

Binary Operation:

Let S be a non-empty set. The binary operation $*$ is a function

$$* : S \times S \longrightarrow S$$

which assigns each ordered pair (a, b) of $S \times S$, a unique element of S .

Suppose $a, b \in S$,

$$a * b \in S$$

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

$$2, 5 \in S, \quad 2 + 5 = 7 \in S$$

$$x, y \in S, \quad x + y \in S$$

Example: Show that multiplication is a binary operation on the set of Natural numbers \mathbb{N} .

Sol: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

$$7, 5 \in \mathbb{N}$$

$$7 \times 5 = 35 \in \mathbb{N}$$

$$x, y \in \mathbb{N}, \quad xy \in \mathbb{N}$$

So multiplication is a binary operation on \mathbb{N} .

Example : Show that division is not a binary operation on the set of Natural Numbers \mathbb{N} .

Sol. $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

$$4, 2 \in \mathbb{N}, \quad 4 \div 2 = 2 \in \mathbb{N}$$

$$2 \div 4 = 0.5 \notin \mathbb{N}$$

for all $x, y \in \mathbb{N}$, $x \div y \notin \mathbb{N}$

So \div is not a binary operation on \mathbb{N} .

Example : Show that subtraction is not a binary operation on \mathbb{N} .

Sol: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

$$2, 3 \in \mathbb{N}, \quad 3 - 2 = 1 \in \mathbb{N}$$

$$2 - 3 = -1 \notin \mathbb{N}$$

for all $x, y \in \mathbb{N}$, $x - y \notin \mathbb{N}$

So '-' is not a binary operation on \mathbb{N} .

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Example : Show that division is a binary operation on \mathbb{R} .

Sol :

$$\frac{2}{3}, \frac{5}{7} \in \mathbb{R}$$

$$\frac{2}{3} \div \frac{5}{7} = \frac{2}{3} \times \frac{7}{5} = \frac{14}{15} \in \mathbb{R}$$

$$\sqrt{2} \div \sqrt{3} = \frac{\sqrt{2}}{\sqrt{3}} \in \mathbb{R}$$

for all $x, y \in \mathbb{R}$, $x \div y \in \mathbb{R}$

Hence ' \div ' is a binary operation on \mathbb{R} .

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}'$$

$$\frac{p}{q}$$

$$\sqrt{2}, \sqrt{3}$$

$$\frac{1}{2}, \frac{5}{7}$$

Example : Show that the operation \circ defined by

$$x \circ y = 0 \quad \text{for all } x, y \in \mathbb{Z}$$

is a binary operation on \mathbb{Z} .

Sol: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$

$$x, y \in \mathbb{Z}, \quad x \circ y = 0 \in \mathbb{Z}$$

$$x, y \in \mathbb{Z}, \quad x \circ y = 0 \in \mathbb{Z}$$

Hence the operation ' \circ ' is a binary operation on \mathbb{Z} .

Example : Show that the operation \circ defined by

$$x \circ y = x + y - xy \quad \text{for all } x, y \in \mathbb{Z}$$

is a binary operation on \mathbb{Z} .

Sol: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$

$$3, 5 \in \mathbb{Z}$$

$$\begin{aligned} 3 \circ 5 &= 3 + 5 - 3 \times 5 \\ &= 8 - 15 \\ &= -7 \in \mathbb{Z} \end{aligned}$$

for $x, y \in \mathbb{Z}$

$$x + y \in \mathbb{Z}, \quad xy \in \mathbb{Z}$$

$$x + y - xy \in \mathbb{Z} \quad \Rightarrow \quad x \circ y \in \mathbb{Z}$$

GROUPOID:

VuBioTechnologist

A non-empty set with a binary operation is called Groupoid.

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

$$(N, +)$$

$$3, 5 \in N,$$

$$3 + 5 = 8 \in N$$

$$x, y \in N, \quad x + y \in N$$

Example:

Show that $(\mathbb{Z}, -)$ is a groupoid under the operation of usual subtraction.

Sol: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$

$$3, 5 \in \mathbb{Z},$$

$$3 - 5 = -2 \in \mathbb{Z}$$

$$\text{for } x, y \in \mathbb{Z}, \quad x - y \in \mathbb{Z}$$

 **Example:**

VuBioTechnologist

Show that (\mathbb{Z}, \div) is not a groupoid under the operation of usual division.

Sol: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$

$$1, 2 \in \mathbb{Z},$$

$$1 \div 2 = 0.5 \notin \mathbb{Z}$$

$$4, 2 \in \mathbb{Z},$$

$$4 \div 2 = 2 \in \mathbb{Z}$$

for all $x, y \in \mathbb{Z}$

$$x \div y \in \mathbb{Z}$$

Example: Show that $N = \{1, 2, 3, \dots\}$ is a semigroup under the operation of addition.

Sol: $(N, +)$ $N = \{1, 2, 3, \dots\}$

1)

$$11, 13 \in N, \quad 11 + 13 = 24 \in N$$

Similarly, for all $x, y \in N$, $x + y \in N$

So N is closed under $+$

2) $7, 8, 9 \in N$

$$(7+8)+9 = 15+9 = 24$$

$$7+(8+9) = 7+17 = 24$$

$$(7+8)+9 = 7+(8+9)$$

for any $x, y, z \in N$,

$$(x+y)+z = x+(y+z)$$



Example: Show that the set (\mathbb{Z}, \circ) is a semi group, where \circ is the binary operation defined by

$$x \circ y = x + y - xy$$

Sol: $\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$

$$2, 3 \in \mathbb{Z}$$

$$\begin{aligned} 2 \circ 3 &= 2 + 3 - 2 \times 3 \\ &= 5 - 6 = -1 \in \mathbb{Z} \end{aligned}$$

- 1) $\left\{ \begin{array}{l} \text{binary operation} \\ \text{closure property} \end{array} \right.$
- 2) Associative law.

for $x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$, $xy \in \mathbb{Z}$

$$\begin{aligned} x + y - xy &\in \mathbb{Z} \\ x \circ y &\in \mathbb{Z} \end{aligned}$$

So the closure property holds.

2) Associative law.

$$(x \circ y) \circ z = x \circ (y \circ z)$$

$$\text{LHS} = (x \circ y) \circ z$$

$$= \underline{\underline{[x + y - xy]}} \circ z = (x + y - xy) + z - (x + y - xy)z$$

$$= x + y - xy + z - xz - yz + xyz$$

$$= x + y + z - xy - yz - xz + xyz \quad \text{--- I}$$

$$\text{RHS} = x \circ (y \circ z)$$

$$= x \circ \underline{\underline{[y + z - yz]}}$$

$$= x + (y + z - yz) - x(y + z - yz)$$

$$= x + y + z - yz - xy - xz + xyz$$

$$= x + y + z - xy - yz - xz + xyz \quad \text{--- II}$$

By I and II,

$$(x \circ y) \circ z = x \circ (y \circ z)$$



MONOID:

VuBioTechnologist

A non-empty set with an ⁽²⁾ associative ⁽¹⁾ binary operation and an identity element is called Monoid.

⁽³⁾ Let S be a non-empty set

1) Let $*$ be the binary operation on S .

for every $x, y \in S$, $x * y \in S$

So closure property holds

2) Associative law holds.

for $x, y, z \in S$,

$$(x * y) * z = x * (y * z)$$

3) Identity element exists in S

for all $x \in S$, $e * x = x * e = x$



Example: Show that the set $W = \{0, 1, 2, 3, \dots\}$ is Monoid under the binary operation of addition.

$$W = \{0, 1, 2, \dots\} \quad (W, +)$$

1) Closure property:

$$13, 15 \in W$$

$$13 + 15 = 28 \in W$$

Hence closure property holds.

2) Associative law:

$$4, 5, 6 \in W$$

$$(4+5)+6 = 4+(5+6)$$

$$9+6=15$$

$$4+11=15$$

for any $x, y, z \in S$, $(x+y)+z = x+(y+z)$

3) Identity element: $e = 0$

$$2+0 = 2 = 0+2$$

for any $x \in W$, $x+0 = x = 0+x$

Since W satisfies all the three conditions, so W is monoid.



MONOID:

A non-empty set with an associative binary operation and an identity element is called Monoid.

⁽³⁾ Let S be a non-empty set

1) Let $*$ be the binary operation on S .

for every $x, y \in S$, $x * y \in S$

So closure property holds

2) Associative law holds.

for $x, y, z \in S$,

$$(x * y) * z = x * (y * z)$$

3) Identity element exists in S
for all $x \in S$, $e * x = x * e = x$

Example: Show that the set $W = \{0, 1, 2, 3, \dots\}$ is Monoid under the binary operation of addition.

$$W = \{0, 1, 2, \dots\} \quad (W, +)$$

1) Closure property: $13, 15 \in W$

$$13 + 15 = 28 \in W$$

Hence closure property holds.

2) Associative law:

$$4, 5, 6 \in W$$

$$(4+5)+6 = 4+(5+6)$$

$$9+6=15 = 4+11=15$$

for any $x, y, z \in S$, $(x+y)+z = x+(y+z)$

3) Identity element: $e = 0$

$$2+0 = 2 = 0+2$$

for any $x \in W$, $x+0 = x = 0+x$

Since W satisfies all the three conditions, so W is monoid.

**GROUP:**

A non-empty set with an associative binary operation, an identity element and the inverses of its all elements is called Group.

$$S \neq \{\} \quad , \quad (S, *)$$

1) Closure property: for $x, y \in S$,

$$x * y \in S$$

So closure property holds.

2) Associative law:

$$\text{for } x, y, z \in S, \quad (x * y) * z = x * (y * z)$$

3) Identity element exists.

$$e \in S, \quad e * x = x * e = x \quad \text{for } x \in S$$

4) Inverses of all elements of S exist in S .

for all $x \in S$, $\exists x^{-1} \in S$ such that

$$x * x^{-1} = e = x^{-1} * x$$

Therefore $(S, *)$ is a group.



Example: Show that the set $\{1, -1\}$ is a group under multiplication.

Sol:

$$G = \{1, -1\}$$

1) Closure Property

$$\text{for } x, y \in G, xy \in G$$

\cdot	1	-1
1	1	-1
-1	-1	1

2) Associative law.

$$(1 \cdot (-1)) \cdot (-1) = 1 \cdot ((-1) \cdot (-1))$$

$$(-1) \cdot (-1) = 1 \cdot (1)$$

$$1 = 1$$

$$(xy)z = x(yz) \quad \text{for all } x, y, z \in G$$

3) Identity Element.

$$e \cdot x = x = x \cdot e \quad \text{for all } x \in G$$

$$e = 1$$

$$1 \cdot x = x \cdot 1 = x \quad \forall x \in G.$$

4) Inverse Element.

for every $x \in G$, $\exists x^{-1} \in G$ s.t.

$$xx^{-1} = x^{-1}x = e$$

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

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

Hence inverse of each element of G exists in G .

So $G = \{1, -1\}$ is a group under multiplication.

Example : Show that $(\mathbb{Z}, +)$ is a group under the binary operation of addition.

Sol: $\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$

1) $10, 15 \in \mathbb{Z}, \quad 10 + 15 = 25 \in \mathbb{Z}$
for every $x, y \in \mathbb{Z}, \quad x + y \in \mathbb{Z}$

So closure property holds.

2) Associative law.

$$3, 4, 7 \in \mathbb{Z}$$

$$(3+4)+7 = 3+(4+7)$$

$$7+7 = 3+11$$

$$14 = 14$$

for $x, y, z \in \mathbb{Z},$

$$(x+y)+z = x+(y+z)$$

3) Identity Element: $e=0$

for any $x \in \mathbb{Z}, \quad 0+x = x+0 = x$

4) Inverse Element of each $x \in \mathbb{Z}.$

$$2 + (-2) = 0$$

$$-10 + (10) = 0$$

for every $x \in \mathbb{Z}, \quad \exists -x \in \mathbb{Z}$

such that

$$x + (-x) = -x + x = 0$$

So $(\mathbb{Z}, +)$ satisfies all conditions of group,
Therefore $(\mathbb{Z}, +)$ is a group.



