1.6   Sifting and the Replacement Theorem

How "big" is a vector space? We intuitively know that a plane is "bigger" than a line, and 3D space is "bigger" than a plane. But in the abstract world of vector spaces, we need a rigorous way to measure this.

The answer lies in the number of vectors in a basis. But there's a potential problem: what if one person finds a basis with 3 vectors, and another person finds a basis for the same space with 4 vectors? If that were possible, our entire concept of "size" would collapse.

In this section, we prove the most important technical result of the chapter: the **Steinitz Replacement Theorem**. This theorem is the "engine" that guarantees every basis of a space has the exact same number of vectors. Once we have this, we can finally define the **Dimension** of a space—a single number that captures its fundamental complexity.

> **Theorem 1.6.1 (Sifting Method).** Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ be a subset of V. Then there exists a subset $S' \subseteq S$ such that:
>
> 1. S' is linearly independent, and
> 2. $\mathrm{span}(S') = \mathrm{span}(S)$.

Proof. For each $r = 1, 2, \dots, m$, we check whether $\mathbf{v}_r$ is a linear combination of the previous terms $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{r-1}$. We:

1. Keep $\mathbf{v}_r$ in S' if $\mathbf{v}_r$ is not a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{r-1}$ (not redundant);
2. Remove $\mathbf{v}_r$ from S' if $\mathbf{v}_r$ is a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{r-1}$ (redundant).

After this process, we obtain a subset S' in which no element is a linear combination of the preceding members anymore. Therefore, by Theorem 1.4.1, S' is linearly independent. Moreover, according to Theorem 1.4.2, removing "redundant members" from S does not change its linear span. Therefore, we have $\mathrm{span}(S') = \mathrm{span}(S)$. ∎

Remark. The sifting method is a powerful algorithmic tool that allows us to "clean up" any set of vectors. Given any collection of vectors, we can systematically remove the redundant ones while preserving the span. This gives us a "cleaned" version that is linearly independent and spans the same space.

This method becomes our "new weapon" in linear algebra proofs. Whenever we encounter a set that might have redundant vectors, we can apply the sifting method to obtain a linearly independent subset with the same span. This technique will be particularly useful in proving results about dimension and in constructing bases from spanning sets.

Example (Sifting Example). Consider $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6\}$ in $\mathbb{R}^3$ where:

$$\mathbf{v}_1 = (1, 1, 1), \qquad \mathbf{v}_2 = (2, 2, 2), \qquad \mathbf{v}_3 = (1, 0, 0),$$
$$\mathbf{v}_4 = (3, 2, 2), \qquad \mathbf{v}_5 = (1, 1, 0), \qquad \mathbf{v}_6 = (0, 0, 1).$$

We apply the sifting method:

- $\mathbf{v}_1 \neq \mathbf{0}$, so $\mathbf{v}_1$ is kept.
- $\mathbf{v}_2 = 2\mathbf{v}_1$, so $\mathbf{v}_2$ is removed.
- $\mathbf{v}_3$ is not a linear combination of $\mathbf{v}_1$, so $\mathbf{v}_3$ is kept.
- $\mathbf{v}_4 = 2\mathbf{v}_1 + 1\mathbf{v}_3$, so $\mathbf{v}_4$ is removed.
- Suppose $\mathbf{v}_5 = a\mathbf{v}_1 + b\mathbf{v}_3$. Then $(1,1,0) = (a+b, a, a)$, which gives $a = 0$ and $a + b = 1$, so $b = 1$. But then the second coordinate gives $1 = a = 0$, which is a contradiction. So $\mathbf{v}_5$ is not a linear combination of $\mathbf{v}_1, \mathbf{v}_3$. Hence, $\mathbf{v}_5$ is kept.
- Since $\dim(\mathbb{R}^3) = 3$, any four vectors cannot be linearly independent. Therefore, $\mathbf{v}_6$ must be a linear combination of $\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_5$. So $\mathbf{v}_6$ is removed.

