Lecture 5: Monoids, Groups, and Their Properties

Summary:

We explore the fundamental structures of monoids and groups. We begin with the multiplication table for the symmetric group S_3. We define binary operations and their properties: identity, associativity, commutativity, and inverses. We define monoids as sets with an associative binary operation and an identity element, with examples from matrices and integers. We investigate invertibility in monoids and define groups as monoids where every element is invertible. We prove the uniqueness of inverses and the cancellation lemma. We show that the symmetric group is a group under composition and provide guidelines for checking if a structure is a group.

Topics Covered: closure of operations, group, monoid, symmetric group

Multiplication table for S_3:

	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(1)(2)(3)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3)(2)$
$(1,3,2)$	$(1,3,2)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3)(2)$	$(2,3)(1)$	$(1,2)(3)$
$(1,2)(3)$	$(1,2)(3)$	$(1,3)(2)$	$(2,3)(1)$	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$
$(1,3)(2)$	$(1,3)(2)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3,2)$	$(1)(2)(3)$	$(1,2,3)$
$(2,3)(1)$	$(2,3)(1)$	$(1,2)(3)$	$(1,3)(2)$	$(1,2,3)$	$(1,3,2)$	$(1)(2)(3)$

Groups

Definition: A binary operation $(\cdot)$ on a set A is a function $A \times A \to A$.

Operations may satisfy

1. $\exists e \in A. \forall a \in A. \;\; a \cdot e = e \cdot a = a$
    - Identity
2. $\forall a, b, c \in A. \; a \cdot (b \cdot c) = (a \cdot b) \cdot c$
    - Associative
3. $\forall a, b \in A. \; a \cdot b = b \cdot a$
    - Commutative
4. If identity e exists, then we may have $\forall a \in A. \; \exists a^{-1} \in A. \; a \cdot a^{-1} = a^{-1} = e$
    - Inverse

Suppose that $(\cdot)$ is a binary operation on A and has identities $e, e' \in A$.

Note that we have

$$\begin{gathered} e' = e' \cdot e = e \\ \implies e = e' \end{gathered}$$

Therefore, identity is unique.

Definition: A monoid is a set M together with binary operation on M such that

1. $\exists e \in A. \forall a \in A. \;\; a \cdot e = e \cdot a = a$
    - Identity
2. $\forall a, b, c \in A. \; a \cdot (b \cdot c) = (a \cdot b) \cdot c$
    - Associative

- Examples of monoid
  - 2×2 real-valued matrices with $+$
    - Matrices with $\det M = 0$ do not have an inverse
  - $(\mathbb{Z}, +)$
  - $(\mathbb{Z}, \cdot)$
    - 0 does not have an inverse

Invertibility in a monoid: Let $(M, \cdot)$ be a monoid. We say that element $a \in M$ is **invertible** means $\exists b \in M$ such that $a \cdot b = b \cdot a = e$ where $e \in M$ is the identity element of M.

Examples of monoids:

- In $(\mathbb{Z}, \cdot)$ the set of invertible elements is $\{1, -1\}$
- $(\mathcal{M}_2(\mathbb{R}), \cdot)$
  - The set of 2×2 real-valued matrices
  - The set of invertible elements is 2 $\times$ 2 matrices with nonzero determinant

Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$$

is invertible $\iff ad - bc \neq 0$.

Proposition (uniqueness of inverses):

Let $(M, \cdot)$ be a monoid. If $b, b' \in M$ are both inverses of $a \in M$, then $b = b'$.

Proof:

We know that

$$b' \cdot \underbrace{(a \cdot b)}_{e} = \underbrace{(b' \cdot a)}_{e} \cdot b$$
$$\implies b' \cdot e = e \cdot b$$
$$\implies b' = b$$
$$QED$$

Let's denote the unique inverse of a as a^{-1} or $(-a)$.

Lemma (a monoid always has at least one invertible element):

Let $(M, \cdot)$ be a monoid.

Then, we know that e is invertible. Moreover, $e^{-1} = e$, since $e \cdot e = e$.

Cancellation lemma:

Let $a \in M$ be an invertible element of the monoid $(M, \cdot)$. Let $x, x' \in M$. Then,

$$a \cdot x = a \cdot x' \implies x = x'$$

Proof:

Multiply on the left by a^{-1}

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot a \cdot x'$$
$$\implies e \cdot x = e \cdot x'$$
$$\implies x = x'$$

$$QED$$

Example:

Let $a \in M$ be invertible. Let $c \in M$. Consider the equation

$$a \cdot x = c$$

$$a \cdot x = c = a \cdot (a^{-1} \cdot c)$$

Therefore, this equation does have a solution. It is $a^{-1} \cdot c$.

Definition:

A group is a monoid $(M, \cdot)$ such that every element $a \in M$ is invertible.

Proposition:
$(S_n, \cdot)$ is a group, where $\cdot$ is composition.

Proof:

1. $S_n \times S_n \to S_n$ (closed) since composition of bijections is a bijection
2. $\text{id} = (1)(2). \dots (n)$
3. Associativity of composition
4. Existence of inverses
   - Follows from the theorem that a function has an inverse $\iff$ it's a bijection

$(S_n, \cdot)$ is called the **symmetric group**.

Note that each row and each column of the multiplication table of $(S_n, \cdot)$ have unique elements because of the cancellation property, since each $\sigma \in S_n$ is invertible.

Checking if something is a group:

1. Closure
   - $(\cdot)$ is a binary operation
2. Identity element
3. Associative
4. Existence of inverses

Examples of groups:

- $(\{(1)(2)(3)\}, \circ)$
- $(\{(1)(2)(3), (1,2)(3)\}, \circ)$