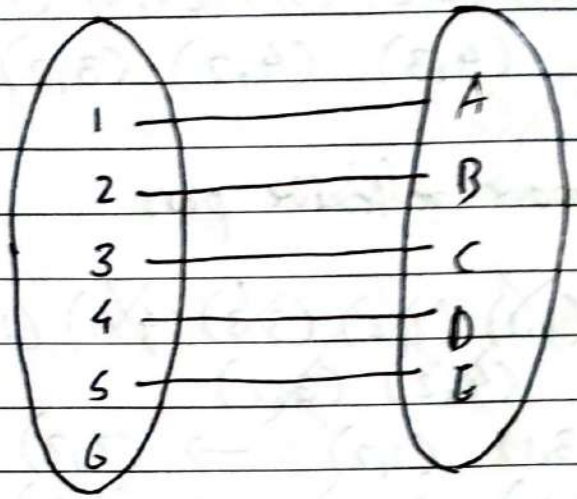
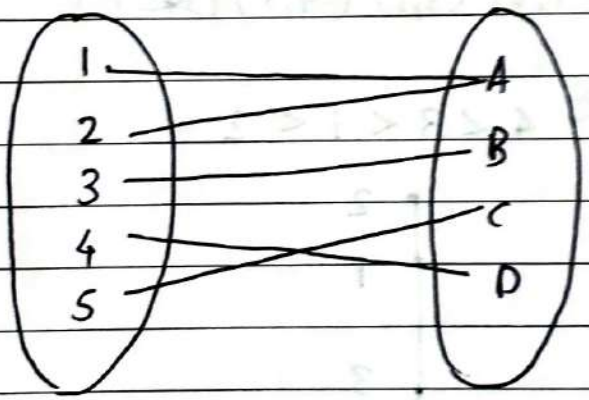
2. Groups.

Function

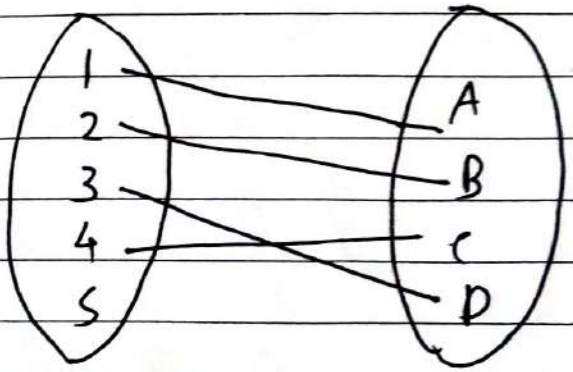
Vein Diagram.



This not function



It is function.



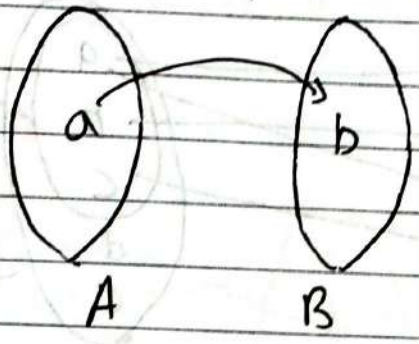
It is not function

If A & B be two non-empty set. A function f from A to B is an assignment or mapping exactly one element of B to each element of A.

$$f(a) = b$$

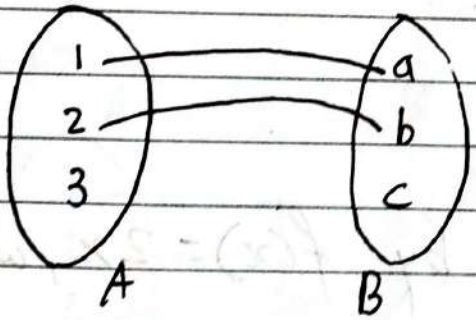
domain

$$f : A \to B \to \text{co-domain}$$



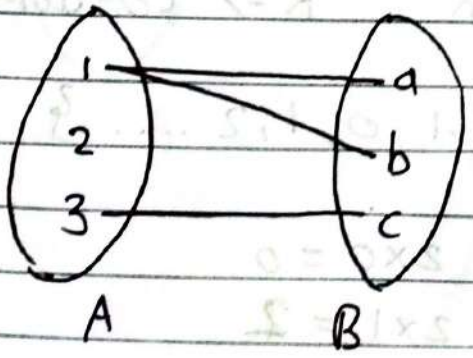
Examples which is not function.

i)

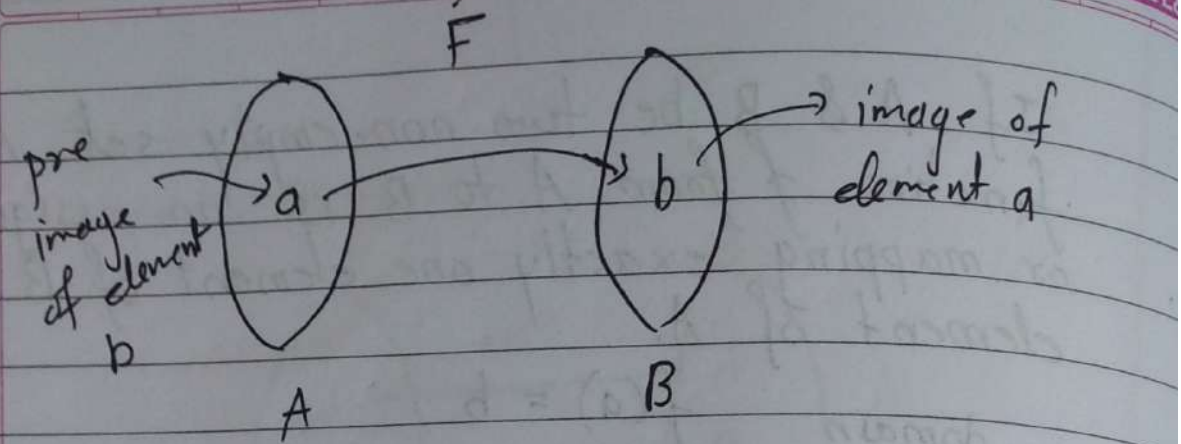


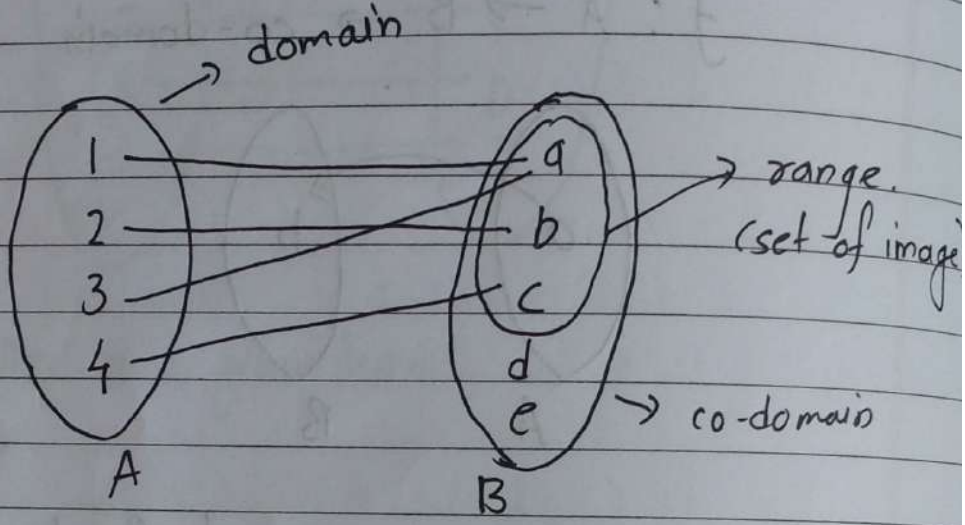
value not assign to 3

2)



1 has two different assignment





Range is always subset of co-domain.