The sifted set is $S' = \{\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_5\} = \{(1,1,1), (1,0,0), (1,1,0)\}$, which is linearly independent and spans the same space as S.

Theorem 1.6.2 (Steinitz Exchange/Replacement Theorem). Let V be a vector space over F. Suppose:

- $G = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ spans V;
- $L = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m\}$ is linearly independent.

Then $m \leq n$.

Proof. The strategy is to insert the vectors from L one-by-one into G and "sift" the resulting set to maintain the spanning property. We rely on the fact that if we add a vector $\mathbf{w}$ to a spanning set S, the set $\{\mathbf{w}\} \cup S$ becomes linearly dependent, allowing us to remove a redundant vector (by Theorem 1.4.2).

Consider the first step. We form the set B_1 by inserting $\mathbf{u}_1$ into G:

$$B_1 = \{\mathbf{u}_1, \mathbf{v}_1, \dots, \mathbf{v}_n\}.$$

Since G spans V, B_1 is linearly dependent. By applying the sifting process (Theorem 1.6.1), we can remove a vector to obtain a new spanning set G_1. Since L is linearly independent, $\mathbf{u}_1 \neq \mathbf{0}$, so the removed vector must be some $\mathbf{v}_i$. Thus:

$$G_1 = \{\mathbf{u}_1\} \cup S_1,$$

where S_1 is a subset of G with size $n - 1$.

Now, consider the general step. Suppose we have successfully exchanged k vectors such that the set

$$G_k = \{\mathbf{u}_1, \dots, \mathbf{u}_k\} \cup S_k$$

spans V, where $S_k \subset G$ contains $n - k$ vectors. We insert the next vector $\mathbf{u}_{k+1}$ to form:

$$B_{k+1} = \{\mathbf{u}_{k+1}\} \cup G_k.$$

Since G_k is a spanning set, $\mathbf{u}_{k+1}$ depends on the vectors in G_k, making B_{k+1} dependent. We must remove a vector to restore the spanning property. We cannot remove any of the $\mathbf{u}_i$'s, as this would imply a linear dependence relation exclusively among elements of L,

contradicting the hypothesis that L is linearly independent. Therefore, we must remove some $\mathbf{v}_j$ from S_k.

This process generates a sequence of subsets of remaining $\mathbf{v}$'s:

$$n = |G| > |S_1| > |S_2| > \cdots > |S_m| \geq 0.$$

Since we are able to perform this exchange m times (once for each $\mathbf{u} \in L$), we must have started with enough $\mathbf{v}$'s to accommodate every removal. Therefore, $n \geq m$. ∎

1.6.1   Consequences of the Replacement Theorem

Having proved the Steinitz Replacement Theorem, the major conclusion we can draw from it is that any (finite) basis of the same vector space will have the same size.

Theorem 1.6.1 (Basis Theorem). If a vector space V over F has a finite basis, then every basis of V has the same number of vectors.

Proof. Let B_1 and B_2 be two bases with n and m vectors respectively.

- Since B_1 is linearly independent and B_2 spans, by Replacement Theorem, $n \leq m$.
- Since B_2 is linearly independent and B_1 spans, by Replacement Theorem, $m \leq n$.

Thus $n = m$. ∎

Definition 1.6.1 (Dimension). A vector space V over F is called **finite-dimensional** if it has a finite basis. The **dimension** of V, denoted $\dim_F(V)$, is the number of vectors in any basis for V. By convention, $\dim_F(\{\mathbf{0}\}) = 0$.

Remark. When the underlying field is clear, we abuse the notation of $\dim_F$ and write it as $\dim$.

Example (Examples of Dimensions). $\dim(F^n) = n$, $\dim(F[x]_{\leq n}) = n + 1$, and $\dim(M_{m \times n}(F)) = mn$.

Theorem 1.6.2 (Size Bounds for Independent and Spanning Sets). Let V be a vector space of dimension n over F, and $S \subseteq V$ be a subset.

1. If $|S| > n$, then S cannot be linearly independent.
2. If $|S| < n$, then S cannot span V.

Proof.

