Prof. Jayanta Biswas:

- **Subgroups:-**

Let (G,o) be a group. Then $o: G\times G \to G$. Let H be a non-empty subset of G. H is said to be stable under 'o' if $\forall a,b \in H$, $aob \in H$. If H is stable then the restriction of 'o' to $H\times H$ is a mapping from $H\times H$ to H, and in this case, the restriction of 'o' to $H\times H$ is called the induced composition on H and we denote this induced composition to H by the same symbol 'o'.

- **Defn:-** Let (G,o) be a group and H be a non-empty subset of G. If (H,o) is a group under the induced composition, then (H,o) is called a subgroup of (G,o).

- **Example:-** (1) Clearly every group (G,o) is a subgroup of itself and $\{e\}$ is a subgroup of the group (G,o), where e is the identity element of G.

(G,o) is called improper subgroup of (G,o) and $\{e\}$ is called trivial subgroup of (G,o).

(2) $(\mathbb{Z},+)$ is a subgroup of the $(\mathbb{Q},+)$.

- **Theorem:-** Let H be a subgroup of a group G. Then
(i) the identity element of H is the identity element of G.
(ii) for $a \in H$, the inverse of a in H is same as the inverse of a in G.

Pf: (i) Let e_H & e_G be identity elements in H and G respectively. Let $h \in H$. Then $h \in G$. Also $e_H o h = h$ and $e_G o h = h$.
$\therefore e_H o h = e_G o h$ in G so that, by right cancellation law, $e_H = e_G$.

(ii) Let e be the identity element in G. Then e is the identity element in H also. Let $a \in H$. Then $a \in G$. Let a' and a'' be inverse of a in H and G respectively. Then
$aoa' = e = aoa''$. ~~This implies that $a' = a''$~~
$\therefore aoa' = aoa''$ in G. This implies that $a' = a''$, by left cancellation law.

• **Theorem:-** Let G be a group. A non-empty subset H of G is a subgroup of G iff (i) $\forall a,b \in H$, $a \circ b \in H$ (ii) $\forall a \in H$, $a^{-1} \in H$.

Pf:- Let H be a subgroup of G. Then H is a group and hence (i) & (ii) are satisfied.

Conversely let H is a non-empty subset of G satisfying (i) & (ii).

Condition (i) implies that H is closed under $\circ$.

Since $H \subseteq G$ and $\circ$ is associative in G, hence $\circ$ is associative in H.

Let $a \in H$. Then $a^{-1} \in H$ (by (ii)).

$\therefore a \circ a^{-1} = e$ (identity element) $\in H$ (by (i)).

Also, by (ii), $a^{-1} \in H$, $\forall a \in H$.

$\therefore H$ is a group so that H is a subgroup of G.

• **Theorem:-** Let G be a group. A non-empty subset H of G is a subgroup of G iff $\forall a,b \in H$, $a \circ b^{-1} \in H$.

Pf:- Let H be a subgroup of G. Then H is a group. Now for all $a, b \in H$, $a, b^{-1} \in H$. This implies that $a \circ b^{-1} \in H$, $\forall a, b \in H$.

Conversely, let H is a non-empty subset of G such that $a \circ b^{-1} \in H$, $\forall a, b \in H$.

Let $a \in H$. Then $a \circ a^{-1} = e \in H$.

Now, $\forall a \in H$, $e \circ a^{-1} = a^{-1} \in H$ ($\because e \in H$)

Now, $\forall a, b \in H$, $a, b^{-1} \in H$. This implies that $a \circ (b^{-1})^{-1} = a \circ b \in H$.

$\because H \subset G$ and $\circ$ is associative in G, hence $\circ$ is associative in H.

$\therefore H$ is a group so that H is a subgroup of G.

• **Theorem:-** Let G be a group.

(i) For any two subgroups H, K of G, $H \cap K$ is a subgroup of G.

(ii) Union of two subgroups of G may not be a subgroup of G.

Pf:- (i) Let e be the identity in G. Then $e \in H, K$ - so that $H \cap K \neq \emptyset$. clearly $H \cap K \subset G$.

