

# Unit VI

## **Algebraic Structures and Coding Theory**

# Topics

- The structure of algebra
- Algebraic Systems, Semi Groups, Monoids, Groups, Homomorphism and Normal Subgroups, and Congruence relations, Rings, Integral Domains and Fields
- Coding theory
- Polynomial Rings and polynomial Codes
- Galois Theory –Field Theory and Group Theory.

## Algebraic systems

- $N = \{1, 2, 3, 4, \dots, \infty\}$  = Set of all natural numbers.  
 $Z = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots, \infty\}$  = Set of all integers.  
 $Q$  = Set of all rational numbers.  
 $R$  = Set of all real numbers.
- **Binary Operation:** The binary operator  $*$  is said to be a binary operation (closed operation) on a non empty set  $A$ , if  
 $a * b \in A$  for all  $a, b \in A$  (Closure property).  
Ex: The set  $N$  is closed with respect to addition and multiplication  
but not w.r.t subtraction and division.
- **Algebraic System:** A set ' $A$ ' with one or more binary(closed) operations defined on it is called an algebraic system.  
Ex:  $(N, +)$ ,  $(Z, +, -)$ ,  $(R, +, \cdot, -)$  are algebraic systems.

# Algebraic Structure

- **Algebraic Structure (Set + Operation + Rules)**
- A non empty set  $S$  is called an algebraic structure w.r.t binary operation  $(*)$  if it follows following axiom (rules):
- **Closure:**  $(a*b)$  belongs to  $S$  for all  $a, b \in S$ .

**Ex :**  $S = \{1, -1\}$  is algebraic structure under  $*$

- As  $1*1 = 1$ ,  $1*-1 = -1$ ,  $-1*-1 = 1$  all results belongs to  $S$ .
- But above is not algebraic structure under  $+$  as  $1+(-1) = 0$  not belongs to  $S$ .

Q. Define Algebraic Structure?  
Algebraic 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 algebraic structure.



He will ~~see~~ define three common algebraic

structures. At the top level, we have a set  $A$ .

Common algebraic structure

$$x + y = y + x$$

$$x \times y = y \times x$$

Groups

Rings

Fields

## Properties

- **Commutative:** Let  $*$  be a binary operation on a set  $A$ .  
The operation  $*$  is said to be commutative in  $A$  if  
 $a * b = b * a$  for all  $a, b$  in  $A$
- **Associativity:** Let  $*$  be a binary operation on a set  $A$ .  
The operation  $*$  is said to be associative in  $A$  if  
 $(a * b) * c = a * (b * c)$  for all  $a, b, c$  in  $A$
- **Identity:** For an algebraic system  $(A, *)$ , an element ' $e$ ' in  $A$  is said to be an identity element of  $A$  if  
 $a * e = e * a = a$  for all  $a \in A$ .
- **Note:** For an algebraic system  $(A, *)$ , the identity element, if exists, is unique.
- **Inverse:** Let  $(A, *)$  be an algebraic system with identity ' $e$ '. Let  $a$  be an element in  $A$ . An element  $b$  is said to be inverse of  $a$  if  
 $a * b = b * a = e$

# Semi Group

- A non-empty set  $S$ ,  $(S, *)$  is called a semigroup if it follows the following axiom:
- **Closure:**  $(a*b)$  belongs to  $S$  for all  $a, b \in S$ .
- **Associativity:**  $a*(b*c) = (a*b)*c \quad \forall a, b, c \text{ belongs to } S$ .

Note: A semi group is always an algebraic structure.

- $(\mathbb{N}, +)$  is a semi group.
- $(\mathbb{N}, \cdot)$  is a semi group.
- $(\mathbb{N}, -)$  is not a semi group..... **WHY? ( $3-5 = -2$ , and  $-2$  does not belong to  $\mathbb{N}$ )**



# Identity element

- The element of a set of numbers that when combined with another number in a particular operation leaves that number unchanged.
- For example, **0 is the identity element under addition** for the real numbers, since if  $a$  is any real number,  $a + 0 = 0 + a = a$ .
- Similarly, **1 is the identity element under multiplication** for the real numbers, since  $a \times 1 = 1 \times a = a$ .

