群论入门

从对称到计数

大青花鱼

群论入门

从对称到计数

大青花鱼

© 2026 大青花鱼

本作品采用知识共享署名-相同方式共享 4.0 国际许可协议（CC BY-SA 4.0）进行许可。
协议全文详见：https://creativecommons.org/licenses/by-sa/4.0/

您可以自由地共享、修改本作品，但须遵守“署名”和“相同方式共享”的条件。

前言

群是现代数学的基础概念，群是研究复杂问题的重要工具，群是展示数学之美的上好途径。

可是，群论怎么入门?

是直接从代数的定义出发，摆弄各种字母等式吗？是看各种精彩美妙的图形，泛泛欣赏对称之美吗?

自从数学教育普及以来，有许多降低群论入门难度的尝试，其主旨不外乎将以上两点调和起来。本书也不例外，不过试图提供一个新的“菜谱”，一本对自学者友好、但又能使其真正登堂入室的书。只要还没使用传统高等数学教材系统学过群论，读这本书就不算迟。

本书的目标是把群的概念和基本性质说清楚。以常见的有限群为例子，把中学数学里说的“对称”讲明白，把传统群论教材中前半部分的内容细致地讲好。主要覆盖子群、商群、群同态和群作用等概念。

要讲清楚这些概念，至少需要什么知识呢?

本书的视角是：群是对称变换的集合。为此，掌握集合与映射是必需的。我们希望用直观的图形变换来理解群，所以基础的几何知识也不可少。除此以外，为了介绍群的应用，我们需要掌握基础的组合计数知识。

从这些知识开始，我们能走多远？本书试图给出一个回答。我们希望读完这本书的人，能计算把正方体的面染成三种颜色的方法有多少，并说得清背后的群论道理。

如何做到这一点呢？纵观以往的尝试，或者从具体现象出发，但不敢多做演算，浅尝辄止；或者早早陷入图形变换的抽象分析，在讨论向量和矩阵中迷失，难以脱身；或者从解高次方程讲起，直奔代数式的丛林，叫人望而却步。本书借鉴了内森 · 卡特 (Nathan

Carter）的《可视群论》（Visual Group Theory）一书的做法，从直观的图形变换出发，但不侧重于严格讨论平面和空间中的运动，而只把它作为演示群变换的工具，专注于展示群自身的结构以及揭示背后的思想。通过图形和图解让读者看见群、理解群、思考群。待到对群的了解足够了，再正式介绍并讨论其代数性质。希望这种方法能避免过往种种弊端，帮助读者揭开群的面纱，真正掌握讨论群的手段。

本书的另一个尝试是采用中文本位的术语体系，故而一部分术语记号与主流中文教材不同。附录中有说明和对照表，方便查阅。本书采用知识共享署名—相同方式共享 4.0 国际许可（CC BY-SA 4.0）发布。读者可以自由复制、传播、改编本书，包括用于教学与商业用途，只需署名并以相同许可发布。

《可视群论》是本书前半讲法的来源，谨此致谢。作为初版，疏漏难免。恳请各位方家斧正，指出错误，提出建议。

目录

前言 **iii**

致读者 **ix**

第一章 什么是群? **1**

1.1 对称和变换 1

1.2 变换的规则 3

1.3 群有哪些? 4

1.4 习题 8

第二章 群是什么样子的? **11**

2.1 连线图 12

2.2 生成与路径 14

2.3 长方形的群 16

2.4 共同的结构 19

2.5 习题 25

第三章 群是代数结构 **27**

3.1 群的乘法表 27

3.2 复合是乘法吗? 29
3.3 群的经典定义 31
3.4 习题 36

第四章 四种常见的群 **43**

4.1 循环群 43
4.1.1 环道 47
4.2 交换群 48
4.3 映轮群 54
4.4 置换群 60
4.5 置换群定理 64
4.6 习题 70

第五章 子群 **75**

5.1 群中之群 76
5.2 往集 78
5.3 往集定理 80
5.3.1 循环群的子群 82
5.3.2 映轮群的子群 83
5.4 习题 85

第六章 商群与同态 **87**

6.1 往合子群和商群 88
6.2 群同态 93
6.3 群同态基本定理 96

6.4 习题 102

第七章 观群 **105**

7.1 观群于集合 105

7.2 轨迹 111

7.3 定子与定元 114

7.4 轨定定理 117

7.5 习题 122

第八章 计数定理 **129**

8.1 计数与群 130

8.2 定元分轨定理 132

8.3 更进一步的计数 138

8.4 习题 143

附录 **153**

附录一 练习题参考解答 **155**

1.1 第一章参考解答 155

1.2 第二章参考解答 161

1.3 第三章参考解答 167

1.4 第四章参考解答 176

1.5 第五章参考解答 189

1.6 第六章参考解答 193

1.7 第七章参考解答 199

1.8 第八章参考解答 211

附录二 本书符号记法常例 **227**

附录三 术语对照表 **231**

致读者

你是一个中学生，对中学数学的知识掌握得差不多了，好奇什么是群论；又或者你已经告别中学了，但中学数学的知识还没有落下，想重新学学数学，了解一下群论是什么。这本书就是为你写的。

这是一本用科普手法写的群论入门教材。它不像传统的代数教材那样，直接从严谨但枯燥的内容开始，讨论抽象的概念。这是一本从想法入手的书。群到底是什么？当数学家们使用群的概念时，他们在想什么？提出想法，理解想法，验证想法，这比直接计算或证明一些高深的定理更重要。如果你想认真学习群论，这本书能带你入门，给你一些基础的概念和丰富的例子，让你在正式踏上学习群论或抽象代数理论的道路前，有机会仔细思考一些基本的问题，准备得更好。前四章能让你看到群的样貌，你产生的很多疑问会在第五、六、七章得到解答，第八章能让你知道，怎么在实际问题中使用群的理论。

如果你只想泛泛了解群的概念和理论，把这本书当作科普读物也没问题。这本书介绍了群的基本性质，并不作过多深入讨论。当你在别的领域里遇到群的概念时，本书的内容能让你有讨论它的基本语言。本书只要求你具备高中水平的数学知识，但可能需要你熟悉集合、映射的语言和代数式的演算。你可以重点阅读前四章，第五、第六章可以大致了解结论。第七章会帮助你更好理解前四章的很多东西，第八章是你不应该错过的。

本书有很多图，希望能帮你看见群的样子。但图并不是一切。群是抽象的概念。但愿当你进入代数的抽象区域时，这些图像能帮你更好地思考。每章末尾有小结，列出了继续阅读前最好掌握的关键内容。每章还配有习题，附录中有所有习题的解答。虽然我们推荐认真学习的读者做一些习题（不必全做），但不做习题也不会妨碍继续阅读。当然，愿意认真做习题的人会得到应有的回报。

本书用语使用中文本位的术语体系，和主流中文用语、符号可能不同。附录二、附

录三有全面的对照表格供查阅。

开始阅读之前，建议你准备好一张纸和一支笔（有不同颜色的笔会更好），最好有一个骰子或小方块，也许准备两个硬币。如果你能使用生成式人工智能服务，可以试试把本书的源代码交给它，让它更好地辅助你阅读。

第一章　什么是群?

1.1　对称和变换

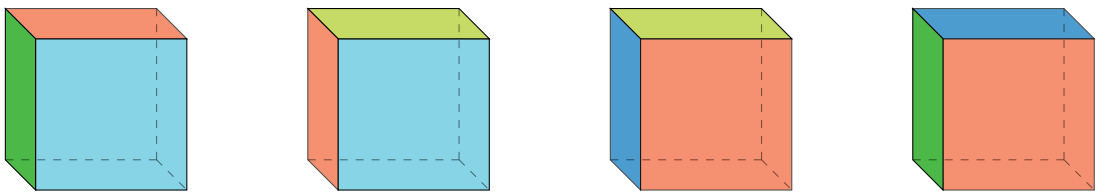
想象一个方块。一小时前你看过它，摆放在地上。现在它还在原来的位置上。可你发现，这方块被动过了。

为什么这么说呢？因为方块各个面的颜色不同。你发现，虽然方块的位置没变化，可原本朝上的一面，现在面向着你。

这是一种怎样的变动呢？最简单的说法是，方块朝前转动了 90°。



不过，也可以说它先朝左转动了 90°，让上面（浅红色）变成左面，保持前后面（蓝色）不变；接着往右转了 90°，让左面（浅红色）变成前面，保持上下面（绿色）不变；然后再往右转动了 90°，让上面（浅绿色）变成右面，保持前后面（红色）不变。

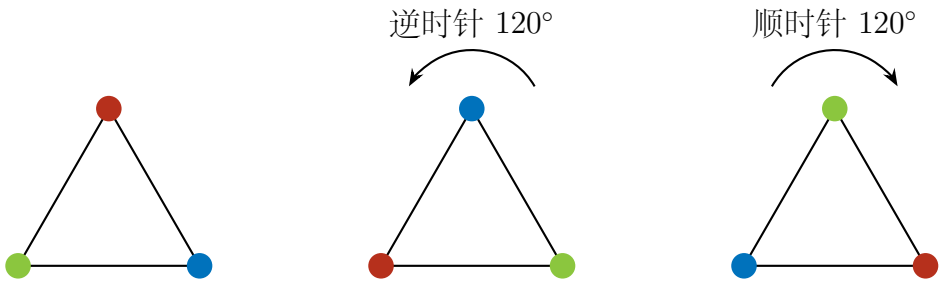


如果这个方块不是正方体，而是长方体呢？那么不需要通过颜色分辨，你就能看出

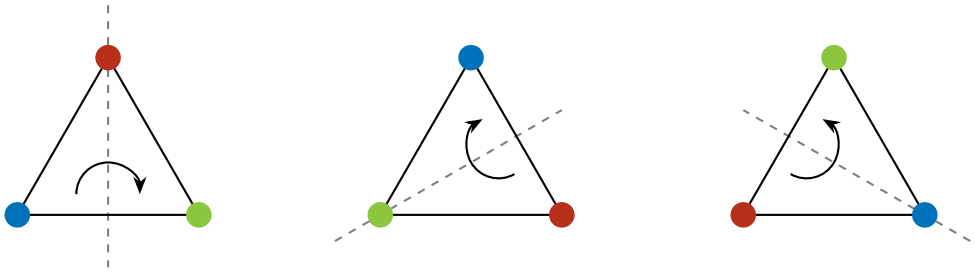
它动过了。因为朝前转动 90° 会让它的形状看起来不一样。

这种区别的背后，是什么在起作用呢?

再想象一个正三角形。按它的中心，逆时针旋转，你会发现，旋转 120° 后，看起来和原来一样。顺时针旋转 120° 也是如此。要区别这些状态，可以给三角形的顶点按逆时针方向依次标上颜色，比如红色、绿色、蓝色。你会发现，前一个旋转把红色顶点转到了绿色顶点的位置，把绿色顶点转到了蓝色顶点的位置，把蓝色顶点转到了红色顶点的位置。后一个旋转则把红色顶点转到了蓝色顶点的位置，把蓝色顶点转到了绿色顶点的位置，把绿色顶点转到了红色顶点的位置。这下我们能清楚区分这两个旋转了。



此外，如果把正三角形沿某条中线翻转，它看起来也不变。可要是我们把顶点标上颜色，就能看到变化了。



而要是三角形不是正三角形，比如三边都不一样长，那么除非旋转一周，否则不会看起来和原来一样。旋转 120° 和沿中线翻转都没用了。

正方体、正三角形都有某种性质，在某些变换下不变，我们称其为**对称性**。日常语言中的对称是指左右手、左右眼这样的关系，也就是按轴线或平面翻转后不变。数学里，我们把“在某些变换下不变”的性质都称为对称性。我们已经讨论过的对称性有平面形的轴对称和中心对称。前面的例子里翻面或旋转不变也是一种对称。对称能帮助我们思考。比如，我们说偶函数的图像关于 y 轴对称，所以只要理解了函数在 $x > 0$ 时的性质，就能让我们理解它在 $x < 0$ 时的性质。不过，对于对称本身，我们还没有展开研究。具

体来说，造成对称的是某种抽象规律，而数学就是抽离表象、揭示内在规律的学科。下面就让我们来研究对称背后的道理。

1.2 变换的规则

为什么正方体和正三角形通过翻转、旋转看起来不变? 因为它们所有的边都一样长，所有的角都一样大，所有的面都一样。这种对称性导致它们在某些变换下不变。反过来说，这些变换刻画了它们的对称性质。通过研究这些变换，我们就能理解对称。

前面的例子里，我们给正三角形的顶点标记了颜色。我们发现，顺时针、逆时针旋转 120°，改变了顶点的颜色。通过这个做法，我们发现有 6 种变换能让正三角形看起来不变。分别是顺时针、逆时针旋转 120°，沿 3 条中线翻转，以及什么也不做（没错，我们把这种“变换”也考虑在内）。这就是我们感兴趣的所有变换。

正方体的情形则更复杂。它有 6 个面。首先可以把任一个面转到朝上；接着，不改变朝上的面，可以把 4 个侧面之一转到正对我们。因此，一共有 $6 \times 4 = 24$ 种转动方法。这就是我们感兴趣的所有变换。

一旦确立了要研究的变换的集合，我们就不再改动了。这个集合就是我们研究的“舞台”。

接着，我们来考察各种变换的关系。

首先，我们只考虑理想的变换。比如某次旋转三角形的时候角度差了一点点，某次转动方块的时候整体位置稍微动了一点，这种问题我们不考虑在内。我们讨论的是抽象的理想的情况。同一个变换每次操作的效果是一致的，每个变换的效果是确定的。

其次，每个变换都是可逆的，逆变换也在集合里。比如，我们有把正三角形沿逆时针旋转 120° 的变换，就有把正三角形沿顺时针旋转 120° 的变换。它恢复“逆时针旋转 120°”这个操作。正方体的变换里，每种方式转过后，也可以逆着转回来。

最后，变换的组合还是某种变换。比如我们会发现：把正三角形沿逆时针旋转 120° 两次，效果和沿顺时针旋转 120° 是一样的。把正方体顶面转到左面、右转 90°、再把顶面转到右侧面，效果和把顶面转到正面是一样的。无论怎么变，结果总是集合里的某种变换。

我们来总结一下这些规则:

1. 有一个确定不变的、由变换构成的集合。
2. 每个变换的效果是确定的。
3. 每个变换的效果是可逆的。
4. 变换的组合还是某种变换。

这就是我们从正三角形和正方体的例子里抽离出来的规则。它们似乎已经足够多了。现在就让我们来研究根据这些规则得到的系统。我们把它称为**群**,看看它有什么性质。

1.3 群有哪些?

首先你可能想要知道,除了正三角形和正方体,还有哪些东西符合这个群的定义。我们大致能想象到正四边形(正方形)、正五边形里大概也有相关的群。不过,更聪明的读者也许会联想到更远的地方。比如,几个人坐在圆桌边上,不同的坐法之间有什么关联呢?我们可以把每种调换位子的方法看作一种变换。所有的变换构成一个集合;每种变换的效果是确定的;调换位子后肯定能调换回来;最后,几个调换位子的方法组合起来,必然也是一种调换位子的方法。所以,不同的坐法背后也是一个群。

又比如,我们玩扑克牌之前也许会洗牌,把牌打乱。每次洗牌都是变换牌的顺序。所有变换扑克牌顺序的方法构成确定的集合;每种方法的结果是确定的;每次洗牌的效果是可逆的(也许经过魔术师的训练才能做到,但我们不难想象理想情况下的效果);最后,无论洗多少次牌,效果也是变换扑克牌的顺序,还是某种变换。所以,扑克牌的所有可能的洗牌变换也是一个群。

我们还可以考虑数学里的场景。比如,考虑模 5 的同余类,我们知道它可以写成:

$$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

从某个数(比如 0)出发,通过加法,我们把它变成属于其他的同余类。比如“加 1”变换就把 0 从同余类 $\overline{0}$ 的成员,变成 $\overline{1}$ 的成员。这样的变换一共 5 种,构成确定的集合;每个变换的效果是确定的。不仅如此,变换的组合仍然是变换。比如“加 1”然后“加 2”的效果就是“加 3”。最后,变换的效果是可逆的,比如加 1 之后再加 4,就能把一个数变回原来的同余类;加 3 之后要变回原来的同余类,只需再加 2。等等。可以验证每个变换都可逆。于是,模 n 同余类通过加法也定义了一个群,记为 $\mathbb{Z}_n$。

群的元素个数可以是无限的。比如，对于圆来说，所有绕圆心的旋转构成群。这样的旋转有无限个。我们沿用集合的称呼，把群的大小称为群的**势**。对于有限个变换构成的群，变换的个数就是群的势。无限个变换构成的群，它的势要和我们常见的无限集合比较，这里不多叙述。

上面的说法，让我们觉得群似乎无处不在。然而，也有些结构并不是群。比如，把以上的模 5 同余类换成自然数集 $\mathbb{N}$，考虑“加 1”、“加 2”等变换，它们确实也构成确定的集合，效果也是确定的，甚至若干个“加几”变换组合起来，还是某种“加几”变换。唯一的问题是：“加几”变换不是可逆的。我们没法通过“加几”把“加 1”的效果逆转。所以“加几”定义的变换集合不是群。不过，如果我们把范围扩大到整数集 $\mathbb{Z}$，就会发现，“加几”又构成群了。因为这时候，“加 -1”就是减 1，能逆转“加 1”的效果了。

我们可以画一个数轴来理解这件事。数轴上，“加几”就是从原点出发往右移到某个整点。如果只考虑自然数，那么只有右半边的数轴。如果考虑全体整数，则变成既可以往左移动，也可以往右移动，这就覆盖了整个数轴，左右对称了。所以群必然体现了某种对称性。不构成群，往往意味着某个方面还不够对称。

例题 1.1

以下的例子里是否包含群?

1. 一枚金币和一枚银币放在桌子上，都分正反面。每次可以选择翻动一枚币。这样的变换有几个？是否构成了群?
2. 同上情况。每次可以选择翻动一枚币、两枚币，或者什么都不做。这样的变换有几个？是否构成了群?
3. 同上情况。每次要么同时翻动两枚币，要么什么都不做。这样的变换有几个？是否构成了群?
4. 考虑集合 A 到 B 的映射，这些映射是否构成了群?
5. 考虑集合到自身的所有映射，这些映射是否构成了群?
6. 考虑集合到自身的所有双射，这些双射是否构成了群?

解答： *1.* 每次恰好翻动一枚币，所以变换只有 2 个：翻金币、翻银币。翻金币后再翻银

币，两枚币都翻面，可是“同时翻两枚”并不在这 2 个变换之中。按规定，两个变换的组合无法用一次变换实现，不在集合里，不满足规则 4。因此不构成群。

2. 变换有 4 个：什么都不做、只翻金币、只翻银币、同时翻两枚。规则 1、2 显然成立。每个变换做两次都恢复原状，因此满足规则 3。再验证规则 4：任取两个不同的变换连续做，效果仍然是这 4 个变换之一。比如“只翻金币”接着“只翻银币”，效果等于“同时翻两枚”；“只翻金币”接着“同时翻两枚”，效果等于“只翻银币”。其他组合也可以逐一验证。这说明任意两种变换连续做的结果是某一个变换。于是对于多于两个变换的组合，可以不断把前两个变换替换成一个，最终简化成一个变换。于是规则 4 满足。综上可知构成群。

3. 变换有 2 个：什么都不做、同时翻两枚。规则 1、2 显然成立。“同时翻两枚”做两次，两枚币都翻了两次，恢复原状，效果等于“什么都不做”。所以它的逆变换就是它自己，满足规则 3。再验证规则 4：两个变换的任意组合仍在集合中。比如“同时翻两枚”接“同时翻两枚”等于“什么都不做”，其余组合更不成问题。同前一题可知规则 4 满足。综上可知构成群。

4. 集合 A 到集合 B 的映射，不一定能两两复合：第一个映射把 A 中的元素映射到 B 中，第二个映射也要从 A 出发，可是它的输入是 B 中的元素。除非 $B = A$，否则复合没有定义，规则 4 无从谈起。即使 $B = A$，一般的映射也未必可逆（比如把 A 中所有元素都映到同一个元素的常映射，就无法从结果还原输入），规则 3 也不满足。因此不构成群。

5. 集合到自身的映射，复合之后仍是集合到自身的映射，满足规则 4。每个映射的效果是确定的，满足规则 2。但并非每个映射都可逆。比如集合 $\{1, 2\}$ 到自身的映射“把 1 和 2 都映到 1”，无论再做任何映射，都不可能把 1 还原为原来的 1 和 2 两个不同的元素。所以规则 3 不满足。因此不构成群。

6. 集合到自身的双射，就是一一对应的映射。规则 1、2 显然成立。每个双射都可逆，且逆映射也是双射，满足规则 3。两个双射复合仍是双射，满足规则 4。因此构成群。

本章小结

本章我们从正三角形和正方体的对称变换出发，抽离出了对称现象背后的规则。一个群就是一个由“变换”构成的系统，它必须满足四个基本条件：

- **集合确定**：变换的集合是明确且固定的。
- **效果确定**：每个变换的效果是确定的，这是变换运算的前提。
- **操作可逆**：每个变换都存在逆变换，能够撤销其效果。
- **组合封闭**：任意两个变换的组合（复合）仍然是该集合中的变换。

通过圆桌座位、洗牌等例子，我们看到群广泛存在于各种具有对称性的场景中。群是描述和研究对称性的语言。群的大小（元素个数）称为群的势。

1.4 习题

以下习题是一些思想实验，目的是帮助你理解我们刚刚讨论的概念。在数学及类似的学科中，习题通常需要一些思考，会让你花费一些时间。本书并不会要求你反复琢磨每一段文字，大可以快速浏览内容，欣赏大略的思想。不过对于较为抽象的概念，只有经过一番思考，才能真正深入地理解其机理。因此，在习题上花费一些时间很正常，不要气馁。

不过，在习题上花费过多的时间，也是没必要的。到附录里查看习题的答案或解题思路，也不必感到不好意思。习题并不是为了刁难人而设置的。因此，思考几分钟无果，就查看答案来掌握思考方法，也是合理的策略。像读小说一样，完全不看习题，直接阅读下一章，也没有问题。

是不是群

1. 将一枚金币和一枚银币放在桌子上。考虑一个动作：交换两枚硬币的位置。这是群吗?

2. 在上述两币旁再放一个金币。仍然只考虑交换前两枚钱币的位置。这是群吗?

3. 你左边的裤袋子里有 5 个弹珠，右边的裤带子里也有 5 个弹珠。考虑两种动作：从左裤袋里拿一个弹珠放到右边裤袋里；以及从右裤袋里拿一个弹珠放到左边裤袋里。这是群吗?

4. 画廊的一间陈列室里有四面墙，其中三面墙上各挂着一幅画，每面墙上一幅。经理想重新排列这三幅画。每面墙只能挂一幅画，靠出口大门的墙不能挂画。

(1) 一共有几种挂画方法?

(2) 如果只允许两种重排方法：交换左墙和中间墙上的画，或者交换左墙和右墙上的画。只通过这两种手段，能实现任意的挂画方法吗?

(3) 这两种重排方法是群吗? 如果不是，还差了什么?

(4) 如果靠出口大门的墙也能挂画了，情况会如何变化? 以上问题的答案会变吗?

谈谈规则

1. 一个群里的变换是否一定有限？是否一定能列举出来？

2. 如果分析某个对象的对称性，发现只有“什么都不做”这个变换满足条件，这表示对象的对称性有什么特征？

3. 对以下每个要求，构造一个额外满足此要求的群。

(1) 变换组合的顺序会影响最终的效果。

(2) 变换组合的顺序不影响最终的效果。

(3) 恰好包含两个变换。

(4) 恰好包含三个变换。

(5) 恰好包含四个变换。

4. 任给一个正整数 n，你能构造一个恰包含 n 个变换的群吗？你能让这个群里出现“变换组合的顺序影响最终效果”的情况吗？

打破规则

下面来谈谈我们给群定的规则是否是必须的。不遵守这些规则会出现什么情况。前两条规则是基础的，离开它我们甚至不能确定我们在讨论什么东西。所以下面只讨论第三、四条规则，想想没了这些规则会得到什么。

1. 仿照以下例子，设计一个仅仅不满足第三条规则的情形。例子：考虑无限多的火柴，变换是“抽出一根火柴划着”。由于火柴划着后就无法复原了，所以效果不可逆，不满足第三条规则。但其他规则都符合。

2. 仿照以下例子，设计一个仅仅不满足第四条规则的情形。例子：考虑所有整数，变换是“加 1”和“减 1”。由于“加 1”重复两次就不再是“加 1”、“减 1”之一，所以不满足第四条规则。但其他规则都符合。

数与群

群和数有天然的联系。因此，讨论数中的群也是理所当然。

1. 考虑前面整数集 $\mathbb{Z}$ 例子里的“加几”群。如果把“加几”的“几”限定为偶数，还构成群吗?

2. 同样，如果限定为奇数，还构成群吗?

3. 同样，如果限定为 3 的倍数，还构成群吗? 如果限制成模 3 余 1 的数呢?

4. 如果把“加几”改为“乘几”，构成群吗?

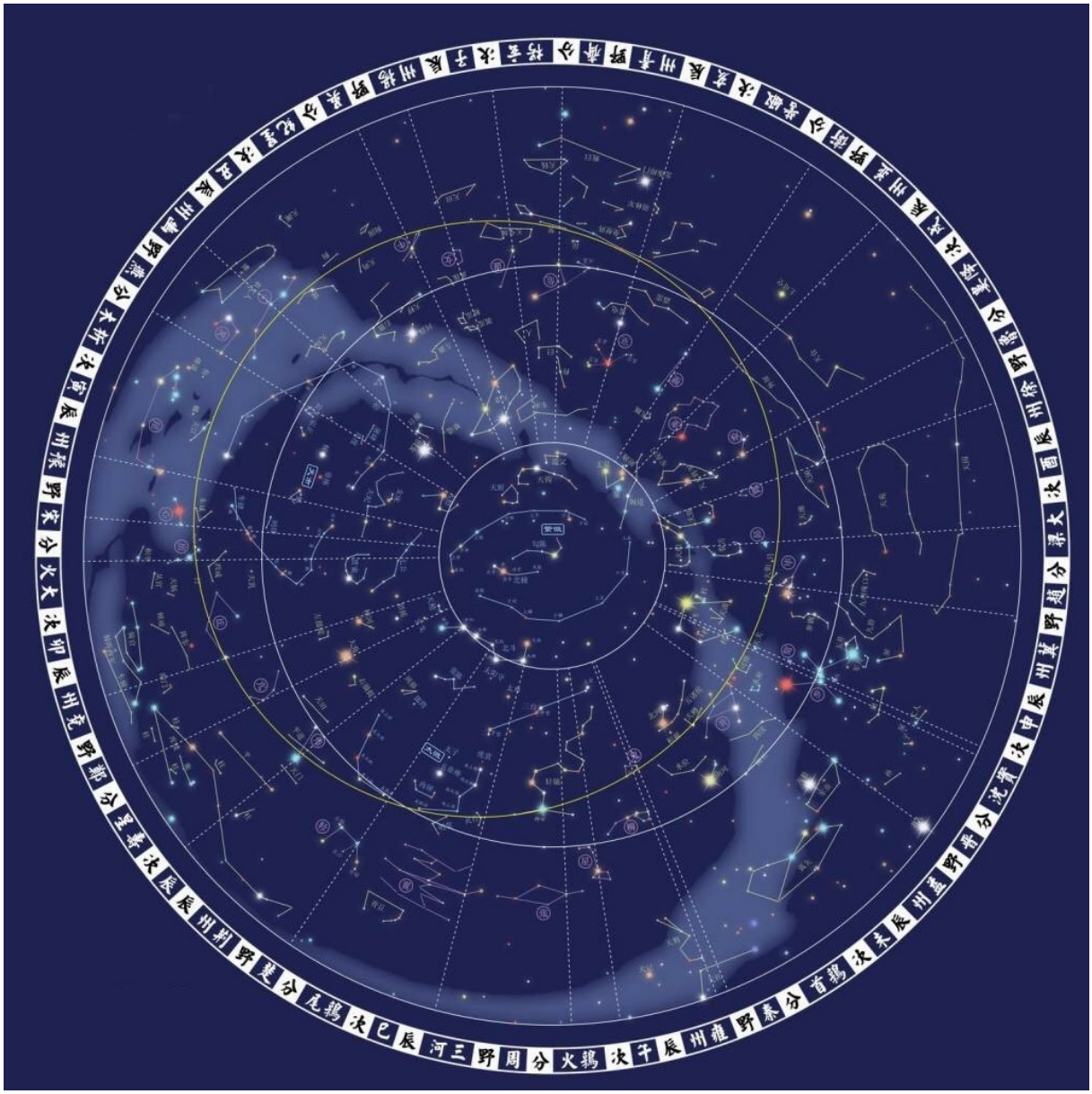
5. 如果把 $\mathbb{Z}$ 改为非零整数集，那么所有“乘几”构成群吗?

6. 如果把 $\mathbb{Z}$ 改为非零有理数集，那么所有“乘几”构成群吗 (这里的“几”可以是任何非零的有理数)?

7. 考虑正整数 n 的同余类: $\overline{0}, \overline{1}, \cdots, \overline{n-1}$。把“乘几”定义为同余类的乘法，那么所有“乘几”构成群吗? 如果只考虑非零同余类呢?

8. 考虑素数 p 的非零同余类: $\overline{1}, \cdots, \overline{p-1}$。设 $\overline{a}$ 是其中一个同余类。如果从 $\overline{a}$ 开始，不断重复乘 $\overline{a}$，能构成所有的非零同余类，就说 a 是模 p 的原根。哪些 a 是原根，哪些不是? 对 $p = 3, 5, 7, 11$ 分别查找原根。

第二章　群是什么样子的?



2.1 连线图

上一章我们引入了“群”的概念，还举出了不少例子。不过，单单用文字来描述群的性质，总仿佛隔着一层薄纱，朦朦胧胧看不清楚。一个群里有多少个变换？这些变换之间是什么关系呢？用文字来描述，反而更让人困惑了。这是因为对称和变换本身就是抽象的概念。我们需要找到把它们看清楚的方法。

正三角形和正方体的例子里，我们试图用图像来理解群，不过做得还不够。正三角形相关的群就有 6 个变换，而正方体相关的群有 24 个变换。我们小时候玩过的魔方，虽然也是正方体，通过把每个面扭转到不同的方向，竟然能够变出四千亿亿种不同的状态。这样繁多的变换，犹如漫天星辰，如何去理解？

古人观天时，想要找到一颗星星，怎么做呢？他们把位置相近的星星在头脑里连起来，想象成互相关联的一个整体。这样，只要找到了最亮的那颗星，就能跟着头脑里的连线，找到其他的星星了。这启发我们用连线的方式来表示变换。我们可以把不同的状态看作“星星”，把状态之间的变换用连线来表示。和天上的星星相比，我们的优势是能够任意排布这些“星星”的位置，方便我们连线。

首先来看正三角形的例子。上一章里我们列举了 6 个变换。这些变换之间有什么联系呢？我们从正三角形的某个状态出发，把它称为初始状态，记为 A_1，然后看它经历不同的变换变成什么样子。

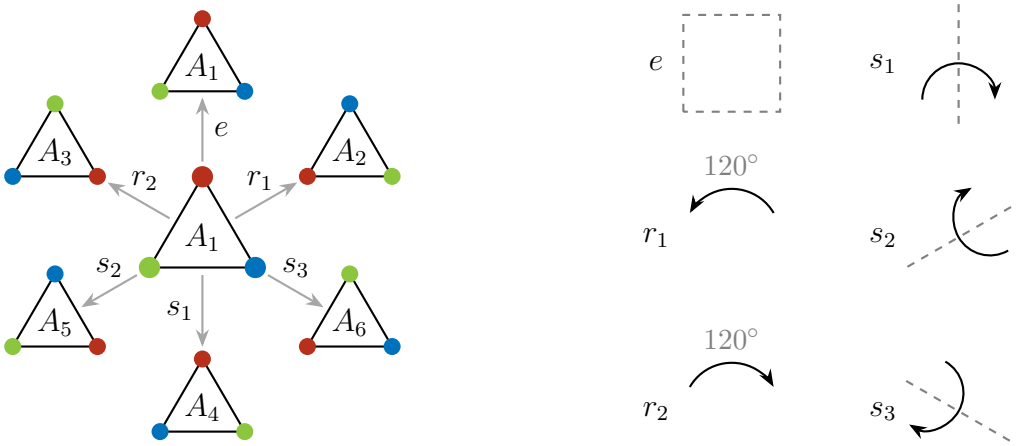


图 2.1: 从初始状态出发的 6 种变换

从上图可以看出，6 个变换把初始状态变成 6 个不同的状态（为了方便说话，我们

把这些变换也用字母标记)。其中“什么都不做”(变换 e)显然保持初始状态不变,而其他 5 个变换都改变正三角形的状态。

接下来我们继续从这 5 个新状态出发,查看不同的变换如何改变它们的状态。

“什么都不做”显然保持任何状态不变,所以我们不再关心它。“逆时针旋转 120°”(变换 r_1)和“顺时针旋转 120°”(变换 r_2)的变换指令也很清晰。对于三种沿中线翻转的变换,我们要解释一下:它们并不跟随顶点变化,而是与绝对位置挂钩,即“沿竖直中线翻转”(变换 s_1)、“沿左下顶点对应中线翻转”(变换 s_2)、“沿右下顶点对应中线翻转”(变换 s_3)。

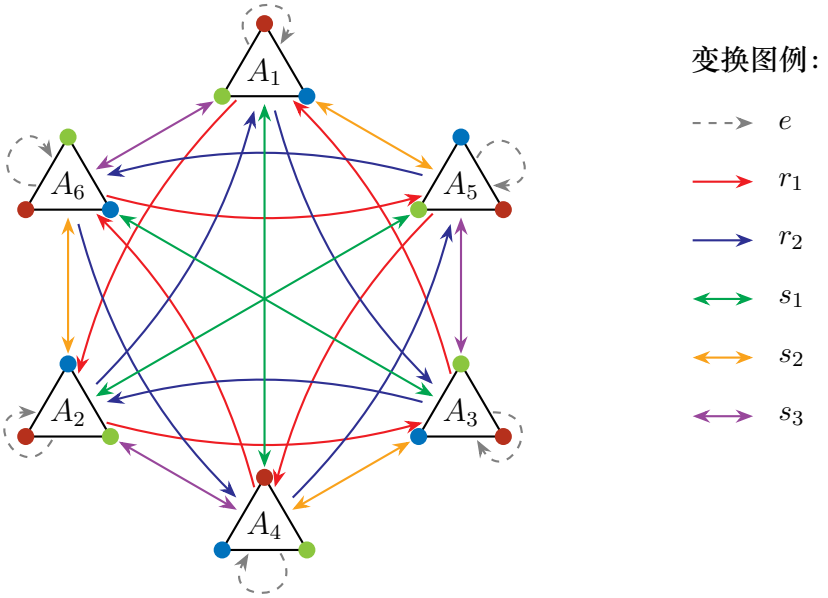


图 2.2: 6 个状态之间的完全连接

从各个变换的效果来看,对 6 个状态继续变换,结果还是在这 6 个状态之中。而且任意两个状态之间都连线了。这说明我们已经掌握了所有的状态,以及任两个状态之间如何变换。每个变换的知识,我们都能通过这个图知道。

不过,完整的图案过于复杂了。我们可以只看其中的一部分。我们再次从初始状态出发,不过这次我们只关心变换 r_1(逆时针旋转 120°)。它把初始状态 A_1 变为 A_2。继续用它改变 A_2,得到 A_3。而用它改变 A_3 则又得到 A_1。这构成一个循环。而变换 r_2(顺时针旋转 120°)则把 A_1 变为 A_3,然后再变为 A_2,最后回到 A_1。

我们也可以从状态 A_4 出发,查看旋转变换的效果。r_1 把初始状态 A_4 变为 A_6。继

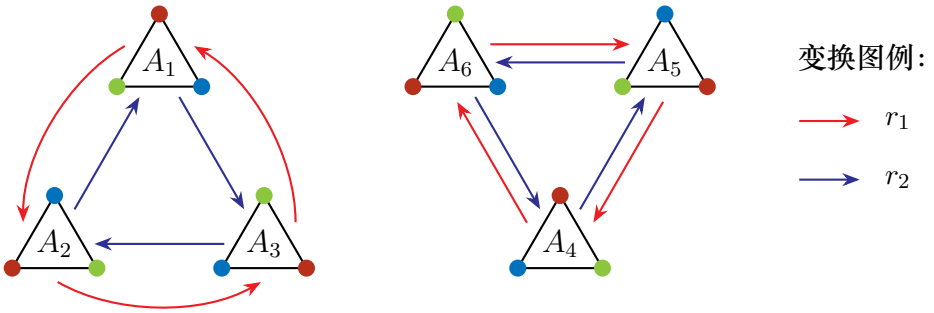


图 2.3: 3 个状态之间通过旋转连接构成循环

续用它改变 A_6，得到 A_5。而用它改变 A_5 则又得到 A_4，构成循环。而变换 r_2 则把 A_4 变为 A_5，然后再变为 A_6，最后回到 A_4。

再来看 s_1（沿竖直中线翻转）这个变换。它把初始状态变为 A_4。再次用它变换 A_4，则回到初始状态 A_1。同理，它把 A_2 和 A_5 互换，A_3 和 A_6 互换。沿其他中线翻转，也有类似效果。

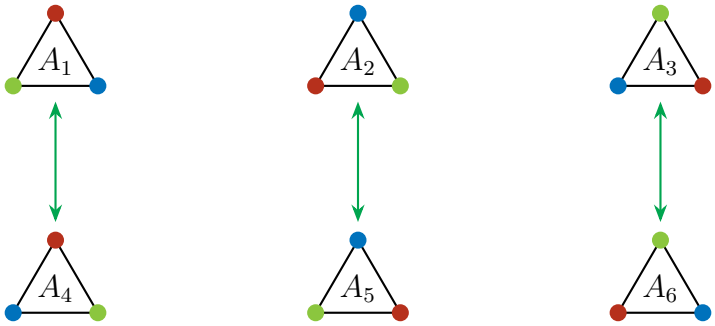


图 2.4: s_1（竖直翻转）的效果：上方顶点不变，左下与右下顶点互换

这些图比完整的图更简单，更方便我们查看。

2.2 生成与路径

上一节我们尝试了两种方法来看清楚一个群。一种是从每个状态出发，研究所有的变换的效果。另一种是只考虑一种变换，不断重复，观察效果。前者能得到所有状态和变换的信息，但太复杂了。后者简单明了，但并不能遍历所有的状态。现在我们再换一种方法来探索：只挑最少的变换，到达所有的状态。

正三角形的对称变换有 6 个状态。如果只看旋转（比如只用 r_1），能到达其中 3 个

状态；如果只看翻转（比如只用 s_1），能到达 2 个状态。但仔细观察可以发现，翻转能够到达旋转到不了的状态。于是我们用 s_1 和 r_1 组合，看能到达哪些状态。我们知道不断重复 r_1 变换，会把 A_1 变成 A_2，再变成 A_3，最后变回 A_1。而 s_1 则把 A_1 变成 A_4。这样，如果接着进行 r_1 变换，就会变成 A_6、A_5，再回到 A_4。最后再进行 s_1 变换，就回到 A_1。于是，我们用 r_1, s_1 两个变换，就到达了所有的状态。

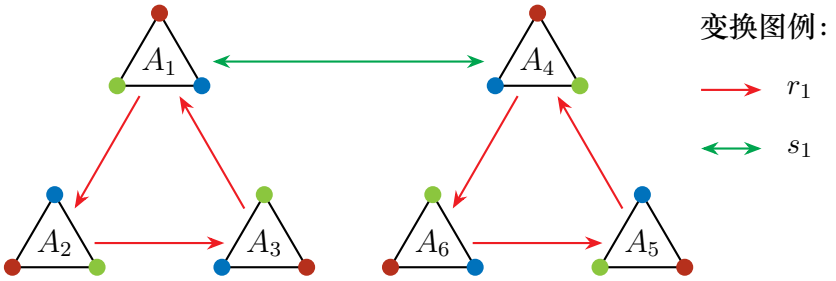


图 2.5: 用两个变换到达所有状态

如果我们把 r_1 制造的两个三状态的循环视为相互独立的“世界”，s_1 就是在两个“世界”之间往返的“通道”。A_1 和 A_4 就是“出入口”。这样的“出入口”还有 A_2 和 A_5，A_3 和 A_6。只要有了这些“出入口”，就能从一个“世界”到达另一个“世界”。因此我们可以把正三角形的对称变换用下图表示。

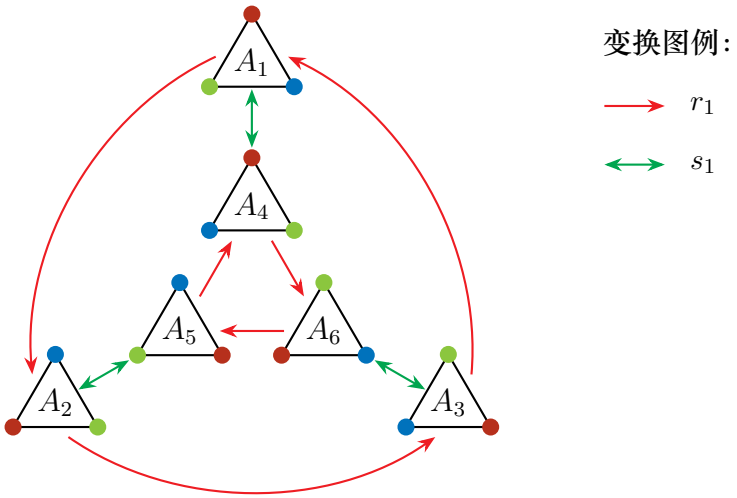


图 2.6: 用两个变换描述 6 个状态之间的关系

这种优美的性质只属于 r_1, s_1 吗？不然。我们可以验证，任何一个旋转变换加上任何一个翻转变换都能达到这个效果。通过观察，你应该可以解释为什么这是对的。实际上，具体用哪个变换并不重要，重要的是理解从一个变换出发，逐步添加变换，得到越来越多的状态的想法。我们说我们用 r_1, s_1 **生成**了整个群。

既然我们能用 r_1, s_1 两个变换到达所有状态，那么其他的变换就可以看作 r_1 和 s_1 的组合了。我们可以具体地写出来：

$$r_2 = r_1 \to r_1, \qquad e = r_1 \to r_1 \to r_1$$

$$s_2 = s_1 \to r_1 \to r_1, \qquad s_3 = s_1 \to r_1$$

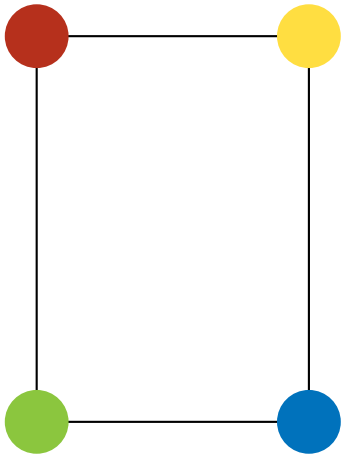
其中 $s_1 \to r_1$ 表示先进行 s_1 变换，再进行 r_1 变换。其余类同。把其他变换表示成 r_1, s_1 组合，称为它的**路径**。探明了路径，我们就知道如何从任一个状态到达另一个状态了。

要注意的是：到达另一个状态的路径并不唯一。比如从 A_1 到 A_5，我们可以用 $s_1 \to r_1 \to r_1$，也可以用 $r_1 \to s_1$。两个路径不同，但能到达同一个状态。

2.3 长方形的群

再来看另一个例子。这次我们考虑一个长方形。如何变换能让它的形状保持不变呢？这次我们将从单个变换开始，逐步增加变换，一步步地找出所有的状态。

首先，和三角形的例子一样，我们给长方形的四个顶点标记不同的颜色（如下图所示）。通过顶点颜色的变化，来表示长方形的对称变换。



首先引入第一个变换：把长方形水平翻转。它把长方形的左边和右边互换。我们称这个变换为 p。于是我们得到了两个状态：初始状态 B_1，以及 p 变换后的状态 B_2。

继续用 p 变换 B_2，我们发现长方形又回到了初始状态。也就是说，只用水平变换 p，我们只能得到长方形的两个状态。

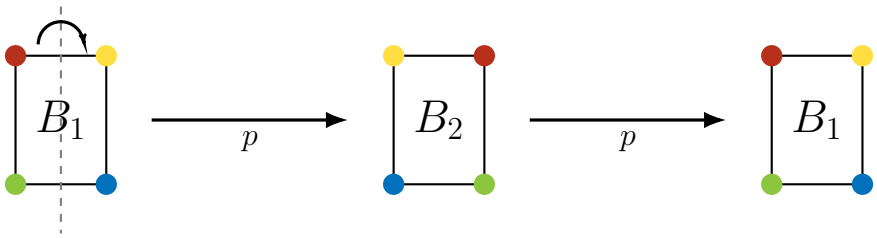


图 2.7: 水平翻转变换 p 的效果：左边和右边互换

于是我们引入第二个变换：把长方形竖直翻转。它把长方形的上边和下边互换。我们称这个变换为 q。它把长方形的初始状态 B_1 变为状态 B_3。继续用 q 变换 B_3，又回到初始状态。现在我们得到了 3 个状态，分别是初始状态 B_1，水平翻转后的状态 B_2，以及竖直翻转后的状态 B_3。

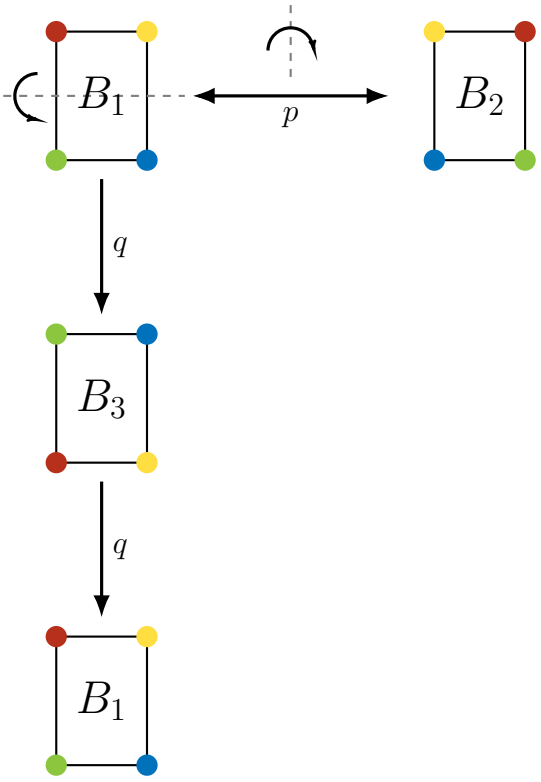


图 2.8: 竖直翻转变换 q 的效果：上边和下边互换

水平翻转变换 p 和竖直翻转变换 q 分别把初始状态带到了 B_2 和 B_3。但继续水平翻转 B_2、竖直翻转 B_3，只会回到初始状态。不过，我们还有别的方法来变换它们，就是竖直翻转 B_2、水平翻转 B_3。我们来看看会发生什么。

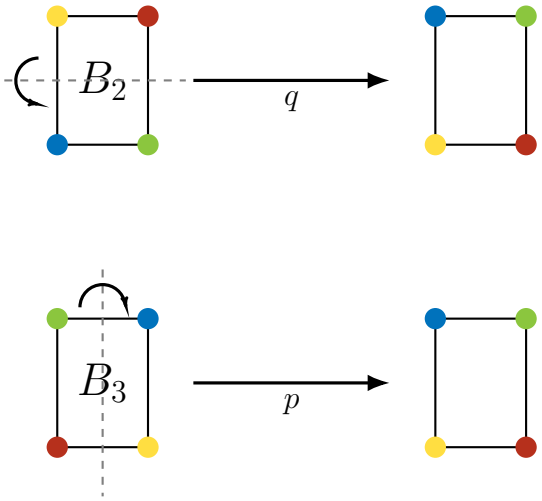


图 2.9: 水平翻转 B_2 与竖直翻转 B_3 的效果相同

我们看到，水平翻转 B_2 与竖直翻转 B_3 的效果是相同的。我们得到了一个新状态 B_4。而继续对 B_4 进行水平翻转和竖直翻转，得到的都还是 B_2 和 B_3。这说明这四个状态就是我们用 p 和 q 两个变换能得到的所有状态。我们可以把它们画在一个图上。

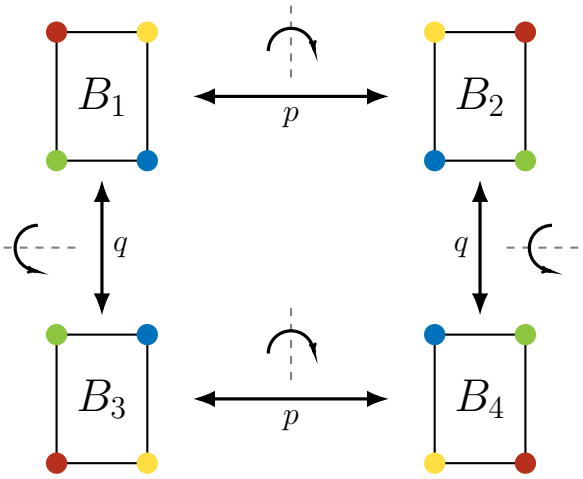


图 2.10: 用 p 和 q 两个变换得到的 4 个状态的关系

这 4 个状态是否就是使得长方形形状保持不变的所有状态呢? 的确如此。我们可以用顶点的颜色来证明:

首先考虑红色顶点，它只能出现在长方形 4 个顶点中的一个顶点上，于是有 4 种可能。一旦红色顶点位置确定，那么黄色顶点必然在它相邻的短边的另一端，绿色顶点必然在它相邻的长边的另一端，而剩下只有一个顶点，就是蓝色顶点的位置。因此，所有

状态只有 4 个，通过变换 p, q，我们已经把它们全部找到了。

以上就是通过不断添加变换生成群的方法。我们把用这种方法生成的图称为群的**生成路径图**。它清楚地显示了群里的变换和各个状态之间的关系。如果你觉得三角形和长方形的对称变换构成的群都太简单了，可以试着用这种方法来研究正方体的旋转构成的群。它比三角形和长方形的例子要复杂不少。如果遇到困难，可以参考附录中的解答。

群的生成路径图显然不是唯一的。它只是一种遍历状态的方法。群的生成路径图仿佛是一张地图。它告诉我们从一个状态出发，经过哪些变换，就能到达另一个状态，指出状态之间的路径。

你也许会说：如何保证我们穷尽了所有的状态呢？实际上，生成路径图并不保证我们穷尽了所有状态。相反，一旦我们发现了一个不在图中的新状态，它必然是我们已知的变换无法达到的（因为之前我们已经穷尽了已知变换所能达到的所有状态）。于是，通过理解它如何从已知状态得来，我们就能扩大我们的地图，生成更多的路径。这就是生成路径图的理念。我们也可以说，生成路径图表示我们已知的变换能生成的群的面貌。

2.4 共同的结构

群之所以重要，在于它提炼了不同现象之间的共同性质。比起具体例子中的状态，我们更关心状态之间的变换。变换体现了对称的规律。

比如，我们可以考虑队列操演时原地“向右转”、“向后转”、“向左转”、“立正”这 4 个动作。这些动作效果确定，可以恢复（比如向左转再向右转就回到原来的状态），组合后没有新动作（比如向右转再向后转就是向左转，等等），所以构成一个群。

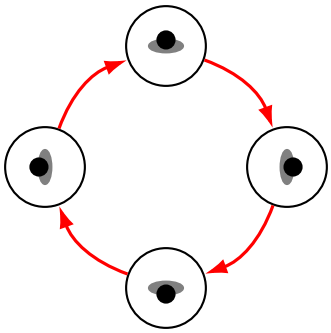


图 2.11: 向右转 4 次回到原本状态

以身体向前作为初始状态，这些动作把身体状态顺次变成向前、向右、向后、向左。因此，一共有 4 个状态，和长方形的对称变换构成的群一样。

但是，我们发现，这两个群的结构不相同。长方形的变换群里，所有变换重复 2 次之后都回到原状态。即便是 B_1 到 B_4 的变换，再重复一次也回到 B_1。但是我们知道，向右转 4 次后，才会回到原来的站位。所以，长方形的对称变换里，没有和“向右转”一样的变换。

