Sri SAI RAM ENGINEERING COLLEGE
INSTITUTE OF TECHNOLOGY
West Tambaram, Chennai - 44

Sairam INSTITUTIONS

SAIRAM DIGITAL RESOURCES

YEAR II

SEM III

MA8351

DISCRETE MATHEMATICS

(Common to CSE & IT)

UNIT 4

ALGEBRAIC STRUCTURES

4.2 GROUPS

SCIENCE & HUMANITIES

4 QUALITY EDUCATION

NBA NATIONAL BOARD of ACCREDITATION

NAAC A+

nirf NATIONAL INSTITUTIONAL RANKING FRAMEWORK

BUREAU VERITAS Certification

GROUPS

Definition

If G is a non empty set and * is a binary operation of G, then the algebraic system {G, *} is called group if the following conditions are satisfied:

1. For all a, b, c ∈ G,

   (a * b) * c = a * (b * c) (Associativity)

2. There exists an element e ∈ G such that, for any a ∈ G,

   a * e = e * a = a (Existence of identity)

3. For every a ∈ G, there exists and element $a^{-1} \in G$ such that

   a * a^{-1} = a^{-1} * a = e (Existence of inverse)

Note

The algebraic system {S, *} is a semigroup, if * is associative. If there exists an identity element e ∈ S, then {S, *} is a monoid. Further if there exists an inverse for each element of S, then {S, *} is a group.

For example, {Z, +} is a group under the usual addition.

Definitions

When G is finite, the numbers of elements of G is called the order of G and denoted by O(G) or |G|. If the element a ∈ G, where G is a group with identity element e, then the least positive integer m for which $a^m = e$ is called the order of the element a and denoted as O(a). If no such integer exists, then a is of infinity order.

A group {G, *}, in which the binary operation * is commutative, is called a commutative group or abelian group.

For example, the set of rational numbers excluding zero is an abelian group under the usual multiplication.

Properties of a Group

1. The identity element of a group (G, *) is unique.

Proof

If possible, let there be two identity elements in the group {G, *}, say e_1 and e_2. Since, e_2 is an identity and , $e_1 \in G$, we have

$$e_2 * e_1 = e_1 * e_2 = e_1 \qquad \text{----- (1)}$$

Since, e_1 is an identity and , $e_2 \in G$, we have

$$e_1 * e_2 = e_2 * e_1 = e_2 \qquad \text{----- (2)}$$

From (1) and (2), we have

$$e_1 = e_1 * e_2$$
$$= e_2$$

Hence, the identity element of a group is unique.

2. The inverse of each element of (G, *) is unique.

Proof

If possible, let b and c be two inverses of the element a ∈ G.

Then, by the existence of inverse

a * b = b * a = e, where e is the identity of G ----- (1)

Similarly $a * c = c * a = e$ ----- (2)

Now $b = e * b$

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

$= c * (a * b)$ by axiom (1)

$= c * e$ by (1)

$= c$ by (1)

Hence, the inverse of an element of (G, *) is unique.

3. The cancellation laws are true in a group

viz., $a * b = a * c \Rightarrow b = c$

and $b * a = c * a \Rightarrow b = c$

Proof

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

$\therefore \quad a * b = a * c \Rightarrow b = c$

i.e., the left cancellation law is valid in a group.

(ii) Given $\quad b * a = c * a$

$i.e., \quad (b * a) * a^{-1} = (c * a) * a^{-1}$

$i.e., \quad b * (a * a^{-1}) = c * (a * a^{-1})$

$i.e., \quad b * e = c * e$

$i.e., \quad b = c$

$\therefore \quad b * a = c * a \Rightarrow b = c$

i.e., the right cancellation law is valid in a group.

4. $(a * b)^{-1} = b^{-1} * a^{-1}$, for any $a, b \in G$.

Proof

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

Also

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

Thus the inverse of $(a * b)$ is $b^{-1} * a^{-1}$ i.e., $(a * b)^{-1} = b^{-1} * a^{-1}$

5. If $a, b \in G$, the equation $a * x = b$ has the unique solution $x = a^{-1} * b$.

Similarly the equation $y * a = b$ has the unique solution $y = b * a^{-1}$.

Proof

Let $c = a^{-1} * b$

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

$a * c = b$ means $x = c$ is a solution of the equation $a * x = b$.

