Discrete Structures (Monsoon 2021)

Ashok Kumar Das

Associate Professor
IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

Group Theory

Algebraic System

Definition

A system consisting of a set and one or more *n*-ary operations on the set is called an **algebraic system** or simply an *algebra*.

An algebraic system is denoted by $\langle S, f_1, f_2, \cdots \rangle$, where S is a non-empty set and $f_1, f_2, \cdots$ are operations defined on S. For example, $f_1 = +$, $f_2 = \times$.

Groupoid

Definition

A non-empty set S with binary composition $\circ$ is called a *groupoid*, if $a, b \in S$, then $a \circ b \in S$.
In other words, $\langle S, \circ \rangle$ is groupoid if S is closed under the composition $\circ$, that is,
[**Closure**] $a \circ b \in S, \forall a, b \in S$.

Example

Let N be the set of natural numbers. Then, $(N, +)$ is a groupoid, since N is closed under addition $+$.

Example

The set $S = \{-2, -1, 0, 1, 2\}$ is NOT a groupoid under addition $+$, since S is not closed under $+$.
For example, $2 + 2 = 4 \notin S$

Semigroup

Definition

A structure $[S, \circ]$ with binary operation $\circ$ is said to be a *semigroup*, if it satisfies the following properties:

(i) **Closure:** $\forall s_1, s_2 \in S, s_1 \circ s_2 \in S$.

(ii) **Associativity:** $\forall s_1, s_2, s_3 \in S, s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$.

Identity

Definition

Let $[S, \circ]$ with binary operation $\circ$ be a structure. Then,

- e_l is the left identity if $e_l \circ s = s, \forall s \in S$.
- e_r is the right identity if $s \circ e_r = s, \forall s \in S$.
- e is the identity if $e \circ s = s$ and $s \circ e = s$, $\forall s \in S$, that is, $e \in S$ is both left and right identity.

Monoid

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Definition

A structure $[S, \circ]$ with binary operation $\circ$ is said to be a *monoid*, if it satisfies the following properties:

(i) **Associativity:** $\forall s_1, s_2, s_3 \in S$, $s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$.

(ii) **Existence of Identity:** $\exists e \in S$, $e \circ s = s \circ e = s$, $\forall s \in S$.

Cycle Semigroup and Monoid

Definition

A structure $[S, \circ]$ with binary operation $\circ$ is said to be a *cyclic semigroup*, if $\exists g \in S$ such that $S = \{g^n | n \in P\}$, where P is the set of positive integers and $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$.

Definition

A structure $[M, \circ, e]$ with binary operation $\circ$ and identity element $e \in M$ is said to be a *cyclic monoid*, if $\exists g \in M$ such that $M = \{g^n | n \in N_0\}$, where N_0 is the set of non-negative integers, that is, $N_0 = N \cup \{0\}$ $= \{0, 1, 2, 3, \ldots\}$ and $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$.

Inverse

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition

Let $[S, \circ]$ with binary operation $\circ$ be a structure. Then,

- $i_l \in S$ is the left inverse of $s \in S$ if $i_l \circ s = e$.
- $i_r \in S$ is the right inverse of $s \in S$ if $s \circ i_r = e$.
- $i \in S$ is the inverse of $s \in S$ if $i \circ s = e$ and $s \circ i = e$, that is, $i \in S$ is both left and right inverse of $s \in S$.

Group

Definition

A group $(G, \circ)$ is a set of elements with a binary operation $\circ$ that associates to each ordered pair (a, b) of elements of G to an element $a \circ b$ in G, such that the following axioms are obeyed:

- **(A1) Closure:** If $a, b \in G$, then $a \circ b \in G$.
- **(A2) Associativity:** If $a, b, c \in G$, then $a \circ (b \circ c) = (a \circ b) \circ c$.
- **(A3) Identity Element:** $\forall a \in G, \exists e \in G$ such that $e \circ a = a \circ e = a$. $e \in G$ is called the identity (left as well as right) of G.
- **(A4) Inverse Element:** For each $a \in G$, there exists an $a^{-1} \in G$, such that $a^{-1} \circ a = a \circ a^{-1} = e$.
  a^{-1} is called the inverse (left as well as right inverse) element in G.

Note: A group $(G, \circ)$ is a monoid with each element in G having an inverse in G.

Group

Definition

A group $(G, \circ)$ is said to be an *abelian* (or commutative) if it satisfies the additional condition:

- **(A5) Commutative:** $a \circ b = b \circ a, \forall a, b \in G$.

Definition

A group $(G, \circ)$ is *cyclic* if every element is of the form g^k (k is a positive integer) of a fixed element $g \in G$. The element g is said to be a *generator* of the group G.

Quasi-group

Definition

A groupoid $(S, \circ)$ is said to be a quasi-group, if for any two elements $a, b \in S$, each of the equations:

$$a \circ x = b$$

and

$$y \circ a = b$$

has a UNIQUE solution in S.

Example

The groupoid $(Z, +)$, where Z is the set of all integers, is a quasi-group, since for $a, b \in Z$, $a + x = b$ and $y + a = b$ have the unique solution $x = y = (b - a) \in Z$.

Group

Problem: Show that the set $S = \{-1, 1, i, -i\}$, where $i = \sqrt{-1}$, with binary composition $\times$ (ordinary multiplication) is a cyclic group.

Group

Problem: Let $[S, \cdot]$ be a semigroup in which $\forall a, b \in S$, $\exists x, y \in S$ such that $x \cdot a = b$ and $a \cdot y = b$. Then, S is a group.