另一方面，我们可以考虑这样的例子：墙上有甲乙两个开关，分别控制一盏电灯。每个开关都有两个状态：开和关。因此两个开关一共有四种状态。它们可以通过拨动甲开关和拨动乙开关来达到。我们可以据此画出对应的群的生成路径图。

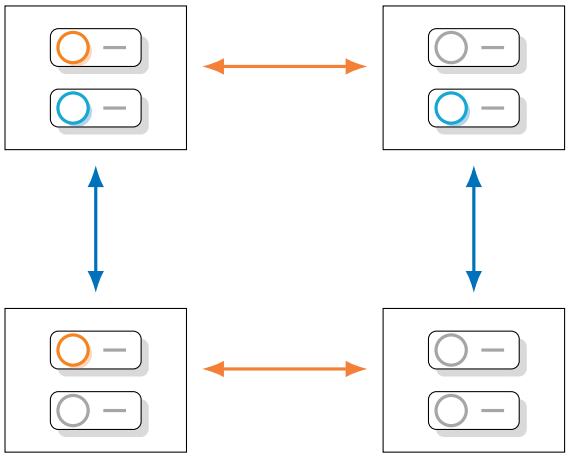


图 2.12: 两个开关的状态图

可以看到，长方形的四种状态对应两个开关的四种状态，而“水平翻转”、“垂直翻转”则对应着“按上面的开关”和“按下面的开关”。如果我们不关注状态的具体内容，只关心箭头的位置和方向，那么我们会发现，这里这些箭头连接状态的方式，和前面长方形的例子是一样的。两个图的结构一致。

所以，这两个群尽管表面上不同，说的是不同的事情，但论及变换的结构，并没有不同。它们反映了两个不同事物的共同本质。我们还可以把两个开关换成两枚硬币，结果也是一样的。

变换的路径图为我们揭示了一种抽象的规律。数学上，我们说这是一种结构上的等同关系。长方形的对称变换构成的群，和两个开关的变换构成的群**同构**。我们认为，这两个群是一样的结构。讨论这个群就等于讨论那个群，讨论那个群就等于讨论这个群，没有任何区别。这个抽象的群，我们称它为**矩群**，记作 J_4。

我们只想讨论群。所以，我们可以忽略各个例子里与群无关的东西。比如说，每个状态具体是什么，究竟是两个开关、两枚硬币还是一个长方形，其实不重要。我们就说它是一个节点，用一个圆点代替。而变换就是从一个节点指向另一个节点的箭头。变换的具体意义也不重要，重要的是变换之间的关系。即两个变换组合起来是哪个变换。于是我们可以为矩群画出以下的图：

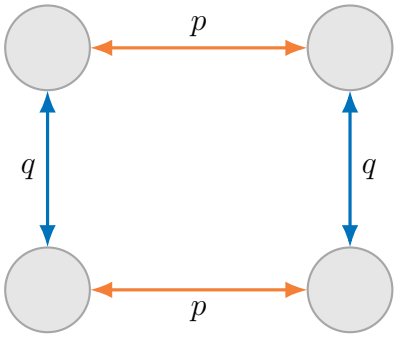


图 2.13: 矩群的生成路径图

矩群由两个变换 p, q 生成。我们不关心这里的 p, q 是什么变换。我们只需要知道，p 和 q 各自重复两次就相当于什么都不走，得到恒等变换 e。它们组合起来则是另一个变换 r，而且不依赖于组合的顺序：

$$r = p \to q = q \to p.$$

而 r 重复两次，也相当于什么都不做。这些关系就是我们从不同的例子里抽离出来的共性。研究这个抽象的群，得到的知识，就能应用到这些不同的例子里。比如，我们会发现：

$$p \to q \to p = q, \qquad q \to p \to q = p.$$

因为从左上角的节点开始，往右、往下、再往左，就得到左下角的节点，效果和直接往下一样。同理，从左上角的节点开始，往下、往右、再往上，就得到右上角的节点，效果和直接往右一样。这个性质反映到开关的例子里，就是按一个开关两次的间隔里按另一个开关，和只按另一个开关效果相同。反映到长方形的例子里，就是水平翻转两次的间隔里垂直翻转一次，效果和只垂直翻转一次一样。一旦掌握了抽象的本质，我们就能用它理解各个具体例子的相关性质。

正三角形的例子也能变成抽象的群。我们忽略正三角形的各种状态，只考虑变换之间的关系，可以画出以下的图：

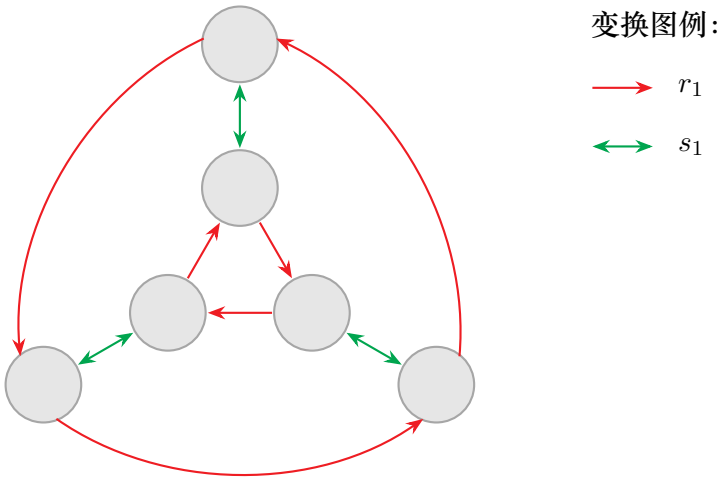


图 2.14: 用两个变换描述 6 个状态之间的关系

这是一个 6 个节点，由两个变换生成的群。我们不需要知道节点的具体含义，也不需要知道 r_1 和 s_1 的具体意义。从图中我们可以看到，r_1 重复三次总回到原节点，而 s_1 重复两次就回到原节点，等等。我们把这个群叫做**三元对称群**，记作 D_3。

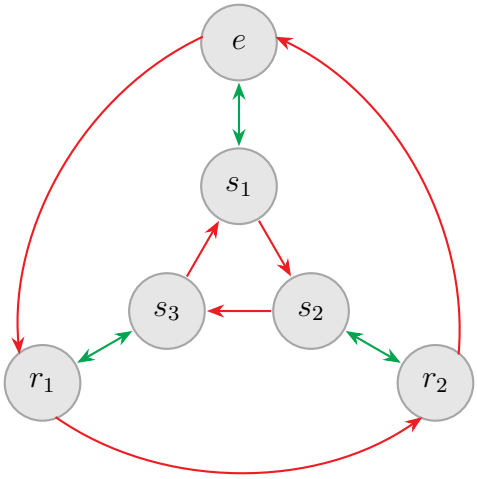


图 2.15: D_3: 用变换标记 6 个状态

既然在生成路径图里，我们关心的是图中各个状态的关系，如何用群中的变换把状态改变。这些状态可以只看作节点，它本身是什么，我们反倒不那么关心。那么，我们可以用变换的名字来标记生成路径图里的状态节点，更方便我们理解群的结构。

具体来说，我们选定一个状态，从它出发，沿着变换构成的路径，把能到达的状态

都标为这些变换复合的结果。我们把原状态视为“什么都不做”的结果，标记为 e。然后把从 e 出发，一次变换能到达的状态，用这些变换的名字来标记。接下来再从这些状态出发，把再经历一次变换能到达的状态，用两次变换的乘积标记，等等。一个状态并不一定只有一种方法到达，我们希望给它一个简便的记法，比如可以给它起一个新名字。新的名字就意味着这个变换和之前的变换都不同。

这样，我们就标记出了群中所有的变换。这种关系是一一对应的。首先每个变换必然都通过至少一个路径到达，因此必然对应某个状态节点。其次，同一个节点对应同样的变换，于是至多有一个名字。于是，群的生成路径图里，把各个状态节点用群的元素（变换）来标记，就能标出群的所有元素（变换）。换句话说，状态节点个数有限时，就是群中变换的个数：图中有多少个状态节点，就说明群里有多少个变换。

要注意的是：这种标记方法不依赖最初选择的状态节点。从任意一个节点出发，都能完成标记。这也是群的生成路径图的特有性质。群的变换之间的对称关系，决定了我们可以这么做。反之，随便用一些节点连成的图，是不具备这种性质的。

本章小结

本章我们引入了“连线图”的方法来显示群的结构。本章的主要内容包括:

- **生成元与生成路径图**: 我们不需要罗列所有变换，而是寻找少数几个“生成元”，通过它们不断组合的路径，遍历群的所有状态。
- **矩群** J_4: 它有 4 个元素，可以通过其中两个翻转变换组合得出。
- **三元对称群** D_3: 它有 6 个元素，可以通过其中一个旋转变换和一个翻转变换组合得出。
- **同构**: 我们发现，长方形翻转、开关拨动、队列转向等截然不同的物理现象，其背后的状态图结构却完全一致。这种剥离了具体场景后，在抽象结构上完全等同的关系，称为“同构”。
- 生成路径图的状态节点和群的变换一一对应。

2.5 习题

1. 为以下的群列出变换能实现的所有状态，然后给出生成这些状态的方法。

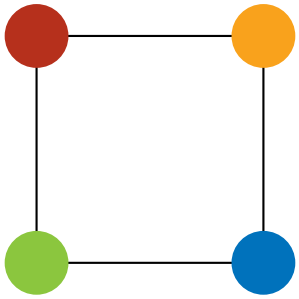
   (1) 单个硬币的翻转变换构成的群。

   (2) k 个硬币的翻转变换构成的群。

   (3) 整数集的加法群（由所有“加几”操作构成的群）。

2. 如何为以上的群画出生成路径图?

3. 考虑平面中一个正方形。允许将它旋转、翻转。我们希望研究有哪些变换让它的位置和形状不变。



   (1) 将正方形的四个顶点染成两两不同的颜色，比如：红、绿、黄、蓝。四个顶点所有可能的颜色组合有几种?

   (2) 考虑将正方形按其中心旋转。哪些旋转变换保持其位置形状不变？这时候的顶点颜色如何变化？列出所有可能达到的状态。

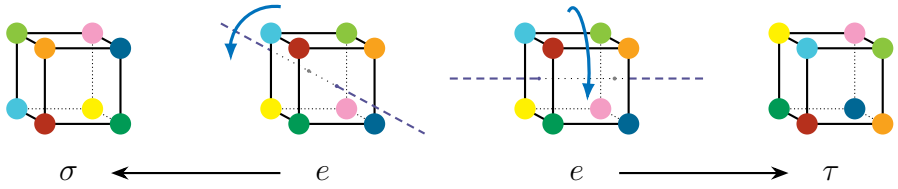
   (3) 考虑将正方形按过中心的轴线翻转。哪些翻转方法保持其位置形状不变？这时候的顶点颜色如何变化？列出所有可能达到的状态。

   (4) 画出以上状态的生成路径图。

   (5) 哪些颜色组合无法通过旋转、翻转形成？为什么？给出你的解释。

4. 本题的目的是初步研究正方体的旋转对称群（记为 T_6）。思考本题时最好准备一个骰子或类似的正方体物件，最好各个面有区别，或者顶点做好了标记，通过实际上手转动正方体，理解它在空间中的旋转。我们考虑 T_6 中两个变换：“朝前转动 90°，左右

面不变”（记为 τ）和“往左转动 90°，前后面不变”（记为 σ）。



(1) 这两个变换，能否生成“往右转动 90°，左右面不变”？如何做到?

(2) 这两个变换，能否生成“往左转动 90°，上下面不变”？如何做到?

(3) 考虑正方体对角顶点的连线，称为顶心对角线。正方体有几条顶心对角线?

(4) 我们按照顶心对角线与正方体朝上一面的交点（也是该面的四个顶点）来给相关顶心对角线命名，分别称为左前、左后、右前、右后顶心线。描述以左前顶心线为轴的旋转变换如何确保正方体位置形状不变。这样的变换有几个?

(5) 用 τ 和 σ 能否生成上面提到的变换？如何做到?

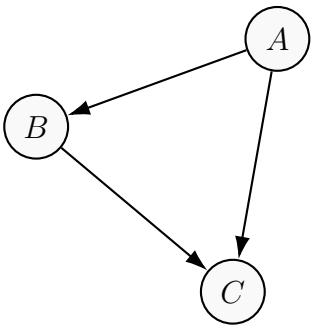
(6) 考虑正方体一条棱和与它相对的棱。两条棱的连线过正方体中心。这样的连线称为对棱中线。正方体有几条对棱中线?

(7) 我们按照对棱中线与正方体朝上一面的交点（也是该面四条边的中点）来给相关对棱中线命名，分别称为前、后、左、右对棱线。描述以左对棱线为轴的旋转变换如何确保正方体位置形状不变。这样的变换有几个?

(8) 用 τ 和 σ 能否生成上面提到的变换？如何做到?

5. 构想一个群的例子，使其连线图（生成路径图）与矩群一样。

6. 下图为何不是群的生成路径图？它违反了哪条规则？给出解释。



第三章　群是代数结构

3.1　群的乘法表

上一章里，我们通过各种例子研究了不同的群。群是一种抽象的结构。群由变换构成，而变换之间的关系，决定了群的结构。我们说，这种关系是一种代数的关系。

这是什么意思呢？我们来看上一章中讨论的群的性质。对于矩群 J_4，我们有以下关系成立：

$$e = p \to p = q \to q = p \to q \to p \to q.$$

对于三元对称群 D_3，我们有以下关系成立：

$$r_2 = r_1 \to r_1, \qquad e = r_1 \to r_1 \to r_1$$

$$s_2 = s_1 \to r_1 \to r_1, \qquad s_3 = s_1 \to r_1$$

等等。这些关系就和代数算式一样。我们可以把操作 $\to$ 看作一种运算法则，而运算的结果就是另一个变换。我们把这种关系称为代数关系，说群是一种抽象的代数结构。

到目前为止，我们已经了解了不少和群有关的知识。不过，目前数学界对群的正式定义，和我们对群所下的非正式定义，还有些不同。为了更好地学习群的知识，我们会逐步转到数学家广泛采用的定义，用标准的语言来讨论群。下面我们要了解的就是一种更标准地描述群的方法：群的乘法表。就如数字有乘法表一样，群作为代数结构，也可以构造自己的乘法表。它将是带领我们进入群的正式讨论的重要工具。

从我们熟悉的 D_3 开始。我们知道它包含 6 个变换。这些变换以任意方式组合，得到的还是 6 个变换中的某个变换。而变换的种种组合方式，拆解到底，最基本的就是：两个变换作为映射组合起来，成为一个新变换。我们称为两个变换的**复合**。复合的规则就是群 D_3 的本质。所以，我们直接把这些变换称为**群的元素**。把变换的复合操作称为

群的乘法。它和乘法确实有类似之处：把两个元素变成另一个元素。我们可以调查所有变换复合的效果到底是哪个变换，然后将结果总结成一张表格：

表 3.1: 三元对称群（D_3）的乘法表

$\cdot$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_1	r_2
s_2	s_2	s_3	s_1	r_2	e	r_1
s_3	s_3	s_1	s_2	r_1	r_2	e

这个乘法表里列出了群 D_3 里任意两个变换复合成另一个变换的规则。其中左起第一列和上数第一行是行头和列头，标记了作为“乘数”的元素，里面罗列了群的所有元素。而表格中则记录了元素相乘的结果。要找到两个变换复合的结果，只需要在列头中找到前一个变换，然后在行头中找到后一个变换，则它们分别所在的行和列相交处的内容，就是它们复合的结果。

比如，如果我们想查询先 r_1 后 s_3 复合的结果：$r_1 \to s_3$，就到上边列头找到 r_1：它在第 2 列；然后在左边行头里里找到 s_3：它在最后一行。于是，r_1 和 s_3 复合的效果，就是最后一行第 2 列的内容：s_1：

$$s_1 = r_1 \to s_3.$$

反之，要填写这个表，也只需要按这个规则，把任两个变换复合的结果填进去即可。

比起让人眼花缭乱的变换关系图，群的乘法表更一目了然，而且便于查询。

为了方便，我们直接像乘法一样记录这些“运算”。实际上，我们已经有和乘法很像的记录方法。我们讨论的变换本质上都是映射。因此，作为映射，变换 a, b 的复合可以写作 $b \circ a$。这个写法里，左右顺序似乎颠倒了。这是为了照顾映射的写法。变换 a 作为映射作用于一个自变量 x，记作 $a(x)$，而 b 继续作用于 $a(x)$，记作 $b(a(x))$。因此，我

们习惯把“先 a 后 b”的复合映射记为 $b\circ a$，约定：

$$(b\circ a)(x)=b(a(x)).$$

而本书开篇以来一直只把变换视为对象，所以“先 a 后 b”记录为 $a\to b$。看起来左右顺序和 $b\circ a$ 颠倒了。不过，我们早已预见到了这个顺序的问题，所以用箭头来指示顺序。我们完全可以把“先 a 后 b”记录为 $b\leftarrow a$。只要跟着箭头的方向，先后顺序就不会错。所以这个记法问题并不会妨碍我们讨论问题。我们完全可以这样写：

$$r_2=r_1\to r_1=r_1\leftarrow r_1,\qquad e=r_1\to r_1\to r_1=r_1\leftarrow r_1\leftarrow r_1,$$
$$s_2=s_1\to r_1\to r_1=r_1\leftarrow r_1\leftarrow s_1,\qquad s_3=s_1\to r_1=r_1\leftarrow s_1.$$

这个写法看起来没那么“自然”，但这仅仅是因为我们看文章时习惯了从左到右阅读而已。跟着箭头的方向来看，先后顺序并没有改变。而我们约定**用乘号代替左向箭头**，即 $ab=a\cdot b=a\leftarrow b=b\to a$，于是上面的等式可以改写为：

$$r_2=r_1\leftarrow r_1=r_1\cdot r_1=r_1^2,\qquad e=r_1\leftarrow r_1\leftarrow r_1=r_1\cdot r_1\cdot r_1=r_1^3,$$
$$s_2=r_1\leftarrow r_1\leftarrow s_1=r_1\cdot r_1\cdot s_1=r_1^2s_1,\qquad s_3=r_1\leftarrow s_1=r_1\cdot s_1=r_1s_1.$$

这里变换作为群元素的乘法顺序和左向箭头对应，也和映射的复合记法一致。ab 就是 $a\leftarrow b$ 的意思，也就是“先 b 后 a”。本书采用这种约定方法，是“变换优先”思想的产物。按照这个约定，当我们看到群的元素乘积 ab，要记得在乘法表的左侧行头里找 a（后变换，写在左），而在上方列头找 b（先变换，写在右），这样找到的行列交点才是 $ab=a\leftarrow b=b\to a$。

我们也可以把矩群的规则做成乘法表：

其中的 p,q 就是我们在长方形的例子里提到的水平翻转和竖直翻转，r 则是两者结合的效果。

3.2 复合是乘法吗?

上一节中，我们把变换的复合写成了乘法式子。我们自然会问：真的能这么写吗？换句话说，变换的复合，是否就一定满足乘法的性质呢？

表 3.2: 矩群（J_4）的乘法表

$\cdot$	e	p	q	r
e	e	p	q	r
p	p	e	r	q
q	q	r	e	p
r	r	q	p	e

这个疑问是有道理的：作为变换的复合，我们说的“群的乘法”并不满足数字的乘法的所有性质。首先这里并没有“群的加法”来帮我们定义“乘法”，它只是一类独立的运算。其次，群的乘法满足乘法结合律，因为变换复合时，考虑复合的先后顺序，不影响其最终效果。具体来说，如果有三个变换 a, b, c，那么思考它们的复合：

$$a \to b \to c$$

时，可以先考虑操作 $a \to b$ 的效果，然后考虑它与 c 复合的效果。也可以先考虑操作 $b \to c$ 的效果，再考虑 a 之后进行这个操作的效果。这只是思考角度不同，最终的结果并不会改变。但群的乘法一般不满足乘法交换律，也就是说，改变变换的顺序，确实会改变效果，即：

$$a \to b, \qquad b \to a$$

这两个复合变换的结果往往是不同的。比如在 D_3 中，$r_1 s_1 = s_3$，而 $s_1 r_1 = s_2$。

但群里的元素也有可以交换顺序的。最典型的是：任何变换都可以与自己交换顺序。这个道理写成代数的形式是显然的：

$$a \to a \;=\; a \to a.$$

此外，“什么也不做”的恒等变换 e，可以与任何变换交换顺序：

$$e \to a \;=\; a \to e \;=\; a.$$

这个道理似乎也很明白：既然什么都不做，那么在前还是在后，也不会有分别。

此外还有一些可以交换顺序的情况，是群元素自身的特性决定的。比如，矩群中的元素 p, q，可以交换顺序。我们验证过这一点。也正因为 p, q 可交换顺序，矩群才成为

矩群。这种可以交换顺序的性质并不是对所有元素都成立的。如果一个群里的所有变换复合时都可以交换顺序，就说群的乘法满足交换律。这样的群叫做**交换群**。矩群就是交换群，三元对称群则不是交换群。

群的乘法虽然不是“真的乘法”，但在各种数学书籍里，我们都习惯这么叫。有时候我们也把交换群的运算叫做“群的加法”。总之，这个称呼也是一种滥用了的习惯。你可以把它看作一种修辞手法，以后我们还会经常这么称呼。

3.3 群的经典定义

现代群论教科书里介绍群的方式，往往不像我们这样，先慢悠悠地聊各种例子，而是一上来就给出群的经典定义。要知道，我们虽然一开始就给出了一个群的“土法定义”，但在正经数学家的眼里，那个定义有些儿戏了。大多数教科书给群下的定义是这样的：

定义 3.1 群

给定集合 S，如果它满足以下条件，就说它是**群**。

1. 有二元运算 $*$，使得 $\forall\, a,b \in S$，$a*b \in S$。
2. 结合律：$\forall\, a,b,c \in S$，总有 $(a*b)*c = a*(b*c)$。
3. 有幺元：即有 S 中元素 e，使得 $\forall\, a \in S$，$a*e = e*a = a$。e 称为群的**幺元**。
4. 有逆元：$\forall\, a \in S$，有 $b \in S$，使得 $a*b = b*a = e$。b 称为 a 的**逆元**。当我们使用乘法表示群运算时，a 的逆元一般记作 a^{-1}。

相比我们在第一章里给出的“土法”定义，这个定义显然更严谨、更精确，表述更清晰。不过，看这个定义，对具体的群长什么样子，很难有直观的认知。毕竟，这只是一些抽象的代数运算规则。不过，既然我们在前两章已经用着不那么严谨的定义讨论了一大堆群的东西，现在，我们正好可以利用我们对群的具体认识，反过来一条条地来看这些形式化的定义。

首先，这个定义里提到了一个新词：二元运算。这个词听起来很厉害，其实也就是说，运算 $*$ 接受两个东西，输出一个东西，就和加减乘除一样。具体来说，我们知道这个运算 $*$ 就是我们之前说的变换的复合操作。正式的定义里，直接把变换看作集合的元素了，把变换的复合看作一种运算，把两个变换拿来运算，得出一个变换作为结果。这

是一种抽象的视角，彻底剥离了群元素的属性，再通过后面的定义一条条加回来。

定义里的第一个条件是说，二元运算接受两个元素后，输出的必须也是群里的元素。也就是说，变换无论怎么复合，结果必须还在集合里。这也是我们“土法”定义里的规则 4。

接下来是结合律，也是我们讨论过的性质。从变换的角度来看，结合律是显然的性质。如果从纯粹抽象的集合元素出发，就需要人为规定运算满足结合律了。

然后是“幺元”的概念。幺元，也称为**单位元**、**空元**，就是和任何元素运算之后都不改变对方的元素。换句话说，就是我们的视角中的“什么都不做”的变换。在我们的“土法”定义里，也没有包括幺元，因为“什么都不做”的变换似乎是显然存在的。正式定义从集合与元素的角度出发，就需要说明幺元存在了。要注意的是，定义中并没有规定幺元只有一个。但从直觉上来说，幺元（也就是“什么都不做”）理当是惟一的。在正式定义中，可以由定义直接推出：

定理 3.1 幺元惟一

群恰有一个幺元。

证明：设 e_1, e_2 是群 $(G, *)$ 的幺元，那么按定义，$e_1 = e_1 * e_2 = e_2$。 □

最后是“逆元”的概念。这就是我们的“土法”定义里的规则 3。从变换的视角看来，变换可逆是自然的要求。如果一个变换不可逆转，那么让它代表对称性质就有些勉强了。换句话说，可逆也是一种对称性质。

要注意的是，由于群的乘法不像数的乘法一样可交换，群元素乘积的逆元需要仔细对待，要从映射复合的角度来理解。比如：如何逆转 $ab = a \leftarrow b$ 的效果？由于 b 变换先进行，a 变换后进行，要逆转效果，需要首先逆转后进行的 a 变换，然后再逆转 b 变换。因此，ab 的逆元是 $a^{-1} \to b^{-1}$，也就是 $b^{-1}a^{-1}$。多个元素乘积的逆元也是如此，顺序要倒过来。

另一种定义可逆的方法则不直接说明有一个“逆元”，而是用类似解方程的说法：

定义 3.2 互反律

说集合 S 中的二元运算 $*$ 满足互反律，就是指 $\forall a, b \in S$，都能找到 $x, y \in S$ 使得

$$a * x = y * a = b.$$

这种定义下，我们把逆元定义为方程 $a*x=y*a=e$ 的解。两个方程如果都有解，那么解就是逆元。反之，按逆元的定义，互反律必然成立，令 $x=a^{-1}b$、$y=ba^{-1}$ 即可。这说明两种定义是等价的。

也许你会问：这两个方程的解，就一定是同一个吗？这是个好问题。一般情况下，两个解并不相同。但是，如果运算 $*$ 满足结合律，并且有幺元，我们就能确保这一点。我们可以直接通过下面这个等式来说明：

$$y=y*e=y*(a*x)=(y*a)*x=e*x=x.$$

这个结论还顺带证明了**逆元是惟一的**：如果 x,y 都是 a 的逆元，那么它们是方程 $a*x=y*a=e$ 的解，因此相等。

由逆元存在性可以得到一个实用的性质：

定理 3.2 群的消去律

设 a,b,c 是某个群的元素。如果 $a*c=b*c$，那么 $a=b$。同样地，如果 $c*a=c*b$，那么 $a=b$。

证明：使用结合律和逆元定义即可。以下只给出前半的证明。请你模仿给出后半的证明。

$$a=a*e=a*(c*c^{-1})=(a*c)*c^{-1}=(b*c)*c^{-1}=b*(c*c^{-1})=b*e=b.$$

□

现在我们对群有两种角度来看待。一个是从开篇引入的变换的动态视角：群是由一些变换构成的，这些变换改变对象的状态，并且满足某些规则。它们的性质揭示了对象的对称性。另一个是我们刚刚审视完的集合的静态视角：群是某些元素的集合，配备了一种二元运算。这个运算满足几种基本性质，一般称为群的乘法。这两种视角是等价的，各有各的好处。有些群论里的定理、结论，用一种视角来看，会比另一种更好理解。保持多种视角来看问题，对于学习总是有益的。

按照群的经典定义，我们不需要考虑群的元素是否是某种变换了。只要有某个二元运算，让集合里的元素满足群的定义，集合就成了群。我们不妨来看几个例子。

例题 3.1

证明所有整数关于整数的加法构成群。

解答：把整数集记为 $\mathbb{Z}$。整数的加法是二元运算。整数加整数，总是得到整数。其次整数的加法满足结合律（而且满足交换律）。任何整数加 0 得到自己，所以 0 是幺元。任何整数加上它的相反数得到 0，所以它的相反数就是它的逆元。至此我们验证了整数的加法满足群的所有要求，因此 $\mathbb{Z}$ 关于加法构成群，而且是交换群。

例题 3.2

考虑模 n 同余类的集合：$\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$，证明它关于同余类的加法构成群。

解答：首先来回忆同余类的加法。同余类的加法是这样的：两个同余类 $\overline{a},\overline{b}$ 的和，是 $a+b$ 所在的同余类。这样的加法显然是二元运算，而且加法的结果按定义还是同余类。

接下来验证同余类的加法满足结合律。即证明对任何同余类 $\overline{a},\overline{b},\overline{c}$ 都有：

$$\left(\overline{a}+\overline{b}\right)+\overline{c}=\overline{a}+\left(\overline{b}+\overline{c}\right).$$

按照同余类加法的规则，$\overline{a}+\overline{b}$ 是 $a+b$ 所在的同余类，因此它加上 $\overline{c}$ 的和，就是 $(a+b)+c$ 所在的同余类。同理，$\overline{a}$ 与 $\overline{b}+\overline{c}$ 的和，就是 $a+(b+c)$ 所在的同余类。而整数的加法满足结合律：$(a+b)+c=a+(b+c)$。所以这两个数所在的同余类是一个同余类。这就证明了同余类的加法满足结合律。同理，由于整数的加法满足交换律，我们还可以证明同余类的加法满足交换律。

然后说明幺元和逆元的存在性。同余类 $\overline{0}$ 里的元素都是 n 的倍数，因此加上任何同余类里的元素 a，不改变 a 模 n 的余数。这说明对任何同余类 $\overline{a}$，总有

$$\overline{0}+\overline{a}=\overline{a}+\overline{0}=\overline{a}.$$

因此 $\overline{0}$ 是幺元。而对同余类 $\overline{a}$，它与 $\overline{n-a}$ 的和就是

$$\overline{a}+\overline{n-a}=\overline{n-a}+\overline{a}=\overline{n}=\overline{0}.$$

所以 $\overline{n-a}$ 就是 $\overline{a}$ 的逆元。

于是按照群的定义，$\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$ 关于同余类的加法构成群，记为 $\mathbb{Z}_n$。$\mathbb{Z}_n$ 是交换群。

本章小结

本章我们的视角从动态转到静态，把群看作配备了运算法则的集合。

- **乘法表**：我们学会了用乘法表来展示群内所有元素两两运算的结果，它是研究群结构的重要工具。为了方便，我们把群的运算称为乘法（或加法），约定两个变换 a, b 的复合 $a \to b$ 是乘法 ba。
- **幺元与逆元**：幺元就是恒等变换，任何元素与它相乘都得到自身。元素的逆元与元素相乘得到幺元。
- **群的正式定义**：我们给出了群的经典定义：群是配备了二元运算的集合，满足结合律，存在幺元，任何元素总有逆元。
- **交换群**：如果群的乘法还满足交换律，则称其为交换群。我们验证了：整数加法群和模 n 同余类加法群是典型的交换群。

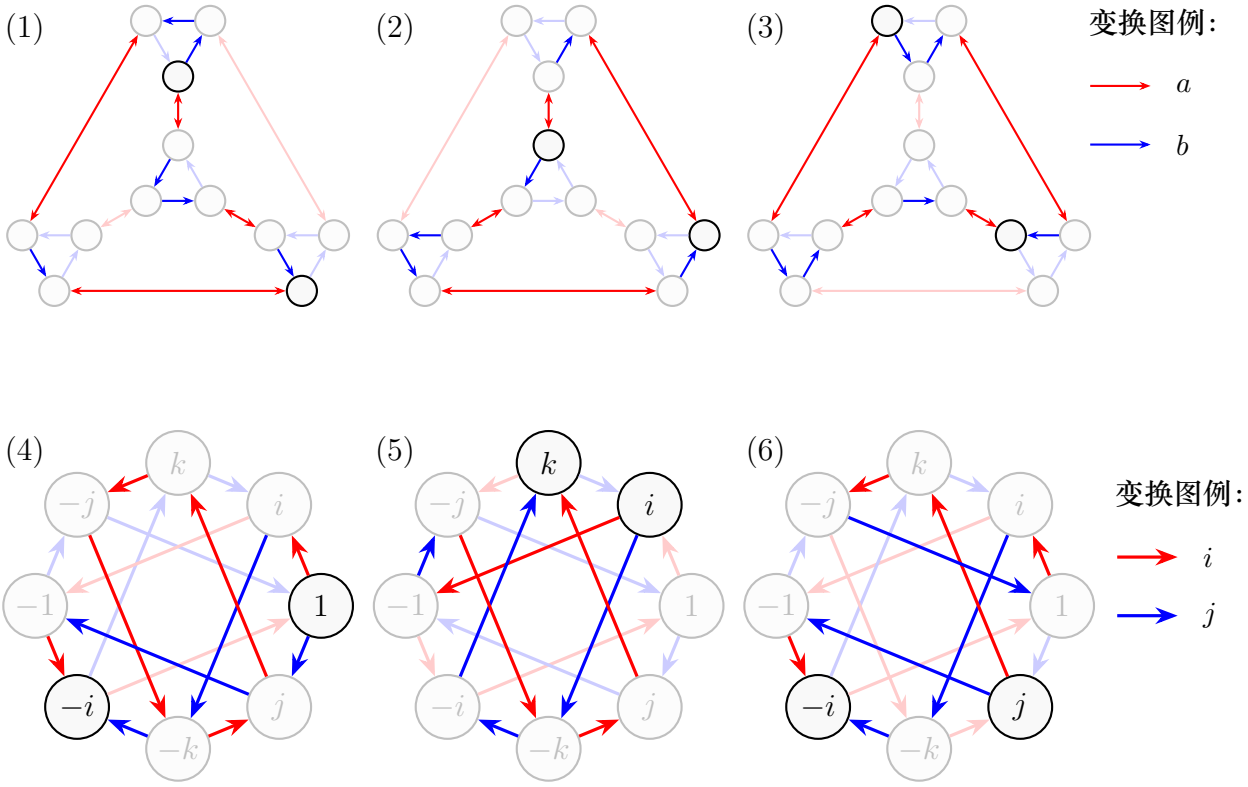
3.4 习题

群运算和乘法表

1. 考虑两个电灯开关构成的群。用 S 表示按上边开关，用 X 表示按下边开关。以下的等式哪些是真的？哪些是假的？

$$SSX = XSSX \qquad S = XSX$$
$$XS = SXSXSX \qquad S^8 = X^{100}$$

2. 充分利用高亮箭头，把以下图中高亮的路径写成群元素乘法的等式。



3. 判断以下集合中的运算是否是交换的。

(1) 整数集中的乘法运算。

(2) 有理数集中的减法运算。

(3) 实系数 2×2 矩阵的矩阵乘法运算。

(4) 模 p 非零同余类的乘法运算（p 为素数）。

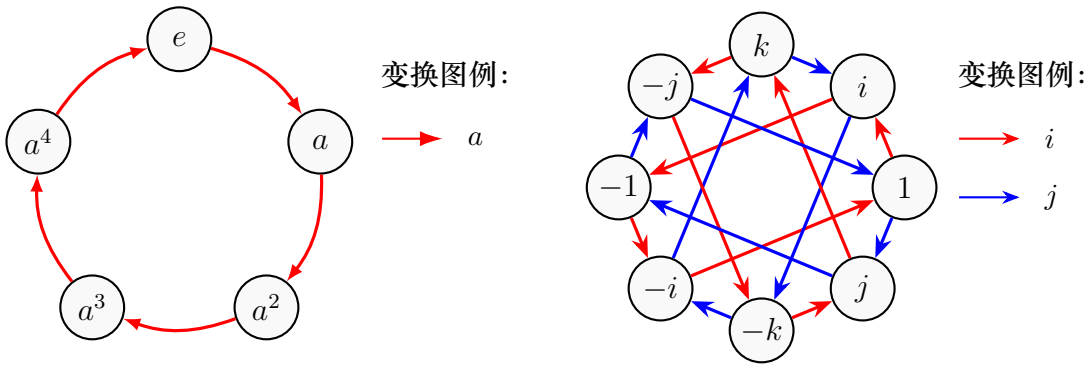
(5) 从 $[0;1]$ 映射到 $[0;1]$ 的连续函数集的复合运算。

4. 如何写出整数加法群的乘法表？给出你的想法。

5. 下图是一张没填完的群乘法表。怎样将它补完？补完的方式不止一种。分别讨论每种情况对应的群有什么特点。

$\cdot$	e	a	b	c
e				
a		e		
b				
c				

6. 下图是五元循环群 C_5 和四元数群 U_4 的生成路径图。



(1) C_5 中，a^3 是什么变换？它如何改变图中的状态？

(2) C_5 中，a^5 是什么变换？它如何改变图中的状态？

(3) U_4 中，ij 和 ji 分别是什么变换？它如何改变图中的状态？

(4) U_4 中，jji 是什么变换？它如何改变图中的状态？

(5) 写出两个群的乘法表。

似群非群

1. 考虑以下二元运算的乘法表：

$\cdot$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

(1) 说明为什么这个二元运算不满足结合律（可以用式子表示）。

(2) 这个二元运算下，各个元素有逆元吗？为什么这么说？

2. 考虑以下二元运算的乘法表：

$\cdot$	e	a	b
e	e	a	b
a	a	a	b
b	b	b	b

(1) 说明这个二元运算满足结合律（可以用式子表示）。

(2) 这个二元运算下，各个元素有逆元吗？为什么这么说？

3. 考虑以下二元运算的乘法表：

$\cdot$	e	a	b
e	e	a	b
a	a	b	b
b	b	b	b

(1) 这个二元运算满足结合律吗？为什么这么说？

(2) 这个二元运算下，各个元素有逆元吗？为什么这么说？

4. 解释以下的乘法表对应的运算为什么不构成群？

(1)

$\cdot$	e	a	b	c
e	e	a	c	b
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(2)

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c

(3)

$\cdot$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	e	b
b	b	d	c	a	e
c	c	b	e	d	a
d	d	e	a	b	c

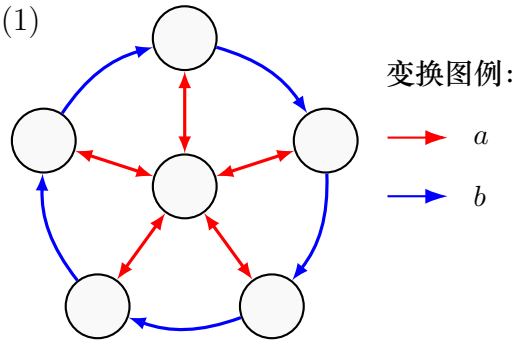
(4)

$\cdot$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

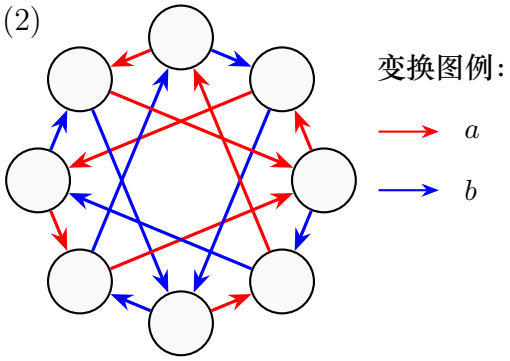
5. 为什么说群的乘法表里，群的每个元素在每一行恰好出现一次？每一列是否也有这样的情况？

6. 解释以下的图为什么不是群的生成路径图？

(1)



(2)



群的代数定义

1. 验证以下的集合是否关于提到的运算构成群。

   (1) 所有 3 的倍数关于整数的加法。

   (2) 所有 3 的倍数关于整数的乘法。

(3) 正实数关于乘方。

(4) 所有完全平方数关于整数的乘法。

(5) 所有非零的完全平方有理数关于有理数的乘法。完全平方有理数指能够写成两个完全平方数相除的商的数。

(6) 所有素数有理数关于有理数的乘法。素数有理数指能写成两个素数商的数。

(7) 模 n 的简化同余系关于同余类的乘法。简化同余系指与 n 互素的同余类的集合。

(8) 由 2 和 3 不断相乘、相除、取相反数得到的所有数的集合：$\{\pm 2^n 3^m \mid n, m \in \mathbb{Z}\}$，关于有理数的乘法。

(9) 分母为完全平方数的非零既约分数的集合，关于有理数的乘法。

2. 验证以下的集合是否关于提到的运算构成群。

(1) 整系数一元整式的集合 $\mathbb{Z}[X]$ 关于整式的加法。

(2) 实系数一元整式的集合 $\mathbb{R}[X]$ 关于整式的加法。

(3) 整系数一元整式的集合 $\mathbb{Z}[X]$ 关于整式的乘法。

(4) 实系数一元整式的集合 $\mathbb{R}[X]$ 关于整式的乘法。

(5) 实系数非零一元有理式的集合 $\mathbb{R}(X)$ 关于有理式的乘法。其中 $\mathbb{R}(X)$ 是所有能表示为非零一元整式的商的式子的集合：

$$\mathbb{R}(X) = \left\{ \frac{P(X)}{Q(X)} \,\middle|\, P, Q \in \mathbb{R}[X],\ P, Q \neq 0 \right\}$$

(6) 偶系数一元整式的集合 $\mathbb{B}[X]$ 关于整式的加法。其中 $\mathbb{B} = \{2n \mid n \in \mathbb{Z}\}$。

(7) 奇系数一元整式的集合 $\mathbb{J}[X]$ 关于整式的加法。其中 $\mathbb{J} = \{2n+1 \mid n \in \mathbb{Z}\}$。

3. 考虑一个二元群 $\{e, a\}$，其中 e 是幺元。

(1) 证明：$aa = e$。

(2) 写出二元群 $\{e, a\}$ 的乘法表。证明：二元群只有一种。

4. 考虑一个三元群 $\{e, a, b\}$，其中 e 是幺元。

(1) 证明：$ab = e$。

(2) 用反证法证明：$aa \neq e$。

(3) 写出三元群 $\{e, a, b\}$ 的乘法表。证明：三元群只有一种。

5. 根据五元循环群 C_5 和四元数群 U_4 的生成路径图，给出群里每个元素的逆元素。用乘法表的话，如何找到逆元素?

第四章　四种常见的群

上一章我们学习了群的正式定义，现在我们来了解四种常见的群。它们来自日常生活和生产中的种种现象和规律，反映了自然界和社会运行中对称性的体现和作用。

第一种群是循环群。循环群不仅是最简单的群结构，也是非常常见的一类。它不仅在生活中出现，也出现在更复杂的群里，是理解群的重要基础。循环群对应着群论中“环道”的概念，对我们理解接下来介绍的交换群和映轮群十分有帮助。最后我们会介绍置换群。置换群揭示了群和排列组合的关系，将为我们理解对称性提供非常关键的帮助。

本章的四种群不但会帮助你理解群的基本性质，而且会为你以后深入学习群论时提供丰富的例子，把抽象的思考过程变成直观的变换。请准备好在你的头脑里建设一个“群的博物馆”，将你即将见识的各种各样的群分门别类地存放在你的记忆中。它们的图像会在你以后遇到相关问题时生动地浮现出来。

4.1　循环群

回忆我们前几章提到的正三角形的对称变换群。里面包含了 6 个变换。其中 r_1 把正三角形逆时针旋转 120°。我们注意到，r_1 重复三次后，就回到初始状态。在生成路径图中，r_1 构成了一个三元循环。

讨论矩群时，我们用“向右转”对应的 4 元群来和它对比。里面的“向右转”重复 4 次后回到初始状态。如果我们把它的生成路径图画出来，就是一个 4 元循环。

这种由单个变换不断重复得到循环的现象，对应的群叫做**循环群**。循环群常常由旋转变换得到，揭示旋转、轮转的对称性质。上面两个例子都是关于旋转的变换。此外还有风车、螺旋桨、车轮等等。

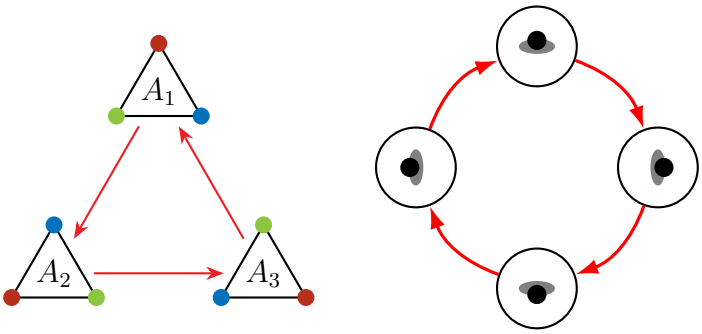


图 4.1: 三元循环和四元循环

一般来说，n 元循环群就是有 n 个元素的循环群。具体来说，某个变换 a 出发，不断重复，得到新的变换。直到某次得到恒等变换 e，把次数记为 n。那么 $a, a^2, \cdots, a^n = e$ 就构成一个 n 元循环群。a 称为这个循环群的**生成元**。我们一般把 n 元循环群记作 C_n：

$$\mathsf{C}_n = \{e, a, a^2, \cdots, a^{n-1}\}.$$

注意我们写到 a^{n-1} 为止，因为 $a^n = e$ 在一开始已经写过了。

以上说法也许让你感到疑惑。首先，从变换 a 出发，不断重复，就一定能得到恒等变换 e 吗？答案是未必。但如果能得到，那么首次得到 e 的次数，就是 a 生成的循环群的大小。之前每一次重复，得到的都是新变换，和之前的变换都不一样。

这是为什么呢？让我们反过来思考。如果不断重复变换 a 时，某次出现的变换 a^j 和之前某个变换 a^i 一样：

$$0 < i < j, \quad a^j = a^i.$$

其中 i, j 是正整数。考虑 a^{j-i}，它表示做了 a^j 变换后，逆向做 i 次 a 变换得到的结果。但 $a^j = a^i$，所以结果应该就是回到原状态，所以 $a^{j-i} = e$。但由于 i 是正整数，$j - i < j$。也就是说，在得到 a^j 之前，我们必然已经得到了 $a^{j-i} = e$。这就证明：e 必然在任何重复出现的变换之前出现。得到 e 之前，不会有变换出现两次。$a, a^2, \cdots, a^n = e$ 中任何两个元素都不一样。这说明

$$\mathsf{C}_n = \{e, a, a^2, \cdots, a^{n-1}\}$$

里确实有 n 个元素。

以下是 n 元循环群的生成路径图：

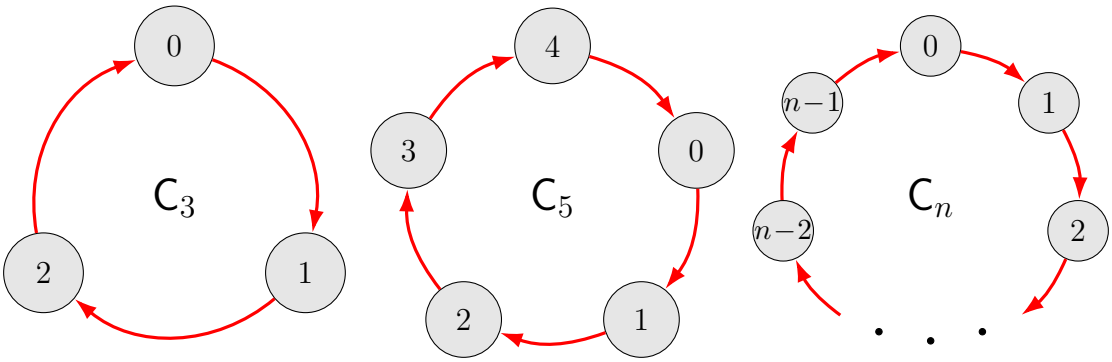


图 4.2: 3 元、5 元乃至 n 元循环群

循环群的生成路径图是一个圈。沿着走一圈就遍历了所有的元素。我们通常把 n 元循环群中的元素顺次记为 $0, 1, \cdots, n-1$。从 0 出发，第 1 个元素记为 1，第二个元素记为 2 等等，最后一个元素记为 $n-1$。这是因为模 n 的同余类 $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ 关于加法构成一个循环群：从 $\overline{1}$ 开始不断加 $\overline{1}$，就能得到所有 n 个同余类。

考察循环群里各号元素的关系，还可以用上一章引入的乘法表。当然，如果我们选择用 0 到 $n-1$ 来编号的话，这个表应该叫做加法表。下面是 $n=5$ 和 $n=12$ 时的例子：

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

图 4.3: 5 元循环群的加法表

我们把相同的数用同样颜色的方格表示，可以发现循环群的加法表有美妙的规律。从右上到左下的各条对角线上总有相同的数值，因而有相同的颜色。我们用彩虹的颜色给从小到大的数逐个配色，就能得到彩虹一般的视觉效果。这个规律也很好解释，它让我们联想到平面直角坐标系上的直线：

$$x + y = n.$$

它和水平线成 45 度角。要注意这里我们的“竖轴”是往下的。

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

图 4.4: 12 元循环群的加法表

最后，我们讨论“永远得不到 e”的情况。也就是说，从群中某个变换 a 出发，不断重复，但得到的序列

$$a, a^2, a^3, \cdots, a^n, a^{n+1}, \cdots$$

里没有 e。这种情况下，这个序列里的变换两两不同。因为我们已经证明了：如果有 $a^i = a^j$，就会出现 e。因此，群的元素个数是无限的。此外，考虑 a 的逆元 a^{-1}，它不断重复的结果也是两两不相同的序列：

$$a^{-1}, a^{-2}, a^{-3}, \cdots, a^{-n}, a^{-n-1}, \cdots$$

其中 a^{-n} 就是 a^{-1} 重复 n 次的结果：$a^{-n} = (a^{-1})^n$。

把以上两个序列和 e 合并，写成集合：

$$\mathsf{C}_a = \{a^n \mid n \in \mathbb{Z}\}.$$

可以验证：这个集合是一个群。它有无限多个元素。我们把 C_a 叫做变换 a 生成的**无限**

循环群。即便它并没有真的“循环”，可它和循环群一样，都是靠 a（及其逆变换）不断重复得来的。之后我们会看到，它确实和循环群有很多共同点，足以被归为一类。

4.1.1 环道

循环群不仅简单，而且是研究其他群的基础。任何群里总“隐藏”着循环群。比如我们研究过的三元对称群 D_3 中，就包含了三元循环群。实际上，从任意群里找一个不是幺元的元素 a，不断重复它，要么会在某个时刻得到 e，要么永远得不到 e。如果在第 n 次重复时首次得到 e，就说明我们找到了 a 生成的 n 元循环群。如果永远得不到 e，就说明我们找到了 a 生成的无限循环群。于是任何群里总有一部分是循环群。a 生成的这个循环群称为 a 的**环道**。a 生成的循环群的元素个数，叫做环道的长度或 a 的**阶**。

三元对称群 D_3 的例子里，变换 r_1 构成一个长度为 3 的环道：$\{r_1, r_1^2, r_1^3 = e\}$。$r_2$ 也构成长度为 3 的环道：$\{r_2, r_2^2, r_2^3 = e\}$。$s_1, s_2, s_3$ 则各自属于一个长度为 2 的环道。由于 $r_2 = r_1^2$，所以 r_2 的环道其实就是 r_1 的环道。s_1, s_2, s_3 各自的环道则与 r_1, r_2 的环道不一样，只有 e 是共同元素。

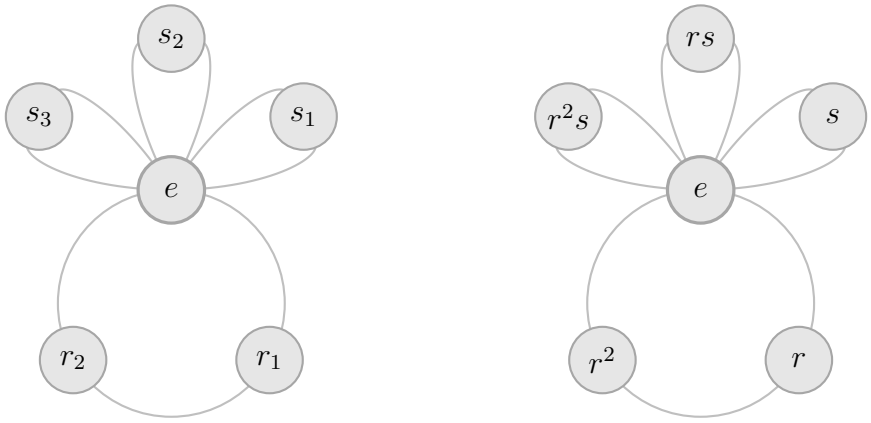


图 4.5: 映轮群 D_3 的环道图

群的每个元素都有自己所属的环道。我们把 e 看作“原点”。从 e 出发，每次根据不同元素的环道，要么沿着环道走一个圈，再回到 e；要么得到序列：

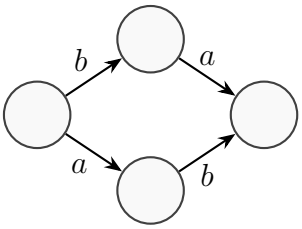
$$a^{-n}, \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots, a^n, \cdots$$

