1 Finite-Dimensional Vector Spaces

Not all vector spaces come in the same size. Ituitively, this makes sense given the feeling of having more room to move about in the space of $\mathbf{R}^3$ than the mere plane of $\mathbf{R}^2$. In fact, although $\mathbf{R}^2$ and $\mathbf{R}^3$ contain infinitely many points, it can be shown that, in the everyday sense of "size", the size of $\mathbf{R}^3$ is indeed bigger than $\mathbf{R}^2$ (some infinities are bigger than others). Linear algebra focues mainly on the properties of finite-dimensional vector spaces, which are introduced in this chapter.

The basic tools needed to understand the structure of functions (or mappings) between finite-dimensional vector spaces are also defined in this chapter, namely span, linear independence, basis, and dimension.

1.1 Span and Linear Independence

Adding up scalar multiples of vectors in a list gives what is called a **linear combination** of the list.

Linear Combinations and Span

> **Definition: Linear Combination**
>
> A **linear combination** of a list $v_1, \ldots, v_m$ of vectors in $\mathbf{V}$ is a vector of the form
>
> $$a_1 v_1 + \cdots + a_m v_m$$
>
> where $a_1, \ldots, a_m \in \mathbf{F}$.

Some mathematicians use the term **linear span** or **linear hull**, which means the same thing as span. The concept of span is particularly useful for describing the cardinality or "size" of a vector space. For dealing with notions of "sizes" of infinite sets, words like "larger" and "smaller" are defined in terms of subset relations. In other words, a set $\mathbf{A}$ is bigger than a set $\mathbf{B}$ implies that $\mathbf{B} \subset \mathbf{A}$.

> **Definition: Span, Generating Set**
>
> The set of all linear combinations of a list of vector $v_1, \ldots, v_m \in \mathbf{V}$ is called the **span** of $v_1, \ldots, v_m$, denoted $\mathbf{span}(v_1, \ldots, v_m)$. In other words
>
> $$\mathbf{span}(v_1, \ldots, v_m) = \{a_1 v_1 + \cdots + a_m v_m : a_1, \ldots, a_m \in \mathbf{F}\}.$$
>
> To express that a vector space $\mathbf{V}$ is a span of a set $v_1, \ldots, v_m$, one commonly uses the following phrases:
>
> - $v_1, \ldots, v_m$ **spans** $\mathbf{V}$;
>
> - $v_1, \ldots, v_m$ **generates** $\mathbf{V}$;
>
> - $\mathbf{V}$ is spanned by $v_1, \ldots, v_m$;
>
> - $\mathbf{V}$ is generated by $v_1, \ldots, v_m$;
>
> - $v_1, \ldots, v_m$ is a spanning set of $\mathbf{V}$;
>
> - $v_1, \ldots, v_m$ is a generating set of $\mathbf{V}$;
>
> The span of the empty list () is defined to be zero.

In general, the substructure (subgroup, subring, subalgebra, subspace) generated by some list of elements in a mathematical structure is the smallest substructure containing at least those elements in the list.

> **Theorem: Span is the smallest containing subspace**
>
> The span of a list of vectors in V is the smallest subspace of V containing all the vectors in the list.

Proof:

To show that $\mathbf{span}(v_1, \ldots, v_m)$ is the "smallest" subspace of V containing $v_1, \ldots, v_m$ is to show that $\mathbf{span}(v_1, \ldots, v_m)$ is a subspace *and simultaneously* a subset of any subspace of V containing $v_1, \ldots, v_m$. Take any list $v_1, \ldots, v_m \in V$ and $\lambda, a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbf{F}$.

First $\mathbf{span}(v_1, \ldots, v_m)$ is demonstrated to be a subspace.

1. The additive identity $\mathbf{0} \in \mathbf{span}(v_1, \ldots, v_m)$ because $0v_1 + \cdots + 0v_m = \mathbf{0} + \cdots + \mathbf{0} = \mathbf{0}$.
2. The $\mathbf{span}(v_1, \ldots, v_m)$ is closed under addition because $(a_1 v_1 + \cdots + a_m v_m) + (b_1 v_1 + \cdots + b_m v_m) = a_1 v_1 + b_1 v_1 + \cdots + a_m v_m + b_m v_m = (a_1 + b_1)v_1 + \cdots + (a_m + b_m)v_m \in \mathbf{span}(v_1, \ldots, v_m)$ because $(a_j + b_j) \in \mathbf{F}$ for every $j \in \{1, \ldots, m\}$.
3. The $\mathbf{span}(v_1, \ldots, v_m)$ is closed under scalar multiplication because $\lambda(a_1 v_1 + \cdots + a_m v_m) = \lambda(a_1 v_1) + \cdots + \lambda(a_m v_m) = (\lambda a_1)v_1 + \cdots + (\lambda a_m)v_m \in \mathbf{span}(a_1, \ldots, a_m)$ because $(\lambda a_j) \in \mathbf{F}$.

