Chapter 1

有限群：引论

对称操作可以是离散的，也可以是连续的。其中离散的对称变换比较容易描述。在本章中，我们会说明群论相关的记号，并引入一些在低阶有限群下的基本概念。最简单的对称操作是反映（reflection）：

$$P: \quad x \to x\prime = -x$$

将其重复两次，则得到恒等变换 (Identity Transformation，注：有些文献会写为 E)：

$$I: \quad x \to x\prime = x$$

符号化的写法是：

$$PP = I$$

反映操作有很多例子。考虑一个等腰三角形，经过关于其垂直轴的反映操作后，三角形保持不变。在几何上这个操作通常被记为 σ。反映操作发生在 x-y 平面上，这时的反映操作也记为 σ_z。

其次简单的对称操作是旋转（Rotation）操作。在二维情形下，旋转操作是基于一个点进行的。而在三维情形下，旋转则围绕一个轴发生。对于一个正方形，在经过逆时针旋转 90° 后，显然形状不发生变化。反过来的逆操作，顺时针旋转也是一样。四次重复的 90° 旋转操作结果与恒等变换相同。一般地，逆时针旋转 $(2\pi/n)$ 的操作会生成循环群 Z_n，其中 n 为整数。连续的 n 次上述旋转操作的结果即恒等操作。只有在二维情形中，反映操作与 180° 的旋转操作相同。
另一个对称操作是关于一个点的反演（inversion），记为 i。在几何上，它包括一次关于一个平面的反映和一次在该平面上的 180° 旋转

$$i = \sigma_h Rot(180^\circ)$$

反映和反演有时也被称为瑕旋转（improper rotations）。他们和旋转一样都需要一个对称中心。

1.1 群公理

一个群 $\mathcal{G}$ 是一组算符的集合，

$$\mathcal{G}: \quad \{a_1, a_2, \ldots, a_k, \ldots\}$$

以及一个具有下列性质的操作 “$\star$”。
封闭性。对任意的有序群元素对 a_i 和 a_j，存在一个群元素 a_k 使得

$$a_i \star a_j = a_k \tag{2.1}$$

对任意的 i，j，k 成立。**可结合性**。操作 $\star$ 满足结合律

$$(a_i \star a_j) \star a_k = a_i \star (a_j \star a_k) \tag{2.2}$$

单位元素。群 $\mathcal{G}$ 包含唯一的元素 e 使得

$$e \star a_i = a_i \star e = a_i \tag{2.3}$$

对所有下标 i 成立。特别地：

$$e \star e = e$$

逆元素。对每一个群元素 a_i，$\mathcal{G}$ 中都存在唯一的一个对应的逆元素，记做 $(a_i)^{-1}$

$$a_i \star (a_i)^{-1} = (a_i)^{-1} \star a_i = e \tag{2.4}$$

当群 $\mathcal{G}$ 包含有限个元素时：

$$(\mathcal{G}: \quad a_1, a_2, \ldots, a_k, \ldots, a_n)$$

称 $\mathcal{G}$ 为有限群，n 为群的阶。

接下来我们会讨论具有有限个元素的群。不过要注意的是，也有许多包含无限个元素的群，我们现在举出几个例子。

- 包含零的实数集。在加法下 $(\star \to +)$ 构成一个无限群。其元素包含零、正实数和复实数。它满足闭合性：若 x 和 y 为实数，那么他们的和 $x+y$ 也会是实数。每个元素 x 有一个逆元素 $-x$，于是有：
$$x + (-x) = 0, \qquad x + 0 = 0 + x$$
我们发现 0 在其中发挥了单位元素的作用。
- 实数系在乘法下（$\star \to \times$）同样构成一个无限群。对任意实数 x 和 y，其乘积 xy 仍是实数；x 的逆元素为 $1/x$；单位元素为 1。在这个例子中，0 被排除掉了。
- 形为 $\frac{n}{m}$ 的有理数，其中 m 和 n 是非零整数。容易验证有理数同样构成一个无限群。

1.2 低阶有限群

我们从讨论阶数低于 13 的有限群开始（参考 Ledermann[14]）。在这个过程中我们会引入很多记号，熟悉许多有用的数学概念，同时认识一些无处不见的群以及它们实现的各个方面。

2 阶群

我们已经提及过这个只有两个元素的独特的群，称为 $\mathcal{Z}_2$。其中一个元素是恒等操作，e，另一个元素 a 必须是它自身的逆，于是我们可以得到如下的乘法表。

$\mathcal{Z}_2$	e	a
e	e	a
a	a	e

根据物理场景的不同，a 可以是各种函数，例如奇偶操作（注：parity operation，即反演操作），关于某一轴的反映操作，一个 180° 的旋转操作，等等。

3 阶群

阶数为 3 的群只有一个。这也很容易看出来：一个元素是恒等操作 e。令 a_1 为第二个元素。那么群元素 $a_1 \star a_1$ 则必定是第三个群元素。否则 $a_1 \star a_1 = a_1$ 将引向 $a_1 = e$，或者 $a_1 \star a_1 = e$ 则将群封闭使其成为 2 阶群。所以必有 $a_1 \star a_1 = a_2$，即第三个群元素，且 $a_1 \star a_2 = a_2 \star a_1$。这就是 $\mathcal{Z}_3$ 群，三阶循环群，它由如下的乘法表定义。

$\mathcal{Z}_2$	e	a_1	a_2
e	e	a_1	a_2
a_1	a_1	a_2	e
a_2	a_2	e	a_1

同时它遵循

$$a_1 \star a_1 \star a_1 = e$$

说明 a_1 是一个三阶元素，表示一次 120° 的旋转。

显然上述论证可以扩展到任意的 n 上，$\mathcal{Z}_n$，即 n 阶循环群，由一个阶数为 n 的元素 a 经过重复生成

$$\mathcal{Z}_n : \quad \{e, a, a \star a, a \star a \star a, \ldots, (a \star a \cdots a \star a)_{n-1}\}$$

有

$$(a \star a \cdots a \star a)_k \equiv a^k, \qquad a^n = e$$

如果我们将其中不同的群元素写为 $a_j = a^{j-1}$，那么我们可以推断出 $a_i \star a_j = a_j \star a_i$。一个群中，如果任意两个元素能够对易，那么我们称这个群是阿贝尔的 (注：Abelian)。不具备这个性质的群则称为非阿贝尔的。

4 阶群

构造所有可能的包含四个元素 $\{e, a_1, a_2, a_3\}$ 的群同样简单。只有两种可能的情况。其一是我们的朋友四阶循环群 $\mathcal{Z}_4$。它由 90° 的旋转产生。我们注意到这个循环群有一个有趣的实现：

$$a : z \to z' = iz \tag{2.5}$$

其中 z 为复数。显然，a 的阶数为 4，它生成 $\mathcal{Z}_4$。

另一个四阶群是二面体群（注：dihedral group）$\mathcal{D}_2$。它具有如下的乘法表。

$\mathcal{Z}_2$	e	a_1	a_2	a_3
e	e	a_1	a_2	a_3
a_1	a_1	e	a_3	a_2
a_2	a_2	a_3	e	a_1
a_3	a_3	a_2	a_1	e

这个群是阿贝尔的，它的乘法表关于其对角线对称。它有时也被称为 $V(Vierergruppe)$ 或克莱因四元群（Klein's four-group）。

阶数为 2n 的二面体群 $\mathcal{D}_n$ 是我们接触到的第一个包含无限个群的家族。他们有着简洁的物理含义，即将一个平面正多边形映射回其自身。$n = 2$ 的情形对应于一条线段的不变群：线段关于其中点的两组 180 旋转操作是不变的。其一为绕垂直纸面的轴的转动，另一个则是绕在纸面上的轴的转动。而围绕线段本身的转动则显然也是不变的。其乘法表展示了 3 个阶数为 2 的元素，对应于三维空间中三个绕任意正交轴的 180 旋转操作。它也有很多其他的实现方式，例如在 (2×2)

矩阵中

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}. \tag{2.6}$$

一个有趣的实现涉及到函数相关性。考虑一下的四个映射（函数）

$$f_1(x) = x, \quad f_2(x) = -x, \quad f_3(x) = \frac{1}{x}, \quad f_4(x) = -\frac{1}{x}. \tag{2.7}$$

容易验证它们在 $\mathcal{D}_2$ 群上封闭。$\mathcal{D}_2$ 和 $\mathcal{Z}_4$ 群的区别在于 $\mathcal{Z}_4$ 群包含一个四阶的元素，而 $\mathcal{D}_2$ 中则没有。