可以看作“直线”。这样可以生成整个群。把群元素按照环道画出的图也叫**环道图**。比如上图是 D_3 的环道图。为了方便，只记录 $r = r_1$，$r_2 = r_1^2 = r^2$。它们和 e 构成三元环道。三个翻转变换 s_1, s_2, s_3（记为 $s_1 = s, s_2 = rs, s_3 = r^2 s$）则分别对应二元环道。

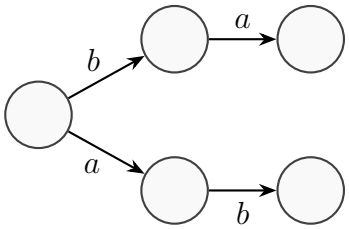
4.2 交换群

一个群的变换如果能够任意交换顺序而效果不变，就说是它是交换群。循环群就是一种交换群（是一种基本而常见的交换群）。考虑生成循环群的变换 a，其他的变换都是它重复的结果。所以无非是先重复几次、后重复几次的区别，交换顺序并不改变最终的效果。“朝三暮四”的成语用在这里正合适。

如何看一个群是不是交换群呢？首先我们可以观察它的连线图（最好是完全连线图）。从任一节点（状态）出发，先通过变换 a 再通过变换 b 到达的节点，是否和先通过变换 b 再通过变换 a 到达的节点一样？如果能找到不一样的情况，就说明它不是交换群。如果总是一样，那么它就是交换群了。



先 a 后 b 和
先 b 后 a 效果相同



先 a 后 b 和
先 b 后 a 效果不同

另一种方法是查看它的乘法表。交换群的变换可以交换顺序：$ab = ba$。在乘法表里，体现为 a 行 b 列的内容与 b 行 a 列的内容相同。

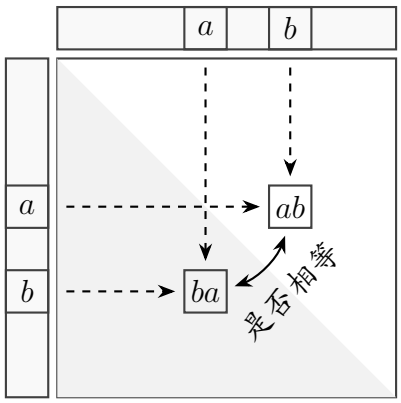


图 4.6: 检查群的乘法表：主对角线两侧对应的格子，元素是否相等

直观来看，如果把乘法表按着主对角线（从左上到右下的对角线）折叠，对角线两侧的变换刚好重叠。或者说，沿主对角线翻转，乘法表内容不变。这也是一种对称性的

体现——乘法表的对称性对应着乘法先后顺序可交换的对称性。

除了循环群，还有哪些交换群的例子呢？交换群的一个重要场景是晶体的微观结构。什么是晶体呢？晶体是一种固体，构成它的最小粒子在空间中按照一个固定的模式不断重复排列。你可以想象在立体空间里搭起一个无限延伸的脚手架，构成一个个一模一样排列的格子，每个格点上放一个完全相同的小球。无论你站在这个手脚架的哪个位置，向任何方向看，看到的排列方式都完全一样。这种“无限重复、处处相同”的规律就是典型的晶体的特征。

以食盐（氯化钠）为例：钠离子和氯离子交替排列，形成一个个小立方体，每个钠离子上下左右前后都是氯离子，每个氯离子上下左右前后都是钠离子。我们可以建立一个理想的模型。在模型里，这个立方体网格向上下、前后、左右无限重复。因此，我们如果将整个网格整体往上平移两个小立方体边长的距离（以下称为“一格”），会得到完全一样的网格。同理，整体往下、往左、往右、往前、往后平移一格，也会得到完全一样的网格。我们把这样的平移变换视为群的元素，生成的群称为**立体平移群**或**空间平移群**。

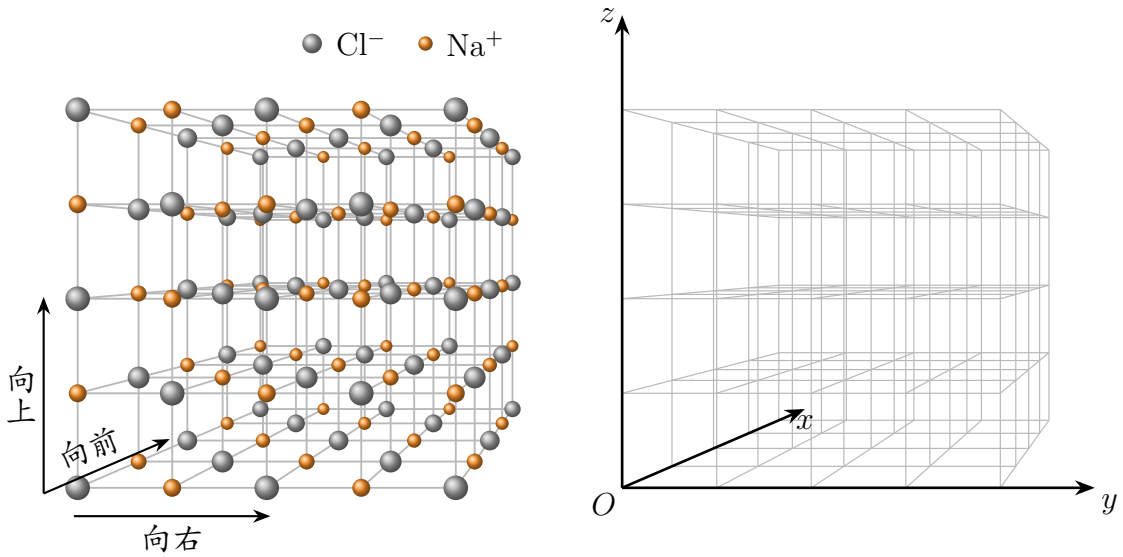


图 4.7: 氯化钠（食盐）的晶体结构

这个群里的变换可以用三个生成变换来生成：往前、往右、往上平移一格。往后、往左、往下平移一格无非是它们的逆变换。而这三个变换重复的效果，和它们的顺序无关。比如：往上再往前的效果，与往前再往上没有分别；往前再往右的效果，和往右再往前一样。所以，食盐晶体的空间平移群是一个交换群。

怎样表示这个群呢？我们可以选定一个点作为起点，记录一个变换把起点变到哪里了。比如，设变换把它变到往前平移 a 格、往右平移 b 格、往上平移 c 格后到达的位置。那么，无论你先往前还是先往右、先往上还是先往左，只要累计往前平移 n 格、往右平移 b 格、往上平移 c 格，就会到达同一个位置。这就是交换群的性质。所以，群的任何元素都可以表示为 $a\imath + b\jmath + c\kappa$ 的形式，其中 a, b, c 是整数[①]，$\imath, \jmath, \kappa$ 分别指往前、往右、往上平移一格的变换。我们可以把食盐晶体的空间平移群写作：

$$\{a\imath + b\jmath + c\kappa \mid a, b, c \in \mathbb{Z}\}$$

我们可以考虑起点为原点的空间直角坐标系，以往前、往右、往上分别为坐标轴方向，把晶体里两个小立方体边长的长度作为坐标轴单位长度，那么，变换总把起点变到某个坐标是整数的位置：(a, b, c)。我们发现：坐标的记录方法，就暗示了不同坐标轴方向的变换没有“关联”，可以任意交换顺序。比如，b 记录在 a 的旁边，用逗号隔开，于是 b 的值无论增减，都和 a 无关。这让我们想到构造以下形式的集合：

$$S = \{(x, y) \mid x \in \mathsf{C}_m, y \in \mathsf{C}_n\}.$$

其中 m, n 是正整数。集合 S 有 $m \times n$ 个元素。我们可以用数数的方式把这 mn 个元素列出来。设 $\mathsf{C}_m = \{\overline{1}_m, \overline{2}_m, \cdots, \overline{m}_m = \overline{0}_m\}$，$\mathsf{C}_n = \{\overline{1}_n, \overline{2}_n, \cdots, \overline{n}_n = \overline{0}_n\}$，那么当 $x = \overline{1}_m$ 时，可以列出 $(\overline{1}_m, \overline{1}_n), (\overline{1}_m, \overline{2}_n), \cdots, (\overline{1}_m, \overline{n}_n)$ 这 n 个元素，$x = \overline{2}_m$ 时，可以列出 $(\overline{2}_m, \overline{1}_n), (\overline{2}_m, \overline{2}_n), \cdots, (\overline{2}_m, \overline{n}_n)$ 这 n 个元素，等等。这些元素两两不相同，因为我们约定了 (x, y) 中逗号前的对象和逗号后的对象无关。

继续给这个集合定义二元运算：

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

其中 x_1, x_2 是第一份 C_m 样本中的元素，而 y_1, y_2 是第二份 C_n 样本中的元素。可以验证，S 配备了这个运算，就满足了群的要求，成了一个群。而且，由于 C_n 本身是交换群，所以 $x_1 + x_2 = x_2 + x_1$、$y_1 + y_2 = y_2 + y_1$。于是

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1).$$

这说明 S 也是交换群。我们把 S 称为 C_m 和 C_n 的**群架积**，记为 $S = \mathsf{C}_m \times \mathsf{C}_n$（在不至于混淆的情况下也简称架积）。这里的乘号很好理解，因为 S 的元素个数就是 C_m 的元素个数与 C_n 的元素个数的乘积。

[①]约定往前 -1 格就是往后 1 格，其他方向类似。

我们可以想象一个平面坐标系。把 C_m 和 C_n 的元素分别对应横轴和纵轴的整点坐标：$(\bar{i}_m, \bar{j}_n) \mapsto (i, j)$，那么 S 的元素就好像平面的 mn 个格点（坐标为整数的点）。因此 S 的构造方式就好比把两个坐标轴架设成平面坐标系，用坐标轴上的整点构建平面的格点一样。

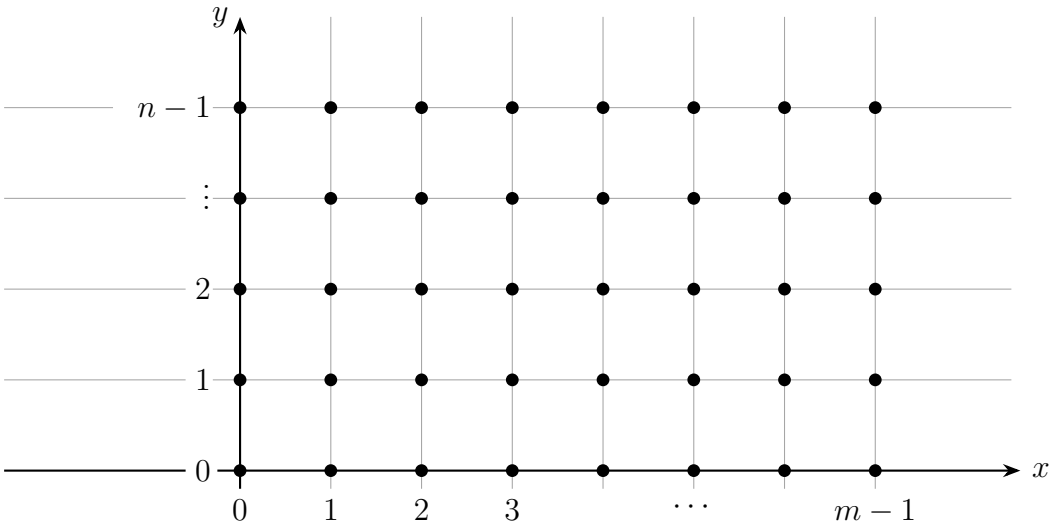


图 4.8: 平面上的格点

架积是构建交换群的重要方法。构建交换群 $\mathsf{C}_m \times \mathsf{C}_n$ 的过程中，我们其实已经说明了：只要群 G_1, G_2 是交换群，那么其架积 $G_1 \times G_2$ 就是交换群。于是从循环群这种最简单最基础的交换群开始，通过架积，就可以构造出各种各样的交换群。比如，食盐晶体的空间平移群就可以看作整数加法群 $(\mathbb{Z}, +)$ 架积得到。考虑群元素 $a\imath + b\jmath + c\kappa$，它可以表示成 (a, b, c)，因为变换 $\imath, \jmath, \kappa$ 可以交换顺序，互不干扰。于是食盐晶体的空间平移群就是

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(a, b, c) \mid a, b, c \in \mathbb{Z}\}.$$

简记为 $\mathbb{Z}^3$，它的群运算定义为：

$$(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$$

另一个例子是我们讨论过两个开关的状态群。每个开关的状态都独立于其他开关，因此，两个开关的状态群就是 $\mathsf{C}_2 \times \mathsf{C}_2$。而我们已经论证过，它同构于矩群 J_4。也就是说，J_4 其实就是两个 C_2 的架积，记为 $\mathsf{J}_4 \cong \mathsf{C}_2 \times \mathsf{C}_2$。

$\mathsf{C}_2 \times \mathsf{C}_2$ 有 4 个元素，分别写为 (e_1, e_2)、(e_1, a_2)、(a_1, e_2)、(a_1, a_2)。其中 $\{e_1, a_1\}$ 是第一个 C_2，$\{e_2, a_2\}$ 是第二个 C_2。实际上，由于两个群独立变化，我们不需要如此严格区分。不至于混淆的时候，我们可以直接把这 4 个元素记为：(e, e)、(e, a)、(a, e)、(a, a)。

再来考虑 $\mathsf{C}_3 \times \mathsf{C}_2$。我们可以类似地写出它的元素：$(e,e)$、$(e,b)$、$(a,e)$、$(a,b)$、$(a^2,e)$、$(a^2,b)$。注意这里我们使用乘法来表示 C_3 和 C_2 的群运算。它和我们见过的 D_3 一样，有 6 个元素。但结构并不相同。从 (a,b) 出发，不断重复，可以得到：

$$
\begin{aligned}
(a,b)^1 &= (a,b), & (a,b)^2 &= (a^2,b^2) = (a^2,e),\\
(a,b)^3 &= (a,b)(a^2,e) = (a^3,be) = (e,b), & (a,b)^4 &= (a,b)(e,b) = (ae,b^2) = (a,e),\\
(a,b)^5 &= (a,b)(a,e) = (a^2,b), & (a,b)^6 &= (a,b)(a^2,b) = (a^3,b^2) = (e,e).
\end{aligned}
$$

这说明 (a,b) 的环道遍历 $\mathsf{C}_3 \times \mathsf{C}_2$。可以验证，$\mathsf{C}_3 \times \mathsf{C}_2$ 同构于 C_6。

$\mathsf{C}_3 \times \mathsf{C}_2$ 同构于 C_6 会让天真的人认为 $\mathsf{C}_m \times \mathsf{C}_n$ 同构于 C_{mn}。但事实并非如此。我们已经知道，J_4 不同构于 C_4。用 $\mathsf{C}_4 \times \mathsf{C}_2$ 可以更清楚地看到这一点。

$\mathsf{C}_4 \times \mathsf{C}_2$ 有 8 个元素：(e,e)、(e,b)、(a,e)、(a,b)、(a^2,e)、(a^2,b)、(a^3,e)、(a^3,b)。同样从 (a,b) 开始重复，会发现：

$$
\begin{aligned}
(a,b)^1 &= (a,b), & (a,b)^2 &= (a^2,b^2) = (a^2,e),\\
(a,b)^3 &= (a,b)(a^2,e) = (a^3,be) = (a^3,b), & (a,b)^4 &= (a,b)(a^3,b) = (a^4,b^2) = (e,e).
\end{aligned}
$$

这说明 (a,b) 的环道长度为 4，无法遍历整个群。问题在于：C_3 的生成元是 3 阶的，不断自乘时，会和 C_2 的生成元“错开”，不会“过早”同时变为幺元。而 C_4 的生成元是 4 阶的，于是在自乘 4 次之后，两边同时变为幺元，得到 $\mathsf{C}_4 \times \mathsf{C}_2$ 的幺元。

懂得整数相关知识的读者会想到：要让两边不“过早”同时变为幺元，遍历整个群，就是要求两个阶数的最小公倍数等于其乘积。也就是说，$\mathsf{C}_m \times \mathsf{C}_n$ 同构于 C_{mn}，当且仅当 m,n 互素。这个结论是正确的，我们在习题中会严格证明。

下面列出一些通过架积得到的交换群的环道图。其环道比循环群更加复杂。从图中可以看出，一个元素并不一定只属于一个环道。幺元显然属于任何环道。此外，别的元素也可能属于多个环道。比如 $\mathsf{C}_4 \times \mathsf{C}_2$ 中，(a^2,e) 就同时属于 $(e,e),(a,e),(a^2,e),(a^3,e)$ 和 $(e,e),(a,b),(a^2,e),(a^3,b)$ 这两个环道。

反过来，是否任何交换群都可以通过循环群的架积得到呢？正式的群论教材会给出一般的结论。本书不做涉及。

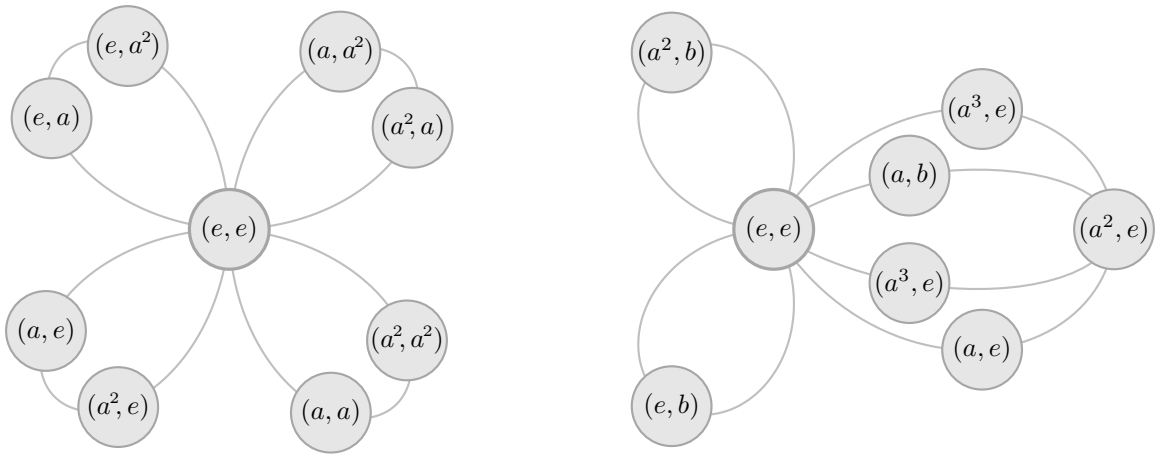


图 4.9: 左：$\mathsf{C}_3 \times \mathsf{C}_3$ 的环道图；右：$\mathsf{C}_4 \times \mathsf{C}_2$ 的环道图

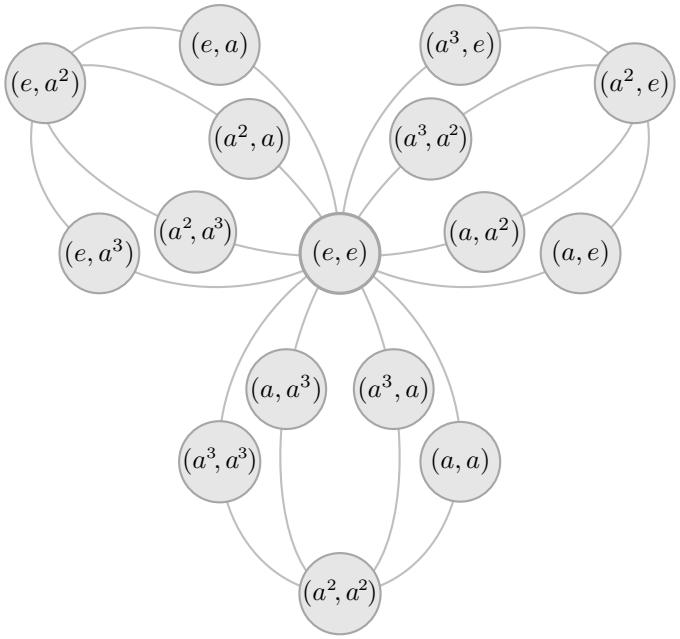


图 4.10: $\mathsf{C}_4 \times \mathsf{C}_4$ 的环道图

4.3 映轮群

循环群和交换群是结构较为简单明白的群。现在我们要进入群的领域中更加复杂晦涩的“深水区域”了。非交换群（也就是存在不可交换的元素的群）是群论中的难点，但也是群的真正美妙所在。

首先让我们来看稍微“加一点”非交换元素的结果——**映轮群**。映轮群的基本例子就是我们研究了很久的三元对称群 D_3。让我们来回忆 D_3 的结构。我们曾经用旋转变换 r_1 和翻转变换 s_1 来生成 D_3：

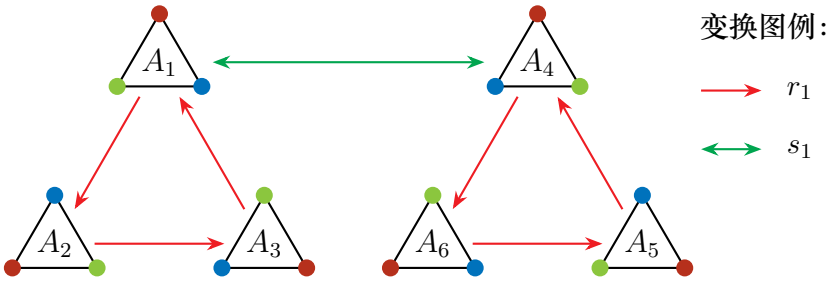


图 4.11: 正三角形的映轮群，两个循环互为映照

可以看到，A_1, A_2, A_3 和 A_4, A_5, A_6 分别在旋转变换下成为轮转的循环，而这两个循环之间的关系，就如同镜像一样，互为映照。这也是映轮群名字的由来。一般来说，**映轮群定义为正多边形的对称变换构成的群**。对称变换指保持正多边形的位置和形状不变的刚性变换，数学里叫做保距变换——它保持任何两点的距离不变。也就是说，没有伸缩、扭曲等变形手段。

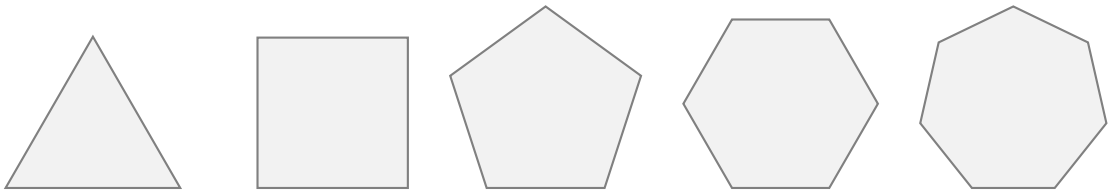


图 4.12: 各种正多边形

平面中的保距变换只有平移、旋转、翻转（轴对称）、滑移翻转四类。而平移和滑移翻转无法保持中心位置不变，所以能保持正多边形位置和形状不变，看起来和原来一样的对称变换，只有旋转和翻转两种。更具体来说，必然是按正多边形中心的旋转，和过正多边形中心的轴线的翻转变换。比如，除了恒等变换，正三角形的映轮群包括两类变

换：按中心的 120° 旋转，和关于三条中线的翻转变换。

对一般的正多边形来说，它的映轮群里也有这样两类变换。对正 n 边形来说，首先是按中心的 $\frac{360^\circ}{n}$ 旋转。这样的旋转有 $n-1$ 个。

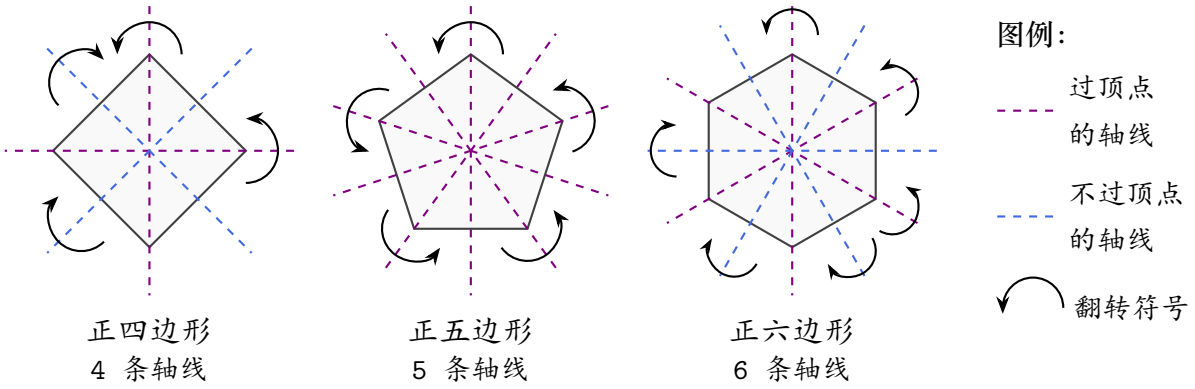


图 4.13: 正多边形按对称轴翻转

翻转的情况则复杂一点。如果 n 是奇数，那么过正 n 边形顶点和中心的直线过对边的中点。按这条中线翻转，正 n 边形不动不变。如果 n 是偶数，那么过正 n 边形顶点和中心的直线过对面另一顶点。按这条对角线翻转，正 n 边形不动不变。此外，如果 n 是偶数，那么过正 n 边形某边中点和正多边形中心的直线过对边的中点。按这条轴线翻转，正 n 边形不动不变。分别统计可知，无论 n 是奇数还是偶数，都有 n 条轴线，使得翻转后正 n 边形不动不变。

综合统计，正 n 边形的映轮群有 $n+(n-1)+1=2n$ 个元素，恰好是 C_n 的两倍。

下面来分析这些变换之间的关系。

正三角形的例子里，六个状态被分为两个三元循环，分别是顺时针和逆时针旋转构成的。而翻转变换则在这两个三元循环之间，把一个传递到另一个。这说明：翻转的效果是旋转无法做到的。旋转在三元循环里变换状态，而翻转则跳出循环。另外，两个循环的方向相反。因此，先翻转、旋转、再翻转回来的效果，就等于反向旋转。记 r 为某个旋转变换，s 为某个翻转变换，那么总有：

$$srs = r^{-1}.$$

这个关系也可以写成 $rs = sr^{-1}$、$sr = r^{-1}s$、$srsr = e$ 等等（别忘了 $s^2 = e$）。

对于一般的正 n 边形，以上这些关系也成立。可以按类似正三角形的方法生成各种状态。

下图是一个正八边形的映轮群的示意图。这是一个正八边形的停车标志，中间是一个“停”字。可以看到，正八边形的映轮群有 8 个旋转变换和 8 个翻转变换，总共 16 个元素。



图 4.14: 正八边形映轮群 D_8 的变换效果

我们可以根据“停”字的形态来理解这些变换。上排的 8 个状态是逆时针旋转变换的效果，而下排的 8 个状态里，首先可以看到“停”字左右翻转了过来。下排的 8 个状态既可以看作是从左上角正常“停”字左右翻转后（下排左起第一个），顺时针旋转的效果；也可以看作是先逆时针旋转到上排对应的角度，然后左右翻转的效果。如果仔细看，还可以发现，下排是从左上角正常“停”字出发，按照正八边形的某条对称轴直接翻转的效果。你可以自行体会 $sr = r^{-1}s$ 和 $srs = r^{-1}$ 的直观含义。

再来说明一般正 n 边形的情况。为了好说话，我们不妨把正 n 边形按逆时针顺次编号：$1, 2, \cdots, n$。

首先用按中心的逆时针 $\frac{360^\circ}{n}$ 旋转：r 来生成一个 n 元循环。它把正 n 边形不断轮转。选定一个顶点——比如 1 号——来研究的话，r 把 1 号顶点送到 2 顶点，重复之后把它送到 3 号顶点，再重复则是 4 号顶点，等等。重复 n 次之后回到原顶点。因此我们有 r 生成的 n 元循环群，对应 n 个状态。每个状态下的正 n 边形顶点 $1, 2, \cdots, n$ 都是逆时针排列的。

现在引入一个翻转变换 s，比如按过 1 号顶点和正多边形的中心的轴线翻转，就得到正 n 边形顶点新的状态：$1, 2, \cdots, n$ 按顺时针次序排列了。翻转后不断旋转，又能得到 n 个状态。这 n 个状态下的正 n 边形，由于经过翻转，顶点 $1, 2, \cdots, n$ 都是顺时针排列的。这 n 个状态和之前的 n 个状态都不一样。

我们把前 n 个状态分别记为 $1^+, 2^+, \cdots, n^+$，把后 n 个状态记为 $1^-, 2^-, \cdots, n^-$，那么变换 $e, r, r^2, \cdots, r^{n-1}$ 把状态 1^+ 分别变换为 $1^+, 2^+, \cdots, n^+$，而变换 $s, rs, r^2s, \cdots, r^{n-1}s$ 则分别把状态 1^+ 变为 $1^-, 2^-, \cdots, n^-$。

rs 后再次做翻转 s，得到 $srs = r^{-1} = r^{n-1}$，所以 2^- 经过 s 指向 n^+。同理，3^- 经过 s 指向 $n-1^+$，等等。于是我们可以画出以下生成路径图：

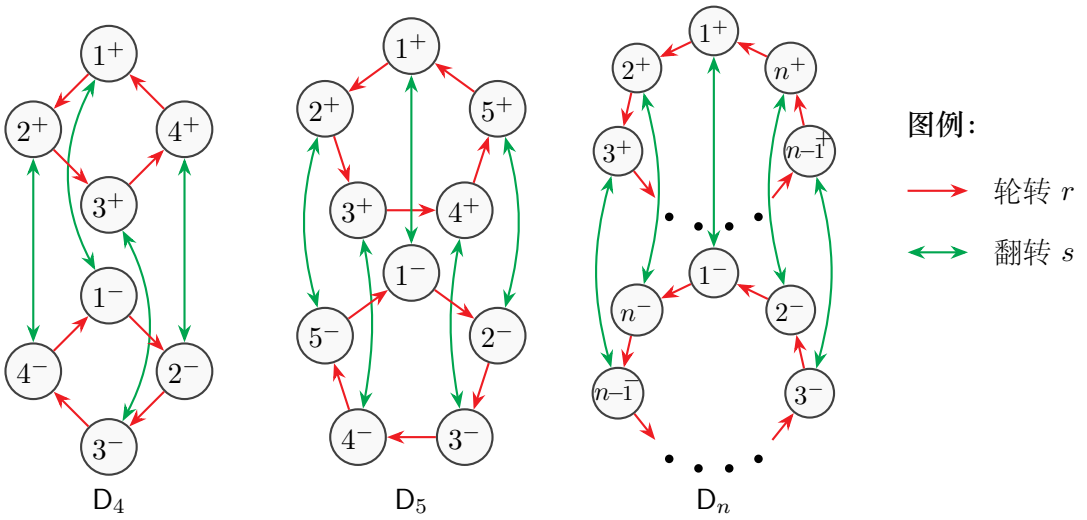


图 4.15: 映轮群 D_n 的生成路径图

从上图可以看到，旋转变换 r（红色箭头）构成上下两个轮转的循环，而翻转变换 s（绿色箭头）则交换正负状态。为了更好地展示每个状态节点的意义，我们还可以把状态用从初始状态 1^+ 到达该状态所需要的变换来命名：

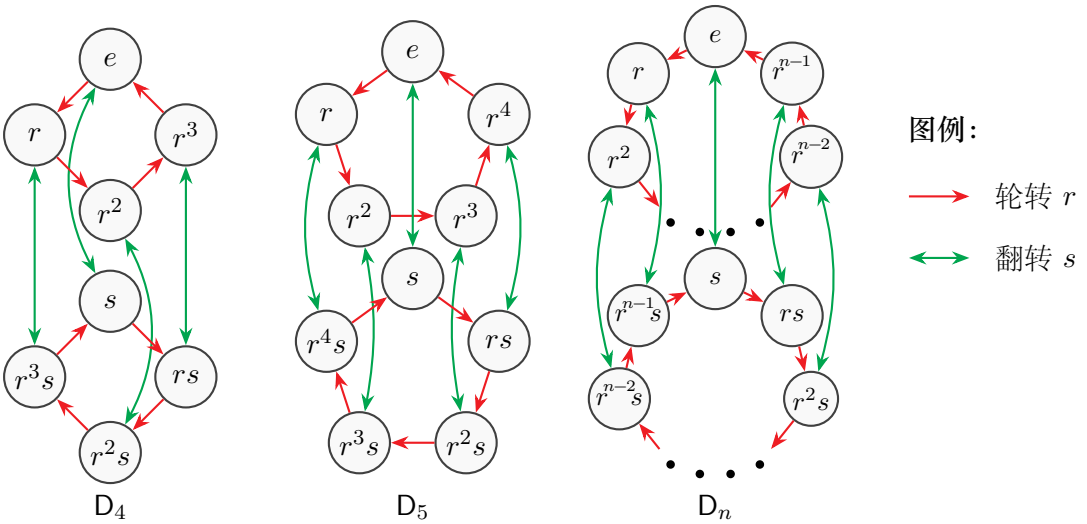


图 4.16: 映轮群 D_n 的生成路径图

这样我们可以看到 s 的作用。比如，在 D_4 中，s 乘以 rs（表示 rs 到达的状态再经

过 s 变换）得到 r^3：

$$r^3 \;=\; s \leftarrow rs \;=\; srs.$$

而 s 乘以 $r^3 s$（表示 $r^3 s$ 到达的状态再经过 s 变换）则得到 r：

$$r \;=\; s \leftarrow r^3 s \;=\; sr^3 s.$$

一般来说，在 D_n 中有 $r^2 = sr^{n-2}s$、$r^{n-2} = sr^2 s$，等等。我们知道 $r^n = e$，所以 r^{n-i} 就是 r^i 的逆变换。因此以上等式也可以写为：

$$\forall\, i = 1, 2, \cdots, n-1, \qquad \left(r^i\right)^{-1} \;=\; r^{n-i} \;=\; sr^i s.$$

再来看映轮群的乘法表。生成路径图里，我们能看到状态分为两类。这个两分的特征在乘法表里也明显能体现出来。下面是 D_5 的乘法表。

	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
e	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	e	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	e	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	e	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	e	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s	r^4s	r^3s	r^2s	rs	e	r^4	r^3	r^2	r
rs	rs	s	r^4s	r^3s	r^2s	r	e	r^4	r^3	r^2
r^2s	r^2s	rs	s	r^4s	r^3s	r^2	r	e	r^4	r^3
r^3s	r^3s	r^2s	rs	s	r^4s	r^3	r^2	r	e	r^4
r^4s	r^4s	r^3s	r^2s	rs	s	r^4	r^3	r^2	r	e

图 4.17: 映轮群 D_5 的乘法表

这是一个 10×10 的表格。能看出整张表被上下左右分为四块，像个“田”字。每块内部有自己的规律。左半区和右半区仿佛结构一致；上半区和下半区仿佛对称。这当然是因为我们把旋转 e, r, r^2, r^3, r^4 和翻转 s, rs, r^2s, r^3s, r^4s 两类按顺序分别排列了。

乘法表的左上块显然就是循环群 C_5，也就是生成路径图里的上轮。右下块的元素和左上块一模一样，都只有 e, r, r^2, r^3, r^4。左下和右上块的元素则都只有 s, rs, r^2s, r^3s, r^4s。

把前者记为集合 E，后者记为集合 S，我们可以得到这样的规律：E 中元素和 S 中元素复合，得到 S 中元素。E 中元素自相复合，或 S 中元素自相复合，则得到 E 中元素。如果我们单纯考虑一枚硬币的翻转状态，也会得到同样的规律。也就是说，D_5 的乘法表，在大体上的行为，和二元循环群 C_2 的 2×2 的乘法表一致。这个现象背后是群的一种关键的性质，在后面的章节将重点讨论。

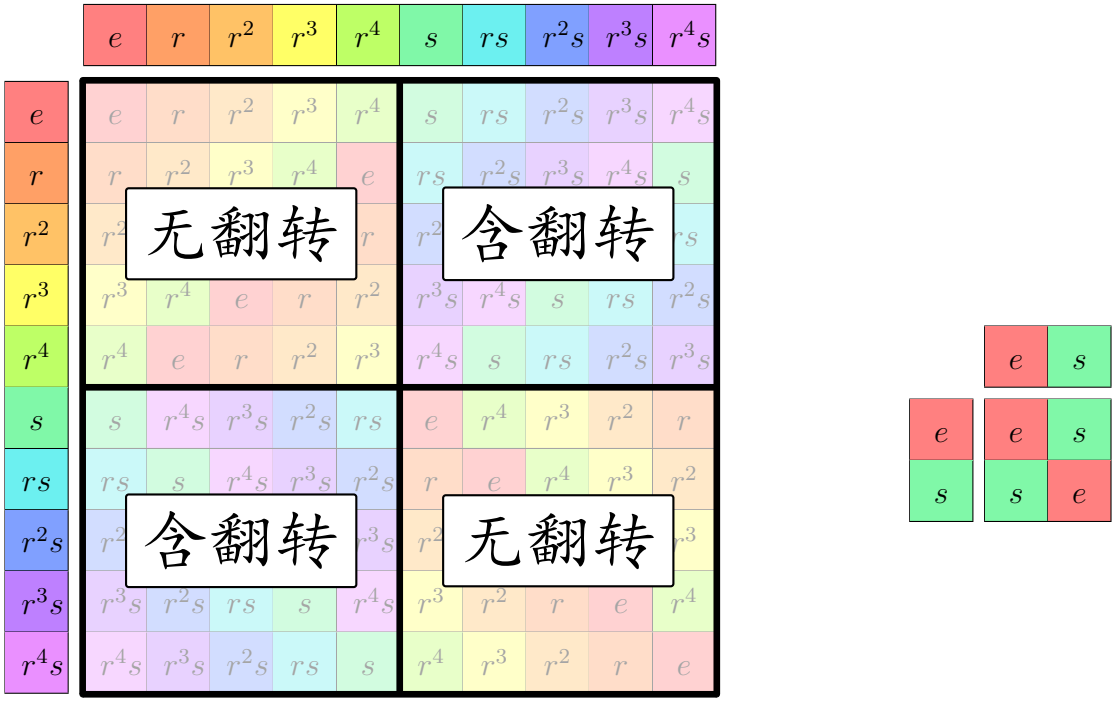


图 4.18: D_5 乘法表按翻转分块后与 C_2 的对比

最后来看映轮群的环道。对任意的旋转变换 r 和任意的翻转变换 s，我们建立过这样的关系：

$$srs = r^{-1}.$$

两边右乘上 r 就得到：

$$srsr = r^{-1}r = e.$$

也就是说，连做两次 sr 变换，等于什么也不做。类似地，考察 $rsrs$：在上式两边左乘 r，得到：

$$r = r \leftarrow (srsr) = rsrsr = (rsrs) \leftarrow r.$$

于是 $rsrs$ 也等于 e。实际上，翻转和旋转的组合 rs 或 sr，还是翻转，只不过对称轴变了。因此，映轮群里，旋转变换的循环是一个环道（对应一个循环群），而翻转变换则各自构成环道。

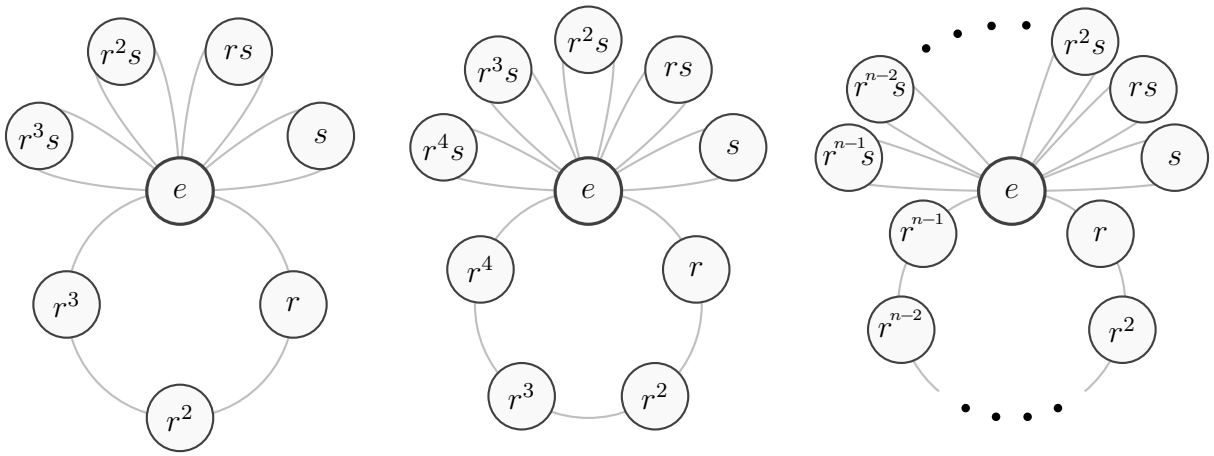


图 4.19: $\mathsf{D}_4, \mathsf{D}_5$ 以及一般的 D_n 的环道图

要注意区别的是：状态的循环轮转，不等于环道。环道是变换作为群元素的循环，总包括幺元。而状态的循环则不一定包括初始状态。

4.4 置换群

我们很早就接触过置换的概念。把 n 个互不相同的物品排成一列，有多少种方法？思考这个问题的时候，可以从某种排列出发。其他的方法，都是把物品的位置换一换得到的。这种变换就是**置换**。置换就是从 n 元集合到自身的一一对应：物品还是那些物品，只不过位置换了，顺序变了。

我们知道，把 n 个互不相同的物品排成一列，有 $n!$ 种方法。也就是说，如果把完全不变也看作置换，那么 n 个物品一共有 $n!$ 种置换。如果把正三角形的顶点编号看作固定位置，那么旋转和对称变换都是变换了把三种颜色放进顶点的方法，把不同的颜色分别放入不同的位置，因此就是某种置换。同理，考虑正方体的旋转时，如果把八个顶点看作固定位置并编号，那么每种旋转变换都是变换了把八种颜色放入顶点的方法，把不同的颜色分别放入不同的位置，因此是一种置换。

置换与对称有密切联系。置换构成的群称为**置换群**，在群论中有重要位置。

首先来看一个典型的例子：三种颜色的小球从左到右排成一列。假设某种排列（比如红黄蓝）是初始状态，那么任何一种重新的排列方法，都是初始状态的置换。

显然，一共有 $3! = 6$ 种排列方法，如下图所示：

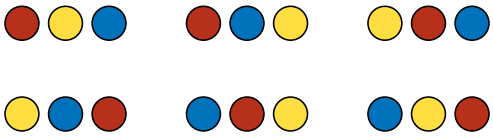
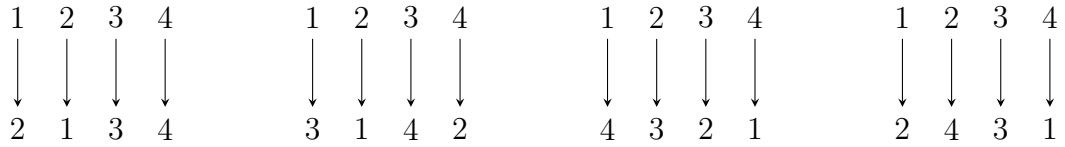
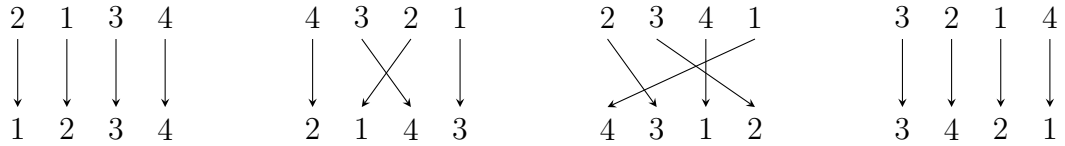


图 4.20: 三个小球的所有排列方法

对于一般的情况，为了好说话，我们用数字来编号：$1,2,\cdots,n$。如果把这 n 个数字从左到右排成一行：$1,2,\cdots,n$，记为初始状态。那么，$1,2,\cdots,n$ 的任意排列方法，都是从这个状态出发，把数字的位置换一换得到的。因此，对应一个置换。反之，从初始状态出发，任意的置换方法，得到的总是 $1,2,\cdots,n$ 的某种排列。我们用以下方法来记录一个置换：把初始状态的数字写成一行，把置换后的数字也写成一行，然后用箭头从置换前的数字指向置换后的数字，说明它变换的结果。比如，下图就是 $1,2,3,4$ 的几种置换：



要注意的是：这个表示方法其实不关心初始状态数字的顺序，只关心用箭头从置换前的数字指向置换后的数字。我们可以把初始状态换为别的顺序，甚至把置换后的数字也改变顺序。以上四个置换分别可以写为：



我们甚至可以把初始状态的数字写成纵列。



这个规则和表示映射的箭头是一样的。因此我们可以方便地用它来表示置换的复合：只需要跟着箭头即可。比如下面的置换复合把 1 变为 2，然后再变为 4；把 2 变为

1，然后再变为 3；把 3 变为 3，然后再变为 2；把 4 变为 4，然后再变为 1。

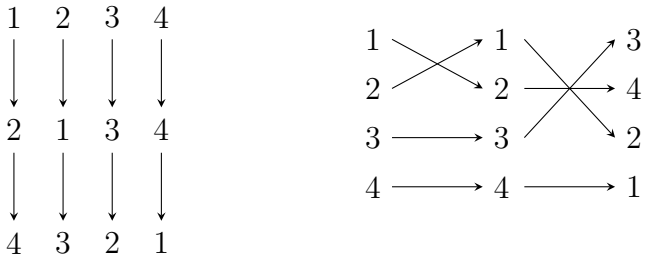
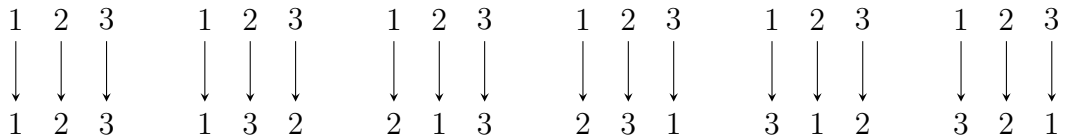


图 4.21: 两种方法记录置换的复合：把 (1234) 变为 (2134)，再变为 (4321)。

所有 n 个元素的置换，或者说 n 元集合的所有双射，按照映射的复合运算，构成群吗？不难验证，答案是肯定的。首先，容易验证置换的复合运算满足封闭性：置换的复合仍然是置换。其次，映射的复合运算满足结合律。再者，恒等映射是置换的复合运算的单位元。最后，每个置换都是双射，因此必然有逆映射，逆映射也是置换，按定义逆转置换的效果，这就是逆元的定义。因此，所有 n 元置换构成群。我们称它为 **n 元全置换群**，记为 S_n。它有 $n!$ 个元素。比如，S_3 有 $3! = 6$ 个元素，S_4 有 $4! = 24$ 个元素。一般集合 X 上的全置换群则记为 S_X。

具体的置换群长什么样子呢？S_1 是单元群，S_2 是二元群。我们已经了解过了。S_3 有 $3! = 6$ 个元素，即 6 种三元置换。

如何理解这些置换呢？我们希望将它们分类。一个想法是按置换的不动点分类，即它保持多少个位置不变。重排三个物品，可以保持 $0, 1, 2, 3$ 个位置不变。要注意的是：恰好 2 个不变是做不到的。因为一共 3 个物品，如果两个位置不变，那么剩下那个的位置也不会变。3 个位置都不变的是恒等变换。1 个位置不变，说明另两个物品交换位置。这样的置换有 3 个。剩下的 2 个置换则是完全移位，没有不变的位置。



分别研究后两类置换。恰好交换两个位置的置换，称为**对换**，即把一对物品交换。对换两次就是恒等变换。所有位置都变了的两个置换，一个把 1 变为 2、把 2 变为 3、把 3 变为 1；一个把 1 变为 3、把 3 变为 2、把 2 变为 1。这样把一组对象轮转移位的置换称为**轮换**。如果有 k 个对象被移位，就称为 k **元轮换**，说轮换的长度是 k。这两个轮换都是 3 元轮换，各自重复两次会变成对方。而如果重复三次，那么都变为恒等变

换。这个结构非常眼熟。我们猜想：S_3 就是映轮群 D_3。

定理 4.1

三元全置换群同构于正三角形的映轮群：$\mathsf{S}_3 \cong \mathsf{D}_3$。

事实上确实如此。把正三角形顶点所在的固定位置编号为 $1, 2, 3$，那么，D_3 里的各种变换，就是顶点位置的变换。比如，逆时针旋转 $120°$ 的效果，就是把顶点从 1 转到 2，从 2 转到 3，从 3 转到 1。因此，我们可以把它和置换：$1 \to 2,\ 2 \to 3,\ 3 \to 1$ 对应起来。如下图，D_3 里的每个变换，都恰好对应 S_3 里的一个三元置换。

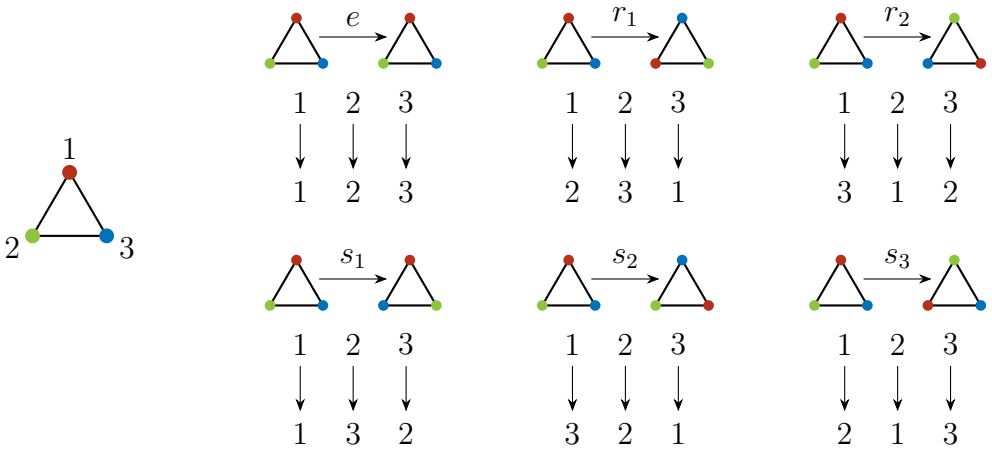


图 4.22: 映轮群 D_3 和全置换群 S_3 的对应关系

可以看出，三个翻转变换就是对换。因为按中线翻转保持中线上的顶点不变，交换另两个顶点。而两个旋转变换就是完全移位的 3 元轮换。按这个方式，我们建立了 S_3 和映轮群 D_3 之间的一一对应。我们可以接着逐个验证三元置换两两组合的效果，即群 S_3 的乘法。其运算律和 D_3 对应变换的运算律是一样的。例如，先对换 1 和 2（对应 s_3），再对换 2 和 3（对应 s_1），得到 $(3\,1\,2)$（对应 r_2）。而 $r_2 = s_3 \to s_1$。这说明两者的群乘法表一模一样，因此两者同构。我们之前把 D_3 称为三元对称群，并不是错误，而是因为 D_3 确实包含了三元变换的所有对称性。

注意：S_3 和 D_3 的关系只是巧合。$n \neq 3$ 时，S_n 和 D_n 并不同构。前者有 $n!$ 个元素，后者只有 $2n$ 个。随着 n 增大，差别会越来越大。

4.5 置换群定理

全置换群代表了怎样的对称性呢？全置换群对应集合的对称性。回顾集合的定义：集合是无序的，它只关心一个元素是否属于它，不关心它的元素按什么方式罗列。因此，集合经过任何置换都不改变。这就是全置换群对应的对称性。我们也称全置换群为集合的**对称群**。n 元全置换群就是 n 元集合的对称群，简称 $\boldsymbol{n}$ **元对称群**。

