

## 第三章 行列式

### 3.3 乘法定理

**定理 3.10** 设  $A, B \in M_n(\mathbb{R})$ . 则

$$\det(AB) = \det(A) \det(B).$$

证明. (矩阵法) 如果  $A$  或  $B$  不满秩, 则  $AB$  也不满秩 (第二章第四讲定理 6.25 (i)). 故  $\det(AB) = 0$  (第三章第一讲定理 2.14). 同理  $\det(A) \det(B) = 0$ . 故定理成立.

断言. 设  $C, M \in M_n(\mathbb{R})$  且  $C$  是初等矩阵. 则

$$\det(CM) = \det(C) \det(M) = \det(MC).$$

断言的证明. 设  $C = F_{i,j}$ . 如果  $i = j$ , 则  $C = E$ . 断言显然成立. 如果  $i \neq j$ . 则  $\det(CM) = \det(MC) = -\det(M)$ . 而  $\det(C) \det(M) = -\det(M)$ . 断言也成立.

设  $C = F_{i,j}(\alpha)$ ,  $i \neq j$ . 则  $\det(CM)$ ,  $\det(MC)$  和  $\det(C) \det(M)$  都等于  $\det(M)$ . 故断言成立.

设  $C = F_i(\lambda)$ . 则  $\det(CM)$ ,  $\det(MC)$  和  $\det(C) \det(M)$  都等于  $\lambda \det(M)$ . 断言成立.

设矩阵  $A$  满秩. 则存在初等矩阵  $C_1, C_2, \dots, C_p$  使得

$$A = C_1 C_2 \cdots C_p$$

(第二章第五讲定理 7.14 和第六讲推论 8.6). 由断言可知,

$$\det(A) = \det(C_1) \det(C_2 \cdots C_p) = \det(C_1) \det(C_2) \cdots \det(C_p). \quad (1)$$

类似地

$$\begin{aligned} \det(AB) &= \det(C_1(C_2 \cdots C_p B)) \\ &= \det(C_1) \det(C_2 \cdots C_p B) \quad (\text{断言}) \\ &= \det(C_1) \det(C_2) \cdots \det(C_p) \det(B) \\ &= \det(A) \det(B) \quad ((1)). \end{aligned}$$

定理成立.

(映射法) 定义:

$$\begin{aligned} f: \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_n &\longrightarrow \mathbb{R} \\ (\vec{B}^{(1)}, \dots, \vec{B}^{(n)}) &\mapsto \det(A\vec{B}^{(1)}, \dots, A\vec{B}^{(n)}) = \det(AB) \end{aligned}$$

由行列式的双重线性和矩阵乘法的分配律可直接验证  $f$  是多重线性的. 再根据行列式的斜对称性可知  $f$  也是斜对称的. 由第三章第一讲等式 (4) 可知,

$$f(\vec{B}^{(1)}, \dots, \vec{B}^{(n)}) = w \det(B),$$

其中  $w = f(\mathbf{e}_1, \dots, \mathbf{e}_n)$ . 故

$$w = \det(AE_n) = \det(A).$$

于是,  $\det(AB) = \det(A) \det(B)$ .  $\square$

**注解 3.11** 由上述定理可知,

$$\det(BA) = \det(B) \det(A) = \det(AB).$$

故  $\det(AB) = \det(BA)$ . 即行列式是关于方阵乘法的交换不变量.

**例 3.12** 展开

$$D = \begin{vmatrix} 1 & \cos(\theta_1) & \cos(2\theta_1) \\ 1 & \cos(\theta_2) & \cos(2\theta_2) \\ 1 & \cos(\theta_3) & \cos(2\theta_3) \end{vmatrix}.$$

解. 由行列式乘积定理, 我们有

$$D = \begin{vmatrix} 1 & \cos(\theta_1) & 2\cos(\theta_1)^2 - 1 \\ 1 & \cos(\theta_2) & 2\cos(\theta_2)^2 - 1 \\ 1 & \cos(\theta_3) & 2\cos(\theta_3)^2 - 1 \end{vmatrix} = \begin{vmatrix} 1 & \cos(\theta_1) & \cos(\theta_1)^2 \\ 1 & \cos(\theta_2) & \cos(\theta_2)^2 \\ 1 & \cos(\theta_3) & \cos(\theta_3)^2 \end{vmatrix} \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{vmatrix}.$$

故  $D = 2(\cos(\theta_3) - \cos(\theta_1))(\cos(\theta_3) - \cos(\theta_2))(\cos(\theta_2) - \cos(\theta_1))$ .

