2.8 Automorphisms :-

Definition:

An isomorphism of a group G onto itself called an Automorphism of G.

Example :1

Show that the mapping $T: G$ is defined by $T(x) = -x$ for all $x \in G$. Where G is the additive group of integers.

Soln:

obviously, the mapping T is one-one onto.

Let x_1, x_2 be any two elements of G.

Then $T(x_1 + x_2) = -(x_1 + x_2)$

$= (-x_1) + (-x_2) = T(x_1) + T(x_2)$

Hence T is an automorphism of G.

Example: 2

Show that $T: a \to a^{-1}$ is an automorphism of a group G iff G is abelian.

Solution:

Let $T: G \to G$ be such that

$T(x) = x^{-1} \quad \forall\ x \in G$

The function T is one-one.

$\therefore (x) = (y) \Rightarrow x^{-1} = y^{-1}$

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

Also if $x \in G$, then $x^{-1} \in G$ and we have

$$T(x^{-1}) = (x^{-1})^{-1} = x$$

$\therefore$ T is onto.

Now Suppose G is abelian

Let x, y be any two elements of G.

Then $T(xy) = (xy)^{-1}$

$= y^{-1}x^{-1} = x^{-1}y^{-1}$ [$\because$ G is abelian]

$= T(x) \cdot T(y)$

$\therefore$ T is an automorphism of G.

Converse:

Suppose T is an automorphism of G.

Let $x, y \in G$.

We have $T(xy) = (xy)^{-1}$

$= y^{-1}x^{-1} = x^{-1}y^{-1}$ [$\because$ G is abelian]

$= T(y)T(x)$

$= T(yx)$ [$\because$ T is an automorphism].

Since T is one-one.

$T(xy) = T(yx)$

$\Rightarrow xy = yx \Rightarrow$ G is abelian.

Lemma 2.8.1

If G is a group, then $A(G)$, the set of automorphism of G, is also a group.

Proof:

Let I be the mapping of G which sends every

element onto itself.

i.e $xI = x$ for all $x \in G$

I is an trivial Automorphism of G.

Let $\mathcal{A}(G)$ denote the set of all automorphism of G is a subset of the set of one-to-one mappings of G onto itself. It is denoted as $A(G)$.

i.e $\mathcal{A}(G) \subset A(G)$.

For elements of $\mathcal{A}(G)$ we can use the product of $A(G)$. This product satisfies **ASSOCIATIVE law** in $A(G)$ is also in $\mathcal{A}(G)$ (obviously).

I be the **unit element** of $A(G)$ is in $\mathcal{A}(G)$.

Next we show that $\mathcal{A}(G)$ is a subgroup of $A(G)$ and so itself is a group.

If T_1, T_2 are in $\mathcal{A}(G)$, we know that $T_1 T_2 \in A(G)$.

For all $x, y \in G$.

$$(xy)\,T_1 = (xT_1)\,(yT_1)$$

$$(xy)\,T_2 = (xT_2)\,(yT_2)$$

$$\therefore (xy)T_1T_2 = ((xy)\,T_1)\,T_2$$

$$= ((xT_1)(yT_1))\,T_2$$

$$= (xT_1T_2)\,(yT_1T_2)$$

$$\Rightarrow T_1T_2 \in \mathcal{A}(G)$$

Next we show that $T^{-1} \in \mathcal{A}(G)$.

If $T \in \mathcal{A}(G)$, $x, y \in G$, Then

$((xT^{-1})(yT^{-1}))T = ((xT^{-1})T)((yT^{-1})T)$

$= (xI)(yI)$

$= xy.$

$(xT^{-1})(yT^{-1}) = (xy)T^{-1}$

$\Rightarrow T^{-1} \in A(G)$

$\therefore A(G)$ is a subgroup of $A(G)$ and also itself is a group.

Lemma 2.8.2.

$I(G) \cong G/Z$ where $I(G)$ is the group of inner automorphisms of G, and Z is the centre of G.

Proof:

Let G be a group for $g \in G$

$T_g : G \to G$ by $xT_g = g^{-1}xg$ for all $x \in G$.

We claim that T_g is automorphism.

T_g is onto

For given $y \in G$, let $x = gyg^{-1}$

Then $xT_g = g^{-1}xg$

$= g^{-1}(gyg^{-1})g$

$= (g^{-1}g)y(g^{-1}g) = y.$

$\therefore T_g$ is onto.