Examples:

i) $f : Z \to R$

defined by $f(x) = 2x$, where $x \in Z$

$\Rightarrow$ $Z \Rightarrow$ Domain $\quad R \Rightarrow$ Co-domain.

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

$f(0) = 2 \times 0 = 0$

$f(1) = 2 \times 1 = 2$

Date / /
Page L&W

2)

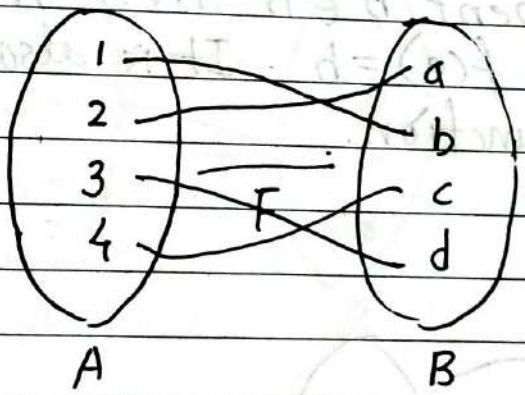
$f: Z \to R$

$f(x) = x^2 \quad x \in Z$

$\Rightarrow \quad Z = \{ \ldots -1, 0, 1 \ldots \}$

$R = \{ 0, 1, 4 \ldots \}$

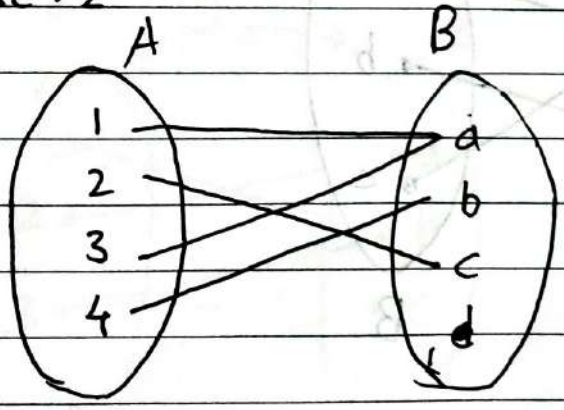
★ case: 1



every element of set A has distict images.

one-one function.

case: 2



every element of co-domain B at least one pre-image in A

onto function.

Date 28/09/24
Page

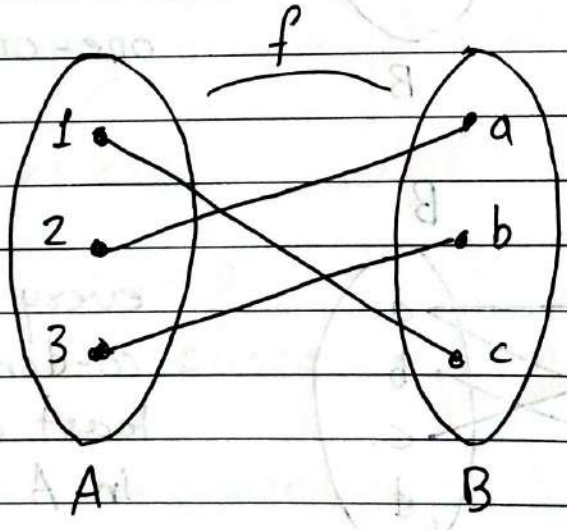
* One to one function

A function f is said to be one to one or one-one if and only if $f(a) = f(b) \Rightarrow a = b$ in the domain for all a, b in the domain of f. It is also called as injective function.

* On to function.

A function $(f : A \longrightarrow B)$ f from A to B) is called onto if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. It is also called surjective function.

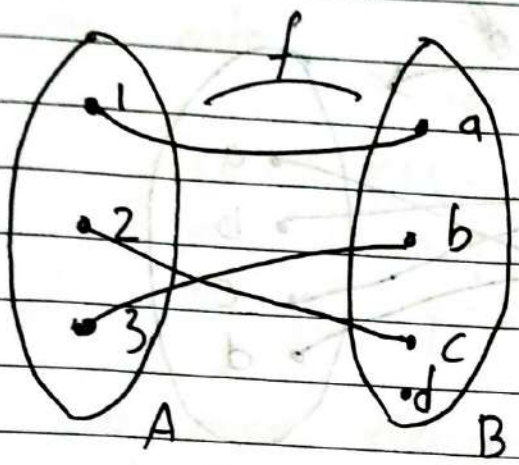
i)



f is one-one and onto function

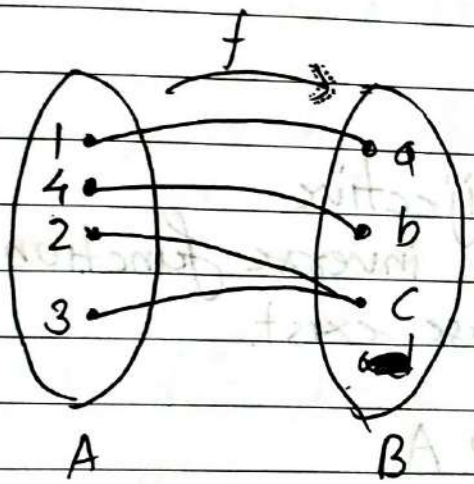
It is also called bijective function

ii)



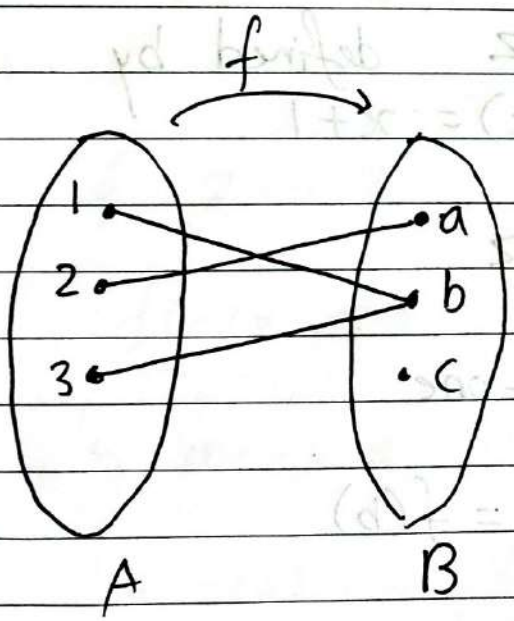
f is one-one but not onto.

iii)



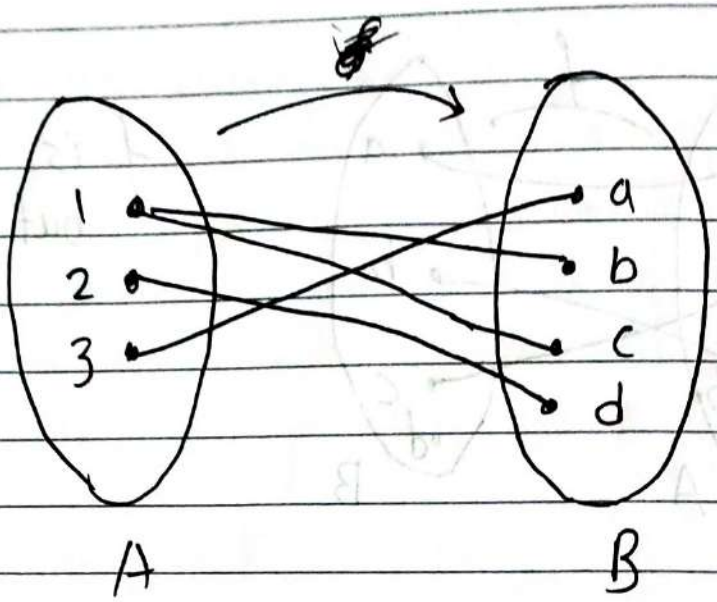
f is not one-one but f is onto function.

iv)



f is neither one-one nor onto.

iv)



Not function.

