- **Integral Powers of an element of a group :-**

Let (G, o) be a group and $a \in G$. Then $a o a$, $a o a o a$, ... all belong to G.

Define: $a^0 = e$,

$a^n = a o a o \cdots o a$ (n factors); and

$\bar{a}^n = \bar{a}^1 o \bar{a}^1 o \cdots o \bar{a}^1$ (n factors), $n \in Z^+$.

- **Laws of indices :-** For $m, n \in Z$, $a \in G$,

(i) $a^m o a^n = a^{m+n}$, (ii) $(a^m)^n = a^{mn}$, (iii) $(a^n)^{-1} = \bar{a}^n$.

- **Order of an element of a group :-**

Let (G, o) be a group and $a \in G$.

The order of a is the least positive integer n such that $a^n = e$ and is denoted by $O(a)$.

If the $O(a)$ is not finite then a is said to be of infinite order or of order zero.

For additive group, the least positive integer n s.t. $na = e$ gives $O(a)$.

Examples:

1. In the group $(S, \cdot)$, where $S = \{1, -1, i, -i\}$,

$O(1) = O(e) = 1$, since $1^1 = e$.

$O(-1) = 2$, since $(-1)^2 = 1 = e$.

$O(i) = 4 = O(S)$, since $i^4 = 1$.

$O(-i) = 4 = O(S)$, since $(-i)^4 = 1$.

2. In the group $(Z_5, \oplus_5)$, $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$,

$O(\bar{0}) = 1$, since $1 \cdot \bar{0} = \bar{0} = e$

$O(\bar{1}) = 5$, since $5 \cdot \bar{1} = \bar{5} = \bar{0}$ [$\bar{1} \oplus_5 \bar{1} \oplus_5 \bar{1} \oplus_5 \bar{1} \oplus_5 \bar{1} = 5 \cdot \bar{1}$]

$O(\bar{2}) = 5$, since $5 \cdot \bar{2} = \bar{10} = \bar{0}$

$O(\bar{3}) = 5$, since $5 \cdot \bar{3} = \bar{15} = \bar{0}$

$O(\bar{4}) = 5 = O(Z_5)$, since $5 \cdot \bar{4} = \bar{20} = \bar{0}$.

3. In the group $(U_8, \odot_8)$, $U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$,

$O(\bar{1}) = 1$, since $(\bar{1})^1 = \bar{1} = e$

$O(\bar{3}) = 2$, since $(\bar{3})^2 = \bar{3} \odot_8 \bar{3} = \bar{9} = \bar{1} = e$,

$O(\bar{5}) = O(\bar{7}) = 2$, since $(\bar{5})^2 = \bar{25} = \bar{1}$, $(\bar{7})^2 = \bar{49} = \bar{1}$.

4. In the group $(\mathbb{Z}, +)$, the order of the identity element 0 is 1. And " " " each non-identity element is infinite. Because,
$\nexists$ any finite n s.t. $na = e = 0$ for $a(\neq e) \in \mathbb{Z}$.
e.g. let us take $a = 1$, then $\nexists$ any +ve integer n s.t. $n.1 = 0 (= e)$.

5. In the Klein's group $(V, \circ)$, $V = \{e, a, b, c\}$, where $c = a \circ b$, $a^2 = b^2 = c^2 = e$.
$O(e) = 1$, $O(a) = O(b) = O(c) = 2$.

Note:
(i) The order of the identity element is always 1.
(ii) " " " non " " " never 1.

THEOREM relating order of an element in a group:

Th. (1). Let a be an element of a group (G, o). Then

(i) $O(a) = O(a^{-1})$;

(ii) if $O(a) = n$ and $a^m = e$, then $n \mid m$.

(iii) if $O(a) = n$, then $a, a^2, \ldots, a^{n-1}, a^n (= e)$ are distinct.

(iv) if $O(a) = n$, then for $m \in \mathbb{Z}^+$, $O(a^m) = \dfrac{O(a)}{\gcd(m, O(a))} = \dfrac{n}{\gcd(m,n)}$.

