13

Algebraic Structures

If there exists a system such that it consists of a non-empty set and one or more operations on that, set, then that system is called an algebraic system. It is generally denoted by $(A, op_1, op_2, ..., op_n)$, where A is a non-empty set and $op_1, op_2, ..., op_n$ are operations on A.

An algebraic system is also called an algebraic structure because the operations on the set A define a structure on the elements of A.

N-ARY OPERATION

A function $f: A \times A \times ... A \to A$ is called an n-ary operation.

BINARY OPERATION

Consider a non-empty set A and a function f such that $f: A \times A \to A$ is called a binary operation on A. If $*$ is a binary operation on A, then it may be written as $a * b$.

A binary operation can be denoted by any of the symbols $+, -, *, \oplus, \Delta, \square, \vee, \wedge$ etc.

The value of the binary operation is denoted by placing the operator between the two operands.

e.g., (*i*) The operation of addition is a binary operation on the set of natural numbers.

(*ii*) The operation of subtraction is a binary operation on set of integers. But, the operation of subtraction is not a binary operation on the set of natural numbers because the subtraction of two natural numbers may or may not be a natural number.

(*iii*) The operation of multiplication is a binary operation on the set of natural numbers set of integers and set of complex numbers.

(*iv*) The operation of set union is a binary operation on the set of subsets of a universal set. Similarly, the operation of set intersection is a binary operation on the set of subsets of universal set.

TABLES OF OPERATION

Consider a non empty finite set $A = \{a_1, a_2, a_3, ..., a_n\}$. A binary operation $*$ on A can described by means of table as shown in Fig. 1.

	a_1	a_2	a_3		a_n
a_1	a_1*a_1				
a_2		a_2*a_2			
a_3			a_3*a_3		
a_n					a_n*a_n

Fig. 1.

e empty in the jth row and kth column represent the element a_j*a_k.

ample 1. *Consider the set $A = \{1, 2, 3\}$ and a binary operation $*$ on the set A defined by*

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

present operation $*$ as a table on A.

l. The table of the operation is shown in Fig. 2.

*	1	2	3
1	4	6	8
2	6	8	10
3	8	10	12

Fig. 2.

TIES OF BINARY OPERATIONS

re are many properties of the binary operations which are as follows :

losure Property. Consider a non-empty set A and a binary operation * on A. Then under the operation *, if $a * b \in A$, where a and b are elements of A.

peration of addition on the set of integers is a closed operation.

ample 2. *Consider the set $A = \{-1, 0, 1\}$. Determine whether A is closed under (i) (ii) multiplication.*

l. (*i*) The sum of the elements is $(-1) + (-1) = -2$ and $1 + 1 = 2$ does not belong to A. s not closed under addition.

The multiplication of every two elements of the set are

$-1 * 0 = 0$; $-1 * 1 = -1$; $-1 * -1 = 1$

$0 * -1 = 0$; $0 * 1 = 0$; $0 * 0 = 0$

$1 * -1 = -1$; $1 * 0 = 0$; $1 * 1 = 1$

ce, each multiplication belongs to A hence A is closed under multiplication.

ample 3. *Consider the set $A = \{1, 3, 5, 7, 9, \ldots\}$, the set of odd +ve integers. Determine is closed under (i) addition (ii) multiplication.*

l. (i) The set A is not closed under addition because the addition of two odd numbers an even number which does not belong to A.

SEMIGROUP

Let us consider, an algebraic system $(A, *)$, where $*$ is a binary operation on A. Then, the system $(A, *)$ is said to be a semi-group if it satisfies the following properties :

1. The operation $*$ is a closed operation on set A.
2. The operation $*$ is an associative operation.

Example 8. *Consider an algebraic system $(A, *)$, where $A = \{1, 3, 5, 7, 9, ...\}$, the set of all positive odd integers and $*$ is a binary operation means multiplication. Determine whether $(A, *)$ is a semi-group.*

Sol. Closure property. The operation $*$ is a closed operation because multiplication of two +ve odd integers is a +ve odd number.

Associative property. The operation $*$ is an associative operation on set A. Since for every $a, b, c \in A$, we have

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

Hence, the algebraic system $(A, *)$ is a semigroup.

Example 9. *Consider the algebraic system $(\{0, 1\}, *)$, where $*$ is a multiplication operation. Determine whether $(\{0, 1\}, *)$ is a semigroup.*

Sol. Closure property. The operation $*$ is a closed one on the given set since

$$0 * 0 = 0 \; ; \; 0 * 1 = 0 \; ; \; 1 * 0 = 0 \; ; \; 1 * 1 = 1.$$

Associative property. The operation $*$ is associative since we have

$$(a * b) * c = a * (b * c) \; \forall \; a, b, c$$

Since, the algebraic system is closed and associative. Hence, it is a semi-group.

Example 10. *Let $(A, *)$ be semi-group. Show that for a, b, c in A, if $a * c = c * a$ and $b * c = c * b$, then $(a * b) * c = c * (a * b)$.*

Sol. Take L.H.S., we have

$$(a * b) * c \quad \Rightarrow \quad a * (b * c) \qquad [\because \; * \text{ is associative}$$

$$\Rightarrow \quad a * (c * b) \qquad [\because \; b * c = c * b$$

$$\Rightarrow \quad (a * c) * b \qquad [\because \; * \text{ is associative}$$

$$\Rightarrow \quad (c * a) * b \qquad [\because \; a * c = c * a$$

$$\Rightarrow \quad c * (a * b) \qquad [\because \; * \text{ is associative}$$

Which is equal to R.H.S.

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

SUBSEMIGROUP

Consider a semigroup $(A, *)$ and let $B \subseteq A$. Then the system $(B, *)$ is called a subsemigroup if the set B is closed under the operation $*$.

e.g., Consider a semigroup (N, +), where N is the set of all natural numbers and + is an addition operation. The algebraic system (E, +) is a subsemigroup of (N, +), where E is a set of +ve even integers.

SEMIGROUP

...nsider a nonempty set $\Lambda = \{a_1, a_2, \ldots\ldots, a_n\}$.
...e Λ^* is the set of all finite sequences of elements of Λ, *i.e.*, Λ^* consists of all words ...be formed from the alphabet of Λ.
... β and γ are any elements of Λ^*, then $\alpha \,.\, (\beta \,.\, \gamma) = (\alpha \,.\, \beta) \,.\, \gamma$
...ere $*$ is a concatenation operation, which is an associative operation as shown above.
...hus $(\Lambda^*, *)$ is a semigroup. This semigroup $(\Lambda^*, *)$ is called the free semigroup gener-...
...ed by Λ.

