UNIT - II

MODERN ALGEBRA

Algebraic Structure $(S, *)$

set

binary operator

1. Closure Property

In an algebraic structure $(S, *)$

Let $a, b \in S$

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

then $(S, *)$ holds closure law.

2. Associative Law

In an algebraic structure $(S, *)$

Let $a, b \in S$

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

then $(S, *)$ holds associative law

3. Existence of Identity :

In an algebraic structure $(S, *)$

Let $a, e \in S$

If $a * e = a$,

then 'e' is the identity of $(S, *)$

4. Existence of Inverse

In an algebraic structure $(S, *)$

Let $a, b, e \in S$

If $a * b = e$,

then a and b are inverse of each other.

5. Commutative Law

In an algebraic structure $(S, *)$

Let $a, b \in S$

If $a * b = b * a$,

then $(S, *)$ holds commutative law.

Algebraic Structure

Grouped
- group
- semigraph
- monoid
- abelion gp

Ringed
- ring
- field
- integral domain

group holds 1. 2. 3. 4.

semi group holds 1. 2.

monoid holds 1. 2. 3.

- abelion group is a gp which holds only 5.

Q. Let the operation '$*$' be defined on the set of integers as $a*b = a+b+2$, $\forall\ a,b \in Z$

Show that $(Z, *)$ is an Abelian Group.

A. 1. Closure Law :

In $(S, *)$, if $a*b = c \in S$ $\forall\ a, b, c \in S$

In $(Z, *)$

Let $a, b \in Z$

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

Add^n of integers is also an integer.

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

2. Associative Law :

In $(S, *)$, $a*(b*c) = (a*b)*c$ $\forall\ a,b,c \in S$

In $(Z, *)$

Let $a, b, c \in S$

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

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

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

Hence, $(Z, *)$ ~~is~~ holds associative Law.

3. Existence of identity:

$$a * e = a, \qquad \forall\ a, e \in S$$

Let $a, e \in Z$,

$$a * e = a$$

$$a + e + 2 = a$$

$$e = -2$$

4. Existence of inverse:

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

Let $a, b, e \in Z$,

$$a * b = e$$

$$a + b + 2 = e$$

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

$$\boxed{b = -4 - a}$$

5. Commutative Law:

$$a * b = b * a$$

$\forall\ a, b \in S$

Let $a, b \in Z$

$$a * b = b * a$$

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

$\because$ add^n of no. is commutative

$\therefore$ ~~Z(~~ $(Z, *)$ holds commutative

Q. Let $G = \{ (a,b) \mid a,b \in R,\ a \neq 0 \}$

Define binary operation '$*$' ~~my~~ on G by

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

$\forall\ (a,b),\ (c,d) \in G$

Show that $(G, *)$ is a group and find if it's albelion.

A. 1. Closure Law:

In $(S, *)$, $a*b = c \in S \quad \forall\ a,b,c \in S$

In $(G, *)$, let $(a,b), (c,d) \in G$

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

Add^n & Multiplication of a Real no. is a Real No., $\therefore$ $(G, *)$ holds closure law.

2. Associative Law:

In $(S, *)$, $a*(b*c) = (a*b)*c \quad \forall a,b,c \in S$

In $(G, *)$, let $(a,b), (c,d), (e,f) \in G$

~~a*~~

$$(a,b) * ((c,d) * (e,f)) = ((a,b) * (c,d)) * (e,f)$$
$$(a,b) * (ce,\ ed+f) = (ac,\ bc+d) * (e,f)$$
$$(ace,\ bce+ed+f) = (ace,\ bce+ed+f)$$

Hence, $(G, *)$ ~~is~~ holds associative law.

3. Existence of identity:

In $(S, *)$, $a * e = a$ $\forall\ a, e \in S$

In $(G, *)$, Let $(a, b), (c, d), (e, f) \in G$

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

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

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

$\boxed{e = 1}$ $b + f = 0$

$\boxed{f = 0}$

4. Existence of inverse:

In $(S, *)$, $a * b = e$, $\forall\ a, b, e \in S$

In $(G, *)$, let $(a, b), (c, d), (e, f) \in G$

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

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

$c = e/a$, $b/a + d = 0$

$\boxed{c = 1/a}$, $\boxed{d = -b/a}$

5. Commutative Law:

In $(S, *)$, $a * b = b * a$, $\forall\ a, b \in S$

In $(G, *)$, Let $(a, b), (c, d) \in$

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

$(ac, bc + d) = (ac, \cancel{bc + dc}\ ad + b)$

not commutative.

