MTL104 : Linear Algebra **Spring 2020-21**

Lecture 1

Date : 3 Feburary 2021 Scribe: Dhananjay Kajla

Note: *LaTeX template courtesy of UC Berkeley EECS dept.*

Disclaimer: These notes are **unofficial** and were meant for personal use. Therefore accuracy of these notes are not guaranteed. And therefore the liability for any factual errors does not lie with either the author or the instructor.

1.1 Definitions

1.1.1 Subfield

- A subfield of a field K is a subset L of K that is a field with respect to the field operations inherited from K.
- Example : $\mathbb{R}$ is a subfield of $\mathbb{C}$

1.1.2 Characteristic of a field

- If F is a field, it may be possible to add the unit element($\mathbf{1}$) to itself a finite number of times to obtain $\mathbf{0}$. That is,

$$\mathbf{1} + \mathbf{1} + \mathbf{1} + ... + \mathbf{1} = \mathbf{0}$$

- This is not possible in the field of complex numbers.
- In such cases where it is not possible to obtain $\mathbf{0}$ by adding $\mathbf{1}$ a finite number of times then the field F is a field of *characteristic zero.*
- Otherwise, the least n such that adding $\mathbf{1}$ n times results in $\mathbf{0}$ is called the *characteristic* of the field.

1.1.3 Ring

- A ring is a set R with two binary operations $+, \cdot$ such that :
    1. Both operations are closed.
    2. R is *abelian* under addition.
    3. Multiplication is distributed over addition on both left and right.
    4. Multiplication is associative
- Note that $\mathbf{1}$ might not be an element of the ring.
- In case $\mathbf{1} \in R$, then R is called a ring with unity.
- A commutative division ring is called a field.

1.1.4 Finite Fields

- If the number of elements in a field is finite, then the field is called a finite field.
- Example : If $\mathbb{Z}_n = \{x; 0 \leq x < n\}$, then Z_p is a finite field if p is a prime number.
- Also note that Z_4 is not a field.

1.2 Vector Spaces

1.2.1 Definition

- Elements of a field are called scalars.
- $(V, +, \cdot)$ is called a vector space over a field K if :
- $\cdot : V \times V \to V$ and $+ : V \times V \to V$ exist, such that :
  1. $(V, +)$ is an abelian group.
  2. $\alpha \in F$ and $x, y \in V$, then : $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$
  3. $\alpha, \beta \in F$ and $x \in V$, then : $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$
  4. $\alpha, \beta \in F$ and $x \in V$, then : $(\alpha\beta) \cdot x = \alpha(\beta \cdot x)$
  5. $\forall x \in V$, $\mathbf{1} \cdot x = x$
- Example : n-tuple space

1.2.2 Example

- Take n-tuple space as an example.
- Let V be the set of all ordered n-tuples of elements of any field F for a fixed integer n. That is,

$$V = \{(a_1, a_2, ..., a_n) : a_i \in F\}$$

- Then V is a vector space over F, with the following $\cdot$ and $+$:
  1. Let $x = (a_1, a_2, ..., a_n)$ and $y = (b_1, b_2, ..., b_n)$
  2. $x + y = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$ (Addition)
  3. $\alpha x = (\alpha a_1, \alpha a_2, ..., \alpha a_n)$ (Scalar Multiplication)
  4. $x = y$ iff $\forall i \in \{1, 2, ..., n\}, a_i = b_i$

1.2.3 Properties

1. A vector space over a field K can be regarded as a vector space over any of it's subfield(S) of F
2. F(F) is a vector space over any field F.
   - $\mathbb{R}$ is not a vector space over $\mathbb{C}$ as it is not closed under scalar multiplication.
3. Set f(x) of polynomials over a field F is a vector space. (With conventional addition and multiplication)

4. The set of all convergent sequences is a vector space over the field of real numbers.
5. The set of all finite matrices with real elements is a vector space over real numbers
6. Let K be an arbitrary field. Let X be any non-empty set. Consider the set V of all funcitons from X to K. The sum of any two functions $f, g \in V$ is the function $f + g \in V$ defined by :

$$(f + g)(x) = f(x) + g(x)$$

Where the scalar product with $\alpha \in K$, $f \in V$, $\alpha f \in V$ is defined by :

$$(\alpha f)(x) = \alpha f(x)$$

is a vector space over the field K.

