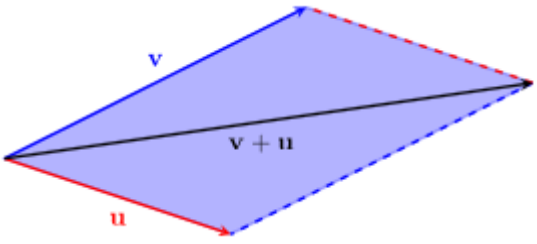
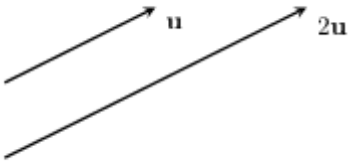
感受伽羅瓦：向量空間與子域

在前面各章，我們介紹了與群和環有關的基本理論，群和環分別是包含一種和兩種運算的重要代數結構。由本章開始，我們將把注意力放在環的一個重要次類－域之上。但在詳細討論域之前，須先介紹另一種代數結構－「向量空間」，因為這種代數結構的某些概念在域上有重要應用。

向量(vector) 本來是物理學上的概念，是指一種既有大小又有方向的量，以區別於只有大小而沒有方向的純量(scalar)。舉例說，溫度、質量、電荷量等便是純量，而力、速度、電場強度等則是向量。物理學上常用箭頭代表向量，其中箭頭的長度和方向分別代表向量的大小和方向。

向量除了可用來表示某些物理量外，還可進行數學運算，最重要的運算有兩種：(i) 我們可以對兩個向量 $\vec{u}$ 和 $\vec{v}$[1]進行加法運算，得出另一個向量 $\vec{u}+\vec{v}$。向量的加法結果可用「平行四邊形法則」求得；(ii) 我們也可以把一個純量 k 與一個向量 $\vec{u}$ 進行純量乘法(scalar multiplication)，得出另一個向量 $k\vec{u}$。純量乘法的直觀意義就是把向量按其原有方向 (若 $k>0$) 或反方向 (若 $k<0$) 延長 (若 $|k|>1$) 或縮短 (若 $|k|<1$)。下面左圖展示運用「平行四邊形法則」計算 $\vec{v}+\vec{u}$，右圖則顯示 $2\vec{u}$ 是把 $\vec{u}$ 按其原有方向延長一倍的結果。



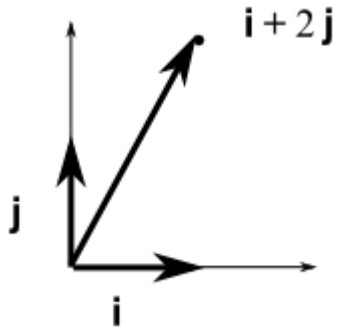


為方便進行計算，一般會為向量引入一個坐標系 (包括坐標原點、坐標軸和各條坐標軸上的單位長度)，並為每條坐標軸引入一個單位向量(unit

[1]以下將沿用學界的習慣，在表示物理學或幾何學上的一般向量時，在代表向量的字母上加上小箭頭 (單位向量則加上小帽子)；但在表示抽象代數學上的向量時，則不加任何附加符號。

vector)，這個單位向量的方向與所在坐標軸的方向一致，其長度則等於所在坐標軸的單位長度，這樣便可把任何向量唯一地表示成單位向量的線性組合(linear combination)。線性組合的定義如下：設 $\hat{v_1}$、...、$\hat{v_n}$ 為單位向量，那麼這些單位向量的線性組合就是 $a_1\hat{v_1} + \cdots + a_n\hat{v_n}$，其中 a_1、...、a_n 是純量，這些純量稱為向量 $\vec{v}$ 相對於不同單位向量的分量(component)。

舉例說，下圖顯示一個平面直角坐標系及其上的兩個單位向量 $\hat{i}$ 和 $\hat{j}$ 以及 $\hat{i}$ 和 $\hat{j}$ 的一個線性組合：$\hat{i} + 2\hat{j}$。請注意下圖中的單位向量提供了坐標系的所有信息：這兩個單位向量的共同源點就是坐標原點，兩個單位向量的方向和長度就是兩個坐標軸的方向以及其上的單位長度。