Let $a, b \in H \cap K$ be arbitrary. Then $a, b \in H$ and $a, b \in K$.
$\therefore a \circ b^{-1} \in H$ and $a \circ b^{-1} \in K$ ($\because H, K$ are subgroups of G).
$\therefore a \circ b^{-1} \in H \cap K$. $\therefore H \cap K$ is a subgroup of G.

(ii) Consider the group $G = (\mathbb{Z}, +)$ and the subgroups $H = (2\mathbb{Z}, +)$, $K = (3\mathbb{Z}, +)$ of G.
Now $2 \in H \Rightarrow 2 \in H \cup K$ and $3 \in K \Rightarrow 3 \in H \cup K$.
But $2 + 3 = 5 \notin H, K$ so that $2 + 3 = 5 \notin H \cup K$.
$\therefore H \cup K$ is not a subgroup of G.

H.T. Problem:- Consider the group $GL(2, \mathbb{R})$ of all 2×2 real non-singular matrices under multiplication. Prove that $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R}) \mid \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1 \right\}$ is a subgroup of $GL(2, \mathbb{R})$.

Hints:- For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in H$, prove that $AB^{-1} \in H$.

- The centre of a group:- Let G be a group and $H = \{x \in G \mid xy = yx, \forall y \in G\}$. Clearly $H \subset G$.
Since $ey = y = ye$, $\forall y \in G$, hence $e \in H$ so that $H \neq \phi$.
Let $a, b \in H$ be arbitrary. Then $ay = ya$, $\forall y \in G$ —(1) and $by = yb$, $\forall y \in G$, i.e., $b^{-1}y = yb^{-1}$, $\forall y \in G$ —(2).
Now $(ab^{-1})y = a(b^{-1}y) = a(yb^{-1})$ (by (2)) $= (ay)b^{-1} = (ya)b^{-1}$ (by (1))
$= y(ab^{-1})$, $\forall y \in G$.
$\therefore ab^{-1} \in H$ so that H is a subgroup of G.
This subgroup of G is called the centre of G and is denoted by $Z(G)$.

- The centraliser of an element in a group:-
Let G be a group and let $a \in G$. Let $H = \{x \in G \mid xa = ax\}$.
Clearly $H \subseteq G$. Since $ea = a = ae$, hence $e \in H$ so that $H \neq \phi$. Let $x, y \in H$ be arbitrary. Then $xa = ax$ —(1) and $ya = ay$, i.e., $y^{-1}a = ay^{-1}$ —(2).
Now, $(xy^{-1})(a) = x(y^{-1}a) = x(ay^{-1})$ (by (2))
$= (xa)y^{-1} = (ax)y^{-1}$ (by (1))
$= a(xy^{-1})$
$\therefore xy^{-1} \in H$ so that H is a subgroup of G.
This subgroup is called the centraliser of the element a and is denoted by $C(a)$.

• **Cyclic subgroup generated by an element:-**

Let G be a group and $a \in G$. Let $H = \{a^n \mid n \in \mathbb{Z}\}$.
Clearly $H \subset G$. Clearly $a = a^1 \in H$ so that $H \neq \phi$.
Let $x = a^m, y = a^n \in H$ be arbitrary. Then $m, n \in \mathbb{Z}$.
Now, $xy^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n} \in H$ ($\because m-n \in \mathbb{Z}$)
$\therefore H$ is a subgroup of G.
This subgroup is called the cyclic subgroup of G generated by the element a and is denoted by $\langle a \rangle$.

• **Examples:-** ① Consider the Klein's 4 group $V = \{e, a, b, c\}$.

Then $\langle e \rangle = \{e^n \mid n \in \mathbb{Z}\} = \{e\}$.
$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{e, a\}$.

② Consider the group $(\mathbb{Z}_6, +)$.

Then $\langle \bar{0} \rangle = \{\bar{0}\}$
$\langle \bar{2} \rangle = \{m\bar{2} \mid m \in \mathbb{Z}\} = \{\bar{0}, \bar{2}, \bar{4}\}$.

