第三章 向量空间

总是从最简单的例子开始.

——David Hilbert

第一节 $\mathbf{R}^n$ 的子空间

向量空间的基本模型——这章的主题——是 n 维实向量空间 $\mathbf{R}^n$ 的子空间．我们在本节里讨论它们．向量空间的定义将在第三节给出．

尽管行向量写起来占的空间少，但矩阵乘法定义使列向量用起来更方便，所以，我们通常情况下使用列向量．为节省空间，我们有时用矩阵的转置形式$(a_1, \cdots, a_n)^t$ 写列向量．如同第一章提到的，我们不区分列向量和 $\mathbf{R}^n$ 中有相同坐标的点．列向量常记为小写字母 v 或 w，并且如果 v 等于$(a_1, \cdots, a_n)^t$，则称$(a_1, \cdots, a_n)^t$ 为 v 的坐标向量．

考虑向量的两个运算：

【3.1.1】

$$\text{向量加法：}\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}+\begin{bmatrix}b_1\\ \vdots\\ b_n\end{bmatrix}=\begin{bmatrix}a_1+b_1\\ \vdots\\ a_n+b_n\end{bmatrix}$$

$$\text{标量乘法：}c\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}=\begin{bmatrix}ca_1\\ \vdots\\ ca_n\end{bmatrix}$$

这些运算使 $\mathbf{R}^n$ 成为一个向量空间.

(3.1.1)的 $\mathbf{R}^n$ 的一个子集 W 是子空间，如果它有下述性质：

【3.1.2】

78 (a) 如果 w 与 w' 是 W 里的向量，则 $w+w'$ 也是 W 里的向量.

(b) 如果 w 是 W 里的向量，c 是 $\mathbf{R}$ 的数，则 cw 也是 W 里的向量.

(c) 零向量在 W 里.

有另一种方式叙述子空间的条件：

【3.1.3】 W 是非空的，并且如果 $w_1, w_2, \cdots, w_n$ 是 W 里的元素，而 $c_1, c_2, \cdots, c_n$ 是标量，则线性组合 $c_1w_1+c_2w_2+\cdots+c_nw_n$ 也是 W 里的向量.

齐次线性方程组给出的例子：已知一个系数在 $\mathbf{R}$ 里的 $m\times n$ 矩阵 A，$\mathbf{R}^n$ 中所有坐标向量为齐次方程 $AX=0$ 的解的集合是一个子空间，称为 A 的迷向子空间．虽然这是很简单的，但我们将检验子空间的条件.

- $AX=0$ 与 $AY=0$ 蕴含着 $A(X+Y)=0$：如果 X 与 Y 都是解，则 $X+Y$ 也是解.

- $AX=0$ 蕴含着 $AcX=0$：如果 X 是一个解，则 cX 也是解.
- $A0=0$：零向量是解.

零空间 $W=\{0\}$ 与整个空间 $W=\mathbf{R}^n$ 是子空间. 一个子空间是真子空间，如果它不是二者之一. 下一个命题描述了 $\mathbf{R}^2$ 的真子空间.

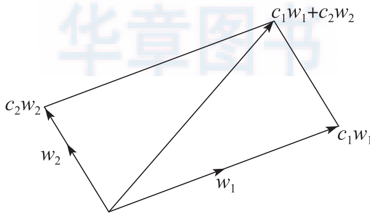
【3.1.4】命题 令 W 是 $\mathbf{R}^2$ 的真子空间，且 w 是 W 的一个非零向量. 则 W 由 w 的标量倍数 cw 组成. 不同的真子空间有唯一的公共零向量.

由已知非零向量 w 的标量倍数 cw 组成的子空间称为由 w 张成的子空间. 几何上，它是 $\mathbf{R}^2$ 中通过原点的直线.

命题的证明 首先注意由非零向量 w 张成的子空间 W 也是由 W 所包含的任意其他非零向量 w' 所张成的. 这是因为如果 $w'=cw$ 且 $c\neq 0$，则任一倍数 aw 也可写成 $ac^{-1}w'$ 的形式. 因此，分别由向量 w_1 和 w_2 张成的子空间 W_1 和 W_2 如果有非零的公共向量 v，则这两个子空间相等.

其次，$\mathbf{R}^2$ 的非零子空间 W 含非零元素 w_1. 因为 W 是子空间，所以它包含由 w_1 张成的子空间 W_1，并且如果 $W_1=W$，那么 W 由一个非零向量的标量倍数组成. 我们证明如果 W 不等于 W_1，那么它是整个空间 $\mathbf{R}^2$. 令 w_2 是在 W 里而不在 W_1 里的元素，并且令 W_2 是由 w_2 张成的子空间. 由于 $W_1\neq W_2$，这两个子空间的交仅含有 0 向量. 所以，向量 w_1 和 w_2 的任一个都不是另一个的倍数. 因此，w_i 的坐标向量(称为 A_i)是不成比例的，从而以这些向量作为列的 2×2 分块矩阵 $A=[A_1\,|\,A_2]$的行列式非零. 在此情形下，对任意向量 v 的坐标向量 B 解方程 $AX=B$，得线性组合 $v=w_1x_1+w_2x_2$. 这表明 W 是整个空间 $\mathbf{R}^2$. ■

几何上从向量加法的平行四边形法则也可看出每个向量是线性组合 $c_1w_1+c_2w_2$. 79



我们给出的 $\mathbf{R}^2$ 的子空间的描述在第四节通过维数概念进行阐明.

第二节 域

如同在第一章开始所提到的，本质上，关于矩阵运算的所有结论对于复数矩阵如同实数矩阵一样都是成立的，对于其他数系也是都成立的. 为描述这些数系，我们列出“标量”所需要的性质，这样就产生了域的概念. 在转到本章主要话题——向量空间——之前我们在此介绍域.

复数域 $\mathbf{C}$ 的子域是要描述的最简单的域. $\mathbf{C}$ 的子域是在四则运算加、减、乘、除下封闭且包含 1 的任意子集. 换言之，F 是 $\mathbf{C}$ 的一个子域，如果它具有下列性质：

【3.2.1】 $(+, -, \times, \div, 1)$

- 若 a，$b\in F$，则 $a+b\in F$.
- 若 $a\in F$，则 $-a\in F$.
- 若 a，$b\in F$，则 $ab\in F$.
- 若 $a\in F$ 且 $a\neq 0$，则 $a^{-1}\in F$.
- $1\in F$.

这些蕴含着 $1-1=0$ 是 F 的一个元．另一种叙述方式是说 F 是加群 $\mathbf{C}^{+}$ 的子群，而且 F 的非零元构成乘法群 $\mathbf{C}^{\times}$ 的子群.

一些 $\mathbf{C}$ 的子域的例子如下：

(a) 实数域 $\mathbf{R}$.

(b) 有理数(即整数的分数)域 $\mathbf{Q}$.

(c) 形如 $a+b\sqrt{2}$的所有复数的域 $\mathbf{Q}[\sqrt{2}]$，其中 a，$b\in\mathbf{Q}$.

抽象域的概念比起 $\mathbf{C}$ 的子域更难于掌握，但它包含了重要的新的域类，其中包括有限域.

【3.2.2】定义 域 F 是具有称为加法和乘法的两个合成法则

$$\begin{array}{ccccccc} F\times F & \xrightarrow{+} & F & \quad 和 \quad & F\times F & \xrightarrow{\times} & F \\ a,b & \rightsquigarrow & a+b & & a,b & \rightsquigarrow & ab \end{array}$$

80 并且满足下列公理的集合：

(i) 加法使 F 成为阿贝尔群 F^{+}，其单位元记为 0.

(ii) 乘法是交换的，并且使 F 的非零元集成为一个阿贝尔群 $F^{\times}$，其单位元记为 1.

(iii) 分配律：对所有 a，b，$c\in F$，$a(b+c)=ab+ac$.

前面两个公理分别描述加法和乘法的合成法则．第三个公理(也就是分配律)是联系加法和乘法的.

实数满足这些公理，但它们就是通常代数运算所需要的全部公理，这一事实只有在使用它们后才能理解.

下一引理解释零元在乘法运算上的作用.

【3.2.3】引理 令 F 是域.

(a) F 的元素 0 与 1 是不同的.

(b) 对 F 里的所有元素 a，有 $a0=0$ 与 $0a=0$.

(c) F 里的乘法满足结合律，并且 1 是恒等元.

证明

(a) 公理(ii)蕴含着 1 不等于 0.

(b) 因 0 是加法恒等元，故 $0+0=0$．于是 $a0+a0=a(0+0)=a0$．由于 F^{+} 是群，因此可消去 $a0$ 得 $a0=0$，从而得 $0a=0$.

(c) 因 $F-\{0\}$是阿贝尔群，故乘法运算限制到这个子集时是结合的．我们需要证明当这

些元素至少有一个是 0 时，$a(bc)=(ab)c$. 在这种情形下，(b)表明所讨论的乘积为零. 最后，元素 1 是 $F-\{0\}$上的恒等元. (b)中置 $a=1$ 就证明了 1 在 F 的所有元素上是恒等的. ■

除复数的子域之外，最简单的域是称为素域的一些有限域，下面就来描述它们. 在第二章第九节中，我们看到，模 n 同余类的集合 $\mathbf{Z}/n\mathbf{Z}$ 具有由整数的加法和乘法导出的加法和乘法法则. 对于整数，除了公理(ii)中乘法逆的存在性以外，域的所有公理都成立. 整数对除法不封闭. 正如我们面前所指出的，这些公理也延续到了同余类的加法和乘法. 但没有理由假定同余类存在乘法逆，事实上，逆也不一定存在. 例如，类 2 模 6 没有乘法逆. 因而，下面的事实是令人惊奇的：若 p 是素数，则所有模 p 非零的同余类皆有逆，这样集合 $\mathbf{Z}/p\mathbf{Z}$ 是域. 这个域称为素域，通常记作 $\mathbf{F}_p$.