Example: Show that $(\mathbb{Z} - \{0\}, \cdot)$ is not a group under the binary operation of multiplication.

Sol: $\mathbb{Z} - \{0\} = \{ \dots, -2, -1, 1, 2, \dots \}$

1) Closure property:

$$3, 4 \in \mathbb{Z}, \quad 3 \times 4 = 12 \in \mathbb{Z}$$

for any $x, y \in \mathbb{Z}, \quad xy \in \mathbb{Z}$

2) Associative law:

$$2, 5, 4 \in \mathbb{Z} - \{0\}$$

$$\begin{aligned} (2 \times 5) \times 4 &= 2 \times (5 \times 4) \\ 10 \times 4 &= 2 \times 20 \\ 40 &= 40 \end{aligned}$$

for $x, y, z \in \mathbb{Z} - \{0\}$

$$(xy)z = x(yz)$$

3) Identity Element: $e = 1 \in \mathbb{Z} - \{0\}$

$$1 \cdot x = x \cdot 1 = x \quad \forall x \in \mathbb{Z} - \{0\}$$

4) Inverse Element of each $x \in \mathbb{Z} - \{0\}$

$$2 \times \left(\frac{1}{2}\right) = 1 \quad \text{but}$$

$$x \bar{x} = e \quad \frac{1}{2} \notin \mathbb{Z} - \{0\}$$

for any $x \in \mathbb{Z} - \{0\}$, there is no inverse.

i.e. $\frac{1}{x} \notin \mathbb{Z} - \{0\}$

So $\mathbb{Z} - \{0\}$ is not a group.



Example: Show that $G = \{1, \omega, \omega^2\}$ is a group under multiplication, where ω is cube root of unity.

Sol: $G = \{1, \omega, \omega^2\}$

\cdot	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$$x = \sqrt[3]{1}$$

$$x = (1)^{1/3}$$

$$x^3 = 1$$

$$1, \omega, \omega^2$$

$$\boxed{\omega^3 = 1}$$

$$\omega^2 \omega^2 = \omega^4$$

$$= \omega^3 \omega$$

$$= 1 \cdot \omega$$

$$= \omega$$

1) It is clear from the table that closure property holds.

2) Associative law:

$$1, \omega, \omega^2 \in G$$

$$(1 \cdot \omega) \cdot \omega^2 = 1 \cdot (\omega \cdot \omega^2)$$

$$\omega \cdot \omega^2 = 1 \cdot \omega^3$$

$$\omega^3 = \omega^3$$

$$1 = 1$$

for any $x, y, z \in G$,

$$(xy)z = x(yz)$$

3) Identity element:

$$e = 1$$

$$\omega \cdot 1 = 1 \cdot \omega = \omega$$

$$\omega^2 \cdot 1 = 1 \cdot \omega^2 = \omega^2$$

$$1 \cdot 1 = 1 \cdot 1 = 1$$

4) Inverse Element of each element $x \in G$.

$$1 \cdot (1) = 1 \Rightarrow (1)^{-1} = 1$$

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

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

Hence G satisfies all the conditions of a group. Hence G is a group under multiplication.



Example: Show that $G = \{ 1, -1, i, -i \}$ is a group under multiplication.

Sol:

1) Closure Property

It is clear from the table that the closure property holds.

\cdot	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

2) Associative law

$$(i \cdot (-i))(-1) = i \cdot ((-i) \cdot (-1))$$

$$(1)(-1) = i \cdot (i)$$

$$i = \sqrt{-1}$$

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

for any $x, y, z \in G$, $(xy)z = x(yz)$

3) Identity Element: $e = 1$

for any $x \in G$, $1 \cdot x = x \cdot 1 = x$

4) Inverse element of each $x \in G$.

$$x \cdot x^{-1} = e = x^{-1} \cdot x$$

$$\begin{array}{l|l} (1)(1) = 1 & (i)(-i) = 1 \\ (-1)(-1) = 1 & (-i)(i) = 1 \end{array}$$

$$(1)^{-1} = 1, \quad (-1)^{-1} = (-1)$$

$$(i)^{-1} = -i, \quad (-i)^{-1} = i$$

Theorem : In a group G , the identity element is unique.

Proof: Contrarily suppose that identity element is not unique.

Let e & e' be two identity elements.

for all $x \in G$,

$$xe = x = ex$$

$$e'e = e' = ee' \quad \text{--- (1)}$$

$$ee' = e = e'e \quad \text{--- (2)}$$

Now

By (1) & (2),

$$e = e'$$

Hence e is unique.

Theorem : The only idempotent element in a group G is the identity.

Proof: Let $a \in G$ be an idempotent element.

$$a^2 = a$$

$$aa = a$$

$$a^{-1}(aa) = a^{-1}a$$

$$(a^{-1}a)a = e$$

$$ea = e$$

$$a = e$$

Hence proved.

Definition :

An element a of a group G is called idempotent if $a^2 = a$.

$$a \in G, \quad a^2 = a$$

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

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I^2 = I$$

Theorem : In a group G , the inverse of each element is unique.

Proof: Suppose Contrarily that the inverse of each element of G is not unique.

So let \bar{a}^{-1} & \bar{a}'^{-1} be the inverses of $a \in G$.

$$\bar{a}^{-1}a = e = a\bar{a}^{-1} \text{ --- ①}$$

and $\bar{a}'^{-1}a = e = a\bar{a}'^{-1} \text{ --- ②}$

Consider $a\bar{a}'^{-1} = e$

$$\bar{a}'^{-1}(a\bar{a}'^{-1}) = \bar{a}'^{-1}e$$

$$(\bar{a}'^{-1}a)\bar{a}'^{-1} = \bar{a}'^{-1}$$

$$e\bar{a}'^{-1} = \bar{a}'^{-1} \quad \text{by ②}$$

$$\bar{a}'^{-1} = \bar{a}^{-1}$$

Hence the inverse of each element is unique.

Theorem : If G is a group, then $(a^{-1})^{-1} = a \quad \forall a \in G$

Proof: Since G is a group, and $a \in G$,

$$a^{-1} \in G \quad a^{-1}a = aa^{-1} = e \quad \text{--- (1)}$$

$$(a^{-1})^{-1} \in G \quad (a^{-1})^{-1}a^{-1} = e = a^{-1}(a^{-1})^{-1} \quad \text{--- (2)}$$

from (2)

$$(a^{-1})^{-1}a^{-1} = e$$

$$((a^{-1})^{-1}a^{-1})a = ea$$

$$(a^{-1})^{-1}(a^{-1}a) = a$$

$$(a^{-1})^{-1}e = a$$

$$(a^{-1})^{-1} = a$$

Hence the proof.



Theorem : Let G be a group, then $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a, b \in G$

Proof: Since G is a group

and $a, b \in G \Rightarrow a^{-1} \in G, b^{-1} \in G$

then $ab \in G$

So $(ab)^{-1} \in G$

Therefore,

$$(ab)^{-1}ab = e$$

$$((ab)^{-1}ab)b^{-1} = eb^{-1}$$

$$((ab)^{-1}a)(bb^{-1}) = b^{-1}$$

$$((ab)^{-1}a)e = b^{-1}$$

$$((ab)^{-1}a) = b^{-1}$$

$$((ab)^{-1}a)a^{-1} = b^{-1}a^{-1}$$

$$(ab)^{-1}(aa^{-1}) = b^{-1}a^{-1}$$

$$(ab)^{-1}e = b^{-1}a^{-1}$$

$$(ab)^{-1} = b^{-1}a^{-1}$$

Hence proved.



Theorem : For any three elements a, b, c of a group G ,

$$(i) \quad ab = ac \Rightarrow b = c \quad (\text{Left Cancellation Law})$$

$$(ii) \quad ba = ca \Rightarrow b = c \quad (\text{Right Cancellation Law})$$

Proof:

$$(i) \quad ab = ac$$

$$\bar{a}^{-1}(ab) = \bar{a}^{-1}(ac)$$

$$\because a \in G, \bar{a}^{-1} \in G$$

$$(\bar{a}^{-1}a)b = (\bar{a}^{-1}a)c$$

$$eb = ec$$

$$b = c$$

Hence proved.

$$(ii) \quad ba = ca$$

$$(ba)\bar{a}^{-1} = (ca)\bar{a}^{-1}$$

$$b(a\bar{a}^{-1}) = c(a\bar{a}^{-1})$$

$$be = ce$$

$$b = c$$

Hence proved.



ORDER OF A GROUP

The number of elements in a group G is called order of the group.

It is denoted by $O(G)$ or $|G|$.

Finite Group:

If a group has a finite number of elements, then it is called a finite group.

In simple words, a finite group has a finite order.

Infinite Group:

If a group has an infinite number of elements, then it is called an infinite group.

In simple words, an infinite group has an infinite order.

Example: What is the order of the group $G = \{1, -1, i, -i\}$?

Sol: Since there are 4 elements in the group G .

$$\text{So } o(G) = 4$$

$$|G| = 4$$

Example: What is the order of the group

$$G = \{1, -1, i, -i, j, -j, k, -k\}?$$

Sol: Since there are 8 elements in the group G .

So the order of G is 8

$$o(G) = 8$$

$$|G| = 8$$

Example: What is the order of the group $(\mathbb{Z}, +)$?

$$\text{Sol: } \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Since there are infinite many elements in \mathbb{Z}

$$o(\mathbb{Z}) = \infty$$

$$|\mathbb{Z}| = \infty$$

Example: What is the order of the group $\{2^k : k = 0, \pm 1, \pm 2, \dots\}$?

$$\text{Sol: } G = \{2^k : k = 0, \pm 1, \pm 2, \dots\}$$

Since the values of k are infinite
So there are infinite many elements of the group in form 2^k .

So order of the group is infinity

$$|G| = \infty$$

ORDER OF AN ELEMENT OF A GROUP

Let G be a group and $a \in G$, then the order of 'a' is the least +ve integer n such that

$$a^n = e \quad \text{where 'e' is identity.}$$

$$G = \{1, -1\} \quad \begin{array}{l} (1)^1 = 1 \\ \text{Order of } 1 = 1 \\ (1)^2 = 1 \\ (1)^3 = 1 \end{array}$$

$$e = 1 \quad \begin{array}{l} (-1)^1 = -1 \\ (-1)^2 = 1 \\ \text{order of } -1 = 2 \\ (-1)^4 = 1 \\ (-1)^6 = 1 \\ (-1)^8 = 1 \end{array}$$

Example: Find the order of each element of the group $G = \{1, -1, i, -i\}$

Sol: (G, \cdot) Here $e = 1$

$$(1)^1 = 1 \Rightarrow e^n = 1 \Rightarrow n = 1 \Rightarrow \boxed{o(1) = 1}$$

$$(-1)^2 = (-1)(-1) = 1 \Rightarrow \boxed{o(-1) = 2}$$

$$(i)^2 = -1 \quad \because i = \sqrt{-1}$$

$$(i)^3 = i^2 \cdot i = -1 \cdot i = -i$$

$$(i)^4 = i^2 \cdot i^2 = (-1)(-1) = 1 \Rightarrow \boxed{o(i) = 4}$$

$$(-i)^2 = i^2 = -1$$

$$(-i)^3 = (-i)^2 (-i) = (-1)(-i) = i$$

$$(-i)^4 = (-i)^2 (-i)^2 = (-1)(-1) = 1$$

$$\Rightarrow \boxed{o(-i) = 4}$$

Example: Find the order of each element of the group

$$G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

of residue class modulo 5, under addition.

