

第一章 预备知识

2.5 二阶行列式

行列式 (determinant) 在一定条件下可以通过线性方程组的系数表示该方程组解. 我们在这里讨论二阶行列式的情形. 设实系数二阶方阵

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

它的行列式定义为 $ad - bc$, 记为 $\det(A)$ 或 $|A|$.

命题 2.1 关于未知数 x, y 的实系数线性方程组

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases}$$

是确定的当且仅当其系数矩阵的行列式非零. 此时方程组的解等于

$$x = \frac{\begin{vmatrix} e & b \\ f & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, \quad y = \frac{\begin{vmatrix} a & e \\ c & f \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}.$$

证明. 设方程组是确定的. 则 a, c 不全为零. 不妨设 $a \neq 0$.
由高斯消去法得

$$\begin{pmatrix} a & b & e \\ c & d & f \end{pmatrix} \longrightarrow \begin{pmatrix} a & b & e \\ 0 & d - a^{-1}cb & f - a^{-1}ce \end{pmatrix}.$$

由第一讲定理 2.5 (ii) 可知, $d - a^{-1}cb \neq 0$. 于是, $ad - cb \neq 0$.

反之, 设 $ad - cb \neq 0$. 则 a, c 不全为零. 不妨设 $a \neq 0$.
于是, 上述的消元过程和结果不变, 且 $d - a^{-1}cb \neq 0$. 由第一讲定理 2.5 (ii) 可知, 原方程组是确定的. 此时

$$y = \frac{f - a^{-1}ce}{d - a^{-1}cb} = \frac{\begin{vmatrix} a & e \\ c & f \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}.$$

代入第一个方程得

$$x = \frac{\begin{vmatrix} e & b \\ f & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}. \quad \square$$

3 线性方程组的解集

关于集合的基本语言见 <http://www.mmrc.iss.ac.cn/~zml/LinearAlgebra-2022-2023/LectureNotes/LA1-2.pdf> 第3节.

设 S_1, \dots, S_k 是非空集合. 它们的笛卡尔积 (*Cartisian Product*) 是指集合

$$\{(x_1, \dots, x_k) \mid x_1 \in S_1, \dots, x_k \in S_k\}.$$

记为 $S_1 \times \dots \times S_k$. 当 S_1, \dots, S_k 都等于集合 S 时. 集合 $\underbrace{S \times \dots \times S}_k$ 简记为 S^k . 例如二维实平面可简记为 \mathbb{R}^2 .

如果集合中含有有限多个元素, 则该集合称为有限集. 否则称之为无限集. 对有限集 S , 它中元素的个数记为 $|S|$ 或 $\text{card}(S)$, 其中 card 是 *cardinality* 的缩写. 特别地, $\text{card}(\emptyset) = 0$. 对于无限集, $\text{card}(S) = \infty$.

最后, 我们用集合论的语言来刻画线性方程组的解. 设 L 是关于未知数 x_1, \dots, x_n 的线性方程组. 令

$$\text{sol}(L) = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mid \alpha_1, \dots, \alpha_n \in \mathbb{R} \text{ 使得 } x_1 = \alpha_1, \dots, x_n = \alpha_n \text{ 是 } L \text{ 的解} \right\}.$$

称之为 L 的解的集合. 则 L 相容当且仅当 $\text{sol}(L) \neq \emptyset$; L 确定当且仅当 $\text{card}(\text{sol}(L)) = 1$.

命题 3.1 设齐次线性方程组是 H 的系数矩阵是 A , 设 L 是以 $(A|\mathbf{b})$ 为增广矩阵的线性方程组. 设

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

是 (L) 的一个解. 则

$$\text{sol}(L) = \left\{ \begin{pmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{pmatrix} \mid \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \in \text{sol}(H) \right\}.$$

证明. 令 $A = (a_{i,j})_{m \times n}$,

$$\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad \text{和} \quad S = \left\{ \begin{pmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{pmatrix} \mid \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \in \text{sol}(H) \right\}.$$

设

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in S.$$

则存在

$$\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} \in \text{sol}(H) \quad \text{使得} \quad \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \alpha_1 + \mu_1 \\ \vdots \\ \alpha_n + \mu_n \end{pmatrix}$$

对任意 $i \in \{1, \dots, m\}$,

$$\sum_{j=1}^n a_{i,j} \lambda_j = \sum_{j=1}^n a_{i,j} (\alpha_j + \mu_j) = \sum_{j=1}^n a_{i,j} \alpha_j + \sum_{j=1}^n a_{i,j} \mu_j = b_i + 0 = b_i.$$

故

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \text{sol}(L).$$

我们有 $S \subset \text{sol}(L)$.

