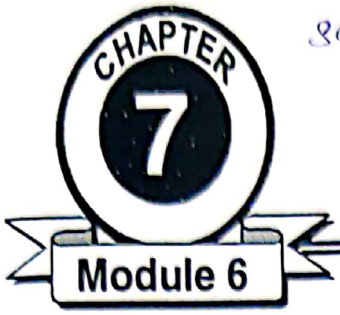
3rd week 4th week.
Th → 3 to 4 | Th → 2 to 3.
4th week
Fri → 1 to 3 / 2 to 3.
Sat → 1 to 3 | Sat → 1 to 3/2



Algebraic Structures

Syllabus

Algebraic Structures with one binary operations, semigroup, monoid and groups, Abelian group, Isomorphism, Homomorphism and Automorphism, Cyclic groups, Normal Subgroup, Codes and group codes.

Introduction :

In this chapter, we study sets with additional structure, induced by one or more binary operations on the elements of the set. These discrete structures are called as **'algebraic systems'** as they obey a set of rules or axioms which are similar to the rules of addition and multiplication of numbers in elementary algebra. In fact many of these structures are prototype models of mathematical systems, with which we are familiar.

We first introduce a general algebraic system and discuss its properties. We then can centrate our attention on some special algebraic systems such as semigroups, monoids and groups.

An important application of groups is in coding theory where techniques are developed for detecting and correcting errors in transmitted data. The section on codes discusses some of these techniques in detail.

Besides coding theory, algebraic systems are also widely applied in the design of computer hardware and development of software especially formal language theory and finite states machines.

We also study briefly several classes of algebraic systems with 2 binary operations. It is clear that given two algebraic systems $(A, \star)$ and $(A, *)$, we can always 'combine' them to yield an algebraic system with two binary operations. $(\Delta, \star, *)$.

Scanned by CamScanner

Syllabus Topic : Algebraic Structures with one binary

7.1 Binary Operations Revisited :

A **'binary operations'** on a set 'A' is an everywhere defined function $f : A \times A \rightarrow A$. Observe the following properties that a binary operation must satisfy :

1. Since Dom (f) = A × A, f assigns an element f (a, b) of A to each ordered pair (a, b) in A × A.
   That is, the binary operation must be defined for each ordered pair of elements of A.
2. Since of binary operation is a function, only one element of A is assigned to each ordered pair.

Thus we can say that a binary operation is a rule that assigns to each. Ordered pair of elements of A unique element of A.

Instead of the customary letter nomes for functions, we use "P [eratpr Symbols" such as H, *, +,·, □, ⊕,... as the names of binary operations on set· Thus, we can write

★ (a_1, a_2) or a_1 ★ a_2

It should be emphasized that if a and b are elements in A, then a * b ∈ A, and this property is often described by saying that A is closed under the operation *.

7.1.1 Examples :

1. Let A = Z. Define a * b as a + b. The * is a binary operation on Z.
2. Let A = IR. Define a * b as a / b. Then * is not a binary operation since it is not defined for every ordered pair of elements of A. For example 3 * 0 is not defined, since we cannot divide by zero.
3. Let A = Z^+. Define a * b as a – b. Then * is not a binary operation since it does not assign an element of A to every ordered pair of elements of A, for example 2 * 5 ∉ A.
4. Let A = Z. Define a * b as a number less than both a and b. Then * is not a binary operation, since it does not assign a unique element of A to each ordered pair of elements of A ; for example, 8 * 6 could be 5, 4, 3, 1 and so on. Thus in this case, * would be a relation from A × A to A but not a function.
5. Let A = Z. Define a * b as max {a, b}. Then * is a binary operation for example, 2 * 4 = 4, – 3 * (– 5) = – 3.
6. Let A = P(S), for some set S. If V and W are subsets of S, define V * W as V ∪ W, then * is a binary operation on A. Moreover, if we define V *' W as V ∩ W, then *' is another binary operation on A.
7. Let M be the set of all n × n Boolean matrices. Define **A** * **B** as **A** ∨ **B**. Then * is a binary operation. This is also true of **A** ∧ **B**.
8. Let L be a lattice. Define a * b as a ∧ b (the greatest lower bound of a and b). Then * is a binary operation on L. This is also true of a ∨ b. (The least upper bound of a and b).

Scanned by CamScanner

7.1.2 Tables :

If $A = \{a_1, a_2, \ldots a_n\}$ is a finite set, we can define a binary operation on A by means of a table as shown in Fig. 7.1. The entry in the i^{th} row and j^{th} column denotes the element $a_i * a_j$ position i, j, denotes the element $a_i * a_j$.

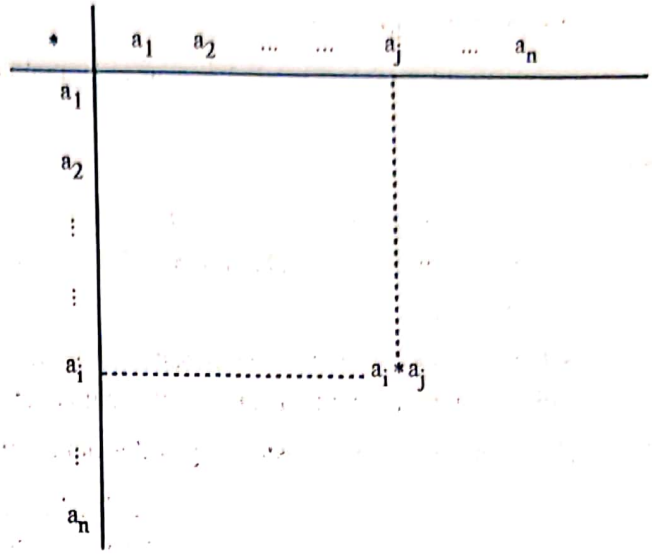


Fig. 7.1

Example :

1. Let A = {0, 1}. We define the binar operations ∨ and ∧ by the following tables,

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

If A = {a, b} we shall now determ the number of binary operations that can be defined on A. Every binary operation * on A can be desc ed by the table.

*	a	b
a		
b		

Since every blank can be filled with the element a or b we conclude that there are $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ or 16 ways to complete the ble. Thus there are 16 binary operations on A.

7.1.3 Algebraic System :

A set together with a number of op tions on the set is called an **algebraic system.**

Examples :

1. Consider the set of natural num s N together with the usual addition and multiplication operation of integers, + and ·. arly, (N, +, ·) is an algebraic system with two binary operations.
2. Let □ be a binary operation on N uch that □ (a, b) is equal to 0 or 1 depending on whether the sum of a and b is even or o and Δ be a ternary operation on N such that Δ (a, b, c) is equal to the maximum of a, b nd c (N, □, Δ) is also an algebraic system with two operations. (one binary operation one ternary operation).

Scanned by CamScanner

7.1.4 Properties of Binary Operations :

(1) Commutative property :

A binary operation on a set A is said to be commutative if $a * b = b * a$ for all elements a and b in A.

Example :

1. The binary operation of addition on **Z** is commutative.
2. The binary operation of subtraction on **Z** is not commutative since.

   $2 - 3 \neq 3 - 2$

   A binary operation that is described by a table is commutative if and only if the entries in the table are symmetric with respect to the main diagonal.
3. The binary operation shown in Fig. 7.2 is not commutative, since $a * b$ is c while $b * a$ is b.

*	a	b	c	d
a	a	c	b	d
b	b	c	b	a
c	c	d	b	c
d	a	a	b	b

Fig. 7.2

4. The binary operation shown in Fig. 7.3 is commutative since the entries in the table are symmetric with respect to the main diagonal.

*	a	b	c	d
a	a	c	b	d
b	c	d	b	a
c	b	b	a	c
d	d	a	c	d

Fig. 7.3

(2) Associative property :

A binary operation * on a set A is said to be **associative** if

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

for all elements a, b and c in A.

Examples :

1. The binary operation of addition on **Z** is associative.
2. The binary operation of subtraction on **Z** is not associative, since

   $2 - (3 - 5) \neq (2 - 3) - 5$

(3) Idempotent property :

A binary operation * on a set A is said to be **idempotent** if

$$a * a = a.$$

Scanned by CamScanner

7.1.5 Exampl :

Example 1 :

Let L be a l e. The ry oper n defined by a * b = a ∧ b is commutative, associative. It also satisfies the id otent p rty a ∧ . A partial converse of this example is also true.

Example 2 : Sh e relat given b = a^b is a binary operation on set of natural numbers, is it ass tive ? \ **MU - Dec. 05, May 07**

Solution :

Given : aob = , a and e natural number

Let boa = , a and e natural number

aob = oa

a^b =

∴ Given re on o is n an assoc e operation.

Syllabus Top : Mon ds, Se groups and Groups, Abelian Group, Cyclic Grou Normal Subgroup

7.2 Semigr os, Mo oids a Groups :

7.2.1 Semigr p : **MU - May 16**

7.2.1.1 Definiti n :

MU - May 99, Dec. 2000, May 10, May 13

Let (A, *) an alg aic syste where * is a binary operation on A. (A, *) is called a **semigroup** if the llowing c ditions a satisfied.

1. * is a close eration.
2. * is an assc tive oper on.

The semig p (A, *) aid to be mmutative if * is a commutative operation.

7.2.1.2 Examp s :

Example 1 :

Let A be set of positive even integers {2, 4, 6, ...} and + be the ordinary addition operation of integ . Since + a closed eration on A and is also an associative operation, (A, +) is a semigroup. Addit is comm tive ope ion, so (A , +) is a commutative semigroup.

Example 2 :

Let S be a nite alph et. Let A note the set of all non-empty strings of letters from S. (For example, let S = , β, γ}. have A {α, β, γ, αα, αβ, αγ, ..., ααα, ααβ, ...}). Let · be a binary

Scanned by CamScanner

operation on A such that for any two strings a and b in A, a b yields a string which is the concatenation of strings a and b, (for example αα αγβ = ααααγβ). Then (A,·) is a commutative semigroup.