• **Note:-** For a group G, if $G = \langle a \rangle$ for some $a \in G$, then G is called a cyclic group generated by a.

• **Cosets:-** Let G be a group, H be a subgroup of G and $a \in G$. The set $aH = \{ah \mid h \in H\}$ is called a left coset of H in G. Clearly $aH \subseteq G$.

• **Ex:-** Consider the group $(\mathbb{Z}, +)$ and the subgroup $(3\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$. Then for $1 \in \mathbb{Z}$, we have
$1 + 3\mathbb{Z} = \{3x + 1 \mid x \in \mathbb{Z}\}$.

• **Theorem:-** Let H be a subgroup of a group G. Then for $h \in H$, $hH = H$.

Pf:- $hH = \{hx \mid x \in H\} \subseteq H$, since $hx \in H, \forall x \in H$ ($\because h \in H$).
Now for all $x \in H$, $x = h(h^{-1}x) \in hH$, since $h^{-1}x \in H$ ($\because h \in H \Rightarrow h^{-1} \in H$).
$\therefore H \subseteq hH$. $\therefore hH = H$.

• **Note:-** From above theorem, we can say that H is a left coset of itself. Also, H can be expressed as $H = eH$, e being the identity element.

• **Theorem:-** Let H be a subgroup of a group G and $a \in G - H$. Then $aH \cap H = \phi$.

Pf:- If possible, let $aH \cap H \neq \phi$. Let $p \in aH \cap H$. Then $p \in aH$ and $p \in H$. Therefore $p = ah_1$, $p = h_2$ for some $h_1, h_2 \in H$.

$\therefore ah_1 = h_2$, i.e, $a = h_2h_1^{-1} \in H$ ($\because h_1, h_2 \in H \Rightarrow h_2h_1^{-1} \in H$), a contradiction ($\because a \in G - H$).
$\therefore aH \cap H = \phi$.

• **Theorem:-** Let H be a subgroup of a group G. Any two left cosets of H in G are either identical or they have no common element.

Pf:- Let aH and bH be any two left cosets of H in G. Then either $aH \cap bH \neq \phi$ or $aH \cap bH = \phi$.
Let $aH \cap bH \neq \phi$. Let $p \in aH \cap bH$. Then $p = ah_1 = bh_2$, for some $h_1, h_2 \in H$. Therefore $a = bh_2h_1^{-1}$ —(1) and $b = ah_1h_2^{-1}$ —(2)

Let $x \in aH$ be arbitrary. Then $x = ah_3$, for some $h_3 \in H$.
$\therefore x = b(h_2h_1^{-1}h_3)$ (by(1))
$\in bH$ ($\because h_1, h_2, h_3 \in H \Rightarrow h_2h_1^{-1}h_3 \in H$).
$\therefore aH \subseteq bH$.
Let $y \in bH$ be arbitrary. Then $y = bh_4$, for some $h_4 \in H$.
$\therefore y = a(h_1h_2^{-1}h_4)$ (by(2)).
$\in aH$ ($\because h_1, h_2, h_4 \in H \Rightarrow h_1h_2^{-1}h_4 \in H$)
$\therefore bH \subseteq aH$. Hence $aH = bH$.
$\therefore$ Either $aH = bH$ or $aH \cap bH = \phi$.

• **Theorem:-** Let H be a subgroup of a group G. Let $a, b \in G$. Then $aH = bH$ iff $a^{-1}b \in H$.