反之, 设

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \text{sol}(L).$$

则

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \alpha_1 + (\lambda_1 - \alpha_1) \\ \vdots \\ \alpha_n + (\lambda_n - \alpha_n) \end{pmatrix}.$$

对 $i \in \{1, \dots, m\}$,

$$\sum_{j=1}^n a_{i,j} (\lambda_j - \alpha_j) = \sum_{j=1}^n a_{i,j} \lambda_j - \sum_{j=1}^n a_{i,j} \alpha_j = b_i - b_i = 0.$$

故

$$\begin{pmatrix} \lambda_1 - \alpha_1 \\ \vdots \\ \lambda_n - \alpha_n \end{pmatrix} \in \text{sol}(H).$$

我们有 $\text{sol}(L) \subset S$.

综上所述, $\text{sol}(L) = S$. \square

4 映射

4.1 定义、例子和类型

定义 4.1 设 S 和 T 是两个非空集合, $f \subset S \times T$. 如果对任意的 $x \in S$, 存在唯一 $y \in T$ 使得 $(x, y) \in f$. 则称 f 是从 S 到 T 的映射 (map).

通常我们把从 S 到 T 的映射 f 记为:

$$\begin{aligned} f : S &\longrightarrow T \\ x &\mapsto y, \end{aligned}$$

其中, $(x, y) \in f$. 因为 y 唯一, 所以我们把 y 记为 $f(x)$. 该映射也简记为 $f : S \longrightarrow T$.

例 4.2 从国科大在读学生的学号到对应学生的姓名是一个映射. 但从学生姓名到他们对应的学号就不一定是映射, 这是因为有重名的可能.

以下映射在今后经常会经常用到.

例 4.3 映射

$$\begin{aligned} f : S &\longrightarrow S \\ x &\mapsto x. \end{aligned}$$

称为集合 S 上的恒同映射, 通常记为 id_S , 其中 id 是 *identity* 的缩写.

设 S' 是集合 S 的非空子集, $f : S \rightarrow T$ 是映射. 则

$$\begin{aligned} g : S' &\longrightarrow T \\ x &\mapsto f(x) \end{aligned}$$

是从 S' 到 T 的映射. 称之为 f 在子集 S' 上的限制, 并记为 $f|_{S'}$. 反之, 考虑映射 $h : S' \rightarrow T$. 如果 $f|_{S'} = h$, 则称 f 是 h 的扩展. 显然 f 是 $f|_{S'}$ 的扩展. 但它的扩展可能不止一个.

例 4.4 设 S' 是 S 的非空子集. 定义

$$\begin{aligned} i_{S'} : S' &\longrightarrow S \\ x &\mapsto x \end{aligned}$$

称为 S' 到 S 的嵌入.

例 4.5 映射

$$\begin{aligned} p_1 : S \times T &\longrightarrow S \\ (x, y) &\mapsto x \end{aligned}$$

称为从 $S \times T$ 到 S 的投影 (*projection*). 类似地, 我们可以定义从 $S \times T$ 到 T 的投影.

定义 4.6 考虑映射 $f : S \rightarrow T$.

(i) 如果对任意 $x_1, x_2 \in S$ 且 $x_1 \neq x_2$, 我们都有

$$f(x_1) \neq f(x_2).$$

则称 f 是单射 (injection).

(ii) 如果对任意 $y \in T$, 存在 $x \in S$ 使得 $y = f(x)$, 则称 f 是满射 (surjection).

(iii) 如果 f 既是单射又是满射, 则称 f 是双射 (bijection).

例 4.7 恒同映射是双射.

考虑映射

$$\begin{aligned} f: \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2. \end{aligned}$$

它既不是单射也不是满射. 设 $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. 则 $f|_{\mathbb{R}^+}$ 是单射.

嵌入 $i'_S: S' \longrightarrow S$ 是单射, 投影 $p_S: S \times T \longrightarrow S$ 是满射. 函数 $\cos: \mathbb{R} \longrightarrow \mathbb{R}$ 不是单射. 但 $\cos|_{[0, \pi]}$ 是单射.