Q1 $(Z^+, *)$

$x * y = xy$

Q2. $(Z^+, *)$

$x * y = y$

Q3. $(Z^+, *)$

$x * y = x + y + xy$

Q4. $(Z^+, *)$

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

Q5. $(Z^+, *)$

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

A.1. $x * y = xy$ $(Z^+, *)$

<u>closure law</u>: In $(S, *)$, $a*b = c \in S$ $\forall a, b, c \in S$

Let $x, y \in Z^+$ in $(Z^+, *)$

$x*y = xy$

Multiplication of two +ve integers gives a +ve integer. $\therefore$ $(Z^+, *)$ holds closure law.

<u>associative law</u>: In $(S, *)$, $a*(b*c) = (a*b)*c$

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

Let $x, y, z \in Z^+$ in $(Z^+, *)$

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

$x*(yz) = xy*z$

$xyz = xyz$

$\therefore$ $(Z^+, *)$ holds associative Law

<u>existence of identity</u>: In $(S, *)$, $a*e = a$ $\forall a, e \in S$

let $x, e \in Z^+$ in $(Z^+, *)$

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

<u>existence of inverse</u>: In $(S, *)$, $a * b = e$ $\forall a, b, e \in S$

Let $x, y, e \in Z^+$ in $(Z^+, *)$

$$x * y = e$$
$$xy = 1$$
$$x = 1/y$$

$\because$ $1/y$ will not belong to Z^+

$\therefore$ existence of inverse is not held by $(Z^+, *)$

$\therefore$ $x*y = xy$, ~~in~~ $(Z^+, *)$ is a monoid

A2. $(Z^+, *)$

$x * y = y$

<u>closure law</u>: In ~~St~~ $(S, *)$, $a*b = c \in S$ $\forall a, b, c \in S$

In $(Z^+, *)$, let $x, y \in Z^+$

$x * y = y$

Binary operation on two +ve integers gives a +ve integer.

$\therefore$ ~~Z~~ $(Z^+, *)$ holds closure law.

<u>associative law</u>: In $(S, *)$, $a*(b*c) = (a*b)*c$ $\forall a, b, c \in S$

In $(Z^+, *)$, let ~~a+b~~. $x, y, z \in Z^+$

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

$x*z = y*z$

$z = z$

$\therefore$ $(Z^+, *)$ holds associative law.

<u>existence of identity</u>: In $(S, *)$, $a*e = a$, $\forall a, e \in S$

In $(Z^+, *)$, let $x, e \in Z^+$

$(Z^+, *)$
$\therefore$ Semi-graph

$x * e = x$

$\boxed{e = x}$

$\because$ identity is not unique i.e, keeps on changing, $\therefore$ $(Z^+, *)$ doesnt hold existence of identity

For Finite Numbers

$+_m \quad \times_m$

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

Add^n Modulo

$\downarrow$

Same mechanism for Multiplication Modulo

$+_6$	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

$x * e = x$

$x +_6 e = x$

$\Downarrow$

0

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

$$5 = 5$$

Theorem: The identity element (if it exists) of any algebraic structure is unique.

$(S, *)$

Let $e_1, e_2 \in S$

Let e_1 be the identity

$e_1 * e_2 = e_2$ ——— (1)

Let e_2 be the identity

$e_1 * e_2 = e_1$ ——— (2)

$\therefore \boxed{e_1 = e_2}$

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

$(S, *)$

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

Let b_1 be the inverse

$a * b_1 = e$ —— (1)

Let b_2 be the inverse

$a * b_2 = e$ —— (2)

$a * b_1 = a * b_2$

using left cancellation law,

$\boxed{b_1 = b_2}$

Theorem: In a group $(G, *)$:

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

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

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

now, $a * a^{-1} = e$ —— (1)

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

(existence of ~~identi~~ inverse)

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

using right cancellation law,

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

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

since, $a*b \in G$ (closure law)

hence, $(a*b)^{-1} \in G$

$$(a*b)*(a*b)^{-1} = e \quad \text{—(1)}$$
$$(a*a^{-1})*(b*b^{-1}) = e \quad \text{—(2)}$$
(existence of identity)

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

using left cancellation law,

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

Theorem: If ~~A~~ a and b be arbitrary elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelion.

I.

$$(ab)^2 = a^2b^2$$
$$(ab)(ab) = (aa)(bb)$$
$$a(ba)b = a(ab)b$$

using LCL,

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

using RCL,

$$\boxed{ba = ab}$$

∴ commutative law

II. $ba = ab$

using binary operation, w/ b

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

using binary operation, w/ a

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

~~a b~~

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

~~(ab)(ab) =~~

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

Theorem: Show that if $a^2 = a$, then $a = e$, $a \in G$

$$a^2 = a$$

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

acc. law of identity:

$$a \cdot e = a \quad \text{———} \quad (11)$$

from (1) & (11),

$$a \cdot a = a \cdot e$$

by ~~RCL~~, LCL,

$$\boxed{a = e}$$

Order of an element

The order of an element g in a group G is the smallest +ve integer in N such that $g^N = e$. If no such integer exists, we say g has ∞ order.