Example 3 :

The set P(S) where S is a set, together with the operation of union is a commutative semigroup.

Example 4 :

The set Z with the binary operation of subtraction is not a semigroup, since subtraction is not associative.

7.2.1.3 Sub-semigroup :

Let (A, *) be a semigroup and let B be a non-empty subset of A. Such that B is closed under *. Then (B, *) is itself a semigroup and B called a semigroup of (A, *).

7.2.2 Monoid :

MU - May 99, May 2000, May 10, Dec. 2000 , May 16

7.2.2.1 Identity :

Let (A, *) be an algebraic system where * is a binary operation on A. An element in A, e, is said to be a **left identity** if for all x in A, e * x = x. For example for the algebraic system shown in Fig. 7.4 both β and δ are left identifies.

Since, $\beta * \alpha = \alpha$

$\beta * \beta = \beta$

$\beta * \gamma = \gamma$

$\beta * \delta = \delta$

And $\delta * \alpha = \alpha$

$\delta * \beta = \beta$

$\delta * \gamma = \gamma$

$\delta * \delta = \delta$

*	α	β	γ	δ
α	δ	α	β	γ
β	α	β	γ	δ
γ	α	β	γ	γ
δ	α	β	γ	δ

Fig. 7.4

An element in A, e is said to a **right identity** if for all x in A. x * e = x. For example, for the algebraic system shown in Fig. 7.5 α is a right identity.

Since $\alpha * \alpha = \alpha$

$\beta * \alpha = \beta$

$\gamma * \alpha = \gamma$

$\delta * \alpha = \delta$

An element is said to be an **identity** if it is both a left identity and a right identity.

*	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

Fig. 7.5

Scanned by CamScanner

For example, let (A, * : an algebraic system where A is a set of coloured lights and * is a binary operation such that a * is the resultant coloured light when light a is combined with light b. Clearly, white light is the iden of the algebraic system.

As another example, le , +) be an algebraic system, where N is the set of natural numbers and + is the ordinary addition ope n of integers. Clearly 0 is the identity of the algebraic system.

7.2.2.2 Definition :

Let (A, *) be an alge system, where * is a binary operation on A. (A, *) is called a **monoid** if the following conditions are isfied.

1. * is a closed oper n
2. * is an associative operation
3. There is an identi

7.2.2.3 Examples :

Example 1 : Let A be a set c eople of different heights. Let Δ be a binary operation such that a Δ b is equal to the taller one of a a b. We note that (A, Δ) is a monoid where the identity is the shortest person in A.

Example 2 : The semigrou S) defined in Example 3 (Section 7.2.3) has the identity ϕ. Since,

$$\phi * A = \phi \cup A = A = A \cup \phi = A * \phi$$

for any element A ∈ P(S). ence P(S) is a monoid.

7.2.2.4 Submonoid

MU - May 07

Let (A, *) be a monoi d let B be a non-empty subset of A. Then (B, *) is called a **submonoid** of (A, *) if

1. B is closed under *
2. The identity element e . B.

Example :

Let E = {0, 2, 4, 6}. n (E, +) is a submonoid of (Z, +)

7.2.3 Group :

MU - Dec. 98, May 99, May 2000, May 01, May 10, May 16

7.2.3.1 Inverse :

Let (A, *) be an algebraic system with an identity e. Let a be an element in A. An element b is said to be a **left inverse** of a if b * a = e. An element b is said to be a **right inverse** of a if a * b = e. For example for the algebraic system shown in Fig. 7.6, α is an identity. So β is a left inverse of γ, and δ is a right inverse γ

$$B * \gamma = \alpha \qquad \gamma * \delta = \alpha$$

Scanned by CamScanner

*	α	β	γ	δ
α	α	β	γ	δ
β	β	δ	α	γ
γ	γ	β	β	α
δ	δ	α	γ	δ

Fig. 7.6

An element b is said to be an **inverse** of a, if it is both a left and a right inverse of a. Clearly if b is an inverse of a, a is also an inverse of b.

7.2.3.2 Definition :

Let (A, *) be an algebraic system, where * is a binary operation. (A, *) is called a **group** if the following conditions are satisfied.

1. * is a closed operation.
2. * is an associative operation
3. There is an identity.
4. Every element in A has a left inverse.

Because of associativity, a left inverse, of an element is also a right inverse of the element in a group.

7.2.3.3 Commutative/Abelian Group :

MU - Dec. 02

A group (A, *) is called a **commutative group** or an **Abelian group** if * is a commutative operation.

7.2.3.4 Finite and Infinite Group :

A group (A, *) is said to be **finite group,** if A is a finite set and **infinite group**, if A is an infinite set. The size of A is often referred to as the order of the group.

e.g. (i) The group (Z, +) is of infinite order. (ii) The group $(Z_m, +)$ is of finite order viz m.

Examples :

1. The set of all integers Z with the operation of addition is a group. The identity element is the number 0 and for every $n \in Z$, its inverse is (– n).
2. The set $Q^* = Q - \{0\}$ of non–zero rational numbers is a group under multiplication. The identity element is the number 1 and inverse of each element $p/q \in Q^*$ is q/p.
3. The set of all **non–zero** real numbers under the operation of multiplication is a group with the number 1 as the identity element, and inverse of each number a is 1/a.

Scanned by CamScanner

4. Let n be any positive integer ($n > 0$). For elements $x, y \in Z$, d a relat ≡ on them as $x \equiv y$ or $x = y \pmod n$ if $x - y$ is divisible by n. The relation is quivale relation and for each element $x \in Z$, we obtain the corresponding equivalence clas .

There are in all n distinct equivalence classes. Let Z_n denote th of all valence classes, Z_n is called as set of **residue classes modulo n,** where $[x] = [y]$ implies y (mo

For any two elements $[x], [y] \in Z_n$ define $[x] + [y] = [x + y]$. (an eas e that + is both associative and commutative. The identity element is [0], and for each [Z_m, it erse is $[m - x]$, since $[x] + [m - x] = [x + m - x] = [m] = [0]$. Thus $(Z_m, +)$ is an Abel roup.

7.2.3.5 Exercise Set - 1 (Solved) :

Example 1 :

Let $A = \{a, b\}$, which of the following tables in Fig. 7.7, de a semi p on A? Which define a monoid on A?

(a)

*	a	b
a	a	b
b	a	a

(b)

*	a	b
a	a	b
b	b	b

(c)

*	b
a	a
b	b

(d)

*	a	b
a	a	b
b	b	a

(e)

*	a	b
a	a	a
b	b	b

(f)

*	b
a	b
b	a

Fig. 7.7

Solution :

(a)

*	a	b
a	a	b
b	a	a

(i) First we verify that * is binary operation and set A closed under t inary o tion * is a binary operation and for any $a, b \in A$, $a * b$ also belongs to A.

So set A is closed under the binary operation of *.

(ii) We next verify associativity

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

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

$$b = b$$

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

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

$$a \neq b$$

Scanned by CamScanner

$\therefore$ binary operation $*$ is not associative. So it is neither a semigroup nor a monoid.

(b)

*	a	b
a	a	b
b	b	b

(i) For any two elements a and b belonging to A, $a * b \in A$. So set A is closed under the binary operation $*$.

(ii) Now check for associativity.

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

Hence $*$ is associative.

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

(iii) Now check for identity

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

$\therefore$ 'a' is identity element.

So algebraic system $(A, *)$ is monoid.

(c)

*	a	b
a	b	a
b	a	b

(i) For any two elements $a, b \in A$

$$a * b \in A$$

So A is closed under the binary operation $*$.

(ii) Now check for associativity

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

$\therefore$ $*$ is associative operation

$\therefore$ The algebraic system $(A, *)$ is semigroup.

Scanned by CamScanner

(iii) Now ch for iden

a * b = b * a = a

b * b = b * b = b

∴ 'b' is ntity ele

∴ Alg c syste , *) is m oid.

(c

*	b
a	b
b	a

(i) For any elemen b ∈ A, b ∈ A. S A is closed under the binary operation *.

(ii) Now ch for asso vity

a * (a * b) = (a * a) * b

a * b = a * b

b = b

b * (a * b) = (b * a) * b

b * b = b * b

a = a

∴ The ebraic sy n (A, *) emigrou

Now ch for iden element

a * a = a * a = a

a * b = a = b

'a' is i ity elem

∴ Alg ic syste A, *) is m oid.

(

*	a	b
a	a	a
b	b	b

(i) For any elemen , b ∈ A, b ∈ A.

∴ Set closed u r the bi y operati *.

(ii) Now ch for asso ivity

a * (a * b) = (a * a) * b

a * b = a * b

= a

b * (a * b) = (b * a) * b

b * b = b * b

b = b

∴ * is ociative ration

∴ The ebraic sy n (A, *) semigrou

(iii Now ch for ider

a * = a * a = a

Scanned by CamScanner

$a * b = a$ and $b * a = b$

$\therefore$ There is no identity element

Hence algebraic system (A, *) is not monoid.

(f)

*	a	b
a	b	b
b	a	a

(i) For any two elements $a, b \in A$, $a * b \in A$

$\therefore$ Set A is closed under the binary operation *,

(ii) Now check for associativity

$$b * (a * b) = (b * a) * b$$
$$b * b = a * b$$
$$a \neq b$$

$\therefore$ * is not associative operation

$\therefore$ The algebraic system (A, *) is not semigroup. So it is not monoid also.

Example 2 :

Determine whether the set together with the binary operation is a semigroup, a monoid or neither. If it is a monoid specify the identity if it is a semigroup or a monoid, determine if it is commutative.

