(\mathbb{Z}, +)$ cyclic generated by 1 and -1.

$(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ is not cyclic.

2) $(\mathbb{Z}_n, +)$ cyclic.

$= \langle 1 \rangle = \langle n-1 \rangle = \langle k \rangle$, $(k, n) = 1$

k is a generator of $\mathbb{Z}_n$ iff $\gcd(k, n) = 1$

$\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

$= \langle a \rangle = \langle a^3 \rangle = \langle a^7 \rangle = \langle a^9 \rangle$

$|a^k| = |a| = n$ iff $\gcd(k, n) = 1$.

$\rightarrow = \dfrac{|a|}{\gcd(k, n)}$

The set of generators of $\mathbb{Z}_n = U(n)$.

3) $U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle = \langle 7 \rangle$

$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4\} = \{3, 9, 7, 1\}$

$= \langle 7 \rangle$.

$U(8)$, $U(12)$ is not cyclic.

$K-4$ is not A cyclic.

4) $(n\mathbb{Z}, +)$ is cyclic.

$= \langle n \rangle = \langle -n \rangle$.

$(\mathbb{Z}, +)$, Let $r, s \in \mathbb{Z}^+$.

$H = \{ r.m + s.n : m, n \in \mathbb{Z} \}$

is a subgroup of $\mathbb{Z}$.

[$0, r, s \in H$. H is nonempty.

Let $r.m_1 + sn_1$, $r.m_2 + s.n_2 \in H$

Then $(rm_1 + sn_1) + (r(-m_2) + s(-n_2))$

$= r(m_1 - m_2) + s(n_1 - n_2)$

$\in H$ [$\because$ $m_1 - m_2 \in \mathbb{Z}$, $n_1 - n_2 \in \mathbb{Z}$]]

$H = \{ r.m + s.n : m, n \in \mathbb{Z} \}$

$= d\mathbb{Z}$, $d \in \mathbb{Z}^+$

$= \langle d \rangle$

d is the g.c.d. (r, s).

Ex:— 6, 9.

$H = \{ 6.m + 9.n : m, n \in \mathbb{Z} \}$

$= \{ \ldots -6, -3, 0, 3, 6, 9, 12, \ldots \}$

$= 3\mathbb{Z}$

$3 = \gcd(6, 9)$.

Theorem:— Every cyclic group is abelian.

$\Rightarrow$ G cyclic. $a \in G$.

$G = \langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$

Let $a^p, a^q \in G \Rightarrow a^p \cdot a^q = a^{p+q}$

$= a^{q+p} = a^q \cdot a^p$.

$\therefore$ G is abelian.

$\therefore$ Non-abelian $\Rightarrow$ Non-cyclic.

Ex :- D_n.

Converse of the theorem is not true.

Ex :- K-4 group.

Theorem :-

Let G be a group and $a \in G$.

If a has infinite order, then all distinct powers of a are distinct group elements.

If a has finite order, say n, then $\langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$

and $a^i = a^j$ iff $n / i-j$.

H/W