★ $f: A \to B$ is bijective
then it is inverse function.
↳ it's inverse exist.

$$f^{-1}: B \to A.$$

i) $f: Z \to Z$ defined by
$f(x) = x+1$

$\Rightarrow$ $f: Z \to Z$

★ for one-one

If $f(a) = f(b)$

$a = b$

f is one-one function

Date / /
Page L&W

* for onto

domain → $f(x) = \underbrace{x+1}_{\text{co-domain}} = y$ ← co-domain.

$\Rightarrow x+1 = y$

$\Rightarrow x = y-1$

for every element y in co-domain there is an element x in the domain

$\therefore f$ is onto function.

$\hookrightarrow$ f is bijective function.

$\hookrightarrow$ f^{-1} exists.

$\hookrightarrow$ $f^{-1} : z \to z$

$f^{-1}(x) = x-1$

ii) $f : z \to z$

$f(x) = x^2$

$\Rightarrow$

for one-one.

If $f(a) = f(b)$

$a^2 = b^2$

$\Rightarrow a = \pm b$

$a = b$ or $a = -b$

f is not one-one.

* for onto

$$f(x) = x^2 = y$$

$$\Rightarrow x^2 = y$$
$$\Rightarrow x = \pm\sqrt{y}$$

If $y = 2 \Rightarrow x = \pm\sqrt{2} \notin Z$

for every element of the co-domain there doesn't exist x in domain.

$\therefore f$: is not onto.

$\hookrightarrow f$ is not bijective

$\hookrightarrow f^{-1}$ is not exist.

iii) $f: N \longrightarrow Z$ defined by $f(x) = x^2$

$\rightarrow$ for one-one.

If $f(a) = f(b)$

$a^2 = b^2$

$\Rightarrow a = b$

Date 30/9/21
Page L&W

Domain is N. so only five no.

f: is one-one function.

iv) $F: R \to R$

$f(x) = 2x+1 \Rightarrow f^{-1}(x) = \frac{x-1}{2}$

F is one-one
F is onto
F is bijective
F^{-1} exists

$f(x) = 2x+1 = y$

$2x = y-1$

$x = \frac{y-1}{2}$

$f^{-1}: R \to R$

$f^{-1}(x) = \frac{x-1}{2}$

f is onto

* for one-one

$f(a) = f(b)$

$2a+1 = 2b+1$

$a = b$

F is one-one.

Mathematical Induction

i) Show that if n is a positive integer, then

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}$$

⇒ let $P(n) = 1 + 2 + \dots + n = \frac{n(n+1)}{2}$

Basic step:

For $n = 1$

L.H.S = 1

R.H.S = $\frac{1(1+1)}{2} = 1 = L.H.S$

$\therefore P(n)$ is true for $n = 1$

Inductive step:

Assume that $P(n)$ is true for $n = k$

i.e $1 + 2 + \dots + k = \frac{k(k+1)}{2}$ ....(2)

Then we have to show that $P(n)$ is true for $n = k+1$

i.e $1 + 2 + \dots + k + k+1 = \frac{(k+1)(k+2)}{2}$ ....(2)

L.H.S = $1 + 2 + \dots + k + 1$

$$= \frac{k(k+1)}{2} + (k+1)$$

$$= (k+1)\left[\frac{k}{2} + 1\right]$$

$$= \frac{(k+1)(k+2)}{2} = R.H.S$$

$\therefore$ $P(n)$ is true for $n = k+1$

$\therefore$ By using the principal of mathematical induction.

$\therefore$ $P(n)$ is true for all +ive integers n

i.e $1 + 2 + \dots + n = \frac{n(n+1)}{2}$

2) Use mathematical induction to show that

$$1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$$

for all non-negative integer n.

$\Rightarrow$ let $P(n) = 1 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$ — ①

$\downarrow$

2^0

Basic step:

For $n=0$

$L.H.S = 2^0 = 1$

$R.H.S = 2^{0+1} - 1 = 2-1 = 1$

$L.H.S = R.H.S$

$\therefore P(n)$ is true for $n=0$.

Inductive step:

assume that $P(n)$ is true for $n=k$

$$1 + 2^1 + 2^2 + \dots + 2^k = 2^{k+1} - 1 \quad \text{— (2)}$$

Then we have to prove that $P(n)$ is true for $n = k+1$.

i.e $1 + 2^1 + 2^2 + \dots 2^k + 2^{k+1} = 2^{k+2} - 1$

$L.H.S = (1 + 2^1 + 2^2 + \dots + 2^k) + 2^{k+1}$

$= 2^{k+1} - 1 + 2^{k+1}$

$= 2 \cdot 2^{k+1} - 1$

$= 2^{k+2} - 1$

$= R.H.S$

$\therefore$ P(n) is true for $n = k+1$

$\therefore$ By using the principal of mathematical induction P(n) is true for all non-negative integers.

(1+2+3) Use mathematical induction to prove the inequality $n < 2^n$ for all +ive int. n.

$\Rightarrow$

Date 2/10/21
Page

Binary Operation

The binary operation is said to be binary operation on set A. If $a * b \in A$ for all $a, b \in A$.

Ex: $N = \{1, 2, 3 \ldots\}$

$a = 2 \quad b = 5$

$a + b = 7 \in N$

For all $a, b, \in N$ Then $a + b \in N$.

∴ Addition is the binary operation on set of natural number.

$a = 2 \quad b = 5$

$a - b = -3 \notin N$

∴ Substraction is not binary operation on set N.

∴ Multiplication is binary operation of N

∴ Division is not binary operation on N.

Ex: 2

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

$\Rightarrow$ Add^n, Subt^n, Mult^n } Binary operation on Z

Div - is not Binary operation on Z.

Algebric System:-

A system consisting of a set S and one or more binary operation defined on the set will be called as algebrac system

Ex:- $(N, +), (N, \times), \Rightarrow (N, +, \times)$ $(N, -) \times$

$R(+, \times)$, $Q(+, \times)$

$= 2^{k+2} - 1 = R.I$

Semi group :-

let $(A, *)$ be an Algebric system the $(A, *)$ is called semi group If $*$ is associative.

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

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

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

$a - (b - c) = (a - b) - c$

Wise

Ex :- i) $(N, +)$

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

$a = 2 \quad b = 3 \quad c = 4$

$2 + (3 + 4) = 9$

$(2 + 3) + 4 = 9$

$(N, +)$ is semigroup.

Ex :- 2) $(N, -)$ $\Rightarrow$ not algebric system

$\Rightarrow$ not semi-group

Semigroup = Algebric system.

Ex :- 3) $(N, \times)$

$a = 2 \quad b = 3 \quad c = 4$

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

$(2 \cdot 3) \cdot 4 = 24$

$2 \cdot (3 \cdot 4) = 24$

Yes mult^n is associative

$(N, \times)$ is semigroup.