...CT OF SEMIGROUP

...heorem. *If $(S_1, *)$ and $(S_2, *)$ are semigroups, then $(S_1 \times S_2, *)$ is a semigroup, where $*$ ...ed by $(s_1', s_2') * (s_1'', s_2'') = (s_1' * s_1'', s_2' * s_2'')$.*

...oof. The semigroup $S_1 \times S_2$ is closed under the operation $*$.

...sociativity of $*$. Let $a, b, c \in S_1 \times S_2$

$$\begin{aligned} a * (b * c) &= (a_1, a_2) * ((b_1, b_2) * (c_1, c_2)) \\ &= (a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2) \\ &= (a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2) \\ &= ((a_1 *_1 b_1) *_1 c_1, (a_2 *_2 b_2) *_2 c_2) \\ &= (a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2) \\ &= ((a_1, a_2) * (b_1, b_2)) * (c_1, c_2) \\ &= (a * b) * c. \end{aligned}$$

...ce $*$ is closed and associative. Hence $S_1 \times S_2$ is a semigroup.

...UENCE RELATION

An equivalence relation R on the semigroup $(S, *)$ is called a congruence relation if

$$\begin{aligned} &aRa' \quad \text{and} \quad bRb' \\ &(a * b)\, R\, (a' * b') \end{aligned}$$

...ample 11. *Let $(I, +)$ be a semigroup and R is an equivalence relation on I defined by aRb iff $a \equiv b$ (MOD 3).*

...]. If a and b yield the same remainder when divided by 3, then we have 3 divides $(a - b)$.

...w, if $a \equiv b$ (MOD 3) and $c \equiv d$ (MOD 3) then 3 divides $a - b$ and 3 divides $c - d$.

...us, we can write $a - b = 3m$ ...(*i*)

$c - d = 3n$ ...(*ii*)

...re m and n are same integer of I.

...lding eqns. (*i*) and (*ii*), we have

$$(a - b) + (c - d) = 3m + 3n \quad \text{or} \quad (a + c) - (b + d) = 3(m + n)$$

$$a + c = b + d \text{ (MOD 3)}$$

...us, the relation is a congruence relation.

Example 12. *Consider the set A = {a, b}. Let (A*, •) is the semigroup generated by A, also let R is a relation on A defined by αRβ iff α and β have the same number of a's.*

Show whether the relation R is a congruence on (A, •).*

Sol. First of all we will show that R is an equivalence relation. So, for that we will check reflexive, symmetric and transitive properties of the relation R.

Reflexive. αRα for any α ∈ A* since α has same number of *a*'s as itself. Thus, R is reflexive.

Symmetric. If α and β have same number of *a*'s, then αRβ or we can say βRα. Thus, R is symmetric.

Transitive. If αRβ, it means α and β have same number of *a*'s. If βRγ, it means β and γ have same number of *a*'s. It implies α and γ have same number of *a*'s *i.e.*, αRγ. Thus, R is transitive.

Hence, R is an equivalence relation.

To show that R is a congruence relation, let us assume that $\alpha R \alpha_1$ and $\beta R \beta_1$. It means α and α_1 have same number of *a*'s and β and β_1 have same number of *a*'s. We know that the number of *a*'s in α . β is the sum of number of *a*'s in α and the number of *a*'s in β.

From the above discussion, we can say that the number of *a*'s in α .β is same as in $\alpha_1 . \beta_1$.

Hence $(\alpha . \beta)\ R\ (\alpha_1 . \beta_1)$

which shows that R is a congruence relation.

Example 13. *Consider the semigroup (I, +), where + is an addition operation. Let $f(x) = x^2 - 2x - 3$ and also let R is a relation on I defined by aRb iff f(a) = f(b).*

Show whether R is a congruence relation.

Sol. It can be easily shown that the relation R is an equivalence relation on the set I.

To check whether R is congruence relation or not, we will try to find two pair of numbers *a*R*b* and *c*R*d* but $(a + b)\ \mathrm{R}\ (c + d)$ if possible. Then we will say R is not a congruence relation.

Thus, we have

$2\ \mathrm{R}\ 0$ *i.e.*, $f(2) = f(0) = -3$

and $-2\ \mathrm{R}\ 4$ *i.e.*, $f(-2) = f(4) = 5$

But $(2 + (-2))\ \mathrm{R}\ (0 + 4)$ *i.e.*, $0\ \mathrm{R}\ 4$

As $f(0) = -3$ and $f(4) = 5$

Hence, R is not a congruence relation.

MONOID

Let us consider an algebraic system (A, *o*), where *o* is a binary operation on A. Then the system (A, *o*) is said to be a monoid if it satisfies the following properties.

(*i*) The operation *o* is a closed operation on set A.

(*ii*) The operation *o* is an associative operation.

(*iii*) There exists an identity element w.r.t. the operation *o*.

Example 14. *Consider an algebraic system (N, +), where the set N = {0, 1, 2, 3, 4, ...} the set of natural numbers and + is an addition operation. Determine whether (N, +) is a monoid.*

Sol. Closure property. The operation + is closed since sum of two natural numbers is a natural number.

Associative property. The operation + is an associative property since we have
$(a + b) + c = a + (b + c) \forall a, b, c \in N.$

Identity. There exists an identity element in set N w.r.t. the operation +. The element identity element w.r.t. the operation +. Since, the operation + is a closed, associative ere exists an identity. Hence, the algebraic system (N, +) is a monoid.

ONOID

Let us consider a monoid (M, o), also let S $\subseteq$ M. Then (S, o) is called a submonoid of if and only if it satisfies the following properties.

(i) S is closed under the operation o.

(ii) There exists an identity element $e \in T$.

t us consider, a monoid (M, *),where * is a binary operation and M is a set of all integers. M_1, *) is a submonoid of (M, *), where M_1 is defined as

$M_1 = \{a^i \mid i$ is from 0 to n, a positive integer and $a \in M\}$.

P

Let us consider an algebraic system (G, *), where * is a binary operation on G. Then the (G, *) is said to be a group if it satisfies following properties.

i) The operation * is a closed operation.

i) The operation * is an associative operation.

i) There exists an identity element w.r.t. the operation *.

v) For every $a \in G$, there exists an element $a^{-1} \in G$ such that

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

e algebraic system (I, +), where I is the set of all integers and + is an addition operation, up. The element 0 is the identity element w.r.t. the operation +. The inverse of every t $a \in I$ is $-a \in I$.

Example 15. *Determine whether the algebraic system (Q, +) is a group where Q is the set ational numbers and + is an addition operation.*

Sol. Closure property. The set Q is closed under operation +, since the addition of two al numbers is a rational number.

Associative Property. The operation + is associative, since $(a + b) + c = a + (b + c) \forall a,$ Q.

