which takes every member of G to itself and this permutation is denoted by I

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

It is easy to verify that $\alpha o I = I o \alpha$.

<u>Inverse permutation</u> → Since a permutation is one-one onto and as such it is invertiable the inverse of any permutations α is denoted by α^{-1} and is obtained by interchanging the rows of α

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} \text{ then } \alpha^{-1} = \begin{pmatrix} 2 & 4 & 5 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

clearly $\alpha o \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = I = \alpha^{-1} o \alpha$

Thus the inverse of every permutation exists and belongs to the set of all permutations in a group.

<u>Permutation multiplication</u> is <u>not commutative</u> in general.

We have shown that

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

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

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

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

Hence $\alpha o \beta \neq \beta o \alpha$. It is such that $\alpha o \beta$ permutations replaces 1 by 1 whereas $\beta o \alpha$ permutation replace 1 by 5.

Prove that
The $\lfloor n$ permutations from a group under permutation multiplication in a group
or [P.T. symmetric set of degree n is a group]

Proof → The set of all permutations of the set having n elements is called symmetric set on $\lfloor n$ symboles and of degree n and is denoted by S_n.

Let $S = \{a_1, a_2, \dots, a_n\}$ so that
$S_n = \{P : P$ is a permutation of degree $n\}$

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

$$\beta = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} \text{ and } \gamma = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

be any three permutations of degree n belonging to the set S_n where b_i, c_i and d_i are same as a_i but in different order.

(i) Closure property → That is product of two permutations is again a permutation belonging to set S_n

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

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

Which is again a permutation of degree n belonging to the set S_n. Thus closure property hold in S_n

(ii) Associative property → $$(\alpha \circ \beta) \circ \gamma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} \circ \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

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

$$\alpha o(\beta o \gamma) = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} o \begin{pmatrix} b_1 & b_2 & --- & b_n \\ d_1 & d_2 & --- & d_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ d_1 & d_2 & --- & d_n \end{pmatrix}$$

Thus $(\alpha o \beta) o \gamma = \alpha o (\beta o \gamma)$. Hence permutation multiplication is associative.

(iii) Identity → Consider the permutation I

$$I = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ a_1 & a_2 & --- & a_n \end{pmatrix} \text{ and } I = \begin{pmatrix} b_1 & b_2 & --- & b_n \\ b_1 & b_2 & --- & b_n \end{pmatrix}$$

Let $\alpha = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix}$ be any other permutations obtained by in belonging to S_n.

$$\alpha o I = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} o \begin{pmatrix} b_1 & b_2 & --- & b_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} = \alpha$$

$$\text{and } I o \alpha = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ a_1 & a_2 & --- & a_n \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} = \alpha$$

Since, $\alpha o I = I o \alpha = \alpha$ and such that permutations I is the identity permutation which belongs to S_n.

(iv) Existence of Inverse → Let us denote by α^{-1} the permutations obtained by interchanging the row in permutation α.

i.e $\alpha^{-1} = \begin{pmatrix} b_1 & b_2 & --- & b_n \\ a_1 & a_2 & --- & a_n \end{pmatrix}$ clearly.

α^{-1} is also a permutation of degree n. since b_i's are nothing but a_i's but in a different order.

$$\text{Now, } \alpha o \alpha^{-1} = \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix} o \begin{pmatrix} b_1 & b_2 & --- & b_n \\ a_1 & a_2 & --- & a_n \end{pmatrix}$$

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

$$\text{and } \alpha^{-1} o \alpha = \begin{pmatrix} b_1 & b_2 & --- & b_n \\ a_1 & a_2 & --- & a_n \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & --- & a_n \\ b_1 & b_2 & --- & b_n \end{pmatrix}$$

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

$\therefore \alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = I$

~~Since $\alpha\circ\alpha^{-1} = \alpha^{-1}\circ\alpha = I$~~ as such α^{-1} is ~~the inverse of permutation and that α^{-1} is again a permutation belonging to S_n thus~~

Inverse of each permutation exists and belong to the set S_n

Thus S_n is a group.

S_n is not a abelian group since product of permutations does not obey commutative law.

Cyclic permutation → A permutation which replace n objects cyclically is called a cyclic (or circular) permutation of degree n.

Ex: Hence the permutation

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

such that $1 \to 2$, $2 \to 3$, $3 \to 4$, $4 \to 5$ and $5 \to 1$

i.e the last no. goes to first.

~~In other words a permutation in which element in the first line is replaced by the no. succeeding it and the last being replaced by first is called a cyclic permutation.~~

Note → Having understand what we mean by a cyclic permutation. We can adopt a one line notation only for a cyclic permutation where $\alpha = (1,2,3,4,5)$ would mean a cyclic permutation meaning there by that each no in the first line is replaced by its sucessive on the right and the last one by first i.e

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

Expression of any permutation in terms of cyclic :-

Consider the permutation.