Date / /
Page L&W

★ Monoid:-

A non-empty set A with binary operation $*$ defined on A is called Monoid If $*$ satisfies the following properties

i) $a*(b*c) = (a*b)*c$ for all $a,b,c \in A$

ii) There exist an element $e \in A$ such that $a*e = e*a = a$ for any $a \in A$ e is called an identity of A.

$a*e = e*a = a$.

$\Rightarrow$ $a+e = e+a = a \Rightarrow e = 0$

$e = 0$ additive identity of A.

$a.e = e.a = a$

$e = 1$ multiplicative identity of A.

In short

Monoid = semigroup + existence of identity

(for add^n $e=0$ & for multp^n $e=1$)

Ex:- $(N, +)$ $N = \{1, 2, 3 \ldots\}$

$a+e = e+a = a$

$a = 2$

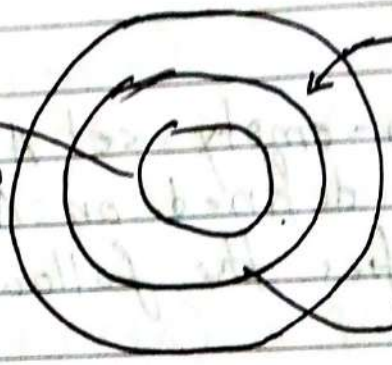
$2+e = e+2 = 2$

$e = 0 \notin N$

$\therefore (N, +)$ is not monoid.

Date 4/10/21
Page

Algebraic system
⇒ set with one or more binary operation



monoid
= semigroup + identity

semigroup
=

i) $(z, +)$ → yes monoid.
$e = 0 \in z$

ii) $(z, -)$ → X monoid

iii) (z, x) → ✓
$e = 1 \in z$

$z^* = z - \{0\}$

$Q^* = Q - \{0\}$

$R^* = R - \{0\}$

iv) $(z^*, +)$ → X

v) $(Q, +)$ → ✓

vi) $(R, +)$ → ✓

vii) (Q, x) → ✓

viii) (R, x) →

Date / /
Page L&W

Monoid

Algebric system

i) Associative properties

ii) identity property (Add e=0) (Mul e=1)

i) $(Q, +)$

⇒ for all $a, b, c \in Q$

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

Q is associative under addition.

ii) $\exists \; e = 0 \in Q$

such that $a + e = e + a = a$

for any $a \in Q$.

$(Q, +)$ is monoid

i) $a = \frac{1}{2} \quad b = \frac{1}{3} \quad c = \frac{1}{4}$

$$(a+b)+c = \left(\frac{1}{2} + \frac{1}{3}\right) + \frac{1}{4} = \frac{5}{6} + \frac{1}{4}$$

$$= \frac{26}{24} = \frac{13}{12}$$

$$a+(b+c) = \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) = \frac{1}{2} + \frac{7}{12} = \frac{12+14}{24}$$

$$= \frac{26}{24} = \frac{13}{12}.$$

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

★ Group.

A group is non-empty set G with the binary operation $*$ defined on G with the following properties.

i) $(a * b) * c = a * (b * c)$ for any $a, b, c \in G$

ii) There exist a unique element $e \in G$ such that $a * e = e * a$ for any $a \in G$.

iii) for every $a \in G$ there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$ where a^{-1} is called inverse of a.

In short

Group = Monoid + existence of inverse property.

Ex:

i) $(N, +) \rightarrow X$.

ii) $(N, *) \xrightarrow{(N, \times)} \checkmark$ monoid

$e = 1 \in N$.

$a \cdot a^{-1} = a \cdot a^{-1} = 1 = e$

$a \cdot a^{-1} = 1$

$a = 2 \qquad 2 \cdot a^{-1} = 1$

$\Rightarrow \quad a^{-1} = \frac{1}{2} \notin N$

$(N, \times)$ is not group.

iii) $(Z, +)$

$\Rightarrow$

i) associative ii) $e = 0 \in Z$

iii) $a * a^{-1} = a^{-1} * a = e.$

$\Rightarrow \quad a + a^{-1} = a^{-1} + a = 0.$

$a + a^{-1} = 0$

$a = 6$

$a + (a^{-1}) = 0$

$6 + (a^{-1}) = 0$

$a^{-1} = -6$

Under addition inverse of element a is $(-a)$

$0 + 0 = 0.$

$(Z, +)$ is Group.

iv) $(Z, \dot{\times})$

i) associative ✓ ii) identity ✓ $e=1$

iii) Inverse ✗

$a \cdot a^{-1} = a^{-1} \cdot a = e = 1$

$a = 4 \quad a^{-1} = \frac{1}{4}$.

$(Z, \times)$ is not group

v) $(Q, +)$

i) associative ✓ ii) identity ✓

iii) inverse ✓

$\frac{1}{3} - \frac{1}{3} = 0$.

$(Q, +)$ is Group.

vi) $(Q, \times)$

i) associative ✓ ii) identity ✓

iii) $\left(\frac{1}{3}\right) \times 3 = 1 \qquad -\frac{2}{3} \times -\frac{3}{2} = 1$

inverse ✗ for 0 not exist.

(Q, x) is not group.

vii) (Q^*, x)

It is group $Q^* = Q - \{0\}$

viii) $(R, +)$

It is group.

ix) (R, x) $a = 0 \in R$ a^{-1} of 0 not exist

It is not group.

x) (R^*, x) is group.

Finte set.

i) Let

$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Is (A, x) is group or not?

Binary operation.

$\Rightarrow$ for all $a, b \in A$ then $a * b \in A$.

In this set ~~so~~ there is no binary operation.

It is not a group in any operation.

Date 7/10/24
Page

ii) $A = \{-1, 0, 1\}$

$(A, +)$

$a = -1 \quad b = 0 \quad c = 1$

$(a+b)+c = (-1+0)+1 = 0$

$a+(b+c) = -1+(0+1) = 0$

$e = 0$.

iii) Inverse exist.

$(A, +)$ is group.

Abelian Group

Group G is called abelian group.

A Group $(G, *)$ is called abelian group if $a * b = b * a$ for all a, b, c

Ex:

i) $(Z, +)$, $(Q, +)$, $(R, +)$, $(Q^*, \times)$, $(R^*, \times)$.

Ex:

$$M_{22} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R, ad - bc \neq 0, |A| \neq 0 \right\}$$

Date 8/10/21
Page L&W

(M_{22}, X)

Multiplication of matrix is binary.

i) for all $a, b, c \in G$ # Associative

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

Associative property.

$A, B, C \in M_{22}$

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

ii) Identity properties

$a + e = a \qquad e = 0$

$a \cdot e = a \qquad e = 1$

$A \cdot I = A \qquad e = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$A + 0 = A \qquad e = 0.$

iii) Existence of inverse.

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

$a \cdot a^{-1} = e = 1$

$A \cdot A^{-1} = I$

exist. $(|A| \neq 0)$ for every $A \in M_{22}$ A^{-1}

$(M_{22}, \times)$ is group.

$A, B \in M_{22}$

$A \cdot B \neq B \cdot A$

(matrix mutiplication is not commutative

$(M_{22}, \times)$ is not abelian group.

Cyclic Group :-

A group G, with $(G, *)$ is called cyclic group if their exist an element $a \in G$ such that every element of G can be return as a^n, for some integer n.

$$G = \langle a \rangle = \{ a^n / n \in Z \}$$

we say that G is generated by a or a is generator of G.

