第一章　群

近世代数的主要研究对象是具有代数运算的集合, 这样的集合称为代数系. 群就是具有一个代数运算的代数系. 群的理论是近代数学的一个重要分支, 它在物理学、化学、信息学等许多领域中都有着广泛的应用.

本章和下一章介绍群的初步理论. 这一章的第一节讨论等价关系和集合的分类及它们之间的联系. 这一节的内容虽不属于群论的范畴, 但等价关系和集合的分类却是近世代数中经常出现的两个基本概念, 所以先做一个介绍. 第二到第四节介绍群、子群、群同构的概念及有关性质. 这是了解群的第一步. 第五第六节较为详细地讨论了两类最常见的群 —— 循环群与置换群. 学习这部分内容可以熟悉群的运算和性质, 加深对群的理解. 最后一节是选学内容, 介绍置换群的某些应用，初学时可以略去, 并不影响后面的学习.

§1　等价关系与集合的分类

在数学研究中, 我们常常要对一个集合的元素加以比较, 希望通过元素之间的联系去了解整个集合. 另一方面, 我们也常常要把一个集合分成若干个子集, 以便对各个子集进行分类研究, 或对其中某些特殊子集加以讨论, 从而了解整个集合的性质. 例如, 在实数集中, 任意两个实数 a 与 b 之间就有 a 大于 b 或 a 不大于 b 两种情况. 同时, 根据一个实数是否大于零, 我们可以把整个实数集合分解为正实数集 $\mathbf{R}^+$, 负实数集 $\mathbf{R}^-$ 和单独一个数 0 组成的集合 $\{0\}$ 这三个子集合. 又如, 数域 F 上的一元多项式环 $F[x]$ 中, 对任意两个多项式 $f(x)$ 与 $g(x)$, 有 $f(x)$ 整除 $g(x)$ 或 $f(x)$ 不整除 $g(x)$ 两种情况; 并且, 根据一个多项式被一个非零多项式 $g(x)$ 所除的余式, 可以把整个多项式环 $F[x]$ 分解为许多个子集, 不同的子集没有公共元素, 同一个子集中的多项式在被 $g(x)$ 除时余式都相同.

将上面两个例子中所涉及的概念加以推广, 我们就得到集合上一般的关系的概念和集合的分类的概念. 这一节的主要目的就是来介绍这两个概念以及它们之间的联系.

定义 1.1　设 S 是一个非空集合, $\mathcal{R}$ 是关于 S 的元素的一个条件. 如果对 S 中任意一个有序元素对 (a,b), 我们总能确定 a 与 b 是否满足条件 $\mathcal{R}$, 就称 $\mathcal{R}$ 是 S 的一个**关系** $(relation)$. 如果 a 与 b 满足条件 $\mathcal{R}$, 则称 a 与 b 有关系 $\mathcal{R}$, 记作 $a\,\mathcal{R}\,b$; 否则称 a 与 b 无关系 $\mathcal{R}$. 关系 $\mathcal{R}$ 也称为二元关系.

上面提到的实数集中元素之间的大于和 $F[x]$ 中多项式的整除都是关系.

例 1 设 S 是一个非空集合, S 的所有子集组成的集合记为 $\mathcal{P}(S)$. 因为对 S 的任意两个子集 A, B, $A \subseteq B$ 或 $A \nsubseteq B$ 有且仅有一个成立, 所以集合的包含关系 "$\subseteq$" 是 $\mathcal{P}(S)$ 的一个关系. 进一步讨论可以发现, 这个关系还具有下面两条性质:

(1) 反身性, 即对 S 的任一子集 A, 有 $A \subseteq A$;

(2) 传递性, 即对 S 的任意子集 A, B, C, 如果 $A \subseteq B$, $B \subseteq C$, 则有 $A \subseteq C$. □

例 2 在整数集 $\mathbf{Z}$ 中, 规定 $a \mathcal{R} b \Longleftrightarrow a \mid b$. 因为 $a \mid b$ 与 $a \nmid b$ 有且仅有一个成立, 所以 "$\mid$" 是 $\mathbf{Z}$ 的一个关系. 这个关系也具有反身性和传递性. □

例 3 在整数集 $\mathbf{Z}$ 中, 规定 $a \mathcal{R} b \Longleftrightarrow (a, b) = 1$ (即 a 与 b 互素). 因为 $(a, b) = 1$ 与 $(a, b) \neq 1$ 有且仅有一个成立, 所以是 $\mathbf{Z}$ 的一个关系. 这个关系既不满足反身性也不满足传递性, 但却满足所谓的对称性, 即: 对任意两个整数 a, b, 由 $(a, b) = 1$ 可推出 $(b, a) = 1$. □

同时具有反身性、对称性和传递性三条性质的关系是我们特别感兴趣的.

