我們常常看到一個 vector space 中, 若一個集合中向量的個數太多時, 就不會是 linearly independent 了. 例如在 $\mathbb{R}^2$ 中任意 3 個向量 $\mathbf{v}_1=(a_1,b_1),\mathbf{v}_2=(a_2,b_2),\mathbf{v}_3=(a_3,b_3)$ 就一定會 linearly dependent. 這事實的原因便是我們要找到 $c_1,c_2,c_3\in\mathbb{R}$ 使得 $c_1\mathbf{v}_1+c_2\mathbf{v}_2+c_3\mathbf{v}_3=\mathbf{0}$, 就等同於解

$$x_1\mathbf{v}_1+x_2\mathbf{v}_2+x_3\mathbf{v}_3=x_1(a_1,b_1)+x_2(a_2,b_2)+x_3(a_3,b_3)=(0,0),$$

亦即解聯立方程組

$$\begin{cases} a_1x_1+a_2x_2+a_3x_3 &=0\\ b_1x_1+b_2x_2+b_3x_3 &=0\end{cases}$$

這是有三個未知數 x_1,x_2,x_3 但僅有兩個方程式的齊次聯立方程組, 我們知道一定有無窮多解, 也就是說存在 $c_1,c_2,c_3\in\mathbb{R}$ 不全為 0 使得 $c_1\mathbf{v}_1+c_2\mathbf{v}_2+c_3\mathbf{v}_3=\mathbf{0}$. 因此 $\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3$ 一定是 linearly dependent. 我們可以利用這個概念證明以下著個重要的定理.

Lemma 3.5.5. 設 V 為 *vector space over* $\mathbb{F}$ 且 $\mathbf{v}_1,\dots,\mathbf{v}_n\in V$. 若 $\mathbf{w}_1,\dots,\mathbf{w}_m\in\mathrm{Span}(\mathbf{v}_1,\dots,\mathbf{v}_n)$ 且 $m>n$, 則 $\mathbf{w}_1,\dots,\mathbf{w}_m$ 為 *linearly dependent.*

Proof. 由於 $\mathbf{w}_1,\dots,\mathbf{w}_m\in\mathrm{Span}(\mathbf{v}_1,\dots,\mathbf{v}_n)$, 因此對任意 $j=1,\dots,m$, $\mathbf{w}_j$ 都可以寫成 $\mathbf{v}_1,\dots,\mathbf{v}_n$ 的 linear combination. 也就是說, 存在 $a_{1,j},\dots,a_{i,j},\dots,a_{n,j}\in\mathbb{R}$ 使得

$$\mathbf{w}_j=a_{1,j}\mathbf{v}_1+\cdots+a_{i,j}\mathbf{v}_i+\cdots+a_{n,j}\mathbf{v}_n.$$

現在我們要找到 $c_1,\dots,c_m\in\mathbb{R}$ 不全為 0 使得 $c_1\mathbf{w}_1+\cdots+c_m\mathbf{w}_m=\mathbf{0}$, 便證得 $\mathbf{w}_1,\dots,\mathbf{w}_m$ 為 linearly dependent. 現將 $c_1\mathbf{w}_1+\cdots+c_m\mathbf{w}_m$ 中每一個 $\mathbf{w}_j$ 換成 $\mathbf{v}_1,\dots,\mathbf{v}_n$ 的 linear combination 後會等於

$$(c_1a_{1,1}+\cdots+c_ma_{1,m})\mathbf{v}_1+\cdots+(c_1a_{i,1}+\cdots+c_ma_{i,m})\mathbf{v}_i+\cdots+(c_1a_{m,1}+\cdots+c_ma_{m,m})\mathbf{v}_m. \quad (3.1)$$

因此若我們能找到 $c_1,\dots,c_m\in\mathbb{F}$ 使得式子 (3.1) 中每個 $\mathbf{v}_i$ 的係數等於 0, 便可得到 $c_1\mathbf{w}_1+\cdots+c_m\mathbf{w}_m=\mathbf{0}$. 因此我們只要找到聯立方程組

$$\begin{cases} a_{1,1}x_1+\cdots+a_{1,m}x_m &=0\\ \qquad\vdots & \\ a_{i,1}x_1+\cdots+a_{i,m}x_m &=0\\ \qquad\vdots & \\ a_{n,1}x_1+\cdots+a_{n,m}x_m &=0\end{cases}$$