用横杠记号并且选取模 p 同余类的通常代表元，

【3.2.4】 $$\mathbf{F}_p=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}=\mathbf{Z}/p\mathbf{Z}$$

【3.2.5】定理 令 p 是一个素整数. 每一个非零同余类$\overline{a}(\bmod p)$有乘法逆，因而 $\mathbf{F}_p$ 是阶为 p 的域.

在给出此定理证明之前先讨论下面定理. 81

如果 a 和 b 是整数，则$\overline{a}\neq 0$ 意思是 p 不能整除 a，而$\overline{ab}=\overline{1}$意思是 $ab\equiv 1(\bmod p)$. 这个定理用同余的术语可以叙述如下：

【3.2.6】 设 p 是素数，并设 a 是不能被 p 整除的任意整数. 则有整数 b 使得 $ab\equiv 1(\bmod p)$.

一般来说，求同余类$\overline{a}(\bmod p)$的逆并不容易，但当 p 不大时，可以通过反复试验找到. 一个系统的方法是计算$\overline{a}$的幂. 例如，设 $p=13$ 而$\overline{a}=\overline{3}$，则$\overline{a}^2=\overline{9}$而$\overline{a}^3=\overline{27}=\overline{1}$. 我们幸运地得到：$\overline{a}$的阶为 3 且$\overline{3}^{-1}=\overline{3}^2=\overline{9}$. 另一方面，$\overline{6}$的幂遍历模 13 的每一个非零同余类. 计算幂也许不是求得$\overline{6}$的逆的最快的方法，但定理告诉我们非零同余类集 $\mathbf{F}_p^{\times}$ 构成群. 所以，$\mathbf{F}_p^{\times}$ 的每一元素$\overline{a}$是有限阶的，并且如果$\overline{a}$有阶 r，它的逆将是$\overline{a}^{(r-1)}$.

为了利用这种推理证明定理，我们需要消去律.

【3.2.7】命题(消去律) 令 p 是一个素整数，并且令$\overline{a}$，$\overline{b}$与$\overline{c}$是 $\mathbf{F}_p$ 的元素.

(a) 如果$\overline{a}\,\overline{b}=\overline{0}$，那么$\overline{a}=\overline{0}$或$\overline{b}=\overline{0}$.

(b) 如果$\overline{a}\neq\overline{0}$并且如果$\overline{a}\,\overline{b}=\overline{a}\,\overline{c}$，那么$\overline{b}=\overline{c}$.

证明

(a) 我们用整数 a 与 b 表示同余类$\overline{a}$与$\overline{b}$. 这时引理的断言变成：如果 p 整除 ab，那么 p 整除 a 或 p 整除 b. 这是推论 2.3.7.

(b) 如果$\overline{a}\neq\overline{0}$并且$\overline{a}(\overline{b}-\overline{c})=\overline{0}$，那么由(a)知$\overline{b}-\overline{c}=\overline{0}$. ■

定理 3.2.5 的证明 设$\overline{a}\in F_p$ 是任意非零元. 考虑幂 1，$\overline{a}$，$\overline{a}^2$，$\overline{a}^3$，…因为有无限多个幂而 $\mathbf{F}_p$ 中仅有有限多个元素，所以必有两个幂是相等的，比如说$\overline{a}^m=\overline{a}^n$，其中 $m<n$. 在等式两边消去$\overline{a}^m$ 得：$\overline{1}=\overline{a}^{(n-m)}$. 因此，$\overline{a}^{(n-m-1)}$是$\overline{a}$的逆. ■

为方便下面讨论，我们去掉字母上面的横杠，相信我们记得住何时用整数何时用同余类以及规则(2.9.8)：

如果 a 和 b 是整数，那么 $\mathbf{F}_p$ 中 $a=b$ 意味着 $a\equiv b(\bmod\ p)$.

一般来说，与同余一样，域 $\mathbf{F}_p$ 中的计算也可以通过整数来进行，除了除法以外．可以用 $\mathbf{F}_p$ 中的元素构成的矩阵 A 进行运算，不加变化地重复第一章的讨论.

假如要在素域 $\mathbf{F}_p$ 中求解 n 个具有 n 个未知量的线性方程的方程组．以合适的方式选择同余类的代表，将方程组用一个整数方程组表示，比如说，$AX=B$，其中 A 是一个 $n\times n$ 整数矩阵，而 B 是一个整数列向量．要在 $\mathbf{F}_p$ 中解方程组，我们模 p 求矩阵 A 的逆．公式
82 $\operatorname{cof}(A)A=\delta I$ 对整数矩阵成立，其中 $\delta=\det A$(定理 1.6.9)，因而当矩阵元素由其同余类代替时，其在 $\mathbf{F}_p$ 中也成立．若 δ 的同余类非零，则可以通过计算 $\delta^{-1}\operatorname{cof}(A)$在 $\mathbf{F}_p$ 中求 A 的逆.

【3.2.8】推论 令 $AX=B$ 是 n 个具有 n 个未知量的线性方程组，其中 A，B 的元素属于 $\mathbf{F}_p$．设 $\delta=\det A$．如果 δ 不为零，则方程组在 $\mathbf{F}_p$ 中有唯一解.

例如，考虑线性方程组 $AX=B$，其中

$$A=\begin{bmatrix}8 & 3\\ 2 & 6\end{bmatrix},\quad B=\begin{bmatrix}3\\ -1\end{bmatrix}$$

因为系数是整数，所以对任意素数 p，$AX=B$ 定义 $\mathbf{F}_p$ 上的一个方程组．A 的行列式是 42，故对所有不能整除 42 的 p，亦即对所有不同于 2，3 和 7 的 p，方程组在 $\mathbf{F}_p$ 中有唯一解．例如，若 $p=13$ 当(mod 13)取值时，得到 $\det A=3$．因为在 $\mathbf{F}_{13}$ 中 $3^{-1}=9$，故在 $\mathbf{F}_{13}$ 中模 13 有

$$A^{-1}=\begin{bmatrix}6 & -3\\ -2 & 8\end{bmatrix}=\begin{bmatrix}2 & -1\\ 8 & 7\end{bmatrix},\quad X=A^{-1}B=\begin{bmatrix}7\\ 4\end{bmatrix}$$

方程组在 $\mathbf{F}_2$ 或 $\mathbf{F}_3$ 中无解，但在 $\mathbf{F}_7$ 中碰巧有解，虽然在这个域中 $\det A\equiv 0$(模 7).

元素属于素域 $\mathbf{F}_p$ 的可逆矩阵为我们提供了有限群的新例子——有限域上的一般线性群：

$$GL_n(\mathbf{F}_p)=\{\text{元素属于 }\mathbf{F}_p\text{ 的 }n\times n\text{ 可逆矩阵}\}.$$
$$SL_n(\mathbf{F}_p)=\{\text{元素属于 }\mathbf{F}_p\text{ 的 }n\times n\text{ 可逆矩阵且行列式为 }1\}$$

例如，元素在 $\mathbf{F}_2$ 里的 2×2 可逆矩阵的群含有 6 个元素：

【3.2.9】 $$GL_2(\mathbf{F}_2)=\left\{\begin{bmatrix}1 & \\ & 1\end{bmatrix},\begin{bmatrix}1 & 1\\ 1 & \end{bmatrix},\begin{bmatrix} & 1\\ 1 & 1\end{bmatrix},\begin{bmatrix} & 1\\ 1 & \end{bmatrix},\begin{bmatrix}1 & 1\\ & 1\end{bmatrix},\begin{bmatrix}1 & \\ 1 & 1\end{bmatrix}\right\}$$

这个群同构于对称群 S_3．按上面顺序所列的矩阵与对称群 S_3 的元素的通常列表$\{1, x, x^2, y, xy, x^2y\}$对应一致.

素域 $\mathbf{F}_p$ 有一个性质，即它使素域与 $\mathbf{C}$ 的子域区别开来，这个性质就是 1 自己相加若干次后得到 0，事实上是 p 的倍数．域 F 的特征 p 是作为加群 F^+ 的一个元素 1 的阶，倘若阶是有限的．它是使得 m 个 1 的和 $1+\cdots+1$ 为零的最小正整数 m．如果 1 的阶是无限的，即在 F 中 $1+\cdots+1$ 从不为 0，则我们说域 F 有特征零，这似乎有点违背常规．因此，$\mathbf{C}$ 的

子域有特征零，而素域 $\mathbf{F}_p$ 有特征 p.

【3.2.10】**引理** 任何域 F 的特征或者为零，或者为一个素数. 83

证明 为避免混淆，令$\bar{0}$和$\bar{1}$分别表示域 F 中的加法恒等元和乘法恒等元. 如果 k 是正整数，则用$\bar{k}$表示 k 个$\bar{1}$的和. 假设特征 m 不是零，那么 1 生成加群 F^+ 的阶为 m 的循环子群 H，且$\overline{m}=\bar{0}$. 由$\bar{1}$生成的循环子群 H 的不同元素是$\bar{k}$，这里 $k=0$，1，…，$m-1$（命题 2.4.2）. 假设 m 不是素的，比如说 $m=rs$，并且 $1<r$，$s<m$，那么，$\bar{r}$和$\bar{s}$属于乘法群$F^\times=F-\{0\}$，但积 $\bar{r}\,\bar{s}$（其值为$\bar{0}$）却不在 $F^\times$ 里. 这与 $F^\times$ 是群矛盾. 所以，m 是素的. ■

素域 $\mathbf{F}_p$ 有一个著名的性质.

