第3章　群　　论

3.1　群的基础知识

回忆一下，一个集合 G 上的**二元运算**（binary operation），只是一个从 G^2 到 G 的函数。一旦我们在一个集合上定义了一个或多个二元运算，就得到了一个**代数系统**（algebraic system）。出于将要阐明的原因，我们特别关注一类特殊的代数系统，即群。

定义 3.1.1　所谓**群**（group）是指形如 $(G, \cdot)$ 的代数系统，其中 G 是集合，$\cdot$ 是 G 上的一个二元运算，且满足以下条件：

- 存在一个**单位元**（identity element，identity）$1 \in G$，使得对所有 $a \in G$，有 $1 \cdot a = a \cdot 1 = a$。
- 运算 $\cdot$ 是结合的，即对所有 a、b、$c \in G$，都有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。
- 每个元素 $a \in G$ 都有**逆元**（inverse），记作 a^{-1}，满足 $a \cdot a^{-1} = a^{-1} \cdot a = 1$。

为简便起见，我们常常简称 G 为群，而不显式地写出 $(G, \cdot)$。

这个定义相当抽象——这也正是这门数学分支通常被称为**抽象代数**（abstract algebra）的原因。您可能会觉得具体的例子比抽象定义更易于理解。下面是一个可能有帮助的例子：

例 3.1.1　**克莱因四元群**（Klein four-group）[①] 是指代数系统 $(\{1, a, b, c\}, \cdot)$，其中：

- $1 \cdot a = a \cdot 1 = a$；$1 \cdot b = b \cdot 1 = b$；$1 \cdot c = c \cdot 1 = c$。
- $a \cdot a = b \cdot b = c \cdot c = 1$。
- $a \cdot b = b \cdot a = c$；$b \cdot c = c \cdot b = a$；$c \cdot a = a \cdot c = b$。

您能验证它确实构成一个群吗？为什么？

克莱因四元群（中的运算 $\cdot$）是可交换的（为什么？），然而群的定义并不要求交换性。接下来我们看两个**不可交换群**的例子。

例 3.1.2　考虑一个正三角形 ABC。一共有如下 6 种将其映射为自身的几何变换。

（1）恒等变换，即不做任何操作。

（2）顺时针旋转 120°。

（3）逆时针旋转 120°。

（4）一个镜像对称变换。

---

① 菲力克斯 • 克莱因（Felix Klein, 1849—1925），德国数学家、教育家。19 岁在波恩大学获得博士学位，23 岁成为教授。职业生涯的后 27 年任教于哥廷根大学；在他的领导下，特别在他聘请了大卫 • 希尔伯特（David Hilbert）之后，该校成为世界数学中心。他是国际数学教育委员会的创始主席。除了克莱因四元群外，他的重要贡献还包括克莱因瓶——一种无边界的曲面。

（5）镜像对称变换后跟一个顺时针旋转 120°。

（6）镜像对称变换后跟一个逆时针旋转 120°。

令 G 为上述6个变换的集合，$\cdot$ 为变换的复合运算。您能看出 $(G, \cdot)$ 构成一个群吗？它为什么不是可交换的？请解释。

解答： 我们跳过它为何是群的讨论，直接说明为什么它不是可交换的。注意，复合运算的顺序是不可调换的：先做镜像对称变换再随便往哪个方向旋转 120°，与先往这个方向旋转再做镜像对称变换并不等价。 ■

例 3.1.3 设 M 为所有 $n \times n$ 的非奇异实矩阵的集合 $(n \geqslant 2)$，$\times$ 表示矩阵乘法，则 $(M, \times)$ 构成一个群。显然这个群也是不可交换的。

阅读完以上例子后，您应该对群这个抽象概念有所理解了。一个自然的问题是：定义中要求存在的单位元和逆元是否唯一？答案是肯定的。

命题 3.1.1 在一个群中，单位元是唯一的，且每个元素的逆元也是唯一的。

证明： 假设群 G 中存在两个单位元，分别为 1 和 $1'$。根据定义，有 $1 \cdot 1' = 1$（因为 $1'$ 是单位元），也有 $1 \cdot 1' = 1'$（因为 1 也是单位元），故 $1 = 1'$。因此，单位元是唯一的。

假设 $a \in G$ 有两个逆元，分别为 a^{-1} 和 $a^{\star}$。显然，

$$a^{-1} = a^{-1} \cdot (a \cdot a^{\star}) = (a^{-1} \cdot a) \cdot a^{\star} = a^{\star}$$

因此逆元也唯一。 ■

另一个自然的问题是关于运算律。常见的运算律包括交换律、结合律、分配律和消去律。定义中要求群必须满足结合律，而例 3.1.2 表明群不一定满足交换律。又由于群上只有一种运算，因而没有“分配律”一说。那么剩下的问题是消去律是否成立。

命题 3.1.2 消去律对任何群都成立。即，对任意群 G，以及任意的 a、b、$c \in G$，若 $a \cdot c = b \cdot c$，则 $a = b$；若 $c \cdot a = c \cdot b$，亦有 $a = b$。

证明： 由 $a \cdot c = b \cdot c$ 可得 $a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1}$，即 $a = b$。另一种情形亦可类似证明。 ■

与命题 3.1.2 密切相关的是以下关于方程的结果。

命题 3.1.3 在任意群 G 中，对任意 a、$b \in G$，方程 $a \cdot x = b$ 和 $x \cdot a = b$ 总在 G 中有解。

命题 3.1.1、命题3.1.2 和命题 3.1.3 描述了群的一些基本性质。请仔细研究例 3.1.1、例3.1.2 和例 3.1.3 中的群，以验证这些性质。

对于命题 3.1.2 和命题 3.1.3，一个自然的疑问是它们的逆是否成立。也就是说，若某代数结构满足消去律，或方程 $a \cdot x = b$、$x \cdot a = b$ 有解，那么它是否一定是群？在讨论这些问题前，我们需要先介绍一些新定义。

定义 3.1.2 若一个代数系统 $(G, \cdot)$ 的二元运算 $\cdot$ 满足结合律，则称其为半群（semigroup）。

例 3.1.4 所有 $n \times n$ 奇异实矩阵在矩阵乘法下构成一个半群。它不是群，因为没有单

位元和逆元。

根据定义 3.1.2，我们现在可以更精确地提出问题：在一个半群中，如果满足消去律，或者方程 $a \cdot x = b$ 与 $x \cdot a = b$ 总有解，我们是否可以确定该半群一定是群？为了回答这个问题，我们需要一个涉及左右单位元及左右逆元的引理。

回顾单位元的定义，对于所有 $a \in G$，都有 $a \cdot 1 = 1 \cdot a = a$。

定义 3.1.3 若对所有 $a \in G$，有 $a \cdot 1 = a$，我们称 1 是一个*右单位元*；若对所有 $a \in G$，有 $1 \cdot a = a$，我们称 1 是一个*左单位元*。

因此，一个单位元实际上是一个同时为左单位元与右单位元的元素。

类似地，群的定义要求存在 a^{-1} 使得 $a \cdot a^{-1} = a^{-1} \cdot a = 1$。

定义 3.1.4 若 a^{-1} 满足 $a \cdot a^{-1} = 1$，我们称它为 a 的*右逆元*；若 a^{-1} 满足 $a^{-1} \cdot a = 1$，我们称它为 a 的*左逆元*。

因此，a 的逆元实际上是一个同时为左逆元与右逆元的元素。

引理 3.1.1 在一个半群中，如果同时存在左单位元和右单位元，则它们相等，也就是说，该半群具有单位元。

在一个有单位元的半群中，如果某元素同时具有左逆元和右逆元，则这两个逆元相等，也就是说，该元素具有逆元。

利用上述引理，我们可以很容易地回答前面的问题：对于消去律，有限半群中答案为“是”，无限半群中答案为“否”；对于方程恒有解的情况，答案恒为“是”。

命题 3.1.4 如果一个有限半群满足消去律，那么它是一个群。

证明： （从此以后，我们常省略乘法符号 $\cdot$。）

对 $a \in G$，考虑集合 $aG = \{ax \mid x \in G\}$。这个集合中有多少个不同的元素？由于满足消去律，对于所有 $b \neq c$，必有 $ab \neq ac$。（否则，根据消去律得到 $b = c$，与 $b \neq c$ 矛盾。）因此，$|aG| = |G|$。由于 $aG \subseteq G$ 且 G 是有限集合，得到 $aG = G$。类似地，考虑集合 $Ga = \{xa \mid x \in G\}$，同样可以得到 $Ga = G$。

由于 $aG = G$，存在 $e \in G$ 使得 $ae = a$。由于 $G = Ga$，对所有 $b \in G$，存在 c 使得 $b = ca$。因此，$be = cae = ca = b$。这说明 e 是一个右单位元。同理，可以证明存在左单位元。于是可以推出存在单位元，记作 1。

对于任意 $a \in G$，由于 $aG = G$，必存在 $x \in G$ 使得 $ax = 1$，即 a 有右逆元。由 $Ga = G$，得 a 也有左逆元。结合这两点，可以推出 a 有逆元。因此，G 是一个群。 ■

我们在命题 3.1.4 的证明中使用的符号 aG 和 Ga 是非常常用的记号，所以请您务必记住。

命题 3.1.5 存在一个无限半群满足消去律但不是群。

证明： 一个满足题设的半群是 $(\mathbb{Z}^+, +)$，其中 $\mathbb{Z}^+$ 是正整数集合，$+$ 是加法运算。很容易验证这是一个半群，且满足消去律。然而，它没有单位元——注意自然数 1 并不是这个半群的单位元，而整数 0 则不在这个半群之中。因此，它不是群。 ■

命题 3.1.6 在一个半群 G 中，若对所有 a、$b \in G$，方程 $ax = b$ 和 $xa = b$ 都有解，

则 G 是一个群。

证明： 做法与命题 3.1.4 类似。

首先，方程 $ax = a$ 有解。设其解为 e，则 $ae = a$。对于所有 $b \in G$，方程 $b = xa$ 有解，设其解为 c，于是 $b = ca$。因此，$be = cae = ca = b$，说明 e 是一个右单位元。同理可得存在一个左单位元。于是，存在一个单位元，记作 1。

现在，对所有 $a \in G$，方程 $ax = 1$ 和 $xa = 1$ 都有解，这意味着 a 同时有右逆元和左逆元。因此，a 一定有逆元。

综上，G 是一个群。 ■

在学习了群的基本性质及其逆命题之后，我们以两个稍显复杂的例题作为 3.1 节的结尾。

例 3.1.5 构造一个 21 阶群和一个 22 阶群，要求在其中交换律都不成立。

解答： 为了构造使交换律不成立的 21 阶群，我们考虑某些矩阵之间的乘法运算。

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \{1,2,4\},\ b \in \{0,1,2,3,4,5,6\} \right\}$$

G 中两个矩阵相乘，会得到

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix}$$

看起来似乎仍然在 G 中。因此，G 有可能构成一个群。为了让 $|G| = 21$，我们限定矩阵中的 $a \in \{1,2,4\}$，$b \in \{0,1,2,3,4,5,6\}$。然而，这就意味着上面的乘积矩阵中必须有 $aa' \in \{1,2,4\}$，$ab'+b \in \{0,1,2,3,4,5,6\}$。为了达到这个目标，我们规定这里的加法、乘法都是对模 7 而言的。容易验证，在这样限制之后，G 恰好是一个 21 阶群，并且其中交换律不成立。

为了构造使交换律不成立的 22 阶群，我们采用与例 3.1.2类似的思路，考虑将正 11 边形映射到其自身的 22 个变换。更形式化一点，我们可以定义 $H = \{0,1,2,\cdots,10\} \times \{0,1\}$。对所有 $a,b \in \{0,1,2,\cdots,10\}$，定义运算如下：

$$(a,0)\cdot(b,0) = ((a+b) \bmod 11, 0), \quad (a,1)\cdot(b,0) = ((a+b) \bmod 11, 1),$$
$$(a,0)\cdot(b,1) = ((b-a) \bmod 11, 1), \quad (a,1)\cdot(b,1) = ((b-a) \bmod 11, 0)$$

容易验证，H 是一个 22 阶群，并且其中交换律不成立。 ■

例 3.1.6 设 G 是一个群，且 x、$y \in G$（$x \neq y$，$x \neq 1$，$y \neq 1$）满足

$$x^m = 1, \quad (xy)^2 = 1, \quad (x^2y)^2 = 1 \quad (m \geqslant 3,\ m \in \mathbb{Z})$$

对于任意小于 m 的正整数 k 都有 $x^k \neq 1$，且对于任意非单位元 $a \in G$，存在一个正整数 n 和一些元素 $a_1, a_2, \cdots, a_n$，使得

$$a = a_1 a_2 \cdots a_n$$

且每个 a_i 要么为 x，要么为 y。求 $|G|$。

解答： 由 $(x^2y)^2 = 1 = (xy)^2$ （两边左乘 x^{-1}，并且两边右乘 $y^{-1}x^{-1}$）得 $xyx = y$。于是，又可以推出 $y^2 = xyxy = 1$。（这也等价于 $y^{-1} = y$。）再次考虑 $(xy)^2 = 1$，可得

$yx = x^{-1}y^{-1} = x^{-1}y$。

利用上面得到的 $y^2 = 1$ 和 $yx = x^{-1}y$ 可以将任何由 x, y 构成的串中所有的 y 推到右边：每次交换 y 与 x 的顺序时，x 的指数取负。重复这个过程，任何元素都可以化为 x^k 或 $x^k y$ $(k \in \mathbb{Z})$。再由 $x^m = 1$ 知道，可以限制 $0 \leqslant k \leqslant m-1$。

若存在 i、j 使 $x^i = x^j y$，两边左乘 x^{-j} 得 $x^{i-j} = y$。于是从 $y^2 = 1$，$(xy)^2 = 1$ 两式分别得到 $x^{2(i-j)} = 1$ 和 $x^{2(i-j+1)} = 1$，从而可推出 $x^2 = 1$，与 $m \geqslant 3$ 矛盾。因此 $\{x^k : 0 \leqslant k \leqslant m-1\}$ 与 $\{x^k y : 0 \leqslant k \leqslant m-1\}$ 互不相交，且各含 m 个不同元素。可见，$|G| = 2m$。 ■

3.2 子群、陪集与拉格朗日定理

群是一种有趣的代数结构，尤其是当一个群包含另一个群时。

定义 3.2.1 设 $(G, \cdot)$ 是一个群，$H \subseteq G$ 是一个非空集合。若 $(H, \cdot)$ 也是一个群，则称 H 是 G 的一个子群（subgroup），记作 $H \leqslant G$。

例 3.2.1 考虑一个任意群 $(G, \cdot)$。您可能会好奇，在不使用群的其他性质的前提下，是否可以识别出它的一些子群。答案是肯定的。

- G 显然至少有两个子群：一个是最大子群，即它自身；另一个是 $\{1\}$，称为*平凡子群*（trivial subgroup）。[①]
- 能够与 G 中所有元素交换的元素构成一个子群。形式化地说，$Z(G) = \{c | \forall a \in G, ac = ca\}$ 是 G 的一个子群；这个子群通常称为 G 的*中心*（center）。
- 更一般地，对任意固定的子集 $S \subseteq G$，所有能与 S 中所有元素交换的 G 中元素也构成一个子群。形式化地说，$\{c | \forall a \in S, ac = ca\} \leqslant G$。

例 3.2.2 回忆例 3.1.2 中定义的群 G。设 S 为只包含恒等变换与镜像对称变换的子集。请验证 $S \leqslant G$。

解答： 任取 a、$b \in S$，必有 $ab \in S$。S 中包含恒等变换，且每个元素的逆元是它自身。所以 S 是一个子群。 ■

如果对所有 a、$b \in H$，均有 $ab \in H$，那么称 H 在运算 $\cdot$ 下是*封闭*的。显然，一个子集 H 是子群当且仅当它在 $\cdot$ 下封闭、包含单位元 1，且每个元素在 H 中都有逆元。在实际操作中，验证一个子集是否是子群并不总需要检查这 3 个条件。有一种更简洁的判别方法。

命题 3.2.1 在一个群 G 中，非空子集 H 是子群，当且仅当对所有 $a, b \in H$，有 $a^{-1}b \in H$。

证明： “必要性”是显然的。因此我们只需证明“充分性”。

首先，单位元必须在 H 中：$1 = a^{-1}a \in H$。

其次，对所有 $a \in H$，其逆元也在 H 中：$a^{-1} = a^{-1} \cdot 1 \in H$。

再次，对所有 a、$b \in H$，有 $ab = (a^{-1})^{-1}b \in H$。 ■

① 这里我们不把 $\varnothing$ 当作一个群。

由于对称性，在命题 3.2.1 中的条件 $a^{-1}b \in H$ 也可以替换为 $ab^{-1} \in H$。请分别使用命题 3.2.1 及其这个变式，证明例 3.2.1 和例 3.2.2 中列出的集合确实是子群。

例 3.2.3 在例 3.1.3 中我们看到，所有 $n \times n$ 非奇异实矩阵（$n \neq 2$）构成一个群。请证明所有 $n \times n$ 的对角实矩阵（$n \neq 2$，其中对角线上的元素都不为 0）构成一个子群。

解答： 考虑任意两个对角实矩阵 $M_1 = \mathrm{diag}(a_1, a_2, \cdots, a_n)$ 和 $M_2 = \mathrm{diag}(b_1, b_2, \cdots, b_n)$，其中所有对角元素均不为 0。我们有

$$M_1^{-1} M_2 = \mathrm{diag}\left(\frac{b_1}{a_1}, \frac{b_2}{a_2}, \cdots, \frac{b_n}{a_n}\right)$$

