Linear Algebra

Swayam Chube

July 30, 2022

Contents

Chapter 1

Vector Spaces

Definition 1.1 (Vector Space). A *vector space* V over a field F consists of a set on which two operations (called *addition* and *scalar* multiplication) are defined so that for each pair of elements $x, y \in V$ there is a unique element $x + y \in V$ and for each element $a \in F$ and each element $x \in V$, there is a unique element $ax \in V$ such that the following conditions hold

1. (Commutativity of Addition) For all $x, y \in V$, $x + y = y + x$
2. (Associativity of Addition) For all $x, y, z \in V$, $(x + y) + z = x + (y + z)$
3. (Additive Identity) There exists an element $0 \in V$ such that $x + 0 = x$ for all $x \in V$
4. (Additive Inverse) For each element $x \in V$, there exists an element $y \in V$ such that $x + y = 0$
5. (Scalar Identity) For each element $x \in V$, $1x = x$
6. (Associativity of Scalar Multiplication) For each pair of elements $a, b \in F$ and each element $x \in V$, $(ab)x = a(bx)$
7. (Distributivity over Vectors) For each element $a \in F$ and each pair of elements $x, y \in V$, $a(x + y) = ax + ay$
8. (Distributivity over Scalars) For each pair of elements $a, b \in F$ and each element $x \in V$, $(a + b)x = ax + bx$

The elements of the field F are called **scalars** and the elements of the vector space V are called **vectors**

Definition 1.2 (Subspace). A subset W of a vector space V over a field F is called a **subspace** of V if W is a vector space over F with the operations of addition and scalar multiplication defined on V.

Theorem 1.3. Let V be a vector space and W a subset of V. Then W is a subspace of V if and only if the following three conditions hold for the operations defined in V.

1. $0 \in W$
2. $x + y \in W$ whenever $x, y \in W$
3. $cx \in W$ whenever $c \in F$ and $x \in W$

Proof. Commutativity of Vector Addition, Associativity of Vector Addition, Associativity of Scalar Multiplication, Distributivity over Vectors and Scalars are implicit from V. The existence of Additive Identity is guaranteed by the first condition. Let $x \in W$ and -1 be the additive inverse of 1 in F. Then $(-1)x \in W$, further, $x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0$, which implies the existence of Additive Inverse for vectors. This finishes the proof. ■

In other words, W is a subspace of V if and only if W contains the zero vector, and is closed under addition and scalar multiplication.

Definition 1.4 (Direct Sum). A vector space V is called the *direct sum* of W_1 and W_2 if W_1 and W_2 are subspaces of V such that $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$. We denote that V is the direct sum of W_1 and W_2 by writing $V = W_1 \oplus W_2$.

Theorem 1.5. Let W_1 and W_2 be subspaces of a vector space V.

1. $W_1 + W_2$ is a subspace of V thatcontains both W_1 and W_2.
2. Any subspace that contains both W_1 and W_2 must also contain $W_1 + W_2$.

Proof.

1. Since $0 \in W_1 \cap W_2$, $0 \in W_1 + W_2$. For any $x, y \in W_1 + W_2$, there exist $x_1, y_1 \in W_1$ and $x_2, y_2 \in W_2$ such that $x = x_1 + x_2$ and $y = y_1 + y_2$. Thus, $x + y = x_1 + x_2 + y_1 + y_2 = (x_1 + y_1) + (x_2 + y_2) \in W_1 + W_2$. Further, for any $c \in F$, $c(w_1 + w_2) = cw_1 + cw_2 \in W_1 + W_2$.

2. Straightforward.

■

Definition 1.6. Let W be a subspace of a vector space V over a field F. For any $v \in V$, the set $\{v\} + W$ is called the *coset of* W *containing* v. It is customary to denote this coset by $v + W$. Let $V/W = \{v + W \mid v \in V\}$. Addition and scalar multiplication are defined as

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W \qquad a(v + W) = av + W$$

for all $v, v_1, v_2 \in V$ and $a \in F$.

Theorem 1.7. Let W be a subspace of a vector space V. Then,

1. $v + W$ is a subspace of V if and only if $v \in W$

2. $v_1 + W = v_2 + W$ if and only if $v_1 - v_2 \in W$

3. V/W is a vector space

Proof.

1. If $v \in W$, then $v + W = W$. If $v + W \leq V$, then $0 \in v + W$, thus $-v \in W$, as a result, $v = -(-v) \in W$.

2. Trivial

3.

■

Definition 1.8. Let S be a nonempty subset of a vector space V. The *span* of S, denoted $\operatorname{span}(S)$ is the set consisting of all linear combinations of the vectors in S. For convenience, we define $\operatorname{span}(\emptyset) = \{0\}$.