T_g is homomorphism

For $x, y \in G$,

$(xy)T_g = g^{-1}(xy)g$

$= g^{-1}x(gg^{-1})yg$

$$= (g^{-1}xg)(g^{-1}yg)$$

$$= (x T_g)(y T_g).$$

consequently, T_g is homomorphism of G onto itself.

Further to prove that T_g is 1-1

For, if $x T_g = y T_g$

$$g^{-1}xg = g^{-1}yg$$

$$x = y \qquad \text{[using cancellation laws]}.$$

T_g is called the inner automorphism of G.

If G is non abelian, there is a pair $a, b \in G$ such that $ab \neq ba$.

But then $b T_a = a^{-1}ba \neq b$

$\therefore T_a \neq I$ [$\because$ G is non abelian].

Thus for a non abelian group G, there exists non trivial automorphism.

Let $I(G) = \{ T_g \in A(G) / g \in G \}$

Now to show that $I(G)$ is a subgroup of $A(G)$.

We compute that T_{gn}, for $g, n \in G$.

If $x \in G$, then by definition.

$$x T_{gh} = (gh)^{-1} x (gh)$$

$$= h^{-1}(g^{-1}xg)h$$

$$= h^{-1}(g^{-1}xg)h$$

$$= (g^{-1}xg) T_h$$

$$= x T_g T_h$$

$$x T_g T_g^{-1} = [x T_g] T_g^{-1}$$

$$= (g^{-1}xg) T_g^{-1}$$

$$= (g^{-1})^{-1}(g^{-1}xg)g^{-1}$$

$$= (g^{-1})^{-1} g^{-1} x g g^{-1}$$

$$= x$$

$\Rightarrow T_{gh} = T_g T_h$ $\Rightarrow T_{g^{-1}} = (T_g)^{-1}$

Thus $I(G)$ is a subgroup of $A(G)$.

$I(G)$ is called the group of Inner automorphism of G and it is suggestive.

Next, we defined the mapping

$\psi : G \to A(G)$ by $\psi(g) = T_g$ $\forall\ g \in G$.

Then $\psi(gh) = T_{gh} = T_g T_h = \psi(g)\psi(h)$.

$\therefore \psi$ is a homomorphism of G into $A(G)$ whose image is $I(G)$.

Next we have to find the kernel of ψ.

Suppose let K be the kernel and $g_0 \in K$

Then $\psi(g_0) = I$.

By definition $\psi(g_0) = T_{g_0}$

comparing this above, $T_{g_0} = I$.

But this says that for any $x \in G$,

$$x T_{g_0} = x .$$

But By defn $x T_{g_0} = g_0^{-1} x g_0$

So $x = g_0^{-1} x g_0$

$\Rightarrow g_0 x = x g_0$

$\therefore g_0$ must commute with all elements of G.

But the centre of G it is ~~defini~~ denoted as Z,

i.e z was defined to be precisely all elements

in G which commute with every elements of G.

Thus $K \subset Z \rightarrow I$

Next we take if $z \in Z$ Then $x T_I = z^{-1} x z$

$$x T_z = z^{-1}(xI) = z^{-1}(zx) \qquad [\because xz = Ix]$$

$$= (z^{-1}z)\, x.$$

$$x T_z = x \Rightarrow T_z = I$$

$$\Rightarrow z \in K.$$

Thus $Z \subset K$ — II

From I & II

$$K = Z$$

Summarizing, ψ is a homomorphism of G into A(G) whose image is I(G) and kernel I.

Using Fundamental theorem of homomorphism.

$$I(G) \cong G/Z$$

Definition: Inner Automorphism of G.

If G is a group, the mapping

$T_g : G \rightarrow G$ defined by $T_g(x) = g^{-1}xg$ $\forall$ $x \in G$ is an automorphism of G is known as inner automorphism of G.

Lemma : 2.8.3.

Let G be a group and ϕ an automorphism of G. If $a \in G$ is of order $O(a) > 0$, then $O(\phi(a)) = O(a)$.

Proof:

Suppose that ϕ is an automorphism of a group G and $a \in G$ has order n.

Then $\phi(a)^n = \phi(a^n) = \phi(e) = e$.

Hence $\phi(a)^n = e$.

If $\phi(a)^m = e$ for some $0 < m < n$, then $\phi(a^m) = \phi(a)^m = e$

$\Rightarrow$ $a^m = e$ $[\because \phi$ is 1-1$]$

which is contradiction $[\because O(a) = n]$

Hence $O(\phi(a)) = O(a)$.

2.9. Cayley's Theorem.

Lemma

Theorem 2.9.1: (Cayley's)

Every group is isomorphic to a subgroup of A(S) for some appropriate S.