的一組解 $x_1=c_1,\dots,x_m=c_m$, 就可以使得 $c_1\mathbf{w}_1+\cdots+c_m\mathbf{w}_m=\mathbf{0}$. 然而這個 homogeneous linear system 的方程式個數 n 少於未知數個數 m. 也就是說將它對應的矩陣化為 echelon form 時, 其 pivot 的個數 (小於等於 n) 必少於 variables 的個數 m, 也就是存在著 free variables, 因此由此方程組有 $x_1=\cdots=x_n=0$ 這一組解知此方程組有其他解 (參考 Lemma 1.3.3), 即存在不全為 0 的 $c_1,\dots,c_m\in\mathbb{F}$ 使得 $x_1=c_1,\dots,x_m=c_m$ 為其一組解. 故得證 $\mathbf{w}_1,\dots,\mathbf{w}_m$ 為 linearly dependent. □

Question 3.9. 假設 $\mathbf{v}_1,\dots,\mathbf{v}_n$ 為 *linearly independent.* 若 $\mathbf{w}_1,\dots,\mathbf{w}_k\in\mathrm{Span}(\mathbf{v}_1,\dots,\mathbf{v}_n)$ 且 $k<n$, 試證明 $\mathrm{Span}(\mathbf{w}_1,\dots,\mathbf{w}_k)\neq\mathrm{Span}(\mathbf{v}_1,\dots,\mathbf{v}_n)$.

假設 W 為 V 的 subspace, 且 $\mathbf{w}_1,\ldots,\mathbf{w}_n \in W$ 為 linearly independent. 如果 $\mathbf{w}_1,\ldots,\mathbf{w}_n$ 不是 W 的 spanning vectors (即 $\mathrm{Span}(\mathbf{w}_1,\ldots,\mathbf{w}_n) \subsetneq W$), 則我們可以在 W 中選取 $\mathbf{w}_{n+1}$ 滿足 $\mathbf{w}_{n+1} \not\in \mathrm{Span}(\mathbf{w}_1,\ldots,\mathbf{w}_n)$. 此時 Lemma 3.5.4 告訴我們 $\mathbf{w}_1,\ldots,\mathbf{w}_n,\mathbf{w}_{n+1}$ 仍保持 linearly independent. 利用這個概念我們可以回答 finitely generated vector space 的 subspace 也是 finitely generated.

Proposition 3.5.6. 假設 V 為 *finitely generated vector space.* 若 W 為 V 的 *subspace,* 則 W 為 *finitely generated vector space.*

Proof. 依 V 為 finitely generated 的假設, 存在 $\mathbf{v}_1,\ldots,\mathbf{v}_n \in V$ 滿足 $\mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n) = V$. 由於 $\{\mathbf{0}\} = \mathrm{Span}(\mathbf{0})$ 為 finitely generated, 我們僅需要考慮 $W \neq \{\mathbf{0}\}$ 的情況. 我們用反證法, 假設 W 不是 finitely generated. 現任取 $\mathbf{w}_1 \in W$ 其中 $\mathbf{w}_1 \neq \mathbf{0}$. 由於 W 不是 finitely generated, 我們知 $\mathrm{Span}(\mathbf{w}_1) \neq W$, 亦即存在 $\mathbf{w}_2 \in W$ 且 $\mathbf{w}_2 \not\in \mathrm{Span}(\mathbf{w}_1)$. 由 Lemma 3.5.5 知 $\mathbf{w}_1,\mathbf{w}_2$ 為 linearly independent. 同理, 因 W 不是 finitely generated, 我們知 $\mathrm{Span}(\mathbf{w}_1,\mathbf{w}_2) \neq W$ 亦即存在 $\mathbf{w}_3 \in W$ 且 $\mathbf{w}_3 \not\in \mathrm{Span}(\mathbf{w}_1,\mathbf{w}_2)$. 由 Lemma 3.5.4 知 $\mathbf{w}_1,\mathbf{w}_2,\mathbf{w}_3$ 為 linearly independent. 這樣一直下去, 利用數學歸納法假設我們得 $\mathbf{w}_1,\ldots,\mathbf{w}_k \in W$ 為 linearly independent. 由於 $\mathrm{Span}(\mathbf{w}_1,\ldots,\mathbf{w}_k) \neq W$, 存在 $\mathbf{w}_{k+1} \in W$ 且 $\mathbf{w}_{k+1} \not\in \mathrm{Span}(\mathbf{w}_1,\ldots,\mathbf{w}_k)$. 因此再由 Lemma 3.5.4 知 $\mathbf{w}_1,\ldots,\mathbf{w}_k,\mathbf{w}_{k+}$ 為 linearly independent. 我們利用數學歸納法證明了, 若 W 不是 finitely generated, 則對任意 $m \in \mathbb{N}$, 皆存在 $\mathbf{w}_1,\ldots,\mathbf{w}_m \in W$ 為 linearly independent. 然而這在 $m > n$ 是會造成矛盾的. 因為此時由於 $\mathbf{w}_1,\ldots,\mathbf{w}_m \in W \subseteq V = \mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, Lemma 3.5.5 告訴我們 $\mathbf{w}_1,\ldots,\mathbf{w}_m$ 必為 linearly dependent. 因此知 W 為 finitely generated vector space. □

