Left Coset: Let G be a group and H be a subgroup of G. Let $a \in G$; then $\forall h \in H,\ a * h \in G$; the subset $\{a * h : h \in H\}$ is called a **left coset of H in G,** denoted by, $aH = \{ah : h \in H\}$.

In additive notation: $a + H = \{a + h : h \in H\}$

Example: Let, $G = (\mathbb{Z}, +)$ and $H = (3\mathbb{Z}, +)$

There are three distinct left cosets of H in G:

$0 + H = \{3n + 0 : n \in \mathbb{Z}\} = H$

$1 + H = \{3n + 1 : n \in \mathbb{Z}\}$

and, $2 + H = \{3n + 2 : n \in \mathbb{Z}\}$

Note: There are other left cosets, but they are not distinct as,
$3 + H = 0 + H,\ 4 + H = 1 + H,\ 5 + H = 2 + H$ etc.

Example: Let $G = (S_3, .)$ and $H = (A_3, .)$

There are two distinct left cosets : A_3 and $\rho_3 A_3 = \{\rho_3, \rho_4, \rho_5\}$.

Note: Other cosets are not distinct as, $\rho_4 A_3, \rho_5 A_3$ are equal to $\rho_3 A_3$.

Result: Let G be a group and H be a subgroup of G and $h \in H$, Then $hH = H$.

let $p \in hH \Rightarrow p = hh_1\ ,\ h_1 \in H \Rightarrow p \in H\ [\because hh_1 \in H]$; hence $hH \subset H$ ... (1)

Again, let $q \in H$, as H is a group itself$\Rightarrow$ $hx = q$ has a unique soln. in H, say h_2

Then $q = hh_2 \in hH$; hence $H \subset hH$ ... (2);

Combining (1)& (2) we get, $H = hH$.

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

Let, $x \in aH \cap H \Rightarrow x \in aH$ & $x \in H$

Then, $x = ah_1$ & $x = h_2$, (say) for some $h_1, h_2 \in H$

Thus $ah_1 = h_2 \Rightarrow a = h_2 h_1^{-1} \in H$ [contradiction]

Hence the result.

Result: Let G be a group and H be a subgroup of G. Any two left cosets of G are either disjoint or identical.

Let $aH,\ bH$ be any two left cosets of H in G, for $a, b \in G$

Either, $aH \cap bH = \phi$ or they have common elements.

Let, $p \in aH \cap bH \Rightarrow p \in aH$ & $p \in bH \Rightarrow p = ah_1$ & $p = bh_2$, $h_1, h_2 \in H$

Thus $ah_1 = bh_2 \Rightarrow a = bh_2 h_1^{-1}$ & $b = ah_1 h_2^{-1}$

Let, $x \in aH \Rightarrow x = ah_3,\ h_3 \in H \Rightarrow x = bh_2 h_1^{-1} h_3 = bh_4\ [h_4 = h_2 h_1^{-1} h_3 \in H]$

Hence, $x \in bH \Rightarrow aH \subset bH$ ... (1)

Again, let $y \in bH \Rightarrow y = bh_5, h_5 \in H \Rightarrow y = ah_1 h_2^{-1} h_5 = ah_6 [h_6 = h_1 h_2^{-1} h_5 \in H]$

Hence, $y \in aH \Rightarrow bH \subset aH$ ... (2); Combining $(1), (2)$ we get, $aH = bH$.

Result: Let G be a group and H be a subgroup of G. Any two left cosets $aH, bH, a, b \in G$ are identical iff $a^{-1}b \in H$.

Let, $aH = bH \Rightarrow ah_1 = bh_2$, $h_1, h_2 \in H \Rightarrow a^{-1}b = h_1h_2^{-1} \in H$

Conversely, let $a^{-1}b \in H \Rightarrow a^{-1}b = h_3 \Rightarrow b = ah_3$ and $a = bh_3^{-1} = bh_4$ $[h_4 = h_3^{-1}]$

Let, $p \in aH \Rightarrow p = ah_5 = bh_4h_5 = bh_6$, $[h_6 = h_4h_5] \Rightarrow p \in bH \Rightarrow aH \subset bH \ldots (1)$

Let $q \in bH \Rightarrow q = bh_7 = ah_3h_7 = ah_8$, $[h_8 = h_3h_7] \Rightarrow q \in aH \Rightarrow bH \subset aH..(2)$

Combining (1) & (2), we get the result.

Result: Let G be a group and H be a subgroup of G. Then $G = \cup_{x \in G} xH$

Let, $p \in \cup_{x \in G} xH \Rightarrow p \in xH$ for some $x \in G \Rightarrow p = xh_1 \in G \Rightarrow \cup_{x \in G} xH \subset G \ldots (1)$

Conversely, if $y \in G \Rightarrow y \in yH \Rightarrow y \in \cup_{x \in G} xH \Rightarrow G \subset \cup_{x \in G} xH \ldots (2)$

Combining (1) & (2), we get the result.