If binary operation is addition then

$a^n = \underbrace{a + a \ldots\ldots + a}_{n \text{ times}} = a \cdot n$

If binary operation is multiplication.

$$a^n = \underbrace{a \times a \times a \ldots \times a}_{n \text{ times}}$$

Ex: $G = \{1, -1, i, -i\}$

i) show that ~~Is~~ G is group under multiplication.

ii) Is G is abelian group.

iii) Is G is cyclic group if it is cyclic find it's generator.

⇒ Composition table.

multiplication ↓ / → X

X	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	+1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Inverse from composition table

$1 \times 1 = 1$ $(G, \times)$ is group.

$-1 \times -1 = 1$

$i \times -i = 1$

$-i \times i = 1$

ii) from table

$a \cdot b = b \cdot a$ for all $a, b \in G$

$(G, \times)$ is abelian group.

iii) Let

$a = 1 \in G$

$a^n = (1)^n = \{1\} \neq G$

$a = 1$ is not generator

for $a = -1$

$a^n = (-1)^n = \{1, -1\}$

$a = -1$ is not generator.

for $a = i$

$n=1 \quad n=2 \quad n=3 \quad n=4$

$a^n = (i)^n = \{i, -1, -i, 1\}$

$a = i$ is the generator of G.

$(G, \times)$ is cyclic group.

also for $a = -i$ is the generator of G.

Date 10/10/21
Page L&W

$(Z, +)$ $\quad n \in Z$

$\Rightarrow$

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

for $a = 0$

$a^n = \underbrace{a + a \ldots \ldots a}_{n \text{ times}} = an$

$a^n = (0)^n = n \cdot a = n \times 0 = 0 = \{0\} \neq Z$

$a = 0$ is not generator of $(Z, +)$

for $a = 1$

$a^n = (1)^n = n(1) = n = \{\ldots -2, -1, 0, 1, 2 \ldots\}$
$= Z$

$a = 1$ is generator of $(Z, +)$

for $a = -1$

$a^n = (-1)^n = n(-1) = -n = \{\ldots -2, -1, 0, 1, 2 \ldots\}$
$= Z$

$a = -1$ is generator of $(Z, -)$.

for $a = 2$

$a^n = n.a = n.2 = \{\ldots -4, -2, 0, 2, 4 \ldots\}$

$a = 2$ is not generator of group $(Z, +)$

$(Z, +)$ is cyclic group with two generator

iii) $(Q, +)$ Is it cyclic group.

⇒ for element $a = 0 \in Q$

$a^n = n.a = n.0 = \{0\} \neq Q$

$a = 0$ is not a generator of $(Q, +)$

for $a = 1$

$a^n = n.(1) = \{\ldots 2, 1, 0, -1, -2 \ldots\} = Z$

$\neq Q$

$a = 1$ is not a generator of $(Q, +)$

for $a = \frac{3}{5}$

$a^n = n.\left(\frac{3}{5}\right) = \left\{\ldots \frac{-6}{5}, 0, \frac{3}{5}, \frac{6}{5} \ldots\right\} \neq Q$

$a = \frac{3}{5}$ is not a generator of $(Q, +)$

for every element $a \in Q$

$$\langle a \rangle = \{ n.a \mid n \in z \} \neq Q$$

Q ~~has~~ not Q has no generator there for $(Q, +)$ is not cyclic group.

iv) $(R, +)$ is not cyclic group.

Divides

If $a, b \in Z$ and a/b $b = c.a$ $c \in Z$

a/b $a \not/ b$ → not divide.

Ex: Is 2 divides 4.

=)

$a = 2$ $b = 4$ $b = c.a$

$4 = c.2$

$c = 2$.

Ex Is 4 divides 2.

=)

$a = 4$ $b = 2$ c

$2 = \left(\frac{1}{2}\right) \times 4$ $c \notin Z$

It is not possible.

Ex:- 3/6 , 6/3 , 2/5

Division algorith.

$a, b \in z$ such that $a = bq + r$ → remainder

quotient

$0 \le r < b$

Ex:- $a = 5 \quad b = 2$

$5 = 2.2 + 1$

$a=5 \quad b=2 \quad q=2 \quad r=1$

$a = -5 \quad b = 2$

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

$= -6 + 1$

$= -5$

Date 12/10/21
Page

Modular Arithmetic (concept of congruence).

If a & b are integers & m is Z^+ (positive integer) then a is congruent to b modulo m we say if m divides a-b. i.e $\frac{a-b}{m}$ = integers.

$$a \equiv b \pmod{m}$$

Ex: a = 17 b = 5 m = 6

=> $a - b = 17 - 5 = 12$

i.e $\frac{a-b}{m} = \frac{12}{6} = 2 \in Z$

m divides a-b

6 divides 12

i.e $17 \equiv 5 \pmod{6}$

Ex: a = 50 b = ? m = 24

=> $50 = 2 \pmod{24}$

24 hour clock 12 hour clock

21 $21 = 9 \pmod{12}$

Ex: $a = 24 \quad b = 14 \quad m = 6$

$\Rightarrow$

$a - b = 24 - 14 = 10$

$\Rightarrow \quad \frac{a-b}{6} = \frac{10}{6} = \frac{5}{3} \notin Z^+$

m doesn't divides a-b

$a \not\equiv b \pmod m$

$24 = 14 \pmod 6$

$a \equiv b \pmod m$

$c \equiv d \pmod m$

$\Rightarrow \quad a + c = b + d \pmod m$

$a \equiv b \pmod m$

$c \equiv d \pmod m$

$ac = bd \pmod m$

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

$m = 5$

$1 \equiv 1 \pmod 5$
$2 \equiv 2 \pmod 5$
$3 \equiv 3 \pmod 5$
$4 \equiv 4 \pmod 5$
$5 \equiv 0 \pmod 5$

$6 \equiv 1 \pmod 5$
$7 \equiv 2 \pmod 5$
$8 \equiv 3 \pmod 5$
$9 \equiv 4 \pmod 5$
$10 \equiv 0 \pmod 5$
$11 \equiv 1 \pmod 5$

$-1 = (4) \pmod 5 \Rightarrow -1 = (-1)5 + 4$

$-2 = (3) \pmod 5 \quad -2 = (-2)5 + 4$

$-3 = (2) \pmod 5$

$-4 = (1) \pmod 5$

$-5 = (0) \pmod 5$

$Z_5 = \{0, 1, 2, 3, 4\}$

$Z_{10} = \{0, 1, 2 \ldots 9\}$

$Z_m = \{0, 1, 2 \ldots (m-1)\}$.
modulo m.

$+_m$ = Addition modulo m

X_m = Multiplication modulo m.

$Z_5 = \{0, 1, 2, 3, 4\}$

$2, 3 \in Z_5$

$2 +_5 3 = 5 = 0.$

$2 +_5 4 = 6 = 1$

$2 X_5 3 = 6 = 1 \quad 16 = 1$

$2 X_5 4 = 8 = 3$

$3 X_5 4 = 12 = 2$

Date 18/10/21
Page

Z = Infinite Set

Z_m = Set of Integer under modulo

$+_m$ ⇒ Addition $\times_m$ ⇒ multiplic

Composition Table:

$+_5$	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

1) for all $a, b, c \in Z_5$

$a +_5 (b +_5 c) = (a +_5 b) +_5 c$

for all $a, b, c \in Z_5$

Z_5 is associative under $+_5$

ii) $c = 0 \in Z_5$

s.t $a + e = a$ for all $a \in Z_5$

(iii)

$a^n = n.a = n.a = \{0\} \neq Z_5$

$b.a = 0$ is not generator of $(Z_5, +_5)$

for $a = 1$

$a^n = n = \{0, 1, 2, 3, 4\} = Z_5$

for $a = -1$

$a^n = n = \{0, 1, 2, 3, 4\} = Z_5$

$-1 = (-1)(5) + 4 \rightarrow r$

$a = 1$ is generator of $(Z_5, +_5)$

$(Z_5, +_5)$ is cyclic group.