四阶群有一个我们还没有遇到的共同特点：它们中一些元素构成的子集同样是一个群。在我们的例子中，这个子集构成的群是 $\mathcal{Z}_2$。$\mathcal{Z}_2$ 是 $\mathcal{Z}_4$ 的子群，由 (e, a^2) 生成，表示为

$$\mathcal{Z}_4 \supset \mathcal{Z}_2$$

至于 $\mathcal{D}_2$ 群，它包含三个 $\mathcal{Z}_2$ 子群，分别由 (e, a_1),(e, a_2) 和 (e, a_3) 生成。由于 $a_1 \star a_2 = a_2 \star a_1$，前两个 $\mathcal{Z}_2$ 群的元素能够相互对易，我们可以用前两个对易的 $\mathcal{Z}_2$ 群的直积（注：*direct product*）表示 $\mathcal{D}_2$ 群

$$\mathcal{D}_2 = \mathcal{Z}_2 \times \mathcal{Z}_2 \tag{2.8}$$

这是一种一般数学结构的第一个，也是最简单的例子。

注释：**直积**

设 $\mathcal{G}$ 和 $\mathcal{K}$ 为两个群，其群元素分别为 $\{g_a\}, a = 1, \ldots, n_g$ 和 $\{k_i\}, i = 1, \ldots, n_k$。我们现在按照如下的乘法规则构造新的群元素 (g_a, k_i):

$$(g_a, k_i)(g_b, k_j) = (g_a \star g_b, k_i \star k_j) \tag{2.9}$$

这些元素显然满足群公理，构成了一个阶数为 $n_g n_k$ 的群，称为群 $\mathcal{G}$ 和 $\mathcal{K}$ 的直积或克罗内克 (Kronecker) 积，记作 $\mathcal{G} \times \mathcal{K}$。由于 $\mathcal{G}$ 和 $\mathcal{K}$ 的操作发生在不同的空间内，它们总是可以被视为对易的子群，直积产生的群元素也可以被简单地记为 (g_a, k_i)。这种构造方式提供了一个简单的方法来产生更高阶的群。

注释：**拉格朗日定理** *(Lagrange's theorem)*

这个定理给出了存在子群的必要条件。考虑一个元素为 $\{g_a\}, a = 1, 2, \ldots, N$ 的群 $\mathcal{G}$，具有包

含 n 个元素 $(h_1, h_2, \ldots, h_n) \equiv h_i, i = 1, 2, \ldots, n < N$ 的子群 $\mathcal{H}$,

$$\mathcal{G} \supset \mathcal{H}$$

取 $\mathcal{G}$ 中不属于 $\mathcal{H}$ 的元素 g_1，那么具有形式 $g_1 \star h_i$ 的 n 个元素显然是 $\mathcal{G}$ 中的元素，但不是 $\mathcal{H}$ 的元素。若其中某个元素属于 $\mathcal{H}$，即存在 i 和 j，使:

$$g_1 \star h_i = h_j$$

，则有

$$g_1 = h_j \star (h_i)^{-1}$$

属于群 $\mathcal{H}$，这与前设矛盾，故集合 $\{h_i\}$ 与集合 $\{g_1 \star h_i\}$ 没有公共元素。重复上述过程，取 $\mathcal{G}$ 中不属于 $\mathcal{H}$ 和不属于 $g_1\mathcal{H}$ 的元素 g_2。那么集合 $\{g_2 \star h_i\}$ 与 $\{h_i\}$ 和 $\{g_1 \star h_i\}$ 均没有公共元素，因为如果他们存在重叠，那么将存在某组 i 和 j，使得

$$g_1 \star h_i = g_2 \star h_j$$

这表明 $g_2 = g1 \star h_k$，与前设矛盾。我们不断重复上述过程直到组成集合 $g_k \star h_i$ 后群 $\mathcal{G}$ 中没有其他元素。于是我们可以将完整的群 $\mathcal{G}$ 写为（右）陪集分解（*coset decomposition*）

$$\begin{aligned} \mathcal{G} &= \{h_i\} + \{g_1 \star h_i\} + \cdots + \{g_k \star h_i\} \\ &\equiv \mathcal{H} + g_1 \star \mathcal{H} + \cdots + g_k \star \mathcal{H} \end{aligned} \tag{2.10}$$

其中任意两集合不重叠：$\mathcal{G}$ 的阶数因而必为其子群阶数的倍数。于是我们有拉格朗日定理。
*若阶数为 N 的群 $\mathcal{G}$ 有阶数为 n 的群 $\mathcal{H}$，那么 N 必为 n 的整数倍*其倍数 $k = N/n$ 称为 $\mathcal{H}$ 在 $\mathcal{G}$ 中的指数（*index*)。这一定理将在后续为我们节省很多工作。

令 a 是有限群 $\mathcal{G}$ 的一个元素并组成下列序列

$$a, a^2, \ldots, a^k, \ldots$$

序列中均为群 $\mathcal{G}$ 的元素，由于假设 $\mathcal{G}$ 是有限的，序列中的元素必然存在重复，存在某个 $k > l$

$$a^k = a^l \to a^{k-l} = e$$

即有限群中的任意元素的某一幂次等于恒等元素。当 $a^n = e$，我们称 a 是一个 n 阶的元素。令 k 为 $\mathcal{G}$ 中任意元素 b 的阶，它产生 $\mathcal{G}$ 的循环子群 $\mathcal{Z}_k$。由拉格朗日定理，k 必为 n 的倍数，其中 n 为 $\mathcal{G}$ 的阶。

作为进一步的应用，令群 $\mathcal{G}$ 的阶为素数 p。由于素数没有其他因数，其任意元素的阶必为 1 或 p。故必有 $\mathcal{G} = \mathcal{Z}_p$：我们不需要构造阶数为 5，7，11，……的群，它们都是循环群，同时拉格朗日定理告诉我们阶数为素数的循环群没有子群。

6 阶群

从我们刚刚学到的内容可以知道，至少有两个 6 阶群：由 60° 旋转生成的循环群 $\mathcal{Z}_6$，以及由直积 $\mathcal{Z}_2 \times \mathcal{Z}_3$ 产生的群。然而这两个群实际上是相同的。为了证明这一点，令 a 和 b 分别为 $\mathcal{Z}_3$ 和 $\mathcal{Z}_2$ 的生成元。那么有 $a^3 = b^2 = e$，同时 $ab = ba$。考虑 $\mathcal{Z}_2 \times \mathcal{Z}_3$ 中的元素 ab。显然，$(ab)^3 = b$，而 $(ab)^6 = (b^2) = e$，故 ab 的阶为 6。所以这两个群中均有一个阶数为 6 的元素，这两个群必定是相互同构 *(isomorphism)* 的

$$\mathcal{Z}_6 = \mathcal{Z}_2 \times \mathcal{Z}_3 \tag{2.11}$$

这一推论成立的原因在于 6 的两个因数 2 和 3 是互质的。

任意其他阶数为 6 的群必须包含一个 3 阶的元素 $a(a^3 = e)$。若 b 是另一个元素，我们很容易发现 6 个元素 (e, a, a^2, b, ab, a^2b) 是不同的，它们必定组成一个阶数为 6 的群。

特别地，元素 b^2 必须为 e,a 或者是 a^2。后两者意味着 b 的阶数为 3，与假设矛盾。故元素 b 的阶必为 2：$b^2 = e$。现在我们考虑元素 ba。它可能是 ab 或 a^2b。若 $ab = ba$，我们会发现 ab 的阶为 6，矛盾。所以 6 阶群是非阿贝尔的。因此必有 $ba = a^2b$；于是得到如下二面体群的乘法表。

D_3	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	e	a_4	a_5	a_3
a_2	a_2	e	a_1	a_5	a_3	a_4
a_3	a_3	a_5	a_4	e	a_2	a_1
a_4	a_4	a_3	a_5	a_1	e	a_2
a_5	a_5	a_4	a_3	a_2	a_1	e

这会是你看到的最后一张乘法表！有一种好的多的方式来表达它所包含的信息。我们注意到所有的群元素都能从一个 3 阶元素 $a_1 \equiv a$，以及一个 2 阶元素 $a^3 \equiv b$ 得到；a 和 b 是这个群的生成元 *(generator)*。

