

最后验证  $um + vn = g$ .

断言 2. 对  $i = 0, 1, \dots, k$ ,  $u_i m + v_i n = r_i$ .

断言 2 的证明. 对  $i$  归纳.  $i = 0, 1$  时, 根据  $u_0, v_0, r_0$  和  $u_1, v_1, r_1$  初始值的设定可知,

$$u_0 m + v_0 n = r_0 \quad \text{和} \quad u_1 m + v_1 n = r_1.$$

设  $i > 2$  且结论对  $2, 3, \dots, i-1$  都成立. 由归纳假设可知:

$$u_{i-2} m + v_{i-2} n = r_{i-2} \quad \text{和} \quad u_{i-1} m + v_{i-1} n = r_{i-1}.$$

于是,  $q_i u_{i-1} m + q_i v_{i-1} n = q_i r_{i-1}$ . 由此得出,

$$(u_{i-2} - q_i u_{i-1}) m + (v_{i-2} - q_i v_{i-1}) n = r_{i-2} - q_i r_{i-1}.$$

根据扩展 Euclid 算法循环中第 (c) 步和  $r_i = \text{rem}(r_{i-2}, r_{i-1})$  可知:  $u_i m + v_i n = r_i$ . 断言 3 成立.

取  $i = k$  得  $u_k m + v_k n = r_k$ , 即  $um + vn = g$ .  $\square$

**注解 7.12** 如果我们只计算整数的最大公因子, 则在扩展的辗转相除法中无需计算序列  $q_2, q_3, \dots, u_0, u_1, u_2, u_3, \dots$ , 和  $v_0, v_1, v_2, v_3, \dots$ ,

**例 7.13** 计算  $\text{gcd}(95, 57)$ .

解. 设  $r_0 = 95, r_1 = 57$ . 则

$$\begin{cases} r_2 = \text{rem}(r_0, r_1) = \text{rem}(95, 57) = 38, \\ r_3 = \text{rem}(r_1, r_2) = \text{rem}(57, 38) = 19, \\ r_4 = \text{rem}(r_2, r_3) = \text{rem}(38, 19) = 0. \end{cases}$$

于是,  $r_3 = \gcd(95, 57) = 19$ .

**例 7.14** 计算  $u, v \in \mathbb{Z}$  使得  $u \times 95 + v \times 57 = \gcd(95, 57)$ .

解. 设  $r_0 = 95, u_0 = 1, v_0 = 0, r_1 = 57, u_1 = 0, v_1 = 1$ . 则

$$\left\{ \begin{array}{l} r_2 = \text{rem}(r_0, r_1) = \text{rem}(95, 57) = 38, \\ q_2 = \text{quo}(r_0, r_1) = \text{quo}(95, 57) = 1 \\ u_2 = u_0 - q_2 u_1 = 1, \quad v_2 = v_0 - q_2 v_1 = -1 \\ \\ r_3 = \text{rem}(r_1, r_2) = \text{rem}(57, 38) = 19, \\ q_3 = \text{quo}(r_1, r_2) = \text{quo}(57, 38) = 1 \\ u_3 = u_1 - q_3 u_2 = -1, \quad v_3 = v_1 - q_3 v_2 = 2 \\ \\ r_4 = \text{rem}(r_2, r_3) = \text{rem}(38, 19) = 0. \end{array} \right.$$

于是,  $\underbrace{(-1)}_u \times 95 + \underbrace{2}_v \times 57 = 19$ .

**例 7.15** 上一讲定理 7.2 的另一个证明. 令:

$$S = \{am + bn \mid a, b \in \mathbb{Z}\}.$$

则  $S$  中有正整数. 令  $g$  是  $S$  中的最小正整数. 则存在  $u, v \in \mathbb{Z}$  使得  $um + vn = g$ .

下面我们验证  $g = \gcd(m, n)$ . 设  $d$  是  $m, n$  的公因子. 根据上一讲引理 7.1 可知  $d \mid g$ . 于是,  $d \leq g$ . 设

$r = \text{rem}(m, g)$ . 则存在  $q \in \mathbb{Z}$  使得  $m = qg + r$ . 于是,

$$qum + qvn = qg \implies qum + qvn = m - r \implies (1 - qu)m + (-qv)n = r.$$

由  $g$  的极小性和  $r \in \{0, 1, \dots, g - 1\}$  可知,  $r = 0$ . 故  $g|m$ .

