MODULE - V - ALGEBRAIC STRUCTURES

Syllabus

* Algebraic structures - Algebraic system - properties
* Homomorphism and Isomorphism
* Semigroup and monoid - cyclic monoid
* Subsemigroup and submonoid
* Homomorphism and Isomorphism of semigroup and monoids.
* Group - Elementary properties, subgroup, symmetric group on three symbols.
* The direct product of two groups
* Group Homomorphism, Isomorphism of groups.
* Cyclic group
* Right Coset, Left Coset - Lagranges theorem.

Operation (function, transformation, mapping or correspondence)

An n-ary operation on A is a function f from A^n to A which associates a unique value in A to every ordered n-tuple whose members are also in A
1-ary is known as unary, 2-ary is known as binary
3-ary is known as ternary

Eg Let P(S) be the powerset of non empty S. Then for any A, B, C of P(S). complementation is unary. operation union, intersection, symmetric difference $\oplus$ defined by $A\oplus B = (A\cup B)-(A\cap B)$ are binary operation. $A\cap B\cap C$ is ternary operation. $\bigcup_{i=1}^{n} A_i$ is n-ary operation

Introduction

operation:-

An operation is a function which takes more input values (called operands) to a well defined output value.

Depending upon the number of operands there are many operations

1- ary or unary (one ~~operator~~ operand) Eg:- $A^T, \neg A, A^{-1}$

2-ary or binary (2 ~~operators~~ operands) Eg:- $A+B,\ A-B,\ A\cdot B, \cdots$

3-ary or ternary (3 ~~operators~~ operands) Eg:- $A\cap B\cap C,\ A\cup B\cup C \cdots$

$\vdots$

n-ary (n ~~operators~~ operand) Eg:- $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$.

Closure Property

A set S is said to be closed w.r.t an operation if this operation on members of S always produces another member of S.

Eg:- 1) Set of integers with operation addition & multiplication is closed

2) But Z with division is not closed

Reason :- $\frac{4}{3}$ is not an integer.

$\therefore$ Z is not closed under division.

Eg: 3 Let $S = \{A / A_{m \times n} \text{ real matrix}\}$.

S is closed under matrix addition & substraction. but S is not closed under the unary operation of transposition. Because A^T is $n \times m$ matrix $\notin S$.

4. Set of all odd integers are not closed w.r.t addition. Because sum of 2 odd numbers is even.

Algebraic Systems

An algebraic system or mathematical system consists of a set, with an operation on the set and accompanying properties which are taken as axioms of the system.

ie An algebraic system or simply an algebra is a system consisting of a non empty set A and one or more n-ary operations on the set 'A' and is denoted by $\langle A, f_1, f_2, f_3, \dots \rangle$

An algebraic structure is an algebraic system $\langle A, f_1, f_2, \dots R_1, R_2 \dots \rangle$ wherein addition to operations f_i the relations R_i are defined on A. This leads to a structure on the elements of A.

General properties of an algebraic system

Let A be a nonempty set and $+$ and $\cdot$ (not necessarily the usual addition and multiplication) be any two closed binary operations on A. Then for any elements a, b, c of A, we have

	Property	
I)	Associative property for $+$	: $(a+b)+c = a+(b+c)$
II	Commutative property for $+$	: $a+b = b+a$
III	Identity element 0 for $+$	: $a+0 = 0+a = a$ for any $a \in A$.
IV	Inverse element under $+$ ~~exist~~	: For each $a \in A$, there exist $b \in A$ (called negative of a) s.t. $a+b = b+a = 0$
V	Associative property for $\cdot$	: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
VI	Commutative property for $\cdot$	: $a \cdot b = b \cdot a$
VII	Identity element 1 for $\cdot$	: $a \cdot 1 = 1 \cdot a = a$
VIII	Distributive law of $\cdot$ over $+$	: a) $a \cdot (b+c) = a \cdot b + a \cdot c$ b) $(b+c) \cdot a = b \cdot a + c \cdot a$
IX	Cancellation property	: $a \cdot b = a \cdot c \Rightarrow b = c$ provided $a \neq 0$
X	Idempotent Property	: $a+a = a$ $a \cdot a = a$

Eg: The algebraic system $(z, +, \cdot)$ with usual addition & multiplication satisfies all properties from I to IX

Eg 2: Let $M_2(Z)$ denote the set of all 2×2 matrices with integer entries. Here $+$ and $\cdot$ denote the usual matrix addition and multiplication. Then $(M_2(Z), +, \cdot)$ is an algebraic system which is closed under $+$ and $\cdot$ and satisfies associativity (1) and commutativity (2) for $+$

Additive identity (3) 0 is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ for any $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Additive (4) inverse is $-A$

Matrix multiplication is associative but not commutative ($AB \neq BA$).

multiplicative identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $(IA = AI = A)$

Cancellation property is not valid $AB = AC$ $A \neq 0$ $\not\Rightarrow B = C$.

eg: $\begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 3 & 4 \end{bmatrix}$

$\cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \neq \begin{bmatrix} 5 & 7 \\ 3 & 4 \end{bmatrix}$

Eg 3) Let $P(S)$ be the powerset of S Then algebraic system $\{P(S)\ \cup\ \cap\}$ satisfies all properties <u>except</u> 1) inverse element