Question 3.10. 利用在 $P(\mathbb{F})$ 中對於任意 $n \in \mathbb{N}$, $x^n, x^{n-1},\ldots,x,1$ 為 *linearly independent,* 證明 $P(\mathbb{F})$ 不是 *finitely generated vector space.*

前面提過若 $\mathbf{v}_1,\ldots,\mathbf{v}_n \in V$, 要知道 $\mathbf{v} \in V$ 是否屬於 $\mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$ 這是一個存在性的問題, 也就是問是否存在 $c_1,\ldots,c_n \in \mathbb{F}$ 使得 $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$. 但若已知 $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n \in \mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 是否會存在另一組 $c'_1,\ldots,c'_n \in \mathbb{F}$ 使得 $\mathbf{v} = c'_1\mathbf{v}_1 + \cdots + c'_n\mathbf{v}_n$ 呢? 這個唯一性的問題就會和 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 是否為 linearly independent 有關了. 我們有以下的結果.

Proposition 3.5.7. 假設 V 為 *vector space over* $\mathbb{F}$ 且 $\mathbf{v}_1,\ldots,\mathbf{v}_n \in V$.

(1) 若 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 *linearly dependent,* 則對任意 $\mathbf{v} \in \mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 將 $\mathbf{v}$ 寫成 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 的 *linear combination* 的寫法不唯一. 也就是說存在 $c_1,\ldots,c_n \in \mathbb{F}$ 以及 $c'_1,\ldots,c'_n \in \mathbb{F}$ 其中某個 $c_i \neq c'_i$ 使得 $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = c'_1\mathbf{v}_1 + \cdots + c'_n\mathbf{v}_n$.

(2) 若 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 *linearly independent,* 則對任意 $\mathbf{v} \in \mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 將 $\mathbf{v}$ 寫成 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 的 *linear combination* 的寫法唯一. 也就是說若 $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$ 則對任意 $c'_1,\ldots,c'_n \in \mathbb{F}$ 其中某個 $c_i \neq c'_i$, 皆有 $\mathbf{v} \neq c'_1\mathbf{v}_1 + \cdots + c'_n\mathbf{v}_n$.

Proof. (1) 因為 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 linearly dependent, 故存在 $d_1,\ldots,d_n \in \mathbb{F}$ 且某個 $d_i \neq 0$ 使得 $d_1\mathbf{v}_1 + \cdots + d_n\mathbf{v}_n = \mathbf{0}$. 現若 $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$, 考慮 $c'_j = c_j + d_i \in \mathbb{F}$, for $j = 1,\ldots,n$. 此時因

$d_i \neq 0$, 故知 $c_i \neq c_i'$, 但我們仍有

$$c_1'\mathbf{v}_1+\cdots+c_n'\mathbf{v}_n=(c_1+d_1)\mathbf{v}_1+\cdots+(c_n+d_n)\mathbf{v}_n=$$
$$(c_1\mathbf{v}_1+\cdots+c_n\mathbf{v}_n)+(d_1\mathbf{v}_1+\cdots+d_n\mathbf{v}_n)=c_1\mathbf{v}_1+\cdots+c_n\mathbf{v}_n+\mathbf{0}=c_1\mathbf{v}_1+\cdots+c_n\mathbf{v}_n.$$