注释：**表示 *(Presentation)***

有限群的表示是列出其生成元、它们的阶以及定义群所需的其他关系。同一个群可能有多种表示。例如，D_3 的简单表示为：

$$< a, b | a^3 = b^2 = e; bab^{-1} = a^{-1} > \tag{2.12}$$

由于有两个生成元，我们称 D_3 具有为二的秩。D_3 也是正三角形的对称群。

TBD：图示

它的三阶元素描述了绕正三角形 ABC 中心 O 的 60° 旋转。三个二阶元素是关于三条顶点到中心的轴 OA, OB 和 OC 的反映操作。

还有一种更好的方式来表示这个群。由于这个正三角形到自身的映射等价于对其三个顶点进行置换，那么群操作就是标记三个顶点的字母的排列。例如，关于 OC 轴进行的反映操作交换了顶点 A 和 B 的位置，就相当于翻转了字母 A 和 B 的排列，称为对换 *(transposition)*，并记为符号 $(A \quad B)$。另外两个反映操作则是 $(B \quad C)$ 和 $(A \quad C)$。关于 O 的 120° 旋转则是对三个字母的置换，记为符号 $(A \quad B \quad C)$，意为 $A \to B \to C \to A$ 的变换。我们称对换为 2-轮换，像 $(A \quad B \quad C)$ 这样的置换为 3-轮换。轮换记号会几乎在处处用到。我们会注意到群里的这些操作产生了所有的 3! 种对三个对象的排列。一般来说，n 个对象会有 $n!$ 种排列。显然，它们会构成一个称为置换群 S_n 的群。在上面的例子中，我们发现 $D_3 = S_3$。

我们也可以把这三个顶点理解为这种轮换所作用的向量的分量。那么群操作就会表示为一个 (3×3) 的矩阵，作用在一个元素标记为 A，B 和 C 的列向量上。我们可以通过如下的计算确认这一点：

$$b = (AB) \to \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = (ABC) \to \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{2.13}$$

群操作就是简单的矩阵乘法。比如：

$$ab = (ABC)(AB) = (BC) \to \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{2.14}$$

等等。

这种几何上的解释给具有 2n 个元素的二面体群 $\mathcal{D}_n$ 提供了一种扩展的理解，即正 n 边形的对称群。-关于正 n 边形中心的 n 个 $(2\pi/n)$ 弧度的旋转操作显然使其保持不变 -同样地，有 n 个镜面反映操作使其保持不变。如果 n 是奇数，例如正三角形，反映操作的 n 个对称轴是从其中心向其顶点的 n 条连线；而若 n 是偶数，例如正方形，那么 $2/n$ 条对称轴是从中心向顶点的连线，另外 $2/n$ 条对称轴则是穿过中心向两条相对的边的中点的连线。相应地，它的群表示是

$$\mathcal{D}_n :< a, b | a^n = b^2 = e; bab^{-1} = a^{-1} > . \tag{2.15}$$

8 阶群

到现在为止，如何构造各种具有 8 个元素的群应该已经比较明显了。首先我们知道 8 阶循环群

$\mathcal{Z}_8$，以及二面体群 $\mathcal{D}_4$，如下的长方形的对称群。

TBD 图示

我们也可以通过直积来构造 $\mathcal{Z}_2 \times \mathcal{Z}_2 \times \mathcal{Z}_2 = \mathcal{D}_2 \times \mathcal{Z}_2$，以及 $\mathcal{Z}_4 \times \mathcal{Z}_2$。

这些群是否是不同的呢？显然，直积 $\mathcal{Z}_4 \times \mathcal{Z}_2$ 包含一个四阶元素，它与只包含二阶元素的 $\mathcal{Z}_2 \times \mathcal{Z}_2 \times \mathcal{Z}_2$ 是不同的。另外，它不含八阶元素，因而也不会是 $\mathcal{Z}_8$。

任意的其它的八阶群一定至少包含一个四阶元素。设其为 a，有 $(a)^4 = e$。令 b 是一个不同的元素，b 的阶数一定是 2 或者 4。那么我们得到 8 个不同的元素：

$$\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

这个集合构成一个群。我们考虑两种可能性。

其一，$b^2 = e$。这里有三种可能性：$ba = a^2b$ 导致矛盾；$ba = ab$ 意味着这个群是阿贝尔的，也就是 $\mathcal{Z}_4 \times \mathcal{Z}_2$；最后是 $ba = a^3b$，那么 ab 是一个二阶元素，产生二面体群 $\mathcal{D}_4$。

另一种可能性是 $b^4 = e$。在这个情况下，我们必有 $b^2 = a^2$，同样存在三种可能：首先，$ba = a^2b$ 导致矛盾；$ba = ab$ 得到阿贝尔群 $\mathcal{Z}_4 \times \mathcal{Z}_2$。第三种可能 $ba = a^3b$ 产生一个新的群，称为四元数群（quaternion group）$\mathcal{Q}$。与其展示冗长的乘法表，用两个四阶生成元写出它的表示更加方便：

$$\mathcal{Q} :< a, b | a^4 = e, a^2 = b^2, bab^{-1} = a^{-1} > . \tag{2.16}$$

$\mathcal{Q}$ 是一个秩为 2 的群。

为什么它被叫做四元数群呢？四元数是实数和复数的推广。实数和复数的一个性质是两个数的乘积的模等于两个数的模的乘积，即赫尔维茨性（Hurwitz property）。对于复数 $z = x + iy$，其模定义为

$$N(z) = \sqrt{z\bar{z}} \tag{2.17}$$

其中 $\bar{z} = x - iy$。对任意两个复数 w 和 z，我们有

$$N(zw) = N(z)N(w). \tag{2.18}$$

这个性质对实数来说是平凡的。四元数是实数和复数的推广。它同样具有赫尔维茨性。一个四元数类似于一个具有三个虚部的复数

$$q = x_0 + e_1x_1 + e_2x_2 + e_3x_3, \quad \bar{q} = x_0 - e_1x_1 - e_2x_2 - e_3x_3 \tag{2.19}$$

定义

$$N(q) = \sqrt{q\bar{q}} \tag{2.20}$$

容易验证，对任意两个四元数，

$$N(qq\prime) = N(q)N(q\prime), \tag{2.21}$$

只要有

$$(e_1^2) = (e_2^2) = (e_3^2) = 1, \quad e_1e_2 = -e_2e_1 = e_3, \tag{2.22}$$

加上类似上式的循环组合，产生了哈密顿 (Hamilton) 著名的四元代数。它也可以通过 (2×2) 的泡利（Pauli）（或菲利克斯 · 克莱因）矩阵实现:

$$e_j = -i\sigma_j, \quad \sigma_j\sigma_k = \delta_{jk} + i \in_{jkl} \sigma_l \tag{2.23}$$

其中

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.24}$$

四元数群的生成元是虚部单位构成的四元数的乘积

$$a : q \to q\prime = e_1q, \quad b : q \to q\prime = e_2q \tag{2.25}$$

我们很快就会看到，八阶的四元数群是我们遇到的第一个有限双环 *(dicyclic)(binary diheral)* 群构成的无穷系列。

9 阶群

与其把读者拉入繁重的代数运算过程，我们直接说明一个定理（将在后文证明），它断言素数平方阶数的群一定是阿贝尔的。有两个不同的九阶群:

$$\mathcal{Z}_9; \quad \mathcal{Z}_3 \times \mathcal{Z}_3. \tag{2.26}$$

10 阶群

在 10 阶上并没有新的群类型。由于 5 和 2 是互质的，只有一个循环群:

$$\mathcal{Z}_{10} = \mathcal{Z}_2 \times \mathcal{Z}_5,$$

和使正五边形保持不变的二面体群 $\mathcal{D}_5$。

12 阶群

首先，我们有一些比较显然的 12 阶群:

$$\mathcal{Z}_{12}; \quad \mathcal{D}_6; \quad \mathcal{Z}_6 \times \mathcal{Z}_2; \quad \mathcal{Z}_4 \times \mathcal{Z}_3; \quad \mathcal{D}_3 \times \mathcal{Z}_2; \quad \mathcal{D}_2 \times \mathcal{Z}_3,$$

不过，这些群并不全是不同的：由于 4 和 3 是互质的，我们会得到：

$$\mathcal{Z}_{12} = \mathcal{Z}_4 \times \mathcal{Z}_3$$

是同构的，同样地：

$$\mathcal{Z}_2 \times \mathcal{Z}_6 = \mathcal{Z}_2 \times \mathcal{Z}_2 \times \mathcal{Z}_3 = \mathcal{D}_2 \times \mathcal{Z}_3$$