这仍是一个对角实矩阵，并且所有对角线元素仍不为 0。因此，这些矩阵构成的集合是一个子群。 ■

到目前为止，我们已经了解了如何判断一个子集是否是子群。接下来我们研究子群之间的关系。

命题 3.2.2 在一个群 G 中，如果 H 和 K 都是子群，则 $H \cap K$ 也是子群。

证明： 对所有 a、$b \in H \cap K$，有 a、$b \in H \Rightarrow a^{-1}b \in H$；$a$、$b \in K \Rightarrow a^{-1}b \in K$。因此，$a^{-1}b \in H \cap K$。所以 $H \cap K$ 是一个子群。 ■

不同于子群的交是子群，两个子群的并不一定是子群。这里给出一个具体例子：考虑克莱因四元群 $\{1, a, b, c\}$。$\{1, a\}$ 与 $\{1, b\}$ 都是子群，并且它们的交 $\{1\}$ 也是子群。但它们的并 $\{1, a, b\}$ 不是子群，因为 $ab = c \notin \{1, a, b\}$。

若我们只考虑真子群（即不是整个群的子群），则可以证明以下结论。

例 3.2.4 如果一个群等于 n 个真子群的并集，那么 n 的最小值是多少？

解答： 还是考虑克莱因四元群 $\{1, a, b, c\}$。它的 3 个真子群 $\{1, a\}$、$\{1, b\}$、$\{1, c\}$ 的并集恰好等于它本身，所以 $n = 3$ 肯定是可以的。倘若我们能证明 n 不能等于 2，那就说明 n 的最小值为 3。

下面我们证明 n 不能等于 2。设 G 是一个群。并且假设 H_1、$H_2 < G$（也就是 H_1、$H_2 \leqslant G$ 但 H_1、$H_2 \neq G$），$H_1 \neq H_2$。我们将证明 $H_1 \cup H_2 \neq G$。

若 H_1、H_2 之一包含于另一个，则它们的并等于较大的那个子群，因此不等于 G。

若两者均不包含于对方，则可以选取 $a \in H_1$ 使得 $a \notin H_2$，以及 $b \in H_2$ 使得 $b \notin H_1$。现在考虑元素 ab 属于哪个子群：若 $ab \in H_1$，则 $b = a^{-1}ab \in H_1$，与 $b \notin H_1$ 矛盾；若 $ab \in H_2$，则 $a = ab \cdot b^{-1} \in H_2$，与 $a \notin H_2$ 矛盾。因此我们找到了一个不属于 H_1 也不属于 H_2 的元素，说明 $H_1 \cup H_2 \neq G$。

需要说明的是，以上对于 $H_1 \cup H_2 \neq G$ 的证明是可以简化的。稍后学习了拉格朗日定理，请大家再想想这个证明可以如何简化。 ■

接下来，我们将围绕一个新概念——陪集，研究子群的一些基本性质。

定义 3.2.2 设 G 是一个群，$H \leqslant G$。对 $a \in G$，集合 $aH = \{ah \mid h \in H\}$ 是 H 在 G 中的一个左陪集（left coset），集合 $Ha = \{ha \mid h \in H\}$ 是一个右陪集（right coset）。

例 3.2.5 考虑例 3.2.2 中的群 G 及其子群 $S \leqslant G$，总共有如下 3 个不同的左陪集。

（1）子群 S 本身就是一个左陪集。

（2）设 a 为顺时针旋转 120°。左陪集 aS 含有两个元素，一个是 a 本身，另一个是先进行 120° 顺时针旋转后再镜像对称的变换，或者等价地，先镜像对称后再进行 120° 逆时针旋转。

（3）剩下的两个变换，分别是 120° 逆时针旋转和先镜像对称后再进行 120° 顺时针旋转，共同构成第3个左陪集。

现在我们来看右陪集：

（1）子群 S 本身是一个右陪集。

（2）右陪集 Sa 包含两个元素，一个是 a 本身，另一个是先镜像对称后进行 120° 顺时针旋转的变换。注意 $Sa \neq aS$！

（3）剩下的两个变换，分别是 120° 逆时针旋转和先镜像对称后 120° 逆时针旋转，构成第3个右陪集。这个右陪集也不等于第3个左陪集。

显然，总有 $a \in aH$ 且 $a \in Ha$。一个自然的问题是，如果我们取另一个元素 $b \in aH$（或 $b \in Ha$），是否可以将 aH（或 Ha）写为 bH（或 Hb）？答案是肯定的。

命题 3.2.3 设 G 是一个群，$H \leqslant G$。对任意 $b \in aH$，有 $bH = aH$；对任意 $b \in Ha$，有 $Hb = Ha$。

证明： 对任意 $b \in aH$，存在 $h \in H$ 使得 $b = ah$。对任意 $c \in aH$，存在 $h' \in H$ 使得 $c = ah'$。显然，$c = ahh^{-1}h' = bh^{-1}h'$ 而 $h^{-1}h' \in H$，所以 $c \in bH$。这说明 $aH \subseteq bH$。

反过来，对任意 $c \in bH$，存在 $h' \in H$ 使得 $c = bh'$。显然，$c = bh^{-1}hh' = ahh'$ 而 $hh' \in H$，因此 $c \in aH$。这说明 $bH \subseteq aH$。

综上，$aH = bH$。同理可证 $Ha = Hb$。 ■

因此，当我们将陪集写为 aH 或 Ha 时，只是选用了其中的一个元素作为“代表”。陪集中的任意元素都可以作为代表，因为所得到的整个集合总是不变的。在例 3.2.5 中，aS 其实也可以写作 bS，其中 b 是先做镜像对称变换再做 120° 逆时针旋转所得到的变换。

命题 3.2.4 设 G 是一个群，$H \leqslant G$。H 在 G 中的所有左陪集（或右陪集）构成 G 的一个划分。

证明： 考虑两个不同的左陪集 aH 和 bH。我们将通过反证法证明它们是互不相交的。假设存在 $c \in aH$ 且 $c \in bH$。根据命题 3.2.3，有 $aH = cH$ 且 $bH = cH$，从而 $aH = bH$，这与假设矛盾。

接下来证明所有左陪集的并等于 G。对任意 $g \in G$，显然有 $g \in gH$。因此 G 是所有左陪集并集的子集。又由于所有左陪集都是 G 的子集，它们的并集也在 G 中。两者结合可知，所有左陪集的并集就是 G。

因此，左陪集族是 G 的一个划分。同理，右陪集族也是 G 的一个划分。 ■

让我们回到例 3.2.5。在该例中，左陪集/右陪集族是否构成一个划分？显然是的。事实上，这不仅是一个划分，而且是一个等势划分。下面我们证明这在一般情况下也成立。

命题 3.2.5 设 G 是一个群，$H \leqslant G$。那么 H 在 G 中的每个左陪集（或右陪集）与 H 等势。

证明： 对任意 $a \in G$，映射 $f : x \mapsto ax$ 是一个从 H 到 aH 的满射。因此，为了证明 $|aH| = |H|$，我们只需证明 f 是单射，即对所有 b、$c \in H$（$b \neq c$）有 $ab \neq ac$，而这一点可由消去律得到。 ■

命题 3.2.5 在群论中具有广泛应用，其中最重要的应用可能就是在证明拉格朗日定理时。

定理 3.2.1 (拉格朗日定理 (Lagrange's Theorem)[①]) 设 G 是一个有限群，$H \leqslant G$。则 $|H|$ 整除 $|G|$。

证明： 由命题 3.2.5 可知，$|G| = n|H|$，其中 n 是不同陪集的个数。因此，$|H|$ 整除 $|G|$。 ■

（现在您已经学习过拉格朗日定理，让我们回忆前面刚学过的例 3.2.4。使用拉格朗日定理，可以极其简单地证明任意两个真子群的并集不等于群本身。您知道该怎么证吗？）

在研究了陪集的势之后，下面我们考虑一个给定的子群可以有多少个左陪集或右陪集。也许很容易猜到左陪集的个数与右陪集的个数必须相等，但是它们为什么相等呢？背后的道理何在？有人会说，根据拉格朗日定理，每个左/右陪集大小相同，所以左/右陪集的个数都等于群的阶数除以子群的阶数。然而，这个说法忽略了无限群，因为拉格朗日定理仅仅适用于有限群。

也有人会说，“把每个左陪集 aH 直接映射到右陪集 Ha 不就行了吗，这是从左陪集族到右陪集族的双射。”可是，这实际上并不是一个双射，甚至都不是一个良好定义的映射—请您仔细思考其原因。

下面，我们将探讨一个例题，即例 3.2.6，其结论可以很轻松地推出左右陪集族的势相等。这样，我们可以引入一个新的概念，将左陪集族或者右陪集族的势被称为子群在群中的指数（index）。当群为 G、子群为 H 时，指数记作 $[G : H]$。

例 3.2.6 假设 G 是一个群，H、$K \leqslant G$。用记号 HgK 来表示集合 $\{hgk : h \in H, k \in K\}$。证明：$|\{HgK : g \in G\}| = |\{KgH : g \in G\}|$。（如果令 $K = \{1\}$，就得到 H 的左右陪集族的势相等。请您自行推导这个重要结论。）

解答： 我们定义一个从 $\{HgK : g \in G\}$ 到 $\{KgH : g \in G\}$ 的函数 f：$f(HgK) = Kg^{-1}H$。首先证明 f 确实是一个良定义的函数。考虑两个不同的元素 g_1、$g_2 \in G$，使得 $Hg_1K = Hg_2K$，我们需要证明代表元素 g_1、g_2 的选择不会影响映射的结果，也就是 $Kg_1^{-1}H = Kg_2^{-1}H$。由 $Hg_1K = Hg_2K$ 得到，存在 $h \in H$、$k \in K$ 使得 $1 \cdot g_1 \cdot 1 = hg_2k \Rightarrow g_1^{-1} = k^{-1}g_2^{-1}h^{-1}$。由此可知 $Kg_1^{-1}H = Kk^{-1}g_2^{-1}h^{-1}H = Kg_2^{-1}H$。

对所有 a、$b \in G$，若 $Ka^{-1}H = Kb^{-1}H$，则存在 $k \in K$，$h \in H$ 使得 $a^{-1} = kb^{-1}h$。这意味着 $a = h^{-1}bk^{-1} \Rightarrow HaK = Hh^{-1}bk^{-1}K = HbK$，因此 f 是单射。另一方面，任

---

① 约瑟夫-路易·拉格朗日（Joseph-Louis Lagrange，1736—1813），数学家、天文学家。出生在南欧的一个小王国（现在属于意大利），部分祖先是法国人。在都灵大学学习期间，他对数学毫无兴趣——他最喜欢的学科是拉丁文。一个偶然的契机使他对数学产生兴趣，并在短短一年之内成为一位杰出的数学家。尽管不久后因对数学的众多贡献而声名鹊起，但他拒绝了著名的普鲁士科学院的邀请，理由是“欧拉在那里”。后来，当欧拉离开普鲁士时，欧拉推荐拉格朗日继任自己的位置。为此，国王亲自致信拉格朗日，说“欧洲最伟大的国王”应当拥有“欧洲最伟大的数学家”。于是，拉格朗日接受了邀请。

普鲁士国王去世后，拉格朗日移居法国，受到法国国王的诸多褒奖。法国大革命期间，拉格朗日受到拉瓦锡的保护，但拉瓦锡自己后来却被判处死刑。因此，拉格朗日在拉瓦锡死后写下名言：“让这颗头颅落地只需一瞬，而再要有这样的头脑诞生，连一百年都不够。”具有讽刺意味的是，拉格朗日自己始终安然无恙，并持续获得荣誉。他后来出任法国参议员，并第一个在法国吞并其祖国的法案上签字。

如果您读过小说《三体》，您可能会感兴趣：拉格朗日是三体问题的早期研究者之一，拉格朗日点就是以他的名字命名的。

意一个 $Kg^{-1}H$ 都可以找到原像 HgK，因此 f 也是满射。可见 f 是一个双射，从而得到 $|\{HgK : g \in G\}| = |\{KgH : g \in G\}|$。 ■

我们刚刚完成了对陪集基本性质的研究。回顾例 3.2.1、例 3.2.2 和例 3.2.3，验证这些性质将会很有帮助。

虽然陪集总是相对于某个特定的子群定义的，但有时我们需要判断一个子集是否为某个陪集，而不关心它是否子群。为此，我们将（用于刻画子群的）命题 3.2.1扩展到陪集的情形。

命题 3.2.6 设 G 是一个群，H 是其子群。若一个子集 C 是左陪集，则对所有 a、$b \in C$，有 $a^{-1}b \in H$；若 C 是右陪集，则对所有 a、$b \in C$，有 $ab^{-1} \in H$。

证明： 若 $C = dH$（其中 $d \in G$），则对所有 a、$b \in C$，存在 h、$h' \in H$ 使得 $a = dh$，$b = dh'$。因此，

$$a^{-1}b = (dh)^{-1}(dh') = h^{-1}d^{-1}dh' = h^{-1}h' \in H$$

C 是形如 Hd 的右陪集的情况可用类似方式证明。 ■

值得注意的是，命题 3.2.6 仅扩展了命题 3.2.1 中的“必要性”的部分，而非“充分性”的部分。我们将后一部分的扩展留作习题（见习题 101）。

3.3 循环群、生成元与有限生成群

循环群是一类非常重要的群。它们结构简单，容易理解，并且在很多地方（包括许多其他群的内部）都可以找到它们的身影。

定义 3.3.1 如果一个群 G 中存在某个元素 $g \in G$，使得对所有 $a \in G$，都存在整数 k 使得 $a = g^k$，那么称 G 为一个*循环群*（cyclic group），称 g 为 G 的一个*生成元*（generator）。

例 3.3.1 例 3.1.1 中的克莱因四元群不是循环群。

例 3.3.2 例 3.1.2 中的几何变换群不是循环群，但其中大小为 2 的子群（仅包含恒等变换和镜像对称变换）是循环群；该子群的生成元是镜像对称变换。另一个大小为 3 的子群，由恒等变换、120° 顺时针旋转和 120° 逆时针旋转组成，也是循环群；我们可以用 120° 顺时针旋转或 120° 逆时针旋转作为该子群的生成元。

例 3.3.3 证明例 3.1.3 中的非奇异矩阵群 $(n \neq 2)$ 不是循环群。

解答： 容易看出，非奇异矩阵群是不可数的，而我们将在命题 3.3.5 中看到，无限循环群是可数的。 ■

一个满足交换律的群称为*阿贝尔群*（Abelian group）[①]。显然，循环群必为阿贝尔群。

例 3.3.4 例 3.1.1 中的克莱因四元群是阿贝尔群。

---

① 尼尔斯·阿贝尔（Niels Abel, 1802—1829），挪威数学家。在中学时期就被数学老师发现其数学天赋，并受到鼓励与指导。进入大学时，他已是挪威全国最优秀的数学人才。不幸的是，他仅活到 26 岁。在他短暂的生涯中，经济拮据，仅获得了一次小额资助去国外访问，而这次旅行在当时被视为“失败”。他是早逝的数学天才的代表之一（另一位代表是法国数学家伽罗华，21 岁去世）。

阿贝尔证明了五次及更高次多项式的根一般不能用根式表示。一个多世纪后，华罗庚还曾专文向中国公众解释这一结果。

例 3.1.2 中的几何变换群不是阿贝尔群，但其中的两个循环子群是阿贝尔群，因为任意循环群都是阿贝尔群。

例 3.1.3 中的非奇异矩阵群不是阿贝尔群。

例 3.2.1 中定义的任意群的中心是阿贝尔群。

在理解了循环群之后，我们可以进一步探讨阶与*共轭元*的概念。我们将建立一些与群元素阶相关的重要结论，这在后续学习中非常有用。

定义 3.3.2 在群 G 中，一个元素 a 的阶（order）是最小的正整数 n，使得 $a^n = 1$。如果不存在这样的正整数，则称 a 的阶是无限的。

在群 G 中，若存在 $c \in G$ 使得 $a = c^{-1}bc$，则称 a 与 b *共轭*（conjugate）。显然，a 与 b 共轭当且仅当 b 与 a 共轭。因此，谈论共轭时哪一个在前并不重要。（事实上，共轭关系是一个等价关系——请自行验证。）

命题 3.3.1 若 a 与 b 共轭，则它们的阶相同：$\mathrm{order}(a) = \mathrm{order}(b)$。

例 3.3.5 在例 3.1.2 中的几何变换群中，120° 顺时针旋转与 120° 逆时针旋转都是 3 阶元素。它们是共轭的：若对 120° 顺时针旋转前后各施加一次镜像对称变换，其效果就是一次 120° 逆时针旋转。

为了进一步熟悉共轭的概念，我们可以尝试一个更有挑战的问题。

例 3.3.6 下面给出**柯西-弗罗贝尼乌斯引理**（Cauchy–Frobenius Lemma）（也称**伯恩赛德引理**（Burnside's Lemma））[①]的一种特殊情况。请写出您的证明。

设 G 是一个 n 阶群。对任意元素 $x \in G$，x 的所有共轭元素构成的集合称为一个*共轭类*（conjugacy class）。容易看出，所有共轭类构成群 G 的一个划分。设共轭类的个数为 k，请证明：

$$|\{(a,b) \in G^2 : ab = ba\}| = kn$$

解答： 考虑任意一个共轭类 C。显然，我们只需证明

$$|\{(a,b) \in C \times G : ab = ba\}| = n$$

首先，我们证明对所有 $c \in C$，集合 $\{(c,b) : cb = bc, b \in G\}$ 的大小是常数（即，c 变化时其大小不变）。设 $c_0 = \arg\max_c |\{(c,b) : cb = bc, b \in G\}|$。对于任意其他元素 $g^{-1}c_0g \in C$，容易验证 $c_0b = bc_0$ 意味着

$$g^{-1}c_0g \cdot g^{-1}bg = g^{-1}bg \cdot g^{-1}c_0g$$

因此，

$$|\{(g^{-1}c_0g, b) : g^{-1}c_0g \cdot b = b \cdot g^{-1}c_0g, b \in G\}| \geqslant |\{(c_0,b) : c_0b = bc_0, b \in G\}|$$

