- Generator & cyclic group -

A group G is called cyclic if there is element a in G such that $G = \{a^i \mid i \in \mathbb{Z}\}$ such an element a is called a generator.

We may indicate that G is a cyclic group Generated by a.

We writting $G = [a]$

e.g. (1) The set of integers $\mathbb{Z}$ under ordinary addition is cyclic because both 1 & -1 are generator

$\langle 1 \rangle = [1] = \{i \cdot 1 \mid i \in \mathbb{Z}\} = \mathbb{Z}$.

$\langle -1 \rangle = [-1] = \{i(-1) \mid i \in \mathbb{Z}\} = \mathbb{Z}$.

(2) The set $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots \overline{n-1}\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again 1 & $-1 = n-1$ are generators.

Q Find the generators of $\mathbb{Z}_8$

→ Here $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

So

$[\bar{0}] = \{i\bar{0} \mid i \in \mathbb{Z}\} = \{0\}$

$[\bar{1}] = \{i\bar{1} \mid i \in \mathbb{Z}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{0}\} = \mathbb{Z}_8$

$6 \times 7 = 42$

$[\bar{2}] = \{i\bar{2} \mid i \in \mathbb{Z}\} = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\}$

$[\bar{3}] = \{i\bar{3} \mid i \in \mathbb{Z}\} = \{\bar{3}, \bar{6}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\} = \mathbb{Z}_8$

$[\bar{4}] = \{i\bar{4} \mid i \in \mathbb{Z}\} = \{\bar{4}, \bar{0}\}$

$[\bar{5}] = \{i\bar{5} \mid i \in \mathbb{Z}\} = \{\bar{5}, \bar{2}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{3}, \bar{0}\}$

$[\bar{6}] = \{i\bar{6} \mid i \in \mathbb{Z}\} = \{\bar{6}, \bar{4}, \bar{2}, \bar{0}\}$

$[\bar{7}] = \{i\bar{7} \mid i \in \mathbb{Z}\} = \{\bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1},$

[1] & [3], are generators of Z_8 addition modulo 8. $\langle 5 \rangle$,

Q Find the generators of U(10)

→

$U(n) = \{ k \mid k < n, \gcd(k, n) = 1 \}$

If $n = 10$ $U(10) = \{ k \mid k < 10, \gcd(k, 10) = 1 \}$

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

$\langle 1 \rangle = \{ 1^i \mid i \in \mathbb{Z} \}$
$= \{1\}$

$\langle 3 \rangle = \{ 3^i \mid i \in \mathbb{Z} \} = \{3, 9, 7, 1\} = U(10)$

$\langle 7 \rangle = \{ 7^i \mid i \in \mathbb{Z} \} = \{7, 9, 3, 1\} = U(10)$

$\langle 9 \rangle = \{ 9^i \mid i \in \mathbb{Z} \} = \{9, 1\}$

Generators of U(10) are $\langle 3 \rangle$ & $\langle 7 \rangle$

Theorem :- Every cyclic group is isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/(n)$ for some $n \in \mathbb{N}$.

→ If $G = [a]$ is an infinite group
Consider the mapping $\psi : \mathbb{Z} \to G$.
given by $\psi(i) = a^i$

Let $i, j \in \mathbb{Z}$ such that.
$\psi(i) = a^i$, $\psi(j) = a^j$

1) ψ is one-one ←
consider $i \neq j \Rightarrow a^i \neq a^j$
$\Rightarrow \psi(i) \neq \psi(j)$
$\therefore$ ψ is one-one

2) ψ is onto -

Let $\psi(i) = j$

$\Rightarrow a^i = j$

$\Rightarrow \log a^i = \log j$

$\Rightarrow i \log a = \log j$

$\Rightarrow i = \frac{\log j}{\log a} \Rightarrow \log_a j =$

$\therefore$ ψ is onto.

3) ψ is homomorphism :-

Let $i, j \in \mathbb{Z} \Rightarrow i+j \in \mathbb{Z}$.

$$\psi(i+j) = a^{i+j} = a^i \cdot a^j$$

$$\psi(i+j) = \psi(i) \cdot \psi(j)$$

$\therefore$ ψ is homomorphism.

$\therefore$ ψ is isomorphism.

Next suppose $G = [a]$ is a cyclic group of finite order n

i.e $O(a) = n \Rightarrow a^n = e$.

then $G = \{e, a, a^2, \text{---} a^{n-1}\}$

Consider the mapping $\psi : \mathbb{Z}(n) \longrightarrow G$ given by $\psi(\bar{i}) = a^i$

1) ψ is homomorphism :-

Let $\bar{i}, \bar{j} \in \mathbb{Z}_n$ such that $\psi(\bar{i}) = a^i$ &
$\psi(\bar{j}) = a^j$

$$\therefore \psi(\bar{i}+\bar{j}) = \psi(\overline{i+j}) = a^{i+j}$$
$$= a^i \cdot a^j$$
$$= \psi(\bar{i}) \cdot \psi(\bar{j})$$

$\therefore$ ψ is homomorphism.

Scanned by CamScanner

2) Injective :-

Let $\bar{i}, \bar{j} \in \mathbb{Z}_n$ then .

$\bar{i} = \bar{j}$

$\Leftrightarrow$ i.e $i \equiv j \mod n$

$\Leftrightarrow n \mid i-j$

$\Leftrightarrow i-j = nk \quad k \in \mathbb{N}$

$\Leftrightarrow a^{i-j} = a^{nk}$

$\Leftrightarrow a^i . a^{-j} = (a^n)^k \Leftrightarrow a^{i-j} = e^k = e$

i.e $a^{i-j} = e$

$\Leftrightarrow \frac{a^{i-j}}{} a^j = e . a^j$

$\Leftrightarrow a^i = a^j \Rightarrow \varphi(\bar{i}) = \varphi(\bar{j})$

3) Surjective :-

Let $i \in \mathbb{Z}/(n)$ then $\varphi(\bar{i}) = j$

$\Rightarrow a^i = j$

$\Rightarrow i \log a = \log j$

$\Rightarrow i = \frac{\log j}{\log a}$

$\Rightarrow i = \log_a j$

$\therefore \varphi$ is surjective.

$\therefore \varphi$ is isomorphism.

Every cyclic groups of the order (infinite or finite) are isomorphic.

Theorem :- Every subgroup of cyclic group is cyclic

$\rightarrow$ Let $G = [a]$ be a cyclic group. and Let H be a subgroup of G.

If H is a trivial subgroup

$H = \{e\} = [e] \quad \therefore H$ is cyclic

$\log_a j$

j //

Scanned by CamScanner

the result is obvious..

So let H be a proper subgroup of G. i.e $H \neq \{e\}$

If $a^i \in H$ then $a^{-i} \in H$. Hence there is a least positive integer m such that

$$b = a^m \in H.$$

<u>claim</u> - H is cyclic group of G.

Let $i \in \mathbb{Z}$, $i \neq 0$, $a^i \in H$.

By Division algorithm.

$$i = mq + r \quad \text{where } 0 \leq r < m.$$

$$\Rightarrow r = i - mq$$

$$\Rightarrow a^r = a^{i-mq} \Rightarrow a^r = a^i (a^m)^{-q}.$$

$$\Rightarrow a^r = a^i b^{-q} \in H.$$

Hence $r = 0$ then $a^i b^{-q} = 1$

$$\Rightarrow a^i = b^q$$

a^i is $a \{e, a, a^2 \cdots a^{i-1}\} = b^q$, $q \in \mathbb{Z}$

$\therefore H = [b]$ is cyclic group.

- <u>Theorem</u> -

Let G be a finite cyclic group of order n and Let d be a positive divisor of n. Then G has exactly one subgroup of order d.

→

Let G be a finite cyclic group of order n. i.e $G = [a]$ i.e $o(a) = n$

and Let d be a positive divisor of n.

If $d = 1$ it ~~hst~~ is trivially true.

Therefore $1 < d < n$ & put $m = n/d$

& $G = [a]$ then $b = a^m$ is of order d.

i.e $b^d = (a^m)^d$

$\Rightarrow b^d = (a^{n/d})^d$

$b^d = a^n = e$.

i.e $b^d = e$.

i.e $[b] = \{e, b, b^2 - - - b^{d-1}\}$

$\therefore$ b has order d which is cyclic

$\therefore$ [b] is a cyclic subgroup of order d

We next show $[a^m]$ is the only subgroup of order d. By previous Theorem

Every subgroup of cyclic group is cyclic so, $H = [b]$ i.e $H = \langle a^m \rangle$

Where m is the least positive integer such that $a^m \in H$

Now by division algorithm

Let $n, m \in \mathbb{Z}$ & $\exists$ q, r are unique integer such that

$n = mq + r$, Where $0 \leq r < m$ —(1)

We have $a^n = a^{mq+r}$

$\Rightarrow e = a^{mq} \cdot a^r$

$\Rightarrow a^r = a^{-mq} \Rightarrow a^r = (a^m)^{-q} \in H$

Thus $r = 0$ $\Rightarrow$ So eq^n (1) becomes

$n = mq \Rightarrow$ ~~n/m~~ $q = n/m$.

$\Rightarrow$ ~~m/n~~.

$\therefore d = |H| = |\langle a^m \rangle| = n/m = d$.

i.e $|H| = |\langle a^m \rangle| = |\langle a^{n/d} \rangle| = d$.

$\therefore$ H is only subgroup of order d.

Scanned by CamScanner

Page No
Date

* Theorem (Lagrange).

Let G be a finite group. Then the order of any subgroup of G divides the order of G.

* Corollary :-

Let G be a finite group of order n. Then for every $a \in G$ $o(a)/n$ & hence $a^n = e$. Consequently, Every finite group of prime Order is cyclic & hence abelian.

→ Let $a \in G$. By Lagrange's theorem: the order of the cyclic subgroup [a] divides n. So $o(a)/n$.

If n is prime and $a \neq e$ the order of [a] must be n. Hence $[a] = G$ & G is cyclic.

e.g ① Let G be a group & $a, b \in G$ such that $ab = ba$ if $o(a) = m$, $o(b) = n$ & $(m, n) = 1$ then $o(ab) = mn$.

→ Let $o(a,b) = k$ i.e $(ab)^k = e$

Consider $(ab)^{mn} = a^{mn} \cdot b^{mn} = (a^m)^n \cdot (b^n)^m = e$

we know that If $a^n = e$ & $n \neq 0$ then $o(a)/n$.

$\therefore$ k/mn Also

$(ab)^k = e = a^k \cdot b^k$

So, $a^k = b^{-k}$

Thus,

$o(a^k) = o(b^{-k}) = o(b^k)$

But $a^m = e = (a^k)^m = e$.

