

5

Define Group and abelian group (commutative)

If binary operation $*$ defined on a non-empty G set satisfies the following postulates (properties) then G is said to be group.

① closure: $a, b \in G \Rightarrow a * b \in G$

② Associative: $\forall a, b, c \in G$
 $\Rightarrow (a * b) * c = a * (b * c)$

③ Existence of Identity:-
 $\forall a \in G \exists e \in G$ such that

$$a * e = a = e * a$$

here e is a identity element

④ Existence of Inverse:-
For $a \in G, \exists b \in G$ such that
 $a * b = e = b * a$
 $a * a^{-1} = e$

here, b is inverse element of a in G

\rightarrow Then G is said to be a group under binary operation $*$

Notation: $(G, *)$

\rightarrow A Group $(G, *)$ is said to be abelian or (commutative) group if $a * b = b * a; \forall a, b \in G$

* Some examples of group and abelian group

① $(\mathbb{Z}, +)$ is a group
i.e. \mathbb{Z} is a group under binary operation addition $+$,

moreover $(\mathbb{Z}, +)$ is abelian group.

② $(\mathbb{Z}, \cdot) \rightarrow$ this is not a group.
because for $a \in \mathbb{Z} \nexists \frac{1}{a} \in \mathbb{Z}$

i.e. Inverse element does not exist.

③ $(\mathbb{Q}, +)$ is a group as well as abelian.

④ (\mathbb{Q}, \cdot) is not a group and abelian
because Inverse of 0 does not exist

⑤ (\mathbb{Q}, \cdot) is a group
because 0 is not include.

⑥ (\mathbb{R}^0, \cdot) is group but
 (\mathbb{R}, \cdot) is not group.

multiplication-multiplication

(Ex) ^{*} set $C = \{a+ib / i^2 = -1, a, b \in \mathbb{R}\}$ of all complex numbers form a group under addition as well as multiplication (multiplication)

Ans:

$$z_1 = a_1 + ib_1 \in C$$

$$z_2 = a_2 + ib_2 \in C$$

$$z_3 = a_3 + ib_3 \in C$$

→ binary operation "multiplication"

$$\begin{aligned} \textcircled{1} z_1 \cdot z_2 &= (a_1 + ib_1) \cdot (a_2 + ib_2) \\ &= a_1 a_2 + ia_1 b_2 + ib_1 a_2 + i^2 b_1 b_2 \\ &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2) \in C \end{aligned}$$

∴ closure holds

$$\textcircled{2} (z_1 \cdot z_2) \cdot z_3 = [(a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2)] \cdot (a_3 + ib_3)$$

$$= [a_1 a_2 - b_1 b_2 + i(a_1 b_2 + b_1 a_2)] (a_3 + ib_3) \quad \textcircled{1}$$

$$= a_3 (a_1 + ib_1)$$

$$(a_1 + ib_1) + [(a_1 + ib_1) \cdot (a_2 + ib_2)] \cdot (a_3 + ib_3)$$

$$[(a_1 + ib_1) + (a_2 + ib_2)] \cdot (a_3 + ib_3)$$

∴ Associativity holds

$$(a_1 + ib_1) \cdot (1 + i0)$$

$$a_1 + ib_1 + i0 + i^2 0$$

③ For $z_1 = a_1 + ib_1 \in \mathbb{C} \exists (1, 0) \in \mathbb{C}$
such that $z_1 = (a_1, b_1) \cdot (1, 0)$
 $= (a_1, b_1)$
 $= z_1$

Here, $(1, 0)$ is identity element in \mathbb{C}

④ For $z = (a, b) \in \mathbb{C} \exists \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) \in \mathbb{C}$
such that $(a, b) \cdot \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = (1, 0)$

→ Here, $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is an inverse element

of $z(a, b)$

→ binary operation "Addition"

① $z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2)$
 $= (a_1 + a_2) + i(b_1 + b_2) \in \mathbb{C}$