(2) 現假設 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 linearly independent, 對任意 $\mathbf{v}\in\mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 假設存在 $c_1,\ldots,c_n\in\mathbb{F}$ 以及 $c_1',\ldots,c_n'\in\mathbb{F}$ 滿足 $\mathbf{v}=c_1\mathbf{v}_1+\cdots+c_n\mathbf{v}_n$ 以及 $\mathbf{v}=c_1'\mathbf{v}_1+\cdots+c_n'\mathbf{v}_n$, 此時 $(c_1-c_1')\mathbf{v}_1+\cdots+(c_n-c_n')\mathbf{v}_n=\mathbf{0}$, 故由 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 linearly independent 知 $c_1-c_1'=\cdots=c_n-c_n'=0$, 即 $c_1=c_1',\ldots,c_n=c_n'$, 得證 $\mathbf{v}$ 寫成 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 的 linear combination 的寫法唯一. □

3.6. Basis and Dimension

對於一個 vector space V, 我們希望能找到一個集合 S 使得 $V=\mathrm{Span}(S)$. 這樣我們要了解 V 便只要了解 S 即可. 當然了 S 越大越容易展成 V, 但是我們又希望其越小越好, 這樣就可以用小一點的集合來了解 V. 如何找到這樣大小合宜的 S 便是 basis 的概念.

假設 V 是 over $\mathbb{F}$ 的 vector space 且 $V\neq\{\mathbf{0}\}$. 我們可以在 V 中任取非零向量 $\mathbf{v}_1$, 考慮 $\mathrm{Span}(\mathbf{v}_1)$. 若 $\mathrm{Span}(\mathbf{v}_1)=V$, 則我們找到集合 $S_1=\{\mathbf{v}_1\}$ 使得 $\mathrm{Span}(S_1)=V$, 且由於 $\mathbf{v}_1\neq\mathbf{0}$, 依定義 S_1 是 linearly independent. 若 $\mathrm{Span}(\mathbf{v}_1)\subsetneq V$, 表示存在 $\mathbf{v}_2\in V$ 且 $\mathbf{v}_2\notin\mathrm{Span}(\mathbf{v}_1)$, 此時考慮 $S_2=\{\mathbf{v}_1,\mathbf{v}_2\}$. 由於 $\mathbf{v}_2\notin\mathrm{Span}(\mathbf{v}_1)$, 我們知 $\mathbf{v}_1,\mathbf{v}_2$ 是 linearly independent, 故若 $\mathrm{Span}(S_2)=V$, 我們找到了 S_2 是 V 的 spanning set 且 S_2 為 linearly independent. 這樣一直下去假設我們找到 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 為 V 的 spanning set 且為 linearly independent. 此時有了 spanning set 的存在性以及 linearly independent 的唯一性, 則 V 中的元素都可以唯一寫成 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 的 linear combination, 也因此我們有以下的定義.

Definition 3.6.1. 假設 V 為 vector space. 若 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 為 V 的 spanning set 且為 linearly independent, 則稱 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 V 的一組 *basis*.

首先要注意 spanning set 未必是 linearly independent. 例如在 $\mathbb{R}^2$ 中 $\{\mathbf{v}_1=(1,0),\mathbf{v}_2=(0,1),\mathbf{v}_3=(1,1)\}$ 是 $\mathbb{R}^2$ 的 spanning set, 但不是 linearly independent (因 $\mathbf{v}_3=\mathbf{v}_1+\mathbf{v}_2$). 同樣的 linearly independent 的元素未必形成 spanning set. 例如在 $\mathbb{R}^3$ 中 $\mathbf{w}_1=(1,0,0),\mathbf{w}_2=(0,1,0)$ 就是 linearly independent, 但 $\mathrm{Span}(\mathbf{w}_1,\mathbf{w}_2)\neq\mathbb{R}^3$. 因此要說明 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 V 的一組 basis, 必須說明 $\mathrm{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)=V$ 以及 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 linearly independent, 缺一不可. 當然了, 若 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 為 V 的 spanning set 或 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 為 linearly independent 其中只要任一項不滿足, 則知 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 不是 V 的 basis. 例如前面舉的例子 $\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3$ 就不是 $\mathbb{R}^2$ 的 basis, 而 $\mathbf{w}_1,\mathbf{w}_2$ 也不是 $\mathbb{R}^3$ 的 basis. 接下來我們看幾個常見的 vector space 的 basis.