**例 3.13** 设  $A = ((\alpha_i + \beta_j)^{n-1})_{n \times n}$ . 展开  $\det(A)$ .

解. 注意到

$$\begin{aligned} (\alpha_i + \beta_j)^{n-1} &= \sum_{k=0}^{n-1} \binom{n-1}{k} \alpha_i^k \beta_j^{n-1-k} \\ &= \left( \binom{n-1}{0} \alpha_i^0, \binom{n-1}{1} \alpha_i, \dots, \binom{n-1}{n-1} \alpha_i^{n-1} \right) \begin{pmatrix} \beta_j^{n-1} \\ \beta_j^{n-2} \\ \vdots \\ \beta_j^0 \end{pmatrix}. \end{aligned}$$

故

$$A = \begin{pmatrix} \binom{n-1}{0} & \binom{n-1}{1}\alpha_1 & \cdots & \binom{n-1}{n-1}\alpha_1^{n-1} \\ \binom{n-1}{0} & \binom{n-1}{1}\alpha_2 & \cdots & \binom{n-1}{n-1}\alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{n-1}{0} & \binom{n-1}{1}\alpha_n & \cdots & \binom{n-1}{n-1}\alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} \beta_1^{(n-1)} & \beta_2^{n-1} & \cdots & \beta_n^{n-1} \\ \beta_1^{(n-2)} & \beta_2^{n-2} & \cdots & \beta_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

由行列式的基本性质和乘积定理可知,

$$\det(A) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1} \binom{n-1}{k} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)(\beta_j - \beta_i).$$

**例 3.14** 设  $A \in \mathbb{R}^{m \times n}$  和  $B \in \mathbb{R}^{n \times m}$ . 则我们有 *Sylvester* 行列式恒等式:

$$\det(E_m + AB) = \det(E_n + BA).$$

证明. 由第二章例 10.11 可知, 存在矩阵  $C_1, C_2, C_3, C_4 \in M_{m+n}(\mathbb{R})$  使得

$$C_3 C_1 \begin{pmatrix} E_m + AB & O \\ O & E_n \end{pmatrix} C_2 C_4 = \begin{pmatrix} E_n & O \\ O & E_n + BA \end{pmatrix}.$$

由关于分块行列式的定理可知,

$$\det(C_1) = \det(C_2) = \det(C_3) = \det(C_4) = 1.$$

再根据行列式乘积定理,

$$\det \begin{pmatrix} E_m + AB & O \\ O & E_n \end{pmatrix} = \det \begin{pmatrix} E_n & O \\ O & E_n + BA \end{pmatrix}.$$

故  $\det(E_m + AB) = \det(E_n + BA)$ .  $\square$

## 4 行列式的应用

### 4.1 矩阵的逆

设  $i, j \in \{1, 2, \dots, n\}$ . Kronecker 符号

$$\delta_{i,j} := \begin{cases} 0 & \text{如果 } i \neq j, \\ 1 & \text{如果 } i = j \end{cases}.$$

利用 Kronecker 符号, 单位矩阵可以表示为  $(\delta_{i,j})_{n \times n}$ .

**引理 4.1** 设  $A = (a_{i,j}) \in M_n(\mathbb{R})$ . 则

$$\sum_{k=1}^n a_{i,k} A_{j,k} = \delta_{i,j} |A| \quad \text{和} \quad \sum_{k=1}^n a_{k,j} A_{k,i} = \delta_{i,j} |A|,$$

其中  $A_{i,j}$  代表  $A$  关于第  $i$  行第  $j$  列的代数余子式,  $i, j \in \{1, 2, \dots, n\}$ .