【3.2.11】**定理**（乘法群的结构） 令 p 是素数，素域的乘法群 $\mathbf{F}_p^\times$ 是阶为 $p-1$ 的循环群.

我们把这个定理的证明推迟到第十五章给出，在那里将证明每个有限域的乘法群都是循环群（定理 15.7.3）.

注 循环群 $\mathbf{F}_p^\times$ 的生成元称为模 p 本原根.

有两个模 7 本原根，亦即 3 和 5，有四个模 11 本原根. 去掉数字上面的横杠，模 7 本原根 3 的幂 3^0，3^1，3^2，…以下面的顺序列出了 $\mathbf{F}_7$ 的非零元素：

【3.2.12】
$$\mathbf{F}_7^\times=\{1,3,2,6,4,5\}=\{1,3,2,-1,-3,-2\}$$

因此，有两种方式——加法的和乘法的——列出 $\mathbf{F}_p$ 的非零元素. 如果 α 是模 p 本原根，则

【3.2.13】
$$\mathbf{F}_p^\times=\{1,2,3,\cdots,p-1\}=\{1,\alpha,\alpha^2,\cdots,\alpha^{p-2}\}$$

第三节 向 量 空 间

有了一些例子和域的概念后，我们给出向量空间的定义.

【3.3.1】**定义** 域 F 上的**向量空间** V 是满足下面合成法则的集合：

(a) 加法：$V\times V\to V$，记为 v，$w \rightsquigarrow v+w$，其中 v，$w\in V$，

(b) 标量乘法：$F\times V\to V$，记为 c，$v\rightsquigarrow cv$，其中 $c\in F$，$v\in V$.

这两个合成法则满足下列公理：

- 加法使 V 成为交换群 V^+，并带有恒等元，记为 0.
- $1v=v$，对所有 $v\in V$ 成立.
- 结合律：$(ab)v=a(bv)$，对所有 a，$b\in F$ 和 $v\in V$ 成立.
- 分配律：$(a+b)v=av+bv$ 和 $a(v+w)=av+aw$，对所有 a，$b\in F$ 和 v，$w\in V$ 成立. 84

元素在域 F 中的列向量的加法和标量乘法如(3.1.1)所定义，这样的列向量空间 F^n 构成域 F 上的向量空间.

一些实向量空间例子（$\mathbf{R}$ 上向量空间）如下：

【3.3.2】**例**

(a) 令 $V=\mathbf{C}$ 是复数集，忘掉两个复数的乘法，仅记住加法 $\alpha+\beta$ 和实数 r 与复数 α 的乘法 $r\alpha$. 这些运算使 V 成为一个实向量空间.

(b) 实多项式 $P(x)=a_nx^n+\cdots+a_0$ 的集合是一个实向量空间，多项式的加法和实数与多项式的乘法按合成法则进行.

(c) 实直线上的连续实值函数的集合是一个实向量空间，函数的加法 $f+g$ 和实数与函数的乘法按合成法则进行.

(d) 微分方程$\frac{d^2y}{dt^2}=-y$ 的解集合是一个实向量空间. ■

当我们视其为向量空间时，每个例子都有比看上去更复杂的结构. 这是很典型的. 任一个特例肯定有区别于其他例子的额外特征，但这不是缺点. 相反地，抽象方法的好处在于公理的结果能够应用到许多不同的情形.

与群的子群和同构类似的两个重要概念是子空间和同构. 与 $\mathbf{R}^n$ 的子空间一样，域 F 上向量空间 V 的子空间 W 是在加法和标量乘法运算下封闭的非空子集. 子空间 W 称为 V 的一个真子空间，如果它既不是整个空间 V，也不是零空间$\{0\}$. 例如，微分方程(3.3.2)(d)的解空间是实直线上所有连续函数空间的真子空间.

【3.3.3】命题 令 $V=F^2$ 是元素在域 F 中的列向量组成的向量空间. V 的每个真子空间 W 是由单个非零向量 w 的标量倍数$\{cw\}$组成的. 不同的真子空间仅有零向量作为公共向量.

命题 3.1.4 的证明搬过来即可.

【3.3.4】例 令 F 是素域 $\mathbf{F}_p$. 空间 F^2 含有 p^2 个向量，其中有 p^2-1 个非零向量. 因为有 $p-1$ 个非零标量，由非零向量 w 张成的子空间 $W=\{cw\}$将含有 $p-1$ 个非零向量. 所以，F^2 含有$(p^2-1)/(p-1)=p+1$ 个真子空间. ■

在同一个域 F 上，一个向量空间 V 到另一个向量空间 V'的同构 φ 是一个与合成法则相容的一一映射 $\varphi:V\to V'$，即对所有 v，$w\in V$ 及所有 $c\in F$ 满足条件

【3.3.5】 $$\varphi(v+w)=\varphi(v)+\varphi(w) \quad 和 \quad \varphi(cv)=c\varphi(v)$$

85 的一一映射.

【3.3.6】例

(a) 令 $F^{n\times n}$表示域 F 上的 $n\times n$ 矩阵的集合，该集合是域 F 上的向量空间，它同构于长度为 n^2 的列向量的空间.

(b) 如果同(3.3.2)(a)一样，把复数集看作实向量空间，使得$(a, b)^t \rightsquigarrow a+bi$ 的映射 $\varphi:\mathbf{R}^2\to\mathbf{C}$ 是一个同构. ■

第四节 基和维数

本节讨论在向量空间中使用加法和标量乘法时所用的术语. 新的概念有张成、线性无关和基.

这里使用向量的有序集会很方便. 我们已将无序集用花括号括起来表示，为了区别有序集和无序集，将有序集用圆括号括起来表示. 这样有序集(v, w)和(w, v)是不同的，而无序集$\{v, w\}$和$\{w, v\}$是相同的. 有序集允许重复. 这样(v, v, w)是一个有序集，且

它与(v, w)不同，这与无序集的习惯不同，无序集$\{v, v, w\}$和$\{v, w\}$表示同一个集合.

注 令V是域F上的向量空间，并设$S=\{v_1, v_2, \cdots, v_n\}$是$V$中元素的一个有序集，$S$的一个线性组合是形如

【3.4.1】 $$w = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n, \quad c_i \in F$$

的向量.

为方便起见，允许标量出现在向量的任一边．我们简单地约定：如果v是一个向量，c是一个标量，则记号vc和cv代表由标量乘法得到的同一向量．所以，

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = v_1 c_1 + v_2 c_2 + \cdots + v_n c_n$$

矩阵记号提供书写线性组合的紧凑方式，并且也是我们书写向量有序集的方式．由于里面的元素是向量，所以称$S=(v_1, v_2, \cdots, v_n)$是超向量．向量空间里两个元素的乘法没有定义，但有标量乘法．这允许我们把超向量S和F^n里的列向量X的乘积理解为

【3.4.2】 $$SX = (v_1, \cdots, v_n)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1 x_1 + \cdots + v_n x_n$$

由标量乘法和向量加法计算右边，我们得到另一个向量，即一个标量系数x_i写在了右边的线性组合.

我们拿线性方程

【3.4.3】 $$2x_1 - x_2 - 2x_3 = 0 \quad 或\ AX = 0, \quad 其中\ A = (2, -1, -2)$$

在$\mathbf{R}^3$的解子空间W作为例子．两个特解w_1和w_2以及它们的线性组合$w_1 y_1 + w_2 y_2$如下所示.

【3.4.4】 $$w_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \quad w_1 y_1 + w_2 y_2 = \begin{bmatrix} y_1 + y_2 \\ 2y_2 \\ y_1 \end{bmatrix}$$

如果我们写$S=(w_1, w_2)$，而w_i如(3.4.4)里所示，且$Y=(y_1, y_2)^t$，那么，组合$w_1 y_1 + w_2 y_2$可写成矩阵形式SY. 86

注 写成$S=(v_1, v_2, \cdots, v_n)$的线性组合的所有向量的集合构成$V$的子空间，称为由集合$S$张成的子空间.

同本章第一节中一样，这个张成(子空间)是V的包含S的最小子空间，常常记为Span$S$．单个向量(v_1)的张成是v_1的标量倍数cv_1的子空间.

可以定义无限多个向量集合的张成．我们将在本章第七节讨论这样的张成．现在假设集合都是有限的.

【3.4.5】**引理** 令S是V中向量的一个有序集，设W是V的子空间．如果$S \subset W$，则Span$S \subset W$.