Sol: Here $e = \bar{0}$

$$\bar{0} = \bar{0} \Rightarrow \boxed{o(\bar{0}) = 1}$$

$$\bar{1} + \bar{1} = \bar{2}$$

$$\bar{1} + \bar{1} + \bar{1} = \bar{3}$$

$$\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{4}$$

$$\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0} \Rightarrow \boxed{o(\bar{1}) = 5}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 5} \\ \underline{5} \\ 0 \end{array}$$

$$\bar{2} + \bar{2} = \bar{4}$$

$$\bar{2} + \bar{2} + \bar{2} = \bar{1}$$

$$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{3}$$

$$\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{0}$$

$$\boxed{o(\bar{2}) = 5}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 6} \\ \underline{5} \\ 1 \end{array}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 8} \\ \underline{5} \\ 3 \end{array}$$

$$\begin{array}{r} 2 \\ 5 \overline{) 10} \\ \underline{10} \\ 0 \end{array}$$

$$\boxed{a^n = e}$$

$$\boxed{na = e}$$

$$\bar{3} + \bar{3} = \bar{1}$$

$$\bar{3} + \bar{3} + \bar{3} = \bar{4}$$

$$\bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{2}$$

$$\bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0}$$

$$\boxed{o(\bar{3}) = 5}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 6} \\ \underline{5} \\ 1 \end{array}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 9} \\ \underline{5} \\ 4 \end{array}$$

$$\begin{array}{r} 2 \\ 5 \overline{) 12} \\ \underline{10} \\ 2 \end{array}$$

$$\begin{array}{r} 3 \\ 5 \overline{) 15} \\ \underline{15} \\ 0 \end{array}$$

Similarly, $\boxed{o(\bar{4}) = 5}$



Theorem: If n is the order of an element 'a' of a group G , then for any integer m ,

$$a^m = e \text{ if and only if } m = qn, \text{ where } q \text{ is an integer.}$$

or

$$a^m = e \text{ if and only if } n \text{ divides } m.$$

Sol: Given $a \in G$ $10 = 5 \times 2$
 $a^n = e$ — n is ① least +ve integer

Suppose $a^m = e$ — ②

By division algorithm, there exist

$q, r \in \mathbb{Z}$, such that

$$m = qn + r \quad 0 \leq r < n$$

By ②

$$a^m = e$$

$$a^{qn+r} = e$$

$$a^{qn} \cdot a^r = e$$

$$(a^n)^q \cdot a^r = e$$

$$e^q \cdot a^r = e$$

$$e \cdot a^r = e$$

$$a^r = e$$

$$\because a^n = e$$

$$e^q = e$$

$$e \cdot a^r = a^r$$

It is possible only when $r = 0$

$$m = qn + r$$

$$= qn + 0$$

$$m = qn$$

n divides m

Conversely, suppose that

$$m = qn$$

Consider $a^m = a^{qn}$

$$= (a^n)^q$$

$$= (e)^q$$

$$\because a^n = e$$

$$a^m = e$$

Hence it is proved.



Theorem: Show that in a group, the order of an element is same as that of its inverse.

Proof: Let G be a group, $a \in G$

suppose $a^n = e$ — (1)

$$(a^{-1})^m = e \quad \text{--- (2)}$$

Now we have to prove that $n = m$.

By eq (1)

$$a^n = e$$

$$a^{-n} a^n = a^{-n} e$$

$$a^{-n+n} = a^{-n}$$

$$e = a^0 = a^{-n}$$

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

But the order of a^{-1} is m , so m must divide n — I

By eq (2),

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

$$a^{-m} = e$$

$$a^m a^{-m} = a^m e$$

$$a^{m-m} = a^m$$

$$a^0 = a^m$$

$$e = a^m$$

But the order of a is n , so n must divide m — II

It is possible only when $m = n$

Hence it is proved.

Theorem: Let G be a group and $a, b \in G$. Show that the orders of ab and ba are equal.

Proof:- let $(ab)^n = e$ ——— (1)

$(ba)^m = e$ ——— (2)

from eq (1) $(ab)^n = e$

$(ab)(ab) \dots (ab) = e$ n -factors

$a^{-1}a(bab \dots ab) = a^{-1}e$

$e(baba \dots bab) = a^{-1}$

$ba.ba \dots ba.b = a^{-1}$

$\underline{b}a.\underline{b}a \dots \underline{b}a.\underline{b}a = a^{-1}a$

$(ba)^n = e$

By (2), the order of ba is m .

Therefore m must divide n ——— (A)

From (2), $(ba)^m = e$

$ba.ba \dots ba = e$ m -factors

$b^{-1}(ba.ba \dots ba) = b^{-1}e$

$b^{-1}b(a.ba \dots ba) = b^{-1}$

$e(abab \dots ba) = b^{-1}$

$ab.ab \dots ab.a = b^{-1}$

$(ab.ab \dots ab.a)b = b^{-1}b$

$ab.ab \dots ab.ab = e$

$(ab)^m = e$

But from eq (1), the order of ab is n .

So n must divide m . ——— (B)

By (A) & (B), $m = n$

$o(ba) = o(ab)$

Hence the proof.

Abelian Group:

Let $(G, *)$ be a group, then G is called an Abelian group or Commutative group if the commutative law holds in G with respect to $*$, i.e.

$$x * y = y * x \quad \text{for all } x, y \text{ in } G$$

Non-Abelian Group:

Let $(G, *)$ be a group, then G is called a Non-Abelian group or Non-Commutative group if the commutative law does not hold in G with respect to $*$, i.e.

$$x * y \neq y * x \quad \text{for all } x, y \text{ in } G$$



Set

Example: Show that the group $(\mathbb{Z}, +)$ is an Abelian Group.

Sol: $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

$$10 + 21 = 31$$

$$21 + 10 = 31$$

for all $x, y \in \mathbb{Z}$,

$$x + y = y + x$$

\mathbb{Z} is an abelian group.

$$\begin{matrix} 3-2=1 \\ 2-3=-1 \end{matrix}$$

- 1) Closure property
- 2) Associative law
- 3) Identity
- 4) Inverse
- 5) Commutative law

Set

Example: Show that the group $(\mathbb{R}, +)$ is an Abelian Group.

Sol:

$$2 \cdot 5 + 3 \cdot 5 = 6 \cdot 5$$

$$3 \cdot 5 + 2 \cdot 5 = 6 \cdot 5$$

for $x, y \in \mathbb{R}$,

$$x + y = y + x$$

So commutative law holds.

So $(\mathbb{R}, +)$ is an abelian group.

Example: Show that the group $G = \{1, \omega, \omega^2\}$, where ω is the cube root of unity, is an Abelian Group.

Sol: $G = \{1, \omega, \omega^2\}$

$$\omega \cdot \omega^2 = \omega^3 = 1$$

$$\omega^2 \cdot \omega = \omega^3 = 1$$

for all $x, y \in G$,

$$xy = yx \text{ So commutative law holds}$$

So G is an abelian group.

.	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$$\begin{matrix} x = (1)^{1/3} \\ x^3 = 1 \\ \{1, \omega, \omega^2\} \\ \omega^3 = 1 \end{matrix}$$

$$\begin{matrix} \omega^4 = \omega^3 \omega \\ = 1 \cdot \omega \\ = \omega \end{matrix}$$

Example: Show that the group $\{1, -1, i, -i\}$ is an Abelian Group.

$$G = \{1, -1, i, -i\}$$

$$i(-i) = 1$$

$$(-i)i = 1$$

$$-1 \cdot i = -i$$

$$i \cdot (-1) = -i$$

for any $x, y \in G$,

$$xy = yx$$

So G is an abelian group.

.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1



Set

Example: Show that the group $\{1, -1, i, -i, j, -j, k, -k\}$ is a Non-Abelian Group.

Sol:

$$ij = -ji$$

$$ij \neq ji$$

$$jk = -kj$$

$$jk \neq kj$$

$$ki = -ik$$

$$ki \neq ik$$

So the given is not abelian.

1) Closure property

2) Associative law

3) Identity

4) Inverse exists.

5) Commutative law

Example: Show that the set of non-singular matrices of order 2 is a Non-Abelian Group.

Sol: $G =$ Set of non-singular matrices of order 2.

1) Closure property.

$$\text{Let } A, B \in G, \quad AB = C \in G$$

2) Associative law.

$$(AB)C = A(BC)$$

3) Identity Element exists

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ such that}$$

$$AI = A = IA \quad \forall A \in G$$

4) Inverse of each element in G .

Since G has non-singular matrices, so for all $A \in G$,

$$\exists \bar{A} \in G, \quad \bar{A}A = I = A\bar{A}$$

5) Commutative law.

In general,

$$AB \neq BA$$

So commutative law does not hold,

So G is a non-abelian group.



Theorem:

Show that a group G is abelian if and only if $(ab)^2 = a^2 b^2$ for all a, b in G .

Proof: Let G be an abelian,

$$ab = ba \quad \text{--- ① for all } a, b \in G$$

Consider $(ab)^2 = (ab)(ab)$

$$= a(ba)b$$

$$= a(ab)b \quad \text{by ①}$$

$$= (aa)(bb)$$

$$= a^2 b^2 \quad \text{Hence proved}$$

Now conversely suppose that

$$(ab)^2 = a^2 b^2$$

$$(ab)(ab) = (aa)(bb)$$

$$a(ba)b = a(ab)b$$

$$a^{-1}(a(ba)b) = a^{-1}(a(ab)b)$$

$$a^{-1}a(ba)b = a^{-1}a(ab)b$$

$$e(ba)b = e(ab)b$$

$$(ba)b = (ab)b$$

$$((ba)b)b^{-1} = ((ab)b)b^{-1}$$

$$(ba)(bb^{-1}) = (ab)(bb^{-1})$$

$$(ba)e = (ab)e$$

$$ba = ab$$

So the commutative law holds,
So G is an abelian group.

Hence the proof.



Theorem:

If a group G is such that

$$a \cdot a = e \quad \text{for all } a \text{ in } G$$

where e is identity, then G is an Abelian Group.

Proof: Let $a, b \in G$,

$$a \cdot a = e \quad \text{--- (1)}$$

$$b \cdot b = e \quad \text{--- (2)}$$

By (1) $a^{-1}(a \cdot a) = a^{-1}e$

$$(a^{-1}a)a = a^{-1}$$

$$ea = a^{-1}$$

$$a = a^{-1} \quad \text{--- (3)}$$

By (2)

$$b \cdot b = e$$

$$b^{-1}(b \cdot b) = b^{-1}e$$

$$(b^{-1}b)b = b^{-1}$$

$$eb = b^{-1}$$

$$b = b^{-1} \quad \text{--- (4)}$$

Since $a, b \in G$, $ab \in G$

$$ab = (ab)^{-1}$$

$$= b^{-1}a^{-1}$$

$$ab = ba$$

$$\therefore (ab)^{-1} = b^{-1}a^{-1}$$

Since commutative law holds,
So G is an abelian group.

Theorem:

If each element of a group G is its own inverse, then show that G is an Abelian Group.

Proof: let $a, b \in G,$

$$a = a^{-1} \quad \text{--- (1)}$$

$$b = b^{-1} \quad \text{--- (2)}$$

Since $a, b \in G,$ $ab \in G$

$$(ab) = (ab)^{-1}$$

$$ab = b^{-1}a^{-1}$$

$$ab = ba$$

$$\begin{aligned} \therefore (ab)^{-1} \\ = b^{-1}a^{-1} \end{aligned}$$

So G is an abelian group.



Theorem:

If a group G has three elements, then show that G is an Abelian Group.

Proof: Let $G = \{e, a, b\}$

From the table, it is clear that $a^2 \in G$

There are three possibilities

\cdot	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

$$a \neq b \neq e$$

- (i) $a^2 = e$
- (ii) $a^2 = a$
- (iii) $a^2 = b$

Case (i): Suppose $a^2 = e$ \times

Since $ab \in G$, then

$$1) ab = e \Rightarrow a(ab) = ae$$

$$2) ab = a \Rightarrow b = e \text{ Not}$$

$$3) ab = b$$

$$(ab)b^{-1} = bb^{-1}$$

$$ae = e$$

$$a = e \text{ Not}$$

$$\Rightarrow a^2 b = a$$

$$e b = a$$

$$b = a$$

It is not possible.

