510: **Fall 2019**

Lecture 3: Vector Spaces and Linear Spaces

Lecturer: L.J. Ratliff

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

References: Appendix A.2 & A.3 of **[C&D]**; Chapter 1 and 2 of **[Ax]**

1 A Review of Fields and Rings

Definition 1. A field $\mathbb{F}$ is an object consisting of a set of elements and two binary operations

1. addition $(+)$
2. multiplication $(\cdot)$

such that the following axioms are obeyed:

- *Addition $(+)$ satisfies the following*: for any $\alpha,\ \beta,\ \gamma \in \mathbb{F}$,
  - associative: $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$
  - commutative: $\alpha+\beta=\beta+\alpha$
  - $\exists$ identity element $0 \in \mathbb{F}$ such that $\alpha+0=\alpha$
  - $\exists$ inverse: $\forall \alpha \in \mathbb{F}$, $\exists(-\alpha) \in \mathbb{F}$ such that $\alpha+(-\alpha)=0$
- *Multiplication $(\cdot)$ satisfies the following*: for any $\alpha,\ \beta,\ \gamma \in \mathbb{F}$,
  - associative: $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma)$
  - commutative: $\alpha\cdot\beta=\beta\cdot\alpha$
  - $\exists$ identity element 1 such that $\alpha\cdot 1=\alpha \quad \forall\alpha\in\mathbb{F}$
  - $\exists$ inverse: $\forall\alpha\neq 0$, $\exists\alpha^{-1}$ such that $\alpha\cdot\alpha^{-1}=\alpha^{-1}\cdot\alpha=1$
  - distributive (over $(+)$):

$$\begin{aligned}\alpha\cdot(\beta+\gamma) &= \alpha\cdot\beta+\alpha\cdot\gamma\\ (\beta+\gamma)\cdot\alpha &= \beta\cdot\alpha+\gamma\cdot\alpha\end{aligned}$$

Note. Throughout this course, a field $\mathbb{F}$ is either $\mathbb{R}$ or $\mathbb{C}$. If not clear from context, assume $\mathbb{C}$ as it is the more general case.

DIY Exercise. Show that

- the polynomials in s w/ coefficients in $\mathbb{R}$ (denoted by $\mathbb{R}[s]$) is *not a field*
- strictly proper rational functions, denoted by $\mathbb{R}_{p,o}(s)$ is *not a field*

Definition 2 (Ring)**.** A ring is the same as a field *except* the multiplication operator is not commutative and there is no inverse for non-zero elements under the multiplication operator.

DIY Exercise. Show that the set $\{0, 1\}$ with

- $(\cdot)$ = binary AND
- $(+)$ = binary XOR

is a field.

2 Vector Spaces (or Linear Spaces)

Before formally defining a vector space, let's consider some examples.

- A plane (set of all pairs of real numbers): $\mathbb{R}^2 = \{(x, y)|\ x, y \in \mathbb{R}\}$
- More generally, $\mathbb{R}^n = \{(x_1, \ldots, x_n)|\ x_i \in \mathbb{R}, i \in \{1, \ldots, n\}\}$

Definition. A vector space $(V, \mathbb{F})$ is a set of vectors V, and a field of scalars $\mathbb{F}$, and two binary operations:

- vector addition '+'
- scalar multiplication '$\cdot$' (multiplication of vectors by scalars)

such that

– **addition.** is associative, commutative, $\exists$ identity element, $\exists$ inverse element
– **scalar multiplication.** distributes, $\exists$ multiplicative and additive identities

Examples.

1. $(\mathbb{F}^n, \mathbb{F})$ the space of n-tuples in $\mathbb{F}$ over the field $\mathbb{F}$ is a vector space. (i.e. $(\mathbb{R}^n, \mathbb{R})$, $(\mathbb{C}^n, \mathbb{C})$)

3 Vector subspaces (or linear subspaces)

Let $(V, \mathbb{F})$ be a linear space and W a subset of V (denoted $W \subset V$). Then $(W, \mathbb{F})$ is called a *subspace* of $(V, \mathbb{F})$ if $(W, \mathbb{F})$ is itself a vector space.

How to check if W is a subspace of V?

step 1. verify that W is a subset of V (thus W inherits the vector space axioms of V)

step 2. verify *closure* under vector addition and scalar multiplication—i.e. $\forall w_1, w_2 \in W$, $\forall \alpha \in \mathbb{F}$,

$$\alpha w_1 + \alpha w_2 \in W$$

This is equivalent to...

Defn. A subspace W of V is a subset of V such that

1. $0 \in W$
2. $u, v \in W \implies u + v \in W$
3. $u \in W$, $\alpha \in \mathbb{F} \implies \alpha u \in W$

Examples.

- Is $\{(x_1, x_2, 0) |\ x_1, x_2 \in \mathbb{F}\}$ is a subspace of $\mathbb{F}^3$? (e.g., is a plane in $\mathbb{R}^3$ is a subspace?)
- Prove that if W_1, W_2 are subspaces of V, then
  i) $W_1 \cap W_2$ is a subspace
  ii) $W_1 \cup W_2$ is *not* necessarily a subspace

4 Sums and Direct Sums

Suppose $W_1, \ldots, W_m$ are subspaces of V. The sum of the W_i's, denoted by $W_1 + \cdots + W_m$ is defined to be the set of all possible sums of elements in $W_1, \ldots, W_m$—i.e.,

$$W_1 + \cdots + W_m = \{w_1 + \cdots + w_m |\ w_i \in W_i, \forall i \in \{1, \ldots, m\}\}$$

DIY Exercise. Show the following:

$$W_1, \ldots, W_m \text{ subspaces of } V \implies \sum_{i=1}^{m} W_i \text{ subspace of } V$$

Example. Consider $U = \{(x, 0, 0) \in \mathbb{F}^3 |\ x \in \mathbb{F}\}$ and $W = \{(0, y, 0) \in \mathbb{F}^3 |\ y \in \mathbb{F}\}$. Show that $U + W = \{(x, y, 0)|\ x, y \in \mathbb{F}\}$ is a subspace of $\mathbb{F}^3$.

