First Read on Linear Algebra, Lecture 1

Apiros3

First Version : August 23, 2025
Last Updated : August 23, 2025

1 Overview

At its heart, linear algebra studies the *spaces of vectors*. (Roughly) a vector is something that can be added to other vectors or be scaled by and 'behaves well'. A vector space is the whole collection of such objects together with rules on how to add and scale. Crucially, it talks about any setting where these operations act consistently. The next question we then act is what the structure preserving maps between vector spaces are. These are called *linear transformations*. Vector spaces behave extremely nicely when compared to other algebraic structures, which makes talking about them very pleasant.

2 Vector Spaces

We first begin by giving a formal definition of what a vector space is.

2.1 Fields and Vector Spaces

Definition 2.1.1. *A **Field**, denoted $\mathbb{F}$ is a tuple $(\mathbb{F}, +, \cdot, 0, 1)$, on some set $\mathbb{F}$ with binary operators $+$ and $\cdot$ such that the following rules hold:*

- ***Associativity** of operands: for any $a, b, c \in \mathbb{F}$ we have $(a+b)+c = a+(b+c)$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
- ***Commutativity** of opearnds: for any $a, b \in \mathbb{F}$ we have $a + b = b + a$ and $a \cdot b = b \cdot a$.*
- ***Identities**: for any a, we have two distinct elements 0 and 1 in X such that $a + 0 = a$ and $a \cdot 1 = a$*
- ***Additive Inverse**: for every a in $\mathbb{F}$ there exists an element in $\mathbb{F}$ denoted $-a$ called the additive inverse of a such that $a + (-a) = 0$.*
- ***Multiplicative Inverse**: for every $a \neq 0$ in $\mathbb{F}$, there exists an element in $\mathbb{F}$ denoted a^{-1} called the multiplicative inverse of a such that $a \cdot a^{-1} = 1$.*
- ***Distributivity** of multiplication over addition: for any $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.*

Intuitively, a field is a set in which we can do addition, subtraction, multiplication, and division on. This is extremely powerful, and is often key in why vector spaces behave in a nice way.

Lemma 2.1.2. *For any field $\mathbb{F}$ and an element $a \in \mathbb{F}$, the additive and multiplicative inverses are unique.*

Proof. Suppose we have some $b, c \in \mathbb{F}$ such that $a + b = 0$ and $a + c = 0$. Then,

$$c = c + 0 = c + (a + b) = (c + a) + b = (a + c) + b = 0 + b = b + 0 = b$$

The proof for multiplication is similar. □

The above lemma shows that when we write $-a$ or a^{-1}, we are talking about some unique element in $\mathbb{F}$, which justifies our notation.

Example 2.1.3. We cover some basic examples of fields:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- For a prime p, $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, the finite field with p elements.

Additionally, some examples of structures which are not fields:

- $\mathbb{Z}$, $\mathbb{N}$.
- $M_n(\mathbb{R})$, the $n \times n$ matrices with elements in $\mathbb{R}$.

Definition 2.1.4. *A **vector space** over a field $\mathbb{F}$ is a non-empty set V together with a binary operation $V \times V \to V$ given by $(u, v) \mapsto u + v$ and a map $\mathbb{F} \times V \to V$ given by $(\lambda, v) \mapsto \lambda v$ that satisfy the **vector space axioms**:*

- *Addition is commutative, associative, has an identity, and has inverses over V*
- *Distributivity: for all $u, v \in V$ and $\lambda, \mu \in \mathbb{F}$, $\lambda(u + v) = \lambda u + \lambda v$ and $(\lambda + \mu)v = \lambda v + \mu v$*
- *Multiplication interaction: for all $v \in V$ and $\lambda, \mu \in \mathbb{F}$, $(\lambda\mu)v = \lambda(\mu v)$*
- *Identity for scalar multiplication: $1v = v$ for all $v \in V$*

*We refer to $\mathbb{F}$ as the **field of scalars** or the **base field**. Elements of V are called **vectors** and elements of $\mathbb{F}$ are called **scalars**.*

While there are many axioms, the most important aspects of a vector space is the closure of V under addition and scalar multiplication, alongisde the existence of a zero vector $0_V \in V$.