**证明.** 当  $i = j$  时, 结论由第三章第一讲定理 3.3 直接得出. 设  $i \neq j$ . 令  $B$  是把  $A$  中第  $j$  行换成  $\vec{A}_i$  后得到的矩阵. 因为  $B$  中由两行相同, 所以  $\det(B) = 0$ . 把  $B$  按第  $j$  列展开, 再用第三章第一讲定理 3.3 得出

$$\sum_{k=1}^n a_{i,k} A_{j,k} = \det(B) = 0.$$

另一个等式可通过对列进行类似操作得出.  $\square$

**定义 4.2** 设  $A = (a_{i,j}) \in M_n(\mathbb{R})$ . 矩阵

$$\begin{pmatrix} A_{1,1} & A_{2,1} & \cdots & A_{n,1} \\ A_{1,2} & A_{2,2} & \cdots & A_{n,2} \\ \vdots & \vdots & \cdots & \vdots \\ A_{1,n} & A_{2,n} & \cdots & A_{n,n} \end{pmatrix}$$

称为  $A$  的伴随矩阵. 记为  $A^\vee$ .

**引理 4.3** 利用上述符号, 我们有

$$A^\vee A = AA^\vee = |A|E.$$

证明. 设  $A^\vee = (b_{i,j})_{n \times n}$ . 则  $A^\vee A$  中位于第  $i$  行第  $j$  列处的元素是

$$\sum_{k=1}^n b_{i,k} a_{k,j} = \sum_{k=1}^n A_{k,i} a_{k,j} = \delta_{i,j} |A| \quad (\because \text{引理 4.1}).$$

故  $A^\vee A = |A|E_n$ . 类似地,  $AA^\vee$  中位于第  $i$  行第  $j$  列处的元素是

$$\sum_{k=1}^n a_{i,k} b_{k,j} = \sum_{k=1}^n a_{i,k} A_{j,k} = \delta_{i,j} |A| \quad (\because \text{引理 4.1}).$$

故  $AA^\vee = |A|E_n$ .  $\square$ .

**定理 4.4** 设  $A \in M_n(\mathbb{R})$  可逆. 则

$$A^{-1} = \frac{1}{|A|} A^\vee.$$

证明. 根据引理 4.3, 我们有

$$\left(\frac{1}{|A|}A^\vee\right)A = \frac{1}{|A|}(A^\vee A) = \frac{1}{|A|}|A|E = E.$$

由第二章第五讲推论 7.16, 定理成立.  $\square$

**注解 4.5** 设  $A$  可逆. 则

$$A^{-1} = \begin{pmatrix} \frac{A_{1,1}}{|A|} & \frac{A_{2,1}}{|A|} & \cdots & \frac{A_{n,1}}{|A|} \\ \frac{A_{1,2}}{|A|} & \frac{A_{2,2}}{|A|} & \cdots & \frac{A_{n,2}}{|A|} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{A_{1,n}}{|A|} & \frac{A_{2,n}}{|A|} & \cdots & \frac{A_{n,n}}{|A|} \end{pmatrix}.$$

该公式说明当  $A$  中的元素都是整数时,  $A^{-1}$  中的元素都是以  $|A|$  为公分母有理数.

## 4.2 Cramer 法则

**定理 4.6** 设  $A \in M_n(\mathbb{R})$  和  $\mathbf{b} = (b_1, \dots, b_n)^t \in \mathbb{R}^n$ . 再设  $\mathbf{x} = (x_1, \dots, x_n)^t$  是未知数向量. 则方程组  $A\mathbf{x} = \mathbf{b}$  确定当且仅当  $A$  可逆. 此时, 该方程组的唯一解是

$$x_i = \frac{\det(\vec{A}^{(1)}, \dots, \vec{A}^{(i-1)}, \mathbf{b}, \vec{A}^{(i+1)}, \dots, \vec{A}^{(n)})}{\det(A)},$$

$$i = 1, 2, \dots, n.$$

证明. 定理中的必要充分条件是第二章第三讲推论 4.3 和第五讲的定理 7.14 的直接推论. 再设  $A$  可逆. 则  $\mathbf{x} = A^{-1}\mathbf{b}$ .