于是上面的例子中实际上只有两个 12 阶的阿贝尔群，$\mathcal{Z}_4 \times \mathcal{Z}_3$ 和 $\mathcal{Z}_6 \times \mathcal{Z}_2$，以及一个非阿贝Ⓕ的群：

$$\mathcal{D}_6 = \mathcal{D}_3 \times \mathcal{Z}_2 \tag{2.27}$$

12 阶群还有两个新的非阿贝尔群。其一是四面体群，$\mathcal{T}$，一个规则（正）四面体的对称群（附：经典甲烷。。）

TBD 图示

它的四一个面都是正三角形，它们各自在关于轴 OA，OB，OC 和 OD 的两个旋转下能够保持不变。同时，有三个关于连接相对的边的轴（例如 AD、BC 中点的连线）的二阶旋转使其保持不变。加上恒等操作，构成了一个具有十二个元素的群。这个群有 3 个二阶群元素和 8 个 3 阶群元素。一个描述这个（以及任意其他的）有限群的优雅的方法是将其中的对称操作理解为对标记四面体四个顶点的四个字母 A，B，C，D 的置换。我们之前已经在等边三角形上使用过这种构造方法。这十二个元素恰好可以分解成两个元素的交换和绕中心到顶点的轴的旋转的乘积：

$$(AB)(CD), \quad (AC)(BD), \quad (AD)(BC), \tag{2.28}$$

后者可以写为：

$$(ABC), (ACB); \quad (ABD), (ADB); \tag{2.29}$$

$$(ACD), (ADC); \quad (BCD), (BDC); \tag{2.30}$$

加上单位元素，构成了四面体群，$\mathcal{T}$。容易验证它由下列两个 4×4 的矩阵生成

$$a = (12)(34) \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}; \quad b = (123) \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.31}$$

(附：这种矩阵称为排列矩阵（permutation matrix）) 它们产生了 $\mathcal{T}$ 的四维矩阵表示。我们很快会看到由于任意群操作都能被视为一个置换，这个过程能够推广到所有有限群上。出于完整性的

考虑，我们把它的表示写为：

$$\mathcal{T} :< a, b|a^2 = b^3 = (ab)^3 = e > . \tag{2.32}$$

四面体群还与一个有无限个群的家族中的一个成员是同构的，这些群称为交错（*alternating*）群 $\mathcal{A}_n(\mathcal{T} = \mathcal{A}_4)$，从 n 个字母的偶轮换中产生。

另一个非阿贝尔的十二阶群，Γ，由两个元素 a 和 b 生成，它的表示如下：

$$\Gamma : \quad < a, b|a^6 = e, b^2 = a^3, bab^{-1} = a^{-1} > \tag{2.33}$$

它的生成元可以写为泡利自旋矩阵的形式：

$$a = \frac{1}{2}(\sigma_0 + i\sqrt{3}\sigma_3) = \frac{1}{2}\begin{pmatrix} 1+i\sqrt{3} & 0 \\ 0 & 1-i\sqrt{3} \end{pmatrix}; b = i\sigma_1 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}. \tag{2.34}$$

这个群是之前提到的双环群 $\mathcal{Q}_{2n}$ 中的一员。一般的 $\mathcal{Q}_{2n}$ 具有如下的表示：

$$\mathcal{Q}_{2n} : \quad < a, b|a^{2n} = e, b^2 = a^n, bab^{-1} = a^{-1} > . \tag{2.35}$$

我们在上述关于低阶有限群的有限探索中已经遇到了了五个来自包含无限个有限群的群族的成员：由一个 n 阶元素生成的循环群族 $\mathcal{Z}_n$；由一个 n 阶元素和一个 2 阶元素生成的 2n 阶的二面体群 $\mathcal{D}_n$。在 $n > 2$ 时，$\mathcal{D}_n$ 是非阿贝尔的。在六阶群中，我们发现了对三个对象的置换群 $\mathcal{S}_3$，它是无限群族 $\mathcal{S}_n$ 中的一员。这个群族中的群对应于 n 个对象的置换。在八阶群中我们遇到了四元数群 $\mathcal{Q}f_4$，来自于双环群族 $\mathcal{Q}_{2n}$。在十二阶群中，我们遇到了另一个双环群 $\mathcal{Q}_6$，以及四面体群 $\mathcal{T}$。后面我们会将其记为 $\mathcal{A}_4$，无限群族 $\mathcal{A}_n$ 中的一员。$\mathcal{A}_n$ 群是表示 n 个对象的偶置换的群。在每一个阶数上，我们都遇到了由更低阶数的群的直积所产生的新群。

我们将结果总结在两张表中。在表 2.1 中，非阿贝尔群以星号标出。我们在这张表中展示群的名字和它们的同构关系。表 2.2 给出了最高到 200 阶的有限群的数目，其中阿贝尔群的数目列在括号内。这些结果来自 Lomont[**?**]。

表 2.2 是十分令人惊奇的。可以预料的是，我们发现阶数为素数的群都只有一个。另一个规律是阶数为素数的平方时都只有两个阿贝尔的群。而如果阶数是素数的两倍呢？另外，我们也能注意到表中有一些特别大的数字，其中有特别多的非阿贝尔群。随着阶数的增大，这种现象愈发明显。例如，阶数为 384 时，有 20154 个非阿贝尔群，而阶数为 390 的非阿贝尔群只有 11 个。

为了更深入地研究这些群，我们必须建立更系统的方法。可以从更基础的构成要素获得群吗？是否有一些群比其他的群更重要（译注：这里原文用的是 more equal than others 这个梗，这里取了意）？不论你是否相信，我们现在所构造出的群没有一个是数学家们所理解的“基本的”群：

最小的这类“基本”非阿贝尔群恰好包含十六个元素，对应于五个对象的偶置换！

1.3 置换

对群的系统性研究是由埃瓦里斯特 · 伽罗华在对多项式方程的根的研究中开创的（我们随后会展开这一部分）。置换操作的确在对有限群的研究中有着中心地位。因为任意的 n 阶有限群都可以被看作对 n 个字母的置换操作集合。我们已经看到过几个这方面的例子。在本章中，我们会系统性地建立这一理念。

一个对 n 个可辨对象 $1, 2, 3, \ldots k, \ldots, n,$ 的排列将他们重新排布为不同的顺序，比如 $a_1, a_2, a_3, \ldots, a_k, \ldots, a_n$。这一变换 $k \to a_k, \quad k = 1, 2, \ldots, n$ 表示成如下的符号：

$$\begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \tag{2.36}$$

它显然满足所有的群公理，例如：

$$\begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & ... & a_n \\ b_1 & b_2 & ... & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & ... & n \\ b_1 & b_2 & ... & b_n \end{pmatrix} \tag{2.37}$$

等等。每种排列都有一个唯一的逆排列，而恒等排列则保持这个序列不变。显然，n 个字母的 n! 种排列构成了一个群，称为对称群（*symmetric group*），记为 $\mathcal{S}_n$。

我们用更准确的循环记号来标记置换。我们之前已经遇到过这种记号。一个将 $k < n$ 个对象映射回其自身，而保持其余部分不变的置换操作被称为一个 *k*-轮换 *(k-cycle)*。以四个对象的置换为例，我们将其写为：

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \sim (1234). \tag{2.38}$$

从左到右读为 $1 \to 2, 2 \to 3, 3 \to 4, 4 \to 1$。另一个 4-轮换的元素是

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \sim (1324) \tag{2.39}$$

此外，我们有

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \sim (12)(3)(4) \tag{2.40}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \sim (12)(34) \tag{2.41}$$

以及

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \sim (132)(4). \tag{2.42}$$

为清晰起见，上面的例子中保留了单轮换的记号，后续我们会省略这部分。

一个置换的度（degree）是指其作用的对象的数量。置换可以被分为称为类（*classes*，正式定义见后文）的若干类型。在上面的四个对象的例子中，这些类包括：作用于两个对象的对换，(xx)；两个对换的乘积，(xx)(xx)；3-轮换，(xxx)；和 4-轮换，(xxxx)。

