第一章　群论基础

§1.1　集合论预备知识

§1.1.1　集合的定义

我们首先回顾一下集合的定义.

将一些不同的对象放在一起, 即为**集合** (set), 其中的对象称为集合的**元素** (element). 在本书中, 我们将使用大写字母 $A, B, C, \ldots$ 来表示集合, 用小写字母 $a, b, c, \ldots$ 来表示集合中的元素. 记 A 为一个集合. 如果 a 是 A 中的元素, 则称 a 属于 A, 记为 $a \in A$ 或 $A \ni a$, 否则记为 $a \notin A$. 我们也可以将集合 A 表示为 $A = \{a \mid a \in A\}$, 其中 $a \in A$ 可以用 A 中元素满足的共同性质代替, 比如说偶数集合=$\{a$ 为整数 $\mid a$被2 整除$\}$. 注意到集合中元素总是不重复的.

如果集合 A 中的每一个元素均是集合 B 中元素, 则称 A 是 B 的**子集** (subset), 换言之, 即若 $a \in A$, 则 $a \in B$. 此时我们记为 $A \subseteq B$ 或 $B \supseteq A$. 可以用图 1.1 来表示 $A \subseteq B$.

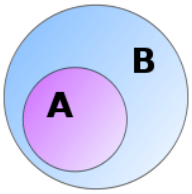


图 1.1: 集合的包含关系

如果集合 $A \subseteq B$ 且 $B \subseteq A$, 即 $a \in A$ 当且仅当 $a \in B$, 称 A 与 B **相等**, 并记为 $A = B$. 如果 $A \subseteq B$ 且 $A \neq B$, 我们称 A 为 B 的**真子集** (proper subset), 记为 $A \subset B$ 或者$A \subsetneq B$.

不含任何元素的集合称为**空集** (empty set), 记为 $\emptyset$. 由定义可知, 空集 $\emptyset$ 是任何集合的子集, 且是任何非空集合的真子集.

如果集合A的元素个数有限, 称A 为**有限集** (finite set), 其元素个数称为**集合的阶** (cardinality 或order), 记为$|A|$. 元素个数无限的集合称为**无限集** (infinite set), 它的阶定义为 ∞.

§1.1.2　集合的基本运算

一般来说, 集合有如下的四种基本运算.

(I) **集合的交** 设 A, B 为两个集合, 则A 与 B 的**交集** (intersection)为

$$A \cap B := \{x \mid x \in A \text{ 且} x \in B\}.$$

可以用图 1.2 表示集合的交. 在上式中, 记号:= 表示的是将其右边的集合记作$A \cap B$.

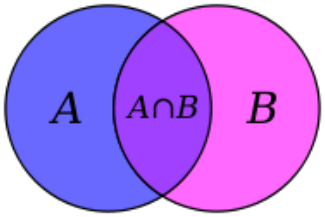


图 1.2: 集合的交

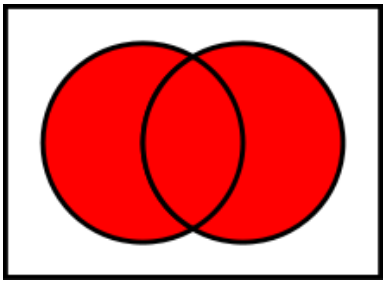


图 1.3: 集合的并

更一般地, 设 I 为集合, 设 I 中每个元素 i 对应集合 A_i, 则集合 $A_i(i \in I)$ 的交为

$$\bigcap_{i\in I} A_i := \{x \mid x \in A_i, \text{对每个} i \in I \text{成立}\}.$$

(II) **集合的并** 设集合 A, B 如上所示, 则A **与** B **的并集** (union)为

$$A \cup B := \{x \mid x \in A \text{ 或} x \in B\}.$$

可以用图 1.3 表示集合的并. 更一般地, 集合 $A_i(i \in I)$ 的并为

$$\bigcup_{i\in I} A_i := \{x \mid x \in A_i, \text{ 对某个} i \in I \text{ 成立}\}.$$

如果 A_i 两两不交(即交集为空集), 我们称 $\bigcup_{i\in I} A_i$ 为**不交并**(disjoint union), 并记为 $\bigsqcup_{i\in I} A_i$.

(III) **集合的差集与补集** 设 A, B 为某固定集合 U 的子集, 则A **对** B **的补集或差集** (complement)为

$$A - B = A\backslash B := \{x \mid x \in A \text{ 且} x \notin B\}.$$

它可用图 1.4 表示. 由差集定义, 我们有

$$A = (A \cap B) \sqcup (A - B).$$

A **在** U **中的补集**为

$$A^c := \{x \in U \mid x \notin A\}.$$

它可用图 1.5 表示.

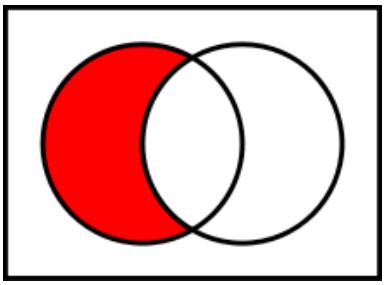


图 1.4: 集合的差集$A - B$

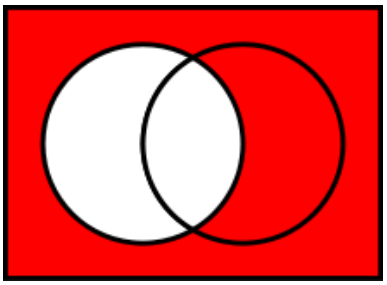


图 1.5: 集合的补集A^c

由定义可知, 如果A, B为有限集, 则 $A\cup B, A\cap B$ 均为有限集, 且

$$|A\cup B| = |A| + |B| - |A\cap B|. \tag{1.1}$$

这是**容斥原理** (inclusion-exclusion principle)的简单形式. 更进一步地, 我们有容斥原理的一般形式:

命题1.1. 设 A_i, $i = 1, \cdots, n$ 为某固定集合U 的有限子集, 则

$$|A_1\cup\cdots\cup A_n| = \sum_{j=1}^{n}(-1)^{j-1}\sum_{\{i_1,\cdots,i_j\}\subseteq\{1,\cdots,n\}}|A_{i_1}\cap\cdots\cap A_{i_j}|. \tag{1.2}$$

命题1.2. 设 A_i $(i\in I)$ 为某固定集合 U 的子集, 则

$$\bigcap_{i\in I}A_i^c = \Big(\bigcup_{i\in I}A_i\Big)^c. \tag{1.3}$$

通俗地说, 就是补集的交等于并集的补.

证明. 我们有

$$\begin{aligned} x\in\bigcap_{i\in I}A_i^c &\Longleftrightarrow x\in A_i^c \text{ 对任意}i\in I \text{ 成立}\\ &\Longleftrightarrow x\notin A_i \text{ 对任意}i\in I \text{ 成立}\\ &\Longleftrightarrow x\notin\bigcup_{i\in I}A_i, \text{ 即 } x\in\Big(\bigcup_{i\in I}A_i\Big)^c. \end{aligned}$$

等式得证. □

(IV) **集合的笛卡尔积** 集合 A 与 B 的**笛卡尔积** (Cartesian product)是由所有元素对 (a,b) (其中 $a\in A, b\in B$) 构成的集合, 即

$$A\times B := \{(a,b)\mid a\in A, b\in B\}.$$

更进一步地, 集合族 A_i $(i\in I)$ 的笛卡尔积为

$$\prod_{i\in I}A_i := \{(a_i)_{i\in I}\mid a_i\in A_i\}.$$

如所有的A_i 均为A, 我们通常用A^I 表示其笛卡尔积. 特别地, 我们用A^n 表示n 个A 的笛卡尔积.

注记. 我们可以用一个简单例子来理解集合.

- 班级 $\longleftrightarrow$ 集合,
- 班上的学生 $\longleftrightarrow$ 元素,
- 班上的一个学习小组 $\longleftrightarrow$ 子集合,
- 所有不参加该学习小组的人 $\longleftrightarrow$ 补集,
- 学校的所有班级 $\longleftrightarrow$ 集合构成的集族.

§1.1.3 一些常用的集合记号

在本书中, 我们将经常使用如下集合:

- $\mathbb{Z}_+$: 正整数集合;
- $\mathbb{N} = \mathbb{Z}_+ \cup \{0\}$: 自然数集合;
- $\mathbb{Z}$: 整数集合;
- $\mathbb{Q}$: 有理数集合;
- $\mathbb{R}$: 实数集合;
- $\mathbb{C}$: 复数集合;
- $F[X]$: F ($F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等) 上的(一元) 多项式的集合.

§1.1.4 映射, 合成律和结合律

设 A, B 为两个集合. 如果对 A 中每个元素 a, 均有唯一元素 $b \in B$ 与之对应, 我们称此对应为 A 到 B 的**映射** (map), 记为

$$f : A \to B, \quad a \mapsto b = f(a).$$

有时候, 我们也记之为

$$A \xrightarrow{f} B.$$

集合A 称为 f 的**定义域**, $f(A) = \{f(a) \mid a \in A\} \subseteq B$ 称为f 的**值域** 或**像集**. b 称为a 的**像**, a 称为b 的一个**原像**.

当集合B 是数(如有理数或者实数) 的集合时, 映射f 习惯上称为**函数** (function).

如果对元素 $a_1, a_2 \in A$, 当 $f(a_1) = f(a_2)$ 时, 即有 $a_1 = a_2$, 我们称映射 f 为**单射** (injective); 如果对任意 $b \in B$, 存在 $a \in A$, 使得 $f(a) = b$, 我们称 f 为**满射** (surjective); 如果 f 既是单射, 又是满射, 我们称 f 为**一一对应** (one-to-one correspondence), 或**双射** (bijective).

设f 与g 为集合A 到B的两个映射. 如果对于A 中任意元素a, 均有$f(a) = g(a)$, 则称映射f 与g **相等**, 记为$f = g$.

设 $f : A \to B, g : B \to C$ 为映射, 则映射

$$g \circ f : A \to C, \quad a \mapsto g(f(a))$$

称为 f 与 g 的**复合映射**(或谓**复合律**, composition law).

命题1.3 (**结合律**)**.** 设 $f : A \to B$, $g : B \to C$ 与$h : C \to D$ 为集合间的映射, 则

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

定义1.4. 设 S 为集合. 我们称映射 $f : S \times S \to S,\ (a,b) \mapsto p$ 为 S 上的一个**二元运算** (binary operation).

注记. 在数学应用中, 记号 $p = f(a,b)$ 并不是一个很简洁的记号. 实际上, 我们经常使用 $+, \times, *, \cdot$ 等符号来表示二元运算, 即

$$\boxed{p = ab,\ a \times b,\ a + b,\ a * b,\ a \cdot b, \text{诸如此类.}}$$

例1.5. 加法, 减法和乘法是实数集$\mathbb{R}$上的二元运算, 除法是$\mathbb{R}^\times := \mathbb{R}\backslash\{0\}$ 上的二元运算.

例1.6. 记 Σ_A 为集合 A 到自身的所有映射的集合, 则映射的复合构成 Σ_A 上的二元运算.

记 S_A 为集合 A 到自身的所有双射构成的集合, 则映射的复合构成 S_A 上的二元运算.

定义1.7. 集合 S 上的二元运算如果满足条件: 对所有 $a,b,c \in S$,

$$(ab)c = a(bc), \tag{1.4}$$

则称该二元运算满足**结合律** (associative law). 如果对任意 $a,b \in S$,

$$ab = ba, \tag{1.5}$$

则称其满足**交换律** (commutative law).

注记. 如果直接用$f(a,b)$ 表示二元运算ab, 则(1.4) 即等式

$$f(f(a,b),c) = f(a,f(b,c)),$$

而(1.5) 即等式

$$f(a,b) = f(b,a).$$

由此可以看出使用乘法记号表示二元运算的简洁性.

容易看出, 上面例子中的二元运算均满足结合律, 但映射的复合一般并不满足交换律. 事实上, 我们有如下基本事实:

$$\boxed{\boxed{\textbf{结合律是更一般的规律.}}}$$

在本书中, 我们将赋予给定集合一个或数个(满足结合律)的二元运算, 从而赋予该集合群, 环或者域的代数结构.

§1.1.5 等价关系, 等价类与分拆

定义1.8. 集合 A 中的元素间的关系 $\sim$ 称为**等价关系** (equivalence relation), 是指下述三条性质成立:

(1) (**自反性**) 对所有 $a \in A, a \sim a$.

(2) (**对称性**) 如果 $a \sim b$, 则 $b \sim a$.

(3) (**传递性**) 如果 $a \sim b$ 且 $b \sim c$, 则 $a \sim c$.