1.2.4 Cartesian Product

- Suppose G is a non-empty set, Then :

$$G \times G = \{(a, b); a \in G, b \in G\}$$

1.2.5 Binary Operation

- If $f : G \times G \to G$, then f is said to be a binary operation on the set G
- We often use the symbols $+, \times, \cdot, \circ$, etc to denote binary operations.
- For e.g., '+' is a binary operation in G only iff

$$\forall a, b \in G,\ a + b \in G \text{ and a+b is unique}$$

1.2.6 Conventions

- $\mathbb{N}$ - Set of Natural Numbers
- $\mathbb{Z}$ - Set of Integers
- $\mathbb{Q}$ - Set of Rational Numbers
- $\mathbb{R}$ - Set of Real Numbers
- $\mathbb{C}$ - Set of Complex Numbers

1.2.7 Algebraic Structure or Algebraic System

- A non-empty set G equipped with one or more binary operations is called an algebraic structure.
- Suppose * is a binary operation on G, then $(G, *)$ is an algebraic structure.
- E.g.
  - $(\mathbb{N}, +)$
  - $(\mathbb{R}, +, \cdot)$

1.2.8 Group

- Suppose S is a non-empty set and let * be a binary operation defined on S.
- i.e. $* : S \times S \to S$
- We say $(S, *)$ is a group if it satisfies the following properties :
  - $\forall a, b, c \in S,\ a * (b * c) = (a * b) * c$
  - $\exists z \in S$ such that, $\forall a \in S, a * z = z * a = a$ (Identity)
  - $\forall a \in S,\ \exists a^{-1} \in S$such that, $a * a^{-1} = a^{-1} * a = z$ (Inverse)

1.2.9 Abelian/Commutative Group

- If $(S,*)$ is a group such that $\forall a,b \in S,\ a*b = b*a$ (* is Commutative), then $(S,*)$ is called an Abelian group or Commutative Group.

1.2.10 Field

- Suppose F is a non-empty set equipped with two binary operations called addition and multiplication, denoted by '+' and $'\cdot'$, respectively.
- That is, $\forall a,b \in F$, we have : $a+b \in F$ and $a \cdot b \in F$.
- Then the algebraic structure $(F,+,\cdot)$ is called a field, if the following properties are satisfied :
    1. Addition is commutative. i.e. $\forall a,b \in F,\ a+b = b+a$
    2. Addition is associative. i.e. $\forall a,b,c \in F,\ a+(b+c) = (a+b)+c$
    3. $\exists \mathbf{0} \in F$ (called zero), such that $\forall a \in F,\ a+\mathbf{0} = \mathbf{0}+a = a$
    4. $\forall a \in F,\ \exists(-a) \in F$, such that : $a+(-a) = \mathbf{0}$
    5. Multiplication is commutative. i.e. $\forall a,b \in F,\ a \cdot b = b \cdot a$
    6. Multiplication is associative. i.e. $\forall a,b,c \in F,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
    7. $\exists \mathbf{1} \in F$ (called zero), such that $\forall a \in F,\ a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$
    8. $\forall a \in F \setminus \{\mathbf{0}\},\ \exists a^{-1} \in F \setminus \{\mathbf{0}\}$, such that : $a \cdot a^{-1} = \mathbf{1}$
    9. Multiplication Distributes over addition, i.e. $\forall a,b,c \in F,\ a \cdot (b+c) = a \cdot b + a \cdot c$ (left distribution) and $\forall a,b,c \in F,\ (a+b) \cdot c = a \cdot c + b \cdot c$ (right distribution)
- Notice that property 1-4 essentially states that $(F,+)$ is abelian. Similarly properties 5-8 states that $(F,*)$ is abelian.
- Note that **0** is called that Zero element of the field(F) and **1** is called the Unity element of the field(F).
- Equivalently, $(F,+,\cdot)$ is a field iff
    1. (F, +) is an abelian group.
    2. (F, $\cdot$) is an abelian group.
    3. Addition and Multiplication are linked by distributive property for both left and right distribution.
- Equivalently, A commutative division ring is a field.