BASES OF FINITE-DIMENSIONAL VECTOR SPACES

ROHAN RAMCHAND

Let $S = \{v_1, v_2, ..., v_n\} \subseteq V/F$, where V is a vector space over field F.

Definition 1. *S is said to* **span** *V iff*

$$\forall v \in V \ \exists \alpha_1, \alpha_2, ..., \alpha_n \in F : v = \sum_{i=1}^{N} \alpha_i v_i.$$

In other words, every vector in V can be written as a **linear combination** *of the vectors in S.*

Definition 2. *A set $X = \{u_1, u_2, ..., u_n\} \subseteq V$ is* **linearly dependent** *if*

$$\begin{aligned} \exists \alpha_1, \alpha_2, ..., \alpha_n \in F : \alpha_{i_0} \neq 0 & \\ \wedge \quad 0 &= \sum_i \alpha_1 u_i \\ &= \alpha_{i_0} u_{i_0} + \sum_{i \neq i_0} \alpha_i u_i = 0 \\ u_{i_0} &= -\sum_{i \neq i_0} \frac{\alpha_i}{\alpha_{i_0}} u_i. \end{aligned}$$

In other words, every vector can be written as a linear combination of every other vector.

Definition 3. *Let*

$$\delta_x(y) = \begin{cases} 1 & y = x \\ 0 & \textit{otherwise} \end{cases}.$$

$\delta_x(y)$ is known as the **delta function***.*

Example. *Let F be a field and $V = F^n$ a vector space over that field. Let $e_i = (\delta_i(1), \delta_i(2), ..., \delta_i(n))$. The set $S = \{e_1, e_2, ..., e_n\}$ is a basis of V.*

Example. *Let $\mathbb{R}[X]$ be the vector space of real-valued polynomials over $\mathbb{R}$. Let $S_n = \{1, x, x^2, ..., x^n\}$ for some natural number n. S is linearly independent; however, it does not span $\mathbb{R}[X]$, since any term of degree $n+1$ cannot be expressed as a linear combination of the elements of S.*

Let $\mathbb{R}_{\leq n}[X]$ be the vector space of real-valued polynomials over $\mathbb{R}$ whose highest term is of or less than order n. Since any polynomial of degree n can be expressed as a linear *combination of $x^i, i \leq n$, S_n spans $\mathbb{R}_{\leq n}[X]$. Therefore, since S_n spans and is linearly independent on $\mathbb{R}_{\leq n}[X]$, S_n is the basis of this vector space.*

Additionally, the space $\mathbb{R}[X]$ does not have a finite spanning set, since it can only be spanned by a set containing every power of x expressed in the space.

Let X be a finite set and $V = F(X)$ be the space of F-valued functions on X.

Theorem 1. *The set $S_V = \{\delta_x : x \in X\}$ is a basis on V.*

Proof. Let $f \in F(X)$ be an F-valued function on X. Let $\alpha_x = f(x) \forall x \in X$. Then for some $y \in X$

$$\begin{aligned} f(y) &= (\sum_{x \in X} f(x)\delta_x)(y) \\ &= \sum_{x \in X} f(x)\delta_x(y) \\ &= f(y) && \text{(since } \delta_x(y) = 0 \text{ if } x \neq y \text{, the sum is nonzero only at } x = y\text{)} \end{aligned}$$

Therefore, S_V spans V.

Let $\mathbf{0}$ be the zero function (i.e. the function $\forall x \in X$ $\mathbf{0}(x) = 0$). Assume S_V is linearly dependent; then for some $x_0 \in X$,

$$\left(\sum_{x \in X} \alpha_x \delta_x \right)(x_0) = \mathbf{0}(x_0)$$
$$\alpha_{x_0} = 0$$

Therefore, the only way for a function to equal zero as a linear combination of the elements of S_V is for every coefficient to equal zero; therefore, S_V is linearly independent.

Therefore, since S_V both spans V and is linearly independent on V, it is a basis for V and the proof is complete. $\square$

The following theorems are properties of bases. The first is given without proof.

Theorem 2. (1) *Let S be a linearly independent set on a finite vector field V. Let $S' \subseteq S$. Then S' is linearly independent on V.*

(2) *Let S be a spanning set of a finite vector field V. Let $S' \subseteq S$. Then S' is a spanning set of V.*

Theorem 3. *Let V be a finite-dimensional vector space. Then V admits a basis.*

The following lemmas are used in the proof of this theorem and are given without proof.

Lemma 1. *Let V be a finite-dimensional vector space. Then there exists a set $S \subseteq V$ that spans V.*

Lemma 2. *Let V be a finite-dimensional vector space and S be a spanning, linearly dependent set on V. Then there exists at least one element $v_i \in S$ such that $S' = S - \{v_i\}$ is linearly independent. Then S' spans V.*

Proof. Let $S = \{v_1, v_2, ..., v_n\} \subseteq V$ be a spanning set of a finite space V.

(1) If S is linearly independent, the proof is complete.