定义1.9. 集合 A 作为它的一些子集合的不交并, 称为 A 的一个**分拆** (partition).

设 $\sim$ 是 A 上的一个等价关系. 如 $a \in A$, 记 $[a] = \{b \in A \mid b \sim a\}$, 即 $[a]$ 为 A 中所有与 a 等价的元素构成的子集合, $[a]$ 称为a 所在的**等价类** (equivalent class). 则

$$[a] \cap [b] = \begin{cases} [a] = [b], & \text{如果} a \sim b, \\ \varnothing, & \text{如果} a \nsim b. \end{cases}$$

记$A/\sim$ 为A 中所有等价类构成的集合, 即

$$A/\sim := \{[a] \mid a \in A\} \quad (\text{去掉重复项}).$$

故A 可以写为不交并

$$A = \bigsqcup_{[a] \in A/\sim} [a]. \tag{1.6}$$

由此我们得到 A 的一个分拆. 反过来, 如果 $A = \bigsqcup\limits_{i \in I} A_i$ 为A 的分拆, 则很容易在 A 上定义等价关系:

$$a \sim b \quad \text{当且仅当} \quad a, b \text{ 属于同一个 } A_i.$$

故我们有如下结果

定理1.10. 集合 A 的分拆与定义在A上的等价关系一一对应.

例1.11. 整数集合 $\mathbb{Z}$ 可以分拆为偶数集合和奇数集合的不交并. 另一方面, 在 $\mathbb{Z}$ 上可以定义等价关系: $a \sim b$ 如果 $a - b$ 是偶数, 则偶数集合是此等价关系中 0 所在的等价类, 奇数集合为 1 所在的等价类.

设 $f : A \to B$ 为集合间的映射. 对于元素 $b \in B$, 令b 的原像集合 $f^{-1}(b) = \{a \in A \mid f(a) = b\}$, 则 $f^{-1}(b)$ 为 A 的子集. 对于B 中不同的元素b 和b', 有$f^{-1}(b) \cap f^{-1}(b') = \varnothing$. 并且, $f^{-1}(b) = \varnothing$ 当且仅当 $b \notin f(A)$. 故我们得到分拆

$$A = \bigsqcup_{b \in f(A)} f^{-1}(b). \tag{1.7}$$

我们称集合A 的这个分拆为**映射 f 决定的分拆**. 它决定的等价关系即

$$a \sim a' \iff f(a) = f(a').$$

例1.12. 如果$\sim$ 是集合A 上的等价关系, 对于自然映射

$$\pi : A \to A/\sim, \quad a \mapsto [a],$$

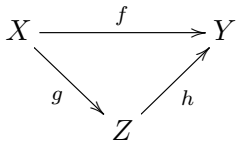
可以看出, π 所决定的分拆即等价关系$\sim$ 所决定的分拆.

例1.13. 定义映射 $f : \mathbb{Z} \to \{0, 1\}$, 其中 $f(2n) = 0$, $f(2n+1) = 1$. 则映射 f 决定的等价关系和分拆即与例1.11 给出的等价关系是同一等价关系.

例1.14. 设 $f : \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ 为实数减法映射 $(x, y) \mapsto x - y$, 则 $f^{-1}(a)$ 为直线 $y = x - a$. 实平面 $\mathbb{R}^2$ 由映射 f 决定的分拆即是平行直线束 $y = x - a$ $(a \in \mathbb{R})$ 的不交并.

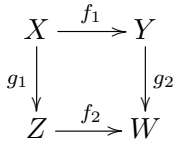
§1.1.6 映射分解和交换图表

设$f : X \to Y$ 和$g : X \to Z$ 为给定映射, 如果存在映射$h : Z \to Y$, 使得$f = h \circ g$, 我们称f **通过**g **分解** (factors through g). 如果g由Z 明显给出, 有时也称f **通过**Z **分解** (factors through Z). 我们通常可以通过图表



来表示f 通过g 的分解. 这里, 从X 经过不同路线到Y的映射: 经过水平路线的映射f, 经过右下然后右上得到的复合映射$h \circ g$, 是同一个映射. 我们将这样的图表称为**交换图表** (commutative diagram).

交换图表的概念可以做进一步推广. 设有一个由集合作为顶点, 集合间映射作为有向边组成的有向图(图表), 我们称此有向图为**交换图表**, 如果图中任意两点间沿着箭头方向的不同路径得到的复合映射是同一映射. 例如, 图表



如果满足$f_2 \circ g_1 = g_2 \circ f_1$, 则此图表为交换图表.

习　　题

习题1.1.1. 设B, $A_i (i \in I)$均是集合Ω的子集. 试证:

(1) $B \bigcap (\bigcup\limits_{i \in I} A_i) = \bigcup\limits_{i \in I} (B \bigcap A_i)$;

(2) $B \bigcup (\bigcap\limits_{i \in I} A_i) = \bigcap\limits_{i \in I} (B \bigcup A_i)$;

(3) $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$.

习题1.1.2. 对于任何集合X, 我们用id_X 表示X 到自身的恒等映射. 设 $f : A \to B$ 是集合间的映射, A 是非空集合. 试证:

(1) f 为单射当且仅当存在 $g : B \to A$, 使得 $g \circ f = \mathrm{id}_A$;

(2) f 为满射当且仅当存在 $h : B \to A$, 使得 $f \circ h = \mathrm{id}_B$;

(3) f 为双射当且仅当存在唯一的$g : B \to A$, 使得$f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$. 这里的$g$ 称为f 的**逆映射**, 通常记为f^{-1}. 证明双射的逆映射也是双射, 并讨论逆映射与映射的原像集合之间的关系.

习题1.1.3. 如果 $f : A \to B$, $g : B \to C$ 均是一一对应, 则 $g \circ f : A \to C$ 也是一一对应, 且 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

习题1.1.4. 设$P(A)$ 是集合 A 的全部子集所构成的集族, $M(A)$ 为所有A 到集合$\{0, 1\}$ 的映射构成的集合. 试构造$P(A)$ 到$M(A)$ 的双射. 特别地, 如 A 为有限集, 试证 $|P(A)| = 2^{|A|}$, 换言之, n 元集合共有 2^n 个子集.

习题1.1.5. 设 X 是无限集, Y 是X 的有限子集. 证明存在双射$X - Y \to X$.

习题1.1.6. 证明等价关系的三个条件是互相独立的, 也就是说, 已知任意两个条件不能推出第三个条件.

习题1.1.7. 设集合 A 中关系满足对称性和传递性, 且对 A 中任意元素都和某元素有关系, 证明此关系为等价关系.

习题1.1.8. 设 A, B 是两个有限集合.
(1) A 到 B 的不同映射共有多少个?
(2) A 上不同的二元运算共有多少个?

习题1.1.9. 证明容斥原理(命题 1.1).

§1.2 群的基本概念和例子

§1.2.1 群的定义和例子

我们首先给出群的定义.

定义1.15. 集合 G 及其上的二元运算 $\cdot$ 称为**群** (group), 如果它们满足下述三条公理:

(1) 结合律成立, 即对元素 $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(2) 存在**单位元** (identity element) $1 = 1_G$, 即对任意 $a \in G$,

$$a \cdot 1 = 1 \cdot a = a.$$

单位元也称为**幺元**.

(3) G 上每个元素 a 均有**逆元** (inverse), 即存在元素 $a^{-1} \in G$ 使得

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

称二元运算 $\cdot$ 为**群的乘法** (multiplication).

注记. (1) 习惯上, 我们常常省略乘法运算, 称 G 为群, 且记 $a \cdot b$ 为 ab.

(2) 如果 $(G, \cdot)$ 仅满足结合律, 我们称之为**半群** (semigroup); 如果 $(G, \cdot)$ 满足结合律且存在单位元, 我们称之为**含幺半群** (monoid).

本书中的很大篇幅, 从群论的定义开始, 到有限域的知识, 直至书的最后一章Galois理论, 都离不开200年前诞生的法国天才数学家埃瓦里斯特 · 伽罗瓦(Évariste Galois，1811年10月25日—1832年5月31日, 图 1.6) 的伟大工作. 伽罗瓦在不到21岁的生命里给数学留下了一笔辉煌的遗产. 他建立了抽象代数两大基本理论: 群论和以他命名的Galois 理论. 他的不朽理论是当代代数和数论研究的基本支柱, 是数学走向抽象化的标志. 在本书, 我们将使用他的工作, 证明一般n 次方程根式解不存在, 并回答古典几何两大难题, 即使用直尺和圆规三等分角和构造正多边形问题. 伽罗瓦的工作在生前不被世人承认, 直到1843 年才由刘维尔(Joseph Liouville) 检查并确认, 整理后于1846年在他创办的杂志Journal de Mathématiques Pures et Appliquées 出版.

图 1.6: 伽罗瓦像

例1.16. 由群的定义, 群 G 一定包含单位元 1_G. 另一方面, 仅由单位元构成的集合$\{1\}$ 在乘法运算$1 \cdot 1 = 1$ 下满足群的三个公理, 因此它构成群. 这是最简单的群.

命题1.17. 设 G 为群, 则下述性质成立:

(1) G 中元素的逆元唯一, 即元素a的逆a^{-1}是唯一确定的.

(2) **消去律**成立, 即: 如果 $ab = ac$, 则 $b = c$; 如果 $ba = ca$, 则 $b = c$.

证明. (1) 如果 b, c 为 $a \in G$ 的逆元, 则

$$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c.$$

(2) 如果 $ab = ac$, 则 $a^{-1}(ab) = a^{-1}(ac)$, 由结合律即得 $b = c$. □

定义1.18. 元素个数有限的群称为**有限群** (finite group), 其元素个数称为它的**阶** (order). 元素个数无限的群称为**无限群**(infinite group), 其阶记为∞.

定义1.19. 如果群 G 上的乘法运算满足交换律, 我们称 G 为**阿贝尔群** (abelian group), 亦称为**交换群** (commutative group). 我们常常用加法 $+$ 来表示阿贝尔群 G 的二元运算, 并将其上的单位元记为 0 或 0_G, 记 a 的逆元为 $-a$.

19世纪20年代的数学天空, 双星闪耀, 一位是伽罗瓦, 另外一位就是挪威数学家尼尔斯 · 阿贝尔(Niels Abel，1802年8月5日—1829年4月6日). 阿贝尔和伽罗瓦都是在年纪轻轻的时候做出了数学史上影响深远的工作, 又同样命途多舛, 英年早逝. 阿贝尔以证明五次方程的根式解的不可能性和对椭圆函数论的研究而闻名. 由于他发现方程的(伽罗瓦)群的交换性可以推出求根公式的存在性, 法国数学家Camille Jordan (若当标准型的发现者)将交换群命名为阿贝尔群. 为纪念阿贝尔, 挪威政府从2003年起开始颁发阿贝尔奖, 这是当今数学界的最高荣誉之一. 图 1.7 为挪威政府1978年发行以阿贝尔像为背景的500克朗钞票.

图 1.7: 挪威钞票上的阿贝尔像

我们首先给出阿贝尔群的一些例子.

例1.20. (1) 集合$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 在加法运算下构成无限阿贝尔群, 0 为其加法单位元.

(2) 集合$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$, $\mathbb{R}^\times = \mathbb{R} - \{0\}$, $\mathbb{C}^\times = \mathbb{C} - \{0\}$ 在乘法运算下构成阿贝尔群, 1 为其乘法单位元.

例1.21. 整数集 $\mathbb{Z}$ 模 n 的剩余类集合 $\{\bar{0} = 0 \mod n, \bar{1}, \cdots, \overline{n-1}\}$ 构成加法阿贝尔群, 我们记之为 $\mathbb{Z}/n\mathbb{Z}$. 今后如不特别说明, 在 $\mathbb{Z}/n\mathbb{Z}$ 中, 我们将移除$^-$, 将 $\bar{a}$ 直接记为a.

特别地, 如果 $n = p$ 是素数, 记 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 则 $\mathbb{F}_p$ 是加法阿贝尔群. 同时, $\mathbb{F}_p^\times = (\mathbb{F}_p - \{0\}, \times)$ 是乘法阿贝尔群, 这是因为根据整数的同余理论, 如果 $a \not\equiv 0 \mod p$, 则存在 $b \in \mathbb{Z}$, 使得 $ab \equiv 1 \mod p$.

注记. 在上述两个例子中, 我们实际上给出了**域**的几个常见例子: 有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$, 复数域 $\mathbb{C}$ 和有限域 $\mathbb{F}_p$. 它们的共同点都是: 本身是加法阿贝尔群, 而其中非零元集合又构成乘法阿贝尔群, 而且加法和乘法满足**分配律**, 即 $(a+b)c = ac + bc$ 对其中任何 3 个元素 a, b, c 均成立. 这些共同点将构成域的定义, 我们将在本书稍后详细阐述. 在此之前, 我们提到的域即是指上述 4 个例子.

