Linear Algebra and Applications

Sartaj Ul Hasan

विद्याधनं सर्वधन प्रधानम्

Department of Mathematics
Indian Institute of Technology Jammu
Jammu, India - 181221

Email: sartaj.hasan@iitjammu.ac.in

Lecture 10

(Aug 08, 2019)

Sets

Definition of Set

A set is the collection of "<u>well-defined</u>" objects.

Note that this is merely a "working definition" of a set. The word 'well-defined' means that there should not be any ambiguity in determining the fact the whether the object belongs to set or not.

- A set is denoted by Capital Letters.
- Objects that belongs to set are called "elements".
- Elements are denoted by small letters.
- If a is an element of set A, then mathematically it can be represented by $a \in A$ and read as " a belongs to set A".

Standard Notations

- The set of natural numbers consists of the positive whole numbers:

$$\mathbb{N} = \{1, 2, 3, \cdots\}$$

- The set of integers consists of zero and the positive and negative whole numbers:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

- The set of rational numbers contains all fractions of the form a/b where a and b are integers and $b \neq 0$. Two rational numbers a/b and c/d are equal exactly when $ad = bc$. The set of rational numbers will be denoted by $\mathbb{Q}$.
- Two other sets of importance: the set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$.
- $\mathbb{Q}^* := \mathbb{Q} - \{0\}, \mathbb{R}^* := \mathbb{R} - \{0\}$, and $\mathbb{C}^* := \mathbb{C} - \{0\}$
- $\mathbb{Z}_p := \{0, 1, 2, \cdots, p-1\}$ and $\mathbb{Z}_p^* := \mathbb{Z}_p - \{0\}$, p is a prime number.

Cartesian Product of Sets

Let A and B be two sets. The set $A \times B$ which is collection of all ordered pair (a, b) such that $a \in A$ and $b \in B$ is called Cartesian product of set A and B.

Example Let $A := \{1, 2, 3\}$ and $B := \{a, b, c\}$ then
$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)(3, a), (3, b)(3, c)\}$.

Definition of Binary operation

Let S be a set. The rule of assigning elements of $S \times S$ to unique elements of set S is called *binary operation*.
$* : S \times S \to S$ is called binary operation.

Example: Addition, multiplication, subtraction are binary operation on set $\mathbb{Z}$.

- The rule of assigning the elements of a set A to elements of set B in such a way that no two elements of set B are assigned to an element of set A is called *mapping*.
- The fact that image of $(s, t) \in S \times S$ must be in set S is known as *closure property*

Algebraic structure or algebraic system

A set S together with one or more operations on S is called *Algebraic structure or algebraic system*. Mathematically it can be represented by tuples like $(set, operations)$.

Example: $(\mathbb{Z}, +)$ and $(\mathbb{N}, \cdot)$.

Groupoid, Semigroup, Monoid

An algebraic structure consisting of a non-empty set and a binary operation defined on it is called *groupoid*.

An algebraic structure consisting of a non-empty set with associative binary operation is called *semigroup*.

A semi group is called *monoid* if there exist unique identity element.

Properties of Operations

Properties of Operations on a Set S: Let $*$ be an operation on a set S.

1. $*$ is said to be **closed** on S provided $a * b \in S$ for all $a, b \in S$. (NB: if $*$ is closed on S, it will be called a composition on S.)
2. $*$ is said to be **associative** on A provided $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.
3. $*$ is said to be **commutative** on A provided $a * b = b * a$ for all $a, b \in S$.
4. An element $e \in S$ is said to be an **identity element** (or **neutral element**) for $*$ provided $a * e = e * a = a$ for all $a \in S$.

   Remark: There can be at most one identity element for an operation $*$ on a set S.
5. Suppose that the operation $*$ on the set S has an identity element e, and suppose that $a \in S$. An element b is said to be an inverse of a provided $a * b = b * a = e$.

Groups

- **Definition**: Let $*$ be an operation on a non-empty set G. We call the pair $(G, *)$ a group provided:
  1. The operation $*$ is closed on G, that is, $g * h \in G$ for all $g, h \in G$.
  2. The operation $*$ is associative, that is, $(g * h) * k = g * (h * k)$ for all $g, h, k \in G$.
  3. There is an identity element $e \in G$ such that $g * e = e * g = g$ for all $g \in G$.
  4. For every element $g \in G$, there is an inverse element $h \in G$, such that $g * h = h * g = e$.
- **Notation**: To have a group, we need to have both a set G and an operation on G. We can use any suitable symbol for the operation; if it is a previously known operation, we may use the standard symbol. If we are talking about general groups, we will use either $*$ or $\cdot$ or no symbol at all.
- **Definition**: Let $(G, *)$ be a group. If the operation $*$ is also commutative, the group will be called an **abelian group**. Groups which are not abelian are sometimes referred to as **nonabelian**.

Properties of Groups

Proposition

Let $(G, *)$ be a group.

(a) The identity element of G is unique.

(b) The inverse element of any element of G is unique.

[**Remarks**: In view of uniqueness of the inverse, we may use the notation a^{-1} for the inverse of a.]

(c) Cancellation Law: for $a, b, c \in G$, if $a * b = a * c$, then $b = c$.

(d) The equations $a * x = b$ and $x * a = b$, where $a, b \in G$, have the solutions $x = a^{-1} * b$ and $x = b * a^{-1}$ respectively.

(e) For $a \in G$, and n a positive integer, define $a^n := a * a * \cdots * a$ (n times), $a^{-n} := a^{-1} * a^{-1} * \cdots * a^{-1}$ (n times) and $a^0 := e$ (identity element of the group G). Then the usual exponentiation laws hold, i.e. $a^m * a^n = a^{m+n}, a^m * a^{-n} = a^{m-n}$ and $(a^m)^n = a^{mn}$.

(d) For $a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$

Examples of Groups

1. $(\mathbb{Z}, +)$ is an abelian group.
2. $(\mathbb{Q}, +)$ is an abelian group.
3. $(\mathbb{R}, +)$ is an abelian group.
4. $(\mathbb{C}, +)$ is an abelian group.
5. $(\mathbb{Q} - \{0\}, \times)$ is an abelian group.
6. $(\mathbb{R} - \{0\}, \times)$ is an abelian group.
7. $(\mathbb{C} - \{0\}, \times)$ is an abelian group.

Remark: All of the above are groups which are familiar from before - in all these groups, the underlying set is infinite. Such groups are known as infinite groups.

- Note that: $(\mathbb{Z}, \times)$ is NOT a group.
- Note that: $(\mathbb{Q}, \times)$ is NOT a group.
- Note that: $(\mathbb{R}, \times)$ is NOT a group.
- Note that: $(\mathbb{C}, \times)$ is NOT a group.