② $(z_1 + z_2) + z_3 = [(a_1 + ib_1) + (a_2 + ib_2)] + (a_3 + ib_3)$
 $= (a_1 + ib_1) + [(a_2 + ib_2) + (a_3 + ib_3)]$
 $= z_1 + (z_2 + z_3)$

$$(a_1 + ib_1) + (0 + i0)$$

$$a_1 + ia_1 + ib_1 + i^2 b_1$$

③ For $z_1 = a_1 + ib_1 \in \mathbb{C} \exists (0, 0) \in \mathbb{C}$

$$\Rightarrow z_1 = (a_1 + ib_1) + (0, 0)$$

$$= (a_1 + 0) + i(b_1 + 0)$$

$$= (a_1 + ib_1)$$

$$= z_1$$

Here, $(0, 0)$ is identity element

④ For $z = (a, b) \in \mathbb{C} \exists \left(\frac{-a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \in \mathbb{C}$

$$\exists (a, b) + \left(\frac{-a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = (0, 0)$$

Here, $\left(\frac{-a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$ is an inverse element

of $z = (a, b)$

addition

$$z_1 = (a_1 + ib_1) \Rightarrow \underline{a_1 - ib_1}$$

$$(a_1 - b)$$

$$\boxed{a \times \bar{a} = e}$$

$$(a_1 + ib_1) + (-a_2 + ib_2) = 0$$

Inverse element

$$(a_1 - a_2) + i(+b_1 - b_2) = 0$$

$$0 + i0 = 0$$

$$0$$

3.2) (2×2) matrix Group is not Abelian group.

Date _____

Page _____

(Ex-2) Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0, a, b, c, d \in \mathbb{R} \right\}$

Then P.T G is a group under binary operation of product in matrices.

Solⁿ:- \rightarrow

Let $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$

$C = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \in G$

① $AB = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in G$

$= \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$

\therefore closure holds

② $(AB) \cdot C = A(B \cdot C)$

$= \left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right] \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$

$= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \left[\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \cdot \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \right]$

$= A(B \cdot C)$

③ For $A \in G$, $\exists I \in G$ such that $A.I = A = I.A$

here, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity matrix.

④ For $A \in G$, $\exists A^{-1} \in G$ such that

$$A^{-1}A = A.A^{-1} = I$$

Here, $A^{-1} = \frac{\text{adj } A}{|A|}$ where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\frac{\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}{(ad - bc)}$$

is inverse matrix
 (G, \cdot) is Group.

(S.Q) but, (G, \cdot) is not abelian group.

Order of the element of a :-

Suppose G is a given group and $a \in G$. If there exist a smallest positive integer m such that

$a^m = e$, then m is called the order of element a denoted by $O(a)$.
 $O(a) = m$

eg $G = \mathbb{Z} \Rightarrow a = -1 \Rightarrow O(-1) = 2$
order

If there does not exist m such that $(\exists) a^m = e$ then $O(a) = \infty$ or $O(a) = \infty$

I.M.P
(S.Q)

Note:- If $a^n = e \Rightarrow O(a) \leq n$ or $O(a) \mid n$

(Ex) If $G = \{1, -1, i, -i\}$ is group then find out order of each element in G

solⁿ

$(1)^1 = 1 \Rightarrow O(1) = 1$

$(-1)^2 = 1 \Rightarrow O(-1) = 2$

$(i)^4 = 1 \Rightarrow O(i) = 4$

$(-i)^4 = 1 \Rightarrow O(-i) = 4$

Thm In a group G , $\forall a \in G$, $a^{-1} = a$ (or $a^2 = e$) then G is abelian.

Proof \rightarrow Let $a \in G$ and $a^{-1} = a$.
 for $a, b \in G \Rightarrow a \cdot b \in G$
 $\Rightarrow (a \cdot b)^{-1} = ab$ (\because Inverse exist)
 $\Rightarrow b^{-1} \cdot a^{-1} = ab$
 $\Rightarrow ba = ab$ ($\because a^{-1} = a, b^{-1} = b$)

G is abelian. (commutative)

(EX) If G there are 5 elements then prove that G is abelian.

