Honors Linear Algebra

MATH0540

Professor Melody Chan

Brown University

Edited by

Richard Tang

Contents

Chapter 1

Fundamentals of Linear Algebra

§1.1 Sets

Sets serve as a fundamental construct in higher-level mathematics. We start with a brief introduction to set theory.

Definition 1.1.1: Sets

A **set** is a collection of elements.

1. $x \in X$ means x is an element of X.
2. $x \notin$ means x is not an element of X.
3. $X \subset Y$ means X is a subset of Y (i.e. $\forall x \in X, x \in Y$.)
4. $X = Y \iff X \subset Y \wedge Y \subset X$.
5. $A \cap B := \{x \mid x \in A \wedge x \in B\}$ means set intersection.
6. $A \cup B := \{x \mid x \in A \vee x \in B\}$ means set union.
7. $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ means set difference.

Example 1. *Let*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}.$$

denote the set of integers, and let

$$\mathbb{Z}^+ = \{0, 1, \dots\}.$$

denote the set of positive integers.

§1.1.1 Set Builder notation

Sets may be defined formally with set-builder notation:

$$X = \{\ expression \mid rule\}.$$

Example 2. *1. Let E represent the set of all even numbers. This set is expressed*

$$E = \{n \in \mathbb{Q} \mid \exists k \in \mathbb{Z} \text{ s.t. } n = 2k\}.$$

2. Let A represent the set of real numbers whose squares are rational numbers:

$$A = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}.$$

§1.1.2 Cartesian Products

Definition 1.1.2: Ordered Tuples

An **ordered pair** is defined (x, y). An n**-ordered tuple** is an ordered list of n items

$$(x_1, \ldots, x_n).$$

Definition 1.1.3: Cartesian Products

Let A, B be sets. The **cartesian product** $A \times B$ is defined

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

Similarly, define the n-fold cartesian product

$$A^n := A \times A \times \cdots \times A.$$

Example 3. $\mathbb{R}^2$ *and* $\mathbb{R}^3$ *are examples of commonly known Cartesian products, which represent the 2D- and 3D-plane respectively.*

Example 4. R^n *is a first example of a* ***vector space.*** *Let* $n \in \mathbb{Z}^+ \cup \{0\}$*:*

1. *(Addition in R^n) We define an* ***addition operation*** *on $\mathbb{R}^n$ by adding coordinate-wise*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

2. *(Scaling) Given $(x_1, \ldots, x_n) \in \mathbb{R}^n, \lambda \in \mathbb{R}$, we define*

$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

Remark 1. $\mathbb{R}_0 = \{0\}$.

§1.1.3 Functions

Let A, B be sets. Informally, a function $f : A \to B$ deterministically returns an element $b \in B$ for each $a \in A$. We write $f(a) = b$.

Example 5. *The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ maps $\mathbb{R}$ to the subset*

$$S \subset \mathbb{R} = \{\left(x, x^2\right) \mid x \in \mathbb{R}\}.$$

Definition 1.1.4: Functions

Let A, B be sets. A function $f : A \to B$ is a subset $G_f \subset A \times B$ such that $\forall a \in A, !\exists b \in B$ s.t. $(a, b) \in G_f$. We write $f(a) = b$ when $(a, b) \in G_f$.

Definition 1.1.5: Codomain

Given a function $f : A \to B$, A is the **domain** of f, and B is the **codomain** or **target** of f. Let the **range** of f be defined as

$$\{b \in B \mid f(a) = b, a \in A\}.$$

The range is the subset of B.

Definition 1.1.6: Bijectivity

Let $f : A \to B$ be a function.

1. f is **injective**, or an **injection**, if $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
2. f is **surjective**, or a **surjection**, if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$. Equivalently, the range is the whole codomain.
3. f is **bijective**, or a **bijection**, if it is both injective and surjective. Equivalently, $\forall b \in B$, there is a unique $a \in A$ such that $f(a) = b$.

§1.2 Fields

Roughly speaking, a **field** is a set, together with operations addition and multiplication. Vector spaces may be defined *over* fields.

Definition 1.2.1: Fields

A **field** is a set $\mathbb{F}$ containing elements named 0 and 1, together with binary operations $+$ and $\cdot$ satisfying:

- **commutativity**: $a + b = b + a, a \cdot b = b \cdot a \ \forall a, b \in \mathbb{F}$.