Pf:- Let $aH = bH$ —(1)
Now $a = ae \in aH = bH$. Therefore $a = bh_1$, for some $h_1 \in H$.
$\therefore a^{-1}b = h_1^{-1} \in H$.
Conversely let $a^{-1}b \in H$. Then $a^{-1}b = h_2$, for some $h_2 \in H$. —(1)
Let $x \in aH$ be arbitrary. Then, $x = ah_3$, for some $h_3 \in H$.
$\therefore x = b(h_2^{-1}h_3)$ (by(1))
$\in bH$ ($\because h_2, h_3 \in H \Rightarrow h_2^{-1}h_3 \in H$).
$\therefore aH \subseteq bH$.
Let $y \in bH$ be arbitrary. Then $y = bh_4$, for some $h_4 \in H$.
$\therefore y = a(h_2h_4)$ (by(1)).
$\in aH$ ($\because h_2, h_4 \in H \Rightarrow h_2h_4 \in H$)
$\therefore bH \subseteq aH$. $\therefore aH = bH$.

H.W. • **Problem:-** Let H be a subgroup of the group G and $a, b \in G$. Then $b \in aH$ iff $a^{-1}b \in H$.

⑥ • **Theorem**:- Any two left cosets of a subgroup H in a group G have the same cardinality.

[Two sets A and B are said to have the same cardinality if ∃ a bijective map $f: A \to B$]

Pf:- Let aH and bH be any two left cosets of H in G.
Define $f: aH \to bH$ by $f(ah) = bh$, $\forall h \in H$.
Now prove that f is injective and surjective.

• **Theorem [Lagrange]**:- The order of every subgroup of a finite group G is a divisor of the order of G.

Pf:- Let H be a subgroup of the finite group G.
Let $o(G) = n$. Then $o(H)$ is finite.

Since any two left cosets of H in G are either identical or they have no common element, we can consider the set S of all distinct left cosets of H in G.
∵ G is a finite group, hence S is a finite set.
Let $S = \{x_1H, x_2H, \cdots, x_mH\}$, where $x_iH \cap x_jH = \phi$, for $i, j = 1, 2, \cdots, m$ with $i \neq j$. ——— (1)
Then $G = \bigcup_{i=1}^{m} (x_iH)$. ——— (2)
Now all these left cosets in S, have the same cardinality.
Since H is a left coset of H in G, hence x_iH has $o(H)$ elements, for $i = 1, 2, \cdots, m$.
∴ From (1) & (2), we have $o(G) = m \cdot o(H)$
∴ $o(H)$ is a divisor of $o(G)$.

■ **Order of an element**:-
Let G be a group and $a \in G$. a is said to be of finite order if ∃ a positive integer n s.t. $a^n = e$. The order of a is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$.
If $o(a)$ is not finite, then a is said to be of infinite order.

• Example:- ① In the group $(Z_6, +)$, $o(\bar{1}) = 6$, $o(\bar{2}) = 3$, $o(\bar{3}) = 2$, $o(\bar{4}) = 3$, $o(\bar{5}) = 6$, $o(\bar{0}) = 1$.

② In the Klein's 4-group $V = \{e, a, b, c\}$, $o(a) = o(b) = o(c) = 2$.

③ In the group $(Z, +)$, the order of each non-zero element is infinite.

• Theorem:- Let a be an element of a group G. Then

(i) $o(a) = o(a^{-1})$, (ii) if $o(a) = n$ and $a^m = e$, then n divides m.

(iii) if $o(a) = n$, then $a, a^2, \cdots, a^n (= e)$ are distinct elements of G.

(iv) if $o(a)$ is infinite and p is a positive integer then $o(a^p)$ is infinite.

Pf:- (i) Case-I:- Let $o(a) = n$. Then $a^n = e$.

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

$\therefore o(a^{-1})$ is finite. Let $o(a^{-1}) = m$. Then clearly $m \leq n$.

Now $(a^{-1})^m = e \Rightarrow a^{-m} = e \Rightarrow (a^m)^{-1} = e \Rightarrow a^m = e^{-1} = e$

$\Rightarrow n \leq m$.

$\therefore n = m$, i.e., $o(a) = o(a^{-1})$.

Case-II:- Let $o(a)$ is infinite. If possible, let $o(a^{-1}) = n$.

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

$\therefore o(a)$ is finite, a contradiction.

$\therefore o(a^{-1})$ is infinite.

$\therefore o(a) = o(a^{-1})$.