定义 1.2 设 $\mathcal{R}$ 是非空集合 S 的一个关系, 如果 $\mathcal{R}$ 满足:

(E1) 反身性, 即对任意的 $a \in S$, 有 $a \mathcal{R} a$;

(E2) 对称性, 即若 $a \mathcal{R} b$, 则 $b \mathcal{R} a$;

(E3) 传递性, 即若 $a \mathcal{R} b$, 且 $b \mathcal{R} c$, 则 $a \mathcal{R} c$.

则称 $\mathcal{R}$ 是 S 的一个**等价关系**(*equivalence relation*), 并且如果 $a \mathcal{R} b$, 则称 a 等价于 b, 记作 $a \sim b$.

定义 1.3 如果 $\sim$ 是集合 S 的一个等价关系, 对 $a \in S$, 令

$$[a] = \{x \in S \mid x \sim a\}.$$

称子集 $[a]$ 为 S 的一个**等价类**(*equivalence class*). S 的全体等价类的集合称为集合 S 在等价关系下的**商集**(*quotient set*), 记作 $S/\sim$.

例 4 易知, 三角形的全等、相似, 数域 K 上 n 阶方阵的等价、相似、相合等都是等价关系, 而例 1、例 2、例 3 及本节开头所述的关系都不是等价关系. □

例 5 设 m 是正整数, 在整数集 $\mathbf{Z}$ 中, 规定

$$a \mathcal{R} b \Longleftrightarrow m \mid a - b, \quad \forall a, b \in \mathbf{Z}.$$

则:

(1) 对任意整数 a, 有 $m \mid a - a$;

(2) 若 $m \mid a - b$, 则 $m \mid b - a$;

(3) 若 $m \mid a - b$, $m \mid b - c$, 则 $m \mid a - c$.

所以 $\mathcal{R}$ 是 $\mathbf{Z}$ 的一个等价关系. 显然 a 与 b 等价当且仅当 a 与 b 被 m 除有相同的余数, 因此称这个关系为**同余关系**(*congruence relation*), 并记作 $a \equiv b \pmod{m}$ (读作"a 同余于 b, 模 m"). 整数的同余关系及其性质是初等数论的基础 (参见 [1]).

设 $a \in \mathbf{Z}$, 则

$$\begin{aligned}[a] &= \{x \in \mathbf{Z} \mid x \equiv a \pmod m\} \\ &= \{x \in \mathbf{Z} \mid m | x-a\} \\ &= \{a+mz \mid z \in \mathbf{Z}\}.\end{aligned}$$

$[a]$ 称为整数集 $\mathbf{Z}$ 的一个(与 a 同余的)模 m 剩余类, 在数论中, $[a]$ 常记作 $\overline{a}$, 而相应的商集称为 $\mathbf{Z}$的模 m 剩余类集, 常记作 $\mathbf{Z}_m$.

由于

$$\overline{a} = \overline{b} \Longleftrightarrow m \mid a-b,$$

易知

$$\begin{aligned}&\overline{0} = \{\cdots, -2m, -m, 0, m, 2m, \cdots\}, \\ &\overline{1} = \{\cdots, -2m+1, -m+1, 1, m+1, 2m+1, \cdots\}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\overline{m-1} = \{\cdots, -m-1, -1, m-1, 2m-1, 3m-1, \cdots\},\end{aligned}$$

是模 m 的全体不同的剩余类, 所以

$$\mathbf{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}. \quad \square$$

集合的等价关系常和下面的概念联系在一起.

定义 1.4 如果非空集合 S 表成若干个两两不相交的非空子集的并, 则称这些子集为集合 S 的一种**分类** (*partition*), 其中每个子集称为一个**类** (*class*). 如果 S 的子集族 $\{S_i \mid i \in I\}$ 构成 S 的一种分类, 则记作 $\mathcal{P} = \{S_i \mid i \in I\}$.

由此定义可知, 集合 S 的子集族 $\{S_i \mid i \in I\}$ 构成 S 的一种分类当且仅当:

(P1) $S = \bigcup\limits_{i \in I} S_i$;

(P2) $S_i \cap S_j = \varnothing$, $i \neq j$.

