4.2 SUBGROUP & CYCLIC GROOUP; COSETS

4.2.1 Definition of Subgroup. A non-empty subset H of a group $(G, \circ)$ is said to be a subgroup of G, if H itself is a group under the binary operation '$\circ$' of G.

Since every set is a subset of itself, so G itself is a subgroup of G. Again the subset of G containing only identity element is also a subgroup of G. Thus every group $(G, \circ)$ has at least two sub-groups. These two are called *trivial or improper* subgroups. All other subgroups are called *non-trivial or proper subgroups.*

Illustration. (i) The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

(ii) The additive group of even integers is a subgroup of the additive group of all integers.

Theorem 1. The identity element of a subgroup is the same as that of the group.

Proof. Left as an exercise.

Theorem 2. The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Proof. Left as an exercise.

Inverse of a Subgroup.

Let H be a subgroup of $(G, \circ)$. Then we define the inverse of H as $H^{-1} = \{h^{-1} : h \in H\}$.

Thus H^{-1} is the subgroup of G consisting of the inverses of the elements of H.

Note. *If fact this definition can be extended for any subset of a group.*

Theorem 3. If H is any subgroup of a group $(G, \circ)$, then $H^{-1} = H$

Proof. Let $h \in H$. Then $h \in H \Rightarrow h^{-1} \in H$ [$\because H$ is itself a group]

$\Rightarrow (h^{-1})^{-1} \in H^{-1} \Rightarrow h \in H^{-1}$ $\quad \therefore \quad H \subseteq H^{-1}$

Again let $k \in H^{-1}$. Since $(k^{-1})^{-1} = k$, so $k^{-1} \in H$

As H is a subgroup, so $k \in H$

Thus $k \in H^{-1} \Rightarrow k \in H \therefore H^{-1} \subseteq H$ Hence $H = H^{-1}$.

Note. *The converse of the above theorem is not true i.e. if $H = H^{-1}$, then H may not be the subgroup of G.For example, consider the multiplicative group $(G, \times)$ where $G = \{1, -1\}$. Let $H = \{-1\}$. Then $H^{-1} = \{-1\} = H$ as -1 is the inverse of -1 in G. But H is not a subgroup of G, as H is not closed w.r.t multiplication.*

Theorem 4. A non-empty subset H of a group $(G, \circ)$ is a subgroup of G if and only if (i) $a, b \in H \Rightarrow a \circ b \in H$,

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof. The conditions are necessary :

Let H be a subgroup of $(G, \circ)$. Then H is itself a group. So H is closed w.r.t the operation '$\circ$'. $\quad \therefore \quad a, b \in H \Rightarrow a \circ b \in H$

Again, since H is a group, so $a \in H \Rightarrow a^{-1} \in H$

The conditions are sufficient :

(a) By (i), H is closed w.r.t the operation '$\circ$'

(b) The operation '$\circ$' is associative in H, as it holds in G

(c) By (ii), $a \in H \Rightarrow a^{-1} \in H$

$\because a \in H \Rightarrow a^{-1} \in H \Rightarrow a \circ a^{-1} \in H \Rightarrow e \in H$

$\therefore$ The identity element e is in H

(d) By (ii), inverse of each element of H exists in H.

Hence H is a group w.r.t the operation '$\circ$' Thus H is a subgroup of G.

Theorem 5. The necessary and sufficient condition for a non-empty subset H of a group $(G, \circ)$ to be a subgroup is that $a, b \in H \Rightarrow a \circ b^{-1} \in H$.

Proof. The condition is necessary :

Let H be a subgroup of $(G, \circ)$. So H is itself a group.

$\therefore \quad b \in H \Rightarrow b^{-1} \in H$

$\therefore \quad a \in H, b^{-1} \in H \Rightarrow a \circ b^{-1} \in H$, as H is closed under the operation '$\circ$'.

The condition is sufficient :

Let $a, b \in H \Rightarrow a \circ b^{-1} \in H$.Then (i) $a, a \in H \Rightarrow a \circ a^{-1} \in H \Rightarrow e \in H$

Thus the identity e is an element of H.

(ii) Now e, $a \in H \Rightarrow e \circ a^{-1} \in H \Rightarrow a^{-1} \in H$

Thus the inverse of each element of H exists in H

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

$\therefore \quad a, b \in H \Rightarrow a \circ (b^{-1})^{-1} \in H \Rightarrow a \circ b \in H$

$\therefore$ H is closed w.r.t the operation '$\circ$'

(iv) The operation '$\circ$' is associative in H as it holds in G.

Hence H is a group w.r.t the operation '$\circ$' . Thus H is a subgroup of G.

Theorem 6. A necessary and sufficient condition for a non-empty finite subset H of a group $(G, \circ)$ to be a subgroup is that

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

Proof. The condition is necessary :

Let H be a subgroup of $(G, \circ)$. So H is itself a group. Then H must be closed w.r.t the operation '$\circ$'.

$\therefore \quad a, b \in H \Rightarrow a \circ b \in H$

The condition is sufficient :

Let a be any element of H. Then $a^2 = a \circ a \in H$, $a^3 = a \circ a^2 \in H$ and so on, by the given condition.

Since H is a non-empty finite subset, so there is a positive integer n such that $a^n = e$, the identity element

Now $a \circ a^{n-1} = a^n = e \quad \therefore a^{-1} = a^{n-1} \in H \quad \therefore a \in H \Rightarrow a^{-1} \in H$

Hence by Theorem 4, H is a subgroup of $(G, \circ)$.

Note. *The above theorem is not valid for infinite subset. For example $(Z, +)$ is a group and Z_+ is a subset of Z consisting of all positive integers. Then Z_+ is closed w.r.t the addition but not a subgroup of Z, as $0 \notin Z_+$.*

Theorem 7. Intersection of any two subgroups of a group $(G, \circ)$ is a subgroup of G. *[W.B.U.T. 2007, 2008, 2015]*

Proof. Let H_1 and H_2 be any two subgroups of G.

Then $H_1 \cap H_2 \neq \phi$, as $e \in H_1$ and $e \in H_2$

Now let $a,\ b \in H_1 \cap H_2$

$\therefore a,\ b \in H_1$ and $a,\ b \in H_2$. But H_1 and H_2 are subgroups of G.

Therefore $a,\ b \in H_1 \Rightarrow a \circ b^{-1} \in H_1$ and $a,\ b \in H_2 \Rightarrow a \circ b^{-1} \in H_2$.

$\therefore a \circ b^{-1} \in H_1 \cap H_2$. Hence $a,\ b \in H_1 \cap H_2 \Rightarrow a \circ b^{-1} \in H_1 \cap H_2$

Thus $H_1 \cap H_2$ is a subgroup of G.

Note (i) *The intersection of any family of subgroups of a group is a subgroup.*

(ii) *The union of any two subgroups of a group is not necessarily a subgroup.* *[W.B.U.T. 2008]*

For example, let $(Z, +)$ be the additive group of integers. Then $H_1 = \{0, \pm 2, \pm 4, \pm 6, \cdots\}$, $H_2 = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$ are both subgroups of $(Z, +)$. But $H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \cdots\}$ is not a subgroup of $(Z, +)$, since $2 + 3 = 5 \notin H_1 \cup H_2$ i.e. $H_1 \cup H_2$ is not closed. Again if we take the subgroup $H_3 = \{0, \pm 4, \pm 8, \pm 16, \cdots\}$ of G, then $H_1 \cup H_3 = H_1$ is a subgroup of G.

Theorem 8. The union of any two subgroups of a group $(G, \circ)$ is a subgroup of G if and only if one is contained in the other.

Proof. Let H_1 and H_2 be any two subgroups of the group $(G, \circ)$ such that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Then $H_1 \cup H_2 = H_2$ or H_1. But H_1 and H_2 are both subgroups of G. Hence $H_1 \cup H_2$ is a subgroup of G.

Next let $H_1 \cup H_2$ be a subgroup of $(G, \circ)$.

If possible let $H_1 \not\subset H_2$ or $H_2 \not\subset H_1$.

Then $H_1 \not\subset H_2 \Rightarrow$ there exists $a \in H_1$ and $a \notin H_2$ ... (i)

and $H_2 \not\subset H_1 \Rightarrow$ there exists $b \in H_2$ and $b \notin H_1$ ... (ii)

$\therefore a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$

$\therefore a \circ b \in H_1 \cup H_2$, since $H_1 \cup H_2$ is a subgroup of G.

$\Rightarrow a \circ b \in H_1$ or, $a \circ b \in H_2$

Let $a \circ b \in H_1$. Since H_1 itself is a group, so $a \in H_1 \Rightarrow a^{-1} \in H_1$.

$\therefore a^{-1} \circ (a \circ b) \in H_1 \Rightarrow (a^{-1} \circ a) \circ b \in H_1 \Rightarrow b \in H_1$ which contradicts (ii).

Hence either $H_1 \subseteq H_2$ or, $H_2 \subseteq H_1$.

Product of two Subgroups.

If H and K are two subgroups of the group $(G, \circ)$, then

$HK = \{x : x = h \circ k,\ h \in H,\ k \in K\}$.

Obviously $HK \subseteq G$. Also it can be easily verified that

$$(HK)^{-1} = K^{-1} H^{-1}.$$

Theorem 9. Let H and K be two subgroups of a group $(G, \circ)$ Then HK is a subgroup of G if and only if $HK = KH$.

Proof. Suppose HK be subgroup of G.

Let $hk \in HK$. Then $(hk)^{-1} \in HK$, as HK is a subgroup of G.

$\therefore (hk)^{-1} = h_1 k_1$ for some $h_1 \in H,\ k_1 \in K$

$\therefore\ hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, as $k_1^{-1} \in K,\ h_1^{-1} \in H$

Thus $hk \in HK \Rightarrow hk \in KH \quad \therefore\ HK \subseteq KH$ ... (i)

Next let $k_2h_2 \in KH$.

Then $k_2 \in K,\ h_2 \in H \Rightarrow k_2^{-1} \in K, h_2^{-1} \in H$

$\Rightarrow h_2^{-1}k_2^{-1} \in HK \Rightarrow \left(h_2^{-1}k_2^{-1}\right)^{-1} \in HK$, as HK is a subgroup of G

$\Rightarrow \left(k_2^{-1}\right)^{-1}\left(h_2^{-1}\right)^{-1} \in HK \Rightarrow k_2h_2 \in HK \quad \therefore\ KH \subseteq HK$ ... (ii)

From (i) and (ii), $HK = KH$.

Now, suppose $HK = KH$.

Let $\alpha = h_3k_3 \in HK, \quad \beta = h_4k_4 \in HK$

Then $\alpha\beta = (h_3k_3)(h_4k_4) = h_3(k_3h_4)k_4 = h_3(h_5k_5)k_4$

[$\because\ HK = KH$, so $k_3h_4 = h_5k_5$, for some $h_5 \in H,\ k_5 \in K$]

$= (h_3h_5)(k_5k_4) = h_6k_6 \in HK$ where $h_6 = h_3h_5 \in H,\ k_6 = k_5k_4 \in K$

$\therefore\ \alpha, \beta \in HK \Rightarrow \alpha\beta \in HK$ ... (iii)

Again $\alpha^{-1} = (h_3k_3)^{-1} = k_3^{-1}h_3^{-1} \in KH = HK$

$\therefore\ \alpha \in HK \Rightarrow \alpha^{-1} \in HK$ ... (iv)

$\therefore$ From (iii) and (iv), HK is a subgroup of G.

Note. *If H and K are two subgroups of an abelian group G, then HK is a subgroup of G.*

Illustrative Example.

