Module 7: Linear Algebra I

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

July 21, 2023

Outline

Today:

- Vector spaces and subspaces
- Linear independence and bases
- Linear maps, null space, range

Vector spaces & subspaces

$\mathbb{F}$-vector space

Definition

We call V a **vector space** if the following hold:

(A) *Commutativity in addition:* $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ for all $\mathbf{u},\mathbf{v}\in V$

(B) *Associativity in addition:* $\mathbf{u}+(\mathbf{v}+\mathbf{w})=(\mathbf{u}+\mathbf{v})+\mathbf{w}$ for all $\mathbf{u},\mathbf{v},\mathbf{w}\in V$

(C) *Existence of a neutral element, addition:* There exists a vector $\mathbf{0}$ such that for any $\mathbf{v}\in V$, $\mathbf{0}+\mathbf{v}=\mathbf{v}$

(D) *Additive inverse:* For every $\mathbf{v}\in V$, there exists another vector, which we denote $-\mathbf{v}$, such that $\mathbf{v}+(-\mathbf{v})=\mathbf{0}$.

(E) *Existence of a neutral element, multiplication:* For any $\mathbf{v}\in V$, $1\times\mathbf{v}=\mathbf{v}$

(F) *Associativity in multiplication:* Let $\alpha,\beta\in\mathbb{F}$. For any $\mathbf{v}\in V$, $(\alpha\beta)\mathbf{v}=\alpha(\beta\mathbf{v})$

(G) Let $\alpha\in\mathbb{F},\mathbf{u},\mathbf{v}\in V$. $\alpha(\mathbf{u}+\mathbf{v})=\alpha\mathbf{u}+\alpha\mathbf{v}$.

(H) Let $\alpha,\beta\in\mathbb{F},\mathbf{v}\in V$. $(\alpha+\beta)\mathbf{v}=\alpha\mathbf{v}+\beta\mathbf{v}$.

Statistical Sciences
UNIVERSITY OF TORONTO

$\mathbb{F}$: field ($\mathbb{R}$ or $\mathbb{C}$)

Elements of the vector space are called vectors.
Most often we will assume $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$.

Example

The following are vector spaces:

- $\mathbb{R}^n$
- $\mathbb{C}^n$
- $C(\mathbb{R};\mathbb{R})$, continuous functions from $\mathbb{R}$ to $\mathbb{R}$
- $M_{n\times m}$, matrices of size $n \times m$
- $\mathbb{P}_n$ (polynomials of degree n, $p(x) = a_0 + a_1x + \ldots + a_nx^n$).

Lemma

For every $\mathbf{v} \in V$, $0\mathbf{v} = \mathbf{0}$.

Proof.

$$0\vec{v} = (0+0)\vec{v} = 0\vec{v} + 0\vec{v}$$

Add the additive inverse of $0\vec{v}$ to both sides: $\vec{0} = 0\vec{v}$

$\square$

Lemma

For every $\mathbf{v} \in V$, we have $-\mathbf{v} = (-1) \times \mathbf{v}$.

Proof.

We want to show $\vec{v} + (-1) \times \vec{v} = \vec{0}$.

$$\vec{v} + (-1) \times \vec{v} = (1 + (-1))\vec{v} = 0\vec{v} = \vec{0}$$

$\square$

Definition

A subset U of V is called a **subspace** of of V if U is also a vector space (using the same addition and scalar multiplication as on V).

Proposition

A subset U of V is a subspace of V if and only if U satisfies the following three conditions:

1. $\mathbf{0} \in U$
2. Closed under addition: $\mathbf{u}, \mathbf{v} \in U$ implies $\mathbf{u} + \mathbf{v} \in U$
3. Closed under scalar multiplication: $\alpha \in \mathbb{F}$ and $\mathbf{u} \in U$ implies $\alpha\mathbf{u} \in U$

Proof. ($\Rightarrow$) If $\mathcal{U}$ is a subspace of $\mathcal{V}$, then it is a vector space, so (1), (2), (3) hold.