例1.22. 令 $\zeta_n = \exp(\frac{2\pi i}{n}) = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, 则集合 $\mu_n = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ 是由复数域 $\mathbb{C}$ 上所有 n 次单位根构成的集合. 在复数乘法意义下, μ_n 是乘法阿贝尔群, 称为 n **次单位根群** (group of roots of unity).

更一般地, 单位圆 $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ 是无限乘法阿贝尔群.

我们再来看非交换群的例子.

例1.23 (**一般线性群**)**.** 设 V 是域 F 上的 n 维线性空间, 其中$F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 或 $\mathbb{F}_p$. 由线性代数可知, 取定 V 上的一组基, 则 V 上线性变换由它在这组基下的n 阶方阵唯一确定. 记

$$\mathrm{M}_n(F) = \{F\text{上}n\text{阶方阵}\},$$
$$\mathrm{GL}_n(F) = \{F\text{上}n\text{阶可逆方阵}\}.$$

则 $\mathrm{M}_n(F)$ 在矩阵加法意义下是阿贝尔群, 在乘法意义下是含幺半群, 但不是群. $\mathrm{GL}_n(F)$ 在矩阵乘法意义下构成群, 我们称之为F 上的n 阶**一般线性群** (general linear group). 如果 $n = 1$, 则 $\mathrm{GL}_n(F) = F^\times$, 即 F 的乘法群, 它是一个阿贝尔群; 如果 $n > 1$, 则 $\mathrm{GL}_n(F)$ 不是交换群. 今后如果不强调域 F, 我们记n 阶一般线性群为 GL_n.

例1.24 (**正四面体的旋转变换群**)**.** 考虑所有保持四面体$ABCD$ 不变的旋转变换（绕某一直线旋转轴旋转）, 这里有三种情况.

1. 有两个顶点不动, 则所在边不动为轴，剩下两个点也不可能动, 故为恒等变换.
2. 有且仅有一个顶点不动（参见图1.8）. 不妨设A 点不动, 则轴过A且BCD所在面不动，故轴垂直该平面，从而正三角形 BCD 的中心 O 也不动. 以AO 为轴的旋转变换通过旋转 $\frac{2\pi}{3}$ 或 $\frac{4\pi}{3}$ 将 B, C, D 旋转到 C, D, B 或 D, B, C, 共有两个变换. 若考虑一般情形, 将顶点 A 变动, 则共得到 $4 \times 2 = 8$ 种旋转变换.

3. 所有顶点都动(参见图1.9). 若 A 旋转到 B, 则轴在C，D和AB的中点决定的平面上（即垂直AB），故 B 不能旋转到 C 或 D（否则若B旋转到C则轴也在A，D和BC的中点决定的平面上，两个平面的交过D，从而D不动）即 B 必然旋转到 A. 因此 C 旋转到 D, D 旋转到 C. 即 AB 中点 M 与 CD 中点 N 连接的直线保持不动. 这样的情况共有 3 种.

若以变换复合作为乘法, 这12种正四面旋转变换的全体构成正四面体的旋转变换群, 恒等变换为其单位元. 可以验证第二类变换和第三类变换的复合不交换, 故正四面体的旋转变换群是12 阶非阿贝尔群.

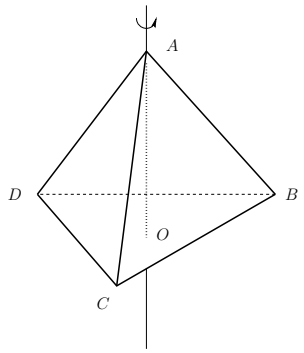


图 1.8: 恰有一个不动点的情形

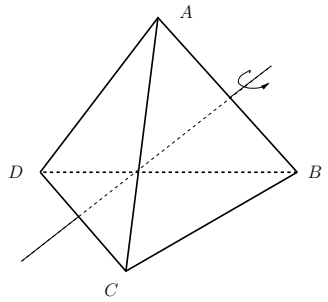


图 1.9: 所有顶点都动的情形

例1.25. 更一般地, 设 S 是一个刚体, 即不可压缩和拉伸的物体. 保持 S 不变的运动构成一个群, 称为 S 的**刚体运动群**. 一般而言它不是阿贝尔群.

例1.26 (**对称群**)**.** 设 A 为非空集合. 记 A 到自身的映射集合为 M_A. A 到自身的一一对应称为 A 的**置换** (permutation). 记A 的所有置换集合为 S_A. 则 M_A 在映射复合作为乘法意义下是含幺半群但不是群, 而 S_A 是群, 其单位元为恒等映射, 我们称 S_A 为 A 的**对称群** (symmetric group) 或**置换群** (permutation group).

特别地, 设 $A=\{1,2,\ldots,n\}$, 记 $S_A=S_n$, 则 S_n 为 $\{1,\ldots,n\}$ 所有置换构成的集合. 我们知道 S_n 中含有 $n!$ 个置换. 如果 $n=2$, 则 $S_2=\{\mathrm{id},\tau\}$, 其中 $\tau(1)=2,\tau(2)=1$. 容易验证 S_2 为阿贝尔群. 当 $n\geqslant 3$ 时, S_n 不是交换群.

例1.27. 我们来计算一下有限域 $\mathbb{F}_p$上的n阶一般线性群 $\mathrm{GL}_n(\mathbb{F}_p)$ 的阶.

如果 $A=(a_{ij})\in \mathrm{GL}_n(\mathbb{F}_p)$, 记$\alpha_i=(a_{ij})_{j=1}^n$ 为A 的第i个行向量. 则 $\alpha_1\neq 0$ 有p^n-1 种选择方式; α_2 不在α_1 生成的1维 $\mathbb{F}_p$ 向量空间中, 有p^n-p 种选择方式; 同理对 $2\leqslant i\leqslant n$, α_i 不在由$\alpha_1,\cdots,\alpha_{i-1}$ 生成的$i-1$ 维 $\mathbb{F}_p$ 向量空间中, 有p^n-p^{i-1} 种选择方式. 故A 共有 $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ 可能选择. 故 $\mathrm{GL}_n(\mathbb{F}_p)$ 是有限群, 阶为 $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

§1.2.2 子群和群的直积

有了群的概念和例子, 我们希望

(1) 研究群的结构,

(2) 构造更多的群的例子.

这时候, 需要子群与直积的概念.

定义1.28. 设 G 为群. 如果 H 是 G 的子集, 且对 G 的乘法运算构成群, 则称 H 是 G 的**子群** (subgroup), 记为 $H \leqslant G$. 如果 $H \neq G$, 称 H 为 G 的**真子群** (proper subgroup), 记为 $H < G$.

例1.29. 对任意群 G, $\{1\}$ 和 G 均是 G 的子群, 称为 G 的**平凡子群** (trivial subgroup).

例1.30. 加法群$n\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群. 乘法群μ_n 和 S^1 是 $\mathbb{C}^\times$ 的子群. $\{\pm 1\}$ 是 $\mathbb{R}^\times$ 的子群.

由定义可知, 要验证 H 为 G 的子群, 只需验证如下三点, 即
(1) $1 \in H$.
(2) 如果 $a \in H$, 则 $a^{-1} \in H$.
(3) 如果 $a, b \in H$, 则 $ab \in H$.

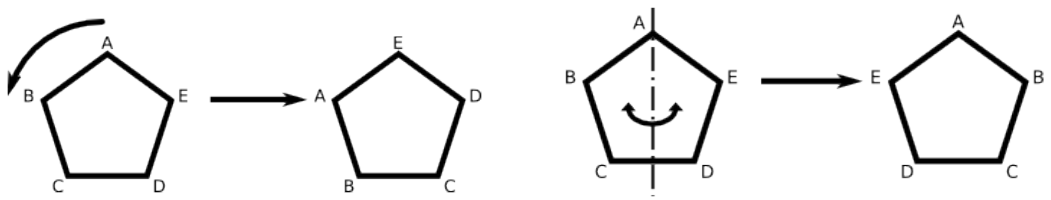
命题1.31. 非空子集合 H 是群 G 的子群当且仅当对任意 $a, b \in H, ab^{-1} \in H$.

证明. 如果 $H \leqslant G, a, b \in H$, 则 $b^{-1} \in H, ab^{-1} \in H$. 反过来, 取 $a \in H$, 则 $1 = aa^{-1} \in H$. 对任意$a \in H$, 由于$1, a \in H$, 则 $a^{-1} = 1 \cdot a^{-1} \in H$. 最后，对任意 $a, b \in H$, 有$b^{-1} \in H$, 从而 $ab = a(b^{-1})^{-1} \in H$. 故$H$ 是G 的子群. □

例1.32. 令$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{R} \right\}$, 则$H$ 是一般线性群$\mathrm{GL}_2(\mathbb{R})$ 的子群. 这是因为

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix}.$$

例1.33 (**二面体群**)**.** 设 P 是正 n 边形 ($n \geqslant 3$), 保持 P 不变的所有刚性变换有两种: 旋转和反射, 如图 1.10 所示.



(a) 旋转 (b) 反射

图 1.10: 正5边形的旋转和反射

记 D_n 为所有旋转和反射在复合意义下构成的群, 则 D_n 为正 n 边形的对称群, 称为**二面体群** (dihedral group). D_n 的所有元素包括: 恒等变换, $n-1$ 个旋转, n 个反射, 故为$2n$ 阶群.

由于保持正n 边形不变的每个刚性变换由它的n 个顶点的置换唯一确定, 故 二面体群D_n 是S_n 的子群.

注记. 二面体群在不同文献中被记为 D_n 或 D_{2n}. 习惯上, 几何学家喜欢用 D_n(强调正多边形的边数)来表示它, 而代数学家则喜欢用 D_{2n} (强调正多边形对称群的阶)来表示它. 在本书中我们采用几何学家的记号.

定义1.34. 设 G_1, G_2 为群, 则 G_1 与 G_2 (作为集合的) 的笛卡尔积 $G = G_1 \times G_2$ 在乘法运算

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

下构成群: 它的单位元是 $1_G = (1_{G_1}, 1_{G_2})$, 元素 (g_1, g_2) 的逆是 (g_1^{-1}, g_2^{-1}). 群 G 称为 G_1 与 G_2 的**直积** , 或者称为它们的**笛卡尔积**.

注记. (1) 由定义立知群的直积的阶等于群的阶的乘积.

(2) 如果 H_1 和 H_2 分别是 G_1 和 G_2 的子群, 则 $H_1 \times H_2$ 是 $G_1 \times G_2$ 的子群. 特别地, $G_1 \times G_2$ 有子群 $\{1_{G_1}\} \times G_2$ 和 $G_1 \times \{1_{G_2}\}$.

§1.2.3 GL_n 的子群: 典型群

在数学研究中, 最重要的一类群是一般线性群 GL_n 的子群, 称为**典型群** (classical group). 关于典型群的研究和应用贯穿于数学研究的各个学科分支. 由于一般线性群来自于线性代数, 线性代数知识在研究典型群的时候起着十分重要的作用. 我们下面介绍几类典型群.

(I) **特殊线性群**

设 F 为域, 则 F 上行列式为 1 的 n 阶方阵集合

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det A = 1\} \tag{1.8}$$

构成 $\mathrm{GL}_n(F)$ 的一个子群, 称为 F 上的 n 阶**特殊线性群** (special linear group). 另外, 我们令

(i) $T_n(F)$ 为对角线元全为 1 的 n 阶上三角阵;

(ii) $\mathrm{Diag}_n(F)$ 为 n 阶可逆对角阵集合;

(iii) $B_n(F)$ 为 n 阶可逆上三角阵集合.

则它们均为 $\mathrm{GL}_n(F)$ 的子群, 且 $T_n(F) \leqslant \mathrm{SL}_n(F)$, $\mathrm{Diag}_n(F) \leqslant B_n(F)$.

在 2 阶特殊线性群 $\mathrm{SL}_2(\mathbb{R})$ 中, 所有整系数矩阵构成子群 $\mathrm{SL}_2(\mathbb{Z})$, 即 $\mathbb{Z}$ **上的** 2 **阶特殊线性群**. 类似地, 设 N 为大于 1 的正整数. 我们仍然可以在系数在 $\mathbb{Z}/N\mathbb{Z}$ 上的 2 阶矩阵

上定义行列式, 其中行列式为 1 的矩阵的集合

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \,\middle|\, a,b,c,d \in \mathbb{Z}/N\mathbb{Z},\ ad-bc=1 \right\} \tag{1.9}$$

以矩阵乘法作为乘法, 就构成 $\mathbb{Z}/N\mathbb{Z}$ **上的 2 阶特殊线性群**. 同理, 当阶数 2 换成一般的 n 时, 我们就得到 $\mathbb{Z}$ 上和$\mathbb{Z}/N\mathbb{Z}$ 上的 n 阶特殊线性群.