$\Rightarrow o(a^k) | m$.

Similarly $o(b^k) | n$.

$\therefore o(a^k)$ divides $(m,n) = 1$

$\therefore o(a^k) = 1$ so $a^k = e$. But then $m|k$ & $n|k$

Consequently $mn | k$ $\because k | mn$.

$\therefore k = mn$.

$\therefore o(ab) = mn$

Example ② Let $H = [a]$ and $k = [b]$ be cyclic group of orders m & n respectively Such that $\gcd(m,n) = 1$ Then $H \times k$ is a cyclic group of order mn.

→ Let H & K are cyclic groups of order m and n i.e $a^m = e$ & $b^n = e$.

Then $H \times K = \{(a,b) \mid a \in H, b \in K\}$

Claim :- $H \times K$ is cyclic group of order mn.

Let $o(a,b) = d$

Now $(a,b)^{mn} = (a^{mn}, b^{mn}) = ((a^m)^n, (b^n)^m)$

$= (e^n, e^m) = (e,e)$

$\in H \times k$

$o(a,b) = mn$ in $H \times k$

$\therefore d | mn$ —①

also $(e,e) = (a,b)^d = (a^d, b^d)$

i.e $a^d = e$, $b^d = e$

So, $m|d$ & $n|d$

$\Rightarrow mn | d$ —②

By ① & ② we get $d = mn$.

Scanned by CamScanner

$\because |H \times K| = mn$

i.e $(H \times K)^{mn} = e$.

$\therefore$ (a,b) generates group $H \times K$ if $\gcd(m,n)=1$

~~② Let G be a group & $a,b \in G$ such that $ab=ba$ If $o(a)=m$, $o(b)=n$ & $(m,n)=1$ then $o(ab)=mn$.~~

~~→ Let $o(ab)=k$ i.e $(ab)^k=e$~~

~~Consider $(ab)^{mn} = a^{mn} \cdot b^{mn} = (a^m)^n (b^n)^m = e \cdot e = e$.~~

~~Which gives~~

<u>Theorem</u> – Let G be a group and let a belong to G If a has infinite order. then all ~~distinct~~ powers of a are distinct group elements. If a is finite order say n then $\langle a \rangle = \{e, a, a^2 --- a^{n-1}\}$ & $a^i = a^j$ iff $n \mid i-j$

→ Consider G be a group and $a \in G$

If a has infinite order.

There is no nonzero n such that

$a^n = e$.

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

we must have $i-j=0$.

$\therefore$ a^i, a^j are distinct power of a are distinct elements.

Now we consider. If a has finite order.

i.e $|a|=n$ i.e $a^n=e$.

We will prove that

$$\langle a \rangle = \{e, a, a^2 --- a^{n-1}\}$$

Let the element $e, a, a^2 --- a^{n-1}$ are distinct for it $a^i = a^j$ with $0 \le j < i \le n-1$

then $a^{i-j} = e$ i.e $o(a) = i-j$

Which is contradiction to the least positive integer such that

$$a^n = e \quad \text{i.e.} \quad o(a) = n.$$

Now,

Suppose that a^k is an arbitrary member of $\langle a \rangle$.

By division algorithm $\exists$ integers q & r such that

$$k = nq + r \quad \text{with } 0 \le r < n$$

Then

$$a^k = a^{nq+r} = a^{nq} \cdot a^r$$

$$a^k = (a^n)^q \cdot a^r$$

$$\Rightarrow a^k = e \cdot a^r$$

$$\Rightarrow a^k = a^r \quad 0 \le r < n$$

So, that

$$a^k = \{e, a, a^2 --- a^{n-1}\}$$

Next we assume that $a^i = a^j$

To show that $n \mid i-j$

Suppose $a^i = a^j$

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

Again by division algorithm there are unique integers q & r such that

$$i-j = nq + r \quad \text{with } 0 \le r < n.$$

$$a^{i-j} = a^{nq+r}$$

$$a^{i-j} = (a^n)^q\, a^r \qquad [a^n = e]$$

i.e $a = (e)^q a^r$

$\Rightarrow a^r = e$ i.e $r = 0$.

$\therefore \quad i-j = nq$

$\Rightarrow \quad n \mid i-j$

Conversaly, If $n \mid i-j$

i.e $i-j = nq$

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

$\Rightarrow a^{i-j} = (a^n)^q$.

but We know that $a^n = e$.

$\therefore \quad a^{i-j} = e$

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

multipling a^j on both sides

$\Rightarrow a^i = a^j$

e.g - prove that there are exactly $\phi(d)$ elements of a cyclic group of order d that can generate it.

→ Let G be a finite cyclic group of order n & let d be a positive divisor of n then G has exactly one subgroup of order d

$\therefore$ Every element of order d also generates the subgroup $\langle a \rangle$

If a^k generates $\langle a \rangle$ iff gcd $(k, d) = 1$.

$\therefore$ it has $\phi(d)$ elements of a cyclic group of order d.

§ Relation :-

Let G be a group generated by a subset x of G. A set of eqⁿ ($r_i = 1$) that suffices to construct the multiplication table of G is called a set of defining relation for the group.

§ Normal subgroup :-

Let G be a group. A subgroup N of G is called a normal subgroup of G written as $N \trianglelefteq G$ if $xNx^{-1} \subset N$ for every $x \in G$.

Note:- ① The subgroups $\{e\}$ & G itself are normal subgroups of G.
② If G is abelian then every subgroup of G is a normal subgroup.

Thᵐ - Let N be a subgroup of a group G then the following are equivalent

i) $N \trianglelefteq G$
ii) $xNx^{-1} = N$ for every $x \in G$
iii) $xN = Nx$ for every $x \in G$
iv) $(xN)(yN) = xyN$ $\forall x, y \in G$

→ Let N be a subgroup of G i.e $N < G$

i) ⇒ ii) Let $N \trianglelefteq G$ Let $x \in G$.

By definition $xNx^{-1} \subset N$

Also $x^{-1} \in G$

$\therefore x^{-1}N(x^{-1})^{-1} \subset N$

$\Rightarrow x^{-1}Nx \subset N$.

$\therefore N = x(x^{-1}Nx)x \subset xNx^{-1}$

$\Rightarrow N = xNx^{-1}$ $\forall x \in G$

ii) $\Rightarrow$ iii) Let $Nx = (xNx^{-1})x$ $\because N = xNx^{-1}$ $\forall x \in G$..

$= xNx^{-1}x$

$Nx = xNe$ $\forall x \in G$

$(x.x^{-1} = e)$

$\therefore Nx = xN$ $\forall x \in G$.

iii) $\Rightarrow$ iv) Let $(xN)(yN) = x(Ny)N$

$= x\,yNN$ $\because x, y \in G$

$= (xy)NN.$ $xN = Nx$, $yN = Ny$

Now $NN \subset N$ — (1)

Because N is closed under multiplication

On the other hand $N = eN \subset NN$.

$\therefore N \subset NN$ — (2)

By (1) & (2) we get $N = NN$.

$\therefore (xN)(yN) = xyNN.$

$= xyN.$ $\forall x, y \in G$

iv) $\Rightarrow$ i) Let $xNx^{-1} = xNx^{-1}e$.

$\subset (xNx^{-1}N)$

$\in xx^{-1}NN$

$\in eN = N$

$\therefore xNx^{-1} \subset N$ $\forall x \in G$.

Hence $N \trianglelefteq G$.

Example- Let $SL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ \begin{matrix} ad - bc = 1 \\ a, b, c, d \in \mathbb{R} \end{matrix} \right\}$

is a subgroup of $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle/ \begin{matrix} a, b, c, d \in \mathbb{R} \\ ad - bc \neq 0 \end{matrix} \right\}$

under matrix multiplication. show that

$$SL(2,\mathbb{R}) \Delta GL(2,\mathbb{R})$$

→ First We know that $SL(2,\mathbb{R})$ is a subgroup of $GL(2,\mathbb{R})$

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ be identity matrix.

$\therefore |I| = 1 \quad \therefore I \in SL(2,\mathbb{R})$

$\therefore SL(2,\mathbb{R})$ be nonempty set.

Now, $A, B \in SL(2,\mathbb{R})$
To show that $AB^{-1} \in SL(2,\mathbb{R})$

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ & $a_1d_1 - b_1c_1 = 1$

& $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ & $a_2d_2 - b_2c_2 = 1$.

$$AB^{-1} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1d_2 - b_1c_2 & -a_1b_2 + b_1a_2 \\ c_1d_2 - d_1c_2 & -c_1b_2 + d_1a_2 \end{bmatrix}$$

$$|AB^{-1}| = (a_1d_2 - b_1c_2)(-c_1b_2 + d_1a_2) - (-a_1b_2 + b_1a_2)(c_1d_2 - d_1c_2)$$

$$= -\cancel{a_1b_2c_1d_2} + a_1a_2d_1d_2 + b_1b_2c_1c_2 - \cancel{a_2b_1c_2d_1} + \cancel{a_1b_2c_1d_2} - a_1b_2c_2d_1 - \cancel{a_2b_1c_1d_2} + \cancel{a_2b_1c_2d_1}$$

$$= a_1d_1(a_2d_2 - b_2c_2) - b_1c_1(a_2d_2 - b_2c_2)$$

$$= (a_1d_1 - b_1c_1)(a_2d_2 - b_2c_2)$$

$|AB^{-1}| = 1$

So, $AB^{-1} \in SL(2, \mathbb{R})$

$\because$ $SL(2, \mathbb{R})$ be a subgroup of $GL(2, \mathbb{R})$

We show that $SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$

For any $A \in GL(2, \mathbb{R})$ & $B \in SL(2, \mathbb{R})$.
i.e $|A| \neq 0$. $|B| = 1$.

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1})$$
$$= \det(A) \cdot 1 \cdot \det(A^{-1})$$
$$= \cancel{\det(A)} \cdot \frac{1}{\cancel{\det(A)}} = 1.$$

$\therefore$ $ABA^{-1} \in SL(2, \mathbb{R})$ $\forall A \in GL(2, \mathbb{R})$

$\therefore$ $SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$

§ <u>Quotient group</u>:-

Let N be a normal subgroup of G. The group G/N is called the quotient group of G by N. The homomorphism $G \to G/N$ given by $x \to xN$ is called the natural (or canonical) homomorphism of G onto G/N.

i.e $G/N = \{xN \mid x \in G\}$ defined $x, y \in G$.
$$(xN) \cdot (yN) = (xy)N$$

§ G/N is group under multiplication.

Theorem: Let N be a normal subgroup of the group G. Then G/N is a group under multiplication. The mapping $\phi: G \rightarrow G/N$ given by $x \longrightarrow xN$ is a surjective homomorphism & $\mathrm{Ker}\,\phi = N$.