\rightarrow Let $G = \{e, a, b, c, d\}$

\cdot	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	e	d	a	c
c	c	d	a	b	e
d	d	b	c	e	a

from table we can say that G is abelian.

(EX) In G , There are 4 elements
then prove that G is abelian

→ Let $G = \{e, a, b, c\}$

•	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	a	c
c	c	b	a	e

→ from table we say that G is abelian

Def Sub group:-

A non-empty subset H of a group G is called sub group of G . If H itself a group under the same binary operation as that of G .

Note-① For any group G ,
 $H_1 = \{e\}$ and $H_2 = \{G\}$ are always sub group of G . both these sub group are called improper sub groups of a group G .

A group different from these two sub group is called proper sub group

(Ex) If $G = (\mathbb{C}; \cdot)$ and $H = \{a+ib \in G \mid a^2+b^2=1\}$

then P.T. H is subgroup of G .

Proof:- $z_1 = a_1 + ib_1$; $a_1^2 + b_1^2 = 1$

$z_2 = a_2 + ib_2$; $a_2^2 + b_2^2 = 1$

$z_1, z_2 \in H$.

$$\begin{aligned} (1) \quad z_1 \cdot z_2 &= (a_1 + ib_1)(a_2 + ib_2) \\ &= a_1 a_2 + ia_1 b_2 + ib_1 a_2 + i^2 b_1 b_2 \\ &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1) \end{aligned}$$

such that

$$\begin{aligned} &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2 \\ &= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + b_1^2 a_2^2 \\ &= a_1^2 (a_2^2 + b_2^2) + b_1^2 (b_2^2 + a_2^2) \\ &= a_1^2 + b_1^2 \quad (\because a_2^2 + b_2^2 = 1, a_1^2 + b_1^2 = 1) \\ &= 1 \end{aligned}$$

H is a subgroup

(2) For $z_1 = a_1 + ib_1 = (a_1, b_1) \in H$.

$$\exists \quad z_1^{-1} = (a_1 - ib_1) \left(\frac{a_1}{a_1^2 + b_1^2}, \frac{-b_1}{a_1^2 + b_1^2} \right) \in H.$$

such that $z_1, z_1^{-1} = e = (1, 0)$

H is a subgroup.

Thm A finite subset H of G is a subgroup of G if it is closed under multiplication.

Proof: ① Let $a \in H \Rightarrow a \cdot a \in H$
 $\Rightarrow a^2 \in H$
 $\Rightarrow a^2 \cdot a \in H$
 $\Rightarrow a^3 \in H$
 $\Rightarrow \dots \dots a^n \in H.$

but

H is finite,

\therefore All those elements cannot be distinct

② $\therefore \exists r, s$ such that $a^r = a^s$ ($r > s > 0$)

Taking $a^r \bar{a}^s = a^s \bar{a}^s$

$$\therefore a^{r-s} = e \in H$$

$$\therefore a^{r-s} \in H.$$

③ and $a, b, c \in H \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c.$

④ $a^{r-s-1} \in H \Rightarrow a^{r-s} \cdot a^{-1} \in H.$
 $\Rightarrow e \cdot a^{-1} \in H.$
 $\Rightarrow a^{-1} \in H.$

$\Rightarrow H$ is subgroup of $G.$

(Ex-4) For a commutative group G
 $H = \{ a \in G / o(a) \text{ is finite} \}$ is a
 subgroup of G .

Solⁿ: - since, $e \in G$, $e \in H$.
 then $H \neq \emptyset$

\rightarrow Let $a, b \in H \Rightarrow o(a) = m; o(b) = n$.

($\because o(a) + o(b)$ is finite)

$\Rightarrow o(a) = m, o(b) = n$.

Now, $(ab^{-1})^{mn} = a^{mn} \cdot (b^{-1})^{mn}$

$o(a) = m$
 $\rightarrow a^m = e$

$= (a^m)^n \cdot ((b^{-1})^n)^m$

$= e^m \cdot e^n$

$= e$

$\Rightarrow o(ab^{-1}) \leq mn$

$\Rightarrow o(ab^{-1})$ is finite

$\Rightarrow ab^{-1} \in H$

$\therefore H$ is a subgroup of G .

