Permutation

Paper: C201

Course: Mathematics (H) UG.

Sem: 2nd Sem

Prepared by Dr. Ajoy Kumar Maiti

Permutation :

Defn : Let S be a non-empty finite set. A permutation is a bijective mapping $f: S \to S$.

Let $S = \{a_1, a_2, \dots a_n\}$ Then the number of bijections from S onto S is $n!$. Thus the permutation f is denoted by symbol

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

Identity Permutation :

The identity permutation is is also a bijective mapping. is is said to be the identity permutation and denoted by i. $\therefore$ $i = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$.

Multiplication of permutation :

Let $f: S \to S$, $g: S \to S$ be two permutations on S.

Since range f = domain g, the composite mapping $gof: S \to S$ is defined. Since f and g are both bijective mapping, so gof is also a bijective mapping. Therefore, gof is a permutation on S. Similarly, fog is also a permutation on S. The products $g.f$ and $f.g$ are defined by compositions gof and fog respectively.

If $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$, $g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \cdots & g(a_n) \end{pmatrix}$

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

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

Since, the composition of mappings is not commutative, $f.g \neq g.f$, in general.

Multiplication of permutations on S is associative, since composition of mappings is associative.

Inverse of permutation:

Let f be a permutation on S. Since f is a bijective mapping, it admits the unique inverse of f i.e $f^{-1}: S \to S$. So, f^{-1} is also bijective mapping. Therefore f^{-1} is a permutation on S

$$\text{and } f \cdot f^{-1} = f^{-1} \cdot f = i$$

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

Ex. Let $S = \{1, 2, 3, 4\}$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

Since $f \cdot f^{-1} = i = f^{-1} \cdot f$

So $f^{-1} f(1) = 1$, $f^{-1} \cdot f(2) = 2$, $f^{-1} f(3) = 3$, $f^{-1} f(4) = 4$.

Therefore, $f^{-1}(1) = 1$, $f^{-1}(3) = 2$, $f^{-1}(4) = 3$, $f^{-1}(2) = 4$.

$$\therefore f^{-1} = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Cycle: Let $S = \{a_1, a_2, \ldots, a_n\}$ A permutation $f: S \to S$ is said to be a cycle of length r or an r-cycle if there are r elements $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ in S such that $f(a_{i_1}) = a_{i_2}$, $f(a_{i_2}) = a_{i_3}$, $\ldots$ $f(a_{i_{r-1}}) = a_{i_r}$, $f(a_{i_r}) = a_{i_1}$.

and $f(a_j) = a_j$, $j \neq i_1, i_2, \ldots, i_r$.

The cycle denoted by $(a_{i_1}, a_{i_2}, \ldots, a_{i_r})$ or by $(a_{i_2}, a_{i_3}, \ldots, a_{i_r}, a_{i_1})$

Otherwise: Let S be a finite set and $x \in S$. Let $f \in A(S)$, the of permutations. There exists +ve integer m such that $x, f(x), f^2(x), \ldots, f^{m-1}(x)$ are all distinct and $f^m(x) = x$. We call $(x, f(x), f^2(x), \ldots, f^{m-1}(x))$ a cycle of f.

Note: Multiplication of two disjoint cycles is commutative.

Order of a permutation:

Let f be a permutation on a finite set S. The order of f

is the least positive integer n such that $f^n = i$, i being the identity permutation.

<u>Theorem</u>: <u>The order of an r-cycle is r.</u>

<u>Proof</u>: Let $p = (a_1, a_2, \ldots, a_r)$ be an r-cycle on the set $S = \{a_1, a_2, \ldots, a_n\}$.

Then $p(a_1) = a_2$, $p^2(a_1) = p(a_2) = a_3$, ... $p^r(a_1) = p(a_r) = a_1$.

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 $s = r+1, \ldots, n$.

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

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

Therefore, p^r is the identity permutation.

r is the least positive integer such that $p^r = i$

Because if $p^m = i$ for some positive integer $m < r$ then $p^m(a_1)$ must be a_1 which is not so.