根据定理 4.4 和注释 4.5,

$$x_i = \frac{1}{|A|} (A_{1,i}, \dots, A_{n,i}) \mathbf{b}, \quad i = 1, 2, \dots, n,$$

其中  $A_{k,i}$  是矩阵  $A$  关于第  $k$  行和第  $i$  列的代数余子式. 而

$$(A_{1,i}, \dots, A_{n,i}) \mathbf{b} = \sum_{k=1}^n b_k A_{k,i}.$$

它是行列式  $\det(\vec{A}^{(1)}, \dots, \vec{A}^{(i-1)}, \mathbf{b}, \vec{A}^{(i+1)}, \dots, \vec{A}^{(n)})$  按第  $i$  列展开的表达式 (第三章第一讲定理 3.3).  $\square$

**注解 4.7** 利用上述定理中的符号, 令

$$A_i = \det(\vec{A}^{(1)}, \dots, \vec{A}^{(i-1)}, \mathbf{b}, \vec{A}^{(i+1)}, \dots, \vec{A}^{(n)}).$$

则当  $A$  可逆时, 方程组  $A\mathbf{x} = \mathbf{b}$  的唯一解是

$$x_1 = \frac{\det(A_1)}{\det(A)}, \quad \dots, \quad x_n = \frac{\det(A_n)}{\det(A)}.$$

该公式说明当  $A$  中的元素和  $\mathbf{b}$  中的坐标都是整数时, 方程组的解是以  $\det(A)$  为公分母的有理数.

### 4.3 子式和矩阵的秩

**定义 4.8** 设  $A = (a_{i,j}) \in \mathbb{R}^{m \times n}$ ,  $i_1, \dots, i_k \in \{1, \dots, m\}$  不必两两不同,  $j_1, \dots, j_k \in \{1, 2, \dots, n\}$  也不必两两不同. 则



行列式

$$\det \begin{pmatrix} a_{i_1, j_1} & a_{i_1, j_2} & \cdots & a_{i_1, j_k} \\ a_{i_2, j_1} & a_{i_2, j_2} & \cdots & a_{i_2, j_k} \\ \vdots & \vdots & \cdots & \vdots \\ a_{i_k, j_1} & a_{i_k, j_2} & \cdots & a_{i_k, j_k} \end{pmatrix}$$

称为  $A$  的一个  $k$  阶子式 (minor). 记为

$$M_A \begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ j_1 & j_2 & \cdots & j_k \end{pmatrix}.$$

例 4.9 设

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}.$$

则

$$M_A \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \det \begin{pmatrix} 1 & 2 \\ 5 & 6 \end{pmatrix}, \quad M_A \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \det \begin{pmatrix} 7 & 8 \\ 3 & 4 \end{pmatrix}.$$

显然, 如果  $i_1, \dots, i_k$  中有两个相同或  $j_1, \dots, j_k$  中有两个相同, 则对应的子式等于零.

**引理 4.10** 设  $A \in \mathbb{R}^{m \times n}$ . 则  $A$  中有  $k$  列线性无关当且仅当  $A$  中有  $k$  阶子式非零.

证明. 设  $\vec{A}^{(j_1)}, \dots, \vec{A}^{(j_k)}$  线性无关. 令

$$B = (\vec{A}^{(j_1)}, \dots, \vec{A}^{(j_k)}) \in \mathbb{R}^{m \times k}.$$

则  $\text{rank}(B) = k$ . 故可设行向量  $\vec{B}_{i_1}, \dots, \vec{B}_{i_k}$  线性无关. 于是, 上一讲定理 2.13 蕴含矩阵  $B$  的  $k$  阶子式

$$M_B \begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ 1 & 2 & \cdots & k \end{pmatrix} \neq 0.$$

即矩阵  $A$  的  $k$  阶子式

$$M_A \begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ j_1 & j_2 & \cdots & j_k \end{pmatrix} \neq 0.$$