Next $\mathbf{span}(v_1, \ldots, v_m)$ is demonstrated to be a subset of any subspace $U \subseteq V$ containing $v_1, \ldots, v_m$.

1. $v_1, \ldots, v_m \in U \implies a_1 v_1 + \cdots + a_m v_m \in U$ because U is a subspace.
2. $\mathbf{span}(v_1, \ldots, v_m) := \{a_1 v_1 + \cdots + a_m v_m : a \in \mathbf{F}\}$
3. $\mathbf{span}(v_1, \ldots, v_m) \subseteq U$.

$\square$

> **Example: Natual Basis**
>
> Suppose $n \in \mathbf{N}$. Show that
>
> $$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$$
>
> spans $\mathbf{F^n}$. Here the jth vector in the list above is the n-tuple with 1 in the jth slot and 0 in all the other slots.
> Suppose $(x_1, \ldots, x_n) \in \mathbf{F^n}$. Then
>
> $$(x_1, \ldots, x_n) = (x_1, 0, \ldots, 0) + \cdots + (0, \ldots, 0, x_n) = x_1(1, 0, \ldots, 0) + \cdots + x_n(0, \ldots, 0, 1)$$
>
> Thus $(x_1, \ldots, x_n) \in \mathbf{span}((1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1))$, as desired.

Now we can make one of the key definitions in linear algebra. Recall that every list, by definition, has a finite length.

> **Definition: Finite Dimensional Vector Space**
>
> A vector space is called **finite-dimensional** if some list of vectors in it spans the space.

The above example shows that $\mathbf{F^n}$ is a finite-dimensional vector space for every positive integer n.

With the usual operations of addition and scalar multiplication, $\mathcal{P}(\mathbf{F})$ is a vector space over $\mathbf{F}$. As such, $\mathcal{P}(\mathbf{F})$ is a subspace of $\mathbf{F}^{\mathbf{F}}$.

It will later be shown that the coefficients of the polynomial uniquely determine the polynomial.

Definition: degree of a polynomial, deg p

- A polynomial $p \in \mathcal{P}(\mathbf{F})$ is said to have **degree** m if there exists scalars $a_0, a_1, \ldots, a_m \in \mathbf{F}$ with $a_m \neq 0$ such that

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

  for all $z \in \mathbf{F}$. If p has degree m, we write $\deg p = m$.

- The polynomial that is identically 0 is said to have degree $-\infty$.

We use the convention that $-\infty < m$, which means that the polynomial 0 is in $\mathcal{P}_m(\mathbf{F})$.

Definition: $\mathcal{P}_m(\mathbf{F})$

For any $m \in \mathbb{N}$, $\mathcal{P}_m(\mathbf{F})$ denotes the set of all polynomials with coefficients in $\mathbf{F}$ and degree at most m.

Example: Finite-dimensional vector space

$\mathcal{P}_m(\mathbf{F})$ is a finite dimensional vector space for each non-negative integer m.

Definition: Infinite-dimensional vector space

A vector space is called **infinite-dimensional** if it is not finite dimensional.

Example: Infinite-dimensional vector space

$\mathcal{P}(\mathbf{F})$ is infinite dimensional.

Linear Independence

Suppose $v_1, \ldots, v_m \in V$ and $v \in \mathbf{span}(v_1, \ldots, v_m)$. By the definition of span, there exists $a_1, \ldots, a_m \in \mathbf{F}$ such that

$$v = a_1 v_1 + \cdots + a_m v_m.$$

Consider the question of whether the choice of scalars in the expression is unique. Suppose $c_1, \ldots, c_n \in \mathbf{F}$ is another set of scalars such that

$$v = c_1 v_1 + \cdots + c_m v_m.$$

Subtracting the last two equations, we have

$$0 = (a_1 - c_1)v_1 + \cdots + (a_m - c_m)v_m.$$

If the only way to write 0 as a linear combination of $v_1, \ldots, v_m$ is by taking 0 for each scalar then, $a_j = c_j$ (the choice of scalars for each vector in $\mathbf{span}(v_1, \ldots, v_m)$ must be unique). This situation is so important that we give it a special name, linear independence.

