UNIT - I

Group:

Definition:

Eg - 2:

Let $(Z, +)$ is a

Soln:

$H = N = \{1, 2, 3, \ldots\}$

$G = Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

i) Associative:

$1, 2, 3 \in H \subseteq G$

$(1+2)+3 = 1+(2+3)$

$6 = 6 \in H \subseteq G$

ii) Identity:

$3+0 = 0+3 = 3$

$0 \notin H$

iii) Inverse:

$4 + (-4) = 0 \notin H$

$\therefore (N, +)$ is not a subgroup of $(Z, +)$.

Theorem 3.15:

Proof:

i) Let e' & e'' be the identity of element of H & G respectively.

$a \in H \subseteq G$ identity property

$ae' = e'a = a \rightarrow (1)$

$ae'' = e''a = a \rightarrow (2)$

From (1) & (2)

$ae' = e''a$

$e' = e''$

(ii) a' & a'' are the inverse of a in G respectively.

$$aa' = a'a = e \quad \rightarrow (3)$$

$$aa'' = a''a = e \quad \rightarrow (4)$$

$$aa' = aa''$$

$$a' = a''$$

Theorem 3:16 :

proof :

Let H be a subgroup of G.

The resultant following immediately from theorem 3.15.

Theorem 3.17 :

proof :

Let H be a subgroup of G.

Then. $a, b \in H$

$$ab^{-1} \in H$$

$$ab^{-1} \in H$$

$$ab \in H \Rightarrow ab^{-1} \in H$$

Sufficient part :

Given $a, b \in H \Rightarrow ab^{-1} \in H$

To prove :

H is a subgroup of G

$$ab^{-1} \in H$$

$$a \in H$$

$$aa^{-1} \in H$$

$$aa^{-1} \in H$$

$$ea^{-1} \in H$$

$$e \in H$$

Identity

$ae \in H$

$ea^{-1} \in H \Rightarrow ea^{-1} \in H$

$\therefore a^{-1} \in H$

Inverse :

$a, b \in H$

$ab^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$

closure

$ab \in H$

$a, b \in H \Rightarrow ab \in H$

Theorem 3.18 :

Proof :

Let $a \in H$

$a \cdot a \in H$

$a^2 \in H$

$a \cdot a^2 \in H$

$a^3 \in H$

$\vdots$

$a^n \in H$

$a, a^2, a^3, \ldots a^n$ are all element of H.

$\therefore$ H is a finite

$\therefore$ $a, a^2, \ldots a^n$ are all element cannot distinct.

$\therefore a^r = a^s \in H$

(i.e.,) $e = a^s / a^r \in H \quad (r < s)$

$e = a^{s-r}$

$a^{s-r} = e \in H$

$\therefore e \in H$

Let $a^n = e$ for some n

$a^{n-1} = a^{-1} \in H$

$\therefore$ Thus H is subgroup of G.

$\therefore$ Hence proved.

Theorem 3.19 :

Proof :

H & K are subgroup of G.

To prove :

$H \cap K$ is a subgroup of G.

$\therefore$ H & K are subgroup.

$e \in H$ & $e \in K$

$\Rightarrow e \in H \cap K$

$\Rightarrow H \cap K \neq 0$

let $a, b \in H$

$a, b \in H$ & $a, b \in K$ $\therefore \{a, b \in H \cap K\}$

$ab^{-1} \in H$ & $ab^{-1} \in K$

$\Rightarrow ab^{-1} \in H \cap K$

By theorem : (3.17 theorem statement)

$\therefore$ $H \cap K$ is a subgroup of G.

Theorem - 3.20 :

Proof :

The N.P :

Given :

$H \subseteq K$ (or) $K \subset H$

To · prove :

HUK is a subgroup of G

$HUK = K$ (or) $HUK = H$ $\because$ { $H \leq K$ are subgroup of G }

$\therefore$ HUK is a subgroup of G.

The S·P :

Given :

HUK is a subgroup of G.