反之, 设上述矩阵  $A$  的  $k$  阶子式非零. 则上述矩阵  $B$  中的行向量  $\vec{B}_{i_1}, \dots, \vec{B}_{i_k}$  线性无关 (上一讲定理 2.13). 于是,  $\text{rank}(B) = k$ . 故  $B$  中的列向量线性无关. 即  $\vec{A}_{j_1}, \dots, \vec{A}_{j_k}$  线性无关.  $\square$

**定理 4.11** 设  $A \in \mathbb{R}^{m \times n}$  非零. 则下列命题等价.

- (i)  $\text{rank}(A) = r$ ;
- (ii)  $A$  中所有大于  $r$  阶的子式都等于零且存在一个  $r$  阶子式非零;
- (iii)  $A$  中所有  $r+1$  阶的子式都等于零且存在一个  $r$  阶子式非零.

证明. (i)  $\implies$  (ii) 由引理 4.10 直接可得.

(ii)  $\implies$  (iii) 显然.

(iii)  $\implies$  (i) 假设  $\text{rank}(A) > r$ . 则  $A$  中存在  $r + 1$  列线性无关. 根据引理 4.10 可知,  $A$  有  $r + 1$  阶非零子式, 矛盾. 于是,  $\text{rank}(A) \leq r$ . 因为  $A$  中有  $r$  阶非零子式, 所以  $A$  中有  $r$  个线性无关的列向量. 由此可知,  $\text{rank}(A) \geq r$ . 故  $r = \text{rank}(A)$   $\square$

**例 4.12** 设  $A \in \mathbb{R}^{(n-1) \times n}$  和  $\mathbf{x} = (x_1, \dots, x_n)^t$  是未知数向量. 如果  $\text{rank}(A) = n - 1$ , 则

$$\text{sol}(A\mathbf{x} = \mathbf{0}) = \left\langle \begin{pmatrix} |A_1| \\ -|A_2| \\ \vdots \\ (-1)^{n-1}|A_n| \end{pmatrix} \right\rangle,$$

其中  $A_i$  是  $A$  去掉第  $i$  列得到的  $(n - 1)$  阶方阵.

证明. 设

$$B_i = \begin{pmatrix} \vec{A}_i \\ \vec{A}_1 \\ \vdots \\ \vec{A}_{n-1} \end{pmatrix} \in M_n(\mathbb{R}), \quad i = 1, 2, \dots, n - 1.$$

则  $\det(B_i) = 0$  (第三章第一讲行列式的性质 (S1)). 对  $B_i$  按第一行展开得

$$a_{i,1}|A_1| - a_{i,2}|A_2| + \cdots + (-1)^{(n-1)} a_{i,n}|A_n| = 0, \quad i = 1, 2, \dots, n - 1.$$

故  $(|A_1|, -|A_2|, \dots, (-1)^{n-1}|A_n|)^t$  是  $A\mathbf{x} = \mathbf{0}$  的一个解. 因为  $\text{rank}(A) = n - 1$ , 所以

$$\dim(\text{sol}(A\mathbf{x} = \mathbf{0})) = 1.$$

于是, 我们只要证明  $(|A_1|, -|A_2|, \dots, (-1)^{n-1}|A_n|)^t$  非零即可. 根据定理 4.11,  $|A_1|, \dots, |A_n|$  至少有一个非零.

**注解 4.13** 定理 4.11 给出了一种通过行列式计算矩阵秩的方法. 该方法虽然效率较低, 但不需要计算非零实数的逆. 这对于把秩推广到交换环上的矩阵有一定帮助.

## 4.4 坐标空间中的超平面

**定义 4.14** 坐标空间  $\mathbb{R}^n$  的  $n - 1$  维线性流形称为超平面 (*hyperplane*).

我们来利用行列式表示超平面方程.

**引理 4.15** 设  $U$  是  $\mathbb{R}^n$  中  $d$  维子空间, 其中  $0 \leq d < n$ . 则存在  $A \in \mathbb{R}^{(n-d) \times n}$  使得  $U = \text{sol}(A\mathbf{x} = \mathbf{0}_{n-d})$ .