> **Definition: Linearly Independent**
>
> - A list $v_1, \ldots, v_n$ of vectors in V is called **linearly independent** if the only choice of $a_1, \ldots, a_n \in \mathbf{F}$ that makes $a_1 v_1 + \cdots + a_n v_n$ equal to 0 is $a_1 = \cdots = a_n = 0$.
>
> - The empty list () is also declared to be linearly independent.

> **Definition: Linearly dependent**
>
> - A list $v_1, \ldots, v_n$ of vectors in V is called **linearly dependent** if it is not linearly independent.

The following theorem repeatedly proves to be useful in solving many theorems deeper in the subject.

> **Theorem: Linear Dependence Lemma**
>
> Suppose $v_1, \ldots, v_m$ is a linearly dependent list in V. Then there exists $j \leq m$ such that the following hold:
>
> - $v_j \in \mathbf{span}(v_1, \ldots, v_{j-1})$;
>
> - If the jth term is removed from $v_1, \ldots, v_m$, the span of the remaining list equals $\mathbf{span}(v_1, \ldots, v_m)$.

Proof:

The following procedure demonstrates the first proposition. Assuming $v_1, \ldots, v_m$ is linearly dependent, by definition,

$$\exists a_1, \ldots, a_m \in \mathbf{F} \text{ not all 0 such that } \mathbf{0} = a_1 v_1 + \cdots + a_m v_m.$$

For any such combination, select the highest value of $j \in \{1, \ldots, m\}$ such that $a_j \neq 0$. Notice,

$$-a_j v_j = a_1 v_1 + \cdots + a_{j-1} v_{j-1} \implies v_j = \frac{a_1}{-a_j} v_1 + \cdots + \frac{a_{j-1}}{-a_j} v_{j-1} \text{ (which is possible since } a_j \neq 0)$$

Hence there exists $j \leq m$ such that,

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

For the second proposition, the following procedure demonstrates that v_j can be removed without changing the span. Building on the previous result,

$$v_j \in \mathbf{span}(v_1, \ldots, v_{j-1}) \implies \exists b_1, \ldots, b_{j-1} \in \mathbf{F} \text{ such that } v_j = b_1 v_1 + \cdots + b_{j-1} v_{j-1}.$$

This situation means any element $w \in \mathbf{span}(v_1, \ldots, v_m)$, we have,

$$\begin{aligned}
w &= a_1 v_1 + \cdots + a_{j-1} v_{j-1} + a_j \mathbf{v_j} + a_{j+1} v_{j+1} + \cdots + a_m v_m \\
&= a_1 v_1 + \cdots + a_{j-1} v_{j-1} + a_j (\mathbf{b_1 v_1} + \cdots + \mathbf{b_{j-1} v_{j-1}}) + a_{j+1} v_{j+1} + \cdots + a_m v_m \\
w &= (a_1 + \mathbf{a_j b_1}) \mathbf{v_1} + \cdots + (a_{j-1} + \mathbf{a_j b_{j-1}}) \mathbf{v_{j-1}} + a_{j+1} v_{j+1} + \cdots + a_m v_m
\end{aligned}$$

This bidirectional procedure demonstrates that

$$\mathbf{span}(v_1, \ldots, v_m) = \mathbf{span}(v_1, \ldots, v_{j-1}, v_{j+1}, \ldots v_m).$$

$\square$

> **Theorem: Length of a linearly independent list $\leq$ length of spanning list**
>
> In a finite-dimensional vector space, the length of every linearly indepenedent list of vectors is less than or equal to the length of every spanning list of vectors.

Proof:

Suppose $v_1, \ldots, v_n$ is linearly independent in V and $w_1, \ldots, w_m$ spans V. Since $w_1, \ldots, w_m$ spans $V, \exists a_1, \ldots, a_m, b_1 \in \mathbf{F}$ where

$$v_1 = a_1 w_1 + \cdots + a_m w_m \implies \mathbf{0} = b_1 v_1 + a_1 w_1 + \cdots + a_m w_m,$$

which is linearly dependent. By the Linear Dependence Lemma, it is possible to discover one $w_j \in \mathbf{span}(v_1, w_1, \ldots, w_{j-1})$ and remove it, resulting in one v being added and one w being removed, while the resulting list (of length m) continues to span V.

