

抽象代数的研究对象是有运算的集合，即代数系统，
确切地说，一个代数系统，
是指由一个集合和定义在该集合中的一种或多种运算构成的一个系统，
我们首先简单回顾集合的相关概念，以及集合的一些运算性质，
并给出剩余类集合及集合的笛卡儿积等概念，
我们称一些研究对象组成的总体为集合，构成集合的对象称为集合的元素，
令 A 是一个集合，若对象 a 属于 A ，则用 $a \in A$ 表示，
反之，若对象 a 不属于 A ，那么用 $a \notin A$ 表示，
我们熟知的全体自然数就构成一个集合，以符号 N 表示，
全体整数也构成一个集合，以符号 Z 表示，
类似地，全体有理数、实数和复数均构成集合，分别用 Q, R 和 C 表示，
令 A 和 B 是两个集合，
若对属于 A 的任意 a 都有 a 属于 B ，则称集合 A 是集合 B 的子集
记为 $A \subseteq B$ 或记为 $B \supseteq A$ ，读作 A 包含于 B 或 B 包含 A ，
特别地，
如果 A 包含于 B 并且 B 包含于 A ，那么称集合 A 和 B 相等，记为 $A=B$ ，
我们规定不包含任何元素的集合为空集，并记为 $\emptyset$
空集是任何集合的子集，即对于任意的集合 A 都有空集包含于 A
代数学研究的一个根本目标就是对所研究的对象进行有目的的分类，
对于集合，可以给出一种最简单的分类，即按集合中所含元素的个数分类，
如果一个集合含有有限多个元素，则称其为有限集，
否则，称其为无限集，我们熟知的 N, Z, Q, R 和 C 都是无限集，

有限集举例:

$\{1, 2, 3\}, \{a_1, a_2, \dots, a_n\}, \{\text{春}, \text{夏}, \text{秋}, \text{冬}\}$ 和 $\{x \mid -2 \leq x \leq 3, x \text{ 属于 } \mathbb{Z}\}$ 等等,

另外, 如果我们按“余数”考虑整数集合,

则可以定义一些更有意思的、后文经常用到的无限集和有限集,

例如, 如果我们对整数按被 3 除的余数进行考察的话, 则有

(1) 被 3 除而余数是 0 的整数集合的子集合为 $\{0, \pm 3, \pm 6, \pm 9, \dots\}$

(2) 被 3 除而余数是 1 的整数集合的子集合为 $\{\dots, -5, -2, 1, 4, 7, 10, \dots\}$

(3) 被 3 除而余数是 2 的整数集合的子集合为 $\{\dots, -7, -4, -1, 2, 5, 8, \dots\}$

进一步, 如果我们将上面的这三个集合分别记为 $\bar{0}$, $\bar{1}$ 和 $\bar{2}$

并将集合 $\bar{0}$, $\bar{1}$ 和 $\bar{2}$ 看成是元素,

那么可以构造一个新的有限集合 $\{\bar{0}, \bar{1}, \bar{2}\}$, 我们将其记为 $\mathbb{Z}_3$

对属于 $\mathbb{Z}^+$ 的任意的一个正整数 n ($\mathbb{Z}^+$ 表示正整数集合), 我们有如下的定义,

定义 1.1 设 a, b 属于 $\mathbb{Z}$,

若 a, b 被 n 除后余数相等, 则称 a 与 b 模 n 同余, 记其为 $a \equiv b \pmod{n}$,

并称集合 $\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$ 为模 n 与 a 同余的剩余类

(也简称为模 n 的剩余类), 其中的 a 则称为剩余类 $\bar{a}$ 的代表元素,

例如, 取 $a = 26, b = 14, n = 12$,

由于 26 除以 12 的余数是 2, 14 除以 12 的余数也是 2,

因此根据定义, 我们可以说 26 与 14 模 12 同余, 记作 $26 \equiv 14 \pmod{12}$,

显然, $\mathbb{Z}_3$ 是所有模 3 的剩余类构成的集合,

所有模 n 的剩余类构成的集合记为 $\mathbb{Z}_n$, 即 $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

命题 1.1 在 Z_n 中下列结论成立:

(1) a 属于 $\bar{a}$

(2) 若 b 属于 $\bar{a}$, 则 $\bar{b} = \bar{a}$

(3) $\bar{b} = \bar{a}$ 的充分必要条件是存在整数 t , 使得 $a - b = nt$,

证: (1) 因为 $a \equiv a \pmod{n}$, 所以 a 属于 $\bar{a}$

(2) 对属于 b 的任意 c , 由定义 1.1 知 $c \equiv b \pmod{n}$,

又由 b 属于 $\bar{a}$ 有 $b \equiv a \pmod{n}$, 因此 $c \equiv a \pmod{n}$, 即 c 属于 $\bar{a}$, 所以 $\bar{b}$ 包含于 $\bar{a}$

类似地, 可以证明 $\bar{b}$ 包含 $\bar{a}$, 因此 $\bar{b} = \bar{a}$

(3) 若 $\bar{b} = \bar{a}$, 则由(1)知 b 属于 $\bar{a}$, 因此 $b \equiv a \pmod{n}$,

再由整数的带余除法($x=yq+r$)可知存在整数 t , 使得 $a-b=nt$,

反之, 若 $a-b=nt$, 则 $b \equiv a \pmod{n}$, 所以, 由(2)有 $\bar{b} = \bar{a}$

由命题 1.1(2)知 $\bar{a}$ 中任何元素都是 $\bar{a}$ 的代表元素, 因此剩余类的代表元素不唯一
集合之间存在我们熟知的一些运算关系:

交集 $A \cap B = \{x | x \in A \text{ 且 } x \in B\}$, 例如, $\{1, 2, 3\} \cap \{2, 3, 4, 5\} = \{2, 3\}$,

并集 $A \cup B = \{x | x \in A \text{ 或 } x \in B\}$, 例如, $\{1, 2, 3\} \cup \{2, 3, 4, 5\} = \{1, 2, 3, 4, 5\}$,

差集 $A - B = \{x | x \in A, x \notin B\}$ 等, 例如, $\{1, 2, 3\} - \{2, 3, 4, 5\} = \{1\}$,

更一般地, 基于某个指标集 I (可以是无限集), 我们可以定义

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{x | \forall i \in I, x \in A_i\}$$

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x | \exists i \in I, x \in A_i\}$$

命题 1.2 设 A, B, C 均为集合，则 $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ ，

证：首先，证明 $(A \cap B) \cup C$ 包含于 $(A \cup C) \cap (B \cup C)$ ，

对属于 $(A \cap B) \cup C$ 的任意 x ，有 x 属于 $A \cap B$ 或 x 属于 C ，

若 x 属于 $A \cap B$ ，则 x 属于 A 且 x 属于 B ，

从而有 x 属于 $A \cup C$ 且 x 属于 $B \cup C$ ，即 x 属于 $(A \cup C) \cap (B \cup C)$ ，

若 x 属于 C ，则 x 属于 $A \cup C$ 且 x 属于 $B \cup C$ ，从而 x 属于 $(A \cup C) \cap (B \cup C)$ ，

于是对属于 $(A \cap B) \cup C$ 的任意 x ，总有 x 属于 $(A \cup C) \cap (B \cup C)$ ，

即 $(A \cap B) \cup C$ 包含于 $(A \cup C) \cap (B \cup C)$ ，

其次，证明 $(A \cup C) \cap (B \cup C)$ 包含于 $(A \cap B) \cup C$

对属于 $(A \cup C) \cap (B \cup C)$ 的任意 x ，有 x 属于 $A \cup C$ 且 x 属于 $B \cup C$ ，

如果 x 不属于 C ，则有 x 属于 A 且 x 属于 B ，即 x 属于 $A \cap B$ ，

所以 x 属于 $(A \cap B) \cup C$ ，

如果 x 属于 C ，则显然有 x 属于 $(A \cap B) \cup C$ ，

于是，对属于 $(A \cup C) \cap (B \cup C)$ 的任意 x ，总有 x 属于 $(A \cap B) \cup C$ ，

即 $(A \cup C) \cap (B \cup C)$ 包含于 $(A \cap B) \cup C$

至此，有 $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ ，

事实上，关于集合的“ $\cap, \cup$ ”运算，还有许多很好的性质，

例如，我们很容易验证

$A \cap B = B \cap A, A \cup B = B \cup A,$

$(A \cap B) \cap C = A \cap (B \cap C), (A \cup B) \cup C = A \cup (B \cup C)$ 等等，