同理  $g|n$ .  $\square$

**定义 7.16** 设  $m, n \in \mathbb{Z}$ . 如果  $\text{gcd}(m, n) = 1$ , 则称  $m$  和  $n$  互素.

**定理 7.17** 设  $m, n \in \mathbb{Z}$  不全为零. 则  $m, n$  互素当且仅当存在  $u, v \in \mathbb{Z}$  使得  $um + vn = 1$ .

证明. 设  $m, n$  互素. 则  $\text{gcd}(m, n) = 1$ . 由定理 7.17 可知, 存在  $u, v \in \mathbb{Z}$  使得  $um + vn = 1$ . 反之, 设存在  $u, v \in \mathbb{Z}$  使得  $um + vn = 1$  和  $g = \text{gcd}(m, n)$ . 因为  $g|m$  和  $g|n$ , 所以  $g|1$  (上一讲引理 7.1). 故  $g = 1$ .  $\square$

**命题 7.18** 设  $m, n \in \mathbb{Z}^+$ . 则

$$\text{lcm}(m, n) = \frac{mn}{\text{gcd}(m, n)}.$$

证明. 断言. 设  $a, b \in \mathbb{Z}^+$  互素满足  $an = bm$ . 则  $an$ , 即  $bm$  是  $m, n$  的最小公倍数.

断言的证明. 设  $\ell = an$ . 则  $\ell = bm$ . 因为  $m|\ell$  且  $n|\ell$ , 所以  $\ell$  是  $m, n$  的公倍数. 再设  $s$  是  $m, n$  的另一个公倍数. 则存

在整数  $a', b'$  使得  $s = a'n = b'm$ . 因为  $a, b$  互素, 所以定理 7.17 蕴含存在  $u, v \in \mathbb{Z}$  使得

$$\begin{aligned} ua + vb = 1 &\implies uas + vbs = s \\ &\implies ua'an + vb'bm = s \quad (\because a'n = b'm = s) \\ &\implies \ell(ua' + vb') = s \quad (\because an = bm = \ell) \\ &\implies \ell | s. \end{aligned}$$

于是,  $\ell$  是最小公倍数. 断言成立.

设  $g = \gcd(m, n)$ . 则存在正整数  $p, q$  使得  $m = pg$  和  $n = qg$  且  $\gcd(p, q) = 1$ . 而

$$\frac{mn}{g} = pqg = pn = qm.$$

由断言可知,  $mn/g$  是最小公倍数.  $\square$

## 7.2 素数

**定义 7.19** 设  $p$  是大于 1 的整数. 如果  $p$  不能写成两个大于 1 的整数之积, 则称  $p$  是素数 (*prime*).

**例 7.20** 证明: 任何大于 1 的整数都是有限个素数之积.

证明. 设  $n$  是大于 1 的整数. 我们对  $n$  归纳. 当  $n = 2$  时显然. 设  $n > 2$  且结论对大于 1 且小于  $n$  的整数都成立. 如果  $n$  是素数, 则结论显然成立. 否则存在两个大于 1 且

小于  $n$  的整数  $i, j$  使得  $n = ij$ , 由归纳假设,  $i$  和  $j$  都是素数的乘积. 故  $n$  也是.  $\square$

素数包括:  $2, 3, 5, 7, 11, 13, 17, 19, \dots$

### 例 7.21

$$24 = 2^3 \times 3, \quad 10969629647 = 104729 \times 104743.$$

### 例 7.22 证明: 素数有无穷多个.

证明. 假设素数只有有限个:  $p_1, \dots, p_k$ . 令  $n = p_1 \cdots p_k + 1$ . 由上例可知, 存在某个素数整除  $n$ . 不妨设该素数是  $p_1$ . 根据第一章第四讲引理 7.1,  $p_1 | 1$ , 矛盾.  $\square$