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

By interchanging the column.

The above permutation β can be written as- which is interpreted as $1 \to 3, 3 \to 2$ and $2 \to 1$ where as $\beta = \{1, 3, 2\}$ the missing symboles 4 and 5 remain unchange in the permutation. i.e $4 \to 4$ and $5 \to 5$

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

Thus the cyclic β is cyclic and is representing by cycle (1, 3, 2) whose length is 3 the no. of elements in 3

Again consider the permutation

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

As the product of mutually disjoint cycles i.e. cycles having no. elements common cycle.

$$f = (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 4 & 5 \end{pmatrix} \text{ as permutation.}$$

If $f = (1\ 2\ 3)$ and $g = (4\ 5)$

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

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

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

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

Hence the cyclic permutation is commutative.

Cayley's Theorem

STATEMENT → Every finite group 'G' is isomorphic to a permutation group & If G is not finite then every group is isomorphic ~~a group of one one onto function isomorphic~~ to a subgroup of symmetric group $A(G)$.

Proof →

Let G be a finite group and $a \in G$ be a arbitrary. We define a mapping :-

$$f_a : G \longrightarrow G \text{ by}$$

$$f_a(x) = ax \; \forall x \in G$$

$\{f_a(x) = f_a(y)$, $ax = ay$, $x = y$

~~What will effect~~

First we shall prove f_a is a permutation i.e. f_a is one one and onto. Taking $f_a(x_1) = f_a(x_2)$; $x_1, x_2 \in G$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$ (by left cancellation law)

$\Rightarrow f_a$ is one one

∴ Again $f_a : G \to G$ is one one and G is finite

$\Rightarrow f_a$ is onto

∴ f_a is one one and onto and so 'f_a' is permutation

Let $G' = \{f_a : a \in G\}$

set of permutations

Now we shall prove that G' is a group under permutation multiplication

Let $a, b, c \in G$ be arbitrary and e be identity element of G

Let a^{-1} be inverse of a

(i) Closure property

Let $f_a, f_b \in G'$

$(f_a f_b)(x) = f_a f_b(x)$

$= f_a(bx) = abx$

$\Rightarrow (ab)x = \cancel{}\ f_{ab}(x)$

$\therefore f_a f_b = f_{ab} \in G'$ $\{\because a, b \in G \Rightarrow ab \in G\}$

$\therefore$ closure property hold in G'

(ii) Associative law

$f_a(f_b f_c) = f_a(f_{bc})$

$= f_{a(bc)} = f_{(ab)c}$ $\{\because a(bc) = (ab)c\}$

$= \cancel{(f_a f_b)} f_c\ f_{ab} f_c = (f_a f_b) f_c$

(iii) Existence of identity

clearly $f_e \in G'$ and is identity element since

$f_a f_e = f_{ae} = f_a$

(iv) Existance of inverse

Let $a \in G$

$\Rightarrow a, a^{-1} G$

$\Rightarrow f_a, f_{a^{-1}} \in G'$

$f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$ $\{\because aa^{-1} = a^{-1}a = e\}$

and $f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$

$\Rightarrow f_{a^{-1}}$ is inverse of f_a

$\therefore$ Each element of G' is investiable. From (i) to (iv)

it follows that G' it is a group

Now we shall prove that

$G \cong G'$, we define a mapping $g: G \to G'$

Such that $g(x) = \cancel{}\ f_x \quad \forall x \in G$.

'g' is one one since

$g(x_1) = g(x_2)$; $x_1, x_2 \in G$

$\Rightarrow \cancel{}\ f_{x_1} = f_{x_2}$

$\Rightarrow \cancel{f(x_1) = f(x_2)}$ $f_{x_1}(x) = f_{x_2}(x)$

$\Rightarrow x_1 x = x_2 x$

$\Rightarrow x_1 = x_2$ by right hand cancellation law.

2003

Show that element $a \in Z$, the centre

G is finite $a \in G \Rightarrow O[N(a)] = O(G)$

Ans Proof $\rightarrow$ Let $a \in Z$

Then by the defination of Z

$$ax = xa \ \forall \ x \in G$$

Now $N(a) = \{x \in G ; ax = xa\}$

Now $a \in Z \Rightarrow ax = xa \ \forall \ x \in G$ [by

$\Rightarrow x \in N(a) \ \forall x \in G$ by defn of

$\Rightarrow N(a) = G$ [$\because N(a) \subseteq G$ and eac

If the group G is finite then

$N(a) = G$

$\Rightarrow O[N(a)] = O[G]$

~~If the group G is finite~~

~~N(a) = G~~

~~$\Rightarrow O[N(a)] = O(G)$ Proved~~

Hence if the group G is fi

iff $O[N(a)] = O(G)$

—x—