考虑矩群 J_4。它有 4 个元素，分别是 e, p, q, pq。如果把矩形的四个顶点编号为 $1, 2, 3, 4$，那么每个变换都是按顺序把四种颜色放入顶点，因此是某种置换。我们可以把 J_4 的四个元素与 S_4 中的四个置换对应起来。

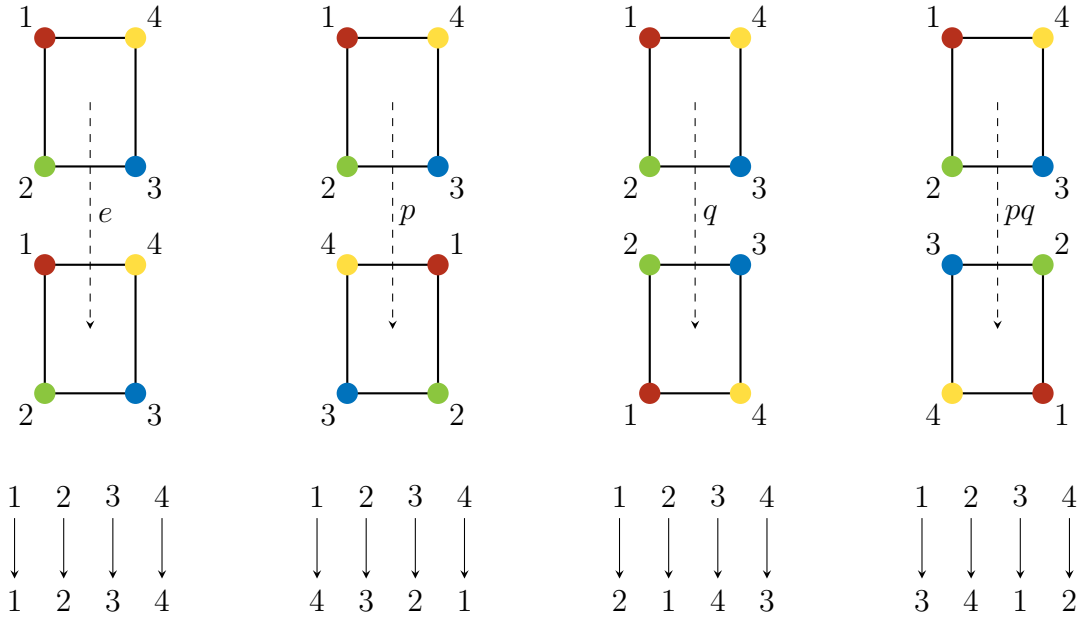


图 4.23: 矩群元素对应的置换

再来看另一个前面提过的例子：正方体的旋转群。我们知道，正方体的旋转群有 24 个元素。把正方体的八个顶点编号为 $1, 2, \cdots, 8$，每个旋转变换都是按顺序把八种颜色放入顶点，因此是某种置换。但我们讨论正方体的旋转群时，并不会涉及 8 个顶点的全部置换（8 个元素的置换一共有 $8! = 40320$ 种）。也就是说，n 元置换构成的群，并不一定是所有可能的 n 元置换的集合。

进一步，我们会想：是否所有的群，都可以看作某些置换的集合呢？为此，我们需要让每个群元素对应一个置换。

对于 n 个元素的群 G，考虑它的乘法表。我们发现，乘法表的每一行，似乎都可以看作一个置换。比如幺元就对应恒等变换：它乘以任何元素得到该元素自身。这个想法是否成立呢？为了好说话，把 G 的元素编号，记为 $1, 2, \cdots, n$。比如矩群有四个元素，就记为 $1, 2, 3, 4$。于是整个群就记为 $G = \{1, 2, \cdots, n\}$。我们只需要说明，单个群元素乘以所有元素的结果，必然是不重复不遗漏的，于是构成 $1, 2, \cdots, n$ 的置换。

·	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

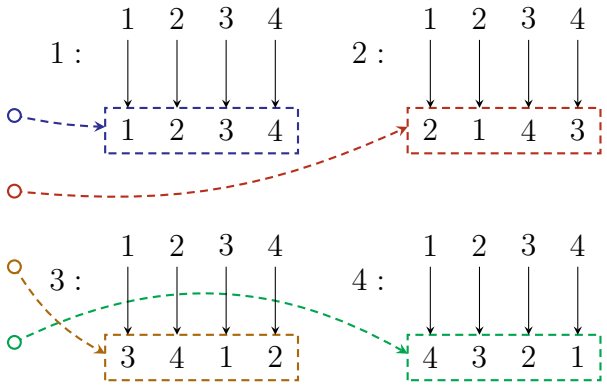


表 4.1: 矩群 J_4 的乘法表。每行都可以看作一个置换。

下面来说明这一点。考虑映射：

$$\begin{aligned} T_i : G = \{1, 2, \cdots, n\} &\longrightarrow \quad G \\ j \qquad &\longmapsto j \to i \ = \ i \cdot j \end{aligned}$$

它表示了第 i 行的群乘法结果（要注意的是这里的“$\cdot$”是群的乘法，而不是整数的乘法）。首先，T_i 的结果必然不会重复。如果 $x, y \in G$ 使得

$$T_i(x) = i \cdot x = i \cdot y = T_i(y),$$

那么两边同时在左侧乘以 i^{-1}，就得到 $x = y$。因此，T_i 的结果不会重复。其次，群的每个元素都有逆元，所以对于任意 $j \in G$，都有 $i^{-1} \cdot j \in G$，使得

$$T_i(i^{-1} \cdot j) = i \cdot (i^{-1} \cdot j) = (i \cdot i^{-1}) \cdot j \ = \ e \cdot j \ = \ j.$$

这说明 T_i 的结果也不会遗漏。也就是说，乘法表的第 i 行的结果，恰好是 n 元置换，我们称其为群元素 i 对应的**行置换**。

考虑行置换的集合：$T = \{T_i \mid i \in G\} \subseteq \mathsf{S}_n$，可以验证，集合 T 关于映射的复合构

成群。首先，映射的复合运算满足结合律。其次，按定义：

$$\begin{aligned}&\forall i,j\in G,\\ &\quad\forall x\in G,\quad (T_i\circ T_j)(x)=T_i(T_j(x))=T_i(j\cdot x)\\ &\qquad\qquad =i\cdot(j\cdot x)=(i\cdot j)\cdot x\\ &\qquad\qquad =T_{i\cdot j}(x).\end{aligned}$$

即 $T_i\circ T_j = T_{i\cdot j}$。这个结果首先说明 T 的元素关于映射的复合运算封闭：复合的结果还在 T 里。其次，它给出了复合结果与 i,j 的关系。T_i 与 T_j 的复合，等同于 i,j 在群中的乘积对应的行置换。于是：

1. 幺元 e 对应的行置换 T_e 也是 T 中的幺元：$\forall\, i\in G$，$T_e\circ T_i=T_{e\cdot i}=T_i$，$T_i\circ T_e=T_{i\cdot e}=T_i$。
2. T_i 的逆元是 $T_{i^{-1}}$：$\forall\, i\in\{1,2,\cdots,n\}$，$T_{i^{-1}}\circ T_i=T_{i^{-1}\cdot i}=T_e$，$T_i\circ T_{i^{-1}}=T_{i\cdot i^{-1}}=T_e$。

于是，T 关于映射的复合构成群。

考虑群 G 的元素 i 和行置换 T_i 的对应关系：

$$\begin{aligned}\phi:\qquad G &\longrightarrow T\\ i &\longmapsto T_i\end{aligned}$$

它显然是满射，而且也是单射：若 $T_i=T_k$，计算幺元 e 的像，得

$$i=i\cdot e=T_i(e)=T_k(e)=k\cdot e=k,$$

故 $i=k$。于是 ϕ 是双射。此外，按照前面的结果，它满足：

$$\forall i,j\in G,\quad \phi(i)\circ\phi(j)=T_i\circ T_j=T_{i\cdot j}=\phi(i\cdot j).$$

这说明 ϕ 把群 G 的乘法关系完全复刻到了 T 里。按我们之前的说法，既然关系完全一模一样，这两个群就是同构的，讨论 G 就是讨论 T，反之亦然。ϕ 称为两者之间的**同构映射**，它具体说明了两个群同构的方式。

要注意的是：以上的证明不仅适用于 n 元群，也适用于元素个数无限的群。实际上，行置换 T_i 的想法虽然来自乘法表的行，但它的定义并不依赖于乘法表，我们完全可以形式地定义：

$$\begin{aligned}T_i: G &\longrightarrow G\\ j &\longmapsto i\cdot j\end{aligned}$$

而以上的证明也无需改变，因为证明方法并不需要用到元素个数有限的条件。因此，我们得到结论：

定理 4.2 置换群定理

> 任何群都同构于某个由置换构成的群。
> n 个元素的群，同构于某个由 n 元置换构成的群。

这个定理揭示了群的基本性质：所有的群，本质上都是由置换构成的。我们可以用置换构造出任意一个群。

要注意的是，n 元群并不是只能同构于 n 元变换构成的群。比如前面介绍的 D_3 同构于 S_3。而按照以上推导，D_3 同构于某个 6 元置换构成的群（因为 D_3 有 6 个元素）。当然，由于它们同构，本质上都是同一个群。

当 $n > 3$ 时，全置换群的元素个数增长得非常快。S_4 有 24 个元素，S_5 有 120 个元素，S_6 则有 720 个元素了。这么多元素的群，十分复杂，只靠逐个元素去分析，已经不现实。我们可以勉强分析一下 S_4。S_4 的元素个数和第一章里提到的正方体的旋转群一样多。实际上，这两个群是同构的。

定理 4.3

> 四元全置换群同构于正方体的旋转群：$\mathsf{S}_4 \cong \mathsf{T}_6$。

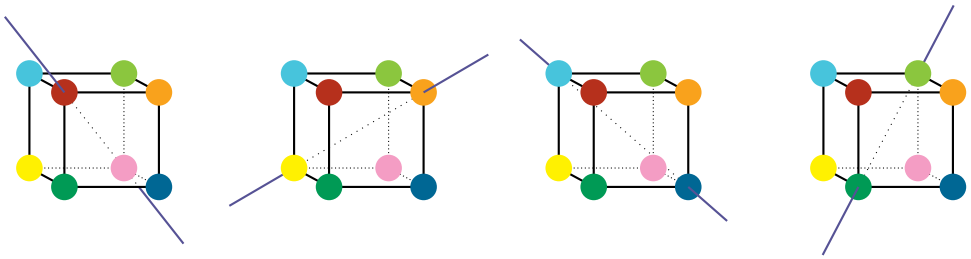


图 4.24: 正方体的四条顶心对角线

为了看清这一点，可以考虑正方体的顶心对角线，即穿过正方体中心和一对顶点的对角线。顶心对角线有四条，把正方体的 8 个顶点分成四对。旋转正方体前后，顶心对角线仍然是顶心对角线。所以，正方体的旋转变换实际上是四条顶心对角线的重排。把四条顶心对角线编号，那么正方体的任何旋转都对应一个 4 元置换。我们把这个对应关系记为映射 ϕ。通过枚举所有旋转和 4 元置换的一一对应关系（见图 4.25）可知，映射 ϕ 是双射。此外，ϕ 传递群运算：旋转作为映射的复合，自然对应着顶心对角线变换的

复合，因此对应 4 元置换的复合。因此，ϕ 是群的同构。正方体的旋转群，就是 S_4。

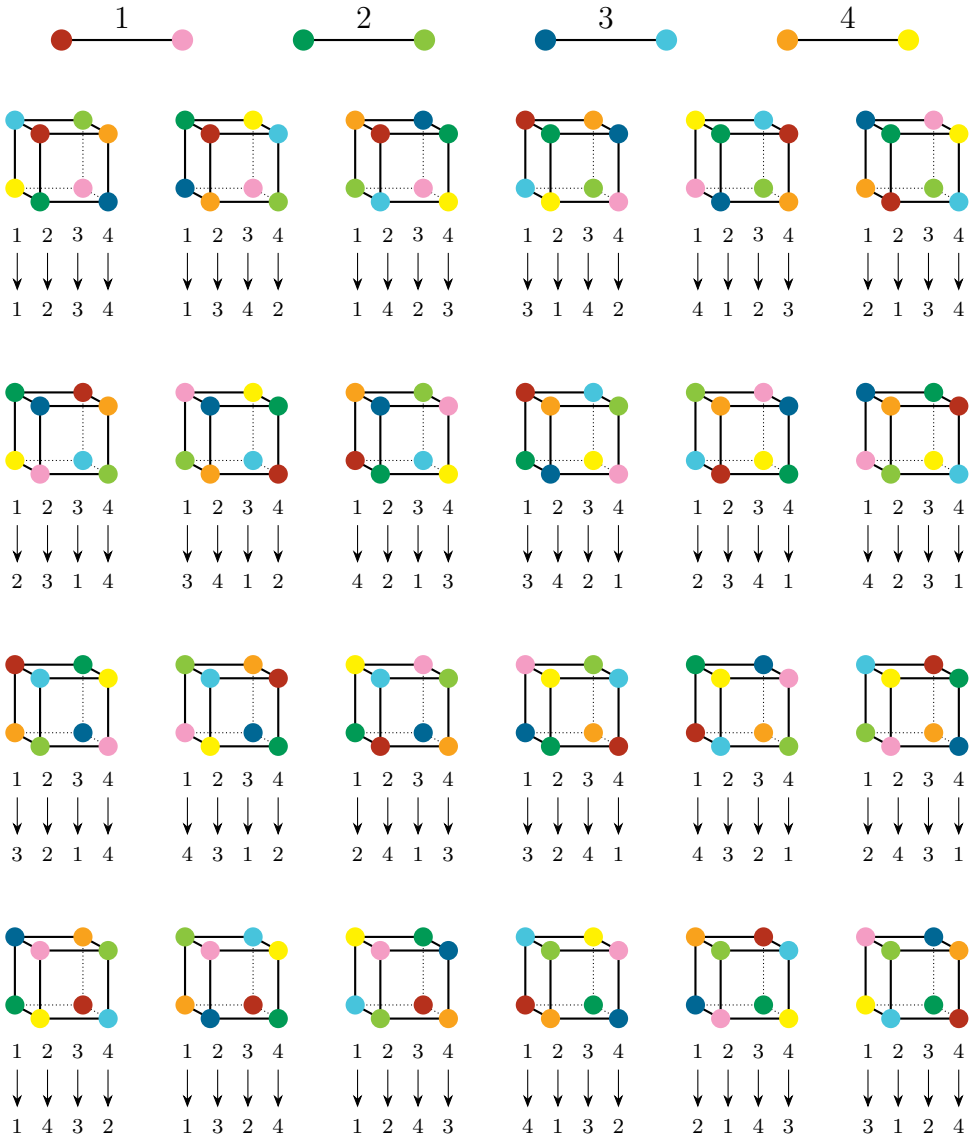


图 4.25: 正方体旋转与 4 元置换按顶心对角线一一对应

本章小结

本章详细探讨了四种基础且重要的群。主要知识点包括：

- **循环群**：由单个元素不断重复生成的群。
- **环道**：群中元素不断重复生成的循环群。它的长度叫做群元素的阶。
- **群的架积**：由两个或多个群组合而成的新群，其元素为各群元素的有序组合，运算按分量进行。循环群的架积是交换群。
- **映轮群**：描述正多边形所有对称操作（旋转和翻转）的群。正 n 边形的映轮群有 $2n$ 个元素。其中 n 个元素是旋转变换，另外 n 个是翻转变换。
- **置换群**：集合到自身的双射构成的群，群运算为映射的复合。
- **对换**和**轮换**：恰好交换两个位置的置换称为对换。对换两次就是恒等变换。把一组对象每个都移到下一位，最后一个放到第一位，这样完全移位的置换称为轮换。
- **置换群定理**：所有群都同构于某个由置换构成的群。
- **三元全置换群同构于正三角形的映轮群**。
- **正方体的旋转群同构于四元全置换群**。

4.6　习题

循环群与交换群

1. 设 k 是任取的整数,a 是 n 元循环群 C_n 的生成元。那么，对于哪些整数 k，有 $a^k = e$? 这些整数构成的集合有什么特征?

2. 考虑 n 元循环群 $\mathsf{C}_n = \{a, a^2, \cdots, a^n = e\}$。对正整数 $k > 1$，设 $b = a^k$。我们想了解：b 不断自乘，得到的环道是怎样的?

(1) 如果 k 是 n 的因数：$n = mk$，证明：b 的环道长度为 m。

(2) 如果 k 和 n 互素，证明：b 能生成 C_n 全体元素。

(3) 一般情况下，记 d 为 k 和 n 的最大公约数，$n = md$，证明：b 的环道长度为 m。

3. 考虑 k 个二元循环群架积得到的群 C_2^k。它一般记为

$$\mathsf{C}_2^k = \{(n_1, n_2, \cdots, n_k) \,|\, n_1, n_2, \cdots, n_k \in \{0, 1\}\}.$$

其中元素运算为按分量的同余加法：$(n_1, n_2, \cdots, n_k) + (m_1, m_2, \cdots, m_k)$ 的第 i 位是 $n_i + m_i$ 模 2 的余数。

(1) 证明：按照架积的定义，任何 $x \in \mathsf{C}_2^k$ 都满足 $x + x = e$。

(2) 说明为何 C_2^k 构成群。说出群的幺元和任何元素的逆元。

(3) 设 a, b 为正整数，证明：C_2^{a+b} 与 C_2^a、C_2^b 架积得到的群同构。

4. 考虑两个循环群 C_n、C_m 架积得到的群：$\mathsf{C}_n \times \mathsf{C}_m$。记 C_n、C_m 的幺元分别为 e_1, e_2。设 a, b 分别为 C_n、C_m 的生成元。

(1) 考虑 (a, b)，它的逆元素是什么?

(2) (a, b) 不断自乘得到 $(a, b), (a^2, b^2), \cdots (a^k, b^k), \cdots$。找出使得 $(a^k, b^k) = (e_1, e_2)$ 的最小正整数 k。k 有什么性质?

(3) 证明：如果 m, n 互素，(a, b) 能生成 $\mathsf{C}_n \times \mathsf{C}_m$。

(4) 证明：如果 m, n 不互素，那么没有任何群元素能单独生成整个 $\mathsf{C}_n \times \mathsf{C}_m$。

映轮群和置换群

1. 存在恰有 77 个元素的映轮群吗?

2. 研究映轮群 D_4。

(1) D_4 有几个元素? 列出 D_4 所有元素，并定性说明它们与 D_3 元素的相似之处。

(2) 如何生成 D_4? 研究 D_4 的生成路径图，说明相关的变换如何生成整个群。

(3) 给出 D_4 各个元素的环道。对比 D_4 的环道图，分析哪些元素的环道和环道图上不一样。

(4) 写出 D_4 的乘法表。

3. 写出 S_1 到 S_{10} 这 10 个全置换群的势。

4. 研究 S_4。

(1) S_4 有几个元素? 用本章中介绍的写法，列出所有的元素（4 元置换)。

(2) 为了方便，我们采用更简单的方法表示 S_4 的元素：在圆括号中列出 $1,2,3,4$ 置换后的结果。比如 $(2\,4\,1\,3)$ 就表示 $1\mapsto 2,\ 2\mapsto 4,\ 3\mapsto 1,\ 4\mapsto 3$ 的置换。说明本章中的记法和这种记法如何转换。

(3) 考虑置换 $\tau_1=(2\,3\,4\,1)$，它表示怎样的置换? 写出它的环道。

(4) 考虑置换 $\tau_2=(2\,1\,3\,4)$，它表示怎样的置换? 写出它的环道。

(5) 考虑置换 $\tau_3=(2\,1\,4\,3)$，它表示怎样的置换? 写出它的环道。

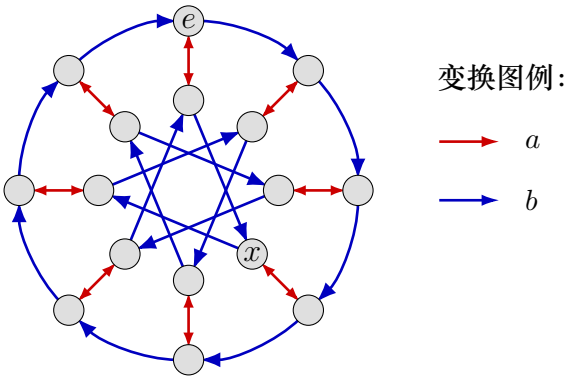
(6) 考虑置换 $\tau_4=(2\,3\,1\,4)$，它表示怎样的置换? 写出它的环道。

(7) 计算 S_4 中所有元素的环道长度。一共有几种环道长度?

(8) 计算 $\tau_1,\tau_2,\tau_3,\tau_4$ 两两相乘的结果。这 4 个变换中，有哪些是交换的? 哪些不是?

5. 下图是某个群 G 的生成路径图。

(1) 群 G 有几个元素?



(2) 按图解释群 G 是如何生成的？它和 D_8 有何不同？

(3) 我们想研究群中元素 x 的环道。首先，请用 a, b 表示 x。

(4) 在生成路径图中找出表示 x 不断自乘的路径。这条路径什么时候回到 e？

(5) 画出 x 的环道。

(6) 按此方法找出所有群元素的环道，并分类整理。

6. 正四面体是最简单的正多面体。它由 4 个正三角形围成，有 4 个顶点、4 个面、6 条棱。研究其旋转群，即保持正四面体位置形状不变的旋转变换构成的群 A_4。

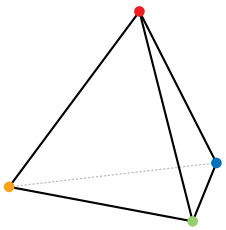


图 4.26: 正四面体

(1) 这些旋转变换都围绕过正四面体中心的轴线旋转。给定顶点，过该顶点和中心的直线，称为（过）该顶点的中线。绕一顶点中线的旋转变换，有几个保持正四面体位置形状不变？如何描述这些旋转变换。

(2) 给定正四面体的一条棱，我们把顶点和这条棱不相关的另一条棱称为它的对棱。对棱中点的连线过正四面体中心，称为对棱中线。正四面体有几条对棱中线？证明：绕任一条对棱中线，有一个旋转变换保持正四面体位置形状不变。

(3) 给正四面体的顶点染色（见上图）。以上提及的 A_4 的元素分别如何变换这些顶点

的颜色? 用 4 元置换表示。

(4) 验证以下等式，并说明它们的含义：

$$(4\,2\,1\,3) = (2\,1\,4\,3) \circ (1\,3\,4\,2) \circ (2\,1\,4\,3)$$
$$(4\,2\,1\,3) = (3\,1\,2\,4) \circ (1\,3\,4\,2) \circ (3\,1\,2\,4)$$

(5) 说明为何 4 元置换中的对换（只交换两个顶点）不能通过旋转得到。

(6) 说明为何 4 元置换中的 4 元轮换（变换所有顶点，环道长度为 4）不能通过旋转得到。

(7) 说明 A_4 一共有几个元素。

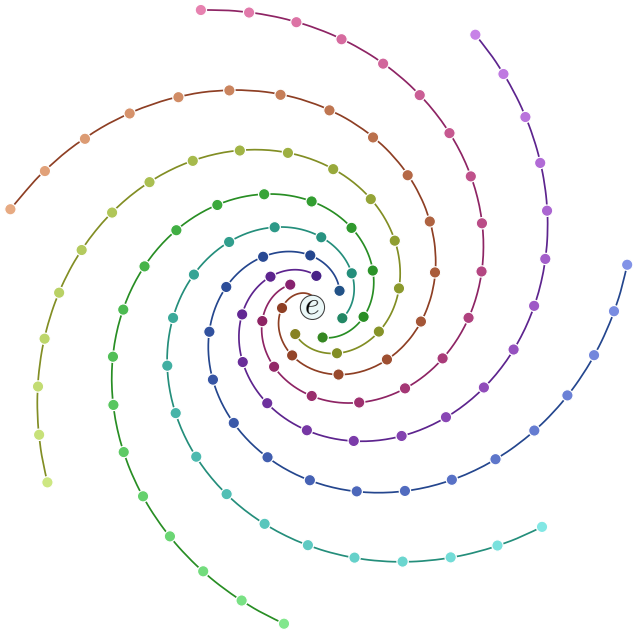
(8) 画出 A_4 的环道图。

(9) 最后研究 A_4 的生成路径图。使用 τ_1, σ_1 作为生成元。我们在第 4 问中已经用 τ_1 和 σ_1 表示了 τ_2。计算 τ_1, σ_1 的各种复合结果，找出用 τ_1 和 σ_1 表示 τ_3, τ_4 的方法。

(10) 从已知能用 τ_1, σ_1 表示的元素出发，不断复合 τ_1，得到用 τ_1 串联 A_4 所有元素的 4 个三元循环。

(11) 寻找用 σ 关联这些三元循环的“通路”。最终画出 A_4 的生成路径图。

第五章　子群



前面我们已经熟悉了群的概念，并了解了一些常见的群。从这一章开始，我们将进入真正的群论学习了。新的概念和术语将不断冒出来，也会越来越抽象。我们将要更多地开动大脑来分析问题。各种图解会帮助我们直观理解这些新概念，但你也需要逐渐学会从代数的角度来思考，熟悉如何摆弄各种等式，理解符号的含义。从这一章开始，我们将把重点放在叙述定理上。首次阅读时，不必纠缠于定理的详细证明，更应该关心整体的想法和思路。

更深入地研究群，就是要回答以下问题：如何描述群的结构？群与群之间的联系如何？我们的思路是“分而合之”：能否把大的群分解为小群的组合，通过研究小群，来理解大群的结构。本章的重点是“分”，不断寻找群里面的更小的群，直到容易理解为止。然后用小群来“分割”大群，剖析它的结构。

5.1 群中之群

我们在前几章已经遇到过“群中之群”的概念。比如环道其实就是群中元素构建的循环群。这说明每个复杂的群里其实都蕴含着更小更简单的群。我们把这个想法推广为：

定义 5.1 子群

如果群 $(G,\cdot)$ 的非空子集 H 关于运算“$\cdot$”也构成群，就说 $(H,\cdot)$ 是 $(G,\cdot)$ 的**子群**，记作 $H \trianglelefteq G$。如果 H 是 G 的真子集，就说说 $(H,\cdot)$ 是 $(G,\cdot)$ 的**真子群**，记作 $H \triangleleft G$。

前一章中提到的，群中元素的环道，显然都是子群。比如 D_3 中的旋转 r 的环道 $\{e, r, r^2\}$ 就是 D_3 的循环子群，记作 $\{e, r, r^2\} \triangleleft \mathsf{D}_3$。它和 C_3 同构。随意一点的话，也可以看作 $\mathsf{C}_3 \triangleleft \mathsf{D}_3$。翻转 s 的环道 $\{e, s\}$ 也是 D_3 的循环子群，记作 $\{e, s\} \triangleleft \mathsf{D}_3$。

一般的群有哪些子群呢？任何群都有幺元 e，一元群 $\{e\}$ 是该群的子群。另外，任何群总是自己的子群，但不是真子群。

再来看一些别的例子。考虑群 $\mathsf{C}_3 \times \mathsf{C}_2$：

$$\mathsf{C}_3 \times \mathsf{C}_2 \;=\; \{(x, y) \mid x \in \mathsf{C}_3,\, y \in \mathsf{C}_2\}$$

它是循环群 $\mathsf{C}_3 = \{e, a, a^2\}$ 和 $\mathsf{C}_2 = \{e, b\}$ 的架积，内含 6 个元素，分别是：

$$(e,e),\;\; (e,b),\;\; (a,e),\;\; (a,b),\;\; (a^2,e),\;\; (a^2,b)$$

可以验证：$\{(e,e),\ (a,e),\ (a^2,e)\}$ 构成群，$\{(e,e),\ (e,b)\}$ 也构成群。因此我们得到 $\mathsf{C}_3 \times \mathsf{C}_2$ 的两个子群。观察还能发现：这两个群分别同构于 C_3 和 C_2。不严格地说，C_3 和 C_2 是 $\mathsf{C}_3 \times \mathsf{C}_2$ 的两个子群。

类似地还有矩群 $\mathsf{J}_4 = \mathsf{C}_2 \times \mathsf{C}_2$，它有 $\{e, p\}$、$\{e, q\}$ 和 $\{e, pq\}$ 三个子群。

上一章我们提到，任何群都同构于置换构成的群。集合上置换构成的群，就是该集合上全体置换构成的全置换群的子群。因此，置换群定理也可以叙述为：任何群都同构于全置换群的子群。

我们自然会问：怎么判别群的子集是不是它的子群呢？严格来说，我们可以按照群的定义对子集进行验证。满足群的定义的子集，自然就是子群。不过，我们希望有更便捷的方法来识别。子集要成为子群，首先必须有幺元；其次，运算的结果不能“跑出去”，

必须还在子集里。这两点满足后，由于子集的元素是群元素，所以自然遵循结合律。最后还要验证逆元也在子集里。把这些要点再浓缩一下，就变成：

定理 5.1 子群的判别方法

设 H 是群 $(G,\cdot)$ 的非空子集。如果 $\forall a,b\in H$，$ab^{-1}\in H$，那么 $H\trianglelefteq G$。

这个方法的巧妙之处在于：首先取 $a=b$，就得到 $e=ab^{-1}\in H$；接着令 $a=e$，就得到 $\forall b,\ b^{-1}=eb^{-1}\in H$；最后，$\forall a,b\in H$，由于 $b^{-1}\in H$，$ab=a\left(b^{-1}\right)^{-1}\in H$。于是，之前说的三个要点都满足了。

我们用这个方法来分析一个更抽象的例子：设有 n 个编号小球，n 元置换将它们重新排列。考虑保持 1 号球位置不变的所有置换的集合 K。K 是否是 n 元全置换群 S_n 的子群？

首先，恒等变换 $e\in K$，所以 K 不是空集。按照以上结论，我们只需要验证：

$$\forall\, a,b\,\in\,K,\quad ab^{-1}\,\in\,K.$$

首先，两个不改变 1 号球位置的置换复合，仍然不改变 1 号球位置。其次，不改变 1 号球位置的置换，如果要恢复原状，自然也不涉及 1 号球。因此它的逆变换也在 K 中。所以 $ab^{-1}\in K$。这就说明 K 是子群。当然，不改变 1 号球位置的 n 元置换，实际上就是关于 2 到 n 号球的 $n-1$ 元置换。所以 K 其实就是 S_{n-1}。我们实际上证明了 $\mathsf{S}_{n-1}\trianglelefteq\mathsf{S}_n$。

环道给我们提供了寻找子群的灵感。给定群 G 中的几个元素 $x_1,x_2,\cdots,x_n\in G$，把它们任意运算的结果都放在一起，是否就是子群呢？首先，我们必须定义“任意运算的结果”。即便我们的思路是放任这些元素随意组合，还是要有底线：必须是有限次运算的结果。毕竟我们没有定义过“无限次运算”。也就是说，任意运算结果构成的集合 S 长这个样子：

$$S\ =\ \left\{a_1^{i_1}a_2^{i_2}\cdots a_m^{i_m}\,\middle|\,m\in\mathbb{N},\,i_1,i_2,\cdots,i_m\in\mathbb{Z},\,a_1,a_2,\cdots,a_m\in\{x_1,x_2,\cdots,x_n\}\right\}.$$

按照 5.1来判定，要说明 $a_1^{i_1}a_2^{i_2}\cdots a_m^{i_m}$ 乘 $b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}$ 逆元的积在 S 里。首先，$b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}$ 的逆元是 $b_k^{-j_k}\cdots b_2^{-j_2}b_1^{-j_1}$。于是乘积为 $a_1^{i_1}a_2^{i_2}\cdots a_m^{i_m}b_k^{-j_k}\cdots b_2^{-j_2}b_1^{-j_1}$。这确实也是有限次运算的结果，因此在 S 里。这就说明 S 是子群。我们称其为由 $x_1,x_2,\cdots,x_n$ **生成的子群**，记为 $\langle x_1,x_2,\cdots,x_n\rangle$，如果记 $X=\{x_1,x_2,\cdots,x_n\}$，则生成的子群也记作 $\langle X\rangle$。X 中的元素称为**生成元**。单个元素生成的子群就是循环子群。多个元素生成的子群则更为复杂。

用生成子群的观念来看 D_3，我们可以看到，D_3 就是由逆时针旋转 120° 的变换 r 和翻转变换 s 生成的。生成路径图清楚地说明了这一点。从 r 开始可以得到三个变换，就是作为 r 环道的循环子群 $\{e, r, r^2\}$，而加入 s 以后，再次生成了三个变换 s, rs, r^2s，构成了整个 D_3：$\mathsf{D}_3 = \langle r, s\rangle$。

一般来说，映轮群 D_n 也是按照这种方式生成的：逆时针旋转 $\frac{360^\circ}{n}$ 的变换 r 生成了 n 个元素的循环子群，然后加入翻转变换 s，得到整个 D_n：$\mathsf{D}_n = \langle r, s\rangle$。

5.2 往集

我们已经知道，群的子集并不总是它的子群。比如 D_3 的子集 $\{s, rs, r^2s\}$ 就不是它的子群。不过，$\{s, rs, r^2s\}$ 作为子群 $\{e, r, r^2\}$ 的“映照”，不同于随意取的子集。我们可以将它看作是子群 $\{e, r, r^2\}$“往 s 走之后的结果”，即把每个元素都乘以 s。由于 $s^2 = e$，再“往 s 走”会回到原本子群 $\{e, r, r^2\}$。所以不断“往 s 走”能得到两个子集，分别是子群 $\{e, r, r^2\}$，以及 $\{s, rs, r^2s\}$。

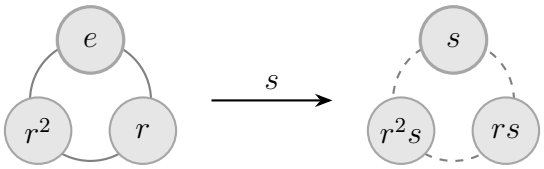


图 5.1: $\{e, r, r^2\}$ 的所有元素“往 s 走”

$\{s, rs, r^2s\}$ 和 $\{e, r, r^2\}$“一样大”，都有三个元素，拼起来，就是整个 D_3。

另一个例子是子群 $\{e, s\}$“往 r 走之后的结果”：$\{r, sr\}$ 和 $\{r^2, sr^2\}$。由于 r 的环道更长，所以“往 r 走”可以得到三个子集。$\{r, sr\}$、$\{r^2, sr^2\}$ 都和 $\{e, s\}$ 一样大，而且三者拼起来就是整个 D_3。

要注意的是：当我们说“把每个元素都乘以 s”时，并没有区分是左乘还是右乘。实际上这是有区别的。“往左走”和“往右走”，结果不一定一样。对于 $\{e, r, r^2\}$ 来说，“沿 s 往左走”和“沿 s 往右走”的结果都是 $\{s, rs, r^2s\}$。对于 $\{e, s\}$ 来说，“沿 r 往左走”（用 r 左乘每个元素）得到 $\{r, rs\}$、$\{r^2, r^2s\}$，“沿 r 往右走”（用 r 右乘每个元素）则得到 $\{r, sr\}$、$\{r^2, sr^2\}$。我们知道 $sr \neq rs$：$sr = r^2s$，$rs = sr^2$。所以，“沿 r 往左走”得到的三个子集是 $\{e, s\}$、$\{r, rs\}$、$\{r^2, sr\}$，“沿 r 往右走”得到的三个子集则是 $\{e, s\}$、$\{r, sr\}$、$\{r^2, rs\}$。它们构成 D_3 的两种不同的划分方法。

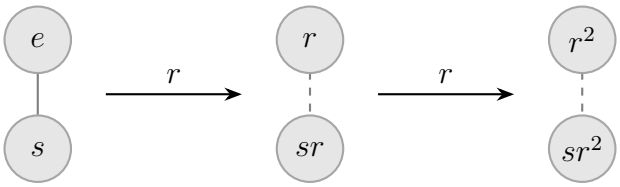


图 5.2: $\{e, s\}$“沿 r 往右走”

无论是“往左走”还是“往右走”，都能不重不漏地划分整个群。这个方法可以帮助我们理解子群和群的关系。我们设想：是否对任何群，总能通过不断选取子群以外的元素，复刻出和子群一样大小的子集，然后拼出整个群？这样，是否就可以用子群为“单位”来理解群呢？通过理解子群，就能更好地理解整个群了。

给定子群 $H \trianglelefteq G$ 和 $a \in G$，我们把通过以上方法得到的子集称为子群 H（关于 a）的**往集**。如果 a 乘在 H 中元素的左边，就称为**左往集**，记为 aH；如果 a 乘在 H 中元素的右边，就称为**右往集**，记为 Ha：

$$aH = \{ah \mid h \in H\}, \qquad Ha = \{ha \mid h \in H\}.$$

如果 $a \in H$，那么根据子群的性质，aH 和 Ha 都是 H。如果 $a \notin H$，那么 aH 和 Ha 都不是 H。事实上，这时 aH（或 Ha）和 H 没有共同元素。

命题 5.1

子群 H 的任何往集要么是 H，要么和 H 完全不相交。

证明：首先验证 aH 的情况。假设 $a \notin H$。$\forall b \in aH$，按定义有 $h \in H$ 使得 $b = ah$，即 $bh^{-1} = ahh^{-1} = a$。反设 $b \in H$，那么 $a = bh^{-1} \in H$，和 $a \notin H$ 矛盾！所以，$b \notin H$。这就说明 aH 和 H 没有共同元素。Ha 的情况类似。 □

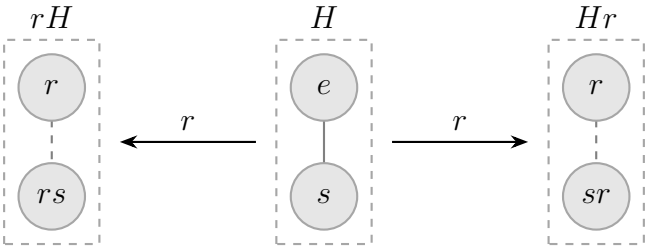


图 5.3: $H = \{e, s\}$ 沿 r 的左往集 rH 和右往集 Hr

进一步，我们还可以讨论任何两个往集之间的关系。给定左往集 aH、bH。如果它们俩有共同元素，比如有 $h_1, h_2 \in H$ 使得 $ah_1 = bh_2$，那么 $a = bh_2h_1^{-1}$。$h_2h_1^{-1} \in H$，所

以 $a \in bH$。于是：

$$\forall h \in H,\ ah = bh_2h_1^{-1}h \in bH.$$

这说明 $aH \subseteq bH$。同理，可以说明 $bH \subseteq aH$。也就是说，$aH = bH$。这个结论说明：

命题 5.2

子群 H 的两个左往集（或两个右往集）要么完全不相交，要么是同一个集合。

要注意的是：左往集和右往集可以相交而不是同一个集合。比如我们已经验证过的：$\{e, s\} \trianglelefteq \mathsf{D}_3$ 的左往集 $\{r, rs\}$ 和右往集 $\{r, sr\}$ 有共同元素 r，但 $rs \neq sr$，因此不是同一个集合。

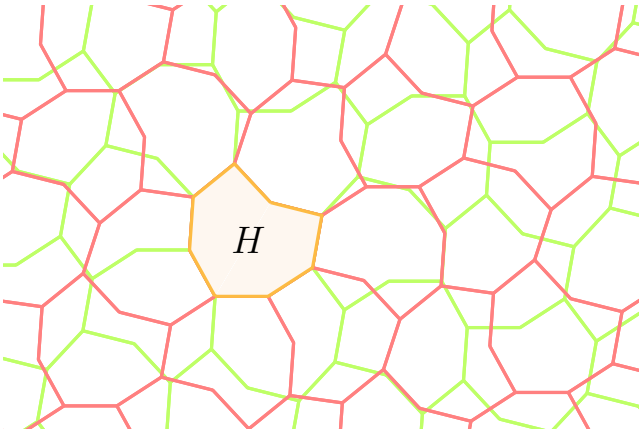


图 5.4: 子群的左往集和右往集，往往不重合

如果 $b \in aH$，那么 bH 和 aH 相交，因此 $bH = aH$。反之，如果 $b \notin aH$，那么 bH 和 aH 不相交。因此，考虑有限群 G 的子群 $H \trianglelefteq G$ 所有左往集的集合：

$$\{aH \mid a \in G\}.$$

它大概不会有 G 那么多元素。

5.3 往集定理

子群有几个往集呢？以左往集为例，按之前 D_3 例子里的方法穷举：

1. 从 H 出发：H 是自己的左往集。
2. 把 H 视为“已知范围”，在 H 之外找 $a \in G$，则 aH 是另一个左往集。

3. 把 $H \cup aH$ 视为“已知范围”，在 $H \cup aH$ 之外再找 $b \in G$，则 bH 又是一个不同的左往集。
4. 以此类推，不断把新找到的左往集并入“已知范围”。由于“已知范围”不断扩大，总有无法再扩大的时候。这时统计累次得到的左往集即可。

那么，到底有几个左往集呢？首先来证明之前已经观察到的现象：

定理 5.2

> 子群 H 的往集和它一样大。

证明：设 aH 是子群 H 的左往集。考虑映射：

$$\begin{aligned} f: \quad H &\longrightarrow aH \\ h &\longmapsto ah. \end{aligned}$$

f 显然是满射。而如果 $ah_1 = ah_2$，那么两边左乘 a^{-1} 就得到 $h_1 = h_2$。因此 f 是单射。于是 f 是双射。这说明 aH 和 H 一样大。同理，Ha 也和 H 一样大。 □

因此，按以上的方法不断找 H 的往集，就是从 G 里不断“挖出”一块块和 H 一样大的子集。注意要一直往同一个方向“挖”。假设“挖”了 k 次之后，不再有剩下的元素了，那么，就有 k 个不同的往集。而这时我们发现：G 的元素个数就是 H 的 k 倍。也就是说，往集的个数可以用群和子群的元素个数相除得到，我们把这个结论记为：

定理 5.3 往集定理

> 有限群 G 的子群 H 的左往集个数（或右往集个数）乘以 H 的元素个数，就是 G 的元素个数。

我们还得到一个附带的结果：

定理 5.4 群势定理

> 有限群的元素个数是其子群的倍数。子群的势整除群的势。

群 G 的元素个数记为 $|G|$，于是以上结果可以写成：$|H|$ 整除 $|G|$。

这个结果说明：用往集“除”群，不会有整数除法那样“除不尽”的情况。我们可以这样理解：穷举时，如果某次“已知范围”外剩下某个元素 a，则考虑 aH（这里假设是左往集的情况，右往集则考虑 Ha）。aH 和“已知范围”里的往集必然都不相交，否

则就会等于某个往集。因此，要么不剩下任何元素，要么剩下的元素能够凑成一个往集，和其他往集一样大小。这就说明了：不会有整数除法那样的“除不尽的余数”问题。

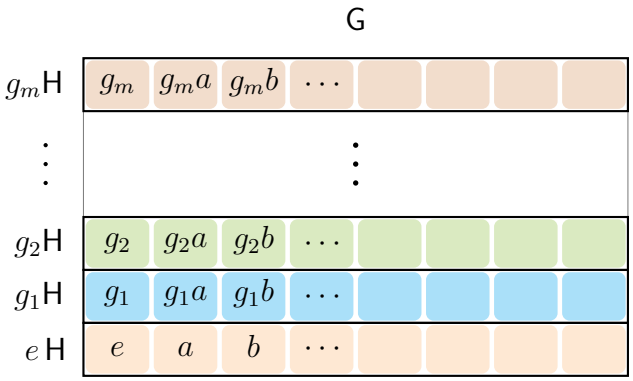


图 5.5: 可以想象把子群元素和往集元素整齐地层层排列，构成整个群，没有“散乱”的部分。任何元素都归属于某一层，任一层都能和底层（子群自身）排列对齐。

往集定理（群势定理）可以帮助理解子群的性质。下面来分析常见群的子群性质。

5.3.1 循环群的子群

循环群 C_n 有 n 个元素，根据群势定理，它的任何子群 H 的势必然是 n 的因数。设 C_n 的生成元为 a，那么 H 的元素都能写成 a^k 的形式，其中 $1 \leqslant k \leqslant n$ 是正整数。

我们把 a^k 的 k 称为循环群元素的**指数**。考虑 H 中指数最小的元素，记为 a^i。对 H 中其他元素 a^k，由子群的性质可知，$a^{k-i}, a^{k-2i}, \cdots$ 都在 H 中。其中指数没有比 i 更小的正整数，说明 k 是 i 的倍数。也就是说，H 只由 $a^i, a^{2i}, \cdots$ 形式的元素构成。注意 $a^n = e \in H$，所以 n 也是 i 的倍数。

考虑 a^i 的环道：$a^i, a^{2i}, \cdots, a^n = e$。其中元素两两不同，都在 H 中。它是 H 的子群。另一方面，H 中元素的指数 k（$1 \leqslant k \leqslant n$）都是 i 的倍数，因而总在 a^i 的环道里。也就是说，H 就是 a^i 的环道：

$$H = \langle a^i \rangle = \{a^i, a^{2i}, \cdots, a^n = e\}.$$

设 H 有 m 个元素，则 $n = im$。于是 i 也是 n 的因数。也就是说，循环群 C_n 的任何子群都是循环群，其生成元 $b = a^i$ 是 C_n 的生成元 a 的乘方，其指数 i 就是群势 n 除以子群势 m 的商。我们也说 i 是**循环群子群的指数**。

反过来，只要正整数 m 整除 n，记 $n = im$，那么 $\{a^i, a^{2i}, \cdots, a^n = e\}$ 就是 C_n 的子群。

我们可以用钟表作为例子。钟面上有 12 个数字，每个数字看作一个状态，那么每过一个小时，钟表的时针“转一个字”（比如从 1 转到 2），这个变换就生成一个有 12 元素的循环群：转 12 次就是绕钟面一周，回到原来的刻度。它同构于循环群 C_{12}。而这种转一周的方法，还可以是每次“转 2 个字”、“转 3 个字”、“转 4 个字”、“转 6 个字”。这些转法就对应着 C_{12} 的真子群。这些子群的生成元的指数是 12 的真因数。

5.3.2 映轮群的子群

再来看映轮群。群 D_3 有 6 个元素，因此，D_3 的子群，只可能是一元群、二元群、三元群和六元群。一元群 $\{e\}$ 和六元群（D_3 自身）都是显然的。二元群为 $\{e, s\}$、$\{e, rs\}$、$\{e, r^2s\}$，三元群为 $\{e, r, r^2\}$。这就是 D_3 元素的环道。除此以外，e 和 r、r^2 无法组成二元群，e 和 s, rs, r^2s 中任两个无法组成三元群。因此，以上即为群 D_3 的所有子群。

类似可以研究群 D_n 的子群。D_n 有 $2n$ 个元素，其中所有的 n 旋转构成环道，由逆时针旋转 $\frac{360^\circ}{n}$ 的旋转 r 生成，另外 n 个元素为翻转变换。按照群势定理，它的子群的势整除 $2n$，比如是一元群、二元群、n 元群、$2n$ 元群。一元群 $\{e\}$ 和 $2n$ 元群（D_n 自身）都是显然的。二元群包括翻转变换的环道，n 元群则主要包括 r 的环道。此外，作为循环群，只要正整数 m 整除 n，那么就有子群 $\langle r^{\frac{n}{m}} \rangle$。最后，$r^{\frac{n}{m}}$ 和某些翻转变换 s 能生成 $2m$ 个元素的子群。

以上分析中，我们发现，并没有很好的办法来找出给定大小的子群。群势定理告诉我们子群的势整除群势。但反过来，给定群势的某个因数 m，群有没有 m 元子群呢？有几个呢？这些问题都是群势定理回答不了的。一般来说，给定群势的某个因数 m，群未必有 m 元子群。那么，对怎样的群和怎样的因数 m，群一定有 m 元子群呢？这个问题至今仍然未完全解决。解决它需要对群的结构做更深入的了解、更本质的刻画。正式的群论教材会对群本身的结构和性质进行更多的探讨，给出这个问题的部分回答。本书不作涉及。

本章小结

本章开始探讨群的内部结构。主要知识点包括：

- **子群**：群 G 的非空子集 H 如果在群的运算下也构成一个群，就说它是 G 的子群，记为 $H \trianglelefteq G$。
- **子群的判定方法**：如果群 G 的非空子集 H 里，任何两个元素 a, b 都满足 $ab^{-1} \in H$，那么 H 就是 G 的子群。
- **生成子群**：群的某些元素 $x_1, x_2, \cdots$ 按“列出它们所有有限乘积”的方法，可以构成子群，称为 $x_1, x_2, \cdots$ 生成的子群，记为 $\langle x_1, x_2, \cdots \rangle$。
- **往集**：用子群的元素去乘群中的某个元素所得到的集合。往集将群划分为大小相等、互不相交的子集。左往集和右往集往往不重合，给出群的不同分划。
- **往集定理**：有限群的子群的往集个数，乘以子群的势，等于群势。
- **群势定理**：往集定理的推论，说明有限群的势是子群的势的倍数，子群的势是它的因数。
- **循环群的子群**：$\mathsf{C}_n = \langle a \rangle$ 的子群总是循环群，其 m 元子群为 $\langle a^{\frac{n}{m}} \rangle$。

5.4 习题

1. 以下关于子群的说法，哪些是正确的?

   (1) C_3 同构于 D_3 的子群。

   (2) D_3 同构于 S_3 的子群。

   (3) C_3 同构于 C_6 的子群。

   (4) C_3 同构于 C_8 的子群。

   (5) C_3 同构于 $\mathsf{C}_3 \times \mathsf{C}_8$ 的子群。

   (6) C_6 同构于 $\mathsf{C}_3 \times \mathsf{C}_4$ 的子群。

   (7) $n\mathbb{Z}$ 同构于 $\mathbb{Z} \times \mathbb{Z}$ 的子群。

   (8) $\mathbb{Z}_n$ 同构于 $\mathbb{Z}$ 的子群。

2. 证明：两个子群的交集仍然是子群。两个子群的并集仍然是子群吗?

3. 设 H 是群 G 的子群，证明：$\forall g \in H$，$gHg^{-1} = \{ghg^{-1} \,|\, h \in H\}$ 也是 G 的子群。

4. 考虑正四面体的旋转群 A_4（见第四章练习题 6)。

   (1) 说明 A_4 同构于什么样的 4 元置换群（可使用第四章练习题 6 的结论)?

   (2) 说明 A_4 同构于 S_4 的子群。

   (3) 在 A_4 中找一个子群，使得它同构于 J_4。说明为什么两者同构。

   (4) 说明为什么 A_4 没有同构于 C_6 的子群。

   (5) 说明为什么 A_4 没有同构于 D_3 的子群。

5. 以下群的子集生成的子群是怎样的?

(1) $\{\overline{2},\overline{3}\}\subset\mathbb{Z}_{12}$

(2) $\{\overline{4},\overline{6}\}\subset\mathbb{Z}_{12}$

(3) $\{\overline{6},\overline{10}\}\subset\mathbb{Z}_{18}$

(4) $\{\overline{18},\overline{30}\}\subset\mathbb{Z}_{36}$

(4) $\{8,12\}\subset 2\mathbb{Z}$

(5) $\{24,42\}\subset\mathbb{Z}$

(6) $\{18,39,66\}\subset\mathbb{Z}$

(7) $\{r^2,s\}\subset\mathsf{D}_4$

6. 证明：$n>2$ 时，存在一个 $2n$ 元的群，它由两个元素生成，且这两个元素的阶都是 2。

7. 证明：D_4 同构于 S_4 的子群。

8. 找出以下子群除自身以外的往集。左右往集相等吗?