→ Let N be a normal subgroup of the group G.

Let $e \in G$ $\therefore eN \in G/N$.

$\therefore G/N$ is non empty.

(1) Closure property:

Let $xN, yN \in G/N$ $\forall x, y \in G$.

$$(xN).(yN) = (xy)N \in G/N, \quad xy \in G.$$

(2) Associative property:

Let $xN, yN, zN \in G/N$, $x, y, z \in G$

$$xN[(yN).(zN)] = xN[(yz)N]$$
$$= (xyz)N \quad \text{—(1)}$$
$$[(xN)(yN)]zN = [(xy)N]zN$$
$$= (xyz)N \quad \text{—(2)}$$

By (1) & (2) we get

$$xN[(yN)(zN)] = [(xN)(yN)]zN$$

(3) Existance of Identity:

Let $xN \in G/N$ $\forall x \in G$ then

$$(xN)(eN) = (xe)N$$
$$= xN.$$

$\therefore \exists\, eN = N \in G/N$ identity in G/N.

(4) Existance of inverses :-

Let $xN \in G/N$ Such that

$$(xN)(x^{-1}N) = (xx^{-1})N$$
$$= e.N$$
$$= N.$$

$\therefore$ $xN \in G/N$ have inverses $x^{-1}N \in G/N$

$x^{-1} \in G$.

Now consider the mapping

$$\phi : G \to G/N \text{ given by}$$
$$\phi(x) = xN$$

To show That ϕ is surjective homomorphism & $\ker\phi = N$.

(1) ϕ is one-one:$\Rightarrow$ Let $x, y \in G$.

Consider $\phi(x) = \phi(y)$

$$\Rightarrow xN = yN.$$
$$xN(yN)^{-1} = (yN)(yN)^{-1}$$
$$(xN)(y^{-1}N) = yy^{-1}NN.$$
$$= eN$$
$$(xy^{-1})N = N$$
$$\Rightarrow xy^{-1} = 1.$$
$$\Rightarrow xy^{-1}y = y \quad . \Rightarrow \underline{\underline{x = y}}.$$

$\therefore$ ϕ is one-one

(2) ϕ is onto :-

Let $a \in G/N$ i.e $a = \cancel{y}N$

So, consider $\phi(x) = a$.

$$\therefore xN = yN.$$
$$\therefore \cancel{x=y} \; y = x \in G.$$

$\therefore$ ϕ is onto.

(3) We show that ϕ is homomorphism.

For all $x, y \in G$

& $\phi(x) = xN$ & $\phi(y) = yN$.

So, $xy \in G$.

$$\phi(xy) = (xy)N = (xN)(yN)$$
$$= \phi(x) \cdot \phi(y)$$

Scanned by CamScanner

Hence ϕ is homomorphism.
To prove : $\ker\phi = N$.
~~To~~ By definition of kernel of ϕ.

$$\ker\phi = \{x \in G \mid \phi(x) = N\}$$

$$= \{x \in G \mid xN = N\}$$

Further $xN = eN$ iff $x \in N$.

$$\ker\phi = N.$$

e.g
Note ① If G is an abelian group and $N \Delta G$.
then G/N is abelian.

→ We know that G is abelian
i.e $\forall\, x, y \in G \Rightarrow xy = yx$.

To show that G/N is abelian.
i.e $\forall\, (xN), (yN) \in G/N \Rightarrow (xN)(yN) = (yN)(xN)$

Now, consider $(xN), (yN) \in G/N$, $x, y \in G$.

$$\therefore (xN)(yN) = (xy)N$$
$$= (yx)N \qquad (\because G \text{ is abelian})$$
$$= (yN)(xN)$$

$\therefore$ G/N is abelian.

② If G is cyclic group and $N \Delta G$ then G/N is cyclic.

→

Let $G = \langle a \rangle$ be a cyclic group generated by a & $N \Delta G$. So, N is subgroup of G.

By Theorem - Every subgroup of cyclic group is cyclic.

$\therefore$ N is cyclic.

To prove :- G/N is cyclic.

Let $G/N = \{aN \mid a \in G\}$ We know that G is cyclic $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$

$$G/N = \{a^i N \mid i \in \mathbb{Z}\}$$

$$= \{(aN)^i \mid i \in \mathbb{Z}\}$$

$$G/N = \langle aN \rangle.$$

$\therefore$ The group G/N is generates by aN

$\therefore$ G/N is cyclic.

③ The centre of a group $Z(G)$ is normal subgroup of G.

→ Let G be a group with identity e.

& $Z(G) = \{x \in G \mid xa = ax \ \forall a \in G\}$.

To show that $Z(G)$ is subgroup of G.

Let $e \in G$. $ea = a \cdot e \ \forall a \in G$.

$\therefore$ $e \in Z(G)$

$\therefore$ $Z(G)$ is nonempty.

Now, $a, b \in Z(G)$

i.e $xa = ax$ & $xb = bx$ $\forall a, b \in G$.

$xa^{-1} = a^{-1}x$ & $xb^{-1} = b^{-1}x$ $\forall a^{-1}, b^{-1} \in G$

$(ab^{-1})x = a(b^{-1}x)$ Associative)

$= a(xb^{-1})$ $(\because b^{-1}x = xb^{-1})$

$= (ax)b^{-1}$

$= (xa)b^{-1}$ $(\because ax = xa)$.

$= x(ab^{-1})$ $\forall ab^{-1} \in G$.

$\therefore$ $ab^{-1} \in Z(G)$.

$\therefore Z(G)$ is subgroup of G.

We show that $Z(G) \triangle G$.

Consider $a \in G$ & $x \in Z(G)$

$\Rightarrow ax = xa \quad \forall a \in G$.

Then,

$$axa^{-1} = xaa^{-1}$$
$$= xe$$
$$= x \in Z(G)$$

$\therefore axa^{-1} \in Z(G) \quad \forall a \in G, \forall x \in Z(G)$

$\therefore aZ(G)a^{-1} \subseteq Z(G) \quad \forall a \in G$.

$\therefore Z(G)$ is normal subgroup of G.

$Z(G) \triangle G$.

* **Definition** -

Let G be a group and let S be a nonempty subset of G. The normalizer of S in G is the set

$$N(S) = \{x \in G \mid xSx^{-1} = S\}$$

The normalizer of a singleton $\{a\}$ is written as $N(a)$.

* **Theorem** -

Let G be a group. For any nonempty subset S of G. $N(S)$ is a subgroup of G further for any subgroup H of G.

i) $N(H)$ is ~~a~~ the largest subgroup of G in which H is normal.

ii) If K is a Subgroup of $N(H)$ then H is a normal subgroup of KH.

proof - Let G be a group then To prove that $N(S)$ is subgroup of G.

Let $N(S) = \{x \in G \mid xSx^{-1} = S\}$.
We know that $e \in G$ such that
$ese^{-1} = S \Rightarrow e \in N(S)$.
$\therefore N(S)$ is nonempty

Let $x, y \in N(S)$
$xSx^{-1} = S$, $ySy^{-1} = S$, $x, y \in G$.

To prove - $xy^{-1} \in N(S)$
Consider,

$$(xy^{-1})(S)(xy^{-1})^{-1} = (x y^{-1}) S (y x^{-1})$$
$$= x(y^{-1} S y) x^{-1}$$
$$= x(y^{-1}(ySy^{-1})y)x^{-1}$$
$$= x(y^{-1}y\, S\, y^{-1}y)x^{-1} \quad (\because y^{-1}y = e)$$
$$= x(eSe)x^{-1} = xSx^{-1} = S$$

$\therefore (xy^{-1})S(xy^{-1})^{-1} = S$.

$\therefore xy^{-1} \in N(S)$
$\therefore N(S)$ is subgroup of G.

i) Let H be subgroup of G then $hHh^{-1} = H$ $\forall h \in H$.
$\therefore H$ is a subset and hence a subgroup of $N(H)$ Further By definition,
$xHx^{-1} = H \quad \forall x \in N(H)$
$\therefore x \in N(H)$
Hence $H \Delta N(H)$. So, $H < N(H)$.
$\therefore H \subset N(H)$. $\because N(H)$ is largest subgroup

of G in which $H \Delta N(H)$.

ii) Let K be a subgroup of $N(H)$

i.e $K < N(H)$

Let $k \in K$, $kHk^{-1} = H$

$\Rightarrow kHk^{-1}k = Hk$

$\therefore kH = Hk \quad \forall k \in K$

$\therefore KH = HK$.

$\therefore KH$ is a subgroup of $N(H)$

$H \subset KH$.

~~i.e~~ H is subgroup of HK.

Now, $h \in H$ & $h_1k_1 \in HK$ for $h_1 \in H$ & $k_1 \in K$

$$h_1k_1h(h_1k_1)^{-1} = h_1k_1hk_1^{-1}h_1^{-1}$$

$$= h_1k_2h_2h_1^{-1} \qquad \because k_1hk_1^{-1} = k_2h_2 \in KH$$

$$= h_1k_2h_3 \qquad \therefore h_3 = h_2h_1^{-1} \in H.$$

$$\in HK$$

$\therefore (h_1k_1)H(h_1k_1)^{-1} \in HK. \quad \forall h_1k_1 \in HK$.

$\therefore H \Delta HK$.

* Definition :-

Let G be a group. For any $a, b \in G$ $aba^{-1}b^{-1}$ is called a commutator in G. The subgroup of G generated by the set of all commutators in G is called the commutator subgroup of G (or the derived group of G) and denoted by G'

$$G' = \{ a, b \in G \mid aba^{-1}b^{-1} \}$$

Theorem - Let G be a group and Let G' be the derived group of G Then

i) $G' \trianglelefteq G$

ii) $\frac{G}{G'}$ is abelian.

iii) If $H \trianglelefteq G$ then $\frac{G}{H}$ is abelian iff $G' \subset H$.

→ i) G' is clearly subgroup of G by definition of derived group.

To prove :- $G' \trianglelefteq G$

Let $x = aba^{-1}b^{-1} \in G'$, $a, b \in G$ any commutator in G.