任意的置换都可以按上述的方式进行分解。考虑一个对 n 个对象的任意置换。取其中一个对象，例如 k，追踪其在置换中的变化序列 $k \to a_k^{[1]} \to a_k^{[2]} \to \cdots \to k$。由于对象的数量是有限的，这个序列最终会回到 k 本身而终止。这里有两种可能性，其一是我们必须遍历 n 个对象才能返回 k，此时这个置换是一个 n-轮换

$$(ka_k^{[1]}a_k^{[2]}\cdots a_k^{[n-1]}). \tag{2.43}$$

或者它会在仅 r 次迭代后提前终止。在这种情况下，令 m 是没有遍历到的 $(n-r)$ 个对象之一。然后追中它在置换中的变化 $m \to a_m^{[1]} \to a_m^{[2]} \to \cdots a_m^{[s-1]} \to m$，它会在 s 次迭代后返回它自身。同样地这里会有两种情形，若 $s = (n-r)$，那么、所有的元素都被遍历，置换可以写为：

$$(ka_k^{[1]}a_k^{[2]}\cdots a_k^{[r-1]})(ma_m^{[1]}a_m^{[2]}\cdots a_m^{[n-r-1]}). \tag{2.44}$$

而如果 $s < (n-r)$，那么我们还需要继续处理剩下的 $(n-r-s)$ 个对象。不断重复上述过程，直到所有的对象都被考虑，我们会得到如下的轮换分解：

$$(ka_k^{[1]}a_k^{[2]}\cdots a_k^{[r-1]})(ma_m^{[1]}a_m^{[2]}\cdots a_m^{[s-1]})\cdots(ta_t^{[1]}a_t^{[2]}\cdots a_t^{[u-1]}), \tag{2.45}$$

其中 $r+s+\cdots+u = n$。这个分解是唯一的，因为它并不取决于我们从哪一个元素开始进行分解，也和我们在每一步中的选择无关。我们刚刚的证明可以总结为如下的结论：

每个置换均可唯一分解为作用于不相交的集合上的轮换。

此外，任何置换也可分解为（不可交换的）对换乘积：

$$(a_1a_2\cdots a_n) = (a_1a_2)(a_1a_3)\cdots(a_1a_n). \tag{2.46}$$

如果在这种分解中换位的次数是偶数（奇数），则该排列称为偶排列（奇排列）。两个偶排列的乘积是偶排列，且偶排列形成一个阶为 $n!/2$ 的子群，称为交错群 *(alternating group)*$\mathcal{A}_n$。

在我们的例子中，$\mathcal{T} = \mathcal{A}_4$，偶置换是形似 (12)(34) 这样的对换的乘积，而类似于 (123) = (12)(13) 这样的 3-轮换，同样是两个对换的乘积。$\mathcal{S}_4$ 中不属于 $\mathcal{A}_4$ 的元素是奇置换，即那些包含一个对换和一个 4-轮换的元素。由于两个奇置换的乘积是一个偶置换，奇置换并不能构成群。

考虑对 n 个对象的一个置换，它由 α_1 个 1-轮换，α_2 个 2-轮换，...，α_k 个 k-轮换描述：

$$n = \sum_{j=1}^{k} j\alpha_j. \tag{2.47}$$

我们想要找出具有这种循环结构的排列的数量。这类似于将 n 个不同的对象放进 α_1 个 1 维盒子，α_2 个 2 维盒子，...。会有两种类型的冗余：对于相同类型的 α_j 个盒子，我们预计会有 $\alpha_2!$ 种冗余来自于盒子的交换。此外，会有 j 种方式来把一个对象放进一个 j 维的盒子里，那么 α_j 个盒子将会产生 j^{α_j} 的冗余。因此，具有这种循环结构的排列的数量为：

例如，$\mathcal{S}_4$ 的 24 个元素可以分为：1 个恒等元素、6 个 2-轮换、3 个双对换、8 个 3-轮换和 6 个 4-轮换。

$$\frac{n!}{\prod_j^k j^{\alpha_j}\alpha_j!}. \tag{2.48}$$

令 $\mathcal{G}$ 是一个具有 g_a 个元素的群，其中 $a = 1, 2, \ldots, n$。取其中一个元素 g_b，用它构造 n 个元素 $g_1g_b, g_1g_b, \ldots, g_ng_b$，然后将 g_b 关联到排列：

$$P_b = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ g_1g_b & g_2g_b & g_3g_b & \cdots & g_ng_b \end{pmatrix}. \tag{2.49}$$

对 $\mathcal{G}$ 中的每一个元素，都可以做这样的操作，从而产生 n 个不同的排列。此外，这种构造方式还会保持乘法表的一致性：

$$g_ag_b = g_c \to P_aP_b = P_c. \tag{2.50}$$

$\{P_a\}$ 构成了 $\mathcal{G}$ 的一个群表示。由于 P_a 满足群公理，它们构成了 n 个对象的置换的一个子群。于是我们可以引出凯莱定理（Cayley's theorem）：

所有的 n 阶有限群都与置换群 $\mathcal{S}_n$ 的某个子群同构。

这些 n 度的置换 P_a 构成了一种表示，称为正则表示 *(regular representation)*。其中每一个 P_a 是一个 $(n \times n)$ 的矩阵，作用于排列为列矩阵（译注：或者应该说列向量?）的 n 个对象上。这些矩阵非常庞大。例如，8 阶的四元数群由 (8×8) 的矩阵构成，而实际上我们之前已经构造过同一个群的 (2×2) 矩阵表示。显然正则表示是冗余的。这种表示被称为可约的。我们很快就会建立一套系统方法来找到有限群的不可约表示。不过首先我们需要再引入一些概念，它们将在我们界定（译注：这里原文是 characterization，我拿不太准该翻成什么。。）有限群的过程中非常有用。

1.4 基本概念

在本节中,我们会介绍许多新的概念和工具,它们对系统性地研究有限群至关重要(见 Carmichael[?] 及 Hall[?] 的著作)。我们还会给出古代科学书籍中常见的注释(*scholia*, 边缘上的解释性记述)。(译注:我想到一个笑话,但可惜这里地方太小。。)

1.4.1 共轭 *(Conjugation)*

这是一种极为重要的操作,在这一操作之下任何乘法表都不变。令 $\mathcal{G}$ 是一个群,其中包含元素 g_a。我们定义任意元素 g_a 关于任意另一个群元素 g 的共轭为:

$$\tilde{g}_a \equiv g g_a g^{-1}. \tag{2.51}$$

显然,上述变换将群乘法表映射回其自身:

$$g_a g_b = g_c \to \tilde{g}_a \tilde{g}_b = \tilde{g}_c, \tag{2.52}$$

因为:

$$g g_a g^{-1} g g_b g^{-1} = g(g_a g_b) g^{-1} = g g_c g^{-1}. \tag{2.53}$$

这是保持乘法表不变的映射的一个例子。这种保持算规则不变的操作称为同态 *(homomorphism)*。另外,由于共轭是一一对应的映射(译注:同时它是集合自身到自身的映射),它是一种特殊的同态,称为自同构 *(automorphism)*。由于它是由群中的一个元素作用而产生的,共轭这种特殊的映射又被称为内自同构 *(inner automorphism)*。如果元素 g_a 和 g_b 能够对易,那么 g_a 关于 g_b 是自共轭的,反之亦然。

共轭有一个重要性质是它不会改变群元素的轮换结构。为了验证这一点,我们考虑一个群元素,它将一个 n 阶群中的 5 个元素进行轮换,写作置换 $P = (klmpq)$。为了验证上述性质,考虑下式:

$$g P g^{-1} = (g(k) g(l) g(m) g(p) g(q)) \tag{2.54}$$

其中 $g(k)$ 是群操作 g 对群元素 k 的作用,其他类似。只要注意到:

$$g P g^{-1} g(k) = g P(k) = g(l) \tag{2.55}$$

对于 g 的共轭将 $k \to l$ 替换为 $l \to k$。从而我们得到以下结论:共轭不会改变排列的循环分解结构,共轭元素具有相同的循环结构。

注释:**类** *(Classes)*

我们可以利用共轭将任意群中的元素划分为不相重合的集合。任取一个元素 g_b，将其与所有 $\mathcal{G}$ 中的元素作共轭操作：

$$C_b: \quad \widetilde{g}_b = g_a g_b g_a^{-1}, \quad \forall g_a \in G, \tag{2.56}$$

上述操作产生元素 C_b 的集合，称为一个类。现在再选取 $\mathcal{G}$ 中不属于 C_b 的一个元素 g_c，然后构造一个新的类：

$$C_c: \quad \widetilde{g}_c = g_a g_c g_a^{-1}, \quad \forall g_a \in G. \tag{2.57}$$