- **associativity**: $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c,\ \forall a, b, c \in \mathbb{F}$.
- **identities**: $0 + a = a, 1 \cdot a = a\ \forall a \in \mathbb{F}$.
- **additive inverse**: $\forall a \in \mathbb{F}, \exists b \in \mathbb{F}$ s.t. $a + b = 0$.
- **multiplicative inverse**: $\forall a \in \mathbb{F} \setminus \{0\}, \exists c \in \mathbb{F}$ s.t. $ac = 1$.
- **distributivity**: $a \cdot (b + c) = a \cdot b + a \cdot c\ \forall a, b, c \in \mathbb{F}$.

Example 6. $\mathbb{R}^+ \setminus \{0\}$ *is **not** a field under* $+, \cdot$.

Example 7. *(Finite Fields) Let p prime (e.g. $p = 5$). Define*

$$\mathbb{F}_p = \{0, \ldots, p - 1\},$$

with binary operations $+_p, \cdot_p$ given by addition and multiplication modulo p. We claim (without proof) that $\mathbb{F}_p$ is a field.

Example 8. *Let $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Elements of $\mathbb{C}$ are called **complex numbers**. Formally, a complex number is an ordered pair $(a, b)\,, a, b \in \mathbb{R}$. We define addition as*

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

and multiplication as

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Showing $\mathbb{C}$ is a set is left as an exercise for the reader.

Proposition 1.2.1: $\mathbb{C}$ Multiplicative Inverse

For every $\alpha \in \mathbb{C} \setminus \{0\}$, there exists $\beta \in \mathbb{C}$ with $\alpha \cdot \beta = 1$.

Proof. Given $\alpha \in \mathbb{C} \setminus \{0\}$, let us write $\alpha = a + bi$. Then not both $a, b = 0$. Let $\beta = \frac{a}{a^2+b^2} + -\frac{b}{a^2+b^2} i$. Then $\alpha\beta = (a + bi)\left(\frac{a}{a^2+b^2} + -\frac{b}{a^2+b^2}\right) = 1$.
Thus $\forall \alpha \in \mathbb{C} \setminus \{0\}, \exists \beta \in \mathbb{C}$ s.t. $\alpha \cdot \beta = 1$. $\square$

$\mathbb{R}^n$ and $\mathbb{C}^n$ are specific examples of fields, but by no means the only ones (for instance, $\mathbb{F}^2$ with addition and multiplication modulo 2 is a field). Fields serve as the underlying set of numbers and operations that vector spaces are built on. In this course, we focus primarily on $\mathbb{R}$ and $\mathbb{C}$; but many of the definitions, theorems, and proofs work interchangeably with abstract fields.

§1.3 Vector Spaces

Vector spaces serve as the fundamental abstract structure of linear algebra. All future topics will build on vector spaces. Roughly, a vector space V is a set of **vectors** with an addition operation and scalar multiplication, where scalars are drawn from a field $\mathbb{F}$. We now formalize this definition.

Definition 1.3.1: Vector Spaces

Given a field $\mathbb{F}$, A **vector space** over $\mathbb{F}$, denoted $V_{\mathbb{F}}$, is a set V, together with vector addition on V

$$+ : V \times V \longrightarrow V$$

and scalar multiplication on V

$$\cdot : \mathbb{F} \times V \longrightarrow V$$

satisfying the following properties:

- (additive associativity) For all $u, v, w \in V$, $u + (v + w) = (u + v) + w$.
- (additive identity) There exists an element $0 \in V$ such that $v+0 = 0+v = 0$.
- (additive inverse) For all $v \in V$, there exists $w \in V$ such that $v+w = w+v = 0$. We denote $w = -v$.
- (commutativity) For all $v, w \in V$, $v + w = w + v$.
- (scalar multiplicative associativity) For all $\alpha, \beta \in \mathbb{F}, v \in V$, $\alpha(\beta v) = (\alpha\beta)v$.
- (scalar multiplicative identity) There exists an element $1 \in \mathbb{F}$ such that $1v = v$ for all $v \in V$.
- (Distributive Law I) For every $\alpha \in \mathbb{F}$, $v, w \in V$, $a \cdot (v + w) = a \cdot v + a \cdot w$.
- (Distributive Law II) For every $\alpha, \beta \in \mathbb{F}, v \in V$, $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$.

We call elements of $\mathbb{F}$ **scalars**, and elements of V **vectors**, or **points**.

