⊛ Commutative binary operation

A binary operation is defined on a non empty set S is said to be commutative if $a * b = b * a$, $\forall\ a, b \in S$.

⊛ Associative binary operation

A binary operation $*$, on a set S is said to be associative if $a * (b * c) = (a * b) * c$ $\forall\ a, b, c \in S$.

$a * b = \max(a, b)$	$a \diamond b = a$	$a \diamondsuit b = a^b$
→ Binary operation	→ binary operation	→ binary operation
→ Commutative $a*b = b*a$	→ not comm.	→ not comm.
→ Associative $(a*b)*c = a*(b*c)$	→ asso. $(a \diamond b) \diamond c = a \diamond (b \diamond c)$	→ not asso.

⊛ Let S is a set and $*$ is a binary operation and $n \in N$

Then $a^n = a * a * a \ldots\ldots * a$ (n times)

Hence a^n is defined so only if $*$ is associative.

⊛ $(ab - a - b)$ is commutative but not associative.

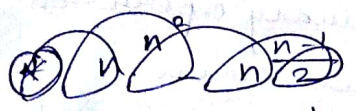
Composition Table / Cayley table

$S = \{a_1, a_2 \ldots\ldots, a_n\}$ $*$ is the binary operation

$*$	a_1	a_2	a_3	.....	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	.....	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	.....	$a_2 * a_n$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	.....	$a_3 * a_n$
⋮					
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	.....	$a_n * a_n$

Ishani Sen

* We can say its commutative, the diagonals will be symmetric
* We can check is binary if each block will fill up and have unique values.
* No. of distinct binary operations on a set of n elements is n^{n^2} (permutation, n^2 cells, n elements)



* $n^{\frac{n^2+n}{2}}$ - no. of distinct binary operations which is commutative.

Identity element (not commutative as only true for particular element)

Let a be a binary operator defined as a set S. Then an element $e \in S$ is said to be the identity element of S under * if, $a * e = a = e * a \quad \forall\, a \in S$

→ $e = 0$, in $\langle R, + \rangle$
$e = 1$, in $\langle R, * \rangle$
$e = I_n$, in $\langle M_{n\times n}, \times \rangle$

→ $S = N = \{1, 2, \dots\}$
$a * b = \max(a, b)$, here $e = 1$ {as max, so we pick smallest element of S}

$a \diamond b = a$, no identity element

$a \diamond b = a^b$, no identity element

Proposition 1 :

The identity element in a set under a specific binary operation is unique. ∴

Proof : Let e_1 and e_2 be 2 distinct identity elements.

a, b
a*a ≠ a*b = b
a, e
e*e

considering e_1 as the identity element, we get

$$e_1 * e_2 = e_2 = e_2 * e_1 \quad \text{—— (1)}$$

Again considering e_2 as the identity element we get,

$$e_1 * e_2 = e_1 = e_2 * e_1 \quad \text{—— (2)}$$

From (1) and (2) since * is a binary operation.

$e_1 = e_2$ ⟶ a contradiction

Hence proved, that there is unique identity element.

Inverse element

Let * be a binary operation, defined on 'a' set S and a is an arbitary element in S. An element 'b' is said to be the inverse of 'a' if $a * b = e = b * a$; $\hookrightarrow \in S$

eg - in $\langle R, + \rangle$, the inverse of 'a' is '-a'.

in $\langle R, \cdot \rangle$, the inverse of $a \neq 0$ is $1/a$.

The inverse of a is denoted as a^{-1}

eg - 2^{-1} in $\langle R, + \rangle = -2$

2^{-1} in $\langle R, \cdot \rangle = 1/2$

- $a^n = a * a * a \ldots$ n times

$a^0 = e \longrightarrow$ axiom

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

Application always depends on operation.

Proposition 1:

Let 'a' be an arbitary element in $\langle S, * \rangle$. Then the inverse of 'a' is unique, where it is associative

let a_1 and a_2 be 2 distinct inverses and a be the inverse.

$$a * a_1 = e = a_1 * a$$

$$a * a_2 = e = a_2 * a$$

$$a * a_1 = a * a_2$$

operating a_1 on both sides

$$a_1 * (a * a_1) = a_1 * (a * a_2)$$

$$(a_1 * a) * a_1 = (a_1 * a) * a_2$$

$$\Rightarrow a_1 = a_2 \longrightarrow \text{contradiction}$$

Hence proved, that there is unique inverse.