By the second part of the Linear Dependence Lemma, there exists scalars such that

$$v_j = b_1 v_1 + \cdots + a_m w_m \implies \mathbf{0} = b_1 v_1 + \cdots + b_j v_j + \cdots + a_m w_m$$

By the Linear Dependence Lemma, there exists one vector that can be removed while leaving the span (all of V) unchanged. Since the v's are linearly independent, the above equality requires that at least one a_j will be non-zero. The process of placing one v, producing a dependent list, and removing one w while leaving the span unchanged continues until either we run out of v's or w's. If we run out of w's, we necessarily also run out of v's (or else the remaining v's would be in the span of the previous v's, which contradicts our assumption).

Hence $m \leq n$, as desired. $\qquad\square$

1.2 Bases

The following section derives crucial theorems built on concepts of linear independence and span.

> **Definition: Basis**
>
> A **basis** of $\mathbf{V}$ is a list of vectors in $\mathbf{V}$ that is linearly independent and spans $\mathbf{V}$.

The next result explains why bases are useful.

> **Theorem: Criterion for basis**
>
> A list $v_1, \ldots, v_n$ of vectors in $\mathbf{V}$ is a basis of $\mathbf{V}$ if and only if every $v \in \mathbf{V}$ can be written uniquely in the form
> $$v = a_1 v_1 + \cdots + a_n v_n$$
> where $a_1, \ldots, a_n \in \mathbf{F}$

Proof:

Suppose $v_1, \ldots, v_m$ is a basis for V and

$$
\begin{aligned}
v = a_1 v_1 + \cdots + a_m v_m &= c_1 v_1 + \cdots + c_m v_m \\
\implies \mathbf{0} &= (a_1 - c_1) v_1 + \cdots + (a_m - c_m) v_m \\
\implies a_1 &= c_1 \cdots = a_m = c_m \\
\implies & \text{ there is a unique way to write } v.
\end{aligned}
$$

For the converse, $\forall v \in V$, there exists a unique list of scalars $a_1, \ldots, a_m$, such that

    1. **Spanning Condition** $v = a_1 v_1 + \cdots + a_m v_m$

    2. **Linear Independence** $\mathbf{0} = a_1 v_1 + \cdots + a_m v_m \iff a_1 = \cdots = a_m = 0$

Hence, $v_1, \ldots, v_m$ is a basis for V. $\qquad\square$

> **Theorem: Spanning list contains a basis**
>
> Every spanning list in a vector space can be reduced to a basis of the vector space.

Proof:

Suppose $w_1, \ldots, w_m$ spans V and is dependent. The Linear Dependence Lemma states that we can remove any element in the span of the previous vectors without altering the span of the entire list. It has already been shown that the length of a linearly independent list $\leq$ length of spanning list. Therefore, if $v_1, \ldots, v_n$ is linearly independent in V, then reducing $w_1, \ldots, w_m$ to a basis requires removing no more than $m - n$ vectors from $w_1, \ldots, w_m$. $\qquad\square$

> **Theorem: Basis of finite-dimensional vector space**
>
> Every finite-dimensional vector space has a basis

Proof:

Take any finite-dimensional vector space V, and suppose $v_1, \ldots, v_n$ generates V. It has already been shown every spanning list in a vector space can be reduced to a basis of the vector space. Since $v_1, \ldots, v_n$ can be reduced to a basis, V has a basis. $\qquad\square$

> **Theorem: Linearly independent list extends to a basis**
>
> Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.

Proof:

Take any finite-dimensional vector space V, and suppose $v_1, \ldots, v_n$ generates V and $w_1, \ldots, w_m$ is independent in V. Using the same substitution procedure as the Linear Dependence Lemma, it is possible to substitute each w_j for exactly m v's to create a new list that includes each w followed by enough v's to make the new list span V. This can be reduced to a basis. $\qquad\square$

> **Theorem: Every subspace of V is part of a direct sum equal to V**
>
> Suppose V is finite-dimensional and U is a subspace of V. Then there is a subspace W of V such that $V = U \oplus W$.

