:- Unit - 2 :-

Modern Algebra

* **Algebric Structure $(S, *)$:-** A algebric structure consists of a set and a binary operations $(S, *)$.

* **Properties :-**

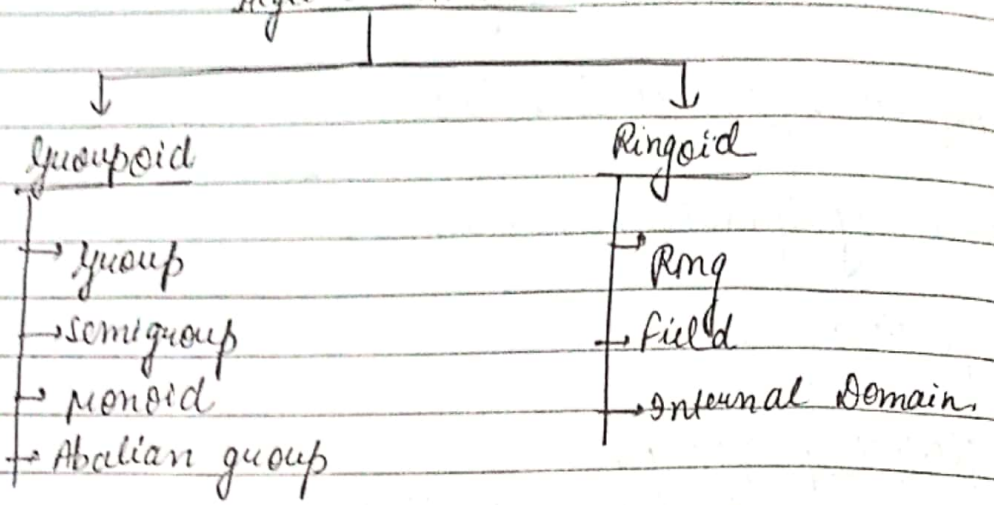
(i) **Closure property :**
In an algebric structure $(S, *)$
let $a, b \in S$.
If $a * b = c \in S$.
then $(S, *)$ holds closure law.

(ii) **Associative law :-**
In an algebric structure $(S, *)$
Let $a, b, c \in S$.
If $a * (b * c) = (a * b) * c$. then
$(S, *)$ holds associative law.

(iii) **Existence of identity :-**
In an algebric structure $(S, *)$, let $a, e \in S$
If $a * e = a$, then 'e' is the identity of $(S, *)$.

(iv) **Existence of inverse :-**
In an algebric structure $(S, *)$, let $a, b, e \in S$.
If $a * b = e$, then a & b are inverse of each other.

(v) **Commutative law :-**
In an algebric structure $(S, *)$, let $a, b \in S$,
If $a * b = b * a$ then $(S, *)$ holds commutative law.



1. Groupoid :-

(a) Group: An algebraic structure is said to be a group if it holds closure, associative, existence of identity and existence of inverse properties.

(b) Semigroup:- An algebric structure is said to be a semi-group if it holds closure and associative law.

(c) Monoid :- An algebric structure is said to be a monoid if it holds closure property, associative law and existence of ~~inverse~~ identity.

(d) Abelian group :- A group which holds a commutative property.

Eg: Let the operation '*' be defined on the set of integers as; $a * b = a + b + 2$ for all $a, b \in Z$.

Show that $(Z, *)$ is an abelian group.

(d) $(Z, *)$

$a * b = a + b + 2$

$\forall a, b \in Z$

① Closure law: In $(S, *)$,

If $a * b = c \in S$, $\forall a, b, c \in S$

In $(Z, *)$

Let $a, b \in Z$

$a * b = a + b + 2$

Addition of integers is also an integer

Hence $(Z, *)$ holds closure law.

② Associative law: In $(S, *)$,

$a * (b * c) = (a * b) * c$.

$\forall a, b, c \in S$

Let $a, b, c \in Z$.

$a * (b * c) = (a * b) * c$

$a * (b + c + 2) = (a + b + 2) * c$

$a + b + c + 4 = a + b + c + 4$

LHS = RHS ∴ It satisfies this law also.

③ Existence of Identity: $a * e = a$, $\forall a, e \in S$

Let $a, e \in Z$.