由于这个不等式的右边已经是最大值，左右两边只能相等。这也就说明，对所有 $c \in C$，集合 $\{(c,b) : cb = bc, b \in G\}$ 的大小是相等的。

---

① 该引理最早由法国数学家柯西（本书后面会予以介绍）证明，后来德国数学家弗罗贝尼乌斯也独立证明了该引理。然而，英语国家的大量读者从英国数学家伯恩赛德的著作中首次学到该引理，因而将其误称为伯恩赛德引理。在此段史实得到澄清后，部分数学家幽默地称之为“那条不属于伯恩赛德的引理”（the lemma that is not Burnside's）。

接下来，固定 $c \in C$，证明

$$|\{(c,b) : cb = bc, b \in G\}| = \frac{n}{|C|}$$

设 $C = \{g_1^{-1}cg_1, g_2^{-1}cg_2, \cdots, g_{|C|}^{-1}cg_{|C|}\}$。由于 C 包含 c 的所有共轭元，对于每个 $g \in G$，存在某个 g_i 使得 $g^{-1}cg = g_i^{-1}cg_i$。据此我们可以将 G 分成 $|C|$ 个互不相交的子集 $S_1, S_2, \cdots, S_{|C|}$，将 g 放入 S_i 当且仅当 $g^{-1}cg = g_i^{-1}cg_i$。由于对任意不同的 i, j 都有 $g_i^{-1}cg_i \neq g_j^{-1}cg_j$，所以划分是良定义的。

我们接下来证明这些子集大小相等。对 $i \neq j$，令

$$\varphi : g \mapsto g_i g^{-1} g_j$$

对 $g \in S_i$，有

$$g^{-1}cg = g_i^{-1}cg_i \Rightarrow c = gg_i^{-1}cg_ig^{-1} \Rightarrow g_j^{-1}cg_j = g_j^{-1}gg_i^{-1}cg_ig^{-1}g_j$$

所以 $g_ig^{-1}g_j \in S_j$。易见该映射是单射，故 $|S_i| \leqslant |S_j|$。根据对称性，立刻得到 $|S_j| \leqslant |S_i|$，于是 $|S_i| = |S_j|$。可见 G 被划分成这些等势子集，每个子集的势为 $\dfrac{n}{|C|}$。

考虑子集 $S = \{g | g^{-1}cg = c, g \in G\}$，其势正是使 $cb = bc$ 的 b 的数量。因此，

$$|\{(c,b) : cb = bc, b \in G\}| = \frac{n}{|C|}$$

所以，每个共轭类 C 中都有 $|C| \cdot \dfrac{n}{|C|} = n$ 对可交换的元素 $(a,b) \in C \times G$。总共有 k 个共轭类，因此总的可交换的对数为：$|\{(a,b) \in G^2 : ab = ba\}| = kn$。 ■

群的势也被称为它的阶（order）。

命题 3.3.2 在有限群中，一个元素是生成元，当且仅当它的阶等于群的阶。

证明： 设 G 是循环群，生成元为 g，$|G| = n$。

首先，我们证明 g 的阶 $\mathrm{order}(g) \geqslant n$。反设存在 $1 \leqslant \alpha < n$ 使得 $g^\alpha = 1$，则对任意整数 k，$g^k = g^{k \bmod \alpha}$，说明 G 中最多只有 $\alpha < n$ 个不同元素，矛盾。

其次，假设 $\mathrm{order}(g) > n$，则考虑 $g^0, g^1, \cdots, g^{\mathrm{order}(g)-1}$ 共 $\mathrm{order}(g)$ 个元素。因 $\mathrm{order}(g) > n$，它们不可能两两不同。所以，存在 $\alpha > \beta$ 使得 $g^\alpha = g^\beta$，即 $g^{\alpha-\beta} = 1$，与 $\mathrm{order}(g)$ 的最小性矛盾。

最后，若 $\mathrm{order}(g) = |G|$，则 $g^0, g^1, \cdots, g^{\mathrm{order}(g)-1}$ 两两不同且共有 $|G|$ 个，因此 g 为生成元。 ■

定理 3.3.1 设 G 是有限群，则对任意 $a \in G$，a 的阶 $\mathrm{order}(a)$ 能整除 $|G|$。因此，$a^{|G|} = 1$。

证明： 设 $S = \{1, a, a^2, \cdots, a^{\mathrm{order}(a)-1}\}$。若 $a^\alpha = a^\beta$ 且 $\alpha > \beta$，则 $a^{\alpha-\beta} = 1$，与 $\mathrm{order}(a)$ 的最小性矛盾。因此 S 中元素两两不同。容易验证 S 是循环子群，a 是生成元。由命题 3.3.2 知 $|S| = \mathrm{order}(a)$。

由于 $S \leqslant G$，由拉格朗日定理得 $\mathrm{order}(a)$ 能整除 $|G|$。从而 $a^{|G|} = 1$。 ■

上述定理中的构造循环子群的技巧非常实用。类似方法也可以用于解决下面的例题。

例 3.3.7 早在群的概念出现之前，高斯在他的名著《算术研究》中证明了一条数论定

理。如果我们将该定理用群论语言重新叙述一遍，那么会是这样的：

定理 3.3.2 设 $\mathbb{Z}_{2^n}^\star$ 表示模 2^n 的乘法群，易见该群的元素是 $1,3,5,\cdots,2^n-1$。对于每一个大于 2 的整数 n，$\mathbb{Z}_{2^n}^\star$ 都不是循环群。

请证明该定理。

解答： 首先，我们证明在任意有限循环群中，单位元 1 的平方根最多只有 2 个。设 G 是循环群，元素为 $g^0,g^1,\cdots,g^{n-1}$，两两不同。若 $(g^k)^2=1$，则 $g^{2k}=1$，说明 $n\mid 2k$。因 $0\leqslant 2k\leqslant 2(n-1)$，故只能有 $k=0$ 或 $k=\dfrac{n}{2}$ 两种情况。所以 1 的平方根至多是 1 和 $g^{n/2}$（若 n 为偶数）。

但在 $\mathbb{Z}_{2^n}^\star$ 中，1 有至少 4 个平方根：±1 与 $2^{n-1}\pm1$。因此，$\mathbb{Z}_{2^n}^\star$ 不是循环群。 ■

本题的另一做法由谢模阳同学给出；他于 2022 年春季修读本课程，当时是大一新生。

解答： 我们采用反证法。假设存在某个 $n\geqslant 3$，使得 $\mathbb{Z}_{2^n}^\star$ 是循环群，且 g 是其生成元。则存在整数 a_0、a_1、a_2、a_3，使得 $g^{a_i}\equiv 2i+1 \pmod{2^n}$（$i=0,1,2,3$）。这意味着

$$g^{a_i}\equiv 2i+1 \pmod 8$$

令 $g'=g \bmod 8$。显然 $g'\in\mathbb{Z}_8^\star$，且 $(g')^{a_i}\equiv 2i+1 \pmod 8$。由于 1、3、5、7 是 $\mathbb{Z}_8^\star$ 中的所有元素，g' 是 $\mathbb{Z}_8^\star$ 的生成元。然而，$\mathbb{Z}_8^\star$ 显然不是循环群，矛盾。 ■

接下来我们给出一个用于判断循环群的有用命题，以及一些精确刻画循环群的性质。

命题 3.3.3 素数阶群都是循环群。

证明： 由定理 3.3.1，该群中任一非单位元的阶只能是群的阶。这说明任一非单位元都是生成元，因此该群是循环群。 ■

定义 3.3.3 设 $(G,\ \cdot)$ 和 $(H,\star)$ 是两个群，f 是从 G 到 H 的函数。如果对所有 $a,b\in G$，有 $f(a\cdot b)=f(a)\star f(b)$，那么称 f 为一个**同态映射**（homomorphism）。若存在这样的同态映射，则称 G **同态**（homomorphic）于 H。

若这个同态映射是双射，则称其为**同构映射**（isomorphism）。此时，G 与 H **同构**（isomorphic），记作 $G\cong H$。

直观上，两个群同构意味着它们本质上是“相同”的群，只是元素和运算的命名不同。在数学中，我们通常不关心命名，因此同构的群常常被视为“相同”的群。

一个群同态于另一个群但不同构，意味着前者并不等同于后者，但它的结构可以在某种意义上被“压缩”或“简化”，从而得到后者。因此，后者保留了前者的某些性质，但并不保留全部性质。

例 3.3.8 在例 3.1.1 的克莱因四元群中，将 a、b、c 分别替换为 x、y、z，其余结构保持不变，得到另一个 4 阶群。定义映射 f 为：$f(a)=x,f(b)=y,f(c)=z,f(1)=1$。显然 f 是一个同构映射，从而这两个群同构。请注意：阶相同的群未必同构。

从例 3.1.2 中的几何变换群到 $(\{0,1\},\oplus)$ 可以建立如下同态映射：恒等变换、120° 顺时针旋转、120° 逆时针旋转映到 0；其余三个变换映到 1。这个同态映射不是同构映射，因为它不是双射。事实上，这两个群的阶不同，所以它们绝对不可能同构。

从例 3.1.1 中的克莱因四元群到例 3.1.2 中的几何变换群，不存在任何同态满射[①]。（您能看出为什么吗?）同样也不能找到从后者到前者的同态满射。（您能看出为什么吗?）

基于刚刚定义的同构，我们现在陈述关于循环群结构的基本结果，即命题 3.3.4 与命题 3.3.5。

命题 3.3.4 设 $\mathbb{Z}_n=\{0,1,\cdots,n-1\}$，$+_n$ 为模 n 加法运算。对于任意正整数 n，每个 n 阶循环群都与 $(\mathbb{Z}_n,+_n)$ 同构。

证明： 设 G 是一个 n 阶循环群，g 是其生成元。我们可以将 G 中的每个元素写成 g 的幂。定义从 G 到 $\mathbb{Z}_n$ 的函数 f：令 $f(g^k)=k \bmod n$。

对于任意 a、$b\in G$，存在整数 α、β，使得 $a=g^\alpha$，$b=g^\beta$。显然有：

$$f(a)=f(g^\alpha)=\alpha \bmod n,\quad f(b)=f(g^\beta)=\beta \bmod n,\quad f(ab)=f(g^{\alpha+\beta})=(\alpha+\beta) \bmod n$$

故 $f(a)+_n f(b)=f(ab)$，即 f 是群同态映射。

若 $f(g^\alpha)=f(g^\beta)$，则 $\alpha\equiv\beta\ (\mathrm{mod}\ n)$，从而 $g^\alpha=g^{\beta+tn}$。由于 G 的阶为 n，$g^{tn}=1$，故 $g^\alpha=g^\beta$，因此 f 是单射。

对任意 $\alpha\in\mathbb{Z}_n$，$g^\alpha\in G$ 且 $f(g^\alpha)=\alpha$，所以 f 是满射。综上，f 是双射，故 $G\cong\mathbb{Z}_n$。

■

命题 3.3.5 每一个无限循环群都与 $(\mathbb{Z},+)$ 同构。

命题 3.3.4 与命题 3.3.5 分别揭示了有限与无限循环群的结构。接下来我们从另一个角度看循环群：它们可以视作一种特殊的*有限生成群*（finitely generated group），定义如下。

命题 3.3.6 设 G 是一个群，对于任意 $a_1,a_2,\cdots,a_k\in G$，定义

$$\langle a_1,a_2,\cdots,a_k\rangle=\{b_1b_2\cdots b_m\mid b_i\in\{a_1,a_1^{-1},a_2,a_2^{-1},\cdots,a_k,a_k^{-1}\},m\in\mathbb{Z}^+\cup\{0\}\}$$

那么 $\langle a_1,a_2,\cdots,a_k\rangle$ 是 G 的一个子群，称为由 $a_1,a_2,\cdots,a_k$ *生成*的子群。

证明： 对于任意 $c,d\in\langle a_1,a_2,\cdots,a_k\rangle$，可写成 $c=b_1b_2\cdots b_u$，$d=b_1'b_2'\cdots b_v'$，其中所有 b_i,b_j' 均属于 $\{a_1,a_1^{-1},a_2,a_2^{-1},\cdots,a_k,a_k^{-1}\}$。则 $c^{-1}d=b_u^{-1}\cdots b_1^{-1}b_1'\cdots b_v'$ 仍属于 $\langle a_1,a_2,\cdots,a_k\rangle$。因此该集合在运算下封闭，构成子群。 ■

例 3.3.9 如前所述，例 3.1.1 中的克莱因四元群不是循环群，因此没有生成元。然而，它可以由 a、b 生成，也可以由 b、c 生成，或由 c、a 生成。因此 $\langle a,b\rangle=\langle b,c\rangle=\langle c,a\rangle$，等于该克莱因四元群本身。

类似地，例 3.1.2 中的几何变换群不是循环群，也没有生成元，但它可以由两个元素共同生成——120° 顺时针旋转、镜像对称变换。

从理论上讲，任一有限群都是有限生成的，因为它可以由所有元素共同生成。但在实际应用中，我们通常希望找到最小的生成元集合，如例 3.3.9 中那样。相对而言，一个无限群可能是有限生成的，也可能不是，见例 3.3.10。

例 3.3.10 所有整数 n 维向量的集合构成一个加法群。该无限群可以被 n 个向量生成：$(1,0,\cdots,0)$, $(0,1,\cdots,0)$, $\cdots$, $(0,0,\cdots,1)$。

---

① 如果不要求满射的话，从任意群 G 到任意群 H 总可以建立一个同态映射，因为只需要把 G 的每个元素都映射到单位元即可。

所有正实数构成一个乘法群。该无限群无法被任何有限子集有限生成，因为由有限集合生成的子群必然是可数的（为什么?），而该群是不可数的（为什么?）。

下面我们给出有限生成群的等价定义：

命题 3.3.7 设 G 是一个群，$a_1, a_2, \cdots, a_k \in G$，则有：

$$\langle a_1, a_2, \cdots, a_k \rangle = \bigcap_{a_1, a_2, \cdots, a_k \in H, H \leqslant G} H$$

证明： 设 $b_1 b_2 \cdots b_\ell \in \langle a_1, a_2, \cdots, a_k \rangle$。对所有满足 $a_1, a_2, \cdots, a_k \in H$ 且 $H \leqslant G$ 的子群 H，由于 $b_i \in H$，有 $b_1 b_2 \cdots b_\ell \in H$。因此，

$$\langle a_1, a_2, \cdots, a_k \rangle \subseteq \bigcap_{a_1, a_2, \cdots, a_k \in H, H \leqslant G} H$$

另一方面，$\langle a_1, a_2, \cdots, a_k \rangle$ 本身是一个包含 $a_1, a_2, \cdots, a_k$ 的子群，于是

$$\bigcap_{a_1, a_2, \cdots, a_k \in H, H \leqslant G} H \subseteq \langle a_1, a_2, \cdots, a_k \rangle$$

两式结合即可得证。 ■

正如前面所述，循环群是一种特殊的有限生成群。更具体地说，它是由单个元素生成的群。

命题 3.3.8 在群 G 中，$g \in G$ 是生成元当且仅当 $G = \langle g \rangle$。若 g 的阶 $\operatorname{order}(g)$ 是有限的，则

$$\langle g \rangle = \{1, g, \cdots, g^{\operatorname{order}(g)-1}\}$$

在学习了有限生成群之后，我们来看一个例题来巩固理解。

例 3.3.11 以下定理在 19 世纪便已经出现（参见文献 [90]），请给出您的证明。

定理 3.3.3 设 G 是由 n 个元素生成的阿贝尔群，则 G 的任意子群都可以由不超过 n 个元素生成。

一个容易想到的思路是：G 的生成元中某些可能也能生成子群，因此子群的生成元个数不超过 n。但这个思路并不总是正确，因为子群可能不包含任何原始生成元。例如，考虑加法群 $\mathbb{Z}_4$ 及其子群 $\{0, 2\}$，虽然 $\mathbb{Z}_4$ 是由 1 生成的，但 $\{0, 2\}$ 并不包含 1。所以我们需要换一种方法。

仔细观察可以发现，线性代数可能有所帮助。下面是一种“伪解”：

伪解： 设 $G = \langle g_1, g_2, \cdots, g_n \rangle$。由于 G 是阿贝尔群，G 中任一元素可表示为 $g_1^{k_1} g_2^{k_2} \cdots g_n^{k_n}$，其中 $k_1, k_2, \cdots, k_n \in \mathbb{Z}$。即每个元素对应一个整数向量 $(k_1, k_2, \cdots, k_n)$，可称为该元素的坐标向量。

我们可以验证，子群中的所有坐标向量构成一个“线性子空间”：对于任意两个向量 $(k_1, k_2, \cdots, k_n)$ 与 $(j_1, j_2, \cdots, j_n)$，它们的和为 $(k_1 + j_1, k_2 + j_2, \cdots, k_n + j_n)$，对应元素为 $g_1^{k_1+j_1} g_2^{k_2+j_2} \cdots g_n^{k_n+j_n}$。只要 $g_1^{k_1} g_2^{k_2} \cdots g_n^{k_n}$ 与 $g_1^{j_1} g_2^{j_2} \cdots g_n^{j_n}$ 都属于子群，则它们之积也在子群中。同样，当我们将一个向量 $(k_1, k_2, \cdots, k_n)$ 乘以整数 m 时，结果为 $(mk_1, mk_2, \cdots, mk_n)$，对应元素为 $g_1^{mk_1} g_2^{mk_2} \cdots g_n^{mk_n}$，也仍属于子群（只要原始元素在子群中）。

因此，子群的坐标向量集合构成一个线性子空间，可以选出一组基。由于子群中的每个向量都是基的整系数线性组合，对应的群元素是相应幂的乘积，所以这些元素能生成该子群。基的维数不会超过 n，因此子群最多由 n 个元素生成。 ■

上述“伪解”尝试用线性代数来解决，然而其关于线性空间的定义是不规范的。当我们定义线性空间时，我们必须明确我们所选择的作为标量的数域（一个数域需要满足一些特殊性质，例如非零元素均有乘法逆元）；然而整数集合并不是数域，我们并不能把它作为标量的集合。而如果您选择使用实数域，那么由于没法保证所有子空间的基都是原空间基的整系数线性组合，上述的论证根本没办法生效。