(a) Z^+ where * is defined as ordinary multiplication.

(b) Z^+ where $a * b$ is defined as max [a, b]

(c) Z, where $a * b = a + b - ab$

Solution :

(a) $(Z^+, *)$:

(i) Multiplication of two positive integers is a positive integer. So set Z^+ is closed under binary operation * (multiplication).

(ii) $(Z^+, *)$ is associative as ordinary multiplication is associative operation.

(iii) So algebraic system $(Z^+, *)$ is a semigroup $(Z^+, *)$ has identity element 1, as 1 multiplied by any number is that number itself

$\therefore$ $(Z^+, *)$ is monoid.

(iv) * is commutative operation i.e. $a * b = b * a$

(b) (i) Maximum of any two positive integers is a positive integer.

$\therefore$ set Z^+ is closed under binary operation *.

(ii) Now check for associativity suppose $a > b > c$

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

Scanned by CamScanner

$\therefore$ 'max' is an associative operation.

$\therefore$ The algebraic system $(Z^+, \max)$ is a semigroup.

(iii) For any element $a \in Z^+$

$$1 \max a = \max a\ 1 = a$$

$\therefore$ 1 is identity element

$\therefore$ Algebraic system $(Z^+, \max)$ is monoid.

(iv) $\therefore$ Max is commutative operation.

$\because$ $\max(a, b) = \max(b, a)$

(c) Get set Z is set of integers

(i) For any $a, b \in Z$, $a * b \in Z$,

So set Z is closed under binary operation $*$.

(ii) Now check for associativity

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

$$(a + b - ab) * c = a * (b + c - bc)$$

$$a + b - ab + c - (a + b - ab)\, c = a + b + c - bc - a\,(b + c - bc)$$

$$= a + b - ab + c - (ac + bc - abc) = a + b + c - bc - (ab + ac - abc)$$

$$a + b - ab + c - ac - bc + abc = a + b + c - bc - ab - ac + abc$$

$$-ac - bc = -bc - ac$$

$$bc + ac = bc + ac$$

$\therefore$ $*$ is associative operation

$\therefore$ Algebraic system $(Z, *)$ is semigroup

(iii) Now check for identity

$$a * 0 = a + 0 - a * 0$$

$$= a$$

$\therefore$ '0' is identity element

$\therefore$ Algebraic system $(Z, *)$ is monoid

(iv) and $a * b = a + b - ab$

$$b * a = b + a - ba$$

$$\therefore\ a * b = b * a$$

$\therefore$ It is commutative operation.

Example 3 : Let G be a group prove that the identity element e is unique **MU - May 98, Dec. 05**

Solution :

Suppose that $f \in G$, f is identity element of G and $f \neq e$.

We will now show that $f = e$, a contradiction which completes the proof.

$$f = f * e \quad \text{since e is an identity}$$

$$= e \quad \text{since f is an identity}$$

Scanned by CamScanner

Example 4 : Let G be the group, prove that each element a in G has only one inverse in G.
MU - May 98, Dec. 02, May 04

Solution :

If possible consider b, c ∈ G are two inverses of a such that a * b = I and a * c = I

where I = identity element

$\Rightarrow$ a * b = a * c

$\Rightarrow$ b = c ...left cancellation property

$\therefore$ Inverse is unique.

$\therefore$ Each element 'a' in Group G has one inverse.

Example 5 : Show that if every element in a group is its own inverse, then the group must be Abelian.
MU - Dec. 98, Dec. 13, May 15

Solution :

The inverse exists for all x ∈ A as x * x = e i.e. every element is its own inverse

$\therefore$ Now, the identity is e

$\therefore$ x * e = e * x = x $\because$ by definition of identity

$\therefore$ x * e = e * x

$\therefore$ But for all y ∈ A. y * y = e

$\therefore$ x * y * y = y * y * x

Now, we see that y * y is another element of A say b

x * b = b * x

For all x ∈ A

$\therefore$ (A, *) is an Abelian group.

Example 6 : State and prove right or left cancellation property for a group.
MU - May 97, May 99, May 09

Solution :

Let G be a group and let a, b, c be elements of G then

(a) ab = ac implies that b = c **(left cancellation property)**

(b) ba = ca implies that b = c **(right cancellation property)**

Suppose that ab = ac

Multiplying both sides of this equation by a^{-1} on the left, we obtain

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$ $\because$ associativity

$eb = ec$ $\because$ by definition of inverse

$b = c$ by definition of an identity.

Scanned by CamScanner

Example 7 : t (A, *) be an algebraic system where * is a binary operation. Such that for any a and b A. a * b = a.

Show that * is an associative operation.

Can * ever be a commutative operation. **MU - May 97**

Solution :

(i) * (b * c) = a * b = a ... by definition ...(1)

a * b) * c = a * c = a ... by definition ...(2)

From I tions (1) and (2)

a * (b * c) = (a * b) * c ∴ * is associative operation

(ii) No, cor er a, b ∈ A

Then : b = a
a = b
} by definition of (A, *)

∴ a * b * a unless a = b

∴ * c ever be a commutative operation

Example 8 : etermine whether the set together with the binary operation * is a semigroup, monoid or group. Justify your answer.

) Set of real numbers with a * b = a + b + 2.

) The set of m × n matrices under the operation of multiplication.

MU - Dec. 96, May 2000

Solution :

(a) (i) F check for associativity

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

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

a + b + c + 2 + 2 = a + b + 2 + c + 2

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

(ii) S f real number is closed under the binary operation *.

T efore it is a semigroup.

(iii) I s an identity element i.e. – 2,

(–2) = a + (– 2) + 2

= a

Hence it monoid.

(iv) Every element in this set has an inverse.

For any ment a in this set a^{-1} is

$a * a^{-1} = -2$

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

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

Scanned by CamScanner

$\therefore a + a^{-1} = -4$

$\therefore a^{-1} = -4 - a$

$\therefore a^{-1} = -(4 + a)$

$\therefore$ Hence it is a group.

(b) Multiplication of matrices is not associative operation

$\therefore$ It is not a semigroup, not a monoid, not a group

Example 9 : Let G be a group and let a and b elements of G then

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

MU - May 98, May 03, May 04, Dec. 05, May 06, May 12

Solution :

(a) We show that a acts as an inverse for a^{-1}

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

Since the inverse of an element is unique we conclude that $(a^{-1})^{-1} = a$

(b) We easily verify that

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

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

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

Example 10 : Show that a group G is Abelian if and only if $(ab)^2 = a^2b^2$ for all elements a and b in G.

MU - Dec. 96, Dec. 98, May 99, Dec. 99, Dec. 08, Dec. 10, May 14, May 16

Solution :

Proof : Part I :

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

$\therefore a * b * a * b = a * a * b * b$

Premultiply by a^{-1} and post multiply by b^{-1} on both sides

$\therefore a^{-1} * a * b * a * b * b^{-1} = a^{-1} * a * a * b * b * b^{-1}$

$\therefore b * a = a * b$

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

and $e * x = x$

Now since $b * a = a * b$

G is an Abelian group.

Scanned by CamScanner

Part II :

Now assume G is Abelian

Therefore $a * b = b * a$

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

$= a * (b * a) * b$ ∵ associative

$= a * (a * b) * b$ ∵ Abelian

$= (a * a) * (b * b)$ ∵ associative

$= a^2 b^2$

Hence proved.

Example 11 : Let G be the set of all non–zero real numbers and let $a * b = \frac{ab}{2}$. Show that (G, *) is an Abelian group. **MU - May 03, May 09, May 14**

Solution :

(i) We first verify that * is a binary operation. If a and b are elements of G then ab/2 is a non zero real number and hence is in G.

(ii) We next verify associativity since

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)\,c}{4}$$

and since $$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)\,c}{4}$$

the operation * is associative.

(iii) The number 2 is the identity in G, for if $a \in G$, then

$$a * 2 = \frac{(a)\,(2)}{2} = a = \frac{(2)\,(a)}{2} = 2 * a$$

(iv) Finally, if $a \in G$, then $a' = 4/a$ is an inverse of a, since

$$a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)\,(a)}{2} = \frac{4}{a} * a = a' * a$$

(v) Since $a * b = b * a$ for all a and b in G, we conclude that G is an Abelian group.

Example 12 : Let G be a group, and let a and b be elements of G. Then

(a) The equation $ax = b$ has a unique solution in G.

(b) The equation $ya = b$ has a unique solution in G. **MU - May 98, Dec. 05**

Solution :

Proof :

(a) The element $x = a^{-1}b$ is a solution of the equation $ax = b$ since

$$a(a^{-1}b) = (aa^{-1})\,b = eb = b$$

Scanned by CamScanner

Suppose now that x_1 and x_2 are two solutions of the equations $ax = b$. Then $ax_1 = b$ and $ax_2 = b$.

Hence $ax_1 = ax_2$

$\therefore$ $x_1 = x_2$

(b) The proof is similar to that of part (a).

Example 13 : Let (A, *) be a semigroup let a be an element of A. Consider a binary operation + on A such that for every x and y in A.

$x + y = x * a * y$

Show that + is an associative operation. **MU - Dec. 97**

Solution :

Here we have to prove that + is an associative operation.

Proof : i.e. To prove that

$$(x + y) + z = x + (y + z)$$

L.H.S. $= (x + y) + z = (x * a * y) + z$

$= x * a * y * a * z$ $\rightarrow$ definition of +

R.H.S. $= x + (y + z) = x + (y * a * z)$

$= x * a * y * a * z$ $\rightarrow$ definition of +

From above we see that LHS = RHS.

Hence we conclude that + is an associative operator.