Proof:

Let G be a group FOR the set S we will use the elements of G. ;i.e put $S = G$.

If $g \in G$, define a function.

$T_g : S(=G) \longrightarrow S(=G)$ by

$T_g : S \to S$ $\quad T_g(x)$ (or) $x T_g = xg$.

First we claim that $T_g \in A(S)$

[where $A(S)$ be the set of all 1-1 mappings of the set S onto itself].

T_g is 1-1

[if images are equal then elements are equal].

For, if $x, y \in S$ and $xT_g = yT_g$

i.e $xT_g = yT_g$ images are equal

$$xg = yg$$

$$\Rightarrow x = y \quad \text{[using cancellation law]}.$$

elements are equal.

$\therefore$ T_g is 1-1

T_g is onto.

[Every element in codomain has pre-image in the domain].

Take $y \in G$ element in the codomain.

If we choose $x = yg^{-1}$. for some $x \in G$.

$$\Rightarrow xT_g = xg = (yg^{-1})g = y(g^{-1}g) = y$$

$$\Rightarrow xT_g = y.$$

$\Rightarrow$ T_g is onto.

Let $A(S) = \{T_g / g \in G\}$ defined by a composition of function $T_g \cdot T_h = T_{gh}$

Next we prove that $A(S)$ forms a group.

closure:

If $T_g \cdot T_h \in A(S)$ Then $g, h \in G$ so $gh \in G$

$\therefore \quad T_{gh} \in A(S)$.

Associative:

If $T_a, T_b, T_c \in A(S)$ for some $a, b, c \in G$.

$(T_a T_b) T_c = (T_{ab}) T_c$

$= T_{abc} = T_{a(bc)} = T_a T_{bc}$

$= T_a (T_b T_c)$

Identity: Let $e \in G$ [$\because$ e is identify of G)

$T_g T_e = T_{ge} = T_g$

$T_e T_g = T_{eg} = T_g$

T_e is identity of $A(S)$.

Inverse:

Let $a \in G$ Then $\exists\, a^{-1} \in G$ such that

$T_a T_{a^{-1}} = T_{aa^{-1}} = T_e$

$T_{a^{-1}} T_a = T_{a^{-1}a} = T_e$

$T_{a^{-1}}$ is the inverse of T_a.

$\therefore$ $A(S)$ forms a group.

Next we define $\psi : G \to A(S)$ is defined by

$\psi(g) = T_g$ for some $g \in G_1$.

ψ is homomorphism: Let $g, h \in G_1$

$$\psi(gh) = T_{gh}$$
$$= T_g T_h = \psi(g)\psi(h)$$

$\therefore \psi$ is homomorphism.

Next we define Kernel of ψ.

Let us K be the Kernel of ψ for some $g_0 \in K$. Then $\psi(g_0) = T_{g_0}$.

T_{g_0} is the identity map on S FOR some $x \in G_1$,

In particular for $e \in G_1$,

$$e\, T_{g_0} = e \longrightarrow (1)$$

But $e\, T_{g_0} = e\, g_0 = g_0 \longrightarrow (2)$

compare (1) & (2) we get

$$g_0 = e.$$

Hence $K = (e)$

$\therefore \psi$ is an isomorphism of G_1 into $A(S)$.

Hence the proof:

PERMUTATIONS

permutations:

Definition:

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

The number of elements in the finite set S is known as the degree of permutation.

Symbol for a permutation:

Let $S = \{a_1, a_2, a_3 \ldots\ldots a_n\}$

be a finite set having n distinct elements

If $f: S \to S$ and f is one-one onto.

Then,

f is a permutation of degree n.

Let, $f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$, $\ldots\ldots f(a_n) = b_n$.

where,

$\{b_1, b_2, \ldots b_n\} = \{a_1, a_2, \ldots, a_n\}$ i.e, $b_1, b_2, \ldots, b_n$ is nothing but some arrangement of the n element of S.

We find it convenient to introduce a two line notation to write this permutation.

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ b_1 & b_2 & b_3 \ldots b_n \end{pmatrix}$$

If $S = \{1, 2, 3, 4\}$ is a finite set having four elements.

Then,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

are all permutations of degree 4,

Here in the permutation f the elements 1, 2, 3, 4 have been replaced respectively by the elements 2, 4, 1, 3.

Thus,

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

Each element in the first row is to replaced by the element directly below in the second row.