Lemma 2.1.5. *Let V be a vector space over a field $\mathbb{F}$. The additive identity is unique.*

Proof. Let 0_V and $0'_V$ be additive identities. We have,

$$0_V = 0_V + 0'_V = 0'_V$$

where we use the fact $0'_V$ is an additive identity on the first equality, and that 0_V is an additive identity on the second. □

Proposition 2.1.6. *Let V be a vector space over a field $\mathbb{F}$. Fix a $v \in V$ and $\lambda \in \mathbb{F}$. Then,*

1. $\lambda 0_V = 0_V$
2. $0v = 0_V$
3. $(-\lambda)v = -(\lambda v) = \lambda(-v)$
4. *if $\lambda v = 0_V$ then $\lambda = 0$ or $v = 0_V$*
5. $-v = (-1)v$

Proof. Exercise. □

Example 2.1.7. We cover some examples of vector spaces:

- The plane $\mathbb{R}^2$ over $\mathbb{R}$ with usual vector addition and scalar multiplication.
- Similarly, $\mathbb{R}^n$ over $\mathbb{R}$ with usual vector addition and scalar multiplication.
- The space of $m \times n$ matrices over $\mathbb{R}$ or $\mathbb{C}$
- The set of all real valued functions $f : \mathbb{R} \to \mathbb{R}$ over $\mathbb{R}$ with addition and scalar multiplication defined pointwise.
- Let X be any set. Defining $\mathbb{R}^X := \{f : X \to \mathbb{R}\}$ gives a vector space.
- For some fixed n, the set of real polynomials of degree at most n over $\mathbb{R}$.
- The set of real differentiable functions over $\mathbb{R}$.
- All sequences of real numbers over $\mathbb{R}$.
- The trivial vector space $\{0\}$
- The set of rational numbers $\mathbb{Q}$ as a vector space over $\mathbb{Q}$
- $\mathbb{R}$ as a vector space over $\mathbb{Q}$

2.2 Subspaces

When a mathematical object has some structure, we often also consider the subsets of that object with the same structure.

Definition 2.2.1. *Let V be a vector space over $\mathbb{F}$. A **subspace** of V is a non-empty subset of V that is closed under addition and scalar multiplication. That is, it is a subset $U \subseteq V$ such that*

- $U \neq \emptyset$
- *for all $u, w \in U$, $u + w \in U$*
- *for all $\lambda \in \mathbb{F}$ and $u \in U$, $\lambda u \in U$.*

where the operations are inherited from the structure of V. When U is a subspace of V, we write $U \leq V$.

Proposition 2.2.2 (Subspace Test)**.** *Let V be a vector space over $\mathbb{F}$, and let U be a subset of V. Then $U \leq V$ if and only if*

1. *$0_V \in U$*
2. *$\lambda u + w \in U$ for all $u, w \in U$ and $\lambda \in \mathbb{F}$.*

Proof. ($\Rightarrow$) Suppose that U is a subspace of V. As U is nonempty, we can pick a $u \in U$, and as U is closed under scalar multiplication, $0u = 0_V \in U$. Take any $u, w \in U$ and $\lambda \in \mathbb{F}$. Then $\lambda u \in U$ as U is closed under scalar multiplication, and $\lambda u + w \in U$ as U is closed under addition.

($\Leftarrow$) Suppose that $0_V \in U$ and that $\lambda u + w \in U$ for all $u, w \in U$ and $\lambda \in \mathbb{F}$. First, U is nonempty as $0_V \in U$. Given any $u, w \in U$, we have $u + w = 1u + w \in U$, so is closed under addition. Given $u \in U$ and $\lambda \in \mathbb{F}$, $\lambda u = \lambda u + 0_V \in U$ so is closed under scalar multiplication. Hence U is a subspace of V. □

Remark 2.2.3. Let V be a vector space over $\mathbb{F}$, and $U \leq V$. Then the addition / scalar multiplication operations on V restricted to U make U a vector space over $\mathbb{F}$. The operation is well-defined as $U \leq V$ ensures closure of the operations, and other properties are inherited from the structure of V.