(II) **正交群与特殊正交群**

在 $\mathbb{R}^n$ 上给定标准内积

$$\langle X, Y \rangle = X^T Y,$$

其中 ^{T}表示转置, 则 $\mathbb{R}^n$ 成为欧几里得空间. 方阵 A 称为**正交方阵**(orthogonal matrix) 或**正交阵**, 是指 A 保持 $\mathbb{R}^n$ 上的标准内积不变, 即对任意 $X, Y \in \mathbb{R}^n$,

$$\langle AX, AY \rangle = X^T A^T A Y = X^T Y,$$

亦即

$$A^T A = A A^T = I. \tag{1.10}$$

由此我们知道: (i) 单位矩阵是正交阵; (ii) 正交阵的乘积是正交阵; (iii) 正交阵的逆也是正交阵. 因此所有正交方阵的集合

$$\mathrm{O}_n(\mathbb{R}) := \{ A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T A = A^T A = I \} \tag{1.11}$$

构成一个群, 即 $\mathbb{R}$ 上的 n 阶**正交群** (orthogonal group). 更一般地, 设 Q 为 n 维实空间 V 上非退化对称双线性型. 由惯性定理, 存在 V 上一组基使得 Q 由如下形式给出:

$$Q(u,v) = X^T \left(\begin{smallmatrix} I_p & \\ & -I_q \end{smallmatrix} \right) Y \quad (p+q=n),$$

其中 X, Y 为向量 u, v 在此基下的坐标. 所有保持双线性型 Q 不变的可逆方阵的集合

$$\mathrm{O}_{p,q}(\mathbb{R}) := \left\{ A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T \left(\begin{smallmatrix} I_p & \\ & -I_q \end{smallmatrix} \right) A = \left(\begin{smallmatrix} I_p & \\ & -I_q \end{smallmatrix} \right) \right\} \tag{1.12}$$

也构成群, 称为**广义正交群** (generalized orthogonal group). 我们称

$$\mathrm{SO}_n(\mathbb{R}) := \mathrm{O}_n(R) \cap \mathrm{SL}_n(\mathbb{R}), \tag{1.13}$$

$$\mathrm{SO}_{p,q}(\mathbb{R}) := \mathrm{O}_{p,q}(R) \cap \mathrm{SL}_n(\mathbb{R}) \tag{1.14}$$

为**特殊正交群** (special orthogonal group) 和**广义特殊正交群** (generalized special orthogonal group).

例1.35. 当 $n = 2$ 时, 我们有

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \,\middle|\, \theta \in \mathbb{R} \right\},$$

$$\mathrm{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \pm\sin\theta & \pm\cos\theta \end{pmatrix} \,\middle|\, \theta \in \mathbb{R} \right\}.$$

更进一步地, 对一般的域 F, 设 Q 为域F 上 n 维线性空间 V 上的非退化对称双线性型, 我们可以类似定义 F 上保持双线性型 Q 不变的正交群和特殊正交群.

(III) **酉群和特殊酉群**

设 V 是 n 维复线性空间, Q 是 V 上非退化Hermite 双线性型, 则存在 V 的一组基, 使得 Q 在此基下可表示如下:

$$Q(u,v) = Q(X,Y) = \overline{X}^T Y.$$

方阵 A 称为**酉阵** (unitary matrix) 是指它保持 Q 不变, 即 A 满足

$$\overline{A}^T A = A\overline{A}^T = I. \tag{1.15}$$

由此我们知道: (i) 单位矩阵是酉阵; (ii) 酉阵的乘积是酉阵; (iii) 酉阵的逆也是酉阵. 因此

$$\mathrm{U}(n) := \{A \mid \overline{A}^T A = A\overline{A}^T = I\} \tag{1.16}$$

是 $\mathrm{GL}_n(\mathbb{C})$ 的一个子群, 称为**酉群** (unitary group). 它的子群

$$\mathrm{SU}(n) = U(n) \cap \mathrm{SL}_n(\mathbb{C}), \tag{1.17}$$

称为**特殊酉群** (special unitary group).

例1.36. 当 $n=1$ 时, $\mathrm{U}(1) = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, $\mathrm{SU}(1) = \{1\}$.

当 $n=2$ 时,

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

(IV) **辛群**

设 V 是实线性空间, $Q(x,y)$ 是 V 上的非退化反对称双线性型. 由 Q 的非退化性, 我们知 $\dim V = 2n$ 为偶数, 且存在 V 的一组基使得

$$Q(u,v) = X^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} Y,$$

其中 X, Y 为 u, v 在基下的坐标. 所有保持 Q 不变的方阵的集合, 即为群

$$\mathrm{Sp}_{2n}(\mathbb{R}) = \left\{ A \mid A^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \right\}, \tag{1.18}$$

称为**辛群** (symplectic group).

注记. 如果 $A \in \mathrm{Sp}_{2n}(\mathbb{R})$, 可以证明 $\det A = 1$, 故没有特殊辛群的说法.

§1.2.4 群的同态与同构

研究群的性质, 离不开研究群与其它群的关系, 这些关系如同研究集合间的关系一样, 是由群之间的映射来决定的. 但必须注意到, 群不仅是集合, 它上面有乘法运算, 故群与群之间的映射应该保持乘法运算. 我们有如下的定义.

定义1.37. 设 G_1 与 G_2 为群, 映射 $f: G_1 \to G_2$ 称为**群同态** (homomorphism) 是指对任意 $g, h \in G_1$,

$$f(gh) = f(g)f(h).$$

(注意到上式左边 $g \cdot h$ 是群 G_1 中的乘法运算, 右边 $f(g) \cdot f(h)$ 是 G_2 中的乘法运算.)

如 f 作为集合映射为单射, 称 f 为**单同态** (monomorphism). 如 f 为满射(epimorphism), 称 f 为**满同态**. 如 f 为双射, 则称 f 为**同构** (isomorphism), 记为 $f: G_1 \cong G_2$.

命题1.38. 设$f: G_1 \to G_2$ 为群同态, 则

(1) 群同态总是将单位映到单位, 即$f(1_{G_1}) = 1_{G_2}$.

(2) 群同态总是将逆元映到逆元, 即对于$g \in G_1$, $f(g^{-1}) = f(g)^{-1}$.

证明. 由$f(1_{G_1}) = f(1_{G_1} \cdot 1_{G_1}) = f(1_{G_1}) \cdot f(1_{G_1})$, 再由消去律即得(1).

若$g \in G_1$, 则

$$f(g) \cdot f(g^{-1}) = f(g \cdot g^{-1}) = f(1_{G_1}) = 1_{G_2},$$

故 $f(g^{-1}) = f(g)^{-1}$, (2) 得证. □

我们来看一些群同态和同构的例子.

例1.39. 如果H 是G 的子群, 则包含映射$i: H \to G$, $h \mapsto h$ 为群同态, 且是单同态.

例1.40. 行列式映射 $\det: \mathrm{GL}_n(F) \to F^\times$, $A \mapsto \det A$ 是群的满同态.

例1.41. 我们定义 $\varphi: \mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{m} = m \mod n \mapsto \zeta_n^m$, 则 φ 是群同构.

例1.42. 对于 $\sigma \in S_n$, 我们定义 $A_\sigma \in \mathrm{GL}_n$ 如下

$$A_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix},$$

则 $A_\sigma = (a_{ij})$ 为 $(0,1)$ 矩阵, 且

$$a_{ij} = \begin{cases} 1 & \text{若} j = \sigma^{-1}(i), \\ 0 & \text{若不然.} \end{cases}$$

映射 $\sigma \mapsto A_\sigma$ 为 S_n 到 GL_n 的单同态. 由此我们可以视对称群 S_n 为一般线性群 GL_n 的子群, A_σ 也称为**置换矩阵**.

例1.43. 酉群$S^1 = \mathrm{U}(1)$ 和特殊正交群 $\mathrm{SO}_2(\mathbb{R})$ 同构, 同构映射为

$$e^{2\pi i\theta} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

例1.44. 设$\mathbb{R}_+^\times$ 为所有正实数构成的乘法群, 则指数函数

$$\exp:\ \mathbb{R} \to \mathbb{R}_+^\times, \quad x \mapsto e^x$$

是群同构. 其逆为对数函数

$$\log = \ln:\ \mathbb{R}_+^\times \to \mathbb{R},\ y \mapsto \ln y.$$

在群论研究中, 经常将同构视为相同, 或者说在同构意义下一样. 另一方面, 也会研究同构群之间可以构造多少种同构. 我们有

定义1.45. 群 G 到自身的同构称为 G 的**自同构** (automorphism).

命题1.46. (1) 群 G 的所有自同构在复合映射作为乘法意义下构成群, 称为 G 的**自同构群**, 记为 $\mathrm{Aut}G$.

(2) 如 $\varphi : G \to H$ 为群 G 到群 H 的同构. 则 G 到 H 的所有同构为集合 $\varphi\mathrm{Aut}G = \{\varphi \circ f \mid f \in \mathrm{Aut}G\}$.

证明. (1) 只需验证群的定义3公理即可, 而这些都是显然的.

(2) 首先, $\varphi \circ f : G \xrightarrow{f} G \xrightarrow{\varphi} H$ 为 G 到 H 的同构. 另一方面, 如 φ' 为 $G \to H$ 的同构, 则 $\varphi^{-1} \circ \varphi' : G \to H \to G$ 为 G 的自同构. 故 $\varphi' = \varphi \circ (\varphi^{-1} \circ \varphi') \in \varphi\mathrm{Aut}G$. □

习 题

习题1.2.1. 令 A 是任意非空集合, G 是群, $\mathrm{Map}(A, G)$ 是 A 到 G 的所有映射的集合, 对任意两个映射 $f, g \in \mathrm{Map}(A, G)$, 定义乘积 fg 是这样的映射: 对任意 $\alpha \in A$, $fg(\alpha) = f(\alpha)g(\alpha)$. 试证 $\mathrm{Map}(A, G)$ 是群.

习题1.2.2. 设A 为集合, $P(A)$ 为A 的子集构成的集合族. 在$P(A)$ 上定义二元运算如下:

$$X \triangle Y = (X \cap Y^c) \cup (X^c \cap Y).$$

证明在此运算下$P(A)$ 构成交换群, 且每个子集的逆即自身.

习题1.2.3. 从平面到自身的映射如果保持平面上任何两点的距离, 则称为**保距映射**. 证明保距映射都是双射, 且所有保距映射在函数复合意义下构成群.

习题1.2.4. 设G 是群, $x, y \in G$. 证明: $(x^{-1})^{-1} = x$ 且 $(xy)^{-1} = y^{-1}x^{-1}$.

习题1.2.5. 判断下面哪些2 阶方阵集合在矩阵乘法意义下构成群:

(1) $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$, $ac \neq b^2$.

(2) $\left(\begin{smallmatrix} a & b \\ c & a \end{smallmatrix}\right)$, $a^2 \neq bc$.

(3) $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$, $ac \neq 0$.

(4) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $a, b, c, d \in \mathbb{Z}$, $ad \neq bc$.

习题1.2.6. 证明集合$\bigcup_{n\geq 1} \mu_n$ 在复数乘法意义下构成群.

习题1.2.7. 如果 A 是群 G 的子群, B 是群 H 的子群, 证明$A \times B$ 是$G \times H$ 的子群. 举例说明不是所有 $\mathbb{Z} \times \mathbb{Z}$ 的子群都是如此得到的.

习题1.2.8. 设 $(G, \cdot)$ 是群. 证明 $G^{\mathrm{op}} = (G, \circ)$, $a \circ b = b \cdot a$ 是群, 称为 G 的**反群**.

习题1.2.9. 设 G 是含幺半群, 证明 G 中的可逆元集合 $G^\times$ 构成群.

习题1.2.10. 令 G 是 n 阶有限群, $a_1, a_2, \ldots, a_n$ 是群 G 的任意 n 个元素, 不一定两两不同. 试证: 存在整数 p 和 q, $1 \leqslant p \leqslant q \leqslant n$, 使得

$$a_p a_{p+1} \cdots a_q = 1.$$

习题1.2.11. 设 A, B, H 是群 G 的子群, 且 $H \subseteq A \cup B$. 证明 $H \subseteq A$ 或者 $H \subseteq B$.

习题1.2.12. 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

习题1.2.13. (1) 验证 $\mathrm{SL}_n(F)$, $T_n(F)$, $\mathrm{Diag}_n(F)$, $B_n(F)$ 均为 $\mathrm{GL}_n(F)$ 的子群, 且 $T_n(F) \leqslant \mathrm{SL}_n(F)$, $\mathrm{Diag}_n(F) \leqslant B_n(F)$.