Date 21/10/21
Page

Ex: $G = Z_4 = \{0, 1, 2, 3\}$.

i) $H = Z_4$ is subgroup of $G = Z_4$ under addition modulo 4.

2) $H = \{0\} = \{e\}$ is subgroup of G.

Coset

Let $(G, *)$ be the group and $(H, *)$ be the subgroup of G. for any $a \in G$ the set $a * H = \{a * h / h \in H\}$ is called left coset of H determine by a.

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

If operation is addition then $a + H = \{a + h / h \in H\}$ = Left coset.

$H + a = \{h + a / h \in H\}$ = Right coset.

If operation is multiplication

$a \times H = \{a \times h / h \in H\}$ = Left coset

$H \times a = \{h \times a / h \in H\}$ = Right coset.

Ex: $G = Z_4 = \{0,1,2,3\} = (Z_4, +_4)$
& $H = \{0,2\}$ is subgroup of $(Z_4, +_4)$
then Find left and right coset.

Sol^n

$Z_4 = \{0,1,2,3\}$

$H = \{0,2\}$

Left coset

for $a \in G$

$$a(+_4)H = \{a(+_4)h \mid h \in H\}$$

for $a = 0$.

$$\Rightarrow \quad 0(+_4)H = \{0(+_4)h \mid h \in H\}$$

$$= \{0,2\}$$

for $a = 1$

$$\Rightarrow \quad 1(+_4)H = \{1(+_4)h \mid h \in H\}$$

$$= \{1,3\}$$

for $a = 2$

$$\Rightarrow \quad 2(+_4)H = \{2(+_4)h \mid h \in H\}$$

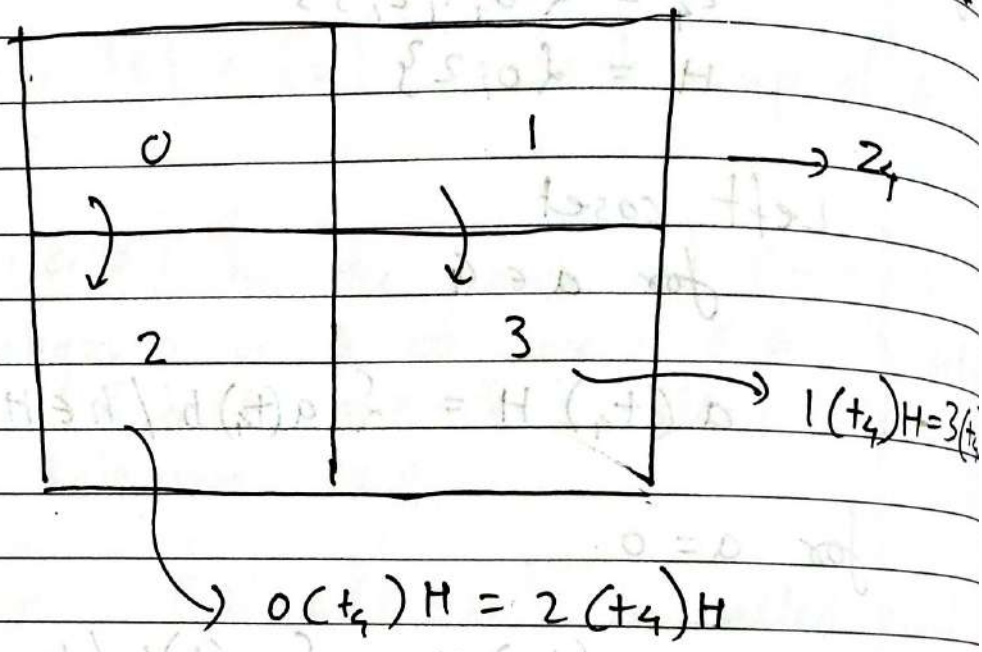
$$= \{2,0\}$$

$$= \text{coset for element } 0.$$

iv for $a=3$

$3(+_4)H = \{3(+_4)h \mid h \in H\}$

$= \{3, 1\}$ = coset of $a=1$



Right coset

i) for $a=0$

$H(+_4)0 = \{h(+_4)0 / h \in H\}$

$= \{0, 2\}$

ii) for $a=1$

$H(+_4)1 = \{h(+_4)1 / h \in H\}$

$= \{1, 3\}$

iii) for $a=2$

$$H(+_4)2 = \{ h(+_4)2 \mid h \in H \}$$
$$= \{0, 2\}$$

iv) for $a=3$

$$H(+_4)3 = \{ h(+_4)3 \mid h \in H \}$$
$$= \{3, 1\}.$$

Here Left coset & Right coset are equal.

Ex: $G = \{1, -1, i, -i\}$ is group under multiplicat. & $H = \{1, -1\}$ is subgroup of G under multiplication then find left cosets & Right cosets.

=) $G = \{1, -1, i, -i\}$

$H = \{1, -1\}$

Left coset

for $a=1$

=> $1(\times)H = \{ 1 \times h \mid h \in H \}$

$= \{1, -1\}$

for $a = -1$

$\Rightarrow -1 \times H = \{-1 \times h \mid h \in H\}$

$= \{-1, 1\}$

for $a = i$

$\Rightarrow i \times H = \{i \times h \mid h \in H\}$

$= \{i, -i\}$

for $a = -i$

$-i \times H = \{-i \times h \mid h \in H\}$

$= \{-i, i\}$

Right coset

for $a = 1$

$= H \times 1 = \{h \times 1 \mid h \in H\}$

$= \{1, -1\}$

for $a = -1$

$= H \times -1 = \{h \times -1 \mid h \in H\}$

$= \{-1, 1\}$

Date 22/10/21
Page L&W

for $a = i$

$$H \times i = \{ h \times i \mid h \in H \}$$
$$= \{ i, -i \}$$

for $a = -i$

$$H \times -i = \{ h \times -i \mid h \in H \}$$
$$= \{ -i, i \}$$

Left coset = Right coset.

Normal subgroup

A subgroup H of G is said to be normal subgroup if for every $a \in G$, $a * H = H * a$.

Ex: $G = (Z_4, +_4)$
$H = \{0, 2\}$

$\Rightarrow$ for every $a \in G$ $a(+_4)H = H(+_4)a$
$\Rightarrow$ Left coset = Right coset
Hence H is normal subgroup of G.

* Normal subgroup denoted by "N"

2) $G = \{1, -1, i, -i\}$
$H = \{1, -1\}$ is subgroup under multip

⇒ for every $a \in G$

$a \times H = H \times a$.
Left coset = Right coset

Here H is the normal subgroup of G

3) $G = (Z, +)$ be group and $H = (2Z, +)$ is subgroup of G

⇒ Z is commutative under +

∴
Left coset = Right coset.

★ Every subgroup of abelian group is normal subgroup.

☆ Q. Factor or Quotient Group.

Let N be the normal subgroup of G then G/N is the set of all ~~que~~ cosets of N in G.

G/N is called as quotient group.

Date / /
Page L&W

Ex 1) $G = (\mathbb{Z}, +)$ $H = (2\mathbb{Z}, +)$ is Normal subgroup then $\mathbb{Z}/2\mathbb{Z}$ is quotient group.