Ex. 1. *Let $(G, \circ)$ be a group and $a \in G$. Then show that the set $H = \{a^n : n \in Z\}$ of all integral powers of a is a subgroup of G.*

Here $H = \{\cdots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \cdots\}$

Let $a^m, a^n \in H$ where $m, n \in Z$, the set of all integers

Then the inverse of a^n is $\left(a^n\right)^{-1}$ i.e., a^{-n}

$\therefore\ a^m \cdot \left(a^n\right)^{-1} = a^m \cdot a^{-n} = a^{m-n} \in H$, as $m - n \in Z$

$\therefore\ a^m, a^n \in H \Rightarrow a^m \cdot \left(a^n\right)^{-1} \in H$. Therefore H is a subgroup of G.

Note. *The above subgroup is called the cyclic subgroup of G generated by the element a and is denoted by $\langle a \rangle$.*

Ex. 2. *Given Z, the group of integers with addition and H, a subset of Z consisting all multiples of a positive integer m, i.e. $km (k = 0, \pm 1, \pm 2, \cdots)$. Show that H is subgroup of G.* [*W.B.U.T. 2003*]

Let $a = rm, b = sm$ be any two elements of H where r and s are some integers. Then the inverse of $b = sm$ is $-sm$

i.e., $-b = (-s)m$.

$\therefore\ a + (-b)$

$= rm + (-sm) = (r - s)m \in H$, as $r - s$ is also an integer.

Thus $a \in H, b \in H \Rightarrow a + (-b) \in H$ i.e., $a - b \in H$

Hence H is a subgroup of G.

Ex. 3. *Let $GL(2, R)$ be the multiplicative group of all real non singular matrices of order 2. Show that the set*

$H = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1\right\}$ *is a subgroup of $GL(2, R)$.*

Since $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$, so H is a non-empty set.

Let $A, B \in H$. Then $\det A = 1,\ \det B = 1$.

$\left[\because \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1\right]$

Now $\det(AB) = \det A \cdot \det B = 1$.

So $AB \in H \quad \therefore\ A, B \in H \Rightarrow AB \in H$

Again, since $\det A = 1 \neq 0$, so A^{-1} exist and

$$\det A^{-1} = \frac{1}{\det A} = 1 \quad \left[\because AA^{-1} = I_2\right]$$

$\therefore A^{-1} \in H \quad \because A \in H \Rightarrow A^{-1} \in H$.

Therefore H is a subgroup of $GL(2, R)$.

Ex. 4. *The subset H of a group $(G, \circ)$ is defined by*

$H = \{x \in G : x \circ g = g \circ x \ \forall g \in G\}$.

Prove that H is a subgroup of G.

Since $e \circ g = g \circ e$, so $e \in H$.

Therefore H is a non-empty set.

Let $h_1, h_2 \in H$. Then $h_1 \circ g = g \circ h_1$ and $h_2 \circ g = g \circ h_2 \ \ \forall g \in G$

Now, $(h_1 \circ h_2) \circ g = h_1 \circ (h_2 \circ g) = h_1 \circ (g \circ h_2)$

$= (h_1 \circ g) \circ h_2 = (g \circ h_1) \circ h_2 = g \circ (h_1 \circ h_2) \ \ \forall g \in G$

$\therefore \quad h_1 \circ h_2 \in H \ \ \because \quad h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$

Again $h_1 \circ g = g \circ h_1 \ \ \forall g \in G$

$\therefore \ h_1^{-1} \circ (h_1 \circ g) \circ h_1^{-1} = h_1^{-1} \circ (g \circ h_1) \circ h_1^{-1}$

$\Rightarrow (h_1^{-1} \circ h_1) \circ (g \circ h_1^{-1}) = (h_1^{-1} \circ g) \circ (h_1 \circ h_1^{-1})$

$\Rightarrow e \circ (g \circ h_1^{-1}) = (h_1^{-1} \circ g) \circ e \Rightarrow g \circ h_1^{-1} = h_1^{-1} \circ g \Rightarrow h_1^{-1} \in H$

$\therefore \ h_1 \in H \Rightarrow h_1^{-1} \in H$.

Therefore H is a subgroup of G.

Note. **(i)** *The above subgroup H is called the centre of G and is denoted by $Z(G)$. Obviously $Z(G)$ is a commutative subgroup of G.*

(ii) *If $a \in G$, then the subset defined by*

$C(a) = \{x \in G : x \circ a = a \circ x\}$ is called the centraliser or Normalizer of the element a and is also a subgroup of G.

Ex. 5. *Determine whether the following subset H is a subgroup of the group G :*

(i) $H = \{1, 2, -1\}$, $G = (Z, +)$ (ii) $H = \{[0], [3]\}$, $G = (Z_6, +)$

(i) Here H is a non-empty finite subset of Z but is not closed w.r.t the operation addition, as $1 + (-1) = 0 \notin H$. Hence H is not a subgroup of G.

(ii) Here H is a non-empty finite subset and is closed w.r.t. the addition of residue classes, as

$[0] + [3] = [3]$, $[0] + [0] = [0]$, $[3] + [3] = [6] = [0]$.

Hence H is a subgroup of G. (by Theorem 6)

Ex. 6. *Let H be a subgroup of a group $(G, 0)$. Also let for $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\}$. Prove that gHg^{-1} is a subgroup of G.*

[The operations 'o' between two elements is understood.]

Let $\overline{H} = gHg^{-1}$. Also let $a = ghg^{-1} \in \overline{H}$ and $b = gh_1g^{-1} \in \overline{H}$.

Then $h, h_1 \in H$.

Now $ab^{-1} = (ghg^{-1})(gh_1g^{-1})^{-1} = (ghg^{-1})\left((g^{-1})^{-1}h_1^{-1}g^{-1}\right)$

$= (ghg^{-1})(gh_1^{-1}g^{-1}) = gh(g^{-1}g)h_1^{-1}g^{-1} = ghh_1^{-1}g^{-1} \ \ [\because g^{-1}g = e]$

Now $h, h_1 \in H$ and H is a subgroup of G, so $hh_1^{-1} \in H$ and hence

$ab^{-1} = ghh_1^{-1}g^{-1} \in gHg^{-1} = \overline{H}$. $\quad \therefore \ a, b \in \overline{H} \Rightarrow ab^{-1} \in \overline{H}$

Therefore $\overline{H} = gHg^{-1}$ is a subgroup of G.

Ex. 7. *Let G be an abelian group. Prove that the subset $S = \{p \in G : p = p^{-1}\}$ forms a subgroup of G.* [W.B.U.T. 2005]

Since $e = e^{-1}$, so $e \in S$. Therefore S is a non-empty set.

Let $x \in S$. Then $x^{-1} \in S$, as $x = x^{-1} \ \ \therefore \ x \in S \Rightarrow x^{-1} \in S$.

Next let $x, y \in S$. Then $x = x^{-1}$, $y = y^{-1}$

$\therefore\ xy = yx$, as G is abelian and $x, y \in G$

$\Rightarrow xy = y^{-1}x^{-1} \Rightarrow xy = (xy)^{-1} \Rightarrow xy \in S$.

Hence S is a subgroup of G.

4.2.2. Cyclic Group. [W.B.U.T. 2012, 2005]

Definition. A group $(G, \circ)$ is called cyclic if there exists an element a in G such that every element of G can be expressed as a^n where n is an integer (positive, negative or 0). The element a is called the *generator* of the cyclic group.

Thus if a be the generator of the cyclic group G, then $G = \{a^n : n \in Z\}$ which is denoted by $G = \langle a \rangle$ or $\{a\}$.

Note. *There may be more than one generator of a cyclic group.*

Illustration. **(i)** The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic, as we can write $G = \{i, i^2, i^3, i^4\}$

Here i is a generator of G.

Also we can write $G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$

So, $-i$ is a generator of G.

(ii) The group of integers, $\langle Z, + \rangle$ is a cyclic group with generator 1 because any positive integer m of Z can be expressed as $m = 1+1+1+\cdots+ \text{to } m \text{ times} = 1^m$, any negative integer $-m$ can be expressed as $(-1)+\cdots+(-1) = 1^{-m}$ and 0 can be expressed as $0 = 1^0$.

Theorem 1 Every Cyclic Group is an abelian group. [W.B.U.T. 2013, 2012, 2004]

Proof. Let $(G, \circ)$ be a cyclic group generated by a.

Also let $x, y \in G$.

Then there exist integers r and s such that $x = a^r$, $y = a^s$.

Now $x \circ y = a^r \circ a^s = a^{r+s} = a^{s+r} = a^s \circ a^r = y \circ x$

Therefore $x \circ y = y \circ x \ \forall\ x, y \in G$ $\therefore$ G is abelian

Note. *Converse of the above theorem is not true.*

For example, consider the set $G = \{e, a, b, c\}$ and let '$\circ$' be the binary operation defined on G by

$e \circ a = a \circ e = a, e \circ b = b \circ e = b, e \circ c = c \circ e = c$.

$e \circ e = a \circ a = b \circ b = c \circ c = e,$

$a \circ b = b \circ a = c, a \circ c = c \circ a = b, b \circ c = c \circ b = a$.

Then the composition table is given below :

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

From the above table it follows that $(G, \circ)$ is an abelian group of order 4 but is not cyclic group as

$\langle e \rangle = \{e\}$, $\langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}$ and $\langle c \rangle = \{e, c\}$

The above group $(G, \circ)$ is known as *Klein's 4-group* and is denoted by K_4.

Theorem 2. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof. Let $x \in G$. Then there exist an integer r such that $x = a^r$.

Now $x = a^r = (a^{-1})^{-r} = (a^{-1})^p$ where $p = -r$ is an integer.

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

Note. *If $G = \langle a \rangle$ be an infinite cyclic group, then G has exactly two generators a and a^{-1}.*

Theorem 3. Let $(G, \circ)$ be a finite cyclic group generated by a. Then $0(G) = n$ if and only if $0(a) = n$.

Proof. Let $0(a) = n$.

Then $a^n = e$, the identity element of G and $a^s \neq e$ for $0 < s < n$. If $s > n$, then by division algorithm there exist integers q, r such that

$s = nq + r,\ 0 \leq r < n \quad \therefore \quad a^s = a^{nq+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$

Thus there are only n distinct elements $a, a^2, a^3, \cdots, a^n$ in G.

Hence $0(G) = n$.

Next let $0(G) = n$.

Suppose $0(a) = m$. Then by previous arguments $0(G) = m$ and hence $m = n$. $\therefore \quad 0(a) = n$.

Theorem 4. A finite group $(G, \circ)$ is cyclic if and only if there exists an element $a \in G$ such that $0(a) = 0(G)$.

Proof. Let $(G, \circ)$ be a cyclic group generated by a.

Then by Theorem 3, we have $0(a) = 0(G)$.

Next let us assume G be a finite group of order n and G has an element a such that $0(a) = 0(G)$ i.e. $0(a) = n$. Then $a^1, a^2, \cdots, a^{n-1}, a^n (= e)$ are distinct elements in G and hence $G = \{a^1, a^2, \cdots, a^n (= e)\} = \langle a \rangle$. Thus G is a cyclic group.

Theorem 5. Let $G = \langle a \rangle$ be a cyclic group of order n. Then for any integer r where $1 \leq r < n$, a^r is a generator of G if and only if r and n are relative primes.

Proof. Let r be relatively prime to n.

Also let $H = \langle a^r \rangle$ be a cyclic subgroup of G.

Obviously $H \subset G$ ... (i)

Since r is relatively prime to n, so there exist two integers u, v such that $ur + vn = 1$

$\therefore \quad a^1 = a^{ur} \cdot a^{vn} = (a^r)^u \cdot (a^n)^v = (a^r)^u \in H \quad \left[\because a^n = e \Rightarrow (a^n)^v = e\right]$

which shows that $G \subset H$ ... (ii)

$\therefore$ From (i) and (ii), $H = G$ and hence a^r is a generator of G.