Identity. The element 0 is the identity element. Hence $a + 0 = 0 + a = a \forall a \in Q$.

Inverse. The inverse of every element $a \in Q$ is $-a \in Q$. Hence the inverse of every nt exists.

Since, the algebraic system $(a, +)$ satisfy all the properties of a group, hence $(a, +)$ is a

Example 16. *Consider an algebraic system (Q, *),where Q is the set of rational numbers is a binary operation defined by*

$$a * b = a + b - ab \forall a, b \in Q.$$

Determine whether (Q, +) is a group.

Sol. Closure property. Since the element $a, b \in Q$ for every $a, b \in Q$, hence, the set Q is closed under the operation *.

Associative property. Let us assume $a, b, c \in Q$, then we have

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

Similarly, $a * (b * c) = a + b + c - ab - ac - bc + abc.$

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

$\therefore$ * is associative.

Identity. Let e is an identity element. Then we have $a * e = a \; \forall \; a \in Q$

$\therefore$ $a + e - ae = a$ or $e - ae = 0$

or $e(1 - a) = 0$ or $e = 0$

Similarly, $e * a = a \; \forall \; a \in Q$

Therefore, for $e = 0$, we have $a * e = e * a = a$

Thus 0 is the identity element.

Inverse. Let us assume an element $a \in Q$. Let a^{-1} is an inverse of a, where $a^{-1} \in Q$. Then we have

$$a * a^{-1} = 0 \qquad \text{[Identity]}$$

$\therefore$ $a + a^{-1} - aa^{-1} = 0$

or $$a^{-1}(1 - a) = -a \quad \text{or} \quad a^{-1} = \frac{a}{a - 1}$$

Now, $\frac{a}{a-1} \in Q$, if $a \neq \frac{1}{a}$

Therefore, every element has inverse such that $a \neq 1$.

Since, the algebraic system (Q, *) satisfy all the properties of a group. Hence, (Q,*) is a group.

Theorem II. *Show that the identity element in a group is unique.*

Proof. Let us assume that there exists two identity elements of G *i.e.*, e and e'.

Since, $e \in G$ and e' is an identity.

We have $e'e = ee' = e$

Also, $e' \in G$ and e is an identity. We have $e'e = ee' = e'$

$\therefore$ $e = e'$

Hence, identity in a group is unique.

Theorem III. *Show that inverse of an element a in the group is unique.*

Proof. Let us assume that $a \in G$ be an element. Also, assume that a_1^{-1} and a_2^{-1} be two inverse elements of a.

Then we have

$$a_1^{-1}a = aa_1^{-1} = e \quad \text{and} \quad a_2^{-1}a = aa_2^{-1} = e$$

Now, $$a_1^{-1} = a_1^{-1}e = a_1^{-1}(aa_2^{-1}) = (a_1^{-1}a)a_2^{-1} = ea_2^{-1} = a_2^{-1}$$

Thus, the inverse of an element is unique.

...heorem IV. *Show that* $(a^{-1})^{-1} = a$ *for all* $a \in G$, *where* G *is a group and* a^{-1} *is an*

...roof. Given that a^{-1} is an inverse of a. Then, we have

$$aa^{-1} = a^{-1}a = e$$

...his implies that a is also an inverse of a^{-1}. Therefore $(a^{-1})^{-1} = a$.

...heorem V. *Show that* $(ab)^{-1} = b^{-1}a^{-1}$ *for all* $a, b \in G$.

...roof. We have to prove that ab is inverse of $b^{-1}a^{-1}$.

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

...ow, take L.H.S.

$$(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1} = [a(bb^{-1})]a^{-1}$$
$$= (ae)a^{-1} = aa^{-1} = e$$

...milarly, the R.H.S. *i.e.*, $(b^{-1}a^{-1})(ab) = e$

...ence proved.

...heorem VI. *Prove the left cancellation law i.e.,* $ab = ac \Rightarrow b = c \; \forall \; a, b, c \in G$.

...roof. Consider that $ab = ac$.

...hen, we have $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac)$ $[\because ab = ac]$

$$= (a^{-1}a)c = ec = c$$

...ence, $ab = ac \Rightarrow b = c$.

...heorem VII. *Prove the right cancellation law i.e.,* $ba = ca \Rightarrow b = c \quad \forall \; a, b, c \in G$.

...roof. Consider that $ba = ca$.

...hen, we have $b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1}$ $[\because ba = ca]$

$$= c(aa^{-1}) = ce = c$$

...ence, $ba = ca \Rightarrow b = c$.

o(G)

...AND INFINITE GROUP

...group (G, *) is called a finite group if G is a finite set.

...group (G, *) is called an infinite group if G is an infinite set.

...or example : The group (I, +) is an infinite group as the set I of integers is an infinite set.

...or example : The group G = {1, 2, 3, 4, 5, 6, 7} under multiplication modulo 8 is a finite ...s the set G is a finite set.

...R OF GROUP

...he order of the group G is the number of elements in the group G. It is denoted by |G|.

...p of order 1 has only the identity element *i.e.*, ({e} *).

...A group of order 2 has two elements *i.e.*, one identity element and one some other ele-

For example : *Let ({e, x}, *) be a group of order 2. The table of operation is shown in* ...).

*	e	x
e	e	x
x	x	e

Fig. 3.

The group of order 3 has three elements *i.e.*, one identity element and two other elements.

For example : *Let $(\{e, x, y\}, *)$ be a group of order 3. The table of operation is shown in (Fig. 4).*

*	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Fig. 4.

For example : *Consider an algebraic system $(\{0, 1\}, +)$ where the operation + is defined as shown in (Fig. 5).*

+	0	1
0	0	1
1	1	0

Fig. 5.

The system $(\{0, 1\}, +)$ is a group. In this 0 is identity element and every element is its own inverse.

SUBGROUP

Let us consider a group $(G, *)$. Also, let $S \subseteq G$; then $(S, *)$ is called a subgroup if it satisfies following conditions :

(*i*) The operation * is closed operation on S.

(*ii*) The operation * is an associative operation.

(*iii*) As e is an identity element belonged to G. It must belong to the set S *i.e.*, The identity element of $(G, *)$ must belong to $(S, *)$.

(*iv*) For every element $a \in S$, a^{-1} also belongs to S.

e.g., Let (G, +) be a group, where G is a set of all integers and (+) is an addition operation. Then (H, +) is a subgroup of the group G, where $H = [\{2K \mid K \in G\}$, the set of all even integer]

e.g., Let G be a group. Then the two subgroups of G are G and $G_1 = \{e\}$ is the indentity element.