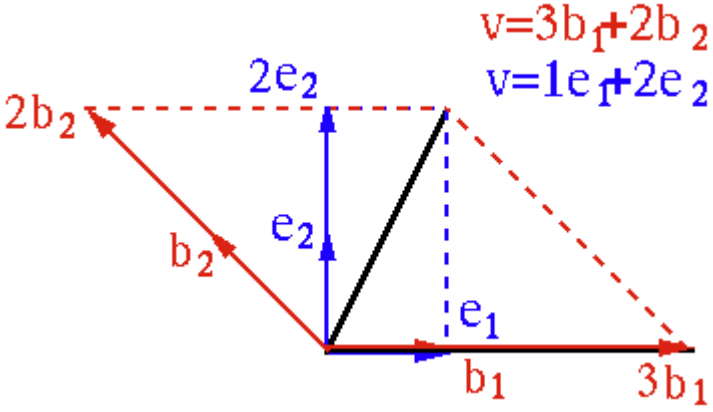
把向量表示成單位向量的線性組合後，便容易進行向量的加法和純量乘法，設 $a\hat{i} + b\hat{j}$ 和 $c\hat{i} + d\hat{j}$ 為任意向量，k 為任意純量，則

$$\begin{aligned} (a\hat{i} + b\hat{j}) + (c\hat{i} + d\hat{j}) &= (a + c)\hat{i} + (b + d)\hat{j} \qquad (1) \\ k(a\hat{i} + b\hat{j}) &= ka\hat{i} + kb\hat{j} \qquad (2) \end{aligned}$$

請注意如果暫時忘記上述兩條公式中的 a、b、c、d、k、$\hat{i}$ 和 $\hat{j}$ 所代表的不同類型的量 (即純量和向量)，把它們統統當作普通實數處理，那麼以上兩式中的運算完全符合實數的加法和乘法法則。特別地，我們看到純量乘法對向量加法滿足分配性，即有 $(a + c)\hat{i} = a\hat{i} + c\hat{i}$ 和 $k(\hat{i} + \hat{j}) = k\hat{i} + k\hat{j}$[2]。這就是把向量表示成單位向量的線性組合的優點，它使我們在進行向量的加法和純量乘法時，可以沿用實數的加法和乘法法則。

上述例子中的坐標系是直角坐標系，即各坐標軸互相垂直的坐標系，這是人們最熟悉的坐標系。但在表示向量時，其實也可使用「斜角坐標系」，即各坐標軸並非互相垂直的坐標系。下圖展示同一個向量 $\vec{v}$(即黑色的向量)在不同坐標系下的情況，其中藍色的坐標系是直角坐標系，紅色的則是斜角坐標系：

[2]另外還可證明，(1) – (2) 所定義的加法和純量乘法運算跟前述用「平行四邊形法則」進行的向量加法運算以及把向量的純量乘法運算理解為延長／縮短向量的觀點是一致的。



上圖顯示不同坐標系各有不同的單位向量，其中 $\hat{e}_1$ 和 $\hat{e}_2$ 是直角坐標系下的單位向量，$\hat{b}_1$ 和 $\hat{b}_2$ 則是斜角坐標系下的單位向量。向量 $\vec{v}$ 在不同的坐標系下有不同的分量，因而表示為不同的形式。在直角坐標系下，$\vec{v}$ 相對於 $\hat{e}_1$ 和 $\hat{e}_2$ 的分量分別是 1 和 2，因而表示為 $\hat{e}_1 + 2\hat{e}_2$；在斜角坐標系下，$\vec{v}$ 相對於 $\hat{b}_1$ 和 $\hat{b}_2$ 的分量則分別是 3 和 2，因而表示為 $3\hat{b}_1 + 2\hat{b}_2$。

斜角坐標系是對傳統直角坐標系的推廣，但請注意在平面上並非任何兩個單位向量都可構成坐標系。如果兩個單位向量連成一條直線 (即「共線」colinear)，那麼對於不在這條直線上的點，我們無法求這些點相對於這些單位向量的分量，因此這兩個單位向量不能構成坐標系。類似地，在三維空間上也並非任何三個單位向量都可構成坐標系。如果三個單位向量處在同一個平面上 (即「共面」coplanar)，那麼對於不在這個平面上的點，我們無法求這些點相對於這些單位向量的分量，因此這三個單位向量也不能構成坐標系。