Therefore, the order of p is r.

<u>Theorem</u>: Every permutation on a finite set is either a cycle or it can be expressed as a product of disjoint cycles.

<u>Proof</u>: See S.K. Mapa (if necessary).

<u>Theorem</u>: The order of a permutation on a finite set is the l.c.m. of the lengths of its disjoint cycles.

<u>Proof</u>: See S.K. Mapa (if necessary).

<u>Transposition</u>:

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_r, a_s).

A 2-cycle is itself a transposition.

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

Theorem: Every permutation on a finite set (containing at least two elements) can be expressed as a product of transpositions.

Proof: See S.K. Mapa (if necessary).

Even Permutation: A permutation is said to be even if it can be expressed as the product of an even number of transpositions.

Odd Permutation: A permutation is said to be an odd permutation if it can be expressed as the product of an odd number of transpositions.

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

Ex: Find the order of the permutations

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 2 & 8 & 6 & 7 \end{pmatrix}$.

Ans: (i) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix}$

$= (1\ 4\ 5)(2\ 6)$

f is expressed as the product of two disjoint cycles $(1\ 4\ 5)$ and $(2\ 6)$.

We know that order of a permutation is the l.c.m of the disjoint cycle lengths.

So, the order of $f = \text{l.c.m}\{3, 2\}$
$= 6$.

$\therefore\ O(f) = 6$. i.e. $f^6 = i$ = identity permutation.

(ii) Try your self.

$\boxed{\text{Ex-2}}$: Find fg, gf, f^{-1} where $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix}$

and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix}$.

Ans:

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

$$g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix}.$$

Since $f^{-1} \cdot f = i$ $\therefore$ $f^{-1}f(1) = 1$, $f^{-1}f(2) = 2$, $f^{-1}f(3) = 3$,
$f^{-1}f(4) = 4$, $f^{-1}f(5) = 5$, $f^{-1}f(6) = 6$.

Therefore. $f^{-1}(2) = 1$, $f^{-1}(4) = 2$, $f^{-1}(3) = 3$, $f^{-1}(5) = 4$,
$f^{-1}(6) = 5$, $f^{-1}(1) = 6$.

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

$$= \cancel{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

$\boxed{\text{Ex-3}}$: Find the images of the elements 3 and 4 if

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & & & 3 \end{pmatrix}$ be an odd permutation.

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & & & 4 & 3 \end{pmatrix}$ be an even permutation.

Ans (i) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & & & 3 \end{pmatrix}$ be an ~~odd~~ permutation

We have find $f(3)$ and $f(5)$.

Here $f(3) = 2$ or 5

and $f(4) = 2$ or 5.

If $f(3) = 2$ and $f(4) = 5$ then the above permutation becomes $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$

$= (1\ 4\ 5\ 3\ 2)$

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

So f is even permutation. Because f has even number of transpositions.

But given that f ~~is~~ is odd permutation.

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

(ii) Try yourself

$\boxed{\text{Ex-4}}$: Examine whether the permutations (i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 2 & 8 & 6 & 7 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 5 & 3 & 2 \end{pmatrix}$.

are odd or even.

Ans (i) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 2 & 8 & 6 & 7 \end{pmatrix}$

$= (1\ 4\ 3)(2\ 5)(6\ 8\ 7)$

$= (1\ 3)(1\ 4)(2\ 5)(6\ 7)(6\ 8)$

So f has odd number of transposition. $\therefore$ f is odd permutation

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

Proof: Let $S = \{a_1 a_2 \cdots a_n\}$. Let f be a permutation on S. Let us consider the elements $a_1, f(a_1), f^2(a_1), \cdots$. All these can not be distinct, since all of them belong to S as S is finite set.

Let r be the least positive integer such that $f^r(a_1) = a_1$.

Then $a_1, f(a_1), f^2(a_1), \cdots f^{r-1}(a_1)$ are r distinct elements of S because if $f^p(a_1) = f^q(a_1)$ for some positive integer p and q such that $0 < p < q < r$.

then $f^{q-p}(a_1) = a_1$ holds and this contradicts that r is the least positive integer $(\because q-p < r)$ satisfying $f^r(a_1) = a_1$.