元素在F中的$m \times n$矩阵的列空间是由该矩阵的列张成的F^m的子空间．它有如下重

要解释：

【3.4.6】命题 令 A 是一个 $m\times n$ 矩阵，B 是一个列向量，A 与 B 的元素都在域 F 里．方程组 $AX=B$ 在 F^n 里有解 X 当且仅当 B 在 A 的列空间里．

证明 令 A_1，A_2，…，A_n 表示 A 的列向量．对任一个列向量 $X=(x_1, x_2, \cdots, x_n)^t$，矩阵之积 AX 是列向量 $A_1x_1+\cdots+A_nx_n$．这是矩阵列向量的线性组合，是列空间的一个元素，并且，若 $AX=B$，那么 B 是这个线性组合． ■

向量 v_1，…，v_n 间的线性关系是等于零的任一线性组合——在 V 中成立的形如

【3.4.7】
$$v_1x_1+v_2x_2+\cdots+v_nx_n=0$$
的任一个方程，其中系数 $x_i\in F$．线性关系是有用的，因为如果 x_n 不是零，则由方程(3.4.7)可解出 v_n．

【3.4.8】定义 向量的一个有序集 $S=(v_1, \cdots, v_n)$称为无关的，或线性无关的，如果除了系数 x_i 皆为零的平凡关系(即 $X=0$)外，这个集合的向量间没有线性关系 $SX=0$．不是无关的集合是相关的．

无关集合 S 里不能有相同的向量．若 S 里的两个向量 v_i 和 v_j 是相等的，则 $v_i-v_j=0$ 是其他系数都为零的形如(3.4.7)的一个线性关系．还有，无关集合里没有零向量，因为若 v_i 是零，则 $v_i=0$ 就是一个线性关系．

【3.4.9】引理

(a) 一个向量的集合(v_1)是无关的当且仅当 $v_1\neq 0$．

(b) 两个向量的集合(v_1, v_2)是线性无关的当且仅当其中任一向量都不是另一向量的倍数．

87 (c) 线性无关集合在任意重新排序后仍是线性无关集合．

设 V 是空间 F^m，并且已知集合 $S=(v_1, v_2, \cdots, v_n)$里诸向量的坐标向量．那么方程 $SX=0$ 给出了具有 n 个未知量 x_i 的 m 个齐次线性方程的方程组，我们可通过解这个方程组确定无关性．

【3.4.10】例 令 $S=(v_1, v_2, v_3, v_4)$为 $\mathbf{R}^3$ 里一个向量集合，其坐标向量为

【3.4.11】
$$A_1=\begin{bmatrix}1\\0\\1\end{bmatrix},\quad A_2=\begin{bmatrix}1\\2\\0\end{bmatrix},\quad A_3=\begin{bmatrix}2\\1\\2\end{bmatrix},\quad A_4=\begin{bmatrix}1\\1\\3\end{bmatrix}$$

用 A 表示列为这些向量的矩阵：

【3.4.12】
$$A=\begin{bmatrix}1&1&2&1\\0&2&1&1\\1&0&2&3\end{bmatrix}$$

这些向量的一般线性组合具有 $SX=v_1x_1+v_2x_2+v_3x_3+v_4x_4$ 的形式，它的坐标向量是 $AX=A_1x_1+A_2x_2+A_3x_3+A_4x_4$．齐次方程 $AX=0$ 有非平凡解，因为这是一个具有四个未知量的三个齐次方程的方程组．所以，集合 S 是相关的．另一方面，由(3.4.12)的前三

列构成的 3×3 矩阵 A' 的行列式等于 1，于是方程 $A'X=0$ 只有平凡解．所以，(v_1, v_2, v_3)是无关集合． ■

【3.4.13】定义 向量空间 V 的一个基是线性无关且张成 V 的一个向量集合$(v_1, \cdots, v_n)$．

我们常用如 $\boldsymbol{B}$ 的粗体符号表示基．上面定义的集合(v_1, v_2, v_3)是 $\mathbf{R}^3$ 的一个基，因为方程 $A'X=B$ 对所有 B 都有唯一解(见 1.2.21)．在(3.4.4)中定义的集合(w_1, w_2)是方程 $2x_1-x_2-2x_3=0$ 的解空间的一个基，尽管我们还未证明这个结论．

【3.4.14】命题 集合 $\boldsymbol{B}=(v_1, \cdots, v_n)$是基当且仅当每个向量 $w\in V$ 可以以唯一方式写为组合 $w=v_1x_1+v_2x_2+\cdots+v_nx_n=\boldsymbol{B}X$．

证明 无关性的定义可以重新叙述为零向量仅有一个作为线性组合的表达式．如果每个向量可唯一地写成组合，那么 $\boldsymbol{B}$ 是无关的，并且张成 V．所以，它是一个基．反过来，假设 $\boldsymbol{B}$ 是基，那么，V 中每个向量 w 都可写成线性组合．设 w 有两种方式写成线性组合，比如说，$w=\boldsymbol{B}X=\boldsymbol{B}X'$．令 $Y=X-X'$，则 $\boldsymbol{B}Y=0$．这是线性无关向量 $v_1, v_2, \cdots, v_n$ 间的一个线性关系．所以，$X-X'=0$．这两个线性组合是相同的． ■

设 $V=F^n$ 是列向量空间．同以前一样，e_i 表示在第 i 个位置为 1 而其他位置为 0 的列向量(见(1.1.24))．集合 $\boldsymbol{E}=(e_1, e_2, \cdots, e_n)$是 F^n 的一个基，称为标准基．如果 F^n 里的向量 v 的坐标向量是 $V=(x_1, x_2, \cdots, x_n)^t$，则 $v=\boldsymbol{E}X=e_1x_1+e_2x_2+\cdots+e_nx_n$ 是 v 写成标准基的唯一表达式． 88

我们现在讨论把张成、无关性和基三个概念联系起来的主要事实．最重要的结果是定理 3.4.18．

【3.4.15】命题 令 $S=(v_1, v_2, \cdots, v_n)$是向量的一个有序集，设 w 是 V 里的任一向量，并且 $S'=(S, w)$是把 w 添加到 S 里得到的集合．

(a) $\mathrm{Span}S=\mathrm{Span}S'$ 当且仅当 $w\in\mathrm{Span}S$．

(b) 假设 S 是无关的．那么 S' 是无关的当且仅当 $w\notin\mathrm{Span}S$．

证明 这是非常基本的结果，所以，我们略去大部分证明．我们仅证明，如果 S 是无关的，但 S' 不是无关的，则 w 属于 S 的张成．若 S' 是相关的，则有某个线性关系

$$v_1x_1+v_2x_2+\cdots+v_nx_n+wy=0$$

其中系数 $x_1, x_2, \cdots, x_n$ 和 y 不全为零．如果系数 y 为零，则表达式变为 $SX=0$，因为假设 S 是无关的，故也得 $X=0$．于是关系是平凡的，与假设矛盾．所以，$y\neq0$，从而 w 可表示为 $v_1, v_2, \cdots, v_n$ 的线性组合． ■

注 向量空间 V 称为有限维的，如果存在有限集合 S，它张成 V．否则，V 是无限维的．

本节后面余下部分所讨论的向量空间均是有限维的．

【3.4.16】命题 令 V 是有限维向量空间．

(a) 令 S 是张成 V 的有限子集，并设 L 是 V 的无关子集．可通过把 S 的元素添加到 L 的办法得到 V 的一个基．

(b) 令 S 是张成 V 的有限子集，可通过去掉 S 的元素的办法得到 V 的一个基．

证明

(a) 如果 S 包含在 Span$L$ 里，则 L 张成 V，于是，它是一个基(3.4.5). 如果 S 不包含在 Span$L$ 里，则在 S 里选一个元素 v，使其不含在 Span$L$ 里. 由命题 3.4.15，$L'=(L,v)$是无关的. 我们用 L'替换 L. 因为 S 是有限的，故这种过程常常仅有限多步就结束了. 所以，我们最终得到 V 的一个基.

(b) 如果 S 是相关的，则存在线性关系 $v_1c_1+v_2c_2+\cdots+v_nc_n=0$，其中某个系数(比如说 c_n)是非零的. 从这个方程解出 v_n，这表明 v_n 在前 $n-1$ 个向量集合 S_1 的张成里. 命题 3.4.15(a)表明 Span$S$=SpanS_1. 所以，S_1 张成 V. 我们用 S_1 替换 S. 继续这个过程，最后必得到一个无关但仍张成 V 的集合：一个基.

注意 如果 V 是零向量空间$\{0\}$，那么这个证明会出问题. 因为从 V 中的任何向量(它们全部都等于零)集合开始，我们的过程会将它们一次一个地丢掉，直到只剩下一个向量
89 v_1. 因为 $v_1=0$，故集合(v_1)是相关的. 我们如何进行这个过程？零向量空间并不特别有意义，但它会潜伏在某个角落里，等待我们踏进它的陷阱. 我们必须允许在诸如解齐次线性方程组的某些运算过程中出现的向量空间可能是零空间. 为了避免今后需要把这种情形特别提出来，我们采用下面的定义：

【3.4.17】

- 空集是线性无关的.
- 空集的张成是零空间$\{0\}$.

这样，空集是零向量空间的基. 这些定义使我们能够扔掉最后一个向量 v_1，这样证明就不会出问题了. ■

现在我们来介绍关于无关的主要事实.

【3.4.18】定理 令 S 与 L 是向量空间 V 的有限子集. 假设 S 张成 V，并且 L 是无关的. 那么 S 至少含有同 L 一样多的元素：$|S|\geqslant|L|$.

同以前一样，$|S|$表示阶，即集合 S 的元素的个数.

证明 设 $S=(v_1, v_2, \cdots, v_m)$，$L=(w_1, w_2, \cdots, w_n)$，假设$|S|<|L|$，亦即 $m<n$，证明 L 是相关的. 为此，证明存在线性关系 $v_1x_1+v_2x_2+\cdots+v_nx_n=0$，其中系数 x_i 不全为零. 记这个未确定的关系为 $LX=0$.