TO · prove :

$H \subseteq K$ (or) $K \subseteq H$

Assume the contradiction

$H \not\subseteq K$ and $K \not\subseteq H$

Let $a \in H$; $a \notin K$ and

$b \in K$; $b \notin H$ and

$\Rightarrow$ $a, b \in HUK$

$\Rightarrow$ $ab \in HUK$ { $\because$ HUK is a subgroup of G }

$\Rightarrow$ $ab \in H$ & $ab \in K$

case (i) :

$ab \in H$

$\therefore a \in H$

$a^{-1} \in H$ { H is a subgroup of G }

$a^{-1}(ab) \in H$ { $\because$ H is a closed }

$(a^{-1}a)b \in H$ { $\because$ associatative · pro }

$eb \in H$ { $\because$ identity }

$\therefore$ $b \in H$

which is not a contradiction $\{\because b \in H\}$

Case (ii) :

$ab \in K$

$\therefore b \in K$

$b^{-1} \in K$ $\{\because$ by the inverse property$\}$

$(ab)\,b^{-1} \in K$ $\{\because$ by closed$\}$

$a(bb^{-1}) \in K$ $\{\because$ associative property$\}$

$ae \in K$ $\{$identity$\}$

$\therefore a \in K$

which is contradiction not our assumption is wrong. Hence

$H \subseteq K$ (or) $K \subseteq H$

$\therefore$ Hence proved

Theorem - 3.21 :

Proof :

The N.P :

Given :

AB is a subgroup of G

To prove :

$AB = BA$

First to check $AB \subseteq BA$

Let $x \in AB$

$x^{-1} \in AB$ $\{\because$ AB is a subgroup of G$\}$

Let $x^{-1} = ab$; $a \in A$, $b \in B$

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

$x = b^{-1}a^{-1} \in BA$ {$a \in A$, $b \in B$, $A \& B$ are subgroup}

(i.e.,) $x \in ba$

Hence $AB \subseteq BA \rightarrow (1)$

Next to prove; $BA \subseteq AB$

Let $x \in BA$

$x = ba$; $b \in B$, $a \in A$

$(x^{-1})^{-1} = (ba)^{-1}$ ($\because a \in A$, $b \in B$, $A \& B$ are subgroup) $\Leftarrow$

$x = a^{-1}b^{-1} \in AB$

(i.e;) $x^{-1} \in AB$

$\therefore x \in AB$ (AB is a subgroup)

Hence $BA \subseteq AB \rightarrow (2)$

From (1) & (2)

$AB = BA$

The S.P:

Given:

$AB = BA$

To prove:

AB is a subgroup of G

Let $x, y \in AB$

$xy^{-1} \in AB$

Let $x = a_1 b_1$; $a_1 \in A$, $b_1 \in B$

$y = a_2 b_2$; $a_2 \in A$, $b_2 \in B$

$xy^{-1} = (a_1 b_1)(a_2 b_2)^{-1}$

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

Now $b_2^{-1} a_2^{-1} \in BA$ (since $AB = BA$)

$\therefore b_2^{-1} a_2^{-1} \in AB$

Again,

$b_2^{-1} a_2^{-1} = a_3 b_3$ ($a_3 \in A$, $b_3 \in B$)

$xy^{-1} = a_1 b_1 a_3 b_3$

Now $b_1 a_3 \in BA$ (since $AB = BA$)

$\therefore b_1 a_3 \in AB$

$\Rightarrow b_1 a_3 \in BA$

$\therefore b_1 a_3 = a_4 b_4$

$xy^{-1} = a_1 (a_4 b_4) a_3$

$= (a_1 a_4)(b_4 b_3)$

$xy^{-1} \in AB$

By theorem : 3.1T

AB is a subgroup of G

$\therefore$ Hence proved.

Problem - 1 :-

Proof :

$a^0 \in H$

$e \in H$

$\Rightarrow H \neq 0$

let $x, y \in H$

$x = a^s$; $y = a^t$; $s, t \in Z$

$xy^{-1} = a^s (a^t)^{-1}$

$= a^s a^{-t}$

$xy^{-1} = a^{s-t}$

(i.e;) $xy^{-1} \in H$

By theorem 3.17

H is a subgroup.

Theorem - 3.22 :

Proof :

Let G be a cyclic group generated by a.

(i.e;) $G = \langle a \rangle$

$= \{a^n / n \in z\}$

Let $x, y \in G$

$x = a^r, y = a^s$

$xy = a^r \cdot a^s$

$= a^{r+s}$

$= a^{s+r}$ $(\because s+r \in z)$

$= a^s \cdot a^r$

$= yx$ $\{\because xy = yx\}$

$\therefore$ G is a abelian.