2) cancellation property

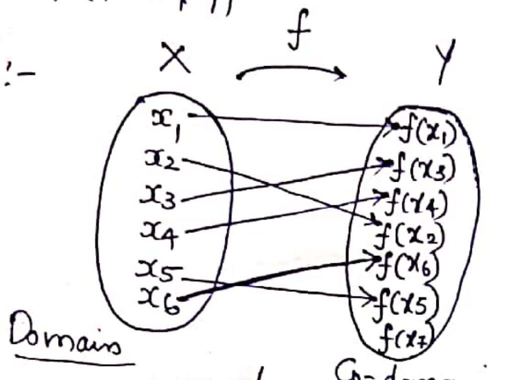
$f: X \to Y$ $\quad (X, \cdot), (Y, *)$

I

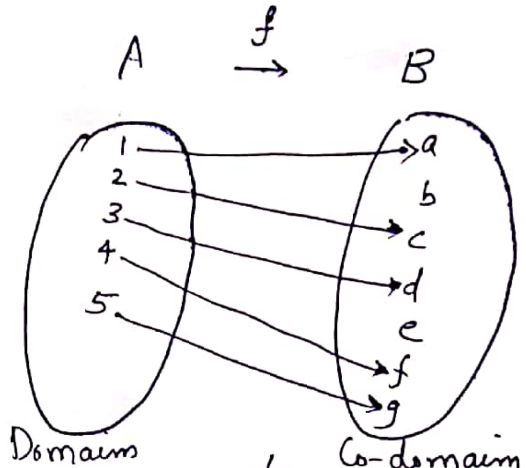
f is **one-to one** if each element of Y appears at most once as the image of an element of X.

ie $|X| \le |Y|$

Eg:-



one to one

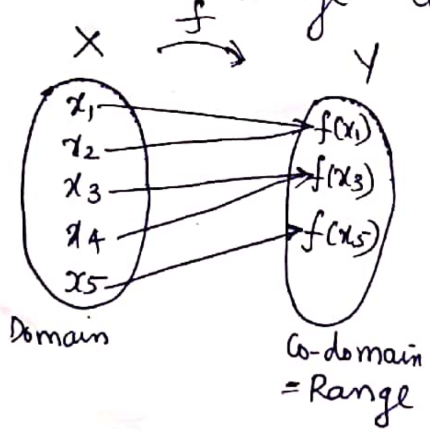


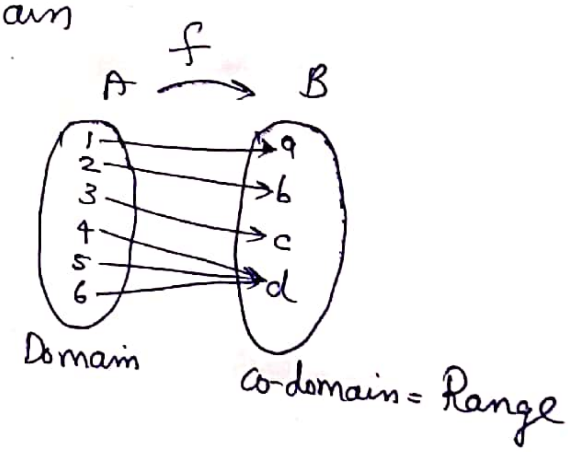
one to one

II

onto $f: X \to Y$ is called onto if $f(X) = Y$

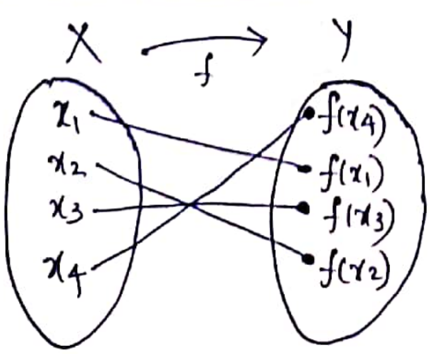
Range = Co-domain



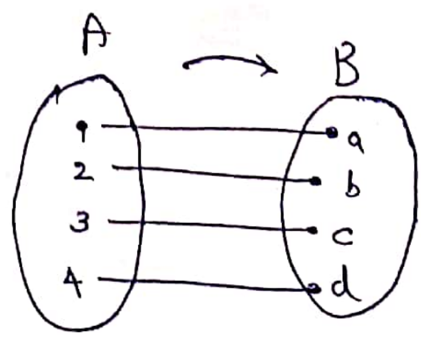


III

one-one onto



one-one onto



one one onto

Homomorphism and Isomorphism

Let $(X, \circ)$ and $(Y, *)$ be two algebraic system where $\circ, *$ are both n-ary operations. A function $f: X \to Y$ is known as a homomorphism from $(X, \circ)$ to $(Y, *)$ if for any $x_1, x_2 \in X$ we have

$$\boxed{f(x_1 \circ x_2) = f(x_1) * f(x_2).}$$

Note

If $f: X \rightarrow Y$ is onto, f is known as epimorphism.

If $f: X \rightarrow Y$ is oneto one, f is known as monomorphism.

If $f: X \rightarrow Y$ is one to one-onto, f is known as isomorphism.

* If $(X, \cdot)$ is $(Y, *)$ are two algebraic systems, ~~structures~~ such that an isomorphism exists b/w them, then, $(X, \cdot)$ and $(Y, *)$ are said to be isomorphic and then two algebraic systems are structurally indistinguishable.

Scanned with CamScanner

II

SEMIGROUPS & MONOIDS

Semigroups

An Algebraic system $(S, \cdot)$ is know as a semigroup where (i) S is non empty & (2 properties)
(ii) $\cdot$ is an associative binary operation.