(2) If S is linearly dependent,

$$\exists\ i_1 : v_{i_1} = \sum_{i \neq i_1} \alpha_i v_i.$$

Then define $S' = S - \{v_{i_1}\}$. By lemma, S' spans V.

These cases are repeated as necessary until $S^* = S - \{v_1, v_2, ..., v_j\}$ for some $j < n$ is a linearly independent set. (S^* is guaranteed to be non-empty, since the empty set cannot span a non-empty vector space.) Then S^* is a basis of V and the proof is complete. □

Theorem 4. *Let V be a finite space with basis $B = \{v_1, v_2, ..., v_n\}$. By definition,*

$$\forall v \in V\ \exists\, \alpha_1, \alpha_2, ..., \alpha_n : v = \sum_{i \leq n} \alpha_i v_i.$$

These coefficients $\alpha_1, \alpha_2, ..., \alpha_n$ are unique.

Proof. Let $v \in V$ and assume its coefficients as defined above are non-unique:

$$v = \sum_{i \leq n} \alpha_i v_i = \sum_{i \leq n} \beta_i v_i$$

$$\therefore \sum_{i \leq n} (\alpha_i - \beta_i) v_i = \mathbf{0}$$

$$\therefore \forall\, i \leq n : \alpha_i - \beta_i = 0$$

$$\therefore \forall\, i \leq n : \alpha_i = \beta_i$$

□

We are now equipped to define the notion of the *dimension* of a vector space. However, we will first need to prove a fundamental theorem of vector spaces.

Theorem 5. *Let V be a finite space. Let $B_1 = \{v_1, v_2, ..., v_m\}$ and $B_2 = \{u_1, u_2, ..., u_n\}$ be bases of V of length m and n, respectively. Then $m = n$.*

We will rely on the following lemma in the proof of this statement.

Lemma 3. (the Exchange Lemma) Let $S = \{v_1, ..., v_n\}$ be a spanning set and let $L = \{u_1, ..., u_m\}$ be a linearly independent set on a finite space V. Then $m \leq n$.

Proof. Assume by contradiction that $m > n$. Let $u_1 \in L_0$ be an element of the linearly independent set L_0. By definition of spanning,

$$u_1 = \sum_i \alpha_i v_i$$

for some $\alpha_1, ..., \alpha_n$, where at least one α_{i_1} is nonzero. Then

$$v_{i_1} = \frac{1}{\alpha_{i_1}} u_1 - \sum_{i \neq i_1} \frac{\alpha_i}{\alpha_{i_1}} v_i.$$

We will now "swap" this vector $v_{i_1} \in S$ with the vector $u_1 \in L_0$: let $S_1 = S_0 - \{v_{i_1}\} \cup \{u_1\}$. Since any vector $v \in V$ can be written as

$$v = \sum_{i=1}^{n} \beta_i v_i = \beta_{i_1} v_{i_1} + \sum_{i \neq i_1} \beta_i v_i,$$

where β_i is the corresponding coefficient for each vector $v_i \in S$, S_1 spans V.

This process is then repeated n times (since $n < m$ by assumption). Then $S_n = \{u_1, ..., u_n\}$ is a spanning set by the proof above, and therefore $u_{n+1} = \sum_{i=1}^{n} \alpha_i u_i$. Since this implies that u_{n+1} is linearly dependent on the vectors in L_0, we have reached a contradiction. Therefore, $m \leq n$ and the proof is complete. □

We can now prove the theorem above.

Proof. Since B_1 is a spanning set and B_2 is a linearly independent set on V, $n \leq m$. However, B_1 is a linearly independent set and B_2 is a spanning set on V as well, so $m \leq n$. Therefore, $m = n$. □

We have arrived at the fundamental result, therefore, that all bases on finite spaces are of equal length. This length is known as the dimension of V.

Definition 4. *Let V be a finite space with basis $B = \{v_1, v_2, ..., v_n\}$. Then $\dim V = n$.*

We will now state two corollaries about the relationship of spanning sets and linearly independent sets to bases. Both are provided without proof.

Corollary 1. *Let S be the spanning set of a vector space V such that $\dim V = n$. Then $\#S \geq n$.*

Corollary 2. *Let L be a linearly independent set over a vector space V such that $\dim V = n$. Then $\#L \leq n$.*

With these corollaries, we can now state and prove two theorems of spanning sets of and linearly independent sets on a finite space.

Theorem 6. *Let S be the spanning set of a vector space V with $\dim V = n$. Then if $\#S = n$, S is a basis.*

Proof. Assume by contradiction that $S = \{v_1, ..., v_n\}$ is not a linearly independent set. Then $\exists\, i_1 : v_{i_1} = \sum_{i \neq i_1} \alpha_i v_i$. Then $S_1 = S - \{v_1\}$ is also a spanning set; however, $\#S_1 = n - 1 < n$, which is a contradiction. Therefore, S is linearly independent and spanning and is thus a basis. $\square$

Theorem 7. *Let L be a linearly independent set on a vector space V with $\dim V = n$. Then if $\#L = n$, L is a basis.*

Proof. Assume by contradiction that L is not spanning. Then $\exists\, v \in V$ such that v cannot be expressed as a linear combination of the vectors in L. Then let $L_1 = L \cup \{v\}$; by definition, L_1 is linearly independent. However, $\#L_1 = n+1 > n$, which is a contradiction; therefore, L is spanning and linearly independent and is thus a basis. $\square$

Ordered Bases

We now seek to induce some form of order on the notion of a basis.