Let us consider r cycle $p_1 = (a_1, f(a_1), f^2(a_1), \cdots, f^{r-1}(a_1))$.

If $r = n$ then $f = p_1$ and the theorem is proved.

If $r < n$, let a_m be the 1st element among $a_2, a_3, \cdots, a_n$ such that a_m does not belong to the cycle p_1.

Let us consider the elements $a_m, f(a_m), f^2(a_m), \cdots$. Neither of these belong to p_1 because if $f^i(a_1) = f^j(a_m)$ for some positive integers i, j then $f^{i-j}(a_1) = a_m$, a contradiction.

So we arrive at cycle $p_2 = (a_m, f(a_m), f^2(a_m), \cdots, f^{s-1}(a_m))$ of length s.

If $r + s = n$ then f is the product of disjoint cycles p_1 and p_2.

If $r + s < n$, let a_k be the 1st element among $a_2, a_3 \cdots a_{m-1}, a_{m+1}, \cdots, a_n$ which does not belong to p_1 or p_2

Proceeding in the same way, this process terminates after finite number of steps as S is finite set.

So the decomposition of f as the product $p_1 \cdot p_2 \cdot p_3 \cdots p_t$ of disjoint cycles.

Note: Since multiplication of disjoint cycles is commutative as the order of the factors $p_1, p_2, \cdots p_t$ in which they appear in the decomposition of f is not unique.

Disjoint Permutation: Two permutations f and g on a finite set S are called disjoint if (i) for any $x \in S$, $f(x) \neq x$ $\Rightarrow g(x) = x$ and (ii) for any $x \in S$, $g(x) \neq x \Rightarrow f(x) = x$

Example: Let $f = (12)$ and $g = (1,3)$ be two permutations in S_3.

Here, $f(1) = 2$ and $g(1) = 3 \neq 1$

So, f and g are not disjoint permutation in S_3.

Again, in S_5, $f = (1\,3\,2)$, $g = (4\,5)$ are disjoint.

Theorem: Prove that any two disjoint permutations are commutative.

Proof: Let f and g be any two disjoint permutation on a finite set S. We have to show that $fog = gof$.

Let $x \in S$.

Suppose $f(x) \neq x$ then $g(x) = x$

Let $f(x) = y$ then $y \neq x$

Now, $(gof)(x) = g(f(x)) = g(y) = y$ because if $g(y) \neq y$ then $f(y) = y$

$\Rightarrow f(y) = f(x)$ $(y = f(x))$

$\Rightarrow y = x$ (f is one one)

which contradicts the above $f(x) = y$.

and $(fog)(x) = f(g(x)) = f(x) = y$

Hence $fog = gof$ $\forall x \in S$, such that $f(x) \neq x$.

Again if $x \in S$ be such that $f(x) = x$, then $g(x) \neq x$.

Proceeding as above, we have $fog = gof$.

Hence the Theorem.

Ex The cycles (2435) and (168) are disjoint cycles whereas (4532) and (138) are not disjoint.

Let $\alpha = (2435)$ $\beta = (168)$.

$$\alpha\beta = (2435)(168) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 5 & 3 & 2 & 8 & 7 & 1 \end{pmatrix}$$

$$\beta\alpha = (168)(2435) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 5 & 3 & 2 & 8 & 7 & 1 \end{pmatrix}$$

Hence $\alpha\beta = \beta\alpha$.

Theorem: The order of a permutation on a finite set is the l.c.m of the lengths of its disjoint cycles.

Proof: Let f be a permutation on the set $S = \{a_1, a_2, \cdots, a_n\}$ and let f be expressed as the product of disjoint cycles $p_1, p_2, \cdots, p_m$ of lengths $r_1, r_2, \cdots, r_m$ respectively. Then $f = p_1 p_2 \cdots p_m$.