Theorem - 3.23 :

Proof :

"G" be a cyclic group generated by "a"

(i.e;) $G = \langle a \rangle$

$= \{a^n / n \in z\}$

Let H be a subgroup of G

$\Rightarrow H \leq G$

$H = \{a^n / n \in Z\}$

Let m be the least +ve integer. $a^m \in H$

Claim :-

a^m is the generator of H.

Let $b \in H$

$\Rightarrow b = a^n$

Let $n = mq + r$; $0 < r < m$

now, $b = a^n$

$= a^{mq+r}$

$a^r = ba^{-mq}$

$= b(a^m)^{-q}$

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

$\Rightarrow b(a^m)^{-q} \in H$

$\therefore b \in H$

$a^r \in H$, $0 < r < m$

which is $\Rightarrow \Leftarrow$ to the assumption that "m", is the least +ve integer

$\therefore r = 0$

$\Rightarrow b = a^{mq}$

$= (a^m)^q$

Every element of H is some power of a^m.

(a) a^m is the generator of G.

$\therefore H$ is cyclic

$\therefore$ Hence proved.

Theorem - 3.24

Proof :

Case (i) :

Order is finite

Let a be an element of G of order "n".

$\therefore$ By definition

"n" be the least +ve integer $\ni : a^n = e$

G is the cyclic group generated by "a".

$\Rightarrow G = \langle a \rangle$

$G = \{ a^n / n \in Z \}$

$\therefore a^0, a^1, a^2, \ldots a^n$ are all element of G.

Claim :

$e, a, a^1, a^2 \ldots a^{n-1}$ are all distinct.

Suppose $a^r = a^s$

$\Rightarrow e = a^{s-r}$

which is $\Rightarrow \Leftarrow$ to "n"

least +ve integer

$\therefore$ All element are distinct

(ie) $O(G) = n$

$\therefore$ Hence $O(a) = O(G)$

Case (ii) :

order is infinite

Let "a" is infinite order.

$\therefore$ If no $\pm$ve integer $n \ni : a^n = e$.

$\therefore G = \langle a \rangle$

The element $a, a^2, \ldots a^n$ are all distinct

$\therefore O(G)$ is infinite

Hence $o(a) = o(G)$

Theorem - 3.25

Proof:

Let G be a group and $a \in G$. Then, the order of "a" is the same as the order of the cyclic group generated by a.

Let G be a finite group

Let $a \in G$

To Prove:

o(a) is finite

Suppose order of "a" is finite

By result.

$\langle a \rangle$ is the cyclic subgroup of G. of infinite order.

which is $\Rightarrow \Leftarrow$ to "G" is finite.

$\therefore$ order of "a" is finite $\Rightarrow \Leftarrow$

Theorem - 3.26:

Proof:

Given:

"a" be an element of order n in G.

$\therefore$ By definition

"n" is a least +ve integer $\ni : a^n = e$

The N.P:

Given:

n/m

To prove:

$a^m = e$

$\therefore n/m$

$\Rightarrow m = nq \quad \{\because m/n = q\}$

Now, $a^m = a^{nq}$

$= (a^n)^q$

$= e^q$

(ie) $a^m = e^q$

The S.P:

Given:

$a^m = e$

To prove:

n/m

Suppose n/m

$\therefore m = nq + r$

Now $a^m = a^{nq+r}$

$= a^{nq} \cdot a^r \quad 0 < r < n$

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

$= a^n \cdot a^r$

$= e \cdot a^r$

(ie) $a^m = a^r$

$\Rightarrow a^r = e \quad 0 < r < n$

which is $\Rightarrow \in$ to "n" is least +ve integer

$\therefore r = 0$

$\Rightarrow m = nq$

$\therefore n/m$

$\therefore$ Hence Proved

Theorem - 3.27

Proof:

Let the order "a" is n. "n" be the least +ve integer $\ni : a^n = e$

Now,

$$(a^{-1})^n = (a^n)^{-1}$$
$$= e^{-1}$$
$$= e$$

(ie) $(a^{-1})^n = e$

To prove :-

"n" is the least +ve integer

Suppose $0 \leq m < n$ ∋ : $(a^{-1})^m = e$

$$(am)^{-1} = e$$
$$a^m = e^{-1}$$
$$a^m = e, \quad 0 < m \leq n$$

order of a is m.

which is $\Rightarrow \Leftarrow$

"n" is the least +ve integer

order of $a^{-1} = n$

Proof (ii) :

Let the order of "a" is "n".