## Identity Element

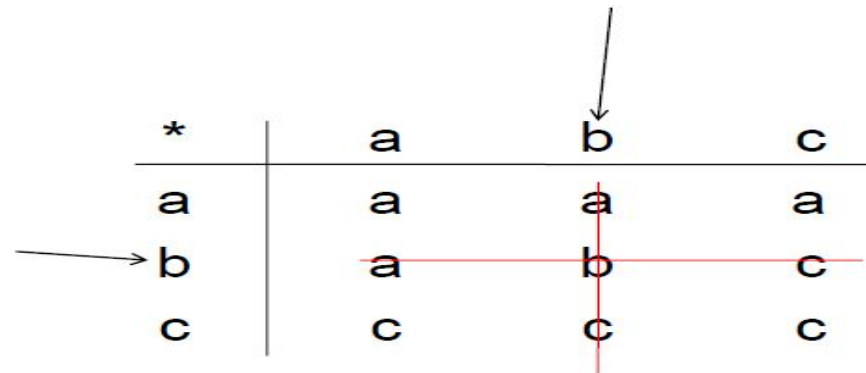
Left Identity  
 $e * X = X$

Right Identity  
 $X * e = X$

Identity Element  
 $e * X = X * e = X$

# Monoid

## Identity Element



A Cayley table for a monoid with three elements: a, b, and c. The table is a 3x3 grid with a header row and header column. The header row is labeled with the operation '\*' and the elements a, b, c. The header column is labeled with the elements a, b, c. The body of the table contains the results of the operation. The element 'b' is the identity element, as shown by the red lines highlighting the row and column where the result is the same as the input. An arrow points to the row labeled 'b' on the left, and another arrow points to the column labeled 'b' at the top.

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

Left Identity – Rows - b

Right Identity – Column – b

Identity Element – b

# Monoid



- A non-empty set  $S$ ,  $(S, *)$  is called a monoid if it follows the following axiom:
- - Closure:**  $(a * b)$  belongs to  $S$  for all  $a, b \in S$ .
  - **Associativity:**  $a * (b * c) = (a * b) * c \quad \forall a, b, c \text{ belongs to } S$ .
  - **Identity Element:** There exists  $e \in S$  such that  $a * e = e * a = a \quad \forall a \in S$
- Note: A monoid is always a semi-group and algebraic structure.

# Monoid

- Examples:
- Ex : (Set of integers,  $*$ ) is Monoid as 1 is an integer which is also identity element .
- (Set of natural numbers,  $+$ ) is not Monoid as there doesn't exist any identity element. But this is Semigroup.
- But (Set of whole numbers,  $+$ ) is Monoid with 0 as identity element.

# Monoid

- Let  $E = \{0, 2, 4, 6, \dots\}$   
 $(E, +)$  is monoid ---?

$+$	 0	2	4	6
 0	0	2	4	6
2	2	4	6	8
4	4	6	8	10
6	6	8	10	12



# Homomorphism of groups

- Let  $(G,o)$  &  $(G',o')$  be 2 groups, a mapping “f ” from a group  $(G,o)$  to a group  $(G',o')$  is said to be a homomorphism if –

$$f(aob) = f(a) o' f(b) \quad \forall a,b \in G$$

The mapping  $f : G \rightarrow G'$  may neither be a one-one nor onto mapping, i.e, ‘f’ needs not to be bijective.

- **Example –**

If  $(\mathbb{R}, +)$  is a group of all real numbers under the operation '+' &  $(\mathbb{R} - \{0\}, *)$  is another group of non-zero real numbers under the operation '\*' (Multiplication)

- $f$  is a mapping from  $(\mathbb{R}, +)$  to  $(\mathbb{R} - \{0\}, *)$ ,

- $f(a) = 2^a$  ;  $\forall a \in \mathbb{R}$

Then  $f$  is a homomorphism like –

- $f(a+b) = 2^{a+b} = 2^a * 2^b = f(a).f(b)$  .

So the rule of homomorphism is satisfied & hence  $f$  is a homomorphism.

- **Homomorphism Into –**

A mapping 'f', that is homomorphism & also Into.

- **Homomorphism Onto –**

A mapping 'f', that is homomorphism & also onto.