4.2 像集和原像集

设 $f: S \longrightarrow T$ 是映射, 且 $S' \subset S$. 集合

$$f(S') = \{f(x) \mid x \in S'\}$$

称为 S' 在 f 下的像集. 特别地, $f(S)$ 称为 f 的像集, 记为 $\text{im}(f)$, 这里 im 是 image 的缩写. 映射 f 是满射当且仅当 $f(S) = T$.

设 $T' \subset T$. 集合

$$f^{-1}(T') = \{x \in S \mid f(x) \in T'\}$$

称为 T' 在 f 下的原像集(逆像集). 由映射的定义可知 $f^{-1}(T) = S$.

设 $t \in T$. 我们称 $f^{-1}(\{t\})$ 是 t 关于 f 的纤维(*fibre*). 我们可以利用纤维来描述单射、满射和双射. 映射 f 是单射当且仅当关于 f 的每个纤维至多含有一个元素, f 是满射当且仅当它的每个纤维非空, f 是双射当且仅当它的每个纤维恰好含有一个元素.

例 4.8 设 $f: \mathbb{R} \rightarrow \mathbb{R}$ 由公式 $f(x) = \sin(x)$ 给出. 则

$$\text{im}(f) = [-1, 1], \quad f((0, \pi)) = (0, 1], \quad f^{-1}(\{0\}) = \{k\pi \mid k \in \mathbb{Z}\}.$$

4.3 映射的复合

设 $f: S \rightarrow T$ 和 $g: T \rightarrow U$ 是两个映射. 则我们可以定义一个新的映射

$$\begin{aligned} \phi: S &\longrightarrow U \\ x &\longmapsto g(f(x)). \end{aligned}$$

我们称该映射为 f 和 g 的复合 (*composition*), 记为 $g \circ f$. 复合可以通过下列图表形象地表示:

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ & \searrow^{g \circ f} & \downarrow g \\ & & U. \end{array}$$

命题 4.9 设 $f : S \rightarrow T$ 和 $g : T \rightarrow U$ 是两个映射.

- (i) 如果 f 和 g 都是单射, 则 $g \circ f$ 也是单射;
- (ii) 如果 f 和 g 都是满射, 则 $g \circ f$ 也是满射;
- (iii) 如果 f 和 g 都是双射, 则 $g \circ f$ 也是双射.

证明. (i) 设 $x, y \in S$ 且 $x \neq y$. 因为 f 是单射, 所以 $f(x) \neq f(y)$. 又因为 g 是单射, 所以 $g(f(x)) \neq g(f(y))$. 于是, $g \circ f$ 是单射.

(ii) 设 $z \in U$. 因为 g 是满射, 所以存在 $y \in T$ 使得 $g(y) = z$. 又因为 f 是满射, 所以存在 $x \in S$ 使得 $y = f(x)$. 于是, $g \circ f(x) = g(f(x)) = g(y) = z$. 故 $g \circ f$ 是满射.

(iii) 是 (i) 和 (ii) 的简单推论. \square

设 $f : S \rightarrow T$ 和 $g : T \rightarrow S$ 是两个映射. 则 $g \circ f : S \rightarrow S$ 和 $f \circ g : T \rightarrow T$ 是两个有意义的映射. 当 $S \neq T$ 时, 这两个映射不同. 事实上, 当 $S = T$ 时, 交换律 $g \circ f = f \circ g$ 也不成立.

例 4.10 设

$$\begin{array}{ccc} f: \mathbb{R} \longrightarrow \mathbb{R} & \text{和} & g: \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto x^2 & & x \mapsto x + 1. \end{array}$$

则对任意的 $x \in \mathbb{R}$, $g \circ f(x) = g(x^2) = x^2 + 1$. 而

$$f \circ \text{id}_S(x) = f(\text{id}_S(x)) = f(x).$$

故 $f \circ \text{id}_S = f$. 类似地,

$$\text{id}_T \circ f(x) = \text{id}_T(f(x)) = f(x).$$

故 $\text{id}_T \circ f = f$. \square

下面我们证明映射的复合满足结合律.