Example 14 : If (G, *) is an Abelian group, then for all $a, b \in G$ show that $(a * b)^n = a^n * b^n$. **MU - Dec. 97, May 01, Dec. 13, Dec. 15**

Solution :

(i) Basis step : For n = 1

$(a * b)' = a' * b'$

$\therefore$ $a * b = a * b$

$\therefore$ Statement is true for n = 1

(ii) Induction step :

Let the given statement be true for some n = k where $k \in N$.

$\therefore$ $(a * b)^k = a^k * b^k$ ...(1)

To prove the statement for n = k + 1

Scanned by CamScanner

$$(a * b)^{k+1} = (a * b)^k * (a * b) \quad \text{... definition of } a^n$$

$$\therefore \quad (a * b)^{k+1} = a^k * b^k * a * b \quad \text{... from Equation (1)}$$

$$\therefore \quad (a * b)^{k+1} = a^k * a * b^k * b \quad \because (G, *) \text{ is an Abelian group}$$

$$(a * b)^{k+1} = a^{k+1} * b^{k+1} \quad \because \text{definition of } a^n$$

Using the principle of mathematical induction we state that

$$(a * b)^n = a^n * b^n \text{ for all } n \in N$$

Example 15 : Let (A, *) be a monoid such that for every x in A, $x * x = e$, where e is the identity element. Show that (A, *) is an Abelian group. **MU - Dec. 97, May 00, May 01**

Solution :

(A, *) is a monoid

where $\forall x \in A$

$$x * x = e \text{ where e is the identity element}$$

Now,

(i) (A, *) is a monoid

$\therefore$ * is associative over the set A

(ii) As (A, *) is a monoid it has the identity element

(iii) The inverse exists for all $x \in A$ as $x * x = r$ i.e. every element is its own inverse

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

$\therefore$ Now, the identity is e.

$$\therefore x * e = e * x = x \quad \because \text{by definition of identity}$$

$$\therefore x * e = e * x$$

$\therefore$ But for all $y \in A \quad y * y = e$

$$\therefore x * y * y = y * y * x$$

Now, we see that y * y is another element of A say b

$$\therefore x * b = b * x$$

For all $x \in A$

$\therefore$ (A, *) is an Abelian group

Example 16 : Let S = {x|x is real number and $x \neq 0, x \neq -1$} consider the following functions.

$f_i = S \to S, \; i = 1, 2, \ldots 6$

$f_1(x) = x; \; f_2(x) = \frac{1}{x}; \; f_3(x) = 1 - x$

$f_4(x) = \frac{x}{1-x}; \; f_5(x) = \frac{1}{1-x}; \; f_6(x) = \frac{x-1}{x}$

Show that $G = \{f_1, f_2, \ldots f_6\}$ is a group under operation composition.

Give multiplication table for G. **MU - Dec. 03, Dec. 05**

Scanned by CamScanner

Solution : To show that (G, *) is group under operation composition

$$(f_2 * f_3)(x) = f_2 * [f_3(x)] = f_2 * (1 - x)$$

$$= \frac{1}{(1-x)}$$

$$\therefore \quad f_1 * (f_2 * f_3)(x) = f_1 * \frac{1}{(1-x)} = \frac{1}{(1-x)}$$

Now $$(f_1 * f_2)(x) = f_1 * f_2(x) = f_1 * \frac{1}{x} = \frac{1}{x}$$

$$\therefore \quad [(f_1 * f_2) * f_3](x) = (f_1 * f_2) * f_3(x) = (f_1 * f_2) * (1 - x)$$

$$= \frac{1}{(1-x)}$$

$\therefore$ Associative

f_1 is identity element as $f_1(x) = x$

$$\therefore \quad f_1 * f_2(x) = f_1 * \left(\frac{1}{x}\right)$$

$$= \frac{1}{x}$$

each of $f_1\ f_2\ f_3\ f_4 f_5$ has its inverse under composition i.e. e.g. inverse of f_5 is f_4.

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

Multiplication table.

×	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_2	f_6	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_2	f_3	f_4

Example 17 : Write all permutations of the elements of the set {1, 2, 3}. Show that this set of permutations of the elements of the set (1, 2, 3) forms a group under the composition of permutations. **MU - May 97, Dec. 97, May 99, Dec. 99, May 2000**

Solution :

The permutations are enumerated below

1. 1, 2, 3 2. 1, 3, 2 3. 2, 1, 3

4. 2, 3, 1 5. 3, 1, 2 6. 3, 2, 1

Scanned by CamScanner

Let the order of three elements be {1, 2, 3} = A. Now, we define permutations of A as

$$P_1(A) = 1, 2, 3 \qquad P_2(A) = 1, 3, 2$$

$$P_3(A) = 2, 1, 3 \qquad P_4(A) = 2, 3, 1$$

$$P_5(A) = 3, 1, 2 \qquad P_6(A) = 3, 2, 1$$

where 1, 2, 3 denotes the index of element in set A

e.g. if $A = \{3, 2, 1\}$ then $P_1(A) = 3, 2, 1$

Now, to show that the above set of functions

$$P = \{P_1(A), P_2(A), P_3(A), P_4(A), P_5(A), P_6(A)\}$$

is a group under the composition of permutations considering any triple of functions on A. Then it can be shown that the operation is associative

$$(P_1(A) \cdot P_2(A)) \cdot P_3(A) = 3, 1, 2 \qquad \ldots(1)$$

$$P_1(A)\,(P_2(A) \cdot P_3(A)) = 3, 1, 2 \qquad \ldots(2)$$

From Equations (1) and (2) it is seen that the operation is associative.

There is an identity function.

i.e. $P_1(A)$

e.g. $P_1(3, 2, 1) = 3, 2, 1$

or $P_k(A) \cdot P_1(A) = P_k(A) \qquad \ldots(3)$

Thus an identity exists.

An inverse exists for every element such that,

$$P_k(A) \cdot P_{k-1}(A) = \{1, 2, 3\} \qquad \ldots(4)$$

The list of functions and inverse functions is tabulated below

Function	$P_1(A)$	$P_2(A)$	$P_3(A)$	$P_4(A)$	$P_5(A)$	$P_6(A)$
Inverse	$P_1(A)$	$P_2(A)$	$P_3(A)$	$P_5(A)$	$P_4(A)$	$P_6(A)$

From Equations (1), (2), (3), (4) the set of permutations of the elements of the set {1, 2, 3} forms a group under the composition of permutations.

Example 18 : Let Q be the set of positive rational numbers which can be expressed in the form 2^a3^b, where a and b are integers. Prove that algebraic structure (Q, ·) is a group. Where · is multiplication operation. **MU - Dec. 02, May 05, May 06, May 12**

Solution :

To show that (Q, ×) is a group.

We need to show closed, associative, identity and inverse property.

Scanned by CamScanner

For a_1, a_2, b_1, b_2 integers, $a_1 + a_2, b_1 + b_2$ are also integers.

$\therefore \quad (2^{a1}\, 3^{b1}) \cdot (2^{a2}\, 3^{b2}) = 2^{a1+a2} \cdot 3^{b1+b2} \in Q$

For $2^{a1}\, 3^{b1}, 2^{a2}\, 3^{b2} \in Q$

$\therefore$ Set Q is closed under multiplication operation.

Now check for associativity

$$(2^{a1}\, 3^{b1}) \cdot [(2^{a2}\, 3^{b2})\,(2^{a3}\, 3^{b3})] = 2^{a1}\, 3^{b1} \cdot [2^{a2+a3}\, 3^{b2+b3}]$$
$$= 2^{a1+a2+a3}\, 3^{b1+b2+b3}$$
$$= (2^{a1+a2}\, 3^{b1+b2}) \cdot 2^{a3}\, 3^{b3}$$
$$= [(2^{a1} 3^{b1}) \cdot (2^{a2}\, 3^{b2})] \cdot [2^{a3}\, 3^{b3}]$$

$\therefore$ This binary operation is associative.

Now check for identity element for a, b as integers = 0

$$2^a\, 3^b = 1$$

$\therefore$ for each $2^a 3^b$ there exists $1 = 2^0\, 3^0$

Such that $(2^a\, 3^b) \cdot (2^0\, 3^0) = 2^a 3^b$

$\therefore$ Identity element exists for a, b as integers = 0

Now find inverse

For each a, b as integers

There exists –a, –b such that

$$(2^a\, 3^b) \cdot (2^{-a}\, 3^{-b}) = 2^0\, 3^0 = 1$$

$\therefore$ Inverse exists

$\therefore$ $(Q, \times)$ is group

Example 19 : If S is non-empty set. Prove that the set P(S) (power set of S), where $A \mathbin{\dot{}} B = A \oplus B$ (Symmetric difference of A and B) is abelian group. **MU - Dec. 06**

Solution :

(1) $\oplus$ is binary operation

If $A, B \in P(S)$ then $A \oplus B \in P(S)$

(2) $\oplus$ is Associative

(3) $\{\}$ is identity element

(4) a^{-1} is left inverse of a

(5) $A \oplus B = B \oplus A \quad A, B \in P(S)$

$\therefore$ So it is abelian group

Example 20 : Let G be the set of rational numbers other than 1. Let define an operation $*$ on G by $a * b = a + b - ab$ for all $a, b \in G$. Prove that $(G, *)$ is a group. **MU - Dec. 13**

Scanned by CamScanner

Solution :

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

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

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 $a * e = a \; \forall \; a \in Q$.

$$\therefore \; a + e - ae = a \quad \text{or} \quad e - ae = 0$$
$$\text{or} \; e(1 - a) = 0 \quad \text{or} \quad e = 0, \text{ if } 1 - a \neq 0$$

Similarly, for $e * a = a \; \forall \; a \in Q$, we have $e = 0$

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. Then we have

$$a * a^{-1} = 0 \qquad \therefore \; a + a^{-1} - aa^{-1} = 0$$
$$\text{or} \; a^{-1}(1 - a) = -a \; \text{or} \; a^{-1} = \frac{a}{a - 1}, \; a \neq 1.$$
$$\text{Now} \; \frac{a}{a - 1} \in Q, \; \text{if } a \neq 1$$

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.