Proposition 2.2.4. *Let V be a vector space over $\mathbb{F}$ and $W \leq U \leq V$. Then $W \leq V$.*

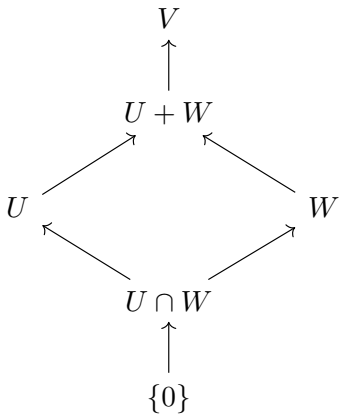
Proof. Follows from definitions. □

Proposition 2.2.5. *Let V be a vector space. Let $U, W \leq V$. Then $U + W \leq V$ and $U \cap W \leq V$, where*

$$U + W := \{u + w \mid u \in U, w \in W\}$$

Proof. Exercise. □

Remark 2.2.6. $U + W$ is the smallest subspace of V which contains U and W, and $U \cap W$ is the largest subspace of V which is contained in both U and W. The following is a simple representation of this fact. Intuitively, $U + W$ is the smallest subspace that contains U and W as we need closure by addition, which forces us to be able to add any two elements in U and W.



Example 2.2.7. We finish this subsection with some examples of subspaces.

- Let $\mathbb{R}[x]$ denote all real coefficient polynomials in a variable x over $\mathbb{R}$. This is a subspace of the set $\{f : \mathbb{R} \to \mathbb{R}\} =: \mathbb{R}^{\mathbb{R}}$
- The only subspaces of $\mathbb{R}$ are $\{0\}$ and $\mathbb{R}$.
- Nontrivial subspaces of $\mathbb{R}^2$ correspond to a line through the origin, and every line corresponds to a subspace.

2.3 Basis

Definition 2.3.1. *Let V be a vector space over $\mathbb{F}$. A **linear combination** of $u_1, \ldots, u_m \in V$ is a vector $\alpha_1 u_1 + \cdots + \alpha_m u_m$ where $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$.*

Definition 2.3.2. *Let V be a vector space over $\mathbb{F}$. We say that the set $S \subseteq V$ (where S may be finite or infinite) has a **spanning set** generated over $\mathbb{F}$, defined by*

$$\langle S \rangle_{\mathbb{F}} = \{\sum_{i=0}^{n} a_i v_i \mid n \geq 0, a_1, \ldots, a_n \in \mathbb{F}, v_1, \ldots, v_n \in S\}$$

*This is the set of all finite linear combinations of elements in S. We say that S **spans** V if $V = \langle S \rangle_{\mathbb{F}}$.*

Remark 2.3.3. When a span is generated by some set S of elements of V, it is the smallest subspace of V that contains S. Note that a linear combination always talks about a finite sum, even when S is infinite.

Notation 2.3.4. When we are working with a finite $S := \{v_1, \dots, v_n\}$, we often omit the set notation, writing $\langle v_1, \dots, v_n \rangle$ to mean $\langle S \rangle$. The base field subscript is omitted when it is clear what field we are working under.

Lemma 2.3.5 (Steinitz Exchange Lemma)**.** *Let V be a vector space over a field $\mathbb{F}$. Take any finite $X := \{v_1, \dots, v_n\} \subseteq V$. Suppose now we have a $u \in \langle X \rangle$ but $u \notin \langle X \backslash \{v_i\} \rangle$ for some i. Let*

$$Y := (X \backslash \{v_i\}) \cup \{u\}$$

Then, $\langle Y \rangle = \langle X \rangle$.

Proof. Let $u \in \langle X \rangle$. Then, we can find $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that

$$u = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

By assumption, there is some $v_i \in X$ such that $u \notin \langle X \backslash \{v_i\} \rangle$. Without loss of generality, take $i = n$. As $u \notin \langle X \backslash \{v_n\} \rangle$, $\alpha_n \neq 0$. This gives

$$v_n = \frac{1}{\alpha_n}(u - \alpha_1 v_1 - \cdots - \alpha_{n-1} v_{n-1})$$

Taking any $w \in \langle Y \rangle$, then we can write w as a linear combination of elements in Y. Replacing u with $\alpha_1 v_1 + \cdots + \alpha_n v_n$, we can write w as linear combination of elements of X. This gives $\langle Y \rangle \subseteq \langle X \rangle$. Noting that $w \in \langle X \rangle$, we can write w as a linear combination of elements of X. Replacing v_n by the equality above, we can write w as a linear combination of elements of Y. This gives $\langle X \rangle \subseteq \langle Y \rangle$. □