Example 3.6.2. 假設 $\mathbb{F}$ 是一個 field, 我們考慮以下常見 over $\mathbb{F}$ 的 vector spaces.

(A) 在 $\mathbb{F}^n$ 中考慮 $\mathbf{e}_1=(1,0,\ldots,0),\mathbf{e}_2=(0,1,0,\ldots,o),\ldots,\mathbf{e}_n=(0,0,\ldots,o,1)$ (即 $\mathbf{e}_i$ 為 i-th entry 為 1, 其他 entry 為 0 的向量), 由於對任意 $(c_1,\ldots,c_n)\in\mathbb{F}^n$, 我們有 $(c_1,\ldots,c_n)=c_1\mathbf{e}_1+\cdots+c_n\mathbf{e}_n$, 知 $\mathrm{Span}(\mathbf{e}_1,\ldots,be_n)=\mathbb{F}^n$. 又若 $c_1\mathbf{e}_1+\cdots+c_n\mathbf{e}_n=\mathbf{0}$, 表示 $(c_1,\ldots,c_n)=(0,\ldots,0)$,

亦即 $c_1 = \cdots = c_n = 0$, 故知 $\mathbf{e}_1, \ldots, be_n$ 為 linearly independent. 因此 $\mathbf{e}_1, \ldots, \mathbf{e}_n$ 為 $\mathbb{F}^n$ 的一組 basis. 這一組 basis 是 $\mathbb{F}^n$ 中最直接且最常用的 basis 所以我們又稱之為 $\mathbb{F}^n$ 的 *standard basis*.

(B) 在 $M_{m\times n}(\mathbb{F})$ 中, 考慮 E_{ij}, 為 (i,j)-th entry 為 1, 其他 entry 為 0 的 $m \times n$ matrix. 則利用和 $\mathbb{F}^n$ 上類似的證法, 我們可以知 $\{E_{ij} : 1 \le i \le m, 1 \le j \le n\}$ 是 $M_{m\times n}(\mathbb{F})$ 的 spanning set 且為 linearly independent, 故為 $M_{m\times n}(\mathbb{F})$ 的一組 basis.

(C) 在 $P_n(\mathbb{F})$ 中 $\{1, x, x^2, \ldots, x^n\}$ 可展成 $P_n(\mathbb{F})$ 且為 linearly independent, 所以是 $P_n(\mathbb{F})$ 的 basis. 這組 basis 也稱為 $P_n(\mathbb{F})$ 的 *standard basis*.

在 Definition 3.6.1 中 V 可由有限多個元素所展成, 所以此時的 V 依定義是 finitely generated vector space (Definition 3.4.3), 不過我們提過一般的 vector space 未必會是 finitely generated, 所以對於一般的 vector space, 我們有以下 basis 的定義.

Definition 3.6.3. 假設 V 為 vector space 且 $S \subseteq V$. 若 S 為 V 的 spanning set 且為 linearly independent, 則稱 S 為 V 的一組 *basis*.

由於我們已定義 $\mathrm{Span}(\emptyset) = \{\mathbf{0}\}$ 且 $\emptyset$ 為 linearly independent, 所以依照 Definition 3.6.3, 我們說空集合 $\emptyset$ 是 zero vector space $\{\mathbf{0}\}$ 的 basis. 另外在 Example 3.4.4 中我們知道 $P(\mathbb{F})$ 不是 finitely generated. 然而很容易看出 $\{1, x, x^2, \ldots\}$ 是 $P(\mathbb{F})$ 的 spanning set 且為 linearly independent, 所以 $\{1, x, x^2, \ldots\}$ 是 $P(\mathbb{F})$ 的 basis.

我們碰到的第一個問題便是 basis 的存在性問題. 也就是說, 對於一般的 vector space 是不是都會有 basis. 接下來我們要說明非零的 finitely generated vector space 都會有 basis. 其實這對於不是 finitely generated 的 vector space 也對, 不過由於這會牽涉到較抽象的邏輯概念而且我們以後談論的 vector space 都是 finitely generated, 所以我們不去談論它. 在本講義中我們僅探討 finitely generated vector space.