Next let $G = \langle a^r \rangle$

Also let the greatest common divisor of r and n be d and $d \neq 1$. i.e., $d > 1$. Then $\frac{r}{d}$ and $\frac{n}{d}$ must be positive integers.

Now $(a^r)^{\frac{n}{d}} = (a^n)^{\frac{r}{d}} = e^{\frac{r}{d}} = e$

Obviously $\frac{n}{d}$ is a positive integer less than n. Hence $0(a^r) < n$. Therefore a^r is not a generator of G which contradicts our assumption. Hence $d = 1$. Therefore r is prime to n.

Note. (i) *The total number of generators of a cyclic group G of order n will be equal to the number of integers less than n and prime to n. Thus, if G be a cyclic group of order 12, generated by a, then all generators of G are* a, a^5, a^7, a^{11}.

(ii) *A cyclic group of prime order p generated by a has* $(p-1)$ *generators and all generators are* $a, a^2, a^3, \cdots, a^{p-1}$.

Thus, if G be a cyclic group of order 5 generated by a, then all generators of G are a, a^2, a^3, a^4.

(iii) *A cyclic group having infinite number of elements has two generators.*

Theorem 6. Every subgroup of a cyclic group is cyclic.

Proof. Let H be a subgroup of a cyclic group $G = \langle a \rangle$

If $H = G$ or $\{e\}$, then obviously H is cyclic. So let H be a proper subgroup of G. Then all elements of H are integral powers of a. If $a^m \in H$, then $(a^m)^{-1} \in H$ i.e., $a^{-m} \in H$. So H contains elements which are positive as well as negative integral powers of a. Let n be the least positive integer such that $a^n \in H$. We shall show that $H = \langle a^n \rangle$.

Let $a^s \in H$. Then by division algorithm, there exist integers q and r such that $s = nq + r,\ 0 \leq r < n$

Now, $a^n \in H \Rightarrow (a^n)^q \in H \Rightarrow a^{nq} \in H \Rightarrow (a^{nq})^{-1} \in H \Rightarrow a^{-nq} \in H$

$\therefore a^s \in H,\ a^{-nq} \in H \Rightarrow a^s \cdot a^{-nq} \in H \Rightarrow a^{s-nq} \in H \Rightarrow a^r \in H$

which is possible only when $r = 0$, as n is the least positive integer such that $a^n \in H$. $\therefore\ s = nq \quad \therefore\ a^s = a^{nq} = (a^n)^q$

Thus every element $a^s \in H$ is of the form $(a^n)^q$. Hence $H = \langle a^n \rangle$ is cyclic.

Theorem 7. Every proper subgroup of an infinite cyclic group is infinite,

Proof. Left as an exercise.

Theorem 8. If $a \neq e$ be an element of a Group G then the set $\{a^n : n \in z\}$ is a cyclic subgroup of G.

Proof. Left as an excercise.

Illustrative Example.

Ex. 1. *Show that the set $G = \{1, 2, 3, 4, 5, 6\}$ form a cyclic group under the operation multiplication modulo 7. Find all generators of this group.* [W.B.U.T. 2003, 2008]

We have seen that the set G forms a group of order 6 under operation $\times_7$. We shall now show that the group G is cyclic. For this we now find an element $a \in G$ such that $0(a) = 6$.

We see that $0(3) = 6$ because $3^1 = 3,\ 3^2 = 3 \times_7 3 = 2,\ 3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6,\ 3^4 = 3^3 \times_7 3 = 6 \times_7 3 = 4, 3^5 = 3^4 \times_7 3 = 4 \times_7 3 = 5$

$3^6 = 5 \times_7 3 = 1$, the identity element.

$\therefore\ G$ is cyclic and 3 is a generator.

Now 5 is prime to 6. So 3^5 i.e. 5 is also a generator.

Ex. 2. *Show that the group $(Z_5, +)$, i.e. the additive group of all integers modulo 5 is cyclic. Find all generators of Z_5.*

Here $Z_5 = \{[0], [1], [2], [3], [4]\}$

Now, $0[1] = [0],\ 1 \cdot [1] = [1],\ 2[1] = [1] + [1] = [2],\ 3[1] = [3],\ 4[1] = [4]$

$5[1] = [5] = [0]$, the identity element.

Thus, $0([1]) = 5$. So $(Z_5, +)$ is cyclic and $[1]$ is a generator.

Since 5 is prime, so all other generators are $2[1]$

i.e., $[2]$, $3[1]$ i.e. $[3]$, $4[1]$ i.e., $[4]$.

Ex. 3. *Show that the group $(Q, +)$ is not cyclic.*

If possible let $(Q, +)$ be a cyclic group generated by an element $a \in Q$. Then $a \neq 0$ and every element of Q can be written as na for some integer n.

Now $\frac{1}{3}a \in Q$ but $\frac{1}{3}a$ cannot be expressed as na for some integer n. Hence a is not a generator of $(Q, +)$. Therefore $(Q, +)$ is not a cyclic group.

Ex. 4. *If $G = \langle a \rangle$ is a cyclic group of order 40, find all distinct elements of the cyclic subgroup*

(i) $\langle a^8 \rangle$ (ii) $\langle a^{10} \rangle$.

(i) Here $\langle a^8 \rangle = \{(a^8)^n : n \in Z\}$

Now $0(a) = 0(G) = 40,\ \therefore\ a^{40} = e$, the identity element.

$\therefore\ (a^8)^5 = e \Rightarrow 0(a^8) = 5.$

$\therefore\ \langle a^8 \rangle = \{(a^8)^0, (a^8)^1, (a^8)^2, (a^8)^3, (a^8)^4\} = \{e, a^8, a^{16}, a^{24}, a^{32}\}$

(ii) Since $(a^{10})^4 = e$, so $0(a^{10}) = 4$

$\therefore\ \langle a^{10} \rangle = \{(a^{10})^0, (a^{10})^1, (a^{10})^2, (a^{10})^3\} = \{e, a^{10}, a^{20}, a^{30}\}.$

Ex. 5. *Show that a cyclic group of prime order has no proper non-trivial subgroup.* [W.B.U.T. 2005]

Let $(G, \circ)$ be a finite cyclic group of prime order p.

Let H be a subgroup of G. By Lagrange's theorem the order of every subgroup is a divisor of the order of G. Hence $0(H) = 1$ or $0(H) = p$ as p is prime. Thus G can have no proper subgroups.

Ex. 6. *Show that the n-th roots of unity form a cyclic group under ordinary multiplication.*

Let $x = (1)^{\frac{1}{n}} \quad \therefore x^n = 1$

or, $x^n = \cos 0 + i \sin 0 = \cos 2k\pi + i \sin 2k\pi, \ k = 0, \pm 1, \pm 2, \cdots$

$\therefore \ x = (\cos 2k\pi + i \sin 2k\pi)^{\frac{1}{n}}, \ k = 0, 1, 2, \cdots, (n-1)$

$= \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \ k = 0, 1, 2, \cdots, (n-1)$ [By D'Moiver's Theorem]

$= e^{\frac{2k\pi i}{n}}$.

Thus the set G of n-th roots of unity is given by

$$G = \left\{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \cdots, e^{\frac{2(n-1)\pi i}{n}}\right\} = \left\{1, w, w^2, \cdots, w^{n-1}\right\}$$

,where $w = e^{\frac{2\pi i}{n}}$.

First we shall show that G forms a group under multiplication.

(i) It is obvious that $z_1, z_2 \in G \Rightarrow z_1 z_2 \in G$

So G is closed w.r.t the operation multiplication.

(ii) Multiplication is associative on the set of complex number C and G is a subset of C. So multiplication is associative on G.

(iii) Now $1 \in G$ and $1 \cdot z = z \cdot 1 = z \ \ \forall z \in G$. So 1 is the identity element.

(iv) If $w^p \in G, \ 1 \le p \le n-1$, then $w^{n-p} \in G$ and

$w^{n-p} \cdot w^p = w^p . w^{n-p} = w^n = 1$ [$\because$ w is the n-th root of unity]

So, w^{n-p} is the inverse of w^p. Hence $(G, \circ)$ is a group.

Again all elements of G are integral power of w and $w^n = 1$.

Hence w i.e. $e^{\frac{2\pi i}{n}}$ is a generator of order n.

4.2.3. Cosets.

Right cosets & Left cosets.

Let H be a subgroup of a group G. Also let a be an element of G. Then the subset $\{ha : h \in H\}$ is called a *right coset* of H in G and is denoted by Ha. Thus $Ha = \{ha : h \in H\}$.

Similarly, $aH = \{ah : h \in H\}$ is called a *left coset* of H in G.

Note. *(1) Since $He = H = eH$, so H itself is a right as well as a left coset of H.*

(2) Again, since H is a subgroup of G,so $e \in H$ and $ea = a \in Ha$. Thus if Ha is any right coset, then at least one element $a \in Ha$. Consequently every right coset is non-empty. Similarly every left coset is non-empty.

(3) When G is an abelian group, then $ah = ha \ \forall \ h \in H$ and hence the right coset Ha is equal to the corresponding left coset aH. But if the group G is not abelian, then we may have $aH = Ha$ or $aH \neq Ha$.

Illustration. Consider the additive group of integers $(Z, +)$, where $Z = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$ and $H = 3Z = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$ be a subgroup of $(Z, +)$. Let us form the right coset of H in $(Z, +)$ as given below :

$0 \in G$ and $H = H + 0 = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$

$1 \in G$ and $H + 1 = \{1 + 0, 1 \pm 3, 1 \pm 6, \cdots\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$

$2 \in G$ and $H + 2 = \{2 + 0, 2 \pm 3, 2 \pm 6, \cdots\} = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$

$3 \in G$ and $H + 3 = \{3 + 0, 3 \pm 3, 3 \pm 6, \cdots\} = \{0, \pm 3, \pm 6, \cdots\} = H$

Similarly $H + 4 = H + 1, H + 5 = H + 2$,

$H + (-1) = H + 2, H + (-2) = H + 1$ and so on.

Thus, we get only three distinct right cosets $H, H + 1, H + 2$.

Obviously $Z = H \cup (H + 1) \cup (H + 2)$.

Theorem 1. If H is any subgroup of a group G and $h \in H$, then $Hh = H = hH$.

Proof. Let $h \in H$ and hh_1 be an arbitrary element of hH.

Then $h_1 \in H$ by definition of *left coset*

Since H is a subgroup and $h, h_1 \in H$, so $hh_1 \in H$. Thus every element of hH is an element of H. Hence $hH \subset H$ ... (i)

Again let $h_1 \in H$ be arbitary.

Now $h_1 = (hh^{-1})h_1 = h(h^{-1}h_1) \in hH$

$[\because h \in H \Rightarrow h^{-1} \in H$ and $h_1, h^{-1} \in H \Rightarrow h^{-1}h_1 \in H]$

Thus every element h_1 of H is also an element of hH.

Hence $H \subset hH$ ... (ii)

From (i) and (ii), $hH = H$. Similarly it can be proved that $Hh = H$.

Theorem 2. Let H be a subgroup of a group G and let $a, b \in G$. Then (i) $aH = bH$ if and only if $a^{-1}b \in H$ (ii) $Ha = Hb$ if and only if $ba^{-1} \in H$.

Proof. (i) Let $aH = bH$

Then for some $h_1, h_2 \in H$, $ah_1 = bh_2 \Rightarrow a^{-1}b = h_1h_2^{-1}$

But $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$, as H is a subgroup of G.

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

Conversely, let $a^{-1}b \in H$.

Then $a^{-1}bH = H$ [$\because h \in H \Rightarrow hH = H$ by Theorem 1]

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

(ii) Proof is similar to (i)

Theorem 3. Any two right or left cosets of a subgroup are either disjoint or identical.