If possible, let $x = d$ be another solution of the equation $a * x = b$.

Then $a * c = a * d = b$

By left cancellation, we get $c = d$.

i.e., $x = a^{-1} * b$ is the unique solution of the equation $a * x = b$.

Similarly we can prove that $y = b * a^{-1}$ is the unique solution of $y * a = b$.

6. $(G,*)$ cannot have an idempotent element except the identity element.

Proof

If possible, let a be an idempotent element of $(G,*)$ other than e.

Then $a * a = a$ ----- (1)

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

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

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

$= a * e$

$= a$

Hence the only idempotent element of G is its identity element.

PERMUTATION

Definition

A bijective mapping of a non-empty set $S \rightarrow S$ is called a permutation of S.

For example, if $S = \{a, b\}$, the two possible permutations of $\{a, b\}$ are $\{a, b\}$ and $\{b, a\}$. In this section, we will represent the two permutations as

$$p_1 = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \quad \text{and} \quad p_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

where the first row of p contains the elements of S in the given order and the second row gives their images.

Now the set $S_2 = \{p_1, p_2\}$ is the set of all possible permutations of the element of S.

Let $*$ denote a binary operation on S_2 representing the right composition of permutations, viz., when $i, j, = 1, 2, p_i * p_j$ means the permutation obtained by permuting the elements of S by the application of p_i, followed by the application of p_j .

In other words, if p_i and p_j are treated as functions and $\bullet$ denotes the usual left composition of functions, then $p_i * p_j = p_j \bullet p_i$ for $i, j = 1, 2$.

For example,

$$p_2 * p_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} a & b \\ a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} a & b \\ a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ b & a \end{pmatrix} = p_2$$

PERMUTATION GROUP

Definition

The set G of all permutations on a non-empty set S under the binary operation $*$ of right composition of permutations is a group $\{G,*\}$called the permutation group.

If $S=\{1,2,\dots,n\}$, the permutation group is also called the symmetric group of degree n and denoted by S_n. The number of elements of S_n or $|S_n|=n!$, since there are $n!$ permutations of n elements.

Now let us verify that $\{S_3,*\}$,where $S=\{1,2,3\}$ is a group under the operation of right composition of permutations.

There will be $3!=6$ permutations of the elements 1, 2, 3 of S.

i.e., $S=\{1,2,\dots,n\}$ $S_3=\{p_1,p_2,p_3,p_4,p_5,p_6\}$, where

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The Cayley's compostion table of permutations on S_3 is given below:

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_6	p_5	p_2	p_1	p_4
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_1	p_6	p_3	p_2
p_6	p_6	p_3	p_2	p_5	p_4	p_1

Note

To obtain $p_i * p_j$, it will be convenient if we rewrite the first row of p_j so as to coincide with the second row of p_i.

Using the above table, all the three axioms of a group are easily verified.

For example, $(p_2 * p_4) * p_6 = p_3 * p_6 = p_4$

Also $p_2 * (p_4 * p_6) = p_2 * p_3 = p_4$

Thus associativity is satisfied.

Now $p_1 * p_i = p_i * p_1 = p_1$, for $i = 1, 2, 3, \dots 6$

Thus the existence of the identity element (in this example, $e = p_1$) is verified.

Also $p_1^{-1} = p_1, p_2^{-1} = p_1, p_3^{-1} = p_5, p_4^{-1} = p_4, p_5^{-1} = p_3$, and $p_6^{-1} = p_6$.

Thus the existence of inverse of each element is verified.

Hence $\{S_3, *\}$ is a group.

However this symmetric group is not abelian, since, for example, $p_2 * p_3 = p_4$, where as $p_3 * p_2 = p_6$.

DIHEDRAL GROUP

Definition

The set of transformations due to all rigid motions of a regular polygon of n sides resulting in identical polygons but with different vertex names under the binary operation of right composition $*$ is a group called dihedral group, denoted by $\{D_n, *\}$.

By rigid motion, we mean the rotation of the regular polygon about its centre through angles $1 \times \frac{360}{n}, 2 \times \frac{360}{n}, \ldots, n \times \frac{360}{n}$, in the anticlockwise direction and reflection of the regular polygon about its lines of symmetry.

