Unit 6: Algebraic Structures

Topic 1: Monoid, Semigroup, and Group

Outline

1. Introduction
   - Topics to be covered
   - Applications and Objectives
2. Basics of algebraic structures
   - Binary operation
   - Properties of binary operation
3. Semigroup, Monoid, and Group
   - Subgroup
   - Order of an element
   - Problems

Introduction

Computer Science basically deals with real world problems of communications and security. In certain real world phenomenon, a suitable mathematical model is required to represent, and then study of the model becomes important to understand the phenomenon.

Algebraic structures are certain mathematical structures based on sets equipped with binary operations to represent different models of computer science.

The main topics to be covered in this module are

1. Binary operations
2. Semi-group, Monoids, and group
3. Cyclic group
4. Group homomorphism
5. Rings, fields, and lattices.

Applications and Objectives

There are many applications of combinatorics in computer science. For example,

1. Cryptography
2. Coding theory
3. Automata Theory
4. Formal language

To understand basic concepts of different algebraic structures.

Outline

1. Introduction
   - Topics to be covered
   - Applications and Objectives
2. Basics of algebraic structures
   - Binary operation
   - Properties of binary operation
3. Semigroup, Monoid, and Group
   - Subgroup
   - Order of an element
   - Problems

Basics of algebraic structures

An algebraic structure has the following components:

- A non-empty set.
- Operations defined on the set.
- Special elements of the set possessing special properties, called constants (generally identity).

Binary operation

Definition (Binary Operation)

Let S be a non-empty set. Then a binary operation $*$ on S is a function $*: S \times S \to S$.

For example, addition $(+)$, multiplication $(\times)$ are binary operations on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. However, subtraction $(-)$ is not binary operation on $\mathbb{N}$, division $(\div)$ is not binary operation $\mathbb{Q}$, but in $\mathbb{Q}^{\times}$.

If $*$ is a binary operation defined on a set S with constant c, then the corresponding algebraic structure is denoted by $(S, *, c)$.

If two algebras have the same number of operations, same number of constants, and the operations are of the same **arity**, we call that both the algebras are of same **signature or species**.

Properties of binary operation

Based on the additional properties satisfied by a binary operation $*$ (or $*$ and $\oplus$) on a set A, the binary operations are classified as follows:

1. **Commutative binary operation:** $a * b = b * a$ for all $a, b \in A$.
2. **Associative binary operation:** $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$.
3. **Distributive binary operations:** $a * (b \oplus c) = a * b \oplus a * c$ and $(a \oplus b) * c = a * c \oplus a * c$ for all $a, b, c \in A$.

If a number of algebras satisfy a set of properties, together with signature, then we call the algebras of same **variety**.

Elements under binary operation

Definition (Identity Element)

Let $*$ be a binary operation defined on a set S. Then an element e of S is said to be a **left identity (or right identity)** for $*$ in S if $e * x = x$ (or $x * e = x$) for all $x \in S$.

For example, the right identity of $a * b = a + 2b$ is 0, but left inverse does not exist (not unique) in $\mathbb{Z}$.

Theorem

If both left and right identity of an algebraic structure exist, then both are equal (called identity).

Elements under binary operation

Definition (Inverse Element)

Let $*$ be a binary operation defined on a set S with identity e. If $x * y = e$ for $x, y \in S$, then x is called **right inverse** of y and y is called **left inverse** of x. If $x * y = y * x = e$, then x and y are called inverse of each other.

In multiplication of matrices, there are elements having different right inverse and left inverse.

Theorem

If an element has both right and left inverse with respect to an associative binary operation, then left and right inverse elements are equal (called inverse).

Outline

1. Introduction
   - Topics to be covered
   - Applications and Objectives
2. Basics of algebraic structures
   - Binary operation
   - Properties of binary operation
3. Semigroup, Monoid, and Group
   - Subgroup
   - Order of an element
   - Problems

Monoid, Semigroup, and Group

Based on properties satisfied by an algebraic structure $(S, *)$, we have the following kinds of varieties:

- **Semigroup:** $*$ is binary operation on S and $*$ is associative in S.
- **Monoid:** $*$ is binary operation on S, $*$ associative in S, and identity element exist of $*$ in S.
- **Group:** $*$ is binary operation on S, $*$ associative in S, identity element exist of $*$ in S, and every element of S has inverse with respect to $*$.

It is easy to see that

$$\text{Group} \Rightarrow \text{Monoid} \Rightarrow \text{Semigroup},$$

but the converse is not true.

Monoid, Semigroup, and Group

Based on properties satisfied by an algebraic structure $(S, *)$, we have the following kinds of varieties:

- **Semigroup:** $*$ is binary operation on S and $*$ is associative in S.
- **Monoid:** $*$ is binary operation on S, $*$ associative in S, and identity element exist of $*$ in S.
- **Group:** $*$ is binary operation on S, $*$ associative in S, identity element exist of $*$ in S, and every element of S has inverse with respect to $*$.