因为 S 张成 V，故 L 的每个元素 w_j 是 S 的线性组合，比如说，$w_j=v_1a_{1j}+v_2a_{2j}+\cdots+v_ma_{mj}=SA_j$，其中 A_j 是系数列向量. 我们把这些列向量写成 $m\times n$ 矩阵

【3.4.19】
$$A=\begin{bmatrix} | & & | \\ A_1 & \cdots & A_n \\ | & & | \end{bmatrix}$$

于是

【3.4.20】
$$SA=(SA_1,\cdots,SA_n)=(w_1,\cdots,w_n)=L$$

在未定线性组合里用 SA 替换 L：

$$LX = (SA)X$$

标量乘法的结合律蕴含着 $(SA)X=S(AX)$. 对标量矩阵乘法的结合律的证明也是一样的(我们略去证明). 如果 $AX=0$，那么组合 LX 也是零. 现在，由于 A 是 $m\times n$ 矩阵，且 $m<n$，故齐次方程组 $AX=0$ 有非平凡解 X. 因此，$LX=0$ 就是我们要求的线性关系. ■

【3.4.21】**命题** 令 V 是有限维向量空间.

(a) V 的任两个基有相同的阶(元素个数相同).

(b) 令 $\boldsymbol{B}$ 是一个基. 如果有限向量集 S 张成 V，那么 $|S|\geqslant|\boldsymbol{B}|$，并且 $|S|=|\boldsymbol{B}|$ 当且仅当 S 是基. 90

(c) 令 $\boldsymbol{B}$ 是一个基. 如果向量集 L 是无关的，那么 $|L|\leqslant|\boldsymbol{B}|$，并且 $|L|=|\boldsymbol{B}|$ 当且仅当 L 是基.

证明

(a) 这里我们注意到，两个有限基 $\boldsymbol{B}_1$ 与 $\boldsymbol{B}_2$ 有相同阶，我们将在推论 3.7.7 里证明有限维向量空间的每个基都是有限的. 在定理 3.4.18 里取 $S=\boldsymbol{B}_1$ 和 $L=\boldsymbol{B}_2$ 表明 $|\boldsymbol{B}_1|\geqslant|\boldsymbol{B}_2|$，类似地，$|\boldsymbol{B}_2|\geqslant|\boldsymbol{B}_1|$.

(b)和(c)由(a)与命题 3.4.16 可得. ■

【3.4.22】**定义** 有限维向量空间 V 的维数是基中的向量个数. 维数记为 $\dim V$.

列向量空间 F^n 的维数是 n，因为标准基

$$\boldsymbol{E} = (e_1, e_2, \cdots, e_n)$$

含有 n 个元素.

【3.4.23】**命题** 如果 W 是有限维向量空间 V 的子空间，则 W 是有限维的，并且 $\dim W\leqslant\dim V$. 进一步，$\dim W=\dim V$ 当且仅当 $W=V$.

证明 我们从 W 的任意无关向量集 L 开始，该集合可能为空集. 如果 L 不张成 W，则在 W 中选取一向量 w 使之不含于 L 的张成里. 因此，$L'=(L, w)$ 是无关的(3.4.15). 用 L' 替换 L.

显然，如果 L 是 W 的无关子集，那么将其视作 V 的子集时也是无关的. 因而，由定理 3.4.18 知 $|L|\leqslant\dim V$. 所以，添加元素到 L 的过程经过有限多步就能结束，我们就得到 W 的一个基. 因为 L 至多含有 $\dim V$ 个元素，故 $\dim W\leqslant\dim V$. 如果 $|L|=\dim V$，那么命题 3.4.21(c)表明 L 是 V 的一个基，所以，$W=V$. ■

第五节 用基计算

引入基的目的是提供一种计算的方法，本节我们将学习如何使用它. 考虑两个主题：如何用一组基表出一个向量，以及如何将同一个向量空间的两个不同的基联系起来.

设给定向量空间 V 的一个基 $\boldsymbol{B}=(v_1, \cdots, v_n)$. 记住：这意味着每一个向量 $v\in V$ 可以用恰好一种形式表示为线性组合：

【3.5.1】 $$v = v_1x_1 + \cdots v_nx_n, \quad x_i \in F$$

标量 x_i 称为 v 的坐标，而列向量

【3.5.2】
$$X=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$$

称为 v 关于这个基的坐标向量.

例如，$(\cos t,\ \sin t)$是微分方程 $y''=-y$ 的解空间的一个基. 该微分方程的每个解都是这组基的线性组合. 若已知另一解 $f(t)$，则 f 的坐标向量$(x_1,\ x_2)^{t}$ 是使 $f(t)=(\cos t)x_1+$
91 $(\sin t)x_2$ 的一个向量. 显然，为求 X 我们需要知道关于 f 的某些信息. 不需要很多：仅仅确定两个系数即可. f 的大多数性质隐含在解微分方程的事实里.

我们永远能做的是，已知 n 维向量空间的一个基 $\boldsymbol{B}$，从向量空间 F^n 到 V 定义一个向量空间同构(见 3.3.5)：

【3.5.3】
$$\psi:F^n\to V \quad 映 \quad X\rightsquigarrow \boldsymbol{B}X$$

我们常用 $\boldsymbol{B}$ 表示这个同构，因为它映向量 X 到 $\boldsymbol{B}X$.

【3.5.4】命题 令 $S=(v_1,\ v_2,\ \cdots,\ v_n)$是向量空间 V 的子集，设 $\psi:F^n\to V$ 为其定义是 $\psi(X)=SX$的映射. 那么

(a) ψ 是单射当且仅当 S 是无关的.

(b) ψ 是满射当且仅当 S 张成 V.

(c) ψ 是双射当且仅当 S 是 V 的基.

这个命题可由无关、张成和基的定义得到.

已知一组基，V 中向量 v 的坐标向量可由映射 ψ(3.5.3)的逆得到. 除非进一步明确地给出基，否则不会有逆函数的精确公式，但同构的存在本身就很有意义.

【3.5.5】推论 每个 n 维向量空间 V 同构于列向量空间 F^n.

注意，当 $m\neq n$ 时 F^n 与 F^m 不同构，因为 F^n 有具有 n 个元素的基，而基中元素的个数仅依赖于向量空间. 因此，域 F 上的有限维向量空间被完全分类. 列向量空间 F^n 是同构类的代表元.

n 维向量空间同构于列向量空间 F^n 的事实允许我们只要选定一个基，就能把向量空间的任何问题化简为熟悉的列向量的代数. 不幸的是，同一个向量空间 V 有许多组基. 当给出一个自然的基时，将 V 与同构的向量空间 F^n 等同起来是有用的，而当给出的基对问题不太合适时，那就不行了. 这种情形下，我们需要变换坐标，亦即基变换.

例如，齐次线性方程组 $AX=0$ 的解空间几乎没有自然基. 方程 $2x_1-x_2-2x_3=0$ 的解空间 W 的维数是 2，前面我们展示过它的一组基：$\boldsymbol{B}=(w_1,\ w_2)$，其中 $w_1=(1,\ 0,\ 1)^{t}$ 与 $w_2=(1,\ 2,\ 0)^{t}$(见(3.4.4)). 利用这个基，我们得到向量空间的同构 $\boldsymbol{R}^2\to W$，记为 $\boldsymbol{B}$. 由于方程中的未知量标记为 x_i，因此这里需要选取另一符号来表示 $\boldsymbol{R}^2$ 的变量元素. 我们将使用 $Y=(y_1,\ y_2)^{t}$ 表示. 同构 $\boldsymbol{B}$ 映 Y 到(3.4.4)显示的 $\boldsymbol{B}Y=w_1y_1+w_2y_2$ 的坐标向量.

然而，关于两个特解 w_1 与 w_2 没有非常特别之处，其他大部分解对用起来也一样. 解

$w_1'=(0,2,-1)^t$ 与 $w_2'=(1,4,-1)^t$ 为我们提供 W 的另一组基 $\boldsymbol{B}'=(w_1',w_2')$. 任一组基都能唯一表出解. 解可表示为如下任一形式： 92

【3.5.6】
$$\begin{bmatrix} y_1+y_2 \\ 2y_2 \\ y_1 \end{bmatrix} \quad 或 \quad \begin{bmatrix} y_2' \\ 2y_1'+4y_2' \\ -y_1'-y_2' \end{bmatrix}$$

基的变换

假设给定同一个向量空间 V 的两个基，比如 $\boldsymbol{B}=(v_1,\cdots,v_n)$ 和 $\boldsymbol{B}'=(v_1',\cdots,v_n')$. 我们希望做两个计算. 首先问：两个基是如何联系起来的？其次，一个向量 $v\in V$ 关于每一个基都有坐标，但它们却是不同的. 因而我们问：两个坐标向量是如何联系起来的？这些就是称为基变换的计算，在后面几章中它们将是非常重要的. 如果你不谨慎地组织记号，它们会让你头疼.