Case (ii): Suppose $a^2 = a$

$$aa = a$$

$$a^{-1}(aa) = a^{-1}a$$

$$(a^{-1}a)a = e$$

$$ea = e$$

$$a = e$$

Not possible.

Case (iii)

$$G = \{e, a, a^2\}$$

Clearly the elements of the group G satisfy commutative law. So G is an abelian group.

$$a^2 = e \quad \times$$

$$a^2 = a \quad \times$$

$$a^2 = b$$

Subgroups

Definition: Let $(G, *)$ be a group and H be a subset of G . If H is itself a group under the same binary operation $*$, then H is called a Subgroup of G

Examples: (1) $H = \{1, -1\}$ is a subgroup of $\{1, -1, i, -i\}$ under the binary operation of \cdot .

(2) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

(3) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$

(4) $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$

Remarks: If H is a subset of a group G and H is a group under different binary operation than that of group G , then H is not called a subgroup of G .

$$H = \{1, -1\} \quad (H, \cdot)$$

$$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}, \quad (\mathbb{Z}, +)$$

$$H \subset \mathbb{Z}$$

H is not a subgroup of \mathbb{Z} .



Trivial Subgroups:

Every group G has at least two subgroups $\{e\}$ and G itself. These two subgroups $\{e\}$ and G are called trivial subgroups of G .

Example : $G = \{1, -1, i, -i\}$

$$\{1\}, \{1, -1, i, -i\}$$

Non-Trivial Subgroups:

Any subgroups of a group G , other than $\{e\}$ and G are called non-trivial subgroups of G .

Example : $G = \{1, -1, i, -i\}$

Trivial Subgroups : $\{1\}, \{1, -1, i, -i\}$

Non-Trivial Subgroups : $\{1, -1\}$



Theorem :

Let $(G, *)$ be a group. A non-empty subset H of G is a subgroup of G if and only if

$$(i) a, b \in H \Rightarrow a * b \in H$$

$$(ii) a \in H \Rightarrow \bar{a}' \in H,$$

where \bar{a}' is the inverse of a .

Proof:

Suppose H is subgroup of G .

Since H is a group,

so closure property holds \Rightarrow for any $a, b \in H$,
 $a * b \in H$

and inverse of each element of H exists

$$\Rightarrow \text{for all } a \in H, \bar{a}' \in H$$

Hence the proof.

conversely, suppose that

$$\text{for } a, b \in H, a * b \in H \quad \text{--- (1)}$$

$$\text{for } a \in H, \bar{a}' \in H \quad \text{--- (2)}$$

C_1 : closure property holds by (1)

C_2 : Associative law:

Since $H \subset G$ and associative law holds in G , so the associative law holds in H , too.

C_3 : By (2), for $a \in H$, $\bar{a}' \in H$, so inverse of every element of H exists

C_4 : By (1), $a, \bar{a}' \in H$, $a * \bar{a}' \in H$

So identity exists in H . $e \in H$

So H is the subgroup of G .



Theorem:

The intersection of any collection of subgroups of a group $(G, *)$ is a subgroup of G .

Proof: Let $(G, *)$ be a group.

$\{H_d, d \in I\}$ be a collection of subgroups of G . $\bigcap_{d \in I} H_d$ is the intersection

of all $H_d, d \in I$.

Suppose $a, b \in \bigcap_{d \in I} H_d$

$\Rightarrow a, b \in H_d$, for all $d \in I$

$\Rightarrow a * b^{-1} \in H_d$, for all $d \in I$
 $\because H_d$ are groups.

$\Rightarrow a * b^{-1} \in \bigcap_{d \in I} H_d$

Hence $\bigcap_{d \in I} H_d$ is a subgroup of G .

Hence the proof.

Let $a, b \in H$
 $a * b^{-1} \in H$
So H is
a subgroup.



Theorem:

The union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.

Proof: $H \cup K$ is a subgroup of G
if and only if

either $H \subset K$ or $K \subset H$

Suppose either $H \subset K$ or $K \subset H$ — (1)

When $H \subset K \Rightarrow H \cup K = K$

Since K is a subgroup of G

so $H \cup K$ is also a subgroup of G

When $K \subset H \Rightarrow H \cup K = H$

Since H is a subgroup of G ,

So $H \cup K$ is also a subgroup of G

Hence the proof.

Now suppose that $H \cup K$ is a subgroup of G ,
then we have to show that either $H \subset K$ or
 $K \subset H$.

Suppose contrarily, $H \not\subset K$ or $K \not\subset H$

If $a \in H$, then $a \notin K$ — (A)

If $b \in K$, then $b \notin H$ — (B)

Then $a, b \in H \cup K$

$\Rightarrow a * b \in H \cup K$ $\because H \cup K$ is a subgroup
of G

$\Rightarrow a * b \in H$ or $a * b \in K$

When $a * b \in H$, then $a^{-1} * (a * b) \in H$

$(a^{-1} * a) * b \in H$

$e * b \in H$

$b \in H$

which contradicts to (B)

When $a * b \in K$, then

$(a * b) * b^{-1} \in K$

$a * (b * b^{-1}) \in K$

$a * e \in K$

$a \in K$

which contradicts (A)

So our supposition that

$H \not\subset K$ or $K \not\subset H$ is wrong.

Therefore either $H \subset K$ or $K \subset H$

Hence the proof.



Theorem:

The union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.

Proof: $H \cup K$ is a subgroup of G
if and only if

either $H \subset K$ or $K \subset H$

Suppose either $H \subset K$ or $K \subset H$ — (1)

When $H \subset K \Rightarrow H \cup K = K$

Since K is a subgroup of G
so $H \cup K$ is also a subgroup of G

When $K \subset H \Rightarrow H \cup K = H$

Since H is a subgroup of G ,
So $H \cup K$ is also a subgroup of G
Hence the proof.

Now suppose that $H \cup K$ is a subgroup of G ,
then we have to show that either $H \subset K$ or
 $K \subset H$.

Suppose contrarily, $H \not\subset K$ or $K \not\subset H$

If $a \in H$, then $a \notin K$ — (A)

If $b \in K$, then $b \notin H$ — (B)

Then $a, b \in H \cup K$

$\Rightarrow a * b \in H \cup K$ $\because H \cup K$ is a subgroup
of G

$\Rightarrow a * b \in H$ or $a * b \in K$

When $a * b \in H$, then $a^{-1} * (a * b) \in H$
 $(a^{-1} * a) * b \in H$
 $e * b \in H$
 $b \in H$

which contradicts to (B)

When $a * b \in K$, then

$(a * b) * b^{-1} \in K$

$a * (b * b^{-1}) \in K$

$a * e \in K$

$a \in K$

which contradicts (A)

So our supposition that

$H \not\subset K$ or $K \not\subset H$ is wrong.

Therefore either $H \subset K$ or $K \subset H$

Hence the proof.



Definition: Let G be a group under multiplication, then G is called Cyclic group, if each element of G can be written as a power of an element $a \in G$

Let $a \in G$,

for all $x \in G$,

$$x = a^n$$

for $n \in \mathbb{N}$.

$$G = \langle a : a^n = e \rangle$$

Example:

$$G = \{1, -1\}$$

$$(-1)^1 = -1$$

$$(-1)^2 = 1$$

So G is a cyclic group generated by -1 .



Example : Let $G = \{1, -1, i, -i\}$. Show that G is a cyclic group.

Sol: $G = \{1, -1, i, -i\}$

$$(1)^1 = 1$$

$$(1)^2 = 1$$

$$(-1)^1 = -1$$

$$(-1)^2 = 1$$

$$(-1)^3 = -1$$

$$(-1)^4 = 1$$

$$(i)^1 = i \checkmark$$

$$(i)^2 = -1 \checkmark$$

$$(i)^3 = i^2 \cdot i$$

$$= -i \checkmark$$

$$(i)^4 = i^2 \cdot i^2$$

$$= (-1)(-1)$$

$$= 1 \checkmark$$

$$i = \sqrt{-1}$$

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

$$i^2 = -1$$

$$G = \langle i : i^4 = 1 \rangle$$

$$(-i)^1 = -i \checkmark$$

$$(-i)^2 = i^2 = -1 \checkmark$$

$$(-i)^3 = -i^3 = -(-i^2 \cdot i)$$

$$= -(-1)i$$

$$= i \checkmark$$

$$(-i)^4 = i^4 = i^2 \cdot i^2 = (-1)(-1)$$

$$= 1 \checkmark$$

$$G = \langle -i : (-i)^4 = 1 \rangle$$

Theorem : Every cyclic group is an abelian group.

Proof: Let G be a cyclic group with the generator a .

Let $x, y \in G$ such that

$$x = a^m, \quad y = a^n \quad m, n \in \mathbb{Z}$$

Consider $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$

$$xy = yx \quad \text{for } x, y \in G$$

Hence G is an abelian group.



Remark 1: A cyclic group may have two generators.

$$G = \{1, -1, i, -i\}$$

$$|G| = 4$$

$$(i)^1 = i$$

$$(-i)^1 = -i$$

$$i^4 = (-i)^4 = 1$$

$$(i)^2 = -1$$

$$(-i)^2 = -1$$

$$|i| = |-i| = 4$$

$$i^3 = -i$$

$$(-i)^3 = i$$

$$i^4 = 1$$

$$(-i)^4 = 1$$

$$G = \langle i \rangle$$

$$G = \langle -i \rangle$$

Remark 2: $a \in G$

$$\boxed{a^n = e} \quad \checkmark$$

$$a a a \dots a = a^n$$

n-times

$$a a = a^2$$

$$a a a = a^3$$

$$G = \{1, -1, i, -i\}$$

$$(G, +)$$

$$a \in G$$

$$e' \in G$$

$$\boxed{na} = a + a + \dots + a = e'$$

$$a + a = 2a, \quad a + a + a = 3a$$



Theorem : Every subgroup of a cyclic group is cyclic.

Proof: Let G be a cyclic group generated by $a \in G$.

Let H be a subgroup of G .

$$a^k \in H \quad k \text{ is least +ve integer}$$

Let $b \in H$ be an arbitrary element of H

So $b = a^m \in H$ for some integer m .

$$k < m \quad \text{--- (1)}$$

By division algorithm, $\exists q, r$ such that

$$m = qk + r, \quad 0 \leq r < k \quad k \nmid m$$

Consider $a^m = a^{qk+r}$ --- (2)

$$a^m = a^{qk} \cdot a^r$$

$$a^m \cdot a^{-qk} = a^{qk} \cdot a^r \cdot a^{-qk}$$

$$= a^{qk - qk} \cdot a^r$$

$$a^m \cdot (a^k)^{-q} = a^0 \cdot a^r$$

$$a^m \cdot (a^k)^{-q} = a^r, \quad 0 \leq r < k$$

Since $a^k \in H$, $(a^k)^{-q} \in H$ $\therefore H$ is subgroup.

Also $a^m \in H$, $a^m \cdot (a^k)^{-q} \in H$

$$a^r \in H$$

It is possible when $r=0$

$$\text{So } a^m = a^{qk+0}$$

$$b = a^m = (a^k)^q$$

Hence a^k is the generator of H

Therefore H is a cyclic group.

Hence the proof.



Theorem: The order of a cyclic group is equal to the order of its generator.

VuBioTechnologist

Proof: Let G be a cyclic group generated by a .

and $|G| = n$

So its elements are a, a^2, a^3, \dots, a^n .