Then

$$x^{-1} = (aba^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1}$$
$$= bab^{-1}a^{-1} \in G,$$

is also commutator.

moreover for any $g \in G$.

$$gxg^{-1} = g(aba^{-1}b^{-1})g^{-1}$$

$$= gaebea^{-1}eb^{-1}g^{-1} \quad (\because e \in G)$$

$$= ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} \quad (\because g^{-1}g = e)$$

$$= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})$$

$$= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G'$$

$\therefore gxg^{-1} \in G'$ for $x \in G'$

Now any element y in G' is a product of a finite number of commutators Say $y = x_1 \cdot x_2 \cdots x_n$ Where $x_1, x_2 \cdots x_n$ are commutators Then. for any $g \in G$.

$$gyg^{-1} = gx_1x_2 \cdots x_n g^{-1}$$

$= g x_1 e x_2 e \cdots e x_n g^{-1}$

$= g x_1 g^{-1} g x_2 g^{-1} g \cdots g^{-1} g x_n g^{-1}$

$g y g^{-1} = (g x_1 g^{-1})(g x_2 g^{-1})(g x_3 g^{-1}) \cdots (g x_n g^{-1}) \in G'$

$\therefore \quad G' \triangleleft G.$

Hence G' is a normal subgroup of G.

ii) To show that G/G' is abelian.

For $a, b \in G$.

Here $\frac{G}{G'} = \{ aG' \mid a \in G \}$

To prove $(aG')(bG') = (bG')(aG')$

$(aG')(bG')(aG')^{-1}(bG')^{-1} = (aG')(bG')(a^{-1}G')(b^{-1}G')$

$= (aba^{-1}b^{-1})G' = G'$

$\therefore \quad (aG')(bG')(aG')^{-1}(bG')^{-1} = G'$

multipling Right hand side by (bG')

$(aG')(bG')(aG')^{-1}(bG')^{-1}(bG') = (bG')G'$

$\therefore \quad (aG')(bG')(aG')^{-1} = (bG')$

$(aG')(bG') = (bG')(aG')$

$\therefore$ G/G' is abelian.

iii) Suppose G/H is abelian ~~then~~ & $H \triangleleft G$

for any $a, b \in G$. i.e $(aH)(bH) = (bH)(aH)$

Consider $x \in G'$ i.e $x = aba^{-1}b^{-1}$

$(aba^{-1}b^{-1})H = (aH)(bH)(a^{-1}H)(b^{-1}H)$

$= \underbrace{(aH)(bH)}(aH)^{-1}(bH)^{-1}$

$= (bH)(aH)(aH)^{-1}(bH)^{-1}$

$= (bH)\, H\, (bH)^{-1}$ $\qquad (\because (aH)(aH)^{-1} = H)$

$= (bH)(bH)^{-1}$

$= H.$

$\therefore (aba^{-1}b^{-1})H = H.$

i.e $xH = H$ iff $x \in H$.

$\therefore G' \subset H.$

Conversaly, suppose that $G' \subset H$.

i.e $x = aba^{-1}b^{-1} \in H$, $a, b \in G$

To prove G/H is abelian i.e $(aH)(bH) = (bH)(aH)$

$\therefore (aba^{-1}b^{-1})H = H.$

$\Rightarrow (aH)(bH)(a^{-1}H)(b^{-1}H) = H$

i.e $(aH)(bH)(aH)^{-1}(bH)^{-1} = H$

By Right ~~hand~~ Side multipling (bH)

$\therefore (aH)(bH)(aH)^{-1}(bH)^{-1}(bH) = H(bH)$

$\therefore (aH)(bH)(aH)^{-1}H = (bH)$

again multipling (aH) Right side.

$$(aH)(bH)(aH)^{-1}(aH) = (bH)(aH)$$

$$(aH)(bH)H = (bH)(aH)$$

$$\therefore (aH)(bH) = (bH)(aH).$$

e.g ① If $A < G$ and $B \triangle G$ then $A \cap B \triangle A$ & $AB < G$

$\rightarrow$ Suppose $A < G$ & $B \triangle G$.

$\Rightarrow A < G$ & $B < G$. (By def^n of normal)

obviously, $A \cap B < A$

$\therefore A \cap B$ is Subgroup of A

We show that $A \cap B \triangle A$.

Let $a \in A$, $x \in A \cap B \Rightarrow x \in A$ & $x \in B$

$axa^{-1} \in A$, $axa^{-1} \in B$. $(\because B \triangleleft G)$

Thus $\forall a \in A$ $\forall x \in A \cap B$.

$\Rightarrow$ $axa^{-1} \in A \cap B$

$\therefore$ $A \cap B \triangle A$

To prove :- $AB < G$

Let $e = e \cdot e \in AB$. $(e \in A, e \in B)$

$\therefore$ AB is nonempty.

Let $x, y \in AB$.

$x = a_1 b_1$ $y = a_2 b_2$. $a_1, a_2 \in A$, $b_1 b_2 \in B$

$x = a_1 b_1$ $y^{-1} = b_2^{-1} a_2^{-1}$

$\therefore$ $xy^{-1} = a_1 b_1 b_2^{-1} a_2^{-1}$

$= a_1 b_3 a_2^{-1}$ $(\because b_3 = b_1 b_2^{-1})$

$= a_1 b_4$ $(\because b_4 = b_3 a_2^{-1})$

$\therefore a_1 b_4 \in AB$ $a_1 \in A$, $b_4 \in B)$

$\therefore$ $xy^{-1} \in AB$.

$\therefore$ $\underline{AB < G}$

(2) Let N & M are normal subgroup of G such that $N \cap M = \{e\}$ then $nm = mn$ $\forall n \in N$ $\forall m \in M$

$\rightarrow$ If $n \in N$, $m \in M$

N and M are normal.

i.e $n^{-1} m^{-1} n \in M$ & $m^{-1} n m \in N$.

$n^{-1} m^{-1} n m = (n^{-1} m^{-1} n) m$

$= MM \in M$.

& also

$n^{-1} m^{-1} n m = n^{-1} (m^{-1} n m) \in NN \in N$.

Scanned by CamScanner

$n^{-1}m^{-1}nm \in N \cap M = \{e\}$

$\Rightarrow n^{-1}m^{-1}nm = e.$

$\Rightarrow (mn)^{-1}nm = e.$

multipling (mn) by left side.

$(mn)(mn)^{-1}nm = (mn)e.$

$\Rightarrow nm = mn \quad \forall n \in N, \forall m \in M$

③ If G is a group and H is a subgroup of index 2 in G then H is normal subgroup of G.

→ If $a \notin H$ then by hypothesis, $G = H \cup aH$ & $aH \cap H = \phi$ Also $G = H \cup Ha$, $Ha \cap H = \phi$.
Thus $aH = Ha$, $a \notin H$.
But clearly, $aH = Ha \quad \forall a \in H$.
Hence $\forall g \in G$. $gH = Hg \Rightarrow gHg^{-1} = H \quad \forall g \in G$.
proving that H is normal in G.

④ Give an example of a group G having subgroups K & T such that $K \triangle T \triangle G$ but K is not a normal subgroup of G.

→ Let G be the octic group $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$

$\sigma^4 = e = \tau^2 \quad \& \quad \tau\sigma = \sigma^3\tau$

Chose $T = \{e, \sigma^2, \tau, \sigma^2\tau\}$ & $K = \{e, \tau\}$
Clearly, From the defining relations of the octic group. T & K are subgroups
Since The index of T is 2, $T \triangle G$.
Also K as a subgroup of T has index 2
& Thus $K \triangle T$

· However K is not normal in G because if we choose $\sigma \in G$ & $\tau \in K$

then $\sigma^{-1}\tau\sigma = \sigma^{-1}\sigma^{3}\tau = \sigma^{2}\tau \notin K$.

$\therefore K \ntrianglelefteq G$.

(5) If G is a group with center $Z(G)$ & if $\frac{G}{Z(G)}$ is cyclic then G must be abelian

→ Let $\frac{G}{Z(G)}$ be generated by $xZ(G)$, $x \in G$.

i.e $\frac{G}{Z(G)} = \{ xZ(G) \mid x \in G \}$

Let $a, b \in G$ then $aZ(G)$ is an element of $\frac{G}{Z(G)}$ must be of the form $x^{m}Z(G)$, $m \in \mathbb{Z}$

i.e $aZ(G) = x^{m}Z(G)$

Thus,

$a = x^{m}y$ for some $y \in Z(G)$

$b = x^{n}z$ for some $z \in Z(G)$ for some n

So that

$ab = (x^{m}y)(x^{n}z)$

$= x^{m} \cdot x^{n} yz = x^{m+n} yz$ — (1) $y \in Z(G)$

& $ba = (x^{n}z)(x^{m}y)$

$= x^{n} \cdot x^{m} zy = x^{m+n} zy$ — (2) $z \in Z(G)$

Hence by (1) & (2) we get

$ab = ba \quad \forall a, b \in G$

$\therefore G$ must be abelian.

Homework

e.g ⑤ If N & M are normal subgroup of G prove that NM is also a normal subgroup of G

→ We know that $N \Delta G$ & $M \Delta G$.

i.e $N < G$ & $M < G$.

and for any $g \in G$

$gng^{-1} \in N$ for $n \in N$ & $gmg^{-1} \subset M$ for $m \in M$

Then show that $NM \Delta G$.

We obiviously say $NM < G$.

for any $g \in G$. & $nm \in NM$, $n \in N$, $m \in M$

$$\begin{aligned} gnmg^{-1} &= gnemg^{-1} \\ &= gng^{-1}gmg^{-1} \quad (\because g^{-1}g = e) \\ &= (gng^{-1})(gmg^{-1}) \in NM \quad \cancel{\text{for } n \in N} \; (\because N \Delta G, M \Delta G) \end{aligned}$$

$\therefore$ $gnmg^{-1} \in NM$. for $nm \in NM$.

$\therefore$ $gNMg^{-1} \subset NM \quad \forall g \in G$.

$\therefore$ NM is normal in G

- Definition :-

Let G and H be group. A mapping $\phi : G \to H$ is said to be Isomorphism if it is one-one, onto and homomorphism

- Theorem - $\boxed{\text{First isomorphism Theorem}}$

Let $\phi : G \longrightarrow G'$ be a homomorphism of groups then $\frac{G}{\ker\phi} \cong Im(\phi)$

Hence In particular if ϕ is surjective then

$$\frac{G}{\ker\phi} \cong G'$$

proof - Let G, G' be groups with identity e and e' respectively and $\phi : G \to G'$ is a homomorphism then.

$$K = \ker\phi = \{ x \in G \mid \phi(x) = e' \}$$

& $\operatorname{Im}\phi = \{ x \in G \mid \phi(x) \}$ is subgroup of G'

& hence $\operatorname{Im}\phi$ is a group.

$\frac{G}{K} = \{ x \in G \mid xK \}$ is a group under coset multiplication

$(xK)(yK) = (xy)K \quad \forall x, y \in G$ with —(1)

identity K.

Define $\psi : \frac{G}{K} \to \operatorname{Im}\phi$. ~~defin~~ by,

$$\psi(xK) = \phi(x) \quad \forall x \in G. \quad —(2)$$

i) ψ is well defined & ~~one-one~~:-

Since $xK = yK$.