为了真正解出例 3.3.11，我们将在 4.6 节里借助于格（lattice）。倘若您更喜欢不用格的解法，您也可以在文献 [18] 中找到另一个解答。

下面是关于循环群的子群的命题和例题。

命题 3.3.9 循环群的任意子群也是循环群。

证明： 设 G 是循环群，g 为其生成元。任意子群 H 可写为 $H=\{g^x \mid x\in X\}$，其中 $X\subseteq\mathbb{Z}$。令 $m=\gcd(X)$，则存在有限多个整数 $k_1,k_2,\cdots,k_t$，使得 $m=\sum_{i=1}^{t}k_ix_i$，其中 $\forall i,\ x_i\in X$。[①] 因此，

$$g^m=g^{\sum k_ix_i}=\prod(g^{x_i})^{k_i}\in H$$

对任意 $g^x\in H$，x 可被 m 整除，故 $g^x=(g^m)^{x/m}$。故 $H=\langle g^m\rangle$ 是循环群。 ■

例 3.3.12 若一个真子群没有包含于任何其他真子群之中，则称其为极大子群（maximal subgroup）。假如一个群有极大子群且只有不超过两个极大子群，那么它是什么群？

解答： 我们分两种情况：

第一种情况，只有一个极大子群。设 G 是群，H 是其唯一的极大子群。任取 $x\in G\setminus H$，考虑 $\langle x\rangle$。因为 $\langle x\rangle\not\subseteq H$，所以它无法被包含于任何极大子群中。因此只能是 $\langle x\rangle=G$，即 G 是循环群。

第二种情况，恰有两个极大子群。设 G 是群，H、K 是其仅有的两个极大子群。根据例3.2.4的结论，$H\cup K\neq G$。因此，可以取 $g\in G\setminus(H\cup K)$，考虑其生成的子群 $\langle g\rangle$。很显然，$\langle g\rangle$ 不是 H 的子群也不是 K 的子群，所以它只能是 G 本身。然而，这就意味着 G 是循环群。

综上，这个群只能为循环群。（当然，不是每个循环群都有不超过两个极大子群。您能否为上面讨论的两种情况各给出一个具体的循环群作为例子？更进一步的分析将依赖于后面学到的知识，您可以在学完本章后再予以思考。） ■

循环群的代数结构在数学的其他领域中产生了许多非常有趣的作用，比如在数学分析之中。回忆：实数的子集若在任意两个（不相等的）实数间都包含一个元素，则称其是稠密（dense）的。令人惊讶的是，以下结论是成立的。

---

① 您可能会怀疑，当 X 为无限集时，为什么能保证 $\gcd(X)$ 等于 X 中有限多个元素的线性组合？事实上，只要任取 $x\in X$，对于 x 的任何一个比 $\gcd(X)$ 大的约数 y，都存在 $x'\in X$，使得 $y\nmid x'$。由于这样的 y 只有有限多个，从而找到的 x' 也只有有限多个。我们把这些 x' 和原来的 x 放在一起组成一个有限集，立刻可以发现这个有限集的最大公约数等于 $\gcd(X)$(为什么？)，也就是等于 m。因此，$\gcd(X)$ 等于这个有限集中元素的一个线性组合。

定理 3.3.4 设 $\mathbb{R}$ 为实数集。若 S 是 $(\mathbb{R},+)$ 的非空真子群，则 S 要么是循环群，要么是稠密的。

证明： 显然 $a\in S$ 当且仅当 $-a\in S$。定义 $S^+=\{a>0\mid a\in S\}$。

情况 A： S^+ 有最小元 m。则所有元素为 m 的整数倍，否则会产生比 m 更小的正元素，矛盾。故 $S=\langle m\rangle$。

情况 B： S^+ 无最小元。则存在单调递减的正数列 $a_1>a_2>\cdots$，显然该数列必然收敛。于是，只要 k 足够大，就可以使得 $\epsilon=a_k-a_{k+1}$ 任意小。换句话说，S^+ 中存在任意小的元素 ϵ。而对于任意 $b>c\in\mathbb{R}^+$，我们选择 $\epsilon<b-c$，就可以保证 $c<(\lfloor c/\epsilon\rfloor+1)\epsilon<b$。而显然 $(\lfloor c/\epsilon\rfloor+1)\epsilon\in S^+$。这说明 S^+ 在正实数中稠密。由对称性，S 在 $\mathbb{R}$ 中稠密。 ■

例 3.3.13 对于一个正数 x 而言，如果存在 $d\in\{1,2,\cdots,9\}$ 和整数 k，使得 $x\in[d\cdot 10^k,(d+1)\cdot 10^k)$，那么就称 x **以数字 d 开头**。（请注意，这个定义与我们的直觉是一致的。这里的所谓以数字 d 开头，就是指在十进制下，最高位的非 0 数字为 d。）

现在假设 m 是一个正整数，d 是一个不等于 0 的十进制数字。倘若在集合 $\{m^k\mid k\in\mathbb{Z}\}$ 中只有有限多个（可以为 0 个）元素以数字 d 开头，求 m 和 d 的值。

解答： 若 $m=10^t$（t 为整数），则显然 $\{m^k\mid k\in\mathbb{Z}\}$ 中所有的数都以数字 1 开头。因此当 $m=10^t$（t 为整数）且 $d\neq 1$ 时，以 d 开头的 m^k 恰好有 0 个（有限多个），满足题设要求。而若 $m=10^t$（t 为整数）且 $d=1$，则不满足题设要求。

下面证明没有其他解。也就是说，若 m 不是 10 的整数次幂，则对每个非 0 数字 d，$\{m^k\mid k\in\mathbb{Z}\}$ 中都有无限多个元素以 d 开头。

注意 m^k 以 d 开头当且仅当存在整数 ℓ，使得 $m^k\cdot 10^{-\ell}\in[d,d+1)$。后面这个式子等价于 $k\log_{10}m-\ell\in[\log_{10}d,\log_{10}(d+1))$。于是，我们考虑集合 $S=\{k\log_{10}m-\ell\mid k,\ell\in\mathbb{Z}\}$。容易看出 $(S,+)$ 是一个群。（怎么看出来的？您看出来了吗？）同样容易看出，$(S,+)$ 不是循环群—倘若它是循环群，则立刻可以推出 m 是 10 的整数次幂，矛盾。（怎么推出的？请您推一推。）因此得到 S 是稠密的，也就意味着 S 有无限多个元素属于区间 $[\log_{10}d,\log_{10}(d+1))$。（还记得从稠密性怎么得到区间含有无限多个元素吗？）

综上所述，满足条件的解仅为 $m=10^t$（t 为整数），$d\in\{2,3,\cdots,9\}$。 ■

习 题 集 6

习题 93 (难度 1.3) 设 $(G,\cdot)$ 为一个群 $(|G|\geqslant 2)$，X 为任意非空集合 $(|X|\geqslant 2)$。又设 $a\in G, a\neq 1$。令 $F=\{f:X\to G\}$。定义 F 上的二元运算 $+$ 为：$(f+g)(x)=f(x)\cdot g(x)$。容易看出 $(F,+)$ 是一个群。（您看出来了吗？）

（1）请找出 $(F,+)$ 的一个大于 1 阶的真子群。

（2）请找出 $(F,+)$ 的一个大于 1 阶的循环子群。

习题 94 (难度 0.5) 在集合 $\mathbb{R}$ 上定义二元运算 $\star$：$a\star b=\max\{a,b\}$。然后定义二元运算 $\sharp$：$a\sharp b=2a-b$。

（1）运算 $\star$ 在 $\mathbb{R}$ 上是否满足交换律？是否满足结合律？是否满足消去律？

（2）运算$\sharp$在$\mathbb{R}$上是否满足交换律？是否满足结合律？是否满足消去律？

习题 95 (难度1.5) 请找到一个非阿贝尔群G ($|G| \geqslant 2$)以及 $S \subset G$ ($|S| \geqslant 2$)，使得S既是某个子群的左陪集，又是另外一个子群的右陪集。

习题 96 (难度1.8) 假设O是平面上一个固定的点，L是以O为端点的一条射线。G是L围绕O所做的旋转构成的集合。用P表示整系数多项式构成的集合。考虑G上的复合运算和P上的加法运算，不难看出，G和P都是群。（您看出来了吗？）是否存在$H \leqslant G$，使得$H \cong P$？

习题 97 (难度1.7) 假设G是有限群，并且$999 \leqslant |G| \leqslant 1000$。从$G$到其本身的同构映射$f$满足：对于任意$g \in G$, $f(g) = g^{998}$。求$|G|$。

提示：您可以使用 柯西定理：若 p 为素数且 $p \mid n$，则n阶群中存在p阶元素。

习题 98 (难度1.7) 设 G 为有限阿贝尔群，x是一个36阶元素，y 则是一个63阶元素。求xy的阶数。

习题 99 (难度2.5) 设$k > 2$为整数，$(S, \cdot)$ 为半群，而$\{A, B\}$ 为 S 的一个划分。如果 A（或 B）中的任意k个（可以相同的）元素的积总是属于 A（或 B），那么就可以保证$(A, \cdot)$ 和 $(B, \cdot)$之一必为半群，但无法保证$(A, \cdot)$ 和 $(B, \cdot)$均为半群。求满足以上条件的k的最小值。

习题 100 (难度2.7) 假设G为1000阶群。$S \subset G$且$|S| = 188$。已知S中的一个元素为8阶，且$\langle S\rangle \neq G$。求证：存在$T \subseteq G$ ($|T| \geqslant 200$) 使得对于任意$x \in T$，都存在$u, v \in S$满足$ux = xv$。

习题 101 (难度1.5) 设 G 是群，H 是其子群。定义关系：$R_L = \{(a, b) \mid a^{-1}b \in H\}$，$R_R = \{(a, b) \mid ab^{-1} \in H\}$。

（1）证明：R_L 和 R_R 都是等价关系。

（2）证明：R_L 的等价类是左陪集，R_R 的等价类是右陪集。

习题 102 假设G是一个群，$H \leqslant G$，$J \leqslant H$。并且$Z(G) \cap H = Z(H)$，$Z(H) \cap J = Z(J)$。如果在J中，$Z(J)$有无限多个左陪集，那么在G中$Z(G)$是否有可能只有有限多个左陪集？

习题 103 (难度1.8) 是否存在一个阿贝尔群，其元素的阶正好包含$1, 2, \cdots, 2020$，而不包含任何大于 2020 的整数或者无穷？若存在，请构造一个；若不存在，请证明。

习题 104 (难度1.8) 证明：对任意正整数 k，有限生成群 $\langle a_1, a_2, \cdots, a_k\rangle$ 是可数集。

习题 105 (难度3.1) 回忆对于集合A和B，符号AB可以表示集合$\{ab | a \in A, b \in B\}$。因此，我们可以用$A^k$来表示集合$\{a^k | a \in A\}$。请注意$A^k$这个符号也可以用来表示$k$个集合$A$的笛卡儿积。所以每次该符号出现时，其意义需要按照上下文来理解。

请为以下定理给出您的证明。

定理 3.3.5 (循环群子群结构定理) 群 G 是循环群，当且仅当其任意子群都可以表示为 G^m（m 为非负整数）。

习题 106 (难度2.3) m阶群G是由n个不同元素$a_1, a_2, \cdots, a_n$生成的（m、n均为正整数）。证明：存在一个序列$b_0, b_1, b_2, \cdots, b_{mn-1}$满足以下条件：$G$的每个元素在该序列中都恰好出现$n$次；对于每个$i (0 \leqslant i \leqslant mn-1,\ i \in \mathbb{Z})$，都存在$a_j$ ($1 \leqslant j \leqslant n,\ j \in \mathbb{Z}$)使得$b_i = b_{(i+1) \bmod mn} a_j$或者$b_i = b_{(i+1) \bmod mn} a_j^{-1}$。

习题 107 (难度2.9) 设G是一个群，且G所有元素的阶都是奇数。若对任意$x, y \in G$，都有$(x^{-1}y^{-1})^2(xy)^2 = 1$，证明：对于任意$x, y \in G$，都有$(xyx)^2 = yx^4y$。

习题 108 (难度 3.1) 关于有限指数的子群，我们有如下两个定理。

定理 3.3.6 若 A、B 均为群 G 的有限指数的子群，则有：

$$[G : A \cap B] \leqslant [G : A][G : B]$$

等号成立当且仅当 $G = AB$。

定理 3.3.7 若 A、B 均为群 G 的有限指数的子群，且两个指数互质，则 AB 也是 G 的子群，并且

$$[G : AB] = \frac{[G : A][G : B]}{[A : A \cap B]}$$

请利用定理 3.3.6来证明定理 3.3.7的前一半，即证明 AB 为子群即可，不需要证明关于其指数的等式。

习题 109 (难度 0.9) 设 G 是有限生成群。若对任意 $g \in G$，都有 $g^2 = 1$，证明：G 是有限群。

习题 110 假设 G 为一个有限阶群。求证：如果 G 中有元素具有不止一个平方根，那么单位元一定具有不止一个平方根。

提示：您还是可以使用 *柯西定理*：若 p 为素数且 $p \mid n$，则 n 阶群中存在 p 阶元素。

习题 111 (难度 3.2) 假设 G 为群，但并非阿贝尔群，$H < G$。对任意 $x \in G \setminus H$ 和 $y \in G$，存在唯一的 $h \in H$ 使得 $y^{-1}xy = h^{-1}xh$。证明：存在至少两个不同的子群 C_1、$C_2 \leqslant G$ 满足下列 2 个条件。

（1）$G = C_1H = C_2H$。

（2）$C_1 \cap H = C_2 \cap H = \{1\}$。

习题 112 (难度 2.9) 一个域（field）是满足以下 3 条性质的 $(F, +, \cdot)$：（1）$(F, +)$ 是阿贝尔群，其单位元记作 0；（2）$(F \setminus \{0\}, \cdot)$ 也是阿贝尔群，其单位元记作 1；（3）对所有 a、b、$c \in F$，有 $a \cdot (b + c) = ab + ac$。

对正整数 n，定义 na 为 n 个 a 相加得到的和。定义一个域的特征（characteristic）为最小正整数 n，使得对任意 $a \in F$，$na = 0$。如果没有这样的正整数，那么特征为 0。

现在设 F 是一个域，其子集 $\{a_0, a_1, \cdots, a_{15}\}$ 中恰好含有一个 0。对每个 $i = 0, 1, \cdots, 15$，定义 $b_i = \sum_{j=1}^{8} a_{(j+i) \bmod 16}$。已知 $b_0, b_1, \cdots, b_{15}$ 是 $a_0, a_1, \cdots, a_{15}$ 的一个排列。又已知 b_0 有两个不相等的平方根。求域 F 的特征。

写作题

习题 113 $SO(3)$，即三维空间中所有旋转构成的群，在机器人研究中具有重要作用。请在不超过 1000 字的篇幅内说明其用途及重要性。

3.4 正规子群、商群与同构定理

我们已经学习了子群与陪集。对任意子群，其对应的左陪集或右陪集可以将整个群划分为若干个等大小的部分，这是一个非常强的结果。然而，一个不那么令人满意的事实是：

左陪集未必等于右陪集，反之亦然。这使我们思考：是否真的存在一个叫“陪集”的东西，还是说实际上只有左陪集与右陪集，所谓“陪集”只是这两个概念的统称？

事实上，存在一类特殊的子群，称为**正规子群**，它们使得左陪集与右陪集总是相等。对于这些子群，我们无须区分左右陪集，而可以直接称之为“陪集”（coset）。

定义 3.4.1 设 G 是一个群，若对所有 $a \in G$，都有 $aH = Ha$，则称 H 为 G 的一个**正规子群**（normal subgroup），记作 $H \trianglelefteq G$。

例 3.4.1 与例 3.2.1 类似，考虑一个任意群 $(G, \cdot)$。我们研究其中的若干子群是否为正规子群：

- 最大子群 G 本身与最小子群 $\{1\}$ 显然都是正规子群。
- 群的中心 $Z(G) = \{c \in G \mid \forall a \in G, ac = ca\}$ 也是正规子群。
- 而对于任意子集 $S \subseteq G$，集合 $\{c \in G \mid \forall a \in S, ac = ca\}$ 不一定是正规子群。（您能给出一个不是正规子群的具体例子来吗？）

例 3.4.2 回忆例 3.2.2 中的几何变换群 G 及其子群 S。问：S 是否为正规子群？

解答： 设 a 为 120° 顺时针旋转，b 为镜像对称变换。则 $aS = \{a, ab\} \neq \{a, ba\} = Sa$，因此 S 不是正规子群。 ■

例 3.4.3 设 G 为有限群。倘若 G 的每个子群都是正规子群，那么称之为**戴德金群（Dedekind group）**。在文献中可以发现，数学家对戴德金群给出了很多种等价定义，下面是其中的两种。

（1）倘若对于有限群 G 的任意两个元素 a, b，都存在正整数 m 使得 $(ab)^m = ba$，就称 G 为戴德金群。

（2）倘若有限群 G 的每个循环子群都是正规子群，那么称 G 为戴德金群。

请证明这两种定义都与上面所给的标准定义等价。

解答： 我们先证明由（2）可以推出（1）。对任意 a、$b \in G$，由于 $\langle ab \rangle$ 是正规子群，故有 $b\langle ab \rangle b^{-1} = \langle ab \rangle$。于是，$ba = babb^{-1} \in \langle ab \rangle$，也就是存在整数 m 使得 $ba = (ab)^m$。考虑到 G 为有限群，$\langle ab \rangle$ 的阶数也必然有限，所以必然存在正整数 m 使得 $ba = (ab)^m$。

再证明（1）推出标准定义。对任意 a、$b \in G$，存在正整数 m 使

$$(b \cdot ab^{-1})^m = ab^{-1} \cdot b = a \implies ba^m b^{-1} = a \implies ba^m = ab$$