(1) $6\mathbb{Z}\lhd\mathbb{Z}$

(2) $6\mathbb{Z}\lhd 2\mathbb{Z}$

(3) $\langle\overline{3}\rangle\lhd\mathbb{Z}_{12}$

(4) $\langle r^2\rangle\lhd\mathsf{D}_4=\langle r,s\rangle$，其中 $sr=r^3s$。

9. 设群 G 有子群 H。如果有 $a,b\in G$，使得 $aH=bH$，判断以下说法是否正确：

(1) $Ha=Hb$。

(2) $Ha^{-1}=Hb^{-1}$。

(3) $a^2H=b^2H$。

10. 设 p 是素数。证明：p 元群是循环群。

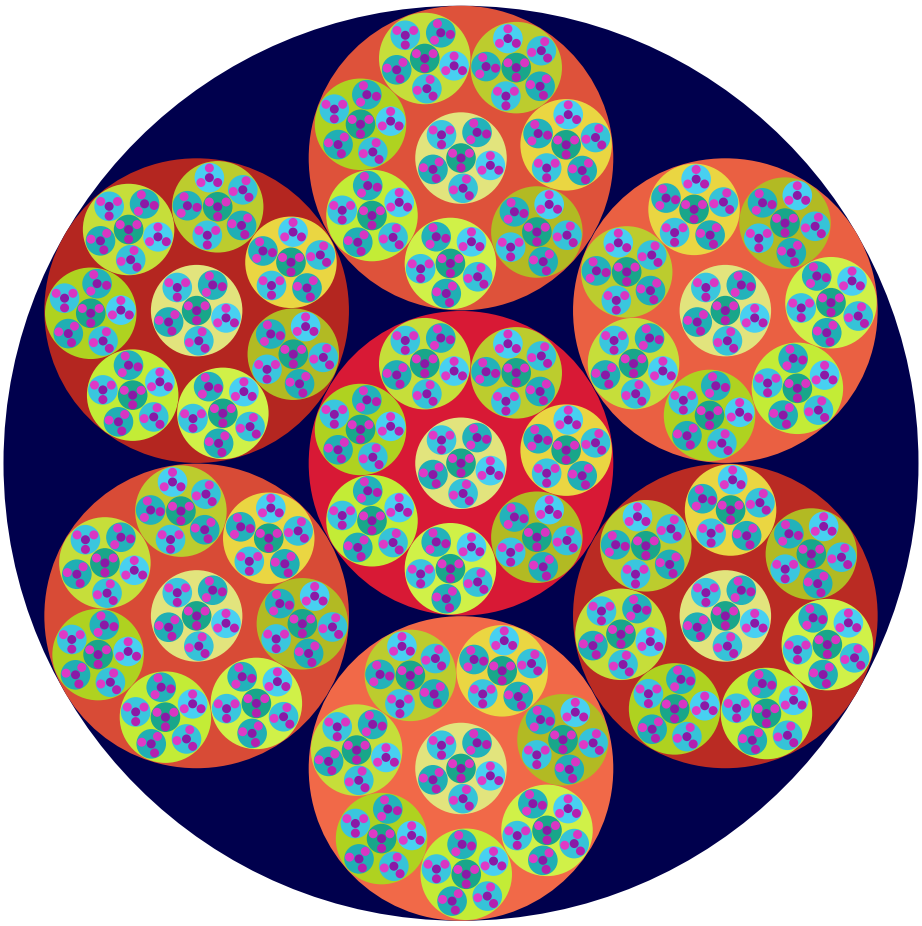
11. S_X 是集合 X 的对称群。

(1) 给定 $a\in X$，考虑集合 $H_a=\{\sigma\in\mathsf{S}_X\,|\,\sigma(a)=a\}$。证明 H_a 是 S_X 的子群（注意这里 X 可能是无限集合）。

(2) 设 $a\neq b\in X$，考虑集合 $H_a^b=\{\sigma\in\mathsf{S}_X\,|\,\sigma(a)=b\}$。$H_a^b$ 是 S_X 的子群吗?

(3) H_a 和 H_a^b 有什么关系? 具体说明。

第六章　商群与同态



这一章是对群自身结构的更深入探讨。这个方向是研究群论的必经之路，主要回答“群本身到底长什么样”的问题。本章涉及的内容更加抽象复杂，偏向对代数结构的审视。不过，如果你更关心如何使用群来分析有对称性的对象，那么可以只了解本章涉及的主要概念，而把精力放在下一章。

上一章提到，通过子群，我们把群划分成相同大小的集合。而接下来我们会看到，在满足一定的条件时，这些集合会构成新的群。新的群和原来的群能建立深刻的联系。为此，我们引入群同态的概念，说明群与群之间的关系，并最终给出一个美妙的结论。

6.1 往合子群和商群

通过子群，我们把群划分成一个个往集。接下来我们自然会想：要是把这些往集看作一个个元素，是否也能构成群呢？观察映轮群的乘法表时，我们留意到，表格可以分为“田”字四块，而这四块的关系和 C_2 的乘法表一致。现在来看，这是因为我们把子群 $\{e, r, \cdots, r^{n-1}\} \triangleleft \mathsf{D}_n$ 的元素归为一组，把它的往集归为另一组，才观察到这个规律。

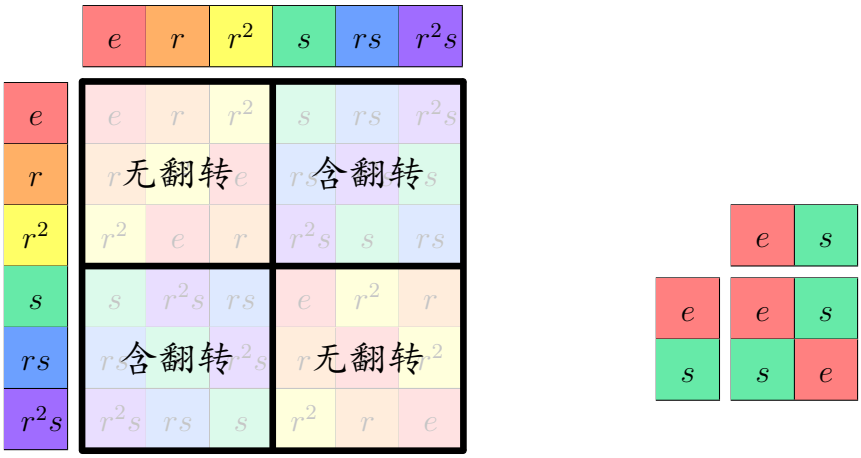


图 6.1: D_3 乘法表，行头、列头里，子群 $\{e, r, r^2\}$ 与其往集 $\{s, rs, r^2s\}$ 分开排列

这个结果十分美妙：我们把映轮群 D_n 分成四块，单块内部构造是循环群 C_n 或其往集，而“大尺度”上的构造是翻转构成的群 C_2。它把 D_n 拆分为两个层次，各自说明群的一个特征。我们希望对其他群和子群，也有这么美妙的规律。能够实现吗？

让我们尝试对 D_3 的另一个子群 $\{e, s\}$ 进行类似构造。比如，我们把乘法表的表头按 $\{e, s\}$ 以及它的两个左往集 $\{r, rs\}$、$\{r^2, r^2s\}$ 来分组。我们会发现，如果把 D_3 的乘法表按照这样的方法“分块”，就达不到之前按 $\{e, r, r^2\}$ 及其往集分组的效果。因为不是每一“块”的内容都能“同心协力”，总会有元素“跑到别处”。比如，取往集 $\{r, rs\}$ 中两个元素相乘，既会得到 e 和 s，也会得到 r^2 和 r^2s。这样就无法明确地定义各块之间的运算了。

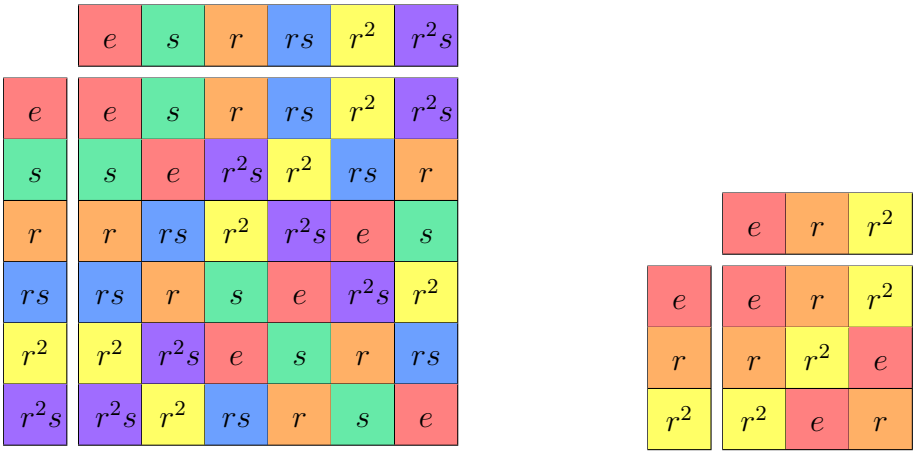


图 6.2: D_3 乘法表的另一种排列（e, s, r, rs, r^2, r^2s）与 C_3 乘法表

用严格的语言来说，前面 D_3 到 C_2 的对应成立，来自子群 $H = \{e, r, r^2\}$ 与其往集 $sH = \{s, rs, r^2s\}$ 之间的关系：

$$\begin{aligned}
H \cdot H &= (eH) \cdot (eH) = (e \cdot e)H = eH &&= H, \\
H \cdot (sH) &= (eH) \cdot (sH) = (e \cdot s)H &&= sH, \\
(sH) \cdot H &= (sH) \cdot (eH) = (s \cdot e)H &&= sH, \\
(sH) \cdot (sH) &= (sH) \cdot (sH) = (s \cdot s)H = eH &&= H,
\end{aligned}$$

其中“$\cdot$”并非群元素的乘法，定义为：

$$\forall\, S_1, S_2 \subseteq G, \quad S_1 \cdot S_2 = \{a \cdot b \mid a \in S_1,\ b \in S_2\}.$$

这样定义的乘法总能得到一个集合，但不一定是往集。我们想要的结果：H 中元素乘以 sH 中元素，总在 sH 中；sH 中元素乘以 sH 中元素，总在 H 中，等等。而子群 $K = \{e, s\}$ 与其往集 $rK = \{r, rs\}$、$r^2K = \{r^2, r^2s\}$ 之间就做不到这点。我们可以从乘法表看出，rK 中元素乘以 rK 中元素，不总在任何一个往集中。

另一方面，我们可以理解：$(aH) \cdot (bH) = cH$，还希望“$\cdot$”和原本的群运算有某种关联（这里集合之间的“$\cdot$”并非原本的群运算），这种要求并不是平凡的。需要设置某个条件，才能让这个“愿望成真”。

计算 $(aH) \cdot (bH)$ 的具体元素：

$$\forall\, h_1, h_2 \in H, \quad (ah_1) \cdot (bh_2) = ah_1bh_2.$$

在前面的例子里，我们希望它属于 $(a\cdot b)H$，即能写成 abh 的形式。困难在于 h_1b 的顺序不是我们期望的：它属于 Hb。如果有某个 $h\in H$，使得 $h_1b=bh$，那么：

$$(ah_1)\cdot(bh_2)=a(h_1b)h_2=abhh_2\in(a\cdot b)H.$$

也就是说，如果 Hb 中的元素其实就是 bH 中的元素，就能定义 $(aH)\cdot(bH)=(a\cdot b)H$。实际上，前面 D_3 到 C_2 的对应里确实有这样的现象：我们选择了子群 $H=\{e,r,r^2\}$，它的左往集和右往集都是 $\{s,rs,r^2s\}$。因此，我们猜想：

命题 6.1

> 给定群 G 的子群 H，如果 $\forall a\in G, aH=Ha$，那么 $\forall\, a,b\in G, (aH)\cdot(bH)=(a\cdot b)H$。

下面来证明它：

证明：$\forall\, a,b\in G$，计算 $(aH)\cdot(bH)$ 的具体元素：

$$\forall\, h_1,h_2\in H,\quad (ah_1)\cdot(bh_2)=ah_1bh_2.$$

由于 $bH=Hb$，有 $h\in H$ 使得 $h_1b=bh$，因此

$$(ah_1)\cdot(bh_2)=a(h_1b)h_2=abhh_2\in(a\cdot b)H.$$

这说明 $(aH)\cdot(bH)\subseteq(a\cdot b)H$。

另一方面，由于 $bH=Hb$，$\forall\, h\in H$，有 $g\in H$ 使得 $bh=gb$，所以

$$abh=agb=(ag)(be)\in(aH)\cdot(bH).$$

这说明 $(a\cdot b)H\subseteq(aH)\cdot(bH)$。两边集合互相包含，因此相等：

$$(aH)\cdot(bH)=(a\cdot b)H$$

□

直观来说，子群 H 的左往集和右往集合而为一，沿着一个元素 a 不再有“往左走”和“往右走”的区别，只有“往 a 走”。我们把这样的子群称为**往合子群**。

定义 6.1 往合子群

若子群 $H \trianglelefteq G$ 使得 $\forall\, a \in G$，$aH = Ha$，则称其为 G 的**往合子群**，记为 $H \trianglelefteq G$。若 $H \triangleleft G$，则记为 $H \triangleleft G$。

一元群 $\{e\}$ 和 G 自身显然都是其往合子群。另外，往合子群成立的条件可以等价地写为 $aHa^{-1} = H$。其中 aHa^{-1} 定义为：

$$aHa^{-1} \;=\; \{aha^{-1} \mid h \in H\}.$$

读者可以自行验证两种写法等价。

如果 H 是群 G 的往合子群，那么其往集构成以下关系：

$$\forall\, a, b \in G, \quad (aH) \cdot (bH) = (a \cdot b)H.$$

由于等式右侧的 $\cdot$ 就是群运算，不难验证，H 的往集的集合：

$$\{aH \mid a \in G\} = \{Ha \mid a \in G\}$$

关于往集之间的 $\cdot$ 运算构成群：

1. 运算 $(aH) \cdot (bH) = (a \cdot b)H$ 契义，且在往集集合中封闭。
2. 它自然继承了群运算的性质：满足结合律、有幺元（eH 是幺元）、有逆元（$a^{-1}H$ 是 aH 的逆元）。

我们把这个群称为 H 除 G 得到的**商群**，记为 $G\!\!\not\!/ H$。

注意：并不是任何子群都能除 G。这里并没有整数除法的“除不尽”的概念。要么子群是往合子群，能除 G 并得到商群；要么子群不是往合子群，无法定义“除 G”这件事，至多说得到若干往集。

根据往集定理，有限群的往合子群、商群的元素个数满足以下关系：

$$\left|G\!\!\not\!/ H\right| \cdot |H| \;=\; |G|.$$

在前面的例子里，$H = \{e, r, r^2\}$ 是 D_3 的往合子群，它除 D_3 得到一个二元群：$\{H, sH\}$，同构于 C_2。$K = \{e, s\}$ 不是 D_3 的往合子群，它无法除 D_3。

什么样的子群是往合子群呢？容易发现，只要 G 是交换群，那么 $\forall\, H \trianglelefteq G$，总有：

$$\forall\, a \in G, \quad aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha.$$

也就是说，**交换群的任何子群都是往合子群**。

要注意的是：往合子群与商群的概念并不只对有限群成立。典型的例子是整数集 $\mathbb{Z}$ 作为加法群的子群。$(\mathbb{Z}, +)$ 是交换群，所以其任何子群都是往合子群。具体来看 $(\mathbb{Z}, +)$ 的子群长什么样子：

设 H 为 $(\mathbb{Z}, +)$ 的任何子群，且不是平凡的一元群 $\{0\}$，则 H 中必有最小的正整数 a。$\forall h \in H$，考虑 h 对 a 的带余除法：

$$h = q \cdot a + r.$$

其中 q, r 是整数，余数 r 满足 $0 \leqslant r < a$。根据群的性质，$r = h + q \cdot (-a) \in H$，但按定义 a 是 H 中最小正整数，因此 $r = 0$。这说明 H 中的元素都是 a 的倍数，于是 H 可以写成 $a\mathbb{Z}$[①]：

$$a\mathbb{Z} = \{a \cdot n \mid n \in \mathbb{Z}\}.$$

注意到我们可以定义 $\{0\} = \{0 \cdot n \mid n \in \mathbb{Z}\} = 0\mathbb{Z}$。换句话说，$(\mathbb{Z}, +)$ 的所有子群都可以写为 $a\mathbb{Z}$ 的形式，其中 a 是整数。

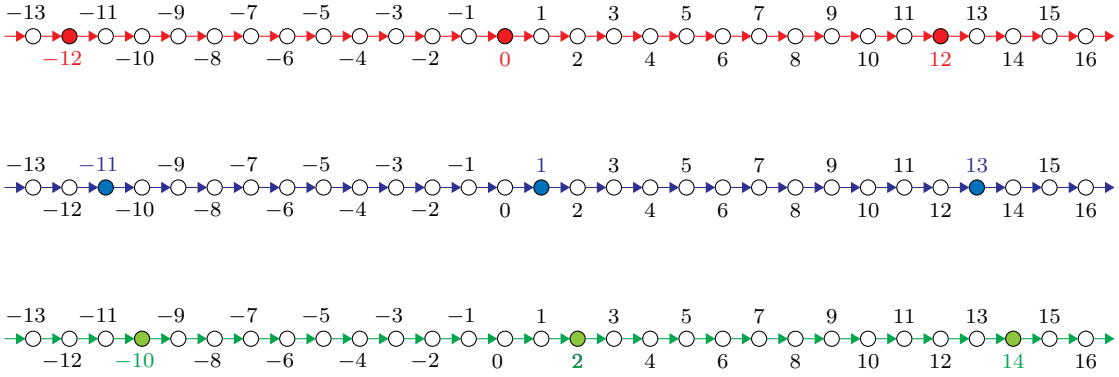


图 6.3: $12\mathbb{Z}$ 的往集举例。其他往集也可以类似画出。这些往集就是模 12 同余的集合。

我们可以验证 $a\mathbb{Z}$ 的左往集总是右往集。

$$\forall\, m \in \mathbb{Z}, \quad m + (a\mathbb{Z}) = \{m + (a \cdot n) \mid n \in Z\} = \{(a \cdot n) + m \mid n \in Z\} = (a\mathbb{Z}) + m.$$

可以看到，$a\mathbb{Z}$ 的往集就是所有模 a 同余的整数的集合。这让我们猜出：a 为正整数时，$a\mathbb{Z}$ 除 $\mathbb{Z}$ 的商群就是模 a 的同余类构成的加法群：

$$\mathbb{Z}/a\mathbb{Z} = \{m + a\mathbb{Z} \mid m \in \mathbb{Z}\} = \{\overline{m} \mid 0 \leqslant m < a, m \in \mathbb{Z}\} = \mathbb{Z}_a.$$

[①]当然，也可以写为 $\mathbb{Z}a$。由于整数乘法可交换，两者相同。不过这是整数乘法的性质，不要与我们在讨论的加法混淆了。

方便起见，在不至于混淆的情况下，我们也可以直接用 $0, 1, \cdots, a-1$ 来指代模 a 的同余类。

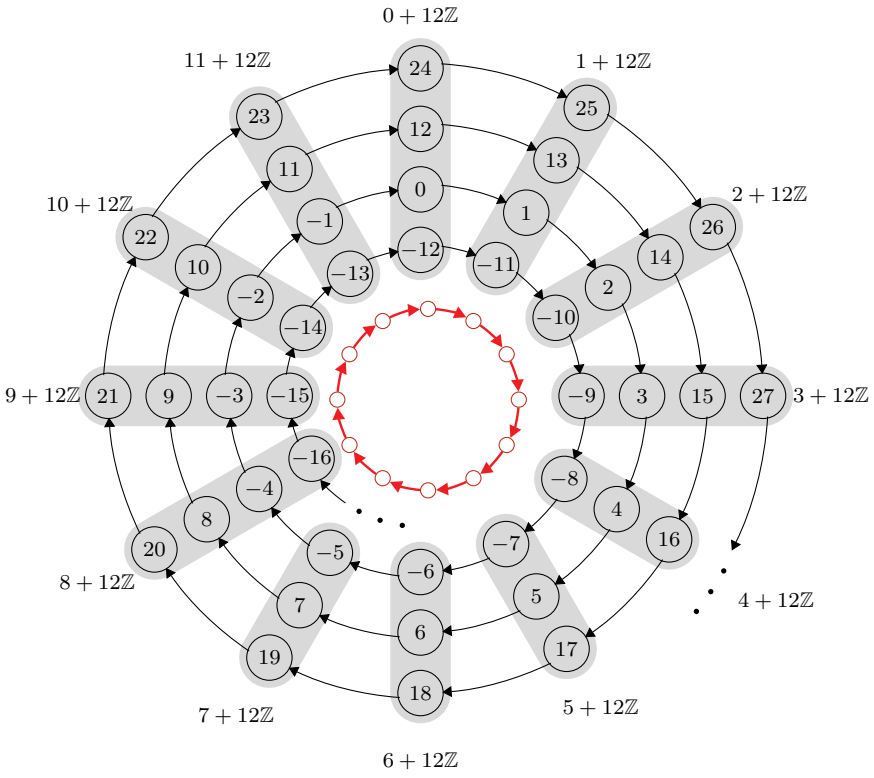


图 6.4: 把 $\mathbb{Z}$ 的生成路径图按 12 为周期卷起来，可以更清晰地看到子群 $12\mathbb{Z}$ 对应的往集和商群的结构。从圆心看，每隔 30 度是一个从中心发散的列，代表一个往集。而往集的排列方式和 C_{12} 一样。

6.2 群同态

往合子群和商群让我们能够把群分解成更小的群，由此，我们建立了群与群之间的一种新联系。这就是我们要介绍的**群同态**。详细的定义为：

定义 6.2 群同态

设 $(G_1, \cdot)$、$(G_2, \bullet)$ 为两个群。如果有映射 $\phi: G_1 \longrightarrow G_2$，使得：

$$\forall\, a, b \in G_1, \quad \phi(a) \bullet \phi(b) \;=\; \phi(a \cdot b),$$

就说 ϕ 是 G_1 到 G_2 的**群同态**，简称**同态**。

同态是比同构更宽松的一种关系。它不要求两个群一模一样，但要求保持群的运算性质不变。如果 ϕ 是满射，就说它是**满同态**；如果它是单射，就说它是**单同态**；如果它是双射，它就是**同构**。

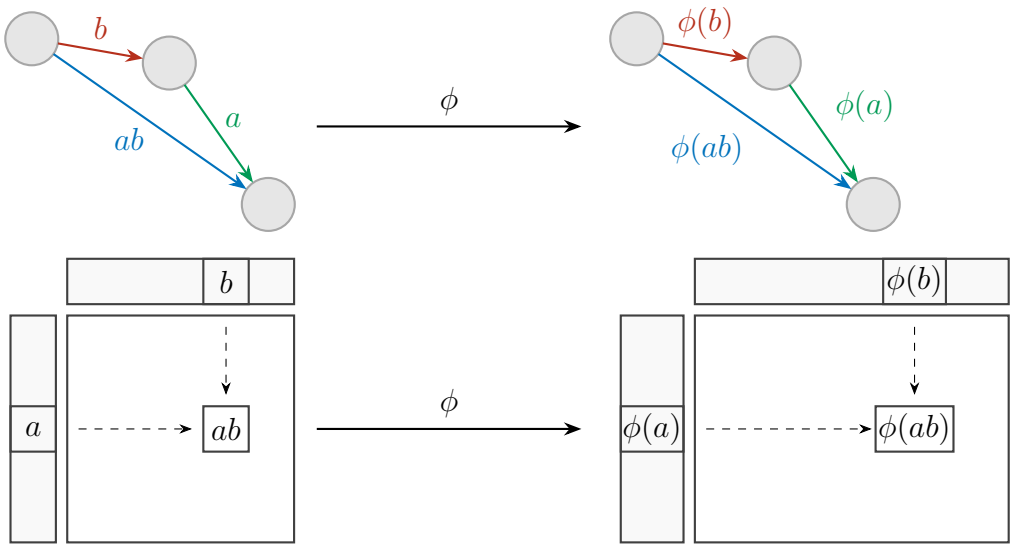


图 6.5: 群同态保持乘法运算

群同态保持群运算的性质可以通过生成路径图和乘法表来表现。生成路径图中，群同态保持所有状态变换的路径效果。如果原来的群里的不同路径把某个状态 A 变换为同一个状态 B，那么经过群同态 ϕ 的变换，这些路径还会把某个状态 A' 变为同一个状态 B'。乘法表则能更明显地体现群同态的效果：如果原来的群里，元素 a, b 乘法结果是 c，那么在新的乘法表里查 a, b 分别经过 ϕ 后的结果：$\phi(a), \phi(b)$，其乘法结果就是 $\phi(c)$。

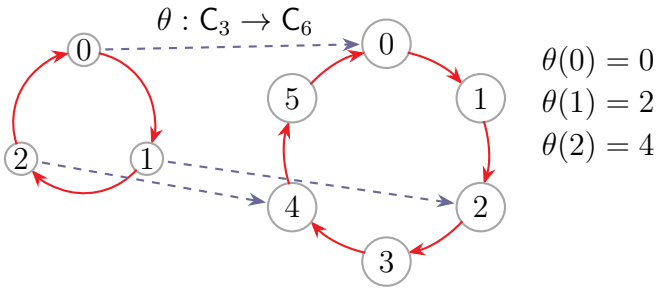


图 6.6: 群同态 θ 把 C_3 映射到 C_6。它的像是环道 $\langle 2 \rangle$，是 C_6 的子群。

更具体来说，群同态有以下的性质：

1. 群同态总把群的幺元映射到幺元：$\phi(e_1) = e_2$。
2. 群同态总把元素的逆元映射到逆元：$\phi(a^{-1}) = (\phi(a))^{-1}$。

3. 群同态与结合律兼容：$(\phi(a) \bullet \phi(b)) \bullet \phi(c) = \phi(a) \bullet (\phi(b) \bullet \phi(c))$。
4. 群同态的像是 G_2 的子群。

我们只证明第一个性质，其余留作练习。

证明：记 e_1, e_2 分别为 $(G_1, \cdot)$、$(G_2, \bullet)$ 的幺元，则：

$$\phi(e_1) \bullet \phi(e_1) = \phi(e_1 \cdot e_1) = \phi(e_1).$$

而 $\phi(e_1) \in G_2$，所以有逆元：有 $y \in G_2$，使得

$$y \bullet \phi(e_1) = e_2.$$

于是，

$$\phi(e_1) = e_2 \bullet \phi(e_1) = (y \bullet \phi(e_1)) \bullet \phi(e_1) = y \bullet (\phi(e_1) \bullet \phi(e_1)) = y \bullet \phi(e_1) = e_2.$$

□

从群到其商群的关系就是一种群同态。我们可以将其写为：

$$\begin{aligned} \phi :\ G &\longrightarrow G\big/H \\ a &\longmapsto aH \end{aligned}$$

按定义，它是满同态。它之所以成为同态，就在于往合子群 $H \trianglelefteq G$ 令其满足了同态的条件：

$$\phi(a) \cdot \phi(b) = (aH) \cdot (bH) = (a \cdot b)H = \phi(a \cdot b).$$

我们还可以用群同态的语言重新叙述置换群定理 4.2。当时提到的映射

$$\begin{aligned} \phi :\qquad G = \{1, 2, \cdots, n\} &\longrightarrow T \\ i &\longmapsto T_i \end{aligned}$$

就是一个群同态。我们验证了，它满足：

$$\forall i, j \in \{1, 2, \cdots, n\}, \quad \phi(i) \circ \phi(j) = T_i \circ T_j = T_{i \cdot j} = \phi(i \cdot j).$$

它不仅是群同态，而且是双射，因此是同构。

以上两个群同态都是满同态。但群同态不一定是满同态。比如图 6.6中的 θ。它把 C_3 元素映射到 C_6 中。另外一类典型的例子是平凡的群同态：

$$\begin{aligned} G_1 &\longrightarrow G_2 \\ a &\longmapsto e_2 \end{aligned}$$

它把 G_1 的任何元素都映射到 G_2 的幺元。可以验证它也是群同态：

$$\forall\, a, b \in G_1, \quad \phi(a) \bullet \phi(b) \;=\; e_2 \bullet e_2 \;=\; e_2 = \phi(a \cdot b).$$

无论 G_2 有多少元素，平凡的群同态都成立。

不过，我们总可以把群同态变为满同态。我们知道群同态的像总是子群，所以只要把到达集从整个群缩减为这个子群，群同态自然就是满同态了。因此，如果群同态 $\phi\colon\ G_1 \to G_2$ 是单同态，通过缩小到达集，我们总能构造出一个群同构。这个同构代表着我们在一个群 G_2 里找到了同构于 G_1 的子群 $\phi(G_1)$。$\phi(G_1)$ 可能有别的方面的性质，但作为群，和 G_1 是一模一样的。因此，我们可以说：G_2 中**嵌入**了 G_1，或者说同态 ϕ 把 G_1 **嵌入**了 G_2，把 ϕ 称为相关的**嵌同态**。比如图 6.6中的 θ 就是把 C_3 嵌入 C_6 的嵌同态。通过 θ，C_6 中嵌入了 C_3，因此，在这个意义上，可以说 C_3 是 C_6 的子群。

6.3 群同态基本定理

是否任何群都可以嵌到另一个群里呢？比如，我们能否把 D_3 嵌到 C_3 或 J_4 里？看起来不太可能。这是因为，D_3 有 6 个元素，太大了。放不到只有 3 个元素的 C_3 和只有 4 个元素的 J_4。能不能变通一下呢？

考虑 G_1 到 G_2 的群同态，它在 G_2 中的像 $\phi(G_1)$ 不可能比 G_1 还“大”。如果 G_1 是有限群，那么 $\phi(G_1)$ 的元素个数不应该比 G_1 的元素个数更多。这是因为按照映射的定义，G_1 中一个元素只能对应 G_2 中的一个元素，不能更多。因此，$\phi(G_1)$ 的元素个数要么等于 G_1 的元素个数，要么更少。

若 $|\phi(G_1)| = |G_1|$，ϕ 就是单同态，我们就把 G_1 嵌到 G_2 中了。那么 $|\phi(G_1)| < |G_1|$ 的情况呢？这说明 ϕ 把 G_1 中的某些元素“藏起来”了。或者说，两个元素经 ϕ 映射到了同一个元素。这说明什么呢？对于一般的映射，我们难以说清。但对于群同态，我们可以得到更清楚的解释。设有 $a, b \in G_1$，使得：

$$\phi(a) \;=\; \phi(b) \in G_2.$$

那么按照群同态的定义，

$$\phi(a \cdot b^{-1}) \;=\; \phi(a) \bullet \phi(b^{-1}) \;=\; \phi(a) \bullet \phi(b)^{-1} \;=\; \phi(a) \bullet \phi(a)^{-1} \;=\; e_2.$$

因此，考虑所有被 ϕ 映射到 e_2 的元素构成的集合：

$$\{x \in G_1, \mid \phi(x) = e_2\} \subseteq G_1,$$

只要 $\phi(a) = \phi(b)$，ab^{-1} 就在这个集合里。这个集合有什么性质呢?

1. $\phi(e_1) = e_2$，所以 G_1 的幺元在集合里。
2. 如果 a, b 在集合里，那么 $\phi(a) = e_2 = \phi(b)$，于是依照前面的推理，ab^{-1} 在集合里。

因此，这个集合是 G_1 的子群，称为**群同态的核**，记作 $\mathrm{Ker}\,(\phi)$ 或 $\mathrm{Ker}\,\phi$。前面的性质可以用另一种方式叙述为：只要 $\phi(a) = \phi(b)$，就有 $\mathrm{Ker}\,(\phi)$ 中的元素 x, x', y, y'，使得

$$ax = x'a = b, \quad by = y'b = a.$$

$\mathrm{Ker}\,(\phi)$ 是 G_1 的子群。所以，如果 G_1 是有限群，那么 $|\mathrm{Ker}\,(\phi)|$ 整除 $|G_1|$。此外，我们还可以考虑 $\mathrm{Ker}\,(\phi)$ 的往集。往集定理告诉我们，$\mathrm{Ker}\,(\phi)$ 的往集构成 G_1 的分划。让我们来看 $\mathrm{Ker}\,(\phi)$ 的一个左往集：$a\mathrm{Ker}\,(\phi)$。里面的元素可以写为 ax，其中 $x \in \mathrm{Ker}\,(\phi)$。于是：

$$\phi(ax) = \phi(a) \bullet \phi(x) = \phi(a) \bullet e_2 = \phi(a).$$

换句话说，左往集 $a\mathrm{Ker}\,(\phi)$ 里所有元素经过 ϕ 都映射到同一个地方，它的像就是 $\{\phi(a)\}$。因此，群同态的核的左往集里，就藏着所有经过 ϕ 映射到一起的元素。而我们知道，$\mathrm{Ker}\,(\phi)$ 的往集的“大小”都一样，都和 $\mathrm{Ker}\,(\phi)$“一样大”。因此，群同态总把“同样多”的元素映射到一起，不多也不少。每一份都和映射到 G_2 的幺元的“一样多”。

上面我们讨论的是左往集，那么右往集呢？按同样的方法可以得到：

$$\forall\, a \in G_1,\ \forall\, x \in \mathrm{Ker}\,(\phi), \quad \phi(xa) = \phi(x) \bullet \phi(a) = e_2 \bullet \phi(a) = \phi(a).$$

因此，右往集 $\mathrm{Ker}\,(\phi)a$ 里所有元素经过 ϕ 也都映射到 $\phi(a)$，它的像也是 $\{\phi(a)\}$。这就是说，左往集 $a\mathrm{Ker}\,(\phi)$ 和右往集 $\mathrm{Ker}\,(\phi)a$ 都是 $\{\phi(a)\}$ 的原像，两者相等!

我们可以更详细地论证：

$$\forall\, a \in G_1,\ \ \forall\, x \in \mathrm{Ker}\,(\phi),$$
$$\phi(a \cdot x) = \phi(a) = \phi(x \cdot a).$$

这说明 $\forall x \in \mathrm{Ker}\,(\phi)$，总有 $y, y' \in \mathrm{Ker}\,\phi$ 使得

$$\begin{aligned} x \cdot a &= a \cdot x \cdot y \in a\mathrm{Ker}\,(\phi), \\ a \cdot x &= y' \cdot x \cdot a \in \mathrm{Ker}\,(\phi)a. \end{aligned}$$

以上关系对任意 $x \in \mathrm{Ker}\,\phi$ 成立。因此，前一个关系说明：$\mathrm{Ker}\,(\phi)a \subseteq a\mathrm{Ker}\,(\phi)$；后一个关系则说明：$a\mathrm{Ker}\,(\phi) \subseteq \mathrm{Ker}\,(\phi)a$。综合起来，就说明 $\mathrm{Ker}\,(\phi)$ 的左往集等于右往集：$a\mathrm{Ker}\,(\phi) = \mathrm{Ker}\,(\phi)a$。而这一点又对所有 $a \in G_1$ 成立。因此，结论为：

命题 6.2

群同态 $\phi : G_1 \to G_2$ 的核是 G_1 的往合子群。

既然 $\mathrm{Ker}\,(\phi)$ 是 G_1 的往合子群，我们就能谈论 $\mathrm{Ker}\,(\phi)$ 除 G_1 的商群。这个商群把映射到同一个值的元素都分组“藏起来”了。我们可以试着把它嵌到 G_2 里。具体来说，可以构造从它到 G_2 的映射：

$$\begin{aligned} \psi : \quad G_1 \big/ \mathrm{Ker}\,\phi &\longrightarrow G_2 \\ a\mathrm{Ker}\,(\phi) &\longmapsto \phi(a) \end{aligned}$$

映射 ψ 和 ϕ 很像，但又有不同。不同在于：商群把 ϕ 中所有“藏起来”的元素都“打包”了，把 G_1 按照 ϕ 的性质分成了一份份，把每一份“压缩”成一个元素。可以说，ψ 是 ϕ 的“精简版”。我们自然期望它是单同态。

首先要说明可以这样定义映射 ψ：在 G_1 中任取元素 a，然后把 $a\mathrm{Ker}\,(\phi)$ 映射到 $\phi(a)$。由于 $\mathrm{Ker}\,(\phi)$ 的往集（左往集等于右往集）构成了 G_1 的分划，不重不漏，所以，a 总是恰好属于某个往集。而这个往集中其他元素也被映射到 $\phi(a)$ 了。因此，一个往集必然只映射到一个值。不会有某个往集里的两个元素让 ψ 映射到两个不同的值。因此，ψ 的定义是没有问题的。

其次，映射 ψ 也是群同态。我们知道作为往合子群，$\mathrm{Ker}\,(\phi)$ 的往集满足：

$$\forall\, a, b \in G_1, \quad (a\mathrm{Ker}\,(\phi)) \cdot (b\mathrm{Ker}\,(\phi)) = (ab)\mathrm{Ker}\,(\phi).$$

因此，

$$\begin{aligned} \forall\, a, b \in G_1, \quad \psi\left(a\mathrm{Ker}\,(\phi)\right) \bullet \psi\left(b\mathrm{Ker}\,(\phi)\right) = \phi(a) \bullet \phi(b) = \phi(ab) = \psi\left((ab)\mathrm{Ker}\,(\phi)\right) \\ = \psi\left(\left(a\mathrm{Ker}\,(\phi)\right) \cdot \left(b\mathrm{Ker}\,(\phi)\right)\right). \end{aligned}$$

这就说明 ψ 是群同态。

最后证明 ψ 是单射。如果有两个往集被“打包”发送到同一个值，那么这两个往集就会产生更紧密的联系。具体来说，如果有 $a, b \in G_1$ 使得 $\psi\left(a\mathrm{Ker}\left(\phi\right)\right) = \psi\left(b\mathrm{Ker}\left(\phi\right)\right)$，那么按 ψ 的定义，$\phi(a) = \phi(b)$，但这就说明 a, b 同属于 $\mathrm{Ker}\left(\phi\right)$ 的某个往集，于是按照往集的性质，$a\mathrm{Ker}\left(\phi\right) = b\mathrm{Ker}\left(\phi\right)$。

ψ 是单同态，因此，如果只考虑 ψ 的像，它就是同构。ψ 的像就是 ϕ 的像：对 $y \in G_2$，只要你能找到 $a \in G_1$ 使得 $y = \phi(a)$，那么按定义，y 就等于 $\psi(a\mathrm{Ker}\left(\phi\right))$。因此，$\psi$ 是 ϕ 的核除 G_1 的商群到 ϕ 的像的同构。换句话说，我们把 G_1 按照 ϕ 的核“打包精简”后，嵌入了 G_2。我们把这个结论称为群同态的基本定理：

定理 6.1 群同态基本定理

设 $\phi : G_1 \to G_2$ 是群同态，那么 ϕ 的核除 G_1 的商群同构于 ϕ 在 G_2 中的像：$\phi(G_1)$。

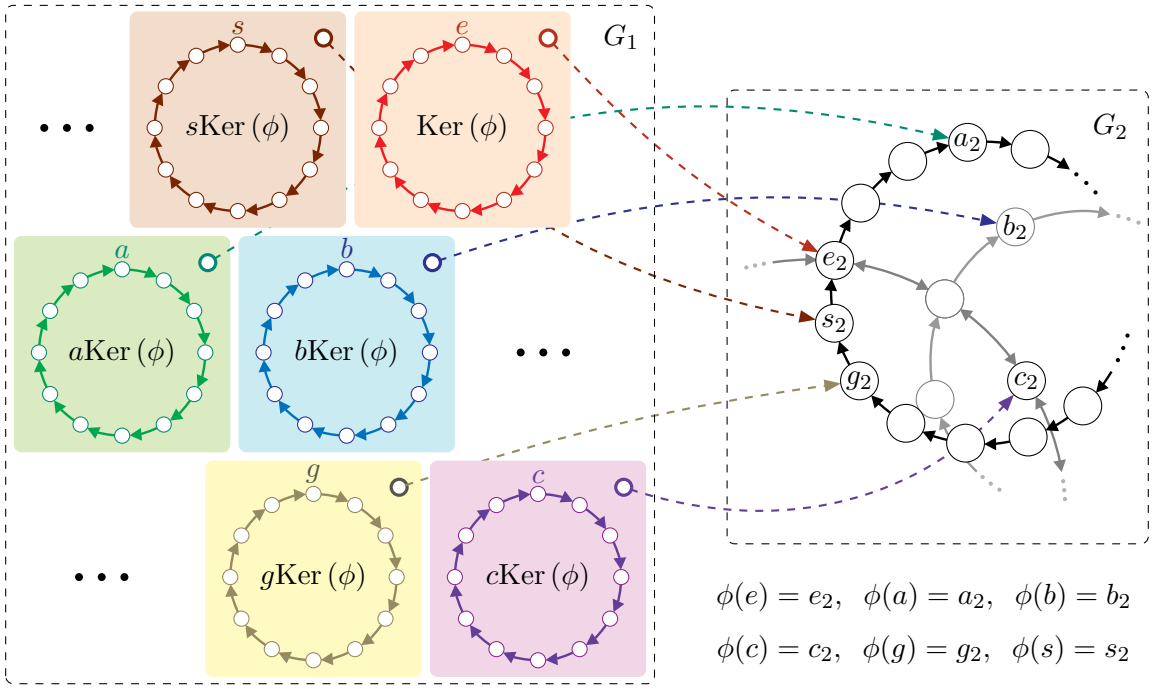


图 6.7: 群同态 ϕ 的核 $\mathrm{Ker}\left(\phi\right)$ 是往合子群。ϕ 把 $\mathrm{Ker}\left(\phi\right)$ 的往集映射为同一元素。

对于有限群，群同态基本定理能告诉我们哪些群同态可以存在。如果从群 G_1 到 G_2 有群同态，那么群同态的核必然是 G_1 的子群。它除 G_1 得到一个商群。这两个群的势都整除 G_1 的势。而这个商群又同构于群同态在 G_2 中的像，因此两者等势。最后，群同态在 G_2 中的像是 G_2 的子群，于是它的势又要整除 G_2 的势。只有满足这些条件，群

同态才存在。否则就不存在这样的群同态。

上面的说法还是很抽象。让我们来看具体的例子。首先分析 D_3 到 J_4 的群同态。这样的群同态如果存在，其商群的势整除 $|\mathsf{D}_3| = 6$，因此只能是 $1, 2, 3, 6$。而商群同构于群同态的像，也就是 J_4 的子群，所以又整除 $|\mathsf{J}_4| = 4$。也就是说，商群只能是一元群或二元群。D_3 到 J_4 的群同态不可能是满同态。

再来看 D_3 到 C_3 的群同态。按同样的方法分析，群同态的核除 D_3 的商群，其势要整除 $|\mathsf{C}_3| = 3$，因此只能是 1 或 3。如果商群是三元群，那么群同态的核是二元群。D_3 的二元子群只有 $\{e, s\}$、$\{e, rs\}$、$\{e, r^2 s\}$，都不是往合子群。都不能作为群同态的核。因此，D_3 到 C_3 的群同态只能是平凡同态。

本章小结

本章继续深入分析了群的内部结构及其相互联系。主要知识点包括：

- **往合子群**：左右往集完全重合的子群。这时各个往集之间可以定义和群运算相容的运算。
- **交换群的任何子群都是往合子群**。
- **商群**：以往合子群的往集为元素构成的新群。
- **群同态**：保持群运算结构的映射，称为群同态。群同态总把幺元映射为幺元，把逆元映射到逆元。
- **群同态的核**：被群同态映射到幺元的元素集合称为群同态的核。群同态的核总是群的往合子群。
- **群同态基本定理**：群同态的核除群得到的商群，同构于群同态的像。

6.4 习题

1. 以下的群和群元素是什么意思？解释你看到的表达式。

(1) $2+12\mathbb{Z} \in \mathbb{Z}/12\mathbb{Z}$

(2) $10+16\mathbb{Z} \in 2\mathbb{Z}/16\mathbb{Z}$

(3) $(5,9)+6\mathbb{Z}\times 12\mathbb{Z} \in (\mathbb{Z}\times\mathbb{Z})/(6\mathbb{Z}\times 12\mathbb{Z})$

(4) $(4,4)+12\mathbb{Z}\times 6\mathbb{Z} \in (4\mathbb{Z}\times 2\mathbb{Z})/(12\mathbb{Z}\times 6\mathbb{Z})$

(5) $\overline{2}+\langle\overline{3}\rangle \in \mathbb{Z}_{12}/\langle\overline{3}\rangle$

(6) $\overline{5}+\langle\overline{4}\rangle \in \mathbb{Z}_{12}/\langle\overline{4}\rangle$

(7) $(\overline{2},\overline{1})+\langle(\overline{0},\overline{2})\rangle \in (\mathbb{Z}_3\times\mathbb{Z}_4)/\langle(\overline{0},\overline{2})\rangle$

(8) $(\overline{1},\overline{3})+\langle(\overline{2},\overline{0})\rangle \in (\mathbb{Z}_8\times\mathbb{Z}_4)/\langle(\overline{2},\overline{0})\rangle$

2. 小明想证明以下结论：如果 H 是交换群 G 的往合子群，那么商群 G/H 也是交换群。他的证明开头是：

> 设 H 是交换群 G 的往合子群，商群为 G/H。取 $a,b \in G/H$，要证明 $ab=ba$。

然后小明不知道如何继续了。

(1) 小明的问题出在哪里？他应该怎么写？

(2) 帮小明完成证明。

3. 子怡要证明：S_4 里没有同构于 C_3 的往合子群。她的证明如下：

> C_3 是交换群，而 S_4 不是交换群。如果 C_3 是 S_4 的往合子群，那么 C_3 的左往集总等于右往集，这就说明商群也是交换群。于是非交换群 S_4 就分解为两个交换群了，这是不可能的。

(1) 子怡的问题出在哪里？如何让她认识到自己的问题？

(2) 帮子怡完成证明。

4. A_4 是正四面体的旋转群，它同构于以下元素构成的 4 元置换群（具体证明见第四章

练习题 6)：

$$\{(1\,2\,3\,4),(1\,3\,4\,2),(1\,4\,2\,3),(3\,2\,4\,1),$$
$$(4\,2\,1\,3),(2\,4\,3\,1),(4\,1\,3\,2),(2\,3\,1\,4),$$
$$(3\,1\,2\,4),(2\,1\,4\,3),(3\,4\,1\,2),(4\,3\,2\,1)\}$$

(1) 证明：A_4 同构于 S_4 的往合子群。

(2) 证明：如果有限群 G 的子群 H 拥有 G 的一半元素，则 H 是 G 的往合子群。

(3) 证明：A_4 没有 6 元子群。

设 $\mathsf{S}_{\mathbb{N}}$ 为自然数集 $\mathbb{N}$ 上的全体置换（即所有 $\mathbb{N}$ 到 $\mathbb{N}$ 的双射）构成的群。$\forall n \in \mathbb{N}$，记 $\mathsf{H}_n = \{\sigma \in \mathsf{S}_{\mathbb{N}} \,|\, \sigma(0) = n\}$。

(4) 证明 $\mathsf{H}_0 \lhd \mathsf{S}_{\mathbb{N}}$。

(5) 记 $\tau \in \mathsf{S}_{\mathbb{N}}$ 为只交换 0 和 1 的对换。证明：$\tau\mathsf{H}_0 \neq \mathsf{H}_0\tau$（提示：在 H_0 中找一个很像 τ 的元素 σ，研究 $\tau\sigma$、$\sigma\tau$）。

(6) 记 $\tau_n \in \mathsf{S}_{\mathbb{N}}$ 为只交换 0 和 n 的对换。证明：$\mathsf{H}_n = \tau_n\mathsf{H}_0$。

(7) $\forall i \in \mathbb{Z}^+$，记 $\mathsf{H}_0^{(i)} = \{\sigma \in \mathsf{H}_0 \,|\, \sigma(1) = i\}$，证明：不同的 $\mathsf{H}_0^{(i)}$ 两两不相交，相互等势。所有 $\mathsf{H}_0^{(i)}$ 构成 H_0 的分划。

(8) 证明：$\mathsf{H}_0^{(1)}$ 和 H_0 之间有双射（提示：考虑 $\Phi : \sigma \mapsto (x \mapsto \sigma(x+1) - 1)$）。

(9) 证明 H_0 和它在 $\mathsf{S}_{\mathbb{N}}$ 的补集之间有双射。综上，你能得到什么结论?

5. 讨论映轮群 D_4 的往合子群。

(1) 设 r, s 为映轮群 D_4 中的逆时针旋转 90° 和水平翻转变换。证明：子群 $\{e, r^2\}$ 是往合子群。

(2) D_4 有其他二元的往合子群吗?

(3) 研究商群 $\mathsf{D}_4 \big/ \langle r^2 \rangle$ 的性质。写出 $\{e, r^2\}$ 的所有往集。它们之间的运算结果如何? 它同构于哪个我们已经学过的群?

(4) 设 M_1 为 r^2 和 s 生成的子群。它同构于哪个我们已经学过的群?

(5) 证明 M_1 是 D_4 的往合子群。研究商群 $\mathsf{D}_4 \big/ M_1$，它有几个元素? 它同构于哪个我们

已经学过的子群?

(6) 找出另外两个由 r^2 和 D_4 其他（非幺）元素生成的 D_4 的往合真子群，分别记为 M_2, M_3。它们对应的商群 $\mathsf{D}_4 \diagup M_2$、$\mathsf{D}_4 \diagup M_3$ 分别有几个元素? 同构于什么子群?

(7) D_4、$\{e, r^2\}$ 和 M_1, M_2, M_3 之间有什么联系? 和对应的商群之间有什么联系? 用自己的话总结一下。

第七章　观群

这一章我们将回到群作为变换的集合这个观念。群元素作为变换，作用于具体的对象、状态，帮助我们更好地理解对象的对称性。反过来，通过观察群中变换如何改变具体的对象，我们也能更好地理解群。这种相互作用就是我们接下来要探讨的主题。

7.1　观群于集合

回到正三角形的例子。讨论保持正三角形形状的对称变换时，我们用三个顶点作为标志来讨论各种变换。如果把这三个顶点看作集合，按逆时针顺序依次记为 $X_3 = \{x_1, x_2, x_3\}$，那么群 D_3 中的变换实际上操纵着 X 的元素，将它们变成别的元素。比如，逆时针旋转 120 度，就是把 x_1 变为 x_2，x_2 变为 x_3，把 x_3 变为 x_1。我们自然会想，这些变换，是否只能施于正三角形的三个顶点?

考虑一个正六边形，其中心和正三角形的中心重合。我们讨论 D_3 对它的顶点有什么作用。可以发现，D_3 的元素也能让正六边形不变。对具体的顶点来说，D_3 里的变换总让它变成另一个顶点。因此，把这六个顶点按逆时针顺序依次记为 $X_6 = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ 的话，我们可以讨论 D_3 操纵 X_6 的元素，将它们变成别的元素。比如，逆时针旋转 120 度，就是把 x_1 变为 x_3，x_2 变为 x_4，把 x_3 变为 x_5，把 x_4 变为 x_6，x_5 变为 x_1，把 x_6 变为 x_2。

反过来，我们也希望观察群的元素如何作用于一般的集合 X，根据它操纵 X 中元素变化显出的现象，反过来讨论群的性质，帮助我们理解群。

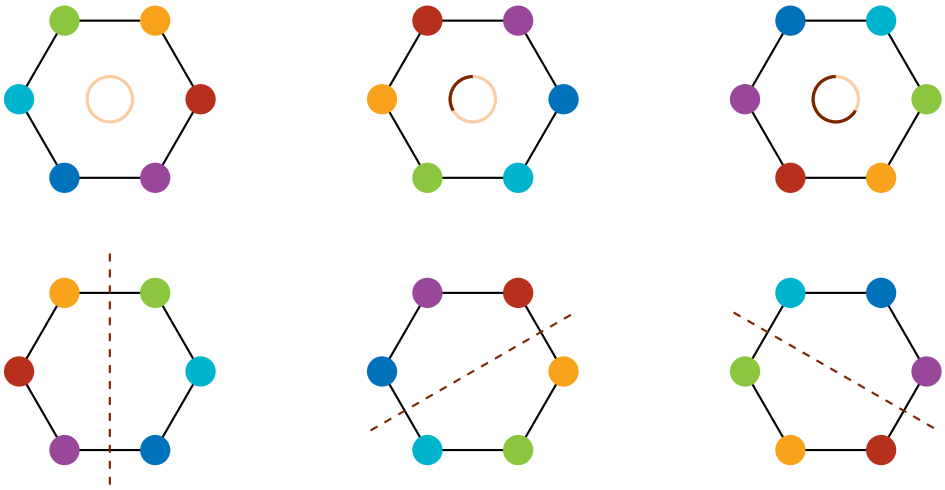


图 7.1: D_3 中的变换对正六边形的操作效果。

一般来说，我们可以考虑群 G 的元素作用于集合 X。它可以写作这样的映射：

$$\begin{aligned} \gamma : G \times X &\longrightarrow X \\ (a, x) &\longmapsto \gamma(a, x) \end{aligned}$$

这里 γ 表示群元素 a 施于集合中元素 x，将其变为集合中元素 $\gamma(a, x)$。当然，γ 不可能是随意的映射。它应该与群中变换的规则兼容：

1. 群变换的组合作用于集合 X 的元素，是其作用复合的效果。换句话说，两个群元素的乘积作用于集合的元素，等于把它们分别作用的效果复合起来。
2. 恒等变换作用于集合 X，仍然是恒等变换。

用严格的语言，可以归结为：

1. $\forall a, b \in G$，$\forall x \in X$，$\gamma(a, \gamma(b, x)) = \gamma(a \cdot b, x)$。
2. $\forall x \in X$，$\gamma(e, x) = x$。

为了方便说话，对于给定的 γ，我们把 $\gamma(a, x)$ 简记为 $a(x)$，读作“a（以 γ）施于 x”。这个写法下，上面两个规则写作：

1. $\forall\, a, b \in G,\ \ x \in X,\ \ (ab)(x) = a(b(x))$.
2. $\forall\, x \in X,\ \ e(x) = x$.