$a * e = a$

$a + e + 2 = a$

$\boxed{e = -2}$

④ Existence of inverse:

$a * b = e$ $\forall a, b, e \in S$.

Let $a, b, e \in Z$

$a * b = e$

$a + b + 2 = -2$ $\Rightarrow$ $\boxed{b = -4 - a}$

MARUTI

3) commutative law: $a * b = b * a \quad \forall\ a, b \in S$.

Let $a, b \in Z$

$a * b = b * a$

$a + b + 2 = b + a + 2$

As addition satisfies commutative prop.

$\therefore a + b = b + a$,

$\therefore$ LHS = RHS.

So (Z, *) is an abelian group.

Ex: Let $G = \{(a, b) \mid a, b \in R, a \neq 0\}$ define a binary operation '*' on G by $(a, b) * (c, d) = (ac, bc + d)$ $\forall\ (a, b), (c, d) \in G$. Show that (G, *) is a group and find if it is abelian also.

Sol: (1) closure law: Let $a, b, c, d \in R$

$(a, b) * (c, d) = (ac, bc + d)$

as a and c both $\in R$ $\therefore$ their product will also $\in R$.

similarly as $b, c, d \in R$ $\therefore$ product of bc and adding it with d will also $\in R$.

$\therefore$ It holds closure law.

(2) Associative law: In (S, *)

$(a, b) * ((c, d) * (e, f)) = ((a, b) * (c, d)) * (e, f)$

LHS

$= (a, b) * (ce, de + f)$

$= (ace, bde + bf)$

$= (ace, bce + de + f)$

RHS

$= (ac, bc + d) * (e, f)$

$= (ace, bce + de + f)$

MARUTI

$\therefore$ LHS = RHS.

$\therefore$ $(S, *)$ holds associative law also.

(3) Existence of Identity: In $(S, *)$,

$(a,b) * (e,f) = (a,b)$

$(ae, be+f) = (a,b)$

$\therefore$ $\boxed{e = 1}$, $\boxed{f = a}$

$(1, 0)$ = Identity //

(4) Existence of Inverse :-

~~$(a,b) * (e,f) = (g,h)$~~

~~$(ae, be+f)$~~

$(a,b) * (c,d) = (e,f)$

$(ac, bc+d) = (e,f)$

$ac = e$ | $bc + d = f$

$c = 1/a$ | $\frac{b}{a} + d = 0$

$\boxed{d = -\frac{b}{a}}$

(5)

Q) (i) $(z^+, *)$

$x * y = xy$

(ii) $(z^+, *)$

$x * y = y$

(iii) $(z^+, *)$ monoid

$x * y = x + y + xy$

(iv) $(z^+, *)$

$x * y = gcd(x, y)$

(v) $(z^+, *)$

$x + y = \max(x, y)$

Sol)

(i) $(z^+, *)$, $x * y = xy$

Closure law:- $gn(S, *)$, $gn(z^+, *)$

Let $x, y \in z^+$

$x * y = xy$

as x and y are two +ve integers, so their product will also be a +ve integer which belongs to our range.

∴ It holds closure law.

Associative law:- $gn(S, *)$, $gn(z^+, *)$

Let $x, y, z \in z^+$.

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

LHS $= x * (yz)$

$\rightarrow xyz$

RHS $= (xy) * z$

$\rightarrow xyz$

∴ LHS = RHS.

∴ It also holds Associative law also.

Existence of Identity: In $(S, +)$, In $(Z^+, *)$

$$x * e = x$$
$$xe = x$$
$$\boxed{e = 1}$$

Existence of Inverse:

$$x + y = e$$
$$xy = 1$$
$$x = \frac{1}{y}$$

If $y = 2$, $\boxed{x = \frac{1}{2}} \notin Z^+$

∴ Inverse not exists.

∴ ~~$\in Z^*$~~ This algebric structure is a monoid.

(ii) $(Z^+, *)$, $x * y = x + y + 2y$

Closure law: In $(Z^+, *)$.

Let $x, y \in Z^+$

$x * y = xy$

Since $y \in Z^+$ hence it holds closure law.

Associative law: In $(Z^+, *)$

Let $x, y, z \in Z^+$

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

LHS:	RHS:
$x * yz$	$y * z$
xyz	yz

LHS = RHS

Existence of Identity:

$$x * e = x$$

$$\boxed{e = x}$$

So everytime identity is changing hence it does not have identity.