**引理 7.23** 设  $p$  是素数,  $a, b \in \mathbb{Z}$ . 如果  $p | (ab)$ , 则  $p | a$  或  $p | b$ .

证明. 设  $p \nmid a$ . 则  $\gcd(p, a) = 1$ . 则  $g | p$ . 定理 7.17, 存在  $u, v \in \mathbb{Z}$  使得  $up + va = 1$ . 于是,  $upb + v(ab) = b$ . 根据上一讲引理 7.1,  $p | b$ .  $\square$

**例 7.24** 设  $p$  是素数,  $k$  是小于  $p$  的正整数. 证明:

$$p \mid \binom{p}{k}.$$

证明. 由  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$  可知  $p! = \binom{p}{k} k!(p-k)!$ . 两次应用上述引理可知,  $p | \binom{p}{k}$  或  $p | k!$ , 或  $p | (p-k)!$ . 反复应用上述引理得出:  $p | \binom{p}{k}$  或  $p | i$ , 或  $p | j$ , 其中  $1 \leq i \leq k$  和  $1 \leq j \leq p-k$ . 因为后两种情形不可能发生, 所以  $p | \binom{p}{k}$ .  $\square$

## 第二章 矩阵

### 1 线性相关性

#### 1.1 坐标空间

设

$$\mathbb{R}^{n \times 1} = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \dots, x_n \in \mathbb{R} \right\}.$$

称为  $n$  维列向量(坐标)空间. 设

$$\mathbb{R}^{1 \times n} = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R}\}.$$

称为  $n$  维行向量(坐标)空间. 这学期我们通常在列空间中描述线性代数的内容. 于是, 记  $\mathbb{R}^{n \times 1}$  为  $\mathbb{R}^n$ , 其中的元素称为向量. 特别地

$$\mathbf{0}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n.$$

称为  $\mathbb{R}^n$  中的零向量. 当  $n$  从上下文可确定时,  $\mathbf{0}_n$  记为  $\mathbf{0}$ .

设

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

是  $\mathbb{R}^n$  中的向量. 我们定义

$$\mathbf{x} + \mathbf{y} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

则向量的加法满足下列规律:  $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ ,

- (i) (交换律)  $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ ;
- (ii) (结合律)  $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$ ;
- (iii) (加法单位元)  $\mathbf{x} + \mathbf{0} = \mathbf{x}$ ;
- (iv) (加法逆)  $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$ , 其中  $-\mathbf{x}$  是把  $\mathbf{x}$  中每个坐标反号后得到的向量.

再设  $\lambda \in \mathbb{R}$ . 我们定义数乘

$$\lambda \mathbf{x} := \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

则“标量”与向量的数乘满足下列规律:  $\forall \lambda, \mu \in \mathbb{R}, \mathbf{x} \in \mathbb{R}^n$ ,

- (i)  $(\lambda\mu)\mathbf{x} = \lambda(\mu\mathbf{x})$ ;
- (ii)  $1\mathbf{x} = \mathbf{x}$ .

进而, 加法和数乘满足下列分配律:  $\forall \lambda, \mu \in \mathbb{R}, \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ ,

$$(i) \lambda(\mathbf{x} + \mathbf{y}) = \lambda\mathbf{x} + \lambda\mathbf{y};$$

$$(ii) (\lambda + \mu)\mathbf{x} = \lambda\mathbf{x} + \mu\mathbf{x}.$$

例 1.1 设

$$\mathbf{x} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}.$$

则

$$2\mathbf{x} + 3\mathbf{y} = 2 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} + \begin{pmatrix} 3 \\ -3 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \\ 6 \end{pmatrix}.$$

例 1.2 设以  $x_1, \dots, x_n$  为实未知数的线性方程组的增广矩阵是  $B = (A|\mathbf{b})$ , 其中  $A \in \mathbb{R}^{m \times n}$ ,  $\mathbf{b} \in \mathbb{R}^m$ . 则该方程组可以表示为

$$x_1 \vec{A}^{(1)} + \dots + x_n \vec{A}^{(n)} = \mathbf{b}.$$

## 1.2 线性组合, 线性相关和线性无关

定义 1.3 设  $\mathbf{w}, \mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ . 如果存在  $\alpha_1, \dots, \alpha_k \in \mathbb{R}$  使得

$$\mathbf{w} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k,$$

则称  $\mathbf{w}$  是  $\mathbf{v}_1, \dots, \mathbf{v}_k$  (在  $\mathbb{R}$  上) 的线性组合.