$\Leftrightarrow y^{-1}xK = K$

$\Leftrightarrow y^{-1}x \in K = \ker\phi$.

$\Leftrightarrow \phi(y^{-1}x) = e'$

$\Leftrightarrow \phi(y^{-1}) \cdot \phi(x) = e'$

$\Leftrightarrow \phi(x) [\phi(y)]^{-1} = e'$

$\Leftrightarrow \phi(x) = \phi(y)$

$\Leftrightarrow \psi(xK) = \psi(yK)$

$\therefore \psi$ is well defined.

ii) By (2) clearly ψ is onto.

iii) ψ is one-one:-

Since $\psi(xK) = \psi(yK) \quad x, y \in G$

$\Rightarrow \phi(x) = \phi(y)$

Scanned by CamScanner

Now

$$\phi(y^{-1}x) = \phi(y^{-1})\,\phi(x) \quad (\because \phi \text{ is homo.})$$

$$\Rightarrow \phi(y^{-1}x) = [\phi(y)]^{-1}\,\phi(x).$$

$$\Rightarrow \phi(y^{-1}x) = [\phi(x)]^{-1}\,\phi(x).$$

$$\Rightarrow \phi(y^{-1}x) = e'$$

$$\Rightarrow y^{-1}x \in \ker\phi.$$

i.e $\quad y^{-1}xK = K.$

$$\Rightarrow xK = yK \quad (\because y \cdot y^{-1} = e).$$

$\therefore$ ψ is one-one

iv) ψ is homomorphism :-

Since $\forall\, xK, yK \in G/K$

we have

$$\psi((xK)(yK)) = \psi((xy)K)$$
$$= \phi(xy)$$
$$= \phi(x)\cdot\phi(y) \quad (\because \phi \text{ is homo})$$

$$\therefore \psi((xK)\cdot(yK)) = \psi(xK)\cdot\psi(yK).$$

$\therefore$ ψ is homomorphism

Thus $\psi : \frac{G}{K} \to \mathrm{Im}\,\phi$ is a one-one, onto group homomorphism.

$$\therefore \frac{G}{K} \cong \mathrm{Im}\,\phi \quad \text{i.e} \quad \frac{G}{\ker\phi} \cong \mathrm{Im}\,\phi.$$

In particular ϕ is surjective map

So, $\mathrm{Im}(\phi) = G'$

$$\Rightarrow \frac{G}{\ker\phi} \cong G'$$

* Corollary – Any homomorphism $\phi : G \to G'$ of a groups can be factored as $\phi : j \circ \psi \circ \eta$ Where $\eta : G \to \frac{G}{\ker\phi}$ is the natural

homomorphism $\psi : \frac{G}{Ker\phi} \longrightarrow Im(\phi)$ is the isomorphism obtained in the theorem. & $j : Im\phi \longrightarrow G'$ is the inclusion map.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\eta"'] & G' \\ \frac{G}{Ker\phi} \arrow[r, "\psi"'] & Im\phi \arrow[u, "J"'] \end{tikzcd}$$

$\rightarrow$ Let $\phi : G \rightarrow G'$ is a group homomorphism with $Ker\phi \trianglelefteq G$.

and

$$\psi : \frac{G}{Ker\phi} \longrightarrow Im(\phi)$$

is given by $\psi(xKer\phi) = \phi(x) \quad \forall x \in G$.

is an onto isomorphism.

Let $J : Im(\phi) \longrightarrow G'$ is given by

$$J(y) = y \quad \forall y \in Im\phi.$$

i.e $J(\phi(x)) = \phi(x)$

and $\eta : G \longrightarrow \frac{G}{Ker\phi}$ is given by

$$\eta(x) = xKer\phi \quad \forall x \in G.$$

Here

$$j \circ \psi \circ \eta(x) = j \circ \psi(\eta(x)) \quad \forall x \in G.$$

$$= j(\psi(\eta(x)))$$

$$= j(\psi(xKer\phi))$$

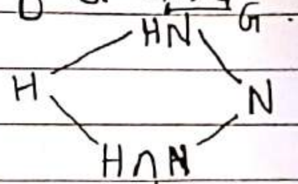
$$= j(\phi(x))$$

$$= \phi(x)$$

$\therefore \; j \circ \psi \circ \eta = \phi$.

* <u>Theorem</u> – [Second isomorphism Theorem].

Let H and N be subgroup of G and $N \trianglelefteq G$ Then $\dfrac{H}{H \cap N} \cong \dfrac{HN}{N}$.



proof:- Let H and N be subgroup of G and $N \trianglelefteq G$. As $HN = NH$ So HN is a subgroup of G Also $H \cap N$ is a subgroup of G.

$\dfrac{HN}{N} = \{ \cancel{x} \, x \in HN \,/\, xN \}$ is a quotient group under coset multiplication into identity N.

$\therefore (xN)(yN) = (xy)N \quad \because xy \in HN$.

Define a function $\phi : H \longrightarrow \dfrac{HN}{N}$ by

$\phi(h) = hN \quad \forall \, h \in H$ —— (1)

i) ϕ is homomorphism :-

~~Let~~ $\cancel{\phi(h_1)} = \cancel{\phi(h_2)} \Rightarrow \cancel{h_1 N = h_2 N}$.

Since $\forall \, h, h' \in H$. we have.

$$\phi(hh') = (hh')N = (hN)(h'N)$$
$$= \phi(h) \cdot \phi(h')$$

ii) ϕ is onto :-

Let any $x \in \dfrac{HN}{N}$, $x \in HN$

Then $x = hn$ for Some $h \in H$, $n \in N$.

$xN = hnN = hN \quad (\because n \in N \subset G \Rightarrow nN = N)$

$xN = \phi(h) =$ domain of ϕ where $h \in H$

Thus, $\forall \, xN \in \dfrac{HN}{N} =$ Codomain of ϕ

$\therefore \phi : H \longrightarrow \dfrac{HN}{N}$ is a onto homomorphism

Scanned by CamScanner

Page No.
Date

iii) $\ker\phi = \left\{ h\in H \mid \phi(h) = N, \text{ identity of } \frac{HN}{N} \right\}$

$= \{ h\in H \mid hN = N \}$

$= \{ h\in H \mid h\in N \}$

$= \{ h \mid h\in H \ \& \ h\in N \} = H\cap N.$

Thus $\phi : H \longrightarrow \frac{HN}{N}$ is a onto homomorphism with $\ker\phi = H\cap N$.

By First isomorphism Theorem of group homomorphism we have

$$\frac{H}{\ker\phi} \cong \frac{HN}{N} \quad \text{i.e} \quad \frac{H}{H\cap N} \cong \frac{HN}{N}.$$

* **Theorem** :- [Third Isomorphism Theorem]

Let H and K be normal subgroup and $K\subset H$ Then

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Proof :- Let G be a group and $H\trianglelefteq G$, $K\trianglelefteq G$, $K\subseteq H$

$\therefore \frac{G}{H} = \{ xH \mid x\in G \}$ is the quotient group under coset multiplication. i.e $(xH)(yH) = (xy)H$ with identity H.

and $\frac{G}{K} = \{ xK \mid x\in G \}$ is the quotient group under coset multiplication $(xK)(yK) = (xy)K$. with identity K.

Define a function $\phi : \frac{G}{K} \longrightarrow \frac{G}{H}$ by

$\phi(xK) = xH \quad \forall\, xK\in G/K$

(1)

i) ϕ is well defined :-

Since $xK = yK$ for $x, y \in G$.

$\Rightarrow y^{-1}xK = y^{-1}yK$.

$\Rightarrow y^{-1}xK = K$ $[\because y^{-1}y = e]$

$\Rightarrow y^{-1}x \in K \subset H$

$\Rightarrow y^{-1}x \in H \Rightarrow y^{-1}xH = H$

$\Rightarrow yy^{-1}xH = yH$

$\Rightarrow xH = yH$ $[y \cdot y^{-1} = e]$

$\Rightarrow \phi(xK) = \phi(yK)$

$\therefore \phi$ is well defined.

ii) By eqn ① clearly ϕ is onto :-

iii) ϕ is a group homomorphism :-

Since $\forall\, xK, yK \in \frac{G}{K}$ we have

$$\phi((xK)\cdot(yK)) = \phi((xy)K)$$

$$= (xy)H$$

$$= (xH)(yH)$$

$$= \phi(xK)\phi(yK).$$

iv) $Ker\phi = \{xK \in G/K \mid \phi(xK) = H\}$

$= \{xK \mid xH = H\}$

$= \{xK \mid x \in H\} = H/K$.

Thus $\phi : \frac{G}{K} \longrightarrow \frac{G}{H}$ is an onto homomorphism with $ker\phi = H/K$.

$\therefore$ By First isomorphism theorem.

Then $\frac{G/K}{Ker\phi} \cong Im\left(\frac{G}{K}\right) = \frac{G}{H}$

$\therefore \frac{G/K}{H/K} \cong G/H$.

Scanned by CamScanner

Page No.
Date

* Theorem – Let G_1 & G_2 be groups and $N_1 \Delta G_1$ and $N_2 \Delta G_2$ Then $\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}$.

proof - Let G_1 and G_2 be groups with identity e_1 & e_2 respectively and $N_1 \Delta G_1$ & $N_2 \Delta G_2$.

$G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$ is a group under componentwise operation with identity (e_1, e_2)

for $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) \quad a_1, b_1 \in G_1 \text{ \& } a_2, b_2 \in G_2.$$

$\frac{G_1}{N_1} = \{xN_1 \mid x \in G_1\}$ is the quotient group under coset multiplication with identity N_1

& $\frac{G_2}{N_2} = \{yN_2 \mid y \in G_2\}$ is the quotient group under coset multiplication with identity N_2

$\therefore \frac{G_1}{N_1} \times \frac{G_2}{N_2} = \{(xN_1, yN_2) \mid x \in G_1, y \in G_2\}$ is a group under multiplication with identity (N_1, N_2)

$$(xN_1, yN_2)(aN_1, bN_2) = ((xN_1)(aN_1), (yN_2)(bN_2)) = (xaN_1, ybN_2)$$

$\forall x, a \in G_1$ & $y, b \in G_2$

Define a function $\phi : G_1 \times G_2 \longrightarrow \frac{G_1}{N_1} \times \frac{G_2}{N_2}$

given by,

Page No.
Date

$\phi(x,y) = (xN_1, yN_2)$ —— (1) $x \in G_1$, $y \in G_2$.

i) clearly ϕ is onto By eq^n (1)

ii) ϕ is a group homomorphism & Since $\forall (a_1,a_2),(b_1,b_2) \in G_1 \times G_2$ we have

$\phi(a_1,a_2) = (a_1N_1, a_2N_2)$

& $\phi(b_1,b_2) = (b_1N_1, b_2N_2)$.