(i.e.,) n be the least +ve integer ∋ :-

$a^n = e$

Claim :-

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

(ie) $b^{-1}ab = b^{-1}ab$

r=1 the value is the assume that is r = k

The result is true.

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

Now to prove $(b^{-1}ab)^{k+1} = b^{-1}a^{k+1}b$

$$(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$$

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

$$= (b^{-1}a^k)(bb^{-1})ab$$

$$= b^{-1}a^k e ab$$

$$= b^{-1}a^k ab$$

$$(b^{-1}ab)^{k+1} = b^{-1}a^{k+1}b.$$

∴ The result is true for $k+1$.

∴ The result is true for every +ve integer.

Now $(b^{-1}ab)^n = b^{-1}a^n b$

$$= b^{-1}eb$$

$$= b^{-1}b$$

$$= e$$

$$(b^{-1}ab)^n = e.$$

Next to check n is the least +ve integer

Suppose $0 \leq n \leq m$ ∋ 1.

$$(b^{-1}ab)^m = e$$

$$b^{-1}a^m b = e$$

$$(b^{-1}b)\,a^m = e$$

$$e \cdot a^m = e$$

$$a^m = e \qquad 0 \leq m \leq n$$

which is $\Rightarrow \Leftarrow$ to the order of "a" is n.

$$(b^{-1}ab)^n = e$$

(i.e.,) ∴ order of $b^{-1}ab = n$

∴ order of a = order $b^{-1}ab$

$\therefore$ order of ab = order of $a^{-1}(ab)a$

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

$= e(ba)$

$= ba$

$\therefore$ order of ab = order of ba

$\therefore$ Hence Proved

Theorem -3.28 :

Proof :

Given :

"a" be an ~~least~~ of G of order of "n".

"n" be the least +ve integer.

$a^n = e$

To prove :

order of $a^s = n/d$

let $n/d = k$, $s/d = l$

where "k" and "l" are relatively prime

$\Rightarrow n = kd$; $s = ld$

Now,

$(a^s)^k = a^{sk}$

$= a^{ldk}$

$= a^{ln}$

$= (a^n)^l$

$= e^l = e$

(i.e.,) $(as)^k = e$

If "m" is the +ve integer ∋ :

$(as)^m = l$

$a^{sm} = e$

n/sm, $\{a^n = e$ "n" is the least +ve$\}$

$\Rightarrow kd/ldm$

$\Rightarrow k/lm$

$\Rightarrow k/m$ { $\because k \& L$ are relatively primes

(i.e.) $k \times d$ }

(i.e.,) $k \leq m$

(i.e.,) "k" is the least +ve integer

$(a^s)^k = e$

(i.e.,) order of $a^s = k$.

(i.e.,) order of $a^s = n/d$.

Corollary - 1 :

Proof :

By the theorem

order of "a" = n

order of $a^s = n/d$

$\therefore n/d < n$

(i.e.,) order of $a^s <$ order of a.

Corollary - 2 :

Theorem 3.24 statement :

Corollary - 3 :

Theorem 3.28 statement.

Problem :

1. **proof :**

Given :

G is finite G contain even number of elements.

To Prove :

Atleast one element in G has order 2.

Let "a" be an element of G of order 2.

$a^2 = e$

$a \cdot a = e$

$a = ea^{-1}$

$a = a^{-1}$

It is enough to prove . F on element different

from e in G whose inverse is itself suppose:-

$S = \{a / a \in G ; a \neq a^{-1}\}$

clearly, $a \in S$, $a^{-1} \in S$ & $a \neq a^{-1}$

$\Rightarrow$ S contains an even numbers of element

$e \in G$ has own inverse

$\Rightarrow e \notin S$.

$S \cup \{e\}$ contains an odd number of element.

$\therefore$ The atleast one element $a \notin S \setminus \{e\}$

(i.e) $a = a^{-1}$

(i.e) order of 'a' is 2.

3. Proof : Result 3.25

In a finite group every element is a finite order.

Given :

"a" be the greater of the cyclic group G.