当  $\mathbf{w} = \alpha \mathbf{v}$ , 其中  $\alpha \in \mathbb{R}$ , 我们说  $\mathbf{w}$  和  $\mathbf{v}$  “平行”. 特别地,  $\mathbf{0}_n$  与  $\mathbb{R}^n$  中的向量都平行.

**例 1.4** 设  $\mathbf{w}, \mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ . 则  $A = (\mathbf{v}_1, \dots, \mathbf{v}_k) \in \mathbb{R}^{n \times k}$  和  $B = (A|\mathbf{w}) \in \mathbb{R}^{n \times (k+1)}$ . 根据例 1.2, 以  $B$  为增广矩阵的  $k$  元线性方程组相容当且仅当  $\mathbf{w}$  是  $\mathbf{v}_1, \dots, \mathbf{v}_k$  的线性组合.

**例 1.5** 设

$$\mathbf{x} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad \mathbf{z} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

判定  $\mathbf{z}$  是不是  $\mathbf{x}$  和  $\mathbf{y}$  的线性组合.

解. 考虑增广矩阵

$$B = (\mathbf{x}, \mathbf{y}|\mathbf{z}) = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & 1 \\ 3 & 0 & 1 \end{pmatrix}.$$

由 Gauss 消去法可知,

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & 1 \\ 3 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & -3 & -1 \\ 0 & -3 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & -3 & -1 \\ 0 & 0 & -1 \end{pmatrix}.$$

于是,  $B$  对应的线性方程组不相容. 故  $\mathbf{z}$  不是  $\mathbf{x}$  和  $\mathbf{y}$  的线性组合(第一章第一讲定理 2.5).

记号. 在  $\mathbb{R}^n$  中,

$$\mathbf{e}_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \mathbf{e}_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \mathbf{e}_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

**注解 1.6** 对任意

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

我们有  $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \dots + x_n\mathbf{e}_n$ . 即  $\mathbb{R}^n$  中的任意向量都是  $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n$  的线性组合.

**定义 1.7** 设  $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ . 如果存在  $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ , 不全为零, 使得

$$\alpha_1\mathbf{v}_1 + \dots + \alpha_k\mathbf{v}_k = \mathbf{0},$$

则称  $\mathbf{v}_1, \dots, \mathbf{v}_k$  (在  $\mathbb{R}$ ) 上线性相关. 否则, 我们称  $\mathbf{v}_1, \dots, \mathbf{v}_k$  (在  $\mathbb{R}$ ) 上线性无关.

由上述定义可知, 一个向量  $\mathbf{v}$  线性相关当且仅当  $\mathbf{v} = \mathbf{0}$ . 如果  $\mathbf{v}_1, \dots, \mathbf{v}_k$  中有一个零向量, 则它们必然线性相关. 两个向量线性无关当且仅当它们不平行.

**例 1.8** 设  $A = (\mathbf{v}_1, \dots, \mathbf{v}_k) \in \mathbb{R}^{n \times k}$ . 根据例 1.2, 以  $A$  为系数矩阵的  $k$  元齐次线性方程组有非平凡解当且仅当  $\mathbf{v}_1, \dots, \mathbf{v}_k$  的线性相关.

**例 1.9** 设

$$\mathbf{x} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad \mathbf{z} = \begin{pmatrix} 5 \\ 1 \\ 6 \end{pmatrix}.$$

判定  $\mathbf{x}, \mathbf{y}, \mathbf{z}$  是否线性相关.

解. 设  $A = (\mathbf{x}, \mathbf{y}, \mathbf{z})$ . 由 Gauss 消去法可知

$$A = \begin{pmatrix} 1 & 1 & 5 \\ 2 & -1 & 1 \\ 3 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 5 \\ 0 & -3 & -9 \\ 0 & -3 & -9 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 5 \\ 0 & -3 & -9 \\ 0 & 0 & 0 \end{pmatrix}.$$

于是, 以  $A$  为系数矩阵的齐次线性方程组有非平凡解. 故  $\mathbf{x}, \mathbf{y}, \mathbf{z}$  线性相关 (第一章第一讲定理 2.7).

