Example

Let E^{ij} denote the $m \times n$ matrix whose only nonzero entry is 1 at the ith row and j th column. Then $\beta = \{E^{ij} : 1 \le i \le m, 1 \le j \le n\}$ is a basis for $M_{m\times n}(\mathbb{F})$.

Consider $M_{2\times 2}(\mathbb{F})$. Then

$$\beta = \left\{\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right\}.$$

Exercise

Let S be the set defined as

$$S := \left\{\begin{bmatrix}a & a\\a & b\end{bmatrix} : a, b \in \mathbb{R}\right\}.$$

(i) Prove that S is a subspace of $M_{2\times 2}(\mathbb{F})$.

(ii) Give a basis for S.

Exercise

Consider $S = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\}$.

(i) Show that S is a subspace of $\mathbb{R}^3$.

(ii) Find a basis for S.

Theorem

Let $V(\mathbb{F})$ be a vector space and $\beta = \{v_i\}_{i=1}^{n}$ be a subset of of V. Then β is a basis for V if and only if each vector $v \in V$ can be expressed uniquely as a linear combination of vectors in β.

Proof: Let β be a basis for V, and take $v \in V$. Then v can be expressed as a linear combination of vectors in β.

Suppose v can be expressed as two linear combinations of vectors in β. That is,

$$\begin{aligned} v &= c_1 v_1 + c_2 v_2 + \cdots + c_n v_n \\ v &= d_1 v_1 + d_2 v_2 + \cdots + d_n v_n \qquad c_i, d_i \in \mathbb{F}, v_i \in \beta\ \forall i \in [n]. \end{aligned}$$

It follows that

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = d_1 v_1 + d_2 v_2 + \cdots + d_n v_n.$$

Subtracting the right-hand side from both sides, then using properties of commutativity, associativity, and distribution, we get

$$(c_1 - d_1)v_1 + (c_2 - d_2)v_2 + \cdots + (c_n - d_n)v_n = \mathbf{0}.$$

Since β is linearly independent, every coefficient $c_i - d_i$ must equal zero. Thus, $c_i = d_i$ for every $i \in [n]$, so the two linear combinations of v are actually the same.

Therefore, every $v \in V$ has a unique presentation as a linear combination of vectors in β.

Conversely, assume any vector $v \in V$ can be expressed uniquely as a linear combination of vectors in β. Then v is in in the the span of β, i.e. $v \in \text{span}(\beta)$. Hence, $\text{span}(\beta) = V$.

Now consider the linear combination

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = \mathbf{0}.$$

Take $v = \mathbf{0} \in V$. By assumption, the above presentation is unique. The trivial solution is when $c_i = 0$ for every $i \in [n]$. It follows that this is the *only* solution. Hence, by definition, β is linearly independent.

These facts combined prove that β is a basis for V. ■

Theorem

If a vector space $V(\mathbb{F})$ is generated by a finite set S, then some subset of S is a basis for V. Hence, V has a finite basis.

Proof: To begin, suppose either S is empty or $S = \{\mathbf{0}\}$. Then $V = \text{span}(\varnothing) = \{\mathbf{0}\}$, and the empty set $\varnothing$ is a subset of S that forms a basis for V.

Otherwise, if S is nonempty and $S \neq \{\mathbf{0}\}$, then S contains a nonzero element v_1. Then $\{v_1\}$ is a linearly independent subset of V.

If possible, we continue choosing vectors $v_2, v_3, \ldots, v_k$ from S such that the set $S_k = \{v_1, v_2, \ldots, v_k\}$ stays linearly independent. Since S is finite, this process will stop at some n.

We have constructed a linearly independent subset of S. That is,

$$\beta \coloneqq \{v_1, v_2, \ldots, v_n\} \subseteq S.$$

Two cases arise: (i) $\beta = S$, and (ii) $\beta \subset S$.

In the first case, by assumption, $\text{span}(\beta) = \text{span}(S) = V$. Since β is linearly independent, it is also a basis of V.

We focus on the second case. Our claim is that β is the desired subset of S which forms a basis for V. We show that $\text{span}(\beta) = V$.

We know that $\beta \subset S \subseteq V$ and that $\text{span}(S) = V$. A previous result**TODO** implies $\text{span}(B) \subseteq \text{span}(S) = V$. Thus, it suffices to show that $V \subseteq \text{span}(B)$. We will show that $S \subseteq \text{span}(S)$.