Proof. Let H be a subgroup of a group G and Ha, Hb be two right cosets of H in G. Suppose Ha and Hb are not disjoint i.e. $Ha \cap Hb \neq \phi$. So let $x \in Ha \cap Hb \Rightarrow x \in Ha$ and $x \in Hb$.

Let $x = h_1a$ and $x = h_2b$ for some $h_1, h_2 \in H$

$\therefore h_1a = h_2b \Rightarrow ba^{-1} = h_2^{-1}h_1$

But $h_1, h_2 \in H \Rightarrow h_2^{-1}h_1 \in H$ [$\because H$ is a subgroup]

$\therefore ba^{-1} \in H \Rightarrow Ha = Hb$ [by (ii) of Theorem 2]

Therefore the two right cosets are identical if they are disjoint.

Thus either $Ha \cap Hb = \phi$ or $Ha = Hb$.

Similarly we can prove that either

$$aH \cap bH = \phi \text{ or } aH = bH.$$

Theorem 4. Let H be a subgroup of a group G. Then there is a one-to one correspondence between any two right (left) cosets of H in G.

Proof. Let Ha, Hb be any two right cosets of H in G where $a, b \in G$.

Let us define a mapping $f : Ha \to Hb$ by $f(ha) = hb \; \forall \; h \in H$.

Let $h_1a, h_2a \in Ha$, $h_1, h_2 \in H$

Then $f(h_1 a) = h_1 b$, $f(h_2 a) = h_2 b$

Now $f(h_1 a) = f(h_2 a) \Rightarrow h_1 b = h_2 b \Rightarrow h_1 = h_2$, by right cancellation law

$\Rightarrow h_1 a = h_2 a$ $\quad \therefore f$ is one-one.

Let $h_3 b$ be any arbitrary element of Hb. Then $h_3 b \in Hb \Rightarrow h_3 \in H \Rightarrow h_3 a \in Ha$. Now $f(h_3 a) = h_3 b$. Thus $h_3 b \in Hb \Rightarrow$ there exist $h_3 a \in Ha$ such that $f(h_3 a) = h_3 b$. So f is onto.

Hence the result.

Similarly it can be shown that there is a one-to-one correspondence between any two left cosets of H in G.

Note. *Since H itself is a right as well as a left coset, so the number of elements in any coset (left or right) of H in G is equal to the number of elements in H i.e., $0(H)$. Hence $0(Ha) = 0(Hb) = 0(H)$.*

Theorem 5. Let H be a subgroup of a group G. Then there is a one-to-one correspondence between the set of left and the set of right cosets of H in G.

Proof : Let U and V denote the sets of left and right cosets of H in G respectively. Let us define a mapping $f: U \to V$ by $f(aH) = Ha^{-1} \quad \forall a \in G$ and $aH \in U$.

Obviously Ha^{-1} is a right coset and hence $Ha^{-1} \in V$.

We have

$aH = bH \Rightarrow a^{-1}b \in H \Rightarrow a^{-1}\left(b^{-1}\right)^{-1} \in H \Rightarrow Ha^{-1} = Hb^{-1}$, by Th.2

$\Rightarrow f(aH) = f(bH) \quad \therefore f$ is well defined.

Now $f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow a^{-1} \circ \left(b^{-1}\right)^{-1} \in H$, by Th 2

$\Rightarrow a^{-1}b \in H \Rightarrow aH = bH$, by Th 2

$\therefore f$ is one-one.

Let Ha be any arbitrary element of V. Then $a^{-1}H \in U$ and $f\left(a^{-1}H\right) = H\left(a^{-1}\right)^{-1} = Ha$.

Thus $Ha \in V \Rightarrow \exists\, a^{-1}H \in U$ such that $f\left(a^{-1}H\right) = Ha$.

So f is onto. Hence the result.

Note : *From the above theorem we conclude that the number of distinct right cosets of H in G is equal to the number of distinct left cosets of H in G i.e. $O(Ha) = O(Hb)$.*

Index of a subgroup.

Let H be a subgroup of a group G. Then the number of distinct right (left) cosets of H in G is called the *index* of H in G and is denoted by $[\, G : H \,]$ or by $i_G(H)$.

Theorem 6. (Lagrange's Theorem) : The order of each subgroup of a finite group is a divisor of the order of the group.

[W.B.U.T. 2004, 2014]

Proof. Let H be a subgroup of a finite group G.

Also let $0(G) = n$ and $0(H) = m$. Let $H = \{h_1, h_2, \cdots, h_m\}$.

Then each right coset $Ha \; \forall\, a \in G$ has m distinct element $h_1a, h_2a, \cdots, h_ma$, as $h_ia = h_ja \Rightarrow h_i = h_j$ by right cancellation law.

Since G is finite, the number of distinct right (or left) cosets of H is G is finite, k, say. Let $Ha_1, Ha_2, \cdots, Ha_k$ be k distinct right (or left) cosets of H in G. Then these right cosets are disjoint and hence

$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$

$\Rightarrow O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k)$

$\Rightarrow O(G) = m + m + \cdots + m$ to k times $\Rightarrow n = km \Rightarrow k = \frac{n}{m}$

$\Rightarrow O(H)$ is a divisor of $O(G)$.

Note. *(1) The index of H in $G = \dfrac{0(G)}{0(H)}$*

(2) If G is a group of prime order p, then G can have no proper subgroups.

(3) The converse of the above theorem is not true. For example the alternating group A_4 is of order 12 but there is no subgroup of A_4 of order 6, though 6 is a divisor of 12 (for details see Alternating group, of Art 5.2.5.)

Theorem 7. Every group of prime order is cyclic

[W.B.U.T. 2007, 2014]

Proof. Let G be a group of prime order p. Since p is a prime, $0(G) > 1$ and hence G has an element $a \neq e$. Let H be a cyclic subgroup generated by a. Then $0(H) > 1$. By Lagrange's theorem $0(H)$ is a divisor of p. But p is prime. Therefore $0(H) = p$. Hence $H = G$. This shows that G is cyclic group.

Theorem 8. Let G be a group of finite order n and $a \in G$. Then $0(a)$ divides n and $a^n = e$.

Proof. Let H be a cyclic subgroup generated by a. Then by Lagrange's theorem $0(H)$ is a divisor of $0(G)$ i.e., n.

But $0(a) = 0(H)$. Consequently $0(a)$ is a divisor of n.

Let $0(a) = m$. Then $n = mk$ for some integer k.

Now $a^m = e$ and hence $a^n = a^{mk} = \left(a^m\right)^k = e$.

Theorem 9. (Fermat's Theorem) : If p is a prime number and a is any integer, then $a^p \equiv a(\text{mod } p)$.

Proof. Let G be the set of all non-zero residue classes of integers modulo p. Then G forms a group of order $p-1$ w.r.t. the multiplication of residue classes, as p is prime. The identity element of this group is [1].

Case (i) Let p be a divisor of a.

Then $[a]=[o]$ and so $[a] \notin G$.

But $p \mid a \Rightarrow p \mid a^p \Rightarrow p \mid a^p - a \Rightarrow a^p \equiv a(\text{mod } p)$

[Here we use the notation $a \mid b$ when a is a divisor of b]

Case (ii) Let p be not a divisor of a

Then $[a] \neq [0]$ and so $[a] \in G$

Hence by theorem 8, we have

$$[a]^{p-1} = [1] \Rightarrow \left[a^{p-1}\right] = [1] \Rightarrow a^{p-1} = 1 (\text{mod } p)$$

$$\Rightarrow p \mid \left(a^{p-1} - 1\right) \Rightarrow p \mid a\left(a^{p-1} - 1\right) \Rightarrow p \mid \left(a^p - a\right) \Rightarrow a^p \equiv a(\text{mod } p)$$

Theorem 10. Let H_1 and H_2 be finite subgroups of a group G. Then the order of the products of two subgroups H_1, H_2 i.e.

$$0(H_1 H_2) = \frac{0(H_1) \cdot 0(H_2)}{0(H_1 \cap H_2)}.$$

Proof. Beyond the scope of the book.

Illustrative Example.

Ex. 1. *Show that* $(Ha)^{-1} = a^{-1}H \ \forall a \in G$, *where* H *is a subgroup of a group* G.

Let $(ha)^{-1} \in (Ha)^{-1}$ be arbitary.

Then $ha \in Ha$ where $h \in H$

and $a^{-1}h^{-1} \in (Ha)^{-1}$

But $h \in H \Rightarrow h^{-1} \in H$, as H is a subgroup.

$\therefore a^{-1}h^{-1} \in a^{-1}H$ or, $(ha)^{-1} \in a^{-1}H \quad \therefore (Ha)^{-1} \subset a^{-1}H$ ... (i)

Next let $a^{-1}h \in a^{-1}H$ be arbitary.

Then $a^{-1}h = a^{-1}\left(h^{-1}\right)^{-1} = \left(h^{-1}a\right)^{-1} \in (Ha)^{-1}$, as $h^{-1} \in H$ and so $h^{-1}a \in Ha$.

$\therefore a^{-1}H \subset (Ha)^{-1}$ ... (ii)

From (i) and (ii), $(Ha)^{-1} = a^{-1}H \ \forall a \in G$.

Ex. 2. *Let* H *be a subgroup of a group* G *and define* $S = \{x \in G : xH = Hx\}$. *Prove that* S *is a subgroup of* G.

Let $x_1, x_2 \in S$. Then $x_1H = Hx_1, x_2H = Hx_2$

First we shall show that $x_2^{-1} \in S$.

We have $x_2H = Hx_2 \Rightarrow x_2^{-1}(x_2H)x_2^{-1} = x_2^{-1}(Hx_2)x_2^{-1}$

$\Rightarrow \left(x_2^{-1}x_2\right)Hx_2^{-1} = x_2^{-1}H\left(x_2x_2^{-1}\right) \Rightarrow Hx_2^{-1} = x_2^{-1}H \Rightarrow x_2^{-1} \in S$.

Now we shall show that $x_1x_2^{-1} \in S$

We have $\left(x_1x_2^{-1}\right)H = x_1\left(x_2^{-1}H\right) = x_1\left(Hx_2^{-1}\right)$ $\left[\because x_2^{-1} \in S \Rightarrow x_2^{-1}H = Hx_2^{-1}\right]$

$= (x_1H)x_2^{-1} = (Hx_1)x_2^{-1} = H\left(x_1x_2^{-1}\right)$ $\therefore x_1x_2^{-1} \in S$

Thus $x_1, x_2 \in S \Rightarrow x_1x_2^{-1} \in S$. Hence S is a subgroup of G.

Ex. 3. *Show that every proper subgroup of a group of order 6 is cyclic.*

Let G be a group of order 6 and H be a proper subgroup of G. Then $0(H)$ is a divisor of 6, by Lagrange's theroem. But divisors of 6 are 1,2, 3 and 6.

Since H is a proper subgroup of G, $0(H) < 6$.

If $0(H) = 1$, then $H = \{e\}$ which is a cyclic group. If $O(H) = 2$, then H is cyclic, as a group of prime order is cyclic. (Th-7, Th-8). If $O(H) = 3$, then also H is cyclic, as 3 is prime and a group of prime order is cyclic.

Thus every proper subgroup of such a group is cyclic.

Ex. 4. *Prove that a finite group cannot be expressed as the union of two of its proper subgroups.*

Let G be a group of order n and H_1, H_2 be its two proper subgroups. If possible, let $G = H_1 \cup H_2$ ... (i)

Since $e \in H_1, H_2$ and $G = H_1 \cup H_2$, so one of H_1 and H_2 (say H_1) must contain more than half of the elements of G.

Let $O(H_1) = m$. Then $\frac{n}{2} < m < n$. Hence m is not a divisor of n which is impossible by Lagrange's theorem. Therefore our assumption (1) is not correct. Thus a finite group cannot be expressed as the union of two of its proper subgroups.