**例 1.10** 证明:  $\mathbf{e}_1, \dots, \mathbf{e}_n \in \mathbb{R}^n$  线性无关.

证明. 设  $\alpha_1, \dots, \alpha_n \in \mathbb{R}$  使得  $\alpha_1 \mathbf{e}_1 + \dots + \alpha_n \mathbf{e}_n = \mathbf{0}$ . 则

$$\alpha_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + \alpha_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \implies \alpha_1 = \dots = \alpha_n = 0.$$

故  $\mathbf{e}_1, \dots, \mathbf{e}_n$  线性无关.

下面的命题总结了关于线性组合、线性相关和无关的基本事实.

**命题 1.11** 设  $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{R}^n$ .

- (i) 如果存在  $i \in \{1, \dots, k\}$  使得  $\mathbf{v}_1, \dots, \mathbf{v}_i$  线性相关, 则  $\mathbf{v}_1, \dots, \mathbf{v}_i, \dots, \mathbf{v}_k$  也线性相关;
- (ii) 如果  $\mathbf{v}_1, \dots, \mathbf{v}_i, \dots, \mathbf{v}_k$  线性无关, 则对任意  $i \in \{1, \dots, k\}$  使得  $\mathbf{v}_1, \dots, \mathbf{v}_i$  也线性无关;
- (iii) 向量  $\mathbf{v}_1, \dots, \mathbf{v}_k$  线性相关当且仅当这些向量中的某个向量是其它向量的线性组合;
- (iv) 再设  $\mathbf{v} \in \mathbb{R}^n$  且  $\mathbf{v}_1, \dots, \mathbf{v}_k$  线性无关. 则  $\mathbf{v}, \mathbf{v}_1, \dots, \mathbf{v}_k$  线性相关当且仅当存在唯一的  $\alpha_1, \dots, \alpha_k \in \mathbb{R}$  使得

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k.$$

证明. (i) 因为  $\mathbf{v}_1, \dots, \mathbf{v}_i$  线性相关, 所以存在  $\alpha_1, \dots, \alpha_i \in \mathbb{R}$ , 不全为零, 使得

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_i \mathbf{v}_i = \mathbf{0}.$$

于是,

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_i \mathbf{v}_i + 0\mathbf{v}_{i+1} + \dots + 0\mathbf{v}_k = \mathbf{0}.$$

因为在  $\alpha_1, \dots, \alpha_i$  中已有非零实数, 所以  $\mathbf{v}_1, \dots, \mathbf{v}_i, \dots, \mathbf{v}_k$  线性相关.

(ii) 是 (i) 的逆否命题.

(iii) 设向量  $\mathbf{v}_1, \dots, \mathbf{v}_k$  线性相关. 则存在  $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ , 不全为零, 使得

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0}.$$

不妨设  $\alpha_1 \neq 0$ . 则

$$\mathbf{v}_1 = -(\alpha_1^{-1} \alpha_2) \mathbf{v}_2 - \dots - (\alpha_1^{-1} \alpha_k) \mathbf{v}_k.$$

反之不妨设  $\mathbf{v}_k$  是  $\mathbf{v}_1, \dots, \mathbf{v}_{k-1}$  的线性组合. 则存在  $\beta_1, \dots, \beta_{k-1} \in \mathbb{R}$  使得

$$\mathbf{v}_k = \beta_1 \mathbf{v}_1 + \dots + \beta_{k-1} \mathbf{v}_{k-1}.$$

于是,  $\beta_1 \mathbf{v}_1 + \dots + \beta_{k-1} \mathbf{v}_{k-1} + (-1) \mathbf{v}_k = \mathbf{0}$ . 故  $\mathbf{v}_1, \dots, \mathbf{v}_{k-1}, \mathbf{v}_k$  线性相关.