$\{e\}, H_1 \rightarrow$ proper subgroup
Identity is subgroup

$$G \neq H_1 \cup H_2$$

(Ex-5) A group cannot be a union of its two proper subgroups.

solⁿ: Suppose H_1, H_2 are two proper subgroups of G , and $G = H_1 \cup H_2$,

where $H_1 \neq \{e\}$ and $H_1 \neq G$,

$H_2 \neq \{e\}$ and $H_2 \neq G$.

As H_1 is proper subgroup of G ,

\exists an element $a \neq e \in G$

$\exists a \notin H_1$ (1) $\therefore a \in H_2$,

with $a \in H_2$ and $a \notin H_1$.

simi, $\exists b \notin H_2$ (2); $b \in H_1$,

Now $a, b \in G \Rightarrow a, b \in G$
 $\Rightarrow ab \in H_1 \cup H_2$ ($\because G = H_1 \cup H_2$)

if $ab \in H_1 \Rightarrow$ then $(ab)^{-1} \in H_1$

$$\Rightarrow a^{-1}(b^{-1}a) \in H_1$$

$$\Rightarrow a^{-1}e \in H_1$$

which is with $e \in H_1$ (1)

if $ab \in H_2 \Rightarrow a^{-1}(ab) \in H_2$

$$\Rightarrow b \in H_2$$

which ... with e a^m

Hence $G = \cup H_i$

(Ex) If $G = \{a^0, a^1, a^2, \dots, a^9 / a^{10} = e\}$

and $H = \{a^0, a^5 / a^{10} = e\}$ then find all right coset of G

Solⁿ: $H = \{a^0, a^5\} = Ha^0 = He$

$$Ha^1 = \{a, a^6\}$$

$$Ha^2 = \{a^2, a^7\}$$

$$Ha^3 = \{a^3, a^8\}$$

$$Ha^4 = \{a^4, a^9\}$$

$$Ha^5 = \{a^5, a^{10}\} = H$$

Ha^6, Ha^7, Ha^8, Ha^9 are not possible ($a^{10} = e$)

Thus $H, Ha^1, Ha^2, Ha^3, Ha^4$ are distinct right cosets.

ch:-8 - Permutation

* Notation:-

(1) $A(S)$ = The set of all one-one correspondence on non-empty sets

$A(S)$ is group under composition of mappings (परिचयन, संयोजन)

अन्यत्र सेवी set
one-one, onto function
होय

(2) S_n :- Symmetric Group of degree n are permutation group of order n

the elements of S_n are called Permutations.

If S contained n elements then group $A(S)$ is denoted by " S_n "

* Definition:-

Let S be a non-empty set.

A one-one and on-to function from S to S is called permutation on S

e.g $f: S \rightarrow S, f(S) = S$

Permutation \rightarrow domain and Codomain is equal

(Ex) Prove that set of all permutation on S is a group under composition.

Solⁿ:- P.T $(A(S), \circ)$ is a group.

$f, g, h \in A(S)$

[1] closure: $f \circ g : S \rightarrow S$
 $f \circ g(S) = f(g(S))$
 $= f(S)$

$f \circ g(S) = S$

$\therefore f \circ g \in A(S)$

[2] Associative:

$(f \circ g) \circ h(S) = (f \circ g)h(S)$

$= f(g(h(S)))$

$= f(g \circ h(S))$

$= f \circ (g \circ h)(S)$

$(f \circ g) \circ h = f \circ (g \circ h)$

[3] identity:-

$f \circ g \in A(S); \exists I \in A(S) \exists$

$f \circ I(S) = f(I(S)) = f(S) = S$

$$f \circ I \circ f^{-1} = s \quad \{1, 2, 3\} \quad (2, 3)$$

$$f \circ I = I \circ f \quad \begin{matrix} 2 & 3 & 1 \end{matrix}$$

[4] Inverse:-
since, $f \in A(S)$

f is one-one & onto.

f^{-1} exists

$$f \circ f^{-1}(s) = I(s) = s.$$

$(A(S), \circ)$ is Group.