以上介紹了物理學或幾何學研究的向量，但我們可以把向量的概念加以推廣，將之看成一種抽象的數學對象，這種數學對象構成一種獨特的代數結構—向量空間(vector space)。設 $(V, +)$ 為交換群，$(F, +', \times')$ 為域，則 V 是 F 上的向量空間，當且僅當對任何 $v \in V$ 和 $a \in F$，都可進行純量乘法，其結果 $av \in V$，而且上述純量乘法運算滿足以下公理 (在以下公理中，$v, w \in V$，$a, b \in F$，1 是 F 的乘法單位元)：

(i) $a(v + w) = av + aw$

(ii) $(a +' b)v = av + bv$

(iii) $(a \times' b)v = a(bv)$

(iv) $1v = v$

此外，我們還把上述集合 V 的元素稱為向量，F 的元素稱為純量。

根據上述定義，任何滿足上述運算公理的交換群 $(V,+)$ 和域 $(F,+',\times')$ 都構成向量空間，而不必考究這些向量和純量是否有物理或幾何意義，以下提供兩個向量空間的例子。在第一個例子中，我們把 $(V,+)$ 和 $(F,+',\times')$ 分別定為 $(\mathbb{R}^2,+)$ 和 $(\mathbb{R},+,\times)$，得到 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$，這個空間的「向量」是由實數組成的有序對 (即 $\mathbb{R}^2$ 的成員)，「純量」則是實數。我們可以為這個空間定義向量的加法和純量乘法運算法則如下，設 $(a,b),(c,d)\in\mathbb{R}^2$，$k\in\mathbb{R}$，則

$$\begin{aligned}(a,b)+(c,d) &= (a+c,b+d) \qquad (3)\\ k(a,b) &= (ka,kb) \qquad (4)\end{aligned}$$

容易看到，這個向量空間上的向量與前述物理學上的平面向量是互相對應的，例如平面向量 $a\hat{i}+b\hat{j}$ 對應著有序對 (a,b)，而 $(3)-(4)$ 所定義的加法和純量乘法運算法則跟前面 $(1)-(2)$ 所定義的同類運算法是一模一樣的。此外，也容易看到這個向量空間上的純量乘法滿足上述各條公理。

在第二個例子中,我們把 $(V,+)$ 和 $(F,+',\times')$ 分別定為 $(\mathbb{Q}[x],+)$ 和 $(\mathbb{Q},+,\times)$，得到 $\mathbb{Q}$ 上的向量空間 $\mathbb{Q}[x]$，這個空間的「向量」是有理係數多項式，「純量」則是有理數。容易看到，任意有理數與有理係數多項式之間都可進行純量乘法，其結果是有理係數多項式，例如有理數 $\frac{1}{3}$ 與有理係數多項式 $6x^2-5x+\frac{1}{2}$ 進行純量乘法的結果是有理係數多項式 $2x^2-\frac{5}{3}x+\frac{1}{6}$，而且這種純量乘法運算滿足上述各條公理。

前面提過，可以為向量引入坐標系，即確定一些單位向量，並把任何向量唯一地表示成這些單位向量的線性組合。請注意這裡包含兩個要求：(i) 任何向量都可表示成單位向量的線性組合；(ii) 上述線性組合是唯一的。上述概念也可推廣至一般的向量空間，從而得到基底(basis) 的概念。設有一個 F 上的向量空間 V，這個向量空間的基底是 V 的一個子集 $W=\{v_1,\ldots,v_n\}$ (其中各個 $v_i\,(1\le i\le n)$ 稱為基底向量(basis vector)) 使得 (i) V 中任何元素都可表示成各個基底向量的線性組合，並且 (ii) 上述線性組合是唯一的，即任何 $v\in V$ 都可唯一地表示成 $v=a_1v_1+\cdots+a_nv_n$，其中 $a_1,\ldots a_n\in F$。根據上述定義，基底向量起著類似單位向量的作用，而上述定義中的各個 $a_i\,(1\le i\le n)$ 則可稱為 v 相對於 v_i 的分量。

以 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$ 為例，這個空間的一個基底是 $W_1=\{(1,0),(0,1)\}$，這是因為 $\mathbb{R}^2$ 中的任何元素 (a,b) 都可唯一地表示成 $(a,b)=a(1,0)+b(0,1)$，例如 $(2,-3)=(2)(1,0)+(-3)(0,1)$。另外又如 $\mathbb{Q}$ 上的向量空間 $\mathbb{Q}[x]$, 這個空間的一個基底是無窮集合 $W_2=\{1,x,x^2,x^3,\ldots,x^n,\ldots\}$，這是因為 $\mathbb{Q}[x]$ 中的任何元素 $a_0+\cdots+a_nx^n$ 都可唯一地表示成 $a_0+\cdots+a_nx^n=a_0(1)+\cdots+$