于是对任意子群 $H \leqslant G$，任意 $h \in H$ 与 $g \in G$，有 $hg = gh^m$，说明 $hg \in gH$，即 $Hg \subseteq gH$。由于 $|Hg| = |H| = |gH|$ 且 G 有限，故 $Hg = gH$，H 为正规子群。

最后，由标准定义推出（2）是平凡的。综上可知，（1）和（2）均与标准定义等价。 ■

给出正规子群的定义后，我们可以介绍几种判断正规子群的方法。首先，任何阿贝尔群的子群必为正规子群；其次，我们可以利用共轭来判断一个子群是否正规。

命题 3.4.1 设 G 是群，H 是其子群。则 H 是正规子群，当且仅当对所有 $g \in G$ 与 $h \in H$，$ghg^{-1} \in H$；换而言之，当且仅当 H 的所有共轭仍在 H 中。

第三，我们还观察到：若一个子群在群中是正规子群，那么它在包含它的任意子群中也必然是正规子群。

命题 3.4.2 设 G 是一个群，$H \leqslant G$。若 $J \subseteq H$ 且 $J \trianglelefteq G$，则有 $J \trianglelefteq H$。

命题 3.4.2 的逆命题是否成立？请看以下反例。

例 3.4.4 找出3个群 G、H、J，使得 $H \trianglelefteq G$，$J \trianglelefteq H$，但 $J \ntrianglelefteq G$。

解答： 考虑一个正方形。存在如下8个将其映射到自身的几何变换。

- 恒等变换；
- 90°、180°、270° 顺时针旋转；
- 镜像对称变换；
- 镜像对称后再进行 90°、180°、270° 顺时针旋转。

设 G 为上述8个变换构成的集合，$\cdot$ 为变换的复合，显然 $(G, \cdot)$ 是一个群。

令 H 为包含恒等变换、180° 旋转、镜像对称以及镜像对称后 180° 旋转的4个变换的集合。容易验证 H 是子群，且除了子群本身之外，其左（或右）陪集只有一个。因此 $H \trianglelefteq G$。

令 J 为只包含恒等变换和镜像对称的集合。显然 $J \leqslant H$ 且左右陪集重合，故 $J \trianglelefteq H$。

但若将 J 视为 G 的子群，注意 90° 旋转与镜像对称顺序不可调换，其左陪集与右陪集不同，故 $J \ntrianglelefteq G$。 ■

命题 3.4.3 设 G 是群，$H \trianglelefteq G$。对任意陪集 aH、bH，任意 $a' \in aH, b' \in bH$，有 $a'b' \in abH$。

根据命题 3.4.3，我们可以定义陪集之间的二元运算：对所有陪集 aH, bH，定义 $aH \cdot bH = abH$。该命题保证该定义良好，因为选取哪个元素为 a、选取哪个元素为 b 都不影响运算结果。这样，所有的陪集放在一起构成一个新的群，称为*商群*。

定义 3.4.2 设 G 是群，$H \trianglelefteq G$。则商群（quotient group）G/H 为 H 的所有陪集组成的集合，运算规则为：$aH \cdot bH = abH$。

命题 3.4.4 G/H 在上述运算下确实构成一个群。

例 3.4.5 回忆例 3.1.3 中的 $n \times n$ 非奇异实矩阵群 $M(n \geqslant 2)$。其中正规子群 $N = \{I, -I\}$。M 被划分为若干个大小为 2 的陪集。对任意 $A \in M$，其对应陪集为 $\{A, -A\}$。乘法运算可以在商群中进行，如：

$$\{A, -A\} \cdot \{B, -B\} = \{AB, -AB\}$$

例 3.4.6 假设 k 为奇数，G 为 $2k$ 阶群。证明：G 最多只有一个 k 阶子群。

解答： 反证法。若存在 J、$H \leqslant G$，使得 $|J| = |H| = k$ 且 $J \neq H$，则存在 $a \in J \setminus H$。由于 $a \in J$，$a^{|J|} = 1 \Rightarrow a^{|H|} = 1$。

另一方面，由于 $|G| = 2k$ 且 $|H| = k$，H 在 G 中除了自身之外只有一个左陪集和一个右陪集。因此，H 的左右陪集必然相等（为什么？），也就是说 H 为正规子群。考虑到 a 是左陪集 aH 的一个元素，在商群 G/H 中有 $(aH)^{|H|} = 1H$，即 $\mathrm{order}(aH)$ 能整除 $|H|$。又因 $\mathrm{order}(aH)$ 也能整除 $|G/H|$，所以 $\mathrm{order}(aH)$ 为 $|H| = k$ 与 $|G/H| = 2$ 的公因数。所以，我们得到 $\mathrm{order}(aH) = 1 \Rightarrow aH = H \Rightarrow a \in H$，矛盾。 ■

商群在群论中非常重要，因为它们与同态紧密相关。下面两个命题指出生成商群的正规子群就是某个群同态的核。

命题 3.4.5 设 G 是群，$f: G \to G'$ 是一个群同态（G' 可为 G 自身）。定义其（同态）核（kernel）

$$\text{kernel}(f) = \{x \in G \mid f(x) = 1\}$$

则 $\text{kernel}(f) \trianglelefteq G$。

命题 3.4.6 设 G 是群，$H \trianglelefteq G$，则存在一个群同态 $f: G \to G'$（G' 可为 G 自身），使得其同态核 $\text{kernel}(f) = H$。

证明： 我们定义一个函数 $f: G \to G/H$，令 $f(a) = aH$。对任意 $a, b \in G$，有

$$f(a) \cdot f(b) = aH \cdot bH = abH = f(ab)$$

因此 f 是一个群同态。显然 $f(a) = H$ 当且仅当 $a \in H$。因为 H 是商群 G/H 的单位元，所以 $\text{kernel}(f) = H$。 ■

关于群同构的主要定理至少有 4 个。标准教材（例如文献 [20, 50, 70]）对它们的命名各异，有时甚至令人困惑——简要总结见文献 [100]。下面我们介绍其中 3 个主要定理，并附上它们的部分命名方式。我们首先给出一个揭示正规子群与群同态之间本质联系的定理。

命题 3.4.5 和命题 3.4.6 告诉我们正规子群与群同态的核完全一致。而定理 3.4.1 更进一步说明：由正规子群生成的商群与该群同态的像是同构的。为了便于理解，我们在图 3.1 中对此进行了图示说明。

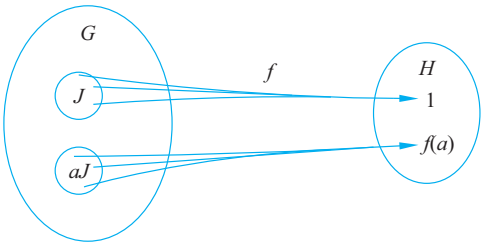

图 3.1 定理 3.4.1 的示意图

定理 3.4.1 (群同构第一定理 (First Isomorphism Theorem)；群同态基本定理 (Fundamental Theorem of Homomorphisms)) 设 G、H 是群，$f: G \to H$ 是一个群同态。则其像 $\text{image}(f)$ 是 H 的子群，且 $\text{image}(f) \cong G/\text{kernel}(f)$。

证明： 对任意 a、$b \in \text{image}(f)$，存在 c、$d \in G$，使得 $f(c) = a, f(d) = b$。则

$$a^{-1}b = f(c)^{-1}f(d) = f(c^{-1}d) \in \text{image}(f)$$

所以 $\text{image}(f) \leqslant H$。

令 $J = \text{kernel}(f)$，定义函数 $g: G/J \to \text{image}(f)$ 为 $g(aJ) = f(a)$。注意该定义是良好的，若 $a' \in aJ$，则存在 $j \in J$ 使得 $a' = aj$，于是

$$f(a') = f(aj) = f(a)f(j) = f(a) \cdot 1 = f(a)$$

所以陪集中元素的选择不影响映射值。

对任意 aJ、$bJ \in G/J$，有

$$g(aJ)\cdot g(bJ)=f(a)f(b)=f(ab)=g(abJ)$$

故 g 是同态映射。

若 $g(aJ)=g(bJ)$，则 $f(a)=f(b)\Rightarrow f(ab^{-1})=1\Rightarrow ab^{-1}\in J$，即 $aJ=bJ$，故 g 是单射。

对任意 $a\in\mathrm{image}(f)$，存在 $a'\in G$，使得 $f(a')=a$，于是 $g(a'J)=a$，故 g 是满射。

综上，g 是同态映射也是双射，所以 $G/J\cong\mathrm{image}(f)$。 ■

例 3.4.7 回忆例 3.1.2 中的几何变换群 G。设 $H=(\{0,1\},\oplus)$。定义函数 $f:G\to H$，将恒等变换及两个旋转映射为 0，将其余 3 个变换映射为 1。容易验证 f 为群同态，其核 $\mathrm{kernel}(f)$ 为恒等变换和两个旋转构成的集合。商群 $G/\mathrm{kernel}(f)$ 含两个元素：$\mathrm{kernel}(f)$ 与其补集。可验证该商群与 H 同构，这正是定理 3.4.1 所描述的。

定理 3.4.1 涉及两个群，其中一个是另一个的正规子群。接下来我们考虑更复杂的情形，即存在三个群，每个较小的群是较大的群的正规子群。图 3.2 展示了该结构（以及后文定理 3.4.3）的示意图。

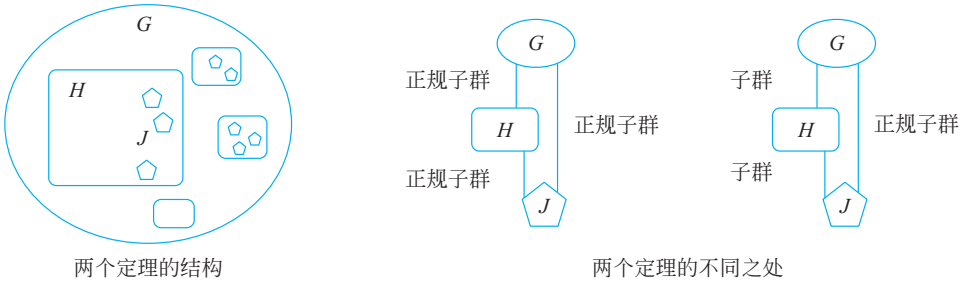

图 3.2 定理 3.4.2 与定理 3.4.3 的结构图示

定理 3.4.2 (群同构第一、第二或第三定理 (First, Second, or Third Theorem of Group Isomorphism)；大一新生定理 (Freshman Theorem)) 设 G、H、J 是群，满足 $J\leqslant H\leqslant G$，且 $J\trianglelefteq G$，$H\trianglelefteq G$。则有 $H/J\trianglelefteq G/J$，且

$$(G/J)/(H/J)\cong G/H$$

证明： 显然 $J\trianglelefteq H$。

首先我们证明 $H/J\leqslant G/J$。对任意 a_1J、$a_2J\in H/J$，必有 $(a_1J)^{-1}a_2J=a_1^{-1}a_2J\in H/J$。所以，$H/J\leqslant G/J$。

然后再证 $H/J\trianglelefteq G/J$。对任意 $aJ\in G/J$，需证 $aJ\cdot(H/J)=(H/J)\cdot aJ$。对任意 $bJ\in H/J$，有 $aJ\cdot bJ=abJ=b'aJ$，其中 $b'\in H$。于是 $aJ\cdot bJ=b'J\cdot aJ$，而 $b'J\in H/J$，故有

$$aJ\cdot H/J\subseteq H/J\cdot aJ$$

反之亦然。故 H/J 为 G/J 的正规子群。

接下来定义 $f:G/J\to G/H$，令 $f(aJ)=aH$。该定义良好（留作练习）。对任意 aJ、$bJ\in G/J$，有

$$f(aJ\cdot bJ)=f(abJ)=abH=aH\cdot bH=f(aJ)\cdot f(bJ)$$

故 f 是群同态。

由定理 3.4.1，$\text{image}(f) \cong (G/J)/\text{kernel}(f)$。又因 $f(aJ) = aH$，故 f 是满射，$\text{image}(f) = G/H$。

而 $\text{kernel}(f) = \{aJ \mid a \in H\} = H/J$。综上，

$$(G/J)/(H/J) \cong G/H$$

■

例 3.4.8 设 $G = (\mathbb{Z}_{30}, +_{30})$，$H = (\{0,5,10,15,20,25\}, +_{30})$，$J = (\{0,15\}, +_{30})$。很容易看出 $J \leqslant H \leqslant G$，$H \triangleleft G$，$J \triangleleft G$。商群 $G/J = \{\{0,15\},\{1,16\},\{2,17\},\cdots,\{14,29\}\}$。商群 $H/J = \{\{0,15\},\{5,20\},\{10,25\}\}$ 显然是 G/J 的一个子群。考虑到运算 $+_{30}$ 是可交换的，我们立即得到 H/J 是一个正规子群。我们可以进一步计算商群 $(G/J)/(H/J)$，其恰好包含 5 个元素。其中一个元素是 $H/J = \{\{0,15\},\{5,20\},\{10,25\}\}$ 本身；另一个元素是 $\{\{1,16\},\{6,21\},\{11,26\}\}$；还有一个元素是 $\{\{2,17\},\{7,22\},\{12,27\}\}$，以此类推。

作为对比，商群 G/H 也恰好包含 5 个元素。其中一个元素是 $H = \{0,5,10,15,20,25\}$ 本身；另一个元素是 $\{1,6,11,16,21,26\}$；还有一个元素是 $\{2,7,12,17,22,27\}$，以此类推。

正如定理 3.4.2 所述，有 $(G/J)/(H/J) \cong G/H$。

例 3.4.9 对于不小于 2 的整数 n 而言，n 阶**特殊线性群**（special linear group）是指所有行列式为 1 的 n 阶方阵构成的乘法群。如果一个上三角矩阵的对角元全部等于 1，那么称其为**幺幂**（unipotent）上三角矩阵。

（1）2 阶特殊线性群有一个子群 G，是由其中所有对角元为正的上三角矩阵构成的。请写出 G 的表达式。

（2）G 有一个子群 N，是由其中所有幺幂上三角矩阵构成的。请写出 N 的表达式。

（3）证明 $N \triangleleft G$。（$N \triangleleft G$ 的意思是 $N \trianglelefteq G$ 但 $N \neq G$。）

（4）请探索商群的结构—G/N 跟您熟悉的什么群同构？

（5）找出（可数）无限多个群 $N_1', N_2', \cdots$，满足 $N \triangleleft N_1' \triangleleft N_2' \triangleleft \cdots \triangleleft G$。

解答： （1）G 的表达式为

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| a, b \in \mathbb{R}, a > 0 \right\}$$

（2）N 的表达式为

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{R} \right\}$$

（3）既然已经知道 N 是子群，为了证明其为正规子群，我们只需要验证其左陪集等于右陪集。对所有 $a, b, b' \in \mathbb{R}$，$a > 0$，有

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab'+b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a^2 b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$$

因此，任意一个左陪集中的元素都属于相应的右陪集。同理也可以证明，任意一个右陪集中的元素也属于相应的左陪集。因此，每个左陪集都等于其对应的右陪集，从而 $N \trianglelefteq G$。

（4）现在我们考虑一个从 G 到 $\mathbb{R}$ 的函数 f，将一个矩阵映射为其左上角元素 a 的对

数 $\log a$。显然有

$$f\left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix}\right) = f\begin{pmatrix} a_1a_2 & a_1b_2+b_1a_2^{-1} \\ 0 & a_1^{-1}a_2^{-1} \end{pmatrix} = \log(a_1a_2)$$

$$= \log a_1 + \log a_2 = f\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix} + f\begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix}$$

这说明 f 是一个同态映射。显然，$\ker(f)=N$，$\mathrm{image}(f)=\mathbb{R}$。因此，$G/N\cong\mathbb{R}$。（这里的 $\mathbb{R}$ 指的是实数的加法群。） ■

第（5）问则不那么简单。看到这个问题时，读者可能不会立刻想到如何构造满足条件的正规子群。一个关键的观察是：此处的结构与定理 3.4.2 中的情形相似。特别地，如果我们成功构造出 $N_1', N_2', \cdots$，那么 $N_1'/N \lhd N_2'/N \lhd \cdots \lhd G/N \cong \mathbb{R}$。因此，我们可以考虑先在 $\mathbb{R}$ 中找出一个正规子群的无限序列，然后尝试将其作为 $N_1'/N, N_2'/N, \cdots$。例如，$\mathbb{Z} \lhd \frac{1}{2}\mathbb{Z} \lhd \frac{1}{4}\mathbb{Z} \lhd \cdots \lhd \mathbb{R}$ 是一个不错的选择。

（5）我们构造如下子集：对于每个正整数 k，

$$N_k' = \left\{ \begin{pmatrix} 2^c & b \\ 0 & 2^{-c} \end{pmatrix} \middle| b\in\mathbb{R},\ c\in\frac{1}{2^{k-1}}\mathbb{Z} \right\}$$

对所有 b_1、$b_2\in\mathbb{R}$，c_1、$c_2\in\frac{1}{2^{k-1}}\mathbb{Z}$，有

$$\begin{pmatrix} 2^{c_1} & b_1 \\ 0 & 2^{-c_1} \end{pmatrix}^{-1}\begin{pmatrix} 2^{c_2} & b_2 \\ 0 & 2^{-c_2} \end{pmatrix} = \begin{pmatrix} 2^{-c_1} & -b_1 \\ 0 & 2^{c_1} \end{pmatrix}\begin{pmatrix} 2^{c_2} & b_2 \\ 0 & 2^{-c_2} \end{pmatrix}$$

$$= \begin{pmatrix} 2^{c_2-c_1} & b_2 2^{-c_1} - b_1 2^{-c_2} \\ 0 & 2^{c_1-c_2} \end{pmatrix} \in N_k'$$