Monoid

A monoid $(M, \cdot)$ is (i) a semigroup (3 properties)
(ii) with an identity (e)

e is unique for $(M, \cdot)$ denoted by $(M, \cdot, e)$

Commututative (abelian) Semigroups & Monoids

In a semigroup $(S, \cdot)$, if $\cdot$ is commutative, then $(S, \cdot)$ is called abelian semigroup. (4 properties)

In a monoid $(M, \cdot)$, if $\cdot$ is commutative, then $(M, \cdot)$ is called abelian Monoid. (4 properties.

Eg:- 1) Consider $(Z^+, +)$. Check whether $(Z^+, +)$ is a commutative semigroup or commutative monoid

Ans:- $Z^+ = \{1, 2, 3, \dots\}$

① Z^+ is non empty & closed under +,

② + is an associative binary operation.

③ + is commutative

④ Additive identity doenot exist.

additive identity $e = 0 \notin Z^+$

$\therefore$ It is a commutative semigroup but not a commutative monoid

2) $(N, +)$

Ans:- $N = \{0, 1, 2, 3, \dots\}$

All the above 4 properties are satisfied

Additive inverse $e = 0 \in N$

$\therefore$ It is a commutative semigroup and commutative monoid

3) $(N, -)$ $N = \{0, 1, 2, 3 \dots\}$

Ans:- Let $2, 3, 4, \in N$

Associative, $2-(3-4) = 2-(-1) = 2+1 = 3$

$(2-3)-4 = -1-4 = -5$

$\therefore 3 \neq -5$, (Not associative)

Hence $(N, -)$ is not a semigroup.

Scanned with CamScanner

4) $(P(S), \cup)$

Ans:- (i) $\cup$ is closed, $P(S)$ is non empty

(ii) $\cup$ is associative

(iii) ϕ is the identity under $\cup$

(iv) $\cup$ is commutative

$\therefore$ $(P(S), \cup)$ is a commutive Monoid

(abelian monoid)

5) $(P(S), \cap)$ (i) Closed

(ii) $\cap$ is assowative

(iii) S is the identity under $\cap$

(iv) $\cap$ is commutative

$\therefore$ $(P(S), \cap)$ is a commutative monoid

Scanned with CamScanner

Cyclic Monoid

A cyclic monoid is a monoid $(M, *, e)$ in which every element of M can be expressed as some powers of a particular element $a \in M$. This element a is said to be the generator of the cyclic monoid, because for any $x \in M$, we have $x = a^n$. for some $n \in N$.

Note: cyclic monoid is an abelian monoid

For any $x, y \in M$ $\quad x = a^m \quad y = a^n$, $m, n \in N$

$$\therefore x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$$

Group (G, o)

A group G is a non empty set together with an operation o if it satisfies the following conditions

- Closure

$\forall a, b \in G \Rightarrow a \circ b \in G$

- Associative

$(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in G$

- Existence of identity

$\exists$ an element $e \in G$ called identity such that

$a \circ e = e \circ a = a \quad \forall a \in G$

- Existence of inverse

$a \in G, \exists a^{-1} \in G$ such that

$a \circ a^{-1} = a^{-1} \circ a = e$. where a^{-1} is called inverse of 'a'

Abelian group

A group (G, o) is called abelian group or commutative group if $a \circ b = b \circ a \quad \forall a, b \in G$.

Examples

1) Integers Z under the operation $+$

$Z = \{ \ldots -3, -2, -1, 0, 1, 2, \ldots \}$.

Let x, y be integers with operation $+$

- Closure : x, y integer $\Rightarrow x+y$ is also integer
- Associative : $\forall x, y, z \in Z$

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

- Identity : $\forall x \in Z$ there exist identity 0 such that $x+0 = 0+x = x$.
- Inverse : $\forall x \in Z$ there exist inverse $-x$ such that $x+-x = e = 0$

$\therefore$ inverse ~~of~~ $+x$ is $-x$.

This group is also abelian group because $a+b = b+a$. $\forall a, b \in G$.

2) $\therefore (Z,+)$ $(R,+)$ $(Q,+)$ all are commutative group

3) The set of all $m \times n$ matrix with matrix operation addition (Matrix addition) is group. Also it is commutative group with zero matrix as identity element and inverse of matrix as $-A$.

Cyclic Monoid - examples

1) Let S be the set of two digit decimal numbers $\{00, 01, 02, \dots 99\}$. (usually we write 00 as 0, 02 as 2 and 09 as 9).
Define $*$ on S s.t. $x*y$ is the remainder when xy is divided by 100, $\forall x, y \in S$.
ⓐ Show that $(S, *)$ is an abelian monoid
ⓑ What is its identity.
ⓒ Determine cyclic monoid generated by 07.

Ans:- ⓐ To show that $(S, *)$ is an abelian monoid

(i) $S = \{00, 01, 02, \dots 99\}$ is closed under $*$.
because when a number is divided by 100, the possible remainders ~~are~~ be 00, 01, 02, ... 99.

(ii) $*$ is associative (because multiplication is associative)
for example

$$(08*13)*84 = \text{remainder}\left(\frac{8\times13}{100}\right)*84 = \text{rem}\left(\frac{104}{100}\right)*84 = 04*84 = \text{rem}\left(\frac{4\times84}{100}\right) = \text{rem}\,\frac{336}{100} = 36$$

$$08*(13*84) = 08*\text{rem}\left(\frac{13\times84}{100}\right) = 08*\left(\frac{1092}{100}\right) = 08*92 = \text{rem}\left(\frac{8\times92}{100}\right) = \text{rem}\,\frac{736}{100} = 36$$

$$\therefore (08*13)*84 = 08*(13*84)$$

(It is true for any 3 elements in S.