C_a 和 C_b 两个类没有公共元素。如果存在这样的元素，那么意味着 g_c 属于 C_b，与我们的假设矛盾。这一过程可以不断重复，直到所有群元素都归属于一个类。我们可以推断任意的 n 阶有限群都可以分解为 $k \leq n$ 个类。

由于上述构造方式并不取决于我们对元素 $g_b, g_c, \ldots,$ 的选取。这种分解方式和 k 都是唯一的。分解产生的类的数量是群的一个特征。任意的 n 阶阿贝尔群都有 n 个类，每个类包含一个元素。恒等元素总是自成一类，通常记为 C_1。

注释：**正规子群** *(Normal subgroup)*

设 $\mathcal{H}$ 是 $\mathcal{G}$ 的一个子群，其元素记为 h_i：

$$\mathcal{G} \supset \mathcal{H}$$

某些子群具有一个非常特殊的性质。如果 h_i 对 $\mathcal{G}$ 中每一个元素 g 的共轭都还是 $\mathcal{H}$ 的元素，即：

$$g h_i g^{-1} = h_j \in \mathcal{H}, \quad \forall g \in G, \tag{2.58}$$

那么子群 $\mathcal{H}$ 是一个正规子群。在这种情况下，数学家们使用记号表示它们的关系：

$$\mathcal{H} \triangleleft \mathcal{G}, \quad (\mathcal{G} \triangleright \mathcal{H}). \tag{2.59}$$

大部分群都有正规子群；那些不具有正规子群的群是非常特殊的，它们称为单 *(simple)* 群，并且构成了所有其他群的基石。

注释：**商群** *(Quotient subgroup)*

为了理解正规子群到底为什么这么特殊，我们考虑一个将群 $\mathcal{G}$ 映射到一个较小的群 $\mathcal{K}$ 的同态映射，

$$\mathcal{G} \to \mathcal{K} \qquad g_a \to k_a$$

它保留了群的乘法表：$g_a g_b = g_c$ 意味着 $k_a k_b = k_c$。令 $\mathcal{H}$ 是群 $\mathcal{G}$ 中被映射为恒等元素的群元构

成的集合（映射的核 *(kernel)*）。

$$\mathcal{H} = 1.$$

显然集合 $h_i \in \mathcal{H}$ 是 $\mathcal{G}$ 的一个子群，此外，由于 $g_a h_i g_a^{-1} \to k_a k_a^{-1} = 1$，它还是一个正规子群。

现在从另一个方面考虑这个问题。我们从群 $\mathcal{G}$ 开始，假设它有一个正规子群 $\mathcal{H}$。考虑陪集 $g_a\mathcal{H}$ 和 $g_b\mathcal{H}$ 中的任意元素 $g_a h_i$ 和 $g_b h_j$ 和它们的乘积：

$$(g_a h_i)(g_b h_j) = g_a g_b g_b^{-1} h_i g_b h_j = g_a g_b (g_b^{-1} h_i g_b) h_j = g_a g_b \tilde{h}_i h_j, \tag{2.60}$$

其中共轭元素 $\tilde{h}_i$ 属于正规子群 $\mathcal{H}$。所以两个陪集的乘积：

$$g_a\mathcal{H} \otimes g_b\mathcal{H} = g_c\mathcal{H}, \tag{2.61}$$

满足群的性质。为了补全群的结构，单位元素是子群 $\mathcal{H}$ 本身，且如果 $g_a g_b = h_i$，那么陪集 $g_a\mathcal{H}$ 和 $g_b\mathcal{H}$ 互为对方的逆。如此构造得到的集合满足群公理（容易验证结合律），构成一个具有 n_g/n_h 个元素的群。这个群称为商 *(quotient* 或 *factor)* 群，

$$\mathcal{G}/\mathcal{H}.$$

它是群 $\mathcal{G}$ 的一个同态像（译注：image），但不是 $\mathcal{G}$ 的子群。

假设 $\mathcal{H}$ 不是 $\mathcal{G}$ 最大的子群。我们将其如下形式的生成元：

$$G : \{g_a, g_\alpha, h_i\}, \tag{2.62}$$

拆分为：

$$\mathcal{G} \supset \mathcal{H}' \triangleright \mathcal{H}, \quad \mathcal{H}' : \{g_\alpha, h_i\}, \tag{2.63}$$

式中的 $\mathcal{H}$ 是 $\mathcal{H}'$ 的正规子群。我们可以构造两个商群：

$$\mathcal{G}/\mathcal{H} : \{g_\alpha\mathcal{H}, g_\alpha\mathcal{H}, \mathcal{H}(=1)\}, \quad \mathcal{K} \equiv \mathcal{H}'/\mathcal{H} : \{g_\alpha\mathcal{H}, \mathcal{H}(=1)\}. \tag{2.64}$$

显然 $\mathcal{K}$ 是 $\mathcal{G}/\mathcal{H}$ 的一个子群：

$$\mathcal{K} \subset \mathcal{G}/\mathcal{H}. \tag{2.65}$$

因为 $\mathcal{H}$ 是一个正规子群，共轭运算满足：

$$\widetilde{g_\alpha\mathcal{H}} = \widetilde{g}_\alpha\mathcal{H}, \quad \widetilde{g}_\alpha = g_\alpha g_\alpha g_\alpha^{-1}. \tag{2.66}$$

因此，如果 $\widetilde{g}_\alpha$ 是 $\mathcal{H}'(\in\{g_\alpha\})$ 的一个元素，$\mathcal{K}$ 是该商群的一个正规子群；反之则不是。不过这样的话，$\mathcal{H}'$ 本身必须是 $\mathcal{G}$ 的正规子群：$\mathcal{G}/\mathcal{H}$ 仅当 $\mathcal{H}$ 不是极大 (译注:maximal) 正规子群时具有一个正规子群。

当 $\mathcal{H}$ 是群 $\mathcal{G}$ 的极大正规子群时，商群 $\mathcal{G}/\mathcal{H}$ 没有正规子群。这个事实为我们打开了一条道路，来系统性地将所有群分解为单群。

1.4.2 单群

具有正规子群的有限群并不稀奇，数学家们不认为它们是基本的（群）。伽罗华，群论的创立者，将所有群分为两类：没有正规子群的*单群*和其他的群。

在伽罗华那里，这是一个非常重要的区分。他在五个对象的交错群 $\mathcal{A}_5$ 的简单性与无法通过根式（使用平方根、立方根等等）找到五次方程的求解公式之间建立了联系！（译注：原来数学上 radical 是根式。。一眼直接幻视自由基。。属于是被化学系害了）

到目前为止我们只接触到过一种单群，即素数阶的循环群 $\mathcal{Z}_p$，它们没有子群。现代数学的一项伟大成就就是近来对所有单群的分类。通常来说，单群都非常大：比如 $\mathcal{A}_5$ 包含 60 个元素，而第二大的单群（不考虑循环群的话）有足足 168 个元素！我们会在完成对李代数的讨论之后重新回到单群的分类问题上。在这里我们先列出几种单群的类型。

- 素数阶的循环群,$\mathcal{Z}_p$。
- 五个或以上对象的交错群,$\mathcal{A}_n$，$n\geq 5$。
- *李型群 (groups of Lie type)* 的无限群族（在后文中定义）。
- 26 个*散在单群 (sporadic groups)*

所有的有限群都能够从单群系统性地构造出来。我们马上就会介绍这种方法。

注释：**合成列** *(Composition series)*

我们可以通过寻找极大正规子群 $\mathcal{H}_1$ 的方式来分解任意的群。如果一个群具有一个正规子群，那么群元素可以划分为 $\mathcal{H}_1$ 和商群 $\mathcal{G}/\mathcal{H}_1$。我们在 $\mathcal{H}_1$ 上重复进行上述流程：我们找到它的极大正规子群 $\mathcal{H}_2$，然后将它的元素划分为 $\mathcal{H}_1$ 和商群 $\mathcal{H}_1/\mathcal{H}_2$，如此反复。这一流程产生了群的*合成列 (composition series)*。它总是在恒等元素上终止：

$$G\triangleright\mathcal{H}_1\triangleright\mathcal{H}_2\triangleright\cdots\triangleright\mathcal{H}_k\ (\text{simple subgroup})\triangleright e, \tag{2.67}$$