Note: Since all distinct left cosets are mutually disjoint, this means that the set of all distinct left cosets of G, form a partition of G.

Result: The order of every subgroup of a finite group G is a divisor of the order of G.

Let H be a subgroup of a finite group G and $o(G) = n$.

Considering the set of all distinct left cosets of H in G.

Since G is finite, the number of distinct left cosets of H in G is also finite.

Let $x_1, x_2, \ldots \ldots, x_m$ in G be such that $x_1H, x_2H, \ldots \ldots, x_mH$ gives the complete list of distinct left cosets of H in G.

Since they are distinct⇒ they are disjoint. [as distinct left cosets are also disjoint]

Then, $G = \cup_{x \in G} xH = \cup_{i=1}^{m} x_iH \Rightarrow o(G) = \sum_{i=1}^{m} o(x_iH)$ [as all left cosets are disjoint]

Again $o(x_iH) = o(H)$, $\forall i = 1, \ldots, m$

Thus, $o(G) = \sum_{i=1}^{m} o(H) = m.o(H)$; i.e. $o(H)$ is a divisor of $o(G)$. Hence the result.

Note: This is known as the **Lagrange's Theorem.**

Defn.: If G be a group and 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 $[G: H]$.

Lagrange's Theorem states that, if G is finite, then $o(G) = [G: H].o(H)$

Result: Every group of prime order is cyclic. [Corollary of Lagrange's Theorem]

Let G be a group of prime order, say, $p \Rightarrow p > 1$.

Then G has more than 1 element. Let $a \in G$ be such that $a \neq e$

Let $H = \langle a \rangle$, the cyclic subgroup generated by $a \Rightarrow o(H) = o(a) > 1$ $[\because a \neq e, o(a) \neq o(e) = 1]$

By Lagrange's theorem, $o(H)$ must divide $p = o(G)$

But since p is prime, $o(H)$ can either be 1 or p.

But $o(H) > 1 \Rightarrow o(H) = p = o(G) \Rightarrow G = H$; i.e. G is cyclic.

Result: In a finite group G order of every element divides $|G|$.

Let $a \in G$ be any element.

Consider $\langle a \rangle$, the cyclic subgroup of G.

Then, $|\langle a \rangle| / |G|$ [By Lagrange's theorem]

but $|\langle a \rangle| = |a|$, hence the result.

Result: If a be any element of a finite group G then $a^{|G|} = e$ (Identity of G).

By previous result $|a|/|G| \Rightarrow |G| = |a|q\ , q \in \mathbb{Z}$

Then, $a^{|G|} = a^{|a|q} = \left(a^{|a|}\right)^q = e^q = e$

Let us consider $\mathbb{Z}_n = \{0,1,2,3,\ldots,n-1\}$ and the binary composition $\times_n$ (multiplication modulo n)

Let $u \in \mathbb{Z}_n$ be a unit (having multiplicative inverse in $\mathbb{Z}_n$) i.e. $u.v \equiv 1\ (mod\, n)$

Then $uv = nq + 1 \Rightarrow uv - nq = 1 \Rightarrow \gcd(u,n) = 1 \Rightarrow u$ is prime to n.

Conversely, let $u \in \mathbb{Z}_n$ be such that $\gcd(u,n) = 1$

Then $\exists p, q \in \mathbb{Z}$ such that $up + nq = 1 \Rightarrow up - 1 = -nq \Rightarrow up \equiv 1\ (mod\, n)$

Now clearly p is not divisible by $n \Rightarrow p \equiv r\ (mod\, n),\ \ 0 \leq r < n$

Then $r \equiv p\ (mod\, n) \Rightarrow ur \equiv up\ (mod\, n) \equiv 1\ (mod\, n)$
$\Rightarrow r$ is the multiplicative inverse of u in $\mathbb{Z}_n \Rightarrow u$ is a unit in $\mathbb{Z}_n$.

Thus $u \in \mathbb{Z}_n$ is a unit iff u is less than n and prime to n.

Result: Let, $U_n = \{all\ units\ of\ \mathbb{Z}_n\}$; then $(U_n, \times_n)$ is a commutative group.

Let $u, v \in U_n \Rightarrow u, v$ are units in $\mathbb{Z}_n \Rightarrow \gcd(u,n) = 1\ \&\ \gcd(v,n) = 1 \Rightarrow \gcd(uv,n) = 1$

Hence uv is a unit; i.e. $uv \in U_n$.

Associativity is true in $\mathbb{Z}_n$ and hence in U_n.