Theorem 1.9. The span of any subset S of a vector space V is a subspace of V. Moreover, any subspace of V that contains S must also contain the span of S.

Proof. If $S = \emptyset$, then we are trivially done. If not, then there is some $s \in S$, as a result, $0 = 0s \in S$. Next, suppose $u, v \in S$. Then we may write $u = \sum_{s\in S} u_s s$ and $v = \sum_{s\in S} v_s s$. Their sum can then be written as $\sum_{s\in S}(u_s + v_s)s \in \operatorname{span}(S)$. Finally, for any $c \in F$ and $u \in S$, $cu = \sum_{s\in S} cu_s s \in S$ and thus S is a subspace of V.

The second statement is trivially true. ■

Definition 1.10. A subset S of a vector space V *generates* V if $\operatorname{span} S = V$.

Definition 1.11 (Linear Dependence, Independence). A subset S of a vector space V is called *linearly dependent* if there exist a finite number of distinct vectors $u_1, u_2, \ldots, u_n$ in S and scalars $a_1, a_2, \ldots, a_n$ not all zero, such that

$$a_1u_1 + \cdots + a_nu_n = 0$$

If S is not linearly dependent, it is said to be *linearly independent*.

We note that nowhere in the above definition have we required S to be finite. The following follows from the contrapositive of the definition

Corollary. A subset S of a vector space V is linearly independent if and only if each finite subset of S is linearly independent.

Equivalently, if S is indeed finite, then $S = \{u_1, \ldots, u_n\}$ is said to be linearly independent if

$$a_1u_1 + \cdots + a_nu_n = 0 \iff a_1 = \cdots = a_n = 0$$

Theorem 1.12. Let S be a linearly independent subset of a vector space V, and let v be a vector in V that is not in S. Then $S \cup \{v\}$ is linearly dependent if and only if $v \in \text{span}(S)$.

Proof. Let $S = \{u_1, \ldots, u_n\}$. Since $S \cup \{v\}$ is linearly independent, there exist scalars, $a_1, \ldots, a_n$ and b, not all zero, such that

$$a_1u_1 + \cdots + a_nu_n + bv = 0$$

One trivially notes that $b \neq 0$, as a result, v can be written as a linear combination of the a_i's and thus, $v \in \text{span}(S)$. ■

Definition 1.13. A *basis* for a vector space V is a linearly independent subset of V that generates V.

It is important to note that a basis need not be unique. For example, the vector space $P_2(\mathbb{R})$ has $\{1, x, x^2\}$ and $\{2, 3x, 5x^2 + 1\}$ as a basis.

Theorem 1.14. Let V be a vector space and $\beta = \{u_1, \ldots, u_n\}$ be a subset of V. Then β is a basis for V if and only if each $v \in V$ can be uniquely expressed as a linear combination of vectors of β, that is, can be expressed in the form

$$v = a_1u_1 + \cdots + a_nu_n$$

for unique scalars $a_1, \ldots, a_n$.

Proof. Suppose β is a basis for V. Then, by definition, any $v \in V$ can be expressed as a linear combination. Suppose $v = a_1u_1 + \cdots + a_nu_n = b_1u_1 + \cdots + b_nu_n$. Then,

$$(a_1 - b_1)u_1 + \cdots + (a_n - b_n)u_n = 0$$

But since the vectors $\{u_1, \ldots, u_n\}$ are linearly independent, $a_i = b_i$ for all $1 \leq i \leq n$. This establishes uniqueness.

Conversely, if each vector in V can be uniquely represented as a linear combination of the elements of β, then $0 \in V$ can be represented only when $a_i = 0$ for all $1 \leq i \leq n$, which implies β is linearly independent. Further, since β generates V, we are done. ■

Theorem 1.15. If a vector space V is generated by a finite set S, then some subsetof S is a basis for V and hence V has a finite basis.

Proof. Let β be a maximal linearly independent set in S. Let $v \in S$. Then $\beta \cup \{v\}$ is linearly dependent, but due to a preceeding theorem, we know that this implies $v \in \text{span}(\beta)$. Thus $S \subseteq \text{span}(\beta)$ and hence $\text{span}(S) \subseteq \text{span}(\beta)$ and β spans V. But since β is linearly independent, it is also a basis for V. ■

Theorem 1.16 (Replacement Theorem). Let V be a vector space that is generated by a set G containing exactly n vectors, and let L be a linearly independent subset of V containing exactly m vectors. Then $m \leq n$ and there exists a subset H of G that contains exactly $n - m$ vectors such that $L \cup H$ generates V.