Proposition 3.6.4. 假設 $V \neq \{\mathbf{0}\}$ 為 *vector space over* $\mathbb{F}$, 且 $S \subseteq V$ 為一個 *finite set* 滿足 $V = \mathrm{Span}(S)$. 則存在 $S' \subseteq S$ 為 V 的一組 *basis*. 也就是說, 若 $V \neq \{\mathbf{0}\}$ 為 *finitely generated vector space over* $\mathbb{F}$, 則存在 $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ 為 V 的一組 *basis*.

Proof. 我們對 S 的元素個數 n 做數學歸納法. 假設 $n = 1$, 即 $V = \mathrm{Span}(\mathbf{v}_1)$, 因 $V \neq \{\mathbf{0}\}$, 知 $\mathbf{v}_1 \neq \mathbf{0}$. 故由 $\mathbf{v}_1$ 本身是 linearly independent, 得證 $S = \{\mathbf{v}_1\}$ 是 V 的 basis. 假設 $n = k$ 時成立, 亦即對所有有 k 元素的集合 S, 若 $V = \mathrm{Span}(S)$, 則存在 $S' \subseteq S$ 為 V 的 basis. 我們要證明當 $n = k+1$ 時亦成立. 現假設 $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_{k+1}\}$ 且 $\mathrm{Span}(S) = V$, 若 S 為 linearly independent, 則依定義令 $S' = S$, 即為 V 的一組 basis. 而若 S 不是 linearly independent, 則不失一般性, 我們假設 $\mathbf{v}_1 \in \mathrm{Span}(\mathbf{v}_2, \ldots, \mathbf{v}_n)$. 此時令 $\tilde{S} = S \setminus \{\mathbf{v}_1\} = \{\mathbf{v}_2, \ldots, \mathbf{v}_n\}$, 因 $V = \mathrm{Span}(\tilde{S})$ 且 $\tilde{S}$ 的元素個數為 k, 故由歸納假設知存在 $S' \subseteq \tilde{S} \subseteq S$ 為 V 的一組 basis. 得證本定理. $\square$

Proposition 3.6.4 說的是當 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 是 V 的 spanning set, 則我們可以在 $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ 中捨去一些元素使其為 linearly independent 且仍為 V 的 spanning set, 故可成為 V 的一組 basis. 反之, 若 $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ 為 V 的一組 linearly independent set, 則我們可以加入一些元素

擴大 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$, 使其成為 V 的 spanning set 且仍保持 linearly independent, 故可成為 V 的一組 basis. 我們有以下的定理.

Proposition 3.6.5. 假設 $V \neq \{\mathbf{0}\}$ 為 *vector space over* $\mathbb{F}$, 且 $V = \operatorname{Span}(\mathbf{u}_1,\ldots,\mathbf{u}_m)$. 若 $S = \{\mathbf{v}_1,\ldots,\mathbf{v}_n\} \subseteq V$ 為 *linearly independent,* 則存在 $S' \subseteq \{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 使得 $S \cup S'$ 為 V 的 *basis.*