Q. $2x = 6$

$$\frac{1}{2}(2x) = \frac{1}{2}(6)$$

$$\left(\frac{1}{2} \cdot 2\right) x = 3$$

$$1 \cdot x = 3$$

$$x = 3$$

~~$G = \langle Z, \cdot \rangle$~~

$a * x = b$ in S

1. $*$ should be a binary operation
2. It should be associative
3. Identity
4. There

$a * x = b$ in S

Group

Let S is a non empty set and $*$ is a binary operation, then S is said to be a group if

1. $*$ is associative
2. There exists the identity element e in S wrt $*$.
3. For every 'a' in S, the inverse of a, i.e, a^{-1}, exists in S.

$\bar{0}$ {... −15, −10, −5, 0, 5, 10, ...}

$\bar{1}$ {... −14, −9, −4, 1, 6, 11 ...}

$\bar{2}$ {... −13, −8, −3, 2, 7, 12}

$\bar{3}$ {... −12, −7, −2, 3, 8, 13}

$\bar{4}$ {... −11, −6, −1, 4, 9, 14}

$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$Z_5 = \{0, 1, 2, 3, 4\}$

Group theory

Groups

$\langle Z, + \rangle$, $\langle M_{m\times n}, + \rangle$
$\langle R - \{0\}, \cdot \times \rangle$
$\langle C, + \rangle$

Non-groups

$\langle Z, - \rangle$, $\langle M_{m\times n}, \times \rangle$
$\langle N, - \rangle$
$\langle O, + \rangle$

(*) If we want to find a group with finite elements, we go out of range. This is due to the closure property.

(*) The smallest group is the identity element of an operator.

eg. (1) $\langle \{1, -1, i, -i\}, \times \rangle$ finite 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

finite group.

(2) $\langle \{1, \omega, \omega^2\}, \times \rangle$

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

Q. Verify that the roots of the equation $x^n = 1$, where n is any natural number forms a multiplicative group.

finite group ③ $\langle Z_5, +_5 \rangle \rightarrow \langle \{0,1,2,3,4\}, +_5 \rangle$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

④ $\langle Z_n, +_n \rangle$ finite (inverse of a will be $n-a$)

Q. ST, $\langle Z_n, +_n \rangle$ forms a group.

$+_n$	0	1	2	3	4	5	...	$(n-1)$
0								
1								
2								
3								
4								
5								
⋮								
$n-1$								

Q. $\langle Z_5 - \{0\}, \times_5 \rangle \rightarrow$ group

Q. $\langle Z_6 - \{0\}, \times_6 \rangle$

$\times_6$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	4	5	6	✗ No closure
3	3	4	5	6	1	✗ Doesn't give inverse for all except 1 and 5.
4	4	5	6	1	2	3
5	5	6	1	2	3	4
6	6	1	2	3	4	5

Q. $\langle Z_7 - \{0\}, \times_7 \rangle$ → group ($1 \to 1$, $2 \to 4$, $3 \to 5$, $4 \to 2$, $5 \to 3$, $6 \to 2$)

Q. $\langle Z_8 - \{0\}, \times_8 \rangle$ → not a group
(• no closure
• inverse only for 1, 3, 5, 7)

Proposition

Let $a \in Z_n$. Then $\gcd(a, n) = 1$ iff 'a' has a multiplicative inverse b, i.e., $ab \equiv 1 \pmod{n}$.

Proof: let $\gcd(a, n) = 1$

$\exists\ r, s \in Z$

$ar + ns = 1$

$\Rightarrow -(ar - ns) = ns$

$\Rightarrow n / (ar - 1)$

$\Rightarrow ar \equiv 1 \pmod{n}$

| $\gcd(a, b) = c$
| $\exists\ r, s \in Z$ •
| $ar + bs = c$

If $x \in \{0, 1, 2, \ldots, (n-1)\}$
then $b = x$, else $b = x \pmod n$

Conversely, let a has a multiplicative inverse b, i.e,
$ab \equiv 1 \pmod n$,

let $c = \gcd(a, n)$

Now $ab \equiv 1 \pmod n$

$\Rightarrow n / (ab - 1)$

$\Rightarrow (ab - 1) = nk$, for $k \in N$.