(2) 验证 $\mathrm{O}_n(\mathbb{R})$, $\mathrm{O}_{p,q}(\mathbb{R})$, $\mathrm{Sp}_{2n}(\mathbb{R})$ 均为 $\mathrm{GL}_n(\mathbb{R})$ 的子群.

(3) 验证 $\mathrm{U}(n)$ 是 $\mathrm{GL}_n(\mathbb{C})$ 的子群.

习题1.2.14. 试证群 G 的任意多个子群的交仍是 G 的子群.

习题1.2.15. 设 A 和 B 分别是群 G 的两个子群. 试证: $A \cup B$ 是 G 的子群当且仅当 $A \leqslant B$ 或 $B \leqslant A$. 利用这个事实证明: 群 G 不能表为两个真子群的并.

习题1.2.16. 设 A, B 是群 G 的两个子群. 试证 AB 是 G 的子群当且仅当 $AB = BA$.

习题1.2.17. 设 A 和 B 是有限群 G 的两个非空子集. 若 $|A| + |B| > |G|$, 证明 $G = AB$. 特别地, 如果 S 是 G 的一个子集, $|S| > |G|/2$. 证明对任意 $g \in G$, 存在 $a, b \in S$ 使得 $g = ab$.

习题1.2.18. (1) 确定 $\mathbb{Z}$ 的所有子群.

(2) 确定 $\mathbb{Z}/n\mathbb{Z}$ 的所有子群, 其中 $n \in \mathbb{N}, n \geqslant 2$.

习题1.2.19. 证明: 映射 $f : G \to G$, $a \mapsto a^{-1}$ 是 G 的自同构当且仅当 G 是阿贝尔群.

习题1.2.20. 设 G_1, G_2, G_3 为群, 证明:

(1) $G_1 \times G_2 \cong G_2 \times G_1$;

(2) $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

习题1.2.21. 对下面每一情形, 确定 G 是否同构于 H 和 K 的积.

(1) $G = \mathbb{R}^\times,\ H = \{\pm 1\},\ K = \mathbb{R}_+^\times$.

(2) $G = B_n(F),\ H = \mathrm{Diag}_n(F),\ K = T_n(F)$.

(3) $G = \mathbb{C}^\times,\ H = S^1,\ K = \mathbb{R}_+^\times$.

习题1.2.22. 证明有理数加法群 $\mathbb{Q}$ 和乘法群 $\mathbb{Q}^\times$ 不同构.

习题1.2.23. (1) 令 G 是实数对 $(a,b), a \neq 0$ 的集合. 在 G 上定义

$$(a,b)(c,d) = (ac, ad+b).$$

试证 G 是群.

(2) 证明 G 同构于 $\mathrm{GL}_2(\mathbb{R})$ 的子群

$$H = \left\{ \left(\begin{smallmatrix} a & b \\ & 1 \end{smallmatrix}\right) \mid a \in \mathbb{R}^\times, b \in \mathbb{R} \right\}$$

习题1.2.24. 群 G 的自同构 α 称为没有不动点, 是指对 G 的任意元素 $g \neq 1$, $\alpha(g) \neq g$. 如果有限群 G 具有一个没有不动点的自同构 α 且 $\alpha^2 = 1$, 证明 G 一定是奇数阶阿贝尔群.

§1.3 子群与陪集分解

在上一节我们给出了子群的定义及一些具体例子. 在本节, 我们假设 G 为任意(抽象)群, 我们来研究它的子群与它自身的关系.

§1.3.1 元素的阶与循环群

定义1.47. 设 G 是群, g 是 G 中的元素, 由 g **生成的子群**是指包含 g 的最小子群. 我们用 $\langle g \rangle$ 来表示它. 同样, 如 $S \subseteq G$ 为 G 的子集合, 则由 S 中元素生成的子群称为 S **生成的子群**, 记为 $\langle S \rangle$.

我们首先讨论 $\langle g \rangle$ 中的元素, 由群的公理, 它必包含

(i) $g^k = g \cdots g$, k 个 g 相乘.

(ii) 单位元$1 = g^0$.

(iii) $g^{-k} = g^{-1} \cdots g^{-1}$, k 个 g^{-1} 相乘.

另一方面, 由(i),(ii),(iii)中的所有元素构成的集合的确是 G 的子群. 故

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\},\ \text{此处 } g^k \text{ 可能相同.}$$

定义1.48. 群 G 中元素 g 的**阶**是指满足 $g^k = 1$ 的最小正整数, 此时称 g 为 k **阶有限元**. 如这样的 k 不存在, 称 g 的阶为无穷大, 此时称 g 为**无限阶元**.

引理1.49. (1) 如 g 为 k 阶有限元, 则 $g^n = 1$ 当且仅当 $n \equiv 0 \mod k$, $g^i = g^j$ 当且仅当 $i \equiv j \mod k$. 此时, g 生成的子群 $\langle g\rangle = \{1, g, \ldots, g^{k-1}\}$ 是k 阶有限群.

(2) 如 g 为无限元, 则对于任意整数$i \neq j$, 均有 $g^i \neq g^j$.

证明. (1) 如 g 为 k 阶有限元, 设 $n = kq + r$, $0 \leq r < k$. 如 $r \neq 0$, 则 $g^r \neq 1$. 故

$$g^n = g^{kq+r} = (g^k)^q \cdot g^r = g^r \neq 1.$$

如 $r = 0$, 则 $g^n = g^{kq} = 1$. 综上即证明了 $g^n = 1$ 当且仅当 $n \equiv 0 \mod k$. 由于 $g^i = g^j$ 当且仅当 $g^{i-j} = 1$, 故也等价于 $i \equiv j \mod k$. 由于对任意 n, $n = kq + r$, $g^n = g^r$, 而1, g, $\cdots$, g^{k-1} 两两不同, 故 $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\} = \{1, g, \ldots, g^{k-1}\}$.

(2) 当 g 为无限阶元时, $g^i = g^j \Longleftrightarrow g^{i-j} = 1 \Leftrightarrow i - j = 0$, 即 $i = j$. □

定义1.50. 如 $G = \langle S\rangle$, 称 G 由 S 生成. 此时如 S 为有限集, 称 G 为**有限生成群** (finitely generated). 特别地, 如 G 由一个元素 g 生成, 称 G 为**循环群** (cyclic group), g 为 G 的一个**生成元** (generator).

由定义知循环群必是阿贝尔群. 更进一步地, 我们有

定理1.51. 设 G 为循环群.

(1) 如 G 为有限群, 其阶为 n, 则 $G \cong \mathbb{Z}/n\mathbb{Z}$.

(2) 如 G 为无限群, 则 $G \cong \mathbb{Z}$.

证明. 设 g 为 G 的生成元. 定义

$$\varphi : \mathbb{Z} \to G,\ k \mapsto g^k.$$

易知 φ 为满同态.

当 G 为无限群时, 由引理 1.49, 如 $i \neq j$, 则 $g^i \neq g^j$, 故 φ 为单同态. 因此 φ 为同构.

当 G 为 n 阶有限群时, φ 诱导同态 $\mathbb{Z}/n\mathbb{Z} \to G$, $k \mod n \mapsto g^k$. 由引理 1.49, 此同态既单又满, 故为同构. □

定理1.52. 设 G 为循环群, g 为 G 的生成元, 则

(1) 如 G 为无限群, 则 G 的生成元为 g 或 g^{-1}.

(2) 如 G 为 n 阶有限群, 则 G 的生成元集合为

$$\{g^k \mid 0 \leq k < n, (k, n) = 1\}.$$

(3) G 的自同构群

$$\mathrm{Aut}G \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{如 } G \text{ 为无限群;} \\ (\mathbb{Z}/n\mathbb{Z})^\times, & \text{如 } G \text{ 为 } n \text{ 阶有限群,} \end{cases}$$

且 G 的每个自同构将生成元映为生成元.

证明. (1)和(2): 元素$h=g^a$ 是 G 的生成元当且仅当 $g=h^b$ 对某个 $b\in\mathbb{Z}$ 成立. 故 $g^{ab}=g$. 如 G 为无限群, 则 $ab=1$, 故 $a=\pm1$, 即 $h=g$ 或 g^{-1}. 如果 G 的阶为 n, 则 $ab\equiv 1 \mod n$, 所以 $(a,n)=1$.

(3): 如 $f:G\to G$ 为自同构, g 为生成元, 则 $G=\{f(g^k)=f(g)^k \mid k\in\mathbb{Z}\}$, 故 $f(g)$ 也是G 的生成元. 我们定义映射 φ 如下:

(i) 如 G 为无限群,

$$\varphi:\mathrm{Aut}G\to\{\pm1\},\quad f\mapsto\begin{cases}1, & \text{如 } f(g)=g;\\ -1, & \text{如 } f(g)=g^{-1}.\end{cases}$$

(ii) 如 G 的阶为n,

$$\varphi:\mathrm{Aut}G\to(\mathbb{Z}/n\mathbb{Z})^\times,\quad f\mapsto a \mod n \text{ 如 } f(g)=g^a.$$

则 φ 既单又满, 且 $\varphi(f_1f_2)=\varphi(f_1)\cdot\varphi(f_2)$, 即 φ 为群同构. □

以下我们设 G 是 n 阶循环群. 固定它的一个生成元 g. 则对于任何元素 $a\in G$, 存在整数 k 使得 $a=g^k$, 且所有满足条件的 k 构成模 n 的一个同余类. 我们定义

$$\log_g:\ G\to Z/n\mathbb{Z},\quad a\mapsto k, \tag{1.19}$$

这是循环群之间的同构, 即有

$$\log_g 1=0,\quad \log_g(ab)=\log_g a+\log_g b. \tag{1.20}$$

我们称 $k=\log_g a$ 为 a 关于 g 的**离散对数** (discrete logarithm). 数学在信息安全领域的应用中最重要的一个核心问题就是

问题1.53 (离散对数问题)**.** 已知循环群 G的阶和生成元 g. 对元素 $a\in G$, 如何求 a 关于 g 的离散对数?

命题1.54. 设G 为n 阶循环群, g 是G 的一个生成元, $a\in G$. 则方程$x^k=a$ 在G 中有解当且仅当$d=(k,n)\mid\log_g a$. 且当此条件成立时, 方程共有d 个解.

证明. 设$x=g^y$. 则方程$x^k=a$ 有解等价于存在y, 使得$g^{ky}=g^{\log_g a}$, 即$ky\equiv\log_g a \mod n$ 有解. 根据整数同余理论即知, 方程$x^k=a$ 在G 中有解当且仅当$d=(k,n)\mid\log_g a$.

当$d\mid\log_g a$ 时. 同余方程$ky\equiv\log_g a \mod n$ 的解为$y\equiv\frac{\log_g a}{d}c \mod \frac{n}{d}$, 其中$c$ 为$\frac{k}{d}$ 模$\frac{n}{d}$ 的逆, 故$x^k=a$ 有d 个解g^y, 其中$y=\frac{c\log_g a+in}{d}$ $(0\le i<d)$. □

§1.3.2 陪集和陪集分解

设 H 是群 G 的子群.

定义1.55. 对于 $a \in G$, 集合 $aH = \{ah \mid h \in H\}$ 称为 G 关于 H 的**左陪集** (left coset), $Ha = \{ha \mid h \in H\}$ 称为 G 关于 H 的**右陪集** (right coset).

引理1.56. 陪集 aH 与 bH 要么不交, 要么重合, 且 $aH = bH$ 当且仅当 $b^{-1}a \in H$ (或 $a^{-1}b \in H$). 同理 Ha 与 Hb 要么不交, 要么重合, 且 $Ha = Hb$ 当且仅当 ab^{-1} 或 $ba^{-1} \in H$.

证明. 如 $aH \cap bH \neq \varnothing$. 令 $ah_1 = bh_2$, 则 $b^{-1}a = h_2h_1^{-1} \in H$. 此时

$$ah = ah_1(h_1^{-1}h) = bh_2(h_1^{-1}h) \in bH,$$

$$bh = bh_2(h_2^{-1}h) = ah_1(h_2^{-1}h) \in aH,$$

故 $aH = bH$. 另外, 若$b^{-1}a \in H$则对任意$h \in H$有$ah = b(b^{-1}a)h \in bH$, 也就是$aH \subseteq bH$. 类似有$bH \subseteq aH$. 从而$b^{-1}a \in H \Longrightarrow aH = bH$. 同理可得右陪集情形. □

由引理 1.56, 设 $\{a_iH \mid i \in I\}$ 为 G 关于 H 的所有左陪集构成的集合, 即a_iH 过所有G关于H 的左陪集, 且两两不交. 则

$$G = \bigsqcup_{i \in I} a_iH \tag{1.21}$$

为 G 的一个分拆.