Example 17. *Let (I, +) be a group, where I is the set of all integers and (+) is an addition operation. Determine whether the following subsets of G are subgroups of G.*

(a) The set G_1 of all odd integers. (b) The set G_2 of all positive integers.

Sol. (*a*) The set G_1 of all odd integers is not a subgroup of G. It does not satisfy the closure property, since addition of two odd integers is always even.

...) **Closure property.** The set G_2 is closed under the operation +, since addition of two ...egers is always even.

Associative property. The operation + is associative since $(a + b) + c = a + (b + c)$ for ..., $b, c \in G_2$.

Identity. The element 0 is the identity element. Hence, $0 \in G_2$.

Inverse. The inverse of every element $a \in G_2$ is $-a \notin G_2$. Hence, the inverse of every ...t does not exists.

...Since the system $(G_2, +)$ does not satisfy all the conditions of a subgroup. Hence, $(G_2, +)$ ...subgroup of (I, +).

...IAN GROUP

...Let us consider, an algebraic system (G, *), where * is a binary operation on G. Then the ...(G, *)is said to be an abelian group if it satisfies all the properties of the group plus an ...nal following property :

(i) The operation * is commutative *i.e.*,

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

...nsider an algebraic system (I, +), where I is the set of all integers and + is an addition ...on. The system (I, +) is an abelian group because it satisfies all the properties of a group ...e operation + is commutative for every $a, b \in I$.

Example 18. *Consider an algebraic system (G, *), where G is the set of all non-zero real ...rs and * is a binary operation defined by*

$$a * b = \frac{ab}{4}.$$

*Show that (G, *) is an abelian group.*

Sol. Closure property. The set G is closed under the operation *. Since, $a * b = \frac{ab}{2}$ is ...number. Hence, belongs to G.

Associative property. The operation * is associative. Let $a, b, c \in G$, then we have

$$(a * b) * c = \left(\frac{ab}{4}\right) * c = \frac{(ab)c}{16} = \frac{abc}{16}.$$

Similarly, $$a * (b * c) = a * \left(\frac{bc}{4}\right) = \frac{a(bc)}{16} = \frac{abc}{16}.$$

Identity. To find the identity element, let us assume that e is a +ve real number. Then ...$= a$, where $a \in G$.

$$\frac{ea}{4} = a \quad \text{or} \quad e = 4$$

Similarly, $$a * e = a$$

$$\frac{ae}{4} = a \quad \text{or} \quad e = 4.$$

Thus, the identity element in G is 4.

Inverse. Let us assume that $a \in G$. If $a^{-1} \in Q$ is an inverse of a, then $a * a^{-1} = 4$

Therefore, $$\frac{aa^{-1}}{4} = 4 \quad \text{or} \quad a^{-1} = \frac{16}{a}$$

Similarly, $a^{-1} * a = 4$

Therefore, $\frac{a^{-1} a}{4} = 4$ or $a^{-1} = \frac{16}{a}$.

Thus, the inverse of element a in G is $\frac{16}{a}$.

Commutative. The operation * on G is commutative.

Since, $a * b = \frac{ab}{4} = b * a$.

Thus, the algebraic system (G, *) is closed, associative, identity element, inverse and commutative. Hence, the system (G, *) is an abelian group.

PRODUCT OF GROUPS

Theorem. *Prove that if $(G_1, *_1)$ and $(G_2, *_2)$ are groups, then $G = G_1 \times G_2$ i.e., $(G, *)$ is a group with operation defined by $(a_1, b_1) * (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$.*

Proof. To prove that $G_1 \times G_2$ is a group, we have to show that $G_1 \times G_2$ has the associative property, has an identity and also exists inverse of every element.

Associativity. Let $a, b, c \in G_1 \times G_2$, then

$$\begin{aligned} a * (b * c) &= (a_1, a_2) * ((b_1, b_2) * (c_1, c_2)) \\ &= (a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2) \\ &= (a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2)) \\ &= ((a_1 *_1 b_1) *_1 c_1), ((a_2 *_2 b_2) *_2 c_2) \\ &= (a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2) \\ &= ((a_1, a_2) * (b_1, b_2)) * (c_1, c_2) = (a * b) * c. \end{aligned}$$

Identity. Let e_1 and e_2 are identities for G_1 and G_2 respectively. Then, the identity for $G_1 \times G_2$ is $e = (e_1, e_2)$. Assume same $a \in G_1 \times G_2$.

Then $$\begin{aligned} a * e &= (a_1, a_2) * (e_1, e_2) \\ &= (a_1 *_1 e_1, a_2 *_2 e_2) = (a_1, a_2) = a \end{aligned}$$

Similarly, we have $e * a = a$.

Inverse. To determine the inverse of an element in $G_1 \times G_2$, we will determine it componentwise *i.e.,*

$$a^{-1} = (a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}).$$

Now to verify that this is the exact inverse, we will compute $a * a^{-1}$ and $a^{-1} * a$.

Now $$\begin{aligned} a * a^{-1} &= (a_1, a_2) * (a_1^{-1}, a_2^{-1}) \\ &= (a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1}) = (e_1, e_2) = e \end{aligned}$$

Similarly, we have $a^{-1} * a = e$.

Thus, $(G_1 \times G_2, *)$ is a group.

In general, if $G_1, G_2, \ldots\ldots, G_n$ are groups, then $G = G_1 \times G_2 \times \ldots\ldots \times G_n$ is also a group.

COSETS

Consider an algebraic system (G, *), where * is a binary operation. Now, if (G, *) is a group and let a be an element of G and $H \subseteq G$, then the LEFT COSET $a * H$ of H is the set of elements such that

$$a * H = \{a * h / h \in H\}.$$

RIGHT COSET $H * a$ of H is the set of elements such that

$$H * a = \{h * a / h \in H\}.$$

subset H is itself a left and right coset since $e * H = H * e = H$.

*ample 19. Let us consider a group (G, *), where G is a set having elements {0, 1} and operation. Also, let H = {1} is a subgroup of G. Determine all the left cosets of H*

l. There is only 2 left cosets i.e.,

$$1 * H = H = \{1\}$$

$$0 * H = \{0\}.$$

ample 20. Let (I, +) is a group, where I is the set of all integers and + is an addition and let H = {..., – 4, – 2, 0, 2, 4, 6, 8, ...} be the subgroup consisting of multiples of 2. e all the left cosets of H in I.

l. There are two distinct left cosets of H in I.

$$0 + H = \{..., -6, -4, -2, 0, 2, 4, 6, ...\} = H$$

$$1 + H = \{... -5, -3, -1, 1, 3, 5, 7, ...\}$$

ere is no other distinct left coset because any other left coset coincides with the cosets ve.