4.2.4. Normal Subgroup

Definition. A subgroup H of a group G is said to be normal if $aH = Ha \quad \forall\, a \in G$. Then in symbol, we write $H \Delta G$.

[W.B.U.T. 2002,2005]

Note *(1) $aH = Ha$ does not imply that $ah = ha \; \forall\, h \in H$. But from the definition, it follows that every subgroup of a commutative group is a normal subgroup.*

(2) Every group G has at least two normal subgroups, namely G itself and {e}. These are called ***improper or trivial*** *normal subgroups. All others are called* ***proper*** *normal subgroups.*

(3) For normal subgroups left cosets and right cosets are same.

Simple Group. A group having no proper normal subgroups is called a *Simple Group.*

By Lagrange's Theorem, every group of prime order has no proper sub groups. Hence every group of prime order is simple.

Theorem 1. Let H be a subgroup of a group G. Then H is normal in G if and only if $xhx^{-1} \in H \quad \forall\, h \in H$ and $\forall\, x \in G$.

[W.B.U.T. 2004]

Proof. Let H be a normal subgroup of G.

Then $xH = Hx \; \forall\, x \in G$

Let $h \in H$. Then $xh = h_1 x$ for some $h_1 \in H$

$\Rightarrow xhx^{-1} = h_1 \Rightarrow xhx^{-1} \in H \quad [\because h_1 \in H]$

Next let $xhx^{-1} \in H \quad \forall\, h \in H$ and $\forall\, x \in G$

Let $a \in Hx \;\therefore\; a = h_2 x$ for some $h_2 \in H \Rightarrow$

$$a = (x\,x^{-1})h_2 x = x\left(x^{-1}h_2\left(x^{-1}\right)^{-1}\right)$$

$= xh_3$ where $h_3 = x^{-1}h_2\left(x^{-1}\right)^{-1} \in H$, as $x^{-1} \in G$

$\therefore \; a \in Hx \Rightarrow a \in xH \quad [\because xh_3 \in xH]$

$\therefore \; Hx \subset xH$ ... (i)

Next let $b \in xH \qquad \therefore b = xh_4$ for some $h_4 \in H \Rightarrow$

$b = xh_4\left(x^{-1}x\right) = \left(xh_4x^{-1}\right)x = h_5 x$ where $h_5 = xh_4x^{-1} \in H$

$\therefore b \in xH \Rightarrow b \in Hx \quad [\because h_5 x \in Hx]$

$\therefore xH \subset Hx$ ... (ii)

In virtue of (i) and (ii), we have, $xH = Hx \quad \forall\, x \in G$

Hence H is normal in G.

Theorem 2. A subgroup H of a group G is normal if and only if $xHx^{-1} = H \quad \forall\, x \in G$.

Proof. Let H be a normal subgroup of G. Then

$xH = Hx \quad \forall\, x \in G \Rightarrow xHx^{-1} = Hxx^{-1} \Rightarrow xHx^{-1} = He \Rightarrow xHx^{-1} = H$

Next let $xHx^{-1} = H \quad \forall\, x \in G$

Then $xHx^{-1}x = Hx \quad \therefore\; xHe = Hx \qquad \therefore\; xH = Hx \quad \forall\, x \in G$

Hence H is a normal subgroup of G.

Theorem 3. A subgroup H of a group G is a normal subgroup of G if and only if each left cosets of H in G is a right coset of H in G.

Proof. Let H be a normal subgroup of G. Then $aH = Ha \; \forall \; a \in G$.

So each left coset of H in G is a right coset of H in G.

Next let each left coset of H in G is a right coset of H in G and a be any element of G. Then $aH = Hb$ for some $b \in G$.

Since $e \in H$, so $ae \in aH$ i.e. $a \in aH$.

$\therefore \; a \in Hb \; [\because aH = Hb]$

$\therefore \; a = h_1 b$ for some h_1 in H or, $ab^{-1} = h_1$ ... (1)

Now we shall show $Hb = Ha$.

Let $x \in Hb \; \therefore \; x = h_2 b$ for some h_2 in H

or, $x = h_2 h_1^{-1} h_1 b = h_2 h_1^{-1} ab^{-1} b$ using (1)

$= h_2 h_1^{-1} a = h_3 a$ where $h_3 = h_2 h_1^{-1} \in H$ as H is subgroup.

So $x \in Ha$. Thus $Hb \subset Ha$.

Now let $y \in Ha \; \therefore \; y = h_3 a$ where $h_3 \in H$.

or, $y = h_3 h_1 h_1^{-1} a = h_3 h_1 \left(ab^{-1}\right)^{-1} a$ using (1)

or, $y = h_3 h_1 ba^{-1} a = h_3 h_1 b = h_4 b$

where $h_4 = h_3 h_1 \in H$ as H is subgroup.

$\therefore \; y \in Hb$. Thus $Ha \subset Hb$.

Hence $Hb = Ha$.

Therefore $aH = Ha \; (\because Hb = Ha) \; \therefore \; H$ is normal subgroup.

Theorem 4. The intersection of any two normal subgroups of a group is a normal subgroup.

Proof. Let H_1 and H_2 be any two normal subgroups of a group G. Then $H_1 \cap H_2$ is a subgroup of G as H_1 and H_2 are subgroups of G. Let x be any element of G and $h \in H_1 \cap H_2$. Then $h \in H_1$ and $h \in H_2$.

$\therefore \; xhx^{-1} \in H_1$ [$\because H_1$ is a normal subgroup of G]

and $xhx^{-1} \in H_2$ [$\because H_2$ is a normal subgroup of G]

$\therefore \; xhx^{-1} \in H_1 \cap H_2$

$\therefore \; x \in G$ and $h \in H_1 \cap H_2 \Rightarrow xhx^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is a normal subgroup of G.

Note. *The intersection of any collection of normal subgroups of a group is a normal subgroup of G.*

Illustrative Example.

Ex. 1. *Show that every subgroup of a cyclic group is normal.*

Let G be a cyclic group and H be a subgroup of G.

Let $x \in G$ and $h \in H$.

Then $xhx^{-1} = x\,x^{-1} h$

[$\because$ G is cyclic, so G is abelian $\Rightarrow x^{-1}h = hx^{-1}$]

$= e\,h = h \in H \quad \therefore \; x \in G, \; h \in H \Rightarrow xhx^{-1} \in H$

Hence H is a normal subgroup of G.

Ex. 2. *If G is a group and H is a subgroup of index 2 in G, prove that H is a normal subgroup of G.* [*W.B.U.T. 2005, 2015*]

Since the index of H in G is 2, so there are only two distinct left (right) cosets of H in G and the two distinct left cosets are H, $G - H$. Also, the two distinct right cosets are H, $G - H$.

Let $x \in H$. Then $xH = H$ and $Hx = H \quad \therefore \; xH = Hx$.

Next let $x \notin H$. Then $x \in G - H$

$\therefore \; xH = G - H$, as $G - H$ is the only left coset

Also, $Hx = G - H$ as $G - H$ is the only right coset.

Hence $xH = Hx \; \forall \; x \in G$

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

Ex. 3. *Show that the centre of a group G, given by*

$$Z(G) = \{a \in G : ag = ga \; \forall \; g \in G\}$$

is a normal subgroup of G.

We have already proved in a previous Example that $Z(G)$ is a subgroup of G.

Now for any $g \in G$ and any $a \in Z(G)$

$$gag^{-1} = agg^{-1} = a \cdot e = a \in Z(G)$$

$$\therefore\ g \in G, a \in Z(G) \Rightarrow gag^{-1} \in Z(G)$$

Hence $Z(G)$ is a normal subgroup of G.

Ex. 4. *If H is a subgroup of G and N is a normal subgroup of G, show that $H \cap N$ is a normal subgroup of H.*

Since H and N are subgroups of G, so $H \cap N$ is also a subgroup of G but $H \cap N \subset H$. Therefore $H \cap N$ is a subgroup of H.

Let $x \in H$ and $h \in H \cap N$. Then $h \in H$ and $h \in N$.

So, $xhx^{-1} \in N$, as N is normal. Also $x \in H,\ h \in H \Rightarrow xhx^{-1} \in H$ as H is a subgroup of G.

Hence $xhx^{-1} \in H \cap N, \forall\ x \in N, h \in H \cap N$. Consequently $H \cap N$ is a normal subgroup of H.

Ex. 5. *Prove that a normal subgroup of a group G is commutative with every non-empty subset of G.*

Let K be a normal subgroup and H be a non-empty subset of G. We now prove that $KH = HK$

Let $kh \in KH$ where $k \in K,\ h \in H$.

Then $kh = \left(hh^{-1}\right)kh = h\left(h^{-1}k\left(h^{-1}\right)^{-1}\right) = hk_1$

where $k_1 = h^{-1}k\left(h^{-1}\right)^{-1} \in K$

$\therefore\ kh \in Hk\ \left[\because\ hk_1 \in Hk\right]$ $\qquad \therefore\ KH \subset Hk \qquad \ldots \qquad$ (i)

Again let $h_2k_2 \in HK$ where $h_2 \in H,\ k_2 \in K$

Then $h_2k_2 = h_2k_2\left(h_2^{-1}h_2\right) = \left(h_2k_2h_2^{-1}\right)h_2 = k_3h_2$

where $k_3 = h_2k_2h_2^{-1} \in K$

$\therefore\ h_2k_2 \in KH\ \left[\because\ k_3h_2 \in KH\right]$ $\qquad \therefore HK \subset KH \qquad \ldots \qquad$ (ii)

$\therefore$ In virtue of (i) and (ii), we have, $HK = KH$.

Ex. 6. *If a cyclic subgroup N of G is normal in G, show that every subgroup of N is normal in G.*

Let $N = \langle a \rangle$ for some $a \in G$ and H be a subgroup of N. Then H is cyclic, as every subgroup of a cyclic group is cyclic.

Let $H = \left\langle a^m \right\rangle$ for some positive integer m.

Let $x \in G$ and $h = \left(a^m\right)^r \in H$

$$\therefore\ xhx^{-1} = x\left(a^m\right)^r x^{-1} = x\left(a^r\right)^m x^{-1}$$

$$= \left(x\,a^r\,x^{-1}\right)\left(x\,a^r\,x^{-1}\right) \quad \ldots \text{ to } m \text{ factor} \quad = \left(xa^rx^{-1}\right)^m$$

Now $a^r \in N$ and $x \in G$, so $xa^rx^{-1} \in N$ as N is normal in G.

$\therefore\ xa^rx^{-1} = a^s$ for some integer s

Then $xhx^{-1} = \left(a^s\right)^m = \left(a^m\right)^s \in H$

$\therefore\ xhx^{-1} \in H\ \ \forall\ x \in G$ and $\forall\ h \in H\ \therefore\ H$ is normal in G.

Ex. 7. *Prove that the set of matrices*

$$H = \left\{\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in R, x \neq 0\right\}$$

forms a normal subgroup of $GL(2, R)$, the group of all real non-singular 2×2 matrices. [*W.B.U.T. 2008*]

Let $A = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in H,\ B = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \in H$

Then $x \in R,\ x \neq 0$ and $y \in R,\ y \neq 0$

Now $|B| = y^2 \neq 0\ \ \therefore B^{-1}$ exists.

$$\therefore\ B^{-1} = \frac{1}{y^2}\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} \frac{1}{y} & 0 \\ 0 & \frac{1}{y} \end{pmatrix}$$

$$\therefore\ AB^{-1} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} \frac{1}{y} & 0 \\ 0 & \frac{1}{y} \end{pmatrix} = \begin{pmatrix} \frac{x}{y} & 0 \\ 0 & \frac{x}{y} \end{pmatrix} \in H, \text{ as } \frac{x}{y} \neq 0 \text{ and } \frac{x}{y} \in R$$

$\therefore\ A, B \in H \Rightarrow AB^{-1} \in H\ \ \therefore\ H$ is a subgroup of $GL(2, R)$.