Example 9. *We say V is a vector space over $\mathbb{F}$. A vector space over $\mathbb{R}$ is called a **real vector space**, and a vector space over $\mathbb{C}$ is called a **complex vector space**.*

Example 10. *Let $\mathbb{F}$ be a field.*

1. *For some integers $n \geq 0$, $\mathbb{F}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}\}$ with vector addition defined*

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

and scalar multiplication defined

$$\lambda \cdot (v_1, v_2, \dots, v_n) = (\lambda v_1, \lambda v_2, \dots, \lambda v_n).$$

Note that $F^0 = \{0\}$.

2. $\mathbb{F}^\infty = P\{(a_1, a_2, a_3, \dots) \mid a_j \in \mathbb{F}, j \in \mathbb{N}\}$ *with vector addition and scalar multiplication defined similarly.*

3. *Let* S *be any set; consider* $\{g : S \to \mathbb{F}\}$ *be the set of functions from* S *to* $\mathbb{F}$. *Given* $f, g : S \to \mathbb{F}$, $\lambda \in \mathbb{F}$, *define vector addition* $(f+g) : S \to \mathbb{F}$ *as*

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

and scalar multiplication $\lambda f : S \to \mathbb{F}$ *as*

$$(\lambda f)(x) = \lambda f(x).$$

Perhaps counterintuitively, example 3 subsumes example 1! For example, let $S = \{1, 2, \dots, n\}$, and let $\mathbb{R}^{\{1,\dots,n\}}$ be the set of all functions from $\{1, \dots, n\} \to \mathbb{R}$. One such f may be

$$\begin{aligned} f : \{1, \dots, n\} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = x^2 - 3. \end{aligned}$$

But f can also be thought of as an n-tuple. For instance, with $n = 3$, we can define a function

$$f = (-2, 1, 6) \in \mathbb{R}^3.$$

This is equivalent to $f(1) = -2, f(2) = 1, f(3) = 6$. Similarly, if $f(x) = e^x$, then $f \in \mathbb{R}^{\{1,2,3\}} = \left(e, e^2, e^3\right) \in \mathbb{R}^3$, since $f(1) = e, f(2) = e^2, f(3) = e^3$.

In other words, every n-tuple $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ could be represented as a function $f : \{1, 2, \dots, n\} \to \mathbb{R}$, where $f(1) = x_1, f(2) = x_2, \dots, f(n) = x_n$. The key insight here is that **the function f is the n-tuple**; the one function $f(x) = e^x$ is equivalent to the n-tuple $\left(e, e^2, \dots, e^n\right)$.

From this, we get that the set of functions $\mathbb{R}^{\{1,\dots,n\}} = \mathbb{R}^n$, the set of n-tuples.

Remark 2. *Reinterpret* $\mathbb{F}^0 = \{$*functions* $f : \varnothing \longrightarrow \mathbb{F}\}$. *How many functions are there from* $\varnothing \longrightarrow \mathbb{F}$?
One function $\varnothing = \varnothing \times \mathbb{F}$.

Example 11. *The set of continuous functions* $f : \mathbb{R} \to \mathbb{R}$ *forms a vector space over* $\mathbb{R}$. *In particular, the sum of two continuous functions is continuous; and* $a \cdot f$ *is continuous for any* $a \in \mathbb{R}$, *and* f *continuous.*

But what about fields over fields? Are these vector spaces?

Example 12. *Say $\mathbb{F} \subseteq \mathbb{K}$ ($\mathbb{F}$ is a subfield of $\mathbb{K}$). Then $\mathbb{K}$ is a vector space over $\mathbb{F}$, with addition defined as in $\mathbb{K}$, and with scalar multiplication defined*

$$\lambda \cdot x = \lambda x, \ \textit{where } \lambda \in \mathbb{F}, x \in \mathbb{K}.$$

Thus $\mathbb{C}$ is a real vector space (this is why we draw the complex plane like $\mathbb{R}^2$!).

§1.3.1 Properties of Vector Spaces

We now observe some fascinating properties of vector spaces. Let V be a vector space over a field $\mathbb{F}$.

Proposition 1.3.1: Unique Additive Identity

V has a unique additive identity.

Proof. Suppose $e, e' \in V$ are both additive identities. Then

$$\begin{aligned} e &= e + e' \\ &= e'. \end{aligned}$$

Thus $e = e'$. □

Proposition 1.3.2: Unique Additive Inverse

Every vector $v \in V$ has a unique additive inverse.