同时产生如下的商群：

$$G/\mathcal{H}_1,\mathcal{H}_1/\mathcal{H}_2,\ldots,\mathcal{H}_k; \tag{2.68}$$

一般来说商群并不一定是单群，但是在合成列中产生的商群一定是单群。这是因为在每一步中产生的商群都是由极大正规子群所产生的。这个过程将群分解为组成它的单群。这就是为什么数学家们认为单群是构成所有其他有限群的基本实体。特别地，如果所有的商群都是素数阶的循环群，那么这个群称为可解的 *(soluble 或 solvable，后者是伽罗华使用的术语)*。

上述分解的精妙之处在于，尽管一个群可能有多个合成列，即再分解时可以有若干个正规子群供选择，但合成列总是有一些不变的特性：分解至单位元素所需的步数总是不变的；同时，商群的阶数，称为合成指数（*composition indices*）也总是不变的！因此，它们是一个群的固有特征。

四元数群有若干个子群，所有这些子群都既是正规群也是阿贝尔群；其中最大的子群是 $\mathcal{Z}_4$，然后是 3 个不同的 $\mathcal{Z}_2$。它的三步合成列是：

$$Q \triangleright Z_4 \triangleright Z_2 \supset e, \tag{2.69}$$

随之产生的商群：

$$Q/Z_4 = Z_2; \quad Z_4/Z_2 = Z_2; \quad Z_2. \tag{2.70}$$

它的合成指数是 2，2，2，长度为 3.

我们鼓励读者子集找出群 $\mathcal{Z}_4$ 和 $\mathcal{A}_4$ 的合成列和正规子群。

注释：导出（换位）子群 *(Derived(commutator) subgroups)*

令 a 和 b 为群 $\mathcal{G}$ 的任意两个元素。我们定义它们的交换子 *(commutator)*（译注：也称为换位子）为：

$$[a, b] \equiv a^{-1}b^{-1}ab, \tag{2.71}$$

如果两个元素对易，那么交换子就是单位元素。进一步地，由于 $[b, a] = ([a, b])^{-1}$，所有可能的交换子的乘积构成了一个群 $\mathcal{G}'$，称为导出或者换位子群。容易看出导出子群是一个正规子群。有：

$$\widetilde{[a, b]} = g\left(a^{-1}b^{-1}ab\right)g^{-1} = [\widetilde{a}, \widetilde{b}], \tag{2.72}$$

其中

$$\widetilde{a} = gag^{-1}, \widetilde{b} = gbg^{-1}, \ldots \tag{2.73}$$

所以共轭操作将导出子群映射到其自身。举个例子，我们计算二面体群的导出子群 $\mathcal{D}'_n$。二面体群的元素的形式是：$a^m, a^m b, m = 1, 2, \ldots, n$，同时 $b^2 = e, aba = b$。我们会发现：

$$[a^m, a^k b] = a^{-2m}, \quad [a^m b, a^k b] = a^{2(m-k)} \tag{1.1}$$

所有其他的交换子要么是单位元素，要么是上面交换子的逆。因此，如果 n 是偶数，那么 $\mathcal{D}_n$ 的

换位子群就是循环群 $\mathcal{Z}_{n/2}$，而如果 n 是奇数，那么则是循环群 $\mathcal{Z}_n$。

对于 $\mathcal{G}'$ 来说，有三种情况：$\mathcal{G}'$ 就是 $\mathcal{G}$ 本身，那么 $\mathcal{G}$ 就是一个*完美群 (perfect group)*；$\mathcal{G}' = e$，这说明 $\mathcal{G}$ 是阿贝尔群；除此之外 $\mathcal{G}' \triangleleft \mathcal{G}$，且此时 $\mathcal{G}$ 不是单群。由于具有一个与自身不同且不为 e 的换位子群，$\mathcal{D}_n$ 并不是单群。因此一个（一般的）群可能是完美的（一个群是自身的换位子群并不意味着它没有正规子群），而非阿贝尔的单群则一定是完美群。

1.4.3 西罗定理 *(Sylow's criteria)*

设 p 是一个素数。称所有群元素的阶数都是 p 的幂次的群为 p-群。p-群可以是阿贝尔的，例如循环群；也可以是非阿贝尔的：例如，$\mathcal{D}_4$ 群的元素的阶数为 2 或 4，因此它是一个西罗 2-群。令 $\mathcal{G}$ 是一个 n 阶群。我们将它的阶数分解为素数幂形式，即 $n = p^m r$，其中 p 是一个素数，r 不能被 p 整除。路德维希 · 西罗提出了如下的一系列定理：

- $\mathcal{G}$ 包含 n_p 个（西罗）p-子群 $\mathcal{G}_p^i, i = 1, 2 \ldots, n_p$，这些子群的阶数为 p^m。
- 所有的 $\mathcal{G}_p^i$ 都是相互同构的，由 $\mathcal{G}_p^j = g\mathcal{G}_p^k g^{-1}, g \in \mathcal{G}$ 相关联。
- n_p 是 r 的因数。
- $n_p = 1 \mathrm{mod}(p)$。

这些定理给特定阶数的群做出了很强的限制。

假设 p 和 q 均为素数，考虑一个阶数为 $n = pq$ 的群。西罗定理告诉我们这种群具有 n_p 个 p 阶子群 $\mathcal{G}_p$ 和 n_q 个 q 阶子群 $\mathcal{G}_q$。这些群只能是循环群。西罗定理要求 n_p 是 q 的因数，因此 $n_p = 1$ 或 q。同时 $n_p = 1, 1 + p, \ldots$，所以如果 $p > q$，那么解就只能是 $n_p = 1$。不过反过来说，$n_q = 1, 1 + q, 1 + 2q \ldots$ 还是可能的，只要它能够整除 p。$n_q = 1$ 是一个始终可行的解，对应于：

$$\mathcal{Z}_{pq} = \mathcal{Z}_p \times \mathcal{Z}_q. \tag{1.2}$$

我们已经看到过这种例子：如果 a 和 b 分别是 $\mathcal{Z}_p$ 和 $\mathcal{Z}_q$ 的元素，那么元素 (a, b) 的阶数显然是 pq。

另一种情况是 $n_q = p$，不过这只有在 $p = 1 \mathrm{mod}(q)$ 时才是可能的。这说明阶数为 pq 的群至多只有两个。而如果 $p \neq 1 \mathrm{mod}(q)$ 的话，则只有一个。如果只有一个西罗子群的话 ($n_p = 1$)，那么它是一个正规子群。

让我们来考虑一些西罗定理的应用。我们可以推断 15 阶群只有一个。因为 $15 = 3 \cdot 5$，又由 $5 \neq 1 \mathrm{mod}(3)$，所以只有 $\mathcal{Z}_{15} = \mathcal{Z}_3 \times \mathcal{Z}_5$。

而当阶数为 21 时，则有两个群。$21 = 3 \cdot 7$，而 $7 = 1 \mathrm{mod}(3)$。除了循环群之外的另一个 21 阶群称为弗罗贝尼乌斯 (Frobenius) 群。它是七个对象的置换群的一个子群。它有一个由 (1234567) 生成的西罗 7-子群和 7 个由 (235) 和 (476) 生成的西罗 3-子群。

使用西罗定理进行分析在寻找单群时非常有用。其原因在于只有一个西罗子群的群不可能是单群。因为共轭运算会将其映射回其自身。举个例子，任意的 $84 = 2^2 \cdot 3 \cdot 7$ 阶群都包含 n_7 个西罗 7-子群。n_7 需要能够整除 12，同时只能取 $1, 8, 15 \ldots$。唯一的可能只能是 $n_7 = 1$，所以不存在 84 阶的单群。

1.4.4 半直积 *(Semi-direct product)*

（在直积之外）还有一种从两个群构造一个新群的方法。这种方法比直积更加精巧。这种构造方式需要两个群 $\mathcal{G}$ 和 $\mathcal{K}$，以及一个群对另一个群的作用。