定理 4.11 设 $f: S \rightarrow T$, $g: T \rightarrow U$ 和 $h: U \rightarrow V$. 则

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

证明. 对任意 $x \in S$,

$$h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x)))$$

且

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

于是, $h \circ (g \circ f) = (h \circ g) \circ f$. \square

映射的结合律可以通过下列交换图形象地表示.

$$\begin{array}{ccccc}
 S & \xrightarrow{f} & T & & \\
 & \searrow^{g \circ f} & \downarrow g & \searrow^{h \circ g} & \\
 & & U & \xrightarrow{h} & V.
 \end{array}$$

即通过红色箭头和蓝色箭头把 S 中一个元素映到 V 中同一个元素. 进而, 我们可以把三个函数 f, g, h 的复合写成 $h \circ g \circ f$. 这一简略的写法也适合多个函数的复合. 例如对映射 $\phi : S \rightarrow S$ 和 $k \in \mathbb{Z}^+$,

$$\phi^k := \underbrace{\phi \circ \cdots \circ \phi}_k.$$

此外, $\phi^0 := \text{id}_S$.

4.4 映射的逆

定义 4.12 设 $f : S \rightarrow T$ 是映射. 如果存在映射 $g : T \rightarrow S$ 使得 $g \circ f = \text{id}_S$ 且 $f \circ g = \text{id}_T$, 则称 f 是可逆映射, g 称为 f 的一个逆映射.

命题 4.13 映射 $f : S \rightarrow T$ 可逆当且仅当 f 是双射.

证明. 设 f 可逆且 g 是 f 的一个逆映射. 对任意 $x, y \in S$ 且 $x \neq y$. 我们有

$$g(f(x)) = (g \circ f)(x) = \text{id}_S(x) = x.$$

同理 $g(f(y)) = y$. 因为 $x \neq y$, 所以 $f(x) \neq f(y)$. 故 f 是单射. 再设 $z \in T$. 令 $x = g(z)$. 则

$$f(x) = f(g(z)) = (f \circ g)(z) = \text{id}_T(z) = z.$$

于是, f 是满射. 综上所述, f 是双射.

反之, 设 f 是双射. 则对于任意 $t \in T$ 存在唯一的 $s_t \in S$ 使得 $f(s_t) = t$. 定义

$$\begin{aligned} g: T &\longrightarrow S \\ t &\longmapsto s_t. \end{aligned}$$

则对任意 $t \in T$, $f \circ g(t) = f(g(t)) = f(s_t) = t$. 故 $f \circ g = \text{id}_T$. 对任意 $x \in S$, 令 $t = f(x)$. 则 $x = s_t$. 我们计算:

$$g \circ f(x) = g(t) = s_t = x.$$

故 $g \circ f = \text{id}_S$. \square

命题 4.14 设映射 $f: S \longrightarrow T$ 可逆, 则它的逆映射唯一.

证明. 设 g, h 是 f 的两个逆映射. 则 $g \circ f = \text{id}_S$. 于是, $(g \circ f) \circ h = \text{id}_S \circ h = h$. 根据映射的结合律,

$$h = g \circ (f \circ h) = g \circ \text{id}_T = g. \quad \square$$

设映射 $f: S \longrightarrow T$ 可逆. 则它的逆记为 f^{-1} .

命题 4.15 (i) 设映射 $f : S \rightarrow T$ 可逆. 则 $f^{-1} : T \rightarrow S$ 也可逆且

$$(f^{-1})^{-1} = f.$$

(ii) (穿衣脱衣规则) 设映射 $f : S \rightarrow T$, $g : T \rightarrow U$ 都可逆. 则 $g \circ f$ 也可逆且

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

证明. (i) 因为 $f \circ f^{-1} = \text{id}_T$ 且 $f^{-1} \circ f = \text{id}_S$, 所以 f^{-1} 可逆且其逆等于 f .

(ii) 由 (i) 可知 $f^{-1} : T \rightarrow S$ 和 $g^{-1} : U \rightarrow T$ 存在. 令 $h = f^{-1} \circ g^{-1}$. 它是从 U 到 S 的映射. 根据结合律, 我们有

$$\begin{aligned} h \circ (g \circ f) &= (f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ \text{id}_T \circ f = f^{-1} \circ (\text{id}_T \circ f) = f^{-1} \circ f = \text{id}_S. \end{aligned}$$

类似地,

$$\begin{aligned} (g \circ f) \circ h &= (g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ \text{id}_T \circ g^{-1} = g \circ (\text{id}_T \circ g^{-1}) = g \circ g^{-1} = \text{id}_U. \end{aligned}$$

结论成立. \square

例 4.16 设 $f : \mathbb{R} \rightarrow \mathbb{R}$ 由公式 $f(x) = \sin(x)$ 给出. 则

$$\begin{aligned} g : [-\frac{\pi}{2}, \frac{\pi}{2}] &\longrightarrow [-1, 1] \\ x &\longmapsto f(x). \end{aligned}$$

则 g 是双射. 其逆映射是 $\arcsin(x)$.