(ie) $G = \langle a \rangle$

$\ni m \neq n \ni : a^m = a^n$

To prove :

G is a finite group

$\therefore m \neq n$

$\Rightarrow m > n$ (or) $n > m$

If $m > n$

Now, $a^m = a^n \Rightarrow a^m - a^n = e$

$\therefore a^{m-n} = e$

Let $m - n = k$ is +ve integer

$\{\because m > n \ m$ is +ve$\}$

(ie) $a^k = e$

$\Rightarrow$ order of a finite

$\therefore G = \langle a \rangle$

$\therefore$ By result

$\therefore$ G is a finite group.

Theorem - 3.29

(i) $a \in H \Leftrightarrow aH = H$

Proof :

The N.P :

Given :

$a \in H$

To prove :

$aH = H$

(ie) $aH \subseteq H$ (or) $H \subseteq aH$

(First to prove :-

$aH \subseteq H$

$x \in aH$

$\therefore x = ah$ (left coset) for some $h \in H$

$a \in H$ & $h \in H$

$\Rightarrow ah \in H$ { $\because$ by closed property }

(ie) $x \in H$

$aH \subseteq H \rightarrow (1)$

Next to prove :-

$H \subseteq aH$

Let $x \in H$

$x = ex$

$= aa^{-1}x$

$= a(a^{-1}x) \in aH$ { $\because a^{-1} \in H, x \in H$

$x \in aH$

$H \subseteq aH \rightarrow (2)$

$\therefore \quad H = aH$

The S.P :

Given :

$aH = H$

To prove :

$a \in H$

$a = ae \in aH$

$a \in aH$

$\therefore (a \in H) \quad \langle aH = H \rangle$

) $aH = bH \Leftrightarrow a^{-1}b \in H$

The N.P :

Given :

$aH = bH$

To prove :

$a^{-1}b \in H$

Now, $aH = bH$

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

$eH = (a^{-1}b)H$

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

$\therefore a^{-1}b \in H$

The S.P :

Given :

$ab^{-1} \in H$

To prove :

$aH = bH$

Now,

$ab^{-1} \in H$

$(ab^{-1})H = H$ (by condition 1)

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

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

$\therefore aH = bH$

(iii) $a \in bH \iff a^{-1} \in Hb^{-1}$.

The N.P :

Given :

$a \in bH$

To. prove :

$a^{-1} \in Hb^{-1}$

Now $a \in bH$

{coset def} $a = bh$ for some $h \in H$

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

$= h^{-1} b^{-1} \in Hb^{-1}$

$\therefore a^{-1} \in Hb^{-1}$

$\therefore a^{-1} \in Hb^{-1}$.

the S.P :

Given :

$a^{-1} \in Hb^{-1}$

TO. prove :

$a \in bH$

$a^{-1} \in Hb^{-1}$

$a^{-1} = Hb^{-1}$ for some $h \in H$

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

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

$a = bh^{-1} \in bH$

$\therefore a \in bH$

(iv) $a \in bH \iff aH = bH$

the N.P :

Given :

$a \in bH$

TO. prove :

$aH = bH$

Now, $a \in bH$

$a = bh$, for some $h \in H$ $\rightarrow$ (1)

First to prove that $aH \subseteq bH$

Let $x \in aH$

$x \in aH_2$ for some $h_2 \in H$

$= (bh_1)h_2$ [$\because$ by condition (i)]

$= b(h_1 h_2)$

(ie) $x \in bH$

$\therefore aH \subseteq bH$ — (1)

Next to prove $bH \subseteq aH$

$x = bh_3$ for some $h_3 \in H$

$= (ah_1)^{-1} h_3$ [$\because a = bh \Rightarrow b = ah^{-1}$]

$= a(h_1^{-1} h_3) \in a$

(ie) $x \in aH$

$bH \subseteq aH$ — (2)

Hence $aH = bH$.

The S.P:

Given:

$aH = bH$

To prove:

$a \in bH$

Now,

$a = ae \in aH (= bH)$

(ie) $a \in bH$

Problem - 2 :-

Soln:

clearly $e \in H$ &

Hence H is non - empty

Let $\alpha, \beta \in H$

Then α & β fix the symbol.

Now,

β fixes the symbol 1.

$\Rightarrow$ β^{-1} fixes the symbol 1.

Hence $\alpha\beta^{-1}$ fixes the symbol 1.

Hence $\alpha\beta^{-1} \in H$

Thus H is a subgroup of S_n.

Problem - 3 :

Let $A, B \in H$

Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

$$A - B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$$

$$= \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in H$$

Hence H is a subgroup of G.

