7 整数的算数

7.1 最大公因子和最小公倍数

以下引理是整除的一个基本性质.

引理 7.1 设 $m, n, d \in \mathbb{Z}$ 且 $d \neq 0$. 如果 $d|m$ 且 $d|n$, 则对于任意 $u, v \in \mathbb{Z}$, $d|(um + vn)$.

证明. 设 $a, b \in \mathbb{Z}$ 使得 $m = ad$ 和 $n = bd$. 则

$$um + vn = uad + vbd = (ua + vb)d.$$

于是, $d|(um + vn)$. □

设 $m, n, c \in \mathbb{Z}^+$. 如果 $c|m$ 且 $c|n$, 则称 c 是 m, n 的公因子. 设 g 是 m, n 的正公因子. 如果任何 m, n 的公因子都整除 g, 则称 g 是 m, n 的最大公因子.

注意到 1 是 m, n 的公因子. 于是 m, n 的最大公因子必然存在且唯一, 并记为 $\gcd(m, n)$.

对于两个非零整数 m, n, 它们的最大公因子定义为 $\gcd(|m|, |n|)$. 如果 $n = 0$, 则它们的最大公因子定义为 $|m|$. 下面我们描述两个计算正整数的最大公因子算法–辗转相除（*Euclidean*）算法.

定理 7.2 设 $m, n \in \mathbb{Z}^+$. 则下列算法在有限步内输出正整数 g, 和整数 u, v 使得

(i) $g = \gcd(m, n)$;

(ii) $um + vn = g$.

扩展的辗转相除法(Extended Euclidean Algorithm)

输入: $m, n \in \mathbb{Z}^+$

输出: $g \in \mathbb{Z}^+$, $u, v \in \mathbb{Z}$ 使得 $g = \gcd(m, n)$ 和 $um + vn = g$.

1. *[初始化]* 令 $r_0 := m$; $r_1 := n$; $i = 1$; $u_0 := 1$; $v_0 := 0$; $u_1 = 0$; $v_1 := 1$;

2. *[循环]* *while* $r_i \neq 0$ *do*

   (a) $i := i + 1$;

   (b) $q_i := \mathrm{quo}(r_{i-2}, r_{i-1})$; $r_i := \mathrm{rem}(r_{i-2}, r_{i-1})$;

   (c) $u_i := u_{i-2} - q_i u_{i-1}$; $v_i := v_{i-2} - q_i v_{i-1}$;

   end do;

3. *[准备返回]* $g := r_{i-1}$; $u := u_{i-1}$; $v := v_{i-1}$;

4. *[返回]* *return* g, u, v;

证明. 首先验证该算法在有限步内必然终止. 注意到算法中的循环产生一个关于余数的严格递减序列

$$r_1 > r_2 > \cdots .$$

因为余数都非负, 所以该余数序列有限步必然终止. 此时最后一项一定是零. 由此可知, 算法终止.

设 算法终止于 $r_{k+1} = 0$. 则算法输出为 $g = r_k$ 且 $\mathrm{rem}(r_{k-1}, r_k) = 0$. 事实上, 算法产生的商序列

$$q_2, \ldots, q_k, q_{k+1}.$$

两序列之间的关系如下

$$r_{i-2} = q_i r_{i-1} + r_i, \quad i = 2, 3, \ldots, k+1. \tag{1}$$

下面我们来验证 $g = \gcd(m, n)$. 根据 (1), 我们有

$$\begin{cases} r_0 = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \vdots \\ r_{k-4} = q_{k-2} r_{k-3} + r_{k-2} \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} = q_k r_{k-1} + r_k \\ r_{k-1} = q_{k+1} r_k \end{cases} \tag{2}$$

断言 *1.* 对 $j = 2, 3, \ldots, k$, $\gcd(r_{j-2}, r_{j-1}) = \gcd(r_{j-1}, r_j)$.

