Groups

Abstract Algebra : Sen, Ghosh, Mukhopadhyay
: Malik, Mordeson, Sen
Higher Algebra : S.K. Mapa.
Abstract Algebra : Sen, Ghosh, Mukhopadhyay, Maity
: Vijay K. Khanna, S.K. Bhambri.

Binary composition:

Let A be a non-empty set. A binary composition or a binary operation on A is a mapping $f : A \times A \longrightarrow A$. Therefore for each ordered pair of elements of A, f assigns a definite element of A. A binary composition is ~~defined by~~ denoted by the symbols like $\circ, *$ etc.

~~Example~~: A binary composition $\circ$ is said to be defined on a non-empty set A if $a \circ b \in A$ for all $a, b \in A$.

In this case the set A is said to be closed under the binary composition $\circ$.

Example : (i) Let $\mathbb{Z}$ be the set of integers. Addition and multiplication is said to be binary composition since

$5 \circ 6 = 5 + 6 = 11 \in \mathbb{Z}$ and $5 \circ 6 = 5 \times 6 = 30 \in \mathbb{Z}$ for $5, 6 \in \mathbb{Z}$

(ii) Let N be the set of natural numbers. Subtraction is not a binary composition on the set N since $2, 3 \in N$ but $2 \circ 3 = 2 - 3 = -1 \notin N$

Let G be a non-empty set and ~~an algebraic sys~~ a binary composition $\circ$ is defined on G. The $(G, \circ)$ is an algebraic system. Also $(G, +, \cdot)$ is also an algebraic system when two binary composition + and . are imposed.

Groupoid : A non-empty set G together with a binary composition $\circ$ ie the algebraic system $(G, \circ)$ is called a Groupoid.

Note : (i) In a groupoid $(G, \circ)$, G is closed under the binary composition $\circ$.

(ii) The set G may form two different groupoids with respect to different binary compositions on it.

(iii) A groupoid $(G, \circ)$ may be commutative and it may have identity element

Semi-group : A non-empty set G together with a binary composition $\circ$ is said to be a semi-group if

(i) G is closed under $\circ$ i.e $a \circ b \in G$ for $a, b \in G$.

and (ii) Binary composition $\circ$ is associative

i.e $a \circ (b \circ c) = (a \circ b) \circ c$ for $a, b, c \in G$.

Example : $(Z, +), (Z, \cdot), (Q, +), (R, +), (Q, \cdot)$ $(R, \cdot)$ are semigroups but $(Z, -)$ is not a semigroup.

Note : A groupoid $(G, \circ)$ is said to be a semigroup if $\circ$ is associative.

Monoid : A non-empty set G together with a binary Composition $\circ$ is said to be monoid if

(i) G is closed under $\circ$

(ii) $\circ$ is associative i.e $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$

and (iii) There exist an element e in G such that

$e \circ a = a \circ e = a$ for all a in G.

Note : A groupoid $(G, \circ)$ containing the identity element e is said to be a monoid if $\circ$ is associative.

Example (i) $(Z, +)$ is a monoid, 0 is the identity element

(ii) $(Z, \cdot)$ is a monoid, 1 is the identity element.

(iii) Let E be the set of all even integers. Then $(E, \cdot)$ is a semigroup but not a monoid.

Identity element

A set S has an identity element e under a binary operation o if $a \circ e = e \circ a = a$ for all $a \in S$. If $a \circ e = a$, then e is called right identity and if $e \circ a = a$ then e is called the left identity.

When $0, a \in S$ and $0 + a = a + 0 = a$, then 0 is the identity element with additive operation +.

If $1 \cdot a = a \cdot 1 = a$, then 1 is the identity element of S under multiplication

Inverse element

Let $a \in S$. If there exists an element b in the set S such that $a \circ b = b \circ a = e$ where e is the identity element of S, then b is called the inverse of a in S and denoted by $\bar{a}^1$ ie $b = \bar{a}^1$.

If $a \circ \bar{a}^1 = e$, then $\bar{a}^1$ is called the right inverse of a and if $\bar{a}^1 \circ a = e$, then $\bar{a}^1$ is called the left inverse of a.

Group

Defⁿ: A non-empty set G together with a binary operation 'o' is called a group if the following axioms are satisfied :-

(i) closure axiom: If $a, b \in G$, then $a \circ b \in G$

(ii) Associative axiom:
$a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$

(iii) Identity axiom: There exists an identity element e in G ie $a \circ e = e \circ a = a$ for every a in G.

(iv) Inverse axiom: G contains an inverse for every element of it. If $a \in G$, then $\bar{a}^1 \in G$ and $a \circ \bar{a}^1 = \bar{a}^1 \circ a = e$.