定义 1.2 设 A 和 B 是两个集合，

则称集合 $A \times B = \{(a, b) | a \in A, b \in B\}$ 为集合 A 和 B 的笛卡儿积，

并规定 $(a, b) = (x, y) \Leftrightarrow a = x, b = y$ ，

例如，当 $A = \{1, 2\}, B = \{3, 4\}$ 时， $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$

一般地，我们可以定义 n (可以是无穷大) 个集合的笛卡儿积为

$$\prod_{i=1}^n A_1 \times \cdots \times A_i \times \cdots \times A_n = \{(a_1, \cdots, a_i, \cdots, a_n) | a_i \in A_i, 1 \leq i \leq n\}$$

并且规定 $(a_1, \cdots, a_i, \cdots, a_n) = (b_1, \cdots, b_i, \cdots, b_n) \Leftrightarrow a_i = b_i, i = 1, \cdots, n$

容易知道，有限个有限集合的笛卡儿积还是有限集合，

显然， $A \times \emptyset = \emptyset \times A = \emptyset$

但是，在一般情况下 $A \times B \neq B \times A$ ，

例如，当 $A = \{1, 2\}, B = \{3, 4\}$ 时，

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\} \neq \{(3, 1), (3, 2), (4, 1), (4, 2)\} = B \times A$$

例 1.1 求集合 $Z_2 = \{\bar{0}, \bar{1}\}$ 和 $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ 的笛卡儿积，

解: $Z_2 \times Z_5$

$$= \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{0}, \bar{3}), (\bar{0}, \bar{4}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2}), (\bar{1}, \bar{3}), (\bar{1}, \bar{4})\}$$

注意， Z_2 中的 $\bar{0}, \bar{1}$ 与 Z_5 中的 $\bar{0}, \bar{1}$ 含义是有区别的，

下面，我们简单回顾一下与映射相关的概念及性质

定义 1.3 设 A 和 B 是两个非空集合， φ 是它们元素之间的对应法则，

若对属于 A 的任意的 a ，在法则 φ 的作用下都有唯一的属于 B 的 b 与之对应，

则称 φ 是集合 A 到 B 的映射，并记 $b=\varphi(a)$ ，

而且称在 φ 下， b 是 a 的像， a 是 b 的原像，

若 φ 是集合 A 到 B 的映射且 $b=\varphi(a)$ ，

则我们时常常用 $\varphi: A \rightarrow B$, $a \rightarrow b$ 或 $A \xrightarrow{\varphi} B$, $a \xrightarrow{\varphi} b$ 表示

另外，对于 A 到 B 的映射 φ ，

若 A 中不同的元素在 φ 下的像不同，则称 φ 是单射

也就是说，对属于 A 的 a_1, a_2 ，当时 $\varphi(a_1)=\varphi(a_2)$ 时，必有 $a_1 = a_2$

若 B 中的每个元素在 φ 下都有原像，则称 φ 是满射，

若 φ 既是单射又是满射，则称 φ 是双射(或称 φ 是一一映射)，

集合 A 到 A 自身的映射称为 A 上的变换，

对于变换，同样有单变换，满变换和双变换的概念，

设 φ 是集合 A 到 B 的映射，若 A_0 是 A 的子集合，则记 $\varphi(A_0)=\{\varphi(a)|a \in A_0\}$ ，

若 B_0 是 B 的子集合，则记 $\varphi^{-1}(B_0)=\{a \in A|\varphi(a) \in B_0\}$ ，

特别地，当 $B_0=\{b\}$ 为单点集时，记 $\varphi^{-1}(b)=\{a \in A|\varphi(a)=b\}$ ，

显然，若 $\varphi(A)=B$ ，则 φ 是满射，

例 1.2 设 A 是一个非空集合，定义 $\varphi: A \rightarrow A$, $a \rightarrow a$ ，

即对属于 A 的任意 a ，有 $\varphi(a)=a$ ，显然， φ 是映射，

一般地，我们称映射 φ 是 A 上的恒等映射，显然，恒等映射是双变换，
集合 A 上的恒等映射记为 id_A 或者 1_A

在不至于引起混淆的情况下，也可以将其简记为 id 或者 1 ，

例 1.3 定义 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_3, n \rightarrow \bar{n}$ ，即对属于 $\mathbb{Z}$ 的任意 n ， $\varphi(n) = \bar{n}$ ，