7.2.3.6 Additive Modulo m :

We define a new type of addition called **"addition modulo m"** and written as $a +_m b$ or $(a + b) \pmod m$, where a and b are integers and m is a positive integer.

By this we mean

$$a +_m b = r, \qquad 0 \leq r \leq m$$

Where r is least non-negative remainder when the ordinary sum of a and b is divided by m, that is we add a and b in the usual way and then from the sum, we remove integral multiples of m in such a way that the remainder r which is left out is either 0 or positive integer less than m.

Scanned by CamScanner

For e.g.

(i) $14 +_6 8 = 22 \% 6 = 4$

(ii) $5 +_6 3 = 8 \% 6 = 2$

(iii) $9 +_{12} 3 = 12 \% 12 = 0$

(iv) $3 +_3 1 = 4 \% 3 = 1$

(v) $-23 +_3 3 = -20 \% 3 = (-3) \times 7 + 1 = 1$

7.2.3.7 Examples :

Example 1 : Prove that the set G = {0, 1, 2, 3, 4, 5} is an Abelian group of order 6 with respect to addition modulo 6. **MU - Dec. 04, May 07, Dec. 09, Dec. 11, May 13, May 16**

Solution :

$+_6$	0	1	2	3	4	5	
0	0	1	2	3	4	5	$0 + 0 \bmod 6 = 0$
1	1	2	3	4	5	0	$0 + 1 \bmod 6 = 1$
2	2	3	4	5	0	1	$0 + 2 \bmod 6 = 2$
3	3	4	5	0	1	2	$0 + 3 \bmod 6 = 3$
4	4	5	0	1	2	3	$0 + 4 \bmod 6 = 4$
5	5	0	1	2	3	4	$0 + 5 \bmod 6 = 5$

} 1^{st} row

Similarly other rows are calculated.

(i) All the entries in the composition table are elements of the set G. Hence G is closed with respect to addition modulo 6 ($+_6$).

(ii) The composition $+_6$ is associative. If a, b, c are any three elements of G, then

$$a +_6 (b +_6 c) = (a +_6 b) +_6 c$$

Let $a = 1, b = 2, c = 3,$

$$1 +_6 (2 +_6 3) = (1 +_6 2) +_6 3$$

$$1 +_6 5 = 3 +_6 3$$

$$0 = 0$$

Let $a = 3, b = 4, c = 5$

$$3 +_6 (4 +_6 5) = (3 +_6 4) +_6 5$$

$$3 +_6 3 = 1 +_6 5$$

$$0 = 0$$

Hence, $+_6$ is an associative operation. Since it is satisfying for all a, b, c, $\in$ G.

(iii) If a is any element of G, then from the composition table we see that

$$0 +_6 a = a = a +_6 0 = 0$$

Scanned by CamScanner

that is, $0 +_6 0 = 0 +_6 0 = 0$

$0 +_6 1 = 1 +_6 0 = 1$

$0 +_6 2 = 2 +_6 0 = 2$

$0 +_6 3 = 3 +_6 0 = 3$

$0 +_6 4 = 4 +_6 0 = 4$

$0 +_6 5 = 5 +_6 0 = 5$

$\therefore$ 0 is identity element.

(iv) From the composition table we can also see the left inverses of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively. Since,

$$0 +_6 0 = 0 \quad 1 +_6 5 = 0 \quad 2 +_6 4 = 0$$

$$3 +_6 3 = 0 \quad 4 +_6 2 = 0 \quad 5 +_6 1 = 0$$

e.g. $4 +_6 2 = 0 = 2 +_6 4$ implies 4 is the inverse of 2.

(v) The composition is commutative as the corresponding rows and columns in the position are *identical*.

(vi) The number of elements in the set G = 6

$\therefore$ $(G, +_6)$ is a finite Abelian group of order 6.

7.2.3.8 Multiplication Modulo 'P' :

A new type of multiplication known as **"multiplication modulo P"** and written as $a \times_p b$ where a and b are any integers and p is fixed positive integer is defined as :

$$a \times_p b = r \qquad 0 \leq r < p \text{ where}$$

Where r is the least non-negative remainder when ab (ordinary product of a and b) is divided by p.

e.g. (i) $8 \times_5 3 = 24 \bmod 5 = 4$

(ii) $4 \times_7 2 = 8 \bmod 7 = 1$

Scanned by CamScanner

7.2.3.9 Examples :

Example 1 : Prove that the set G = {1, 2, 3, 4, 5, 6} is a finite Abelian group of order 6 with respect to multiplication modulo 7.

MU - May 06, May 10, Dec. 10, May 11, May 12, May 14, Dec. 15, May 17

Solution :

$\times_7$	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

$2 \times 1 \bmod 7 = 2$
$2 \times 2 \bmod 7 = 4$
$2 \times 3 \bmod 7 = 6$
$2 \times 4 \bmod 7 = 1$
$2 \times 5 \bmod 7 = 3$
$2 \times 6 \bmod 7 = 5$

} 2^{nd} row

Similarly row 1, row 3, row 4, row 5, and row 6 are calculated.

(i) All the entries in the composition table are elements of G. Hence G is closed under multiplication modulo 7 ($\times_7$)

(ii) The composition of $\times_7$ is associative. Let a, b, c are any three elements of G, then

$$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$$

Let $a = 1,\ b = 2,\ c = 3$

$$1 \times_7 (2 \times_7 3) = (1 \times_7 2) \times_7 3$$
$$1 \times_7 6 = 2 \times_7 3$$
$$6 = 6$$

Let $a = 4,\ b = 5,\ c = 6$

$$4 \times_7 (5 \times_7 6) = (4 \times_7 5) \times_7 6$$
$$4 \times_7 2 = 6 \times_7 6$$
$$1 = 1$$

Hence, $\times_7$ is an associative operation. Since it is satisfying for all $a, b, c \in G$.

(iii) We have $1 \in G$

If a is any element of G, then from the composition table, we can see that

$$1 \times_7 a = a = a \times_7 1$$

that is,
$$1 \times_7 0 = 0 \times_7 0 = 0$$
$$1 \times_7 1 = 1 \times_7 1 = 1$$
$$1 \times_7 2 = 2 \times_7 1 = 2$$
$$1 \times_7 3 = 3 \times_7 1 = 3$$
$$1 \times_7 4 = 4 \times_7 1 = 4$$

Scanned by CamScanner

$$1 \times_7 5 = 5 \times_7 1 = 5$$

$$1 \times_7 6 = 6 \times_7 1 = 6$$

$\therefore$ 1 is an identity element

(iv) From the composition table, we can see that the left inverses of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6 respectively. Since,

e.g. $3 \times_7 5 = 1 = 5 \times_7 3$ i.e. inverse of 3 is 5.

(v) The composition $\times_7$ is commutative as the corresponding rows and columns in the table are identical.

(vi) The set has 6 elements hence group $(G, \times_7)$ is a finite Abelian group of order 6.

Example 2 : Let Z_4 i.e. G = {0, 1, 2, 3}

(i) Prepare its composition table with respect to 'x_4' (ii) Is it a group ?

MU - Dec. 08

Solution : Let G = { 0, 1, 2, 3,}

(i) Composition table with respect to 'X_4'

X_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) (a)The set G is closed under the operation X_4 because all elements belongs to composition table are belong to set G.

(b) Now check for associativity for any a, b, c $\in$ G

$$(a\, X_4\, b)\, X_4\, C = a\, X_4\, (b\, X_4\, C)$$

Let a = 1, b = 2, c = 3

$$(1\, X_4\, 2)\, X_4\, 3 = 1\, X_4\, (2\, X_4\, 3)$$

$$2\, X_4\, 3 = 1\, X_4\, 2$$

$$2 = 2$$

'X_4' is an associative operation.

(c) For any element a in set A

$1\, X_4\, a = a\, X_4\, 1 = a$ that is

$0\, X_4\, 1 = 1\, X_4\, 0 = 0$

$1\, X_4\, 1 = 1\, X_4\, 1 = 1$ $\therefore$ '1' is identity element.

$2\, X_4\, 1 = 1\, X_4\, 2 = 2$

$3\, X_4\, 1 = 1\, X_4\, 3 = 3$

(d) Left inverse of 0 and 2 is not exists. Hence (a, X_4) is not a group.

Scanned by CamScanner

7.2.3.10 Cyclic Group :

Definition :

MU - Dec. 97, Dec. 98, May 99, Dec. 2000, May 13

A group (G, *) is said to be a **cyclic group** if there exists an element a ∈ G such that every element of G can be written as some power of a, viz a^k, for some integer k. By a^k, we mean a * a * a ... a (k times). We then say that G is generated by a or a is a generator of G.

A cyclic group is Abelian, since for any two elements a^r, $a^s \in G$,

$$a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r.$$

Examples :

(i) The group $(Z_m, +)$ is cyclic group of order m, generated by 1.

(ii) Let S be the unit circle, and let P_0 be the rotation of the circle through an angle $2\pi/n$. Then the set of rotations $\{P_0, P_0 2, P_0 3, \ldots, P_n{}^n\}$ forms a cyclic group of order n, under the operation composition of functions.

Theorem :

Let G be a cyclic group of order n. Then n is the smallest positive integer such that $a^n = e$, where a is a generator of G.

Proof :

Consider the subset $\{a, a^2, \ldots\ldots\}$ of G. Since G is finite, the power of a must terminate at some stage. Hence, there exists positive integers r and s. Such that $a^r = a^s$.

