Unit - VI

Groups and Rings

Introduction

∴ In this chapter we will study some algebric structures, groups, rings, integral domains and fields.

Q. Define Algebric Structure?

Algebic Structures :-

Cryptography requires set of integers & specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebic structure.

We will define three common algebic structure

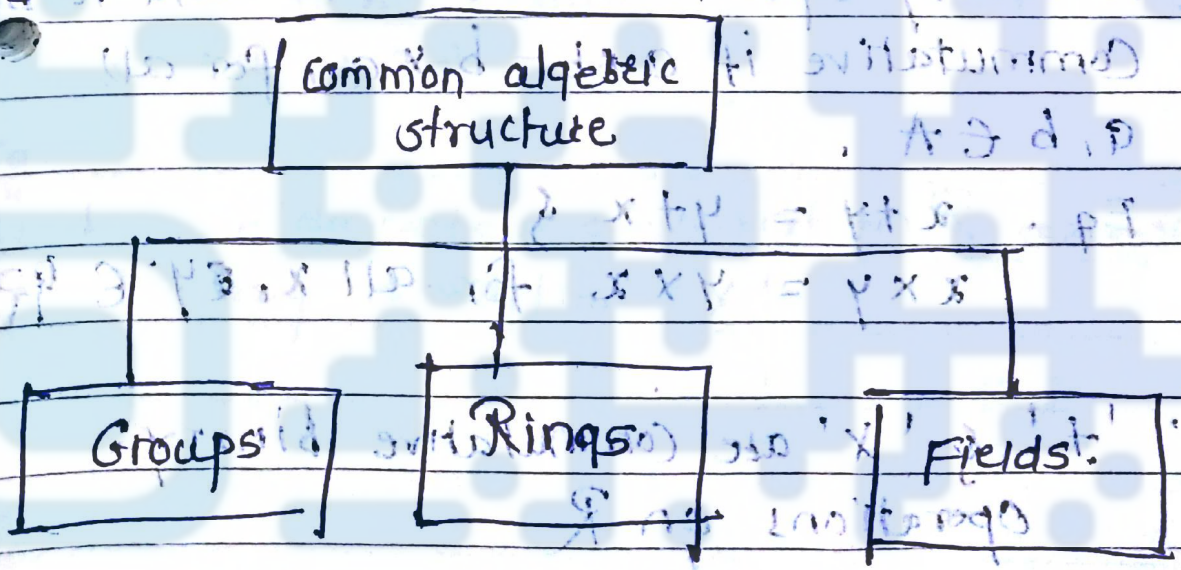

fig. 1.

Q. Explain binary operation & its properties?

* Binary operations.

I] Let A be any non empty set. A function $f: A \times A \to A$ is called the binary operation on the set A.

'*' is a binary operation on the set A iff $a*b \in A$, $\forall a, b \in A$, & $a*b$ is unique.

* Properties of binary operations.

I] Commutative Property:

A binary operation '*' on A is said to be Commutative if $a*b = b*a$; for all $a, b \in A$.

Eg. $x+y = y+x$ &
$x \times y = y \times x$ for all $x, y \in \mathbb{R}$

∴ '+' & '×' are commutative binary operations on R.

II] Associative Property

A binary operation '*' on set A. is said to be associative if $a*(b*c) = (a*b)*c$; $\forall a, b, c \in A$

eg. '+' and '×' are associative on the set of real numbers.
'−' is not associative on R.

III] Idempotent.

A binary operation '*' on set A is said to be idempotent if $a*a = a$ for all $a \in A$

Eg.
1] 1 is idempotent element in R w.r.t binary operation '×'

Eg.
Determine whether or not following operations on the set of integers Z are associative.

i] Division ;
Division on the set of integers is not associative as
$(a/b)/c \neq a/(b/c)$

ii] Exponentiation on the set of integers is not associative as
$(a^b)^c \neq a^{(b^c)}$

* Consider the binary operation * defined on the set $A = \{a, b, c, d\}$ by the following table

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

find i] $c * d$ & $d * c$ ii] $b * d$ and $d * b$
iii] $a * (b * c)$ and $(a * b) * c$
iv] Is * commutative, associative?