L SUBGROUP

nsider a group (G, *) and subgroup (H, *) of the group, then the (H, *) is called a ub-group if for any $a \in G$, we have

$$aH = Ha.$$

e meaning of the above definition is that if H is a normal sub-group, then both the left t cosets of H in G are equal.

heorem VIII. *Show that every sub-group H of an abelian group G is normal.*

roof. Let us assume any element $a \in H$

lso, assume any element $b \in G$

hen we have $b^{-1}ab = ab^{-1}b = ae \quad \because \quad b^{-1}b = e$

Ve know that $a \in H = a \quad \because \quad ae = a$

ence, H is a normal sub-group.

MORPHISMS

Let $(G_1, *)$ and $(G_2, 0)$ be two algebraic systems, where * and 0 both are binary opera- Then, the mapping $f : G_1 \to G_2$ is said to be homomorphism from $(G_1, *)$ to $(G_2, 0)$ such r every $a, b \in G$, we have

$$f(a * b) = f(a) \,.\, f(b).$$

ISOMORPHISM

Let $(G_1, *)$ and $(G_2, 0)$ be two algebraic system, where $*$ and 0 both are binary operations. The systems $(G_1, *)$ and $(G_2, 0)$ are said to be isomorphic if there exists an isomorphic mapping $f : G_1 \to G_2$.

When two algebraic systems are isomorphic, the system are structurally equivalent and one can be obtained from another by simply remaining the elements and the operation.

Example 21. *Let $(A_1, *)$ and $(A_2, \square)$ be the two algebraic systems as shown in (Fig. 6). Determine whether the two algebraic systems are isomorphic.*

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\square$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Fig. 6.

Sol. The two algebraic systems $(A_1, *)$ and $(A_2, \square)$ are isomorphic and $(A_2, \square)$ is an isomorphic image of A_1, such that

$$f(a) = 1.$$
$$f(b) = w$$
$$f(c) = w^2.$$

AUTOMORPHISM

Let $(G_1, *)$ and $(G_2, 0)$ be two algebraic systems, where $*$ and 0 both are binary operations on G_1 and G_2 respectively. Then an isomorphism from $(G_1, *)$ to $(G_2, 0)$ is called an automorphism if $G_1 = G_2$.

RINGS

An algebraic system $(R, +, .)$ where R is a set with two arbitrary binary operations $+$ and $.$, is called a ring if it satisfies following conditions

(*i*) $(R, +)$ is an abelian group.

(*ii*) $(R, \cdot)$ is a semigroup.

(*iii*) The multiplication operation, $.$, is distributive over the addition operation $+$ *i.e.*,

$$a(b + c) = ab + ac \text{ and } (b + c)a = ba + ca \text{ for all } a, b, c \in R.$$

For example : Consider M be the set of all matrices of the type $\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$ over integers under matrix addition and matrix multiplication. Thus M form a ring.

For example : The set $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ under the operation addition and multiplication modulo 9 forms a ring.

TYPES OF RINGS

1. Commutative Rings. A ring $(R, +, .)$ is called a commutative ring if it holds the commutative law under the operation of multiplication *i.e.*,

$$a \,.\, b = b \,.\, a, \text{ for every } a, b \in R$$

For example : Consider a set E of all even integers under the operation of addition and multiplication. The set E forms a commutative ring.

2. Ring with Unity. A ring (R, + ,.) is called a ring with unity, if it has a multiplicative identity i.e.,

$$a \,.\, e = e \,.\, a = a \text{ for every } a \in R$$

For example : Consider a set M of all 2×2 matrices over integers under matrix multiplication and matrix addition. The set M forms a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

3. Ring with Zero Divisions. If $a \,.\, b = 0$, where a and b are any two non-zero elements of the ring (R, + ,.), then a and b are called divisions of zero and the ring (R, + ,.) is called ring with zero division.

4. Ring without Zero Division. An algebraic system (R, + ,.) where R is a set with two binary binary operation + and., is called a ring without divisors of zero if for every $a, b \in R$, above

$$a \,.\, b \neq 0 \;\Rightarrow\; a \neq 0 \quad \text{and} \quad b \neq 0.$$

RINGS

A subset A of a ring (R, + ,.) is called a subring of R, if it satisfies following conditions.

(i) (A, +) is a subgroup of the group (R, +)

(ii) A is closed under the multiplication operation *i.e.*, $a \,.\, b \in A$, for every $a, b \in A$.

For example : The ring (I, + ,.) of integers is a subring of ring (R, + ,.) of real numbers.

Points to be Noted

(i) If R is any ring then {0} and R are subrings of R.

(ii) Sum of two subrings may not be a subring.

iii) Intersection of subrings is a subring.

For example. Consider the ring M of 2×2 matrices of integers under matrix addition and matrix multiplication. Now, S, the set of all matrices of the type $\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}$ where x, y are integers is a subring of M.

Theorem IX. *Show that* $(-a)(-b) = ab$ *is a ring R.*

Proof. We have $(-a)(-b) = -[a(-b)] = -(-ab) = ab$

Hence proved.

Theorem X. *Show that* $a(b - c) = ab - ac$ *is a ring R.*

Proof. We have $a(b - c) = -a[b + (-c)] = ab + a(-c) = ab - ac$

Hence proved.

Theorem XI. *Show that* $a \,.\, 0 = 0 \,.\, a = 0$ *for all* $a \in R$, *where R is a ring.*

Proof. We have $a \,.\, 0 = a \,.\, (0 + 0)$

$\Rightarrow$ $a \,.\, 0 = a \,.\, 0 + a \,.\, 0$

$\Rightarrow \quad a \cdot 0 + 0 = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0$ [Using left cancellation law]

Hence proved.

Theorem XII. *Show that* $a(-b) = (-a)b = -ab$ *for all* $a, b \in R$, *where* R *is a ring.*

Proof. We know that $a \cdot 0 = 0 \Rightarrow a(-b + b) = 0$

$\Rightarrow \quad a(-b) + ab = 0 \Rightarrow a(-b) = -(ab)$

Similarly, we have $(-a)b = -ab$. Hence proved.

INTEGRAL DOMAIN

Let us consider, an algebraic system (D, +, *) where + and * are two binary operations. The algebraic system (D, +, *) is called an integral domain if it satisfies the following conditions.

1. (D, +) is an abelian group.
2. The operation * is commutative. Also, if we have $z \neq 0$ and $z * x = z * y$; then we have $x = y$. Hence 0 is the additive identity.
3. The operation * is distributive over the operation +.

Example 22. *Let us consider an algebraic system* $(I, +, *)$ *where* I *is the set of all integers and* + *and* * *are the operations of addition and multiplication integers respectively. Determine whether* $(I, +, *)$ *is an integral domain.*

Sol. The algebraic system (I, +) is an abelian group. Here, the identity element is 0 and inverse of every element a is $-a$.