因此，N_k' 是一个（真）子群。对所有 a_1、b_1、$b_2\in\mathbb{R}$（$a_1>0$），$c\in\frac{1}{2^{k-1}}\mathbb{Z}$，有

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} 2^c & b_2 \\ 0 & 2^{-c} \end{pmatrix} = \begin{pmatrix} a_1 2^c & a_1b_2+b_1 2^{-c} \\ 0 & a_1^{-1}2^{-c} \end{pmatrix}$$

$$= \begin{pmatrix} 2^c & a_1(a_1b_2+b_1 2^{-c}-b_1 2^c) \\ 0 & 2^{-c} \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix}$$

这意味着任意一个左陪集中的元素都属于对应的右陪集。类似地也可以证明，任意一个右陪集中的元素也属于对应的左陪集。因此，每一个左陪集都等于其对应的右陪集，从而 N_k' 是 G 的正规子群。显然有 $N \lhd N_1' \lhd N_2' \lhd \cdots \lhd G$。

定理 3.4.2 讨论的是三层嵌套结构 $J\leqslant H\leqslant G$，其中 J 与 H 都是 G 的正规子群。我们接下来要考虑的是更一般的情形，其中中间层子群 H 不一定是正规子群。结果显示，每一个这样的中间层子群都对应于 G/J 的一个子群。从某种意义上说，定理 3.4.2 是我们下面将要证明的定理 3.4.3 的一个特例。不过由于定理 3.4.2 中涉及的是正规子群，我们可以获得关于商群的进一步结论；而在定理 3.4.3 所讨论的更一般的情形中，子群可能并不正规，因此我们无法谈论相应的商群结构。

定理 3.4.3 (群同构第三或第四定理 (Third or Fourth Theorem of Group Iso-

morphism)；对应定理 (Correspondence Theorem)；格定理 (Lattice Theorem)) 设 G 是一个群，$J \trianglelefteq G$。那么存在一个双射 f，从集合 $\{H \mid J \subseteq H,\ H \leqslant G\}$ 映射到集合 $\{H' \mid H' \leqslant G/J\}$，满足对任意 H 有 $f(H) = H/J$。

证明： 我们构造 f 如下：对于所有满足 $J \subseteq H$ 且 $H \leqslant G$ 的子群 H，令 $f(H) = \{aJ \mid a \in H\}$。显然 $f(H) \subseteq G/J$。由于 $J \trianglelefteq G$，可知 $J \trianglelefteq H$，因此 $f(H) = H/J$ 对每个 H 成立。

首先我们证明 $f(H) \leqslant G/J$。对任意 aJ、$bJ \in f(H)$，有 $(aJ)^{-1} \cdot bJ = a^{-1}bJ$。由于 a、$b \in H$，所以 $a^{-1}b \in H$，进而 $a^{-1}bJ \in f(H)$。因此 $f(H)$ 是 G/J 的子群。

接下来我们通过反证法证明 f 是单射。假设 $f(H_1) = f(H_2)$，但 $H_1 \neq H_2$。则必存在一个元素只属于 H_1 而不属于 H_2。不妨设 $a \in H_1$ 但 $a \notin H_2$。由于 $aJ \in f(H_1)$，且 $f(H_1) = f(H_2)$，所以 $aJ \in f(H_2)$。因此存在 $a' \in aJ$ 使得 $a' \in H_2$。但这意味着存在 $j \in J$ 满足 $a' = aj$，即 $a = a'j^{-1} \in H_2$，这与 $a \notin H_2$ 矛盾。

最后我们证明 f 是满射。对任意 $H' \leqslant G/J$，令 $H = \cup_{C \in H'} C$。显然 $f(H) = H'$，只需验证 $J \subseteq H$ 且 $H \leqslant G$。由于 $J = 1J \in H'$，显然 $J \subseteq H$。对任意 a_1、$a_2 \in H$，存在 C_1、$C_2 \in H'$ 使得 $a_1 \in C_1$，$a_2 \in C_2$，因此 $a_1^{-1}a_2 \in C_1^{-1}C_2$ $(C_1^{-1}C_2 \in H')$，也意味着 $a_1^{-1}a_2 \in H$。所以 H 对乘法封闭，并包含单位元与逆元，从而 $H \leqslant G$。

综上所述，f 是所需的双射。 ■

例 3.4.10 设群 G 的元素为形如 (a, b) 的有序对，其中 $a = 0$ 或 1，b 为来自例 3.1.2 的几何变换。群运算定义为 $(a, b)(a', b') = (a \oplus a', bb')$。令 $J = \{(0, \text{恒等}), (1, \text{恒等})\}$，显然有 $J \trianglelefteq G$。

由定理 3.4.3，所有包含 J 的 G 的子群对应于 G/J 的子群。例如，考虑 $H = \{(0, \text{恒等}), (1, \text{恒等}), (0, \text{镜像对称}), (1, \text{镜像对称})\}$。这是 G 的一个包含 J 的子群。它对应于 G/J 中的子群：

$$\{\{(0, \text{恒等}), (1, \text{恒等})\}, \{(0, \text{镜像对称}), (1, \text{镜像对称})\}\}$$

定理 3.4.3 可以应用于广泛的场景。下面我们用一个非平凡的问题来说明其用法。

例 3.4.11 设 G 是一个群，$N \trianglelefteq G$。商群 G/N 是由若干正有理数 $r_1, r_2, \cdots, r_k$（$k \geqslant 1$）有限生成的加法群。换言之，对任意 $x \in G/N$，存在整数 $c_1, c_2, \cdots, c_k$，使得 $x = c_1 r_1 + c_2 r_2 + \cdots + c_k r_k$。证明：对任意正整数 n，G 都具有一个正规子群 H，使得 $[G : H] = n$。

解答： 首先我们证明 G/N 是一个无限循环群。我们总可以将每个 r_i 改写为相同分母的形式：$r_i = \dfrac{p_i}{q}$。令 $p = \gcd(p_1, p_2, \cdots, p_k)$，那么 $x \in G/N$ 等价于 $x = c \cdot \dfrac{p}{q}$，其中 c 是整数。因此，G/N 是由 $\dfrac{p}{q}$ 生成的循环群，且是无限的。

接下来，由于 G/N 是无限循环群，它与整数加法群同构。后者具有指数为 n 的正规子群，即所有 n 的倍数组成的加法群。故 G/N 也有一个指数为 n 的正规子群。根据定理 3.4.3，这意味着 G 具有一个指数为 n 的正规子群，且该子群包含 N。 ■

3.5 柯西定理、p-群与西罗定理

在本节中，我们主要关注素数阶的群或子群。我们将首先给出一个重要结论：柯西定理（Cauchy's Theorem）[①]。在正式给出和证明适用于任意有限群的柯西定理之前，我们先证明一个适用于有限 Abel 群的特殊情形。

命题 3.5.1 设 G 是一个有限 Abel 群，p 是一个素数。若 $p \mid \text{order}(G)$，则 G 具有一个 p 阶子群。

证明： 使用数学归纳法对 $\text{order}(G)$ 进行归纳。当 $\text{order}(G) = 2$ 时，命题显然成立。

现在假设该命题对于所有 $\text{order}(G) < n$ 的情况成立，考虑 $\text{order}(G) = n$ 的情形。取 $a \in G$，令 $q = \text{order}(a)$。若 $p \mid q$，则 $\langle a^{\frac{q}{p}} \rangle$ 就是我们所需的 p 阶子群。若 $p \nmid q$，则由拉格朗日定理可知，$\dfrac{n}{q}$ 是正整数，且 $p \mid \dfrac{n}{q}$。由于 G 是 Abel 群，$\langle a \rangle \trianglelefteq G$。商群 $G/\langle a \rangle$ 的阶为 $\dfrac{n}{q}$。根据归纳假设，$G/\langle a \rangle$ 具有一个 p 阶子群 H。由于 p 阶群必为循环群，H 具有一个生成元 h，满足 $h^p = \langle a \rangle$ 且 $h \neq \langle a \rangle$。

现在取 $b \in h$。由 $h^p = \langle a \rangle$ 可得 $b^p \in \langle a \rangle$，即存在 k 使得 $b^p = a^k$。由于 $\gcd(p, q) = 1$，存在整数 u, v 使得 $up + vq = 1$。因此，

$$(a^{-uk}b)^p = a^{-ukp}b^p = a^{-ukp}a^k = a^{-ukp+k} = a^{-ukp-vkq+k} = 1$$

再因为 $b \notin \langle a \rangle$，可得 $a^{-uk}b \neq 1$，即 $\text{order}(a^{-uk}b) = p$，从而 $\langle a^{-uk}b \rangle$ 就是我们所需的 p 阶子群。 ■

实际上，我们证明了一个比命题 3.5.1更强的结论——我们找到了一个 p 阶的群元素，它可以作为该子群的生成元。

例 3.5.1 回忆例 3.1.1 中的克莱因四元群。它是一个有限 Abel 群，因此命题 3.5.1 适用。事实上，它的阶的唯一的素因子为 2，而且它确实具有 2 阶的子群：$\{1, a\}, \{1, b\}, \{1, c\}$ 都是其子群。

现在我们来给出柯西定理的完整表述及其证明。虽然该定理有多个不同的证明方法，我们选择展示 McKay [58] 提供的一种非常优美的证明方式[②]。

定理 3.5.1 (柯西定理 (Cauchy's Theorem)) 设 G 是一个有限群，p 是一个素数。如果 $p \mid \text{order}(G)$，则 G 具有一个 p 阶子群。

证明： 令 S 为满足这样条件的 p 元组构成的集合——每个 p 元组所有分量的乘积等于单位元，即

$$S = \{(a_1, a_2, \cdots, a_p) | a_1 a_2 \cdots a_p = 1, a_1, a_2, \cdots, a_p \in G\}$$

显然，$|S| = |G|^{p-1} \Rightarrow |S| \equiv 0 \pmod{p}$。在集合 S 上定义一个等价关系 $\sim$，若 b 是通过循环

① 奥古斯丁-路易 • 柯西（Augustin-Louis Cauchy，1789—1875），法国数学家、工程师、物理学家。其父曾担任法国参议院秘书长，因此他深度参与政治活动。作为保皇主义者，终其一生都拒绝向任何共和政府宣誓效忠。这一立场一度危及他在公立大学的教授任命。可能正因为这个原因，他与拉格朗日（Lagrange）关系密切，同时也与许多人为敌。柯西毕业于巴黎综合理工学院（Ecole Polytechnique），但他认为数学研究比工程实践更有趣。他一生撰写了大约 800 篇研究论文，您应该已经见过他证明的一些重要结果，并且今后还会继续看到。

② James H.McKay（1928—2012），美国数学家。1953 年获得华盛顿大学博士学位，在奥克兰大学度过大部分职业生涯。至今，该校仍设有以他名字命名的奖学金。他曾在 1972 年担任普特南数学竞赛的负责人。

平移 a 得到的，则有 $a \sim b$。（什么叫循环平移？把 $(a_1, a_2, \cdots, a_p)$ 变成 $(a_p, a_1, a_2, \cdots, a_{p-1})$ 是循环平移，变成 $(a_{p-1}, a_p, a_1, a_2, \cdots, a_{p-2})$ 也是循环平移，……，变成 $(a_2, \cdots, a_p, a_1)$ 同样是循环平移。）容易验证 $\sim$ 是一个等价关系，因此 S 被划分为若干个等价类。

这些等价类的大小只可能是 1 或 p：若 p 元组的所有分量都相同，则其等价类大小为 1；否则，其等价类大小为 p。

显然，$|S|$ 等于落在两种等价类中的 p 元组的个数之和。由于 $|S|$ 是 p 的倍数，落在大小为 p 的等价类中的 p 元组的个数之和也是 p 的倍数，可知落在大小为 1 的等价类中的 p 元组的个数之和也是 p 的倍数。考虑到 $\{(1, \cdots, 1)\}$ 构成一个大小为 1 的等价类，可知大小为 1 的等价类数量不为 0，其中包含的 p 元组数量之和也不为 0。从而我们至少可以找到 p 个 p 元组属于大小为 1 的等价类。从中去掉 $\{(1, \cdots, 1)\}$，我们就找到了 $p-1$ 个形式为 $(a, \cdots, a)$、满足 $a \neq 1$ 且 $a^p = 1$ 的元组。 ■

同样地，我们不仅得到了一个 p 阶的子群，也找到了其生成元。

例 3.5.2 回忆例 3.1.2 中的几何变换群。该群是非阿贝尔群，因此命题 3.5.1 不适用。然而，柯西定理仍然适用：由于该群为 6 阶，我们应能在其中找到一个 2 阶的子群和一个 3 阶的子群。事实上，镜像对称变换生成了一个 2 阶的循环子群，而 120° 顺时针旋转则生成了一个 3 阶的循环子群。

柯西定理的应用有时并不简单。下面我们通过几个例题来展示其应用方式。

例 3.5.3 一个群到其自身的同构映射称为该群的**自同构映射**（automorphism）。关于有限阿贝尔群的自同构映射有如下定理。

定理 3.5.2（幂自同构定理 (power automorphism theorem)） 设 G 是有限阿贝尔群，k 是正整数，则 $f(g) = g^k$ 为 G 的自同构映射当且仅当 k 与 $|G|$ 互质。

请予以证明。

解答： “当”较为简单，读者可以轻易自行写出。我们只证明“仅当”。

如果 H 是 G 的一个循环子群，且不被包含于更大的循环子群中，那么称 H 为 G 的一个*极大循环子群*。根据我们对柯西定理的证明，对于任意素数 $p \mid \mathrm{order}(G)$，一定存在一个 p 阶的循环子群。因此，G 中必存在一个极大循环子群 H 满足 $p \mid \mathrm{order}(H)$。若我们能证明 $\gcd(\mathrm{order}(H), k) = 1$，则 $p \nmid k$；而由于 $\mathrm{order}(G)$ 的每个素因子 p 都不整除 k，从而 $\gcd(\mathrm{order}(G), k) = 1$。

剩下的任务是证明 $\gcd(\mathrm{order}(H), k) = 1$。由于 f 是一个双射，存在 $a \in G$ 使得 $f(a) = h$，其中 h 是 H 的生成元。即 $a^k = h$。若 $a \notin H$，则 $\langle a \rangle$ 是更大的循环子群，与“H 是极大循环子群”矛盾。因此 $a \in H$，可写作 $a = h^\alpha$，于是有 $h^{\alpha k} = h \Rightarrow h^{\alpha k - 1} = 1$，从而 $\mathrm{order}(H) \mid \alpha k - 1$。所以存在整数 m 使得 $m \cdot \mathrm{order}(H) + \alpha k = 1$，即 $\gcd(\mathrm{order}(H), k) = 1$。 ■

例 3.5.4 证明：任何 15 阶的群都是循环群。

解答： 反证法。

设 G 是一个 15 阶的群，且它不是循环群。那么根据 Lagrange 定理，G 中非单位元的阶只能为 3 或 5。进一步地，根据柯西定理，G 必具有一个 5 阶的子群 H_1。

我们接下来证明：G 中不存在另一个5阶的子群。假设存在另一个5阶的子群 H_2。因为 $H_1 \cap H_2$ 也是一个子群，其阶必须整除 5，所以 $H_1 \cap H_2$ 只能是 $\{1\}$。换言之，$H_1 \setminus \{1\}$ 与 $H_2 \setminus \{1\}$ 互不相交。又因为5阶的群是循环群，我们不妨设 $H_1 \setminus \{1\} = \{h, h^2, h^3, h^4\}$，$H_2 \setminus \{1\} = \{g, g^2, g^3, g^4\}$。

考虑如下 25 个元素：$h^i g^j$，其中 i、$j \in \{0, 1, 2, 3, 4\}$。由于 G 的元素个数仅为 15，这 25 个元素中必有重复。设 $h^i g^j = h^k g^\ell$，则有 $h^{i-k} = g^{\ell-j}$。因为 $\{h, h^2, h^3, h^4\}$ 与 $\{g, g^2, g^3, g^4\}$ 不相交，只能有 $i - k = \ell - j = 0$，即 $(i, j) = (k, \ell)$，这与我们假设这些元素中存在重复矛盾。

因此，$G \setminus H_1$ 中的所有元素的阶为 3。考虑左陪集 $bH_1 = \{b, bh, bh^2, bh^3, bh^4\}$。显然，$b^2$ 不在 bH_1 或 H_1 中，因此 $b^2 H_1$ 是除去 H_1 与 bH_1 之外的第三个左陪集。我们接下来考察元素 hb，显然 $hb \notin H_1$。我们分两种情况讨论：

情况 A 若 $hb \in bH_1$。显然 $hb \neq b$，于是存在 $k \in \{1, 2, 3, 4\}$，使得 $hb = bh^k$。则：

$$1 = (bh)^3 = b(hb)hbh = b(bh^k)hbh = b^2 h^{k+1} bh = b^2 bh^{(k+1)k+1} = h^{k^2+k+1}$$

这意味着 $5 \mid (k^2 + k + 1)$，但对于 $k \in \{1, 2, 3, 4\}$，该式恒不成立，矛盾。（在上面的式子中，您能看出来为什么 $b^2 h^{k+1} bh = b^2 bh^{(k+1)k+1}$ 吗？提示：可以使用 $hb = bh^k$。）

情况 B 若 $hb \in b^2 H_1$，那么存在 $h' \in H_1$，使得 $hb = b^2 h'$，从而

$$hb^2 = b^2 h' b = b^{-1} h' b$$

这意味着 $\operatorname{order}(hb^2) = \operatorname{order}(h') = 5$，这与 H_1 之外的元素应为 3 阶相矛盾。

综上，G 必为循环群。 ■

尽管柯西定理如上所示非常有用，但我们还希望更进一步：我们关心的不仅是 p 阶的子群，更关心的是阶为 p 的幂的子群。

定义 3.5.1 对于素数 p，若群 G 的阶为 p^n（其中 n 为正整数），则称 G 是一个 *p-群*（p-group）。若某个 p 群是另一个群（或者它自身）的子群，则称它为后者的一个 *p-子群*（p-subgroup）。