Next let $C=\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in G$, whose determinant, $|C| \neq 0$

$$\therefore C^{-1} = \frac{1}{x_1y_2 - x_2y_1}\begin{pmatrix} y_2 & -y_1 \\ -x_2 & x_1 \end{pmatrix}$$

$$\therefore CAC^{-1} = \frac{1}{x_1y_2 - x_2y_1}\begin{pmatrix} x_1 & y_1 \\ x_2 & x_1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} y_2 & -y_1 \\ -x_2 & x_1 \end{pmatrix}$$

$$= \frac{1}{x_1y_2 - x_2y_1}\begin{pmatrix} xx_1y_2 - xy_1x_2 & 0 \\ 0 & -xy_1x_2 + xx_1y_2 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in H.$$

$\therefore A \in H,\ C \in G \Rightarrow CAC^{-1} \in H$

$\therefore H$ is a normal subgroup of $GL(2, R)$.

Ex. 8. *If H is subgroup of G, let $N(H)=\{g \in G : gHg^{-1} = H\}$. Show that* (i) $N(H)$ is a subgroup of G

(ii) H is a normal subgroup of $N(H)$.

(i) Let $a, b \in N(H)$. Then $aHa^{-1} = H,\ bHb^{-1} = H$

Now $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1})b = b^{-1}Hb \Rightarrow (b^{-1}b)H(b^{-1}b) = b^{-1}Hb$.

$\Rightarrow H = b^{-1}Hb$.

$\therefore (ab^{-1})H(ab^{-1})^{-1} = ab^{-1}Hba^{-1} = a(b^{-1}Hb)a^{-1} = aHa^{-1} = H$

Hence $ab^{-1} \in N(H)$. Thus $a, b \in N(H) \Rightarrow ab^{-1} \in N(H)$

$\therefore N(H)$ is a subgroup of G.

(ii) Next let $h \in H$. Then $hHh^{-1} = H$, as H is a subgroup. Hence $h \in N(H)$.

$\therefore H \subset N(H)$

Now $N(H)$ is a subgroup of G, H is a subgroup of G and $H \subset N(H)$. So H is a subgroup of $N(H)$

Let $p \in N(H)$. Then $pHp^{-1} = H\ \forall p \in N(H)$.

Therefore H is a normal subgroup of $N(H)$.

4.2.5. Permutation Group.

Permutation.

Let S be a finite set having n distinct elements. Then an one-one mapping of S onto itself is called a permutation on S of degree n.

Let $S = \{a_1, a_2, \cdots, a_n\}$ be a finite set having n distinct elements and $f : S \to S$ be a bijective mapping defined by

$$f(a_i) = b_i\ (i = 1, 2, \cdots, n).$$

Then the permutation f can be written as

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix} \text{ or } \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}.$$

Here $\{a_1, a_2, \cdots, a_n\} = \{b_1, b_2, \cdots, b_n\}$ i.e., $b_1, b_2, \cdots, b_n$ is nothing but some arrangement of $a_1, a_2, \cdots, a_n$.

Total number of distinct permutations of degree n is $n!$. The set of all distinct permutation of degree n is called the *symmetric set of permutations of degree n* and is denoted by P_n or S_n.

For example, if $S = \{1, 2, 3, 4\}$, then

$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ etc. are all permutation of degree 4.

Equality of two Permutations.

Two permutations f_1 and f_2 of same degree are said to be equal if $f_1(a) = f_2(a)\ \forall a \in S$.

For example, if $f_1 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, $f_2 = \begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$ are two permutation of degree 3, then $f_1 = f_2$.

Identity Permutation.

A bijective mapping $I : S \to S$ defined by

$I(a_i) = a_i\ (i = 1, 2, \cdots, n)$ is called the *Identity Permutaion.*

Thus $I = \begin{pmatrix} a_1 a_2 \cdots a_n \\ a_1 a_2 \cdots a_n \end{pmatrix}$ or more precisely, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ etc.

Product or Composite of two Permutations

Let $f: S \to S$ and $g: S \to S$ be two permutations on S. Then the composite mapping $f \circ g: S \to S$ is bijective, as f and g are bijective mapping. So $f \circ g$ is a permutation on S and is denoted by fg.

Thus $fg = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ fg(a_1) & fg(a_2) & \cdots & fg(a_n) \end{pmatrix}$

Similarly gf is also a permutation and

$$gf = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ gf(a_1) & gf(a_2) & \cdots & gf(a_n) \end{pmatrix}.$$

Note. (1) *In general $fg \neq gf$, as the composition of mappings is not commutative.*

(2) *Multiplication of permutation is associative, as the composition of mappings is associative. Thus*

$$(fg)h = f(gh) \quad \forall f, g, h \in S_n.$$

Illustration. Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Then $fg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

and $gf = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Obviously $fg \neq gf$.

Inverse of a Permutation.

Let $f: S \to S$ be a permutation on S. Then f is a bijective mapping which has unique inverse $f^{-1}: S \to S$ and f^{-1} is also bijective. Thus f^{-1} is permutation on S and $f f^{-1} = f^{-1} f = I$.

Thus, if $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$, then $f^{-1} = \begin{pmatrix} f(a_1) & f(a_2) & \cdots & f(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$.

Illustration. The inverse of the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ is $f^{-1} = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Cyclic Permutations.

Let $f: S \to S$ be a permutation on $S = \{a_1, a_2, a_3, \cdots, a_n\}$ defined by

$f(a_i) = a_{i+1}, \ i = 1, 2, \cdots, m-1$

$f(a_m) = a_1, \ f(a_i) = a_i, \ i = m+1, m+2, \cdots, n$

Then f can be written as

$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_m & a_{m+1} & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & a_1 & a_{m+1} & \cdots & a_n \end{pmatrix}$ or, $f = (a_1, a_2, a_3, \cdots, a_m)$.

This permutation f is called a *cyclic permutation* or *a cycle of length m* or *m-cycle.*

For example, the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 5 & 6 \end{pmatrix}$ is cyclic which can also be represented by the cycle $(1\ 2\ 4\ 3)$.

Again a cycle can also be represented by a permutation .

For example, let $(1\ 3\ 4\ 2)$ be a cycle of length 4 on the set $\{1, 2, 3, 4, 5, 6\}$. Then the corresponding permutation represented will be

$$\begin{pmatrix} 1 & 3 & 4 & 2 & 5 & 6 \\ 3 & 4 & 2 & 1 & 5 & 6 \end{pmatrix} \text{ i.e. } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 5 & 6 \end{pmatrix}.$$

Note. (1) *A cycle remains unaltered by changing places of its elements without changing the cyclic order of the elements, viz,*

$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$, $(1\ 2) = (2\ 1)$, $(3\ 4) = (4\ 3)$.

(2) *Every cycle of length one will represent the identity permutation.*

Transpositions. A cycle of length two is called a transposition. Thus the cycle (2, 3) is a transposition.

Disjoint Cycles. Two cycles are said to be disjoint if they have no common elements.

For example (1 3 5) and (2 8) are disjoint cycles on the set $\{1,2,3,4,5,6,7,8,9\}$.

Multiplication of Cycles. Multiplication of cycles is the multiplication of permutations represented by them.

For example, if (1 2 3) and (5 4 1) are two cycles on the set $\{1,2,3,4,5\}$ then $(1\ 2\ 3)(5\ 4\ 1)=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&2&3&1&4\end{pmatrix}$

$=\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}=(1\ 5\ 4\ 2\ 3)$

Since a cycle of length one represents the identity permutation, so $(1)(2\ 3\ 4)(5)=(2\ 3\ 4)$.

Inverse of a Cyclic Permutation.

The inverse of a cyclic permutation $(1,2,3,\cdots,n)$ is

$(n,n-1\cdots3,2,1)$ i.e. $(1\ 2\ 3\ \cdots\ n)^{-1}=(n\ \ n-1\ \cdots\ 3\ \ 2\ \ 1)$.

Note. *Every transposition is its own inverse, as* $(1\ 2)^{-1}$ $=(2\ 1)=(1\ 2)$.

Index Law of Permutation

Let f be a permutation on a set S. Then $f\cdot f$ (the composite of f and f) is also a permutation on S and is denoted by f^2.

$\therefore\ f^2=f\cdot f$

Similarly $f^3=f^2\cdot f=f\cdot f\cdot f$.

In this way we define $f^n=f\cdot f\cdot f\cdots n$ factors, $\forall\ n\in N$

Again f^{-1} is a permutation on S. So $f^{-1}\cdot f^{-1}$ is also a permutation on S and is denoted by f^{-2}.

$\therefore\ f^{-2}=f^{-1}\cdot f^{-1}$. Similarly $f^{-3}=f^{-1}\cdot f^{-1}\cdot f^{-1}$

In this way we define $f^{-n}=f^{-1}\cdot f^{-1}\cdot f^{-1}\cdots n$ factors, $\forall\ n\in N$.

Also we define $f^0=I$, the identity permutation

Thus f^n is defined for all integral values of n.

Now the index laws (i) $f^m\cdot f^n=f^{m+n}$ (ii) $(f^m)^n=f^{mn}$ holds for all $m,n\in Z$.

Order of a Permutation.

Let f be a permutation on a finite set. Then the order of f is the least positive integer n such that $f^n=I$, the identity permutation.

Theorem 1. Every permutation on a finite set is either a cycle or it can be expressed as a product of some disjoint cycles.

Proof. Beyond the scope of the book.

Verification of the Theorem.

Consider the permutation $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&3&4&2&5&7&8&6&9\end{pmatrix}$ of degree 9 on the set $\{1,2,\cdots,9\}$.

Then f can be expressed as the product of five disjoint cycles as $f=(1)(2\ 3\ 4)(5)(6\ 7\ 8)(9)$

Theorem 2. The order of a permutation of a finite set is L.C.M of the lengths of its disjoint cycles.

Proof. Beyond the scope of the book.

Note. *The order of an m- cycle is m.*

Theorem 3. Every cycle can be expressed as a product of transposition in infinitely many ways.

Proof. Beyond the scope of the book.

Verification of the Theorem.

Consider the 4- cycle $f=(2\ 3\ 5\ 4)$ on the set $\{1, 2, 3, 4, 5\}$. Then f can be expressed as

$f=(2,4)(2,5)(2,3)$.

Again $f=(2\ 3\ 5\ 4)=(3\ 5\ 4\ 2)=(3,2)(3,4)(3,3)$

As $(1\ 2)(2\ 1)=$ Identity permutation, so we can write f as

$f=(2,4)(2,5)(2,3)(1\ 2)(2\ 1)$ and so on.

Theorem 4. Every permutation can be expressed as the product of transpositions in infintiely many ways.

Proof. Beyond the scope of the book.

Even and Odd Permutations.

A permutation is said to be an even permutation if it can be expressed as the product of an even number of transposition ; otherwise it is said to be an odd permutation.

Illustration. Consider the permutation $f=\begin{pmatrix}1&2&3&4&5&6\\3&6&4&5&1&2\end{pmatrix}$ which is an even permutation, as

$f=(1\ 3\ 4\ 5)(2\ 6)=(1\ 5)(1\ 4)(1\ 3)(2\ 6)$.

Note. (1) *A cycle of length n can be expressed as the product of* $(n-1)$ *transpositions.*

(2) *Identity permutation is always an even permutation.*

(3) *The product of two even or odd permutations is even but the product of an even and an odd permutation is odd.*

Theorem 5. The number of even permutations on a finite set (containing at least two elements) is equal to the number of odd permutation on it.

Proof. Beyond the scope of the book.

Alternating Set of Permutation.

The set of all even permutations of degree n is called alternating set of permutations.

Note : *Then* $0(A_n)=\frac{n!}{2}$, *since,* $A_n \subset S_n$. *and* $0(S_n)=n!$.