$\therefore \phi((a_1,a_2)\cdot(b_1,b_2)) = \phi(a_1b_1, a_2b_2)$ $a_1,b_1 \in G_1$, $a_2,b_2 \in G_2$

$= (a_1b_1N_1, a_2b_2N_2)$.

$= (a_1N_1)(b_1N_2), (a_2N_2)(b_2N_2))$

$= (a_1N_1, a_2N_2)\cdot(b_1N_2, b_2N_2)$

$= \phi(a_1,a_2) \cdot \phi(b_1,b_2)$

iii) $\ker\phi = \{(x,y) \in G_1 \times G_2 \mid \phi(x,y) = (N_1,N_2)\}$.
N_1 is identity in $\frac{G_1}{N_1}$ & N_2 is identity in $\frac{G_2}{N_2}$

$= \{(x,y) \in G_1 \times G_2 \mid (xN_1, yN_2) = (N_1,N_2)\}$

$= \{(x,y) \in G_1 \times G_2 \mid xN_1 = N_1 \text{ \& } yN_2 = N_2\}$

$= \{(x,y) \mid x \in N_1 \text{ \& } y \in N_2\}$

$= N_1 \times N_2$

iv) ϕ is one-one -
Let $(a_1,b_1),(a_2,b_2) \in G_1 \times G_2$

Since $\phi(a_1, b_1) = \phi(a_2, b_2)$

$\Rightarrow (a_1N_1, b_1N_2) = (a_2N_1, b_2N_2)$

$\Rightarrow a_1N_1 = a_2N_1$ & $b_1N_2 = b_2N_2$

$\Rightarrow a_1 = a_2$ & $b_1 = b_2$

$\Rightarrow (a_1, b_1) = (a_2, b_2)$

Thus $\phi : G_1 \times G_2 \longrightarrow \frac{G_1}{N_1} \times \frac{G_2}{N_2}$ is an onto homomorphism with $\ker\phi = N_1 \times N_2$

$\therefore$ By first isomorphism Theorem

$$\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}$$

* Theorem – [Correspondence Theorem]

Let $\phi : G \longrightarrow G'$ be a homomorphism of a group G onto a group G'. Then the following are true.

i) $H < G \Rightarrow \phi(H) < G'$

ii) $H' < G' \Rightarrow \phi^{-1}(H') < G$

iii) $H \Delta G \Rightarrow \phi(H) \Delta G'$

iv) $H' \Delta G' \Rightarrow \phi^{-1}(H') \Delta G$

v) $H < G$ and $H \supset \ker\phi \Rightarrow H = \phi^{-1}(\phi(H))$

vi) The mapping $H \longmapsto \phi(H)$ is a one-one correspondence between the family of subgroup of G containing $\ker\phi$ and the family of subgroups of G' futhermore normal subgroups of G correspond to normal subgroup of G'

Page No.
Date

proof- Let G and G' be group of identities e, e' respectively and $\phi: G \longrightarrow G'$ is a homomorphism i.e $\phi(ab) = \phi(a) \cdot \phi(b)$ $\forall a, b \in G$. also we have $\phi(e) = e'$ & $\phi(a^{-1}) = [\phi(a)]^{-1} \forall a \in G$

i) Let $H < G$ then $\phi(H) = \{x \in H \mid \phi(x)\}$ is a nonempty Subset of G'
Consider any $a, b \in \phi(H)$ then
$a = \phi(x)$, $b = \phi(y)$ for some $x, y \in H$
We know that H is subgroup of G
$\Rightarrow xy^{-1} \in H$
Then $ab^{-1} = \phi(x)[\phi(y)]^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1})$
$\in \phi(H)$
$\forall xy^{-1} \in H$
$ab^{-1} \in \phi(H)$
$\therefore \phi(H)$ is subgroup of G.

ii) Let $H' < G' \Rightarrow e \in \phi^{-1}(H') = \{x \in G \mid \phi(x) \in H'\} \subseteq G$
Consider any $x, y \in \phi^{-1}(H')$ Then
$\phi(x), \phi(y) \in H'$,
$\phi(xy^{-1}) = \phi(x)[\phi(y)]^{-1} \in H'$
$\therefore \phi(xy^{-1}) \in H' \Rightarrow xy^{-1} \in \phi^{-1}(H')$
$\therefore \phi^{-1}(H')$ is Subgroup of G.

iii) Let $H \triangle G$ i.e $H < G$ & $ghg^{-1} \in H$ $\forall h \in H$ $\forall g \in G$ —— (1)
Now $H < G$ & $\phi: G \longrightarrow G'$ is the homomorphism so $\phi(H) < G'$ by (1)
Consider any $g' \in G' = \phi(G)$ $\forall h' \in \phi(H)$
$\therefore g' = \phi(g)$ $h' = \phi(h)$ for some $g \in G$ & $h \in H$.

Page No.
Date

$$g'h'g'^{-1} = \phi(g)\phi(h)\phi(g^{-1}) = \cancel{\phi(g)\phi(h)\phi(g}$$
$$= \phi(ghg^{-1}) \in \phi(H$$

$\therefore \phi(H) \Delta G'$

iv) Let $H' \Delta G'$ i.e $H' < G'$ & $g'h'g'^{-1} \in H'$ $\forall g' \in G', h' \in H'$
$\phi : G \to G'$ is a onto group homomorphism

$$\phi^{-1}(H') < \phi^{-1}(G') < G$$
$\therefore \phi^{-1}(H') < G$ By(ii)

Consider any $g \in G$, $h \in \phi^{-1}(H')$
Then $\phi(g) \in \phi(G) = G'$ $\phi(h) \in H'$
we have
$$\phi(g)\phi(h)[\phi(g)]^{-1} \in H'$$
$$\Rightarrow \phi(ghg^{-1}) \in H'$$
$$ghg^{-1} \in \phi^{-1}(H') \quad \forall g \in G \text{ \& } h \in \phi^{-1}(H')$$

$$\therefore g\phi^{-1}(H')g^{-1} \subset \phi^{-1}(H') \quad \forall g \in G$$

$$\Rightarrow \phi^{-1}(H') \Delta G$$

(v) Let $H < G$ and $\ker\phi \subseteq H$
Now $\forall h \in H \Rightarrow \phi(h) \in \phi(H)$
$\Rightarrow h \in \phi^{-1}(\phi(H))$
$\therefore H \subseteq \phi^{-1}(\phi(H))$ $\forall h \in H$ — (1)

Consider any
$x \in \phi^{-1}(\phi(H))$
$\Rightarrow \phi(x) \in \phi(H) = \{\phi(h) \mid h \in H\}$
$\phi(x) = \phi(h)$ for some $h \in H$
$\therefore \phi(x) =$

Scanned by CamScanner

Now

$\phi(xh^{-1}) = \phi(x)\phi(h^{-1}) = \phi(x)[\phi(x)]^{-1}$
$= e'$

$\Rightarrow xh^{-1} \in \ker\phi \subseteq H$

$\Rightarrow xh^{-1} \in H \quad \forall h \in H$

i.e $xH \subseteq H \Rightarrow x \subseteq H$.

$\therefore \phi^{-1}(\phi(H)) \subseteq H$ —(2)

By (1) & (2)

$H = \phi^{-1}(\phi(H))$.

vi) Let $\mathcal{S}$ be the collection of all subgroup of G containing $\ker\phi$

i.e $\mathcal{S} = \{H \mid H < G \ \& \ \ker\phi \subseteq H\}$ and $\mathcal{G}$ be the collection of all subgroup of G'

i.e $\mathcal{G} = \{H' \mid H' < G'\}$

Here $\phi : G \longrightarrow G'$ be an onto group homomorphism.

Define $F_1 : \mathcal{S} \longrightarrow \mathcal{G}$ by $F_1(H) = \phi(H) \ \forall H \in \mathcal{S}$

(1) F_1 is one-one -

Since $F_1(H_1) = F_1(H_2) \Rightarrow \phi(H_1) = \phi(H_2)$

$\therefore \Rightarrow \phi^{-1}(\phi(H_1)) = \phi^{-1}(\phi(H_2))$

$\Rightarrow H_1 = H_2$

$(\because H_i < G \ \& \ H_i \supseteq \ker\phi \ \forall i = 1, 2)$

(2) F_1 is onto -

Consider any $H' \in \mathcal{G}$ i.e $H' < G'$

Then $\phi^{-1}(H') < G$ and $\ker\phi \subseteq \phi^{-1}(H')$

$[x \in \ker\phi \Rightarrow \phi(x) = e' \in H' < G' \Rightarrow x \in G'$

i.e $x \in \phi^{-1}(H')$ i.e $\ker\phi \subseteq \phi^{-1}(H')]$

$\Rightarrow \phi^{-1}(H') \in \mathcal{S} =$ domain of F_1

& $F(\phi^{-1}(H')) = \phi(\phi^{-1}(H')) = H'$

Thus $\forall H' \in G$ = codomain of F

$\exists \phi^{-1}(H'') \in G$ = domain of F

$\therefore F_1(\phi^{-1}(H')) = H'$ $\therefore F_1$ is onto.

[consider any $y \in H' \subseteq G' = \phi(G)$
$y = F(x) \in H'$ $\forall x \in G$

$\Rightarrow x \in \phi^{-1}(H')$

$\Rightarrow y = F(x) \in \phi(\phi^{-1}(H))$]

By eq^n(iii) $H \Delta G \Rightarrow \phi(H) \Delta G'$.

* **Corollary** -
Let N be a normal subgroup of G any subgroup H' of $\frac{G}{N}$ there is a unique subgroup N of H of G such that $H' = \frac{H}{N}$ Further $H \Delta G$ iff

$$\frac{H}{N} \Delta \frac{G}{N}$$

Proof - Let G be a group and $N \Delta G$ then

$\frac{G}{N} = \{xN \mid x \in G\}$ is a quotient group under coset multiplication $(xN)\cdot(yN) = (xy)N$ $\forall x, y \in G$ with identity N.

The natural homomorphism
$F: G \longrightarrow G/N$ defined by
$F(x) = xN$ $\forall x \in G$
is onto with $\ker(F) = N$.

i) F is homomorphism –

Since $x, y \in G \Rightarrow xy \in G$.

$F(xy) = (xy)N$

$= (xN) \cdot (yN)$

$= F(x) \cdot F(y)$.

ii) $\ker F = \{x \in G \mid F(x) = N$ identity in $G/N\}$

$= \{x \in G \mid xN = x\}$

$= \{x \in G \mid x \in N\} = N$.