The group * is commutative.

Also, for every non-zero integer z, we have

$$z * x = z * y \Rightarrow x = y$$

Also, the operation * is distributive over +. Since, the system (I, +, *) satisfies all the conditions of integral domain. Hence, (I, + ,*) is an integral domain.

FIELD

An algebraic system (F, + ,•), where F is a set with two arbitrary binary operations + and •, is called a field if it satisfies the following conditions

(*i*) (F , +) is an abelian group.

(*ii*) Every non-zero element has a multiplicative inverse.

(*iii*) The operation • is distributive over the operation +.

e.g., The algebraic system (R, +, •) is a field, where R is the set of all real numbers.

Points to Remember

* Every field is a ring.
* Every field is an integral domain but every integral domain is not a field.
* Every finite integral domain is a field.

e.g., The set of rational numbers with addition and multiplication is not a field because the multiplicative inverse of elements do not exists.

SOLVED PROBLEMS

Problem 1. *Let $(S, *)$ be a commutative semigroup. Show that if $x * x = x$ and $y * y = y$,*

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

Sol. Take L.H.S. $(x * y) * (x * y)$

$(x * y) * (y * x)$ [$\because$ $(S, *)$ is a commutative semigroup]

$x * y * y * x \Rightarrow x * y * x$ [$\because$ $y * y = y$]

$x * x * y$ [$\because$ Commutative semigroup]

$x * y$ [$\because$ $x * x = x$]

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

Hence.

Problem 2. *Let $([x, y], .)$ be a semigroup where $x . x = y$ show that*

(i) $x . y = y . x$ *(ii) $y . y = y$.*

Sol. (i) To show that $x . y = y . x$

We know that $x . x . x = x . x . x \Rightarrow x . y = y . x$ [$\because$ $x . x = y$]

Hence proved.

(ii) To show that $y . y = y$

We know that the set (x, y) is closed under the operation. Therefore, we have two options

$x . y = x, \quad x . y = y$

1) Let $x . y = x$

Now assume $y . y = (y . x) . x = (y . x) . x$ [$\because$. is associative]

$= (x . y) . x$ [$\because$ $x . y = y . x$]

$= x . x$ [$\because$ $x . y = x$]

$= y$

2) Let $x . y = y$

Now assume $y . y = (x . x) . y$ [$\because$ $x . x = y$]

$= x . (x . y)$ [$\because$. is associative]

$= x . y$ [$\because$ $x . y = y$]

$= y$

Hence proved.

Problem 3. *Let $(A, *)$ be a semigroup. Further more, for every a and b in A, if $a \neq b$ then $a * a \neq a * a$.*

a) Show that for every a in A

$$a * a = a$$

b) Show that for every a, b in A

$$a * b * a = a$$

c) Show that for every a, b, c in A

$$a * b * c = a * c.$$

Sol. (a) We know that A is a semigroup.

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

Now putting $b = a$ and $c = a$, we have

$$(a * a) * a = a * (a * a)$$

Since A is not commutative semigroup.

Hence $$a * a = a \quad \ldots(i)$$

(*b*) Let us assume that $b \in A$, then we have

$$b * b = b$$

Multiplying both sides by a, we get

$$a * b * b = a * b \quad \text{or} \quad (a * b) * b = a * b \quad [\because * \text{ is associative}]$$

$$a * b = a \quad \ldots(ii)$$

Hence, $[\because * \text{ is associative}]$

So, $$a * b * a = (a * b) * a \quad [\because a * b = a \text{ from } (ii)]$$

$$= a * a \quad [\because a * a = a \text{ from } (i)]$$

$$= a$$

(c) We know that $$a * b * c = (a * b) * c \quad [\because * \text{ is associative}]$$

$$= a * c \quad [\because a * b = a \text{ from } (ii)]$$

Problem 4. *Let* (Z, *) *be an algebraic structure, where z is the set of integers and th operation * is defined by n * m = maximum (n, m). Determine whether* (Z, *) *is a monoid or group or an abelian group.*

Sol. Closure Property

We know that $n * m = \max(n,m) \in \mathbf{Z}$,

$$\forall\, n, m \in \mathbf{Z}$$

Hence * is closed.

Associative property. Let us assume $a, b, c \in \mathbf{Z}$.

Then, we have $a * (b * c) = a *$ max. $(b, c) =$ max. $(a,$ max. $(b, c))$

$$= \max.\ (a, b, c)$$

Similarly, $(a * b) * c = \max.\ (a, b, c)$

Hence * is associative.

Identity. Let e be the identity element. Then max. $(a, e) = a$

Hence, the minimum element is the identity element.

Inverse. The inverse of any element does not exist. Since, the inverse does not exis hence (Z, *) is not a group or abelian group but a monoid as it satisfies the properties closure, associative and identity.

Problem 5. *Let* $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ *and multiplication modulo 8, that is*

$$x \otimes y = (xy) \text{ Mod } 8$$

(i) Prove that $(\{0, 1\}, \otimes)$ *is not a group.*

(ii) Write three distinct groups $(G, \otimes)$ *where* $G \subset S$ *and G has 2 elements.*

Sol. (*i*) (*a*) **Closure property.** The set {0, 1} is closed under the operation ⊗, as sho in table of operation (Fig. 7).

⊗	0	1
0	0	0
1	0	1

Fig. 7.

ssociative property. The operation $\otimes$ is associative. Let $a, b, c \in G$, then we have
$(a \otimes b) \otimes c = a \otimes (b \otimes c)$ e.g., $(0 \otimes 1) \otimes 1 = (0) \otimes 1 = 0$
$0 \otimes (1 \otimes 1) = 0 \otimes (1) = 0$.

larly, dentity. The element 1 is the identity element as for every
$a \in \{0, 1\}$
$e \otimes a = a$.

verse. There must exist an inverse of every element $a \in \{0, 1\}$, such that
$a \otimes a^{-1} = e$

he inverse of element 0 does not exist.
efore, since the inverse of every element $a \in \{0, 1\}$ does not exist. Hence $(\{0, 1\}, \otimes)$ is

he three distinct groups $(G, \otimes)$, where $G \subset S$ and G has 2 elements is as follows
1, 3}, $\otimes$) (*b*) ({1, 5}, $\otimes$) (*c*) ({1, 7}, $\otimes$).

blem 6. *Determine whether a semigroup with more than one idempotent element p.*

Let (A, *) be a semigroup with two idempotent elements a and b. Then we have
$a * a = a$ ...(*a*)
$b * b = b$ ...(*b*) $a \neq b$.

assume that A is a group with identity element e.
$a * e = a$ and $b * e = b$

, (*a*) and (*b*), we have $a * a = a * e$ and $b * b = b * e$
ıe law of left cancellation, we get $a = e = b$
contradiction to $a \neq b$.
:e (A, *) can not be group.

blem 7. *Let G_1 and G_2 be subgroups of a group G*
how that $G_1 \cap G_2$ is also a subgroup of G.
$G_1 \cup G_2$ always a subgroup of G ?