$a_n(x^n)+0(x^{n+1})+\cdots$, 例如 $2x^2-\frac{5}{3}x+\frac{1}{6}=\frac{1}{6}(1)+(-\frac{5}{3})(x)+2(x^2)+0(x^3)+\cdots$。

一個向量空間往往不只一個基底，以 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$ 為例，除了前述的 W_1 外，這個空間的基底還可以是 $W_3=\{(1,1),(1,-1)\}$，這是因為 (a,b) 可唯一地表示成

$$(a,b)=\left(\frac{a+b}{2}\right)(1,1)+\left(\frac{a-b}{2}\right)(1,-1)$$

例如 $(2,-3)=-\frac{1}{2}(1,1)+\frac{5}{2}(1,-1)$。另外又如 $\mathbb{Q}$ 上的向量空間 $\mathbb{Q}[x]$,除了前述的 W_2 外,這個空間的基底還可以是 $W_4=\{1+x^2,x+x^3,\frac{1}{2}x^2,2x^3,x^4,x^5,\ldots,x^n,\ldots\}$，這是因為 $a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+\cdots+a_nx^n$ 可唯一地表示成

$$\begin{aligned} & a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+\cdots+a_nx^n \\ = \; & a_0(1+x^2)+a_1(x+x^3)+(2a_2-2a_0)\left(\frac{1}{2}x^2\right)+\left(\frac{a_3-a_1}{2}\right)(2x^3)+ \\ & a_4(x^4)+\cdots+a_n(x^n)+0(x^{n+1})+\cdots \end{aligned}$$

例如 $2x^2-\frac{5}{3}x+\frac{1}{6}=\frac{1}{6}(1+x^2)+(-\frac{5}{3})(x+x^3)+\frac{11}{3}(\frac{1}{2}x^2)+(\frac{5}{6})(2x^3)+0(x^4)+\cdots$。

前面說過，並非任何單位向量的集合都可構成坐標系；同樣，就某個向量空間而言，並非其中任何向量的集合都可構成基底。為了精確地說明某向量集合構成基底所須滿足的條件，以下先引入「生成空間」、「線性相關」、「線性獨立」等概念。

設有域 F 上的向量空間 V，$W=\{v_1,\ldots,v_n\}$ 是 V 的子集，我們把 W 中各個向量的所有線性組合稱為 W 的生成空間(span)，記作 $\langle v_1,\ldots,v_n\rangle$，即

$$\langle v_1,\ldots,v_n\rangle=\{a_1v_1+\cdots+a_nv_n:a_1,\ldots,a_n\in F\}$$

向量集合 W 是線性相關(linearly dependent) 的當且僅當存在 $a_1,\ldots,a_n\in F$, 其中 a_1、...、a_n 不全為 0, 使得 $a_1v_1+\cdots+a_nv_n=0$[3]；否則這個集合是線性獨立(linearly independent) 的, 或者換句話說, 如有 $a_1v_1+\cdots+a_nv_n=0$, 則必有 $a_1=\cdots=a_n=0$，則 W 是線性獨立的。具備上述概念，我們便可以寫出 $W=\{v_1,\ldots,v_n\}$ 構成向量空間 V 的基底所須滿足的條件如下：(i) $\langle v_1,\ldots,v_n\rangle=V$；(ii) W 是線性獨立的。

以前面討論過的 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$ 和向量集合 $W_1=\{(1,0),(0,1)\}$

[3]由於 V 和 F 中都有加法單位元，兩者都記作 0，這裡要小心分辨究竟是指哪一個 0，一般來說根據上下文不難判斷是指哪個 0，例如在 $a_1\neq 0$ 中的 0 是指 F 中的 0；而在 $a_1v_1+\cdots+a_nv_n=0$ 中的 0 則是指 V 中的 0。

為例，可以證明 W_1 滿足上述兩個條件，因而是 $\mathbb{R}^2$ 的基底。首先，要證明 (i) $\langle (1,0),(0,1)\rangle = \mathbb{R}^2$，證明步驟如下：

$$\begin{aligned}\langle (1,0),(0,1)\rangle &= \{a(1,0)+b(0,1) : a,b \in \mathbb{R}\} \\ &= \{(a,b) : a,b \in \mathbb{R}\} \\ &= \mathbb{R}^2\end{aligned}$$

