

Lecture 2

Date : 4 February 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.

2.1 Definitions

2.1.1 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}

2.1.2 Characteristic of a field

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

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

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

2.1.3 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 **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.

2.1.4 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 \mathbb{Z}_p is a finite field if p is a prime number.
- Also note that \mathbb{Z}_4 is not a field.

2.2 Vector Spaces

2.2.1 Definition

- Elements of a field are called scalars.
- $(V, +, \cdot)$ is called a vector space over a field K if :
 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. $\forall x \in V, 1 \cdot x = x$
- Example : n-tuple space

2.2.2 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,

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

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

2.2.3 Properties

1. A vector space over a field K can be regarded as a vector space over any of its 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 functions 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 .