(ii) Let $o(a) = n$ and $a^m = e$. Then $a^n = e$ and $n \leq m$.

Now, $\exists\ q \in \mathbb{N}$, $r \in \mathbb{N} \cup \{0\}$ s.t. $m = nq + r$ with $0 \leq r < n$.

Now $a^r = a^{m-nq} = a^m \cdot (a^n)^{-q} = e \cdot e^{-q} = e$.

$\therefore r = 0$, since $o(a) = n$ and $0 \leq r < n$.

$\therefore m = nq$, i.e., n divides m.

(iii) If possible, let $a^p = a^q$ with $p, q = 1, 2, \cdots, n$ with $p > q$.

Then $a^{p-q} = e$ and $0 < p - q < n$, a contradiction, since $o(a) = n$.

Hence the result.

(iv) If possible, let $\exists\ p \in \mathbb{N}$ s.t. $o(a^p) = n$. Then $(a^p)^n = e$

i.e., $a^{pn} = e$, i.e., $o(a)$ is finite, a contradiction.

Hence the result.

• **Theorem:-** Each element of a finite group is of finite order.

Pf:- Let G be a finite group and $a \in G$. Then $a, a^2, a^3, \ldots, a^n, \ldots$ all are elements of G. Since G is a finite group, all these elements cannot be distinct. Therefore, $\exists\ p, q \in \mathbb{N}$ with $p > q$ such that $a^p = a^q$. This implies that $a^{p-q} = e$. Therefore $o(a)$ is finite.
Hence the result.

• **Problem:-** If G be a finite group of even order, prove that G contains an odd number of elements of order 2.

Soln:- For any $a \in G$ we have $o(a) = o(a^{-1})$.
If $o(a) < 3$, then $a = a^{-1}$. If $o(a) \geq 3$, then $a \neq a^{-1}$.
Now consider $S = \{\{a, a^{-1}\} \mid a \in G, o(a) \geq 3\}$.
Then S contributes an even number to the number of elements of G. Also, S cannot exhaust all the elements of G because $e \in G$ and $o(e) = 1 < 3$.
Now removing the pairs of elements of S from G, clearly there are even number of elements in G, since $o(G)$ is even.
Now G has exactly one element e with $o(e) = 1$.
$\therefore$ G has an odd number of elements of order 2.

• **Problem:-** Let G be a group. Prove that $o(x) = o(yxy^{-1})$, $\forall\ x, y \in G$. Deduce that $o(ab) = o(ba)$, $\forall\ a, b \in G$.

Soln:- **Case-I:-** Let $o(x) = n$. Then $x^n = e$.
Now $(yxy^{-1})^n = yx^ny^{-1} = yey^{-1} = yy^{-1} = e$
$\therefore$ $o(yxy^{-1})$ is finite. Let $o(yxy^{-1}) = m$. Then $m \leq n$ and $(yxy^{-1})^m = e$.
Now $(yxy^{-1})^m = e \Rightarrow yx^my^{-1} = e \Rightarrow x^m = y^{-1}ey = y^{-1}y = e$
$\Rightarrow n \leq m$.
$\therefore$ $n = m$, i.e., $o(x) = o(yxy^{-1})$.
Case-II:- Let $o(x)$ is infinite. If possible, let $o(yxy^{-1}) = n$. Then $(yxy^{-1})^n = e \Rightarrow yx^ny^{-1} = e \Rightarrow x^n = y^{-1}ey = e$
$\Rightarrow o(x)$ is finite, a contradiction.
$\therefore$ $o(yxy^{-1})$ is infinite.
$\therefore$ $o(x) = o(yxy^{-1})$, $\forall\ x, y \in G$.

Now, $ab = a(ba)a^{-1}$,

Now, $o(ba) = o(a(ba)a^{-1})$

i.e., $o(ba) = o(ab)$

$\therefore o(ab) = o(ba)$, $\forall a, b \in G$.

• **Problem:-** If each element, except the identity, of a group be of order 2, prove that the group is abelian.

Soln:- Let G be a group satisfying the given condition.