Proof:

Suppose U is a subspace of V

$$\implies U \text{ is finite-dimensional}$$
$$\implies U \text{ has a basis (call it } u_1, \ldots, u_k)$$
$$\implies u_1, \ldots, u_k \text{ is linearly independent in } V$$
$$\implies u_1, \ldots, u_k \text{ can be extended to a basis } u_1, \ldots, u_k, w_1, \ldots, w_l \text{ of } V$$
$$\implies \mathbf{span}(w_1, \ldots, w_l) \text{ form a subspace } W \text{ in } V$$

Since $u_1, \ldots, u_k, w_1, \ldots, w_l$ is linearly independent in V, the only way to write $\mathbf{0}$ as a sum of $a_1 u_1 + \cdots + a_k u_k + b_1 w_1 + \cdots + b_l w_l$ is by taking $a_1 = \cdots = a_k = b_1 = \cdots = b_l = 0$.

In other words, the only way to write $\mathbf{0}$ as the sum of $\mathbf{u} \in U$ and $\mathbf{w} \in W$ is by taking $\mathbf{u} = \mathbf{w} = 0$. Hence, $U \oplus W$ is a direct sum. $\qquad\square$

1.3 Dimension

How should dimension be defined? A reasonable definition of dimension should force $\mathbf{F^n}$ to be n. Notice that the standard basis of $\mathbf{F^n}$,

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$$

has length n. It is therefore tempting to define the basis as the length of a basis.

Theorem: Basis length does not depend on basis

Any two bases of a finite-dimensional vector space have the same length.

Proof:

Suppose V is finite-dimensional and B_1 and B_2 are bases in V.

$$B_1 \text{ is linearly independent in } V \text{ and } B_2 \text{ spans } V$$
$$\implies \text{the length of } B_1 \leq \text{ the length of } B_2$$

Also,

$$B_2 \text{ is linearly independent in } V \text{ and } B_1 \text{ spans } V$$
$$\implies \text{the length of } B_2 \leq \text{ the length of } B_1$$

Hence
$$\text{the length of } B_1 = \text{the length of } B_2.$$

$\square$

Definition: Dimension, dim$V$

- The **dimension** of a finite-dimensional vector space is the length of any basis of the vector space.

- The dimension of V (if V is finite-dimensional) is denoted by dim$V$.

Theorem: Dimension of a subspace

If $\mathbf{V}$ is finite-dimensional and $\mathbf{U}$ is a subspace of $\mathbf{V}$, then dim$\mathbf{U} \leq$ dim$\mathbf{V}$.

Proof:

Suppose $\mathbf{V}$ has dimension $n < \infty$ and $\mathbf{U}$ is a subspace of $\mathbf{V}$. Then $\mathbf{U}$ is finite-dimensional and has a basis $u_1, \ldots, u_m$. It has already been shown that the length of a linearly independent list is less than or equal to a spanning list. Since $u_1, \ldots, u_m$ is linearly independent in $\mathbf{V}$ and $\mathbf{V}$ has a basis of length n, $m \leq n \implies$ dim$\mathbf{U} \leq$ dim$\mathbf{V}$. $\square$

The following theorems show that linearly independent or spanning lists of the right length can be known to be a basis.

Theorem: Linearly independent list of the right length is a basis

Suppose $\mathbf{V}$ is finite-dimensional. Then every linearly indepenedent list of vectors in $\mathbf{V}$ with length dim$\mathbf{V}$ is a basis of $\mathbf{V}$.

Proof:

Suppose $\mathbf{V}$ has dimension $n < \infty$ and $v_1, \ldots, v_n$ is independent in $\mathbf{V}$. Since every linearly independent list can be extended to a basis, we can adjoin vectors to $v_1, \ldots, v_n$ to make it a basis. Since a basis requires n elements, no elements need to be added so that $v_1, \ldots, v_n$ is a basis. $\square$

Theorem: Spanning list of the right length is a basis

Suppose $\mathbf{V}$ is finite-dimensional. Then every spanning list of vectors in $\mathbf{V}$ with length $\dim\mathbf{V}$ is a basis of $\mathbf{V}$.

Proof:

Suppose $\mathbf{V}$ has dimension $n < \infty$ and $v_1, \ldots, v_n$ spans $\mathbf{V}$. Since every spanning list can be extended to a basis, we can reduce the list to make it a basis. Since a basis requires n elements, no elements need to be removed so that $v_1, \ldots, v_n$ is a basis. $\qquad\square$

Theorem: Dimension of a sum

If U_1 and U_2 are subspaces of a finite dimensional vector space, then

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

Proof:

$\qquad\square$