其次，要證明 (ii) W_1 是線性獨立的。為此，假設 $a(1,0)+b(0,1)=(0,0)$，並解出 a 和 b 如下：

$$\begin{aligned}a(1,0)+b(0,1) &= (0,0) \\ (a,b) &= (0,0)\end{aligned}$$

由此必有 $a=b=0$，證得 W_1 是線性獨立的[4]。

只要向量集合 W 違反上述兩個條件之中任何一個，W 便不構成基底，以下讓我們看 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$ 的一些反例，首先看違反上述條件 (i) 的一個例子。設 $W_5=\{(1,0)\}$，那麼 W_5 違反條件 (i)(但滿足條件 (ii)，請讀者自行證明這一點)，這是因為

$$\begin{aligned}\langle (1,0)\rangle &= \{a(1,0) : a \in \mathbb{R}\} \\ &= \{(a,0) : a \in \mathbb{R}\} \\ &\neq \mathbb{R}^2\end{aligned}$$

因此 W_5 並不構成基底，事實上，容易看到在 $\mathbb{R}^2$ 中，所有第二坐標不等於 0 的成員 (例如 $(1,1)$) 都不能表示成 W_5 中成員的線性組合。

其次看違反上述條件 (ii) 的例子。設 $W_6=\{(1,0),(0,1),(1,1)\}$，那麼 W_6 違反條件 (ii)(但滿足條件 (i)，請讀者自行證明這一點)，即 W_6 是線性相關的，這是因為存在 $1,-1 \in \mathbb{R}$，其中 1、-1 不全為 0，使得 $(1)(1,0)+(1)(0,1)+(-1)(1,1)=(0,0)$。因此 W_6 並不構成基底，事實上，$\mathbb{R}^2$ 中的每個元素雖可表示成 W_6 中成員的線性組合，但這些線性組合並不唯一，這是因為 $\mathbb{R}^2$ 中的任意成員 (a,b) 既可表示成 $a(1,0)+b(0,1)+(0)(1,1)$，又可表示成 $(a-1)(1,0)+(b-1)(0,1)+(1)(1,1)$ 等等，例如 $(2,-3)=(2)(1,0)+(-3)(0,1)+(0)(1,1)=(1)(1,0)+(-4)(0,1)+(1)(1,1)$ 等等。

前面說過，一個向量空間往往不只一個基底，但可以證明，一個向量空間的任何基底都必然包含相同數目的基底向量，這個數目稱為這個向量空

[4]當 W 所含向量數目頗多時，上述證明方法會變得很繁複，在線性代數中有一些較簡便的方法，可用來確定某一向量集合是否線性獨立，但須引入更多概念，本文不擬介紹，有興趣的讀者請參閱相關書籍。

間的維度(dimension)。以 $\mathbb{R}$ 上的向量空間 $\mathbb{R}^2$ 為例，前面說過 W_1 和 W_3 都是這個向量空間的基底，而這兩個基底都包含兩個基底向量，因此我們說 $\mathbb{R}^2$ 的維度是 2，也可說 $\mathbb{R}^2$ 是 $\mathbb{R}$ 上的二維向量空間。另外又如 $\mathbb{Q}$ 上的向量空間 $\mathbb{Q}[x]$，前面說過 W_2 和 W_4 都是這個向量空間的基底，而這兩個基底都包含無限多個基底向量，因此我們說 $\mathbb{Q}[x]$ 的維度是 ∞，也可說 $\mathbb{Q}[x]$ 是 $\mathbb{Q}$ 上的無限維向量空間。

與向量空間有關的理論在線性代數和抽象代數學上有廣闊的應用，其中一項應用是描述子域(subfield) 的結構。子域的定義跟子環非常相似，給定一個域 $(E, +, \times)$，其子域就是代數結構 $(F, +, \times)$，其中 $F \subseteq E$，$+$ 和 $\times$ 則是繼承自 $(E, +, \times)$ 中的同類運算,而 $(F, +, \times)$ 本身必須滿足域的定義。

舉例說，$\mathbb{R}$ 是域 $\mathbb{C}$ 的子域，因為 $\mathbb{R} \subseteq \mathbb{C}$，而 $\mathbb{R}$ 本身是域。特別地，$\mathbb{R}$ 中元素在加法和乘法下滿足封閉性，即任何兩個實數相加或相乘，所得結果都是實數；$\mathbb{R}$ 的加法單位元 0 和乘法單位元 1 都是實數；每個實數 a 的加法逆元 $-a$ 都是實數，而每個非零實數 a 的乘法逆元 $\frac{1}{a}$ 也是實數。