我们将 $\boldsymbol{B}$ 看作旧基，把 $\boldsymbol{B}'$ 看作新基. 注意新基 $\boldsymbol{B}'$ 中的每个向量是旧基 $\boldsymbol{B}$ 的一个线性组合. 把这个线性组合写为

【3.5.7】
$$v_j' = v_1p_{1j}+v_2p_{2j}+\cdots+v_np_{nj}$$

当用旧基计算时，列向量 $P_j=(p_{1j},p_{2j},\cdots,p_{nj})^t$ 是新基向量 v_j' 的坐标向量. 把这些列向量组成方阵 P，从而得到矩阵方程 $\boldsymbol{B}'=\boldsymbol{B}P$：

【3.5.8】
$$\boldsymbol{B}' = (v_1',\cdots,v_n') = (v_1,\cdots,v_n)\left[\begin{array}{c} \\ P \\ \\ \end{array}\right] = \boldsymbol{B}P$$

P 的第 j 列是新基向量 v_j' 关于旧基的坐标向量. 矩阵 P 称为基变换矩阵.[⊖]

【3.5.9】命题

(a) 令 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 是向量空间 V 的两个基. 基变换矩阵 P 是可逆矩阵，由基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 唯一确定.

(b) 令 $\boldsymbol{B}=(v_1,\cdots,v_n)$ 是向量空间 V 的基. 其他基是形如 $\boldsymbol{B}'=\boldsymbol{B}P$ 的集合，其中 P 是任意可逆 $n\times n$ 矩阵.

证明

(a) 方程 $\boldsymbol{B}'=\boldsymbol{B}P$ 把基向量 v_i' 表示为基 $\boldsymbol{B}$ 的线性组合. 写出的线性组合仅有一种方式(3.4.14)，因此，P 是唯一的. 为证 P 是可逆矩阵，我们互换 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 的作用. 存在矩阵 Q 使得 $\boldsymbol{B}=\boldsymbol{B}'Q$. 因此

$$\boldsymbol{B} = \boldsymbol{B}'Q = \boldsymbol{B}PQ \quad 或 \quad (v_1,\cdots,v_n) = (v_1,\cdots,v_n)\left[\begin{array}{c} \\ PQ \\ \\ \end{array}\right]$$

⊖ 这个基变换矩阵是第 1 版里用过的矩阵的逆矩阵.

这个方程把每个 v_i 表示为$(v_1, \cdots, v_n)$的组合．乘积矩阵 PQ 中的元素是系数．但因 $\boldsymbol{B}$ 是
93 基，故只有一种方式将 v_i 表示为$(v_1, \cdots, v_n)$的组合，也就是 $v_i=v_i$，或用矩阵记号，$\boldsymbol{B}=\boldsymbol{B}I$．所以，$PQ=I$.

(b) 我们必须证明如果 $\boldsymbol{B}$ 是基，并且如果 P 是可逆矩阵，则 $\boldsymbol{B}'=\boldsymbol{B}P$ 也是基．因为 P 是可逆的，故 $\boldsymbol{B}=\boldsymbol{B}'P^{-1}$．这就告诉我们 v_i 在 $\boldsymbol{B}'$的张成里．所以，$\boldsymbol{B}'$张成 V．又由于它与 $\boldsymbol{B}$ 中元素个数相同，故它是基． ■

令 X 和 X'是任一向量 v 关于两个基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$的坐标向量，也就是，$v=\boldsymbol{B}X$，$v=\boldsymbol{B}'X'$．替换 $\boldsymbol{B}=\boldsymbol{B}'P^{-1}$，得矩阵方程

【3.5.10】
$$v=\boldsymbol{B}X=\boldsymbol{B}'P^{-1}X$$

这表明 v 关于新基 $\boldsymbol{B}'$的坐标向量(称为 X')是 $P^{-1}X$．也可以将其写为 $X=PX'$

回顾一下，我们有单个矩阵 P——基变换矩阵，它具有对偶的性质：

【3.5.11】
$$\boldsymbol{B}'=\boldsymbol{B}P \quad 和 \quad PX'=X$$

其中 X，X'表示任意向量 v 关于两个基的坐标向量．每一个性质都刻画了 P．仔细注意两个关系里斜撇符号的位置.

再次回到方程 $2x_1-x_2-2x_3=0$，令 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$是上面(3.5.6)里描述的解空间 W 的基．基变换矩阵解方程

$$\begin{bmatrix} 0 & 1 \\ 2 & 4 \\ -1 & -1 \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}. \text{它是 } P=\begin{bmatrix} -1 & -1 \\ 1 & 2 \end{bmatrix}$$

已知向量 v 关于两个基的坐标向量 Y 与 Y'(在(3.5.6)里出现)由方程

$$PY'=\begin{bmatrix} -1 & -1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} y_1' \\ y_2' \end{bmatrix}=\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}=Y$$

联系.

另一个例子：令 $\boldsymbol{B}$ 是微分方程$\frac{d^2y}{dt^2}=-y$ 的解空间的基$(\cos t, \sin t)$．如果允许复值函数，那么指数函数 $e^{\pm it}=\cos t\pm i\sin t$ 也是解，$\boldsymbol{B}'=(e^{it}, e^{-it})$是解空间的新基．基变换计算是

【3.5.12】
$$(e^{it}, e^{-it})=(\cos t, \sin t)\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

94 基变换矩阵容易确定的一种情形是 V 是列向量空间 F^n，旧基是标准基 $\boldsymbol{E}=(e_1, \cdots, e_n)$，而新基在这里记为 $\boldsymbol{B}=(v_1, \cdots, v_n)$，它是任意的．令 v_i 关于标准基的坐标向量是列向量 B_i．所以，$v_i=\boldsymbol{E}B_i$．把这些列向量组成 $n\times n$ 矩阵，记之为$[\boldsymbol{B}]$：

【3.5.13】
$$[\boldsymbol{B}]=\begin{bmatrix} | & & | \\ B_1 & \cdots & B_n \\ | & & | \end{bmatrix}, \text{则 } (v_1, \cdots, v_n)=(e_1, \cdots, e_n)\begin{bmatrix} | & & | \\ B_1 & \cdots & B_n \\ | & & | \end{bmatrix}$$

即 $\boldsymbol{B}=\boldsymbol{E}[\boldsymbol{B}]$．所以，$[\boldsymbol{B}]$是从标准基 $\boldsymbol{E}$ 到 $\boldsymbol{B}$ 的基变换矩阵.

第六节 直　　和

向量集的无关和张成的概念对于子空间是相似的．如果 W_1，…，W_k 是向量空间 V 的子空间，那么向量 v 的集合可以写为和

【3.6.1】 $$v = w_1 + \cdots + w_k$$

其中 w_i 是 W_i 的向量，所有这样向量 $v\in V$ 的集合称为子空间的和或它们的张成，记为

【3.6.2】 $$W_1 + \cdots, + W_k = \{v \in V \mid v = w_1 + \cdots + w_k, \text{其中 } w_i \in W_i\}$$

子空间的和是含有所有子空间 W_1，…，W_k 的最小子空间，类似于向量集合的张成．

子空间 W_1，…，W_k 称为无关的，如果除了对所有 i 有 $w_i=0$ 的平凡和外，其余的和 $w_1+\cdots+w_k$(其中 $w_i\in W_i$)皆不为零．换言之，空间是无关的，如果

【3.6.3】 $$w_1 + \cdots + w_k = 0(\text{其中 } w_i \in W_i)\text{ 蕴含着对所有 } i \text{ 有 } w_i = 0$$

注意　假设 v_1，…，v_k 是 V 的元素，令 W_i 是向量 v_i 的张成．那么，子空间 W_1，…，W_k 是无关的当且仅当集合$(v_1, \cdots, v_k)$是无关的．如果比较(3.4.8)与(3.6.3)，这是显然的．用子空间叙述更为整洁，因为标量系数不需要放在(3.6.3)里 w_i 的前面．由于每个子空间 W_i 在标量乘法下封闭，因此标量倍数 cw_i 是 W_i 的另一元素．

我们略去下一命题的证明．

【3.6.4】**命题**　令 W_1，…，W_k 是有限维向量空间 V 的子空间，设 $\boldsymbol{B}_i$ 是 W_i 的一个基．

(a) 下列条件是等价的：

- 诸子空间 W_i 是无关的，而且和 $W_1+\cdots+W_k$ 等于 V．
- 把诸基附和在一起所得集合 $\boldsymbol{B}=(\boldsymbol{B}_1, \cdots, \boldsymbol{B}_k)$是 V 的一个基．

(b) $\dim(W_1+\cdots+W_k)\leqslant\dim W_1+\cdots+\dim W_k$，等号成立当前仅当诸子空间无关． 95

(c) 如果对 $I=1, 2, \cdots, k$，W_i' 是 W_i 的子空间，并且 W_1，…，W_k 是无关的，那么 W_1'，…，W_k' 也是无关的．

如果命题 3.6.4(a)的条件得到满足，就说 V 是子空间 W_1，…，W_k 的直和，记为 $V=W_1\oplus\cdots\oplus W_k$：

【3.6.5】 $$V = W_1 \oplus \cdots \oplus W_k,\text{如果 } V = W_1 + \cdots + W_k \text{ 并且 } W_1,\cdots,W_k \text{ 是无关的}$$

如果 V 是直和，则每个向量 $v\in V$ 恰好可以以一种方式写为(3.6.1)的形式．

【3.6.6】**命题**　令 W_1 与 W_2 是有限维向量空间 V 的子空间．

(a) $\dim W_1+\dim W_2=\dim(W_1\cap W_2)+\dim(W_1+W_2)$．

(b) W_1 与 W_2 是无关的当且仅当 $W_1\cap W_2=\{0\}$．

(c) V 是 W_1 与 W_2 的直和当且仅当 $W_1\cap W_2=\{0\}$且 $W_1+W_2=V$．

(d) 如果 $W_1+W_2=V$，则存在 W_2 的子空间 W_2'，满足 $W_1\oplus W_2'=V$．

证明　证明关键部分(a)：选择 $W_1\cap W_2$ 的一个基 $\boldsymbol{U}=(u_1, \cdots, u_k)$，把它扩张为 W_1 的一

个基$(\boldsymbol{U},\boldsymbol{V})=(u_1,\cdots,u_k;v_1,\cdots,v_m)$. 也把$\boldsymbol{U}$扩张为$W_2$的一个基$(\boldsymbol{U},\boldsymbol{W})=(u_1,\cdots,u_k;w_1,\cdots,w_n)$. 于是，$\dim(W_1\cap W_2)=k$，$\dim W_1=k+m$与$\dim W_2=k+n$. 如果证明$k+m+n$个元素的集合$(\boldsymbol{U},\boldsymbol{V},\boldsymbol{W})=(u_1,\cdots,u_k;v_1,\cdots,v_m,w_1,\cdots,w_n)$是$W_1+W_2$的基，命题就成立.