(iii) identity element under $*$ is 01.

(iv) $*$ is commutative because multiplication is commutative

$\therefore$ $(S, *)$ is an abelian monoid

(b) 01 is the identity.

(c) <u>Cyclic monoid generated by 07</u>

$$(07)^2 = 07 * 07 = 49$$

$$(07)^3 = (07)^2 * 07 = 49 * 07 = \text{rem}\left(\frac{49 \times 7}{100}\right) = \frac{343}{100} = 43$$

$$(07)^4 = (07)^3 * 07 = 43 * 07 = \text{rem}\left(\frac{43 \times 7}{100}\right) = \frac{301}{100} = 01$$

$$(07)^5 = (07)^4 * 07 = 01 * 07 = 07$$

$$(07)^6 = (07)^5 * 07 = 07 * 07 = 49 \text{ (repeated)}$$

$$(07)^7 = (07)^6 * 07 = 43$$

Continuing like this we have

$$\langle 07 \rangle = \{01, 07, 49, 43\}.$$

This is the cyclic monoid generated by the generator 07.

$\underline{\underline{\langle 07 \rangle = \{01, 07, 49, 43\}}}$ is a finite cyclic monoid (4 elements)

2) $(N,+,0)$. Is it a cyclic monoid?
What is its generator.

Ans:- $N=\{0,1,2,3,\cdots\}$
$+$ is the binary operation addition.

$(N,+)$ is clearly a monoid (why?
① N is closed under $+$
② $+$ is associative
③ $0 \in N$ is the identity.)

Every element in N can be generated by 1. ie 1 is the generator of N.

$1^2 = 1+1 = 2$ (Here 1^2 means add 1 two times)
$1^3 = 1+1+1 = 3$ ($1^3 \Rightarrow$ add 1 3 times.
$1^4 = 1+1+1+1 = 4$
$\vdots$
$1^n = \underbrace{1+1+\cdots+1}_{n \text{ times}} = n$
$\vdots$

$\therefore$ 1 is the generator of N

$(N,+,0)$ is an infinite cyclic monoid.

3) Is $(N,*)$ a commutative monoid where $x*y=\max\{x,y\}$

Ans:- ① $N=\{0,1,2,3,\cdots\}$ is closed under $*$
② $*$ is associative, because for $x>y>z$

$x*(y*z) = x*\max\{y,z\} = x*y = \max\{x,y\} = x$
$(x*y)*z = \max\{x,y\}*z = x*z = \max\{x,z\} = x$
$\therefore x*(y*z) = (x*y)*z \quad \forall x,y,z \in N$

③ 0 is the identity because $x*0 = x$ $\forall x \in N$
$\max\{x,0\} = x$

④ $x*y = \max(x,y) = \max(y,x) = y*x$
$\therefore (N,*)$ is a commutative monoid

SUBSEMIGROUPS AND SUBMONOIDS

Subsemigroup

2 properties

Let $(S,*)$ be a semigroup and $T \subseteq S$.
Then $(T,*)$ is said to be a subsemigroup of $(S,*)$
if T is closed under the operation $*$.

Submonoid

③ properties

Let $(M,*,e)$ be a monoid and $T \subseteq M$.
Then $(T,*,e)$ is said to be a submonoid of $(M,*,e)$
if T is closed under $*$ and identity $e \in T$

Eg: ① Let $(N,+)$ be a semigroup. $N=\{0,1,2,3,\ldots\}$
$(Z^+,+)$ is a subsemigroup $Z^+=\{1,2,3,\ldots\}$

Reason ① $Z^+ \subseteq N$
② Z^+ is closed under $+$

Eg: ② Let $(N,+)$ be a semigroup. Check whether $(T,+)$ where $T=\{1,3,5,7,\ldots\}$ set of odd integers. is a subsemigroup.

Ans:- $(T,+)$ is not a subsemigroup
Reason: T is not closed under $+$
ie $3+5=8 \notin T$ (8 even integer)
(sum of 2 odd integer = even)

Eg. ③ Let $(R, \cdot, 1)$ be a monoid. Is $(N, \cdot, 1)$ a submonoid?

Ans- Yes. Reason ① N is closed under $\cdot$

② $N \subseteq R$

③ $e = 1 \in N$

$N = \{0, 1, 2, 3 \cdots\}$

$R = \{$set of real nos$\}$

④ Let $(Z, +)$ be a monoid. Is $(\{3\}^+, +)$ a submonoid

Note: $\{3\}^+ =$ All sums of 3 (multiples of 3)

$= \{3n / n \in Z^+\} = \{3, 6, 9, 12, \cdots\}$

Ans- No. Reason Identity element for $(Z, +) = 0$

but $0 \notin \{3\}^+$

$Z = \{\ldots -2, -1, 0, 1, 2, \cdots\}$

$\{3\}^+ = \{3, 6, 9, 12, \cdots\}$

$\therefore \{\{3\}^+, +\}$ is not a submonoid.

But it is a subsemigroup of semigroup $(Z, +)$

~~Result~~ Theorem

Q) Prove that the set of idempotent elements of M for any abelian monoid $(M, *, e)$ forms a submonoid

proof:-

Let A be the set of idempotent elements of M

We have to show that A is closed under $*$.