Theorem - 3.30 :

Proof :

(Sub - I)

Let aH & bH are any two left cosets of H.

Suppose of aH & bH are not disjoint

(i.e,) $aH \cap bH \neq 0$

To prove:

let $c \in aH \cap bH$ & $\therefore aH \cap bH \neq \phi$?

$\Rightarrow c \in aH$ & $c \in bH$ - by theorem 3.29

$\Rightarrow cH = aH$ & $cH = bH$

(i.e) $aH = bH$

$\therefore aH$ & bH are identical

(Sub - ii)

Let $a \in G$

$a = ae \in aH$

(i.e) every element of G is belongs to any one of the left co-set of H.

$\therefore$ union of left coset is G.

(Sub - iii)

Define $f : H \to aH$ by

$f(h) = ah$

Claim:

f is well-defined

$h_1 = h_2$

$ah_1 = ah_2$

$f(h_1) = f(h_2)$

$\therefore$ f is well defined

Claim:

f is 1-1 $\rightarrow$ (one-to-one)

$f(h_1) = f(h_2)$

$ah_1 = ah_2$

$h_1 = h_2$ (by left cancellation Law

$\therefore$ f is 1-1

Claim : f is onto

Let $ah \in aH$ for some $a \in H$ (ie) ah has a preimage h in H.

(ie) Every element of aH has a pre-image in H.

$\therefore f$ is onto

Hence f is a bijection

$\therefore$ Number of elements in aH = Number in H.

Note : 1

The collection of all left co-sets form a partician of the group proof of theorem 3.30.

Thm - 3.30

Note - 2 :

The result is true for right co-sets also.

Result :

[Another proof of thm 3.30]

Let H be a subgroup of G. Define relation in G as $a \sim b \Rightarrow ab^{-1} \in H$.

Claim :- $\sim$ is an equivalent relation.

(refer to book)

Theorem - 3.30

Result - 1 : Theorem 3.29 (left coset)

Result - 2 : Theorem 3.29 (right co-set)

Proof:

Let L & R be the left and Right cosets respectively.

Define. $f : L \to R$ by

$$f(aH) = Ha^{-1}$$

Claim:

f is well defined

$$aH = bH$$

$$a^{-1}b \in H \quad \{\because aH = bH \iff a^{-1}b \in H\}$$

$$a^{-1}b \in Hb^{-1}$$

$$Ha^{-1} = Hb^{-1} \quad \{\because a \in Hb = Ha = Hb\}$$

$$f(aH) = f(bH)$$

f is 1-1:

$$f(aH) = f(bH)$$

$$Ha^{-1} = Hb^{-1}$$

$$a^{-1} \in Hb^{-1} \quad \{\because Ha = Hb \Rightarrow a \in Hb\}$$

$$a^{-1} \in hb^{-1} \text{ for some } h \in H$$

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

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

$$= bh^{-1} \in bH$$

(ie) $a \in bH \quad \{\because a \in bH \iff aH = bH\}$

$$aH = bH$$

$\therefore f$ is 1-1

f is onto :-

Let $Ha \in R$

Ha has a pre-image $a^{-1}H$ in L.

(ie) Every element of R has a pre-image in L

$\therefore$ f is onto

Hence f is a bijection

$\therefore$ Number of element in L = Number of element in R.

Example :

In Z_8, $\oplus$, $H = \{0, 4\}$ is a subgroup.

$0+H = \{0, 4\} = H$

$1+H = \{1, 5\}$

$2+H = \{2, 6\}$

$3+H = \{3, 7\}$

$4+H = \{4, 0\} = H$

Number of left coset is 4.

$\therefore$ Index $= [Z_8 : H] = 4$.

Theorem - 3.32 : (Lagrange's Theorem)

Result : Theorem 3.30

Proof :

Let $O(H) = m$, $[G:H] = r$

$\therefore O(G) = n$

By condition (i) result

"r" left cosets are mutually disjoint

$\therefore$ By condition (iii) of result

Each left coset has 'm' element $\{\because O(H) = m\}$

$\therefore$ There are rm element in the left cosets

By condition (ii) of result

$rm = n \quad \{\because O(a) = n\}$

$\Rightarrow n/m = r$

$\Rightarrow m/n = .$ $\{\because O(H) = m,\ O(G) = n\}$

(i.e) Order of H divides order of G.