必须证明$(\boldsymbol{U},\boldsymbol{V},\boldsymbol{W})$是无关的，且张成$W_1+W_2$. W_1+W_2的元素v有形式$w'+w''$，其中$w'\in W_1$，$w''\in W_2$. 用W_1的基$(\boldsymbol{U},\boldsymbol{V})$来写$w'$，比如说，$w'=\boldsymbol{U}X+\boldsymbol{V}Y=u_1x_1+\cdots+u_kx_k+v_1y_1+\cdots+v_my_m$. 也把$w''$写成$W_2$的基$(\boldsymbol{U},\boldsymbol{W})$的组合$\boldsymbol{U}X'+\boldsymbol{W}Z$. 因此，$V=w'+w''=\boldsymbol{U}(X+X')+\boldsymbol{V}Y+\boldsymbol{W}Z$.

其次，假设已知元素$(\boldsymbol{U},\boldsymbol{V},\boldsymbol{W})$之间的线性关系$\boldsymbol{U}X+\boldsymbol{V}Y+\boldsymbol{W}Z=0$. 记这个关系为$\boldsymbol{U}X+\boldsymbol{V}Y=-\boldsymbol{W}Z$. 这个方程的左边属于$W_1$，而右边属于$W_2$. 所以，$-\boldsymbol{W}Z$属于$W_1\cap W_2$，从而它是基$\boldsymbol{U}$的线性组合$\boldsymbol{U}X'$. 这就给出方程$\boldsymbol{U}X'+\boldsymbol{W}Z=0$. 由于$(\boldsymbol{U},\boldsymbol{W})$是$W_2$的基，它是无关的，所以，$X'$和$Z$是零. 这样，已知关系简化为$\boldsymbol{U}X+\boldsymbol{V}Y=0$. 但$(\boldsymbol{U},\boldsymbol{V})$也是无关集合. 于是，$X$与$Y$是零. 关系是平凡的. ■

第七节　无限维空间

有的向量空间太大了，无法由任意有限的向量集合张成，这样的向量空间称作是*无限维的*. 我们不常用到它们，但因为它们在分析中很重要，所以本节将对它们稍作讨论.

无限维向量空间最简明的例子是无限实行向量

【3.7.1】
$$(a)=(a_1,a_2,a_3,\cdots)$$

96 的空间$\mathbf{R}^\infty$. 也可以把一个无限维向量看作是一个实数序列$\{a_n\}$.

空间$\mathbf{R}^\infty$有许多重要的子空间，下面是一些例子.

【3.7.2】例

(a) 收敛序列：$C=\{(a)\in\mathbf{R}^\infty \mid 极限\lim\limits_{n\to\infty}a_n 存在\}$.

(b) 绝对收敛级数：$\ell^1=\{(a)\in\mathbf{R}^\infty \mid \sum\limits_1^\infty |a_n|<\infty\}$.

(c) 有限个非零项的序列：

$$Z=\{(a)\in\mathbf{R}^\infty \mid a_n=0 \text{ 对有限多个以外的 } n \text{ 成立}\}$$

所有上面的空间都是无限维的，还可以找出更多的无限维空间. ■

现在设V是向量空间，是否无限维都行. 向量的无限维集合S的张成应该是什么呢？困难在于：不可能为无限多个向量的组合$c_1v_1+c_2v_2+\cdots$指定一个取值. 如果讨论的是实数的向量空间，即$v_i\in\mathbf{R}^n$，假如级数$c_1v_1+c_2v_2+\cdots$收敛，则可以为它指定一个值. 但许多级数不收敛，我们就不知道该指定什么值了. 在代数中，习惯上只谈论有限多个向量的组合. 因此，无限集S的张成定义为由那些是S中有限多个元素的组合的向量v组成的集合：

【3.7.3】
$$v=c_1v_1+\cdots+c_rv_r,\quad 其中\ v_1,\cdots,v_r\in S$$

S中的v_i可是任意的，数r可以任意大，与向量v有关：

【3.7.4】
$$\mathrm{Span}S=\{S\text{ 中元素的有限组合}\}$$

例如，设 $e_i=(0,\cdots,0,1,0,\cdots)$ 是 $\mathbf{R}^\infty$ 中第 i 个位置值为 1 且是它仅有的非零坐标的行向量. 设 $\boldsymbol{E}=(e_1,e_2,e_3,\cdots)$ 是这些向量 e_i 的无限集合. 集合 $\boldsymbol{E}$ 不能张成 $\mathbf{R}^\infty$，因为向量

$$w=(1,1,1,\cdots)$$

不是一个(有限)组合，而 $\boldsymbol{E}$ 的张成是子空间 Z(3.7.2)(c).

一个集合 S(不论是否无限)称为无关的，如果除了在下式中使 $c_1=\cdots=c_r=0$ 的平凡关系外，没有其他的有限线性关系：

【3.7.5】
$$c_1v_1+\cdots+c_rv_r=0,\quad v_1,\cdots,v_r\in S$$

这里数 r 也允许是任意的，即条件对任意大的 r 及任意向量 $v_1,\cdots,v_r\in S$ 都成立. 例如，假如 w，e_i 是前面定义的向量，则集合 $S'=(w;e_1,e_2,e_3,\cdots)$ 是无关的. 在这个无关的定义下，命题 3.4.15 仍然成立.

与有限集一样，V 的基 S 是张成 V 的一个无关集合. 这样 $S=(e_1,e_2,e_3,\cdots)$ 是空间 Z 的基. 单项式 x^i 构成多项式空间的一组基. 应用佐恩引理或选择公理可以证明每个向量空间 V 都有一个基(参见附录，命题 A.3.3). 然而 $\mathbf{R}^\infty$ 的一个基中将有多达不可数的元素，因而它无法被明确地写出来. 97

暂时回到向量空间是有限维的情形(3.4.16)，问是否会存在一个无限基，在(3.4.21)中，我们看到任意两个有限基都有同样多的元素. 我们现在证明每个基都是有限的，从而完成讨论. 这由下面的引理来给出.

【3.7.6】引理 设 V 是有限维向量空间，并设 S 是张成 V 的任意集合. 则 S 中含有一个张成 V 的有限子集.

证明 由假设，有一个有限集，比如 $(u_1,\cdots,u_m)$，它张成空间 V. 因为 $\mathrm{Span}S=V$，所以每一个 u_i 是 S 中有限多个元素的线性组合. 因而当将向量 $u_1,\cdots,u_m$ 用集合 S 表出时，仅需要其中的有限多个元素. 我们用到的元素组成一个有限子集 $S'\subset S$. 于是 $(u_1,\cdots,u_m)\subset\mathrm{Span}S'$. 因为 $(u_1,\cdots,u_m)$ 张成 V，所以 S' 亦张成 V. ■

【3.7.7】推论 设 V 是有限维向量空间.

(a) 每个基都是有限的.

(b) 每个张成 V 的集合 S 含有一个基.

(c) 每个无关集 L 是有限的，因而扩张为一个基.

我不必学 8+7：我将记住 8+8 然后减去 1.

T. Cuyler Young, Jr.

练 习

第二节 域[㊀]

2.1 证明：形如 $a+b\sqrt{2}$ 的数构成复数域的一个子域，其中 a，b 是有理数.

㊀ 原文的第一节未给出练习题. ——译者注

2.2 求 5 模 p 的逆，其中 $p=7$，11，13 和 17.

2.3 当系数视为域 $\mathbf{F}_7$ 中的元素时，计算多项式的乘积 $(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1)$. 说明你的答案.

2.4 考虑线性方程组 $\begin{bmatrix}6 & -3\\2 & 6\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}3\\1\end{bmatrix}$.

(a) 当 $p=5$，11，17 时，在 $\mathbf{F}_p$ 中求解.

(b) 当 $p=7$ 时，求解的个数.

2.5 求素数 p 使矩阵

$$A=\begin{bmatrix}1 & 2 & 0\\0 & 3 & -1\\-2 & 0 & 2\end{bmatrix}$$

98 当其元在 $\mathbf{F}_p$ 中时可逆.

2.6 完全地解线性方程组 $AX=0$ 与 $AX=B$，其中

$$A=\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\1 & -1 & -1\end{bmatrix}\quad 和 \quad B=\begin{bmatrix}1\\-1\\1\end{bmatrix}$$

(a) 在 $\mathbf{Q}$ 中 (b) 在 $\mathbf{F}_2$ 中 (c)在 $\mathbf{F}_3$ 中 (d)在 $\mathbf{F}_7$ 中

2.7 通过找本原元，对所有 $p<20$ 的素数证明乘法群 $\mathbf{F}_p^{\times}$ 是循环群.