We have to show that $|a| = n$

$$\text{i.e. } a^n = e$$

Suppose that the order of a is m , $m < n$

$$a^m = e$$

$$a^m a = ea$$

$$a^{m+1} = a$$

$$a^{m+1} a = aa$$

$$a^{m+2} = a^2$$

\vdots

$$a, a^2, a^3, \dots, a^m, a^{m+1}, a^{m+2}, \dots, a^n$$

$$= a, a^2, a^3, \dots, e, a, a^2, \dots, a^n$$

which is a contradiction that there are n elements in G .

$$a^m = e \quad m < n$$

is wrong.

$$a^n = e$$

$$a, a^2, a^3, \dots, a^n$$

$$a^r = a^s \quad 0 < s < r < n$$

$$a^r a^{-s} = a^s a^{-s}$$

$$a^{r-s} = a^{s-s} = a^0 = e$$

$$a^{r-s} = e \quad r-s < n$$

which is the contradiction

$$\text{So } a^r \neq a^s$$

$$a^n = e$$

$$\text{Hence } |a| = n$$

$$\Rightarrow |G| = |a| = n$$

Hence proved.



Theorem: Show that the group $(\mathbb{Q}, +)$ is abelian but not cyclic.

Proof:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$$

Since commutative law holds rational
w.r.t. $+$,

$$a + b = b + a \quad \forall a, b \in \mathbb{Q}$$

So $(\mathbb{Q}, +)$ is an abelian group.

Suppose contrarily that \mathbb{Q} is cyclic
and can be generated by $a \in \mathbb{Q}$.

$$a = \frac{p}{q} \quad p, q \in \mathbb{Z}$$

$$\text{for } x \in \mathbb{Q}, \quad x = na$$

$$\frac{1}{2q} \in \mathbb{Q}, \quad \text{so } \frac{1}{2q} = na$$

$$\frac{1}{2q} = n \frac{p}{q}$$

$$\frac{1}{2} = np \quad \text{--- (1)}$$

$$2 \times 3 = 6$$

But the product of two integers is integer.
So (1) is wrong.

Hence every rational number cannot be
written in form generator. So $(\mathbb{Q}, +)$
is not a cyclic.



Theorem: Let G be a cyclic group of order n generated by a , then for each positive divisor d of n , there is a unique subgroup (of G) of order d .

Proof: $G = \langle a : a^n = e \rangle$

Suppose d divides n , $n = qd$

Let $b \in G$, $b = a^q$

$$\langle b \rangle = \langle a^q \rangle^d$$

$$b^d = a^{qd} = a^n = e$$

$$H = \langle b : b^d = e \rangle$$

which is the required subgroup of G

Suppose Contrarily that subgroup of order d is not unique, there exists another subgroup K of order d . K is generated by an element $c = a^k$.

Since order of K is d , so

$$a^k = c$$

$$(a^k)^d = c^d$$

$$a^{kd} = c^d$$

$$a^n = c^d$$

$$e = c^d$$

$$kd = n, \quad qd = n$$

$$kd = qd$$

$$k = q$$

$$b = a^q = a^k$$

$$K = H$$

Hence H is a unique subgroup of order d .



Theorem: If G is a cyclic group of even order, then prove that there is only one subgroup of order 2 in G .

Proof: Let G be a cyclic group with even order

$$|G| = 2n \quad n \text{ is +ve integer.}$$

By the previous theorem, if a +ve integer d divides order of a group G , then there will be a subgroup of order d .

Since 2 divides $2n$, so there must exist a subgroup of order 2.

Hence the proof.



Left Coset : Let H be a subgroup of a group G and $a \in G$, then the set

$$aH = \{ ah : h \in H \}$$

is called a left coset of H in G determined by a .

Example :

$$G = \{1, -1, i, -i\}$$

$$H = \{1, -1\}$$

$$i \in G, \quad iH = \{i \cdot 1, i(-1)\} = \{i, -i\}$$

Right Coset : Let H be a subgroup of a group G and $a \in G$, then the set

$$Ha = \{ ha : h \in H \}$$

is called a Right coset of H in G determined by a .

Example :

$$G = \{1, -1, i, -i\}$$

$$H = \{1, -1\}$$

$$i \in G, \quad Hi = \{1 \cdot i, -1 \cdot i\} = \{i, -i\}$$

Remark 1 : The left (or right) cosets of H in G determined by the identity element e is H itself.

$$eH = \{ \underline{e}h : h \in H \} = \{ \overset{\checkmark}{h} : h \in H \} = H$$

$$He = \{ h \underline{e} : h \in H \} = \{ h : h \in H \} = H$$

Remark 2 : If the binary operation of the group G is '+', then the left (or right) cosets of H in G determined by a is given by

$$a + H = \{ a + h : h \in H \}$$

$$H + a = \{ h + a : h \in H \}$$



Example : Find all the left costs of $H = \{ 1, -1 \}$ in $G = \{ 1, -1, i, -i \}$.

Sol: $G = \{ 1, -1, i, -i \}$

$$H = \{ 1, -1 \}$$

$$a \in G, aH$$

$$1 \in G, 1H = \{ 1 \cdot 1, 1 \cdot (-1) \} = \{ 1, -1 \} \checkmark$$

$$-1 \in G, -1H = \{ -1 \cdot 1, -1 \cdot (-1) \} = \{ -1, 1 \} \checkmark$$

$$i \in G, iH = \{ i \cdot 1, i \cdot (-1) \} = \{ i, -i \} \checkmark$$

$$-i \in G, -iH = \{ -i \cdot 1, -i \cdot (-1) \} = \{ -i, i \} \checkmark$$

Example : Find all the right cosets of $H = \{ 1, -1 \}$ in $G = \{ 1, -1, i, -i \}$.

Sol: $G = \{ 1, -1, i, -i \}, \quad H = \{ 1, -1 \}$

~~$H_1 = \{ 1 \cdot 1, -1 \cdot 1 \} = \{ 1, -1 \} \checkmark$~~

~~$H_{(-1)} = \{ 1 \cdot (-1), -1 \cdot (-1) \} = \{ -1, 1 \}$~~

~~$H_i = \{ 1 \cdot i, -1 \cdot i \} = \{ i, -i \} \checkmark$~~

~~$H_{-i} = \{ 1 \cdot (-i), -1 \cdot (-i) \} = \{ -i, i \}$~~



Example : Let $G = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$ be the group of residue classes modulo 6 under addition, and $H = \{ \bar{0}, \bar{2}, \bar{4} \}$ is the subgroup of G , then find all left and right cosets of H in G .

$$\begin{array}{r} 1 \\ 6 \overline{) 6} \\ \underline{6} \\ 0 \end{array}$$

Sol: $G = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$, $H = \{ \bar{0}, \bar{2}, \bar{4} \}$

$$\begin{array}{r} 1 \\ 6 \overline{) 6} \\ \underline{6} \\ 0 \end{array}$$

$\bar{0} \in G$, $\bar{0} + H = \{ \bar{0} + \bar{0}, \bar{0} + \bar{2}, \bar{0} + \bar{4} \} = \{ \bar{0}, \bar{2}, \bar{4} \}$ ✓

$\bar{1} \in G$, $\bar{1} + H = \{ \bar{1} + \bar{0}, \bar{1} + \bar{2}, \bar{1} + \bar{4} \} = \{ \bar{1}, \bar{3}, \bar{5} \}$ ✓

$$\begin{array}{l} \bar{3} + \bar{4} = \bar{1} \\ \bar{3} + \bar{2} = \bar{5} \end{array}$$

$\bar{2} \in G$, $\bar{2} + H = \{ \bar{2} + \bar{0}, \bar{2} + \bar{2}, \bar{2} + \bar{4} \} = \{ \bar{2}, \bar{4}, \bar{0} \}$ ✓

$\bar{3} \in G$, $\bar{3} + H = \{ \bar{3} + \bar{0}, \bar{3} + \bar{2}, \bar{3} + \bar{4} \} = \{ \bar{3}, \bar{5}, \bar{1} \}$ ✓

$$\begin{array}{r} 1 \\ 6 \overline{) 6} \\ \underline{6} \\ 0 \end{array}$$

$\bar{4} \in G$, $\bar{4} + H = \{ \bar{4} + \bar{0}, \bar{4} + \bar{2}, \bar{4} + \bar{4} \} = \{ \bar{4}, \bar{0}, \bar{2} \}$ ✓

$\bar{5} \in G$, $\bar{5} + H = \{ \bar{5} + \bar{0}, \bar{5} + \bar{2}, \bar{5} + \bar{4} \} = \{ \bar{5}, \bar{1}, \bar{3} \}$ ✓

$$\begin{array}{r} 1 \\ 6 \overline{) 6} \\ \underline{6} \\ 0 \end{array}$$

Partition of a set A : The collection $\{A_\alpha : \alpha \in I\}$ of subsets of a set A is called the partition of A if

- (i) $A = \bigcup_{\alpha \in I} A_\alpha$
- (ii) $A_\alpha \cap A_\beta = \emptyset$ for $\alpha \neq \beta$





The number of distinct left (or right) cosets of a subgroup H of a group G is called the Index of H in G, and is denoted by $[G : H]$.

Example: $G = \{1, -1, i, -i\}$

$$H = \{1, -1\}$$

$$1 \in G,$$

$$1H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\} \checkmark$$

$$-1 \in G,$$

$$-1H = \{-1(1), -1(-1)\} = \{-1, 1\}$$

$$i \in G,$$

$$iH = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} \checkmark$$

$$-i \in G,$$

$$-iH = \{-i(1), -i(-1)\} = \{-i, i\}$$

Number of distinct left cosets of H in G = 2

$$[G : H] = 2$$

Example : Find the distinct left or (right) cosets of

$$E = \{ 0, \pm 2, \pm 4, \dots \} = \{ 2n : n \in \mathbb{Z} \}$$

in the group $(\mathbb{Z}, +)$.

Sol: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$

$$E = \{ \dots, -4, -2, 0, 2, 4, \dots \}$$

$$\begin{aligned} 0 \in \mathbb{Z}, \quad 0 + E &= \{ \dots, 0 + (-4), 0 + (-2), 0 + 0, 0 + 2, 0 + 4, \dots \} \\ &= \{ \dots, -4, -2, 0, 2, 4, \dots \} \checkmark \end{aligned}$$

$$\begin{aligned} 1 \in \mathbb{Z}, \quad 1 + E &= \{ \dots, 1 + (-4), 1 + (-2), 1 + 0, 1 + 2, 1 + 4, \dots \} \\ &= \{ \dots, -3, -1, 1, 3, 5, \dots \} \checkmark \end{aligned}$$

Number of distinct left cosets = 2

$$[\mathbb{Z} : E] = 2$$



Lagrange's Theorem: Both the order and index of a subgroup of a finite group divide the order of the group.

Proof: Let G be a group and H be its subgroup.

such that $|G|=n$, $|H|=m$

Let $a_i \in G$, a_1H, a_2H, \dots, a_kH be distinct left cosets of H in

Define $\varphi: H \rightarrow a_iH$, $a_i \in G$
by $\varphi(h) = a_i h$ $h \in H$

Since each element $a_i h \in a_i H$ for each $h \in H$, so φ is onto.

Consider $\varphi(h_1) = \varphi(h_2)$ $h_1, h_2 \in H$
 $a_i h_1 = a_i h_2$
 $h_1 = h_2$ $\because a_i \in G$

Hence φ is a one-one function.

So φ is bijective function.

Therefore the no. of elements in H is equal to the no. of elements in $a_i H$.

$$|H| = m = |a_1H| = |a_2H| = \dots = |a_kH|$$

Since the cosets define the partition of G ,

So

$$a_1H \cap a_2H = \emptyset$$

$$a_iH \cap a_jH = \emptyset \quad \text{for } i \neq j$$

$$\text{and } G = a_1H \cup a_2H \cup \dots \cup a_kH$$

$$|G| = |a_1H| + |a_2H| + \dots + |a_kH|$$

$$n = m + m + \dots + m$$

$$n = mk$$

$$6 = 2 \times 3$$

$\Rightarrow m$ divides n & k divides n

$\Rightarrow |H|$ divides $|G|$ & $[G:H]$ divides $|G|$.
Hence the proof.