Proof. Let $v \in V$, and suppose $w, w' \in V$ are both additive inverses of v. Then

$$\begin{aligned} 0 &= v + w \\ w' &= (w + v) + w' \\ w' &= w + (v + w') \\ w' &= w + 0 \\ w' &= w. \end{aligned}$$

Thus $w = w'$. □

Let us also define a notion of subtraction.

Proposition 1.3.3: -v

For any $v \in V$,

$$-v = (-1) \cdot v.$$

Proof. Let $v, -v \in V$ where $-v$ is the inverse of v. Then

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

Since every $v \in V$ has a unique additive inverse, $-v = (-1) \cdot v$. □

§1.4 Subspaces

Subspaces can greatly expand our examples of vector spaces.

Definition 1.4.1: Subspaces

A subset $U \subseteq V$ is a **subspace** (or a **linear subspace**) of V if

1. $\mathbf{0} \in U$.
2. For all $u, w \in U$, $u + w \in U$.
3. For all $u \in U$, $\lambda \in \mathbb{F}$, $\lambda \cdot u \in U$.

We will see that these three properties are enough for U to satisfy the six properties of vector spaces (so U is a vector space as well!).

Example 13. *What are the subspaces of* $\mathbb{R}^2$ *and* $\mathbb{R}^3$*?*

Solution: It turns out that there are only three valid types of subspaces of $\mathbb{R}^2$:

1. The zero vector $\mathbf{0} = (0, 0)$.
2. All lines through the origin ($y = \alpha x$).
3. $\mathbb{R}^2$ itself.

Similarly, there are only four valid types of subspaces of $\mathbb{R}^2$:

1. The zero vector $\mathbf{0} = (0, 0, 0)$.
2. All lines through through the origin.
3. All planes through the origin.
4. $\mathbb{R}^3$ itself.

Let us now do a rough sketch of a proof that the list of subspaces of $\mathbb{R}^2$ is complete.

Proof. Let W be a subspace of R^2. If W has no nonzero vectors, then $W = \{\mathbf{0}\}$. If W has a non-zero vector $v \in V \setminus \{\mathbf{0}\}$, then W must contain the line through v passing through $\mathbf{0}$.
Moreover, if W contains some $w \in V$ not on the line, we have the ability to "turn" the coordinate plane, such that any $u \in V$ can be formed by $\alpha v + \beta w$. □

§1.5 Span

Suppose a friend imagines a subspace $W \subseteq \mathbb{R}^3$. You know that $(1, 0, 0), (0, 1, 0) \in W$. What else do you know must be in W? Well, first, $\mathbf{0} = (0, 0, 0) \in W$ by definition. But moreover, anything in the form $\{(a, b, 0) \mid a, b \in \mathbb{R}\}$ (the xy-plane) must be in W, since any point on the plane can be made by $\alpha \cdot a + \beta \cdot b$ (we will later see that $(1, 0)$ and $(0, 1)$ are **basis vectors** of $\mathbb{R}^2$).

Definition 1.5.1: Linear Combination and Span

A **linear combination** of a list $v_1, \dots, v_n \in V$ is a vector of the form

$$\lambda_1 v_1 + \dots + \lambda_n v_n, \lambda_i \in \mathbb{F}.$$

The **span** (or **linear span**) of $v_1, \dots, v_n$, also denoted $\text{span}(v_1, \dots, v_n)$ is the set of all linear combinations of $v_1, \dots, v_n$:

$$\text{span}(v1, \dots, v_n) : \{a_1 v_1 + \dots + a_m v_m \mid a_i \in \mathbb{F}\}.$$

Proposition 1.5.1: Span is Smallest Subspace

The span of $v_1, \dots, v_m$ is the smallest subspace of V containing $v_1, \dots, v_m$. Precisely:

1. $\text{span}(v_1, \dots, v_m)$ is a subspace of V.
2. Any subspace W of V containing $v_1, \dots, v_m$ also contains $\text{span}(v_1, \dots, v_m)$.