设群 $\mathcal{G}$ 通过将群 $\mathcal{K}$ 中的每一个元素映射为另一个的方式对其作用：

$$\mathcal{G}: \quad k \to k' = k^g, \tag{2.75}$$

其中 $g \in \mathcal{G}$。对任意两个群元素：

$$(k^{g_1})^{g_2} = k^{g_1 g_2} = k^{g'}. \tag{2.76}$$

对任意两个群元素 $k_a, k_b \in \mathcal{K}$，有：

$$(k_a k_b)^g = k_a^g k_b^b, \tag{2.77}$$

如此一来 $\mathcal{K}$ 的乘法表得以保持（同态）

$$k_a k_b = k_c \to (k_a)^g (k_b)^g = k_c^g. \tag{2.78}$$

可以验证元素 (k_a, g_i) 满足结合律，构成一个群

$$(k_a, g_i) \cdot (k_b, g_j) \equiv ((k_a)^{g_j} k_b, g_i g_j) \tag{2.79}$$

这个阶数为 $n_k n_g$ 的新群称为 $\mathcal{G}$ 和 $\mathcal{K}$ 的半直积 *(semi-direct product)*，记为

$$\mathcal{K} \rtimes \mathcal{G}. \tag{2.80}$$

这个有趣的记号用以区别于直积记号。

对于有限群来说，可以想见如下几种可能的情况：一个自然的选择是取 $\mathcal{G}$ 为 $\mathcal{K}$ 的自同构群，有时也称为 $\mathcal{A}ut\ \mathcal{K}$，在这种情况下它们的半直积称为群的全形。

$$Hol(\mathcal{K}) \equiv \mathcal{K} \rtimes \mathcal{A}ut\ \mathcal{K}. \tag{2.81}$$

另一种情况是取 $\mathcal{K}$ 为 $\mathcal{G}$ 的一个正规子群。$\mathcal{G}$ 可以以共轭作用于 $\mathcal{K}$。

我们可以用几个例子来说明这个操作。考虑 $\mathcal{D}_2$ 群，$\mathcal{A}ut\ \mathcal{D}_2 = \mathcal{S}_3$。我们可以构造 $\mathcal{D}_2$ 和 $\mathcal{S}_3$ 或者其他子群的半直积。一般地，有：

$$D_n = Z_n \rtimes Z_2. \tag{2.82}$$

其表示

$$D_n : \quad (a^n = e; b^2 = e; bab^{-1} = a^{-1})$$

表明由 b 生成的 $\mathcal{Z}_2$ 通过共轭作用于 $\mathcal{Z}_n$。

注释：*传递性 (Transitivity)*

传递性的概念在有限群的分类中起着重要作用。我们通过作用于对象集合 $[a_1, a_2, \ldots, a_{n-1}, a_n]$ 的轮换来描述置换操作。$\mathcal{S}_n$ 中的 $n!$ 个置换操作产生 $n!$ 种不同的排列 $[b_1, b_2, \ldots, b_{n-1}, b_n]$。我们用数字标记这些对象，然后从特定的一种排列 $[1, 2, \ldots, (n-1), n]$ 开始。显然任意其他的排列都以通过 $\mathcal{S}_n$ 中的某个置换得到：我们把这样的 $\mathcal{S}_n$ 称为是（单 (singly)）*传递 (transitive)* 的。不具有这种性质的群则称为是*非传递的 (intransitive)*。例如，对由轮换 $(1, 2), (3, 4)$ 生成的对 4 个对象的置换群是非传递的。因为它并不包含将 $[1, 2, 3, 4]$ 映射为 $[3, 2, 1, 4]$ 的置换。因为 $\mathcal{S}_n$ 将任意的 n 个对象的集合映射到另一个，它称为 *n-重传递的 (n-ply transitive)*。换句话说，如果我们将一个元素 g 的*轨道 (orbit)*（译注：你别说还是挺形象的。。）定义为所有由群操作对 g 作用产生的元素的集合，那么一个传递群就只有一个轨道。显然，$\mathcal{S}_n$ 中的任意置换对 $k < n$ 来说当然 (译注：这里本来是一个语气词 fortiori) 也是 k-重传递的。如下的对应关系：

$$\text{偶置换} \to 1, \quad \text{奇置换} \to -1, \tag{2.83}$$

将 $\mathcal{S}_n$ 映射为 $\mathcal{Z}_2$，后者是前者的一个子群。如我们已经知道的，偶置换群 $\mathcal{A}_n$ 构成了这个映射的*核*。因为奇置换的共轭不会改变奇偶性，它是一个正规子群。进而 $\mathcal{S}_n$ 不是单群。又因为 $\mathcal{A}_n$ 是 $\mathcal{S}_n$ 最大的正规子群，我们可以确定它的商群是一个单群：

$$S_n/\mathcal{A}_n = Z_2, \tag{2.84}$$

考虑 $(n-1)$ 个对象构成的数组 $[a_2, a_3, \ldots, a_{n-1}, a_n]$。注意它不包含 a_1。从它产生 $(n-1)$ 维数组 $[a_1, a_3, \ldots, a_{n-1}, a_n]$（其中 a_2 被替换为 a_1）的唯一方法就是通过对换 $(a_1 a_2)$：

$$[a_2, a_3, \ldots, a_{n-1}, a_n] \longrightarrow [a_1, a_3, \ldots, a_{n-1}, a_n]. \tag{2.85}$$

$$_{(a_1 a_2)} \tag{1.3}$$

这是一个奇置换，我们可以从上式推断出 $\mathcal{A}_n$ **不是** (n-1)-重传递的。现在看看包含 $(n-2)$ 个对象的集合 $[a_3, a_4, \ldots, a_{n-1}, a_n]$，其中没有 a_1 和 a_2。同样地，将 a_3 替换为 a_1 的数组 $[a_1, a_4, \ldots, a_{n-1}, a_n]$ 可以通过对换 $(a_1 a_3)$ 获得，不过既然我们有一个 "闲置的" 对象 a_2，我们也可以通过一个偶置换来实现：

$$[a_3, a_4, \ldots, a_{n-1}, a_n] \longrightarrow [a_1, a_4, \ldots, a_{n-1}, a_n]. \tag{2.86}$$

$$(a_3 a_1 a_2) \tag{1.4}$$

若同时将 a_3 和 a_4 替换为 a_1 和 a_2，则可通过两个对换的（偶）乘积实现。因此 $\mathcal{A}_n$ 是 $(n-2)$ 重传递的。

除了 $\mathcal{S}_n$ 和 $\mathcal{A}_n$ 之外，多重传递群的相对而言比较少：有几个双重传递群的无穷群族，以及一个三重传递的无穷群族。这些群都在离散几何中有有趣的解释。此外，还有几个孤立的双重传递群，一个三重传递群，两个四重传递群和两个五重传递群。除了一个之外，所有这些多重传递群都是散在群。

1.4.5 杨表 *(Young Tableaux)*

最后，以作用于五个对象的第一个重要置换群 $\mathcal{S}_5$ 为例，我们展示一种系统的方法来呈现其中的 $5! = 120$ 个置换。我们从如下的轮换分解开始：

$(xxxxx)$	5	24	$+$
$(xxxx)(x)$	$4+1$	30	$-$
$(xxx)(xx)$	$3+2$	20	$-$
$(xxx)(x)(x)$	$3+1+1$	20	$+$
$(xx)(xx)(x)$	$2+2+1$	15	$+$
$(xx)(x)(x)(x)$	$2+1+1+1$	10	$-$
$(x)(x)(x)(x)(x)$	$1+1+1+1+1$	1	$+$

上式中 (x x x x x) 表示一个包含任意元素的轮换。不同轮换的数目与将 5 进行分割的方式一一对应，列于上表中。我们还列出了每一种分割方式的置换的数目，以及他们的奇偶性。每一种 n 的分割方式都与 $\mathcal{S}_n$ 的一个不可约表示相对应。一种常用的表示这样的划分方式是 n 个整数的有序集合 $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_n$。其中每个数由阶数为 k 的轮换的数目 α_k 定义。

$$\lambda_1 = \sum_{i=1}^{n} \alpha_i, \ \lambda_2 = \sum_{i=2}^{n} \alpha_i \ldots \lambda_n = \alpha_n \tag{2.87}$$

举例来说，(x x x x)(x) 对应于 $\alpha_1 = 1$, $\alpha_4 = 1$，它得到的五个整数是 $\{2, 1, 1, 1, 0\}$，简写为

$\{2, 1^3\}$。

这种分割还可以用图案来表示,这种表示方法称为*杨表 (Young Tableaux)*。与分割 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 关联的杨表通过如下的方式获得：水平并排放置 λ_1 个方框，然后在下面再排列 λ_2 个方框，依此类推，直到最小的 λ_k。这样的排列规则将 $\mathcal{S}_5$ 的每一种分割和类与唯一的一个杨表关联起来，如下所示。

TBD 图示

用杨表来表示分割方式在某些情况下非常有用，特别是在确定张量的对称性，以及确定群表示乘积的变换性质的时候。