$\Rightarrow ab - nk = 1$

from this we get, c divides a and n. Hence in eq $ab - nk = 1$, c divides the whole expression and hence it divides 1 too.

$\therefore c = 1$, hence $\gcd(a, n) = 1$.

Proposition: (HW)

$\langle Z_n^*, \times \rangle$ is a group if n is prime.

(• closure
• associative
• inverse)

• A group $a *$ is said to be Abelian (commutative) if the binary operation is commutative.

eg - non commutative group

$\langle M_{n\times n}, \times \rangle$ where M is non singular matrice.

Q. Find / create non-commutative group. (2^{-} - integer)

Proposition 1:

Let G be a group and $a \in G$. Then a^{-1} is unique.

Let a' and a'' be two inverses of a.

$$a * a' = e = a' * a \quad \text{and} \quad a * a'' = e = a'' * a$$

Now,

$a' = a' * e$

$= a + (a + a'')$

$= (a' * a) * a''$ (by associativity)

$= e * a'' = a''$, hence proved.

Proposition 2:

Let G be a group and $a, b \in G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$

Now, $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$ (by associativ

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

$= a * a^{-1} = e$ (where e is the identity)

again,

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

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

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

Hence $(a * b)^{-1} = b^{-1} * a^{-1}$

$\mathbb{Z}, +$
$\mathbb{Q}, +$
$\mathbb{Q}^*, \times$

Proposition 3: Let G be a group and $a, b \in a$. Then $a * x = b$ or $y * a = b$ has unique solution in G for the unknowns x and y. (To prove – solution lies in G and its unique).

Let us consider $a * x = b$.
Then since $a \in G$, a^{-1} exists uniquely in G.

$\therefore a^{-1} * (a * x) = a^{-1} * b$
$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$ (by associativity)
$\Rightarrow e * x = a^{-1} * b$
$\Rightarrow x = a^{-1} * b \in G$ (by closure property)

Since a^{-1} is unique, b is given and $*$ is a binary operation $a^{-1} * b$ is unique and hence even x is unique.

Proposition 4:
Let G be a group and $a, b, c \in G$. Then
(i) $a * b = a * c \Rightarrow b = c$
(ii) $b * a = c * a \Rightarrow b = c$

(i) Since $a \in G$, a^{-1} exists
$\therefore a^{-1} * (a * b) = a^{-1} * (a * c)$
$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ (by associativity)
$\Rightarrow e * b = e * c \Rightarrow b = c$.

Q. Let G be a group and $a \in G$. Then $a * G = G$ where $a * G = \{ag : g < a\}$

To prove $\rightarrow a * G = G$

Let $p \in a * G$, Then $p = ag$, for some $g \in G$.
Since $a, g \in G$ by closure property,
$ag \in G$. $\therefore p \in G$.

This implies that $aG \subseteq G$ ——(1) → improper subset

Now let $g \in G$. Then there exists unique g in G, s.t.

$$g = ag \in aG$$

which implies $a \subseteq aG$ ——(2)

∴ from (1) and (2) we can say that $aG = G$.

finite (repeat cycles)

$1, \omega, \omega^2$

* Let G be a group and $a \in G$, then 'a' is said to be of finite order if there exists atleast 1 integer n, such that, $a^n = e$.
* The smallest positive of all such n's is known as the order of a.
* The order of a is denoted by $O(a)$ or $|a|$.
* If G is finite, then the group G is known as a finite group and the number of elements in G is known as the order of G.

~~Proposition : Let G be a group~~

Theorem : Let G be a group and $a \in G$, Then

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

(ii) if $O(a) = n$ and $a^m = e$ the n is a divisor of m.