Equality of two permulations:

Two permulations f and g of degree n are said to be equal if we have $f(a) = g(a)$ $\forall a \in S$ For ex,

if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

are two permutations of degree 4,

we have, $f = g$

If f and g replace 1 by 2, 2 by 3, 3 by 4 and 4 by 1.

If $f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ b_1 & b_2 & b_3 \ldots b_n \end{pmatrix}$ is a permutation of degree n.

we can write it in several ways.

The interchange of columns will not change the permutation.

$$f = \begin{pmatrix} a_2 & a_1 & a_3 \ldots a_n \\ b_2 & b_1 & b_3 \cdots b_n \end{pmatrix} = \begin{pmatrix} a_n & a_1 \ldots a_2 \\ b_n & b_1 \cdots b_2 \end{pmatrix} = \begin{pmatrix} a_n & a_{n-1} \cdots a_2 & a_1 \\ b_n & b_{n-1} \cdots b_2 & b_1 \end{pmatrix} \text{etc.}$$

$\therefore$ If f and g are two permutations of degree n.

Then we can always write g in such way that first row of g coincides with the second row of f.

Ex:

If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ & $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

are two permutations of degree 4.

Then by interchanging columns we can write

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

Total Number of distinct permutations of degree n:

If S is a finite set having n distinct elements.

Then we shall have n! distinct arrangements of the elements of S.

∴ There will be n! distinct permutations of degree n.

If P_n be the set consisting of all permutations of degree n, then the set P_n will have n! distinct elements.

This set P_n is called the Symmetric Set of permutations of degree n.

$P_n = \{f : f$ is a permutation of degree $n\}$.

The set P_3 of all permutations of degree 3 will have 3!

6 elements obviously:

$$P_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Identity permutation:

If I is a permutation of degree n such that I replaces each element by the element itself. I is called the identity permutation of degree n.

Then,

$$I = \begin{pmatrix} 1 & 2 & 3 \dots n \\ 1 & 2 & 3 \dots n \end{pmatrix} \text{ or } \begin{pmatrix} a_1 & a_2 & a_3 \dots a_n \\ a_1 & a_2 & a_3 \dots a_n \end{pmatrix} \text{ or } \begin{pmatrix} b_1 & b_2 & b_3 \dots b_n \\ b_1 & b_2 & b_3 \dots b_n \end{pmatrix}$$

is the identity permutation of degree n.

Product or composite of two permutations:-

The product or composite of two permutations f and g of degree n denoted by fg is obtained by first carrying out the operation defined by f and then by g.

Suppose,

P_n is the set of all permutations of degree n.

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 \dots a_n \\ b_1 & b_2 & b_3 \dots b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 & b_3 \dots b_n \\ c_1 & c_2 & c_3 \dots c_n \end{pmatrix}$

by any two elements of P_n.

If f and g is denoted multiplicatively by fg.

$$fg = \begin{pmatrix} a_1 & a_2 & a_3 \dots a_n \\ c_1 & c_2 & c_3 \dots c_n \end{pmatrix}$$

f replaces a_1 by b_1 and then g replaces by b_1 by c_1.
So that, fg replace a_1 by c_1.

similarly,

fg replaces a_2 by c_2, a_3 by c_3, ..., a_n by c_n.

obviously,

fg is also a permutation of degree n.

The product of two permutations of degree n is also a permutation of degree n.

$\therefore fg \in P_n \; \forall f, g \in P_n$.

Example: 1

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two Permutations of degree 3.

Soln:

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

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

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

Cond

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

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

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

obviously $fg \neq gf$

fg replaces 1 by 2 while gf replaces 1 by 3.

So fg cannot be equal to gf.

Thus we see that multiplication of permutations is not in general commutation.

Example : 2

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ be two permutations of degree 5.

Soln: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$

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

f replace 1 by 2 and g replaces 2 by 2.

$\therefore fg$ replaces 1 by 2.

f replaces 2 by 3 and g replaces 4 by 5.

$\therefore fg$ replace 3 by 5.

Groups of permutations:

Theorem:

The Set P_n of all permutations on n symbols is a finite group of order $n!$ with respect to composite of mappings as the operation. For $n \leq 2$, this group is abelian and for $n > 2$ it is always non-abelian.

Proof:

Let $S = \{a_1, a_2, \ldots, a_n\}$ be a finite set having n distinct elements.

Let $f = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$ be a permutation degree n.

Here elements $b_1, b_2, \dots b_n$ the second row are simply an arrangement of n elements $a_1, a_2, \dots a_n$ of set S.

If P_n the set of all permutations of degree n then P_n has n! distinct elements.