(v) if $O(a) = n$, then $O(a^p) = n$ iff $\gcd(p, n) = 1$.

(vi) if $O(a)$ is infinite and $p \in \mathbb{Z}^+$, then $O(a^p)$ is infinite.

Proof:

(i) Let $O(a) = n$ (finite). Then $a^n = e$, for n being the least +ve integer.

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

Let $(a^{-1})^m = e$ for $m < n$; then $a^{-m} = e$.

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

$\Rightarrow O(a) < n$, which is a contradiction.

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

Now Let $O(a)$ be infinite, and $O(a^{-1})$ be finite, say, $O(a^{-1}) = K$. $\Rightarrow (a^{-1})^K = e \Rightarrow a^{-K} = e \Rightarrow (a^{-K})^{-1} = e^{-1} = e$

$\Rightarrow a^K = e \Rightarrow O(a)$ is finite, a contradiction.

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

(ii) Let $O(a) = n$ and $a^m = e$.

By division algorithm, $\exists$ unique integers q & r such that $m = q.n + r$, where $0 \le r < n$.

Then $e = a^m = a^{(q.n+r)} = (a^n)^q o a^r = e^q o a^r = e o a^r = a^r$.

$\Rightarrow r = 0$, since $a^n = e$ for least +ve integer n.

$\therefore m = q.n. \Rightarrow n \mid m$.

(iii) Let $O(a) = n$. Let $a^r = a^s$ for $0 < s < r \le n$, for $r, s \in \mathbb{Z}^+$.

$\Rightarrow a^r o a^{-s} = a^s o a^{-s} \Rightarrow a^{r-s} = e$, not possible, since $0 < r - s < n$ and $O(a) = n$.

$\therefore a, a^2, \ldots, a^n (= e)$ are all distinct elements of (G, o).

(iv) Let $O(a)=n$ and $O(a^m)=K$. Then
$a^{mK}=e$. $O(a)=n \Rightarrow n/mK$.
Let $\gcd(m,n)=d$. Then $m=d.u$, $n=d.v$; $\gcd(u,v)=1$.
$n/mK \Rightarrow d.v/d.uK \Rightarrow v/u.K \Rightarrow v/K$, since $\gcd(u,v)=1$.
Again $(a^m)^v=(a^{d.u})^v=a^{u.dv}=a^{u.n}=(a^n)^u=e^u=e$.
Now $O(a^m)=K$ and $(a^m)^v=e \Rightarrow K/v$.
$\therefore$ v/K & $K/v \Rightarrow K=v=\frac{n}{d}=\frac{n}{\gcd(m,n)}$.
$\therefore O(a^m)=\frac{n}{\gcd(m,n)}$.

(v) Let $\gcd(n,p)=1$, then by (iv) $O(a^p)=\frac{n}{\gcd(n,p)}=n$.
Conversely, let $O(a^p)=n$. Then $O(a^p)=\frac{n}{\gcd(n,p)}=n$
$\Rightarrow \gcd(n,p)=1$.

(vi) Let $O(a)$ be infinite and $O(a^p)$ be finite, $p\in Z^+$.
Let $O(a^p)=m \Rightarrow a^{p.m}=e \Rightarrow O(a)$ is finite, a contradiction.
$\therefore O(a^p)$ is infinite whenever $O(a)$ is infinite.

Note: If $p\in Z^-$, then $O(a^p)$ is also infinite, since
$O(a^p)=O((a^p)^{-1})=O(a^{-p})$.

Th. ② (i) Each element of a finite group is of finite order.
(ii) And the order of an element in a finite group cannot exceed the order of the group.

Proof: (i) Let a be an element of a finite group (G,o).
Then $a, a^2, a^3, \ldots$ are all elements of G.
Since G is finite, the elements $a, a^2, a^3, \ldots$ are not all distinct. Hence $a^m=a^n$ for some +ve integers m,n $(m>n)$.
$\therefore a^m o(a^n)^{-1}=a^n o(a^n)^{-1}=e$
$\Rightarrow a^{m-n}=e \Rightarrow O(a)$ is finite whenever $O(G)$ is finite.