这是把群元素看作映射（变换）的视角。隐去的 γ 指定了群元素作为映射施于集合 X 的效果。

举例来说，可以验证，上面提到的以 D_3 的变换施于 X_6 的元素的方法，就满足这两个条件。

定义 7.1

设 G 为群，X 为非空集合，若有映射 $\gamma\colon G\times X \longrightarrow X$ 满足上述两个条件，就称群 G 以 γ 显相于 X，或以 γ 观群 G 于 X，G 在 X 上有**群观**，或称 G 在 X 上**显相**。我们称 X 为观 G 的**相集**。γ 称为 G 在 X 上的**显相映射**，或称在 X 上**观群** G **之法**。$\gamma(a,x)$ 称为 a **以** γ **施于** x **的相**或**结果**。

在正式的定义里，X 可以是任意集合，与 G 不必有任何联系。G 中元素也不必是 X 上的对称变换，变换效果仅仅受前面提到的两个规则约束。以下两个例子说明了这两个规则如何约束群显相的方式。首先我们可以验证前述 D_3 操纵 X_6 的元素的方法满足规则。比如逆时针旋转 120 度的 r 和以竖直中轴翻转的 s，分别把 X_6 中元素进行以下变换：

$$\begin{aligned} &r(x_1)=x_3,\ r(x_2)=x_4,\ r(x_3)=x_5,\ r(x_4)=x_6,\ r(x_5)=x_1,\ r(x_6)=x_2,\\ &s(x_1)=x_1,\ s(x_2)=x_6,\ s(x_3)=x_5,\ s(x_4)=x_4,\ s(x_5)=x_3,\ s(x_6)=x_2. \end{aligned}$$

因此，r 和 s 先后施于 X_6，得到：

$$\begin{aligned} &s(r(x_1))=s(x_3)=x_5,\ s(r(x_2))=s(x_4)=x_4,\ s(r(x_3))=s(x_5)=x_3,\\ &s(r(x_4))=s(x_6)=x_2,\ s(r(x_5))=s(x_1)=x_1,\ s(r(x_6))=s(x_2)=x_6. \end{aligned}$$

另一方面，两者乘积 sr 也是群元素，它的效果是以 x_3,x_6 连线为轴翻转：

$$\begin{aligned} &(sr)(x_1)=x_5,\ (sr)(x_2)=x_4,\ (sr)(x_3)=x_3,\\ &(sr)(x_4)=x_2,\ (sr)(x_5)=x_1,\ (sr)(x_6)=x_6. \end{aligned}$$

对比可知：sr 施于 X_6，与 r、s 先后施于 X_6 效果完全相同。其他情况也可以一一验证。当然，这个效果是由我们观 D_3 于 X_6 之法确定的。它说明我们定义的显相映射是合乎规则的。

下面给出一个不符合规则的显相映射的例子。设 $\{e,a\}$ 是二元群，显相于三元集合 $X_3=\{x_1,x_2,x_3\}$，我们规定显相映射 γ 为：

$$\gamma(a,x_1)=x_2,\ \ \gamma(a,x_2)=x_3,\ \ \gamma(a,x_3)=x_1.$$

这时，按照规则就得到矛盾：

$$x_3 = \gamma(a, x_2) = \gamma(a, \gamma(a, x_1)) = \gamma(a^2, x_1) = \gamma(e, x_1) = x_1.$$

这说明 γ 无法遵循规则，不能当让 $\{e, a\}$ 在 X_3 上显相的映射。

问题的根源在于：群元素 a 在群内有 $a^2 = e$ 的性质，γ 却试图让它施于 x_1 三次后才回到 x_1。这与 a 的性质矛盾。这个反例揭示了一个重要的事实：群的结构决定了显相的可能形态。群中元素满足什么代数关系，它施于集合元素时就必须表现出相应的变换行为。群观不是任意的，它是群结构在外部集合上显出的相。观群不得法，就无法讨论群相。

从以上两个规则，还能推出显相映射 γ 的以下基本性质：

命题 7.1

1. $\forall a \in G$，$\gamma_a :\ x \mapsto \gamma(a, x)$ 总是 X 上的置换（X 到自身的双射）。
2. $\phi :\ a \mapsto \gamma_a$ 是 G 到 S_X 的群同态。

证明：

(1) 我们考虑 a 和 a 的逆元 a^{-1} 对应的映射：$\gamma_a = x \mapsto \gamma(a, x)$，$\gamma_{a^{-1}} = x \mapsto \gamma(a^{-1}, x)$。两者复合的结果是：

$$\begin{aligned} \forall x \in X, \quad (\gamma_a \circ \gamma_{a^{-1}})(x) &= \gamma(a, \gamma(a^{-1}, x)) = \gamma(aa^{-1}, x) = \gamma(e, x) = x, \\ (\gamma_{a^{-1}} \circ \gamma_a)(x) &= \gamma(a^{-1}, \gamma(a, x)) = \gamma(a^{-1}a, x) = \gamma(e, x) = x. \end{aligned}$$

这说明两者复合为恒等变换，因此 γ_a 是 X 到自身的双射，是 X 上的置换。

(2) 按照群同态的定义检验：

$$\forall a, b \in G,\ \forall x \in X, \quad (\gamma_a \circ \gamma_b)(x) = \gamma(a, \gamma(b, x)) = \gamma(ab, x) = \gamma_{ab}(x).$$

这说明 $\phi(a) \circ \phi(b) = \gamma_a \circ \gamma_b = \gamma_{ab} = \phi(ab)$。因此 ϕ 是群同态。

这里的大致想法和证明置换群定理时是一样的。不妨设 X 有 n 个元素，我们要帮它写一个“乘法表”，说明它怎样被 G 的元素操纵，于是行头为 X 中元素，每一列列头为群元素 a，而列的内容就是经 γ_a 映射后的 X 元素重排结果。因此每一列就代表群元素 a 对应的置换 T_a。如果令 $X = G$，我们就回到了证明置换群定理时的场景。在此，我们

以观群于自身的角度，重温置换群定理的证明。考虑映射 γ：

$$\begin{aligned} \gamma : G \times G &\longrightarrow G \\ (a,\ x) &\longmapsto a \cdot x \end{aligned}$$

可验证 γ 是观群法。则 γ_a 是 G 上的置换。而 $a \mapsto \gamma_a$ 是 G 到 S_G 的群同态，并且是双射，所以是同构。即 G 同构于 S_G 的子群。 □

接下来，我们给出几个不同风格的例子，展示群观的多种形态。

例子 7.1 观正方体旋转群于顶点、棱、面

正方体的旋转群 G 有 24 个元素。可以观其于正方体的 8 个顶点构成的集合 V，把顶点变为顶点；也可以观于 12 条棱构成的集合 E，把棱变为棱；还可以观于 6 个面构成的集合 F，把面变为面。

同一个群 G，显相于不同的集合，呈现出不同的面貌。显相于 V 时，我们看到的是顶点如何被旋转变换搬运；显相于 E 时，我们看到的是边如何被旋转变换搬运；显相于 F 时，我们看到的是面如何被旋转变换搬运。群的结构没有变，但它显在不同集合上的相不同。

例子 7.2 观群于自身——左乘观

设 G 为群。令 $X = G$（即把群 G 自身看作一个集合），定义 g 施于 x 为 $g(x) = gx$（即先 x 后 g 的变换）。严格来说，定义左乘映射：

$$\begin{aligned} \gamma : G \times G &\longrightarrow G \\ (a,\ x) &\longmapsto ax \end{aligned}$$

这就是前面提到的用于证明置换群定理的同态。验证两个条件：

1. $(ab)(x) = (ab)x = a(bx) = a(b(x))$.
2. $e(x) = ex = x$.

因此左乘映射是 G 在自身上的群观，称为**左乘观**或**左往观**。

第五章中，子群 H 的左往集 $gH = \{gh \mid h \in H\}$，正是 H 在左乘观下的像。

例子 7.3 观群于自身——往复观

设 G 为群。令 $X = G$，定义 g 施于 x 为 $g(x) = gxg^{-1}$（即先 g^{-1} 再 x 后 g 的变换）。严格来说，定义往复映射：

$$\begin{aligned} \gamma :\ G \times G &\longrightarrow G \\ (a,\ x) &\longmapsto axa^{-1} \end{aligned}$$

验证两个条件：

1. $(ab)(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = a(b(x))$.
2. $e(x) = exe^{-1} = x$.

因此往复映射是 G 在自身上的群观，称为**往复观**。

往复观可能在讨论往合子群时碰到，因为往合子群 H 满足 $\forall a \in G,\ aHa^{-1} = H$。在群观的角度，就是说 H 往复后不变。

例子 7.4 观 S_n 于 $\{1, 2, \ldots, n\}$

全置换群 S_n 的元素本身就是集合 $\{1, 2, \ldots, n\}$ 上的双射。因此天然可观 S_n 于 $\{1, 2, \ldots, n\}$：置换 σ 施于元素 i，得到 $\sigma(i)$。严格来说，定义自然映射：

$$\begin{aligned} \gamma :\ \mathsf{S}_n \times \{1, 2, \ldots, n\} &\longrightarrow \{1, 2, \ldots, n\} \\ (\sigma,\ i) &\longmapsto \sigma(i) \end{aligned}$$

这是最直接的群观：群元素就是变换本身，不需要额外的规则。回忆第四章的置换群定理：任何有限群都同构于某个 S_n 的子群。因此，任何有限群都可以视为某个集合上的置换群，从而天然地显相于该集合。

例题 7.1 观 D_3 于正三角形的三边

除了观 D_3 于正三角形的顶点，还可以观 D_3 于其三边。设三条边为 $X_{\text{边}} = \{\ell_1, \ell_2, \ell_3\}$，其中 ℓ_1 是 x_1 的对边，ℓ_2 是 x_2 的对边，ℓ_3 是 x_3 的对边。

旋转 $120°$ 把 $\ell_1 \to \ell_2 \to \ell_3 \to \ell_1$。过 x_1 的翻转保持 ℓ_1 不动（因为 ℓ_1 是 x_1 的对边，翻转轴过 x_1 且垂直于 ℓ_1），而交换 ℓ_2 和 ℓ_3。

观同一个群 D_3 于顶点集 X_3 和边集 $X_{\text{边}}$，效果不同，但结构相似。

这些例子展示了群观的丰富性：可以于不同的集合观同一个群，也可以于同一个集合观不同的群，还可以观群于自身。接下来，我们要追问一个核心问题：群观到底把集合 X 变成了什么样子？

7.2 轨迹

回到观 D_3 于 $X_3 = \{x_1, x_2, x_3\}$ 的例子。从 x_1 出发，用 D_3 中元素各施于 x_1，能得到哪些元素？

$$e(x_1) = x_1, \quad r(x_1) = x_2, \quad r^2(x_1) = x_3, \quad s(x_1) = x_1, \quad rs(x_1) = x_2, \quad r^2 s(x_1) = x_3.$$

所有可能的结果汇在一起，恰好是 $\{x_1, x_2, x_3\}$，即整个 X_3。也就是说，从 x_1 出发，在 D_3 的作用下，可以到达 X_3 中的任何元素。

再观 D_3 于 X_6（正六边形顶点）。取 x_1，用旋转 $120°$ 反复作用：$x_1 \to x_3 \to x_5 \to x_1$。再用翻转：$s(x_1) = x_1$（过 x_1 的翻转不动）。所以从 x_1 出发，在 D_3 作用下能到达的元素是 $\{x_1, x_3, x_5\}$，而 x_2, x_4, x_6 不在其中。

类似地，从 x_2 出发：$r(x_2) = x_4$，$r^2(x_2) = x_6$，$s(x_2) = x_6$。所以从 x_2 出发能到达 $\{x_2, x_4, x_6\}$。

X_6 被分成了两块：$\{x_1, x_3, x_5\}$ 和 $\{x_2, x_4, x_6\}$。群作用不能把一块中的元素送到另一块中去。

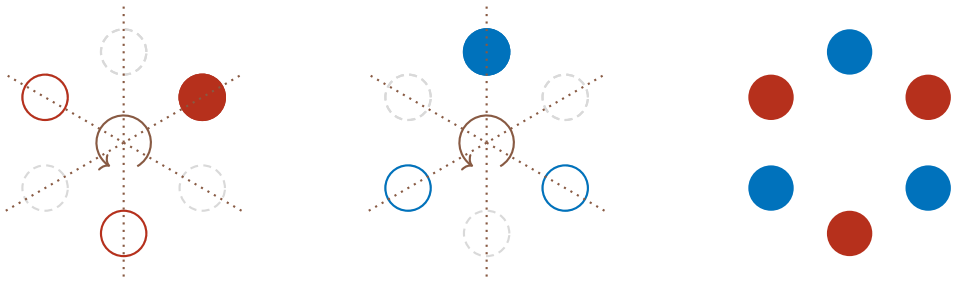


图 7.2: 正六边形顶点经 D_3 变换的轨迹

定义 7.2

以 γ 观群 G 于集合 X。G 中各元素施于 $x \in X$，得到的相，称为 G 在 x 的**轨迹**，记为：

$$\mathcal{O}_G(x) = \{\gamma(a, x) \mid a \in G\},$$

轨迹描述的是：从 x 出发，在群的所有变换下，x 能走到哪些地方。所有轨迹的集合记为 $\mathcal{O}_G(X)$。

命题 7.2

以 γ 观群 G 于集合 X。定义 X 上的关系：$x \sim y$，当且仅当有 $a \in G$ 使得 $\gamma(a, x) = y$。则 $\sim$ 是等价关系，其等价类恰好就是各个轨迹 $\mathcal{O}_G(x)$。因此，轨迹构成 X 的分划。

证明：验证 $\sim$ 满足等价关系的三个条件：

1. **自反性**：$e(x) = x$，所以 $x \sim x$。
2. **对称性**：若 $g(x) = y$，则 $g^{-1}(y) = g^{-1}(g(x)) = (g^{-1}g)(x) = e(x) = x$，所以 $y \sim x$。
3. **传递性**：若 $g(x) = y$，$h(y) = z$，则 $(hg)(x) = h(g(x)) = h(y) = z$，所以 $x \sim z$。

等价类 $\{y \in X \mid x \sim y\}$ 正是 $\{\gamma(a, x) \mid a \in G\} = \mathcal{O}_G(x)$。 □

如果 X 只有一条轨迹，即对任何 x，$\mathcal{O}_G(x) = X$，就说群 G（以 γ）**贯通** X，或称 G 在 X 上显现**通相**。

例子 7.5

以上观法，D_3 贯通 X_3，D_3 不贯通 X_6（有两条轨迹）。正方体旋转群贯通 8 个顶点（任何顶点都能被旋转到任何顶点的位置），贯通 12 条边，也贯通 6 个面。

例子 7.6

考虑全置换群 S_n 的元素 σ 生成的循环子群 $\langle\sigma\rangle$。它如何施于 $\{1, 2, \ldots, n\}$ 的元素 i 呢？设 $\langle\sigma\rangle$ 的长度为 k，则 $\sigma^k(i) = i$。也就是说，至多经过 k 次变换，i 会回到自身。但是否一定要经过 k 次呢？未必。比如以下三元置换：

$$\sigma: \quad 1 \mapsto 1, \quad 2 \mapsto 4, \quad 4 \mapsto 3, \quad 3 \mapsto 2.$$

它的环道长度是 $k = 3$。但 $\sigma(1) = 1$，即元素 1 只需要 1 次变换就回到自身。

我们考虑每个元素 i 经过 σ 多少次回到自身，记为 k_i，并且把它历次 σ 变换的结果依

次记录下来。比如上面的例子里，从 2 开始依次是：$2, \sigma(2) = 4, \sigma^2(2) = 3, \sigma^3(2) = 2$。我们将所有不同的结果依次记为 $(2\,4\,3)$。这就表明 $\langle\sigma\rangle$ 施于这些元素的效果。其他元素经过 σ 永远不会得到这些元素，这些元素经过 σ 也永远不会得到其他元素。它们自成循环。我们把这样的自成循环称为 σ 的**环圈**。各个环圈就是 $\langle\sigma\rangle$ 施于 $\{1, 2, \ldots, n\}$ 各个元素形成的轨迹。

考虑 $\{1, 2, \ldots, n\}$ 的所有元素，我们用 $\langle\sigma\rangle$ 施于这些元素，能得到一个又一个环圈。作为轨迹，它们不重不漏，最终构成 $\{1, 2, \ldots, n\}$ 的分划。比如上面的例子里，$\{1, 2, 3, 4\}$ 就被 $\langle\sigma\rangle$ 划分为环圈 (1) 和 $(2\,4\,3)$。

这给我们提供了一种简便的方法来记录置换 σ。我们知道 $\langle\sigma\rangle$ 会把 $\{1, 2, \ldots, n\}$ 划分为若干个环圈。于是我们把这些环圈写在一起，就能描述 σ 的效果。比如。上面施于 $\{1, 2, 3, 4\}$ 的置换就写为 $(1)(2\,4\,3)$。要知道 σ 对元素 i 的效果，只需查看它在哪个括号里。如果它不在最右边，那么 $\sigma(i)$ 就是它右边的元素；否则 $\sigma(i)$ 就是最左边的元素。

括号里如果只有一个元素 i，说明 $\sigma(i) = i$。我们可以忽略这个括号，不记录它。比如上面施于 $\{1, 2, 3, 4\}$ 的置换可以简记为 $(2\,4\,3)$。所以，查看 σ 对元素 i 的效果时，如果没有记录，就说明 $\sigma(i) = i$。

这样的记法下，如果只有一对括号（一个长度超过 1 的环圈），就说它是一个**轮换**。环圈的长度称为轮换的长度。最长的轮换是 $(1\,2\,\cdots\,n)$，它的长度是 n。最短的轮换（不考虑恒等变换）形如 $(i\,j)$ $(i \neq j)$，就是**对换**。轮换的长度和轮换的环道的长度是一样的。

如果观群于自身，群元素的轨迹会是什么呢？给定 $x \in G$，左往观用所有群元素左乘它，得到 $\{ax \,|\, a \in G\}$，由群的可逆性质可知，它就是 G 自身。也就是说，任何 x 的轨迹都是整个群：左往观群，显通相。

如果不用 G，而用它的子群 H 的元素来左乘 x，结果当然是 Hx。也就是说，以左往观子群，元素的轨迹是子群的右往集。这是同一个事实的不同说法。

如果换成往复观呢？得到的轨迹是 $\{axa^{-1} \,|\, a \in G\}$，这并不一定是整个群了。实际上，如果 G 是交换群，那么 $\{axa^{-1} \,|\, a \in G\}$ 就是 $\{x\}$。因为 $axa^{-1} = x$ 等价于说 $ax = xa$。实际上，要让轨迹为 $\{x\}$，不需要 G 是交换群，只需要 $ax = xa$ 对所有群元素 a 成立即可。我们称这样的 x 为群 G 的**心元**。所有心元构成的集合称为群的**中心**，记

为 $G^{心}$。反之，令 $axa^{-1} \neq x$ 的 a 越多（轨迹越长），说明 x 与 G 中其他元素交换能力越差。这是 x 作为群元素固有的性质。我们把 $\{axa^{-1} \mid a \in G\}$ 称为 x 的（往复）**轨道**。

定理 7.1 中心是群

群 G 的中心总是其子群，称为**心群**。

证明：显然 $e \in G^{心}$。而且 $\forall\, z \in G^{心}$，$\forall\, a \in G$，

$$az = za \;\Rightarrow\; az^{-1} = z^{-1}zaz^{-1} = z^{-1}azz^{-1} = z^{-1}a.$$

因此 $z^{-1} \in G^{心}$。于是 $\forall\, x, y, \in G^{心}$，$\forall\, a \in G$，

$$ax^{-1}y = x^{-1}ay = x^{-1}ya.$$

这说明 $x^{-1}y \in G^{心}$。因此 $G^{心}$ 是子群。 □

不仅如此，由于心元往复为己，所以群的中心作为子群必然往合。可以简单验证：

$$\forall\, a \in G,\ \forall\, h \in G^{心},\quad ah = ha,$$

所以 $aG^{心} = G^{心}a$，因而是往合子群。作为往合子群，$G^{心}$ 有对应的商群。

7.3 定子与定元

轨迹关心的是“x 能走到哪里”。与之相对的问题是：“哪些群元素不变动 x?”

例子 7.7

以前法观 D_3 于 X_3。哪些群元素保持 x_1 不动?

$$e(x_1) = x_1,\quad r(x_1) = x_2,\quad r^2(x_1) = x_3,\quad s(x_1) = x_1,\quad rs(x_1) = x_2,\quad r^2s(x_1) = x_3.$$

只有 e 和 s 保持 x_1 不动。集合 $\{e, s\}$ 构成 D_3 的一个子群。

定义 7.3

以 γ 观群 G 于集合 X。给定 $a \in G$，$x \in X$，若 $\gamma(a,x) = x$，则称 a 是 x 的**定子**，x 是 a 的**定元**。x 所有定子的集合称为 x 的**定子集**：

$$G \supseteq G_x = \{a \in G \mid \gamma(a,x) = x\},$$

a 的所有定元的集合称为 a 的**定元集**：

$$X \supseteq X^a = \{x \in X \mid \gamma(a,x) = x\},$$

定子和定元是对偶的概念：定子是“定住某个特定元素的群元素”，定元是“被某个群元素定住的集合元素”。$a \in G_x \Leftrightarrow x \in X^a$。定子集有以下根本性质：

命题 7.3

观群 G 于集合 X，则 $\forall x \in X$，G_x 是 G 的子群，称为 x 的**定子群**。

证明：用子群的判定方法：取 $a, b \in G_x$，需证 $ab^{-1} \in G_x$。按定义，$b(x) = x$，所以

$$b^{-1}(x) = b^{-1}(b(x)) = (b^{-1}b)(x) = e(x) = x.$$

因此

$$(ab^{-1})(x) = a(b^{-1}(x)) = a(x) = x.$$

所以 $ab^{-1} \in G_x$。因此按子群的判断准则，G_x 是 G 的子群。 □

取 $X = G$，以左乘观群于自身，则任何群元素的定子群都是平凡子群 $\{e\}$，幺元以外任何群元素的定元集都是空集。如果以往复观群于自身，则群元素 x 的定子群可以写为：

$$G_x = \{a \in G \,|\, axa^{-1} = x\} = \{a \in G \,|\, ax = xa\}.$$

即所有与 x 交换的群元素的集合。我们称之为 x 的**交心集**。由上可知，交心集是 G 的子群，也叫**交心群**。而如果换一个角度，把 x 看作群变换来看，那么交心集就是它以往复观的定元集。

回顾用连线图理解群变换的做法，我们用给多边形顶点标记不同颜色的方法来说明变换。这也是一种观群法。如果所有顶点之间没有区别，那么群变换不会改变所见状态，这时图形的定子群就是整个群 G。将顶点染上不同颜色后，各种变换就能造成变化了。

还记得我们把“什么都不做”在连线图里忽略掉这件事吗？实际上，连线图和生成路径图里，每个状态节点都有一个到自身的变换 e，但我们将它忽略了。如果我们不好好把图形染色，就会有更多的变换被忽略掉。

如果我们把连线图里看作群显相于多边形顶点状态的集合 X，状态节点是 X 的元素，那么染色的效果就是把定子群缩减到 $\{e\}$。实际上，如果某个群变换 $a \neq e$ 不改变 X 某个状态 x（$a(x) = x$），我们就说它对 x **无效**。对 x 无效的变换构成它的定子群。在连线图的例子里，这个变换的箭头就从这个节点指向自身。而如果它对整个状态集合都无效，那么就会和“什么都不做”一样，被我们忽略掉。这时我们说 γ 无法让 a 显相。换句话说，这时 a 的定元集是整个 X。反之，如果 e 以外的群元素都能让 X 至少一个元素变动，就说 γ **有效**。有效的观群法里只有 e 的定元集是整个 X，我们说观群法令群在 X 上显**明相**。若 γ 无法令群显明相，我们就无法观整个群：有群元素完全“隐身暗中”，无法被我们通过观群法观察到。

如果更进一步，群元素 a 能让所有 $x \in X$ 都“动起来”（$a(x) \neq x$），就说 a **无定**。无定元的定元集是空集，它不在任何定子群中。在连线图的例子里，多边形顶点两两不同色，就让 e 以外的群元素都成了无定元，把所有状态的定子群都缩减到 $\{e\}$；它们的定元集都是空集。我们称这样的观群法**行健**，群在 X 上显**行相**。行健必然有效，反之不然。行相必然是明相，反之不然。以左乘观群于自身，群必然显行相。以往复观群于自身，则群一般不显行相。

群显行相，但未必贯通。如果有不通达的状态，那么就无法构成完全的连线图。连线图的例子里，我们选择生成元来生成群，确保状态之间相互通达。行健而贯通的观群法 γ，称为**得宜**的。考虑从任意 $x \in X$ 出发的映射：

$$\begin{aligned} \phi_x : \quad G &\longrightarrow X \\ a &\longmapsto \gamma(a, x) = a(x) \end{aligned}$$

如果 G 贯通 X，那么 $\forall y \in X$，总有 $a \in G$ 使得 $\phi_x(a) = a(x) = y$。于是 ϕ_x 是满射。如果 G 在 X 上行健，所以 $\forall a, b \in G$，只要 $a(x) = b(x)$，那么 $x = a^{-1}(a(x)) = a^{-1}(b(x)) = (a^{-1}b)(x)$。这说明 $a^{-1}b = e$，即 $a = b$。于是 ϕ_x 是单射。因此，只要观群得宜，ϕ_x 就是双射，G 和 X 之间能建立一一对应的关系，而且固定出发点后，X 中每个元素到另一个元素的变动，恰好是一个群元素的体现。我们称群在 X 上显**实相**。

连线图就是观群得宜的表现。经过染色后，图形的对称变换构成的群都在其顶点状态集合上行健且贯通，所以我们能够画出连通的生成路径图，并且把状态和群元素一一

对应起来。如果我们不为顶点染上两两不同的颜色，其对称变换构成的群就不一定恰好能对应其顶点状态集合了。

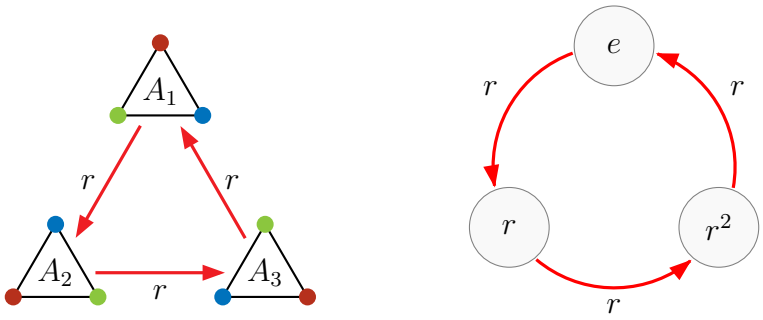


图 7.3: 观群得宜等价于左乘观群于自身

注：既然观群得宜时 G, X 一一对应，考虑以左乘观 G 于自身：$\gamma_{左}$，有：

$$\phi_x(\gamma_{左}(b,a)) = \phi_x(ba) = \gamma(ba,x) = \gamma(b,a(x)) = \gamma(b,\phi_x(a)).$$

这个关系说明了什么呢？说明所有得宜的观群法本质上都是左乘观在另一个集合 X 的“映像”。换句话说，以 $x \in X$ 为起点，依次经过 $a \to b \to c$ 变换得到 $a(x), ba(x), cba(x)$，和从群的幺元 e 出发，左乘得到 a, ba, cba，过程是一样的。两者之间只差一个双射 ϕ_x。也就是说，**得宜的观群法都等价于以左乘观群于自身**。这就是我们能通过连线图揭示群自身结构的原因。

7.4 轨定定理

再来看正方体旋转群的例子。

例子 7.8

观正方体旋转群 $G = \mathsf{T}_6$（24 个元素）于其 8 个顶点。取一个顶点 V_1。哪些旋转保持 V_1 不动？只有绕通过 V_1 和其对心顶点的对角线（称为顶心对角线）的旋转变换：旋转 0°、120°、240°，共 3 个。所以 $|G_{V_1}| = 3$。

观 G 于棱：取一条棱 E_1。保持 E_1 不动的旋转是恒等变换和绕通过 E_1 中点与对棱中点的直线（称为对棱中线）旋转 180° 的变换，共 2 个。所以 $|G_{E_1}| = 2$。

观 G 于面：取一个面 F_1。保持 F_1 不动的旋转：绕通过 F_1 中心与对面中心的直线（称为面心对角线）旋转 0°、90°、180°、270°，共 4 个。所以 $|G_{F_1}| = 4$。

这些观群法都显明相，但都不显行相，因此不得宜。

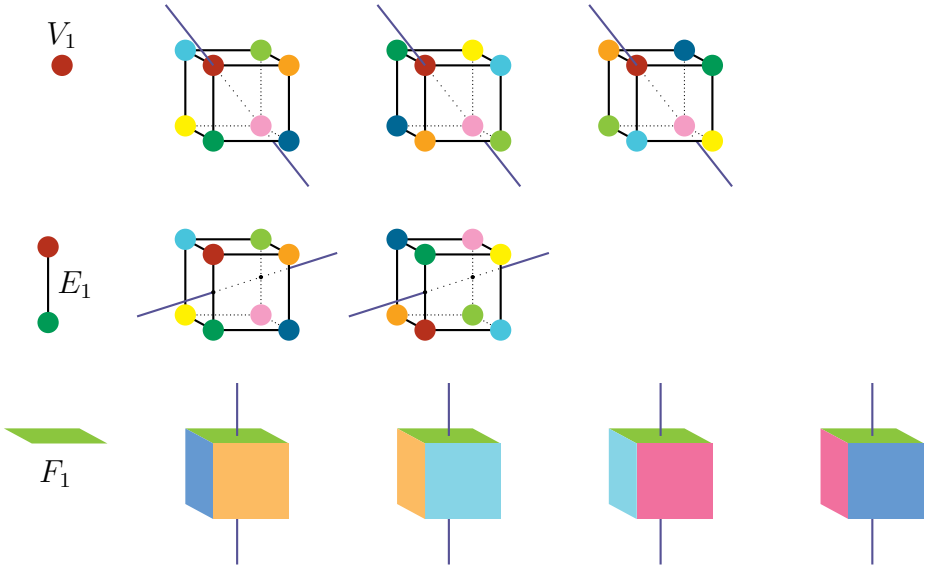


图 7.4: 固定正方体一个顶点、一条棱、一个面不变的旋转

上面的例子中，我们观察到这样一个事实：顶点数、棱数、面数，乘以相应每个对象的定子群元素个数，总得到同一个数：24。也就是正方体旋转群 G 的势。这是巧合吗？还是普遍规律？

相集	$\lvert G\rvert$	$\lvert X\rvert$	$\lvert G_x\rvert$
顶点	24	8	3
棱	24	12	2
面	24	6	4

再来看一些别的例子。观映轮群 D_3 于正三角形的 3 个顶点，保持每个顶点不变的变换只有恒等变换和过该顶点的中线的翻转变换，共 2 个。乘以顶点数 3，得到 $6 = |\mathsf{D}_3|$。仍然符合规律。

但如果我们把正三角形换成正六边形呢？观映轮群 D_3 于正六边形的 6 个顶点。如果 D_3 中的翻转变换过正六边形的顶点，那么保持每个顶点不变的变换有 2 个：恒等变换和过该顶点的中线的翻转变换。但乘以顶点数 6，得到 12，不是 $|\mathsf{D}_3|$ 了。

所以，关键不在于顶点总数，在于每个顶点的轨迹长度。前面的例子里，群总显通相，所有元素的轨迹都贯通整个集合，所以轨迹长度等于集合的势。正六边形的例子里，

两者不再相等，就能看出真正的规律了。正六边形中，每个顶点经 D_3 的轨迹长度为 3，而不是 6。

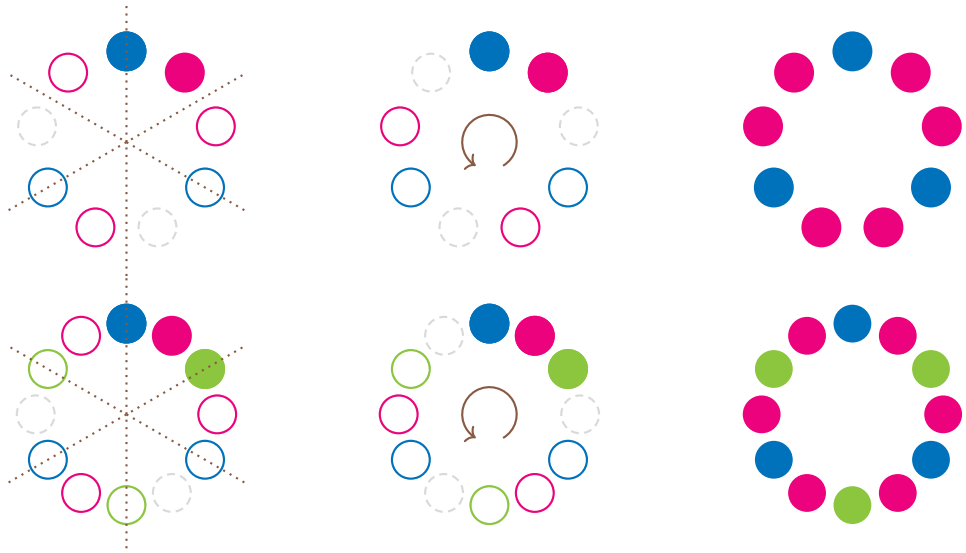


图 7.5: 正九边形和正十二边形顶点经 D_3 变换的轨迹

我们可以用正九边形和正十二边形来验证。假设 D_3 中的翻转变换过正多边形的某顶点。正九边形中，有 3 个顶点在 D_3 的对应翻转变换下不变，另外 6 个顶点则只在恒等变换下不变。分析它们的轨迹：前 3 个顶点归属同一个轨迹，后 6 个顶点归属另一个轨迹。而 $3 \times 2 = 6 \times 1 = 6$。

正十二边形中，有 6 个顶点在 D_3 的对应翻转变换下不变，另外 6 个顶点则只在恒等变换下不变。分析它们的轨迹：前 6 个顶点在旋转变换下，分为两个轨迹。每个轨迹包含 3 个顶点。后 6 个顶点则同属一个轨迹。同样，$3 \times 2 = 3 \times 2 = 6 \times 1 = 6$。

所以，真正的规律是：$|\mathcal{O}_G(x)| \times |G_x| = |G|$。这背后的原理是什么呢？

我们可以这样理解：x 的轨迹就是用 G 中元素不断地变动 x、“移动” x 得到的所有结果，是“x 能到什么地方”的集合，因此，里面各个不同的元素，就是“x 能往哪里走”的不同回答。换句话说，我们可以把 $\mathcal{O}_G(x)$ 里的元素看作某种“往集”的“代表元”。当然，这里的“往集”不是真正的 G 中子群的往集。然而，由于显相映射兼容群运算，我们能够建立群的某个往集与这个“往集”之间的关联映射，也就是同态。这个真正的往集是谁的往集呢？自然就应该是让 x 不动的定子群 G_x 的往集了。下面就把这个结论和证明严格地写出来：

定理 7.2 轨定定理

观有限群 G 于集合 X，则

$$\forall\, x \in X, \quad |G| = |\mathcal{O}_G(x)| \cdot |G_x|.$$

证明：如上所说，证明的关键是建立 G_x 的左往集与轨迹 $\mathcal{O}_G(x)$ 之间的双射。

首先证明：$g(x) = h(x)$ 当且仅当 g 和 h 属于 G_x 的同一个左往集。

若 $g(x) = h(x)$，则 $h^{-1}(g(x)) = h^{-1}(h(x)) = x$，即 $(h^{-1}g)(x) = x$，所以 $h^{-1}g \in G_x$，于是 $g = h(h^{-1}g) \in hG_x$。

反之，若 $g \in hG_x$，即有 $k \in G_x$ 使得 $g = hk$。于是 $g(x) = (hk)(x) = h(k(x)) = h(x)$。

接下来定义从 G_x 的左往集集合到 $\mathcal{O}_G(x)$ 的映射 φ：$gG_x \mapsto g(x)$。

由前可知，φ 的定义与往集代表元的选取无关。φ 是满射，因为按 $\mathcal{O}_G(x)$ 的定义，其中任何元素都可写成 $g(x)$。φ 也是单射，因为若 $g(x) = h(x)$，则 $gG_x = hG_x$。

因此 φ 是双射，左往集的个数等于 $|\mathcal{O}_G(x)|$。

由往集定理，G_x 的左往集个数乘以 $|G_x|$ 就是群 G 的势，即：

$$|G| = |G_x| \cdot |\mathcal{O}_G(x)|.$$

□

这个证明的核心工具是往集。定子群 G_x 是子群，它的左往集把 G 分划成若干块，每一块对应轨迹中的一个元素。轨迹的大小和子群的往集个数，通过往集定理联系起来。

本章小结

本章回到“群是对称性的刻画，群元素是作用于集合的变换”的根本观念，引入**群观**的概念。主要知识点如下：

- **群观与显相**：以显相映射 γ 观群 G 于集合 X，须满足 $\gamma(ab,x)=\gamma(a,\gamma(b,x))$ 与 $\gamma(e,x)=x$。映射 $a\mapsto\gamma_a$ 是 G 到 S_X 的群同态。因此，**群观的本质就是群到置换群的同态**。
- **轨迹**：群元素就是 X 上的变换。从 x 出发，在 G 的所有变换下能到达的元素集合 $\mathcal{O}_G(x)=\{a(x)\mid a\in G\}$。轨迹构成 X 的等价分划。若 X 只有一条轨迹，称 G（以 γ）**贯通** X，显**通相**于 X。
- **观群于自身**：令集合 $X=G$，即观群于自身。有左乘观、往复观等观法。以左乘观群必显通相。
- **环圈**与**轮换**：全置换群 S_n 以 $\gamma(\sigma,i)=\sigma(i)$ 自然显相于 $\{1,2,\cdots,n\}$。其中元素经置换 σ 生成的循环子群的轨迹称为 σ 的环圈。只有一个长度大于 1 的环圈的置换称为轮换。轮换的环道和该环圈等长。
- **定子与定元**：保持 x 不动的群元素构成 G 的子群 G_x，称为 x 的**定子群**；被 a 定住的集合元素构成 X^a，称为 a 的**定元集**。两者是对偶概念：$a\in G_x\iff x\in X^a$。只有幺元能定住 X 全集说明群**有效**，显**明相**；幺元以外都不是定子说明群**行健**，显**行相**。行健且贯通称为**得宜**，此时群到集合有双射，群显**实相**。**观群得宜等价于以左乘观群于自身**。
- **心元与交心**：与所有群元素交换的元素称为**心元**，全体心元构成**心群** $G^{\text{心}}$，它是往合子群。与特定元素 x 交换的群元素构成**交心集**（交心群），它是往复观下 x 的定子群。
- **轨定定理**：观群于集合时，集合元素经群变换的轨迹长度，乘以其定子群势，等于群势。

$$\boxed{|G| \;=\; |\mathcal{O}_G(x)|\cdot|G_x|}$$

轨定定理本质上是往集定理在群观下的体现。

7.5 习题

1. 以下的映射 $\gamma\colon G\times X\to X$ 是观群的显相映射吗? 请说明理由。

(1) G 是 $\{1,-1\}$ 关于乘法构成的群，$X=\{-1,0,1\}$。$\gamma(a,x)=a+x$。

(2) G 是 $\{1,-1\}$ 关于乘法构成的群，$X=\{-1,0,1\}$。$\gamma(a,x)=ax$。

(3) G 是整数加法群 $(\mathbb{Z},+)$，$X=\mathbb{Z}$。$\gamma(a,x)=x+a^2$。

(4) G 是任意非平凡群，$X=G$。$\gamma(a,x)=xa$。

(5) G 是任意非平凡群，$X=G$。$\gamma(a,x)=xa^{-1}$。

(6) G 是模 5 加法群 $\mathbb{Z}_5$，$X=\mathbb{Z}$。$\gamma(a,x)=ax$[①]。

(7) G 是正三角形的对称群 D_3，X 是同中心的正方形顶点集合。$\gamma(a,x)=a(x)$ 表示以 a 变换 x 的结果。

(8) G 是平面直角坐标系中关于过原点和 $(1,1)$ 的单位正方形的映轮群 D_4，$X=\{(m,n)\,|\,m,n\in\mathbb{Z}\}$ 是平面格点集合。$\gamma(a,x)=a(x)$ 表示以 a 变换 x 的结果。

2. 群 G 有 35 个元素，集合 X 有 19 个元素。观 G 于集合 X，使得 X 中元素轨迹长度都大于 1。一共有几个轨迹? 每个轨迹有多长?

3. 观群 G 于 X，证明：$\forall x\in X$，$g\in G$，$g(x)$ 的定子群是 gG_xg^{-1}。

4. 设 p 是素数，n 是正整数，群 G 有 p^n 个元素。证明：G 的中心不只有幺元 e。

5. 设有限群 G 的势为 n，p 是 n 的最小素因数。H 是 G 的子群，其元素个数为 $\frac{n}{p}$。我们想证明 $H\lhd G$。

(1) 说明 H 有几个左往集。

(2) 记 X 为 H 的所有左往集的集合。证明，可以：$\gamma(x,A)\mapsto xA$ 观 G 于 X。

(3) 记 G 到 S_X 的自然群同态 $\varphi\colon x\mapsto\gamma_x$ 的核为 N，证明 $N\subseteq H$。

(4) 证明 $N=H$。并说明为何 $H\lhd G$。

[①]此处的 ax 表示将 a 视为普通整数与 x 相乘。

以下是可以用作正式测验的成套试题。每套试题都有一个主要问题。通过不断解答各个小问，可以逐步得到主要问题的答案。这些试题有两种使用方法。

- 如果你希望检验自己通过本书掌握了多少知识和方法，可以严格地使用这些试题进行测试。每套试题大约需要 3 ～ 4 个小时来解答。你不必答完一道题才开始答下一题，承认之前问题的结论并用来解决后面的问题是允许的。
- 如果你只是希望借着做题来了解更多的知识，那么可以像之前的习题一样，在每小问上思考数分钟，如果仍然没有思路就查看参考解答。这些问题之间的联系和系统性更高，可以多体会问题之间的联系，思考其整体思路。

正方体与正四面体的旋转群

本题的目的在于研究正方体旋转群 $\mathsf{T}_6 \cong \mathsf{S}_4$ 和正四面体的旋转群 A_4 的关系。考虑备有直角坐标系的空间 $\mathbb{R}^3$ 中的正方体。其顶点坐标为集合 $V = \{(\pm 1, \pm 1, \pm 1)\}$。

第一部分 形体探究

1. 考虑以下映射：

$$\begin{aligned} \phi : \quad V &\longrightarrow \{\pm 1\} \\ (x, y, z) &\longmapsto xyz \end{aligned}$$

它将正方体的顶点分为两组，记为集合 $T^+ : \{(x, y, z) \in V \,|\, xyz = 1\}$、$T^- : \{(x, y, z) \in V \,|\, xyz = -1\}$。说明这样分类的 T^+, T^- 两组顶点有什么直观特征。

2. 证明：能够把正方体的顶点分为两个子集，每个子集对应一个正四面体的顶点。这样得到的正四面体的中心在哪里?

3. 证明：T_6 中通过面心的 90° 旋转，把 T^+, T^- 互相变为对方。

4. 证明：T_6 中通过体心的 120° 旋转，把 T^+, T^- 变为自身。

5. 证明：T_6 中通过对棱中线的 180° 旋转，把 T^+, T^- 互相变为对方。

6. 证明：T_6 中任意变换 τ 都把 T^+, T^- 映射到两者之一。即总有 $\tau(T^+) = T^+$ 或 $\tau(T^+) = T^-$，$\tau(T^-) = T^+$ 或 $\tau(T^-) = T^-$。用 ϕ 和 τ 叙述这个性质。

第二部分 观群

7. 记 $\mathsf{T} = \{T^+, T^-\}$，观 T_6 于 T：

$$\begin{aligned} \gamma : \ \mathsf{T}_6 \times \mathsf{T} &\longrightarrow \mathsf{T} \\ (\sigma,\, t) &\longmapsto \sigma(t) \end{aligned}$$

说明它确是观群法，且 T_6 显通相。

8. 记 $H \triangleleft \mathsf{T}_6$ 为 T^+ 的定子群。它有几个元素？说明它是往合子群。

9. 说明群同态 $\varphi : \sigma \mapsto \gamma_\sigma$ 的核和像。

10. 证明商群 $\mathsf{T}_6 \big/ H$ 同构于 S_T，它同构于哪个我们学过的群？

11. 回忆：我们如何把 T_6 中的变换与 S_4 中的置换对应？H 中的变换具体有哪些？对应哪些置换？

12. H 中的变换如何变换 T^+？说明 H 就是正四面体的旋转群 A_4。

第三部分　对换与奇偶性

13. 正方体的哪种旋转对应 S_4 中的对换？它属于 A_4 吗？

14. 证明：通过正方体面心的 $90°$ 旋转可以表示为对换的复合。

15. 证明：S_4 中元素总能表示为对换的复合。

16. 证明：A_4 中的元素总能通过 S_4 中元素重复两次得到：$\forall \sigma \in \mathsf{A}_4$，$\exists \tau \in \mathsf{S}_4$ 使得 $\sigma = \tau^2$。

17. 证明：A_4 中的元素总能表示为偶数个对换的复合，S_4 中其余元素总能表示为奇数个对换的复合。

18. 考虑 $\{\pm 1\}$ 关于乘法构成的群，仍记为 $\{\pm 1\}$。用 γ_σ 给出一个从 S_4 到 $\{\pm 1\}$ 的群同态，使其核为 A_4。

19. 证明：S_4 中元素不可能既表示为偶数个对换的复合，又表示为奇数个对换的复合。

★ ★ ★ ★ ★

对称差积与置换的符号

设正整数 $n \geqslant 2$。记 $\mathbb{R}[x_1, x_2, \cdots, x_n]$ 为所有 n 元实系数整式的集合。对 $\sigma \in \mathsf{S}_n$ 与整式 p，规定

$$\gamma(\sigma,\, p) \;=\; p\big(x_{\sigma(1)},\, x_{\sigma(2)},\, \cdots,\, x_{\sigma(n)}\big)\,,$$

以下也简记为 $\sigma \cdot p$。记

$$\Delta_n \;=\; \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)\,.$$

第一部分　低维观察

1. 证明以 γ 可观 S_n 于 $\mathbb{R}[x_1, x_2, \cdots, x_n]$ 。（即说明它契义，并验证 $\gamma(e, p) = p$ 与 $\gamma(\sigma, \gamma(\tau, p)) = \gamma(\sigma\tau, p)$。）

2. 设 $n = 2$。计算 $(1\,2) \cdot \Delta_2$，并求 Δ_2 的轨迹与定子群。

3. 设 $n = 3$。逐个计算

$$e, \quad (1\,2), \quad (1\,3), \quad (2\,3), \quad (1\,2\,3), \quad (1\,3\,2)$$

施于 Δ_3 的结果，列成表格。哪些置换保持 Δ_3 不变？哪些把它变号？

4. 根据第 2、3 问的观察，猜想：对一般的 n 与 $\sigma \in \mathsf{S}_n$，$\sigma \cdot \Delta_n$ 与 Δ_n 之间有什么关系？

第二部分　符号同态

5. 考虑二元集 $\{i, j\}$ 的集合 $\Gamma_n = \{\{i, j\} \,|\, 1 \leqslant i < j \leqslant n\}$。给定 $\sigma \in \mathsf{S}_n$，考虑 Γ_n 上的映射 $\phi_\sigma :\ \{i, j\} \mapsto \{\sigma(i), \sigma(j)\}$。证明它是双射。

6. 证明：存在唯一的 $\varepsilon(\sigma) \in \{1, -1\}$，使得

$$\sigma \cdot \Delta_n \;=\; \varepsilon(\sigma)\, \Delta_n.$$

7. 定义 $\leftmoon(\sigma) = \varepsilon(\sigma)$。设 $\{1, -1\}$ 关于数的乘法成群。证明 $\leftmoon :\ \mathsf{S}_n \longrightarrow \{1, -1\}$ 是群同态。

8. 证明：任一对换 $(a\,b)$ 都满足 $\operatorname{sgn}\big((a\,b)\big) = -1$。（提示：设 $a < b$，把 Δ_n 的因子分成三类：同时含 a, b 的、恰含 a, b 之一的、两者都不含的。考察交换 x_a, x_b 时每一类的变化。）

9. 求 Δ_n 的轨迹。记 H_n 为 Δ_n 的定子群。

(1) 用轨定定理求 $|H_n|$。

(2) 说明 H_n 是 S_n 的往合子群。

(3) 商群 $\mathsf{S}_n \big/ H_n$ 同构于哪个我们学过的群？

第三部分　奇偶性

我们承认以下结论为真：n 元置换总可以写成有限个对换的复合。以下各问可直接使用该结论。

10. 设 $\sigma = \tau_1\tau_2\cdots\tau_k$，其中每个 τ_i 都是对换。

(1) 证明 $\operatorname{sgn}(\sigma) = (-1)^k$。

(2) 说明 k 的奇偶性由 σ 唯一确定，与所用的分解方式无关。

(3) 我们称 $\operatorname{sgn}(\sigma) = 1$ 的置换为**偶置换**，$\operatorname{sgn}(\sigma) = -1$ 的置换为**奇置换**。说明 H_n 恰是全体偶置换构成的集合，记为 A_n；并说明全体奇置换恰好构成 H_n 的另一个往集。

第四部分　逆序数与例子

11. 定义 $\operatorname{inv}(\sigma)$ 为集合 $\{(i,j) \mid i < j,\ \sigma(i) > \sigma(j)\}$ 的势，称为 σ 的**逆序数**。证明 $\operatorname{sgn}(\sigma) = (-1)^{\operatorname{inv}(\sigma)}$。

12. 对 $n = 2, 3, 4$，按环圈形态列出 S_n 中各类元素的个数、sgn 的值以及逆序数的奇偶。若给出逆序数的精确值，须逐个核对。写出 $\mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4$ 的全部元素。

★ ★ ★ ★ ★

第八章　计数定理

考虑一串项链，它由十几个或几十个珠子串成。如果有三种颜色的珠子可用，数量不限。那么，用 n 个珠子，可以串出多少种不同的项链?

