EE 174 Course : Introduction to linear algebra

Kamel Hariche, Professor, IGEE- UMBB

May 2020

Preface

This book presents some of the fundamental concepts of linear algebra taught in the course entitled $EE174$ at the IGEE Institute of the university of Boumerdes.

Chapter 1

Basic Algebraic Structures

This chapter covers briefly some of the basic algebraic structures needed in linear algebra.

1.1 Sets

The most fundamental structure is the **set** which can be defined as a collection of objects called **elements** of the set. If a is an element of the set A,we write $a \in A$. Clearly the notation $b \notin A$ means that b is not an element of A.

A set is specified either by listing all its elements such as in $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ or by providing rules characterizing its elements such as in $S = \{x/ax^2+bx+c = 0\}$. Notice the curly brackets used to denote sets.

Some of the most commonly used sets are sets of numbers : $\mathbb{N}$ (natural numbers), $\mathbb{Z}$ (integers), $\mathbb{R}$(real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Q}$ (rational numbers). A particular set is the **empty** or **void** set denoted $\varnothing$ containing no elements.

The number of elements of a set is called the **cardinality** of the set.

1.1.1 Subsets

Definition 1 *B is a subset of the set A if and only every element of B is an element of A written as $B \subset A$*

This can be expressed as $B \subset A \Leftrightarrow [\forall b \in B \Rightarrow b \in A]$. Clearly every set is a subset of itself and $\varnothing$ is a subset of any set. When dealing with sets it is convenient to define a **reference** set or the **universe** U so that all sets under consideration are subsets of U.

If we define U, say, as the population of IGEE , then the student body or the faculty body are subsets of U.

1.1.2 Set operations

We can use some operations on sets to construct or generate other sets

Union:

Given the sets A, B we define their union, denoted $A \cup B$ as $A \cup B = \{x/x \in A$ **or** $x \in B\}$. Clearly elements of $A \cup B$ are elements of A or elements of B. The union operation can be extended to more than just two sets as in $A_1 \cup A_2 \cup \cdots \cup A_n = \{x/x \in A_1$ **or** $x \in A_2$ **or**$\cdots$ $x \in A_n\}$.

Intersection:

Given the sets A, B we define their union, denoted $A \cap B$ as $A \cup B = \{x/x \in A$ **and** $x \in B\}$. Clearly elements of $A \cap B$ are elements of A and elements of B. The intersection operation can be extended to more than just two sets as in $A_1 \cap A_2 \cap \cdots \cap A_n = \{x/x \in A_1$ **and** $x \in A_2$ **and**$\cdots$ $x \in A_n\}$. Clearly $A \cap B = \varnothing$ means that A and B have no elements in common.

Complement:

Given the set A in the universe U, we define the complement of A, denoted $\overline{A}$, as $\overline{A} = \{x \in U/x \notin A\}$. We may notice that $A \cap \overline{A} = \varnothing$.

Cartesian product

Given the sets A, B we define their Cartesian product , denoted $A \times B$, as $A \times B$,$= \{(a, b)/a \in A$ **and** $b \in B\}$. It is worth mentioning that the **order** in the pair (a, b) is important. Thus $A \times B$, is a set of **ordered pairs** meaning that $A \times B \neq B \times A$ in general.

Example 2 *Given the set of real numbers $\mathbb{R}$, we can form the Cartesian product $\mathbb{R} \times \mathbb{R} = \{(x, y)/x, y \in \mathbb{R}\}$ representing the Euclidian plane in geometry. For convenience we denote $\mathbb{R} \times \mathbb{R}$ as $\mathbb{R}^2$.*

Here again , we can extend the Cartesian product to more than two sets such as in $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n/a_i \in A_i\}$ where we obtain a set of **ordered n-tuples**.

Example 3 *If L is a set of last names , F a set of first names and A a subset of $\mathbb{N}$ for ages , we can form the Cartesian product $L \times F \times A$ where each element is an ordered triple consisting respectively of the last name, the first name and the age.*

1.2 Groups

Starting with a set, we can construct a more involved algebraic structure called the **group**.

Definition 4 *A group consists of a* ***non-empty*** *set G along with a binary operation denoted $*$ satisfying the following axioms:*
i) $\forall a, b \in G$, *we have* $a * b \in G$ *called the* ***closedness*** *property*
ii) $\forall a, b, c \in G$, *we have* $(a * b) * c = a * (b * c)$ *called the* ***associativity*** *property*
iii) $\exists e \in G$ *called* ***identity element*** *such that* $a * e = e * a = a \quad \forall a \in G$
iv) $\forall a \in G, \exists\ a^{-1} \in G$ *called* ***inverse*** *such that* $a * a^{-1} = a^{-1} * a = e$

It is worth mentioning that the operation $(*)$ may not be commutative , i.e. $a * b \neq b * a$. It follows that , in this case, we may have to differentiate between a **right** identity element and a **left** one. The same goes with the inverse. The closedness property insures that the result of the binary operation on any two elements of G will result in another element of G. The associativity property allows to extend the binary operation to more than two elements. It can be shown (exercise) that the identity element and the inverse are unique. The group constructed this way is denoted as $(G, *)$.