(*i*) Let G_1 and G_2 be two subgroups of G. Then we have
$G_1 \cap G_2 \neq \phi$ [$\because$ Identity element $\cap$ is common to both G_1 and G_2]

how that $G_1 \cap G_2$ is a subgroup, we shall have to prove that
$a \in G_1 \cap G_2$ and $b \in G_1 \cap G_2 \Rightarrow a, b \in G_1 \cap G_2$.

us assume
$a \in G_1 \cap G_2 \Rightarrow a \in G_1$ and $a \in G_2$
$b \in G_1 \cap G_2 \Rightarrow b \in G_1$ and $b \in G_2$.

we know that G_1 and G_2 are subgroups.

refore, $a \in G_1$ and $b \in G_1 \Rightarrow ab^{-1} \in G_1$ ...(*i*)
$a \in G_2$ and $b \in G_2 \Rightarrow ab^{-1} \in G_2$ ...(*ii*)

m (*i*) and (*ii*), we have $ab^{-1} \in G_1 \cap G_2$

is, we have
$a \in G_1 \cap G_2$ and $b \in G_1 \cap G_2 \Rightarrow ab^{-1} \in G_1 \cap G_2$.

ıce $G_1 \cap G_2$ is a subgroup of G.

(*ii*) It is not always necessary that $G_1 \cup G_2$ is a subgroup of G.

Problem 8. *Let (G, o) be a group. Show that (G, o) is an Abelian group if and only if* $(a \circ b)^2 = a^2 \circ b^2$ *for all a and b in G.*

Sol. We know that

$$(a \circ b)^2 = (a \circ b) \circ (a \circ b) = a \circ (b \circ a) \circ b \qquad [\because \circ \text{ is associative}]$$

Now let us assume G is an Abelian group

$$= a \circ (a \circ b) \circ b = (a \circ a) \circ (b \circ b)$$

Hence, $(a \circ b)^2 = a^2 \circ b^2 \quad \forall\, a, b \in G$

Thus, the group G is Abelian if and only if

$$(a \circ b)^2 = a^2 \circ b^2 \quad \forall\, a, b \in G.$$

Problem 9. *Let G = (I, +) be a group, where I is the set of integers and + is an addition operation, also let* $G_1 = \{\ldots\ldots -14, -7, 0, 7, 14, 21, \ldots\ldots\}$ *be a subgroup consisting of the multiples of 7. Determine the cosets of* G_1 *in I.*

Sol. The set I has 7 different cosets (left or right) of G_1, which are as shown below.

$$0 + H = \{\ldots\ldots -14, -7, 0, 7, 14, 21, \ldots\ldots\}$$
$$1 + H = \{\ldots\ldots -13, -6, 1, 8, 15, 22, \ldots\ldots\}$$
$$2 + H = \{\ldots\ldots -12, -5, 2, 9, 16, 23, \ldots\ldots\}$$
$$3 + H = \{\ldots\ldots -11, -4, 3, 10, 17, 24, \ldots\ldots\}$$
$$4 + H = \{\ldots\ldots -10, -3, 4, 11, 18, 25, \ldots\ldots\}$$
$$5 + H = \{\ldots\ldots -9, -2, 5, 12, 19, 26, \ldots\ldots\}$$
$$6 + H = \{\ldots\ldots -8, -1, 6, 13, 20, 27, \ldots\ldots\}$$

All other cosets coincides with any one of the cosets shown above, hence we will not count them.

Problem 10. *Consider G = {1, 5, 7, 11, 13, 17} under multiplication modulo 18.*

(*i*) *Construct the multiplication table of G.*

(*ii*) *Find* 5^{-1}, 7^{-1} *and* 17^{-1}.

(*iii*) *Find the order and group generated by*

(*a*) *5* (*b*) *13.*

(*iv*) *Is G cyclic ?*

Sol. (*i*) We can find $x * y$ in G by finding the remainder when the product xy is divided by 18. The table of multiplication modulo 18 is shown in (Fig. 8).

*	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Fig. 8.

i) We know that a^{-1} is the inverse of a in G. The element 1 is the identity element of G.
e know that

$$aa^{-1} = a^{-1}a = e$$

$$aa^{-1} = 1$$

Hence, (a) $5^{-1} = 11$ [$\because 5 * 11 = 11 * 5 = 1$]

b) $7^{-1} = 13$ [$\because 7 * 13 = 13 * 7 = 1$]

c) $17^{-1} = 17$ [$\because 17 * 17 = 17 * 17 = 1$]

) (a) We have $5^1 = 5, 5^2 = 7, 5^3 = 17$;

hus, the order of the group $|5| = 3$ and the group generated by $5 = \{5, 7, 17\}$.

) Again we have $13^1 = 13$; $13^2 = 7$; $13^3 = 1$;

hus, the order of the group $|13| = 3$ and group generated by $13 = \{1, 7, 13\}$.

) G is not cyclic since G ≠ any of the subgroups generated by 5 and 13.

roblem 11. *Let G be a finite group and H be a subgroup of G. For $a \in G$, define $aH = \{ah : h \in H\}$*

) *Show that $|aH| = |H|$.*

) *Show that for every pair of elements, $a, b \in G$ either $aH = bH$ or aH and bH are*

) *Use the above to argue that the order of H must divide the order of G.*

ol. (a) To show that $|aH| = |H|$

et $H = \{h_1, h_2, h_3, ..., h_n\}$ be the n elements of H.

hen $aH = \{ah_1, ah_2, ah_3, ..., ah_n\}$

ut we know that $ah_i = ah_j$ or $h_i = h_j$

ence, the n elements in aH are disjoint.

herefore, $|aH| = |H|$.

b) Let us assume that $(a * H) \cap (b * H)$ is non empty

lso, let $c \in (a * H) \cap (b * H)$

hen, we have $c \in a * H \Rightarrow a * H = c * H$

lso, $c \in b * H \Rightarrow b * H = c * H$

herefore, $a * H = b * H$.

Since the cosets form a partition of G. Hence $aH = bH$ or aH and bH are disjoint.

(c) Since we know that H is a subgroup of G. Let us assume, that the subgroup H has K nts and let there are b distinct left cosets. From the (b) above, we have seen that the partition the group G and from the (a) above, we have seen that each coset has K ele-

Therefore, the group G must contain K_p elements. Thus, it implies that the order of H divide the order of G.