($\Leftarrow$) Suppose (1), (2), and (3) hold. Let $\vec{v} \in \mathcal{U}$. Then taking $(-1) \times \vec{v}$ gives us the additive inverse of $\vec{v}$ by previous result and $(-1) \times \vec{v} \in \mathcal{U}$.

Other properties can be shown.

Linear (in)dependence and bases

Linear combinations

Definition

A linear combination of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of vectors in V is a vector of the form

$$\alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n = \sum_{k=1}^{n} \alpha_k \mathbf{v}_k$$

where $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$.

Span

Definition

The set of all linear combinations of a list of vectors $\mathbf{v}_1, ..., \mathbf{v}_n$ in V is called the **span** of $\mathbf{v}_1, ..., \mathbf{v}_n$, denoted $\text{span}\{\mathbf{v}_1, ..., \mathbf{v}_n\}$. In other words,

$$\text{span}\{\mathbf{v}_1, ..., \mathbf{v}_n\} = \{\alpha_1 \mathbf{v}_1 + ... + \alpha_m \mathbf{v}_n : \alpha_1, ..., \alpha_n \in \mathbb{F}\}$$

The span of the empty list is defined to be $\{\mathbf{0}\}$.

Basis

Definition

A system of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is called a basis (for the vector space V) if any vector $\mathbf{v} \in V$ admits a unique representation as a linear combination

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n = \sum_{k=1}^{n} \alpha_k \mathbf{v}_k.$$

Example

$\mathbb{R}^n$

- For $\mathbb{F}^n$, $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$ is a basis
- The monomials $1, x, x^2, \ldots, x^n$ form a basis for $\mathbb{P}_n$.

$\mathbb{P}_2 : 1, x, x^2$

Linear independence

Definition

A system of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in V is called *linearly independent* if

$$\sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \mathbf{0}$$

implies $\alpha_i = 0$ for all $i = 1, \ldots, n$.

Otherwise, we call the system *linearly dependent*.

Linear combinations $\alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n$ such that $\alpha_k = 0$ for every k are called trivial.

Spanning set

Definition

A system of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ in V is called *spanning* if any vector in V can be written as a linear combination of $\mathbf{v}_1, \dots, \mathbf{v}_n$. In other words,

$$V = \mathrm{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}.$$

Such a system is also often called generating or complete. The next proposition relates spanning and linearly independent to a basis.

Proposition

A system of vectors $\mathbf{v}_1, \ldots \mathbf{v}_n \in V$ is a basis if and only if it is linearly independent and spanning.

Proof. ($\Rightarrow$) Let $v_1, \ldots, v_n \in V$ be a basis. Let $v \in V$.

$\exists \alpha_i \in F$ s.t. $v = \sum_{i=1}^{n} \alpha_i v_n$. $\Rightarrow v_1, \ldots, v_n$ span V.

Since the representation is unique for each $v \in V$, $\vec{0} = 0v_1 + \ldots + 0v_n$ is the only way to choose α_i s.t. sum $= 0$.

$\therefore v_1, \ldots, v_n$ are linearly independent

$(\Leftarrow)$ Suppose $v_1, \ldots, v_n$ are linearly ind. & span V.

Let $v \in V$. Then since $v_1, \ldots, v_n$ span V, $\exists \alpha_i \in F$

s.t. $v = \sum_{i=1}^{n} \alpha_i v_i$.

We show α_i are unique by contradiction.

Suppose $\exists \beta_i, i=1, \ldots, n$, $\beta_i \neq \alpha_i$, such that

$v = \sum_{i=1}^{n} \beta_i v_i$.

Then $\vec{0} = v - v = \sum_{i=1}^{n} (\alpha_i - \beta_i) v_i$

By linear independence, $\alpha_i = \beta_i \; \forall i = 1, \ldots, n$

$\therefore$ the constants are unique

Proposition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ be spanning. Then $\mathbf{v}_1, \ldots, \mathbf{v}_n$ contains a basis.

Sketch of proof. If $v_1, \ldots, v_n \in V$ are linearly independent, then we're done. Otherwise, $\exists v_i$, $i = 1, \ldots, n$ such that $v_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} \alpha_j v_j$. Remove this v_i.