天真的想法是：每个位置有 3 种选择，n 个位置就有 3^n 种选择，于是可以串出 3^n 种不同的项链。但是，稍微想深一层就知道，一种串法稍微转一转，就可能和另一种串法重合。通过旋转，看似不同的项链实质上是一样的。

如果 n 个位置都用一种颜色的珠子，那么显然只有一种项链。但如果其中有两三个位置用了别的颜色的珠子呢？我们发现，随着不同颜色珠子的位置不同，“稍微转一转”能否重合的结果也不同。这时，光靠直觉或简单数数，已经难以继续了。

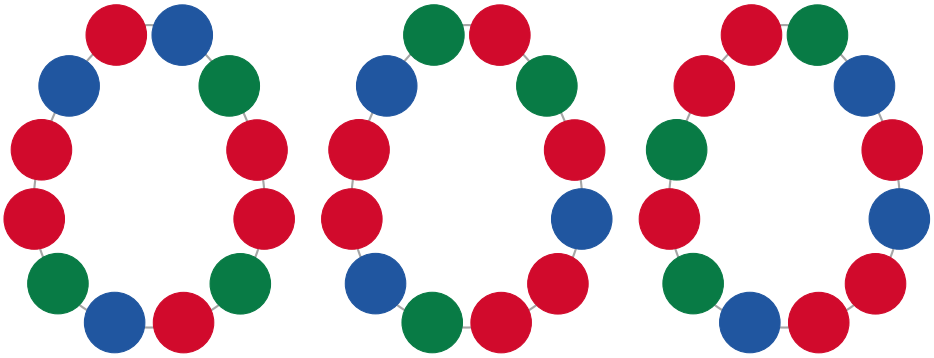


图 8.1: 三种颜色的项链

另一个类似的问题是：如何给正三角形、正方形、正方体或正多面体的顶点染色?我们假设每个顶点可以染成三种颜色之一。同样地，我们会遇到“转一转就是同一个”的问题。这类问题和我们见过的简单组合计数问题不一样。对象自带的某种对称性，让我们需要小心避免重复计数，学会合并某些看似不同的状态。这种计数问题就需要用到群的知识来分析，理解对称性带来的影响。

也许你会说，这种问题是否只是空虚的人想出来打发时间的？现实中真的会遇到这样的问题吗？

现实中确实有类似的问题。有机化学和生物、制药学科中，研究人员需要面对由固定的几种原子（主要是碳、氧、氢以及其他几种元素）或基础“组件”（原子团）组合成的各种分子。n 个原子构成的分子，可以有几种不同的形态结构？每种形态结构的化学、生物性质是否有不同？这是一个非常有意义的问题。而解决这个问题，首先就需要算清楚不同形态结构的数量。

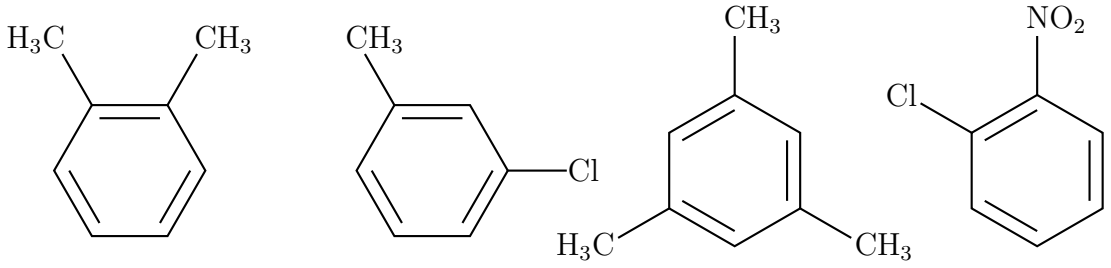


图 8.2: 苯环对接各种组件得到的化合物

举例来说，我们知道苯环是六个碳原子构成的环，可以理解为一个正六边形。它的每个碳原子都有一个能对外连接的碳氢键。这 6 个“接口”可以“接入”不同的组件，替换原有的氢原子，构成不同的分子。比如，其中两个氢原子由甲基代替，就得到二甲苯。二甲苯有几种呢？天真的想法是计算 6 个位置中放两个甲基的方法，得到 15。但显然这 15 种情况有大量重复的，因为旋转后可以互相得到，例如放在 $2,3$ 位和放在 $3,4$ 位、$4,5$ 位并无实际区别。实际上二甲苯只有三种——按照两个甲基之间隔着几个氢来分类——邻二甲苯、间二甲苯和对二甲苯。这个结果不难理解：两个甲基之间的“距离”相同的，自然就是同一种。“距离”最少是 0，最多是 2，因此一共有 $0,1,2$ 三种。

对于更复杂的情况，这种简单分类的想法就行不通了。比如：每个位置可以是氢原子，也可以接入甲基或硝基，这时有几种不同的结构呢？直接数数，你恐怕难以得到结果，而且还会担心数重了或数漏了。这时候，我们需要系统、有理论支撑的方法来进行计算。而群作为表示对称性的抽象结构，就派上用场了。

8.1 计数与群

首先让我们用一个简单的例子来把问题说清楚。假设我们要给一个正方形的四个顶点染色，制作成纪念礼品或小挂件。每个顶点可以染成红色或蓝色（见下图）。

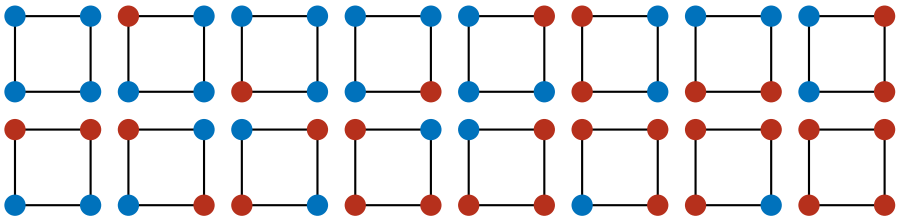


图 8.3: 把正方形四个顶点染成红蓝两色，不考虑对称

如果不考虑正方形带来的对称性，那么一共有 $2^4 = 16$ 种方法。这就是我们要处理的集合 S。S 有 16 个元素，每个元素就是上图中的一种染色方案。

接下来我们要考虑正方形的对称性。作为纪念品或小挂件，我们可以随意旋转、翻转这个正方形。如果两种方案经过旋转或翻转得到同一个结果，就说它们是同一个染色方案。这样，真正的染色方案数量就要少于 16 种了。某些方案（比如第一排第 $2, 3, 4, 5$ 四种方案）会被合并成一个方案。这种现象的背后，是正方形的对称群 D_4 在起作用。

观 D_4 于 S，可以看到，旋转和翻转变换把某些方案变成另一些方案。给定一个方案，D_4 的元素能将它变成哪些别的方案呢？这是我们上一章提过的轨迹。比如，只有一个红色顶点的四个方案，能够通过旋转互相得到，于是它们属于同一个轨迹。而计算在旋转和翻转变换下本质不同的染色方案个数，就是计算 D_4 显于 S 的轨迹个数。

我们可以直接数一下 D_4 显于 S 的轨迹。首先从全蓝的染色方案出发，它在任何旋转和翻转变换下都只是它自己，所以它的轨迹就是自己。它是任何群元素的定元，它的定子群是 D_4。

再来看恰有一个红色顶点的染色方案。这样的方案有 4 个。从任一个方案出发，通过旋转可以得到另外三个。通过翻转也只能得到这三个。所以它的轨迹是所有 4 个恰有一个红色顶点的方案。对每个方案来说，其定子群是以过红色顶点的对角线为对称轴的翻转变换生成的二元群。

恰有两个红色顶点的染色方案有两类。一类是两个红色顶点成对角线；一类是两个红色顶点成一条边。我们把前者称为对角型，后者称为单边型。对角型方案经过旋转和翻转，还是对角型方案；单边型方案经过旋转和翻转也还是单边型方案。因此，我们有两条轨迹：2 个对角型方案和 4 个单边型方案。对角型方案的定子群包括以两条对角线为轴的翻转，以及 180° 的旋转。这个子群有 4 个元素。单边型方案的定子群包括过该边中点和正方形中心的直线为对称轴的翻转，是二元群。

恰有三个红色顶点以及全红的染色方案，分析方法和恰有一个红色顶点、全蓝的分

析方法一样。因此，我们得到 6 条轨迹，长度分别是 $1, 4, 2, 4, 4, 1$。这 6 条轨迹也说明，本质的染色方案有 6 种。

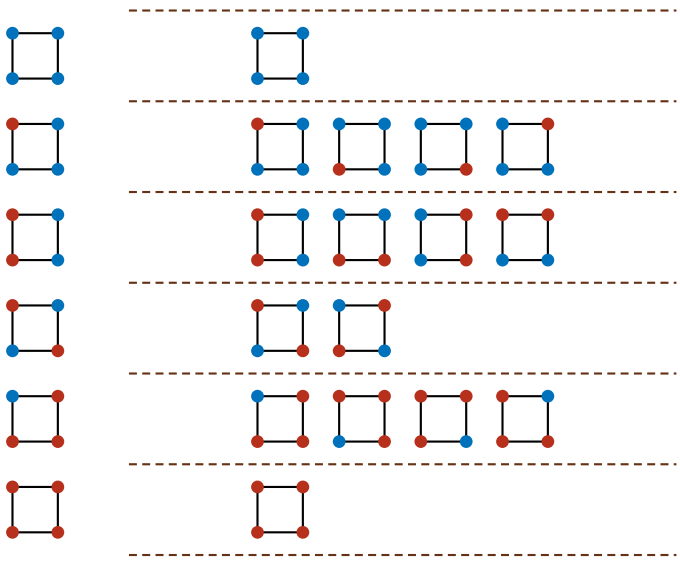


图 8.4: 各个轨迹的元素

以上的解法其实很清晰。上面提到的项链、苯环衍生物等问题，也可以这么解决。写出不考虑对称性时所有的状态 S，找出所有对称性构成的群 G。然后对每个元素 $x \in S$，找出它在 G 的变换下的轨迹，归为一类。所有轨迹的个数就是答案。这个解法的困难在于：当 S 变得很大的时候，分析 S 中各个元素的轨迹，找出轨迹个数，就变成了一个棘手的问题：运算量太大了。比如，如果我们想讨论用三种颜色的 20 个珠子串成一个项链，对应的状态集合 S 就有 $3^{20} \approx 3.49 \times 10^9$ 个元素。逐个分析这些元素在群变换下的轨迹，显然是不现实的。

8.2 定元分轨定理

我们尝试从另一个角度来看这个问题。各个元素的轨迹之所以难数，是因为每个元素的轨迹不一样长。如果 S 的势是 n，其中所有元素的轨迹长度都是 m，那么轨迹数就是 $\frac{n}{m}$ 了。多么轻松！有没有一种方法，把所有元素的轨迹都变得一样长呢？

让我们回忆上一章的结论：

$$\forall\, x \in S, \quad |G| = |\mathcal{O}_G(x)| \cdot |G_x|.$$

这个结论其实在某种意义上告诉我们，为什么 S 中元素 x 的轨迹 $\mathcal{O}_G(x)$ 长短不一。它

们乘以自己的定子群 G_x 的元素个数，都得到群势 $|G|$，可每个元素对应的定子群，大小不一样。于是，作为 $|G|$ 除以 $|G_x|$ 的商，x 的轨迹自然也有长有短了。轨迹越长，说明对应的定子群越小，另一种角度来看，就是这个元素的对称性比较低，能让它不变的变换不多，能让它变来变去的变换很多。反之，轨迹越短，说明这个元素的对称性越高。

于是有这样一个想法：把每个轨迹中的元素都重复 $|G_x|$ 遍，所有元素的轨迹不就都一样长了吗？这时候，我们的自定义“轨迹”长度总是 $|G|$。但这样的“轨迹”有什么意义呢？它可以看作把原来每个轨迹里的元素都按 $|G_x|$ 加权了再来求和。对于原轨迹里的某个 $x \in S$，G_x 表示使得 $g(x) = x$ 的变换 $g \in G$ 的个数。可以理解为这样一个计数器：只要有 $g(x) = x$ 这件事，就记录一次，计数器读数增加 1。因此，所有加权“轨迹”之和，就是“$g(x) = x$ 事件”集合 $A = \{(g, x) \,|\, x \in S, g \in G, g(x) = x\}$ 的元素个数：

$$|A| = \sum_{\mathcal{O} \in \mathcal{O}_G(S)} \sum_{x \in \mathcal{O}} |G_x| = \sum_{x \in S} |G_x|.$$

其中 $\mathcal{O}$ 表示轨迹，$\sum_{\mathcal{O} \in \mathcal{O}_G(S)}$ 表示遍历所有轨迹，$\sum_{x \in \mathcal{O}}$ 表示遍历轨迹中的各个元素 x。于是整体来说就是遍历了 S。

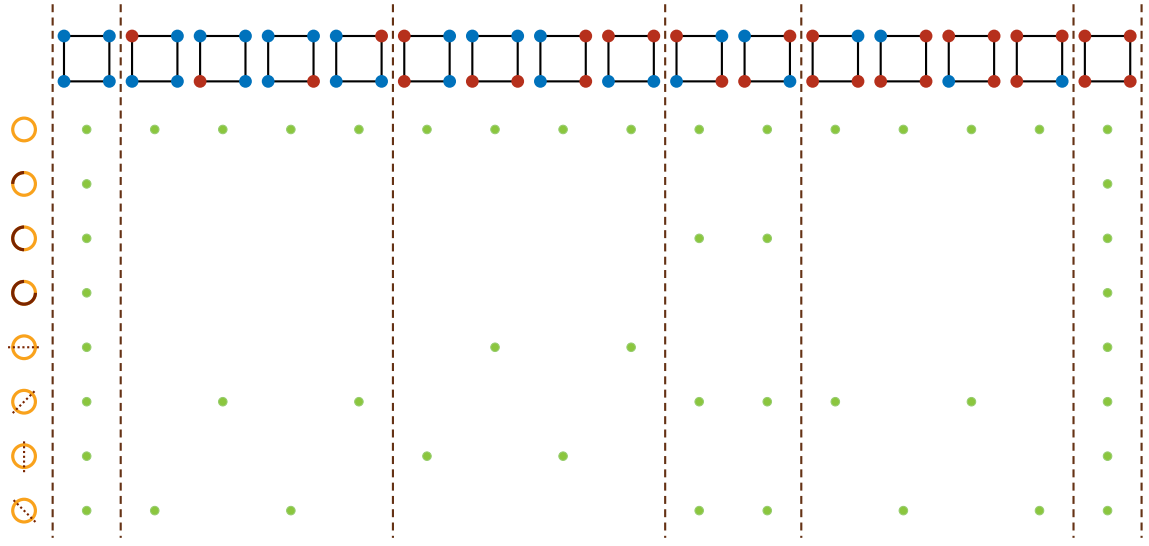


图 8.5: 统计所有“$g(x) = x$ 事件”（绿点）。每个轨迹（虚线栏）内加总都是 8 个。

另一方面，我们可以把 A 看作另一种方法累计的结果，即从 G 中变换的角度来遍历“$g(x) = x$ 事件”。对于 $g \in G$，我们遍历 S，考虑所有的 $g(x)$。只要 $g(x) = x$，计数器读数就增加 1。当 g 也遍历群 G 时，我们会再次得到 A 的元素个数。

$$|A| = \sum_{g \in G} \sum_{g(x) = x} 1 = \sum_{g \in G} |\{x \in S \,|\, g(x) = x\}| = \sum_{g \in G} |S^g|.$$

其中 S^g 就是我们定义过的定元集，它包括被群中的变换 g“定住”的 S 中元素，或者说 g 无法改变的元素。

于是，我们得到这样一个方法：从每个 g 中变换出发，考虑它“定住”的 S 中元素个数 $|S^g|$。遍历 G 后加总，得到 $|A|$，然后利用

$$|A| = \sum_{\mathcal{O}} \sum_{x \in \mathcal{O}} |G_x| = \sum_{\mathcal{O} \in \mathcal{O}_G(S)} |G| = |\mathcal{O}_G(S)| \cdot |G|.$$

就得到：

$$|\mathcal{O}_G(S)| = \frac{|A|}{|G|} = \frac{\sum_{g \in G} |S^g|}{|G|}.$$

我们把这个结论称为**定元分轨定理**。

定理 8.1 定元分轨定理

> 观群 G 于 S，群元素的定元集的平均数，就是 G 分 S 的轨迹数。

我们先用这个方法把正方形染色的例子再算一遍。正方形的旋转和翻转构成映轮群 D_4。D_4 有 8 个元素：$e, r, r^2, r^3, s, rs, r^2s, r^3s$。其中 r 表示逆时针旋转 90°，s 表示沿水平中线翻转。我们来看每个元素能定住哪些状态。

- e 什么都不改变，所以能定住所有 16 个状态。
- r 会把每个顶点变换到相邻顶点。要定住一个状态，就要求该状态的每个顶点都和它相邻顶点同色。于是它只能定住全红、全蓝 2 个状态。r^3 同理。
- r^2 会把对角顶点互换。要定住一个状态，就要求该状态的两对对角顶点同色，至于同什么色，可以自由选择。于是它能定住 $2^2 = 4$ 个状态。
- s 会把上方两顶点和下方两顶点对调。要定住一个状态，就要求该状态两对上下顶点同色，至于同什么色，可以自由选择。于是它能定住 $2^2 = 4$ 个状态。r^2s 是把左右顶点对调，同理可知它也能定住 4 个状态。
- rs 会固定“左下-右上”对角线，而调换“左上-右下”对角线的两顶点。于是，要定住一个状态，就要求该状态的“左上-右下”对角线的两顶点同色，而“左下-右上”对角线的两顶点可以各自自由染色。于是有三次自由染色机会，能定住 $2^3 = 8$ 种状态。r^3s 也是固定一条对角线、调换另一条对角线顶点，同理可知它也能定住 $2^3 = 8$ 种状态。

把以上各项累加，得到：

$$\sum_{g \in G} |S^g| = 16 + 2 + 2 + 2^2 + 2^2 + 2^2 + 2^3 + 2^3 = 48.$$

因此，轨迹数为

$$|\mathcal{O}_G(S)| = \frac{\sum_{g\in G}|S^g|}{|G|} = \frac{48}{8} = 6.$$

结果与之前一致，过程似乎还更费力了。但我们可以看到一个好处：讨论 g 改变的状态时，我们只需要谈论群元素对 4 个顶点的作用效果，而不需要逐个讨论染色方案了。比如我们甚至不需要列出 rs 定住了哪 8 个状态。

当 S 增大时，这个方法尤其有用。来看一个稍微更复杂的例子：用三种颜色的 10 个珠子串成项链。这时 S 有 $3^{10} = 5'9049$ 个元素。逐个分析轨迹长度，计算量就十分大了。让我们用以上方法来计算。首先，对应的群是映轮群 D_{10}。它有 20 个元素，可以用逆时针旋转 36°（10 分之一个圆周）和翻转（比如类比正十边形的沿水平中线翻转）来生成。我们将这两个变换记为 r, s，则

$$\mathsf{D}_{10} = \{r^i \,|\, i = 0, 1, 2, \cdots, 9\} \cup \{r^i s \,|\, i = 0, 1, 2, \cdots, 9\}.$$

相比 D_4，D_{10} 的元素更为陌生，但我们在上一个例子已经找到了一些窍门：关键是分析变换在 10 个位置上的作用：把每个珠子变到哪里去。如果有几个珠子的位置能够通过这个变换形成一个闭环，那么在能被它定住的状态里，这几个珠子都必须同色。

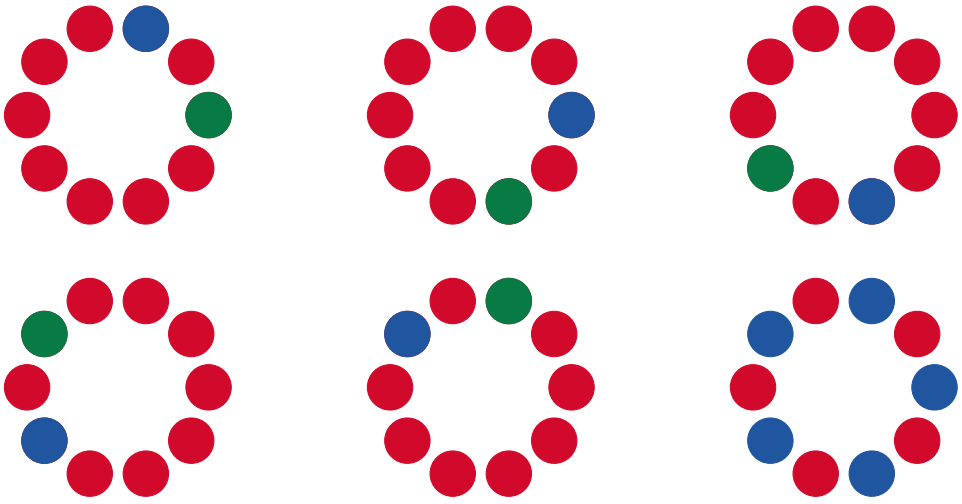


图 8.6: 顺时针旋转 72° 把蓝珠转到绿珠的位置，只有把 5 个位置都染成同色，才不会被顺时针旋转 72° 的变换改变。这 5 个位置构成一个闭环。

为了好说话，我们可以想象把珠子放置在正十边形的顶点上，即相当于讨论如何给正十边形顶点染色。我们给 10 个顶点沿逆时针顺序编号：$1, 2, \cdots, 10$。r 将所有顶点逆时针 36°，s 则把顶点 i 和顶点 $11 - i$ 对调。在 r 的变换中，每个顶点都要和下一个顶

点同色，于是所有顶点都必须同色。因此，它能定住 3 个状态（三种纯色）。而 s 则构建了 5 个“顶点对”。每一对的两个顶点分别被 s 变为对方，因此两者需要同色。至于各对顶点取什么颜色，则是自由选择。因此，有 5 次选择机会，共有 3^5 种状态能被它定住。

这里我们发现，每个变换把 10 个顶点变成了一个个的“小团体”，每个“小团体”都是一个封闭的循环。从另一个角度来看，由于这些“小团体”构成了循环，所以不断重复该变换，就能遍历这个“小团体”。如果用置换的视角来看，这就是在形容 10 元置换的环圈。

没错，以上的讨论中，我们实际上是把 D_{10}“偷换”成了同构于它的置换群。这个置换群由 10 元置换构成，D_{10} 中每个元素都唯一对应一个 10 元置换。而它们的作用效果就由 10 元置换的各个环圈决定。每个环圈内的各个顶点必须同色，而不同环圈的顶点可以不同色。因此，D_{10} 元素 g 的 $|S^g|$，就是对应 10 元置换的环圈数量 $c(g)$ 的函数：

$$|S^g| = 3^{c(g)}.$$

用这个说法把前面的结论“翻译”一遍：r 只有一个环圈（指对应的置换，下同），所以只能定住 3^1 个状态。s 有 5 个环圈，所以可以定住 3^5 个状态。这样，我们彻底把一个关于 S 的计数问题，转为了研究 G 中元素性质的问题。因为 G 中元素环圈数量是群的内在性质，可以只通过讨论 G 而得到，无需讨论 S 了。而很多时候，计算 G 中元素的环圈数量，比统计 S 中元素的轨迹的计算量小得多。

让我们把三色 10 珠项链的问题做完。问题变为分析 D_{10} 各个元素对应 10 元置换的环圈数。首先，幺元 e 对应 10 个环圈。其次，10 个旋转构成 D_{10} 的子群 H，它同构于循环群 C_{10}。r^k 的环圈个数和 k 有关，更准确地说，和 k 与 10 的最大公约数有关。如果 k 与 10 互素，那么 r^k 不断重复能遍历 C_{10}（或者说 H），环圈只有一个。如果 k 与 10 的最大公约数是 d，那么它不断重复只能生成形如 $r^d, r^{2d}, \cdots$ 的元素，因此每个环圈的长度就是 $\frac{10}{d}$。这说明它有 d 个环圈。于是可以列出以下结果：

- $i = 1, 3, 7, 9$：它们和 10 互素，对应的 r^k 只有一个环圈。
- $i = 2, 4, 6, 8$：它们和 10 的最大公约数为 2，对应的 r^k 有 2 个环圈。
- $i = 5$：和 10 的最大公约数为 5，对应的 r^5 有 5 个环圈。

另一方面，D_{10} 的翻转变换可以分为两类，每类 5 个元素。一类的对称轴是对边中点的连线，和 s 一样，对应的置换表现为 5 个对换的复合，有 5 个环圈；另一类的对称轴是

对角顶点，于是这两个顶点各自一个环圈，其他四对顶点分别一个环圈，一共 $2+4=6$ 个环圈。

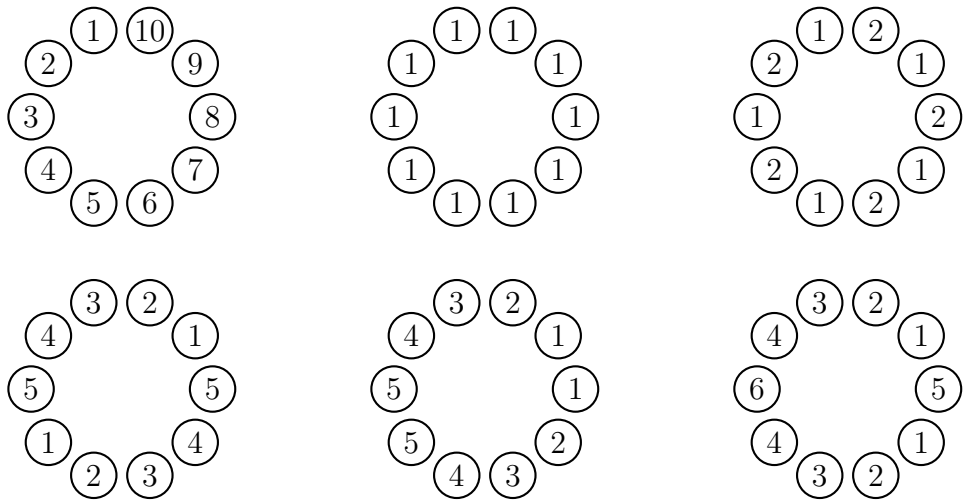


图 8.7: 各类变换形成的环圈：相同数字表示属于同一个环圈。

综上所述，我们得到所有变换的定元集个数并累加：

$$\begin{aligned}\sum_{g\in \mathsf{D}_{10}} |S^g| &= \sum_{g\in \mathsf{D}_{10}} 3^{c(g)} \\ &= 3^{10} + 4\times 3^1 + 4\times 3^2 + 1\times 3^5 + 5\times 3^5 + 5\times 3^6 \\ &= 59049 + 12 + 36 + 243 + 1215 + 3645 \\ &= 64200.\end{aligned}$$

因此，轨迹数为

$$|\mathcal{O}_{\mathsf{D}_{10}}(S)| = \frac{\sum_{g\in \mathsf{D}_{10}} |S^g|}{|\mathsf{D}_{10}|} = \frac{64200}{20} = 3210.$$

显然，相比直接在 S 中寻找 3210 个轨迹，以上方法更方便、更轻松。

让我们把以上的方法和结论总结一下：设有底座集合 X、颜色集合 C，以及把 X 中的元素映射到 C 的所有方案构成的集合 $S = C^X$：

$$C^X = \{f \mid f : X \to C\}.$$

C^X 中每个元素都是从 X 到 C 的映射。

底座集合 X 有某种对称结构或性质，可归纳为群 G。G 以 γ 显相于 X，把 X 中元素变换为另一个元素。此外，群 G 也以 Γ 显相于 S，把一种染色方案变换为另一种

方案。两个群相的显相映射 Γ, γ 之间有天然的关系：

$$\forall g \in G,\ \forall f \in C^X,\ \forall a \in X,\quad \Gamma(g,f)(\gamma(g,a)) = f(a).$$

其中 $\Gamma(g,f)$ 表示变换 g 施于染色方案 f 得到的新方案。$\gamma(g,a)$ 表示变换 g 施于 a 得到的新位置，或者说变成的新元素。以上等式的含义是：原方案中位置 a（或者说元素 a）的染色结果，经过变换 g，在新方案中，被移到了新的位置上。这说明，群变换只是变换底座集合中各个元素，原方案的映射“本质”通过群变换并没有改变，只是转移位置。这也是我们能够通过对称性合并方案，得到本质相同的方案的基础。

在此基础上，我们通过群 G 到 S_X 的同态，把群元素映射到底座集合上的置换，然后统计各个置换的环圈。记 g 对应置换的环圈个数为 $c(g)$。则一个染色方案经 g 不变，当且仅当它对应的置换把同环圈的底座元素都映射到同一个颜色。这样的染色方案，就是把同属一个环圈的元素“捆绑处理”，视为单个元素。因此，所有这样的染色方案个数就是 $|C|^{c(g)}$。于是得到结论：

定理 8.2 染色计数定理

用集合 C 中颜色给对称性由 G 描述的集合 X 中的元素染色，所有本质不同的染色方案的个数为：

$$|\mathcal{O}_G(C^X)| = \frac{\sum_{g\in G} |C|^{c(g)}}{|G|}.$$

其中 $C^X = \{f \mid f : X \to C\}$.

8.3 更进一步的计数

上一节中，我们给出了计算用多种颜色给对称集合染色方案数的方法和相关结论，其原理是计算群元素的环圈个数。我们知道了用三种颜色的 10 个珠子串成的项链有 3210 种。但有的人会接着问更进一步的问题：我的 10 个珠子并不会变。其中 5 个是红色，3 个是黄色，2 个是蓝色。那么，就用这些珠子串成的项链，有几种呢？

这个问题似乎更贴近现实，因为我们并不假设每种颜色的珠子数量可以随便变化。定性来说，这样 10 个珠子串成的不同项链方案，肯定少于 3210 种。我们还可以说，各种“配比”串出来的项链方案数加起来，就是 3210 种。

那么，具体有几种呢？

要知道这个问题的答案，需要把上一节中的细节继续拆解。具体来说，要把每个 $|C|^{c(g)}$ 继续拆开来清算。我们再次来说明 $|C|^{c(g)}$ 是什么意思：我们分析了 g（对应置换）的各个环圈，要让染色方案经 g 不变，方案中每个环圈里的元素必须同色。也就是说，如果一个环圈长度为 2，那么我们要么给这 2 个元素都染红色，要么都染别的颜色。

一个方案中染红色的元素个数，就是各个染红色的环圈元素之和。因此，我们的染色方案如果要满足恰好用 5 个红珠子，那么必然是有几个环圈的长度加起来等于 5，而我们把这几个环圈都染成了红色。

于是，问题化归为：若干个正整数和为 10，有多少种方法从中挑出一些整数，使得其和为 5?

一个很巧妙的方法是采用所谓的母函数方法。利用整式的性质，把这个问题再化归为整式展开和合并同类项的问题。通过巧妙地构造多项式，使得展开、合并同类项后，相应项的系数就是答案。

具体来说，设一共有 k 种颜色（这里 $k=3$），对任意正整数 n，我们考虑这样的基本多项式：$p_n = x_1^n + x_2^n + \cdots + x_k^n$。$p_n$ 就代表了长度为 n 的环圈。用它们为“积木”，对给定的群元素 g，我们从 1 开始搭建我们的多项式 P_g。

逐个考虑 g（对应置换）的环圈：第一个环圈长度为 n_1，就给 P_g 乘以 p_{n_1}；第二个环圈长度为 n_2，就给 P_g 乘以 p_{n_2}；第三个环圈长度为 n_3，就给 P_g 乘以 p_{n_3}；以此类推。这样，如果有 k 个长度为 n 的环圈，P_g 中就有 p_n^k。

在我们的例子里，p_n 可以记为 $p_n = a^n + b^n + c^n$。设 g 是对称轴是对角顶点的翻转变换，那么它有两个长度为 1 的环圈，4 个长度为 2 的环圈。于是我们搭建的 P_g 为：

$$P_g = (a+b+c)^2(a^2+b^2+c^2)^4.$$

我们计算 P_g 中 $a^5b^3c^2$ 的系数。如何计算这个系数呢？整式理论告诉我们：这个系数是“在各个相乘项中找一项，乘起来是 $a^5b^3c^2$ 的方法数”。而每一项中 a,b,c 的乘方指数，就是环圈的长度。所以，计算 P_g 中 $a^5b^3c^2$ 的系数，就是计算经 g 不变的染色方案里，恰用 5 红 3 黄 2 蓝珠子的方案数。而所有这样的方案数在 g 遍历 D_{10} 后加总，就得到我们要的答案。

因此，这个方法并没有直接告诉我们答案，而是把一个组合计数问题化归为有成熟算法的多项式展开和合并同类项问题。而展开多项式和合并同类项都是机械的运算，有确定的计算方法。因此，这个方法的价值在于通过化归，给出了计算方法，而不是直接

给出表达式。

在我们的例子里，展开 P_g 并合并同类项，得到 $a^5b^3c^2$ 的系数为 24。类似地，可以求出其他的 g 对应的 P_g，以及 $a^5b^3c^2$ 的系数。经分析可知，各种非平凡旋转和对称轴是对边中点连线的翻转变换，环圈长度都无法累加出 5 红 3 黄 2 蓝的结果，只有恒等变换 e 和 5 个对称轴是对角顶点的翻转变换对方案数有贡献。其中 $P_e = (a+b+c)^{10}$，其中 $a^5b^3c^2$ 的系数为 2520，因此加起来就得到恰用 5 红 3 黄 2 蓝珠子的总方案数：

$$N = \frac{1 \times 2520 + 5 \times 24}{20} = \frac{2640}{20} = 132.$$

即一共有 132 种恰用 5 红 3 黄 2 蓝珠子的染色方案。

随着自动化的进步，我们可以直接通过编程使用计算机程序计算整系数多项式的特定项系数，也可以使用相关的组合计数结论。读者可以自行查找相关资料，这些问题我们在此不再赘述。

例子 8.1

> 三硝基甲苯是一种常见的化工产品，由三个硝基和一个甲基替代苯环的氢而成。它有多个同分异构体（成分一样但化学结构不同的化合物，这里我们专指保持苯环结构的同分异构体）。计算三硝基甲苯的同分异构体个数。

解答：这里想要计算的是这样的数学问题：正六边形的顶点用三个颜色染色，三种颜色的顶点分别有 $1,2,3$ 个，有几个染色方案？为了方便，把三个颜色称作红、黄、蓝，分别对应甲基、氢和硝基，即要求 1 红 2 黄 3 蓝的染色方案数。

首先，使用上一节的结论可以计算三种颜色的全部染色方案数。这里涉及的群是 D_6。记其中逆时针旋转 60° 和沿水平对边中点连线翻转的变换分别为 r, s。按照同样的方法分析其中元素的环圈：

- $i = 1, 5$ 时，i 与 6 互素，r^i 的环圈只有一个。
- $i = 2, 4$ 时，i 与 6 的最大公约数为 2，对应的 r^i 的环圈有 2 个，每个长度为 3。
- $i = 3$ 时，i 与 6 的最大公约数为 3，对应的 r^i 的环圈有 3 个，每个长度为 2。

过对边中点连线的翻转可分解为三个对换，有 3 个环圈，每个长度为 2。过对角顶点的翻转有 2 个长度为 1 的环圈，和 2 个长度为 2 的环圈。共有 4 个环圈。因此，所有染

色方案数为：

$$\begin{aligned}\frac{1}{|\mathsf{D}_6|}\sum_{g\in\mathsf{D}_6}|X^g| &= \frac{1}{12}\sum_{g\in\mathsf{D}_6}3^{c(g)}\\ &= \frac{1}{12}\left(3^6+2\times3^1+2\times3^2+1\times3^3+3\times3^3+3\times3^4\right)\\ &= \frac{1}{12}\left(729+6+18+27+81+243\right)=\frac{1104}{12}\\ &= 92.\end{aligned}$$

继续精细计算每个 g 对应的 1 红 2 黄 3 蓝染色方案数。由上知对每个群元素 g 需要构建 P_g。要注意的是：要确保有单一一个元素被染红，必须要有长度为 1 的环道，于是非平凡旋转和过对边中点连线的翻转被排除。只需要考虑恒等变换 e 和过对角顶点的翻转 rs, r^3s, r^5s。其多项式分别是：

$$P_e=(a+b+c)^6,\quad P_{rs}=P_{r^3s}=P_{r^5s}=(a+b+c)^2(a^2+b^2+c^2)^2.$$

需要求 P_e、P_{rs}、P_{r^3s}、P_{r^5s} 中 ab^2c^3 的系数。

P_e 的相关项系数 k_e 可以直接代入公式：

$$k_e=\frac{6!}{1!2!3!}=\frac{720}{1\times2\times6}=60.$$

P_{rs} 的相关项系数则通过展开来分析。把 P_{rs} 写为两式乘积：

$$P_{rs}=(a^2+b^2+c^2+2ab+2ac+2bc)(a^4+b^4+c^4+2a^2b^2+2a^2c^2+2b^2c^2).$$

右式中各项 a 的次数都是偶数。要使得 a 的次数为 1，只能取左式中的 $2ab$、$2ac$。$2ac$ 乘以 $2b^2c^2$ 可得 $4ab^2c^3$。$2ab$ 和右式中任何项相乘不得 ab^2c^3。因此 P_{rs} 的相关项系数为 4。同理可算得 P_{r^3s}、P_{r^5s} 的相关项系数也是 4。于是总方案数为：

$$\frac{60+4+4+4}{12}=6.$$

一共有 6 种同分异构体。其中 $2-4-6$ 三硝基甲苯（即 3 个硝基间隔排布呈正三角形，甲基在两硝基之间）最稳定，应用最广泛。

本章小结

本章我们探讨了群论在组合计数中的强大应用，解决了对称性集合的染色计数问题。主要知识点包括：

- 当计数对象集合具有对称性时，许多看似不同的状态通过群变换可以互相重合，它们属于同一个轨迹。本质不同的方案数，就是集合对称性对应的群显于集合的轨迹数。
- **双重计数法**：通过构造群元素与状态配对的“$g(x) = x$ 事件”集合，从“先遍历状态”和“先遍历群元素”两个角度分别求和，建立等式。
- **定元分轨定理**：群分划的轨迹总数，等于群中各元素的定元数的平均值。这避免了逐个分析轨迹长度的困难。
- **染色计数定理**：把染色计数问题转化为群作用于底座集合的效果，再转化为群同构的置换群的环圈分析。若颜色集合大小为 $|C|$，则群元素 g 的定元数为 $|C|^{c(g)}$（$c(g)$ 为 g 对应的环圈数）。于是定元分轨定理转化为：染色方案数，等于所有 $|C|^{c(g)}$ 的平均数。
- 指定每种颜色的使用数量（固定配比）时，通过构造整式（母函数）并计算特定项的系数，可以求出满足特定颜色配比的染色方案数。

我们不仅用群揭示了事物内在的对称结构，还构建了一套系统、严密的计数方法，将复杂的枚举问题转化为对群元素性质的代数计算。

8.4 习题

1. **正方体面染色问题**。给定一个正方体，其 6 个面可以用红、蓝两种颜色染色。

(1) 如果不考虑任何对称性（即对称群只包含恒等变换 e），有多少种染色方法?

(2) 如果只允许绕某一条特定的顶心对角线（例如连接左下前和右上后顶点的轴）进行旋转，有多少种本质不同的染色方法?

(3) 如果允许保持某一对特定对面（例如顶面和底面）作为集合不变的所有旋转（即绕垂直轴旋转，以及绕水平轴和对角轴翻转 180°），有多少种本质不同的染色方法?

(4) 如果允许正方体的所有旋转（即完整的旋转群 T_6），有多少种本质不同的染色方法?

(5) 如果允许用红、蓝、绿三种颜色给正方体的面染色，以上各个情形的染色方法会变成多少种?

(6) 对比以上五问的答案，随着允许的对称操作增多，本质不同的染色方案数如何变化？随着颜色种类增多，本质不同的染色方案数如何变化？尝试从“对称轴的数量”和“群势”的角度给出直观解释。

2. **正五边形染色问题**。给定正五边形：所有边长相等，所有内角都是 108°。

(1) 不考虑对称性，用红、蓝两种颜色给正五边形的顶点染色，有几种染色方法?

(2) 如果允许旋转和翻转，用红、蓝两种颜色给正五边形的顶点染色，有几种染色方法?

(3) 如果允许旋转和翻转，用红、蓝、绿三种颜色给正五边形的顶点染色，有几种染色方法?

(4) 如果只允许旋转，用红、蓝两种颜色给正五边形的顶点染色，有几种染色方法?

(5) 如果只允许旋转，用红、蓝、绿三种颜色给正五边形的顶点染色，有几种染色方法?

(6) 对比以上四问的答案，解释在允许与不允许翻转的情形下，用两种颜色染色和用

三种颜色染色的答案有何差异？理由是什么？

以下是可以用作正式测验的成套试题。每套试题都有一个主要问题。通过不断解答各个小问，可以逐步得到主要问题的答案。这些试题有两种使用方法。

- 如果你希望检验自己通过本书掌握了多少知识和方法，可以严格地使用这些试题进行测试。第一套试题大约需要 2 ~ 3 个小时来解答。第二套试题大约需要 3 ~ 4 个小时来解答。你不必答完一道题才开始答下一题，承认之前问题的结论并用来解决后面的问题是允许的。
- 如果你只是希望借着做题来了解更多的知识，那么可以像之前的习题一样，在每小问上思考数分钟，如果仍然没有思路就查看参考解答。这些问题之间的联系和系统性更高，可以多体会问题之间的联系，思考其整体思路。

六氟化硫的立体异构体

六氟化硫（SF_6）是一种气体分子。它的空间结构是正八面体：硫原子位于中心，六个氟原子分别位于正八面体的六个顶点，这六个位置的地位完全相同。现在设想把其中若干个氟原子换成氯原子，得到 $SF_{6-k}Cl_k$ 这样的化合物。理论上，这样的替换一共能产生多少种不同的空间结构[①]？

在三维空间中，分子可以自由转动。如果两种原子排布能够通过转动完全重合，化学上就把它们看作同一种分子；如果无论怎样转动都不能重合，它们就是不同的分子，称为**立体异构体**。例如，当只有两个氯原子时，若这两个氯原子位于正八面体相对的两个顶点，化学上称为**反式**结构；若位于相邻的两个顶点，则称为**顺式**结构。

下面分四部分，把这个化学问题逐步改写成本章能够处理的计数问题，并完成计算。各小问都可以直接使用前面小问的结论。

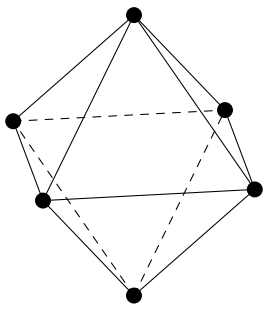


图 8.8: 正八面体

第一部分　化归数学问题

1. 本题中，本章所说的底座集合 X 与颜色集合 C 分别是什么？说明为什么“一种原子排布”就是 X 到 C 的一个映射，并求出不考虑转动时的排布总数 $|S|$，其中 $S = C^X$ 定义为所有 X 到 C 映射的集合。

2. “两种排布能通过转动重合就是同一种分子”，用第七章的语言应当怎样表述？据此说明：本题要求的答案等于什么？

3. 本章处理苯环时用的是映轮群 D_6，其中包含翻转；本题却只允许旋转。说明这两种

[①]其中哪些分子能实际制得，属于化学实验的问题，不在本题讨论范围内。

做法并不矛盾。（提示：苯环的六个取代位置在同一平面内，正八面体的六个顶点不在同一平面内。想一想，把一个平面分子在空间中翻个面，究竟是不是旋转。）

第二部分　数清对称群

4. 正八面体任一顶点可以被转到六个顶点位置中的哪一个？确定之后，正八面体还能怎样转动而不改变这个顶点的位置？由此说明正八面体的旋转共有多少个。把这个群记为 G。

5. 正八面体有 6 个顶点、8 个面、12 条棱。把过中心并连接一对相对顶点、一对相对面中心、一对相对棱中点的直线，分别称为顶点轴、面心轴、棱中轴。

(1) 三类轴各有几条？

(2) 绕每类轴转动多少度能让正八面体回到原位？每条轴上除恒等变换外有几个旋转？

(3) 把三类旋转与恒等变换加起来，核对是否等于第 4 问的结果。

6. 把六个顶点按空间方位命名为上、下、左、右、前、后，其中上与下相对，左与右相对，前与后相对。于是“上—下”是一条顶点轴，左、右、前、后四个顶点围成赤道上的正方形。作为示范，写出绕上下轴（从上往下看逆时针）转 90° 时六个顶点各自的变化，把它写成环圈分解，并给出环圈数 $c(g)$。

第三部分　从旋转到环圈，再到计数

7. 旋转 g 把一种排布 f 变成另一种排布。按本章的约定，这句话说的是：原来在位置 a 上的原子，被搬到了位置 $g(a)$ 上。

(1) “g 定住 f”（即 $f \in S^g$）等价于对每个位置 a 有什么要求？

(2) 由此说明：同一个环圈里的位置必须放同一种原子，不同环圈之间互不影响。

(3) 用环圈数 $c(g)$ 写出 $|S^g|$。

8. 绕上下轴转 180°：写出环圈分解与 $c(g)$。

9. 取上、右、前三个顶点围成的面，它的对面由下、左、后三个顶点围成。绕这条面心轴转 120° 与 240°：写出环圈分解与 $c(g)$。

10. 取连接上与前的棱，它的相对棱连接下与后。绕这条棱中轴转 180°：写出环圈分解与 $c(g)$。

11. 把第 6、8、9、10 问的结果整理成一张表，列出每类旋转的个数、环圈形态、$c(g)$ 与 $2^{c(g)}$，并核对个数之和。

12. 用染色计数定理求出本质不同的排布总数，也就是立体异构体的总数。

第四部分　回到化学

13. 现在固定氯原子恰好两个，即 SF_4Cl_2。

(1) 不考虑转动，从六个位置中选两个放氯原子，有多少种选法?