Let $f = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 \dots b_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$

$$fg = \begin{pmatrix} a_1 & a_2 \dots a_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$$

obviously,

fg is also a permutation of degree n.

Thus $fg \in P_n \; \forall \; f, g \in P_n$.

$\therefore P_n$ is closed with respect to the composition known as product of two permutations.

Associativity:

Permutation multiplication is associative.

Let $f = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}, g = \begin{pmatrix} b_1 & b_2 \dots b_n \\ c_1 & c_2 \dots c_n \end{pmatrix}, h = \begin{pmatrix} c_1 & c_2 \dots c_n \\ d_1 & d_2 \dots d_n \end{pmatrix}$

Then,

$$(fg) = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 \dots b_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \dots a_n \\ c_1 & c_2 \dots c_n \end{pmatrix}$$

$$(fg)h = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ c_1 & c_2 \cdots c_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 \cdots c_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \cdots a_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}$$

Also, $(gh) = \begin{pmatrix} b_1 & b_2 \cdots b_n \\ c_1 & c_2 \cdots c_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 \cdots c_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}$

$$= \begin{pmatrix} b_1 & b_2 \cdots b_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}$$

$$\therefore f(gh) = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 \cdots b_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}.$$

$$= \begin{pmatrix} a_1 & a_2 \cdots a_n \\ d_1 & d_2 \cdots d_n \end{pmatrix}$$

Thus, $(fg)h = f(gh)$

Existence of Identity:

Let $I = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ a_1 & a_2 \cdots a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 \cdots b_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}$

be the identity permutation of degree n.

Then $I \in P_n$

If $f = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}$ is any element of P_n.

we have

$$fI = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 \cdots b_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \cdots a_n \\ b_1 & b_2 \cdots b_n \end{pmatrix}$$

$$= f.$$

Also,

$$If = \begin{pmatrix} a_1 & a_2 \dots a_n \\ a_1 & a_2 \dots a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$$

$$= f$$

$\therefore$ Identity permutation I is the identity element.

Existence of Inverse:

Let $f = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$ be any element of P_n.

Then, $f^{-1} = \begin{pmatrix} b_1 & b_2 \dots b_n \\ a_1 & a_2 \dots a_n \end{pmatrix}$ is also an element of P_n.

Since,

f^{-1} is also a permutation of degree n.

we have,

$$f^{-1} f = \begin{pmatrix} b_1 & b_2 \dots b_n \\ a_1 & a_2 \dots a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & b_2 \dots b_n \\ b_1 & b_2 \dots b_n \end{pmatrix} = I$$

$$f f^{-1} = \begin{pmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 \dots b_n \\ a_1 & a_2 \dots a_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \dots a_n \\ a_1 & a_2 \dots a_n \end{pmatrix} = I$$

$\therefore$ f^{-1} is the inverse of f.

Hence P_n is a group of order $n!$ with respect to product of permutations as composition.

If $n=1$, the set P_n has only one element and every group of order 1 is abelian.

If $n=2$, the set P_n has $2!$ i.e 2 elements and every group of order 2 is again abelian.

Now,

we show that if $n>2$, P_n is abelian.

Let, $$fg = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 2 \end{pmatrix}$$

and $$gf = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n-1 & n \\ 2 & 1 & 3 & 4 \dots & n-1 & n \end{pmatrix}$$

be the two permutations of degree n. when $n>2$.

Then, $$fg = \begin{pmatrix} 1 & 2 & 3 \dots & n-1 & n \\ 1 & 3 & 4 \dots & n & 2 \end{pmatrix}$$

and $$gf = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n-1 & n \\ 3 & 2 & 4 & 5 \dots & n & 1 \end{pmatrix}$$

Obviously $fg \neq gf$

$\therefore P_n$ is non-abelian if $n>2$.

Note: 1

If $f = \begin{pmatrix} a_1 & a_2 & a_3 \dots a_n \\ b_1 & b_2 & b_3 \dots b_n \end{pmatrix}$ be a permutation of degree n, then inverse of f^{-1} is obtained by interchanging the rows of f. Thus $f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 \dots b_n \\ a_1 & a_2 & a_3 \dots a_n \end{pmatrix}$

Note: 2

we can use the numbers $1, 2, 3, \dots n$. or we can use the letters $a_1, a_2, \dots a_n$ or any symbols.

Note: 3.

The group P_n of all permutations of degree n is called the Symmetric group of degree n or the Symmetric group of order n!