(iii) If $O(a) = n$, then $a, a^2, a^3 \ldots a^n (= e)$ are all distinct

(iv) If $O(a) = n$, then $O(a^p) = n$ iff, p is prime to n.

(v) If $O(a)$ is infinite and p is a positive integer, then $O(a^p)$ is infinite.

proof: i) let $o(a) = m$

then $a^m = e \Rightarrow (a^m)^{-1} = e^{-1}$ ——— ①

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

~~let $n < m$, such~~ let $n (\in N) < m$, such that, $(a^{-1})^m = e$.

from ① $a^{-m} = e.e$; $a^{n-m} = e$

$= e$;

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

$a^{m-n} = e^{-1}$ ⟶ contradiction because $o(a) = m$ was ~~stated~~ assumed. Hence m cannot be the order of a as there exists a smaller positive integer than m.

$\therefore o(a) = n$

ii) By division algorithm

$m = nq + r$, for some $q, r \in Z$ and $0 \leq r \leq (n-1)$

now, $a^m = a^{nq+r}$

$\Rightarrow e = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = (e)^q \cdot a^r = a^r$

$\Rightarrow a^r = e$

~~situations $r = 0$~~

~~$1 < r < n-1$~~

which implies $r = 0$, otherwise there will be a contradiction to the fact that $o(a) = n$.

$m = nq$

$\Rightarrow n$ divides m.

(iii) let $a^i = a^j$ for some $i, j \leq n$ and $i > j$.

Then $a^i = a^j$

$\Rightarrow a^{i-j} = e$, the identity in a

Since $(i-j) < n$ and $i > j$, this gives a contradiction that $O(a) = n$. Then the assumption is wrong and $a, a^2, a^3, \ldots a^n$ are distinct

Subgroup

Let G be a group and $H \subset G$. H is said to be a subgroup of G, if H itself is a group under the same binary operation as that of G.

⊛ $G = \langle R, + \rangle$, $H = \langle \mathbb{Q}, + \rangle$ → H is a subgroup of G.

* $G = \langle R, + \rangle$, $H = \langle \mathbb{Q}^*, \times \rangle$ H is a subset of G but not subgroup as different binary operations

Proposition:

Let H be a subgroup of a group G. Then prove that,

(i) The identity element in G and H are same.

(ii) for an element $a \in H$, the inverse of a in H is same is the inverse of a in G.

Proof: Let e_G and e_H be the identity element in G and H respectively. Let $e \in H \subset G$

$$h e_H = h = e_H h.$$

$$h e_G = h = e_G h$$

which implies $h e_H = h e_h$

$$\therefore e_H = e_G$$

(ii) Let the inverse of G and H ~~be expressed~~ h' and h'' respectively.

(iii) Let G and H have different inverses h_1' and h_2'

$$h h_1' = e_G$$
$$h h_2' = e_H$$

Since $e_G = e_H$

$$h h_1' = h h_2'$$
$$h_1' = h_2', \text{ hence proved.}$$

imp

Theorem: Let H be a subset of G, which is a group. Then H is a subgroup iff $\forall a, b \in H$, $ab^{-1} \in H$.

Proof: let H is a subgroup of G and $a, b \in H$. Then $ab^{-1} \in H$ and hence by closure property $a \in H$, $b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Conversely, let $a, b \in H \Rightarrow ab^{-1} \in H$.

→ Since, $a \in H$, $aa^{-1} \in H$, i.e, $e \in H$ hence identity element exists.

→ $e \in H$ and let $a \in H$. Then according to the assumption $ea^{-1} \in H$, i.e, $a^{-1} \in H$. Hence inverse exists.

→ For any element a, b, let $a, b \in H$. Then $b^{-1} \in H$. i.e, $a, b^{-1} \in H$.

Therefore according to the assumption, $(ab^{-1})^{-1} \in H$, i.e $ab \in H$. ∴ H is closed and hence the closure property holds.

Since $H \subset G$, which is a group, the associativity is inherited. Therefore, H is also a group under the same binary operation as that of G. And as $H \subset G$, it also is a subgroup of G.