→ i] $c * d = a$, $d * c = a$
ii] $b * d = c$; $d * b = b$
iii] $b * c = b$ $a * (b * c) = a * b = c$
$a * b = c$
$\therefore (a * b) * c = c * c = a$

iv] * is not commutative since
$b * d \neq d * b$
* is also not associative ; since
$a * (b * c) \neq (a * b) * c$

* Special Algebeic structures.

Q. Define Groupoid, Semi-group, monoid.

1] Groupoid

→ A non empty set K with binary operation '*' is called 'groupoid if the binary operation '*' satisfies

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

In other words, every algebraic structure is groupoid.

Eg. $(R, +)$, $(R, -)$, $(Z, +)$, $(Z, \times)$ are groupoids.

2] Semi Group :

- A non empty set G with binary operation '*' is called a semigroup if it satisfies the following properties

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

i.e. '*' is associative in G

A semigroup is said to be commutative if * is commutative

3] Monoid :

Let G be a non empty set and * be a binary operations on G, $(G, *)$ is called monoid if it satisfies.

1] Associative property :

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

$\forall a, b, c \in G$

ii] Existance of Identity :

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

$e * a = a * e = a \; ; \; \forall a \in G$

the element 'e' is called the identity element.

Eg. 1] $(R, +)$ is a monoid as $a+b \in R, \forall a, b \in R$

2] $0 + a = a = a + 0 = a \; ; \; \forall a \in R.$

0 is the identity element in R wrt. '+'

eg. show that the algebric system $(A, +)$ is a monoid, where A is the set of integers & '+' is a binary operation giving addition of two integers. (4 marks)

→ Let A be the set of all integers and '+' defined on A.

i] closure property :
$a+b \in A$; $\forall a, b, \in A$ as $a+b$ is integer

ii] Associative property

$a+(b+c) = (a+b)+c$; $\forall a, b, c \in A$

iii] Existance of identity element :
for any $a \in A$, $\exists\, 0 \in A$ such that

$a+0 = 0+a = a$

∴ Therefore $(A, +)$ is a monoid.

Q. Define Group & propertis of group.

* Group :-
A group (G) is a set of elements with a binary operation '*' that satisfies the following properties.

i] ~~closure~~
ii] Associativity
iii] ~~Commutativity~~
iv] Existance of identity
v] Existance of inverse

for all $a \in G$, $\exists\, b \in G$ such that

$a * b = b * a = e$

the b is called the inverse of a in $(G, *)$

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

* Abelian Group or commutative Group
A group $(G, *)$ is called an Abelian group if, $a * b = b * a$, $\forall a, b \in G$
i.e * is commutative in $(G, *)$

* Properties of Group

I] The identity element in a group is unique.

suppose e_1 and e_2 are two identity element in group G.

we have

$e_1 e_2 = e_1$; if e_2 is identity element in G

$e_1 e_2 = e_2$; if e_1 is identity element in G

$\Rightarrow e_1 e_2 = e_1 = e_2$

∴ Hence the identity element in group G is unique

II] The inverse of each element in group G is unique.

→ Let a be any element of a group G and let e be identity element in group G.

suppose b and c are two inverses of a in G

$ba = ab = e$ & $ac = ca = e$

$\therefore b = c$

∴ the inverse of each element is unique

III] The inverse of an inverse of the element is the original element

i.e. If the inverse of a is a^{-1}

then $(a^{-1})^{-1} = a$

IV] Prove that the inverse of the product of two elements of a group G is the product of the inverses taken in reverse order

i.e. $(ab)^{-1} = b^{-1} a^{-1}$ $\forall$ $a; b \in G$

V] Prove that the cancellation laws hold in a group i.e. if $a, b, c \in G$ then

$ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$

VI] If a; b are any elements of a group G then equation $ax = b$ and $ya = b$ have unique solution in G

→ 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.

→

Given that $(A, *)$ is a monoid. Therefore it satisfies closure property, associative & the existance of identity

we have $x * x = e$, $\forall x \in A$

$x = x^{-1}$, $\forall x \in A$

Thus inverse exists for all $x \in A$

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

consider

$(a*b) * (b*a)$; $a, b \in A = a * (b*b) * a$

$= a * e * a$

$= a * a = e$

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

$= b * e * b$

$= b * b = e$

Thus $b * a$ is the inverse of $a * b$

but $x = x^{-1}$, $\forall x$ in A

$b * a = a * b$

Thus $(A, *)$ is an abelian group.