- **Isomorphism of Group :**

Let  $(G,o)$  &  $(G',o')$  be 2 groups, a mapping "f " from a group  $(G,o)$  to a group  $(G',o')$  is said to be an isomorphism if –

1.  $f(aob) = f(a) o' f(b) \forall a, b \in G$
2.  $f$  is a one- one mapping
3.  $f$  is an onto mapping.

If 'f' is an isomorphic mapping,  $(G,o)$  will be isomorphic to the group  $(G',o')$  & we write

$$G \cong G'$$

**Note :** A mapping  $f: X \rightarrow Y$  is called :

1. One – One – If  $x_1 \neq x_2$ , then  $f(x_1) \neq f(x_2)$  or if  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ . Where  $x_1, x_2 \in X$
2. Onto – If every element in the set  $Y$  is the  $f$ -image of at least one element of set  $X$ .
3. Bijective – If it is one & Onto.

# Normal Subgroups

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

$$g * h * g^{-1} \in H. \quad (\text{We may write } g h g^{-1} \in H)$$

# Congruence relations

- If  $n$  is a positive integer, we say the integers  $a$  and  $b$  are congruent modulo  $n$  and write  $a \equiv b \pmod{n}$
- if they have the same remainder on division by  $n$
- 7 and 15 are congruent modulo 4: Since  $7 - 15 = -8$ , which is a multiple of 4.
- 17 and 5 are congruent modulo 3: Since  $17 - 5 = 12$ , which is a multiple of 3



# Rings

- The ring is a type of algebraic structure  $(R, +, \cdot)$  or  $(R, *, \cdot)$  which is used to contain non-empty set  $R$ . Sometimes, we represent  $R$  as a ring. It usually contains two binary operations that are **multiplication and addition**.
- An algebraic system is used to contain a non-empty set  $R$ , operation  $\circ$ , and operators  $(+ \text{ or } *)$  on  $R$  such that:
- $(R, \circ)$  will be a semigroup, and  $(R, *)$  will be an algebraic group.
- The operation  $\circ$  will be said a ring if it is distributive over operator  $*$ .

# Rings

- **Right distributive law**

- $(y + z) \cdot x = y \cdot x + z \cdot x$

- **Left distributive law**

- $x \cdot (y + z) = x \cdot y + x \cdot z$

- Types of Ring

# Rings

- **Null ring**

- A ring will be called a zero ring or null ring if singleton  $\{0\}$  is closed with the binary operator  $(+ \text{ or } *)$ . The null ring can be described as follows:
  - $0 + 0 = 0$  and  $0 \cdot 0 = 0$

- **Commutative ring**

- The ring  $R$  will be called a commutative ring if multiplication in a ring is also commutative, which means  $x$  is the right divisor of zero as well as the left divisor of zero. The commutative ring can be described as follows:
  - $x \cdot y = y \cdot x$  for all  $x, y \in R$

# Rings

- **Ring with unity**

- The ring will be called the ring of unity if a ring has an element  $e$  like this:
- $e.x = x.e = x$  for all  $x \in R$

- **Ring with zero divisor**

- If a ring contains two non-zero elements  $x, y \in R$ , then the ring will be known as the divisor of zero. The ring with zero divisors can be described as follows:
- $y.x = 0$  or  $x.y = 0$

# Rings

- **Ring without zero divisor**

- If products of no two non-zero elements is zero in a ring, the ring will be called a ring without zero divisors. The ring without zero elements can be described as follows:

- $xy = 0 \Rightarrow x = 0$  or  $y = 0$
- Properties of Rings
- All  $x, y, z \in R$  if  $R$  is a ring

1.  $(-x)(-y) = xy$

2.  $x0 = 0x = 0$

3.  $(y-z)x = yx - zx$

4.  $x(-y) = -(xy) = (-x)y$

5.  $x(y-z) = xy - xz$

# Integral Domains

- A non-trivial ring (ring containing at least two elements) with unity is said to be an integral domain if it is commutative and contains no divisor of zero ..

A commutative ring with a unity and no zero divisors. This means that if  $a \cdot b = 0$ , then either  $a = 0$  or  $b = 0$ .



# Fields

A commutative ring with a unity where every non-zero element has a multiplicative inverse. ⓘ

Every field is an integral domain, but not every integral domain is a field. For example, the ring of integers is an integral domain but not a field. ⓘ