Cyclic Groups

1. $\langle G = \{\cdots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \cdots\}, \cdot \rangle$

   $\langle G = \{(\frac{1}{2})^n : n \in \mathbb{Z}\}, \cdot \rangle$

   $\langle G = \{(2)^n : n \in \mathbb{Z}\}, \cdot \rangle$

2. $\langle \mathbb{Z}, + \rangle = \langle \mathbb{Z} = (1)^n, n \in \mathbb{Z}^+$

   $1^n = n, \quad n \in \mathbb{Z}^+$

   $1^0 = 0$

   $1^{-n} = -n, \quad n \in \mathbb{Z}^+$

   $1^{-5} = (1)^5 = (-1)^5 = -5$

Proposition: Let G be a cyclic group generated by a i.e. $G = \langle a \rangle$. Then a^{-1} is also a generator of G.

Proof Let $H = \langle a^{-1} \rangle$

Let $\phi \in G$. Then $p = a^k$ for some $k \in \mathbb{Z}$

$\therefore p = a^k = (a^{-1})^{-k}$

$= (a^{-1})^{\ell} \in H$ [where $\ell = -k \in \mathbb{Z}$]

$\therefore G \subseteq H$ —— (1)

Now let $a \in H$, Then $a = (a^{-1})^m$ for some $m \in \mathbb{Z}$

$\therefore a = (a^{-1})^m = a^{-m} = a^n \in G$ (where $n = -m \in \mathbb{Z}$)

$\therefore H \subseteq G$ —— (2)

Proposition: Every cyclic group is abelian.

Proof: Let $G = \langle a \rangle$

Then $p = a^m$, $q = a^n$ for some $m, n \in \mathbb{Z}$

Then $pq = a^m a^n = a^{m+n}$
$= a^{n+m} = a^n a^m = qp$

Since p and q had been chosen arbitrary, the result follows.

Proposition: Let $G = \langle a \rangle$; Then $O(G) = n$, iff $O(a) = n$
↳ generator

$G = \{1, -1, i, -i\}$
↳ generator
$G = \langle i \rangle$

$i^4 = 1$, $O(i) = 4$ | $O(G) = 4$.

Proof: Let $O(a) = n$

i.e, $a, a^2, a^3, \ldots, a^{n-1}, a^n (= e)$ are all distinct

$\therefore \{a, a^2, \ldots, a^{n-1}, e\} \subseteq G$ —— (1)

Let $p = a^m \in G$; $m \in \mathbb{Z}^+$

Then by division algo, $m = nq + r$, $0 \leq r \leq n-1$

$\therefore a^m = a^{nq+r}$
$= (a^n)^q a^r = a^r$

i.e, $a^m \in \{a, a^2, a^3 \ldots a^{n-1}, e\}$

$\therefore G \subseteq \{a, a^2, \ldots, a^{n-1}, e\}$ —— (2)

∴ From ① & ②

$\{a, a^2, \ldots, a^{n-1}, e\} = G$

Hence $O(G) = n$.

Conversely let $O(G) = n$.

let $O(a) = k$,

i.e → $\{a, a^2, \ldots, a^{k-1}, e\}$ are all distinct and $k \leq n$ (due to closure).

Then by the forgoing argument,

$O(G) = k$ → which is a contradiction.

as $O(a) = k \Rightarrow O(a) = n$

hence $k = n$

Proposition: A subgroup of a cyclic group is cyclic.

G → cyclic

H → subgroup.

let g be generator → $G = \{g^n : n \in Z\}$

k is such an integer that $g^k \in H$

then $H = \{e\}$, which is cyclic group.

---

let H be a subgroup of G.

If $H = \{e\}$, $H = \langle e \rangle$ — cyclic

$H \neq \{e\}$, then $a^n \in H$ for some $n \in Z^+$.

let m be smallest int in Z, $a^m \in H$.

$c = a^m$ generates H.

$H \supseteq \langle a^m \rangle = \langle c \rangle$

Proposition: A subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ and $H \leq G$

Case 1: if $H = \{e\}$. Then the proposition is obvious as $a^n = e$.

Case 2: Let H is a proper subgroup of a and $x(\neq e) \in H \subset G$, i.e., $x = a^k$, for some $k \in \mathbb{Z}$. Since H is a subgroup, $x^{-1} \in H$, i.e., $x^{-1} = a^{-k} \in H$

$\therefore$ H contains some integral power of a.

