Module 7: Linear Algebra I

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 18, 2025

Outline

Today:

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

Vector spaces & subspaces

Already assumed $(+) : \underset{(u,v)}{V \times V} \to u+v \in V$, $(\cdot) : \underset{(\alpha,v)}{\mathbb{F} \times V} \to \alpha \cdot v \in V$

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 $\mathbf{v} \in V$, $\overset{?}{1} \times \mathbf{v} = \mathbf{v}$

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

linearity conditions

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, $p(x) = a_0 + a_1 x + \ldots + a_n x^n$).

$\alpha \in \mathbb{R}$

$f, g \in C(\mathbb{R}, \mathbb{R}) \Rightarrow f+g \in C(\mathbb{R}, \mathbb{R})$

$\alpha f \in C(\mathbb{R}, \mathbb{R})$

(polynomial) + (polynomial) = polynomial

α (polynomial) = (polynomial)

Lemma

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

Proof.

Since $\underbrace{0 = 0 + 0}_{\text{scalar}}$, by (H) $0 \cdot v = (0+0) \cdot v \overset{H}{=} 0 \cdot v + 0 \cdot v$.

By (D), there exists additive inverse of $0 \cdot v$.

So, $0 = 0 \cdot v + \underline{(-0 \cdot v)} = (0 \cdot v + 0 \cdot v) + (-0 \cdot v)$

$\overset{(B)}{=} 0 \cdot v + \underbrace{(0 \cdot v + (-0 \cdot v))}_{=0 \text{ by } (D)}$

$\square$

$\overset{(D)}{=} 0 \cdot v + 0$

$\overset{(A)}{=} 0 + 0 \cdot v \overset{(C)}{=} 0 \cdot v$

Lemma

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

Proof.

We need to show $v + (-1) \cdot v = 0$ for any $v \in V$.

Since $0 = 1 + (-1)$, by (H) $\underbrace{0 \cdot v}_{=0 \text{ by the previous lemma}} = 1 \cdot v + (-1) \cdot v.$ by (E), $1 \cdot v = v$

$\therefore\ 0 = v + (-1) \cdot v.$

$\Downarrow$ add $-v$ to both sides

By (D), $-v = -v + 0 = -v + v + (-1) \cdot v = (-1) \cdot v$ //.

□

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. $\mathbf{0} \in U$ 0 in V from (c) belongs to 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. ($\Rightarrow$) ②, ③ holds trivially since $\mathcal{U}$ is a vector space.

Need to show $0_V \in \mathcal{U}$.

Let $u \in \mathcal{U}$. Then $(-1)\cdot u \in \mathcal{U}$.

Since $u + (-1)\cdot u \in \mathcal{U}$, $0_V = (1+(-1))\cdot u = u + (-1)\cdot u \in \mathcal{U}$

V

($\Leftarrow$) Only show (1), the existence of additive inverse.

For any $u \in \mathcal{U}$, we need to show the existence of additive inverse.

By viewing $u \in V$, $-u \overset{?}{=} (-1)\cdot u \in V$.

By ③, $(-1)\cdot u \in \mathcal{U}$. Thus we know $-u \in \mathcal{U}$. //

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

$\langle v_1, \ldots, v_n \rangle$

Definition

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

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

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

$\text{span}\{v_1, \cdots, v_n\}$ is a subspace. V.

Basis

Definition

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

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \ldots + \alpha_n \mathbf{v}_n = \sum_{k=1}^{n} \alpha_k \mathbf{v}_k. \qquad \in \langle v_1, \dots, v_n \rangle$$

Example

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

Linear independence

If $v_1, \dots, v_n$ are linearly dependent,
$\exists\, \alpha_i \neq 0$ s.t. $\sum_{i=1}^{n} \alpha_i v_i = 0$

$\alpha_i v_i = -\sum_{j \neq i} \alpha_j v_j$

since $\alpha_i \neq 0$

Definition

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

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

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

Otherwise, we call the system *linearly dependent*.

$v_i = -\sum_{j \neq i} \frac{\alpha_j}{\alpha_i} \cdot v_j$

v_i is a linear combination of v_j's except v_i.

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

Spanning set

Definition

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

$$V = \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}.$$

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

① existence of linear representation by v_i's $\Leftrightarrow V = \text{span}\{v_i\}$

② uniqueness of such representation

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. ($\Rightarrow$) Suppose $v_1, \ldots, v_n$ is a basis.

It suffices to show $v_1, \ldots, v_n$ are linearly independent.

