Design and Analysis of Algorithms

Vandana M L
Department of Computer Science & Engineering

DESIGN AND ANALYSIS OF ALGORITHMS

Algebraic Structures - Rings, Fields and Groups

Vandana M L

Department of Computer Science & Engineering

Algebra

Algebra is about operations on sets

Algebraic structure

An algebraic structure is a set S together with zero or more operations, each of which is a function from $S^k \rightarrow S$ for some k. The value k is called the arity of the operation

i.e.

Algebraic structure is a collection of objects and one or more operations that can be performed on those objects

Importance of Algebraic Structures

- Discover new systems with similar properties
- Prove theorems about all the systems with similar properties
- Define mathematical models to study real world phenomenon
- Generalization of systems

Algebraic Structures: Categorization

Based on properties of the operations

- Groups
- Field
- Rings
- Vector spaces

etc.

Algebraic Structures: Categorization

Based on number of operations

- Algebraic Systems with one binary operation
  - Semigroups
  - Monoids
  - Groups

- Algebraic Systems with two binary operation
  - Rings
  - Integral Domains
  - Fields

Groups

A group $(S, \oplus)$ is a set S together with binary operation $\oplus$ defined on S for which the following properties hold :

1. Closure :

   For all $a, b \in S$, $a \oplus b \in S$.

2. Identity :

   There exists an element $e \in S$, called the identity of the group,

   $a \oplus e = e \oplus a = a$ for all $a \in S$.

3. Associativity :

   For all $a, b, c \in S$, we have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

4. Inverse :

   For each $a \in S$, there exists a unique element $b \in S$, called the inverse of 'a', such that

   $(a \oplus b) = (b \oplus a) = e$

Abelian Group : A group $(S,\oplus)$ is said to be 'Abelian Group', if it satisfies the commutative property.

$$(a \oplus b) = (b \oplus a)$$

Finite Group : A group $(S,\oplus)$ is said to be 'Finite Group', if it satisfies the property.

$$|S| < \infty$$

Sub-Group : If $(S,\oplus)$ is a group, and $S' \subseteq S$ and $(S',\oplus)$ is also a group, then $(S',\oplus)$ is a subgroup of $(S',\oplus)$

Generators: A set $T \subseteq S$ is said to generate the group $G = (S, \oplus)$ if every element of S can be expressed as a finite product of elements in T

Groups: Examples

- numbers (integer, rational, real, complex) with addition
- integers with addition modulo m (finite group)
- integers relatively prime to m with modulo m multiplication
- permutations of a finite set (not commutative)
- translations and rotations of the plane (not commutative)

Definition:

A ring R is a set together with two binary operations + and x, satisfying the following properties:

1. (R,+) is a commutative group

2. x is associative

3. The distributive laws hold in R:

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

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

Rings: Examples

- Integer Rings

  The set of all even integers, positive, negative, and zero, under the operations arithmetic addition and multiplication is a ring.

- Matrix Rings

  The set of all N × N square matrices over the real numbers under the operations of matrix addition and matrix multiplication constitutes a ring.

- Polynomial Rings

  Polynomials of the form $a_0 + a_1x + a_2x^2 + \cdots$ under the operation of addition and multiplication constitutes a ring

Fields

Definition:

A field F is a set together with two binary operations + and *, satisfying the following properties:

1. (F,+) is a commutative group

2. (F-{0},*) is a commutative group

3. The distributive law holds in F:

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

Importance of Algebraic Structures

- The set of all real numbers under the operations of arithmetic addition and multiplication is a field.

- The set of all rational numbers under the operations of arithmetic addition and multiplication is a field.

- The set of all complex numbers under the operations of complex arithmetic addition and multiplication is a field.

THANK YOU

Vandana M L
Department of Computer Science & Engineering

vandanamd@pes.edu