2.8 令 p 是素数.

(a) 证明费马定理：对每个整数 a，$a^p\equiv a(\bmod p)$.

(b) 证明威尔逊定理：$(p-1)!\equiv -1(\bmod p)$.

2.9 在群 $GL_2(\mathbf{F}_7)$中确定矩阵 $\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$和$\begin{bmatrix}2 & \\ & 1\end{bmatrix}$的阶.

2.10 在域 $\mathbf{F}_2$ 中解释矩阵元素，证明四个矩阵 $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$, $\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$构成一个域.

提示：可利用矩阵加法和乘法各种运算律缩短证明过程.

2.11 证明符号集合 $\{a+bi \mid a,\ b\in\mathbf{F}_3\}$构成有九个元素的域，如果合成法则模仿复数的加法和乘法. 同样的方法对 $\mathbf{F}_5$ 行得通吗？对 $\mathbf{F}_7$ 呢？给出解释.

第三节 向量空间

3.1 (a) 证明向量与域 F 的零元素的标量乘积是零向量.

(b) 证明：若 w 是子空间 W 的元素，则 $-w$ 也在 W 中.

3.2 下列子集中哪些是系数在 F 里的 $n\times n$ 矩阵的向量空间 $F^{n\times n}$ 的子空间？

(a) 对称矩阵$(A=A^t)$ (b) 可逆矩阵 (c) 上三角矩阵

第四节 基和维数

4.1 求 $n\times n$ 对称矩阵$(A=A^t)$空间的一个基.

4.2 设 $W\subset\mathbf{R}^4$ 是线性方程组 $AX=0$ 的解空间，其中 $A=\begin{bmatrix}2 & 1 & 2 & 3\\1 & 1 & 3 & 0\end{bmatrix}$. 求 W 的基.

4.3 证明三个函数 x^2，$\cos x$ 和 e^x 是线性无关的.

4.4 设 A 是一个 $m\times n$ 矩阵，并设 A'为由 A 上作一系列初等行变换得到的矩阵. 证明 A 的行与 A'的行张成同样的子空间.

4.5 令 $V=F^n$ 是列向量空间. 证明 V 的每个子空间都是某个其次线性方程组 $AX=0$ 的解空间. 99

4.6 求方程 $x_1+2x_2+3x_3+\cdots+nx_n=0$ 在 $\mathbf{R}^n$ 里解空间的一个基.

4.7 令$(X_1, \cdots, X_m)$与$(Y_1, \cdots, Y_n)$分别是 $\mathbf{R}^m$ 与 $\mathbf{R}^n$ 的基. mn 个矩阵 $X_iY_j^t$ 构成所有 $m\times n$ 矩阵的向量空间 $\mathbf{R}^{m\times n}$的一个基吗？

4.8 证明 F^n 中向量集$(v_1, \cdots, v_n)$是一个基当且仅当由诸 v_i 的坐标向量构成的矩阵是可逆的.

第五节 用基计算

5.1 (a) 证明集合 $\boldsymbol{B}=((1,2,0)^t,(2,1,2)^t,(3,1,1)^t)$是 $\mathbf{R}^3$ 的基.

(b) 求向量 $v=(1,2,3)^t$ 关于这个基的坐标向量.

(c) 设 $\boldsymbol{B}'=((0,1,0)^t,(1,0,1)^t,(2,1,0)^t)$求从 $\boldsymbol{B}$ 到 $\boldsymbol{B}'$的基变换矩阵 P.

5.2 (a) 当旧基是标准基 $\boldsymbol{E}=(e_1, e_2)$且新基是 $\boldsymbol{B}=(e_1+e_2, e_1-e_2)$时，在 $\mathbf{R}^2$ 中确定基变换的矩阵.

(b) 当旧基是标准基 $\boldsymbol{E}$ 且新基是 $\boldsymbol{B}=(e_n, e_{n-1}\cdots, e_1)$时，在 $\mathbf{R}^n$ 中确定基变换的矩阵.

(c) 令 $\boldsymbol{B}$ 是 $\mathbf{R}^2$ 的基，其中 $v_1=e_1$，而 v_2 是与 v_1 夹角为 $120°$的单位向量. 确定将标准基 $\boldsymbol{E}$ 联系到基 $\boldsymbol{B}$ 的基变换的矩阵.

5.3 令 $\boldsymbol{B}=(v_1, \cdots, v_n)$是向量空间 V 的基. 证明可以由 $\boldsymbol{B}$ 经过有限步下列类型的作用得到任意一个其他基 $\boldsymbol{B}'$.

(i) 对某个 $a\in F$，用 v_i+av_j 代替 v_i，其中 $i\neq j$.

(ii) 对某个 $c\neq 0$ 用，cv_i 代替 v_i.

(iii) 交换 v_i 和 v_j.

5.4 令是 $\mathbf{F}_p$ 素域，且设 $V=\mathbf{F}_p^2$. 证明：

(a) V 的基的个数等于一般线性群 $GL_2(\mathbf{F}_p)$的阶.

(b) 一般线性群 $GL_2(\mathbf{F}_p)$的阶是 $p(p+1)(p-1)^2$，而且特殊线性群 $SL_2(\mathbf{F}_p)$的阶是 $p(p+1)(p-1)$.

5.5 在下列空间里每个维数的子空间有多少个？

(a) $\mathbf{F}_p^3$ (b) $\mathbf{F}_p^4$.

第六节 直和

6.1 证明实 $n\times n$ 矩阵空间 $\mathbf{R}^{n\times n}$是对称矩阵$(A^t=A)$空间和反对称矩阵$(A^t=-A)$空间的直和.

6.2 方阵的迹是它的对角线上元素的和. 令 W_1 是迹为零的 $n\times n$ 矩阵空间. 求子空间 W_2 使得 $\mathbf{R}^{n\times n}=W_1\oplus W_2$.

6.3 令 $W_1, \cdots, W_k$ 是向量空间 V 的子空间，使得 $V=\sum W_i$. 假设 $W_1\cap W_2=0$，$(W_1+W_2)\cap W_3=0$，…，$(W_1+\cdots+W_k)\cap W_k=0$. 证明 V 是子空间 $W_1, \cdots, W_k$ 的直和. 100

第七节 无限维空间

7.1 令 $\boldsymbol{E}$ 是 $\mathbf{R}^\infty$ 中的向量集$(e_1, e_2\cdots)$，设 $w=(1,1,1,\cdots)$. 描述集合$(w, e_1, e_2\cdots)$的张成.

7.2 双边无穷行向量$(a)=(\cdots, a_{-1}, a_0, a_1, \cdots)$构成一个空间，其中 $a_i\in\mathbf{R}$. 证明该空间同构于 $\mathbf{R}^\infty$.

*7.3 对每个正整数 p，可定义空间 ℓ^p 为使得 $\sum|a_i|^p<\infty$的序列的空间. 证明 ℓ^p 是 ℓ^{p+1}的真子空间.

*7.4 令 V 是由可数无限集合张成的向量空间. 证明 V 的每个无关子集是有限的或是可数无限的.

杂题

M. 1 考虑行列式函数 $\det: F^{2\times 2}\to F$，其中 $F=F_p$ 是 p 个元素的素域而 $F^{2\times 2}$ 是 2×2 矩阵的空间．证明这个映射是满射，并且所有非零行列式的值取同样多的次数，但行列式为 0 的矩阵比行列式为 1 的矩阵多.

M. 2 设 A 是 $n\times n$ 实矩阵．证明存在整数 N 使 A 满足非平凡多项式关系 $A^N+c_{N-1}A^{N-1}+\cdots+c_1A+c_0=0$.

M. 3 (多项式路)

(a) 令 $x(t)$ 和 $y(t)$ 是实系数二次多项式．证明路 $(x(t), y(t))$ 的像包含在圆锥曲面上，亦即，存在实二次多项式 $f(x, y)$ 使得 $f(x(t), y(t))$ 恒为零.

(b) 令 $x(t)=t^2-1$ 与 $y(t)=t^3-t$．求非零实多项式 $f(x, y)$ 使得 $f(x(t), y(t))$ 恒为零．在 $\mathbf{R}^2$ 里画出 $\{f(x, y)=0\}$ 的轨迹和路 $(x(t), y(t))$.

(c) 证明每对实多项式 $x(t)$，$y(t)$ 满足某个实多项式关系 $f(x, y)=0$.

*M. 4 设 V 是无限域 F 上的向量空间．证明 V 不是有限多个真子空间的并.

*M. 5 令 α 是 2 的实立方根.

(a) 证明 $(1, \alpha, \alpha^2)$ 在 Q 上是无关的集合，亦即，没有形如 $a+b\alpha+c\alpha^2$ 的关系，其中 a，b，c 是整数.

提示：用 cx^2+bx+a 除 x^3-2.

(b) 证明实数 $a+b\alpha+c\alpha^2$ 构成域，其中 $a, b, c\in\mathbf{Q}$.

M. 6 (辣酱：数学游戏)我的堂兄 Phil 收集辣汁．他有大约一百个不同的瓶子在书架上，它们当中许多(例如 Tabasco 牌子辣酱油)除水外仅有三种成分：辣椒，醋和食盐．Phil 手头最少需要有多少辣汁瓶子以便他混合已有的辣汁能够获得任意一个仅有这三种成分的辣汁配方？

101