We have $a * a = a$, $b * b = b$ $\forall\, a, b \in A$

Prove, 3 properties ① A closed

② $A \subseteq M$

③ $e \in A$

consider $(a*b)*(a*b) = (a*b)*(b*a)$ $\because$ M is abelian

$= a*(b*b)*a$ $\because$ $*$ is associative

$= a*b*a$ $\because$ b is idempotent

$= a*a*b$ $\because$ M is abelian

$= a*b$ $\because$ a is idempotent

$\therefore$ $a*b \in A$

Thus A is closed w.r.t $*$ and $A \subseteq M$.

We know that $e*e=e$ $\therefore$ $e \in A$

Thus $(A, *, e)$ is a submonoid of $(M, *, e)$

HOMOMORPHISM AND ISOMORPHISM OF SEMIGROUP & MONOIDS

Let $(S,*)$ and (T, Δ) be any two semigroups. A function $f: S \to T$ is called semigroup homomorphism if for any two elements $a,b \in S$ we have $\boxed{f(a*b) = f(a) \Delta f(b)}$

* If f is one to one then semi group homomorphism is known as semigroup monomorphism.
* If f is is onto then semigroup homomorphism is called semigroup epimorphism.
* If f is one-one onto then semigroup homomorphism is called semigroup isomorphism.

Note:- If there is a semigroup isomorphism from S onto T, then $(S,*)$ & (T, Δ) are said to be isomorphic.

Q. P.T under semigroup homomorphism, the properties (i) associativity, (ii) idempotency and commutativity are preserved.

Ans:- (i) We have to prove that Δ is associative.

Let $(S, *)$ & (T, Δ) be two semigroups

s $f(a*b) = f(a) \Delta f(b)$ $\forall a, b \in S$.

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

$$f[(a*b)*c] = f(a*b) \Delta f(c)$$
$$= (f(a) \Delta f(b)) \Delta f(c) \quad \text{——} ①$$

$$f[(a)*(b*c)] = f(a) \Delta f(b*c)$$
$$= f(a) \Delta (f(b) \Delta f(c)) \quad \text{——} ②$$

We know that $*$ is associative

ie $f[(a*b)*c] = f[(a)*(b*c)]$

$\therefore$ from ① & ② $(f(a) \Delta f(b)) \Delta f(c) = f(a) \Delta (f(b) \Delta f(c))$

$\therefore$ Δ is associative

(ii) Idempotency

Let $a \in S$ is idempotent ie $a*a = a$

$$f(a*a) = f(a)$$
$$f(a) \Delta f(a) = f(a)$$

$\therefore$ $f(a)$ is idempotent in T.

(iii) Δ is commutative.

for any $a, b \in S$ $\quad a * b = b * a$ (∵ $*$ is abelian)

$$f(a*b) = f(b*a)$$
$$f(a) \Delta f(b) = f(b) \Delta f(a)$$

∴ Δ is commutative (abelian)

MONOID HOMOMORPHISM

Let $(M, *, e_M)$ & (T, Δ, e_T) be any two monoids. A function $f: M \rightarrow T$ is known as monoid homomorphism if for any $a, b \in M$ we have

$$\boxed{\begin{aligned} &f(a*b) = f(a) \Delta f(b) \text{ and} \\ &f(e_M) = e_T \end{aligned}}$$

(identity element in Monoid M) is mapped onto (identity element in Monoid T)

Note:-

The monoid homomorphism preserves

1. Associativity
2. Commutativity
3. Identity
4. Inverse $\longrightarrow$ because $e_T = f(e_M)$

$$= f(a * a^{-1})$$
$$= f(a) \Delta f(a^{-1})$$

∴ $f(a^{-1})$ is the inverse of $f(a)$

Q) Check whether $f: Z^+ \to Z^+$ defined by $f(m) = 2^m$ for any $m \in Z^+$, a semigroup homomorphism where $(Z^+, +)$ and $(Z^+, \cdot)$ are two semigroups.

Ans:- we have to prove that $f(m+n) = f(m) \cdot f(n)$

$$f(m+n) = 2^{m+n}$$
$$= 2^m \cdot 2^n$$
$$= f(m) \cdot f(n)$$

$\therefore$ It is a semigroup homomorphism.

Q) Let $(N, +, 0)$ & $(N, \cdot, 1)$ be two monoids. Check whether $f: N \to N$ defined by $f(m) = 3^m$ $\forall m \in N$ a monoid homomorphism.

Ans:- We have to P.T $f(m+n) = f(m) \cdot f(n)$ & $f(0) = 1$ (identity 0 is mapped onto identity 1)

$f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n)$

$f(0) = 3^0 = 1$ $\therefore$ Monoid homomorphism.

Q) S.T $f: R^+ \to R$ by $f(x) = \ln x$ is ~~an~~ a monoid isomorphism, for $(R^+, \cdot, 1)$ & $(R, +, 0)$

Ans:- We have to prove that

① $f(x \cdot y) = f(x) + f(y) \quad \forall\, x, y \in R^+$

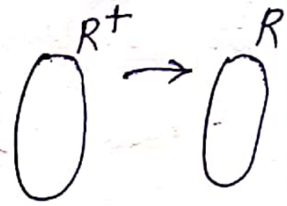
② $f:$ is onto

③ $f:$ is one-one

④ identity element 1 is mapped to identity element 0.

① $f(x \cdot y) = \ln(x \cdot y) = \ln x + \ln y$
$= f(x) + f(y) \quad \forall\, x, y \in R^+$

$\therefore f$ is a homomorphism.