Let $\sum_{i=1}^n \alpha_i v_i = 0$

Since $0 = \sum_{i=1}^n 0 \cdot v_i$, we have 0 represented in two ways.

By the uniqueness of such representation, we must have $\alpha_i = 0, \forall i$.

$(\Leftarrow)$ Suppose $V = \langle v_1, \cdots, v_n \rangle$ and v_i's are linearly independent.

It suffices to show uniqueness of linear representation by $v_1, \cdots, v_n$.

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

Then, $$\underline{\sum_{i=1}^{n} (\alpha_i - \beta_i) \cdot v_i = 0}$$

By linear independence, $\alpha_i - \beta_i = 0 \iff \alpha_i = \beta_i$.

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.

Define $E_1 = \{v_1\}$.

If $v_2 \in \langle v_1 \rangle$, then let $E_2 := \{v_1\}$.

If $v_2 \notin \langle v_1 \rangle$, then let $E_2 = \{v_1, v_2\}$.

If $v_3 \in \operatorname{span} E_2$, then let $E_3 = E_2$.

If $v_3 \notin \operatorname{span} E_2$, then let $E_3 = E_2 \cup \{v_3\}$.

Repeating this process, we have E_n spanning V

and vectors in E_n 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 $V = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. 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.

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.

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 $u_1, \cdots, u_n$ be linearly independent vectors.

Set $E_0 = \{u_1, \cdots, u_n\}$.

Let $v_1, \cdots, v_m$ be a basis of V.

If $v_1 \notin \operatorname{span} E_0$, then $E_1 = E_0 \cup \{v_1\}$,

If $v_1 \in \operatorname{span} E_0$, then $E_1 = E_0$.

Repeat this to v_m.

We can show that E_m is a basis of V.

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

Definition

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

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

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 $0 : V \to V$ defined by $0u = 0$ for any $u \in V$.
- Identity map $Id : V \to V$ defined by $Id(v) = v$ for $\forall v \in V$.

vector space of polynomials.

- Differentiation $D : P(\mathbb{R}) \to P(\mathbb{R})$

$$x^n \to n \cdot x^{n-1}$$

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.

$(S+T)(v) \overset{def}{=} Sv + Tv$

$(\alpha T)(v) \overset{def}{=} \alpha \cdot Tv$

Lemma

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

Proof. Since $0 = 0 + 0$, by linearity of T,

$$T(0) = T(0+0) = T(0) + T(0)$$

$$\therefore \; T(0) = 0.$$

Null space and range

Definition

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

ker T

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

The dimensions of these spaces are often called the following:

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

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) the null space of T is a subspace of U

a) $0 \in \ker T$ is already proved by previous lemma.

b.) Let $u, v \in \ker T$.

Then, $Tu = Tv = 0$.

Thus, $T(u+v) = Tu + Tv = 0+0 = 0$. $\therefore u+v \in \ker T$.

c) Let $\alpha \in \mathbb{F}$, $v \in \ker T$.

Then $T(\alpha v) = \alpha Tv = \alpha \cdot 0 = 0$ $\therefore \alpha v \in \ker T$.

By a) ~ c), we conclude that $\ker T$ is a subspace.

(ii) the range of T is a subspace of V

1) $0 \in \operatorname{Im} T$ since $T0 = 0$.

2) Let $v_1, v_2 \in \operatorname{Im} T$.

Then there exist u_1, u_2 s.t. $v_1 = Tu_1$, $v_2 = Tu_2$.

Thus, $v_1 + v_2 = Tu_1 + Tu_2 = T(u_1 + u_2) \in \operatorname{Im} T$.

3) Let $\alpha \in \mathbb{F}$, $v \in \operatorname{Im} T$.

$\exists\, u \in U$ s.t. $v = Tu$.

$\alpha v = \alpha Tu = T(\alpha u) \in \operatorname{Im} T$.

Therefore, we conclude that $\operatorname{Im} T$ is a subspace.

Example

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

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

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

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

In other words

$u \neq v$ implies $Tu \neq Tv$

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. (⇒) Suppose T is injective.

Let $v \in \ker T$.

Then, $Tv = 0 = T \cdot 0$

Since T is injective, $v = 0$, which means $\ker T = \{0\}$.

(⇐) Suppose $\ker T = \{0\}$.

Let $Tu = Tv$.

Then $T(u - v) = Tu - Tv = 0$.

$\therefore$ $u - v \in \ker T$.

Since $\ker T = \{0\}$, we must have $u - v = 0 \iff u = v$.

Theorem (Rank Nullity Theorem)

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

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

$$\dim \operatorname{Im} T + \dim \ker T = \dim U$$

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