A group containing a finite number of elements is called a finite group.

A group containing infinite number of elements is called infinite group.

Abelian group or Commutative group :—

If in a group G Commutative property satisfied, then that group is called abelian group.

In abelian group, $a \circ b = b \circ a$ for all $a, b \in G$.

Note : An additive abelian group is sometimes called a module.

Ex-1 Show that the set of all integers Z forms an abelian group under additive operation.

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

Soln Let $a, b \in Z$, Then $a+b \in Z$

$\therefore$ closure property satisfied.

Let $a, b, c \in Z$, Then $(a+b)+c = a+(b+c)$

$\therefore$ Associative prop. hold under $+$.

$0 \in Z$ and $0+a = a+0 = a \quad \forall a \in Z$

ie 0 is the identity element in Z.

Let $a \in Z$, Then $-a \in Z$ and $a+(-a) = (-a)+a = 0$

$\therefore -a$ is the inverse of a

$\therefore (Z, +)$ is a group

Also, if $a, b \in Z$, Then $a+b = b+a$ hold

$\therefore$ commutative property under addition hold

$\therefore (Z, +)$ is an abelian group.

If the set contains n elements, then the set of permutations P will contain $n!$ elements, as n distinct elements can be arranged in $n!$ ways

The set of all permutations of a set containing n elements is denoted by P_n

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

$$P_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Symmetric group P_n (or, permutation group)

Th The set P_n of all permutations on a set P of n elements forms a group of order $n!$ under multiplication.

Proof: (i) By the definition of the product of permutation it is clear that $P, Q \in P_n \Rightarrow PQ \in P_n$

$\therefore$ closure axiom satisfied.

(ii) For three permutation $P, Q, R \in P_n$

$$(PQ)R = P(QR)$$

ie, associative law holds in P_n.

(iii) Let $P \in P_n$, then we have

$PI = IP = P$ where I is a permutation in P_n

$\therefore I$ is the identity element in P_n.

(iv) Also, $P\bar{P}^{-1} = \bar{P}^{-1}P = I$ for $P, \bar{P}^{-1} \in P_n$,

$\therefore$ Inverse axiom also satisfied.

Hence, the set P_n forms a group

Symmetric group S_3 B11'07

Let $S = \{1, 2, 3\}$. First we consider all the permutations $p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Then $S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$

S_3 contains $3! = 6$ elements.

The composition table for multiplication of permutation is given by

$*$	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_5	p_3	p_4
p_2	p_2	p_0	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_3	p_2	p_0	p_1
p_5	p_5	p_3	p_4	p_1	p_2	p_0

From the composition table, we see that product of any two permutation is an element of S_3.

$\therefore$ S_3 is closed under multiplication.

A permutation on S is a bijective mapping onto itself. product of permutations is the composition of two bijective mapping. Since composition of mapping is associative, multiplication of permutations is associative.

From the table, we see that for any $p \in S_3$, $p p_0 = p = p_0 p$

$\therefore$ p_0 is the identity element of S_3.

Also it is seen from the table that the inverses of $p_0, p_1, p_2, p_3, p_4, p_5$ are $p_0, p_2, p_1, p_3, p_4, p_5$. i.e, inverse axiom is satisfied.

Hence, S_3 forms a group under multiplication

The multiplication table is not symmetric about the main diagonal. So multiplication is not commutative

So S_3 forms a non-abelian group. It is called the symmetric group of degree 3. The order of the group is 6.

Note: (i) Similarly S_4, the set of all permutations of the set $S=\{1, 2, 3, 4\}$ forms a non-abelian group of degree 4 with 24 elements.

S.Q (i) Construct a non-commutative group containing 6 elements.
ii) Construct a non-commutative group with 24 elements.

Alternating group

The set of all even permutations of the set $S=\{1, 2, 3 \cdots n\}$ forms a group w.r.t multiplication of permutations. This group is called alternating group of degree n and is denoted by A_n.

In particular, Let $S=\{1, 2, 3\}$, then even permutations are $P_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $P_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $P_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

Then $A_3=\{P_0, P_1, P_2\}$ forms a group of degree 3 and order 3.

The composition table is.

*	P_0	P_1	P_2
P_0	P_0	P_1	P_2
P_1	P_1	P_2	P_0
P_2	P_2	P_0	P_1

From the table it is seen that A_3 is closed.
product of permutation is associative.
P_0 is the identity element and the inverses of P_0, P_1, P_2 are P_0, P_2, P_1.

Hence, A_3 forms a group under the product of permutation
From the table it is seen that commutative law holds.

Note: (i) The set of all odd permutations does not form a group. Since product of two odd permutation is even.
∴ closure axiom is not satisfied.