Proof. Given $W \subseteq V$ is a subspace, and $v_1, \dots, v_m \in W$, we wish to show W contains $\text{span}(v_1, \dots, v_m) = \{a_1 v_1 + \dots + a_m v_m \mid a_i \in \mathbb{F}\}$.
Given $a_1, \dots, a_m \in \mathbb{F}$, we wish to show

$$a_1 v_1 + \dots + a_m v_m \in W.$$

We know $a_1 v_1, \dots, a_m v_m \in W$ since W is closed under scalar multiplication. Additionally, $a_1 v_1 + \dots + a_m v_m \in W$ since W is closed under vector addition. Hence W contains $\text{span}(v_1, \dots, v_m)$.
Thus any subspace $W \subseteq V$ of $v_1, \dots, v_m$ also contains $\text{span}(v_1, \dots, v_m)$. Now, we wish to show $\text{span}(v_1, \dots, v_m) = \{a_1 v_1 + \dots + a_m v_m \mid a_i \in \mathbb{F}\}$ is a subspace.
$0 \in \text{span}(v_1, \dots, v_m)$ (choose $a_i = 0$ for every coefficient).
Given $a_1, \dots, a_m \in \mathbb{F}, b_1, \ \dots, b_m \in \mathbb{F}$, we have $(a_1 v_1 + \dots + a_m v_m) + (b_1 v_1 + \dots + b_m v_m) \in \text{span}(v_1, \dots, v_m)$, as $a_1 + b_1 \in \mathbb{F}$.
Thus $\text{span}(v_1, \dots, v_m)$ is a subspace of V. $\square$

Definition 1.5.2: Empty Span

The span of no vectors is $\{0\}$.

Definition 1.5.3: Span Is Vector Space

If $\text{span}(v_1, \dots, v_m) = V$, then $v_1, \dots, v_m$ **span** V, and $v_1, \dots, v_m$ are a **spanning set**.

Definition 1.5.4: Finite Dimentional Vector Spaces

If V is spanned by a **finite** list of of vectors $v_1, \ldots, v_m$ then V is **finite-dimensional**.

Chapter 2

Linear Maps

§2.1 Linear Maps

Definition 2.1.1: Linear Maps

Let V, W be vector spaces over a field $\mathbb{F}$. A function

$$\begin{aligned} T : V &\longrightarrow W \\ v &\longmapsto T(v) \in W. \end{aligned}$$

is a **linear map** if it satisfies, given $v_1, v_2 \in V,\ \lambda \in \mathbb{F}$:

1. $T(v_1 + v_2) = T(v_1) + T(v_2) \in W$.
2. $T(\lambda v) = \lambda T(v)$.

Proposition 2.1.1: Linear Maps Preserve 0

If $T : V \to W$ is a linear map, then $T(\mathbf{0}) = \mathbf{0}$.

Proof. We have

$$\begin{aligned} T(0) &= T(0+0) \\ &= T(0) + T(0). \end{aligned}$$

Adding the additive inverse of $T(0)$ to both sides, we have

$$0 = T(0).$$

$\square$

Proposition 2.1.2: Combination of Linearity Properties

A function $T : V \to W$ is linear if and only if

$$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$$

for all $v_1, v_2 \in V,\ \alpha, \beta \in \mathbb{F}$.

Example 14. *Let V, W be any vector spaces over $\mathbb{F}$.*

1. *The* ***zero map***

$$\begin{aligned} 0 : V &\longrightarrow W \\ v &\longmapsto 0(v) = 0 \end{aligned}$$

is a linear map.

2. *The* ***identity map***

$$\begin{aligned} I : V &\longrightarrow V \\ v &\longmapsto I(v) = v \end{aligned}$$

is a linear map.

3. *Any linear map*

$$\begin{aligned} T : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto T(x) = ax \end{aligned}$$

is a linear map.

Proposition 2.1.3: Linear Maps in R

Let $T : \mathbb{R} \to \mathbb{R}$ be a linear map. Then there is some $a \in \mathbb{R}$ such that $T(x) = ax$ for all $x \in \mathbb{R}$.

Proof. Let $a = T(1)$. Then for any $x \in \mathbb{R}$,

$$T(x) = T(x \cdot 1) = x \cdot T(1) = ax.$$

$\square$

Example 15. *Say* $T : \mathbb{R}^2 \to \mathbb{R}^2$ *is a linear map such that* $T(1, 0) = (2, 1)$ *and* $T(0, 1) = (1, -1)$. *What else do we know?*

- $T(0, 0) = (0, 0)$
- $T(1, 1) = T((1, 0) + (0, 1)) = (2, 1) + (1, -1) = (3, 0)$
- $T(2, 0) = (4, 2)$