∴ The structure is semi group.

3) $(z^+, *)$, $x * y = x + y + 2y$

Closure law: In $(z^+, *)$;

$$x * y = x + y + xy.$$

Since $x + y + xy \in z^+$ As x, y are $\in z^+$

∴ closure law (✓).

Associative law: In $(z^+, *)$;

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

LHS $x * (y + z + 2z) = (x + y + z)$

$x + y + z + 2z + 2(y + z + 2z)$

RHS $(x + y + 2y) * z = x + y + 2y + z + 2z$

LHS: $x * (y + z + yz)$

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

$\rightarrow x + y + z + xy + yz + zx + xyz$

RHS : $(x+y+xy)*z$

$\rightarrow x+y+xy+z+(x+y+xy)z$

$= x+y+z+xy+zx+zy+xyz$

$\therefore$ LHS = RHS

$\therefore$ It is ~~a~~ semi-group. It satisfies the associative law.

Existence of Identity :-

$x * e = x$

$x+e+xe = x$

$e(1+x) = 0$

$e = 0$

existence of inverse :-

$x * y = e$

$x+y+xy = e$

$x+y+xy = 0$

$y(1+x) = -x$

$y = \frac{-x}{1+x}$

$\therefore$ inverse not exists. $(\notin z^+)$

$\therefore$ It is a monoid.

4) $(Z^+, *)$

$$x * y = \gcd(x, y)$$

Closure law:

$$x * y = \gcd(x, y)$$

since $x, y \in Z^+$ therefore their gcd will also be Z^+.

Ans. so it holds closure law.

associative law:

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

LHS:

$\Rightarrow x * (\gcd(y, z))$

$\Rightarrow \gcd(x, \gcd(y, z))$

RHS

$\Rightarrow \gcd(\gcd(x, y), z)$

$\Rightarrow \gcd(\gcd(x, y), z)$

same //

$5+5=10 \% 6 = 4$
$2 \cdot 1 \cdot 6 = 1$

$+_n$ X_n

$(\{0,1,2,3,4,5\}, +_6)$

$0+0 \cdot 1 \cdot 6$
$0+1 \cdot 1 \cdot 6 \to 1$

$x * e = x$
$x + e = x$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$0 +_6 (1 +_6 4)$
$= (0 +_6 1) +_6 4$
$5 = 5$
$=$

$(\{0,1,2,3,4,5\}, \times_6)$

Theorems - the identity element (if it exists) of any algebraic structure is unique.

$(S, *)$
let $e_1, e_2 \in S$
let e_1 is the identity
$e_1 * e_2 = e_2$ — (1)
Let e_2 is the identity
$e_1 * e_2 = e_1$ — (2)

$\boxed{e_1 = e_2}$

Theorems:- For any algebraic structure, the inverse of any element is unique (if it exists)

$(S, *)$

Let $a, b_1, b_2, e \in S$

Let b_1 is the inverse;

$a * b_1 = e$ — (1)

Let b_2 is the inverse;

$a * b_2 = e$ — (2)

$a * b_1 = a * b_2$ ⟶ using left cancellation law.

$\Rightarrow \boxed{b_1 = b_2}$

Theorems In a group $G(G, *)$

1. $(a^{-1})^{-1} = a$ i.e., the inverse of the inverse of an element is equal to the element.
2. $(a*b)^{-1} = b^{-1} * a^{-1}$

Proof 1. Let $a, a^{-1}, (a^{-1})^{-1}, e \in G$

Now, $a * a^{-1} = e$ — (1)

and $(a^{-1})^{-1} * a^{-1} = e$ — (2)

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

using RCL

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

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

Let $a, b, a^{-1}, b^{-1}, e \in G$

Since $a * b \in G$ ——— WM closure law

$(a*b) * (a*b)^{-1} = e$ — (1)

$(a * a^{-1}) * (b * b^{-1}) = e$ — (2)

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

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

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

using LCL

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

Theorem: Show that if a & b be arbitary elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Proof;

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

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

using associative law

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

using LCL;

$(ba)b = (ab)b$

using RCL;

$ba = ab$ H.P

$ab = ba$

binary operatry a both sides.

