Unit-3
Group Theory

- Algebraic systems Examples and general properties
- Semi groups
- Monoids
- Groups
- Sub groups
- Lagrange Thm
- Permutation group

Algebraic systems

- **N = {1,2,3,4,…..∝ } = Set of all natural numbers.**

  Z = { 0, ± 1, ± 2, ± 3, ± 4 , ….. ∝} = Set of all integers.

  Q = Set of all rational numbers.

  R = Set of all real numbers.

- **Binary Operation:** The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if

  $a * b \in A$ for all $a, b \in A$ (Closure property).

  Ex: The set N is closed with respect to addition and multiplication

  but not w.r.t subtraction and division.

- **Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

  Ex: (N, +), (Z, +, –), (R, +, **. , –**) are algebraic systems.

Properties

- **Commutative:** Let $*$ be a binary operation on a set A.

  The operation $*$ is said to be commutative in A if

  $a * b = b * a$ for all a, b in A
- **Associativity:** Let $*$ be a binary operation on a set A.

  The operation $*$ is said to be associative in A if

  $(a * b) * c = a * (b * c)$ for all a, b, c in A
- **Identity:** For an algebraic system (A, *), an element 'e' in A is said to be an identity element of A if

  $a * e = e * a = a$ for all $a \in A$.
- **Note:** For an algebraic system (A, *), the identity element, if exists, is unique.
- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

  $a * b = b * a = e$

Semi group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
  1. * is closed operation on A.
  2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, –) is not a semi group.

- **Monoid:** An algebraic system (A, *) is said to be a **monoid** if the following conditions are satisfied.

  1) * is a closed operation in A.

  2) * is an associative operation in A.

  3) There is an identity in A.

Monoid

- Ex. Show that the set 'N' is a monoid with respect to multiplication.
- Solution: Here, N = {1,2,3,4,……}

1. Closure property : We know that product of two natural numbers is again a natural number.

i.e., $a.b = b.a$ for all $a,b \in N$

$\therefore$ Multiplication is a closed operation.

2. Associativity : Multiplication of natural numbers is associative.

i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

$a.1 = 1.a = a$ for all $a \in N$.

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

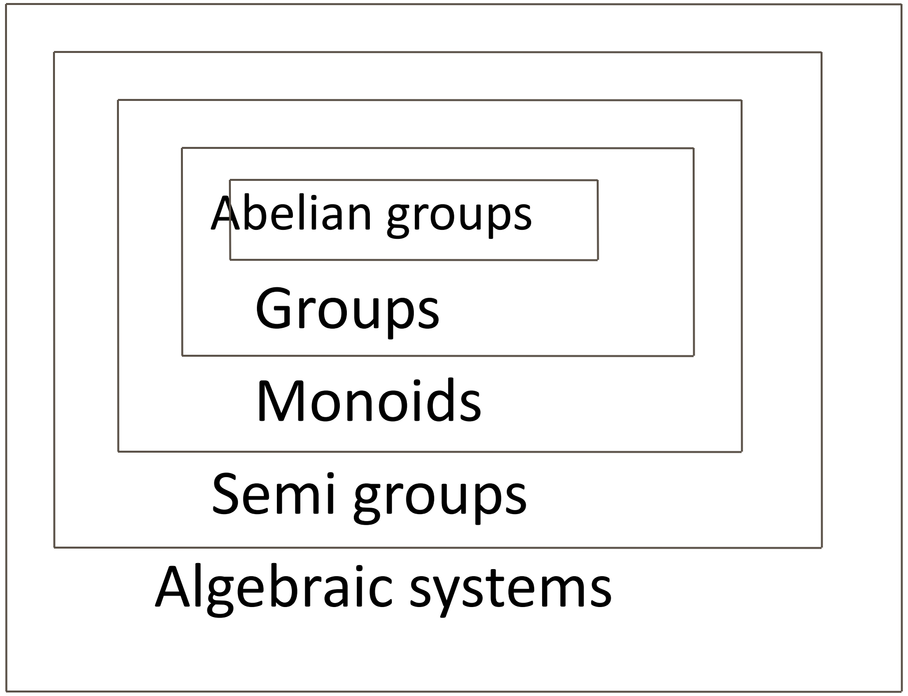
Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.
  1) * is a closed operation.
  2) * is an associative operation.
  3) There is an identity in G.
  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $$a * b = b * a \quad \forall a, b \in G.$$