CYCLIC GROUP

Definition

A group $\{G, *\}$ is said to be cyclic, if there exists an element $a \in G$ such that every element x of G can be expressed as $x = a^n$ for some integer n.

In such a case, the cyclic group is said to be generated by a or a is generator of G, G is also denoted by $\{a\}$.

For example, if $G = \{1, -1, i, -i\}$, then $\{G, \times\}$ is a cyclic group with the generator i, for $1 = i^4, -1 = i^2, i = i^1$ and $-i = i^3$.

For this cyclic group, $-i$ is also a generator.

Properties of a Cyclic Group

1. A cyclic group is abelian.

Proof

Let $\{G,*\}$ be a cyclic group with $a \in G$ as generator.

Let $b, c \in G$. Then $b = a^m$ and $c = a^n$, where m and n are integers.

Now

$$\begin{aligned} b * c &= a^m * a^n \\ &= a^{m+n} \\ &= a^{n+m} \\ &= a^n * a^m \\ &= c * b \end{aligned}$$

Hence $\{G,*\}$ is an abelian group.

2. If a is a generator of a cyclic group $\{G, *\}$, a^{-1} is also a generator of $\{G, *\}$.

Proof

Let $b \in G$. Then $b = a^m$, where m is an integer.

Now $b = (a^{-1})^{-m}$ where $-m$ is an integer.

$\therefore \quad a^{-1}$ is also a generator of $\{G, *\}$.

3. If $\{G, *\}$ is a finite cyclic group generated by an element $a \in G$ and is of order n, then $a^n = e$ so that $G = \{a, a^2, \ldots, a^n (= e)\}$. Also n is the least positive integer for which $a^n = e$.

Proof

If possible let there exist a positive integer $m < n$ such that $a^m = e$.

Since G is cyclic, any element of G can be expressed as a^k, for some $k \in Z$.

When k is divided by m, let q be the quotient and r be the remainder, where $0 \leq r < m$.

Then $$k = mq + r$$

$\therefore$ $$\begin{aligned} a^k = a^{mq+r} &= a^{mq} * a^r \\ &= (a^m)^q * a^r \\ &= e^q * a^r \\ &= e * a^r \\ &= a^r \end{aligned}$$

This means that every element of G can be expressed as a^r, where $0 \leq r < m$.

This implies that G has at most m elements or order of $G = m < n$, which is a contradiction.

i.e., $a^m = e$, for $m < n$ is not possible.

Hence $a^n = e$, where n is the least positive integer. Now let us prove that the elements $a, a^2, a^3, \dots, a^n (= e)$ are distinct.

If it is not true, let , $a^i = a^j$, for $i < j \leq n$

Then $a^{-i} * a^i = a^{-i} * a^j$

i.e., $e = a^{j-i}$, where $j - i < n$,

which again is a contradiction.

Hence $a^i \neq a^j$, for $i < j \leq n$.

4. If $\{G,*\}$ is a finite cyclic group of order n with a as a generator, then a^m is also a generator of $\{G,*\}$, if and only if the greatest common divisor of m and n is 1, where $m < n$.

Proof

Let us assume that a^m is a generator of $\{G,*\}$.

Then, for some integer r,

$$a = (a^m)^r = a^{mr}$$

i.e., $a = a^{mr} * e = a^{mr} * e^s$, where s is an integer.

$$= a^{mr} * (e^n)^s, \text{ since } a^n = e, \text{ by property (3)}$$

$$= a^{mr} * e^{ns}$$

$$= a^{mr+ns}$$

$\therefore$ $$mr + ns = 1$$

$\therefore$ GCD $(m, n) = 1$

To prove the converse, let us assume that GCD $(m, n) = 1$

$\therefore$ There exists two integers p and q such that

$$mp + nq = 1 \quad \text{----- (1)}$$

Let H be the set generated by a^m.

Since, each integral power of a^m will also be an integral power of a.

$$H \subseteq G \quad \text{----- (2)}$$

Now $a^{mp+nq} = a$, by (1)

i.e., $a^{mp} * a^{nq} = a$

i.e., $(a^m)^p * (a^n)^q = a$

i.e., $(a^m)^p * (e)^q = a$, since $a^n = e$

i.e., $(a^m)^p * e = a$, since $e^q = e$

i.e., $(a^m)^p = a$

This means that each integral power of a will also be an integral power a^m.

i.e., $G \subseteq H$ ----- (3)

From (2) and (3), we have $H = G$

i.e., a^m is a generator of G.