Eg. 2 If set G_1 of all rational no's other than 1 with $a * b = a + b - ab$ show that $(G, *)$ is a group.

→

We have, $a * b = a + b - ab$, $\forall a, b \in G$

i] closure group :→

Let $a, b \in G_1$, $a \neq 1$, $b \neq 1$, $\therefore ab \neq 1$

$\therefore a * b = a + b - ab \neq 1$ & $a * b \in G_1$

G_1 is closed w.r.t. $*$.

ii] Associativity :

Let $a, b, c \in G_1$

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

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

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

$= a + ab - abc$ ... ①

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

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

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

$= ab + ac - abc$ ... ②

from eqn ① & ②

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

$\therefore$ '$*$' is associative

→ iii] Existance of the identity :-

Let e be the identity element in Q_1

$a * e = a$

$a + e = ae = a$

$e - ae = 0$

$e(1-a) = 0$

$e = 0$

∴ 0 is the identity element.

iv] Existance of Inverse

Let $a \in Q_1$, $a \neq 1$

Suppose $b \in Q$ is the inverse of a

$a * b = e$

$a + b - ab = 0$

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

$b(1-a) = -a$

$b = \frac{-a}{1-a} = \frac{a}{a-1} \neq 1$ & $b \in Q_1$

The inverse exist for all a in Q_1

Thus, $(Q_1, *)$ is a group

* 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.

→ i] Closure Property :-

Let $a, b \in G$

$a * b = \frac{ab}{2} \in G$, as $ab \neq 0$

ii] Associativity :-

let $a, b, c \in G$

consider $a * (b * c) = a * \left(\frac{bc}{2}\right)$

$= \frac{abc}{2}$

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

'*' is associative in G.

iii] Existance of the identity :-

Let $a \in G$ & $\exists$ e such that,

$a * e = \frac{ae}{2} = a$

$\Rightarrow ae = 2a$

$e = 2$

'2' is the identity element in G

Name - Tharat Abhinav Sudhir

Invoice no

GIMPL/16-17/TR/1099.

Buyer's order no - 033

NB PC HP 15 - AC179TX (T0Z58PA)

iv] Existance of the inverse :-

Let $a \in G$ & $b \in G$ such that

$a * b = e = 2$

$\Rightarrow \frac{ab}{2} = 2$

$ab = 4$

$b = 4/a$

∴ The inverse of a is $\frac{4}{a}$; $\forall a \in G$

v] Commutativity :-

let $a, b \in G$

$a * b = \frac{ab}{2}$

$b * a = \frac{ba}{2} = \frac{ab}{2}$

∴ $*$ is commutative

Thus, $(G, *)$ is an abelian group.

* show that the set $G = \{1, \omega, \omega^2\}$ where ω is the cube root of unity is a group with respect to multiplication

→ Consider the following composition table of G

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

i] Closure Property :- from table all elements belong to G

∴ G is closed w.r.t multiplicn

ii] Associativity :- As all elements of G are complex numbers & multiplⁿ of complex no. is associative

∴ $(G, \times)$ is associative

iii] Existance of the identity :- From the composition table

$1(1) = 1$, $1(\omega) = 1$, $1(\omega^2) \omega^2$

∴ 1 is multiplicative identity in G

iv] Existance of the inverse:
From table the inverses of 1, ω, ω² are 1, ω², ω respectively.
Thus (G, ×) is a group.

* Let (A, *) be a group. Show that (A, *) is abelian group iff $a^2 * b^2 = (a * b)^2$

⟹ Let (A, *) be an abelian group

$a * b = b * a$

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

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

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

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

$a^2 * b^2 = (a * b)^2$ ∴ (1)

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

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

(A, *) is an abelian group.

Prove that the set ℤ of all integers with binary operation * defined by $a * b = a + b + 1$ is such that $\forall a, b \in \mathbb{Z}$ is an abelian group.

* Modulo m

I] Let a & b are any integers and m is a fixed +ve integers then the addition modulo m denoted by $a +_m b$ and defined as $a +_m b = r$; $0 \leq r \leq m$

where r is the least non -ve remainder when a+b is divided by m

eg.