Then, $\forall x (\neq e) \in G$, $o(x) = 2$.

$\therefore x^2 = e$, $\forall x (\neq e) \in G$.

$\therefore x = x^{-1}$, $\forall x \in G$ ($\because e = e^{-1}$ also) —— (1)

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

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

$= (ba)^{-1} = ba$ (by (1)).

$\therefore G$ is abelian.

• **Problem:-** In a group G, a and b are distinct elements of order 2. If a and b commute, prove that $o(ab) = 2$. If a and b do not commute, prove that $o(aba^{-1}) = 2$.

Soln:- $o(a) = 2$, $o(b) = 2$, $a \neq b$.

$\therefore a = a^{-1}$, $b = b^{-1}$, $a \neq b$ —— (1)

Let $ab = ba$.

Now, $ab = e \Rightarrow a = b^{-1} = b$ which is not the case.

$\therefore ab \neq e$ so that $o(ab) > 1$.

Now, $(ab)^2 = abab = a^2b^2$ ($\because ab = ba$)

$= ee = e$.

$\therefore o(ab) = 2$.

Let $ab \neq ba$.

Now, $aba^{-1} = e \Rightarrow b = a^{-1}ea = e$ which is not the case, since $o(b) = 2$.

$\therefore aba^{-1} \neq e$ so that $o(aba^{-1}) > 1$.

Now, $(aba^{-1})^2 = ab^2a^{-1} = aea^{-1} = e$.

$\therefore o(aba^{-1}) = 2$.

H.I. Problem:- (1) Find all elements of order 5 in the group $(\mathbb{Z}_{20}, +)$.

(2) Let G be a group and $a \in G$. Prove that $o(a) = o(xax^{-1})$, $\forall x \in G$. If a be the only element of order 2 in G, deduce that a commutes with every element of G.

(3) Let a, b be fixed positive integers and $H = \{an + by \mid n, y \in \mathbb{Z}\}$. Show that $(H, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

(4) G is an abelian group. Prove that $H = \{g \in G \mid g = g^{-1}\}$ is a subgroup of G.

• Problem:- Let G be an abelian group and n be a fixed positive integer. Prove that $H = \{a^n \mid a \in G\}$ is a subgroup of G.

Soln:- Clearly H is a non-empty subset of G.
Let $x, y \in H$ be arbitrary. Then $x = a^n$, $y = b^n$ for some $a, b \in G$. Now $xy^{-1} = a^n(b^n)^{-1} = a^n(b^{-1})^n = (ab^{-1})^n$ ($\because G$ is abelian) $\in H$ ($\because a, b \in G \Rightarrow ab^{-1} \in G$).
$\therefore H$ is a subgroup of G.

• Problem:- Let H be a subgroup of a group G and $g \in G$. Prove that $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G.

Soln:- Since H is a non-empty subset of G, hence gHg^{-1} is a non-empty subset of G.
Let $x, y \in gHg^{-1}$ be arbitrary. Then $x = gh_1g^{-1}$, $y = gh_2g^{-1}$, for some $h_1, h_2 \in H$.
Now $xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$
($\because h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$)
$\therefore gHg^{-1}$ is a subgroup of G.

• Note:- For a subgroup H of a group G, we can define right coset of H in G as: for $a \in G$, $Ha = \{ha \mid h \in H\}$.

Normal Subgroups:-

• Defn:- A subgroup H of a group G is said to be a normal subgroup of G if $aH = Ha$, $\forall a \in G$.

• Example:- (i) For a group G with identity element e, the subgroups G and $\{e\}$ are normal subgroups of G.
(ii) For the group $(\mathbb{Z}, +)$, the subgroup $(n\mathbb{Z}, +)$ is a normal subgroup of $(\mathbb{Z}, +)$, where $n \in \mathbb{N}$.

H.T. • Problem:- Prove that every subgroup of an abelian group G is a normal subgroup of G.

• Defn:- For a finite group G, if H be a subgroup of G, then the number of distinct left cosets of H in G is called the index of H in G, and is denoted by $[G : H]$.