(iv) 设  $\mathbf{v}, \mathbf{v}_1, \dots, \mathbf{v}_k$  线性相关. 则存在  $\beta, \alpha_1, \dots, \alpha_k \in \mathbb{R}$ , 不全为零, 使得

$$\beta \mathbf{v} + \alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0}.$$

则  $\beta \neq 0$ . 否则, 我们有  $\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0}$  且  $\alpha_1, \dots, \alpha_k$  不全为零. 从而推出  $\mathbf{v}_1, \dots, \mathbf{v}_k$  线性相关, 矛盾. 故

$$\mathbf{v} = -(\beta^{-1} \alpha_1) \mathbf{v}_1 - \dots - (\beta^{-1} \alpha_k) \mathbf{v}_k.$$

再设  $\mathbf{v} = \lambda_1 \mathbf{v}_1 + \cdots + \lambda_k \mathbf{v}_k = \mu_1 \mathbf{v}_1 + \cdots + \mu_k \mathbf{v}_k$ . 其中  $\lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_k \in \mathbb{R}$ . 则

$$(\lambda_1 - \mu_1) \mathbf{v}_1 + \cdots + (\lambda_k - \mu_k) \mathbf{v}_k = \mathbf{0}.$$

因为  $\mathbf{v}_1, \dots, \mathbf{v}_k$  线性无关, 所以  $\lambda_1 = \mu_1, \dots, \lambda_k = \mu_k$ .

逆命题由 (iii) 直接可得.  $\square$

以下引理是建立维数概念的关键.

**引理 1.12 (线性组合引理)** 设  $\mathbf{v}_1, \dots, \mathbf{v}_k; \mathbf{w}_1, \dots, \mathbf{w}_\ell$  是  $\mathbb{R}^n$  中的两组向量. 设对任意  $j \in \{1, 2, \dots, \ell\}$ ,  $\mathbf{w}_j$  是  $\mathbf{v}_1, \dots, \mathbf{v}_k$  的线性组合. 如果  $\ell > k$ , 则  $\mathbf{w}_1, \dots, \mathbf{w}_\ell$  线性相关.

证明. 设  $\mathbf{w}_j = \sum_{i=1}^k \alpha_{i,j} \mathbf{v}_i$ , 其中  $\alpha_{i,j} \in \mathbb{R}, j \in \{1, 2, \dots, \ell\}$ . 再设  $\lambda_1, \dots, \lambda_\ell$  是待定的实数. 则

$$\sum_{j=1}^{\ell} \lambda_j \mathbf{w}_j = \sum_{j=1}^{\ell} \lambda_j \left( \sum_{i=1}^k \alpha_{i,j} \mathbf{v}_i \right) \quad (1)$$

$$= \sum_{j=1}^{\ell} \sum_{i=1}^k (\lambda_j \alpha_{i,j}) \mathbf{v}_i \quad (\text{分配律和结合律}) \quad (2)$$

$$= \sum_{i=1}^k \sum_{j=1}^{\ell} (\lambda_j \alpha_{i,j}) \mathbf{v}_i \quad (\text{和号互换}) \quad (3)$$

$$= \sum_{i=1}^k \left( \sum_{j=1}^{\ell} \lambda_j \alpha_{i,j} \right) \mathbf{v}_i \quad (\text{分配律}) \quad (4)$$

考虑以  $\lambda_1, \dots, \lambda_\ell$  为未知数的齐次线性方程组

$$\sum_{j=1}^{\ell} \lambda_j \alpha_{i,j} = 0, \quad i = 1, 2, \dots, k.$$

根据  $\ell > k$  和第一章第一讲推论 2.8 (红色推论), 上述方程组有非零解  $\lambda_1, \dots, \lambda_\ell \in \mathbb{R}$ . 由 (4) 可知,  $\sum_{j=1}^{\ell} \lambda_j \mathbf{w}_j = \mathbf{0}$ . 故  $\mathbf{w}_1, \dots, \mathbf{w}_\ell$  线性相关.  $\square$

**例 1.13** 设  $\mathbf{u}_1, \dots, \mathbf{u}_m \in \mathbb{R}^n$ . 证明: 如果  $m > n$ , 则  $\mathbf{u}_1, \dots, \mathbf{u}_m$  线性相关.