(ii) Let $O(G)=K$ (finite). And let $O(a)=n$ where a is any element of a finite group (G,o).
Since $O(a)=n$, then there exist n distinct elements $a, a^2, \ldots, a^{n-1}, a^n(=e)$ in (G,o).
If possible, let $K<n$. Then there would exist lesser number $K(<n)$ of distinct elements than n in (G,o), which contradicts the order of (G,o).
$\therefore \boxed{n\le K}$.

Examples:

1. In a group (G,o), $aob = boa$ and $\gcd(o(a), o(b)) = 1$, for $a, b \in G$. Show that $o(aob) = o(a) \cdot o(b)$.

Let $o(a) = m$, $o(b) = n$, $o(aob) = k$. Then $\gcd(m,n) = 1$.

Now $(aob)^{mn} = (aob) o (aob) o \cdots o (aob)$ {mn factors}

$= (aoao\cdots oa) o (bobo\cdots ob)$ {both are mn factors}

$= a^{mn} o b^{mn} = (a^m)^n o (b^n)^m = e^n o e^m = eoe = e$. [$\because aob = boa$]

Hence $(aob)^{mn} = e$ and $o(aob) = k \Rightarrow k \mid mn$.

Now $(aob)^k = e \Rightarrow a^k o b^k = e$ [$\because aob = boa$]

$\Rightarrow a^k = b^{-k} \Rightarrow a^{nk} = (b^n)^{-k} = e^{-k} = e$

$\therefore o(a) = m$ and $a^{nk} = e \Rightarrow m \mid nk$

$\Rightarrow m \mid k$ [$\because \gcd(m,n) = 1$]

Again $(aob)^k = e \Rightarrow b^k = a^{-k} \Rightarrow b^{mk} = (a^m)^{-k} = e^{-k} = e$

$\because o(b) = n$ and $b^{mk} = e \Rightarrow n \mid mk$

$\Rightarrow n \mid k$ [$\because \gcd(m,n) = 1$].

So, $m \mid k$ and $n \mid k \Rightarrow mn \mid k$

Also we get $k \mid mn$, therefore, $k = m \cdot n$

$\therefore o(aob) = o(a) \cdot o(b)$.

2. If (G,o) be a finite group of even order, prove that G contains an odd number of elements of order 2.

Let $S = \{a \in G : a \neq a^{-1}\}$, $T = \{a \in G : a = a^{-1}\}$. Then $G = S \cup T$ where $S = T^c$ and $T = S^c$.

Let us first consider $T = \{a \in G : a = a^{-1}\}$.

$a = a^{-1} \Rightarrow a^2 = e \Rightarrow$ either $a = e$ or $o(a) = 2$.

$\therefore T$ contains the identity element e (of order 1) and all elements of order 2 of the group.

Let us now consider $S = \{a \in G : a \neq a^{-1}\}$.

In S, $a \neq a^{-1} \Rightarrow a^{-1} \neq (a^{-1})^{-1}$, i.e., $a^{-1} \neq a \Rightarrow a^{-1} \in S$.

So $a \in S \Rightarrow a^{-1} \in S$. Hence $\{a, a^{-1}\}$ forms a pair in S. And S contains all such pair of elements.

$\therefore$ The number of elements in S is even.

As $O(G)$ is even, the number of elements in T has to be even. $e \in T$ and so the no. of elements of order 2 in T must be odd and hence in G also.

Ex: Conjugate element →

If a be an element of a group (G, o). An element $b \in G$ is said to be conjugate of a if there exists an $x \in G$ s.t.

$$b = x o a o x^{-1}.$$

$$\Rightarrow x^{-1} o b o x = a.$$

$$\Rightarrow x^{-1} o b o (x^{-1})^{-1} = a \Rightarrow a \text{ is also conjugate of } b.$$

Prove that any conjugate of a has the same order as that of a. Deduce $o(a o b) = o(b o a)$; $a, b \in G$

Let $o(a) = m$, then $a^m = e$

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

Let $(x o a o x^{-1})^k = e$ for some +ve integer $k < m$.