$a(ab) = a(ba)$

binary operatry b both sides

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

using associative law;

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

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

Ex: Show that if $a^2 = a$ then $a = e$, a, b belong an element of a group.

Sol:

If $a^2 = a$ then $a = e$

$a \cdot a = a$ — (1)

$a \cdot e = a$ — (2)

$a \cdot a = a \cdot e$

using LCL;

$\boxed{a = e}$

★ Order of an element and order of a group:-

The order of an element (g) in a group 'G' is the smallest +ve integer 'n' such that $\boxed{g^n = e}$. If no such integer exists, we say g has infinite order.

The no. of elements presented in a group is called order of a group.

$I = (\{1, -1, i, -i\}, \times)$

$O(i) = 4$ ..., $O(1) = 1$

★ cyclic group :-

A group $(G, *)$ is said to be cyclic if all the elements of G can be generated with a specific element of group 'G'. That specific element is known as generator of a group.

$I = (\{1, -1, i, -i\}, \times)$

$(i)^4 = 1$	$(i)^2 = -1$	$(-i)^2 = 1$	$(-i)^3 = i$
$(i)^3 = -i$	$(i)^1 = i$	$(-i)^4 = -1$	$(-i)^2 = (-i)$

$\Rightarrow \langle i \rangle \langle -i \rangle$ are generators.

ex: $(G, +_6)$ where $G = \{0, 1, 2, 3, 4, 5\}$

$(5)^2 = 5 +_6 5 = 4$
$(5)^3 = 3$
$(5)^4 = 2$
$(5)^5 = 1$
$(5)^6 = 0$
$(5)^7 = 5$

$\langle 5 \rangle \langle 1 \rangle$ are ~~generating~~ ~~for~~ generators.

Theorem: Every cyclic group is an abelian group

$(G, *)$

Let $\langle a \rangle$ where $a \in G$

$y = \langle a \rangle = \{a^n : n \in Z\}$

Let $g_1 = a^r$ and $g_2 = a^s$

$g_1 * g_2 = a^r . a^s$

$= a^{r+s}$

$= a^{s+r}$ [because $+$ is commutative]

$= a^s . a^r$

$= g_2 . g_1$.

Sub-groups :-

$(G, *) \longrightarrow (H, *)$ ← It is a sub group of a group G if it also satisfies all four properties.

~~{1}~~ ex: $(\{1, -1, i, -i\}, \times)$

$(\{1\}, \times)$ ✓
$(\{i\}, \times)$ ×
$(\{-i\}, \times)$ ×
$(\{-1\}, \times)$ ×
$(\{1, -1\}, \times)$ ✓
$(\{1, i\}, \times)$ ×
$(\{1, -i\}, \times)$ ×
$(\{-1, i\}, \times)$ ×
$(\{-1, -i\}, \times)$ ×
$(\{i, -i\}, \times)$ ×

$(\{1, -1, i\}, \times)$ ×
$(\{1, -1, -i\}, \times)$ ×
$(\{1, i, -i\}, \times)$ ✓
$(\{-1, i, -i\}, \times)$ ×
$(\{1, -1, i, -i\}, \times)$ ✓

ex: $(\{1, \omega, \omega^2\}, \times)$ $\omega \cdot (e) = \omega$

$(\{1\}, \times)$ ✓
$(\{\omega\}, \times)$ ×
$(\{\omega^2\}, \times)$ ×
$(\{1, \omega\}, \times)$ ×
$(\{1, \omega^2\}, \times)$ ×
$(\{\omega, \omega^2\}, \times)$ ×
$(\{1, \omega, \omega^2\}, \times)$ ✓

* Necessary condition for a sub group :-

In $(G, *)$, ~~let~~ if $a, b \in G$ and $a, b \in H$ and $(H, *)$ and $a * b^{-1} \in H$.
then $(H, *)$ is a sub group of $(G, *)$

Theorem: The intersection of any two subgroups of a group $(G, *)$ is also a sub-group but the union of any two sub-groups of a group is not necessarily a sub-group.