证明. 由注解 1.6 可知,  $\mathbf{u}_1, \dots, \mathbf{u}_m$  都是  $\mathbf{e}_1, \dots, \mathbf{e}_n$  的线性组合. 根据线性组合引理和假设  $m > n$  可知,  $\mathbf{u}_1, \dots, \mathbf{u}_m$  线性相关.  $\square$

**例 1.14** (线性组合的传递性) 设向量  $\mathbf{u}, \mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots, \mathbf{w}_\ell$  在  $\mathbb{R}^n$  中. 如果  $\mathbf{u}$  是  $\mathbf{v}_1, \dots, \mathbf{v}_k$  的线性组合且每个  $\mathbf{v}_i$  都是  $\mathbf{w}_1, \dots, \mathbf{w}_\ell$  的线性组合, 则  $\mathbf{u}$  也是  $\mathbf{w}_1, \dots, \mathbf{w}_\ell$  的线性组合.

证明. 设  $\mathbf{u} = \sum_{i=1}^k \alpha_i \mathbf{v}_i$  和  $\mathbf{v}_i = \sum_{j=1}^{\ell} \beta_{i,j} \mathbf{w}_j$ , 其中  $\alpha_i, \beta_{i,j} \in \mathbb{R}$ . 则  $\mathbf{u} = \sum_{i=1}^k \alpha_i \left( \sum_{j=1}^{\ell} \beta_{i,j} \mathbf{w}_j \right) = \sum_{j=1}^{\ell} \left( \sum_{i=1}^k \alpha_i \beta_{i,j} \right) \mathbf{w}_j$ . 故  $\mathbf{u}$  是  $\mathbf{w}_1, \dots, \mathbf{w}_\ell$  的线性组合.  $\square$

### 1.3 坐标空间中的子空间

**定义 1.15** 设  $U$  是  $\mathbb{R}^n$  中的非空子集. 如果对任意  $\mathbf{x}, \mathbf{y} \in U$  和  $\alpha \in \mathbb{R}$ ,

(i) (加法封闭性)  $\mathbf{x} + \mathbf{y} \in U$ ,

(ii) (数乘封闭性)  $\alpha \mathbf{x} \in U$ .

则称  $U$  是  $\mathbb{R}^n$  中的子空间(subspace).

**命题 1.16** 设  $U$  是  $\mathbb{R}^n$  中的非空子集. 则下列命题等价.

(i)  $U$  是子空间;

(ii)  $U$  中任意两个向量的线性组合仍在  $U$  中;

(iii) 对任意  $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$ ,  $\mathbf{u}_1, \dots, \mathbf{u}_k$  的任意线性组合都在  $U$  中.

证明. “(i)  $\implies$  (ii)” 设  $\mathbf{x}, \mathbf{y}$  是  $U$  中任意的两个向量,  $\alpha, \beta$  是任意两个实数. 如果  $U$  是子空间, 则  $\alpha \mathbf{x}, \beta \mathbf{y} \in U$  (数乘封闭性). 从而  $\alpha \mathbf{x} + \beta \mathbf{y} \in U$  (加法封闭性). 反之, 设  $\alpha \mathbf{x} + \beta \mathbf{y} \in U$ . 取  $\alpha = \beta = 1$  得到加法封闭性, 取  $\beta = 0$  得到数乘封闭性. 故  $U$  是子空间.

“(ii)  $\implies$  (iii)” 当  $k = 1, 2$  时, (ii) 蕴含  $\mathbf{u}_1, \mathbf{u}_2$  的所有线性组合都在  $U$  中. 设  $k > 2$  时且  $U$  中任何  $k - 1$  个向量的线性组合都在  $U$  中. 对任意  $\alpha_1, \dots, \alpha_{k-1}, \alpha_k \in \mathbb{R}$ ,  $\mathbf{u}_1, \dots, \mathbf{u}_{k-1}, \mathbf{u}_k \in U$ , 我们有

$$\sum_{i=1}^k \alpha_i \mathbf{u}_i = \left( \sum_{i=1}^{k-1} \alpha_i \mathbf{u}_i \right) + \alpha_k \mathbf{u}_k \in U.$$

“(iii)  $\implies$  (i)” 由线性组合的定义直接得出.  $\square$

**例 1.17** 设  $A \in \mathbb{R}^{m \times n}$ , 其对应的  $n$  元齐次线性方程组记为  $H$ . 验证  $\text{sol}(H)$  是  $\mathbb{R}^n$  中的子空间.