Then $x o a^k o x^{-1} = e \Rightarrow a^k = x^{-1} o x = e \Rightarrow o(a) < m$, a contradiction.

$\therefore$ m is the least +ve integer s.t. $(x o a o x^{-1})^m = e$

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

Let $o(a)$ be infinite. If possible, let $o(x o a o x^{-1}) = n$.

then $(x o a o x^{-1})^n = e \Rightarrow a^n = e \Rightarrow o(a) < \infty$, a contradiction.

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

Now, $a o b = a o (b o a) o a^{-1} \Rightarrow o(a o b) = o(b o a)$; because $a o b$ & $b o a$ are conjugate

Ex (9) Find the no. of elements of order 5 in the group $(Z_{20}, \oplus)$

Let $o(\bar{m}) = 5$, where $0 < m < 20$. $o(\bar{0}) = 1$, $o(\bar{1}) = 20$.

$o(\bar{1}) = 20$, $o(\bar{m}) = o(m\bar{1}) = \frac{o(\bar{1})}{\gcd(m,20)} = \frac{o(\bar{1})}{\gcd(m, o(\bar{1}))}$.

$5 = \frac{20}{\gcd(m,20)}$.

$\therefore \gcd(m,20) = 20/5 = 4$.

$\therefore \gcd(\frac{m}{4}, 5) = 1$

i.e., $\frac{m}{4}$ is less than 5 & prime to 5,

i.e., $\frac{m}{4} = 1, 2, 3, 4$.

Hence the elements of order 5 are

$\bar{4}, \bar{8}, \bar{12}, \bar{16}$ (no. = 4).

Ex. (10) Find all elements of order 10 in the group $(Z_{30}, \oplus)$

Similar to Ex (9).

Ex. (11) If b be an element of a group and $o(b) = 20$, find the order of the element (i) b^8, (ii) b^{15}.

$o(b) = 20 \Rightarrow b^{20} = e$. Let $o(b^8) = m$ & $o(b^{15}) = n$.

Then $b^{8m} = e$, $b^{15n} = e$., where m, n being the least +ve integers respectively.

Since $o(b) = 20$, $20 | 8m$; Also $20 | 15n$.

$\Rightarrow 5 | 2m$, $\Rightarrow 4 | 3n$.

Since m is the least & n is the least +ve integers, $\therefore m = 5$, $n = 4$ respective.

$\therefore o(b^8) = 5$, $o(b^{15}) = 4$.

Alternatively, $o(b^8) = \frac{o(b)}{\gcd(8, o(b))} = \frac{20}{\gcd(8,20)} = \frac{20}{4} = 5$

$o(b^{15}) = \frac{o(b)}{\gcd(15, o(b))} = \frac{20}{\gcd(15,20)} = \frac{20}{5} = 4$.

Permutation:

Let S be a non-empty finite set, $S = \{a_1, a_2, \ldots, a_n\}$.
A bijective function $f: S \to S$ is said to be a permutation on S.
The number of bijections from S onto S is $n!$.
Let one such bijection be f s.t. $f(a_i) = a_i$; $i = 1, 2, \ldots, n$.
This permutation f is denoted by

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

The identity function is is also a bijection, and it is called identity permutation.

$$i = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Multiplication of permutations :-

Let $f: S \to S$, $g: S \to S$ be two permutations on S.
$gof: S \to S$ is bijective, hence gof is a permutation on S.
$fog: S \to S$ " " " " fog " " " " S.
The products are given by:

$$fg = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f[g(a_1)] & f[g(a_2)] & \cdots & f[g(a_n)] \end{pmatrix}, \quad gf = \begin{pmatrix} a_1 & \cdots & a_n \\ g[f(a_1)] & \cdots & g[f(a_n)] \end{pmatrix}.$$

Since composition of maps is not commutative,

$$fg \neq gf; \text{ in general.}$$

Again, composition of maps is associative,

$$f(gh) = (fg)h, \text{ for 3 permutations } f, g, h \text{ on } S.$$

Inverse of a Permutation :-

$f: S \to S \Rightarrow f^{-1}: S \to S$, since f is a bijection.
f^{-1} is also a bijection.
$\therefore f^{-1}$ is a permutation on S and $ff^{-1} = f^{-1}f = i$.