Cyclic Permutations:

Definition:

Suppose f is a permutation of degree n on a set S leaving n distinct elements. Let it be possible to arrange m elements of the set S in a row in such a way that the f-image of each element in the row is the element which follows it, the f-image of of the as element which is the force element and the remaining n-m elements of the set S are left unchanged by f. Then f is called a cyclic permutation or a cyclic of length m or an m-cycle.

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

we can write form of the cycle

(1 2 3 4 5 6)

which is of length 6.

Permutations represented by a cycle:

(1 3 4 2 6) is a cycle of length 5

Suppose

It represents a permutation of degree 9 on a set is S consisting of the length 1, 2, ... 9.

$$\begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

The image of each element in the cycle (1 3 4 2 6)
The missing elements 5, 7, 8, 9.
However,

If the cycle (1 3 4 2 6) represents a permutation of degree 6 on six symbols 1, 2, 3, 4, 5, 6.

Then the corresponding permutation

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

Important Note:

A cycle does not change by changing the places of its elements provided their cycle order is not changed.

Thus, (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3)

(1 2) = (2 1), (2 3) = (3, 2).

Transpositions Definition:

A cycle of length two is called a transposition.

Thus the cycle (1 3) is a transposition.

It will represent a permutation in which the image of 1 is 3 The image of 3 is 1 and remaining missing elements are left unchanged In the transposition (2 3) is a permutation of degree 3 on three symbols 1, 2, 2.

Then,

the corresponding permutation will be

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Multiplication of cycle:

cycles by multiplying the permutations represented by them.

Ex:

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

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

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

Since, a cycle of length one represents the identity permutation.

$$\therefore (1)\ (1\ 3\ 4)\ (6) = (2\ 3\ 4)$$

Disjoint cycles:

Two cycles are said to be disjoint if they have no symbols in common.

Ex:

$(1\ 3\ 5)$ and $(2\ 6\ 8\ 9)$ are disjoint cycles while $(1\ 3\ 4)$ and $(2\ 3\ 5\ 6)$ are not disjoint.

Theorem:

If f and g are two disjoint cycles, then $fg = gf$ the product of disjoint cycles is commutative.

Proof:

The cycles f and g have no symbols common

∴ The element permuted by f are left unchanged by g and also the elements permuted by g remain the same under f.

we have $fg = gf$

Let $f = (1\ 2\ 3)$ and $g = (1\ 4\ 5)$ represent two permutation on 5 symbols $1, 2, \ldots 5$.

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

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

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

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

$$= gf$$

Inverse of a cyclic permutation:

To prove that $(1\ 2\ 3 \ldots n)^{-1} = (n\ n-1 \ldots 3\ 2\ 1)$, i.e to write the inverse of a cycle we should write its elements in the reverse order.

proof:

we have $(1\ 2\ 3 \ldots n)(n \ldots 3\ 2\ 1)$

$$= \begin{pmatrix} 1 & 2 & 3 \dots n-1 & n \\ 2 & 3 & 4 \dots n & 1 \end{pmatrix} \begin{pmatrix} n & \dots & 4 & 3 & 2 & 1 \\ n-1 & \dots & 3 & 2 & 1 & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \dots n-1 & n \\ 1 & 2 & 3 \dots n-1 & n \end{pmatrix} = I$$

Also, $(n \dots 3\ 2\ 1)(1\ 2\ 3 \dots n) = I$

$\therefore (1\ 2\ 3 \dots n)^{-1} = (n \dots 3\ 2\ 1)$

In particular every transposition is its own inverse. If $(1\ 2)$ is a transposition.

$$(1\ 2)^{-1} = (2\ 1) = (1\ 2)$$

Inverse of a product of cyclic permutations:

If f and g are any two cycles.

then $(fg)^{-1} = g^{-1} f^{-1}$

Also $(fgh)^{-1} = h^{-1} g^{-1} f^{-1}$

If f and g are disjoint cycles

then $(fg)^{-1} = (gf)^{-1}$

$$= f^{-1} g^{-1}$$

$[(1\ 2\ 3)(4\ 5)(2\ 6)]^{-1} = (2\ 6)^{-1} (4\ 5)^{-1} (1\ 2\ 3)^{-1}$

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

Also

$[(1\ 3\ 5)(2\ 4)]^{-1} = (1\ 3\ 5)^{-1} (2\ 4)^{-1}$

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

We shall now give some important results on the product of permutations.

Theorem 1:

Every permutation can be expresed as a product of disjoint cycles.

verification:

let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 8 & 6 & 9 & 7 & 5 \end{pmatrix}$ be a permutation of degree 9 on the set $\{1, 2, \ldots 9\}$

we have,

$f = (4)(6)(1\ 2\ 3)(5\ 8\ 7\ 9)$

Explanation:

First we put down cycles of length one with the help of elements which remain unchanged under f.