Repeat until the v_i that remain are linearly independent.

Definition

An $\mathbb{F}$-vector space V is called *finite dimensional* if there exists a finite list of vectors that span it, i.e. there exist $n \in \mathbb{N}$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ such that $V = \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Otherwise, we call V *infinite dimensional*.

Example

- $\mathbb{F}^n$, $M_{m\times n}$, $\mathbb{P}_n$ are examples of finite dimensional vector spaces
- The $\mathbb{F}$-vector space $\mathbb{P} = \{\sum_{i=1}^n \alpha_i x^i \ : \ n \in \mathbb{N}, \alpha_i \in \mathbb{F}, i = 1, \ldots, n\}$ is infinite dimensional.

Why? Suppose $\mathbb{P}$ is finite dimensional, $\exists\, p_1, \ldots, p_n$ that span $\mathbb{P}$. But $p_1, \ldots, p_n$ have a maximum degree, call it N. Then $x^{N+1} \notin \operatorname{span}\{p_1, \ldots, p_n\}$

Corollary

Every finite dimensional vector space has a basis.

This follows from the fact that every spanning set for a vector space contains a basis.

This can also be extended to infinite dimensional vector spaces, i.e. when we do not assume that there exists a finite spanning set. However, this relies on the Axiom of Choice and is beyond the scope of this course.

$\mathbb{R}^3$: $(1,2,0)$, $(3,1,1)$

Proposition

Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.

Proof.

Let $u_1, \dots, u_n$ be linearly independent vectors in U. Add the basis of U, $v_1, \dots, v_n$ to the set of vectors. Then we reduce it by previous result to a basis that contains the u_i.

Dimension

Proposition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis for V. Then $m = n$.

The proof is omitted,. It relies on the fact that the number of elements in linearly independent systems are always less than or equal to the number of elements in spanning systems.

Definition

Let V be a finite dimensional $\mathbb{F}$-vector space. The number of elements in a basis of V is called the *dimension* of V and is denoted $\dim(V)$.

By the previous definition, the notion of dimension is well-defined.

Dimension

Example

- $\dim(\mathbb{F}^n) = n$
- $\dim(\mathbb{P}_n) = n + 1$
- $\dim\{\mathbf{0}\} = 0$

Linear maps

Linear Maps

$T(\vec{u}+\vec{v}) = T(\vec{u}) + T(\vec{v})$

$T(\alpha\vec{u}) = \alpha T(\vec{u})$

Definition

A map from a vector space U to a vector space V is **linear** if

$$T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}) \quad \text{for any } \mathbf{u}, \mathbf{v} \in V,\ \alpha, \beta \in \mathbb{F}$$

Notation: $\mathcal{L}(U, V)$ is the set of all linear maps from $\mathbb{F}$-vector space U to $\mathbb{F}$-vector space V

Example

- Zero map

$0 : U \to V \quad \vec{u} \mapsto \vec{0}$

- Identity map

$I : V \to V \quad : \quad I\vec{v} = \vec{v} \quad \forall \vec{v} \in V$

- Differentiation

$D \in \mathcal{L}(\mathbb{P}(\mathbb{R}), \mathbb{P}(\mathbb{R}))$ polynomials

$Dp = p'$ $\quad D(\alpha f(x) + \beta g(x)) = \alpha f'(x) + \beta g'(x)$

Theorem

Suppose $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is a basis for U and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis for V. Then there exists a unique linear map $T : U \to V$ such that $T\mathbf{u}_j = \mathbf{v}_j$ for $j = 1, \ldots, n$.

Proof in book.

Theorem

Let $S, T \in \mathcal{L}(U, V)$ and $\alpha \in \mathbb{F}$. $\mathcal{L}(U, V)$ is a vector space with addition defined as the sum $S + T$ and multiplication as the product αT.

The proof follows from properties of linear maps and vector spaces. Note that the additive identity is the zero map.

Lemma

Let $T \in \mathcal{L}(U, V)$. Then $T(\mathbf{0}) = \mathbf{0}$.