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

Cycle :- A permutation $f: S \to S$ is said to be an r-cycle or of order r if there are r elements $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ in S s.t.
$f(a_{i_1}) = a_{i_2}$, $f(a_{i_2}) = a_{i_3}, \ldots, f(a_{i_{r-1}}) = a_{i_r}$, $f(a_{i_r}) = a_{i_1}$, and
$f(a_j) = a_j$ for $j \neq i_1, i_2, \ldots, i_r$.
The cycle is denoted by $(a_{i_1}, \ldots, a_{i_r})$ or $(a_{i_2}, \ldots, a_{i_r}, a$
or in other form keeping a fixed cyclic order.

(2)

Disjoint cycles : Two cycles f and g on the same set S are said to be disjoint if they have no common elements.

Multiplication of two disjoint cycles is commutative

Integral powers :-

If f be a permutation on a set S, then
$f \cdot f$ also " " " S, then
$(f \cdot f) \cdot f = f \cdot (f \cdot f)$ " " " " " S, since it is associative
We define: $f^n = f \cdot f \cdot \ldots \cdot f$ (n factors) $\forall n \in \mathbb{N}$.
Again f^{-1} is a permutation on S,
we define: $f^{-n} = f^{-1} \cdot f^{-1} \cdot \ldots \cdot f^{-1}$ (n factors), $\forall n \in \mathbb{N}$
and $f^0 = i$
$\therefore f^n$ is defined for all n, where $n \in \mathbb{Z}$.

Index laws:

(i) $f^m \cdot f^n = f^{m+n}$
(ii) $(f^m)^n = f^{mn}$
$\Big\}$ $\forall m, n \in \mathbb{Z}$

But $(f \cdot g)^m \neq f^m \cdot g^m$, since $f \cdot g \neq g \cdot f$, in general.

Properties:

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

Note: $i = \begin{pmatrix} a_1 & \ldots & a_n \\ a_1 & \ldots & a_n \end{pmatrix} = (a_1)(a_2)\ldots(a_n)$ is the product of n disjoint cycles of length 1 each.

Order of Permutation:

The order of f is the least +ve integer n s.t. $f^n = i$

(2) The order of an r-cycle is r.

Let $S = \{a_1, a_2, \ldots, a_n\}$ and $p = (a_1, a_2, \ldots, a_r)$ be an r-cycle on S.

Then $p(a_1) = a_2$, $p(a_2) = p(a_3)$

$p\,p(a_1) = a_3 \Rightarrow p^2(a_1) = a_3$, $\ldots$, $p^r(a_1) = p(a_r) = a_1$.

Similarly, $p^r(a_2) = a_2$,

$p^r(a_3) = a_3$.

$p^r(a_r) = a_r$.

Also $p(a_s) = a_s$ for $s = r+1, \ldots, n$.

" $p^r(a_s) = a_s$ " " " "

$\therefore p^r(a_k) = a_k$ for $k = 1, 2, \ldots, n$.

$\therefore p^r$ is the identity permutation.

r is the least +ve integer s.t. $p^r = i$.

For, if $p^m = i$, for some $m < r$, then $p^m(a_1) = a_1$, not true

$\therefore$ order of p is r.

(3). The order of a permutation on a finite sets is the l.c.m. of the lengths of its disjoint cycles.

Transposition: A 2-cycle is called a transposition.

A 1-cycle is the identity and it can be expressed as the product of the transpositions

(a_r, a_s) and (a_s, a_r).

A 3-cycle (a_1, a_2, a_3) can be expressed as the product $(a_1, a_3)(a_1, a_2)$.