Thus $f^n = p_1^n p_2^n \cdots p_m^n$ for each positive integer n, since the multiplication of disjoint cycles is commutative.

$p_1^{r_1} = p_2^{r_2} = \cdots = p_m^{r_m} = i$, i being the identity permutation.

Let s be the common multiple of $r_1, r_2, \cdots, r_m$. Then

$$f^s = p_1^s p_2^s \cdots p_m^s = i$$

Obviously, the least positive integer r for which $f^r = i$ holds, must be the least value of s.

So, r is the l.c.m of $r_1, r_2, \cdots, r_m$

Therefore, the order of f is the l.c.m of $r_1, r_2, \cdots, r_m$.

$\boxed{\text{Ex}}$: Let S be the non empty finite set and f be a permutation on S. For $a, b \in S$, define a relation ρ on S by $a \rho b \Leftrightarrow f^n(a) = b$ for some integer n. Prove that ρ is an equivalence relation.

Ans: Given that $\rho = \{(a, b) \in S \times S : f^n(a) = b\}$

Reflexive: Let $a \in S$ and $a \rho a$ holds

as $f^0(a) = i(a) = a$ where i is the identity permutation.

$\therefore$ $a \rho a$ holds $\forall a \in S$.

Symmetric: Let $a, b \in S$ and $a \rho b$ holds.

$\therefore a \rho b \Rightarrow f^n(a) = b$

$\Rightarrow a = f^{-n}(b) \Rightarrow b \rho a$

Where f^{-n} is the inverse of f^n as f is one one onto.

Transitive: Let $a, b, c \in S$ and $a \rho b$ and $b \rho c$ both holds.

$a \rho b \Rightarrow f^n(a) = b$

$b \rho c \Rightarrow f^m(b) = c$

clearly, $f^{m+n}(a) = (f^m f^n)(a)$
$= f^m(f^n(a)) = f^m(b) = c$.

$\Rightarrow a \rho c$

Hence ρ is an equivalence relation, and thus partition of S into disjoint equivalence classes.

Defn: The equivalence class of any element $a \in S$ is called orbit of a (under f). Thus, $cl(a) = \{x \in S \,/\, x \rho a\}$
$= \{f^n(a) : n$ being integer$\}$ = orbit of a

Theorem: If S is a finite set and $f \in A(S)$, the set of permutations on S then $\exists$ a positive integer m such that orbit of x is $\{x, f(x), f^2(x), \dots, f^{m-1}(x)\}$.

Proof: Since S is finite set so $A(S)$ has finite number of elements. As $f \in A(S)$, $f^2, f^3, \dots$ all are belongs to $A(S)$ and as order of $(A(S))$ is finite, after a certain stage some integral powers of f will be identity of $A(S)$. Let m be the smallest positive integer such that $f^m(x) = x$.

Now, $x, f(x), \dots, f^{m-1}(x)$ will be all distinct as if $f^r(x) = f^s(x)$ for some positive integer r & s such that $0 \leq r < s \leq m-1$ then $f^{s-r}(x) = x$. but $s-r < m$ leads to a contradiction to the choice of m. Hence $x, f(x), f^2(x), \dots f^{m-1}(x)$ are distinct elements of the orbit of x.

To show that the orbit contains no other elements. Suppose, x^t is any other element in the orbit then $\exists$ some integer n s.t. $f^n(x) = x^t$.

But $n = mq + r$. for some integer q and r where $0 \leq r < m$

$\therefore x^t = f^n(x) = f^{mq+r}(x) = f^r\{f^{mq}(x)\} = f^r[f^{mq}(x)]$
$= f^r(x) \quad [\because f^m(x) = x]$
, $0 \leq r \leq m-1$.

Scanned with CamScanner

This implies that x^t is one of the earlier members.

Hence the Theorem.

The following results are proved trivially:

(a) The product of two even permutations is even as sum of two even numbers is even.

(b) The product of two odd permutations is even as the sum of two numbers is even

(c) The product of an even and odd permutation is odd as the sum of an even and odd number is odd.