Ex 2) $G_1 = (Z_4, +_4)$ $H = \{0, 2\}$

$$\Rightarrow G/H = \{ 0(+_4)H, 1(+_4)H, 2(+_4)H, 3(+_4)H \}$$

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

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

Lagrange's theorem.

a divide b ie $a/b \Rightarrow b = ca$

c = must integer.

For any finite group G., and H is subgroup of G then order of H divides the order of G.

order of H (11) order = no. of element

i.e $|H| / |G|$

But converse of this theorem need not be true.

If $|H| / |G|$ then H need not be subgroup of G.

* If $|H| \nmid |G|$ then H is not subgroup of G.

Ex:- i) $G = \{1, -1, i, -i\}$ be group under multiplication.

i) Is $H = \{1, -1, i\}$ is subgroup of G?

⇒ $|H| = 3 \quad |G| = 4$

$= 3 \nmid 4$ i.e order of H $(|H|) \nmid |G|$

H is not subgroup of G.

ii) Is $H = \{-1, i\}$ is subgroup of G?

⇒ $|H| = 2 \quad |G| = 4$

$|H| / |G|$

But H is not subgroup of G

~~$e \neq 1 \in H$~~ $e = 1 \notin H$.

Date 28/10/21
Page L&W

iii) Is $H = \{1, i\}$ is subgroup of G?

⇒ $|H| = 2 \quad |G| = 4$

$|H| / |G|$

i) $e = 1 \in G$

ii) Inverse doesn't exist that's why it is not subgroup.

iv) Is $H = \{1, -1, \}$ is subgroup of G?

⇒ yes.

✱ Homomorphism & Isomorphism of Groups.

Homomorphism ⇒ same + shape
Isomorphism ⇒ identical + shape.

$G = (Z_4, +_4)$

$G' = \{1, i, -1, -i\}$ is group under multiplication.

Z_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

X	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$\phi : G \to G'$

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

for all $a, b \in G$.

Isomorphism = homomorphism + bijection.

$\phi(G, +) \to (G', +)$

$\phi(a+b) = \phi(a) + \phi(b)$

$\phi(a.b) = \phi(a) . \phi(b)$

$\phi(a+b) = \phi(a) . \phi(b)$

$\phi(a.b) = \phi(a) + \phi(b)$

Ex:

$G = (Z, +)$ $\quad G' = (2Z, +)$

$\phi : (G, +) \to (G', +)$

$\phi : (Z, +) \to (2Z, +)$

defined by $\phi(x) = 2x$

for homomorphism

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

i.e $\phi(a+b) = \phi(a) + \phi(b)$

$$\phi(a+b) = 2(a+b)$$
$$= 2a + 2b$$
$$= \phi(a) + \phi(b)$$

$$\phi(a+b) = \phi(a) + \phi(b)$$

$\therefore$ ϕ is homomorphism from G to G'.

i) for one-one.

If $\phi(a) = \phi(b)$

$2a = 2b$

$\Rightarrow$ $a = b$

$\therefore$ ϕ is one-one

ii) for onto.

If $\phi(x) = 2x = y$.

$y \in 2Z$

$\Rightarrow$ $2x = y$

$\Rightarrow$ $y = \frac{x}{2}$ → replace $\boxed{x = \frac{y}{2}}$

Date 29/10/21
Page
L&W

ϕ is onto function.

$\therefore$ for every $y \in 2z$ there exist $x \in z$.

$\therefore$ ϕ is bijective.

$\therefore$ ϕ is isomorphism.

$(z, +)$ & $(2z, +)$ are isomorphic group.

Ex:- Isomorphism = Homomorphism + bijective
$\phi(a*b) = \phi(a) * \phi(b)$ mapping.
(one-one & onto

Ex:- $G = (z, +)$ & $G' = (2z, +)$
are Isomorphism.

Ex:- $G = (R, +)$ & $G' = (R^+, \times)$
$e = 0$ $e = 1$

$\Rightarrow$

$$\phi(a+b) = \phi(a) \times \phi(b)$$

$$\phi : (R, +) \longrightarrow (R^+, \times)$$

defined by $\phi(x) = e^x$ → value of e^x never be 0 & -ve so we put e^x here

Determine G & G' is isomorphism or not?

Date / /
Page L&W

i) for homomorphism.

$$\phi(a+b) = e^{a+b}$$

$$= e^a \cdot e^b$$

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

$$\phi(a+b) = \phi(a) \times \phi(b)$$

ϕ is homomorphism.

ii) for one-one.

If consider $\phi(a) = \phi(b)$

$$e^a = e^b \quad \text{... log on both side.}$$

$$a = b$$

ϕ is one-one.

iii) for onto.

$$\phi(x) = e^x = y$$

$$x = \log y \quad \text{for every } y \in R^+.$$

$$\boxed{y = \log x.}$$

ϕ is isomorphism from G to G'

$\therefore$ groups $G = (R, +)$ & $G' = (R^+, \times)$ are isomorphic group

Fermat's (Little) Theorem:

If p is prime and a is any integer then

$$a^p \equiv a \pmod{p} \qquad a^{p-1} \equiv 1 \pmod{p}$$

cond: $p \nmid a$. p is not factor of a.

Ex:-

$a = 4 \qquad p = 5$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$4^4 \equiv 1 \pmod{5}$$

$$256 \equiv 1 \pmod{5}$$

Q: Find the remainder when 3^{2021} is divided by 11.

$a = 3 \qquad p = 2021 + 1$

$$3^{2020} \equiv \_ \pmod{31}$$

$$\Rightarrow \quad a^{p-1} = 1 \pmod{p}$$

$a = 3 \qquad p = 11$

$$3^{11-1} \equiv 1 \pmod{11}$$

$$3^{10} \equiv 1 \pmod{11} \quad \text{—(1)}$$

$\frac{2021}{p-1} = \frac{2021}{10}$ $\quad q = 202.$

$(3^{10})^{202} = (1)^{202} \pmod{11}$

$3^{2020} = 1 \pmod{11}$

$3 \cdot 3^{2020} = 3 \cdot 1 \pmod{11}$ multiply by 3.

$3^{2021} = 3 \pmod{11}$.

Ex: 2

$4^{2-1} \equiv 1 \pmod{2}$

$4 \not\equiv 1 \pmod{2}$ for P.f a not satisfied.

Ex:

Find the remainder when 3^{100000} divide by 53.

$\Rightarrow$ $a = 3$ $\quad p = 100000.\ 53$

$(3^{52})^{1923} \cdot 3^4 \equiv 3^4 \pmod{53}$ $\quad \frac{100000}{p-1} = 1923$

multiply by 3^4.

$3^{99996} \cdot 3^4 = 3^4 \pmod{53}$.

Date 1/11/21
Page

$3^{100000} = 3^{r} \pmod{53}$

$r = 81 \qquad r < b$

$\frac{81}{53} \Rightarrow 28 = r.$

$\boxed{r = 28}$

Q. How many subgroups are there fro group of order 7.

⇒

$|G| = 7$

⇒ order of subgroup / order of group.

⇒ order of subgroup / 7

$7 = 1, 7.$

↓ ↓

2 sub group

$|H| = 1 \text{ or } 7$

Q Let $S = \{1, 2, 3, 4\}$. Define the binary operation by following table

*	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

*	1	2	3	4
1	1	2	3	4
2	2	1	1	1
3	3	1	1	4
4	4	2	3	4

i) Is $(S, *)$ is semigroup.