4.5 集合的势

设 S 和 T 是两个非空集合. 如果存在双射 $f : S \rightarrow T$, 则称 S 和 T 是等势的, 记为 $\text{card}(S) = \text{card}(T)$. 此外, 空集的势定义为零. 显然, 如果 S 是有限集, 则 T 和 S 等势当且仅当它们的元素个数相同. 与 \mathbb{Z}^+ 等势的集合称为可数集. 集合论中有以下结论.

- (i) 可数集的无限子集一定是可数的.
- (ii) 有理数集 \mathbb{Q} 是可数的.
- (iii) 实数集 \mathbb{R} 是不可数的.
- (iv) 设 S 是集合, $\mathcal{P}(S)$ 是所有 S 的子集构成的集合. 则 S 与 $\mathcal{P}(S)$ 不等势.

我们学习的线性代数只涉及到有限集和无限集, 不涉及到无限集的势.

5 等价关系和序关系

5.1 二元关系

定义 5.1 设 S 是一个非空集合, R 是 $S \times S$ 的子集. 我们称 R 称为 S 上的一个二元关系. 如果 $(a, b) \in R$, 则称 a 和 b 有关系 R , 并记为 aRb .

例 5.2 设 $R = \{(x, x) \mid x \in S\}$. 则对任意 $a, b \in S$, aRb 当且仅当 $a = b$. 换言之, R 是 S 中的等于关系.

例 5.3 设 L 是 \mathbb{R}^2 中所有直线的集合. 设

$$C = \{(l_1, l_2) \in L^2 \mid l_1, l_2 \text{ 有公共点}\}.$$

二元关系 C 代表两直线相交或重合. 设 $P = L^2 \setminus C$. 则 l_1Pl_2 代表 l_1 与 l_2 平行但不重合.

例 5.4 设 $R = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$. 则 R 就是实数集上的 \leq 关系.

5.2 等价关系

定义 5.5 设 S 是非空集合, \sim 是 S 上的二元关系. 如果

(i) 对任意 $x \in S$, $x \sim x$ (自反性),

(ii) 设 $x, y \in S$ 且 $x \sim y$, 则 $y \sim x$ (对称性),

(iii) 设 $x, y, z \in S$, $x \sim y$ 且 $y \sim z$, 则 $x \sim z$ (传递性), 则称 \sim 是等价关系.

例 5.6 例 5.2 中的等于是等价关系. 设 T 是 \mathbb{R}^2 中所有三角形的集合. 则三角形全等和相似都是等价关系.

例 5.3 中的关系 C 不满足传递性, 关系 P 不满足自反性, 例 5.4 中的关系 \leq 不满足对称性. 故它们都不是等价关系.

例 5.7 设 S 是中关村中学所有学生的集合, \sim_c 是该集合上同班同学关系. 该关系是等价关系.

设 $x \in \mathbb{Z}$ 和 $m \in \mathbb{Z}^+$. 则存在唯一整数 $q, r \in \{0, 1, \dots, m-1\}$ 使得

$$x = qm + r.$$

我们来验证唯一性. 再设 $x = um + v$, 其中 $u \in \mathbb{Z}$ 和 $v \in \{0, 1, \dots, m-1\}$. 不妨设 $v \geq r$. 则 $(q-u)m = v-r$. 因为 $m > v-r$, 所以 $v=r$. 由此得出 $q=u$. 我们称 r 是 x 关于 m 的余数, q 是 x 关于 m 的商. 它们分别记为 $\text{rem}(x, m)$ 和 $\text{quo}(x, m)$.

如果存在 $k \in \mathbb{Z}$ 使得 $x = km$, 则称 m 整除 x . 记为 $m \mid x$.

定义 5.8 设 $m \in \mathbb{Z}^+$. 设 $x, y \in \mathbb{Z}$. 我们称 x 和 y 关于 m 同余, 如果 $m \mid (x-y)$. 记为 $x \equiv_m y$ 或 $x \equiv y \pmod{m}$.