Assume r > s. Then $a^{(r-s)} = e$. Since there exists atleast one element with this property, choose m least such that $a^m = e$. Now $m \leq n$, since otherwise order of g is greater than n. We shall show m = n. Suppose m < n. Then for any k such that $m < k \leq n$, by division algorithm k pm + q, where $0 \leq q < m$.

Then $a^k = a^{pm+q} = (a^p)^m * a^q = a^q$

Since, q < m, $a^q \in \{a, a^2, \ldots\ldots, a^m\}$.

Since a is a generator for G, this means $G \subset \{a, a^2, \ldots\ldots, a^m\}$, which is absurd. Hence $m \nleq n$ and therefore m = n.

7.2.3.11 Subgroups :

Definition :

MU - Dec. 98, Dec. 99, Dec. 2000, May 01, Dec. 02, May 04, Dec. 05, Dec. 10

Let (A, *) be a group and B be a subset of A, (B, *) is said to be a **subgroup** of A if (B, *) is also a group by itself. Suppose we want to check whether (B, *) is a subgroup for a given subset B of A. We note that

Scanned by CamScanner

1. We should test whether * is a closed operation on B.
2. * is known to be an associative operation.
3. Since there is only one element e in A such that $e * x = x * e = x$ for all x in A, we must check that e is in B. In other words the identity of (A, *) must be in B as the identity of (B, *)
4. Since the inverse of every element in A is unique for every element b in B, we must check that its inverse is also in B.

Examples :

(i) For a positive integer n, let $H = nZ = \{nx \mid x \in Z\}$. Then (H, +) is a subgroup of (Z, +).

(ii) Let $H = \{0, 4)$ in $(Z_8, +)$ H is then a subgroup of Z_8.

(iii) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication.

Let $H = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad \neq 0\right\}$ H is then a subgroup of G.

(iv) Let G be the group of all non–zero complex numbers a + ib (a, b real) under multiplication.

Let $H = \{a + ib \mid a^2 + b^2 = 1\}$

Then H is a subgroup of G.

(v) The subset $A = \{I, R_1, R_2, R_3\}$ of the group S of the symmetrics of the square, is closed under the operation * because in this subset I is unity (0°), $R_1 = 90°$, $R_2 = 180°$, $R_3 = 270°$. The inverse of 90° is 270°, the inverse of 180° is 180° and the inverse of 270° is 90°.

The subset A contains an identity element 0° and it also contains the inverse of each element in the subset.

The operation * is an associative operation on the large set S so it remains associative when restricted to the subset A. Therefore (A, *) is itself a group and also a subgroup of S.

Note : In any group (G, *) the singleton Set {e} containing only the identity element is a subgroup. The entire set G is also a subgroup.

7.2.3.12 Proper Subgroup :

The subgroup A is called a **proper subgroup** if it is neither the singleton set {e} nor the entire group G.

7.2.3.13 Generation of Subgroups :

Let (G, *) be a group and let S be a non-empty subset of G. Then the subgroup generated by S, denoted by $< S >$ is defined as

(i) If x is an element of S, then x is also an element of $< S >$.

(ii) (a) if x is in $< S >$, then x^{-1} is also in $< S >$

(b) if x and y are in $< S >$ then $x * y$ is also in $< S >$

(iii) Only elements obtained by a finite number of iterations of (a) and (b) are in $< S >$.

Step (i) : Guarantees that the set S is contained in $< S >$ and

Step (ii) : Guarantees that $< S >$ is a subgroup of G.

Scanned by CamScanner

7.2.3.14 Examples :

Example 1 : Generate subgroup by 2 in (Z, +) for set (Z, +) identity element is '0'.

Solution :

Set $S = \{2\}$

Since $2 \in S, 2 \in < S >$

$2 \in < S >$

$\therefore$ Inverse of 2 $= -2 \in < S >$

$2 + 2 = 4 \in < S > -2 + -2 = -4 \in < S >$

$4 + 4 = 8 \in < S > -4 + -4 = -8 \in < S >$

$2 + 4 = 6 \in < S > -2 + -4 = -6 \in < S >$

This subgroup is denoted by $< 2 >$ and it contains even integers

$\therefore < 2 > = < \ldots -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots >$

Example 2 : Find the subgroup generated by [2] in Z_5

Solution :

The elements are Z_5 are

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The inverse of [2] in Z_5 is [3]. It must be in $< [2] >$

Also $2 + 3 = 0$,

$2 + 2 = 4$,

$3 + 3 = 1$ must be in $< 2 >$

Thus all the elements of Z_5 are in $< [2] >$.

$\therefore < [2] > = < 0, 1, 2, 3, 4 >$

Example 3 : Find the subgroup generated by [2] in Z_6.

Solution : The elements in Z_6 are

$+_6$	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

Inverse of [2] in Z_6 is [4]. It must be in $< [2] >$.

Scanned by CamScanner

Also $2+4 = 0, 2+2=4, 4+4=2$

$\therefore \quad <[2]> = <0, 2, 4>$

7.15 Coset :

Definition : MU - Dec. 98, May 01

Let (G, *) be a group and let H be a subgroup of G. For a, b ∈ G, we say a is congruent to b mod H, written as $a \equiv b \bmod H$, if $a * b^{-1} \in H$. One can easily see that the congruence relation is an equivalence relation on G. It therefore partitions G into equivalent classes called as **cosets** of H. The set of equivalence classes is also called as the **quotient** set of G by H.

Let H be a subgroup of a group (G, *). For a ∈ G define

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

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

a is called as the representative element of the coset aH or Ha. If a ∈ H, then Ha = aH = H.

Hence the right cosets of H in G partition G into disjoint subsets. Likewise the left cosets of H in G also a portion of G into disjoint subsets.

The concept of cosets as equivalence classes leads to the following theorem, known as Lagrange's theorem, which gives an important relationship between a group and its subgroup.

Theorem (Lagrange) :

The order of a subgroup of finite order divides the order of the group.

Proof :

Let (G, *) be a finite group of order n and let H be a group of G of order m. Consider a right coset Ha a ∈ G. If a ∈ H, then Ha = H, which means that number of elements in Ha is the same as the order of H. Next let a ∈ G but a ∉ H. Then for any two distinct elements $h_1, h_2 \in H$, $h_1 * a \neq h_2 * a$. Hence distinct elements in Ha correspond to distinct elements in H and vice verse. This means that each right (left) coset contains exactly m elements. Since the right (left) cosets partition G into disjoint subsets, each containing m elements, it follows that since order of G is n, we must have n/m cosets. This proves that m divides n.

7.3.16 Normal Subgroup :

Definition :

MU - Dec. 97, May 99, Dec. 2000, Dec. 02, May 05, May 07, Dec. 10, Dec. 12, May 13

A subgroup H of G is said to be a **normal subgroup** of G if for every a ∈ G, aH = Ha.

A subgroup of an Abelian group is normal.

7.3.17 Examples :

Example 1 : Let $H = \{[0]_6, [3]_6\}$. Find the left and right cosets in group Z_6. Is H a normal subgroup of group Z_6.

Scanned by CamScanner

Solution :

The addition modulo 6 group, table of Z_6 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

This is Abelian group since for all a, $b \in Z_6$,

$$a +_6 b = b +_6 a$$

Left coset of H with respect to a in the set is

$$aH = \{a * h \mid h \in H\}$$

$\therefore$ $0H = \{0 +_6 0, 0 +_6 3\} = \{0, 3\}$

$1H = \{1 +_6 0, 1 +_6 3\} = \{1, 4\}$

$2H = \{2 +_6 0, 2 +_6 3\} = \{2, 5\}$

$3H = \{3 +_6 0, 3 +_6 3\} = \{3, 0\}$

$4H = \{4 +_6 0, 4 +_6 3\} = \{4, 1\}$

$5H = \{5 +_6 0, 5 +_6 3\} = \{5, 2\}$

Right coset of H with respect to a in the set is

$$Ha = \{h * a \mid h \in H\}$$

$\therefore$ $H0 = \{0 +_6 0, 3 +_6 0\} = \{0, 3\}$

$H1 = \{0 +_6 1, 3 +_6 1\} = \{1, 4\}$

$H2 = \{0 +_6 2, 3 +_6 2\} = \{2, 5\}$

$H3 = \{0 +_6 3, 3 +_6 3\} = \{3, 0\}$

$H4 = \{0 +_6 4, 3 +_6 4\} = \{4, 1\}$

$H5 = \{0 +_6 5, 3 +_6 5\} = \{5, 2\}$

Here $0H = H0$ $1H = H1$

$2H = H2$ $3H = H3$

$4H = H4$ $5H = H5$

$\therefore$ H is normal subgroup of Z_6.

Example 2 : Let $G = Z_8$. Determine all left cosets of $H = \{[0] [4]\}$ in G. **MU - May 05**

Solution :

The addition modulo 8 table for group Z_8 is

Scanned by CamScanner

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Left coset of H with respect to a in the set is

$aH = \{a * h \mid h \in H\}$ $\quad \therefore \quad 0H = \{0 +_8 0, 0 +_8 4\} = \{0, 4\}$

$1H = \{1 +_8 0, 1 +_8 4\} = \{1, 5\}$ $\quad 2H = \{2 +_8 0, 2 +_8 4\} = \{2, 6\}$

$3H = \{3 +_8 0, 3 +_8 4\} = \{3, 7\}$ $\quad 4H = \{4 +_8 0, 4 +_8 4\} = \{4, 0\}$

$5H = \{5 +_8 0, 5 +_8 4\} = \{5, 1\}$ $\quad 6H = \{6 +_8 0, 6 +_8 4\} = \{6, 2\}$

$7H = \{7 +_8 0, 7 +_8 4\} = \{7, 3\}$

7.2.3.18 Product Group :

Definition : If G_1 and G_2 are groups, then $G = G_1 \times G_2$ is a **product group** with operation defined by,

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

Example : Let $G_1 = G_2 = Z_2$. For simplicity of notation, let us denote the equivalence class [0] by $\bar{0}$ and [1] by $\bar{1}$. Then the multiplication table for the product group $G_1 \times G_2$ is given below

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

7.2.3.19 Quotient Group :

MU - Dec. 2000

Let N be a normal subgroup of G. Then G/N is the set of cosets of N in G. For two coset elements $g_1N, g_2N \in G/N$ define an operation * on G/N as $g_1N * g_2N = (g_1 * g_2)N$. Note that the operation * on G/N is induced by the operation * in G.