Let $(G, *)$

$H_1 \subseteq G_1$ and $H_2 \subseteq G_1$

$(H_1, *)$, $(H_2, *)$ are two subgroups of $(G, *)$

$H_1 \cap H_2 \neq \phi$ because identity must be there

Let $a, b \in H_1 \cap H_2$

$a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

$a \in H_1$ and $a \in H_2$

$b \in H_1$ and $b \in H_2$

$b^{-1} \in H_1$ and $b^{-1} \in H_2$ (as H_1, H_2 are subgroups ~~to inverse of element~~ should be present)

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

$\Rightarrow \underline{a * b^{-1} \in H_1 \cap H_2}$

$(H_1 \cap H_2, *)$ is also a subgroup.

Let $(Z, +)$ be a group.

$2Z \subseteq Z$

$3Z \subseteq Z$

$(2Z, +)$, $(3Z, +)$ are two sub-groups.

union $\Rightarrow (\{\ldots, -9, -8, -6, -4, -3, -2, 0, 2, 3, 4, 6, 8, 9 \ldots\}, +)$

Now by applying closure law on 2 and 3.

$\Rightarrow 2 * 3 = 5$

and 5 is not present in set.

∴ closure law is not satisfied.

∴ the union of two subsets is not a subgroup

Theorem: The identity element of a sub-group is same as that of a group.

Let $(G, *)$ is a group. and $(H, *)$ is its subgroup

Let $a, e \in G$ and $a, e' \in H$.

$a * e = a$ — (1) $\quad a * e' = a$ — (2)

By equating (1) & (2)

$a * e = a * e'$

using LCL; $\boxed{e = e'}$

★ Cosets :-

Let $(G, *)$ be a group and $H \subseteq G$.

Let $(H, *)$ is also a sub-group.

$H = \{h_1, h_2, h_3 \text{ ---- } h_n\}$

Let $a \in G$.

$a * H = \{a * h_1, a * h_2, a * h_3, \text{ ---- }, a * h_n\}$

It is a coset of $(H, *)$

★ Index of a sub group in a group G :—

If H is a sub group of G, then the no. of distinct right or left cosets of H in G

Date
Page
MARUTI

is called the index of H in G and is denoted by $[G:H]$ or $i_G(H)$

Q: Let G be the additive group of integers and $(3z, +)$ is the subgroup of $(z, +)$ then find the index of $(3z, +)$

Sol) $(z, +) = (\{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}, +)$

$(3z, +) = (\{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}, +)$

$0+3z = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$
$1+3z = \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}$
$2+3z = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$
$3+3z =$
$4+3z =$

So there are only 3 distinct ~~sub groups~~ cosets are possible in this case.

$(0+3z) \cup (1+3z) \cup (2+3z) = z$

$$i_G(3z, +) = 3$$

* Lagrange's theorem :-

The order of each subgroup of a finite group G is a divisor of the order of the group G.

$(G, *)$
$O(G) = n$

$H \subseteq G$
$(H, *)$ $O(H) = m$ $\quad i.e. \; m = \frac{n}{m}$

Let $H = \{h_1, h_2, h_3, \ldots, h_m\}$

$a_1 * H = \{a_1 * h_1, a_1 * h_2, a_1 * h_3, \ldots, a_1 * h_m\}$

$a_2 * H = \{a_2 * h_1, a_2 * h_2, a_2 * h_3, \ldots, a_2 * h_m\}$

$\vdots$

$a_k * H = \{a_k * h_1, a_k * h_2, a_k * h_3, \ldots, a_k * h_m\}$

k distinct cosets

Union = G

Each coset have m elements.

$\therefore \quad k \times m = n$

$\Rightarrow$ m divides n. n.P.

☆ Isomorphism

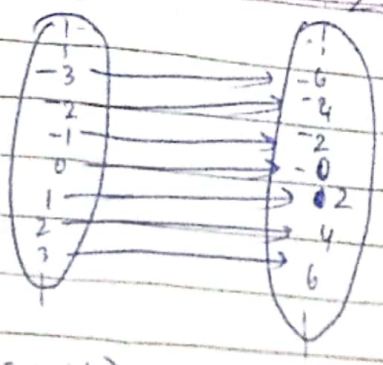
If $(S, *_1)$ & $(T, *_2)$ be two algebric structures

A function $f : S \to T$ is called an isomorphism from $(S, *_1)$ to $(T, *_2)$ if it is one to one correspondence from S to T, and if $f(a *_1 b) = f(a) *_2 f(b)$

Ex: Let $(Z, +)$ and $(T, +)$ are two groups where T is set of all even integers and $f(a) = 2a$. Find whether $(Z, +)$ and $(T, +)$ are isomaphic to each other or not.