Proof.

$$T(\vec{0}) = T(\vec{0} + \vec{0}) = T(\vec{0}) + T(\vec{0})$$

Add $-T(\vec{0})$ to both sides

$$\Rightarrow \vec{0} = T(\vec{0})$$

Null space and range

Definition

Let $T : U \to V$ be a linear transformation. We define the following important subspaces:

- *Kernel or null space*: $\text{null } T = \{\mathbf{u} \in U : T\mathbf{u} = 0\}$
- *Range*: $\text{range } T = \{\mathbf{v} \in V : \exists \mathbf{u} \in U \text{ such that } \mathbf{v} = T\mathbf{u}\}$

The dimensions of these spaces are often called the following:

- *Nullity*: $\text{nullity}(T) = \dim(\text{null}(T))$
- *Rank*: $\text{rank}(T) = \dim(\text{range}(T))$

Proposition

Let $T : U \to V$. The null space of T is a subspace of U and the range of T is a subspace of V.

Proof.

(i) Since $T(0) = 0$, 0 is in null T.

Let $u, v \in \text{null } T$, then $T(u+v) = T(u) + T(v)$

$= 0$

$\Rightarrow u+v \in \text{null } T$

Let $\alpha \in \mathbb{F}, v \in \text{null } T$. $T(\alpha u) = \alpha T(u) = 0$

$\Rightarrow \alpha u \in \text{null } T$

(ii) $T(0) = 0 \Rightarrow 0 \in \text{range } T$

Suppose $v_1, v_2 \in \text{range } T$. $\exists u_1, u_2 \in U$ such that

$T(u_1)=v_1, \quad T(u_2)=v_2$

$\Rightarrow T(u_1+u_2) = T(u_1)+T(u_2)=v_1+v_2.$

Example

(αu is similar)

Zero map from a vector space U to a vector space V:

- The null space is U
- The range is $\{\vec{0}\}$

Differentiation map from $\mathbb{P}(\mathbb{R})$ to $\mathbb{P}(\mathbb{R})$:

- The null space is constants
- The range is $\mathbb{P}(\mathbb{R})$

Definition (Injective and surjective)

Let $T : U \to V$. T is *injective* if $T\mathbf{u} = T\mathbf{v}$ implies $\mathbf{u} = \mathbf{v}$ and T is *surjective* if $\forall \mathbf{v} \in V$, $\exists \mathbf{u} \in U$ such that $\mathbf{v} = T\mathbf{u}$, i.e. if range $T = V$.

Theorem

$T \in \mathcal{L}(U, v)$ *is injective if and only if* null $T = \{\mathbf{0}\}$.

Proof. ($\Rightarrow$) Suppose T is injective. We know $\vec{0} \in \text{null}\, T$.

Suppose $\exists v \in \text{null}\, T$. Then $T(v) = 0 = T(0)$.

Since T is injective, $v = 0$.

$\therefore \text{null}\, T = \{\vec{0}\}$

($\Leftarrow$) Suppose $\text{null}\, T = \{\vec{0}\}$. Let $u, v \in U$ s.t.

$Tu = Tv$.

$\Rightarrow 0 = Tu - Tv = T(u - v)$

$\Rightarrow (u - v) \in \text{null}\, T$

$\Rightarrow u - v = 0 \quad \Rightarrow u = v$

Theorem (Rank Nullity Theorem)

Let $T : U \to V$ be a linear transformation, where U and V are finite-dimensional vector spaces. Then

$$\text{rank } T + \text{nullity } T = \dim U.$$

$$\dim(\text{range } T) + \dim(\text{null } T) = \dim U$$

Proof in the lecture notes (pg. 35).

References

Axler S. *Linear Algebra Done Right*. 3rd ed. Undergraduate Texts in Mathematics. Springer, 2015. Available from: https://link.springer.com/book/10.1007/978-3-319-11080-6

Treil S. *Linear Algebra Done Wrong*. 2017. Available from: https://www.math.brown.edu/streil/papers/LADW/LADW.html