命题 3.5.2 在一个 p 群中，所有元素的阶都是 p 的幂。

我们特别关注那些阶尽可能大的 p 子群，这种子群被称为*西罗*[①] *p-子群*。

定义 3.5.2 设 p 是一个素数，G 是一个群。若 G 的某个 p-子群不被包含于任何更大的 p-子群中，则称其为 G 的 *西罗 p-子群*（Sylow p-subgroup）。

例 3.5.5 回忆例 3.1.2 中的几何变换群。其阶为 6，因此其西罗 2-子群的阶为 2，西罗 3-子群的阶为 3。例 3.5.2 中所找出的两个循环子群正好是西罗 2-子群和西罗 3-子群。

再回忆我们在例 3.4.4 中构造的几何变换群，其阶为 8，因此它的西罗 2-子群的阶为 8，即该群本身就是其西罗 2-子群。

考虑一个新的几何变换群，即将正 120 边形映射到自身的所有变换构成的群，其阶为 240，故其西罗 2-子群的阶为 16。该西罗 2-子群可由一个镜像对称变换和一个 45° 顺时针（或逆时针）旋转生成。

① 彼得·西罗（Peter Sylow，1832—1918），挪威数学家。在担任中学教师和校长期间取得了群论方面的重要突破，后来也获得了大学教授职位和多个荣誉。

定理 3.5.3（西罗第一定理（Sylow's First Theorem）） 设 G 是一个有限群，p 是一个素数，若 $|G| = p^n m$，其中 $\gcd(p, m) = 1$，则有：

- 对所有 $1 \leqslant i \leqslant n$，$G$ 具有 p^i 阶子群。
- 每一个 p^i 阶的子群（$1 \leqslant i < n$）都是某个 p^{i+1} 阶子群的正规子群。

特别地，G 具有一个西罗 p-子群，其阶为 p^n。

我们略去西罗定理的证明（证明可参见标准教材）。下面我们用一个例题来展示西罗定理的应用。

例 3.5.6 请回忆：若一个真子群不是任何其他真子群的真子群，则称其为极大子群。假设有限群 G 恰好有 2 个极大子群。又已知对 $|G|$ 的每个素因子 p，G 的西罗 p-子群均为正规子群。证明：$|G|$ 不可能恰有 3 个素因子。

解答： 反证法。假设 G 有两个极大子群 M、N，且均为正规子群；$|G| = p^a q^b r^c$（p、q、r 为 3 个不同的素数，a、b、c 为正整数）。令 P、Q、R 分别为 G 的西罗-p 子群、西罗-q 子群、西罗-r 子群。M 和 N 这两个极大子群中，必然有一个包含 P、Q、R 中的两个，另外一个包含剩下的一个。不妨设 P、$Q \subset M$，$R \subseteq N$。商群 G/R 为 $p^a q^b$ 阶，所以我们令 X 为 G/R 的西罗-p 子群，Y 为 G/R 的西罗-q 子群。X 对应于 G 的一个 $p^a r^c$ 阶子群 X'，Y 对应于 G 的一个 $q^b r^c$ 阶子群 Y'。

现在我们考虑 X' 包含在哪个极大子群中。倘若 $X' \subseteq M$，则 $p^a r^c | \text{order}(M)$。由于 P、$Q \subset M$，我们又有 $p^a q^b | \text{order}(M)$。合在一起，得到 $p^a q^b r^c | \text{order}(M)$，显然不可能。所以，只能是 $X' \subseteq N$。同理可证，$Y' \subseteq N$。将 $X' \subseteq N$ 和 $Y' \subseteq N$ 合在一起，又可推出 $p^a q^b r^c | \text{order}(N)$，矛盾。 ■

3.6 对称群与置换

前几节讨论的是群的一般理论。本节我们将聚焦于一类特殊的群，称为*对称群*。这类群由*置换* 构成。

定义 3.6.1 集合 X 上的一个*置换*（permutation）是指一个从 X 到其自身的双射。

n 元对称群（symmetric group of degree n）指的是 $(S_n, \circ)$，其中 S_n 是所有 $\{1, 2, \cdots, n\}$ 上的置换构成的集合，$\circ$ 是函数的复合运算。如果 G 是一个无限集合上的所有置换组成的集合，那么 $(G, \circ)$ 是一个无限元对称群（symmetric group of infinite degree）。

例 3.6.1 令 f 为从 $\{1, 2, 3, 4\}$ 到 $\{1, 2, 3, 4\}$ 的函数，满足 $f(1) = 2$，$f(2) = 3$，$f(3) = 1$，$f(4) = 4$，那么 f 是 $\{1, 2, 3, 4\}$ 上的一个置换。

令 g 为从 $\{1, 2, 3, 4\}$ 到 $\{1, 2, 3, 4\}$ 的函数，满足 $g(1) = 4$，$g(2) = 3$，$g(3) = 2$，$g(4) = 1$，那么 g 也是 $\{1, 2, 3, 4\}$ 上的一个置换。

令 h 为从 $\{1, 2, 3, 4\}$ 到 $\{1, 2, 3, 4\}$ 的函数，满足 $h(1) = 1$，$h(2) = 1$，$h(3) = 2$，$h(4) = 3$，那么 h 不是一个置换，因为 $h(1) = h(2)$。

在 $\{1, 2, 3, 4\}$ 上总共有 $4! = 24$ 个置换，它们组成一个对称群 S_4。

恒等置换、f、f^2 共同组成了 S_4 的一个 3 阶子群。

为什么对称群如此重要，以至于我们需要专门用一整节来讨论它？因为从同构的意义上来说，所有的群本质上都是对称群。

定理 3.6.1 (凯莱定理（Cayley's Theorem）[①]) 每一个群都同构于某个对称群的某个子群。特别地，每个 n 阶群都同构于对称群 S_n 的某个子群。

该定理的证明超出本讲内容范围，感兴趣的读者可查阅抽象代数的标准教材。

例 3.6.2 回忆例 3.1.1 中的克莱因四元群。它同构于 S_4 的一个子群 $\{I, f_1, f_2, f_3\}$，其中：

- I 是恒等置换。
- $f_1(1)=2, f_1(2)=1, f_1(3)=3, f_1(4)=4$。
- $f_2(1)=1, f_2(2)=2, f_2(3)=4, f_2(4)=3$。
- $f_3(1)=2, f_3(2)=1, f_3(3)=4, f_3(4)=3$。

再回忆例 3.1.2 中的几何变换群，它同构于 S_3，而 S_3 是 S_6 的一个子群。请您自行写出具体的同构映射。

对于较大的集合上的置换，有时较难理解。一个简化理解的方法是将置换看作是若干对换（transposition）的积。所谓对换，是交换两个元素的位置。

定义 3.6.2 集合 X 上的一个对换是指满足以下条件的一个置换 f：存在 a、$b \in X$，$a \neq b$，使得 $f(a)=b, f(b)=a$；对所有 $c \in X \setminus \{a,b\}$ 则有 $f(c)=c$。我们将这样的对换记作 $(a\ b)$。

例 3.6.3 回忆例 3.6.1 中的置换 f，其中 $f(1)=2$，$f(2)=3$，$f(3)=1$，$f(4)=4$。它可写为 $f=f_1 \circ f_2$，其中：

- $f_1(1)=2, f_1(2)=1, f_1(3)=3, f_1(4)=4$。
- $f_2(1)=3, f_2(2)=2, f_2(3)=1, f_2(4)=4$。

显然 f_1 和 f_2 都是对换。我们可以记为 $f_1=(1\ 2)$，$f_2=(1\ 3)$，从而 $f=(1\ 2)(1\ 3)$。

命题 3.6.1 任意有限集合上的置换都可以表示为若干对换的乘积。

证明： 不妨设 f 是一个在集合 $\{1,2,\cdots,n\}$ 上的置换。开始时，我们设置一个从 1 到 n 的顺序排列。然后，我们反复对当前排列做以下工作，直到没有工作可做：从 $i=1$ 到 n，我们依次检查第 i 个位置上的元素是否为 $f(i)$。若是，则跳过该位置；若不是，我们把第 i 个位置上的元素和 $f(i)$ 对换。记录这个对换。（注意，这样的对换不会影响前 1 到 $i-1$ 个位置上已调整好的元素，因为它只涉及未就位的两个元素。）

最后，将所有记录下来的对换依次相乘，我们最终得到原置换 f。 ■

例 3.6.4 对于 $n \geqslant 2$，证明：要想生成对称群 S_n，需要的对换数量的最小值为 $n-1$。

解答： 首先证明，少于 $n-1$ 个对换不可能生成 S_n。此处需要用到一点图论知识，完全不懂图论的读者可以先翻到第 5 章尤其是 5.3 节，大致了解涉及的概念。

具体而言，将 $1,2,\cdots,n$ 作为 n 个顶点。为了生成 S_n，如果我们可以使用对换 $(i\ j)$，那么我们就将顶点 i 和顶点 j 用一条边连起来。将所有可以使用的对换都变成边之后，我们就

① 阿瑟·凯莱（Arthur Cayley，1821—1895），英国数学家，毕业于剑桥大学三一学院。由于当时学术职位紧缺，毕业后曾任律师多年。后来剑桥新设数学教授职位，他便放弃高薪律所工作，成为一位收入不高的职业数学家。他对代数学和代数几何做出了开创性贡献。

得到了一个图。现在考虑任意的$i,j\in\{1,2,\cdots,n\}$，因为$(i\ j)\in S_n$，在图中顶点i必然是从顶点j可达的。（为什么可达？想想看。）因此，整个图是连通的。而n个顶点的连通图最少有$n-1$条边，也就是说使用少于$n-1$个对换无法生成S_n。

然后证明，确实存在$n-1$个对换，能够生成S_n。具体而言，我们说的$n-1$个对换是$(1\ 2),(1\ 3),\cdots,(1\ n)$。由于$S_n$中的任意置换都可以写成若干对换的乘积，我们只需要证明S_n中每一个对换都可以由这$n-1$个对换得出。现在考虑任意的对换$(i\ j)\in S_n$。我们总可以将其写成$(i\ j)=(1\ i)(1\ j)(1\ i)$，因此命题得证。

直观来说，为了交换i和j，我们先将1与i交换，把1放到j的目标位置；然后将1与j交换，把j放到正确位置。现在1还占据着i的目标位置，因此我们再将它与i交换以完成整个交换。（这是否让您想起了某种排序算法？）■

另一种理解置换的方法是将其视为若干个轮换的乘积。所谓轮换，就是按一定顺序依次将一个元素放到第二个元素的位置，第二个放到第三个的位置，……，最后一个放回第一个的位置。（因此我们前面提到的对换其实就是长度为2的轮换。）

定义 3.6.3 集合X上的一个轮换（cycle）是指集合X上满足以下条件的一个置换f：存在k个不同的元素$a_1,a_2,\cdots,a_k\in X$，使得$f(a_1)=a_2,f(a_2)=a_3,\cdots,f(a_{k-1})=a_k,f(a_k)=a_1$；而对于所有$b\in X\setminus\{a_1,a_2,\cdots,a_k\}$，$f(b)=b$。我们将这样的轮换记作$(a_1\ a_2\ \cdots\ a_k)$。

如果两个轮换没有任何公共元素，我们称它们为互不相交的轮换（disjoint cycles）。如果一组轮换中任意两个都是互不相交的，我们就说这组轮换是互不相交的。

例 3.6.5 回忆例3.6.1中的置换f，其中$f(1)=2$，$f(2)=3$，$f(3)=1$，$f(4)=4$。这是一个轮换，可写作$f=(1\ 2\ 3)$。如果您觉得元素4没有出现看起来不太舒服，那么也可以把f写为两个轮换的乘积：$(1\ 2\ 3)(4)$。

再考虑一个在集合$\{1,2,3,4,5\}$上的置换g，其中$g(1)=3$，$g(3)=1$，$g(2)=4$，$g(4)=5$，$g(5)=2$。它可以写作$g=(1\ 3)(2\ 4\ 5)$。因此，g是两个互不相交的轮换$(1\ 3)$和$(2\ 4\ 5)$的乘积。显然，这个乘积也可以写作$(2\ 4\ 5)(1\ 3)$。一般而言，互不相交的轮换是可以交换的。（为什么？）

相比较而言，轮换$(1\ 2\ 3)$和$(3\ 4\ 5)$并非互不相交。它们的乘积为$(1\ 2\ 3)(3\ 4\ 5)=(1\ 2\ 4\ 5\ 3)$。倘若我们调换顺序，计算$(3\ 4\ 5)(1\ 2\ 3)$，就会得到一个不同的结果$(1\ 2\ 3\ 4\ 5)$。一般而言，具有公共元素的轮换是不可以交换的。

命题 3.6.2 任意有限集合上的置换都可以写成互不相交的轮换的乘积。

证明： 为简单起见，设f是集合$\{1,2,\cdots,n\}$上的置换。我们用归纳法来证明。

基础情形显然成立。假设对$n-1$或更小的情形结论成立，现在我们来证明n的情形。

若$f(1)=1$，那么该置换实际上是集合$\{2,3,\cdots,n\}$上的置换，所以直接使用归纳假设即可。

现在考虑$f(1)\neq1$的情形。定义$f^0(x)=x,f^1(x)=f(x),\cdots,f^{k+1}(x)=f(f^k(x))$。令$m>1$为最小的整数，使得$f^m(1)=1$。我们构造轮换$C_0=(1\ f(1)\ f^2(1)\ \cdots\ f^{m-1}(1))$。

接下来，我们将f限制到集合$\{1,2,\cdots,n\}\setminus\{1,f(1),\cdots,f^{m-1}(1)\}$上，利用归纳假设将其写作若干互不相交的轮换$C_1,C_2,\cdots,C_t$的乘积。

显然，$f = C_0C_1\cdots C_t$，命题得证。 ■

例 3.6.6 数论中有所谓威尔逊定理：对于每个质数 p，都有 $(p-1)! \equiv -1 \pmod p$。在4.1节中，您也会看到此定理的（数论）证明。但是在这里我们要提请读者注意：威尔逊定理也可以用群论方法来证明。更精确地说，我们可以利用西罗定理予以证明。当然，只用我们前面学习过的西罗第一定理恐怕不太够。以下的西罗第二与第三定理应该会有帮助。

定理 3.6.2 (西罗第二与第三定理 (Sylow's Second and Third Theorems)) 假设 G 是一个群，p 是质数，$|G| = p^r m$，其中 $p \nmid m$。

西罗第二定理：若 H_1、H_2 是 G 的两个西罗 p-子群，则存在 $a \in G$，使得 $H_1 = a^{-1}H_2a$。

西罗第三定理：G 中西罗 p-子群的个数 $\equiv 1 \pmod p$，并且能够整除 m。

解答： 由于 $|S_p| = p!$，其所有 p-子群的阶为 p。所以，所有 p-子群同时也是西罗 p-子群。每个 p-子群包含恒等元 1，以及 $p-1$ 个 p 阶的元素。容易证明，任意两个 p-子群除了 1 外没有公共元素（如何证明?）。因此，我们可以先统计所有 p 阶元素的个数，再除以 $p-1$ 得到西罗 p-子群的个数。

p 阶元素的个数是多少？恰好是长度为 p 的轮换个数，因为 S_p 中没有其他 p 阶的置换（请思考为什么）。这样的轮换个数是 $(p-1)!$，因此西罗 p-子群个数为 $(p-2)!$。

结合西罗第三定理得 $(p-2)! \equiv 1 \pmod p$，从而推出 $(p-1)! \equiv -1 \pmod p$。这就是威尔逊定理的一种非常有趣的证明方式，虽然不是最简单的——我们将在之后的数论部分中给出更容易的证明。 ■

如果我们允许轮换之间存在公共元素（即交叉），那么只用很少数量的轮换就可能生成一个较大的对称群。我们通过下面这个例题来说明这一点。

例 3.6.7 证明：存在一个对换和一个 4-轮换，它们可以一起生成整个对称群 S_5。

解答： 取 $\tau = (1\,5)$，$\gamma = (1\,2\,3\,4) \in S_5$。令 $c = \gamma\tau = (1\,2\,3\,4)(1\,5) = (1\,2\,3\,4\,5)$，这是一个 5-轮换。将 τ 通过 c 的幂次进行共轭，可以得到相邻对换：

$$c^{-1}\tau c = (1\,2), \qquad c^{-2}\tau c^2 = (2\,3), \qquad c^{-3}\tau c^3 = (3\,4), \qquad c^{-4}\tau c^4 = (4\,5)$$

这样我们得到了 $s_1 = (1\,2), s_2 = (2\,3), s_3 = (3\,4), s_4 = (4\,5)$。接下来说明这 4 个对换如何生成整个 S_5。

因为 S_5 中的每个置换都可以写成对换的乘积，只需要证明每个对换都可以由这四个对换生成。注意到，对任意 $1 \leqslant i < j \leqslant 5$，有如下恒等式：

$$(i\,j) = s_i s_{i+1} \cdots s_{j-2}\, s_{j-1}\, s_{j-2} \cdots s_{i+1} s_i$$

（直觉上可以理解为：一步步把 i 移到 j 的位置，在那里进行交换，再把它一步步移回来。）因此，s_1, s_2, s_3, s_4 确实可以生成所有的对换 $(i\,j)$。 ■

正如前面例 3.6.5中提到的那样，互不相交的轮换具有一个显著优势。

命题 3.6.3 互不相交的轮换是可交换的。也就是说，如果 C_1、C_2 是互不相交的轮换，那么 $C_1C_2 = C_2C_1$。

基于这个优势，我们非常希望将一个置换写成若干互不相交轮换的乘积。幸运的是，这种表示方式是唯一的。对于一个置换 f，我们称集合 $\{x, f(x), f(f(x)), \cdots\}$ 为一个**轨道**（orbit）。在将 f 写成互不相交轮换乘积的唯一表示中，每个轮换恰好对应一个轨道。例如，