Definition 2.3.6. *Let V be a vector space over $\mathbb{F}$. The set $S := \{v_1, \dots, v_n\}$ is **linearly independent** over $\mathbb{F}$ if*

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

*implies that $a_i = 0$ for all $i = 1, \dots, n$. If we can find a nontrivial set that sums to 0, we call the set **linearly dependent**.*

For a general $S \subseteq V$, we say that S is linearly independent if every finite subset of S is linearly independent.

Example 2.3.7. Some examples of linearly independent and dependent sets:

- The set $\{(0,0,1),(0,1,0)\} \subseteq \mathbb{R}^3$ is linearly independent.
- The set $\{(1,0,1),(0,1,1),(1,1,2)\} \subseteq \mathbb{R}^3$ is linearly dependent
- Let $V = \mathbb{C}$ over $\mathbb{R}$. Then the set $\{1, i\}$ is linearly independent.
- If we view $\mathbb{C}$ as a vector space over $\mathbb{C}$, then the set $\{1, i\}$ is linearly dependent.
- Let $V = \mathbb{R}[x]$. Then the set $\{1, x, x^2, \dots\}$ is an infinite set that is linearly independent

Proposition 2.3.8. *Let $S = \{v_1, \ldots, v_m\}$ be a linearly independet subset of a vector space V. Then,*

$$\alpha_1 v_1 + \cdots \alpha_m v_m = \beta_1 v_1 + \cdots + \beta_m v_m$$

if and only if $\alpha_i = \beta_i$ for all $1 \leq i \leq m$.

Proof. If $\alpha_i = \beta_i$ for all $1 \leq i \leq m$, the result is immediate. Conversely, we can write

$$(\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_m - \beta_m)v_m = 0_V$$

As S is linearly independent, we have $\alpha_i - \beta_i = 0$ for all i. □

Lemma 2.3.9. *Let $v_1, \ldots, v_n$ be linearly independent elements over a vector space V. Let $v_{n+1} \in V$. Then the set $v_1, \ldots, v_{n+1}$ is linearly independent if and only if*

$$v_{n+1} \notin \langle v_1, \ldots, v_n \rangle$$

Proof. ($\Rightarrow$) Suppose that $v_{n+1} \notin \langle v_1, \ldots, v_n \rangle$. Take $\alpha_1, \ldots, \alpha_{n+1}$ such that $\alpha_1 v_1 + \cdots + \alpha_{n+1} v_{n+1} = 0_V$. If $\alpha_{n+1} \neq 0$, rearranging gives us

$$v_{n+1} = -\frac{1}{a_{n+1}}(\alpha_1 v_1 + \cdots + \alpha_n v_n) \in \langle v_1, \ldots, v_n \rangle$$

which is a contradiction. Hence $\alpha_{n+1} = 0$, giving $\alpha_1 v_1 + \cdots \alpha_n v_n = 0$. But $v_1, \ldots, v_n$ are linearly independent, so this means $\alpha_1 = \cdots = \alpha_m = 0$ as well.

($\Leftarrow$) Conversely, suppose that $v_1, v_2, \ldots, v_{n+1}$ are linearly independent. If $v_{n+1} \in \langle v_1, \ldots, v_n \rangle$, then we can find some $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that

$$v_{n+1} = \alpha_1 v_1 + \cdots \alpha_n v_n$$

which after rearranging gives $\alpha_1 v_1 + \cdots + \alpha_n v_n - v_{n+1} = 0_V$, which is a nontrivial solution, contradicting the linear independence of $v_1, \ldots, v_{n+1}$. Hence $v_{n+1} \notin \langle v_1, \ldots, v_n \rangle$. □

Definition 2.3.10. *A **basis** for a vector space V over $\mathbb{F}$ is a set $\mathcal{B}$ who is both spanning and linearly independent. If V has a finite basis, we call V **finite dimensional**.*