Order of a group

The no. of elements present in a group.

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

$$O(i) = 4 \quad , \quad O(1) = 4$$

Cyclic Group

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

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

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

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

$(-i)^3 = i$

$(-i) = -i$

$\langle i \rangle \; \langle -i \rangle \longrightarrow$ generator

$$(G, +_6)$$

when $\quad G = \{0, 1, 2, 3, 4, 5\}$

$(5)^2 = 5 +_6 5 = 4$

$(5)^3 = 5 +_3 5 = 3$

$(5)^4 = 2$

$(5)^5 = 1$

$(5)^6 = 0$

$(5)^7 = 5$ $\qquad$ generator: $\langle 5 \rangle, \langle 1 \rangle$

Theorem: Every cyclic gp is an abelian gp.

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

$G = \langle a \rangle \{a^n, n \in \mathbb{Z}\}$

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

$$g_1 . g_2 = a^r . a^s$$
$$= a^{r+s}$$
$$= a^{s+r} \quad [+ \text{ is commutative}]$$
$$= a^s . a^r$$
$$= g_2 . g_1$$

$\Rightarrow$ commutative

$\Rightarrow$ abelion

Sub-Group

A part of a group following all the properties of a group.

Et $(\{1, -1, i, -i\}, \times)$

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

$(\{i\}, \times)$ $\qquad$ $(\{-1, -i\}, \times)$

$(\{-i\}, \times)$ $\qquad$ $(\{i, -i\}, \times)$

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

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

$(\{1, i\}, \times)$ $\qquad$ $(\{-1, -i, i\}, \times)$

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

Necessary and Important Condⁿ for a gp to be a sub-group

~~G~~ $(G, *)$ $H \subseteq G$ $(H, *)$

$a, b \in G$

$a, b \in H$

if $a * b^{-1} \in H \Rightarrow$ sub group

Theorem : The intersection of 2 sub-groups of a group $(G, *)$ is also a sub-group, but the union of any 2 sub-groups is not necessarily a sub-group

I. Let $(G, *)$

$H_1 \subseteq G$

$H_2 \subseteq G$

$(H_1, *)$ $(H_2, *)$ are two sub groups of $(G, *)$

~~$H_1 \neq H_2$~~ $H_1 \cap H_2 \neq \phi$ bcs 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 $b^{-1} \in H_2$

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

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

$\Rightarrow (H_1 \cap H_2, *)$

II.

$(Z, +)$

$2Z \subseteq Z$

$3Z \subseteq Z$

$(2Z, +)$, $(3Z, +)$

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

$a \in G$
$b \in G$

acc. to closure law

$a * b \in G$

$2 \in Z$
$3 \in Z$

$2 + 3 \notin Z$

$\therefore$ not a sub-group.

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

Let $a, e \in G$ $\quad H \subseteq G$
$a, e' \in H$

By existance of identity,

$a * e = a$ —(I)
$a * e' = a$ —(II)

From (i) and (ii)

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

by LCL,

$$\boxed{e = e'}$$

Coset

$(G, *)$

$H \subseteq G$

$(H, *)$

$H = \{ h_1, h_2, h_3, \ldots, h_n \}$

$a \in G$

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

↳ coset of $(H, *)$

binary opⁿ w/ elements of H
not the subgroup H

$\{ a * h_1, a * h_2, a * h_3, \ldots, a * h_n \}$ → left coset

$\{ h_1 * a, h_2 * a, h_3 * a, \ldots, h_n * a \}$ → right coset

Index of a Sub-Group in G

If $H \subseteq G$, then the no. of distinct right or left cosets of H in G is ~~are~~ called the index of H in G and is denoted by:

$$[G : H] \quad \text{or} \quad i_G(H)$$

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

A. $(3Z, +)$ is the subgroup of $(Z, +)$

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

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

$0 + 3Z = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$1 + 3Z = \{\ldots, \cancel{-10}\ -8, -5, -2, 0, 4, 7, 10, \ldots\}$