Then we start with an element which is not left unchanged:

Thus we start with 1. After 1 we write the image of 1 which is 2.

After 2 we write the image of 2 which is 8 After 8 we do not write an is element but we close the bracket since the image of the last element 3 is the first element 1 of the bracket.

Now,

We start a new bracket. In this bracket. we write an element which has not yet been writtes.

Thus we write 5 After 5 we write 5. After 5 we write the image of 5 which is 8.

After 8 we write the image of 8 which is 7.

After 7 we write image of 7 which is 9.

After 9 we close the bracket since the image of 9 is the first element 5.

Our work is finished since each element has been included in one or the other bracket.

Since cycles of length one represent identity permutation therefore we can omit them.

$f = (1\ 2\ 3)(5\ 8\ 7\ 9)$.

Also we can write $f = (5\ 8\ 7\ 9)(1\ 2\ 3)$ because product of disjoint cycles is commutative.

Theorem 2:

Every cycle can be expressed as a product of transpositions in infinitely many ways.

Verification:

consider the cycle $(1\ 2\ 3 \ldots n)$ of length n.

$(1\ 2\ 3 \ldots n) = (1\ 2)(1\ 3)(1\ 4)\ldots(1\ n-1)(1\ n)$

more generally n-cycle.

$(a_1\ a_2\ a_3 \ldots a_n) = (a_1\ a_2)(a_1\ a_3)\ldots(a_1\ a_n)$

4-cycle.

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

Since, $(2\ 3\ 5\ 4) = (3\ 5\ 4\ 2)$

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

Also $(1\ 2)(2\ 1) =$ Identity permutation

we can write

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

$(2\ 5\ 3)(3\ 5\ 2)$ is also identity permutation

we can write

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

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

5-cycle.

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

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

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

Thus every cycle can be expressed as a product of transposition in infinitely many ways.

In the case of any cycle the number of transpositions is either always odd or always even.

Theorem 8:

Every permutation can be expressed as a product of transpositions in infinitely many ways. combining together the results of theorem 1 and theorem 2.

Even and odd permutations:

definition:

A permutation is said to be an even permutation if it can be expressed as a product of an even number of transpositions otherwise it is said to be an.

This definition will be meaningless if a permutation can be expressed sometimes as a product of an odd number of transpositions and sometimes as a product of even number of transpositions.

we claim this defines an equivalence relation on S.

1. $a \equiv \theta^a$ since $a = a\theta^0 = ae$
2. If $a \equiv \theta^b$, then $b = a\theta^i$, so that $a = b\theta^{-i}$, where $b \equiv \theta^a$.
3. If $a \equiv \theta^b$, $b \equiv \theta^c$, then $b = a\theta^i$, $c = b\theta^j = (a\theta^i)\theta^j = a\theta^{i+j}$, which implies that $a \equiv \theta^c$.

we call the equivalence class of an element $s \in S$ the orbit of S under θ.

Thus the orbit of S under θ consists of all the elements $S\theta^i$, $i = 0, \pm 1, \pm 2, \ldots$.

if S is a finite set and $s \in S$.

There is a smallest positive integer $l = l(s)$ depending on such that $s\theta^l = s$.

The orbit of S under θ consists of elements

$$S, S\theta, S\theta^2, \ldots S\theta^{l-1}$$

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

S consists of the elements $1, 2, \ldots 6$.

Then,

$1 = 1\theta^0, \quad 1\theta^1 = 2, \quad 1\theta^2 = 2\theta = 1.$

The orbit of 3 consists just of 3 that of 4 consists of the element 4.

$4\theta = 5, \quad 4\theta^2 = 5\theta = 6, \quad 4\theta^3 = 6\theta = 4.$

The cycle of θ are $(1, 2), (3), (4, 5, 6)$ Suppose that

$$(i, i_2, \ldots i_r)$$

ψ which sends i_1 into i_2, i_2 into $i_3 \ldots i_{r-1}$ into i_r and i_r into i_1, and leave all the order elements. S consists of elements $1, 2 \ldots 9$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix} (1\ 2\ 3)(5\ 6\ 4\ 1\ 8)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 1 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 & 8 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 3 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

we first find the orbit of 1.