Proof. 我們依然對 S 的元素個數做歸納法, 不過這次是做反向的歸納法. 注意因 $V = \operatorname{Span}(\mathbf{u}_1,\ldots,\mathbf{u}_m)$ 且 $\mathbf{v}_1,\ldots,\mathbf{v}_n$ 為 linearly independent, 故由 Lemma 3.5.5 知 $n \leq m$, 所以我們可以假設 $n = m-t$, 其中 $0 \leq t \leq m-1$. 我們要對 t 做 mathematical induction. 當 $t = 0$ 時表示 $m = n$, 此時我們要說明 $S = \{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 為 V 的 spanning set. 這是因為若 $\operatorname{Span}(S) \neq V$, 表示存在 $\mathbf{w} \in V$ 且 $\mathbf{w} \notin \operatorname{Span}(S)$, 故由 Lemma 3.5.4 知 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n,\mathbf{w}\}$ 為 linearly independent, 但此時 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n.\mathbf{w}\}$ 有 $n+1 = m+1$ 個元素, 多於 $\operatorname{Span}(\mathbf{u}_1,\ldots,\mathbf{u}_m)$ 的 m 個元素, 與 Lemma 3.5.5 相矛盾, 故知 S 為 V 的 spanning set. 再利用已知 S 為 linearly independent, 故令 $S' = \emptyset$ 得證 $S = S \cup S'$ 為 V 的 basis. 現假設 $t = k$ 時成立, 即若 $S = \{\mathbf{v}_1,\ldots,\mathbf{v}_{m-k}\}$ 為 linearly independent, 則存在 $S' \subseteq \{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 使得 $S \cup S'$ 為 V 的 basis. 現考慮 $t = k+1$ 的情形, 即 $S = \{\mathbf{v}_1,\ldots,\mathbf{v}_{m-k-1}\}$ 為 linearly independent. 首先考慮 S 是否為 V 的 spanning set. 若 $V = \operatorname{Span}(S)$, 則依定義知 S 為 V 的一組 basis, 故取 $S' = \emptyset$, 則 $S' \subseteq \{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$, 且 $S \cup S' = S$ 為 V 的 basis. 而若 $\operatorname{Span}(S) \neq V$, 表示 $\{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 中必有一元素 $\mathbf{u}_i \notin \operatorname{Span}(S)$, 否則若 $\mathbf{u}_1,\ldots,\mathbf{u}_m$ 皆屬於 $\operatorname{Span}(S)$, 會造成 $V = \operatorname{Span}(\mathbf{u}_1,\ldots,\mathbf{u}_m) \subseteq \operatorname{Span}(S)$ 之矛盾. 現考慮 $\tilde{S} = S \cup \{\mathbf{u}_i\}$, 因 $\mathbf{u}_i \notin \operatorname{Span}(S)$ 由 Lemma 3.5.4 知 $\tilde{S}$ 為 linearly independent, 再由 $\tilde{S}$ 的元素個數為 $m-k$, 故由歸納假設知存在 $\tilde{S}' \subseteq \{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 使得 $\tilde{S} \cup \tilde{S}'$ 為 V 的 basis. 故令 $S' = \{\mathbf{u}_i\} \cup \tilde{S}'$, 我們有 $S' \subseteq \{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 且 $S \cup S' = S \cup \{\mathbf{u}_i\} \cup \tilde{S}' = \tilde{S} \cup \tilde{S}'$ 為 V 的 basis. □

我們已經知道 finitely generated vector space 的 basis 是存在的, 不過它並不唯一. 例如在 $\mathbb{R}^2$ 中除了 standard basis $\{(1,0),(0,1)\}$ 外, 我們很容易看出 $\{(1,1),(0,1)\}$ 也可以是 $\mathbb{R}^2$ 的 basis. 不過 basis 雖然不唯一, 不過在 finitely generated vector space 中組成 basis 的元素個數是固定的. 我們有以下的定理.

Theorem 3.6.6. 假設 V 為 *vector space over* $\mathbb{F}$, 且 $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ 和 $\{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 皆為 V 的 *basis,* 則 $n = m$.

Proof. 我們用反證法, 假設 $n \neq m$, 不失一般性我們就假設 $m > n$. 因 $V = \operatorname{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 故 $\mathbf{u}_i \in \operatorname{Span}(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, $\forall i = 1,\ldots,m$. 因此由 Lemma 3.5.5 知 $\{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 是 linearly dependent. 此與 $\{\mathbf{u}_1,\ldots,\mathbf{u}_m\}$ 是 basis 的假設相矛盾, 故得證 $m = n$. □

Theorem 3.6.6 告訴我們組成 V 的一組 basis 的元素個數是固定的. 也就是說若找到 n 個元素形成 V 的 basis, 則 V 其他的 basis 一定也會是由 n 個元素所組成. 由於這個重要的結果我們有以下的定義.

Definition 3.6.7. 假設 V 是一個 finitely generated vector space over $\mathbb{F}$. 組成 V 的一組 basis 的元素個數稱為 V over $\mathbb{F}$ 的 *dimension* (維度), 用 $\dim_{\mathbb{F}}(V)$ 來表示.

由於組成 finitely generated vector space 的一組 basis 的元素個數是有限的, 所以以後我們稱 finitely generated vector space 為 *finite dimensional vector space*.