断言 *1* 证明. 我们有 $r_{j-2} = q_j r_{j-1} + r_j$. 根据引理 7.1, r_{j-2}, r_{j-1} 的公因子都是 r_{j-1}, r_j 的公因子, 反之也一样. 断言 1 成立.

由断言 1 可知, $\gcd(m, n) = \gcd(r_0, r_1) = \gcd(r_{k-1}, r_k)$. 故 $\gcd(m, n) = r_k$.

最后验证 $um + vn = g$.

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

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 $2, 3, \ldots, i-1$ 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 $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$ 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 $um + vn = g$. □

注解 7.3 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 $q_2, q_3, \ldots$, $u_0, u_1, u_2, u_3, \ldots$, 和 $v_0, v_1, v_2, v_3, \ldots$,

例 7.4 计算 $\gcd(95, 57)$.

解. 设 $r_0 = 95, r_1 = 57$. 则

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

于是, $r_3 = \gcd(95, 57) = 19$.

例 7.5 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

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

于是, $\underbrace{(-1)}_{u} \times 95 + \underbrace{2}_{v} \times 57 = 19$.

例 7.6 上一讲定理 *7.2* 的另一个证明. 令:

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

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 $d|g$. 于是, $d \leq g$. 设

$r = \mathrm{rem}(m, g)$. 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 $r \in \{0, 1, \ldots, g-1\}$ 可知, $r = 0$. 故 $g|m$. 同理 $g|n$. □

定义 7.7 设 $m, n \in \mathbb{Z}$. 如果 $\gcd(m, n) = 1$, 则称 m 和 n 互素.

定理 7.8 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 $\gcd(m, n) = 1$. 由定理 7.8 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 $g = \gcd(m, n)$. 因为 $g|m$ 和 $g|n$, 所以 $g|1$ (上一讲引理 7.1). 故 $g = 1$. □

命题 7.9 设 $m, n \in \mathbb{Z}^+$. 则

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

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 ℓ 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 7.8 蕴含存在 $u, v \in \mathbb{Z}$ 使得

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

于是, ℓ 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. □

7.2 素数

定义 7.10 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 7.11 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. □

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

例 7.12

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

例 7.13 证明: 素数有无穷多个.

证明. 假设素数只有有限个: $p_1, \ldots, p_k$. 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. □

引理 7.14 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 $\gcd(p, a) = 1$. 由定理 7.8 可知, 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, $p|b$. □

例 7.15 设 p 是素数, k 是小于 p 的正整数. 证明:

$$p \Big| \binom{p}{k}.$$

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 $1 \le i \le k$ 和 $1 \le j \le p-k$. 因为后两种情形不可能发生, 所以 $p|\binom{p}{k}$. □

第二章　矩阵

1　线性相关性

1.1　坐标空间

设

$$\mathbb{R}^{n\times 1}=\{\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\,|\,x_1,\ldots,x_n\in\mathbb{R}\}.$$

称为 n 维列向量(坐标)空间. 设

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

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 $x_1,\ldots,x_n$ 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

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

1.2 线性组合，线性相关和线性无关

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

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

则称 $\mathbf{w}$ 是 $\mathbf{v}_1,\ldots,\mathbf{v}_k$ （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 $\mathbf{w},\mathbf{v}_1,\ldots,\mathbf{v}_k\in\mathbb{R}^n$. 则 $A=(\mathbf{v}_1,\ldots,\mathbf{v}_k)\in\mathbb{R}^{n\times k}$ 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 $\mathbf{v}_1,\ldots,\mathbf{v}_k$ 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,

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

注解 1.6 对任意

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

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

例 1.7 *(线性组合的传递性)* 设向量 $\mathbf{u}$, $\mathbf{v}_1$, $\ldots$, $\mathbf{v}_k$, $\mathbf{w}_1$, $\ldots$, $\mathbf{w}_\ell$ 在 $\mathbb{R}^n$ 中. 如果 $\mathbf{u}$ 是 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 的线性组合且每个 $\mathbf{v}_i$ 都是 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 的线性组合, 则 $\mathbf{u}$ 也是 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 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 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 的线性组合. □

定义 1.8 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$. 如果存在 $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$, 不全为零, 使得

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

则称 $\mathbf{v}_1, \ldots, \mathbf{v}_k$（在 $\mathbb{R}$）上线性相关. 否则, 我们称 $\mathbf{v}_1, \ldots, \mathbf{v}_k$（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 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 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 1.9 设 $A = (\mathbf{v}_1, \ldots, \mathbf{v}_k) \in \mathbb{R}^{n\times k}$. 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 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 的线性相关.