Sol: $f(a) = 2a$

$(Z, +)$, $(2Z, +)$



This is one-one and onto both.

Now $f(a+b)$

$\Rightarrow 2 \cdot (a+b) = 2(a) + 2(b)$

$= f(a) + f(b)$

$\Rightarrow (Z, +)$ and $(T, +)$ are isomorphic to each other.

Theorem: Let $(S, *)$ and $(T, *')$ be monoids. Let $f: S \to T$ be an isomorphism then $f(e) = e'$

Let e' be the identity of S and e' be the identity of T.

T.P. : $f(e) = e'$

$a, e \in S$

$a * e = a$ (as e is identity)

$f(a * e) = f(a)$ (taking functions both sides)

$f(a) *' f(e) = f(a)$ (applying property of isomorphism)

$\Rightarrow f(e)$ is identity element of $(T, *)$

$\Rightarrow \boxed{f(e) = e'}$

H.P.

Date
Page

Ring oid :→ Ring
- Integral Domain
- Field

Ring: an algebric system $(R, +, \cdot)$ is called a ring if :-

(i) $(R, +)$ is an abelian group.
(ii) $(R, \cdot)$ is a semigroup.
(iii) The operation $(\cdot)$ is distributed over $(+)$.

Special types of rings :-

(i) **commutative ring :-** If $(R, \cdot)$ is commutative the $(R, +, \cdot)$ is called a commutative ring.

(ii) **Ring with identity :-** If $(R, \cdot)$ gives existence of identity then we have ring with identity.

(iii) **Ring with unity :-** A unit element of a ring, if it exists. Is an element of the semi-group $(R, \cdot)$. The unit of a ring is generally denoted by 1.

(iv) **Ring with zero divisors :-** A ring is known as ring with zero divisors if $a \cdot b = 0$ when $a = 0$ or $b = 0$

Integral domain :- A ring $(R, +, \cdot)$ is called an integral domain if it is commutative with identity and without zero divisors.

MARUTI

eg: $(R, +_n, \times_n)$.

Field :- A field is a commutative ring with identity in which every non-zero element has a multiplicative inverse.

Theorem: Every finite integral domain is a field but every field is not necessarily an integral domain.

* Permutation group :-

ex: $A = \{1, 2, 3\}$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

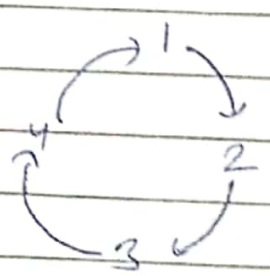
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Total $n!$
$\rightarrow 3! = 6$

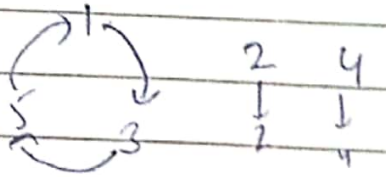
* cyclic permutation :-

arrangement in which every element of cycle is the image for its previous element. first element is the image for last element.

eg: cycle: (1, 2, 3, 4)



cycle (1, 3, 5)



eg: $A = (1, 2, 3, 4, 5)$ $\quad A = (1\ 2\ 3\ 4\ 5)$

$B = (2, 3)(4, 5)$ $\quad B = (2\ 3)\ \ (4\ 5)$

Find $A \times B$?

Sol)

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

(domain: top row; co-domain: bottom row)

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

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

✱ Transpositions :-

ex: $(1\ 3\ 5\ 7)$

$(1\ 3)(1\ 5)(1\ 7)$ → first element is fixed.
If these 3 multiplied @ it will result to same cycle.

ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ express this as product of transpositions!

Sol) $(1\,6)(2\,5\,3)$

$(1\,6)(2\,5)(2\,3)$

ii) $f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

∴ find f^{-1} ?

$\rightarrow f \cdot f^{-1} = I$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ y & z & x & v & w \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ y & z & x & v & w \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$y=1, z=2, x=3, v=4, w=5$

$x=3$
$y=1$
$z=2$
$u=5$
$v=4$

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