证明. 设  $\mathbf{u}_1, \dots, \mathbf{u}_d$  是  $U$  的一组基. 由基扩充定理  $U$  有一组基  $\mathbf{u}_1, \dots, \mathbf{u}_d, \mathbf{u}_{d+1}, \dots, \mathbf{u}_n$ . 利用线性映射基本定理, 存在线性映射  $\phi: \mathbb{R}^n \rightarrow \mathbb{R}^n$  满足

$$\phi(\mathbf{u}_1) = \dots = \phi(\mathbf{u}_d) = \mathbf{0}_n \text{ 和 } \phi(\mathbf{u}_j) = \mathbf{u}_j, \quad j = d + 1, \dots, n.$$

对任意  $\mathbf{v} = \sum_{j=1}^n \alpha_j \mathbf{u}_j$ ,

$$\phi(\mathbf{v}) = \sum_{j=1}^n \alpha_j \phi(\mathbf{u}_j) = \sum_{j=d+1}^n \alpha_j \mathbf{u}_j \Rightarrow \text{im}(\phi) = \langle \mathbf{u}_{d+1}, \dots, \mathbf{u}_n \rangle.$$

故  $\dim(\text{im}(\phi)) = n - d$ . 根据对偶定理,  $\dim(\ker(\phi)) = d$ , 因为  $U \subset \ker(\phi)$ , 所以  $U = \ker(\phi)$ .

设  $M \in M_n(\mathbb{R})$  是  $\phi$  在标准基下的矩阵. 则

$$U = \text{sol}(M\mathbf{x} = \mathbf{0}).$$

由对偶定理可知,  $\text{rank}(M) = n - d$ . 则

$$M \xrightarrow{\text{初等行变换}} \begin{pmatrix} A_{(n-d) \times n} \\ O_{d \times n} \end{pmatrix},$$

$\text{rank}(A) = n - d$  且  $U = \text{sol}(A\mathbf{x} = \mathbf{0}_{n-d})$ .  $\square$

设子空间  $U$  的维数是  $n - 1$ . 则存在  $a_1, \dots, a_n \in \mathbb{R}$ , 不全为零, 使得

$$U = \text{sol}(a_1 x_1 + \dots + a_n x_n = 0).$$

设该子空间的一组基是  $\mathbf{u}_1, \dots, \mathbf{u}_{n-1}$ . 令

$$A = \begin{pmatrix} \mathbf{u}_1^t \\ \vdots \\ \mathbf{u}_{n-1}^t \end{pmatrix}_{(n-1) \times (n)} \quad \text{和} \quad \vec{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \quad (2)$$

则  $A\vec{a} = \mathbf{0}$ . 因为  $\text{rank}(A) = n - 1$ , 所以

$$\vec{a} = \lambda(|A_1|, -|A_2|, \dots, (-1)^{n-1}|A_n|)^t,$$

其中  $\lambda$  是非零实数,  $|A_1|, \dots, |A_n|$  由例 4.12 给出. 取  $\lambda = 1$ .

则  $U$  是齐次线性方程

$$\sum_{i=1}^n (-1)^{i-1} |A_i| x_i = 0$$

的解空间. 设超平面  $P = \mathbf{v} + U$ . 令  $\mathbf{v} = (v_1, \dots, v_n)^t$ . 则  $P$  是方程

$$\sum_{i=1}^n (-1)^{i-1} |A_i| x_i = \sum_{i=1}^n (-1)^{i-1} |A_i| v_i.$$

的解流形.

## 第四章 群、环和域简介

### 1 二元运算

#### 1.1 定义与基本性质

**定义 1.1** 设  $S$  是集合. 映射  $f : S \times S \longrightarrow S$  称为一个  $S$  上的二元运算. 对于任意  $x, y \in S$ ,  $f(x, y)$  也记为  $xy$ .

#### 例 1.2

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\mapsto x + y \end{aligned}$$

加法满足交换律、结合律, 有加法单位元  $0$  和加法逆元.

#### 例 1.3

$$\begin{aligned} - : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\mapsto x - y \end{aligned}$$

减法不满足交换律和结合律.