② We have to prove that every element in R has at least one preimage in R^+

$\forall\, x \in R, \ \exists\, e^x$ in R^+, s.t. $\ln(e^x) = x \therefore f$ is onto

③ $f(x) = f(y)$

$\ln x = \ln y$

$e^{\ln x} = e^{\ln y}$

$x = y$, $\quad f(x) = f(y) \Rightarrow x = y \quad \therefore f$ is one to one

④ $f(1) = \ln 1 = 0$

$\therefore 1$ is mapped onto 0

$\therefore (R^+, \cdot, 1)$ & $(R, +, 0)$ are isomorphic monoids.

1 Show that $(N,*)$ is a semigroup where $x*y = \min(x,y)$. for any $x,y \in N$. Is $(N,*)$ a monoid.

Ans: For any $x<y<z$, $*$ is cloed binary operation

Also the $*$ is associative.

ie $x*(y*z) = x*\min(y,z) = x*y = \min(x,y) = \underline{\underline{x}}$

$(x*y)*z = \min(x,y)*z = x*z = \min(x,z) = x$

$\therefore (N,*)$ is semigroup.

Identity for $(N,*)$ does n't exist, ~~thae~~ that implies $(N,*)$ is not a monoid.

2 Is $(Z^+,\cdot)$ a semigroup, monoid, abelian ?.
Give an example of a sub semigroup that is not a submonoid.

Ans: $(Z^+,\cdot)$ is semigroup, monoid, abelian since

- is associative in Z^+ ie $a*(b*c) = (a*b)*c$

1 is the edentity

- is abelian. ie $a*b = b*a$

Consider $E = \{2,4,6,8,\ldots\}$. Then $(E,\cdot)$ is subsemigroup. But not a submonoid since $1 \notin E$ ie identity is not ~~exist~~ exist in E.

3 What are the submonoids of the commutative monoid $(z, +, 0)$

Any subset of z with identity 0 is a submonoid

eg: $(2z, +, 0)$ is a submonoid of $(z, +, 0)$

$2z = \{\ldots -4, -2, 0, 2, 4, \ldots\}$.

In general $(nz, +, 0)$ is a submonoid. of $(z, +, 0)$

4 State two monoids for $P(S)$. The powerset of S.

$(P(S), \cap, S)$ is a monoid since $\cap$ is associative & S is the identity

$(P(S), \cup, \varphi)$ is another monoid since $\cup$ is associative and φ is the identity.

5 Is $(A, *)$ a monoid abelian where $A = \{1, 2, 3, 6, 12\}$ and $a*b = \gcd\{a, b\}$

$(A, *)$ is monoid and

$a*b = \gcd(a, b) = \gcd(b, a) = b*a$

$\therefore (A, *)$ is abelian.

Here identity element is $\underline{\underline{12}}$.

$[\,1 * 12 = \gcd(1, 12) = \underline{\underline{12}} = 12 * 1 = \gcd(12, 1).\,]$

6 Is $\cdot$ associative given

$\cdot$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

It is not associative since

$c \cdot (b \cdot b) = c \cdot a = c \quad \rightarrow (1)$

$(c \cdot b) \cdot b = b \cdot b = a \quad \rightarrow (2)$

From (1) & (2) $\cdot$ is not associative

7 Find a cyclic subsemigroup of $(M_2(Z), \cdot)$ generated by the element $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$M^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad M^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \dots \quad M^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

cyclic subsemigroup is $\left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \; n \in Z^+ \right\}$.

8 Let $P(S)$ be the powerset of a nonempty set S. Find a isomorphism from semigroup $(P(S), \cup)$ onto semigroup $(P(S), \cap)$.

Let $f(A) = A^c \quad \therefore \forall A \in P(S)$ f is 1-1, onto.

and homomorphism since

$f(A \cup B) = (A \cup B)^c = A^c \cap B^c = f(A) \cap f(B)$

$\therefore f$ is an isomorphism.

9 Which of the following functions f are homomorphism from $(Z^+, +)$ to $(Z^+, \cdot)$.

1) $f(n) = 2^n$ 2) $f(n) = n$ 3) $f(n) = 2n$

4) $f(n) = (-1)^n$ 5) $f(n) = 3^{n+1}$

1) $f(n+m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m)$

$\therefore$ Homomorphism

2 NO

3 NO

4 No

5 No

None of them are isomorphism

In 1 the function is not onto.

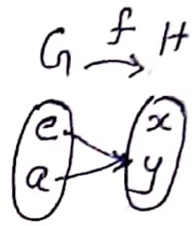
10) Let $(G, \cdot)$ and $(H, *)$ are two monoids, find a monoid, or semigroup homomorphism given that

G

$\cdot$	e	a
e	e	a
a	a	a

H

$*$	x	y
x	x	y
y	y	y



Ans:- Define $f: G \to H$ by $f(e) = y$, $f(a) = y$

we can prove that

$$f(e \cdot a) = f(e) * f(a)$$

LHS $= f(e \cdot a) = f(a)$	RHS $= y * y$
$f(a)$	$= y.$
y	$= y$

$\therefore f(e \cdot a) = f(e) * f(a)$

It is a semigroup homomorphism but not a monoid homomorphism.

(because identity element in G is not mapped onto identity element in H.