$\therefore \ker F = N$.

By correspondance Theorem.

one-one correspondance between subgroup of G containing $N = \ker F$ & subgroup of G/N. then

$\forall H' \in \frac{G}{N}$ $\exists$ unique subgroup H of G

Such that $H' = F(H) = \{F(x) \mid x \in H\}$

$= \{xN \mid x \in H\}$

$F(H) = H' = \frac{H}{N}$.

Moreover $H \Delta G$ iff $F(H) \Delta F(G)$

$\Rightarrow \frac{H}{N} \Delta \frac{G}{N}$.

* Def^n – Let G be a group. A normal subgroup N of G is called maximal normal subgroup if

i) $N \neq G$

ii) $H \Delta G$ & $H \supset N \Rightarrow H = N$ or $H = G$.

Date

Def^n -

A group G is said to be simple if G has no proper normal subgroups i.e G has no normal subgroup except $\{e\}$ and G.

* Corollary -

Let N be a proper normal subgroup of G then N is a maximal normal subgroup of G iff $\frac{G}{N}$ is simple

→ [$N \Delta G$ i.e i) $N \neq G$ and

ii) $H \Delta G$ & $H \supset N$.

$\Rightarrow H = N$ or $H = G$.

$\frac{H}{N} = N$. or $\frac{H}{N} = \frac{G}{N}$.

$\Rightarrow \frac{G}{N} = \{N\}$ or $\frac{G}{N} = \frac{H}{N}$ $\because N \Delta H$.]

* Corollary -

Let H & k be distinct maximal normal subgroups of G then $H \cap k$ is a maximal normal subgroup of H and also k

→ Let H, k be a maximal normal subgroup of G Then $H \cap k$, Hk are normal subgroup of G

& $k \Delta Hk \Delta G$

As we know k is maximal normal subgroup So, $Hk = k$ or $Hk = G$.

Suppose $Hk = k$

Then $\forall h \in H \Rightarrow h = he \in Hk = k$

$\Rightarrow h \in k$

$\Rightarrow H \leq k \Rightarrow H = k$

our Assumation is wrong
Hence $HK = G$.
By Second isomorphism theorem.
$$\frac{H}{H \cap K} \cong \frac{HK}{K} = \frac{G}{K}.$$
As K is a maximal normal subgroup of G.
$\Rightarrow \frac{G}{K}$ as a simple group.
$\Rightarrow \frac{H}{H \cap K}$ is a simple group
$\Rightarrow H \cap K$ is a maximal subgroup of H.
Similarly, $H \cap K$ is maximal subgroup of K.

Example ① Let G be a group such that for some fixed integer $n > 1$ $(ab)^n = a^n \cdot b^n$ $\forall a, b \in G$.
Let $G_n = \{a \in G \mid a^n = e\}$ & $G^n = \{a^n \mid a \in G\}$
Then
$$G_n \Delta G,\ G^n \Delta G \ \& \ \frac{G}{G_n} \cong G^n.$$

Sol^n – Let G be a group with identity e and integer $n > 1$ such that $(ab)^n = a^n \cdot b^n$ $\forall a, b \in G$
Then
$G_n = \{a \in G \mid a^n = e\}$ & $G^n = \{a^n \mid a \in G\}$ are not subset of G $(e \in G_n,\ e \in G^n)$.

i) To prove $G_n \Delta G$:-
Consider any $a, b \in G_n$
then $a^n = e$, $b^n = e$ & $(b^{-1})^n = (b^n)^{-1} = e^{-1} = e$.
Now $ab^{-1} \in G$
$$(ab^{-1})^n = a^n (b^{-1})^n = e \cdot (b^n)^{-1} = e \cdot e = e.$$
$\therefore$ $ab^{-1} \in G_n$

Scanned by CamScanner

$\therefore G_n < G$

Consider any $g \in G$ & $a \in G_n$ i.e $a^n = e$.

Then

$$(gag^{-1})^n = g^n \cdot a^n (g^{-1})^n \quad (\because a^n = e)$$
$$= g^n \cdot g^{-n}$$
$$= e.$$

$\therefore gag^{-1} \in G_n \quad \forall a \in G_n \; g \in G.$

$\therefore g G_n g^{-1} \subset G_n \quad \forall g \in G$

$\Rightarrow G_n \triangleleft G.$

ii) To prove $G^n \triangleleft G$:

Let $e \in G \Rightarrow e^n \in G^n$.

$\therefore G^n$ is nonempty.

Consider any $x, y \in G^n$ then

$x = a^n, \; y = b^n$ for some $a, b \in G$

$\Rightarrow ab^{-1} \in G.$

$$\therefore xy^{-1} = a^n \cdot b^{-n} = a^n (b^{-1})^n$$
$$= (ab^{-1})^n$$

$\Rightarrow xy^{-1} \in G^n \quad \forall x, y \in G.$

Hence $G^n < G.$

Consider any $g \in G$ & any $x \in G^n$

i.e $x = a^n \; \forall a \in G$

Then

$$gxg^{-1} = g a^n g^{-1} = g \underbrace{a \cdots a}_{n \text{ time}} g^{-1}$$

Page No.

Date

$= gaega \cdots ag^{-1}$

$= ga\underbrace{(g^{-1}g)a(g^{-1}g) \cdots (g^{-1}g)}_{n\ times}ag^{-1} \quad (\because g^{-1}g = e)$

$= \underbrace{(gag^{-1})(gag^{-1}) \cdots (gag^{-1})}_{n\ times}$

$= (gag^{-1})^n \in G^n \quad \because gag^{-1} \in G$

$\therefore gxg^{-1} \in G^n \quad \forall x \in G^n, g \in G$

$\Rightarrow gG^ng^{-1} \subset G^n \quad \forall g \in G \quad \Rightarrow G^n \Delta G$

iii) $\frac{G}{G_n} \cong G^n$

Define a function $\phi : G \to G^n$ given by

$\phi(a) = a^n \quad \forall a \in G$

i) clearly, ϕ is onto.

ii) ϕ is a homomorphism:

Since $\forall a, b \in G$ we have

$\Rightarrow \phi(a) = a^n$ & $\phi(b) = b^n$

$\phi(ab) = (ab)^n$

$= a^n \cdot b^n$

$= \phi(a) \cdot \phi(b)$

$\therefore \phi$ is homomorphism.

iii) $\ker\phi = \{a \in G \mid \phi(a) = e\}$

$= \{a \in G \mid a^n = e\}$

$= G_n$

By First isomorphism Theorem.

$\frac{G}{\ker\phi} \cong G^n \Rightarrow$ i.e $\frac{G}{G_n} \cong G^n$.

(2) Let G be a finite group and let T be an Automorphism of G with the property that $T(x) = x$ iff $x = e$ prove that every $g \in G$ can be expressed as $g = x^{-1}T(x)$ for some $x \in G$.

Sol^n - Let G be a finite group with identity e and $T : G \to G$ be an automorphism i.e an onto isomorphism with the property.

$$T(x) = x \text{ iff } x = e$$

Define $F : G \longrightarrow G$ by $F(x) = x^{-1}T(x)$ $\forall x \in G$

i) F is one-one -

Since $F(x) = F(y)$ for $x, y \in G$.

$$\Rightarrow x^{-1}T(x) = y^{-1}T(y)$$

$$\Rightarrow yx^{-1}T(x) = yy^{-1}T(y)$$

$$\Rightarrow yx^{-1}T(x) = T(y) \quad (\because yy^{-1} = e)$$

$$\Rightarrow yx^{-1}T(x)[T(x)]^{-1} = T(y)[T(x)]^{-1}$$

$$\Rightarrow yx^{-1} = T(y)\,T(x^{-1}) \quad (\because T(x)[T(x)]^{-1} = e)$$

$$\Rightarrow yx^{-1} = T(yx^{-1})$$

$$\Leftrightarrow yx^{-1} = e \Rightarrow y = x \Rightarrow x = y$$

$\therefore F$ is one-one.

ii) $F : G \longrightarrow G$ is a one-one function and as G is finite set so F is onto also.

Page No.
Date

$$G = F(G) = \{x \in G \mid F(x)\}$$
$$= \{x \in G \mid x^{-1}T(x)\}.$$

Thus any $g \in G$ we have $g = x^{-1}T(x)$.

(3) Let G be a finite group and T be a automorphism of G with condition $T^2 = I$ & $T(x) = x$ iff $x = e$ prove that G is abelian

→ Let G be a finite group and $T : G \to G$ is an automorphism with property $T(x) = x$ iff $x = e$. then we have.

$$G = \{x^{-1}T(x) \mid x \in G\}$$

Also given $T^2 = I$ identity map on G.

$$\therefore T(x^{-1}T(x)) = T(x^{-1})\, T(T(x)) \quad (\because T \text{ is homo.})$$
$$= T(x^{-1})\, T^2(x)$$
$$= T(x^{-1})\, I(x) \quad (\because T^2 = I)$$
$$= T(x^{-1})x.$$
$$= \left[(T(x^{-1}) \cdot x)^{-1}\right]^{-1}$$
$$= \left[x^{-1}(T(x^{-1}))^{-1}\right]^{-1}$$
$$= \left[x^{-1}T((x^{-1})^{-1})\right]^{-1} = \left[x^{-1}T(x)\right]^{-1} \quad \forall x \in G$$

$$\therefore T(g) = g^{-1} \Rightarrow T(g^{-1}) = (g^{-1})^{-1} = g. \quad \forall g \in G$$

for any $a, b \in G$ we have

$$\to ab \in G$$
$$ab = T((ab)^{-1})$$
$$= T(b^{-1}a^{-1}) \quad (\because (ab)^{-1} = b^{-1}a^{-1})$$
$$= T(b^{-1}) \cdot T(a^{-1}) \quad (\because T \text{ is homo.})$$
$$\Rightarrow ab = ba \Rightarrow G \text{ is abelian}$$

* **Def^n - Automorphism :-**

Let G be a group. A mapping $\phi : G \to G$ which is a one-one, onto homomorphism i.e an onto isomorphism is called an Automorphism of G.

The set of all Automorphism of G is denoted by $Aut(G)$

$$Aut(G) = \{ \sigma \mid \sigma : G \to G \text{ is an onto isomorphism i.e Automorphism} \}$$

Example ① Let $I : G \to G$ given by $I(x) = x$ $\forall x \in G$ is an Automorphism of G

→ Consider $I : G \to G$ be an identity map defined by $I(x) = x$ $\forall x \in G$

The identity map is always one-one & onto.