Theorem 6. The set P_n of all permutations of degree n on n symbols forms a group w.r.t permutation multiplication.

Proof. Let $S=\{a_1,a_2,\cdots,a_n\}$ be a finite set having n distinct elements. Here $P_n=\{f : f$ is a permutation of degree n on $S\}$.

(i) Let $f_1,\ f_2 \in P_n$.

Then $f_1f_2 \in P_n$, as the product of two permutations on S is a permutation on S. So P is closed.

(ii) Let $f_1,f_2,f_3 \in P_n$. Then

$(f_1f_2)f_3=f_1(f_2f_3)$, as the composition of mappings is associative. So permutation multiplication is associative.

(iii) The identity permutation I is the identity element of P_n as $If=fI=f\ \ \forall f \in P_n$.

(iv) Let $f=\begin{pmatrix}a_1&a_2&\cdots&a_n\\f(a_1)&f(a_2)&\cdots&f(a_n)\end{pmatrix}\in P_n$

Then $f^{-1}=\begin{pmatrix}f(a_1)&f(a_2)&\cdots&f(a_n)\\a_1&a_2&\cdots&a_n\end{pmatrix}\in P_n$ and $ff^{-1}=f^{-1}f=I$.

So every element of P_n possesses inverse.

Thus P_n forms a group w.r.t permutation multiplication.

Permutation Group or Symmetric Group.

The group of all permutations of degree n is known as Permutation Group or *Symmetric group of degree n and* is denoted by S_n or P_n.

Note. *This group is non-abelian since* $f_1f_2 \neq f_2f_1$ *in general.*

Theorem 7. The set A_n of all even permutations of degree n forms a group w.r.t permutations multiplication.

Proof. (1) As the product of two even permutation is also an even permutation, so the set A_n is closed.

(ii) The multiplication of permutation is associative on the set P_n and $A_n \subset P_n$. So the multiplication of permutation is associative on A_n.

(iii) If I is the identity permutation of degree n, then I is an even permutation and so $I \in A_n$. Also $If=fI=f\ \ \forall f \in A_n$.

Therefore I is the identity element of A_n.

(iv) Let $f \in A_n$. Then f is an even permutation and so f^{-1} is also an even permutation because $f^{-1}f=I$, an even permutation.

Therefore $f^{-1} \in A_n$.

So every element of A_n possesses inverse.

Thus A_n forms a group w.r.t permutation multiplication.

Alternating Group : The group of all even permutations of degree n is called Alternating Group.

Note. (1) *Here also* $(A_n, \cdot)$ *is non-abelian for* $n>2$.

(2) *In fact* A_n *is a subgroup of* S_n.

(3) *The total number of all even permutations of degree* n *is* $\frac{n!}{2}$. *So order of the alternating group* $(A_n, \cdot)$ *is* $\frac{n!}{2}$.

(4) *As the product of two odd permutations is an even permutation, so the set of all odd permutations is not closed w.r.t multiplication and hence will not form a group.*

Illustrative Examples.

Ex. 1. *Let* $A=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$, $B=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$ *be two permutations. Show that* $AB \neq BA$. [W.B.U. Tech 2004]

We have $AB=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}$

and $BA=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$

Thus $AB \neq BA$.

Ex. 2. *Find the order and inverse of the following permutations :*

(i) $\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$ (ii) $\begin{pmatrix}1&2&3&4&5&6\\3&1&6&5&4&2\end{pmatrix}$

(i) Let $\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}=(1\ 3\ 2\ 4)$

So, A is a cycle of length 4. Hence the order of A is 4. Also the inverse of A is $A^{-1}=\begin{pmatrix}3&4&2&1\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$

(ii) Let $A=\begin{pmatrix}1&2&3&4&5&6\\3&1&6&5&4&2\end{pmatrix}$

A can be written as the product of two cycles $(1\ 3\ 6\ 2),(4\ 5)$

The length of these cycles are 4, 2. So the L.C.M of the length is 4. Hence the order of A is 4.

Again $A^{-1}=\begin{pmatrix}3&1&6&5&4&2\\1&2&3&4&5&6\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&5&4&3\end{pmatrix}$

Ex. 3. *Show that the set* S_3 *of all permutations on three symbols 1, 2, 3 forms a finite non-abelian group of order 6 w.r.t permutation multiplication.*

Here $S_3=\{I,(1\,2),(2\,3),(3\,1),(1\,2\,3),(1\,3\,2)\}$ where I is the identity permutation.

Let $I=f_1,\ (1\ 2)=f_2,(2\ 3)=f_3,\ (3\ 1)=f_4,(1\ 2\ 3)=f_5,(1\ 3\ 2)=f_6$

Then the composition table of the groupoid $(S_3, \circ)$ is given below

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

[$\because f_2f_4=(1\ 2)\ (3\ 1)=(1\,2\,3)=f_5,\ f_2f_3=(1\ 2)\ (2\ 3)=(1\,3\,2)=f_6$,

$f_3f_3=(2\ 3)\ (2\ 3)=f_1, f_5f_5=(1\ 2\ 3)\ (1\ 2\ 3)=(1\ 3\ 2)=f_6$ and so on]

(i) From the above table it is clear that the product of any two elements of S_3 is an element of S_3. So S_3 is closed.

(ii) Since multiplication of permutation is associative in S_n of all permutation of degree n, so it holds for S_3.

(iii) From the table, it is clear that f_1 is the identity element in S_3.

(iv) From the table, it is obvious that the inverse of $f_1, f_2, f_3, f_4, f_5, f_6$ are $f_1, f_2, f_3, f_4, f_6, f_5$ respectively.

Thus every element of S_3 possesses inverse.

(v) As $f_2 f_3 = f_5, f_3 f_2 = f_6$, so $f_2 f_3 \neq f_3 f_2$. Hence the multiplication of permutation is not commutative.

Thus the set S_3 forms a non-abelian group of order 6 w.r.t permutation- multiplication.

Ex. 4. *Find all cyclic subgroups of the symmetric group* S_3.

The elements of S_3 are $f_1, f_2, f_3, f_4, f_5, f_6$ where f_1 is the identity element (for details see previous Example)

$\therefore \langle f_1 \rangle = \{f_1\}$

$\langle f_2 \rangle = \{f_1, f_2\}$, as $f_2^2 = f_1$

$\langle f_3 \rangle = \{f_1, f_3\}$, as $f_3^2 = f_1$

$\langle f_4 \rangle = \{f_1, f_4\}$, as $f_4^2 = f_1$

$\langle f_5 \rangle = \{f_1, f_5, f_6\}$, as $f_5^2 = f_6$, $f_5^3 = f_1$

$\langle f_6 \rangle = \{f_1, f_5, f_6\}$, as $f_6^2 = f_5$, $f_6^3 = f_1$

Thus the cyclic subgroups are $(\{f_1\}, \circ)$ $(\{f_1, f_5, f_6\}, \circ)$,

$(\{f_1, f_3\}, \circ), (\{f_1, f_4\}, \circ), (\{f_1, f_2\}, \circ)$

Ex. 5. *Show that the symmetric group* S_3 *is not cyclic.*

If possible let the symmetric group S_3 is cyclic. Then it is abelian, as every cyclic group is abelian. But this contradicts the fact that the symmetric group S_3 is non-abelian. Hence S_3 is not cyclic.

Alternative Solution : According to Ex. 2., the order of f_2, f_3, f_4, f_5, f_6 are $2, 2, 2, 3, 3$ respectively . So there exists no element of order 6 in S_3 . Hence S_3 is not cyclic.

Ex. 6. *Show that the alternating group* A_3 *is a normal subgroup of* S_3.

Let $\alpha \in S_3$, $\beta \in A_3$.

Then β is an even permutation and α may be odd or even. We now show that $\alpha\beta\alpha^{-1}$ is an even permutation.

Let α be odd. Then α^{-1} is also odd. Now $\alpha\beta$ is odd, as the product of an even and odd permutation is odd.

Consequently $\alpha\beta\alpha^{-1}$ is even, as the product of two odd permutations is even.

Next let α be even. Then α^{-1} is also even. Now $\alpha\beta$ is even, as the product of two even permutations is even.

Consequently $\alpha\beta\alpha^{-1}$ is even.

Thus $\alpha \in S_3, \beta \in A_3 \Rightarrow \alpha\beta\alpha^{-1} \in A_3$.

Hence A_3 is a normal subgroup of S_3.

Ex. 7. *Find four symmetries of a rectangle (not square) and show that they form an abelian group.*

Let us consider a rectangle $ABCD$ with centre 0.

Then four symmetries of $ABCD$ are

$I =$ No rotation (i.e. rotation through 0°)

$r_1 =$ reflection about OX

$r_2 =$ reflection about OY

$r_3 =$ rotation about OZ through 180° in the anti-clockwise direction.

Let '$\circ$' be the composition of mappings.

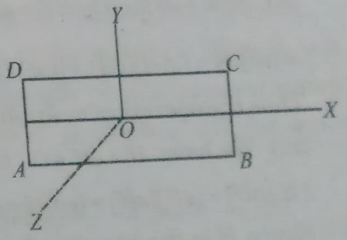
Then obviously

$r_i \circ I = I \circ r_i = r_i \ (i = 1, 2, 3)$

$I \circ I = r_1 \circ r_1 = r_2 \circ r_2 = r_3 \circ r_3 = I$

$r_1 \circ r_2 = r_2 \circ r_1 = r_3, \ r_1 \circ r_3 = r_3 \circ r_1 = r_2$

$r_2 \circ r_3 = r_3 \circ r_2 = r_1$



Let $S = \{I, r_1, r_2, r_3\}$.

Then the composition table of $(S, \circ)$ is given below

$\circ$	I	r_1	r_2	r_3
I	I	r_1	r_2	r_3
r_1	r_1	I	r_3	r_2
r_2	r_2	r_3	I	r_1
r_3	r_3	r_2	r_1	I

From the above table it follows that $(S, \circ)$ forms an abelian group whose identity element is I and each element is its own inverse. This group of order 4 is known as *Klein's- 4- group.*

4.2.6. Quotient Group.

Let H be a normal subgroup of a group G. Then there is no distinction between left and right cosets of H in G. Let G/H be the collection of all cosets of H in G. We shall now show that the set G/H forms a group w.r.t multiplication of cosets defined by $(aH)(bH) = abH, \ \forall a, b \in G$

Theorem 1. The set G/H of all cosets of a normal subgroup H in G is a group w.r.t operation defined by

$$(aH)(bH) = abH, \ \forall a, b \in G. \qquad [W.B.U.T\ 2013]$$

Proof. Here $G/H = \{aH : a \in G\}$.

Let $a, b, c \in G$ so that $aH, bH, cH \in G/H$.

(i) Then $(aH)(bH) = abH \in G/H$ as $a, b \in G \Rightarrow ab \in G$

So, G/H is closed.

(ii) Now $(aH)[(bH)(cH)] = aH(bcH) = a(bc)H$

$= (ab)cH = (abH)(cH) = [(aH)(bH)](cH)$

Thus the operation multiplication in G/H is associative

(iii) We have $H = eH \in G/H$. Then

$(H)(aH) = (eH)(aH) = (ea)H = aH$ and similarly $(aH)(H) = aH$

Hence H is the identity element of G/H.

(iv) As $a \in G \Rightarrow a^{-1} \in G$, so $aH \in G/H \Rightarrow a^{-1}H \in G/H$

Now $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

and $(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$.

So the coset $a^{-1}H$ is the inverse of aH

i.e. $(aH)^{-1} = a^{-1}H$. Thus inverse of each element of G/H exist.

Hence G/H is a group.

Quotient Group : Let H be a normal subgroup of group G. Then the group of all coset aH of H in G, with respect to the composition, $(aH)(bH) = (ab)H$ is callled the Quotient group of H in G.