$f(e) \neq x.$

~~# Next~~

11. Verify that $f: G \to H$ is a monoid homomorphism where $(G, \cdot)$ and $(H, *)$ are monoids defined as follows. Also $f(e) = E$, $f(b) = A$ & $f(a) = A$

G

$\cdot$	e	a	b
e	e	a	b
a	a	a	a
b	b	b	b

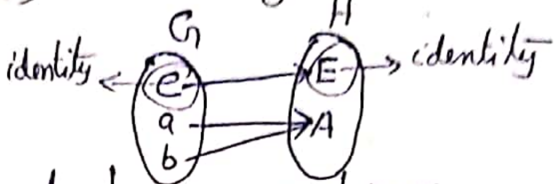
H

$*$	E	A
E		
A		

Ans:- $f(a\cdot b) = f(a) = A$, $f(a) * f(b) = A * A$
$= A$

ie $f(a\cdot b) = f(a) * f(b)$ ∴ subgroup homomorphism

Also $f(e) = E$



∴ f is a ~~subgroup~~ monoid homomorphism.

12 P.T the semigroup $(S,*)$ and (T,Δ) are isomorphic given that $f(a)=y$, $f(b)=x$, $f(c)=z$

S

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

T

Δ	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

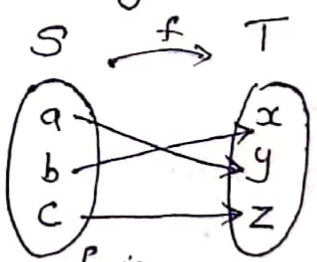
Ans:- prove that $f: S \to T$ is homomorpsim which is one-one & onto

$f(a*b) = f(b) = x$ $f(a)\Delta f(b) = y \Delta x = x$

$f(a*b) = f(a)\Delta f(b)$ $\forall a,b \in S$

$\left.\begin{array}{l} f(a*c) = f(a)\Delta f(c) \\ f(b*c) = f(b)\Delta f(c) \end{array}\right\}$ prove

∴ f is a homomorphism



clearly f is one to one & onto

∴ $f: S \to T$ is isomorphism.

Group (G, o)

A group G is a non empty set together with an operation o if it satisfies the following conditions

- Closure

$\forall a, b \in G \Rightarrow a o b \in G$

- Associative

$(a o b) o c = a o (b o c) \quad \forall a, b, c \in G$

- Existence of identity

$\exists$ an element $e \in G$ called identity such that

$a o e = e o a = a \quad \forall a \in G$

- Existence of inverse

$a \in G, \exists a^{-1} \in G$ such that

$a o a^{-1} = a^{-1} o a = e$. where a^{-1} is called inverse of 'a'

Abelian group

A group (G, o) is called abelian group or commutative group if $a o b = b o a \quad \forall a, b \in G$.

Examples

1) Integers Z under the operation +

$Z = \{ \ldots -3, -2, -1, 0, 1, 2, \ldots \}$.

Let x, y be integers with operation +

- Closure: x, y integer $\Rightarrow x+y$ is also integer
- Associative: $\forall x, y, z \in Z$

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

- Identity: $\forall x \in Z$ there exist identity 0 such that $x+0 = 0+x = x$.
- Inverse: $\forall x \in Z$ there exist inverse $-x$ such that $x+-x = e = 0$

$\therefore$ inverse of $+x$ is $-x$.

This group is also abelian group because $a+b = b+a$. $\forall a, b \in G$.

2) $\therefore (Z, +)$ $(R, +)$ $(Q, +)$ all are commutative group

3) The set of all $m \times n$ matrix with matrix operation addition (Matrix addition) is group. Also it is commutative group with zero matrix as identity element and inverse of matrix as $-A$.

Subgroup

Let G be a group and $\phi \neq H \subseteq G$. If H is a group under the binary operation of G, the we call H as a subgroup of G.

1) For eg:

Let $G = (Z_6, +)$, if $H = \{0, 2, 4\}$. Then H is non empty subset of G. Also $(H, +)$ is a group under the binary operation of G "addition modulo n"

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

2/ The group $(Z, +)$ is a subgroup of $(Q, +)$ which is a subgroup of $(R, +)$

Theorem:

1/ If H is a nonempty subset of a group G then H is a subgroup of G iff

1) for all $a, b \in H$ $ab \in H$

2) for all $a \in H$, $a^{-1} \in H$

2 Every group G has $\{e\}$ and G as subgroups. These are trivial subgroups of G. All others are termed as non trivial or proper.

1) Show that any group G is abelian iff $(ab)^2 = a^2b^2$ $\forall\, a,b \in G$

Pf

Suppose G is abelian group

$$(ab)^2 = (ab)(ab) = a(ba)b = a.(ab).b \quad (\text{abelian})$$
$$= (a\,a)(b\,b)$$
$$= a^2 \cdot b^2$$

Suppose

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

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

$$a(ba)b = a.\,ab^2 \quad \text{cancellation}$$

$$(ba)b = (a.b.)b \quad \text{Cancellation}$$

$$\underline{\underline{ba = ab}}$$

Symmetric group

The symmetric group S_n is the group of permutation on n-objects. usually the objects are labeled as $\{1, 2, 3, \dots n\}$. and elements of S_n are given by bijective functions

$\sigma : \{1, 2, \dots n\} \to \{1, 2, 3, \dots n\}$.

The group operation on S_n is composition of function

In the notation S_n - S denotes symmetric and n denotes size of the ~~group~~ set being permuted here. There are $n!$ ways to permute a set with 'n' elements $\therefore$ S_n is finite with $n!$ elements. ie $|S_n| = n!$

1 For eg: S_3 = Group of permutation on a set with 3 elements.

= permutations of $\{1, 2, 3\}$.