Then by well ordering principle in $\mathbb{Z}$, we can find a least positive $m \in \mathbb{Z}$. Since that $a^m \in H$.

↓ to prove a^m is a generator

Let $p \in H \subset G$. Then $p = a^k$, for some $l \in \mathbb{Z}$,

$\therefore$ by division algorithm

$$l = mq + r \quad \rightarrow 0 \leq r \leq m-1$$

$$\therefore a^l = a^{mq} \cdot a^r = (a^m)^q a^r$$

Therefore $a^r = a^l a^{-mq} = a^{l-mq} \in H$

Such that $r = 0$, otherwise this is a contradiction that m is s.t $a^m \in H$

$$\therefore l = mq$$

$$\therefore p = a^l = (a^m)^q, \quad q \in \mathbb{Z}$$

Since p has been chosen arbitarly, it proves that, any element in H can be expressed as $(a^m)^n$ for some n in $\mathbb{Z}$. Therefore H is a cyclic group, generated by a^m. Hence proved.

Proposition: A cyclic group of prime order has no proper non-trivial subgroup.

↳ trivial subgroup ↳ group itself ↳ identity.

~~Proof by contradiction.~~

Let $O(G) = p$ and $G = \langle a \rangle$

$\therefore a^p = e$, where e is the identity in G.

Let, H is a proper non trivial cyclic subgroup of G, such that $H = \langle a^m \rangle$, where m is the least positive integer, such that $a^m \in H$.

(a^m generates H and a^p lies in H)

Now $e = a^p \in H$

then $a^p = (a^m)^n$, for some $n \in \mathbb{Z}$.

$\Rightarrow p = m \cdot n$

It's a contradiction to the fact that p is prime.

Hence no such H exists.

Permutation

Let S be a non-empty finite set, a bijective (one to one & onto) mapping f from $S \to S$, is said to be a permutation on S.

$f : S \to S$

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

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \cdots & f(a_n) \end{pmatrix}$$

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

$$f_1 = \begin{Bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{Bmatrix}$$

$$f_2 = \begin{Bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{Bmatrix}$$

$$f_3 = \begin{Bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{Bmatrix}$$

3 permutations.

S_n (contains all permutations in S)

Product / Composition :

let $f, g \in S_n$, then

$f \circ g$ / fg is defined as, $fog(u) / fg(u) = f(g(u))$

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

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

$fg(1) = f(g(1)) = f(2) = 1$

$fg(2) = f(g(2)) = f(1) = 3$

$fg(3) = f(g(3)) = f(3) = 2$

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

This is a binary operation as it follows closure property.

$\langle S_n, \circ \rangle$

↓

Symmetric group / permutation group.

$gf(1) = g(f(1)) = g(3) = 3$

$gf(2) = g(f(2)) = g(1) = 2$

$gf(3) = g(f(3)) = g(2) = 1$

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

* eg of a finite group which is non-abelian (non commutative)

$fg \neq gf$.

Inverse

Let $f \in S_n$, and $f : a_i \to a_j$. Then, the inverse of f denoted as f^{-1} is defined as $f^{-1} : a_j \to a_i$.

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

$ff^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \to$ identity $= f^{-1}f$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Longleftrightarrow (1,2,3) \rightarrow$ cyclic

∴ cyclic can be generalised -

$P(a_1) = a_2$, $P(a_2) = a_3$, $P(a_3) = a_4$ ... $P(a_n) = a_1$

$\hookrightarrow (a_1, a_2, a_3 \ldots, a_n) \Leftrightarrow \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$

called an n-cycle.

→ Let $S = \{a_1, a_2 \ldots a_n\}$, a permutation σ in S_n, is said to be a cycle of length r or an r-cycle if there are r elements denoted as $\{a_{i_1}, a_{i_2} \ldots a_{i_r}\}$ such that $\sigma(a_{i_1}) = a_{i_2}$, $\sigma(a_{i_2}) = a_{i_3}$ ... $\sigma(a_{i_r}) = a_{i_1}$ and $\sigma(a_j) = a_j$, $\forall j \notin \{i_1, i_2, \ldots, i_r\}$.