其中, (P1) 说明 $\{S_i\}$ 这些子集无遗漏地包含了 S 的全部元素; (P2) 说明两个不同的子集无公共元素. 从而 S 的元素属于且仅属于一个子集. 所以, 分类必须满足不漏不重的原则.

例 6 设 M 为数域 F 上全体 n 阶方阵的集合, 令 M_r 表示所有秩为 r 的 n 阶方阵构成的子集. 则有

(1) $M = \bigcup\limits_{i=0}^{n} M_i$;

(2) $M_i \cap M_j = \varnothing$, $i \neq j$.

所以 $\{M_i \mid i = 0, 1, \cdots, n\}$ 是 M 的一种分类. $\square$

例 7 $\mathbf{Z}_m = \{\overline{a} \mid a = 0, 1, 2, \cdots, m-1\}$ 是整数集 $\mathbf{Z}$ 的一种分类. $\square$

例 8 对实数集 $\mathbf{R}$, 令子集 $R_i = [i, i+1]$, $i \in \mathbf{Z}$. 由于 $i \in R_i$, 且 $i \in R_{i-1}$, 同一元素在两个子集中重复出现, 所以 $\{[i, i+1] \mid i \in \mathbf{Z}\}$ 不是 $\mathbf{R}$ 的一种分类. $\square$

下面的定理揭示了集合的等价关系与集合的分类这两个概念之间的联系.

定理 1.1 集合 S 的任何一个等价关系都确定了 S 的一种分类, 且其中每一个类都是集合 S 的一个等价类. 反之, 集合 S 的任何一种分类也都给出了集合 S 的一个等价关系, 且相应的等价类就是原分类中的那些类.

证明: 首先, 设 $\sim$ 为集合 S 的一个等价关系, 则

(1) 对任意的 $a \in S$, 由反身性知 $a \in [a]$, 所以 $S = \bigcup\limits_{a \in S} [a]$.

(2) 如果 $[a] \cap [b] \neq \varnothing$, 则有 $c \in [a] \cap [b]$. 于是 $c \sim b$, $c \sim a$, 从而由对称性知 $b \sim c$, 再由传递性知 $b \sim a$. 又对任意的 $b' \in [b]$, 则 $b' \sim b$, 同样由传递性得 $b' \sim a$. 于是 $b' \in [a]$, 因此 $[b] \subseteq [a]$. 同理, $[a] \subseteq [b]$. 所以 $[a] = [b]$. 这说明, 不同的类没有公共元素.

从而由 (P1), (P2) 知, 全体等价类形成 S 的一种分类, 显然每一个类都是 S 的等价类.

其次, 如果已知集合 S 的一种分类 $\mathcal{P}$, 在 S 中规定关系 "$\sim$":

$$a \sim b \Longleftrightarrow a \text{ 与 } b \text{ 属于同一类}, \quad a, b \in S.$$

对任意的 $a \in S$, 由于 a 与其本身属于同一类, 所以 $a \sim a$. 如果 $a \sim b$, 即 a 与 b属于同一类, 自然 b 与 a 也属于同一类, 所以 $b \sim a$. 最后, 如果 $a \sim b$, $b \sim c$, 即 a 与 b 属于同一类, b 与 c 属于同一类, 因而 a 与 c 同在 b 所在的类中, 所以 $a \sim c$. 因此 "$\sim$" 是 S 的一个等价关系. 显然, 由此等价关系得到的等价类就是原分类中的那些类. $\square$

这个定理告诉我们, 一个集合的分类可以通过等价关系来描述. 试比较例 4, 5 及例 6, 7, 可以看出, 这样做在很多情况下是方便的 —— 特别是如果我们能用简单的术语来表述这种关系. 另一方面, 等价关系也可以用集合的分类来表示. 特别是, 通过对集合的各种分类的了解, 使我们能够对集合的不同等价关系及其相互联系进行研究. 不过, 本书不准备对此进行深入的讨论. 我们仅以下面的例子来说明集合的分类对研究集合的等价关系的作用.

例 9 设 $S = \{a, b, c\}$, 试确定集合 S 上的全部等价关系.

解 由定理 1.1知, 只要求出 S 的全部分类, 也即求出 S 的所有可能的子集分划即可.