Now, we check it is homomorphism

Since $\forall x, y \in G$. $I(x) = x$, $I(y) = y$

$\Rightarrow xy \in G$.

$\therefore I(xy) = x \cdot y$

$= I(x) \cdot I(y)$

$\therefore I$ is homomorphism.

Then I is an Automorphism of G

i.e $I \in Aut(G) \neq \phi$.

② Let G be a group for each fixed $g \in G$ such that ~~that~~ the function $I_g : G \to G$ given by $I_g(x) = gxg^{-1}$ $\forall x \in G$ is an

Automorphism of G.

→ Let G is a group $g \in G$ and

$I_g : G \longrightarrow G$ given by
$I_g(x) = gxg^{-1} \quad \forall\, x \in G$ —— (1)

i) I_g is one-one :- Since $x, y \in G$.
Since $I_g(x) = I_g(y)$

$\Rightarrow gxg^{-1} = gyg^{-1}$
pre multipling g^{-1} & post multipling g
we get

$\Rightarrow g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$
$\Rightarrow exe = eye$
$\Rightarrow x = y \qquad (\because g^{-1}g = e)$.

ii) To show onto :-
Consider any $z \in G$ = codomain of I_g
Then
$g^{-1}zg \in G$ = Domain of I_g

s.t. $I_g(g^{-1}zg) = g(g^{-1}zg)g^{-1}$

$= gg^{-1}z \cdot gg^{-1} = z \; (\because gg^{-1}=$
$I_g(g^{-1}zg) = z \in G$ codomain of I_g

$\therefore I_g : G \longrightarrow G$ is an onto mapping

iii) I_g is homomorphism :-
Since $\forall\, x, y \in G$
$I_g(x) = gxg^{-1}$ & $I_g(y) = gyg^{-1}$
we know $xy \in G$

$\therefore$ By ① $I_g(xy) = gxyg^{-1}$

$= gxeyg^{-1}$

$= gx(g^{-1}g)yg^{-1}$ $(\because g^{-1}g = e)$

$= (gxg^{-1})(gyg^{-1}) = I_g(x) \cdot I_g(y)$

Thus $I_g : G \to G$ is an one-one, onto homomorphism

i.e I_g is an Automorphism of G

$\Rightarrow I_g \in Aut(G) \quad \forall g \in G$.

Defn.- Inner Automorphism :-

Let G be a group for each fixed $g \in G$ such that the function $I_g : G \to G$ given by $I_g(x) = gxg^{-1} \quad \forall x \in G$ is an Automorphism of G. All such Automorphism are called inner Automorphism

The set of all inner Automorphism is denoted by $I_n(G)$ or $Inn(G)$

$Inn(G) = \{ I_g \mid g \in G \}$

Where $I_g : G \to G$ Such that

$I_g(x) = gxg^{-1} \quad \forall x \in G$.

④ Let G be a group. A mapping $f : G \to G$ given by $f(x) = x^{-1} \quad \forall x \in G$ is an Automorphism iff G is abelian

proof - Let G be a group and $F: G \to G$ is a function given by $F(x) = x^{-1}$ $\forall x \in G$.

① **F is one-one** -

Since $F(x) = F(y)$ $\forall x, y \in G$.

$\Rightarrow x^{-1} = y^{-1}$

$\Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1}$

$\Rightarrow x = y$

② **F is onto** :-

Since $\forall y \in G$ = codomain of F.

$\Rightarrow \underset{y^{-1} = x}{y^{-1}} \in G$

$\Rightarrow x = y^{-1} \in G$ = domain of F

$F(x) = F(y^{-1}) = (y^{-1})^{-1}$

$= y$ = codomain of F

$\Rightarrow$ Range of F = codomain of F.

$\therefore$ F is onto.

$\therefore$ F is an automorphism of G iff F is homomorphism

iff $F(ab) = F(a) \cdot F(b)$ $\forall a, b \in G$

iff $(ab)^{-1} = a^{-1} \cdot b^{-1}$

iff $(ab)^{-1} = (ba)^{-1}$

iff $(ab) = ba$ $\forall a, b \in G$

$\Leftrightarrow$ G is abelian.

Theorem -

The set $Aut(G)$ of all automorphism of a group G is a group under composition of mapping and $Inn(G) \trianglelefteq Aut(G)$

moreover $\frac{G}{Z(G)} \cong Inn(G)$.

proof- Let G be a group with identity e.

$$A(G) = \{ F \mid F : G \longrightarrow G \text{ is a bijection} \}$$

is permutation group of G under composition mapping with identity $I : G \longrightarrow G$.

&

$$Aut(G) = \{ 6 \mid 6 : G \longrightarrow G \text{ is an automorphi} \} \subseteq A(G).$$

consider any $f, g \in Aut(G)$

i) $f : G \to G$ & $g : G \to G$ are bijective function

$f \circ g : G \longrightarrow G$ is also a bijective function. moreover $x, y \in G$ we have.

$$(f \circ g)(xy) = f(g(xy))$$
$$= f(g(x) \cdot g(y)) \quad (\because g \text{ is homomorphism})$$
$$= f(g(x)) \cdot f(g(y)) \quad (\because f \text{ is homo.})$$
$$= (f \circ g)(x) \cdot (f \circ g)(y)$$

$\Rightarrow f \circ g$ is a homomorphism.

Thus $f \circ g : G \longrightarrow G$ is a one-one & onto homomorphism i.e $f \circ g$ is an automorphism

$$\therefore f \circ g \in Aut(G) \quad \forall f, g \in Aut(G)$$

ii) $f \in Aut(G)$ i.e $f : G \to G$ is a one-one onto then $f^{-1} : G \longrightarrow G$ exist and f^{-1} is also a one-one, onto function. Consider any function $x, y \in G$

Scanned by CamScanner

Then

$$f(f^{-1}(x)\cdot f^{-1}(y)) = f(f^{-1}(x))\cdot f(f^{-1}(y)) \quad (\because f \text{ is homo.})$$

$$= (f\circ f^{-1})(x)\cdot(f\circ f^{-1})(y)$$

$$= I(x)\cdot I(y)$$

$$= xy.$$

$$\Rightarrow f(f^{-1}(x)\cdot f^{-1}(y)) = xy.$$

$$\Rightarrow f^{-1}(xy) = f^{-1}(x)\cdot f^{-1}(y).$$

i.e f^{-1} is homomorphism.

$$\therefore f^{-1}\in Aut(G) \quad \forall f\in Aut(G).$$

Hence, $Aut(G)$ is a subgroup of $A(G)$.

$\therefore$ $Aut(G)$ is group under composition.

I) Now, we show that $Inn(G) \Delta Aut(G)$.

$$\because I_e \in Inn(G) \subseteq Aut(G).$$

$\therefore$ $Inn(G)$ is nonempty.

Consider any $I_a, I_b \in Inn(G)$ Where $a,b\in G$ $\forall x\in G$.

$$(I_a\circ I_b)(x) = I_a(I_b(x))$$

$$= I_a(bxb^{-1}) = a(bxb^{-1})a^{-1}$$

$$= abx(b^{-1}a^{-1})$$

$$= abx(ab)^{-1}$$

$$= I_{ab}(x) \quad \forall x\in G.$$

$$I_a\circ I_b = I_{ab}\in Inn(G).$$

II) For any $I_a\in Inn(G)$ we have. $I_{a^{-1}}\in In(G)$

$$I_a\circ I_{a^{-1}} = I_{a\cdot a^{-1}} = I_e \in Inn(G) \quad \forall I_a\in Inn(G)$$

Date

$$(I_a \circ I_{a^{-1}})(x) = I_a(I_{a^{-1}}(x))$$
$$= I_a(a^{-1}xa)$$
$$= aa^{-1}xaa^{-1} = I(x)$$
$$\Rightarrow I_a \circ I_{a^{-1}} = I_e.$$
$$I_{a^{-1}} = (I_a)^{-1} \in Inn(G)$$

$\therefore$ $Inn(G)$ is a subgroup of the group $Aut(G)$.

$$Inn(G) < Aut(G).$$

Consider any $\sigma \in Aut(G)$ & $I_g \in Inn(G)$.

Then

$$(\sigma \circ I_g \circ \sigma^{-1})(x) = \sigma(I_g(\sigma^{-1}(x))).$$
$$= \sigma(g(\sigma^{-1}(x))g^{-1})$$
$$= \sigma(g)\,\sigma(\sigma^{-1}(x))\,\sigma(g^{-1}) \quad (\because \sigma \text{ is homo.})$$
$$= \sigma(g)\cdot x\cdot[\sigma(g)]^{-1}$$
$$= I_{\sigma(g)}(x) \in Inn(G)$$

$\therefore$ $\sigma \circ I_g \circ \sigma^{-1} \in Inn(G)$

$\Rightarrow$ $\sigma \circ Inn(G) \circ \sigma^{-1} \subset Inn(G) \quad \forall \sigma \in Aut(G)$

$\therefore$ $Inn(G) \Delta Aut(G)$.

III) Define $\phi : G \longrightarrow Inn(G)$ given by
$$\phi(g) = I_g \quad \forall g \in G$$

i) clearly, ϕ is onto

Scanned by CamScanner

ii) ϕ is homomorphism :-

Let $a, b \in G \Rightarrow ab \in G \Rightarrow \phi(a) = I_a, \phi(b) = I_b$

$$\phi(ab) = I_{ab}$$
$$= I_a \circ I_b$$
$$= \phi(a) \circ \phi(b)$$

$\therefore$ ϕ is homomorphism

iii) $\ker\phi = \{a \in G \mid \phi(a) = I \text{ identity map}\}$.

$$= \{a \in G \mid I_a = I\}.$$
$$= \{a \in G \mid I_a(x) = I(x) \quad \forall x \in G\}$$
$$= \{a \mid axa^{-1} = x \quad \forall x \in G\}$$
$$= \{a \mid ax = xa \quad \forall x \in G\}$$
$$= Z(G)$$

Thus $\phi : G \longrightarrow Inn(G)$ is an onto homomorphism with $\ker\phi = Z(G)$.

$\therefore$ By First isomorphism Theorem.

$$\frac{G}{\ker\phi} \cong Inn(G) \Rightarrow \frac{G}{Z(G)} \cong Inn(G).$$

<u>Note</u>- If G is a finite cyclic group of order n. then the order of $Aut(G)$ the group of Automorphism of G is $\phi(n)$ where ϕ is Euler's functions.

i.e $|Aut(Z_n)| = \phi(n)$.

$$|Aut(Z_{20})| = \phi(20) = \phi(2 \times 10)$$
$$= \phi(2^2 \times 5) = 2(2-1)(5-1)$$
$$= 2.1.4 = \underline{\underline{8}}$$