⇒ $a = 2, b = 3, c = 4$

$$(a * b) * c = ((2 * 3) * 4)$$
$$= 1 * 4$$
$$= 4$$

$$a * (b * c) = 2 * (3 * 4)$$
$$= 2 * 4$$
$$= 1$$

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

It is not associative.

$(S, *)$ is not semigroup.

2) Is in given $(S, *)$ has identity element

=) Identity $\quad a * e = e * a = e$

$1 * 1 = 1 \quad 2 * 1 = 2 \quad 3 * 1 = 3$

$4 * 1 = 4$

1 is the identity.

3) Are the element of $(S, *)$ are invertible. If so write the inverse of this element

=)

for $a = 1 \quad a^{-1} = 1 \quad a * a^{-1} = 1$

for $a = 2$

only $a = 1$ is invertible others inverse doesn't exist.

4) Consider $G = \{1, -1, i, -i\}$ be the group under multiplication.

i) Is show that $H = \{1, -1\}$ is normal sub group of G.

=)

Normal subgroup = subgroup +
for every $a \in G$
left coset = right coset
$a * H = H * a$.

Date / /
Page L&W

Subgroup ($H \leq G$)

i) $e = 1 \in H$ ii) for every $a, b \in H$ then $a.b \in H$
iii) for every $a \in H$ then $a^{-1} \in H$.

✓

Every subgroup of abilican group is normal subgroup.

Q. Consider $(Z_6, +_6)$ is group. where $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

i) Is $H = \{0, 1, 2, 3\}$ is subgroup of $(Z_6, +_6)$.

$|G| = 6 \quad |H| = 4.$

$4 \neq 6$

$\Rightarrow |H| \neq |G|$ ∴

H is not subgroup of G.

ii) Is $H = \{0, 1, 2\}$.

$|H| = 3 \quad |G| = 6.$ $3/6$

But inverse doesn't exist H is not subgroup.

iii) Is $H = \{0, 3\}$ is subgroup of a

$|H| = 2 \quad |G| = 6.$

$2 | 6$

i) exist identity yes.

Date 10/11/21
Page L&W

iii) $(Q, +)$

a) Asso ✓
b) Identity ✓
c) Inverse ✓ eg: $a = -1/2$ $a^{-1} = 1/2$
$a = -1$ $a^{-1} = 1$
d) commu property ✓
e) semigroup ✓
f) distributive ✓

$\therefore (Q, +, \cdot)$ is a ring

iv) $(R, +, \cdot)$ is a ring

v) $Z_4 = \{0, 1, 2, 3\}$

Set of integers under modulo 4.

vi) $+_4$

add^n modulo 4

$2 +_4 2 = 0$ $2 + 2 = 4$
$2 +_4 3 = 1$ $2 + 3 = 5$

$+_4 \Rightarrow$ Hi te pahile add kra simple
ani mg tya new no la modulo
under kay ahe tya no ni divide
kr ani remainder sang

$2 + 3 = \underline{5}$

$$\begin{array}{r} 1 \\ 4\sqrt{5} \\ -4 \\ \hline 1 \end{array} \leftarrow 2 +_4 3$$

v) $(Z_4, +_4, \times_4)$

$Z_4 = \{0, 1, 2, 3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

i) Asso ✓

ii) identity ✓

iii) Inverse ($a+b = b+a = 0$)

Here $0+0$ in table is present

for 1 : $1+3 = 0$

2 : $2+2 = 0$

3 : $3+1 = 0$.

Thus it satisfy inverse property (In short check out whether 0 is present in every row).

d) comm property

eg $1+1=2$

$\rightarrow 2+3=1$ & $3+2=1$

$\Rightarrow 2+1=3$ & $1+2=3$.

e) Semi group ✓

f) distributive. ✓

Thus it is a ring.

Date 11/11/2
Page L&W

Rings.

Algebraic structure $(R, +, \cdot)$ is said to be ring

If

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

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

iii) Distribute laws holds.

($\cdot$ → multiplication)

eg. $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$

$(Z_4, +_4, X_4)$, $(M_{22}, +, X)$.

Ex: $(Z_5, +_5, X_5)$ ✓

* Types of Rings.

1) commutative Ring.

Ring = Abelian Group under addition (already commutative)

A Ring $(R, +, \cdot)$ is called commutative ring if $a.b = b.a$ for every $a, b \in R$.

Ex: $(Z, +)$, $(Q, +)$, $(R, +, \cdot)$
$(Z_4, +_4, \cdot)$ $(Z_n, +_n, \times_n)$

$(M_{22}, +, \times)$ is not commutative Ring.

★ Ring with zero divisor

Quotient
Divisor | Dividend
Remainder

Suppose A & B ~~are~~

If $a.b = 0$ where ~~a & b~~ a & b are non zero elements of $(R, +, \cdot)$

then a & b are called as divisors of zero & $(R, +, .)$ is called ring with zero ~~da~~ divisors.

Ex:

$Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$(Z_6, +_6, X_6)$.

$a = 2 \neq 0$, $b = 3 \neq 0$.

But $a.b = 2.3 = 0$.

2 & 3 are called zero of divisor.
3 & 4 are called zero of divisor.
$(Z_6, +_6, X_6)$ ring with zero divisor.

Ring without zero divisor.

$(R, +, .)$ is called ring without zero divisor If $a.b = 0$
$\Rightarrow a = 0$ or $b = 0$.

In other words.

$a \neq 0$, $b \neq 0$ then $a.b \neq 0$.

Ex: $(Z_p, +_p, X_p)$ where p is prime no.
$(Z_7, +_7, X_7)$, $(Z_5, +_5, X_5)$
$(Z, +, X)$ $(R, +, X)$.

Integral domain:

A commutative Ring $(R, +, \cdot)$ without and with zero divisor is called as integral domain.

Ex: $(Z_s, +_s, \times_s)$, $(Z_p, +_p, \times_p)$.
$(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$.

Field.

A commutative Ring with unity is called field.

If every nonzero element has multiplicative inverse.

eg. $(Z, +, \cdot)$ ⇒ It is not a field

$(Q, +, \cdot)$ ✓ $(R, +, \cdot)$

Q. $Z_4 = \{0, 1, 2, 3\}$
Is $(Z_4, +_4, \times_4)$ Field.

⇒ $Z_4^* = Z_4 - \{0\} = \{1, 2, 3\}$.

$\times_4$	1	2	3
1	(1)	2	3
2	2	0	2
3	3	2	(1)

inverse of 2 is not exist

so this (Z_4, X_4, t_4) is not field.

Ex: $Z_5 = \{0, 1, 2, 3, 4\}$.

$\Rightarrow$ $Z_5^* = Z_5 - \{0\} = \{1, 2, 3, 4\}$.

X_5	1	2	3	4
1	(1)	2	3	4
2	2	4	(1)	3
3	3	(1)	4	2
4	4	3	2	(1)

(Z_5, t_5, X_6) is field.

Ex: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$\Rightarrow$ $Z_6^* = Z_6 - \{0\} = \{1, 2, 3, 4, 5\}$.

X_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

It is not field.

Ex $(Z_3, +_3, \times_3)$

$\times_3$	1	2
1	1	2
2	2	1

It is field.

★ $(Z_p, +_p, \times_p)$ is field where p is prime.

$(Z_n, +_n, \times_n)$ is not field where n is not prime.

↳ Every Field is integral domain.

↳ converse need not be true.

↳ Every integral domain need not be field.

eg: $(Z, +, \cdot)$.

↳ Every finite integral domain is field.