$1 \in U_n$ as 1 is less than and prime to n and it is the identity.

Also, for each $u \in U_n$ there exists $v \in U_n$ s.t. $uv \equiv 1\ (mod\ n)$ and hence each element has its inverse.

Again, $\times_n$ is commutative in $\mathbb{Z}_n$ and hence in U_n.

Thus $(U_n, \times_n)$ is a commutative group.

Note: If $n = p\ (prime)$ then $\boldsymbol{U_p = \mathbb{Z}_p - \{0\} = \{1, 2, , 3, 4, \ldots, p-1\}}$ and hence, $\boldsymbol{|U_p| = p - 1}$.

Defn.: If G be a group and H be a subgroup of G, and let $a \in G$ be any element. Then the set $\{ha : h \in H\}$ is called the right coset of H in G and is denoted by Ha.

If $a, b, c \ldots$ are different elements of G then $Ha, Hb, Hc, \ldots$ are the different right cosets of G.

In additive notation: $H + a = \{h + a : h \in G\}$.

All the properties of left cosets are also applicable to right cosets.

i.e. if $a \in H \Rightarrow Ha = H$; any two right cosets are either disjoint or identical.

Lagrange's theorem is also true for right cosets as well.

Normal subgroup:

A subgroup H in G is a normal subgroup if $aH = Ha\ \forall a \in G$. That is if $ah_1 = h_2 a$, for some $a \in G, h_1, h_2 \in H$.

This is denoted by $H\Delta G$.

In every group G & $\{e\}$ are normal subgroups.

If G is commutative, then every subgroup is a normal subgroup.

Result: If G be a group and H be a subgroup of G. If every left coset is also a right coset of H, then $H\Delta G$.

let $a, b \in G$ be such that $aH = Hb$

$a \in aH$ and $b \in Hb$

since $aH = Hb \Rightarrow a \in Hb$, but $a \in Ha$

Ha & Hb has a common element $a \Rightarrow Ha = Hb \Rightarrow aH = Ha$.

Result: If G be a group and H be a subgroup of G. If $[G:H] = 2$, then $H\Delta G$.

There are Two distinct left cosets of H in G, H & $G - H$.

Similarly, there are Two distinct right cosets of H in G, H & $G - H$.

Hence every left coset is also a right coset of H in G.

Hence the result follows.

Result: G be a group and H be subgroup of G. Then $H\Delta G$ iff $h \in H$ & $x \in G \Rightarrow xhx^{-1} \in H$.

let $H\Delta G \Rightarrow xH = Hx,\ x \in G$

$xh = h_1 x,\ \ h, h_1 \in H$

$xhx^{-1} = h_1 \in H$

Conversely, let the condition be true

let, $p \in xH \Rightarrow p = xh_2 = xh_2(x^{-1}x) = (xh_2x^{-1})x = h_3 x \in Hx \Rightarrow xH \subset Hx$ … (1)

again, $q \in Hx \Rightarrow q = h_4 x = xx^{-1}(h_4 x) = x\{x^{-1}h_4(x^{-1})^{-1}\} = xh_5 \in xH \Rightarrow Hx \subset xH$ … (2)

combining (1)& (2) gives $xH = Hx$.

Note1: This is called the **Normality Test** or **Test for Normality.**

Note2: Condition of the above can be restated as $H \triangle G\ iff\ \forall x \in G,\ xHx^{-1} \subset H$

Result: G be a group. Then intersection of two normal subgroups of G is also normal in G.

Let H, K be two normal subgroups of G and $P = H \cap K \Rightarrow P$ is a subgroup of G.
[∵ intersection of two subgroups is again a subgroup]

Let, $p \in P \Rightarrow p \in H \text{ and } p \in K$ and $x \in G$

Since, $H\Delta G,\ p \in H \text{ and } x \in G \Rightarrow xpx^{-1} \in H$

Also, $K\Delta G,\ p \in K \text{ and } x \in G \Rightarrow xpx^{-1} \in K \Rightarrow xpx^{-1} \in P \Rightarrow P\Delta G$.

Note: Intersection of a collection of normal subgroups of G is also a normal subgroup of G.

Result: Let H be a subgroup of a group G and $a \in G$. Then the subset $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a subgroup of G.

$e \in H \;\&\; e = aea^{-1} \in aHa^{-1} \Rightarrow aHa^{-1}$ is non-empty. Let $p, q \in aHa^{-1}$

then $p = ah_1a^{-1} \;\&\; q = ah_2a^{-1},\ h_1, h_2 \in H$

then $pq = (ah_1a^{-1})(ah_2a^{-1}) = ah_1h_2a^{-1} \in aHa^{-1}$

also, $p^{-1} = (ah_1a^{-1})^{-1} = ah_1^{-1}a^{-1} \in aHa^{-1} \Rightarrow aHa^{-1}$ is a subgroup of G.