定义1.57. 集合 $\{a_i \mid i \in I\}$ 称为 G 的一个**左陪集代表元系** (left coset representatives).

同理, 如 $\{Hb_j \mid j \in J\}$ 为 G 关于 H 的所有右陪集构成的集合, 则 $\{b_j \mid j \in J\}$ 称为 G 的一个**右陪集代表元系**(right coset representatives). 注意到, $\{b_j \mid j \in J\}$ 为右陪集代表元系当且仅当

$$G = \bigsqcup_{j \in J} Hb_j \tag{1.22}$$

为 G 的分拆.

引理1.58. 如果 $\{a_i \mid i \in I\}$ 是 G 关于 H 的右(左)陪集代表元系, 则 $\{a_i^{-1} \mid i \in I\}$ 是 G 关于 H 的左(右)陪集代表元系. 特别地, 如 G 关于 H 的左或右陪集代表元系有限, 则左、右陪集代表元系均有限, 且阶数相同.

证明. 因为作为集合

$$(aH)^{-1} = \{(ah)^{-1} \mid h \in H\} = \{h^{-1}a^{-1} \mid h \in H\} = Ha^{-1}.$$

故引理得证. □

定义1.59. 群 G 关于子群 H 的**指数** (index), 记为$(G:H)$, 是指 G 关于 H 的陪集代表元的个数. 如陪集代表元个数无限, 我们规定 $(G:H)$ 等于 ∞.

定理1.60 (拉格朗日定理)**.** 如 G 为有限群, 则

$$|G| = |H| \cdot (G:H) \tag{1.23}$$

注记. 如果规定 $\infty \cdot$ 正整数 $= \infty \cdot \infty = \infty$, 则 G 为无限群时(1.23)也成立.

证明. 由(1.21), 我们有

$$|G| = \sum_{i\in I} |a_i H| = \sum_{i\in I} |H| = |H| \cdot |I| = |H| \cdot (G:H).$$

定理得证. □

约瑟夫-路易 · 拉格朗日(Joseph-Louis Lagrange，1736年1月25 日—1813年4月10日) 是法国籍意大利裔数学家和天文学家, 在数学, 物理和天文等多个领域做出了重大贡献, 他的成就包括我们熟知的微积分拉格朗日中值定理. 在文章 Réflexions sur la résolution algébrique des équations 中, 拉格朗日说明如果将 n 元多项式的 n 个变量用所有 $n!$ 个置换作用, 得到的多项式个数总是 $n!$ 的因子. 这个数实际上就是多项式的稳定子群 H 在对称群 S_n 的指数, 即陪集分解的个数. 这就是拉格朗日定理的起源. 附图1.11是巴黎先贤祠(Pantheon) 中拉格朗日墓.

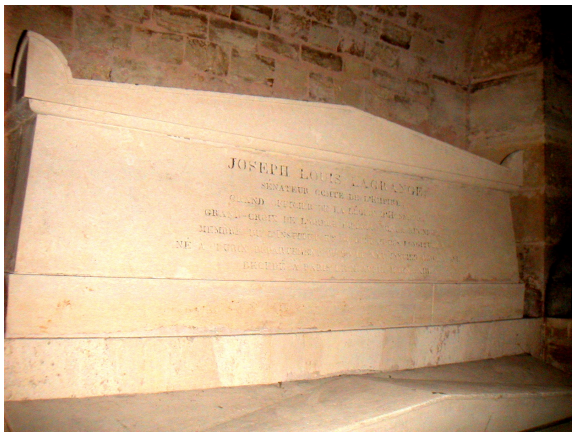


图 1.11: 拉格朗日之墓

拉格朗日定理是群论中第一个重要定理, 它有很多重要推论.

推论1.61. 设 G 为有限群, $x \in G$, 则 $x^{|G|} = 1$, 即元素 x 的阶总是群 G 的阶的因子.

证明. 这是由于元素x 的阶等于子群$\langle x\rangle$ 的阶. □

推论1.62. 素数阶群均是循环群.

证明. 设 $g \neq 1$, $g \in G$, 则 g 的阶必为 p. 故 $G = \{1, g, \ldots, g^{p-1}\} \cong \mathbb{Z}/p\mathbb{Z}$. □

推论1.63 (费马小定理)**.** 设 p 是素数, 则对所有与 p 互素的整数 a,

$$a^{p-1} \equiv 1 \mod p.$$

证明. 这是由于 $a \in \mathbb{F}_p^\times$ 的阶整除群$\mathbb{F}_p^\times$ 的阶 $p-1$. □

皮埃尔 · 德 · 费马(Pierre de Fermat, 1601年8月17日— 1665 年1月12日), 是最伟大的业余数学家, 他对数论, 微积分, 解析几何和概率论的建立都做出卓越贡献. 在数论上费马大定理众所周知, 但费马小定理则有更多实际应用. 用群论的观点而言, 费马小定理及其推广形式欧拉定理都是拉格朗日定理的推论. 在费马的墓碑(图 1.12) 上, 刻着如下文字: “在此处于1665年1月13日安葬了皮埃尔 · 德 · 费马, Edit市议会议员和杰出数学家, 因他的定理 $a^n + b^n \neq c^n$ $(n > 2)$ 而闻名于世. ”

图 1.12: 费马的墓碑

推论1.64. 设 G 为 n 阶循环群, 则对n的正因子d, G 中有唯一 d 阶子群 $\{1, x^{\frac{n}{d}}, \ldots, x^{\frac{n}{d}(d-1)}\}$, 其中 x 为 G 的生成元. 此子群也是循环群.

证明. 首先易验证 $\{1, x^{\frac{n}{d}}, \ldots, x^{\frac{n}{d}(d-1)}\}$ 是 G 的 d 阶循环子群. 另一方面, 设 H 是G 的 d 阶子群, $y \in H$. 记 $y = x^a$, 由于 y 的阶数整除 d, 故 $y^d = x^{ad} = 1$. 所以 $ad = kn$, $y = x^{\frac{n}{d}k}$. □

推论1.65. 对于任意正整数 n, 有下列恒等式:

$$n = \sum_{1 \le d | n} \varphi(d). \tag{1.24}$$

证明. 我们对 n 阶循环群G的元素按阶分类, 对于n的因子d, 我们只要说明阶为 d 的元素个数为$\varphi(d)$. 由元素阶的定义可知任何d阶元都生成一个d阶循环群, 也就是该d阶元素属于G的某个d阶子群, 再由上述推论可知循环群G中有唯一的d阶子群而且为循环群, 从而群G中d阶元的个数为一个d阶循环群中d阶元的个数, 也就是d阶循环群生成元的个数, 恰好为$\varphi(d)$. 故 $n = \sum_{d|n} \varphi(d)$. □

菲利克斯 · 克莱因(Felix Klein, 1849年4月25日– 1925 年6月22日, 图 1.13)以恢复了哥廷根在世界数学的统治地位而闻名于世, 他将哥廷根大学建设成为19世纪末到上个世纪30年代世界数学的中心. 但毋庸置疑, 他1872年发表的爱尔兰根纲领(Erlangen Program) 对于数学研究的影响尤其深远, 其中克莱因开创性的思想是: 几何学分类由它的变换群决定. 从此以后对称群的思想走进几何和物理研究的前沿. 值得说明的是, 100年后领导数学研究前沿的朗兰兹纲领(Langlands Program) 也离不开克莱因与庞加莱对于模函数和自守函数的开创性工作.

图 1.13: 克莱因像

引理1.66. 如果群 G 中任何元素 x 的阶为 1 或者 2, 则 G 为阿贝尔群.

证明. 由于 x 的阶为 1 或 2, 则 $x = x^{-1}$, 故对 $a, b \in G$,

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba,$$

因此 G 为阿贝尔群. □

例1.67. 我们来讨论一下 4 阶群 G 的情况. 如果 G 中包含 4 阶元, 则必为循环群. 否则它的元素的阶均是 1 或者 2, 故它是阿贝尔群, 故必为 $\{1, a, b, ab\}$ 的形式, 其中 $a^2 = b^2 = 1$ 且 $ab = ba$. 则 G 与 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 通过映射 $a \mapsto (1, 0)$, $b \mapsto (0, 1)$ 同构. 我们记 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = K_2$, 称为 **Klein 群**.

定理1.68. 非阿贝尔群的最小阶数为 6.

证明. 如果 G 的阶为 $2, 3, 5$, 即为素数, 故由推论 1.62, G 为阿贝尔群. 如 G 的阶是4, 上面例子说明 G 为阿贝尔群. 我们知道 S_3 的阶为 6 且它不是阿贝尔群. 综上所述,非阿贝尔群的最小阶数为 6. □

由于Lagrange 定理只是 G 关于 H 的陪集分解的一个推论, 直接使用陪集分解公式

$$G = \bigsqcup_{i \in I} g_i H, \tag{1.25}$$

我们有更进一步的应用.

定理1.69. 设群 $K \leqslant H \leqslant G$, 且 $(G : K)$ 有限, 则

$$(G : K) = (G : H) \cdot (H : K).$$

注记. Lagrange 定理, 即为上述定理在 $K = \{1\}$, G 为有限群的特殊情形.

证明. 设G 关于H 以及H 关于K 的左陪集分解分别为

$$G = \bigsqcup_{i \in I} g_i H, \qquad H = \bigsqcup_{j \in J} h_j K.$$

则

$$G = \bigcup_{(i,j) \in I \times J} g_i h_j K.$$

更进一步, 如果 $g_i h_j K = g_{i'} h_{j'} K$, 则 $g_i H \cap g_{i'} H \neq \emptyset$, 所以 $i = i'$, 故 $h_j K = h_{j'} K$, 所以 $j = j'$. 即

$$G = \bigsqcup_{(i,j) \in I \times J} g_i h_j K,$$

为不交并, 故 $\{g_i h_j : i \in I, j \in J\}$ 为 G 关于 K 的左陪集代表元系, 所以

$$(G : K) = (G : H) \cdot (H : K).$$

定理得证. □

定理1.70. 设 G 为有限群, H 与 K 为 G 的子群, 则

(1) $|H|\cdot|K| = |HK|\cdot|H\cap K|$.

(2) $(G:H\cap K) \leqslant (G:H)(G:K)$, 且等号成立当且仅当$HK = G$. 如果 $(G:H)$ 与 $(G:K)$ 互素, 则等号成立.

证明. 首先假设(1)成立来证明(2). 注意到(2) 中的不等式等价于 $|H\cap K|\cdot|G| \geq |H|\cdot|K|$. 由于 $|HK| \leq |G|$, 由(1), 不等式立证, 且等号成立当且仅当 $|HK| = |G|$, 即 $HK = G$. 由于 $(G:H)$ 与 $(G:K)$ 均是 $(G:H\cap K)$ 的因子, 如果它们互素, 则等号必成立.

对于(1), 设 $H\cap K = L$, 令 $\{x_i \mid i = 1,\cdots,m\}$ 为 H 关于 L 的左陪集代表元系, $\{y_j \mid j = 1,\cdots,n\}$ 为 K 关于 L 的右陪集代表元系, 则

$$HK = \left(\bigcup_{i=1}^{m} x_iL\right)\cdot\left(\bigcup_{j=1}^{n} Ly_j\right) = \bigcup_{i,j} x_iLy_j.$$

我们只需证明上述陪集两两不交即可. 如果$x, x' \in \{x_1,\ldots,x_m\}$以及$y, y' \in \{y_1,\ldots,y_n\}$, 有$xLy\cap x'Ly' \neq \emptyset$, 则存在 $\alpha,\beta \in L$, $(x')^{-1}x\alpha = \beta y'y^{-1}$, 故 $(x')^{-1}x \in K$ 且 $y'y^{-1} \in H$. 从而

$$K \ni (x')^{-1}x\alpha = \beta y'y^{-1} \in H.$$

因此 $(x')^{-1}x \in L$ 且 $y'y^{-1} \in L$, 由陪集代表元系即知 $x = x'$ 且 $y = y'$. □

习 题

习题1.3.1. 设

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

试求A, B, AB 和BA 在$\mathrm{GL}_2(\mathbb{R})$ 中的阶.

习题1.3.2. 证明群中元素a 的阶≤ 2 当且仅当$a = a^{-1}$.

习题1.3.3. 设a, b是群G的两个元素, a的阶是7且$a^3b = ba^3$. 证明$ab = ba$.

习题1.3.4. 设x 在群中的阶是n, 求x^k $(k \in \mathbb{Z})$ 的阶.

习题1.3.5. (1) 设G 是有限阿贝尔群. 证明:

$$\prod_{g\in G} g = \prod_{\substack{a\in G\\ a^2=1}} a.$$

(2) 证明Wilson定理: 如p 是素数, 则$(p-1)! \equiv -1 \mod p$.