Theorem : The order of an element of a finite group divides the order of the group.

Proof: Let G be a group & $x \in G$.

$$|G| = n$$

$$|x| = m$$

We show that m divides n .

$$x \in G, \quad H = \langle x \rangle \subset G.$$

$$\text{But } |x| = m, \text{ so } |H| = m$$

By Lagrange's theorem, the order of a subgroup H divides order of the group G .

$$|H| \text{ divides } |G|.$$

$$m \text{ divides } n$$

Hence the proof.



Theorem : A group G whose order is a prime number is necessarily cyclic.

Proof: Let G be a group.

$$|G| = p, \quad p \text{ is prime number.}$$

Let $x \in G$ be a non-identity element.

$$H = \langle x \rangle \subset G$$

By Lagrange's theorem, $|H|$ divides $|G|$.

But $|G| = p$, so $|H|$ can divide $|G|$ only when $|H| = p$ or $|H| = 1$.

Therefore $|H| = p$, but $|G| = p$.

It means $H = G$.

So G must be a cyclic group.

Hence the proof.

Example : Let G be a group of order 89. Can G have a subgroup

- (i) of order 12
- (ii) of order 16
- (iii) of order 24

Justify your answer.

Sol: $|G| = 89$

(i) Let H be a subgroup of order 12.

$$|H| = 12$$

Since 89 is a prime number, and 12 does not divide it, so by Lagrange's theorem, H is not a subgroup of G .

PERMUTATION: Let X be non-empty set. A bijective mapping $\alpha : X \rightarrow X$ is called the permutation on X .



IDENTITY PERMUTATION: Let X be non-empty set.

A bijective mapping $\alpha : X \rightarrow X$ is called the identity permutation on X , if

$$\alpha(x) = x \quad \text{for all } x \in X$$

$$X = \{1, 2, 3\}$$

$$\alpha(1) = 1$$

$$\alpha(2) = 2$$

$$\alpha(3) = 3$$

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

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

$$X = \{x_1, x_2, \dots, x_n\}$$

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \alpha(x_1) & \alpha(x_2) & \dots & \alpha(x_n) \end{pmatrix}$$

$$= \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$$



REMARK: If X has n elements, then total number of permutations on X is $n!$

1) $X = \{1\}$, $n = 1$, Total permutations = $1!$
 $= 1$

$$\left(\begin{matrix} 1 \\ 1 \end{matrix} \right)$$

2) $X = \{1, 2\}$, $n = 2$, Total permutations = $2!$
 $= 2 \times 1 = 2$

$$d_1 = \left(\begin{matrix} 1 & 2 \\ 1 & 2 \end{matrix} \right), \quad d_2 = \left(\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \right)$$

3) $X = \{1, 2, 3\}$, $n = 3$, Total permutations = $3!$
 $= 3 \times 2 \times 1$
 $= 6$

$$d_1 = \left(\begin{matrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{matrix} \right)$$

$$d_4 = \left(\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix} \right)$$

$$d_2 = \left(\begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix} \right)$$

$$d_5 = \left(\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix} \right)$$

$$d_3 = \left(\begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix} \right)$$

$$d_6 = \left(\begin{matrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix} \right)$$



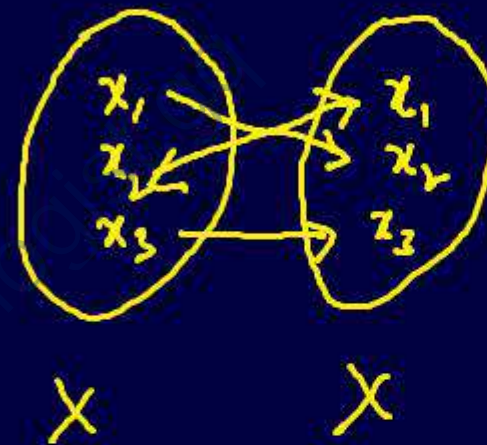
INVERSE PERMUTATION: Let X be a non-empty set and $d : X \rightarrow X$ be a permutation on X such that

$$d(x) = y \quad \forall x, y \in X$$

Then the inverse permutation $d^{-1} : X \rightarrow X$ of d is defined as

$$d^{-1}(y) = x \quad \forall x, y \in X$$

$$\begin{aligned} d(x_1) &= x_3 \\ d(x_2) &= x_1 \\ d(x_3) &= x_3 \end{aligned}$$



$$\begin{aligned} d(x_2) &= x_1 \\ d^{-1}(d(x_2)) &= d^{-1}(x_1) \\ x_2 &= d^{-1}(x_1) \end{aligned}$$

$$\begin{aligned} d(x_1) &= x_2 \\ x_1 &= d^{-1}(x_2) \\ d^{-1}(x_3) &= x_3 \end{aligned}$$

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

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

EXAMPLE: Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$

Find α^{-1} .

Sol: $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

Ans

EXAMPLE : Let $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$

Find β^{-1} .

Sol: $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$

Ans

Q: Write the inverse permutation of $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Sol:

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

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

Ans

Q: Write the inverse permutation of $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

Sol:

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

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

$$\begin{array}{l} 1 \rightarrow 1 \\ 2 \rightarrow 2 \\ 3 \rightarrow 3 \end{array}$$

Ans

Q: Write the inverse permutation of $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

Sol:

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

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Ans

Q: Write the inverse permutation of $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Sol:

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

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

Ans

Q: Write the inverse permutation of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$.

Sol:

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

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

Ans

Q: Write the inverse permutation of $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$.

Sol:

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

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

Ans



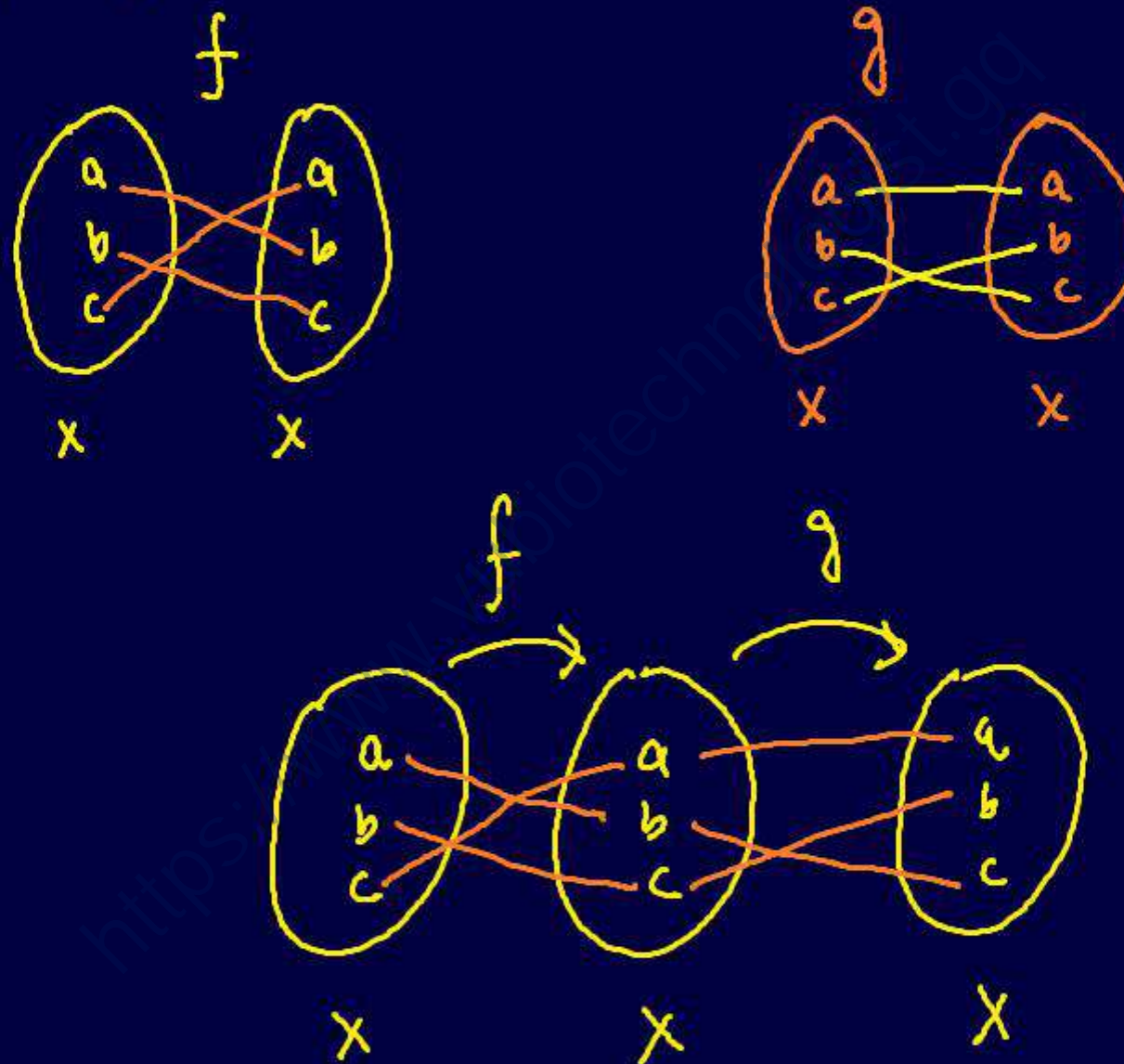
PRODUCT or COMPOSITION OF PERMUTATIONS:

Let $f: X \rightarrow X$ and $g: X \rightarrow X$ be two permutations on a non-empty set X , then the permutation $f \circ g: X \rightarrow X$ on X defined as

$$(x) f \circ g = ((x) f)g \quad \forall x \in X$$

is called the Product or Composition of permutations f and g .

It is also denoted by $f \circ g$.



$$\begin{aligned} f \circ g(x) &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \quad \text{Ans} \end{aligned}$$

PRODUCT or COMPOSITION OF PERMUTATIONS:

Let $f: X \rightarrow X$ and $g: X \rightarrow X$ be two permutations on a non-empty set X , then the permutation $fg: X \rightarrow X$ on X defined as

$$(x)fg = ((x)f)g \quad \forall x \in X$$

is called the Product or Composition of permutations f and g .

It is also denoted by $f \circ g$.