Example 3.6.8. 我們探討在 Example 3.6.2 中的 finite dimensional vector space 的維度為多少.

(A) 考慮 $\mathbb{F}^n$ 中的 standard basis $\{\mathbf{e}_i \mid 1 \leq i \leq n\}$, 因為共有 n 個元素所以 $\dim_{\mathbb{F}}(\mathbb{F}^n) = n$.

(B) 我們知道 $\{E_{ij} \in \mathscr{M}_{m\times n} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ 是 $\mathscr{M}_{m\times n}(\mathbb{F})$ 的一組 basis. 因此 $\dim \mathbb{F}(\mathscr{M}_{m\times n}) = m \times n$.

(C) 我們知道 $\{x^n, \ldots, x, 1\}$ 是 $P_n(\mathbb{F})$ 的 spanning set 且為 linearly independent. 故知 $\{x^n, \ldots, x, 1\}$ 為 $P_n(\mathbb{F})$ 的一組 basis, 因此 $\dim_{\mathbb{F}}(P_n(\mathbb{F})) = n+1$.

大家或許注意到, 我們在表示維度的 dim 符號的下標特別標上 $\mathbb{F}$, 即 $\dim_{\mathbb{F}}$. 這個原因是強調我們將 vector space 看成 over $\mathbb{F}$ 的 vector space 所得的 dimension. 我們曾經提過, 同樣的集合我們有可能看成 over 不同的 field 的 vector space. 在此情況之下它們的 basis 也就會不同, 也因此我們要標示用哪一個 field. 我們看以下的例子.

Example 3.6.9. 我們用 $\mathbb{C}$ 表示 complex numbers (複數) 所成的 field, 而用 $\mathbb{R}$ 表示 real numbers (實數) 所成的 field. 現考慮集合 $\mathbb{C}^2 = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\}$. 很容易檢查用一般的加法及係數積, $\mathbb{C}^2$ 是 vector space over $\mathbb{C}$, 也會是 vector space over $\mathbb{R}$. 首先我們知道 $\{(1,0),(0,1)\}$ 是 $\mathbb{C}^2$ 看成 over $\mathbb{C}$ 的 vector space 的 basis (Example 3.6.2 (A) $n=2$, $\mathbb{F}=\mathbb{C}$ 的情況), 所以我們得 $\dim_{\mathbb{C}}(\mathbb{C}^2) = 2$. 不過 $\{(1,0),(0,1)\}$ 在 over $\mathbb{R}$ 之下就不是 basis 了. 很容易看出來任何 $(1,0),(0,1)$ over $\mathbb{R}$ 的 linear combination 都無法表示 $(i,0)$ 這一個 $\mathbb{C}^2$ 的元素 (這裡 i 是滿足 $i^2=-1$ 的純虛數). 不過 $\{(1,0),(i,0),(0,1),(0,i)\}$ 就是 $\mathbb{C}^2$ over $\mathbb{R}$ 的 spanning set. 這是因為任意 $\mathbb{C}^2$ 的元素都可以寫成 $(a+bi, c+di)$ 其中 $a,b,c,d \in \mathbb{R}$, 所以可得 $(a+bi, c+di) = a(1,0)+b(i,0)+c(0,1)+d(0,i)$. 又 $\{(1,0),(i,0),(0,1),(0,i)\}$ over $\mathbb{R}$ 是 linearly independent. 這是因為若 a,b,c,d 是實數滿足 $a(1,0)+b(i,0)+c(0,1)+d(0,i) = (0,0)$, 即表示 $a+bi=0$ 且 $c+di=0$, 故得 $a=b=c=d=0$. 由此知 $\{(1,0),(i,0),(0,1),(0,i)\}$ 是 $\mathbb{C}^2$ over $\mathbb{R}$ 的 basis, 所以我們有 $\dim_{\mathbb{R}}(\mathbb{C}^2) = 4$.

由 Example 3.6.9, 我們知道要說明一個 vector space 的 dimension 為何, 一定要說明其 over 的 field 是甚麼. 不過一般情形, 當我們很明確知道 over 的 field 是甚麼而沒有如 Example 3.6.9 這種模稜兩可的情形, 我們便會省略直接用 $\dim(V)$ 來表示其 dimension.