证明. 设

$$\mathbf{v} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

是  $H$  的两个解. 则

$$\alpha_1 \vec{A}^{(1)} + \cdots + \alpha_n \vec{A}^{(n)} = \mathbf{0}_m, \quad \beta_1 \vec{A}^{(1)} + \cdots + \beta_n \vec{A}^{(n)} = \mathbf{0}_m.$$

令  $\lambda, \mu$  是两个实数,  $\mathbf{u} = \lambda \mathbf{v} + \mu \mathbf{w}$ . 则

$$\mathbf{u} = \begin{pmatrix} \lambda \alpha_1 + \mu \beta_1 \\ \vdots \\ \lambda \alpha_n + \mu \beta_n \end{pmatrix}.$$

而

$$\sum_{j=1}^n (\lambda \alpha_j + \mu \beta_j) \vec{A}^{(j)} = \lambda \left( \sum_{j=1}^n \alpha_j \vec{A}^{(j)} \right) + \mu \left( \sum_{j=1}^n \beta_j \vec{A}^{(j)} \right) = \mathbf{0}_m.$$

故  $\mathbf{u} \in \text{sol}(H)$ . 根据命题 1.16,  $\text{sol}(H)$  是子空间.  $\square$

**命题 1.18** 设  $\Lambda$  是一个指标集, 对任意  $\lambda \in \Lambda$ ,  $U_\lambda$  是  $\mathbb{R}^n$  中的子空间. 则  $\bigcap_{\lambda \in \Lambda} U_\lambda$  也是子空间.

证明. 设  $\mathbf{v}, \mathbf{w} \in \bigcap_{\lambda \in \Lambda} U_\lambda$ ,  $\alpha, \beta \in \mathbb{R}$ . 因为  $\mathbf{v}, \mathbf{w} \in U_\lambda$ , 其中  $\lambda$  是  $\Lambda$  中任意元素, 所以  $\alpha \mathbf{u} + \beta \mathbf{v} \in U_\lambda$  (命题 1.16). 由此可

知,  $\alpha \mathbf{u} + \beta \mathbf{v} \in \bigcap_{\lambda \in \Lambda} U_\lambda$ . 故  $\bigcap_{\lambda \in \Lambda} U_\lambda$  是子空间(命题 1.16).

□

设  $S_1, \dots, S_k$  是  $\mathbb{R}^n$  的非空子集. 我们定义  $S_1, \dots, S_k$  的和为

$$S_1 + \dots + S_k := \{\mathbf{v}_1 + \dots + \mathbf{v}_k \mid \mathbf{v}_1 \in S_1, \dots, \mathbf{v}_k \in S_k\}.$$

**命题 1.19** 设  $U_1, \dots, U_k$  是  $\mathbb{R}^n$  的子空间. 则  $U_1 + \dots + U_k$  也是子空间.

证明. 设  $\mathbf{x}, \mathbf{y} \in \sum_{i=1}^k U_i$ . 则存在  $\mathbf{u}_i, \mathbf{v}_i \in U_i, i = 1, 2, \dots, k$ , 使得  $\mathbf{x} = \sum_{i=1}^k \mathbf{u}_i$  和  $\mathbf{y} = \sum_{i=1}^k \mathbf{v}_i$ . 则对任意  $\alpha, \beta \in \mathbb{R}$ ,

$$\alpha \mathbf{x} + \beta \mathbf{y} = \alpha \left( \sum_{i=1}^k \mathbf{u}_i \right) + \beta \left( \sum_{i=1}^k \mathbf{v}_i \right) = \sum_{i=1}^k (\alpha \mathbf{u}_i + \beta \mathbf{v}_i).$$

根据命题 1.16,  $\alpha \mathbf{u}_i + \beta \mathbf{v}_i \in U_i, i = 1, 2, \dots, k$ . 我们得到  $\alpha \mathbf{x} + \beta \mathbf{y} \in \sum_{i=1}^k U_i$ . 故  $\sum_{i=1}^k U_i$  是子空间. □

**定义 1.20** 设  $\mathbf{v} \in \mathbb{R}^n$  和  $U$  是  $\mathbb{R}^n$  的子空间. 则  $\{\mathbf{v}\} + U$  简记为  $\mathbf{v} + U$ . 称为一个线性流形.