习题1.3.6. 证明 $f=\frac{1}{x},\ g=\frac{x-1}{x}$ 生成一个函数群, 合成法则是函数的合成, 它同构于二面体群 D_3.

习题1.3.7. (1) S^1 的任意有限阶子群均为循环群.

(2) $\mathbb{Q}$ 不是循环群, 但它的任意有限生成子群都是循环群.

(3)* 设 p 是一个素数,

$$G=\{x\in\mathbb{C}\mid \text{存在 } n\in\mathbb{N} \text{ 使得 } x^{p^n}=1\}$$

的任意真子群都是有限阶循环群.

习题1.3.8. 设 a 和 b 是群 G 的元素, 阶数分别是 n 和 m, $(n,m)=1$ 且 $ab=ba$. 试证 $\langle ab\rangle$ 是 G 的 mn 阶循环子群.

习题1.3.9. 设p 为奇素数, X 是n 阶整系数方阵. 如果$I+pX\in \mathrm{SL}_n(\mathbb{Z})$ 的阶有限, 证明$X=0$.

习题1.3.10. 设g_1,g_2 是群G 的元素，H_1,H_2 是G 的子群. 证明下列两条件等价:

(1) $g_1H_1\subseteq g_2H_2$;

(2) $H_1\subseteq H_2$ 且$g_2^{-1}g_1\in H_2$.

习题1.3.11. 设 G 是 n 阶有限群. 若对 n 的每一因子 m, G 中至多只有一个 m 阶子群, 则 G 是循环群.

习题1.3.12. 举一个无限群的例子, 它的任意阶数不为 1 的子群都有有限指数.

习题1.3.13. (1) 设G 是阿贝尔群, H 是G 中所有有限阶元素构成的集合. 证明H 是G 的子群.

(2)* 举例说明上述结论对于一般群不正确.

习题1.3.14. (1) 设 G 是奇数阶阿贝尔群. 证明由 $\varphi(x)=x^2$ 定义的映射 $\varphi:G\to G$ 是一个自同构.

(2)* 推广(1)的结果.

习题1.3.15. 设G 是阿贝尔群, $\alpha\in\mathrm{Aut}(G)$ 且 $\alpha^2=1$. 令

$$G_1=\{g\in G\mid \alpha(g)=g\},\quad G_{-1}=\{g\in G\mid \alpha(g)=g^{-1}\}.$$

(1) 如果G 是奇数阶有限群, 证明: $G=G_1G_{-1}$ 且 $G_1\cap G_{-1}=1$.

(2) 设 G 满足对任意 $g\in G$, 存在唯一的 $h\in G$ 使得 $h^2=g$, 则(1)中结论仍然成立. 由此证明:

(i) 任何 F 上的矩阵可以写成对称阵和反对称阵之和, 其中 $F=\mathbb{Q},\mathbb{R},\mathbb{C}$.

(ii) 任何函数 $f:\mathbb{R}\to\mathbb{R}$ 可以写成奇函数和偶函数之和.

习题1.3.16. (1) 求有理数加法群 $\mathbb{Q}$ 的自同构群 $\mathrm{Aut}(\mathbb{Q})$.

(2) 求整数加法群 $\mathbb{Z}$ 的自同构群 $\mathrm{Aut}(\mathbb{Z})$.

(3) 计算 Klein 群的自同构群.

(4) 求非零有理数乘法群 $\mathbb{Q}^\times$ 的自同构群 $\mathrm{Aut}(\mathbb{Q}^\times)$.

习题1.3.17. 回答下列问题:

(1) 设p是素数, p方幂阶群是否一定含有p阶元?

(2) 35阶群是否一定同时含有5阶和7阶元素?

(3) 若有限群 G含有 10 阶元 x 和 6阶元 y, 那么群 G 的阶应该满足什么条件?

习题1.3.18. 如果H 与K 是G的子群且阶互素, 证明$H \cap K = 1$.

习题1.3.19. 设 $\mathbb{R}^m$ 为 m 维实向量空间, A 是任意 $n \times m$ 实矩阵, $W = \{X \in \mathbb{R}^m \mid AX = 0\}$. 证明线性方程 $AX = B$ 的解空间或者是空集, 或者是加法群 $\mathbb{R}^m$关于W的陪集.

习题1.3.20. 设 H 和 K 分别是有限群 G 的两个子群, $HgK = \{hgk \mid h \in H,\ k \in K\}$. 试证:

$$|HgK| = |H| \cdot |K : g^{-1}Hg \cap K|.$$

习题1.3.21. 设 a, b 是群 G 的任意两个元素. 试证: a 和 a^{-1}, ab 和 ba 有相同的阶.

习题1.3.22. 设 $f:\ G \to H$ 是群同态. 如果 g是 G的有限阶元, 则 $f(g)$的阶整除g 的阶.

习题1.3.23. 设 A 是群 G 的具有有限指数的子群. 试证: 存在 G 的一组元素 $g_1, \ldots, g_n$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.

习题1.3.24. (1) 证明 $\mathrm{SL}_n(\mathbb{R})$ 由第一类初等矩阵 $I + aE_{ij} (i \neq j)$ 生成, 其中 E_{ij} 的第 (i, j) 元为 1, 其他元为 0.

(2) 证明 $\mathrm{GL}_n(\mathbb{R})$ 由第一类和第三类初等矩阵 $I + aE_{ii}$ $(a \neq -1)$ 生成.

(3)* 证明 $\mathrm{SL}_2(\mathbb{Z})$ 可以由 $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ 和 $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 生成.

习题1.3.25. 对于有限群G, 设$d(G)$ 是最小的正整数s 使得对任意$g \in G$, $g^s = 1$. 证明:

(1) $d(G)$ 是$|G|$ 的因子. 它等于G 中所有元素阶的最小公倍数.

(2) 如果G 是阿贝尔群, 则G 中存在元素阶为$d(G)$.

(3) 有限阿贝尔群G 为循环群当且仅当$d(G) = |G|$.

§1.4 正规子群与商群

我们在上节定义了群 G 关于其子群 H 的左陪集分解

$$G = \bigsqcup_{i \in I} g_i H = \bigcup_{g \in G} gH.$$

记 $G/H = \{g_i H \mid i \in I\}$ 为 G 的所有左陪集构成的集合类.

回忆在线性代数中, 如果 W 是线性空间 V 的子空间, 则商空间 V/W 作为集合即

$$V/W = \{v + W \mid v \in V\}.$$

它首先是加法子群 W 关于群 V的陪集类, 在其上面我们定义加法和数乘, 从而得到线性空间的结构. 注意到它上面的加法和数乘是继承了线性空间V 的加法和数乘, 换言之, 典范商映射 $\pi : V \to V/W$, $v \mapsto \bar{v} = v + W$ 是满的线性映射.

自然, 我们希望 G/H如 V/W 一样, 具有**商群**结构, 其乘法能够**继承** G 的乘法. 基于此, 我们需要对任意 $a, b \in G$, 定义乘法

$$aHbH = abH.$$

而此时在集合意义上,

$$aHbH = \{ah_1bh_2 \mid h_1, h_2 \in H\},$$

故对 $h_1, h_2 \in H$, 需存在 $h \in H$, 使得 $ah_1bh_2 = abh$, 即 $h_1b = b(hh_2^{-1})$, 从而$Hb \subseteq bH$. 所以, 要使 G/H 上有自然的乘法结构, 我们需要如下条件:

对任意 $b \in G$, 有 $Hb = bH$ 或等价条件 $b^{-1}Hb = H$ 成立.

定义1.71. 设G 是群, $x \in G$. 对任意 $g \in G$, gxg^{-1} 称为 x 的**共轭元**, 或者称x 与$x' = gxg^{-1}$ **共轭** (conjugate).

定义1.72. 子群 N 称为 G 的**正规子群** (normal subgroup), 是指对所有 $g \in G$ 有 $g^{-1}Ng = N$. 此时记 $N \lhd G$.

由定义容易验证共轭关系是等价关系, 且子群 N 是 G 的正规子群当且仅当 N 中任意元素的所有共轭元都在 N 中, 即 N 是G 中一些**共轭类** 之并.

例1.73. (1) 如果G 是阿贝尔群, 则$gxg^{-1} = x$ 对所有$g \in G$ 成立, 故x 是它所在共轭类唯一的元素, 因此G 的任何子群都是正规子群.

(2) 更进一步说, 对于任意群G, 元素x 所在共轭类只有一个元素当且仅当它与 G 中所有元素都交换. 所有这些元素构成的集合是G 的正规子群(参考1.4.4), 称为G 的**中心** (center), 记为$Z(G)$.

$$Z(G) = \{x \in G \,\big|\, xg = gx\text{对任意}g \in G\text{成立.}\}$$

我们来看一个最常见的正规子群的例子.

定义1.74. 设 $\varphi : G \to H$ 是群同态.

(1) 映射 φ 的**核** (kernel)为

$$\ker\varphi \triangleq \{g \in G \mid \varphi(g) = 1\} = \varphi^{-1}(1_H) \subseteq G.$$

(2) 映射 φ 的**像** (image)为

$$\mathrm{im}\varphi \triangleq \{h \in H \mid \text{存在}g \in G, \varphi(g) = h\} = \varphi(G) \subseteq H.$$

命题1.75. 设 $\varphi: G \to H$ 是群同态, 则 $\ker\varphi$ 是 G 的正规子群, 而$\mathrm{im}\varphi$ 是 H 的子群.

证明. 由 $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, 我们有

$$\varphi(1) = 1, \quad \varphi(g)^{-1} = \varphi(g^{-1})$$

设 $a, b \in \ker\varphi$, 则

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1,$$

故 $ab^{-1} \in \ker\varphi$, 即$\ker\varphi$ 是 G 的子群.

设 $g \in G, a \in \ker\varphi$, 则

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1,$$

所以 $g^{-1}ag \in \ker\varphi$, 故

$$g^{-1}(\ker\varphi)g \subseteq \ker\varphi,$$

$$\ker\varphi \subseteq g(\ker\varphi)g^{-1}.$$

由g的任意性(取g^{-1})立即有 $g^{-1}(\ker\varphi)g = \ker\varphi$, 所以 $\ker\varphi$ 是 G 的正规子群.

如果 $h_1, h_2 \in \mathrm{im}\varphi$, 令 $\varphi(g_1) = h_1, \varphi(g_2) = h_2$, 则

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = h_1h_2^{-1},$$

所以 $h_1h_2^{-1} \in \mathrm{im}\varphi$, 故 $\mathrm{im}\varphi$ 是 H 的子群. □

例1.76. 行列式映射 $\det: \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ 的核是 $\mathrm{SL}_n(\mathbb{C})$, 故 $\mathrm{SL}_n(\mathbb{C})$ 是 $\mathrm{GL}_n(\mathbb{C})$ 的正规子群.

现在设 $N \lhd G$, 则 G 关于 N 的左(右)陪集为

$$G/N = \{aN \mid a \in G\} = \{Na \mid a \in G\},$$

且

$$aNbN = a(bN)N = abN.$$

记 $\overline{a} = aN$, 定义乘法

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

由上述讨论, G/N 成为一个群, 称为 G 关于 N 的**商群** (quotient group). 可以直接验证商群的乘法与代表元选取取关：若$aN = a_1N$, $bN = b_1N$, 则$a^{-1}a_1, b^{-1}b_1 \in N$. 故有

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = b^{-1}(a^{-1}a_1)b \cdot (b^{-1}b_1) \in N,$$

也就是有$aNbN = (ab)N = (a_1b_1)N = a_1Nb_1N$.

记

$$\pi: G \to G/N, \quad a \mapsto \overline{a} = aN,$$

则 π 是群的满同态, 且 $\ker\pi = N$. 故我们有如下重要注记:

注记. 如果 N 是 G 的正规子群, 则存在群同态 φ, 使得 $N = \ker\varphi$; 反之, 如果 N 是群 G 到另一群的群同态 φ 的核, 则 N 是 G 的正规子群. 我们常常利用此项性质来寻找和判定群 G 的正规子群.

例1.77. (1) 由线性代数可知, 与所有n阶可逆矩阵都交换的矩阵是数量矩阵 xI_n $(x \in F)$, 由此可知 $\{xI_n \mid x \in F^\times\}$ 是一般线性群 $\mathrm{GL}_n(F)$ 的中心, 它对应的商群记为 $\mathrm{PGL}_n(F)$, 称为**射影一般线性群**.

(2) $\mathrm{SL}_2(\mathbb{Z})$ 关于其中心$\{\pm I_2\}$ 的商群记为$\mathrm{PSL}_2(\mathbb{Z})$, 即$\mathbb{Z}$ 上的 2 阶射影特殊线性群. 此群是当代数学研究中最著名的群之一, 也称为**模群** (modular group).