Definition 5. *Let $B = \{v_1, ..., v_n\}$ be the basis of a finite vector space V. Then the* **ordered basis** *over V is an n-tuple of vectors $\vec{B} = (v_1, ..., v_n)$.*

One of the properties of a basis over a vector space V is that any vector in this space can be written as a linear combination of vectors in the basis (since a basis by definition spans a vector space). Let $\varphi_B : V \to F^n = \{\alpha_1, ..., \alpha_\}$ be the mapping from the vector space to the n-tuple of coefficients in F, such that for some $v \in V$

$$v = \sum_{i=1}^{n} \alpha_i v_i.$$

Since B is unordered, the mapping results in a set and is therefore not unique; if, however, $\vec{B}$ is used instead, the mapping becomes unique.

Theorem 8. *Let V be a finite vector space over a field F and $\vec{B} = (v_1, ..., v_n)$ be an ordered basis on V. Define the map*

$$\varphi_{\vec{B}} : V \to F^n : \varphi_{\vec{B}}(v) = (\alpha_1, ..., \alpha_n)$$

such that

$$v = \sum_{i=1}^{n} \alpha_i v_i.$$

Then $\varphi_{\vec{B}}$ is an isomorphism.

Proof. Let $u, v \in V$, such that $u = \sum_{i=1}^n \alpha_i v_i$ and $v = \sum_{i=1}^n \beta_i v_i$. Then $\varphi_{\vec{B}}(u) = (\alpha_1, ..., \alpha_n)$ and $\varphi_{\vec{B}}(v) = (\beta_1, ..., \beta_n)$. By definition of vector addition, $u + v = \sum_{i=1}^n (\alpha_i + \beta_i) v_i$; then

$$\begin{aligned}\varphi_{\vec{B}}(u+v) &= (\alpha_1 + \beta_1, ..., \alpha_n + \beta_n)\\ &= (\alpha_1, ..., \alpha_n) + (\beta_1, ..., \beta_n)\\ &= \varphi_{\vec{B}}(u) + \varphi_{\vec{B}}(v).\end{aligned}$$

Now let $\lambda \in F$ be a scalar; then by definition of scalar multiplication, $\lambda u = \lambda \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n (\lambda \alpha_i) v_i$. Then

$$\begin{aligned}\varphi_{\vec{B}}(\lambda u) &= (\lambda\alpha_1, ..., \lambda\alpha_n)\\ &= \lambda(\alpha_1, ..., \alpha_n)\\ &= \lambda\varphi_{\vec{B}}(u)\end{aligned}$$

Therefore, $\varphi_{\vec{B}}(u+v) = \varphi_{\vec{B}}(u) + \varphi_{\vec{B}}(v)$ and $\varphi_{\vec{B}}(\lambda u) = \lambda\varphi_{\vec{B}}(u)$; then $\varphi_{\vec{B}}$ is a linear transformation.

Let $g : F^n \to V$ such that $g(\alpha_1, ..., \alpha_n) = \alpha_1 v_1 + ...\alpha_n v_n$. Then $g \circ \varphi_{\vec{B}} = \mathrm{Id}_V$ and $\varphi_{\vec{B}} \circ g = \mathrm{Id}_{F^n}$, where Id_V and Id_{F^n} are the identity mappings on V and F^n, respectively. (The proof of this statement is left as an exercise.) □

The mapping $\varphi_{\vec{B}}$ is an isomorphism; moreover, it is a mapping between abstract algebra and linear algebra, as illustrated in the following examples.

Example. *Let $V = \mathbb{R}^2/\mathbb{R}$, with $\vec{B} = ((1,1),(1,-1))$. Then*

$$\varphi_{\vec{B}} \underbrace{(x,y)}_{v \in V} = (\alpha, \beta) = \left(\frac{x+y}{2}, \frac{x-y}{2}\right).$$

This can also be expressed as

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & -\frac{1}{2}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}$$

Example. *Let $V = \mathbb{R}^2$ and let $\vec{B}_\theta = ((\cos\theta, \sin\theta), (-\sin\theta, \cos\theta))$. $\varphi_{\vec{B}_\theta}$ is left as an exercise to the reader.*

$$\begin{aligned}\varphi_{\vec{B}_\theta}^{-1}(\alpha, \beta) &= (x, y)\\ &= \alpha(\cos\theta, \sin\theta) + \beta(-\sin\theta, \cos\theta)\\ &= (\alpha\cos\theta - \beta\sin\theta, \alpha\sin\theta + \beta\cos\theta)\end{aligned}$$

$$\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$