Proof. The proof proceeds by mathematical induction on m. The base case $m = 0$ is trivial. Suppose the hypothesis is true for some $m \geq 0$, we shall show that it is also true for $m + 1$. Let $L = \{v_1, \ldots, v_{m+1}\}$, then $\{v_1, \ldots, v_m\} \subseteq L$ is also linearly independent. Thus, there exists $H \subseteq G$ containing $n - m$ vectors $\{u_1, \ldots, u_{n-m}\}$ such that $L \cup H$ generates V and as a result, there exist scalars such that

$$a_1 v_1 + \cdots + a_m v_m + b_1 u_1 + \cdots + b_{n-m} u_{n-m} = v_{m+1}$$

We note that if $n - m = 0$, then v_{m+1} can be written as a linear combination of $\{v_1, \ldots, v_m\}$, contradictory to the fact that it is linearly independent. Thus $n > m$ or equivalenely $n \geq m + 1$.

Further, without loss of generality, suppose $b_1 \neq 0$. As a result, u_1 can be written as a linear combination of $\{v_1, \ldots, v_{m+1}, u_2, \ldots, u_{n-m}\}$. Let now $H = \{u_2, \ldots, u_{n-m}\}$. Then, $u_1 \in \text{span}(L \cup H)$ and thus

$$\{v_1, \ldots, v_m, u_1, \ldots, u_{n-m}\} \subseteq \text{span}(L \cup H)$$

Thus $L \cup H$ generates V. Further, the size of H is $n - (m + 1)$, which finishes the induction step. ■

Corollary. Let V be a vector space having a finite basis. Then every basis for V contains the same number of vectors.

Proof. Let β be a basis for V with n vectors and γ be another. If γ has more than n vectors, then we may choose a subset $S \subseteq \gamma$ with $n+1$ linearly independent vectors, contradicting the Replacement Theorem. We now obtain $|\gamma| \leq |\beta|$. Reversing the roles of β and γ, we obtain $|\beta| \leq |\gamma|$. This gives us the desired conclusion. ∎

Definition 1.17 (Dimension). A vector space is said to be *finite dimensional*if it has a basis consisting of a finite number of vectors. The unique number of vectors in each basis for V is called the *dimension* of V and is denoted by $\dim(V)$.

Corollary. Let V be a vector space with dimension n.

1. Any finite generating set for V contains at least n vectors, and a generating set for V that contains exactly n vectors is a basis for V
2. Any linearly independent subset of V that contains exactly n vectors is a basis for V
3. Every linearly independent subset of V can be extended to a basis for V

Proof. Let β be a basis for V

1. Let G be a finite generating set for V. Due to a preceeding theorem, G has a basis γ for V. Thus, $|G| \geq |\gamma| = n$. Equality may hold if and only if $G = \gamma$ and is therefore a basis
2. Let S be a linearly independent subset of V with $|S| = n$. Then, due to the replacement theorem, there is a set H of cardinality $n - n = 0$ such that $S \cup H = S$ is a basis for V.
3. It follows from the replacement theorem, that there exists a set H such that $S \cup H$ is of size n and generates V. But due to the first part, we have that $S \cup H$ is a basis.

∎

Example. Let $H \subsetneq \mathcal{M}_n(\mathbb{C})$ be the set of all Hermitian matrices. Then H is an $\mathbb{R}$-vector space with dimension n^2. Further, H is *not* a $\mathbb{C}$-vector space.

Theorem 1.18. Let W be a subspace of a finite-dimensional vector space V. Then W is finite-dimensional and $\dim(W) \leq \dim(V)$. Moreover, if $\dim(W) = \dim(V)$ then $V = W$.

Proof. Since no linearly independent subset of V may have more than n vectors, W must be finite dimensional. Let γ be a basis for W. Since γ is linearly independent in W, it is obviously linearly independent in V and thus $\dim(W) = |\gamma| \leq \dim(V)$. If $|\gamma| = \dim(V)$, then due to a preceeding theorem, γ must be a basis for V and thus $W = \text{span}(\gamma) = V$. ■

It follows from the previous corollary that any basis for W can be extended to a basis for V.

Lemma 1.19. Let V be a vector space having dimension n and let S be a subset of V that generates V

1. There is a subset of S that is a basis for V
2. S contains at least n vectors

Proof.

1. Let β be a maximal linearly independent subset of S. It is not hard to show that $S \subseteq \text{span}(\beta)$ and thus $\text{span}(\beta) = \text{span}(S) = V$ and thus β is a basis for V
2. Since β contains exactly n vectors, S must contain at least n vectors.

■