$\{1, 2, 3\}, \{1, 3, 2\}, \{2, 3, 1\}$,
$\{2, 1, 3\}, \{3, 1, 2\}, \{3, 2, 1\}$

Suppose $f : \{1\ 2\ 3\} \to \{1, 2, 3\}$. & $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$

$\Rightarrow f(1) = 2 \quad f(2) = 3 \quad f(3) = 1$

2) Multiplication in permutation is simply composition

Consider $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$f \quad \circ \quad g$

$f(1) = 2$
$f(2) = 3$
$f(3) = 1$

$g(1) = 3$
$g(2) = 1$
$g(3) = 2$

$f \circ g(1) = f(3) = 1$
$f \circ g(2) = f(1) = 2$
$f \circ g(3) = f(2) = 3$

3 Find $\overset{f}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}}_{\text{II}} \circ \overset{g}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}}_{\text{I}}$

g $1 \to 4$ f $4 \to 2$ $\Rightarrow 1 \to 2$ $f \circ g$.

g	f	$f \circ g$
$1 \to 4$	$4 \to 2$	$1 \to 2$
$2 \to 3$	$3 \to 4$	$2 \to 4$
$3 \to 2$	$2 \to 3$	$3 \to 3$
$4 \to 1$	$1 \to 1$	$4 \to 1$

$$\therefore f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Consider

$$\underset{g}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}} \circ \underset{f}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}}$$

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

$\therefore f \circ g \neq g \circ f$ $\therefore$ Non abelian

Theorem

Every finite group is a subgroup of a symmetric group

Direct product of Group

Consider the groups $(G, \circ)$ and $(H, *)$

Define the binary operation $\circ$ on $G \times H$ by

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$. Then

$(G \times H, \cdot)$ is a group and is called the direct product of G & H.

ie $G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$

1 eg. Consider $(Z_2, +), (Z_3, +)$, on G $Z_2 \times Z_3$,

Define $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

Then G is a group of order 6 where the identity is $(0,0)$ and the inverse is $(1,1)$

ie inverse of $(1, 2)$ is $(1, 1)$.

2 Let $G_1 = Z$ under $+$

$G_2 = \{1, -1, i, -i\}$ under $\times$

$G_1 \times G_2 = \{(x, y) \mid x \in Z, y = \pm 1 \text{ or } \pm i\}$

$(7, -1) \cdot (\bar{3}, i) = (7-3, -1 \cdot i)$

$= (4, -i)$

$(5\ -i) \cdot (0, 1) = (5+0, -i \cdot 1)$

$= (5, -i)$

1) Group Multiplication Table

Consider the group $G, \{1, -1, i, -i\}, \times$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Group of order 1

$*$	e
e	e

Trivial group

Group of order 2

$*$	e	a
e	e	a
a	a	e

Note
Each row & column contains all elements
No duplicates in any row or columns

Group of order 3

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Or

Integers mod 3

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Homomorphism & Isomorphism

If $(G,\circ)$ and $(H,*)$ are groups and $f:G\to H$ then f is called a group homomorphism if for all $a,b\in G$ $f(a\circ b)=f(a)*f(b)$.

Properties

1 Let $(G,\circ)$ and $(H,*)$ be groups with respective identities e_G, e_H. If $f: G\to H$ is a homomorphism then

a) $f(e_G)=e_H$

b) $f(a^{-1})=[f(a)]^{-1}$ $\forall a\in H$

c) $f(a^n)=[f(a)]^n$ $\forall a\in G$ & $\forall n\in Z$

d) $f(S)$ is a subgroup of H for each subgroups S of G

2 If $f:(G,\circ)\to(H,*)$ is a homomorphism, we call f an isomorphism if it is one to one and onto. In this case G, H are said to be isomorphic groups

Cyclic group.

A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$ $a = x^n$ for some $n \in \mathbb{Z}$

Note:

Let G be a cyclic group

If $|G|$ is infinite then G is isomorphic to $(\mathbb{Z}, +)$

If $|G| = n$ where $n > 1$ then G is isomorphic to $(\mathbb{Z}_n, +)$

Left Coset & Right Coset.

If H is a subgroup of G then for each $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called left coset of H in G.

The set $Ha = \{ha \mid h \in H\}$ is a right coset of H in G.

Note
If the operation in G is addition then we write $a+H$ in place of aH. where
$a+H = \{a+h \mid h \in H\}$.

Lagranges theorem

If G is a finite group of order n with H a subgroup of order m, then m divides n.

Pf

If $H = G$, the result follows

otherwise if $m<n$. & there exist an element $a \in G-H$ since $a \notin H$

$$\Rightarrow aH \neq H \quad \Rightarrow aH \cap H = \varphi$$

If $G = aH \cup H$ then $|G| = |aH| + |H| = 2|H|$

and the theorem follows.

If not there exist an element $b \in G-(H \cup aH)$ with $bH \cap H = \varphi = bH \cap aH$ and

$$|bH| = |H|$$

If $G = bH \cup aH \cup H \Rightarrow |G| = 3|H|$.

otherwise we are back to an element $c \in G$ with $c \notin bH \cup aH \cup H$.

The group G is finite so this process terminates and $G = a_1H \cup a_2H \cup \dots \cup a_kH$.

$$\therefore |G| = k|H|$$

$\therefore m$ divides n

Hence the proof

Example

Let G be a group with $|G| = 323$

$\therefore$ Divisors ~~are~~ of 323 are 1, 17, 19, 323.

Possible sub groups are of orders : 1, 17, 19, 329 where $|G| = 323$ $\therefore G, \{e\}$ standard subgroups.

$|\{e\}| = 1$

Anyother group has order 17 or 19.