下面我们来验证 \equiv_m 是等价关系.

- (自反性) 对任意 $x \in \mathbb{Z}$, $m|(x-x)$, 于是, $x \equiv_m x$.
- (对称性) 设 $x, y \in \mathbb{Z}$ 且 $x \equiv_m y$. 则存在 $a \in \mathbb{Z}$ 使得 $(x-y) = am$. 则 $y-x = (-a)m$. 故 $m|(y-x)$. 我们得到 $y \equiv_m x$.
- (传递性) 设 $x, y, z \in \mathbb{Z}$ 满足 $x \equiv_m y$ 和 $y \equiv_m z$. 则存在 $a, b \in \mathbb{Z}$ 使得 $x-y = am$ 和 $y-z = bm$. 于是, $x-z = (a+b)m$. 故 $x \equiv_m z$.

验证完毕.

命题 5.9 设 $a, b \in \mathbb{Z}$ 且 n 是大于 1 的正整数. 则

$$a \equiv_n b \iff \text{rem}(a, n) = \text{rem}(b, n).$$

证明. 设 $a \equiv_n b$. 则存在 $m \in \mathbb{Z}$ 使得 $a-b = mn$. 由此可知 $a = b + mn$. 设 $b = qn + r$, 其中 $q = \text{quo}(b, n)$ 和 $r = \text{rem}(b, n)$. 则 $a = (q+m)n+r$. 因为 $r \in \{0, 1, \dots, n-1\}$, 所以余数的唯一性蕴含 $r = \text{rem}(a, n)$. 故

$$\text{rem}(a, n) = \text{rem}(b, n).$$

反之, 设 $\text{rem}(a, n) = \text{rem}(b, n)$. 则由除法公式可得

$$a-b = (\text{quo}(a, n) - \text{quo}(b, n))n.$$

故 $n|(a-b)$, 即 $a \equiv_n b$. \square

5.3 等价类和商集

设 \sim 是 S 上的等价关系, $x \in S$. 则关于 x 的等价类是

$$\bar{x} = \{y \in S | x \sim y\}.$$

此外, \bar{x} 中的任何一个元素都是该等价类的一个代表元.

注解 5.10 设 \sim 是 S 上的等价关系, $x \in S$. 根据自反性, $x \in \bar{x}$.

命题 5.11 设 \sim 是集合 S 上的等价关系, $x, y \in S$.

$$(i) \quad x \sim y \iff \bar{x} = \bar{y}.$$

$$(ii) \quad x \not\sim y \iff \bar{x} \cap \bar{y} = \emptyset.$$

证明. (i) 设 $x \sim y$ 且 $a \in \bar{x}$. 则 $x \sim a$. 根据对称性, $y \sim x$. 再由传递性, $y \sim a$. 于是, $a \in \bar{y}$. 我们得到 $\bar{x} \subset \bar{y}$. 同理 $\bar{y} \subset \bar{x}$. 故 $\bar{x} = \bar{y}$. 反之, 设 $\bar{x} = \bar{y}$. 根据注释 5.10, $x \in \bar{x}$ 和 $y \in \bar{y}$. 故 $y \in \bar{x}$. 由此得出, $x \sim y$.

(ii) 由 (i) 可知, $\bar{x} \cap \bar{y} = \emptyset \implies x \not\sim y$. 反之, 设 $x \not\sim y$. 若 $z \in \bar{x} \cap \bar{y}$. 则 $x \sim z$ 和 $y \sim z$. 根据对称性和传递性, $x \sim y$. 矛盾. \square

同学等价关系 \sim_c 对应的等价类是该中学所有的班, 每个同学都是所在班的代表元. 集合 \mathbb{Z} 关于 \equiv_2 共有两个等价类: 偶数集和奇数集. 偶数集可记为 $\bar{0}, \bar{2}, \overline{-2}, \dots$, 而奇数集的代表元可记为 $\bar{1}, \overline{-1}, \bar{3}, \overline{-3}, \dots$,

例 5.12 设 $m \in \mathbb{Z}^+$. 则 \mathbb{Z} 关于 \equiv_m 的等价类是

$$\bar{0} = \{km \mid k \in \mathbb{Z}\}, \bar{1} = \{km + 1 \mid k \in \mathbb{Z}\},$$

$$\dots, \overline{m-1} = \{km + m - 1 \mid k \in \mathbb{Z}\}.$$