Algebraic systems



Theorem

- In a Group (G, *) the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

   $a * b = a * c \Rightarrow b = c$ (left cancellation law)

   $a * c = b * c \Rightarrow a = b$ (Right cancellation law)

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

- In a group, the identity element is its own inverse.

- ***<u>Order of a group</u>*** : The number of elements in a group is called order of the group.

- <u>Finite group</u>: If the order of a group G is finite, then G is called a finite group.

Ex. Show that, the set of all integers is a group with respect to addition.

- Solution: Let Z = set of all integers.

  Let a, b, c are any three elements of Z.

1. Closure property : We know that, Sum of two integers is again an integer.

   i.e., $a + b \in Z$ for all $a,b \in Z$

2. Associativity: We know that addition of integers is associative.

   i.e., $(a+b)+c = a+(b+c)$ for all $a,b,c \in Z$.

3. Identity : We have $0 \in Z$ and $a + 0 = a$ for all $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

4. Inverse: To each $a \in Z$, we have $-a \in Z$ such that

   $a + (-a) = 0$

   Each element in Z has an inverse.

Contd.,

- 5. Commutativity: We know that addition of integers is commutative.

  i.e., $a + b = b + a$ for all $a, b \in Z$.

  Hence, $(Z , +)$ is an abelian group.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

- Solution: Let R^* = set of all non zero real numbers.

  Let a, b, c are any three elements of R^* .

1. <u>Closure property</u> : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a . b \in R^*$ for all $a,b \in R^*$.

2. <u>Associativity</u>: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. <u>Identity</u> : We have $1 \in R^*$ and $a .1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. <u>Inverse</u>: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a .(1/a) = 1$ i.e., Each element in R^* has an inverse.

Contd.,

- 5.<u>Commutativity</u>: We know that multiplication of real numbers is commutative.

  i.e., $a \,.\, b = b \,.\, a$ for all $a,b \in R^*$.

  Hence, $(R^*, .)$ is an abelian group.

- <u>Ex:</u> Show that set of all real numbers ‘R’ is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

  The multiplicative inverse of 0 does not exist.

  Hence. R is not a group.

Example

- Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by $n * m$ = maximum of (n, m).

  Show that (Z, *) is a semi group.

  Is (Z, *) a monoid ?. Justify your answer.

- Solution: Let a , b and c are any three integers.

<u>Closure property</u>: Now, $a * b$ = maximum of $(a, b) \in Z$ for all $a,b \in Z$

<u>Associativity</u> : $(a * b) * c$ = maximum of $\{a,b,c\} = a * (b * c)$

$\therefore$ (Z, *) is a semi group.

<u>Identity</u> : There is no integer x such that

$a * x$ = maximum of $(a, x) = a$ for all $a \in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition * defined by

$$a * b = (ab)/2 .$$

- Solution: Let A = set of all positive rational numbers.

Let a,b,c be any three elements of A.

1. <u>Closure property:</u> We know that, Product of two positive rational numbers is again a rational number.

i.e., $a * b \in A$ for all $a,b \in A$.

2. <u>Associativity</u>: $(a*b)*c = (ab/2) * c = (abc) / 4$

$a*(b*c) = a * (bc/2) = (abc) / 4$

3. <u>Identity</u> : Let e be the identity element.

We have $a*e = (a\, e)/2$ …(1) , By the definition of *

again, $a*e = a$ …..(2) , Since e is the identity.

From (1)and (2), $(a\, e)/2 = a \Rightarrow e = 2$ and $2 \in A$.

$\therefore$ Identity element exists, and ‘2’ is the identity element in A.

Contd.,

- 4. <u>Inverse:</u> Let $a \in A$

  let us suppose b is inverse of a.