(1) 如果 S 仅分划为一个子集, 则有 $\mathcal{P}_1 = \{S\}$;

(2) 如果 S 分划为两个子集, 则有

$$\mathcal{P}_2 = \{\{a\}, \{b, c\}\}, \mathcal{P}_3 = \{\{b\}, \{a, c\}\}, \mathcal{P}_4 = \{\{c\}, \{a, b\}\};$$

(3) 如果 S 分划为三个子集, 则有 $\mathcal{P}_5 = \{\{a\}, \{b\}, \{c\}\}$.

因此, S 上共有五个不同的等价关系, 它们是:

$$\sim_1 = \{a \sim a, b \sim b, c \sim c, a \sim b, b \sim a, a \sim c, c \sim a, b \sim c, c \sim b\};$$

$$\sim_2 = \{a \sim a, b \sim b, c \sim c, b \sim c, c \sim b\};$$

$$\sim_3 = \{a \sim a, b \sim b, c \sim c, a \sim c, c \sim a\};$$

$$\sim_4 = \{a \sim a, b \sim b, c \sim c, a \sim b, b \sim a\};$$

$$\sim_5 = \{a \sim a, b \sim b, c \sim c\}.$$

注: 如果用 $B(n)$ 表示一个具有 n 个元素的集合上的不同等价关系的个数, 则有下列的递推公式:

$$B(n+1) = \sum_{k=0}^{n} C_n^k B(k), \quad n \geqslant 1. \tag{1.1}$$

其中, C_n^k 为二项式系数, 并规定 $B(0)=1$, $B(1)=1$. 这个公式的证明以及对数 $B(n)$ 的性质的讨论, 已超出本书的范围. 有兴趣的读者可参考组合数学方面的书籍 (参见 [2]).

习题 1 − 1

1. 试分别举出满足下列条件的关系:

(1) 有对称性, 传递性, 但无反身性;

(2) 有反身性, 传递性, 但无对称性;

(3) 有反身性, 对称性, 但无传递性.

2. 找出下列证明中的错误:

有人断言, 若 S 的关系 $\mathcal{R}$ 有对称性和传递性, 则必有反身性. 这是因为, 对任意的 $a\in S$, 由对称性, 如果 $a\,\mathcal{R}\,b$, 则 $b\,\mathcal{R}\,a$. 再由传递性, 得 $a\,\mathcal{R}\,a$, 所以 $\mathcal{R}$ 有反身性.

3. 证明: 在数域 F 上全体 n 阶方阵的集合 M 中, 矩阵的等价、相合和相似都是等价关系.

4. 设 ϕ 是集合 A 到 B 的映射, $a,b\in A$, 规定关系 “$\sim$”:

$$a\sim b \iff \phi(a)=\phi(b).$$

证明: $\sim$ 是一个等价关系, 并求其等价类.

5. 设 $A=\{1,2,3,4\}$, 在 $\mathcal{P}(A)$ 中规定关系 “$\sim$”:

$$S_1\sim S_2 \iff S_1 \text{ 与 } S_2 \text{ 含有相同个数的元素.}$$

证明: $\sim$ 是 $\mathcal{P}(A)$ 上的一个等价关系, 并求商集 $\mathcal{P}(A)/\sim$.

6. 在有理数集 $\mathbf{Q}$ 中, 规定关系“$\sim$”:

$$a\sim b \iff a-b\in\mathbf{Z}.$$

证明: $\sim$ 是一个等价关系, 并求出所有的等价类.

7. 在复数集 $\mathbf{C}$ 中, 规定关系 “$\sim$”:

$$a\sim b \Longleftrightarrow |a|=|b|.$$

证明: $\sim$ 是 $\mathbf{C}$ 上的一个等价关系, 试确定相应的商集 $\mathbf{C}/\sim$, 并给出每个等价类的一个代表元素.

8. 设集合

$$S=\{(a,b)\mid a,b\in\mathbf{Z},b\neq 0\}.$$

在集合 S 中, 规定关系 “$\sim$”:

$$(a,b)\sim(c,d) \iff ad=bc.$$

证明: $\sim$ 是一个等价关系.

9.* 设 $A=\{a,b,c,d\}$, 试写出集合 A 的所有不同的等价关系.

10.* 不用公式 (1.1), 直接算出集合 $A=\{1,2,3,4,5\}$ 的不同的分类数.

参考文献及阅读材料

[1] 闵嗣鹤, 严士健编. 初等数论. 第2版. 北京: 高等教育出版社, 1990
本书的第1章有关于整数整除性的详细讨论, 第3章则介绍了同余的概念及其性质.

[2] Aigner, M., Combinatorial Theory, Springer-Verlag, Berlin, Heiderberg, New York, 1979