An r-cycle $(a_1, a_2, \ldots a_r)$ can be expressed as the product $(a_1, a_r)(a_1, a_{r-1})(a_1, a_{r-2}) \cdots (a_1, a_3)(a_1, a_2)$ → $(r-1)$ transpo

(4) Every permutation on a finite set can be expressed as a product of transpositions.

Definition: A permutation is said to be even if it is the product of an even no. of transpositions and odd, otherwise

$i = (a_r, a_s)(a_s, a_r)$ → even.

The inverse of an even permn. is even.

" " odd " is odd.

Symmetric Group S_n

Let S_n be the set of all permutations on the set $\{1, 2, \cdots, n\}$ ⊛ A permutation is a bijective map from the set $\{1, 2, \cdots, n\}$ onto itself. ⊛

* To examine if S_n forms a group w.r.t. 'multiplication of permutations'.

(i) Let $f, g \in S_n$ then $f \cdot g \in S_n$ since f and g be two bijective maps and composition of two bijective maps is also a bijection.
$\therefore S_n$ is closed w.r.t. '$\cdot$'.

(ii) Let $f, g, h \in S_n$ then $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ [Associative prop]
Since composition of mappings is associative, multiplication of permutations is associative.

(iii) The identity permutation $i = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S_n$ is the identity element $i \cdot f = f \cdot i = f$; $\forall f \in S_n$

(iv) Let $f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & & f(n) \end{pmatrix} \in S_n$, then $g = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & & n \end{pmatrix} \in S_n$
as f is bijective map.
Here g is the inverse of f, since $g \cdot f = f \cdot g = i$

(v) Multiplication is not commutative, since composition of mappings is not commutative, in general.

eg. $f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix} = (1,2)$, $g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 2 & 1 & \cdots & n \end{pmatrix} = (1,3)$

Then $f \cdot g = (1,2)(1,3) = (1,3,2)$, $g \cdot f = (1,3)(1,2) = (1,2,3)$

$\therefore f \cdot g \neq g \cdot f$.

$\therefore (S_n, \cdot)$ is called the Symmetric group of degree n.

S_n is non-commutative group for $n \geq 3$.

PARTICULAR CASE:

Symmetric group S_3.

Let S be the set of all permutations on the set $\{1, 2, 3\}$. $S = \{\ell_0, \ell_1, \ell_2, \ell_3, \ell_4, \ell_5\}$, where

$\ell_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\ell_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$, $\ell_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$,

$\ell_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$, $\ell_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$, $\ell_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$

Symmetric group S_3.

Let S be the set of permutations on the set $\{1,2,3\}$

$\therefore S = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$, where

$\rho_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\rho_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1,2,3)$, $\rho_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1,3,2)$

$\rho_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2,3)$, $\rho_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1,3)$, $\rho_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1,2)$

The composition table (multiplication table):

$\cdot$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

Multiplication table is not symmetric about the main diagonal, hence multiplication is NOT commutative.

It appears that —
S is closed w.r.t. multiplication of permutations.
Associative property holds from associativity of composition of mappings.
ρ_0 is the identity element.

Inverse of $\rho_0 = \rho_0$
" " $\rho_1 = \rho_2$
" " $\rho_2 = \rho_1$
" " $\rho_3 = \rho_3$
" " $\rho_4 = \rho_4$
" " $\rho_5 = \rho_5$

$\therefore$ S_3 is a non-abelian group, called the symmetric group of degree 3.

The order of $S_3 = 6$.

Alternating group A_n, of degree n.

The set of all even permutations on the set $\{1,2,\cdots,n\}$ forms a group w.r.t. multiplication of permutations.

A_n contains $\frac{1}{2}n!$ elements

A_n is non-commutative group for $n \geq 4$.

In particular, A_3 is the group of all even permutations on the set $\{1,2,3\}$. The elements of A_3 are $A_3 = \{\rho_0, \rho_1, \rho_2\}$. It is a commutative group of order 3.