• **Theorem:-** Let H be a subgroup of a group G and $[G:H]=2$. Then H is normal in G.

Pf:- Since $[G:H]=2$, hence H and $G-H$ are only the left cosets of H in G as well as the right cosets of H in G.
Let $a\in H$. Then $aH=H=Ha$ so that $aH=Ha$.
Let $a\in G-H$. Then $aH=G-H=Ha$ ($\because H\cap aH=\phi=H\cap Ha$).
$\therefore aH=Ha$.
$\therefore aH=Ha, \forall a\in G$ so that H is a normal subgroup of G.

• **Problem:-** Prove that the centre $Z(G)$ of a group G is a normal subgroup of G.
Soln:- $Z(G)$ is a subgroup of G (prove it). Let $H=Z(G)$, and $a\in G$ be arbitrary.
Let $p\in aH$ be arbitrary. Then $p=ah_1$, for some $h_1\in H=Z(G)$
$\therefore p=ah_1=h_1a\in Ha$. $\therefore aH\subseteq Ha$.
Let $q\in Ha$ be arbitrary. Then $q=h_2a$, for some $h_2\in H=Z(G)$
$\therefore q=ah_2\in aH$. $\therefore Ha\subseteq aH$.
$\therefore aH=Ha$. But $a\in G$ was arbitrary. $\therefore aH=Ha, \forall a\in G$.
$\therefore H$, i.e., $Z(G)$ is a normal subgroup of G.

• **Test for normality:-** Let H be a subgroup of a group G. Then H is normal in G iff $\forall h\in H, \forall x\in G, xhx^{-1}\in H$, i.e., iff $xHx^{-1}\subseteq H$, $\forall x\in G$.

• **Th:-** Intersection of two normal subgroups of a group G is normal in G.
Pf:- Let H and K be two normal subgroups of the group G.
Then $H\cap K$ is a subgroup of G ($\because$ intersection of two subgroups of a group is a subgroup of the group)
Let $x\in G$ be arbitrary ~~we shall show that~~ and $y\in H\cap K$ ~~$(\in H)$~~ be arbitrary. Then $y\in H$ and $y\in K$.
$\therefore xyx^{-1}\in H$ ($\because H$ is normal in G) and $xyx^{-1}\in K$ ($\because K$ is normal in G)
$\therefore xyx^{-1}\in H\cap K$.
$\therefore H\cap K$ is a normal subgroup of G.

■ **Quotient group:-** Let H be a normal subgroup of a group G. Then there is no difference between left cosets and right cosets of H in G.
Let G/H be the set of all distinct left cosets of H in G.
Define a binary operation $*$ on G/H by
$aH*bH=(ab)H, \forall aH, bH\in G/H$.

(12) We shall show that this binary operation $*$ is well-defined on G/H. Let $x_1H, x_2H, y_1H, y_2H \in G/H$ be arbitrary s.t. $x_1H = x_2H$ and $y_1H = y_2H$.
Then $x_1^{-1}x_2 \in H$ and $y_1^{-1}y_2 \in H$.
$\therefore x_1^{-1}x_2 = h_1$, $y_1^{-1}y_2 = h_2$, for some $h_1, h_2 \in H$.
Now, $(x_1y_1)^{-1}(x_2y_2) = y_1^{-1}(x_1^{-1}x_2)y_2 = y_1^{-1}h_1y_2 = (y_1^{-1}h_1y_1)(y_1^{-1}y_2)$
$= h_3h_2$, where $y_1^{-1}h_1y_1 = h_3 \in H$, as H is normal in G.
$\in H$.
$\therefore (x_1y_1)H = (x_2y_2)H$, i.e., $(x_1H)*(y_1H) = (x_2H)*(y_2H)$.
$\therefore *$ is well defined on G/H.
Now it can be easily verified that $(G/H, *)$ is a group. This group is called the quotient group of G by H with identity eH, i.e, H.