$1\theta = 2, \quad 1\theta^2 = 2\theta = 3, \quad 1\theta^3 = 3\theta = 8, \quad 1\theta^4 = 8\theta = 5, \quad 1\theta^5 = 5\theta = 6,$

$1\theta^6 = 6\theta = 4, \quad 1\theta^7 = 4\theta = 1.$

The set $\{1, 2, 3, 8, 5, 6, 4\}$.

The orbits of 7 and 9 can be found be $\{7\}, \{9\}$ respectively.

The cycles of θ are $(7), (9), (1, 10, 10^2, \ldots 10^b) = (1, 2, 3, 8, 5, 6, 4)$.

That is at least in this case, θ is the product of its cycles.

That is at least in this case, θ is the product of its cycles.

But this is no accident for it is now trivial to prove.

Lemma 2.10.1 :

Every permutation is the product of its cycles.

Proof:

Let θ be the permutation.

Then its cycles are of the form.

$$(S, S\theta, \ldots S\theta^{t+1}).$$

Since,

The cycles of θ are disjoint.

The image of $S' \in S$ under θ.

which is $S'\theta$, is the same as the image of S' under the product ψ of all distinct cycle of θ

Hence $\theta = \psi$.

which is what we sought to prove.

The reader should take a given permutation

find its cycles, take their product, and verify the lemma.

every permutation can be uniquely expressed as a product of disjoint cycles.

consider,

The m-cycle $(1, 2, \ldots, m)$

$(1, 2, \ldots m) = (1,2)\ (1,3) \ldots (1, m)$

more generally the m-cycle.

$(a_1, a_2, \ldots a_m) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_m)$

The composition is not unique for instance.

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

Since,

every permutation is a product of disjoint cycles and every cycle is a product of 2-cycles, we have proved.

Lemma 2.10.2:

Every permutation is a product of 2-cycles.

we shall refer to 2-cycles as transpositions.

Definition:

A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transpositions.

The definition given just insists that θ have one representation as a product of an even

number of transpositions.

Perhaps it has other representations as a product of an odd number of transpositions consider the polynomial in n-variables.

$$P(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)$$

If $\theta \in S_n$ let θ act on the polynomial $p(x_1, \ldots x_n)$ by

$$\theta\, p(x_1, \ldots, x_n) = \prod_{i<j} (x_{i^\circ} - x_{j^\circ}) \to \prod_{i<j} (x_{\theta(i)} - x_{\theta(j)})$$

It is clear that

$$\theta = P(x_1, \ldots, x_n) \to \pm P(x_1, \ldots, x_n)$$

For instance in S_5, $\theta = (134)(25)$ takes

$$P(x_1, \ldots x_5) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)$$
$$(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)$$
$$(x_3 - x_5)(x_4 - x_5)$$

into

$$(x_3 - x_5)(x_3 - x_4)(x_3 - x_1)(x_3 - x_2)(x_5 - x_4)(x_5 - x_1)(x_5 - x_2)$$
$$(x_4 - x_1)(x_4 - x_2)(x_1 - x_2)$$

we can easily be verified to be $P(x_1, x_2 \ldots x_5)$

$$\theta = P(x_1, \ldots x_n) \to P(x_1, \ldots, x_n)$$

Thus, if a permutation Π can be represented as a product of an even number of transpositions in one representation.

$P(x_1, \ldots, x_n)$ fixed.

... So that any representation of Π as a product of transposition must be leaves $p(x_1, \ldots x_n)$ fixed.

In any representation it is a product of an even number of representations.

We call a permutation odd if it is not an even permutation.

1. The product of two even permutations is an even permutation.

2. The product of an even permutation and an odd one is odd (the product of an odd and even permutation).

3. The product of two odd permutations is an even permutation.

combining even and odd numbers under addition

Let A_n be the subset of S_n.

The product of two even permutations is even

A_n must be a subgroup of S_n.

Let w be group of real numbers 1 and -1 under multiplication.

Define,

$\varphi : S_n \to W$ by $\varphi(s) = 1$

If s is an even permutation $\varphi(s) = 1$

If s is an odd permutation.

By the rules 1, 2, 3 above φ is a homomorphism onto W.

The kernel of φ is precisely A_n

being the kernel of a homomorphism A_n is a normal subgroup of S_n. Theorem 2.7.1 $S_n / A_n \cong W$.

$$2 = o(W) = o\left(\frac{S_n}{A_n}\right)$$

$$= \frac{o(S_n)}{o(A_n)}$$

$$o(A_n) = \frac{1}{2} n!$$

A_n is called the alternating group of degree n.

Lemma 2.10.3:

S_n has as a normal subgroup of index 2 the alternating group. A_n, consisting of all even permutations.