Scanned by CamScanner

With this operation, G/N is a quotient group with identity element eN. The inverse of each element g_1N is naturally g_1^{-1} N.

7.2.3.20 Exercise Set - 2 (Solved) :

Example 1 : Find a set of three real numbers that is closed under addition modulo 2 and multiplication modulo 2. **MU - May 98, May 01**

Solution :

$+_2$	−1	0	1
−1	0	−1	0
0	−1	0	1
1	0	1	0

$\times_2$	−1	0	1
−1	1	0	−1
0	0	0	0
1	−1	0	1

From the above tables we conclude that the set {−1, 0, 1} of real numbers is closed under $+_2$ and $\times_2$.

Example 2 : Let Z_n denote the set of integers (0, 1, 2, ..., n − 1). Let * be binary operation on Z_n such that a * b = the remainder of ab divided by n.

(i) Construct the table for the operation * for n = 4

(ii) Show that $(Z_n, *)$ is a semigroup for any n. **MU - May 97, May 99**

Solution :

(i) The table for the operation * for n = 4

$*_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) The set Z_n is closed under the operation * because for any a, b $\in Z_n$, a * b $\in Z_n$ ...(1)

Now check for associativity for any a, b, c $\in Z_n$.

$$(a *_4 b) *_4 c = a *_4 (b *_4 c)$$

Let a = 1, b = 2, c = 3

$$(1 *_4 2) *_4 3 = 1 *_4 (2 *_4 3)$$

$$2 *_4 3 = 1 *_4 2$$

$$2 = 2$$

$\therefore$ '*' is an associative operation ...(2)

From Equations (1) and (2) we conclude that $(Z_n, *)$ is a semigroup for any 'n'.

Example 3 : Prove that the set A = {0, 1, 2, 3, 4, 5} is a finite Abelian group under addition modulo 6. **MU - May 04, Dec. 16**

Solution : Table addition modulo 6 for the set A is

Scanned by CamScanner

$+_6$	0	1	2	3	5
0	0	1	2	3	5
1	1	2	3	4	0
2	2	3	4	5	1
3	3	4	5	0	2
4	4	5	0	1	3
5	5	0	1	2	4

(i) From table we see that sum of any two elements c belong set.

$\therefore$ Set A is closed under this binary operation.

(ii) For any element a in set A.

$0 +_6 a = a +_6 0 = a$ that is,

$0 +_6 0 = 0 +_6 0 = 0$ $+_6 0 = 0 +_6 1 = 1$

$2 +_6 0 = 0 +_6 2 = 2$ $+_6 0 = 0 +_6 3 = 3$

$4 +_6 0 = 0 +_6 4 = 4$ $+_6 0 = 0 +_6 5 = 5$

$\therefore$ '0' is identity element

(iii) Now check for associativity

For any a, b, c, $\in$ A

$$a +_6 (b +_6 c) = (a +_6 b) +_6 c$$

Let $a = 0, b = 1, c = 2,$

$\therefore$ $0 +_6 (1 +_6 2) = (0 +_6 1) +_6 2$

$0 +_6 3 = 1 +_6 2$

$3 = 3$

Let $a = 3, b = 4, c = 5.$

$\therefore$ $3 +_6 (4 +_6 5) = (3 +_6 4) +_6 5$

$3 +_6 3 = 1 +_6 5$

$0 = 0$

$\therefore$ It is associative. Since it is satisfying for all a , c $\in$ A.

(iv) Left Inverse of 0 is 0, since $0 +_6 0 = 0$

Left Inverse of 1 is 5, since $5 +_6 1 = 0$

Left Inverse of 2 is 4, since $4 +_6 2 = 0$

Left Inverse of 3 is 3, since $3 +_6 3 = 3$

Left Inverse of 4 is 2, since $2 +_6 4 = 0$

Left Inverse of 5 is 1, since $1 +_6 5 = 0$

(v) It is a group of finite elements

Scanned by CamScanner

For any $a, b \in A$

$$a +_6 b = b +_6 a \text{ that is,}$$

Let $a = 2,\ b = 3$

$$2 +_6 3 = 3 +_6 2$$

$$5 = 5$$

Let $a = 4,\ b = 5,$

$$4 +_6 5 = 5 +_6 4$$

$$= 3$$

$\therefore$ $+_6$ is commutative.

$\therefore$ It is a finite Abelian group.

Example 4 : Consider the set A = {1, 2, 3, 4, 5, 6} under the multiplication modulo 7.

(a) Find the multiplication table for the above

(b) Find the inverses of 2, 3 and 5, 6

(c) Prove that it is a cyclic group

(d) Find the orders and the subgroups generated by {3, 4} and {2, 3}

MU - Dec. 99, May 2000, May 15, Dec. 16

Solution :

(a) Multiplication modulo 7 table for set A 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	1	3	2	1

(b) Note that 1 is an identity element of the algebraic system $(A, \times_7)$

Since for any $a \in A$,

$$a \times_7 1 = a = 1 \times_7 a$$

that is,

$$1 \times_7 1 = 1 \times_7 1 = 1$$

$$2 \times_7 1 = 1 \times_7 2 = 2$$

$$3 \times_7 1 = 1 \times_7 3 = 3$$

$$4 \times_7 1 = 1 \times_7 4 = 4$$

$$5 \times_7 1 = 1 \times_7 5 = 5$$

Scanned by CamScanner

$$6 \times_7 1 = 1 \times_7 6 = 6$$

Recall that a^{-1} is that element of G such that $a * a^{-1} = 1$

$$2 \times_7 4 = 1 = 4 \times_7 2 = 1$$

$$3 \times_7 5 = 1 = 5 \times_7 3 = 1$$

$$6 \times_7 6 = 1 = 6 \times_7 6 = 1$$

$\therefore$ Inverse of 2 is 4

Inverse of 4 is 2

Inverse of 3 is 5

Inverse of 5 is 3

Inverse of 6 is 6

(c) We have $2^1 = 2,$

$$2^2 = 2 \times_7 2 = 4$$

$$2^3 = 2^2 \times_7 2 = 4 \times_7 2$$

$$= 1$$

$$2^4 = 2^3 \times_7 2 = 1 \times_7 2$$

$$= 2$$

$\therefore$ Hence $|2| = 3$

$\therefore$ 2 is not generator of this group

We have $3^1 = 3$

$$3^2 = 3 \times_7 3 = 2$$

$$3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6$$

$$3^4 = 3^3 \times_7 3 = 6 \times_7 3 = 4$$

$$3^5 = 3^4 \times_7 3 = 4 \times_7 3 = 5$$

$$3^6 = 3^5 \times_7 3 = 5 \times_7 3 = 1$$

Hence $|3| = 6$

$\therefore$ 3 is generator of this group and this group is cyclic.

(d) Subgroup generated by {3, 4} is denoted by $< \{3, 4\} >$ since 3, 4 are elements of this set they have to be there in $< \{3, 4\} >$

Inverse of 3 is 5, inverse of 4 is 2

$\therefore$ $3, 4, 5, 2, \in < \{3, 4\} >$

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

$3 \times_7 5 = 1$ $\quad 5 \times_7 1 = 5$ $\quad 4 \times_7 4 = 2$ $\quad 1 \times_7 1 = 1$

Scanned by CamScanner

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

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

$\therefore \quad <\{3, 4\}> = <1, 2, 3, 4, 5, 6>$

$\therefore$ Subgroup generated by $\{3, 4\}$ is the set A itself whose order is 6.

Subgroup generated by $\{2, 3\}$ is denoted by $<\{2, 3\}>$.

Since 2, 3 are elements of this set they have to be there in $<\{2, 3\}>$.

Inverse of 2 is 4.

Inverse of 3 is 5

$\therefore$ $2, 3, 4, 5 \in <\{2, 3\}>$

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

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

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

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

$2 \times_7 1 = 2$ $3 \times_7 3 = 2$ $6 \times_7 1 = 6$

$2 \times_7 2 = 4$

$\therefore \quad <\{2, 3\}> = <1, 2, 3, 4, 5, 6>$

$\therefore$ Subgroup generated by $<\{2, 3\}>$ is the set A and is of order 6.

Example 5 : Let G be the group of integers under the operation of addition. Which of the following subsets of G are subgroups of G.

(a) The set of all even integers

(b) The set of all odd integers

Justify your answers. **MU - Dec. 96**

Solution :

(a) (i) Addition of two even integers is an even integer so the set of all even integers is closed under the binary operation 'addition'. ...(1)

(ii) Now check for associativity

For any a, b, c even integers

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

$\therefore$ '+' is associative operation ...(2)

(iii) The set of all even integers also includes the identity element of G i.e. '0' ...(3)

(iv) For any positive even integer left inverse of a is – a.

$\because \quad (-a) + (+a) = 0$

$\therefore$ a and – a both belong to set of even integers ...(4)

$\therefore$ From Equations (1), (2), (3), (4) we conclude that the set of all even integers is subgroup of the set of integers.

Scanned by CamScanner

(b) (i) Addition of two odd inte ...s could be an even integer. So the set of all odd integers is not closed under the binary operati ...ddition'. ...(1)

(ii) The set of all odd integer ...es not include the identity element of G i.e. '0' ...(2)

From Equations (1) and ...we conclude that the set of all odd integers is not subgroup of the set of integers.