$2 + 3Z = \{\ldots, -7, -4, -1, 0, 5, 8, 11, \ldots\}$

$3 + 3Z = \{\ldots, -6, -3, 0, 6, 9, 12, \ldots\}$

$4 + 3Z$

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

$i_G(3Z, +) = 3$

Langrange's Theorem

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

$(G, *)$

$O(G) = n$

$H \subseteq G$

$(H, *)$

$O(H) = m$

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

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

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

$\vdots$

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

$k \times m = n$

$k = \dfrac{n}{m}$

Isomorphism

If $(S, *)$ and $(T, *)$ be two algebraic structures

A function $f \; S \to T$ is called an isomorphism from $(S, *S_2)$ to $(T, * T_2)$

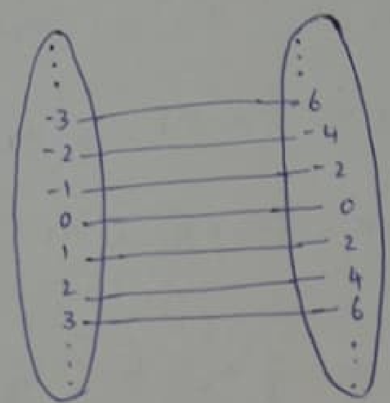
if it is one to one correspondance from S to T and if $f(a*b) = f(a) * f(b)$

Homomorphism if only 2nd cond^n is fulfilled.

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

A. $f(a) = 2a$

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



one - one

$$f(a+b) = 2(a+b)$$
$$f(a+b) = 2(a) + 2(b)$$
$$f(a+b) = f(a) + f(b)$$

$\therefore$ isomorphic

Theorem : Let $(S, *)$ and $(T, *')$ be monoids.

Let $f : S \rightarrow T$ be an isomorphism, then

$f(e) = e'$

$(S, *)$ $(T, *')$

$a, e \in S$, $e' \in T$

$a * e = a$

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

$f(a) *' f(e) = f(a)$

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

Ringoid

- Ring

An algebraic system $(R, +, \times)$ or $(R, +, \cdot)$ is known as a ring if :

(i) $(R, +)$ is an abelion group.

(ii) $(R, \times)$ is a semi-group.

(iii) the operation $\times$ is distributed over $+$

1. Commutative Ring

If $(R, \times)$ is commutative, then $(R, +, \times)$ is known as a commutative ring.

2. Ring with Identity

If $(R, \cdot)$ gives existence of identity, then $(R, +, \cdot)$ is known as a ring w identity.

3. 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.

4. Ring with zero divisors

If $a \cdot b = 0$ when $a = 0$ or $b = 0$

$2 \times_6 3 = 0$ ⟶ ring without 0 diviso

$$\begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Integral Domain

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

11 properties
- 9 ring prop. (8 ring, 1 commutative)
- 1 - ~~commutative~~ identity
- 1 - w/o zero

Eg: $(R, +_n, \times_n)$

Field

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

11 properties
- 8 ring
- 1 commutative
- 1 identity
- 1 inverse

$R - \{0\}$

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

Permutation Group

$A = \{1, 2, 3\}$ → simply take the factorial of the no. of set elements

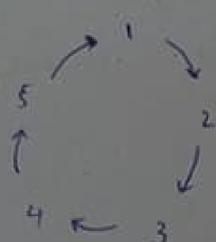
$3! = 6$

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

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

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

Cyclic Permutation



1's img — 2
2's img — 3
3's img. — 4
4's img. — 5
5's img. — 1

$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ → permutation gp for $(1\ 2\ 3)$

$(1\ 2\ 3\ 4)$ $\quad$ $(1\ 3\ 5)$

no. of cyclic elements = no. of elements in the brackets

Q. $A = (1\ 2\ 3\ 4\ 5)$

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

Find $A \times B$

1's inv = 1

A.
$$\begin{array}{r}\text{domain } (x) \\ \text{co domain } (y)\end{array} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \begin{array}{l}\text{domain } (a) \\ \text{codomain } (b)\end{array}$$

make co-domain (y) = codomain (a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \times \xrightarrow{\text{cancelled}} \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = A \times B$$

Transposition

Any ~~cy~~ cycle can be broken down into a cycle containing 2 elements.

$$(1\ 3\ 5\ 7)$$
$$\Downarrow$$
$$(1\ 3)\ (1\ 5)\ (1\ 7)$$

Q. Express $\begin{pmatrix}1&2&3&4&5&6\\6&5&2&4&3&1\end{pmatrix}$ as a product of transposition

A.

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

$$\cancel{(1\ 2\ 3\ 4\ 5\ 6)}$$

$$\cancel{(1\,2)(1\,3)(1\,4)(1\,5)(1\,6)}$$

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

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

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

$$ff^{-1} = I$$

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

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

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

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