Suppose that $W_1, \dots, W_m$ are subspaces of V such that $V = W_1 + \dots + W_m$. We say that V is the direct sum of subspaces $W_1, \dots, W_m$, written as

$$V = W_1 \oplus \dots \oplus W_m$$

if each element of V can be written uniquely as a sum $w_1 + \dots + w_m$ where each $w_i \in W_i$.

Example. Consider $U = \{(x, y, 0) \in \mathbb{F}^3 |\ x, y \in \mathbb{F}\}$ and $W = \{(0, 0, z) \in \mathbb{F}^3 |\ z \in \mathbb{F}\}$. Then $\mathbb{F}^3 = U \oplus W$.

Proposition 1. Suppose that $U_1, \dots, U_m$ are subspaces of V. Then, $V = U_1 \oplus \dots \oplus U_m$ if and only if both the following conditions hold:

1. $V = U_1 + \dots + U_m$
2. the only way to write zero as a sum $u_1 + \dots + u_m$, where each $u_i \in U_i$ is by taking all the $u_i = 0$, $i \in \{1, \dots, m\}$.

Proposition 2. Suppose that U and W are subspaces of V. Then $V = U \oplus W$ if and only if $V = U + W$ and $U \cap W = \{0\}$.

Proof. **DIY Exercise.** □

5 Linear Independence and Dependence

Suppose $(V, \mathbb{F})$ is a linear space. A linear combination of vectors $(v_1, \dots, v_p)$, $v_i \in V$ is a vector of the form

$$\alpha_1 v_1 + \dots + \alpha_p v_p,\ \alpha_i \in \mathbb{F}$$

- The set of vectors $\{v_i \in V,\ i \in \{1, \dots, p\}\}$ is said to be linearly independent if and only if (iff)

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_p v_p = 0,\ \alpha_i \in \mathbb{F} \implies \alpha_i = 0,\ \forall i = 1, \dots, p$$

  where $\alpha_i \in F$.
- The set of vectors is said to be linearly dependent iff $\exists$ scalars $\alpha_i \in \mathbb{F}$, $i \in \{1, \dots, p\}$ *not all zero* such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_p v_p = 0$$

Example. Let $\mathbb{F} = \mathbb{R}$, $k \in \{0, 1, 2, \dots, n\}$, $f_k : [-1, 1] \to \mathbb{R}$ such that $f_k(t) = t^k$. Show that the set of vectors $(f_k)_{k=0}^n$ is linearly independent in $(\mathcal{F}_n([-1, 1], \mathbb{R}), \mathbb{R})$.

proof sketch.

$$(f_k)_0^n = \{f_0, f_1, \dots, f_n\}$$

Hence we need to show that, $\forall\ t \in [-1, 1]$,

$$\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \dots + \alpha_n t^n = 0 \implies \alpha_i = 0, \alpha_i \in \mathbb{R}$$

DIY Exercise. Finish proof.

Span. The set of all linear combinations of $(v_1, \dots, v_p)$ is called the span of $(v_1, \dots, v_p)$. We use the notation

$$\text{span}(v_1, \dots, v_p) = \left\{ \sum_{i=1}^{p} \alpha_i v_i \middle|\ \alpha_i \in \mathbb{F},\ i \in \{1, \dots, p\} \right\}$$

If $\text{span}(v_1, \dots, v_p) = V$, then we say $(v_1, \dots, v_p)$ **spans** V.

Note. If some vectors are removed from a linearly independent list, the remaining list is also linearly independent, as you should verify.

Dimension. The notion of a spanning set let us define **dimension**. If we can find a set of spanning vectors with finite cardinality for a space V, then V is said to be finite dimensional, and otherwise it is said to be infinite dimensional.

Example.
1. $(\mathbb{R}^{n\times n}, \mathbb{R})$, the space of $n \times n$ real valued matrices, has dimension n^2.
2. $\mathrm{PC}([0,1], \mathbb{R})$ is infinite dimensional. Indeed, this can be shown by showing it contains a subspace of infinite dimension: $\mathrm{span}\{(t \to t^n)_0^\infty\}$.

The following is an alternative representation of linear dependence. Indeed, it states that given a linearly dependent list of vectors, with the first vector not zero, one of the vectors is in the span of the previous ones and, furthermore, we can throw out that vector without changing the span of the original list.

Lemma 1. If $(v_1, \ldots, v_p)$ is a linearly dependent set of vectors in V with $v_1 \neq 0$, then there exists $j \in \{2, \ldots, p\}$ such that the following hold:

(a) $v_j \in \mathrm{span}(v_1, \ldots, v_{j-1})$

(b) if the j–th term is removed from $(v_1, \ldots, v_p)$, then the span of the remaining list equals $\mathrm{span}(v_1, \ldots, v_p)$

This lemma let's us prove a stronger result: the cardinality of linearly independent sets is always smaller than the cardinality of spanning sets.

Theorem 1. In a finite-dimensional vector space, the length of every linearly independent set of vectors is less than or equal to the length of every spanning set of vectors.

DIY Exercise. Construct a proof using the above lemma.

Proposition 3. Every subspace of a finite-dimensional vector space is finite dimensional.

You cannot embed an infinite dimensional space in a finite dimensional one.