Note:- ① Element of S_n is denoted by

$$s_n = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Here, σ is permutation

$$= \{1, 2, 3, \dots, n\}$$

② S_n is a group of order $n!$

$$\text{i.e. } |O(S_n)| = n!$$

(EX) If $S = \{1, 2, 3, 4, 5\}$

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

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

and

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

then find $g \circ t$; $t \circ g$; t^{-1} ; g^{-1} .

solⁿ:

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

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

$$t^{-1} = \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}^*$$

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

$$g^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}^*$$

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

(EX) $I \& S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

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

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

Then verify $(f \circ g)^{-1} = (g^{-1} \circ f^{-1})$

and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Solⁿ:

$$(f \circ g)^{-1} = \begin{pmatrix} 7 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 9 & 6 & 2 & 5 & 3 \end{pmatrix}$$

$$(f \circ g)^{-1} = \begin{pmatrix} 7 & 4 & 1 & 8 & 9 & 6 & 2 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \times$$

$$(f \circ g)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 9 & 2 & 8 & 6 & 1 & 4 & 5 \end{pmatrix} \text{--- (1)}$$

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

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

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

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

$$g^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 9 & 2 & 8 & 6 & 1 & 4 & 5 \end{pmatrix} \quad \text{--- (2)}$$

⇒ by eqn (1) & (2) $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

$$\rightarrow (g \circ f) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 9 & 6 & 1 & 3 & 5 & 7 & 8 \end{pmatrix}$$

$$(g \circ f)^{-1} = \begin{pmatrix} 4 & 2 & 9 & 6 & 1 & 3 & 5 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$(g \circ f)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 6 & 1 & 7 & 4 & 8 & 9 & 3 \end{pmatrix} \quad \text{--- (3)}$$

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 6 & 1 & 7 & 4 & 8 & 9 & 3 \end{pmatrix} \quad \text{--- (4)}$$

⇒ by eqn (3) & (4)

$$\underline{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$$

Transposition: 2 cycle!

A function $f: S \rightarrow S$ defined by $f(p) = q$, $f(q) = p$ and $f(i) = i$ for $i \neq p, q$, then permutation is called transposition.

Notation: (p, q)

Also, $f^{-1}: S \rightarrow S$ is also transposition

e.g. $S = \{1, 2, 3, 4, 5\}$

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

$\sigma = (2, 5)$ is transposition.

A permutation $g: S \rightarrow S$ is said to be a cycle of length k if \exists elements $p_1, p_2, p_3, \dots, p_k \in S$ such that

$g(p_1) = p_2, g(p_2) = p_3, \dots, g(p_{k-1}) = p_k$
and $g(p_k) = p_1$.

(where $m \neq p_i$ ($i = 1, 2, 3, \dots, k$))

which is denoted by

$g = (p_1, p_2, \dots, p_k)$

e.g

① $\sigma_1 : S \rightarrow S ; S = \{1, 2, 3\}$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$\sigma_1 = (1 \ 2 \ 3)$ is cycle

② $\sigma_2 : S \rightarrow S ; S = \{1, 2, 3, 4, 5, 6\}$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

$\sigma_2 = (1 \ 2 \ 3 \ 4 \ 5 \ 6)$ is cycle

③ $\sigma_3 : S \rightarrow S ; S = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 6 & 7 & 8 & 1 & 4 \end{pmatrix}$$

$= (1 \ 3 \ 5 \ 7) (4 \ 6 \ 8)$ is cycle.

(EX) If $f = (1 \ 4 \ 5 \ 6) \in S_6$ & $g = (2 \ 1 \ 5) \in S_6$
 $g = (2 \ 1 \ 5) \in S_6$
 then find $g \circ f$ & $f \circ g$

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

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

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

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

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

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

hence composition of two ~~need~~ ^{will} not
 to be again cycle