有趣的是，若域 $(E, +, \times)$ 有子域 $(F, +, \times)$，則 E 可被看成 F 上的向量空間，這個向量空間上的「向量」是 E 的元素，「純量」則是 F 的元素，現在讓我們驗證 E 和 F 的確滿足前面有關向量空間的定義。首先，$(E, +)$ 和 $(F, +, \times)$ 當然分別是交換群和域。其次，對任何 $v \in E$ 和 $a \in F$，當然可以進行純量乘法 (也就是域 E 中的乘法)，其結果 $av \in E$，而且上述純量乘法運算滿足上述四條公理，因為公理 (i)、(iii) 和 (iv) 分別相當於域中乘法對加法的分配性、乘法的結合性和乘法單位元的性質，而公理 (ii) 可由域中乘法對加法的分配性以及乘法的交換性推導而來。把域及其子域看成向量空間的優點是可以把向量空間的某些概念應用於域中，例如可以討論域相對於某子域的基底和維度。

如前所述，$\mathbb{R}$ 是 $\mathbb{C}$ 的子域，因此 $\mathbb{C}$ 可被看成 $\mathbb{R}$ 上的向量空間，其中的「向量」是複數，「純量」則是實數。這個向量空間的一個基底是 $\{1, i\}$，以下證明這個集合滿足前面有關基底的兩個條件。首先，我們有

$$\begin{aligned} \langle 1, i \rangle &= \{a(1) + b(i) : a, b \in \mathbb{R}\} \\ &= \{a + bi : a, b \in \mathbb{R}\} \\ &= \mathbb{C} \end{aligned}$$

因此 $\{1, i\}$ 滿足上述條件 (i)。其次，假設 $a(1) + b(i) = 0$，即 $a + bi = 0$，那麼根據複數的定義，必然有 $a = b = 0$，因此 $\{1, i\}$ 是線性獨立的，即滿足條件 (ii)。總上所述，$\{1, i\}$ 是 $\mathbb{C}$ 的一個基底。

跟其他向量空間一樣，$\mathbb{C}$ 還可以有其他基底。我們在《感受伽羅瓦：環

的同態與同構》中曾指出，複數除了可以表示成 $a+bi\,(a,b\in\mathbb{R})$ 的形式外，也可表示成 $a+b\iota\,(a,b\in\mathbb{R})$ 的形式 (以及其他無限種不同形式)，其中 ι 相等於一般複數表示形式下的 $\sqrt{5}i$，以下讓我們證明 $\{1,\iota\}$ 也滿足前面有關基底的兩個條件。首先，我們有

$$\begin{aligned}\langle 1,\iota\rangle &= \{a(1)+b(\iota):a,b\in\mathbb{R}\}\\ &= \{a+b\iota:a,b\in\mathbb{R}\}\\ &= \{a+b(\sqrt{5}i):a,b\in\mathbb{R}\}\\ &= \{a+\sqrt{5}b(i):a,b\in\mathbb{R}\}\\ &= \mathbb{C}\end{aligned}$$

請注意若 b 是實數，則 $\sqrt{5}b$ 也是實數；反過來，任何實數 c 都可以表達成 $\sqrt{5}b$ 的形式 (取 $b=\frac{c}{\sqrt{5}}$ 即可)，因此上面最後一行是合理的，由此證得 $\{1,\iota\}$ 滿足上述條件 (i)。其次，假設 $a(1)+b(\iota)=0$，即 $a+\sqrt{5}bi=0$，那麼根據複數的定義，必然有 $a=\sqrt{5}b=0$，即 $a=b=0$，因此 $\{1,\iota\}$ 是線性獨立的，即滿足條件 (ii)。總上所述，$\{1,\iota\}$ 是 $\mathbb{C}$ 的另一個基底。

由此可見，$\mathbb{C}$ 的基底 $\{1,i\}$ 和 $\{1,\iota\}$(以及其他無限多個基底) 都含有兩個元素，因此 $\mathbb{C}$ 是 $\mathbb{R}$ 上的二維向量空間，這就是我們在前面各章中曾多次指出複數是二維實數的理據。

連結至數學專題
連結至周家發網頁