EXAMPLE : Find the product of the following permutations

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

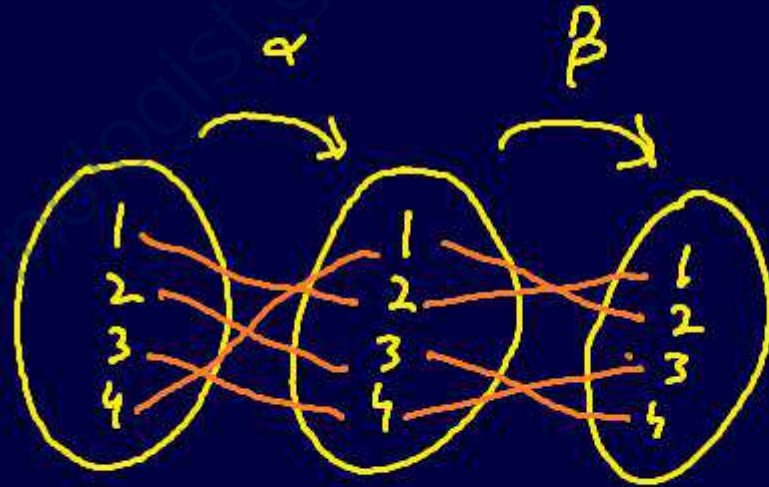
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Sol:

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

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

Ans



EXAMPLE : Find the product or composition $\alpha \circ \alpha$ of the permutation

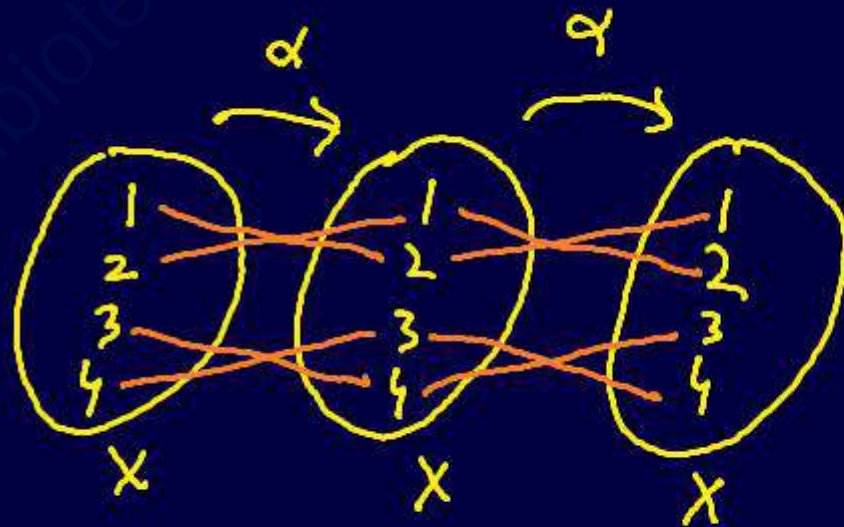
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Sol:

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

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

Ans



EXAMPLE : Find the product or composition $\alpha \circ \alpha$ of the permutation

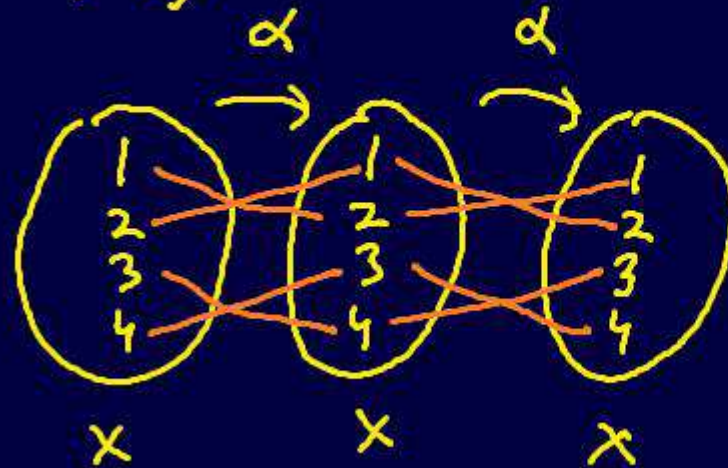
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Sol:

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

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

Ans





EXAMPLE : Let

VuBioTechnologist

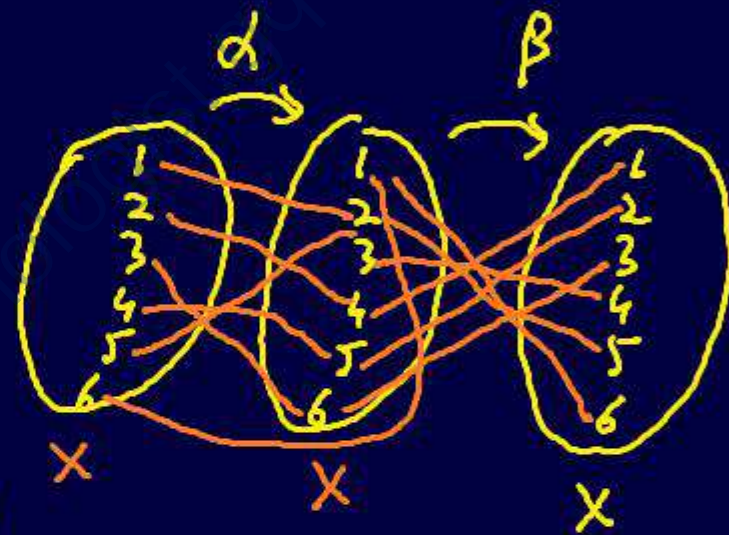
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$$

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

Find $\alpha \circ \beta$, $\alpha \circ \alpha$, $\beta \circ \beta$, $\beta \circ \alpha$.

Sol: $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

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



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

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

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

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

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

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

EXAMPLE : Let

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

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

Show that $\alpha\beta \neq \beta\alpha$

Sol:

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

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

$$\alpha\beta \neq \beta\alpha$$

Example : Multiply the following permutations

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

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

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

Example : Multiply the following permutations

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

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

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

Example : Multiply the following permutations

$$\begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 2 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 3 & 9 & 2 \end{pmatrix}$$

Sol: $\begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 2 & 3 \end{pmatrix} \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 3 & 9 & 2 \end{pmatrix}$

$$= \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 2 & 8 & 6 \end{pmatrix} \text{ Ans}$$

**Example :** Let

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

find $f \circ g$, $f^2 \circ g$ and $f \circ g^3$.

Sol: $f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
 $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

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

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

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

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

Example : Let

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

Show that $f^4 = g^2$.

Sol: $f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

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

$$f^4 = f^3 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \text{--- ①}$$

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

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

$$g^2 = f^4$$

by ①

Hence the proof.



Example: Let

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

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

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

find $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$, h^2 , g^2 .

Solution:

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

Ans

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

Ans

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

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

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

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

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

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

Ans



Cyclic Permutation: Let $X = \{x_1, x_2, x_3, \dots, x_n\}$

then a permutation d is called cyclic permutation or cycle of length n if

$$d = \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_2 & x_3 & x_4 & \dots & x_1 \end{pmatrix} \\ = (x_1 x_2 x_3 \dots x_n)$$

eg.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (12345)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} = (1234)(5) \\ = (1234)$$

$$X = \{x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_n\}$$

$$d = \begin{pmatrix} x_1 & x_2 & \dots & x_k & x_{k+1} & \dots & x_n \\ x_2 & x_3 & \dots & x_1 & x_{k+1} & \dots & x_n \end{pmatrix}$$

$$= (x_1 x_2 \dots x_k)$$

$k < n$

Cycle of length k .

Example : Find the lengths of the following cycles:

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

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

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

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

Ans

Example : Find the following product and express it as a product of cyclic permutations on mutually disjoint sets.

$$(14)(235)(35)(45)$$

$$\begin{aligned}
 \text{Sol: } & (14)(235)(35)(45) \\
 &= \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 5 \\ 3 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 2 & 4 \\ 5 & 2 & 4 & 1 \end{pmatrix} = (1524) \quad \underline{\text{Ans}}
 \end{aligned}$$



Example : Find the following product and express it as a product of cyclic permutations on mutually disjoint sets.

$$(124)(13654)$$

Sol:

$$\begin{aligned} & (124)(13654) \\ &= \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 6 & 5 & 4 \\ 3 & 6 & 5 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 6 & 5 & 4 \\ 6 & 5 & 4 & 3 \end{pmatrix} \\ &= (12)(3654) \quad \underline{\text{Ans}} \end{aligned}$$

Example : Express the following permutation as a product of disjoint cycles:

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

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

$$= \begin{pmatrix} 1 & 8 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} 3 & 6 & 4 \\ 6 & 4 & 3 \end{pmatrix} \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix}$$
$$= (18)(364)(57) \quad \underline{\text{Ans}}$$



Example : Express the following permutation as a product of disjoint cycles:

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

Sol:

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 6 \\ 6 & 2 \end{pmatrix} \begin{pmatrix} 5 & 8 & 7 \\ 8 & 7 & 5 \end{pmatrix} \\ &= (134)(26)(587) \text{ Ans} \end{aligned}$$



Theorem: The set S_n of all permutations defined on a set X with n elements is a group under the operation of composition of permutations.

Proof: 1) Closure property:

Let $f, g \in S_n$, then we have to show $f \circ g \in S_n$.

Since $f, g \in S_n$

So $f: X \rightarrow X$, $g: X \rightarrow X$ are bijective functions

Therefore, the composition of two bijective functions is also bijective.

So $f \circ g: X \rightarrow X$ is bijective

$\Rightarrow f \circ g \in S_n$

So the closure property holds.

2) Associative law.

We have to show that

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

$$\begin{aligned} \text{LHS} &= (x) [(f \circ g) \circ h] \\ &= ((x)(f \circ g)) h = ((x)f) g) h \quad \text{--- (1)} \end{aligned}$$

$$\begin{aligned} \text{RHS} &= (x) [f \circ (g \circ h)] = (x)f) (g \circ h) \\ &= ((x)f) g) h \quad \text{--- (2)} \end{aligned}$$

By (1) and (2)

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

3) Identity permutation: $I(x) \in S_n$

$$f \circ I = I \circ f = f$$

$$(x)(f \circ I) = (x)f) I = (x)f \quad \text{--- (a)} \quad I(x) = x$$

$$(x)(I \circ f) = (x)I) f = (x)f \quad \text{--- (b)}$$

$$f \circ I = I \circ f = f$$

verse Permutation:

Let $f \in S_n$, then $f: X \rightarrow X$ is a bijective mapping. Then $f^{-1}: X \rightarrow X$ is also a bijective mapping. $f^{-1} \in S_n$

$$f \circ f^{-1} = f^{-1} \circ f = I$$

$$\begin{aligned} (x)(f \circ f^{-1}) &= (x)f) f^{-1} && \because y = f(x) \\ &= (y) f^{-1} && f^{-1}(y) = x \\ &= x = I(x) \quad \text{--- I} && \because I(x) = x \end{aligned}$$

$$(y)(f^{-1} \circ f) = (y) f^{-1}) f = (x)f = y$$

$$\text{By I \& II} \quad f^{-1} \circ f = f \circ f^{-1} = I \quad \text{--- II}$$

Symmetric Group : The group S_n of all permutations defined on a set X with n elements is called symmetric group of degree n .

$$n=3, \quad S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}, \quad X = \{1, 2, 3\}$$

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

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

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

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

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

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



Theorem: Show that (S_3, \circ) is a non-abelian group.

Proof: We know that S_3 is a group of permutations on a set X with three elements.

$$X = \{1, 2, 3\}$$

All possible permutations on X are

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

$$d_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$d_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$d_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$d_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$d_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We have to show that

$$d_1 d_2 \neq d_2 d_1$$

$$d_1 d_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{--- (1)}$$

$$d_2 d_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{--- (2)}$$

Hence by (1) and (2), $d_1 d_2 \neq d_2 d_1$.

Hence (S_3, \circ) is a non-abelian group.



Theorem : Find all the subgroups of S_3 .

Proof: $X = \{1, 2, 3\}$

All possible permutations on X are

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

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

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

$$\text{where } \alpha^3 = \beta^2 = (\alpha\beta)^2 = (\alpha^2\beta)^2 = I$$

Trivial subgroups of S_3 : I, S_3

Non-trivial subgroups of S_3 :

$$H_1 = \{I, \alpha, \alpha^2\}, \quad H_2 = \{\beta, I\}$$

$$H_3 = \{\alpha^2\beta, I\}, \quad H_4 = \{\alpha\beta, I\}$$

Transposition : A cycle of length 2 is called transposition.

e.g. $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (12)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (45)$$



Theorem: Every cyclic permutation can be expressed as the product of transpositions.

Proof: Suppose we have a cyclic permutation

$$(a_1 a_2 a_3 \dots a_n) \text{ of length } n.$$

We have to show that

$$(a_1 a_2 a_3 \dots a_n) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_n) \quad \text{--- (1)}$$

We prove it by using mathematical induction.

Step I:

$$n=2$$

$$\text{LHS} = (a_1 a_2), \quad \text{RHS} = (a_1 a_2)$$

So it is true for $n=2$.

$$n=3$$

$$\text{LHS} = (a_1 a_2 a_3)$$

$$\text{RHS} = (a_1 a_2)(a_1 a_3)$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_1 & a_3 & \dots & a_n \\ a_3 & a_2 & 1 & \dots & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_3 & a_2 & 1 & \dots & a_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_1 & \dots & a_n \end{pmatrix} = (a_1 a_2 a_3) = \text{LHS}.$$

So it is also for $n=3$.