1. Given $|S| > n$, and suppose for the sake of contradiction that S is linearly independent. Let B be a basis of V, then we have $|B| = n$ and B is a spanning set of V. By Replacement Theorem, we have

$$\underbrace{|S|}_{\text{size of lin. indep. set}} \leq \underbrace{|B|}_{\text{size of spanning set}} = n.$$

    Giving a contradiction, hence S cannot be linearly independent.

2. Given $|S| < n$, and suppose for the sake of contradiction that S spans V. Let B be a basis of V, then we have $|B| = n$ and B is linearly independent. By Replacement Theorem, we have

$$n = \underbrace{|B|}_{\text{size of lin. indep. set}} \leq \underbrace{|S|}_{\text{size of spanning set}} .$$

    This implies $n \leq |S|$, which contradicts the assumption that $|S| < n$. Hence S cannot span V.

$$\blacksquare$$

Remark.

$$\text{Size of lin. indep. set } \leq \text{ Size of basis } \leq \text{ Size of spanning set.}$$

Theorem 1.6.3 (Basis Extension Theorem). Let V be a finite-dimensional vector space and S be a linearly independent subset of V. Then S can be extended into a basis of V.

Proof. Since V is finite-dimensional, it has a finite basis $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. Consider the set $S \cup B$. Since B spans V, $S \cup B$ also spans V. We apply the Sifting Method (Theorem 1.6.1) to the ordered set formed by listing the elements of S first, followed by the elements of B.

The Sifting Method will keep all elements of S because S is linearly independent. It then proceeds to examine each element of B, keeping those that are not in the span of the vectors already kept. The resulting subset S' spans $\text{span}(S \cup B) = V$ and is linearly independent by construction. Thus, S' is a basis for V that contains S. $\blacksquare$

Corollary 1.2.1 (Existence of Basis). Every finite spanning set of a vector space V contains a basis.

Proof. Apply the Sifting Method to the spanning set. The resulting subset S' is linearly independent by construction and still spans V. Therefore, S' is a basis for V. $\blacksquare$

Theorem 1.6.4 (Dimension Implies Equality). Let V and W be finite-dimensional vector spaces over F. If

1. $W \subseteq V$;
2. $\dim_F(W) = \dim_F(V)$,

then $W = V$.

Proof. If we show $V \subseteq W$ then we are done. Suppose for contradiction that $V \not\subseteq W$. That means there exists some $\mathbf{v} \in V$ that $\mathbf{v} \notin W$.

Let $S = \{\mathbf{w}_1, \dots, \mathbf{w}_n\}$ be a basis of W, (consequently, $\dim_F(W) = n$). Since $\mathbf{v} \notin W$, we have $\mathbf{v} \notin \operatorname{span}(S)$.

That would mean that $S' = \{\mathbf{w}_1, \dots, \mathbf{w}_n, \mathbf{v}\}$ is linearly independent in V. By Replacement Theorem, we have

$$\underbrace{|S'|}_{\text{size of lin. indep. set}} \leq \dim_F(V),$$

which implies $n + 1 \leq n$, which is a contradiction, therefore $V \subseteq W$. ∎

Remark. This theorem makes proving $W = V$ somewhat easier. As if we wanted to prove equivalence before, we can only do it by proving $W \subseteq V$ and $V \subseteq W$. Now we can just prove one side and then state that their dimension is the same.

An immediate consequence of the above theorem is the following:

Theorem 1.6.5 (Maximal Independent Subset is a Basis). Let V be a vector space of dimension n over F. Then any n independent vectors form a basis of V. (We say that "any maximal linearly independent subset forms a basis").

Proof. Let S be a linearly independent set of size n. We want to show that $\operatorname{span}(S) = V$.

Let $W = \operatorname{span}(S)$, this implies that W is a subspace of V, which implies $W \subseteq V$.

Notice that S spans W and S is linearly independent, therefore S is a basis of W. So $\dim_F(W) = |S| = n = \dim_F(V)$. By Theorem 1.6.6, we have $W = V$, then $\operatorname{span}(S) = V$. ∎