$5 +_3 9 = 2$ as $5 + 9 = 14$ and $14 = 3 \times 4 + 2$

II] Let a and b be any integers and m is a fixed +ve integer. Then the multiplication modulo m is denoted by $a \times_m b$ & defined as

$a \times_m b = r$; $0 \leq r \leq m$

where r is the least non -ve remainder when a×b is divided by m

$3 \times_4 5 = 3$ as $3 \times 5 = 15$ & $15 = 4 \times 3 + 3$

III] If a and b are two integers such that a-b is divisibly by a fixed +ve integer m, is called "a congruent to b modulo m" It is denoted by $a \equiv b \pmod m$

eg. $5 \mid (12-2) \Rightarrow 12 \equiv 2 \pmod 5$

eg. Show that $(\mathbb{Z}_6, +)$ is an abelian group

* Complexes and subgroups

Q. Define groups & complexes & subgroups.

Depending upon the nature of subset of a group there are two types of subsets, which are given below,

* Complex of a Group:

Let $(G, *)$ be a group. Any non empty subset of a group G is called a complex of the group.

eg. $H_1 = \{1, 2, 3, 4, 5\}$
$H_2 = \{1, 2, 3, \ldots\}$
$H_3 = \mathbb{Z}$
are complexes of a group $(R, +)$

* Subgroup:

Let $(G, *)$ be a group. A non empty subset H of a group G, is said to be subgroup of G if $(H, *)$ itself is a group.

eg.
$(\mathbb{Z}, +)$ is a subgroup of $(R, +)$

Q. Explain properties of subgroup

→ Properties of subgroup

I] Identity of a subgroup is the same as that of the group

II] Inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

III] order of any element of a subgroup is same as the order of the element regarded as a member of the group.

IV] A necessary & sufficient condition for a non-empty subset H of a group G to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G

Q. Define CosetH ?

* Cosets

Let (G,*) be a group & H be any subgroup of G.

Let $a \in G$ be any element, then the set

$H * a = \{h * a / \forall h \in H\}$ is called a Right coset of H in G

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

Note:

1] $H * a$ and $a * H$ are subsets of G

2] If (G,*) is an abelian group then $H * a = a * H$ in G

eg.

1] Let (Z,+) is a group & $H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ is a subgroup of Z

∴ For $1 \in Z$, $H+1 = \{\ldots, -9, -4, 1, 6, 11 \ldots\}$

$3 \in Z$, $H+3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

$5 \in Z$, $H+5 = \{\ldots, -5, 0, 5, 10, \ldots\} = H$

are right cosets of H in G

* Order of an element of a group

→ Let $(G, \cdot)$ be a group. The smallest positive integer is called the order of an element $a \in G$ if

$a^n = e$ (identity element in G)

It is denoted by $O(a) = n$.

If no such +ve number exists, then we say that a is of infinite order or zero order.

Note:

1] For the order of the group is the number of distinct element in G.

2] The order of the identity element is 1 i.e. $O(e) = 1$.

3] In a group G, $O(a) = O(a^{-1})$; $\forall\ a \in G$

4] In a group G, $O(a) \leq O(G)$

Eg.

$G = \{1, -1, i, -i\}$ is a multiplicative group

1 = identity element in G & $O(G) = 4$

$O(1) = 1$

$O(-1) = 2$ as $(-1)^2 = 1$

$O(i) = 4$ as $(i)^4 = 1$

$O(-i) = 4$ as $(-1)^4 = 1$

Q. Define Cyclic group.

* Cyclic Group

A group G is called cyclic group if $\exists$ at least one element $a \in G$ such that every element $x \in G$ can be written as $x = a^m$ where m in some integer

The element a is called the generator of G and denoted by $G = \langle a \rangle$

Eg.

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

we have

$(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

$\therefore$ i is the generator of $G \Rightarrow G$ is a cyclic group.

also

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$

$\therefore$ -i is also generator of G.

$\therefore G = \langle i \rangle = \langle -i \rangle$

Q. Define normal subgroups, simple group

* Normal Subgroups :-

A subgroup H of a group $(G, *)$ is said to be a normal subgroup of G if all $g \in G$ and all $h \in H$.

$$g * h * g^{-1} \in H$$

Simple Group :- A group G is said to be simple group if it has only two normal subgroups, $\{e\}$ & G.