Step II: Let it be true for $n=k$

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_k) \quad \text{--- (2)}$$

Step III: Now we prove it for $n=k+1$

Consider

$$(a_1 a_2)(a_1 a_3) \dots (a_1 a_k)(a_1 a_{k+1})$$

$$= (a_1 a_2 a_3 \dots a_k)(a_1 a_{k+1})$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{k-1} & a_k & a_{k+1} \\ a_2 & a_3 & a_4 & \dots & a_k & a_1 & a_{k+1} \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \dots & a_k & a_{k+1} \\ a_{k+1} & a_2 & \dots & a_k & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{k-1} & a_k & a_{k+1} \\ a_2 & a_3 & a_4 & \dots & a_k & a_{k+1} & a_1 \end{pmatrix}$$

$$= (a_1 a_2 a_3 \dots a_{k+1}) \text{ Hence it is true for } n=k+1.$$



Theorem : Every permutation of degree n can be expressed as the product of transpositions.

Proof: Since we know that every permutation of degree n can be expressed as the product of disjoint cycles.

We know that every cyclic permutation can be written as the product of transpositions.

Therefore, every permutation of degree n can be expressed as the product of transpositions.

Hence proved.

Example : Express the following permutation as the product of transpositions.

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

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

Ans

Example : Express the following permutation as the product of transpositions.

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

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

Ans

Example : Express the following permutation as the product of transpositions.

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

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

$$= (132564)$$
$$= (13)(12)(15)(16)(14)$$

Ans

Example : Express the following permutation as the product of transpositions.

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

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

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

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

$$= (1\ 2)(1\ 4)(3\ 6)(3\ 5)(7\ 8)(7\ 9) \text{ Ans}$$



Example : Express the following permutation as the product of transpositions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 6 & 2 & 9 & 8 & 3 & 1 & 4 & 5 & 7 \end{pmatrix}$$

$$\begin{aligned} \text{Sol: } & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 6 & 2 & 9 & 8 & 3 & 1 & 4 & 5 & 7 \end{pmatrix} \\ & = \begin{pmatrix} 1 & 10 & 7 \\ 10 & 7 & 1 \end{pmatrix} \begin{pmatrix} 2 & 6 & 3 \\ 6 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 & 9 & 5 \\ 9 & 5 & 8 \end{pmatrix} \\ & = (1 \ 10 \ 7) (2 \ 6 \ 3) (4 \ 9 \ 5 \ 8) \\ & = (1 \ 10) (1 \ 7) (2 \ 6) (2 \ 3) (4 \ 9) (4 \ 5) (4 \ 8) \end{aligned}$$

<https://www.vubio technologist.org>

Even Permutation : A permutation α in S_n is called an even permutation if it can be written as a product of even number of transpositions.

Example :

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

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

Odd Permutation : A permutation α in S_n is called an odd permutation if it can be written as a product of odd number of transpositions.

Example :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 6 & 2 & 9 & 8 & 3 & 1 & 4 & 5 & 7 \end{pmatrix}$$

$$= (1 \ 10)(1 \ 7)(2 \ 6)(2 \ 3)(4 \ 9)(4 \ 5)(4 \ 8)$$

Example : Is the permutation $(1\ 2\ 3)(2\ 5\ 6)(4\ 3\ 5\ 1)$ odd or even ?

$$\text{Sol: } (1\ 2\ 3)(2\ 5\ 6)(4\ 3\ 5\ 1)$$

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

Since there are 7 transpositions,
so the given permutation is an odd
permutation.

Example : Is the permutation $(1\ 4\ 7)(3\ 4\ 5)(8\ 7)(8\ 3\ 4\ 5)$ odd or even ?

Sol: $(1\ 4\ 7)(3\ 4\ 5)(8\ 7)(8\ 3\ 4\ 5)$
 $= (1\ 4)(1\ 7)(3\ 4)(3\ 5)(8\ 7)(8\ 3)(8\ 4)(8\ 5)$

Since these are 8 transpositions, so the given permutation is an even permutation.

Example : Is the permutation $(1\ 2\ 4)(3\ 2\ 5)(6\ 2\ 4\ 5)$ odd or even ?

Sol: $(\underline{1\ 2\ 4})(3\ 2\ 5)(6\ 2\ 4\ 5)$
 $= (1\ 2)(1\ 4)(3\ 2)(3\ 5)(6\ 2)(6\ 4)(6\ 5)$

Since there are 7 transpositions,
so the given permutation is an odd
permutation.

Example : Is the permutation $(1\ 2\ 3\ 4\ 5)(3\ 6\ 5)(2\ 1\ 5)$ odd or even ?

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

Since there are 8 transpositions, so the permutation is an even permutation.

Theorem : The product of two even or two odd permutations is an even permutation.

Proof: Let α and β be two even permutations of length n . Suppose α and β can be expressed as m and p transpositions respectively, then $\alpha\beta$ will contain $m+p-2k$ transpositions, where k is a +ve integer.

Since m , p and $2k$ are even integers, so $m+p-2k$ will also be an even integer.

Let f and g be two odd permutations of length n . Suppose that f & g can be expressed as t and u transpositions respectively, then the product fg will contain $t+u-2k$ transpositions. Hence $t+u-2k$ is an even number, so fg has even transpositions.

Hence the proof.

Q.: The permutation $(1\ 2)(1\ 3)$ is an even permutation.

True



False

<https://www.vubioTechnologist.gq>



Q: The permutation $(\underline{a\ b})(\underline{a\ c})(\underline{a\ d})$ is an even permutation.

True

False ✓

<https://www.vubioTechnologist.gq>

Example: Show that the following permutation is even.

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

Sol.:

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

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

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

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

Since there are 6 transpositions, so it is even.

Order of Permutation : Let α be a permutation. Then the least positive integer m is called order of α if $\alpha^m = I$, where I is an identity permutation.

Example: $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$

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

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

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

$\alpha^3 = I$

So the order of $\alpha = 3$ Ans



Remark : The order of a transposition is 2.

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

$$\beta^2 = \beta \cdot \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

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

$$\beta^2 = I$$

Hence the order of transposition $\beta = 2$ Ans

Theorem : The order of a cyclic permutation of length m is m .

Proof: Let $d = (a_1 a_2 a_3 \dots a_m)$ be a cyclic permutation.

$$d: a_1 \rightarrow a_2, a_2 \rightarrow a_3, \dots, a_m \rightarrow a_1$$

$$d^2: a_1 \rightarrow a_3, a_2 \rightarrow a_4, \dots, a_m \rightarrow a_2$$

$$d^3: a_1 \rightarrow a_4, a_2 \rightarrow a_5, \dots, a_m \rightarrow a_3$$

\vdots

$$d^m: a_1 \rightarrow a_1, a_2 \rightarrow a_2, \dots, a_m \rightarrow a_m$$

$$d^m = I \quad \text{where } I \text{ is identity permutation.}$$

So order of d is m .

Hence the proof.



Example : Find the order of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 1 & 7 & 9 & 6 & 5 & 8 & 12 & 11 & 10 \end{pmatrix}$

Sol:
$$d = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 1 & 7 & 9 & 6 & 5 & 8 & 12 & 11 & 10 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 5 & 7 & 6 & 9 & 8 \\ 7 & 6 & 9 & 8 & 5 \end{pmatrix} \begin{pmatrix} 10 & 12 \\ 12 & 10 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix}$$
$$= \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}}_{d_1} \underbrace{\begin{pmatrix} 5 & 7 & 6 & 9 & 8 \end{pmatrix}}_{d_2} \underbrace{\begin{pmatrix} 10 & 12 \end{pmatrix}}_{d_3}$$

length of $d_1 = 4$

length of $d_2 = 5$

length of $d_3 = 2$

$$\text{LCM}(2, 5, 4) = 20$$

So the order of $d = 20$ Ans

Example : Find the order of

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

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

$$= \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{\alpha_1} \underbrace{\begin{pmatrix} 4 & 5 & 6 \\ 5 & 6 & 4 \end{pmatrix}}_{\alpha_2} = (1\ 2\ 3) (4\ 5\ 6)$$

length of $\alpha_1 = 3$

length of $\alpha_2 = 3$

Order of $\alpha = \text{LCM}(3, 3) = 3$ Ans



Example : Find the order of $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Sol: Let $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}}_{d_1} \underbrace{\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}}_{d_2}$$

length of $d_1 = 2$

length of $d_2 = 2$

order of $\beta = \text{LCM}(2, 2) = 2$ Ans

Example : Find the order of

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

Sol :

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

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

$\underline{\underline{d_1}} \qquad \underline{\underline{d_2}}$

length of $d_1 = 3$

length of $d_2 = 2$

Order of $f = \text{LCM}(2, 3) = 6$ Ans

Example :

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

Show that $f \circ g \neq g \circ f$

Sol:

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

$$\begin{aligned} \text{LHS} = f \circ g &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \text{--- (1)} \end{aligned}$$

$$\begin{aligned} \text{RHS} = g \circ f &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{--- (2)} \end{aligned}$$

By (1) and (2),

$$f \circ g \neq g \circ f$$

Hence proved.



Example : Show by means of an example that the product of two cyclic permutations need not be a cyclic permutation.

Sol: Let $\alpha = (1\ 2\ 5)$, $\beta = (2\ 1\ 4\ 5\ 6)$
be two cyclic permutations.

Then

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

This is not a cyclic permutation.

Hence the product of two cyclic permutations is not a cyclic permutation. Hence proved.



Theorem : Prove that the set A_n of all even permutations in S_n form a subgroup of S_n . Explain why the set B_n of all odd permutations in S_n do not form a subgroup of S_n ?

Proof: Let A_n be the set of all even permutations of S_n . We have to show that A_n is a subgroup of S_n .

Clearly $A_n \subseteq S_n$

Let $\alpha, \beta \in A_n$

$$\left. \begin{array}{l} \alpha, \beta \in A_n \\ \alpha^{-1} \in A_n \end{array} \right\}$$

Since the inverse of even permutation is even permutation.

Therefore, β^{-1} is also an even permutation.

$$\Rightarrow \beta^{-1} \in A_n$$

Since the product of two even permutations is even permutation.

So, $\alpha\beta^{-1}$ is also an even permutation.

Hence $\alpha\beta^{-1} \in A_n$.

So A_n is a subgroup of S_n .

Let B_n be the set of all odd permutations of S_n .

Let $f, g \in B_n$ be two odd permutations.

Since the inverse of odd permutation is $\overline{fg^{-1} \in B_n}$ also an odd permutation.

So g^{-1} is an odd permutation. So $g^{-1} \in B_n$

Since the product of two odd permutations is an even permutation.

So $fg^{-1} \notin B_n$. So B_n is not a subgroup of S_n .

Hence proved.



Example : Given the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$, verify that $\alpha^6 = I$.

Sol: Given
$$\begin{aligned} \alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}}_{\alpha_1} \underbrace{\begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \end{pmatrix}}_{\alpha_2} \end{aligned}$$

length of $\alpha_1 = 2$

length of $\alpha_2 = 3$

Order of $\alpha = \text{LCM}(2, 3)$

$\alpha^6 = I$ Hence proved.



Example : Write (i) all even permutations in S_3
(ii) all odd permutations in S_3

Sol: S_3 is the set of all permutation defined on the set $X = \{1, 2, 3\}$.

All the permutations of S_3 are

$$\checkmark I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3)$$

$$d_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2\ 3)$$

$$d_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)(3)$$

$$\checkmark d_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) = (1\ 2)(1\ 3)$$

$$\checkmark d_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) = (1\ 3)(1\ 2)$$

$$d_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)(2)$$

Since I, d_3, d_4 have even number of transpositions, so I, d_3, d_4 are even permutations.

Since d_1, d_2, d_5 have odd number of transpositions, so d_1, d_2, d_5 are the odd permutations.