**例 1.4** 设  $S = \mathbb{Z} \cup \{+\infty\}$ .

$$\begin{aligned} \dot{+} : S \times S &\longrightarrow S \\ (x, y) &\mapsto \min(x, y) \end{aligned}$$

称之为“热带”加法. 热带加法显然满足交换和结合律. 对于任意  $x \in S$ ,

$$x \dot{+} (+\infty) = x.$$

但  $x$  一般没有逆元.

**定义 1.5** 设  $*$  是  $S$  上的二元运算. 如果对于任意  $x, y, z \in S$ ,

$$x * (y * z) = (x * y) * z,$$

则称  $*$  满足结合律.

**定理 1.6** 设  $*$  集合  $S$  上的二元运算且满足结合律,  $n \geq 3$ ,  $x_1, x_2, \dots, x_n \in S$ . 设  $k, \ell \in \{1, 2, \dots, n-1\}$ . 则

$$(x_1 * \dots * x_k) * (x_{k+1} * \dots * x_n) = (x_1 * \dots * x_\ell) * (x_{\ell+1} * \dots * x_n).$$

证明. 不妨设  $k > \ell$ . 我们对  $n$  归纳. 设  $n = 3$ . 则  $k = 2$  和  $\ell = 1$ . 由结合律可知, 结论成立.

设  $n > 3$  且结论对于小于  $n$  的值成立. 考虑  $n$  时,

$$\begin{aligned} & (x_1 * \dots * x_k) * (x_{k+1} * \dots * x_n) \\ &= (x_1 * \dots * x_\ell * x_{\ell+1} * \dots * x_k) * (x_{k+1} * \dots * x_n) \quad (\ell < k) \\ &= ((x_1 * \dots * x_\ell) * (x_{\ell+1} * \dots * x_k)) * (x_{k+1} * \dots * x_n) \quad (\text{归纳假设}) \\ &= (x_1 * \dots * x_\ell) * ((x_{\ell+1} * \dots * x_k) * (x_{k+1} * \dots * x_n)) \quad (\text{结合律}) \\ &= (x_1 * \dots * x_\ell) * ((x_{\ell+1} * \dots * x_k * x_{k+1} * \dots * x_n)). \quad \square \end{aligned}$$

记号. 设  $x \in S, n \in \mathbb{Z}^+$ . 则

$$x^n = \underbrace{x * \dots * x}_n.$$



当  $S$  上的二元运算以“+”来记时, 我们定义

$$nx = \underbrace{x + \cdots + x}_n.$$

## 1.2 同余运算

设  $n$  是大于 1 的正整数. 在第一章第三讲我们定义了同余关系  $\equiv_n$  (定义 5.8). 设  $\mathbb{Z}_n = \mathbb{Z} / \equiv_n$ . 则

$$\mathbb{Z}_n = \{\bar{a} \mid a \in \mathbb{Z}\}.$$

对于  $\bar{a}, \bar{b} \in \mathbb{Z}_n$ ,  $\bar{a} = \bar{b}$  当且仅当  $a \equiv_n b$ , 即  $n \mid (a - b)$ .

**定义 1.7** 定义  $\mathbb{Z}_n$  上的加法:

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\mapsto \overline{a + b}. \end{aligned}$$

验证良定义如下, 设  $a, b, x, y \in \mathbb{Z}$  使得  $\bar{a} = \bar{x}$  和  $\bar{b} = \bar{y}$ . 则存在  $k, \ell \in \mathbb{Z}$  使得  $a = x + kn$  和  $b = y + \ell n$ . 于是

$$a + b = (x + y) + (k + \ell)n.$$

故

$$\overline{a + b} = \overline{x + y}.$$

由此得出

$$\bar{a} + \bar{b} = \bar{x} + \bar{y}.$$

我们验证了  $+$  是良定义的.

例 1.8 在  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$  中, 我们有

$$\bar{1} + \bar{1} = \overline{1+1} = \bar{2} = \bar{0}.$$

定义 1.9 定义  $\mathbb{Z}_n$  上的乘法:

$$\begin{aligned} \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\longmapsto \overline{ab}. \end{aligned}$$

验证良定义如下, 设  $a, b, x, y \in \mathbb{Z}$  使得  $\bar{a} = \bar{x}$  和  $\bar{b} = \bar{y}$ . 则存在  $k, \ell \in \mathbb{Z}$  使得  $a = x + kn$  和  $b = y + \ell n$ . 于是

$$ab = xy + (ky + \ell x + k\ell n)n.$$

故

$$\overline{ab} = \overline{xy}.$$

由此得出

$$\bar{a}\bar{b} = \bar{x}\bar{y}.$$

我们验证了  $\cdot$  是良定义的.