(d) Inverse of an even (odd) permutation is even (odd).

(e) Identity permutation is always even.

$\boxed{\text{Ex}}$: Show that a cycle of even length is an odd permutation and cycle of odd length is an even permutation.

Ans: Let us consider permutation (1 2 3 4) which is of cycle of even length.

Since (1 2 3 4) = (1 4) (1 3) (1 2), there are odd number of transposition. So (1 2 3 4) is odd permutation.

It is now trivial that the result is generalised to any cycle.

So, $(1\,2\,3\,4 \cdots n) = (1\,n)\ (1\ n-1) \cdots (1\,2)$

proves our assertion.

Symmetric Group S_n:

Prove that the set of all permutations on the set $\{1, 2, 3, \ldots, n\}$ forms a group w.r.to permutation multiplication.

Ans: Let S be the set of all permutations on the set $\{1, 2, 3, \ldots, n\}$.

To show that S forms a group w.r.to permutation multiplication

Closure property: Let f, g be two permutations on the set $\{1,2,\dots,n\}$. Then $f \cdot g$ is also permutation on the set $\{1,2,\dots,n\}$.
Therefore, $f \in S, g \in S \Rightarrow f \cdot g \in S$.

Associative property: A permutation on S is a bijective mapping from the set $\{1,2,\dots,n\}$ onto itself, and multiplication of two permutations is the composition of two bijective mappings. Since composition of mappings is associative, multiplication of permutations is also associative.

Identity Property: The identity permutation $i = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \in S$ and it is the identity element in S as $i \cdot f = f \cdot i = f$ $\forall f \in S$.

Inverse property: Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix} \in S$.
Then the permutation $g = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & & n \end{pmatrix} \in S$
and g is the inverse of f, since $f \cdot g = g \cdot f = i =$ identity permutation.
Therefore the inverse of each element in S exists.
Therefore $(S, \cdot)$ is a group w.r.to permutation multiplication.
This group is called symmetric group of degree n & denoted by S_n and $O(S_n) = \underline{|n}$.

Note: Multiplication of permutation is not commutative.
For ex: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix} = (1\,2)$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix} = (1\,3)$.

$f \cdot g = (12)(13) = (1\,3\,2)$ and $g \cdot f = (13)(12) = (1\,2\,3)$.

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

So, S_n is non-commutative group.

Q. Prove that the set of all permutations on three symbols forms a group w.r.to permutation multiplication.

Scanned with CamScanner

Let S be the set of all permutations on the set $\{1,2,3\}$.
So there are $\lfloor 3$ i.e. 6 elements in S.
The six elements of S are $P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$ $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$, $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$.
$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$.

Let us form a composition table w.r.to permutation multiplication.

	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	P_0	P_5	P_3	P_4
P_2	P_2	P_0	P_1	P_4	P_5	P_3
P_3	P_3	P_4	P_5	P_0	P_1	P_2
P_4	P_4	P_5	P_3	P_2	P_0	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

Closure prop: It is seen from the composition table that S is closed under permutation multiplication.

Associative Prop: A permutation on S is a bijective mapping from the set S onto itself. Multiplication of permutations is the composition of two bijective mappings. Since composition of mappings is associative, so permutation multiplication is associative.

Identity prop: From the above table, it is seen that P_0 is the identity element.

Inverse Prop: The inverses of $P_0, P_1, P_2, P_3, P_4, P_5$ are $P_0, P_2, P_1, P_3, P_4, P_5$ respectively.

The composition table is not symmetric about the main diagonal, so permutation multiplication is not commutative.

Thus, the set S forms a non-abelian group with respect to permutation multiplication. This group is called the symmetric group of degree 3 and order 6. This group is denoted by S_3.

Alternating group A_n :

The set of all even permutations on the set $\{1, 2, 3 \cdots, n\}$ forms group with respect to permutations multiplication.

This group is called the alternating group of degree n and denoted by A_n. A_n contains $\frac{\underline{|n}}{2}$ elements. A_n is a non-commutative group for $n \geq 4$.