It is easy to see that

$$\text{Group} \Rightarrow \text{Monoid} \Rightarrow \text{Semigroup},$$

but the converse is not true.

$(\mathbb{Z}, -, 0)$ is not semigroup, $(\mathbb{N}, +, 0)$ is semigroup but not monoid, and $(\mathbb{N}, \times, 1)$ is monoid but not group.

Monoid, Semigroup, and Group

Based on properties satisfied by an algebraic structure $(S, *)$, we have the following kinds of varieties:

- **Semigroup:** $*$ is binary operation on S and $*$ is associative in S.
- **Monoid:** $*$ is binary operation on S, $*$ associative in S, and identity element exist of $*$ in S.
- **Group:** $*$ is binary operation on S, $*$ associative in S, identity element exist of $*$ in S, and every element of S has inverse with respect to $*$.

It is easy to see that

$$\text{Group} \Rightarrow \text{Monoid} \Rightarrow \text{Semigroup},$$

but the converse is not true.

$(\mathbb{Z}, -, 0)$ is not semigroup, $(\mathbb{N}, +, 0)$ is semigroup but not monoid, and $(\mathbb{N}, \times, 1)$ is monoid but not group.

Some obvious examples of groups are
$(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}^{\times}, \times, 1), (\mathbb{Z}_n, +_n, \bar{0}), (\mathbb{Z}_p, \times_p, \bar{1})$ if p is prime.

Definition

The number of elements present in a group is called **order of the group**. The order an infinite group is undefined.

If a group is of finite order *n*, then we can display all axioms of the group with the help of a $n \times n$ table, called **Caylay table**.

Ex: Construct a Caylay table for algebra $(\{1, \omega, \omega^2\}, *, 1)$, and show that this is a group.

Subgroup

Definition

Let $(G, *, e)$ be a group and H be a subset of G. If $(H, *, e)$ is also a group, then $(H, *, e)$ is called a **subgroup** of $(G, *, e)$.

For example, $(\mathbb{Z}, +, 0)$ is a subgroup of $(\mathbb{Q}, +, 0)$, both of which are subgroup of $(\mathbb{R}, +, 0)$. However, $(\mathbb{Z}_n, +_n, \bar{0})$ is never a subgroup of $(\mathbb{Z}_m, +_m, \bar{0})$ if $m \neq n$.

Subgroup

Theorem (Subgroup Criterion)

1. *Let* $(G, *, e)$ *be a finite group and* H *a nonempty subset of* G*, then* $(H, *, e)$ *is a subgroup of* $(G, *, e)$ *if* $a * b \in H$ *for all* $a, b \in H$.
2. *Let* $(G, *, e)$ *be a group and* H *a nonempty subset of* G*. Then,* $(H, *, e)$ *is a subgroup of* $(G, *, e)$ *if* $ab^{-1} \in H$ *for all* $a, b \in H$.

Order of an element

Definition (Order of an Element)

The order of an element a in a group $(G, *, e)$ with identity e is the smallest positive integer n such that $g^n := g * g * \cdots * g = e$. If no such integer exists, we say a has infinite order. The order of an element a is denoted by $|a|$ or $\mathrm{o}(a)$.

For example,

1. the identity element always has order 1.
2. the order of $1, \omega$, and ω^2 in $(\{1, \omega, \omega^2\}, \times, 1)$ are 1,3,3, respectively.
3. all elements of $(\mathbb{Z}, +, 0)$, except 0, has infinite order.

Problems:

1. Find values of n so that $\mathbb{Z}_n^{\times}$ is a group with respect to (i) addition modulo n (ii) multiplication modulo n.

Problems:

1. Find values of n so that $\mathbb{Z}_n^{\times}$ is a group with respect to (i) addition modulo n (ii) multiplication modulo n.
2. Construct Cayley table to show that the set $\{1, -1, i, -i\}$ is a group with respect to complex number multiplication. Find identity, inverse of each element, and order of each element.

Problems

1. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Find inverse and identity of each element.

Problems

1. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Find inverse and identity of each element.
2. Let G be a group and $a \in G$. Then the set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G generated by a.

Problems

1. Let G be a group and $a, b \in G$. Show that $(ab)^{-1} = b^{-1}a^{-1}$. Under what condition on G, $(ab)^{-1} = a^{-1}b^{-1}$.

Problems

1. Let G be a group and $a, b \in G$. Show that $(ab)^{-1} = b^{-1}a^{-1}$. Under what condition on G, $(ab)^{-1} = a^{-1}b^{-1}$.
2. Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$.

Thank You

Any Question!!!