Example 5 *Consider $\mathbb{N}$ along with the arithmetic operation $(+)$, is $(\mathbb{N}, +)$ a group? Clearly it is not since $a^{-1} = (-a)$ is not a natural number. On the other hand we can check that $(\mathbb{Z}, +)$ satisfies all the axioms, thus it is a group.*

A group $(G, *)$.is said to be a commutative or an **Abelian** group if the binary operation $(*)$ is commutative i.e., $a * b = b * a. \quad \forall a, b \in G$. Clearly for an abelian group

the right and left identity elements are identical. So is the case for the inverse.

1.3 Rings and Fields

1.3.1 Rings

Definition 6 *A ring is a non-empty set R along with two binary operations called* ***addition*** $(+)$ *and* ***multiplication*** $(\cdot)$ *satisfying the following axioms:*
i) $\forall a, b \in R$, *we have* $a + b \in R$
ii) $\forall a, b \in R$, *we have* $a + b = b + a$
iii) $\forall a, b, c \in R$, *we have* $(a + b) + c = a + (b + c)$
iv) $\exists 0 \in R$ *called* ***zero element*** *such that* $a + 0 = 0 + a = a \quad \forall a \in R$
v) $\forall a \in R, \exists\ (-a) \in R$ *called* ***additive inverse*** *such that* $a + (-a) = (-a) + a = 0$
vi) $\forall a, b, c \in R$, *we have* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
vii) $\forall a, b, c \in R$, *we have* $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$

Clearly the first five axioms indicate that $(R,+)$ is an abelian group. To this Abelian group, we define a second binary operation (multiplication) that must be associative and distributive with respect to addition both on the right and on the left.

If the second operation $(\cdot)$ is also commutative i.e. $a \cdot b = b \cdot a$ for all $a, b \in R$ we say that $(R,+,\cdot)$ is a **commutative ring**. Furthermore, if the second operation $(\cdot)$ has an identity element denoted 1 such that $a \cdot 1 = 1 \cdot a = a$ for any $a \in R$, we say that $(R,+,\cdot)$ is a commutative ring with **unit element** 1.

Example 7 *Consider* $\mathbb{Z}$ *along with the arithmetic operations* $(+)$ *and* $(\times)$ *; Is* $(\mathbb{Z},+,\times)$ *a ring? If so, what type of ring? We have seen earlier that* $(\mathbb{Z},+)$ *is a group. Moreover it is an Abelian group. It can easily be checked that associativity of* $(\times)$ *and its distributivity with respect to* $(+)$ *hold, hence* $(\mathbb{Z},+,\times)$ *is a ring. It is a commutative with unit element the integer* 1.

Example 8 *Consider the set of real polynomials of degree* $\leq n$ *i.e.* $P_n = \{p(x)/p(x) = a_0 + a_1x + \cdots + a_nx^n\}$. *Using polynomial addition* $(+)$ *and multiplication* $(\times)$, *check that we can form a commutative ring with unit element* $(P_n,+,\times)$. *It must be noted here that the zero element is the zero polynomial ;i.e.* $0(x) = 0 + 0x + \cdots 0x^n$ *while the unit element is the polynomial* $1(x) = 1 + 0x + \cdots + 0x^n$

1.3.2 Fields

Essentially a field is a commutative ring with unit element where each **nonzero element** has a multiplicative inverse. Hence given a non-empty set F along with two binary operations addition $(+)$ and multiplication $(\cdot)$ forming a commutative ring with unit element $(F,+,\cdot)$ then $(F,+,\cdot)$ is a **field** if and only if for any $a \neq 0$ in F there exits an element a^{-1} in R such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ where 1 is the unit element of $(F,+,\cdot)$.

Elements of a field will be called **scalars** and used extensively in linear algebra.

Example 9 *In the example above , we have seen that* $(P_n,+,\times)$ *is a commutative ring with unit element. However it cannot be a field as the inverse of a polynomial is not necessarily another polynomial: is is a rational function in* x.

Example 10 *It can checked that* $(\mathbb{R},+,\times)$ *and* $(\mathbb{C},+,\times)$, *where* $(+,\times)$ *are the usual arithmetic operations, are fields. In fact these two fields are the most used fields in linear algebra.*

The common fields $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ are simply referred to respectively as the **real** and **complex** fields.. To simplify notation we simply write the real field $\mathbb{R}$ or the complex field $\mathbb{C}$.

We can define a **subfield** $(S,+,\cdot)$ of the field $(F,+,\cdot)$ as any subset $S \subset F$ that satisfies all the axioms of a field along under the inherited binary operations $(+)$ and $(\cdot)$