Discrete Mathematics (ITPC-309)

Algebraic Structures - Part I

Mrs. Sanga G. Chaki

Department of Information Technology

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar

Contents

Algebraic Structures - Definition

1. In mathematics, an algebraic structure consists of
    a) a nonempty set A, also called the underlying set, carrier set or domain,
    b) a collection of operations on A (typically binary operations such as addition and multiplication),
    c) and a finite set of identities, known as axioms, that these operations must satisfy.
2. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.
3. Eg. Suppose * is a binary operation on set G. Then (G, *) is an algebraic structure.
4. Eg. (R, +, .) is an algebraic structure equipped with two operations.

Binary Operation on a Set

1. A binary operation can be understood as a function f (x, y) that applies to two elements of the same set S, such that the result will also be an element of the set S.
2. Examples of binary operations are the addition of integers, multiplication of whole numbers
3. Suppose G is a non-empty set.
4. Let there is an operation G X G = {(a,b) : a E G, b E G)}.
5. If f : G X G → G then f is called a binary operation on a set G.
6. The image of the ordered pair (a,b) under the function f is denoted by afb.
7. Example: An addition is a binary operation on the set N of natural number. The sum of two natural number is also a natural number.
8. Is Subtraction a binary operation on N?

Properties of an Algebraic Structure

1. By a property of an algebraic structure, we mean a property possessed by any of its operations.
2. Important properties of an algebraic system are:
   a) Closure
   b) Associativity
   c) Commutativity
   d) Existence of identity
   e) Existence of inverse
   f) Cancellation Laws
3. Different types of algebraic structures satisfy some or all of these properties.

Closure

1. Consider a non empty set G and a binary operation (•)
2. Closure:
   - If a and b are elements of G, then c = a • b is also an element of G.
3. Example: S = {1,-1} is algebraic structure under binary operation * . Does it satisfy the closure property?
   - As 1*1 = 1, 1*-1 = -1, -1*-1 = 1 all results belong to S.
   - So it satisfies the closure property.
4. Example: Consider set S = {1,-1} and binary operation + . Does it satisfy the closure property?
   - No, as 1+(-1) = 0 not belongs to S. → It is not an algebraic structure.
5. All algebraic structures must follow closure property.

Associativity

1. Consider a non empty set G and a binary operation (•)
2. Associativity:
   - If a, b, and c are elements of G, then (a • b) • c = a • (b • c)
3. (G, •) is called a **semigroup** if it follows both closure and associativity.
4. Example: (Set of integers, +)
5. A semi-group is always an algebraic structure.

Existence of identity element

1. Consider a non empty set G and a binary operation (•)
2. Identity element:
   - For all a in G, there exists an element e, called the identity element, such that e • a = a • e = a.
3. (G, •) is called a **monoid** if it follows closure, associativity, and identity element.
4. Example:
   - (Set of integers,*) is Monoid as 1 is an integer which is also an 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.
5. A monoid is always a semi-group and algebraic structure. .

Existence of Inverse element

1. Consider a non empty set G and a binary operation (•)
2. Identity element:
   - For each a in G, there exists an element a′, called the inverse of a, such that a • a′ = a′ • a = e.
3. (G, •) is called a **group** if it follows closure, associativity, identity element and inverse element.
4. Example:
   - (Set of integers,+) is group. What are the identity and inverse element?
5. A group is always a monoid, semigroup, and algebraic structure.

Commutativity

1. Consider a non empty set G and a binary operation (•)
2. Commutativity:
   - For all a and b in G, we have a • b = b • a.
3. (G, •) is called an **abelian** group or **commutative** group if it follows closure, associativity, identity element, inverse element and commutativity.
4. Every abelian group is a group, monoid, semigroup, and algebraic structure.
5. Find an example of an abelian group.

Group

1. A group is called a **finite group** if the set has a finite number of elements; otherwise, it is an **infinite group**
2. The **order of a group**, $|G|$, is the number of elements in the group.
3. Subgroups: A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G
4. Cyclic Subgroup: If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.
5. Cyclic Group: A cyclic group is a group that is its own cyclic subgroup

Ring

1. A ring, denoted as $R = <\{\ldots\}, \bullet, \square>$, is an algebraic structure with two operations.
2. The first operation must satisfy all five properties required for an abelian group.
3. The second operation must satisfy only the first two.
4. The second operation must be distributed over the first.
5. Distributivity means that for all a, b, and c elements of R, we have

$$a \square (b \bullet c) = (a \square b) \bullet (a \square c) \text{ and } (a \bullet b) \square c = (a \square c) \bullet (b \square c)$$

6. **A commutative ring is a ring in which the commutative property is also satisfied for the second the operation**.

Field

1. A field, denoted by $F = <\{\ldots\}, \bullet, \square >$ is a commutative ring in which the second operation satisfies all five properties defined for the first operation.
2. Except that the identity of the first operation (sometimes called the zero element) has no inverse
3. Finite field - field with a finite number of elements
4. Very important structure in cryptography.
5. **Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer**.
6. **The finite fields are usually called Galois fields and denoted as GF(p^n).**

To do:

1. Given the following sets and the binary operations of addition, multiplication, subtraction and division, find which of the combinations of (set, operations) belong to which category described above.
   - N=Set of Natural Number
   - Z=Set of Integer
   - R=Set of Real Number
   - E=Set of Even Number
   - O=Set of Odd Number