PROBLMES

1. If $\{G,*\}$ is an abelian group, show that $(a * b)^n = a^n * b^n$ for all $a, b \in G$, where n is a positive integer.

Proof

Since, $\{G,*\}$ is an abelian group,

$$a * b = b * a \qquad \text{----- (1)}$$

For $a, b \in G$, we have $(a * b)^1 = (b * a)^1$, by (1)

and $(a * b)^2 = (a * b) * (a * b)$

$= a * (b * a) * b$, by associativity

$= a * (a * b) * b$, by (1)

$= (a * a) * (b * b)$, by associativity

$= a^2 * b^2$

Thus, the required result is true for $n = 1, 2$. Let us assume that the result is valid for $n = m$.

i.e., $(a * b)^m = a^m * b^m$ ----- (2)

Now $(a * b)^{m+1} = (a * b)^m * (a * b)$

$= (a^m * b^m) * (a * b)$, by (2)

$= a^m * (b^m * a) * b$, by associativity

$= a^m * (a * b^m) * b$, since G is abelian

$= (a^m * a) * (b^m * b)$, by associativity

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

Hence, by induction, the result is true for positive integral values of n.

2. Show that the set Q^+ of all positive rational numbers forms an abelian group under the operation $*$ defined by $a * b = \frac{1}{2} ab \,; a, b \in Q^+$.

Proof

When $\quad a, b \in Q^+, \quad \frac{ab}{2} \in Q^+$

$\therefore \quad Q^+$ is closed under the operation $*$

Now $\quad (a * b) * c = \left(\frac{ab}{2}\right) * c$

$= \frac{ab}{2} . \frac{c}{2}$

$$= \frac{abc}{4}$$

$$a * (b * c) = a * \left(\frac{bc}{2}\right)$$

$$= \frac{a}{2} * \frac{bc}{2}$$

$$= \frac{abc}{4}$$

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

Hence $*$ is associative.

Let e be the identity element of Q^+ under $*$

$\therefore$ $$a * e = e * a = a, \text{ for } a \in Q^+$$

i.e., $$\frac{1}{2} ae = a$$

$$ae = 2a$$

$$ae - 2a = 0$$

$$a(e-2)=0$$

Since $a>0$, we get $\quad e=2$

Hence identity element exists.

Let b be the inverse of the element $a \in G$.

Then $\quad a*b=b*a=e=2$

i.e., $\quad \frac{1}{2}\,ab=2$

$$ab=4$$

$\therefore \quad b=\frac{4}{a}\in Q^{+}$

Thus every element of Q^{+} is invertible.

$\therefore \quad (Q^{+},\ *)$ is a group.

Also $\quad b*a=a*b=\frac{1}{2}ab$

$\therefore \quad (Q^{+},\ *)$ is an abelian group.

3. If $*$ is the binary operation on the set R of real numbers defined by

$a * b = a + b + 2ab$,

(a) Find if is a semigroup. Is it commutative?

(b) Find the identity element, if exists.

(c) Which elements have inverses and what are they?

Proof

(a)
$$
\begin{aligned}
(a * b) * c &= (a * b) + c + 2(a * b)c \\
&= (a + b + 2ab) + c + 2(a + b + 2ab)c \\
&= a + b + 2ab + c + 2(ac + bc + 2abc) \\
&= a + b + 2ab + c + 2ac + 2bc + 4abc \\
&= a + b + c + 2ab + 2ac + 2bc + 4abc \\
&= a + b + c + 2(ab + ac + bc) + 4abc
\end{aligned}
$$

$$\begin{aligned} a * (b * c) &= a + (b * c) + 2a(b * c) \\ &= a + (b + c + 2bc) + 2a(b + c + 2bc) \\ &= a + b + c + 2bc + 2ab + 2ac + 4abc \\ &= a + b + c + 2(ab + ac + bc) + 4abc \end{aligned}$$

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

i.e., $*$ is associative.

Hence, $(R, *)$ is a semigroup.

Also $\quad b * a = b + a + 2ba$

$$\begin{aligned} &= a + b + 2ab \\ &= a * b \end{aligned}$$

Hence, $(R, *)$ is a commutative.