Theorem 2. Every quotient group of an abelian group is abelian.

Proof. Let H be a subgroup of an abelian group G. Then H is a normal subgroup of G. So the quotient group G/H exists.

Let $a, b \in G$. Then $aH, bH \in G/H$

Now, $(aH)(bH) = abH = baH$ [$\because$ G is abelian, so $ab = ba$]

$= (bH)(aH)$.

$\therefore (aH)(bH) = (bH)(aH) \ \forall \ aH, bH, \in G/H$

Hence the quotient group G/H is abelian.

Note. *The converse of the above theorem is not true.*

For example, let $G = S_3, H = A_3$. Then the quotient group S_3/A_3 is of order 2 and hence abelian, as every group of order 2 is abelian. But the symmetric group S_3 is not abelian.

Theorem 3. Every quotient group of a cyclic group is cyclic.

Proof. Let H be a subgroup of a cyclic group G. Then H is a normal subgroup of G, as G is abelian. So the quotient group G/H exist. Let a be the generator of G. Then $a^n \in G$ for some integer n. Therefore $a^nH \in G/H$.

Now, $a^nH = (aa \cdots n \ factor)H = (aH)(aH) \cdots n \ factor = (aH)^n$

Hence G/H is a cyclic group and aH is a generator of it.

Note. *The converse of the above theorem is not true.*

For example, let $G = S_3$, $H = A_3$. Then the quotient group S_3 / A_3 is of order 2 and hence cyclic, as every group of prime order is cyclic. But the symmetric group S_3 is not cyclic.

Illustrative Examples.

Ex. 1. *Let S_3 and A_3 be the symmetric group and the alternating group on the set $\{1, 2, 3\}$. Construct the composition table for the quotient group S_3 / A_3.*

Let $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where f_1 = identity permutation $f_2 = (1\ 2), f_3 = (2\ 3), f_4 = (3\ 1), f_5 = (1\ 2\ 3), f_6 = (1\ 3\ 2)$.

Then $A_3 = \{f_1, f_5, f_6\}$. As A_3 is a normal subgroup of S_3, so S_3 / A_3 exists.

Now, $A_3 f_1 = A_3 f_5 = A_3 f_6 = A_3$ and $A_3 f_2 = A_3 f_3 = A_3 f_4$

$\therefore\ S_3 / A_3 = \{A_3,\ A_3 f_2\}$.

Thus the composition table for S_3 / A_3 is as given below

$\circ$	A_3	$A_3 f_2$
A_3	A_3	$A_3 f_2$
$A_3 f_2$	$A_3 f_2$	A_3

$[\because (A_3 f_2)(A_3 f_2) = A_3 f_2 f_2 = A_3 f_1 = A_3]$

Ex. 2. *Let Z be the centre of a group. If G / H is cyclic, prove that G is abelian.*

Since G / Z is cyclic, so let $G / Z = \langle gZ \rangle$ for some $g \in G$.

Let $a \in G$. Then $aZ \in G / Z$

Therefore $aZ = (gZ)^m$ for some integer m.

$= (gZ)(gZ) \cdots m$ factors $= (gg \cdots m \text{ factors})Z = g^m Z$

$\therefore\ a \in g^m Z \Rightarrow a = g^m z_1$, some $z_1 \in Z$

Next let $b \in G$.

Then similarly we get

$b = g^n z_2$ for some $z_2 \in Z$.

$\therefore\ ab = (g^m z_1)(g^m z_2) = g^m z_1 g^m z_2 = g^m g^n z_1 z_2 \quad [\because z_1 \in Z]$

$= g^{m+n} z_2 z_1 \quad [\because z_2 \in Z]$

$= g^{n+m} z_2 z_1 = g^n \cdot g^m z_2 z_1$

$= (g^n z_2)(g^m z_1)\ [\because z_2 \in Z] = ba$

Thus $ab = ba\ \forall\ a, b \in G$. Hence G is abelian.

Ex. 3. *If N is normal in G and $a \in G$, then prove that $o(Na)$ in G/N is a divisor of $o(a)$.*

Let $o(a) = n$ and $o(Na) = m$

Then $a^n = e$, the identity element of $G \quad \therefore\ Na^n = Ne = N$

Now $Na^n = N(aaa' \cdots n \text{ times}) = (Na)(Na) \cdots n \text{ times} = (Na)^n$

Thus $(Na)^n = N$, the identity of G/N. But $o(Na) = m$, so m must be a divisor of n.

Exercise

I. Short Answer Questions

1. Let G be the additive group of integers. Then prove that the set of integers of multiple of 5 is a subgroup of G.

2. Let $(G, *)$ be an abelian group where G is the set of all ordered pairs (a, b) of real numbers $a \neq 0$ and the operation '$*$' is defined by

$(a, b) * (c, d) = (ac, bc + d)$.

Show that the subset H of all those elements of G which are of the form $(1, b)$ form a subgroup G.

3. Prove that those elements of a group G which commute with the square of a given element b of G form a subgroup H of G.

4. If G be an abelian group with identity e, then prove that all elements x of G satisfying $x^2 = e$ form a subgroup of G.

5. Let G be a group in which $(ab)^3 = a^3b^3 \ \forall \ a, b \in G$. Show that $H = \{x^3 : x \in G\}$ is a subgroup of G.

6. Let $(G, \circ)$ be a group and $a \in G$. Then the Centraliser of a is defined by $C(a) = \{x \in G : x \circ a = a \circ x\}$. Prove that the $C(a)$ is a subgroup of G.

7. Show that the multiplicative group of n n-th roots of unity is cyclic.

8. Give an example of a finite abelian group which is not cyclic.

9. Prove that the only right (or left) coset of a subgroup H in a group G which is also a subgroup of G is H itself.

10. Show that every subgroup of an abelian group is normal.

11. Let $G = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad \neq 0\right\}$ and $H = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right\}$ Prove that H is a normal subgroup of the group $(G, \cdot)$.

12. Give an example to show that if H is normal subgroup of G and K is a normal subgroup of H then K may not be a normal subgroup of G.

13. If M and N are two normal subgroup of G and $M \cap N = \{e\}$, then prove that $mn = nm \ \forall \ n \in N, m \in M$.

14. Determine which of the following are even permutation

(a) $f = (123)(12)$ (b) $g = (12345)(123)(45)$

(c) $h = (12)(13)(14)(25)$

15. Examine whether the following permutations is even or odd.

(i) $\begin{pmatrix} 123456789 \\ 254361798 \end{pmatrix}$ (ii) $\begin{pmatrix} 123456 \\ 654312 \end{pmatrix}$ (iii) $\begin{pmatrix} 12345678 \\ 31472586 \end{pmatrix}$

16. Find the inverse of the following permutations :

(i) $\begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$ (ii) $\begin{pmatrix} 12345 \\ 23154 \end{pmatrix}$

17. Show that the group S_3 is non-abelian.

18. Show that A_3 is a subgroup of S_3.

19. Prove that the symmetric group S_3 has a trivial centre.

20. Define a permutation group.

21. Define a dihedral group

22. Define a cyclic group with an example.

23. State the condition for a subset of a group to be a sub group.

24. Find all the subgroups of a group G of prime order.

25. If G is a commutative group, then prove that $H = \{a \in G : a^2 = e\}$ is a subgroup of G.

26. Show that every cyclic group is an abelian group.

27. Show that $(R, +)$ is not a cyclic group.

28. Prove that every proper subgroup of S_3 is cyclic

29. Show that the alternating group A_3 is a normal subgroup of S_3

30. Let G be a group . Show that if $G/Z(G)$ is cyclic, then G is abelian.

31. Show that every subgroup of a cyclic group is normal.

32. Let Z be the centre of a group . If G/H is cyclic, prove that G is abelian

33. Show that group (G, o) when $G = \{1, \omega, \omega^2\}$ is cyclic.

34. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ .is even

35. Show that any two right cosets are either disjoint or identical

36. Using Lagrange 's theorem, prove that every group of prime order is cyclic [*W.B.U.T. 2014*]

37. Prove that a subgroup H of a group G is normal if and only if $x H x^{-1} = H \ \forall x \in G$

38. If G is a group and H is a subgroup of index 2 in G, prove that H is a normal subgroup.

Answers

8. $(G,\cdot)$ where $G=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$

14. (a) odd (b) odd (c) even **15.** (i) odd (ii) even (iii) odd.

16. (i) $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ (ii) $\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$. **24.** $\{e\}$ and G

II. Long Answer Questions

1. Let G be the multiplicative group of all positive real numbers and R be the additive group of all real numbers. Is G a subgroup of R?

2. Show that the elements of finite order in any commutative group G form a subgroup of G.

3. Let $(G,\circ)$ be a group and H be a non-empty subset of G. A relation R defined on G by aRb if $a\circ b^{-1}\in H$ for $a,b\in G$ is an equivalence relation on G. Prove that $(H,\circ)$ is a subgroup of $(G,\circ)$.

4. Find all cyclic subgroups of the group $(Z_5,+)$.

5. Show that the set $G=\{1,\omega,\omega^2\}$ of cube roots of unity is a finite cyclic group.

6. Prove that $(Q_+,\cdot)$ is non-cyclic.

7. If an abelian group of order six contains an element of order 3, show that it must be cyclic group.

8. Let $(G,\circ)$ be an infinite cyclic group generated by a. Prove that a and a^{-1} are the only generators of the group.

9. Show that the residue classes $[1],[3],[5],[7]$ modulo 8 form a multiplicative group. Is this a cyclic group?

10. Let H be a subgroup of a group G and a be an element of G. Let $aH=\{ah:h\in H\}$. Prove that for $b\in G$, if $bH\neq aH$ then $aH\cap bH=\phi$.

11. Show that two right cosets Ha, Hb are distinct if and only if the two left cosets $a^{-1}H$, $b^{-1}H$ are distinct.

12. Use Lagrange's theorem to prove that a finite group cannot be expressed as the union of two of its proper subgroups

13. H is a normal subgroup of G and K is a subgroup of G such that $H\subseteq K\subseteq G$. Show that H is also a normal subgroup of K.

14. Suppose H is the only subgroup of finite order in the group G. Prove that H is a normal subgroup of G.

15. The centre Z of G is defined by $Z(G)=\{z\in G:zx=xz\ \forall x\in G\}$. Prove that every subgroup of $Z(G)$ is a normal subgroup of G.

16. Let S be the set of all real non-singular matrices A with $\det A=1$ and G be the set of all real non-singular $n\times n$ matrices. Prove that $(S,\cdot)$ is a normal subgroup of $(G,\cdot)$.

17. Prove that a subgroup H of a group G is a normal subgroup of G if and only if all its right cosets are also its left cosets.

18. Let Z be the centre of a group G. If $a\in Z$, prove that the cyclic subgroup $\{a\}$ of G generated by a is a normal subgroup of G.

19. Let G be a group in which $(ab)^3=a^3b^3\ \forall a,b\in G$. Prove that $H=\{x^3:x\in G\}$ is a normal subgroup of G.

20. If N is a normal subgroup of G and H is any subgroup of G, prove that NH is a subgroup of G.

21. If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.

22. Show that the set of all possible permutation of the elements of the set $S=\{a,b,c\}$ form a group w.r.t the binary operation of compositions of permuations. [Hints : see illustrative Ex-1 of art 3.8]

23. Prove that the set A_3 of three permutations $(a),(abc),(acb)$ on three symbols a, b, c forms a finite abelian group w.r.t permutation -multiplication.

24. Show that the four permutations I, $(ab),(cd),(ab)(cd)$ on four symbols a,b,c,d form a finite abelian group w.r.t the permuation -multiplication.

25. Prove that every proper subgroup of the symmetric group S_3 is cyclic.

26. Let P_n be the symmetric group on n symbols. Prove that A_n is a normal subgroup of P_n