  Now, $a * b = (a\ b)/2$ ….(1) (By definition of inverse.)

  Again, $a * b = e = 2$ …..(2) (By definition of inverse)

  From (1) and (2), it follows that

  $(a\ b)/2 = 2$

  $\Rightarrow$ $b = (4 / a) \in A$

$\therefore$ (A ,*) is a group.

- Commutativity: $a * b = (ab/2) = (ba/2) = b * a$
- Hence, (A,*) is an abelian group.

Theorem

- Ex. In a group (G, *) , Prove that
  $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a,b \in G$.
- <u>Proof :</u>
- Consider,
- $(a * b) * (b^{-1} * a^{-1})$
- $= (a * (b * b^{-1}) * a^{-1})$ (By associative property).
- $= (a * e * a^{-1})$ (By inverse property)
- $= (a * a^{-1})$ (Since, e is identity)
- $= e$ (By inverse property)
- Similarly, we can show that
- $(b^{-1} * a^{-1}) * (a * b) = e$
- Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Finite groups

- Ex. Show that G = {1, -1} is an abelian group under multiplication.
- Solution: The composition table of G is

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

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are real numbers, and we know that multiplication of real numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of 1 and -1 are 1 and -1 respectively.

Contd.,

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical.

   Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication..

Ex. Show that $G = \{1, \omega, \omega^2\}$ is an abelian group under multiplication. Where $1, \omega, \omega^2$ are cube roots of unity.

- Solution: The composition table of G is

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

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.
3. Identity : Here, 1 is the identity element and $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of $1\ \omega, \omega^2$ are $1, \omega^2, \omega$ respectively.

Contd.,

- Hence, G is a group w.r.t multiplication.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.
- Hence, G is an abelian group w.r.t. multiplication.

Ex. Show that $G = \{1, -1, i, -i\}$ is an abelian group under multiplication.

- Solution: The composition table of G is

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

1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. <u>Associativity</u>: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.
3. <u>Identity</u> : Here, 1 is the identity element and $1 \in G$.

Contd.,

- 4. Inverse: From the composition table, we see that the inverse elements of

  1 -1, i, -i are 1, -1, -i, i respectively.

- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative. Hence, (G, .) is an abelian group.

Modulo systems.

- <u>Addition modulo m</u> ($+_m$)
- let m is a positive integer. For any two positive integers a and b
- $a +_m b = a + b$ if $a + b < m$
- $a +_m b = r$ if $a + b \geq m$ where r is the remainder obtained
- by dividing (a+b) with m.
- <u>Multiplication modulo p</u> ($\times_p$)
- let p is a positive integer. For any two positive integers a and b
- $a \times_p b = a b$ if $a b < p$
- $a \times_p b = r$ if $a b \geq p$ where r is the remainder obtained
- by dividing (ab) with p.
- Ex. $3 \times_5 4 = 2$, $5 \times_5 4 = 0$, $2 \times_5 2 = 4$

Ex.The set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

- Solution: The composition table of G is

$+_6$	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

- 1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Contd.,

- 2. <u>Associativity</u>: The binary operation $+_6$ is associative in G.

  for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

  $2 +_6 (3 +_6 4) = 2 +_6 1 = 3$
- 3. <u>Identity</u> : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.
- 4. . <u>Inverse</u>: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4. 5 are 0, 5, 4, 3, 2, 1 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.
- Hence, $(G, +_6)$ is an abelian group.

Ex.The set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

- Solution: The composition table of G is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- 1. <u>Closure property:</u> Since all the entries of the composition table are the elements of the given set, the set G is closed under $\times_7$.

Contd.,

- 2. Associativity: The binary operation $\times_7$ is associative in G.

  for ex. $(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$ and

  $2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$
- 3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 1 is the identity element.
- 4. . Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5 ,6 are 1, 4, 5, 2, 5, 6 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $\times_7$ is commutative.
- Hence, $(G, \times_7)$ is an abelian group.