易知 φ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_3$ 的满射，但不是单射，

例 1.4 设 φ 是集合 A 到 B 的映射， A_0 是 A 的非空子集，

若 $v: A_0 \rightarrow B$ 是 A_0 到 B 的映射，且对属于 A_0 的任意 a ，有 $v(a) = \varphi(a)$ ，

则称 v 是 φ 在 A_0 上的限制，并记其为 $v = \varphi|_{A_0}$

例 1.5 试证明 $\varphi: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}, (\bar{a}, \bar{b}) \rightarrow \overline{ab}$ 是一个映射

证: 对任意 $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ ，有 $\bar{a} = \bar{c}, \bar{b} = \bar{d}$

于是由命题 1.1(3)可知，存在整数 s, t 使得 $a - c = nt, b - d = ns$ ，

所以 $ab - cd = (a - c)b + c(b - d) = n(tb - cs)$ ，

进而由命题 1.1(3)得 $\overline{ab} = \overline{cd}$ 即相等元素的像相等， φ 是一个映射，

例 1.6 试证明 $\phi: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n, (\bar{a}, \bar{b}) \rightarrow \overline{a + b}$ 是一个映射，

证: 对任意 $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ 有 $\bar{a} = \bar{c}, \bar{b} = \bar{d}$ ，

于是由命题 1.1(3)可知，存在整数 s, t 使得 $a - c = nt, b - d = ns$ ，

所以 $(a + b) - (c + d) = (a - c) + (b - d) = n(t + s)$ ，

进而由命题 1.1(3)有 $\overline{a + b} = \overline{c + d}$ ，即相等元素的像相等， ϕ 是一个映射

例 1.7 试说明 $\tau: \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$, $(\bar{a}, \bar{b}) \rightarrow \overline{ab}$ 不是一个映射,

解: 按照 τ 的定义有 $(\bar{0}, \bar{1}) \rightarrow \bar{0}$, $(\bar{0}, \bar{1}) = (\bar{2}, \bar{1}) \rightarrow \bar{2}$, 即 $(\bar{0}, \bar{1})$ 的像不唯一, 因此 τ 不是一个映射

定义 1.4 设 ψ 是集合 A 到 B 的映射, ϕ 是集合 B 到 C 的映射,

则存在映射 $\phi\psi: A \rightarrow C$, 满足对属于 A 的任意 a , 有 $\phi\psi(a) = \phi(\psi(a))$,

称映射 $\phi\psi$ 是 ϕ 与 ψ 的合成(如图 1.1),

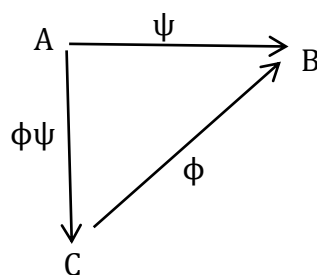


图 1.1

易知, 映射的合成满足结合律,

即对于映射 $\psi: A \rightarrow B$, $\phi: B \rightarrow C$ 和 $\sigma: C \rightarrow D$ 有 $\sigma(\phi\psi) = (\sigma\phi)\psi$,

且对任意映射 $\psi: A \rightarrow B$, 有 $\psi \text{id}_A = \psi$ 和 $\text{id}_B \psi = \psi$,

特别地, 若 ϕ 是集合 A 上的变换,

则我们用 ϕ^t 表示 t 个 ϕ 的合成, 并规定 $\phi^0 = \text{id}_A$

例 1.8 令 $2\mathbb{Z}$ 表示偶数集合, 定义映射 $\psi: \mathbb{Z} \rightarrow 2\mathbb{Z}$, 使得 $\psi(a) = 2a$,

和映射 $\phi: 2\mathbb{Z} \rightarrow \mathbb{Z}$, 使得 $\phi(a) = \frac{1}{2}a$, 求 $\psi\phi$ 和 $\phi\psi$

解: 易知, 合成映射 $\phi\psi = \text{id}_{\mathbb{Z}}$, 合成映射 $\psi\phi = \text{id}_{2\mathbb{Z}}$