Notes :

1] Every subgroup of an abelian group is normal

2] The intersection of normal subgroups is a normal subgroups

Eg.

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

$\therefore (2Z, +), (3Z, +)$ are normal subgroups of $(Z, +)$

Q. Define Quotient groups.

* Quotient Groups :-

Let $(G, *)$ be a group and N be a normal subgroup of G. Let G/N be the collection of all cosets of N in G

$$G/N = \{N * a / a \in G\}$$

$(G/N, *)$ is called the quotient group or factor group.

Theorem 1] Prove that $(G/N, *)$ is a group.

2] Every cyclic group is an abelian group.

Q. Define Homomorphism of groups.

* Homomorphism of Groups:

Let $(G_1, *)$ and (G_2, o) be two groups. A function $f: (G_1, *) \longrightarrow (G_2, o)$ is said to be homomorphism

If $f(a * b) = f(a) \, o \, f(b)$ for all $a, b \in G_1$

i.e. $a * b$ in $G_1 \rightarrow f(a) \, o \, f(b)$ in G_2

Properties of Group Homomorphism

Let $f: G_1 \rightarrow G_2$ be group homomorphism & $(G_1, *)$ & (G_2, o) are groups then

i] $f(e_1) = (e_2)$

ii] $f(a^{-1}) = [f(a)]^{-1}$

Proof:

i] Let $a \in G_1$ and $f(a) G_2$ & e_2 is the identity element in G_2

$\therefore f(a) \, o \, e_2 = f(a)$

$= f(a * e_1)$

$f(a) \, o \, e_2 = f(a) \, o \, f(e_1)$

$\Rightarrow f(e_1) = e_2$

2] Let $a \in G_1$ then $a^{-1} \in G$

$e_2 = f(e_1)$

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

$e_2 = f(a) \, o \, f(a^{-1})$

$\Rightarrow f(a^{-1}) = [f(a)]^{-1}$

Q. Define Isomorphism groups.

* Isomorphism of Groups

Let $(G_1, *)$ & (G_2, o) be two groups. A function $f: (G_2, *) \rightarrow (G_2, o)$ is said to be isomorphism.

If i] f is a homomorphism from $G_1 \rightarrow G_2$

ii] f is bijective function.

If $f: G_1 \rightarrow G_2$ is an isomorphism of groups then G_1 & G_2 are called as isomorphic groups & denoted by $G_1 \cong G_2$

* An isomorphism from G to itself is called as automorphism of Group G.

Q. Let G be a group with identity e show that a function $f: G \to G$ defined by $f(a) \forall = e$, $a \in G$ is a homomorphism

→ We have $f: G \to G$ s.t.
$f(a) = e, \forall a \in G$

Let $a, b, G \Rightarrow f(a), f(b) \in G$

∴ $f(a * b) = e$
$= e * e$
$= f(a) * f(b)$

∴ f is a homomorphism.

* Rings, Integral Domains & Fields

In previous sect^n, we have discussed an algebric structure with a single binary operations, Now, we will study an algebric structures with two binary operations such as rings, integral domains & fields.

Q. Define Rings & properties of rings.

* Rings :-

Let R be a non empty set equipped with two binary operation called addition & multiplication & denoted by '+' & '.' respectively

An algebric structure $(R, +, \cdot)$ is called a ring if it satisfies following axioms.

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

i] closure property :-
for $a, b \in R$, $a + b \in R$

ii] Associativity
for $a, b, c \in R$
$a + (b + c) = (a + b) + c$

iii] Existance of identity :-
For any $a \in R$, $\exists\, 0 \in R$. $a + 0 = 0 + a = a$
∴ 0 is additive identity

iv] Existance of inverse :-

For each $a \in R$, $\exists -a \in R$ such that

$a + (-a) = -a + a = 0$

$-a$ is called additive inverse of a

v] Commutative Property :

for $a, b \in R$

$a + b = b + a$

2] $(R, \cdot)$ is semigroup i.e.

i] closure : $\forall A, b \in R$, $a.b \in R$

ii] Associativity,

for $a, b, c \in R$

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

3] multiplication distributes over addition

$\forall a, b, c \in R$

i] $a \cdot (b + c) = a \cdot b + a \cdot c$ (Right distributive law)

ii] $(a + b) \cdot c = a \cdot c + b \cdot c$ (left —//—)

* Commutative Ring

A ring $(R, +, \cdot)$ is said to be commutative ring if $\forall b \in R$, $a \cdot b = b \cdot a$

* Ring with Unity

A ring $(R, +, \cdot)$ is said to be ring with unity if $\forall a \in R$, $\exists$ $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$

*q. Propertics of Ring

If $(R, +, \cdot)$ is a ring with identity 0 and unit element 1 then following are true for all $a, b, c \in R$

i] $a \cdot 0 = 0 \cdot a = 0$

ii] $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

iii) $(-a) \cdot (-b) = a \cdot b$

iv] Unit element is unique.