设置换 f 作用于集合 $\{1,2,3,4,5,6\}$，且满足 $f(1)=2$，$f(2)=1$，$f(3)=3$，$f(4)=5$，$f(5)=6$，$f(6)=4$，则 f 有3个轨道：$\{1,2\}$、$\{3\}$ 和 $\{4,5,6\}$。因此，f 只有一种方式（注意：不考虑轮换的先后顺序）可被写成互不相交轮换的乘积：$f=(1\ 2)(3)(4\ 5\ 6)$。为简洁起见，我们通常省略单元素轮换 (3)，写作 $f=(1\ 2)(4\ 5\ 6)$。

例 3.6.8 设 n 是大于 2 的偶数。置换 f、g、$h\in S_n$ 满足

$$f\circ g=h\circ(1\ 3\ 5\ \cdots\ n-1)(2\ 4\ 6\ \cdots\ n)$$

用 $c(f)$、$c(g)$、$c(h)$ 分别表示 f、g、h 的轨道的个数。证明：

$$c(f)+c(g)+c(h)\leqslant 2n+2$$

解答： 我们首先证明一个一般性的引理：若 $f_1,f_2,\cdots,f_k\in S_n(k\geqslant 2)$，且 $f=f_1f_2\cdots f_k$，则

$$n-c(f)\leqslant(n-c(f_1))+(n-c(f_2))+\cdots+(n-c(f_k))$$

为了证明此引理，我们注意到，将整个置换作用在集合 $\{1,2,\cdots,n\}$ 上，可以被看作是依次处理每个轨道中的元素。再注意到，将 t 个元素组成的轨道放置好等价于执行一个 t 元轮换，这可以通过 $t-1$ 个对换完成（即依次将第 2 到第 t 个元素与第一个元素交换）。因此，执行整个置换最多需要 $n-c(f)$ 次对换。

利用归纳法可以轻易证明上述算法是最优的—也就是说，使用了最少的对换来实现置换。带着这一结论，我们来看引理中的不等式。不等式左边是实现置换 f 至少需要的对换次数。而不等式右边则是使用某个具体算法（依次将 $f_1,f_2,\cdots,f_k$ 这 k 个置换一一作用在集合 $\{1,2,\cdots,n\}$ 上，其中实现单个 f_i 时所使用的对换次数仍然是上述最优的这种）所需的对换次数。因此，不等式成立。

证完引理之后，我们回到本题。由于

$$(1\ 3\ 5\ \cdots\ n-1)(2\ 4\ 6\ \cdots\ n)=h^{-1}\circ f\circ g$$

使用引理可得

$$n-2\leqslant n-c(f)+n-c(g)+n-c(h^{-1})$$

不难看出 $c(h^{-1})=c(h)$（您能看出来吗?），于是

$$c(f)+c(g)+c(h)\leqslant 2n+2$$

■

例题 3.6.8 中研究的值 $n-c(f)$ 还有另一种写法：用 $\mathrm{Len}(C)$ 表示轮换 C 的长度。若 $f=C_1C_2\cdots C_k$，其中 $C_1,C_2,\cdots,C_k$ 是互不相交轮换，则有 $n-c(f)=\sum_{i=1}^{k}\mathrm{Len}(C_i)-k$。这个值的奇偶性非常重要，我们称其为置换 f 的奇偶性。

定义 3.6.4 若 $\sum_{i=1}^{k}\mathrm{Len}(C_i)-k$ 为奇数，则称 f 为**奇置换**（odd permutation）；若其为偶数，则称 f 为**偶置换**（even permutation）。

例 3.6.9 回顾例 3.6.5 中的置换 $f=(1\ 2\ 3)$，它是偶置换。

例 3.6.5 中的置换 $f_1=(1\ 3)(2\ 4\ 5)$ 是奇置换。

置换 $(1\ 2\ 3)(3\ 4\ 5)=(1\ 2\ 4\ 5\ 3)$ 也是偶置换。

置换 (1 2)(4 5 6)（或等价的 (1 2)(3)(4 5 6)）是奇置换。一般而言，$\sum \mathrm{Len}(C_i) - k$ 无论是否计入类似 (3) 的单元素轮换，其奇偶性都相同。

那么为什么我们需要如此“笨拙”的定义——为什么不能直接使用轮换长度之和的奇偶性作为整体置换的奇偶性呢？这是因为我们定义一个置换为奇置换或偶置换，是基于它可以被表示为奇数个还是偶数个对换的乘积。

命题 3.6.4 一个置换是奇置换（或偶置换）当且仅当它等于奇数个（或偶数个）对换的乘积。

证明：“必要性”较容易证明。我们将该置换写成互不相交轮换的乘积：$f = C_1C_2\cdots C_k$。每个轮换 $C_i = (a_1\ a_2\ \cdots\ a_{\mathrm{Len}(C_i)})$ 可写为 $\mathrm{Len}(C_i) - 1$ 个对换的乘积：$C_i = (a_{\mathrm{Len}(C_i)-1}\ a_{\mathrm{Len}(C_i)})\cdots(a_1\ a_2)$。因此，$f$ 是这些对换的乘积，这些对换的总数为 $\sum \mathrm{Len}(C_i) - k$。

为了证明“充分性”，我们对对换的数量做归纳。基本情形是仅含一个对换，显然成立。假设当对换个数 $\leqslant n-1$ 时命题成立，考虑 n 个对换的情形。设 f 是 $n-1$ 个对换的乘积，令 $(b_1\ b_2)$ 为第 n 个对换。我们只需证明 $f\circ(b_1\ b_2)$ 的奇偶性与 f 不同。我们把 f 写为互不相交轮换的乘积 $C_1C_2\cdots C_k$，其中每个 $C_i = (a_{i1}\ \cdots\ a_{i\mathrm{Len}(C_i)})$。分如下 3 种情况。

情形 A： $b_1, b_2 \notin \bigcup_{i=1}^{k}\{a_{i1},\cdots,a_{i\mathrm{Len}(C_i)}\}$，则 $f\circ(b_1\ b_2)$ 的轮换总长度比 f 增加 2，轮换个数比 f 多 1，奇偶性改变。

情形 B： b_1、b_2 中只有一个在 $\bigcup_{i=1}^{k}\{a_{i1},\cdots,a_{i\mathrm{Len}(C_i)}\}$ 中。不妨设 $b_1 \in \bigcup_{i=1}^{k}\{a_{i1},\cdots,a_{i\mathrm{Len}(C_i)}\}$。假设 $a_{ij} = b_1$。那么在将 f 表示为互不相交的轮换后，我们只需要将 $a_{i,j-1}a_{ij}$ 替换为 $a_{i,j-1}b_2a_{ij}$ 即可，显然，这一操作会改变奇偶性。

情形 C： $b_1, b_2 \in \bigcup_{i=1}^{k}\{a_{i1},\cdots,a_{i\mathrm{Len}(C_i)}\}$。我们进一步将其分为如下 3 种子情形。

子情形 C-1： b_1 与 b_2 属于不同的轮换。设 $b_1 = a_{ij}$，$b_2 = a_{k\ell}$（其中 $i \neq k$）。那么，在将 f 写成不相交轮换的乘积形式时，我们只需将 C_i 和 C_k 替换为一个新的轮换：

$$(a_{i1}\cdots a_{i,j-1}\ a_{k\ell}\cdots a_{k\mathrm{Len}(C_k)}\ a_{k1}\cdots a_{k,\ell-1}\ a_{ij}\cdots a_{i\mathrm{Len}(C_i)})$$

即可将 $f\circ(b_1\ b_2)$ 写成互不相交轮换的乘积形式。显然，该变化会使 $f\circ(b_1\ b_2)$ 的奇偶性与 f 不同。

子情形 C-2： b_1 和 b_2 属于同一个轮换，但在该轮换中不是相邻元素。设 $b_1 = a_{ij}$，$b_2 = a_{ik}$（其中 $j < k-1$）。那么，在将 f 写成互不相交轮换的乘积形式时，我们只需将 C_i 替换为两个轮换：

$$(a_{i1}\cdots a_{i,j-1}\ a_{ik}\cdots a_{i\mathrm{Len}(C_i)}) \quad \text{以及} \quad (a_{ij}\cdots a_{i,k-1})$$

即可将 $f\circ(b_1\ b_2)$ 写成互不相交轮换的乘积形式。此操作同样会改变奇偶性。

子情形 C-3： b_1 和 b_2 在轮换中相邻。设 $b_1 = a_{ij}$，$b_2 = a_{i,j+1}$。那么，在将 f 写成互不相交轮换的乘积形式时，我们只需将 C_i 替换为：

$$(a_{i1}\cdots a_{i,j-1}\ a_{i,j+1}\cdots a_{i\mathrm{Len}(C_i)})$$

即可将 $f\circ(b_1\ b_2)$ 写成互不相交轮换的乘积形式。显然，这一变化也会使 $f\circ(b_1\ b_2)$ 的奇

偶性与 f 不同。 ■

我们以两个综合性的例题来结束关于置换群的学习，其中第一个例题涉及交错群。所谓交错群（Alternating Group）A_n（其中 n 为正整数）是指由集合 $\{1,\cdots,n\}$ 上所有偶置换组成的群。也就是说，$A_n=\{f\mid f \text{ 是偶置换}, f\in S_n\}$。

例 3.6.10 凯莱定理有如下推论，通常称为交错群嵌入（Alternating Group Embedding）：每个有限群都同构于某个交错群的某个子群。请予以证明。

解答： 根据凯莱定理，每个有限群都同构于某个对称群的某个子群，我们只需证明每个对称群的每个子群都同构于某个交错群的某个子群。考虑一个任意的对称群 S_n，以及其任意子群 $G\leqslant S_n$。我们将构造一个满足 $H\leqslant A_{2n}$ 且 $H\cong G$ 的子群 H。

对每个置换 $g\in G$，我们定义一个置换 h 作用在 $\{1,\cdots,2n\}$ 上。其中，对于每个 $i\in\{1,\cdots,n\}$，$h(i)=g(i)$，$h(n+i)=n+g(i)$。（直观上，h 在 $1,\cdots,n$ 上的作用与 g 相同；在 $n+1,\cdots,2n$ 上的作用也完全一致。）容易看出 h 是偶置换，因为它实质上是 g 的两个副本。也容易验证，如果 h_1、h_2 是通过 g_1、g_2 构造的两个置换，那么 $h_1^{-1}h_2$ 也是上述形式的置换，因为它可以看作是 $g_1^{-1}g_2$ 的两个副本。因此，所有这样的 h 构成一个 A_{2n} 的子群，我们将其记作 H。从 G 到 H 的映射显然是双射。由于对任意 g_1、$g_2\in G$，其乘积 g_1g_2 会被映射为 h_1h_2（即 g_1g_2 的两个副本），所以这是一个同构映射。 ■

例 3.6.11 关于置换的奇偶性，数学家在19世纪已经证明了如下定理：假设 n 为正整数，G 为 S_n 的一个子群。如果 G 含有一个奇置换 x，那么 [此处省略若干字……] 就是一个指标为 2 的正规子群。

定理本身给出了指标为 2 的正规子群的构造方法，但我们在这里有意识地略去，以增加证明的难度。在没有看到构造方法的情况下，您能否证明这个指标为 2 的正规子群的存在性？

解答： 令 $H=G\cap A_n$，这显然是个子群。（原来，这就是定理中省略的部分！您想到了吗？）下面，我们将通过构造一个双射 $f:G\to G$ 来证明 $|H|=\dfrac{|G|}{2}$，该映射会将奇置换映射为偶置换，反之亦然。也就是说，当我们把 f 的定义域限制到 H 时，其值域为 $G\setminus H$ 的一个子集。反之，当我们把 f 的定义域限制到 $G\setminus H$ 时，其值域为 H 的一个子集。于是，$|H|\leqslant|G\setminus H|$ 且 $|G\setminus H|\leqslant|H|$，从而得到 $|H|=|G\setminus H|$。这等价于 $|H|=\dfrac{|G|}{2}$，或者说指标为2。这时，除了 H 本身之外，只有一个左陪集，也只有一个右陪集，必然导致左右陪集相等，或者说 H 为正规子群。

现在给出 f 的具体构造：对每个 $y\in G$，定义 $f(y)=xy$。显然，y 与 $f(y)$ 的奇偶性相反。因为群 G 满足消去律，所以函数 f 是单射。因为对任意 $z\in G$，都有 $f(x^{-1}z)=z$，所以 f 也是满射。 ■

习 题 集 7

习题 114 (难度 1.4) 是否存在群 G，使得 $Z(G)$ 同构于克莱因四元群，$G/Z(G)$ 同构于 $\mathbb{Z}_3$？

习题 115 设 G 是一个群，$G=ABC$，且 $A,B,C\triangleleft G$。已知 $A\cong S_2$，$B\cong A_3$，$C\cong\mathbb{Z}_4$。能否确定 $G/(A\cap B\cap C)$ 是什么？

习题 116 (难度 1.1) 请找出对称群 S_5 的一个西罗 5-子群。

习题 117 (难度 1.5) 如果一个正规子群是阶大于 1 的真子群，那么称其为非平凡的（nontrivial）。请证明：任意一个 225 阶群都具有非平凡正规子群。

习题 118 (难度 1.9) （a）证明：若 $\tau\in S_n$ 是一个对换，则对任意 $\sigma\in S_n$，$\sigma^{-1}\tau\sigma$ 仍是对换。

（b）证明：对任意 $\tau\in S_n$，存在某个 $\sigma\in S_n$，使得 $\tau^{-1}=\sigma^{-1}\tau\sigma$。

习题 119 (难度 1.0) 假设 G 是一个 120 阶群，$Z(G)\cong\mathbb{Z}_5$。$G/Z(G)$ 是否有指标为 9 的子群？

习题 120 (难度 1.7) 设 G 是一个 280 阶群，H 是其一个 40 阶子群。证明：只要存在一个元素 $x\notin H$ 使得对于每个 $y\in H$ 都有 $x^{-1}yx\in H$，就一定有 $H\triangleleft G$。

习题 121 (难度 2.1) 设 p、q 为素数，且 $p>q$。设 G 是一个 pq 阶群，H 是其一个 p 阶子群。请证明：$H\trianglelefteq G$。

习题 122 (难度 1.8) 存在几种互相不同构的 14 阶群？

习题 123 (难度 2.1) 请给出下面要求的同构映射，不要给恒等映射 $f(x)=x$。

（1）设 G 为 2000 阶的非阿贝尔群，请给出从 G 到其自身的一个同构映射。

（2）设 G 为 2025 阶的阿贝尔群，且存在 $a\in G$ 使得 $\operatorname{order}(a)\geqslant 3$，请给出从 G 到其自身的一个同构映射。

（3）设 G 为 2048 阶的阿贝尔群，且 G 的所有元素均不超过 2 阶，请给出从 G 到其自身的一个同构映射。

习题 124 (难度 2.9) 设 p 是素数，n 是正整数，G 是一个 p^n 阶的非循环群。证明：G 至少有 $p+n+1$ 个子群。

习题 125 (难度 2.2) 在定理 3.4.2 的证明中，我们定义了一个从 G/J 到 G/H 的函数 $f:aJ\to aH$。证明 f 是良定义的，即对所有 $a'\in aJ$，有 $a'H=aH$。

习题 126 对于群 G，和它的子群 H，所谓 H 在 G 中的**正规化子**（normalizer）是指 $N_G(H)=\{g\in G\mid gHg^{-1}=H\}$。显然，$N_G(H)$ 是 G 的一个子群。（您看出来了吗？）

现在考虑一个质数 p，假设 G 为有限群，P 为其西罗 p-群。求证：G 中西罗 p-群的个数恰好等于 $[G:N_G(P)]$。

习题 127 (难度 2.7) 假设 n 是正整数，且 $Z(S_n)\neq Z(S_{n+1})=Z(S_{n+2})$。求所有可能的 n 值。

习题 128 (难度 2.7) 设 G 是有限群，$H<G$。证明：存在一个共轭类与 H 不相交。

习题 129 (难度 2.3) 设 G 是一群，$H\leqslant G$。若不存在子群 J 满足 $\{1\}<J<H$，则称 H 是 G 的**极小子群**（minimal subgroup）。

实数加法群有没有极小子群？证明您的结论。

习题 130 设 G 是一个 48 阶群。证明存在 H 使得 $\{1\}<H\triangleleft G$。

习题 131 (难度 2.7) 对于群 G 和 H，通常用 $\operatorname{Hom}(G,H)$ 表示从 G 到 H 的所有群同态映射的集合。对任意 $\alpha,\beta\in\operatorname{Hom}(G,H)$，定义运算 $\star$ 如下：对任意 $g\in G$，

$$(\alpha\star\beta)(g)=\alpha(g)\beta(g)$$

可以证明，只要 H 为阿贝尔群，在运算 $\star$ 下 $\mathrm{Hom}(G,H)$ 便构成一个群（在您的解答中可以直接使用这个结论，无需予以证明）。

请计算 $|\mathrm{Hom}(S_3,\mathbb{Z}_{12})|-|\mathrm{Hom}(A_3,\mathbb{Z}_6)|$（这里 $\mathbb{Z}_{12}$ 和 $\mathbb{Z}_6$ 分别是模12和模6的加法群）。

习题 132 请给出一个几乎是阿贝尔群的代数系统。具体而言，该代数系统与阿贝尔群只有两个区别：（1）对于某个特定元素 x 而言，如果 $x\in\{a,b,c\}$，那么结合律 $(ab)c=a(bc)$ 并不总能成立。（2）对于某个特定元素 y 而言，如果 $y\in\{a,b\}$，那么交换律 $ab=ba$ 并不总能成立。除此之外，该代数系统完全满足阿贝尔群的要求。

习题 133 (难度 3.1) 假设群 G 为99阶，其子群 H 为9阶，且已知 H 为阿贝尔群。试问 H 与哪种我们熟悉的群同构？提示：可以按照 G 是否阿贝尔群，分情况讨论。