- Example:- ① Let $G = (\mathbb{Z}_6, +)$, $H = \{\bar{0}, \bar{3}\}$. Then H is a normal subgroup of G. Then $G/H = \{\bar{0}+H = H, \bar{1}+H, \bar{2}+H\}$.
② Let $G = (\mathbb{Z}, +)$, $H = (3\mathbb{Z}, +)$. Then H is a normal subgroup of G. Now $G/H = \{0+H = H, 1+H, 2+H\}$.

- Theorem:- If H be a subgroup of the commutative group G then the quotient group G/H is commutative, but not conversely.

Pf:- Since G is commutative, hence the subgroup H is a normal subgroup of G so that the quotient group G/H exists. Let $aH, bH \in G/H$ be arbitrary. Then $(aH)*(bH) = (ab)H = (ba)H$
$= (bH)*(aH)$ ($\because G$ is commutative)
$\therefore G/H$ is commutative.

To disprove the converse part, consider the non-commutative group S_3. Consider the alternating group A_3 which is a normal subgroup of S_3. Now, the quotient group S_3/A_3 is commutative ($\because S_3/A_3$ is a group of order 2), but S_3 is not commutative.

- Problem:- Let H be a subgroup of G and $[G:H] = 2$. Prove that for every $x \in G$, $x^2 \in H$.

Sol:- Since $[G:H] = 2$, hence H is normal in G so that the quotient group G/H exists and $G/H = \{H, G-H\}$ is a group of order 2. Therefore $(G-H)^2 = H$ ($\because H$ is the identity in G/H).
Let $x \in G$ be arbitrary. If $x \in H$, then $x^2 \in H$.
If $x \in G-H$, then $x^2 \in (G-H)^2 = H$.
$\therefore$ For every $x \in G$, $x^2 \in H$.

• **Problem:-** Let H be a subgroup of a group G such that every left coset of H is also a right coset of H in G. Prove that H is a normal subgroup of G.

Soln:- Let $a \in G$ be arbitrary. Then $aH = Hb$, for some $b \in G$.

Now, $a \in aH = Hb \Rightarrow a = hb$, for some $h \in H$ ——(1).

Again, $aH = Hb \Rightarrow aHa^{-1} = H(ba^{-1}) = H(bb^{-1}h^{-1})$ (by (1))

$= Hh^{-1} \subseteq H$ ($\because h \in H \Rightarrow Hh^{-1} \subseteq H$)

$\therefore aHa^{-1} \subseteq H, \forall a \in G$.

$\therefore H$ is a normal subgroup of G.

• **Problem:-** Let H be a subgroup of a group G such that the product of any two left cosets of H is a left coset of H in G. Prove that H is normal in G.

Soln:- Let $a, b \in G$ be arbitrary. Then $\exists\ c \in G$ such that $(aH)(bH) = cH$. This implies that $Hb = a^{-1}cH$ ——(1).

From (1), we get $b \in Hb = a^{-1}cH$. Therefore $b = a^{-1}ch$, for some $h \in H$. This implies that $bH = a^{-1}cH$ ——(2)

From (1) & (2), we get $bH = Hb$. But $b \in G$ was arbitrary.

$\therefore H$ is a normal in G.

• **Problem:-** Consider the group $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R}, ad \neq 0 \right\}$ under matrix multiplication. Let $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$. Prove that H is a normal subgroup of G.

Soln:- clearly H is a non-empty subset of G.

For any $A = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in H$, we have

$AB^{-1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix} \in H$ so that H is a subgroup of G.

Let $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ be arbitrary and $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in H$ be arbitrary.

Then $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \frac{1}{ad}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$ and

$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \frac{1}{ad}\begin{pmatrix} a & au+b \\ 0 & d \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \frac{1}{ad}\begin{pmatrix} ad & a^2u \\ 0 & ad \end{pmatrix}$

$= \begin{pmatrix} 1 & \frac{au}{d} \\ 0 & 1 \end{pmatrix} \in H$ ($\because ad \neq 0 \Rightarrow d \neq 0$).

$\therefore H$ is a normal subgroup of G.