例 1.10 在  $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$  中, 我们有

$$\bar{2}\bar{4} = \overline{2 \cdot 4} = \bar{8} = \bar{2} \quad \text{和} \quad \bar{2}\bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{0}.$$

### 1.3 单位元和逆元

定义 1.11 设  $*$  是集合上的二元运算. 如果存在  $e \in S$  使得对于任意的  $x \in S$ ,  $x * e = e * x = x$ . 则称  $e$  是关于  $*$  的单位元.

整数关于加法的单位元是 0, 在  $\mathbb{Z}_n$  中关于加法的单位元是  $\bar{0}$ , 在  $\mathbb{R}^{m \times n}$  中关于加法的单位元是  $O_{m \times n}$ . 整数关于乘法的单位元是 1, 在  $\mathbb{Z}_n$  中关于乘法的单位元是  $\bar{1}$ , 在  $M_n(\mathbb{R})$  中关于乘法的单位元是  $E_n$ .

**命题 1.12** 设  $*$  是集合上的二元运算. 设  $e, e' \in S$  是单位元. 则  $e = e'$ .

证明. 注意到  $ee' = e = e'$ .  $\square$

**定义 1.13** 设  $*$  是集合上的二元运算,  $S$  中有关于  $*$  的单位元  $e$ . 设  $x \in S$ . 如果存在  $y \in S$  使得  $y * x = x * y = e$ . 则称  $y$  是  $x$  的逆元,  $x$  是可逆元.

整数,  $\mathbb{Z}_n$ ,  $\mathbb{R}^{m \times n}$  中每个元素关于加法都是可逆的. 整数关于乘法的可逆元是  $\pm 1$ , 在  $M_n(\mathbb{R})$  中关于乘法的可逆元是可逆矩阵.

**例 1.14** 设  $X$  是非空集合, 定义  $X^X$  是从  $X$  到它自身的所有映射的集合. 则复合  $\circ$  是  $X^X$  上的运算. 它的单位是恒同映射. 可逆元是双射.

**命题 1.15** 设  $*$  是  $S$  上有结合律的运算且有单位元  $e$ . 设  $a, b, x \in S$  满足  $ax = e$  和  $xb = e$ . 则  $a = b$ . 特别地,  $x$  可逆且它的逆唯一.

证明. 我们计算

$$ax = e \Rightarrow (ax)b = eb \Rightarrow a(xb) = b \Rightarrow ae = b \Rightarrow a = b. \quad \square$$

**命题 1.16** 设  $\bar{a} \in \mathbb{Z}_n$ . 则  $\bar{a}$  关于乘法可逆当且仅当  $a$  和  $n$  互素.

证明. 设存在  $\bar{b} \in \mathbb{Z}_n$  使得  $\bar{a}\bar{b} = \bar{1}$ . 则

$$ab \equiv_n 1.$$

故存在  $k \in \mathbb{Z}$  使得  $ab - 1 = kn$  即  $ab + kn = 1$ . 由第一章第四讲定理 7.8,  $a, n$  互素.

反之, 设  $a, n$  互素. 同样的定理蕴含存在  $u, v \in \mathbb{Z}$  使得  $ua + vn = 1$ . 故  $\bar{u}\bar{a} = \bar{1}$ . 进而  $\bar{u}\bar{a} = \bar{a}\bar{u} = \bar{1}$ .  $\square$ .

**例 1.17** 计算  $\mathbb{Z}_{15}$  中的所有关于乘法的可逆元.

解. 由上述命题可知, 可逆元是  $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}$ . 它们的逆分别是  $\bar{1}, \bar{8}, \bar{4}, \bar{13}, \bar{2}, \bar{11}, \bar{7}, \bar{14}$ .