Note: The subgroup aHa^{-1} is called the ***conjugate of H*** by a.

Result: G be a group. A subgroup H is normal in $G\ iff\ \ aHa^{-1} = H$ for every $a \in G$.

Let $H\Delta \mathrm{G} \Rightarrow aH = Ha$ for every $a \in G$. Let $p \in aHa^{-1}$

then $p = ah_1a^{-1} = (h_2a)a^{-1} = h_2 \Rightarrow p \in H \Rightarrow aHa^{-1} \subset H$

Again, let $q \in H \Rightarrow qa \in Ha \Rightarrow qa \in aH = ah_3(say)$
$\Rightarrow q = ah_3a^{-1} \in aHa^{-1} \Rightarrow H \subset aHa^{-1}$; Hence $H = aHa^{-1}$

Conversely let $aHa^{-1} = H$ for every $a \in G$. Let $p \in aH$

then $p = ah_4 = ah_4(a^{-1}a) = (ah_4a^{-1})a = h_5a \in Ha \Rightarrow aH \subset Ha$

Again, let $q \in Ha \Rightarrow q = h_6a = (ah_7a^{-1})a = ah_7 \in aH \Rightarrow Ha \subset aH$

Hence $aH = Ha \Rightarrow H\Delta G$.

Note1: In this case H is a self-conjugate subgroup. i.e. for any element in $h_6 \in H$ we have, $h_6 = ah_7a^{-1}$

Note2: If H is a non-empty subset of G , instead of a subgroup, such that $aHa^{-1} = H\ \forall a \in G$, then the result may not be true.

For example, let $G = (\mathbb{Z}, +)$ and $H = \{set\ of\ all\ odd\ integers\}$
then for any $a \in \mathbb{Z}, b \in H, aba^{-1} = a + b - a = b \in H$; so the condition holds, but H is not even a group, let alone a normal subgroup.

Problems on Chapter 3:

1. If $H = \{0,3,6\}$, examine if $(H, +)$ is a subgroup of $(\mathbb{Z}_9, +_9)$. If so, find all distinct left cosets of H in G.
2. If $H \leq G$ and $a \in G$, then show that, $aH \leq G$ if and only if $a \in H$.
3. Find all units in $\mathbb{Z}_{10}$ with respect to the binary composition $\times_{10}$, i.e. multiplication modulo 10, and show that they form an abelian group.
4. Examine if the alternating group A_3 is a normal subgroup of the symmetric group S_3.
5. If $H\Delta G$ and K is any subgroup of G such that, $H \subseteq K \subseteq G$, prove that $H\Delta K$.

Algebra: Chapter – 4
Hints & Solutions:

1. Composition table for H:

$+_9$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

   Since H is a group itself hence, $H \leq G$.
   All distinct left cosets of H in G are:
   $0 + H = \{0,3,6\} = 3 + H = 6 + H\ ; 1 + H = \{1,4,7\} = 4 + H = 7 + H\ ; 2 + H = \{2,5,8\} = 5 + H = 8 + H$

2. If aH is a subgroup, then it contains the identity e. Thus, $aH \cap eH \neq \phi$; and, therefore we must have
   $$aH = eH = H \Rightarrow a \in H$$
   Conversely, if $a \in H$, then, of course, we have $aH = H$.
3. All units are 1,3,7,9.
   Composition table:

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

   From the table it is clear that they form an abelian group.

4. Since, $o(S_3) = 6$ and $o(A_3) = 3 \Rightarrow [S_3 : A_3] = \frac{6}{3} = 2$
   Since index of A_3 in S_3 is 2, hence, $A_3 \,\Delta\, S_3$.

5. If $H \Delta G \Rightarrow \forall x \in G \ and \ h \in H,\ xhx^{-1} \in H \Rightarrow \forall x \in K \ and \ h \in H \ xhx^{-1} \in H$
   (AS $K \subseteq G$)

Assignments on Chapter 4:

1. Give an example of a finite group G and its subgroup H, such that H is not normal in G.
2. If G is a finite group and H is a subgroup of G, then prove that, [G:H] = |G|/|H|.
3. Find a subgroup of order 4 of the alternating group A_4.
4. Let, $H = \{0, \pm 3, \pm 6, \pm 9, \ldots.\}$. Find all distinct left cosets of H in $(\mathbb{Z}, +)$.
5. Find all left cosets of $\{1,11\}$ in the group U_{30}.
6. Let, $H = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{R}, ad \neq 0\right\}$. Examine if H is a normal subgroup of $GL(2, \mathbb{R})$.
7. Let, $H = \{i, (12)(34)\}$ in A_4. Show that H is not normal in A_4.