This is also called the Lagrange's theorem.

Problem 12. *Show that if $G = G_1 \times G_2 \times ..... \times G_n$ is a group and $(a_1, a_2, ..., a_n) \in G$,*

(i) $(a_1, a_2, ..., a_n)^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$

(ii) $(a_1, a_2, ..., a_n)^m = (a_1^m, a_2^m, ..., a_n^m)$.

Sol. (*i*) Let $a \in G$ and also $a^{-1} \in G$. Also assume that

$$a = (a_1, a_2, a_3, \ldots\ldots, a_n) \quad \text{and} \quad a^{-1} = (a_1^{-1}, a_2^{-1}, a_3^{-1}, \ldots\ldots a_n^{-1})$$

Now $$a * a^{-1} = (a_1, a_2, a_3, \ldots\ldots, a_n) * (a_1^{-1}, a_2^{-1}, a_3^{-1}, \ldots\ldots, a_n^{-1})$$
$$= (a_1 * a_1^{-1}, a_2 * a_2^{-1}, \ldots\ldots, a_n * a_n^{-1}) = (e_1, e_2, e_3, \ldots\ldots, e_n)$$

Here e_i is the identity of group G_i.

Since, a^{-1} is the inverse of a. So we can write $(a_1, a_2, a_3, \ldots\ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots\ldots, a_n^{-1})$.

(*ii*) We can prove this by the method of induction. Let us assume that $n = 2$ *i.e.*,

$$(a_1, a_2, a_3, \ldots\ldots, a_n)^2 = (a_1, a_2, a_3, \ldots\ldots, a_n)(a_1, a_2, a_3, \ldots\ldots, a_n)$$
$$= (a_1a_1, a_2a_2, a_3a_3, \ldots\ldots, a_na_n) = (a_1^2, a_2^2, a_3^2, \ldots\ldots, a_n^2)$$

Thus, the result is true for $n = 2$.

Let us assume that it is true for $n = m - 1$ *i.e.*,

$$(a_1, a_2, a_3, \ldots\ldots, a_n)^{m-1} = (a_1^{m-1}, a_2^{m-1}, a_3^{m-1}, \ldots\ldots, a_n^{m-1})$$

Now $$(a_1, a_2, a_3, \ldots\ldots, a_n)^m = (a_1^{m-1}, a_2^{m-1}, a_3^{m-1}, \ldots\ldots, a_n^{m-1})(a_1, a_2, a_3, \ldots\ldots, a_n)$$
$$= (a_1^m, a_2^m, a_3^m, \ldots\ldots, a_n^m)$$

Thus, it is true for $n = m$.

Problem 13. *Show that if* $G = G_1 \times G_2 \times G_3 \ldots\ldots \times G_n$ *is a group and* $(a_1, a_2, a_3, \ldots\ldots, a_n) \in G$, *then*

(*i*) *The identity of G is* $(e_1, e_2, \ldots\ldots, e_n)$, *where* e_i *is the identity of corresponding* G_i.

(*ii*) *The group G is an abelian group iff each of groups* $G_1, G_2, \ldots\ldots, G_n$ *is abelian.*

Sol. (*i*) Let $e = (e_1, e_2, e_3, \ldots\ldots, e_n)$ is the identity for $G_1 \times G_2 \times G_3 \times \ldots\ldots, G_n$, where e_i is the identity for G_i.

Now let us assume that $a \in G_1 \times G_2 \times G_3 \times \ldots\ldots \times G_n$

Then we have $$a * e = (a_1, a_2, a_3, \ldots\ldots, a_n) * (e_1, e_2, \ldots\ldots, e_n)$$
$$= (a_1 * e_1, a_2 * e_2, a_3 * e_3, \ldots\ldots, a_n * e_n)$$
$$= (a_1, a_2, \ldots\ldots, a_n) \qquad [\because a_i * e_i = a_i]$$

Similarly, we can show that $e * a = a$.

Hence, e is the identity of G.

(*ii*) Let $a, b \in G$. Then, we have

$a = (a_1, a_2, a_3, \ldots\ldots, a_n)$ and $b = (b_1, b_2, b_3, \ldots\ldots, b_n)$ belongs to $G_1 \times G_2 \times G_3 \times \ldots\ldots \times G_n$, where a_i, b_i belongs to the corresponding G_i.

Now $$a * b = (a_1, a_2, a_3, \ldots\ldots, a_n) * (b_1, b_2, b_3, \ldots\ldots, b_n)$$
$$= (a_1 * b_1, a_2 * b_2, a_3 * b_3, \ldots\ldots, a_n * b_n)$$

Also $$b * a = (b_1, b_2, b_3, \ldots\ldots, b_n) * (a_1, a_2, a_3, \ldots\ldots, a_n)$$
$$= (b_1 * a_i, b_2 * a_2, b_3 * a_3, \ldots\ldots, b_n * a_n)$$

A group G is an abelian group iff $a * b = b * a$.

Thus, iff $a_i * b_i = b_i * a_i$ for each G_i *i.e.*, the group G is an abelian group if each of the groups $G_1, G_2, G_3, \ldots\ldots, G_n$ is abelian.

Problem 14. *Consider a ring* $(R, +, *)$ *defined by* $a * a = a$.
Determine whether the ring is commutative or not.

Sol. We have given the ring $(R, +, *)$ satisfying the following properties

(*i*) $(R, +)$ is an abelian group.

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

(*iii*) The operation $*$ distributes over $+$.

Also we have, $a * a = a \quad \forall\, a$ in $(R, +, *)$.

To prove that the ring $(R, +, *)$ is commutative. We have to prove that there exists as ity element and $(R, *)$ is a commutative monoid.

Let us assume $a, b \in R$

Also, let $c = a + b$

Since, $+$ is a closed operation, hence $c \in R$.

Then, we have $c * c = c * (a + b)$

We know that, the operation $*$ distributes over $+$.

So, $c * c = (a + b) * (a + b) = a * a + a * b + b * a + b * b$

So, $c = a + b + a * b + b * a \qquad [\because \ a * a = a]$

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

Therefore, $a * b + b * a = e$ is an identity for operation $+$ also $a * b$ is inverse of $b * a$

Again, let us assume $a + a = b$

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

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

$$a + a = a * b \qquad \ldots(i)$$

Similarly, $(a + a) * a = b * a$

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

$$a + a = b * a \qquad \ldots(ii)$$

From (i) and (ii), we have

$$a * b = b * a$$

Thus, the operation $*$ is commutative. Since, $(R, *)$ is a commutative monoid. Therefore, is a commutative ring.