↳ this also can be called a cycle $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

* eg - S_5, $(1\ 2\ 3) \rightarrow$ 3-cycle

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

* eg - identity mapping is a 1-cycle

Imp

Proposition : Every permutation is either a cycle or can be expressed as a product of disjoint cycles.

Proof: let $S = \{a_1, a_2, \ldots, a_n\}$ be a permutation on S. Let φ be a permutation on S. Let us consider the elements $\{a_1, \varphi(a_1), \varphi^2(a_1), \ldots \text{etc}\}$; all these cannot be distinct since all of them belong to S and S is a finite set.

Let r be the least positive integer such that

$$\varphi^r(a_1) = a_1 .$$

Then, $a_1, \varphi(a_1), \varphi^2(a_1), \varphi^3(a_1), \ldots \varphi^{r-1}(a_1)$ are all distinct.

Otherwise, for some p, q, such that $0 < p < q < r$,

$$\varphi^p(a_1) = \varphi^q(a_1)$$

$$\Rightarrow \varphi^{p-q}(a_1) = a_1 \longrightarrow$$ this is a contradiction to the statement that r is the least positive element such that, $\varphi^r(a_1) = a_1$.

Hence all are distinct elements of S.

$\therefore$ we get a r-cycle, φ_1, which can be written as,

$$\varphi_1 = (a_1, \varphi(a_1), \varphi^2(a_1) \ldots \varphi^{r-1}(a_1))$$

if $r = n$, theorem proved.

Otherwise, let $a_m \in S$ such that it doesn't belong to φ_1.

and find $\varphi(a_m), \varphi^2(a_m) \ldots$ etc

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

$$\varphi_1 = \begin{pmatrix} a_1 & \varphi(a_1) & \varphi^2(a_1) \\ 1 & 3 & 2 \end{pmatrix}$$

$$\varphi_2 = (4, 5)$$

None of this belongs to row 1, because otherwise $\varphi^i(a_m) = \varphi^j(a_i)$, which implies $\varphi^{j-1}(a_i) = a_m$. This is a contradiction as we said a_m doesn't belong to ρ_1.

And certainly the process of finding $\varphi(a_m)$, $\varphi^2(a_m)$, etc. . . will stop as at some point it will yield a_m, since S is a finite set, giving us another cycle s_1.

Let us name the cycle s_1 as ρ_2.

if $r + s_1 = n$, then theorem is proved and hence $\varphi_2 = \rho_1 \rho_2$.

Otherwise we can repeat the process for finite number of times and obtain disjoint cycles $\rho_1, \rho_2 \ldots \rho_n$, such that $\varphi = \rho_1 \rho_2 \rho_3 \ldots \rho_n$.

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

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

* Cycle of length 2 is a transposition. Any cycle can be written as a product of a transposition.

$\rho(a_1, a_2, a_3)$

$\rho_1 = (a_1, a_3) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$

$\rho_2 = (a_1, a_2) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$

$\rho_1 \circ \rho_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} = (a_1, a_2, a_3)$

$\Rightarrow \rho = (a_1, a_2, a_3 \ldots\ldots, a_n)$

then

$\rho = (a_1, a_n) \circ (a_1, a_{n-1}) \circ (a_1, a_{n-2}) \cdots \circ (a_1, a_2)$

If the number of such transpositions are even, the permutation is called even permutation. and if no. of transpositions are odd, they are called odd permutation.

Q. Find out $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$ is odd or even.

$\Rightarrow (1\ 3)(4\ 5\ 6\ 8)$

$\Rightarrow (1,3)(4,8)(4,6)(4,5)$ $\longrightarrow$ 4 transposition

$\longrightarrow$ even.

identity can be also written as the product of transpositions.

$(a_r, a_s)(a_s, a_r)$

eg- $S_8 = \{1, 2, 3, 4, 5, 6, 7, 8\}$ $i = (1\ 2)(1\ 2)$ or $(3\ 6)(3\ 6)$ or $(4\ 8)(4\ 8)$