例 1.10 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 1.11 证明: $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{R}^n$ 线性无关.

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

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

故 $\mathbf{e}_1, \ldots, \mathbf{e}_n$ 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 1.12 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$.

(i) 如果存在 $i \in \{1, \ldots, k\}$ 使得 $\mathbf{v}_1, \ldots, \mathbf{v}_i$ 线性相关, 则 $\mathbf{v}_1, \ldots, \mathbf{v}_i, \ldots, \mathbf{v}_k$ 也线性相关;

(ii) 如果 $\mathbf{v}_1, \ldots, \mathbf{v}_i, \ldots, \mathbf{v}_k$ 线性无关, 则对任意 $i \in \{1, \ldots, k\}$ 使得 $\mathbf{v}_1, \ldots, \mathbf{v}_i$ 也线性无关;

(iii) 向量 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 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 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 线性无关. 则 $\mathbf{v}, \mathbf{v}_1, \ldots, \mathbf{v}_k$ 线性相关当且仅当存在唯一的 $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ 使得

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

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

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

于是,

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

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

(ii) 是 (i) 的逆否命题.

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

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

不妨设 $\alpha_1 \neq 0$. 则

$$\mathbf{v}_1 = -(\alpha_1^{-1}\alpha_2)\mathbf{v}_2 - \cdots - (\alpha_1^{-1}\alpha_n)\mathbf{v}_n.$$

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

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

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

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

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

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

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

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 $\lambda_1, \ldots, \lambda_k, \mu_1, \ldots, \mu_k \in \mathbb{R}$. 则

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

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

逆命题由 (iii) 直接可得. □

以下引理是建立维数概念的关键.

引理 1.13 *(线性组合引理)* 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k; \mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 是 $\mathbb{R}^n$ 中的两组向量. 设对任意 $j \in \{1, 2, \ldots, \ell\}$, $\mathbf{w}_j$ 是 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 的线性组合. 如果 $\ell > k$, 则 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 线性相关.

证明. 设 $\mathbf{w}_j = \sum_{i=1}^{k} \alpha_{i,j}\mathbf{v}_i$, 其中 $\alpha_{i,j} \in \mathbb{R}, j \in \{1, 2, \ldots, \ell\}$.

再设 $\lambda_1, \ldots, \lambda_\ell$ 是待定的实数. 则

$$\sum_{j=1}^{\ell} \lambda_j \mathbf{w}_j = \sum_{j=1}^{\ell} \lambda_j \left(\sum_{i=1}^{k} \alpha_{i,j} \mathbf{v}_i \right) \tag{3}$$

$$= \sum_{j=1}^{\ell} \sum_{i=1}^{k} (\lambda_j \alpha_{i,j}) \mathbf{v}_i \quad \text{(分配律和结合律)} \tag{4}$$

$$= \sum_{i=1}^{k} \sum_{j=1}^{\ell} (\lambda_j \alpha_{i,j}) \mathbf{v}_i \quad \text{(和号互换)} \tag{5}$$

$$= \sum_{i=1}^{k} \left(\sum_{j=1}^{\ell} \lambda_j \alpha_{i,j} \right) \mathbf{v}_i \quad \text{(分配律)} \tag{6}$$

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

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

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 $\lambda_1, \ldots, \lambda_\ell \in \mathbb{R}$. 由 (6) 可知, $\sum_{j=1}^{\ell} \lambda_j \mathbf{w}_j = \mathbf{0}$. 故 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 线性相关. □