Let $v \in S$. If $v \in \beta$, then $v \in \text{span}(\beta)$ and we are done. Otherwise, if $v \notin \beta$, then the set $\beta \cup \{v\}$ is linearly dependent because of how we constructed β. We proved last time that this implies $v \in \text{span}(S)$.

Hence, $S \subseteq \text{span}(\beta)$, so $\text{span}(S) \subseteq \text{span}(\beta)$. This implies $V \subseteq \text{span}(\beta)$, and all together, $V = \text{span}(\beta)$. Therefore, β is a basis for V. ■

Note

The Replacement Theorem says we can extend any linearly independent subset to a basis. The above theorem now says we can reduce any spanning set to a basis.

Corollary

Let $V(\mathbb{F})$ be a vector space with a finite basis. Then all bases of V are finite, and those bases all have the same number of vectors.

Proof: Let β be a basis for V for which $|\beta| = n < \infty$. Then, let γ be another basis for V. Since γ is a linearly independent subset of V, the number of vectors in γ must not exceed $|S|$ where $\text{span}(S) = V$.

Given that β generates V by definition, we then have $|\gamma| \leq |\beta|$. Now, reverse the roles of β and γ to see that $|\beta| \leq |\gamma|$. Thus, $|\beta| = |\gamma|$. Therefore, all bases of V have the same cardinality. ■

Definition — **Finite Dimensionality**

A vector space $V(\mathbb{F})$ is **finite-dimensional** if it has a basis consisting of a finite number of vectors.

Definition — **Dimension of a Vector Space**

Let β be a finite basis of a vector space $V(\mathbb{F})$ where $|\beta| = n$, a unique value. Then we call this number n the **dimension** of V. We write this as

$$\dim(V) = n < \infty.$$

Example

The standard basis for $\mathbb{F}^n$ is $\beta = \{e_1, e_2, \ldots, e_n\}$. Since $|\beta| = n$, the dimension of $\mathbb{F}^n$ is $\dim(\mathbb{F}^n) = n$.

Example

$$\dim\left(M_{m \times n}(\mathbb{F})\right) = m \cdot n.$$

Exercise

Show that $\beta = \{1\}$ is a basis for the vector space $\mathbb{C}(\mathbb{C})$, then deduce that the dimension of this space is 1.

Example

The set $\beta = \{1, i\}$ is a basis for $\mathbb{C}(\mathbb{R})$. Therefore, $\dim(\mathbb{C}(\mathbb{R})) = 2$.

Corollary

Let $V(\mathbb{F})$ be a vector space where $\dim(V) = n$.

(i) Any finite generating set for V contains at least n vectors, and any such set containing exactly n vectors is a basis for V.

(ii) Any linearly independent subset of V consisting of exactly n vectors is a basis for V.

(iii) Every linearly independent subset of V can be extended to a basis for V.

The proof is left for the next lecture, but you may try it as an exercise!

Infinite-Dimensional Vector Spaces

We briefly discuss polynomials over a single variable, some subsets of which form infinite-dimensional vector spaces.

Let $P(\mathbb{F})$ be the set of polynomials in the variable x with coefficients in $\mathbb{F}$. That is,

$$P(\mathbb{F}) \coloneqq \left\{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_i \in \mathbb{F}\ \forall i \in [n]\right\}.$$

The degree of a nonzero polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, denoted by $\deg(f)$, is the largest nonnegative integer n for which $a_n \neq 0$. For example,

$$f(x) = 2x + x^4 \Rightarrow \deg(f) = 4.$$

It is convenient to define $\deg(\mathbf{0})$ to be $-\infty$. Note that the degree of any constant polynomial is zero.

Now, define $P_m(\mathbb{F})$ to be polynomials in x with degrees at most m.

$$P_m(\mathbb{F}) \coloneqq \{f \in P(\mathbb{F}) : \deg(f) \leq m\}.$$

Exercise

Prove that $\beta_m \coloneqq \left\{1, x, x^2, \ldots, x^m\right\}$ is a basis for $P_m(\mathbb{F})$.

The above exercise shows that $P_m(\mathbb{F})$ is finite-dimensional. The broader set $P(\mathbb{F})$, however, is **infinite-dimensional**. In fact, $P(\mathbb{F})$ is generated by the infinite basis

$$P(\mathbb{F}) = \langle 1, x, x^2, \ldots \rangle.$$