- **Order of an element of a group:**
- Let (G, *) be a group. Let 'a' be an element of G. The smallest integer n such that $a^n = e$ is called order of 'a'. If no such number exists then the order is infinite.

Examples

- Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.
- The order 1 is
- The order -1 is
- The order i is
- The order -i is

Sub groups

- Def. A non empty sub set H of a group (G, *) is a sub group of G,
- if (H, *) is a group.

Note: For any group {G, *}, {e, * } are trivial sub groups.

- Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.

  H_1 = { 1, -1 } is a subgroup of G .

  H_2 = { 1 } is a trivial subgroup of G.
- Ex. (Z , +) and (Q , +) are sub groups of the group (R +).
- Theorem: A non empty sub set H of a group (G, *) is a sub group of G iff
- i) $a * b \in H \quad \forall\, a, b \in H$
- ii) $a^{-1} \in H \quad \forall\, a \in H$

Cosets

- If H is a sub group of(G, *) and a $\in$ G then the set

$Ha = \{ h * a \mid h \in H\}$ is called a right coset of H in G.

Similarly $aH = \{a * h \mid h \in H\}$ is called a left coset of H is G.

- ***Note:-*** 1) Any two left (right) cosets of H in G are either identical or disjoint.
- 2) Let H be a sub group of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a sub group H is equal to G.

3) Lagrange's theorem: The order of each sub group of a finite group is a divisor of the order of the group.

Lagrange's Theorem

- Lagrange's theorem: The order of each sub group H of a finite group G is a divisor of the order of the group.

Permutation Group

- Definition:-

Let S be a finite set having n distinct elements . A one-one mapping S to S itself is called a permutation of degree n on set S.

Symbol of permutation :

$$Let\ S = \{a_1, a_2, a_3 ......a_n\} be\ a\ finite\ set$$

$with\ n\ distinct\ elements .let\ f : S \rightarrow S\ be\ a\ 1-1\ mapping$

$of\ S\ on\ to\ itself\ .$

$f(a_1) = b_1, f(a_2) = b_2 ......f(a_n) = b_n,\ then\ written\ as\ follows$

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 ......a_n \\ b_1 & b_2 & b_3 & b_4 ....b_n \end{pmatrix}$$

Degree of permutation Group

The number of elements in a finite set S is called as degree on permutation. If n is a degree of permutation mean having n! permutations

Example: Let S=(1,2,3,4,5)and f is a permutation on set S itself.

5! = 120 permutations

Identity permutation

If I is a permutation of degree n such that I replaces each element by itself then I is called identity permutation of degree n.

i.e. $f(a)=a$

Ex. $I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

$\therefore$ I is identity permutation.

Inverse of permutation

Example 1-: Find the inverse of permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

A^{-1} $\therefore$ *Required inverse is* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

Example 2-: Calculate A^{-1} if A= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Equality of Permutations

Two permutations f and g with degree n are said to be equal if f(a)=g(a).

Ex. $f=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $g = \begin{pmatrix} 4 & 3 & 2 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

$\therefore$ f(a)=g(a)

Product of Permutations

The product or composition of two permutation f and g with degree n denoted by f. g, obtained by first carrying out operation defined by f and then g.

i.e. $f \cdot g(x) = f(g(x))$

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

Problem: If $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ $and\, B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$

Find the product of permutation A.B and B.A

Solution: $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ $and\, B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$

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

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

Similarly,

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

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

Example 3-: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$ *and* $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

then compute $f^{-1} o\, g^{-1}$.

Solution-:

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

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

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

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

Example 4-: If $P1=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$, $P2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $P3=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$

Find $(P1 \text{ o } P2)^{-1}$ **and** $(P2 \text{ o } P3)^{-1}$.

Solution-: $P1 \text{ o } P2=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} o \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$

$P2 \text{ o } P3=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} o \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$

Also, we know that if P^{-1} *be the inverse of permutation P, then* $P^{-1} \text{ o } P = I$.

$\therefore (P1 \text{ o } P2)^{-1}$ = *inverse of* $\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$

$\therefore (P2 \text{ o } P3)^{-1}$ = *inverse of* $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$