* Subring :-

Let $(R, +, \cdot)$ be a ring. A non empty subset S of R is said to be subring of R if $(S, +, \cdot)$ is a ring. eg. $(Z, +, \cdot)$ is a subring of $(R, +, \cdot)$

Q. Define Integral domain & fields.

* Integral Domain.

A commutative ring with zero divisors is called an integral domain

eg. eg. $\bar{2}$ is a zero divisor in $(Z_4, +, \cdot)$

as $\bar{2} \cdot \bar{2} = \bar{4} = 0$

so $(Z_4, +, \cdot)$ is Integral domain

* Fields

A commutative ring with unity in which every non zero element possesses their multiplicative inverse is called as field

A field is an integral domain.

* Polynomial Ring

Let R be an arbitary ring & x an intermediate. The set of all polynomials $f(x)$

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

where the a_i's are elements of the ring R and only a finite number of them are equl to zero is called $R[x]$.

$R[x]$ from a ring w.r.t. addition & multiplication of polynomials & hence $R[x]$ is known as polynomial ring.

* Congruence of ring.

r is called a congruence on a groupoid $G = (G, \cdot_G)$ iff.

- r is a binary operation : $\mathbb{O} \subseteq G \times G$
- r is an equivalence
- $(a_1, a_2), (b_1, b_2) \in r \Rightarrow (a_1 \cdot_G b_1, a_2 \cdot_G b_2) \in r$

A factor groupoid of groupoid G according to the congruence r

$G/r = (G/r, \cdot^{G/r})$, $[a]_r \cdot^{G/r} [b]_r$

$= [a \cdot^{G} b]_r$

Ex.

$r \subseteq Z \times Z$; $r = \{(x/y); 3 \text{ divides } x-y\}$

r is a congruence of $(Z, +)$

·	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Q. Explain Group codes?

→ Group Codes :-

In communication, a code is a rule for converting a data (info. or msg) into another form or representation, not necessarily of the same type. In communication & info processing, encoding is the process by which data from a source is converted into some symbols to be communicated. Decoding is the reverse process of encoding.

Q. Explain Hamming distance

→ Hamming Distance

Let x be a word in S_n. The weight of x is denoted by $w(x)$ & defined as $w(x)$ = number of one's in x

eg. $w(0\ 0\ 1\ 0\ 0) = 2$, $w(0\ 0\ 0\ 0\ 0) = 0$

$w = (1\ 1\ 1\ 1\ 1) = 4$

Let $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ be any two elements in $(S_n, \oplus)$. The hamming distance between x & y is denoted by $d(x, y)$ & defined as

$d(x,y)$ = The no. of co-ordinates at which x_i & y_i are different.

$\therefore x = (1\ 0\ 1\ 1\ 0\ 1)$

$y = (0\ 1\ 1\ 1\ 1\ 0)$

$\therefore d(x,y) = 4$

* Generation of codes by using parity checks

* Find the minimum distance of an encoding function $e : B^2 \rightarrow B^5$ given by

$e(0\,0) = 0\,0\,0\,0\,0$, $e(0\,1) = 1\,0\,0\,1\,1$,
$e(1\,0) = 0\,1\,1\,1\,0$, $e(1,1) = 1\,1\,1\,1\,1$

Soln ::

$d[e(0,0), e(0,1)] = 3$
$d[e(0,0), e(1,1)] = 5$
$d[e(0,0), e(01)] = 3$
$d[e(0,0), e(10)] = 3$
$d[e(0,1), e(10)] = 3$
$d[e(01), e(11)] = 2$
$d(e(10), e(11)] = 2$

The minimum along all distance is 2
Thus the minimum distance of an encoding is 2