定义 1.5 设 ψ 是集合 A 到 B 的映射，

若存在集合 B 到 A 的映射 ϕ ，使得 $\phi\psi=\text{id}_A$ ，并且 $\psi\phi=\text{id}_B$

则称 ψ 是可逆映射， ϕ 是 ψ 的逆映射，

命题 1.3 设 ψ 是集合 A 到 B 的映射，若 ψ 是可逆映射，则 ψ 的逆映射是唯一的

证： 设 ϕ 和 θ 是 ψ 的两个逆映射，则 $\theta=\text{id}_A\theta=(\phi\psi)\theta=\phi(\psi\theta)=\phi\text{id}_B=\phi$

既然逆映射是唯一的，如果 ψ 是可逆映射，那么以后我们将 ψ 的逆映射记为 ψ^{-1} ，

特别地，若 ψ 是集合 A 到 A 的可逆映射(变换)， n 是正整数，则记 $\psi^{-n}=(\psi^{-1})^n$

关于逆映射我们有如下性质，

命题 1.4 若 ψ 是集合 A 到 B 的可逆映射， ϕ 是集合 B 到 C 的可逆映射，

则可逆映射的合成 $\psi\phi$ 还是可逆映射，并且 $(\phi\psi)^{-1}=\psi^{-1}\phi^{-1}$

命题 1.5 设 A, B 是非空集合， $\psi: A \rightarrow B$ 是映射，则

(1) ψ 是单射的充分必要条件是存在映射 $\phi: B \rightarrow A$ ，使得 $\phi\psi=\text{id}_A$

(2) ψ 是满射的充分必要条件是存在映射 $\phi: B \rightarrow A$ ，使得 $\psi\phi=\text{id}_B$

证： 在此我们只考证如果存在映射 $\phi: B \rightarrow A$ ，使得 $\phi\psi=\text{id}_A$ ，则 ψ 是单射的情形

事实上，如果 ψ 不是单射，那么存在属于 A 的 $a_1 \neq a_2$ ，使得 $\psi(a_1)=\psi(a_2)$

从而 $\text{id}_A(a_1)=\phi\psi(a_1)=\phi\psi(a_2)=\text{id}_A(a_2)$ ，即 $a_1=a_2$ 矛盾，

以后为了讨论映射问题的方便，我们可使用图形表示映射的合成关系：

多边形的顶点表示集合，有箭头的线段表示映射，

特别地，

如果由始点集合 A 到终点集合 B 所经历的各条线路所组成的映射合成都相等，

则称这样的图形是交换图，

例如，若 $f_n f_{n-1} \cdots f_2 f_1 = g_m g_{m-1} \cdots g_2 g_1$ ，则称图 1.2 是交换图，

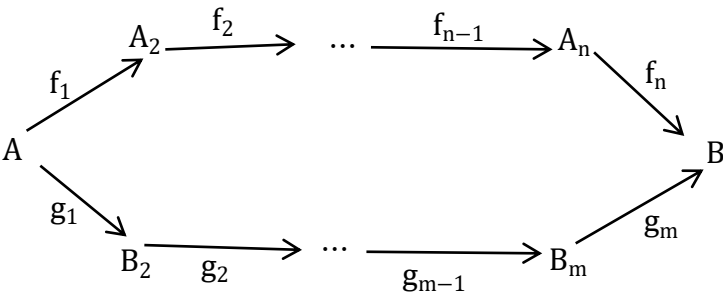


图 1.2

再如，若 $A \xrightarrow{f} B, B \xrightarrow{g} C, A \xrightarrow{\sigma} C$ 是映射，并且它们满足 $g f = \sigma$ ，则图 1.3 是交换图

类似地，若 $A \xrightarrow{f} B, C \xrightarrow{g} D, A \xrightarrow{\sigma} C, B \xrightarrow{\tau} D$ 是映射，并且它们满足 $\tau f = g \sigma$ ，

则图 1.4 是交换图，

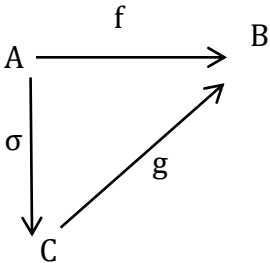


图 1.3

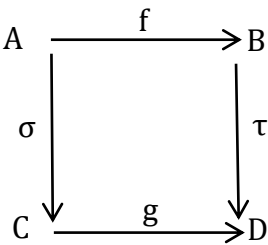


图 1.4