(b) If the identity element exists, let it be e.

Then for any $a \in R$, $\quad a * e = a$

i.e., $\quad a + e + 2ae = a$

$$e + 2ae = 0$$

$$e(1 + 2a) = 0$$

$\therefore \quad e = 0$, since $1 + 2a \neq 0$, for any $a \in R$.

(c) Let a^{-1} be the inverse of an element $a \in R$. Then $a * a^{-1} = e$.

$$a + a^{-1} + 2aa^{-1} = 0$$

$$a^{-1}(1 + 2a) = -a$$

$\therefore \quad a^{-1} = -\frac{a}{1+2a}$

$\therefore$ If $a \neq -\frac{1}{2}$, a^{-1} exists and $= -\frac{a}{1+2a}$.

4. If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$,

(a) Find if $(S, *)$ is a semigroup. Is it commutative?

(b) Find the identity element of S.

(c) Which elements, if any, have inverses and what are they?

Proof

(a) $$\{(a,b) * (x,y)\} * (c,d) = (ax, ay+b) * (c,d)$$
$$= (acx, adx + ay + b)$$
$$(a,b) * \{(x,y) * (c,d)\} = (a,b)(cx, dx + y)$$
$$= (acx, adx + ay + b)$$

Hence, $*$ is associative on S.

$\therefore$ $\{S, *\}$ is a semigroup.

Now $(x,y) * (a,b) = (ax, bx + cy) \neq (a,b) * (x,y)$

$\therefore$ $\{S, *\}$ is not commutative.

Now $(x,y) * (a,b) = (ax, bx+cy) \neq (a,b) * (x,y)$

$\therefore$ $\{S, *\}$ is not commutative.

(b) Let (e_1, e_2) be the identity element of $\{S, *\}$. Then for any $(a,b) \in S$,

Now $(a,b) * (e_1, e_2) = c$

i.e., $(ae_1, \ ae_2 + b) = (a, \ b)$

$\therefore$ $ae_1 = a$ $\quad ae_2 + b = b$

i.e., $e_1 = 1$ $\quad e_2 = 0$

$\therefore$ The identity element is $(1, 0)$.

(c) Let the inverse of $(a, \ b)$ be $(c, \ d)$, if it exists.

Then $(a,b) * (c, \ d) = (1, \ 0)$

i.e., $(ac, \ ad + b) = (1, \ 0)$

$\therefore \quad ac = 1 \qquad ad + b = 0$

i.e., $\quad c = \frac{1}{a} \qquad d = -\frac{b}{a}$

$\therefore$ Thus the element $(a,\ b)$ has an inverse if $a \neq 0$ and its inverse is $\left(\frac{1}{a}, -\frac{b}{a}\right)$.

5. If the permutations of the elements of $\{1, 2, 3, 4, 5\}$ are given by

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$,

$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, find $\alpha\beta$, $\beta\alpha$, α^2, $\alpha\beta$, δ^{-1} and $\alpha\beta\gamma$. Also solve the equation $\alpha x = \beta$.

Solution

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 4 & 5 \\ \beta: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 5 & 4 \end{array}$$

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

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \beta: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 2 & 3 & 5 & 4 \\ \alpha: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 5 & 4 \end{array}$$

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

	1	2	3	4	5
α:	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	2	3	1	4	5
α:	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	3	1	2	4	5

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

	1	2	3	4	5
γ :	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	5	4	3	1	2
β:	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	4	5	3	1	2

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

δ^{-1} is obtained by interchanging the two rows of δ and then rearranging the elements of the first row so as to assume the natural order.

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

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha\beta: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 5 & 4 \\ \gamma: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 3 & 5 & 2 & 1 \end{array}$$

$$\therefore \alpha\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

Solving the equation $\alpha x = \beta$ means finding the value of x that satisfies the equation. Pre-multiplying by α^{-1}, the given equation becomes

$$\alpha^{-1}\alpha x = \alpha^{-1}\beta$$

i.e., $ex = \alpha^{-1}\beta$, where e is the identity permutation.

$\therefore$ $x = \alpha^{-1}\beta$

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

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha^{-1}: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 & 4 & 5 \\ \gamma: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 & 5 & 4 \end{array}$$

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