Example 6 : Let G be a grou ...d let a ∈ G. Define Ha = {x | x ∈ G ...xa = ax} Prove that Ha is ...ubgroup of G. **MU - Dec. 98, Dec. 99**

Solution : Suppose x and y ∈ ...

So that xa = ax and y... ay for all a ∈ G.

We have

$$(xy)\,a = ...(ya) = x(ay) = (xa)\,y = (ax)\,y = a(xy)$$

So that x, y is in G.

and x, y ∈ H → xy ∈ H ...verified

Also, multiplying the eq...ion xa = ...x by x^{-1} on both sides we get

$$x^{-1}(xa)\,x^{-1} = ...^{-1}(ax)\,x^{-1}$$

and using the associativ...w we obtain

$$ax^{-1} = ...^{-1}a$$

Thus x^{-1} is in Ha and

$$x \in ...H \rightarrow x^{-1} \in H \text{ is verified}$$

Hence Ha is a subgroup ...G.

Example 7 : Find all the s...oups of $(Z_5, \oplus)$, where ⊕ is the operation addition modulo 5. Justify your answer. **MU - Dec. 98**

Solution :

The table for $(Z_5, \oplus)$ is

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Identity element of algebraic system $(Z_5, \oplus)$ is '0', since for any element a ∈ Z_5

Scanned by CamScanner

$0 \oplus a = a$

$1 \oplus 4 = 0 = 4 \oplus 1$

$2 \oplus 3 = 0 = 3 \oplus 2$

$\therefore$ Inverse of 1 is 4

Inverse of 4 is 1

Inverse of 2 is 3

Inverse of 3 is 2

So two subgroups of $(Z_5, \oplus)$ viz. $G_1 = \{0, 1, 4\}$, and $G_2 = \{0, 3, 2\}$

Set G_1 is closed under binary operation $\oplus$

Identity element of G i.e. '0' belong to G_1

G_2 is closed under binary operation $\oplus$

Identity element of G i.e. '0' belongs to G_2

$\therefore$ Hence both {0, 1, 4} and {0, 3, 2} are subgroups of G.

Example 8 : Let G be the group and let $H = \{x \mid x \in G \text{ and } xy = yx \text{ for all } y \in G\}$. Prove that H is subgroup of G. **MU - May 03**

Solution :

If (G, X) is group and $H \subseteq G$. Then (H, X) is subgroup if (H, X) is itself a group.

Now for $x, y \in H, x \times y \in H$

$\therefore$ H is closed under multiplication

Also for $x, y, z \in H$

We have $x \times (y \times z) = (x \times y) \times z = x \times y \times z$

$\therefore$ It is associative operation

1 is multiplicative identity since

$x, 1 \in H \Rightarrow x \times 1 = x$

For each $x \in G$ there exists $x^{-1} \in G$.

such that $x \times x^{-1} = 1$

$\therefore$ For each $x \in H$. $x^{-1} \in H$

Such that $x \times x^{-1} = 1$

Also $x \times y = y \times x$ for all $y \in G$

$\therefore$ (H, x) is a group.

Scanned by CamScanner

Syllabus Topic : Isomorphism, Automorphism and Homomorphism of Group

7.3 Isomorphism, Automorphism and Homomorphism of Group :

7.3.1 Isomorphism :

Definition :

MU - Dec. 98, May 99

An algebraic system (B, $*$) is **isomorphic** to the algebraic system (A, $\star$) if we can obtain (B, $*$) from (A, $\star$) by renaming the elements and/or the operation in (A, $\star$). In a more formal but equivalent way, we say that (B, $*$) is isomorphic to (A, $\star$) if there exists a one to one onto function f from A to B such that for all a_1 and a_2 in A.

$$f(a_1 \star a_2) = f(a_1) * f(a_2)$$

The function f is called an **isomorphism** from (A, $\star$), to (B, $*$) and (B, $*$) is called an **isomorphic image** of A.

7.3.1.1 Examples :

Example 1 :

$\star$	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

Fig. 7.8 (a)

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	α	γ
γ	β	δ	δ	γ
δ	α	β	γ	δ

Fig. 7.8 (b)

$f(a) = \alpha$
$f(b) = \beta$
$f(c) = \gamma$
$f(d) = \delta$

The function f is an isomorphism from the algebraic system (A, $\star$) in Fig. 7.8 (a) to the algebraic system (B, $*$) in Fig. 7.8 (b).

Note that the function g such that,

$g(a) = \delta$ $\quad$ $g(b) = \gamma$
$g(c) = \beta$ $\quad$ $g(d) = \alpha$

is also an isomorphism from (A, $\star$) to (B, $*$)

Scanned by CamScanner

Aditi, Danish, Shiva,

Example 2 :

*	a	b
a	a	b
b	b	a

(A, ★)

Fig. 7.9 (a)

⊕	EVEN	ODD
EVEN	EVEN	ODD
ODD	ODD	EVEN

(B, ⊕)

Fig. 7.9 (b)

*	0°	180°
0°	0°	180°
180°	180°	0°

(C, *)

Fig. 7.9 (c)

+	0 ¢	5 ¢
0 ¢	0 ¢	5 ¢
5 ¢	5 ¢	0 ¢

(D, +)

Fig. 7.9 (d)

In Fig. 7.9, the algebraic system (B, ⊕), (C, *), and (D, +) are all isomorphic to the algebraic system (A, ★). As a matter of fact, the system (B, ⊕) corresponds to the addition of even and odd numbers, the system (C, *) corresponds to the rotation of geometric figures in the plane by 0° and 180°, and the system (D, +) corresponds to the situation of purchasing two items in a five-and-ten store, where the element 0¢ in D stands for amounts that are multiples of 10¢, the element 5d stands for amounts that are multiples of 10¢ plus 5¢ and the binary operation + determines whether the total purchase price is a multiple of 10¢ or is a multiple of 10¢ plus 5¢.

7.3.2 Automorphism :

An isomorphism from an algebraic system (A, ★) to (A, *) is called an **automorphism** on (A, ★).

Example : The function f such that,

$$f(a) = d \qquad f(b) = c$$
$$f(c) = b \qquad f(d) = a$$

is an automorphism on the algebraic system (A, ★) in Fig. 7.8 (a).

A physical interpretation of an automorphism on an algebraic system is a way in which the elements in the system interchange their roles.

7.3.3 Homomorphism :

Let (A, ★) and (B, *) be two algebraic systems. Let f be a function from A onto B such that for any a_1 and a_2 in A

$$f(a_1 \star a_2) = f(a_1) * f(a_2)$$

f is called a **homomorphism** from (A, ★) to (B, *) and (B, *) is called a **homomorphic image** of (A, ★).

Example : For the two algebraic systems shown in Fig. 7.10 (a) and (b), the function f such that

Scanned by CamScanner

$f(\alpha) = 1$

$f(\delta) = 0$

$f(\zeta) = -1$

$f(\gamma) = 1$

★	α	β	γ	δ	∈	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	∈
γ	α	γ	α	β	γ	∈
δ	α	β	β	δ	∈	ζ
∈	γ	γ	γ	∈	∈	ζ
ζ	δ	∈	∈	ζ	ζ	ζ

Fig. 7.10 (a)

	1	0	−1
	1	1	0
	1	0	−1
	0	−1	−1

Fig. 7.10 (b)

Is a homomorphism from the algebraic system $(\{\alpha, \beta, \gamma, \delta, \in, \zeta\}, *)$ to the algebraic system $(\{1, 0, -1\}, *)$

7.3.4 Congruence Relation :

MU - May 09

Let (A, ★) be an algebraic system and R be an equivalence relation on A. R is called a **congruence relation** on A (with respect to ★) if (a_1, a_2) and (b_1, b_2) in R implies that $(a_1 \star b_1, a_2 \star b_2)$ is also in R.

Example :

1. For the algebraic system in Fig. 7.11 (a) the equivalence relation R in Fig. 7.11 (b) is a congruence relation.

★	a	b	c	d
a	a	a	c	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	a

Fig. 7.11 (a)

	a	b	c	d
a	√	√		
b	√	√		
c			√	√
a			√	√

Fig. 7.11 (b)

Scanned by CamScanner

2.

★	a	b	c	d
a	a	a	d	c
b	b	a	d	a
c	c	b	a	b
d	c	d	b	a

Fig. 7.11 (c)

	a	b	c	d
a	√	√		
b	√	√		
c			√	√
d			√	√

Fig. 7.11 (d)

For the algebraic system in Fig. 7.11 (c), the equivalence relation R in Fig. 7.11 (d) is not a congruence relation. (For instance, although (a, b) and (c, d) are in R, (a ★ c, b ★ d), which is equal to (d, a) is not in R).

7.3.5 Exercise Set - 3 :

Example 1 : Let (G, *) be a group and $a \in G$. Let $f : G \to G$ be given by $f(x) = a * x * a^{-1}$ for every $x \in G$. Prove that f is an isomorphism of G onto G. **MU : Dec. 98**

Solution :

Let $x, y \in G$

$$f(x * y) = a *(x * y) * a^{-1}$$
$$= a * x * a^{-1} * a * y * a^{-1}$$
$$= f(x) * f(y)$$

$\therefore$ f is a homomorphism.

Suppose that $x \in G$

Then $f(a^{-1} * x * a) = a * a^{-1} * x * a * a^{-1}$

$= x$

So f is **onto** ...(1)

Suppose that $f(x) = f(y)$

then $a * x * a^{-1} = a * y * a^{-1}$

Now $a^{-1} * (a * x * a^{-1}) * a = a^{-1} * (a * y * a^{-1}) * a$

and $x = y$

Thus f is **one to one** ...(2)

$\therefore$ f is an isomorphism of G onto G

Scanned by CamScanner