现在我们讨论群论中最重要定理:

定理1.78 (**同态基本定理**)**.** 设 $\varphi : G \to H$ 为群的同态, 则 φ 诱导的同态

$$\overline{\varphi} : G/\ker\varphi \to \mathrm{im}\varphi$$
$$\overline{\varphi}(\overline{g}) = \varphi(g)$$

为群同构. 换言之, 同态φ 可以分解为$\varphi = i \circ \overline{\varphi} \circ \pi$, 其中$\pi : G \to G/\ker\varphi$ 为自然满同态, $i : \mathrm{im}\varphi \to H$ 为自然单同态, $\overline{\varphi}$ 为同构.

注记. 同态基本定理又称为**第一同构定理**.

证明. (i) 我们首先证明 $\overline{\varphi}$ 是良好定义的, 即它的定义与 g 的选取无关. 事实上, 若 $g\ker\varphi = g'\ker\varphi$, 则 $g' = ga, a \in \ker\varphi$, 所以 $\varphi(g') = \varphi(ga) = \varphi(g)$.

(ii) $\overline{\varphi}$ 是同态. 如果 $\overline{g}_1, \overline{g}_2 \in G/\ker\varphi$, 则

$$\overline{\varphi}(\overline{g_1 g_2}) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).$$

(iii) $\overline{\varphi}$ 是单同态. 如果 $\overline{\varphi}(\overline{g}_1) = \overline{\varphi}(\overline{g}_2)$, 则有 $\varphi(g_1) = \varphi(g_2)$, 故 $\varphi(g_1^{-1}g_2) = 1$, 也就是$g_1^{-1}g_2 \in \ker\varphi$, 即 $\overline{g}_2 = \overline{g}_1$.

(iv) $\overline{\varphi}$ 是满同态是显然的.

由(i)-(iv), 定理得证. □

推论1.79. 设$\varphi : G \to H$ 为群同态, 则

(1) φ 是单同态当且仅当 $\ker\varphi = \{1\}$.

(2) φ 是满同态当且仅当 $\mathrm{im}\varphi = H$.

例1.80. (1) 映射 $\mathbb{R} \to S^1$, $x \mapsto e^{2\pi i x}$ 的核是 $\mathbb{Z}$, 而像就是 S^1, 故由同态基本定理得到群同构 $\mathbb{R}/\mathbb{Z} \cong S^1$.

(2) 对于域 F, 行列式映射诱导同构 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$.

例1.81. (1) 群同态 $\varphi:\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$,

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\mapsto\begin{pmatrix} a \bmod N & b \bmod N\\ c \bmod N & d \bmod N\end{pmatrix}$$

为满同态, 其核为

$$\Gamma(N)=\left\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})\,\middle|\, a\equiv d\equiv 1 \bmod N, b\equiv c\equiv 0 \bmod N\right\},\tag{1.26}$$

称为**主同余子群** (principal congruence subgroup). 关于同态φ满可以按如下思路证明: 设

$$\begin{pmatrix}\bar{x} & \bar{y}\\ \bar{z} & \bar{w}\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),\ x,y,z,w\in\mathbb{Z}.\ \text{记}A=\begin{pmatrix} x & y\\ z & w\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}).$$

首先由矩阵知识存在方阵$X,Y\in\mathrm{SL}_2(\mathbb{Z})$使得$XAY=\mathrm{diag}(x_0,w_0)$. 从而有$x_0w_0\equiv 1(\mathrm{mod}\ N)$. 现在有

$$\begin{pmatrix} w_0 & 1\\ w_0-1 & 1\end{pmatrix}\begin{pmatrix} x_0 & 0\\ 0 & w_0\end{pmatrix}\begin{pmatrix} 1 & -w_0\\ 0 & 1\end{pmatrix}=\begin{pmatrix} x_0w_0 & w_0(1-x_0w_0)\\ x_0(w_0-1) & w_0(x_0+1-x_0w_0)\end{pmatrix}.$$

令

$$B=X^{-1}\begin{pmatrix} 1 & -1\\ 1-w_0 & w_0\end{pmatrix}\begin{pmatrix} 1 & 0\\ x_0(w_0-1) & 1\end{pmatrix}\begin{pmatrix} 1 & w_0\\ 0 & 1\end{pmatrix}Y^{-1},$$

则$B\in\mathrm{SL}_2(\mathbb{Z})$, 由于$\varphi$是群同态, 有$\varphi(B)=\begin{pmatrix}\bar{x} & \bar{y}\\ \bar{z} & \bar{w}\end{pmatrix}$. 由同态基本定理, $\Gamma(N)$ 是$\mathrm{SL}_2(\mathbb{Z})$ 的正规子群, 且

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)\cong\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

(2) 设$N>2$. 考虑群同态$\tau:\Gamma(N)\to\mathrm{SL}_2(\mathbb{Z})\to\mathrm{PSL}_2(\mathbb{Z})$. 则$\ker\tau=\Gamma(N)\cap\{\pm I_2\}=\{I_2\}$, 故$\tau$ 是单同态. 由此我们可以将主同余子群 $\Gamma(N)$ 视为模群$\mathrm{PSL}_2(\mathbb{Z})$ 的子群.

由同态基本定理, 我们可以得到群论中很多重要的结果.

定理1.82 (**第二同构定理**)**.** 如果 $N\lhd G, H\leqslant G$, 则

$$(H\cap N)\lhd H,\quad N\lhd NH\leqslant G$$

且

$$NH/N\cong H/H\cap N.$$

证明. 由于 $N\lhd G$, 则对于 $a_1h_1,a_2h_2\in NH$, 其中$a_1,a_2\in N$, $h_1,h_2\in H$,

$$a_1h_1(a_2h_2)^{-1}=a_1h_1h_2^{-1}a_2^{-1}=\big(a_1(h_1h_2^{-1})a_2^{-1}(h_1h_2^{-1})^{-1}\big)h_1h_2^{-1}\in NH,$$

故 $NH \leqslant G$, 且 $N \lhd NH$.

现在我们定义同态

$$\varphi : H \to NH/N, \quad h \mapsto \overline{h} = hN = Nh,$$

自然 φ 为满同态, 且

$$\ker \varphi = \{h \in H \mid \varphi(h) = 1\} = \{h \in H \mid h \in N\} = H \cap N.$$

由同态基本定理

$$(H \cap N) \lhd H$$

且

$$NH/N \cong H/H \cap N.$$

定理证毕. □

注记. 上述定理中, N 和 H 的条件可以放弱为: N 和 H 均为 G 的子群且 $H \leq N_G(N) = \{g \in G \mid gNg^{-1} = N\}$. 事实上用$N_G(N)$代替$G$即可.

定理1.83 (**第三同构定理**)**.** 如果 $N \lhd G, M \lhd G$ 且 $N \leqslant M$, 则

$$G/M \cong \frac{G/N}{M/N}.$$

证明. 首先定义同态

$$\varphi : G/N \to G/M, \quad gN \mapsto gM.$$

由 $N \leqslant M$ 知 φ 是良好定义的满同态, 且

$$\ker \varphi = \{gN \mid gM = M\} = \{gN \mid g \in M\} = M/N,$$

由同态基本定理,

$$G/M \cong \frac{G/N}{M/N}.$$

定理证毕. □

定理1.84 (**对应定理**, 或称**第四同构定理**)**.** 设 N 是 G 的正规子群. 记 $\mathcal{M}$ 为 G 中包含 N 的所有子群的集合, $\mathcal{M}_0$ 为 $\overline{G} = G/N$ 的所有子群集合, 即

$$\mathcal{M} = \{M \mid N \leqslant M \leqslant G\},$$
$$\mathcal{M}_0 = \{X \mid X \leqslant \overline{G} = G/N\}.$$

则映射 $\alpha : \mathcal{M} \to \mathcal{M}_0,\ M \mapsto \overline{M} = M/N$ 为一一对应, 且此对应满足下列条件: 对于所有$M_1,\ M_2 \in \mathcal{M}$,

(1) $M_1 \leq M_2$ 当且仅当$\overline{M}_1 \leq \overline{M}_2$;
(2) 如果$M_1 \leq M_2$, 则$(M_2 : M_1) = (\overline{M}_2 : \overline{M}_1)$;
(3) $\overline{\langle M_1, M_2\rangle} = \langle \overline{M}_1, \overline{M}_2\rangle$;
(4) $\overline{M_1 \cap M_2} = \overline{M}_1 \cap \overline{M}_2$;
(5) $M \lhd G$ 当且仅当$\overline{M} \lhd \overline{G}$.

证明. 首先, 如果 $N \lhd G$, 则对所有 $N \leqslant M \leqslant G$, $N \lhd M$, 故 M/N 是 G/N 的子群, 即 α 是定义好的.

对于 $X \in \mathcal{M}_0$, 也就是$X = \{a_i N \,|\, i \in I\}$, 记 $\beta(X) = \{g \in G \mid gN \in X\}$, 则 $\beta(N) \supseteq N$. 对于任意$g, h \in \beta(X)$, 且由于 X 为群, 因此有$gN, hN, h^{-1}N = (hN)^{-1} \in X$. 故有$gh^{-1}N = (gN)(h^{-1}N) \in X$, i.e., $gh^{-1} \in \beta(X)$, 即$\beta(X)$ 也是群, 故 β 是 $\mathcal{M}_0$ 到 M 的映射.

要证明α为一一对应, 只需检查

$$\alpha\beta(X) = X, \quad \beta\alpha(M) = M$$

即可, 而这是可以直接验证的.

(1)-(5)的证明由 α 的定义立知, 留作练习. □

习 题

习题1.4.1. 令 $G = \{(a, b) \mid a \in \mathbb{R}^\times, b \in \mathbb{R}\}$, 乘法定义为

$$(a, b)(c, d) = (ac, ad + b).$$

试证: $K = \{(1, b) \mid b \in \mathbb{R}\}$ 是 G 的正规子群且 $G/K \cong \mathbb{R}^\times$.

习题1.4.2. 证明行列式为正的实矩阵组成的 $G = \mathrm{GL}_n(\mathbb{R})$ 的子集 H 构成一个正规子群, 并描述商群G/H.

习题1.4.3. 设 G 是群, $N \leq M \lhd G$.
(1) 如果 $N \lhd G$, 则 $N \lhd M$;
(2) 如果 $N \lhd M$, 则 N 是否一定是 G 的正规子群?

习题1.4.4. 试证:
(1) 群 G的中心 $Z(G)$ 是 G的正规子群.
(2) 群 G的指数为 2的子群一定是 G的正规子群.

习题1.4.5. 证明直积群 $G\times G'$ 的子集 $G\times 1$是一个与 G同构的正规子群, 且 $G\times G'/G\times 1 \cong G'$.

习题1.4.6. 若 $G/Z(G)$ 是循环群, 则 G 是阿贝尔群.

习题1.4.7. 设 G_i $(1 \leq i \leq n)$ 为群, 则

(1) $Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$;

(2) $G_1 \times G_2 \times \cdots \times G_n$ 为阿贝尔群当且仅当每个 G_i 均为阿贝尔群.

习题1.4.8. 设 G 为群.

(1) 对于 $x \in G$, 证明映射 $\sigma_x : g \mapsto xgx^{-1}$ 是 G 的自同构. σ_x 称为**内自同构** (inner automorphism).

(2) 令 $I(G)$ 表示所有 σ_x : $x \in G$ 组成的集合. 试证$I(G)$ 是$\mathrm{Aut}(G)$ 的子群. $I(G)$ 称为**内自同构群**.

(3) 证明$I(G) \cong G/Z(G)$.

习题1.4.9. 试求群 $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{O}_2(\mathbb{R})$, $\mathrm{SO}_3(\mathbb{R})$, $\mathrm{SU}_2(\mathbb{C})$ 的中心.

习题1.4.10. 设 $f : G \to H$ 是群同态, $M \leqslant G$. 试证 $f^{-1}(f(M)) = KM$, 这里 $K = \ker f$.

习题1.4.11. 设 M, N 为 G 的正规子群.

(1) 若 $M \cap N = \{1\}$, 则对任意 $a \in M$, $b \in N$, $ab = ba$.

(2) 更进一步, 如果$MN = G$, 则$G \cong M \times N$.

习题1.4.12. 设 $N \lhd G$, g 是群 G 的任意一个元素. 如果 g 的阶和 $|G/N|$ 互素, 则 $g \in N$.

习题1.4.13. 证明非阿贝尔群的自同构群不是循环群.

习题1.4.14. 当 n 为奇数时, 证明 $\mathrm{O}_n(\mathbb{R}) \cong \mathrm{SO}_n(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$.