(2) 按两个氯原子“相对”还是“相邻”分类，各有多少种？说明每一类中的选法都能通过旋转互相得到。

(3) 由此说明 SF_4Cl_2 恰有两种立体异构体，并指出哪一种是顺式、哪一种是反式。

14. 用轨定定理核对上一问：两种异构体各自的轨迹有多长？定子群各有几个元素？试着把反式构型的定子群中的旋转找出来。

15. 再看氯原子恰好三个的情形。按“三个氯原子两两相邻”与“三个氯原子中有一对相对”分类，各有多少种选法？核对总数，并说明 SF_3Cl_3 也恰有两种立体异构体。

16. 逐个列出 $k = 0, 1, \cdots, 6$ 时 $SF_{6-k}Cl_k$ 的异构体数目，核对它们的和是否等于第 12 问的结果。特别说明 $k = 0, 1, 5, 6$ 时为什么都只有一种，以及 $k = 2$ 与 $k = 4$ 的结果为什么相同。

17. 用本章介绍的方法重新计算“恰好两个氯原子”的情形：对每类旋转写出对应的整式 P_g，求其中 a^2b^4 的系数（a 记氯，b 记氟），再求和取平均，核对是否仍得 2。

★ ★ ★ ★ ★

同构的简单无向图

图论是数学中讨论多个事物之间关联的理论。把实际问题中“某某与某某有关”、“某某与某某无关”这样的信息抽离出来，就是图论讨论的内容。一个**图**由顶点和边构成。顶点表示我们关心的对象，而边则用来描述对象之间的关系。在图论里，我们不关注顶点和边的具体位置，只关注顶点之间是否有边相连。顶点与边共同形成的结构，本身有丰富的性质，能帮助我们了解复杂现象背后的规律。

一个图里，两个顶点之间可能没有边相连，也可能有好几条边相连。如果规定两点之间至多有一条边相连，就说它是**简单图**。有些图的边标明了方向，从一个顶点指向另一个顶点，这样的图叫做**有向图**。规定边没有方向的图叫做**无向图**。n 元简单无向图就是 n 个顶点构成的简单且无向的图。



图 8.9: 有向图与无向图

下面分四部分，使用本章介绍的计数定理研究图论中的一个问题。各小问都可以直接使用前面小问的结论。

第一部分　基本定义和性质

1. 考虑 3 元简单无向图。它最多有几条边？最少有几条边？4 元、5 元简单无向图呢？

2. 简单无向图 Ω 是顶点和边的集合。其中顶点记为 $V = \{v_1, v_2, \cdots, v_n\}$，边记为 $B = \{\{v_1, v_2\}, \{v_2, v_3\}, \cdots\}$，即边为其两端顶点的二元集。$n$ 个顶点构成的简单无向图，最多可以有几条边？我们把所有可能的边的集合记为 E（B 是 E 的子集）。

3. 定义：两个简单无向图 $\Omega = (V, B), \Omega' = (V', B')$ **同构**，就是说有从 V 到 V' 的双射 f，使得 $\forall \{v_i, v_j\} \in B$，都有 $\{f(v_i), f(v_j)\} \in B'$，反之亦然。说明：$V = V'$ 时，用以上定义的 f 可以构造出 E 上的唯一一个置换（以下称为 p_f）。

4. 给定 $\sigma \in \mathsf{S}_n$，证明它对应 n 元简单无向图到自身的一个同构，并说明它如何改变图的边。

5. 以下的图，左图和右图同构吗？如果同构，给出同构的 f，说明它对应怎样的置换（顶点数字 i 表示 v_i）。

〔1〕



〔2〕



〔3〕



6. 如果 n 元简单无向图每两个顶点都有边相连，就称为 n 元**完全图**，记为 K_n。完全图有几条边？有多少个到自身的同构 f？

第二部分　从同构到染色

7. 用红蓝两种颜色给 3 个顶点的完全图的所有边染色。假设顶点之间没有区别，有多少种不同的染色方法？假设顶点标号 $1, 2, 3$，有多少种不同的方法？枚举所有可能。

8. 给定顶点集 $V = \{v_1, \cdots, v_n\}$，E 是所有可能边的集合。证明：以下映射可以观 S_n 于 E：

$$\begin{aligned} \gamma :\ \mathsf{S}_n \times E \quad &\longrightarrow\ E \\ (\sigma,\ \{v_i, v_j\}) &\longmapsto \{\sigma(v_i), \sigma(v_j)\} \end{aligned}$$

并说明 $\sigma \mapsto \gamma_\sigma$ 是群同态。γ 是否令 S_n 显通相？

9. 记 $S = 2^E$ 为 E 的幂集，即所有边子集的集合。证明：以下映射可以观 S_n 于 S：

$$\begin{aligned} \gamma' : \mathsf{S}_n \times S &\longrightarrow S \\ (\sigma, B) &\longmapsto p_\sigma(B) \end{aligned}$$

说明 $p_\sigma(B)$ 的含义。γ' 是否令 S_n 显通相？说明 γ 和 γ' 之间的关系。

10. 用两种颜色给 n 元完全图的边染色。证明：两种染色方案本质相同，等价于观 S_n 于 S 时两个边集属于同一条轨迹。

11. 我们想知道，给定顶点数 n，在假设顶点之间没有区别的情况下，本质不同的简单无向图有多少种。说明：这个问题可以转化为给 n 元完全图的边染色的问题。给出转化后的染色问题的具体叙述，并说明它为何与简单无向图种类问题等价。以 $n = 4$ 的情况为例，列出本章正文中提到的各个对象在这个染色问题里分别是什么：底座集合 X、颜色集合 C、染色方案集合 C^X、群 G。4 元简单无向图的同构类个数等于什么？

第三部分　染色计数

12. S_4 中的置换按环圈个数和长度可分为几类？列出各类置换，每类有多少个？对每类，选取一个代表元 σ，写出 σ 在 E 上划分的轨迹，并计算轨迹个数（为了表示方便，约定 E 中顶点为 i, j 的边简写为 $\overline{ij}$。即 $E = \{\overline{12}, \overline{13}, \overline{14}, \overline{23}, \overline{24}, \overline{34}\}$）。

13. 对每个 $\sigma \in \mathsf{S}_4$，γ_σ 对应几元置换？写出上题中每个代表元 σ 对应的 γ_σ 的环圈结构。

14. 对上面提到的代表元 σ，计算 σ 在染色方案集合 $S = C^X$ 上的定元个数 S^σ。

15. 应用定元分轨定理，计算 4 元简单无向图的同构类个数。

16. 按边数 $k = 0, 1, 2, 3, 4, 5, 6$ 分类，枚举所有 4 元简单无向图（画出每个图的示意图或用边集描述），验证总数与之前得到的结果一致。（提示：k 条边的图与 $6 - k$ 条边的图有什么关系？）

第四部分　更进一步

17. 我们想进一步知道：恰有 k 条边的 4 元简单无向图有几种？设颜色集合 $C = \{0, 1\}$，用 a 标记颜色 0（无边），b 标记颜色 1（有边）。写出基本多项式 p_n，说明它代表什么。对 S_4 的各类置换 σ，逐类根据其环圈结构，搭建多项式 P_σ。

18. 计算

$$P \;=\; \frac{1}{|\mathsf{S}_4|} \sum_{\sigma \in \mathsf{S}_4} P_\sigma$$

展开 P 并合并同类项。说明：P 中 $a^{6-k}b^k$ 的系数，就是恰有 k 条边的 4 元简单无向图的同构类个数。验证各系数与之前枚举的结果一致。

★ ★ ★ ★ ★

附录

附录一　练习题参考解答

1.1　第一章参考解答

什么是群

1. 要注意的是我们默认“什么都不做”必然在集合里，因此变换的集合构成群。逐条检查四条规则：首先，变换的集合 S 是固定的；其次，变换的效果是确定的；第三，互换钱币的效果是可逆的：再次互换即可；最后，互换两次就等于什么都不做，因此“互换”和“什么都不做”不论怎样组合，效果也是“互换”和“什么都不做”之一。于是满足所有规则，构成群。

2. 旁边再放一个金币，但仍然局限于交换前两枚钱币。那么旁边的金币不参与任何变换，任何变换也不会涉及它。这表明变换的集合完全不变，所以还是群。这里要区别钱币的集合与变换的集合。

3. 显然，由于裤袋里一开始只有 5 个弹珠，你无法把“从左裤袋里拿一个弹珠放到右边裤袋里”这件事重复 6 次。不满足规则 4，所以不构成群。

4. (1) 一共有 6 种挂画方法。

(2) 能实现所有挂画方法。记原本墙上的三幅画从左至右分别是 A, B, C。“交换左墙和中间墙上的画”能获得 B, A, C，“交换左墙和右墙上的画”能获得 C, B, A。对 B, A, C 做“交换左墙和右墙上的画”能获得 C, A, B；对 C, B, A 做“交换左墙和中间墙上的画”能获得 B, C, A。对 B, C, A 再做“交换左墙和右墙上的画”能获得 A, C, B。于是得到所有 6 中挂法。

(3) 如果把“只允许这两种重排方法”理解为只由它俩构成的集合，那么不是群。因为显然重复做会得到别的效果。如果把它理解为“只允许这两种重排方法以任意方式组合”，那么构成群，因为上一问中我们已经通过组合实现了所有的挂法。这说明任意两种挂法之间都可以通过两者组合互通，于是任何效果可逆。而不论怎么组合也不会得到新的挂法了。于是满足所有规则，构成群。

(4) 如果靠出口大门的墙也能挂画，则多出一个新选择：空墙。每面墙都可以选为空墙，因此一共有 $4 \times 6 = 24$ 种挂法。只靠“交换左墙和中间墙上的画”和“交换左墙和右墙上的画”，不能实现所有挂法，因为如果靠出口大门的墙挂了画，这两个操作无法移动它。若要实现全部 24 种挂法，需要增加涉及靠出口大门的墙的操作。此外，现在可能有左中右的某墙上不挂画的情况，这时无法“交换”了。因此两操作未必能实现，不构成群。

谈谈规则

1. 群的变换不一定有限的，也不一定能列举出来，比如考虑一个圆，所有保持它形状位置不变的对称变换包括任意绕圆心的旋转，因此有无限个，也无法一一列举。

2. 如果分析对象的对称性时，发现只有“什么都不做”这个变换满足条件，就说明对象没有任何对称性。

3. (1) 变换组合的顺序会影响最终的效果：考虑正方体的旋转群，先朝前转动 90° 再往左转动 90°，和先往左转动 90° 再朝前转动 90°，效果是不一样的。

(2) 变换组合的顺序不影响最终的效果：前面提到的两个钱币的互换群，或者单个硬币的翻转群。

(3) 恰好包含两个变换：前面提到的两个钱币的互换群，或者单个硬币的翻转群。

(4) 恰好包含三个变换：保持正三角形形状位置不变的所有旋转变换。

(5) 恰好包含四个变换：军训时“立正”、“向左转”、“向右转”、“向后转”构成的群。

4. 例子一：模 n 的同余类里“加几”构成的群，“加几”的“几”可以是 $0, 1, \cdots, n$，一共 n 个变换。例子二：正 n 边形的旋转对称群，它包含所有形如 $\frac{k \cdot 360^\circ}{n}$ $(k = 0, 1, \cdots, n-1)$ 的旋转变换，一共 n 个。

“变换组合的顺序影响最终效果”的情况有时可以，有时不可以。比如 $n = 24$ 时，考虑正方体的旋转群（24 个元素），就可以让变换组合的顺序影响最终效果。但比如 $n = 2$ 时，只有“什么都不做”和另一个变换 X。这时，X 重复两次要么得到自己，要么得到“什么都不做”。两种情况下，变换组合的顺序都不影响最终效果。

打破规则

1. 仅仅不满足第三条规则的例子：固定一个圆规的一脚，让另一脚画圆弧，操作是：“沿顺时针画 n 度的圆弧”（n 为正整数）。操作集合固定；效果确定；任意重复组合的效果仍然是沿顺时针画正整数度圆弧。但任何操作不可逆，所以仅仅不满足规则 3。

2. 仅仅不满足第四条规则的例子：考虑军训时“向左转”、“向右转”两个口令。操作集合固定；效果确定；操作是可逆的。但连续两次“向左转”的效果不在集合里。所以仅仅不满足规则 4。

数与群

1. 限定为偶数仍构成群。逐条检查四条规则：首先，变换的集合 S 是固定的：

$$S = \{\text{“加}2k\text{”} \mid k \in \mathbb{Z}\}.$$

S 中变换效果是确定的，也可逆。变换的组合就是加多个偶数。由于多个偶数的和还是偶数，所以仍然在集合里。于是满足所有规则，构成群。

2. 限定为奇数则不构成群。因为两个奇数的和是偶数，不是奇数。因此两个加奇数变换组合后不在集合里，不满足规则 4。

3. 同理，由于 3 的倍数相加还是 3 的倍数，所以满足规则，相关变换构成群。而两个模 3 余 1 的数相加就不再模 3 余 1，所以不满足规则 4，相关变换不构成群。

4. 如果把加法改为乘法，那么 0 作为整数，“乘 0”的效果是得到 0，但这个变换不可逆：你无法从 0 出发再通过乘以某个数得到乘 0 之前的数。因此不满足规则 3，相关变换不构成群。

5. 去掉“乘 0”，考虑“乘 2”，仍然无法复原。比如 1 乘 2 得到 2，但 2 无论乘以哪个整数都无法得到 1。因此不满足规则 3，相关变换不构成群。

6. 如果把数集改为非零有理数集 $\mathbb{Q}^*$，那么不再有乘 0 的问题。此外，对于非零的有理数 r，“乘 r”之后可以通过“乘 r 的倒数”来逆转效果复原（r 的倒数也是非零有理数）。所以满足所有规则，构成群。

7. 同余类的乘法定义为：$\overline{i} \times \overline{j} = \overline{i \times j}$。如果 $i \times j$ 不小于 n，就改为它模 n 的余数。对于所有同余类的集合，同样有“乘 0”的问题，因此不满足规则 3，相关变换不构成群。

如果只考虑非零同余类，就要考虑是否会有乘以某个类得到 $\overline{0}$ 的问题。如果 $\overline{i \times j} = \overline{0}$，那么就超出集合范围了。因此，必须保证任何小于 n 的整数相乘不是 n 的倍数，换句话说，比 n 小的正整数里，除了 1 以外，不能有 n 的因数。这要求 n 是素数。

反之，如果 n 是素数，那么小于 n 的正整数无论怎么乘都不是 n 的倍数，因此总在集合里。

另外，考虑“乘 $\overline{i}$”的效果。如果两个小于 n 的正整数乘 $\overline{i}$ 结果相同，说明两者的差乘 $\overline{i}$ 是 n 的倍数，矛盾！所以 $\overline{1}, \cdots, \overline{n-1}$ 乘 $\overline{i}$ 的结果必然两两不同。而这些结果又必然都在 $\overline{1}, \cdots, \overline{n-1}$ 中，所以实际上是 $\overline{1}, \cdots, \overline{n-1}$ 的重新排列。这说明“乘 $\overline{i}$”是一个一一对应的重排操作，因此总是可逆的。于是满足所有规则，构成群。

8. 首先，如果 $a = 1$，那么如何乘也只能得到自身，不可能得到所有同余类，所以排除 $a = 1$。接下来对 $p = 3, 5, 7, 11$ 逐个检查。

$p = 3$ 时，只有 $a = 2$ 的情况。$\overline{2} \times \overline{2} = \overline{1}$，所以得到了所有非零同余类。$a = 2$ 是原根。

$p = 5$ 时，需要检查 $a = 2, 3, 4$ 的情况。

$$\overline{2} \times \overline{2} = \overline{4}, \qquad \overline{3} \times \overline{2} = \overline{1},$$
$$\overline{4} \times \overline{2} = \overline{3}, \qquad \overline{1} \times \overline{2} = \overline{2}.$$

于是 2 是模 5 原根。

$$\overline{3} \times \overline{3} = \overline{4}, \qquad \overline{2} \times \overline{3} = \overline{1},$$
$$\overline{4} \times \overline{3} = \overline{2}, \qquad \overline{1} \times \overline{3} = \overline{3}.$$

于是 3 是模 5 原根。

$$\overline{4} \times \overline{4} = \overline{1},$$
$$\overline{1} \times \overline{4} = \overline{4}.$$

构成循环，于是永远无法得到 $\overline{2}$ 和 $\overline{3}$，因此 4 不是模 5 原根。实际上，对于更大的素数 p，$(p-1) \times (p-1) = p^2 - 2p + 1$ 模 p 余 1，因此自乘 $p-1$ 必然无法得到其它的类，不是原根。于是模 5 的原根是：$2, 3$。
$p = 7$ 时，需要检查 $a = 2, 3, 4, 5$ 的情况。

$$\overline{2} \times \overline{2} = \overline{4},$$
$$\overline{4} \times \overline{2} = \overline{1},$$
$$\overline{1} \times \overline{2} = \overline{2}.$$

构成循环，于是永远无法得到 $\overline{3}$，因此 2 不是模 7 原根。

$$\overline{3} \times \overline{3} = \overline{2}, \qquad \overline{4} \times \overline{3} = \overline{5},$$
$$\overline{2} \times \overline{3} = \overline{6}, \qquad \overline{5} \times \overline{3} = \overline{1},$$
$$\overline{6} \times \overline{3} = \overline{4}, \qquad \overline{1} \times \overline{3} = \overline{3}.$$

于是 3 是模 7 原根。

$$\overline{4} \times \overline{4} = \overline{2},$$
$$\overline{2} \times \overline{4} = \overline{1},$$
$$\overline{1} \times \overline{4} = \overline{4}.$$

构成循环，于是永远无法得到 $\overline{3}$，因此 4 不是模 7 原根。
实际上我们能预见这一点。$\overline{4}$ 是 $\overline{2}$ 自乘“路上”的一环，所以它自乘就是 $\overline{2}$ 自乘再自乘，于是必然无法得到所有非零同余类。换句话说，只要某个 a 不是原根，那么它自乘“路上”出现过的数也不会是原根。

$$\overline{5} \times \overline{5} = \overline{4}, \qquad \overline{2} \times \overline{5} = \overline{3},$$
$$\overline{4} \times \overline{5} = \overline{6}, \qquad \overline{3} \times \overline{5} = \overline{1},$$
$$\overline{6} \times \overline{5} = \overline{2}, \qquad \overline{1} \times \overline{5} = \overline{5}.$$

于是 5 是模 7 原根。于是模 7 的原根是：$3, 5$。

$p = 11$ 时，需要检查 $a = 2, 3, 4, 5, 6, 7, 8, 9$ 的情况。

$$\begin{aligned} \overline{2} \times \overline{2} &= \overline{4}, & \overline{4} \times \overline{2} &= \overline{8}, \\ \overline{8} \times \overline{2} &= \overline{5}, & \overline{5} \times \overline{2} &= \overline{10}, \\ \overline{10} \times \overline{2} &= \overline{9}, & \overline{9} \times \overline{2} &= \overline{7}, \\ \overline{7} \times \overline{2} &= \overline{3}, & \overline{3} \times \overline{2} &= \overline{6}, \\ \overline{6} \times \overline{2} &= \overline{1}, & \overline{1} \times \overline{2} &= \overline{2}. \end{aligned}$$

于是 2 是模 11 原根。

$$\begin{aligned} \overline{3} \times \overline{3} &= \overline{9}, \\ \overline{9} \times \overline{3} &= \overline{5}, \\ \overline{5} \times \overline{3} &= \overline{4}, \\ \overline{4} \times \overline{3} &= \overline{1}, \\ \overline{1} \times \overline{3} &= \overline{3}. \end{aligned}$$

构成循环，于是永远无法得到 $\overline{2}$，因此 3 不是模 11 原根。此外，在它自乘“路上”的 $9, 5, 4$ 都不是模 11 原根。

$$\begin{aligned} \overline{6} \times \overline{6} &= \overline{3}, & \overline{3} \times \overline{6} &= \overline{7}, \\ \overline{7} \times \overline{6} &= \overline{9}, & \overline{9} \times \overline{6} &= \overline{10}, \\ \overline{10} \times \overline{6} &= \overline{5}, & \overline{5} \times \overline{6} &= \overline{8}, \\ \overline{8} \times \overline{6} &= \overline{4}, & \overline{4} \times \overline{6} &= \overline{2}, \\ \overline{2} \times \overline{6} &= \overline{1}, & \overline{1} \times \overline{6} &= \overline{6}. \end{aligned}$$

于是 6 是模 11 原根。同理可验证 $7, 8$ 是模 11 原根。于是模 11 的原根是：$2, 6, 7, 8$。

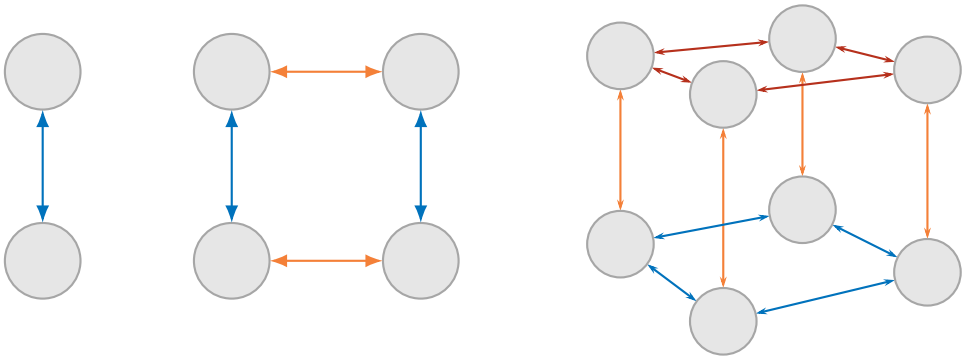
1.2 第二章参考解答

1. (1) **解答**：状态有 2 个：正面朝上、反面朝上。生成这些状态的方法是：进行一次“翻转”操作。

(2) **解答**：每个硬币都有正、反 2 种状态，因此总共有 2^k 个状态。生成这些状态的方法是：分别进行“翻转第 1 枚硬币”、“翻转第 2 枚硬币”……“翻转第 k 枚硬币”这 k 种基本操作。

(3) **解答**：状态有无限多个，对应数轴上所有的整数（整点）。生成这些状态的方法是：进行“加 1”（向右移动一格）或“减 1”（向左移动一格）操作。

2. **解答**：



(1) **单硬币群**：画 2 个节点，用一条双向箭头（或两条方向相反、标记为“翻转”的箭头）连接它们。

(2) **k 个硬币群**：理论上我们可以画 2^k 个节点。每个节点都有 k 条不同颜色（或不同标记）的箭头连出，分别代表翻转第 $1, 2, \ldots, k$ 枚硬币。实际上，这是一个 k 维超立方体的骨架图，想要在平面上画出来，只在 $k = 1, 2$ 时可行。$k = 3$ 时，我们可以画出立体空间中的正方体，每个顶点代表一个节点。$k > 3$ 时，想通过简单直观的方法来表示 k 个硬币的群就比较困难了。这也提醒我们：理解抽象对象时，不能总依赖于直观的图像。抽象对象的本质需要通过代数关系来理解，直观图景能辅助理解、思考，但代数关系才能精确展现抽象对象的实质。

(3) **整数加法群**：画一条向左右两端无限延伸的直线。在直线上标出等距的节点代表整数。向右的箭头标记为“加 1”。当然，这条“无限延伸的直线”实际上也只能画出有限长度。这也提醒我们：理解与无穷有关的抽象对象时，直观图景只能帮

助我们理解其有限的一部分。抽象对象的本质仍然需要通过代数关系来理解。

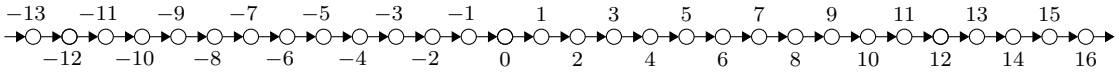
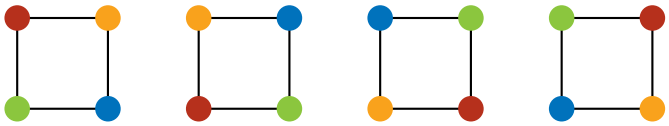


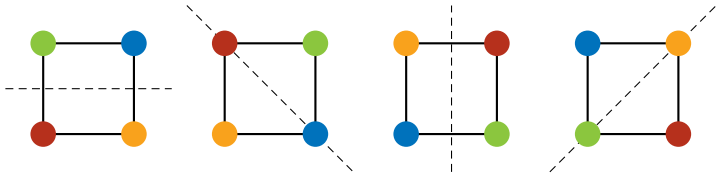
图 一.1: 整数加法群的生成路径图。

3. (1) **解答**：假设四种颜色为红、黄、蓝、绿。将 4 种不同颜色分配给 4 个不同的顶点，共有 $4! = 4 \times 3 \times 2 \times 1 = 24$ 种颜色组合（排列）。

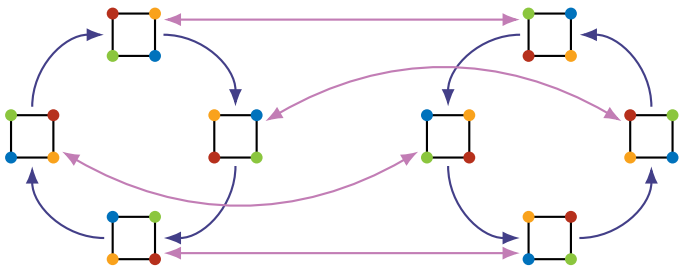
(2) **解答**：保持位置形状不变的旋转变换有 4 种：（逆时针）旋转 0°（什么都不做）、90°、180°、270°。



(3) **解答**：过中心的轴线有 4 条（2 条对角线，2 条对边中点连线），因此有 4 种翻转方法。



(4) **解答**：共有 8 个状态节点。可以用一个旋转变换（如逆时针 90° 旋转）将 4 个旋转状态连成一个环；再用一个翻转变换（如沿水平中线翻转）将这 4 个状态与另外 4 个翻转状态一一对应连接起来。



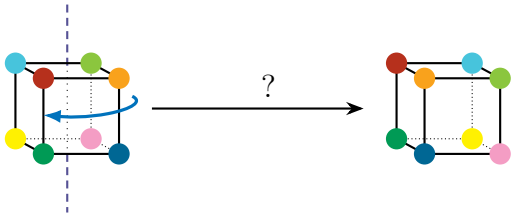
(5) **解答**：24 种组合中，有 16 种无法形成。

解释：旋转和翻转虽然改变了颜色的位置，但无法改变相邻关系。原本不相邻的顶点（对角顶点）不可能经过旋转和翻转变成相邻顶点，反之亦然。三角形的顶点则没有这种区分。因此正方形的旋转和翻转无法得到所有组合，而正三角形可

以。

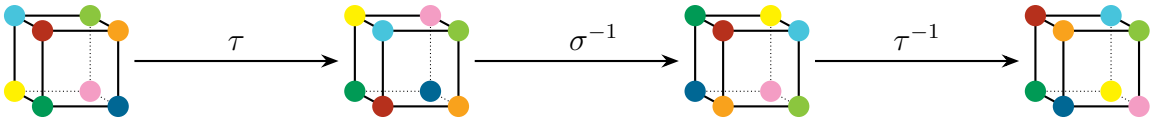
4. (1) **解答**：能。“往右转动 90°”实际上是“往左转动 90°”（即 σ）的逆操作 σ^{-1}。经观察可发现，连续做 4 次 σ 就回到初始状态。因此，做 3 次 σ 等于做 1 次它的逆操作。因此，连续进行三次 σ 变换（即 $\sigma \to \sigma \to \sigma$，或记为 σ^3）即可做到。

(2) **解答**：这个变换的旋转轴既不是 σ 的旋转轴，也不是 τ 的旋转轴。首先要理解这个旋转变换的效果，如何变换顶点（见图）。



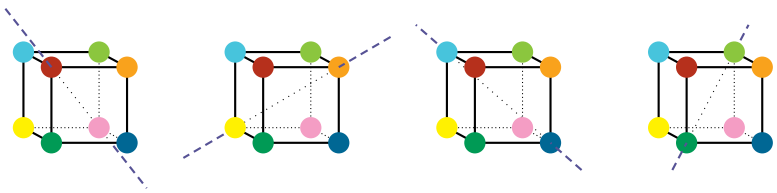
经尝试发现，它可以通过：先做 τ 操作，再做 σ^{-1}，最后做 τ 操作的逆操作 (τ^{-1})，即可得到这个结果。我们将“往左转动 90°，上下面不变”的变换记为 ρ，则

$$\rho = \tau \to \sigma^{-1} \to \tau^{-1}.$$



注：聪明的你可能会记得，我们在第一章开头提过这件事。

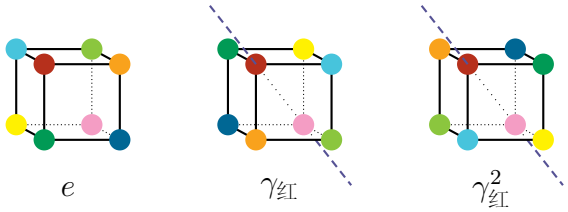
(3) **解答**：正方体有 8 个顶点，每两个相对的顶点连成一条顶心对角线，因此共有 $8 \div 2 = 4$ 条顶心对角线。我们用深浅色来标记对角顶点，因此我们可以把 4 条顶心对角线称为红顶心线、黄顶心线、蓝顶心线和绿顶心线。



(4) **解答**：以左前顶心线（红顶心线）为轴旋转时，左前顶点和右后顶点保持不动，而周围的 6 个顶点在空间中轮换位置。经尝试可发现，绕此轴旋转 120° 和 240° 后，正方体的整体轮廓和占据的空间与原来完全重合。这样的非平凡旋转变换有 2 个（旋转 120° 和 240°）。注意：后者是前者重复两次的结果，也是其逆变换。

而重复三次则恢复原状。这和正三角形的旋转性质一样（想想为什么?）。

(5) **解答**：能。首先我们会发现：不同的顶心线之间，可以通过 τ, σ, ρ 互相转换。把正方体分别按 τ, σ, ρ 旋转，就能把一条顶心线转到另一条顶心线的位置。因此，我们只需要讨论其中一条即可，比如绕红顶心线的旋转 $\gamma_{红}$：



e $\gamma_{红}$ $\gamma_{红}^2$

不难发现，$\gamma_{红}$ 的效果就是上一问中的中间状态，因此我们知道：

$$\gamma_{红} = \tau \to \sigma^{-1}.$$

而另一个旋转是 $\gamma_{红}$ 重复两次（也是它的逆操作!），因此同样可以通过 τ 和 σ 得到。而其他顶心对角线又可以从 $\gamma_{红}, \gamma_{红}^2$ 按 τ, σ, ρ 旋转得到。因此，绕其他顶心线的旋转，可以先绕红顶心线进行对应角度的旋转，然后按 τ, σ, ρ 把结果旋转到相应的顶心线上。

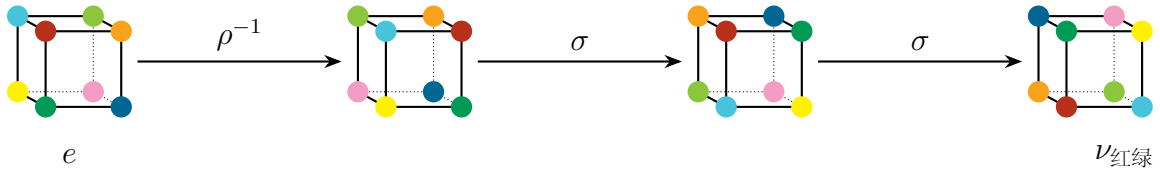
(6) **解答**：正方体有 12 条棱，每两条相对的棱连成一条对棱中线，因此共有 $12 \div 2 = 6$ 条对棱中线。按我们染色的方法，每条对棱中线对应的两条对棱分别是两对深浅色，因此可以命名为红绿中线、红黄中线、红蓝中线、绿黄中线、绿蓝中线和黄蓝中线。

(7) **解答**：以左对棱线（红绿中线，或类似位置）为轴旋转 180°，可以使正方体的上下、前后等面发生对称交换，整体形状和位置保持不变。这样的非平凡旋转变换只有 1 个（即旋转 180°）。



e $\nu_{红绿}$

(8) **解答**：能。首先我们会发现：不同的对棱中线之间，可以通过 τ, σ, ρ 互相转换。把正方体分别按 τ, σ, ρ 不断旋转，就能把一条对棱中线转到另一条对棱中线的位置。因此，我们只需要讨论其中一条即可。比如经尝试发现，可以用以下的方法达到绕红绿中线的旋转效果：



即首先往右转动 90°，上下面不变（这是 ρ 的逆操作），然后连续做两次 σ 操作。如何用 σ 和 τ 实现 ρ 的逆操作呢？就是把每一步都逆转，总体顺序也要逆转，这样就能把 ρ 的效果完全逆转。我们知道

$$\rho = \tau \to \sigma^{-1} \to \tau^{-1}.$$

于是，要逆转 ρ 的效果，需要首先做一次 τ 操作，逆转最右边（最后）的操作 τ^{-1} 的效果；然后做一次 σ 操作，逆转中间 σ^{-1} 的效果，最后做一次 τ^{-1} 的，逆转最左边（最初）的 τ 操作的效果。最终得到：

$$\rho^{-1} = \tau \to \sigma \to \tau^{-1}.$$

这就是用 σ 和 τ 实现 ρ 的逆操作的方法。当然，我们也可以通过观察得知 $\rho^4 = e$，得到 $\rho^{-1} = \rho^3$，从而说明它可以通过 σ 和 τ 生成。

注：至此，σ 和 τ 能生成的旋转变换如下：

1. 不断重复 σ 得到的 3 个旋转：σ, σ^2, σ^3（$\sigma^4 = e$）。
2. 不断重复 τ 得到的 3 个旋转：τ, τ^2, τ^3（$\tau^4 = e$）。
3. $\rho = \tau \to \sigma^{-1} \to \tau^{-1}$，以及不断重复 ρ 得到的 3 个旋转：ρ, ρ^2, ρ^3（$\rho^4 = e$）。
4. 4 条顶心对角线对应的 8 个非平凡旋转。
5. 6 条对棱中线对应的 6 个非平凡旋转。

以上各种旋转都不相同（因为旋转轴不同）。加上“什么都不做”的恒等变换 e，总共生成变换个数为：

$$1 + 3 + 3 + 3 + 8 + 6 = 24.$$

这正好是我们计算过的，保持正方体位置形状不变的所有旋转的个数。因此，我们通过 σ 和 τ，生成了正方体旋转群 T_6 的所有元素。

5. 构想一个群的例子，使其连线图（生成路径图）与矩群一样。

解答：矩群（J_4）的特征是：有 4 个状态，由两个独立的、做两次就复原的操作生成，且这两个操作互不干扰（可交换）。**生活中的例子**：

(1) **十字路口的两个独立红绿灯**：每个灯有“红”和“绿”两种状态。操作 A 是“切换南北向灯的颜色”，操作 B 是“切换东西向灯的颜色”。两个操作各自做两次复原，且先后顺序不影响最终结果。

(2) **两扇独立的弹簧门**：每扇门有“开”和“关”两种状态。操作 A 是“推开左门”，操作 B 是“推开右门”。

(3) **床单的四个角**：考虑只翻转床单的左右和上下。操作 A 是“左右对调”，操作 B 是“上下对调”。

这些例子虽然物理场景不同，但其背后的状态变换结构与矩群完全同构。

6. **解答**：考虑图中 A 节点到 B 节点的变换。什么变换可以逆转它的效果？没有任何变换可以逆转它的效果。实际上，图中三个变换：$A \to B$、$A \to C$、$B \to C$，效果都无法逆转。

因此，图中的变换违反了可逆性规则，不能是群的生成路径图。

1.3 第三章参考解答

群运算和乘法表

1. **思路分析**：两个独立的电灯开关，每个开关“按”一次改变状态，“按”两次恢复原状，因此 $S^2 = e, X^2 = e$。两个开关独立操作，顺序不影响最终结果，因此 $SX = XS$。

   - $SSX = eX = X$；而 $XSSX = X(e)X = X^2 = e$。因为 $X \neq e$，所以 **假**。
   - $XSX = X^2S = eS = S$。所以 **真**。
   - $SXSXSX = (SX)^3$。因为 $(SX)^2 = SXXS = e$，所以 $(SX)^3 = SX$。又因为 $SX = XS$，所以 $XS = SX$。所以 **真**。
   - $S^8 = (S^2)^4 = e$；$X^{100} = (X^2)^{50} = e$。两者相等，所以 **真**。

2. **思路分析**：在生成路径图中，从同一个起点出发，沿着高亮箭头走，无论路径如何曲折，只要终点相同，对应的群元素乘积就相等。

   - (1) 从起点出发，走 a, b, b, a, b 与走 b, b, a, b, a 终点相同。故 $babba = ababb$。
   - (2) 走 b, a, b, b, a, b 与走 a, b, a 终点相同。故 $babbab = aba$。
   - (3) 走 b, b, a, b 与走 a, b, b, a, b, a 终点相同。故 $babb = ababba$。
   - (4) 走 j, i, i, i, j 与走 i, j, i, j, i 终点相同。故 $jiiij = ijiji$。
   - (5) 走 i, j, i, j, j 与走 j, i, i 终点相同。故 $jjiji = iij$。
   - (6) 走 j, i 与走 i, i, j, i, j, j 终点相同。故 $ij = jjijii$。

3. **思路分析**：判断运算是否交换，即验证是否对任意 x, y 都有 $x * y = y * x$。对于不交换的运算，只需举出一个反例即可。

   - **交换**。整数乘法满足交换律。
   - **不交换**。例如 $1 - 2 = -1$，而 $2 - 1 = 1$，$1 - 2 \neq 2 - 1$。
   - **不交换**。矩阵乘法一般不满足交换律。例如 $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$，可验证 $AB \neq BA$。
   - **交换**。整数乘法交换，模 p 同余类的乘法继承了这一性质。
   - **不交换**。函数的复合一般不交换。例如 $f(x) = x^2, g(x) = 1 - x$，则 $f(g(x)) = (1 - x)^2 = 1 - 2x + x^2$，而 $g(f(x)) = 1 - x^2$。

4. **思路分析**：整数加法群 $\mathbb{Z}$ 是一个无限群。它的“乘法表”（此处应为加法表）的行和列都由所有整数构成，因此是一个无限大的表格，无法在纸面上完整画出。我们可以有限表格展示它的部分，比如 $-2,-1,0,1,2$ 对应的行列，然后用代数式示意：第 m 行第 n 列的元素是 $m+n$。

5. **思路分析**：补全乘法表的核心原则是：每行每列的元素不能重复不能遗漏。已知 $a^2=e$，我们可以逐步推导。

首先，e 行和 e 列是显然的。对于 a 行：已有 a,e，剩下 b,c。因为 $a\cdot b$ 不能是 b（否则 $a=e$），所以必有 $a\cdot b=c$，同理可得 $a\cdot c=b$。

对于 a 列：已有 a,e，剩下 b,c。因为 $b\cdot a$ 不能是 b（否则 $a=e$），所以必有 $b\cdot a=c$，同理可得 $c\cdot a=b$。对于 b 行和 c 行，关键在于 $b\cdot b$ 的取值。

现在 b 行已有 b,c，剩下 e,a。这里出现了分歧，导致两种补全方式：

- **情况一**：$b\cdot b=e$。则 $c\cdot b=a$。进而推导出 $b\cdot c=a$, $c\cdot c=e$。此时，幺元以外元素的阶都是 2，且乘法表是对称的，说明这是一个**交换群**，具体为**矩群** J_4。
- **情况二**：$b\cdot b=a$。则 $c\cdot b=e$。进而推导出 $b\cdot c=e$, $c\cdot c=a$。此时，b 的阶为 4（$b^1=b,b^2=a,b^3=c,b^4=e$），乘法表同样是对称的，说明这也是一个**交换群**，具体为**四元循环群** C_4。

情况一：$bb=e$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

情况二：$bb=a$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

注：高亮部分为 b 行 b 列的元素 bb。在 J_4 中 $bb=e$，在 C_4 中 $bb=a$。

6. **思路分析**：结合生成路径图，理解群元素的意义和代数运算。

- C_5 中，a 是逆时针旋转 72°。a^3 是逆时针旋转 216°（或顺时针 144°）。在图中，从 e 出发沿红箭头走 3 步到达 a^3。
- a^5 是旋转 360°，即恒等变换 e。在图中，走 5 步回到起点。
- 右图中，从状态 1 出发，先 i 后 j 到达 $ji=-k$。先 j 后 i 到达 $ij=k$。它们是不同的变换。这直观展示了四元数群不是交换群。
- 右图中，从状态 1 出发，沿红箭头走 1 步到 i，再沿蓝箭头走 2 步，到达 $-i$。

即：$jji = -i$。

- 两个群的乘法表如下：

五元循环群 C_5 的乘法表：

$\cdot$	e	a	a^2	a^3	a^4
e	e	a	a^2	a^3	a^4
a	a	a^2	a^3	a^4	e
a^2	a^2	a^3	a^4	e	a
a^3	a^3	a^4	e	a	a^2
a^4	a^4	e	a	a^2	a^3

四元数群 U_4 的乘法表：

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

似群非群

1. (1) 查表可知：e 为幺元，且 $aa = ab = ba = bb = e$。因此：

$$(aa)b = eb = b, \quad a(ab) = ae = a.$$

然而按定义 $a \neq b$。因此此运算不符合结合律。

(2) e 为幺元，逆元是 e。$ab = ba = e$，所以 a 是 b 的逆元，b 是 a 的逆元。同时，$aa = bb = e$。所以 a 也是 a 的逆元，b 也是 b 的逆元。

结论：各个元素都有逆元，但 a 和 b 的逆元不唯一。（注：在真正的群中，结合律保证了逆元的唯一性。此处逆元不唯一，正是缺乏结合律导致的。）

2. (1) 我们要验证任意 $x, y, z \in \{e, a, b\}$，是否满足 $(xy)z = x(yz)$。
首先可验证 e 是幺元（$ex = xe = x$ 总成立）。因此，当 x, y, z 中有任何一个为 e 时，结合律显然成立。
当 $x, y, z \in \{a, b\}$ 时，观察乘法表可以发现一个规律：对于任意 $u, v \in \{a, b\}$，都有 $uv = v$（例如 $aa = a, ab = b, ba = b, bb = b$）。因此，$(xy)z = yz = z$；同时，$x(yz) = xz = z$。两者恒相等，故该运算满足结合律。

(2) e 为幺元，逆元是 e。
对于元素 a，需要寻找 x 使得 $ax = xa = e$。观察乘法表中 a 所在的行和列：a 行元素为 a, a, b，a 列元素为 a, a, b。其中根本没有 e 出现，因此不存在任何元素与 a 运算后能得到 e。同理，b 的行和列中也没有 e。
结论：e 有逆元 e，但 a 和 b 没有逆元。

3. (1) 与第 2 题类似，我们分情况验证结合律。当 x, y, z 中有 e 时，结合律显然成立。当 $x, y, z \in \{a, b\}$ 时，观察乘法表发现：对于任意 $u \in \{a, b\}$ 和 $v \in \{a, b\}$，都有 $uv = b$（即 $aa = b, ab = b, ba = b, bb = b$）。因此，$(xy)z = bz = b$；同时，$x(yz) = xb = b$。两者恒相等，故该运算满足结合律。

(2) e 为幺元，逆元是 e。
观察 a 所在的行和列，元素只有 a 和 b，没有 e。因此不存在 x 使得 $ax = e$ 或 $xa = e$。同理，b 也没有逆元。**结论**：e 有逆元 e，但 a 和 b 没有逆元。

4. (1) **没有幺元**。观察乘法表，幺元所在的行和列必须与表头完全一致（即 e, a, b, c 的顺序）。但 e 行为 e, a, c, b，a 行为 a, b, c, e，b 行为 b, c, e, a，c 行为 c, e, a, b。没有任何一行是 e, a, b, c，因此该集合在此运算下没有幺元，自然不构成群。

(2) **不满足消去律**。可验证 e 是幺元。观察 a 行，发现 $aa = ab = a$。若左消去 a，则会得到 $a = b$，这与 a, b 是不同元素矛盾。

(3) **导致元素相等的矛盾**。可验证 e 是幺元。我们通过计算 a 的幂次来寻找矛盾。
若此表对应群，查表可知 $aa = c$，$cc = d$，$dd = c$。因此 $c = dd = (cc)(cc) = cccc$。于是消去一个 c 就得到 $ccc = e$。另一方面，查表可知 $a = cd = c(cc) = ccc$。于是 $a = ccc = e$，矛盾!

(4) **不满足结合律**。可验证 e 是幺元。若此表对应群，我们计算 $c(da)$ 和 $(cd)a$。查表可知 $da = b$，$cb = a$，所以 $c(da) = cb = a$。另一方面，查表可知 $cd = b$，$ba = c$，

所以 $(cd)a = ba = c$。所以 $c(da) \neq (cd)a$，该运算不满足结合律，不构成群。

5. 考虑群 G 的乘法表。

对于行：假设在第 x 行中，有两个不同列 y 和 z 对应的元素相同，即 $xy = xz$。因为 G 是群，x 有逆元 x^{-1}。在等式两边左乘 x^{-1}，得到 $x^{-1}(xy) = x^{-1}(xz)$。根据结合律，$y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = z$。这与假设"$y$ 和 z 是不同列" 矛盾。因此，同一行中的元素两两不同。

另一方面，对 G 中任意元素 a，$x(x^{-1}a) = (xx^{-1})a = ea = a$，所以第 x 行第 $x^{-1}a$ 列是 a。因此 G 的每个元素都恰在第 x 行出现一次，不重不漏。

对于列：同理，假设在第 x 列中，有两个不同行 y 和 z 对应的元素相同，即 $yx = zx$。在等式两边右乘 x^{-1}，按同样方法可算出 $y = z$。因此，同一列中的元素两两不同。

另一方面，对 G 中任意元素 a，$(ax^{-1})x = a(x^{-1}x) = ae = a$。所以第 x 列第 ax^{-1} 行是 a。因此 G 的每个元素都恰在第 x 列出现一次，不重不漏。

6. (1) 根据图的设定，a 是中心点 C 与外围节点之间的双向箭头，这意味着 $a^2 = e$（即连续两次 a 变换回到原点）。我们追踪从中心 C 出发的路径：先走 a 到达外围（如 n_0），再走 b 沿蓝色箭头移动到下一个节点（n_1），最后再走 a 回到中心 C。这条“先 a，再 b，再 a”的路径记为 aba。

因为该路径从 C 出发最终回到了 C，所以 $aba = e$。同理，追踪与上面类似的另一条路径：到达外围（如 n_0）后走 b 沿蓝色箭头移动两次（到达 n_2），最后再走 a 回到中心 C。这条“先 a，再两次 b，再 a”的路径记为 $abba$。因为该路径从 C 出发最终回到了 C，所以 $abba = e$。因此，$aba = abba = e$。如果这是一个群，那么左消去 ab、右消去 a，就得到 $b = e$。矛盾！因此该图不是群的生成路径图。

(2) 观察图中正右的节点（记为 n_0）和正左的节点（记为 n_4）。从 n_0 出发，连续走两次红色箭头 a，到达 n_4，连续走两次蓝色箭头，也到达 n_4。因此，$aa = bb$。

再观察正上的节点（记为 n_2）和正下的节点（记为 n_6）。从 n_2 出发，走红色箭头 a 再走蓝色箭头 b，到达 n_6，连续走两次蓝色箭头，也到达 n_6。因此，$ba = bb$。

从等式 $aa = ba = bb$ 出发，用消去律可得到 $a = b$。矛盾！因此该图不是群的生成路径图。

群的代数定义

1. **思路分析**：验证一个集合是否构成群，需要严格检查群的四个代数公理：**封闭性**、**结合律**、**幺元存在性**、**逆元存在性**。只要有一条不满足，即不是群。

(1) 所有 3 的倍数关于整数的加法**是群**。

- **封闭性**：两个 3 的倍数相加，$3m + 3n = 3(m + n)$，仍是 3 的倍数。
- **结合律**：继承自整数加法的结合律。
- **幺元**：$0 = 3 \times 0$ 是 3 的倍数，且对任意 $3m$ 有 $3m + 0 = 3m$。
- **逆元**：$3m$ 的逆元是 $-3m = 3(-m)$，仍在集合中。

(2) 所有 3 的倍数关于整数的乘法**不是群**。因为**没有幺元**。1 不是 3 的倍数，不在集合中。因此集合中没有元素 e，使任何元素乘 e 后得到自身。

(3) 正实数关于乘方**不是群**。不满足**结合律**。乘方运算不满足结合律，例如 $(2^3)^2 = 8^2 = 64$，而 $2^{(3^2)} = 2^9 = 512$，两者不相等。

(4) 所有完全平方数关于整数的乘法**不是群**。

- 若“完全平方数”包含 0，则 0 没有乘法逆元，不满足**逆元存在性**。
- 若“完全平方数”仅指正完全平方数（$1, 4, 9, \ldots$），则 4 的乘法逆元是 $1/4$，不是整数，不在集合中，不满足**逆元存在性**。

(5) 所有非零的完全平方有理数关于有理数的乘法**是群**。

- **封闭性**：两个完全平方有理数相乘，$\left(\frac{p}{q}\right)^2 \times \left(\frac{r}{s}\right)^2 = \left(\frac{pr}{qs}\right)^2$，仍是完全平方有理数。
- **结合律**：继承自有理数乘法。
- **幺元**：$1 = (1/1)^2$ 是完全平方有理数。
- **逆元**：非零完全平方有理数 $\left(\frac{p}{q}\right)^2$ 的逆元是 $\left(\frac{q}{p}\right)^2$，仍在集合中。

(6) 所有素数有理数关于有理数的乘法**不是群**。不满足**封闭性**。例如，$\frac{2}{3}$ 和 $\frac{5}{7}$ 都是素数有理数，但它们的乘积 $\frac{2}{3} \times \frac{5}{7} = \frac{10}{21}$，分子 10 和分母 21 都不是素数，因此结果不是素数有理数。

(7) 模 n 的简化同余系关于同余类的乘法**是群**。

- **封闭性**：若 a, b 均与 n 互素，则 ab 也与 n 互素。
- **结合律**：继承自同余类的乘法。

- **幺元**：$\overline{1}$ 在简化同余系中，且总有 $\overline{a}\overline{1} = \overline{1}\overline{a} = \overline{a}$。
- **逆元**：由倍和析因定理，若 a 与 n 互素，则存在整数 x, y 使得 $ax + ny = 1$。于是 $ax \equiv 1 \pmod{n}$。另外，x 和 n 的任何公因数必然整除 $ax + ny$。由 $ax + ny = 1$ 可知，x 也与 n 互素，故 $\overline{x}$ 在简化同余系中。故 $\overline{x}$ 即为 $\overline{a}$ 的逆元。

(8) $\{\pm 2^n 3^m \mid n, m \in \mathbb{Z}\}$ 关于有理数的乘法**是群**。

- **封闭性**：$(\pm 2^n 3^m) \times (\pm 2^p 3^q) = \pm 2^{n+p} 3^{m+q}$，仍在集合中。
- **结合律**：继承自有理数乘法。
- **幺元**：$1 = 2^0 3^0$ 在集合中。
- **逆元**：$\pm 2^n 3^m$ 的逆元是 $\pm 2^{-n} 3^{-m}$，由于 $n, m \in \mathbb{Z}$，逆元仍在集合中。

(9) 分母为完全平方数的非零既约分数的集合，关于有理数的乘法**不是群**。不满足**逆元存在性**（或**封闭性**）。例如，$\frac{2}{9}$ 是分母为完全平方数的非零分数，但它的逆元 $\frac{9}{2}$ 的分母是 2，不是完全平方数，不在集合中。

2. **思路分析**：整式的加法和乘法同样需要严格验证四条公理。特别要注意整式和有理式的乘法单位元是什么，逆元是什么。

(1) 整系数一元整式的集合 $\mathbb{Z}[X]$ 关于整式的加法**是群**。整式加法满足封闭性、结合律；幺元是 0；整式 P 的逆元是 $-P$：其系数取相反数后仍为整数。

(2) 实系数一元整式的集合 $\mathbb{R}[X]$ 关于整式的加法**是群**。理由同上，实系数整式加法同样满足群的四个公理。

(3) 整系数一元整式的集合 $\mathbb{Z}[X]$ 关于整式的乘法**不是群**。不满足**逆元存在性**。例如整式 X，若存在逆元 $Q(X) \in \mathbb{Z}[X]$ 使得 $X \cdot Q(X) = 1$，则 X 的次数加上 $Q(X)$ 的次数等于 1 的次数（即 0），这要求 X 的次数不大于 0，矛盾。

(4) 实系数一元整式的集合 $\mathbb{R}[X]$ 关于整式的乘法**不是群**。理由同上，实系数整式乘法下，非常数整式均无逆元。

(5) 实系数非零一元有理式的集合 $\mathbb{R}(X)$ 关于整式的乘法**是群**。非零有理式的乘法满足封闭性、结合律；幺元是 1；非零有理式 $\frac{P(X)}{Q(X)}$ 的逆元是 $\frac{Q(X)}{P(X)}$，由于 $P(X) \neq 0$，逆元仍在 $\mathbb{R}(X)$ 中。

(6) 偶系数一元整式的集合 $\mathbb{B}[X]$ 关于整式的加法**是群**。偶系数整式加法满足封闭性

(偶数加偶数仍为偶数)、结合律；幺元是零多项式（系数全为 0，0 是偶数)；逆元是系数取反的整式（偶数的相反数仍是偶数)。

(7) 奇系数一元整式的集合 $\mathbb{J}[X]$ 关于整式的加法**不是群**。

- 不满足**幺元存在性**：0 是偶数，不在奇系数集合中。
- 不满足**封闭性**：例如 $(5X+1)+(-3X+1)=2X+2$。系数为偶数，不在奇系数集合中。

3. **思路分析**：对于元素极少的群，可以通过穷举法（分类讨论）来证明其性质。核心思想是利用“每个元素的逆元必须唯一，且必须在群中”这一性质。

(1) **证明**：在二元群 $\{e,a\}$ 中，元素 a 的逆元 a^{-1} 必须是群中的元素，即 $a^{-1}=e$ 或 $a^{-1}=a$。若 $a^{-1}=e$，则根据逆元定义有 $ae=e$，从而 $a=e$，这与二元群中元素互异（$a\neq e$）矛盾。因此，只能有 $a^{-1}=a$。根据逆元定义，$aa=e$。

(2) **解答**：根据群的性质和前一问的结论，我们可以唯一确定乘法表。幺元 e 满足 $ee=e, ea=a, ae=a$。由上知 $aa=e$。因此，乘法表如下： 由于所有元素的乘

$\cdot$	e	a
e	e	a
a	a	e

积都被唯一确定，因此二元群只有一种。

4. **思路分析**：三元群的推导比二元群稍复杂，需要利用消去律（若 $xy=xz$ 则 $y=z$）以及逆元的唯一性。

(1) **证明**：考察 ab，如果 $ab=a$，那么消去 a 得到 $b=e$，矛盾！所以 $ab\neq a$。同理 $ab\neq b$。因此，只能有 $ab=e$。

(2) **证明**：反设 $aa=e$。由前结论知 $ab=e=aa$。左消去 a 可得 $a=b$。矛盾！
故假设不成立，$aa\neq e$。

(3) **解答**：由第一问知 $ab=e$。用同样思路可证 $ba=e$。由第二问可知 $aa\neq e$。同理可证 $bb\neq e$。如果 $aa=a$，则消去 a 得到 $a=e$，矛盾！所以只能有 $aa=b$。同理只能有 $bb=a$。

综上，我们得到乘法表如下：

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

由于所有元素的乘积都被唯一确定，因此三元群只有一种。

5. **思路分析**：本题旨在建立“生成路径图（直观图像）”与“乘法表（代数结构）”之间寻找逆元的对应关系。

(1) **在生成路径图中找逆元**：生成路径图展示了群元素在生成元作用下的变换关系。给定群元素 x，为了定位它，我们用元素来命名节点。于是，从 e 节点出发，到达 x 节点的变换组合，效果就是 x。而 x 的逆元就是能逆转这个效果的变换。因此，我们从 x 节点再出发，沿生成路径图，回到 e 节点。沿途所有变换组合的效果，就是 x 的逆元。根据群和生成路径图的定义，以上说的两条路径都必然存在。

(2) **在乘法表中找逆元**：乘法表穷举了所有元素对的运算结果。根据逆元的定义，x 的逆元 y 是满足 $x \cdot y = e$ 且 $y \cdot x = e$ 的元素。在乘法表中，寻找 x 的逆元的方法非常直观：

- 找到 x 所在的**列**，在这一列中寻找幺元 e。e 所在的**行**的行标，就是 x 的左逆元。
- 找到 x 所在的**行**，在这一行中寻找幺元 e。e 所在的**列**的列标，就是 x 的右逆元。
- 左逆元等于右逆元，因此通过上述两种方法找到的结果是一致的。

1.4 第四章参考解答

循环群与交换群

1. 设 k 是任取的整数,a 是 n 元循环群 C_n 的生成元。那么，对于哪些整数 k，有 $a^k = e$? 这些整数构成的集合有什么特征?

解答：按定义，$a^n = e$，且对于 $0 < i < n$，有 $a^i \neq e$。
对于任意整数 k，做带余除法，用 n 去除 k，得到：$k = qn + r$，其中 $0 \leq r < n$。那么

$$a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r.$$

要使 $a^k = e$，就必须有 $a^r = e$。根据生成元的性质，只有当 $r = 0$ 时才成立。因此，k 必须是 n 的倍数。另一方面，n 整除 k 时可验证 $a^k = e$。
综上所述，满足 $a^k = e$ 的整数 k 的集合为：

$$\{nz \,|\, z \in \mathbb{Z}\}$$

后面我们会学到，它是整数加法群的子群，记为 $n\mathbb{Z}$。

2. 考虑 n 元循环群 $\mathsf{C}_n = \{a, a^2, \cdots, a^n = e\}$。对正整数 $k > 1$，设 $b = a^k$。我们想了解：b 不断自乘，得到的环道是怎样的?

(1) 如果 k 是 n 的因数：$n = mk$，证明：b 的环道长度为 m。

解答：首先，$b^m = a^{km} = a^n = e$。因此环道长度不超过 m。
设 $0 < i < m$,则 $b^i = \left(a^k\right)^i = a^{ik}$。考虑 $b, b^2, \cdots, b^m$,它们可以写作 $a^k, a^{2k}, \cdots, a^{mk}$。
$0 < i < m$ 时，$ik < mk = n$，因此 $b^i = a^{ik} \neq e$。于是环道长度就是 m。

(2) 如果 k 和 n 互素，证明：b 能生成 C_n 全体元素。

解答：要证明 b 能生成全群，只需证明 b 的环道长度等于 n。
首先，由于 C_n 只有 n 个元素，所以环道长度不大于 n。
设 b 的环道长度为 $j \leqslant n$，则 $e = b^j = a^{kj}$。这说明 n 整除 kj。因为 k 和 n 互素，没有大于 1 的公因数，根据整除的性质，n 必须整除 j。综上，只能有 $j = n$。
既然 b 的环道长度等于群势 n，就说明 $b, b^2, \cdots, b^n$ 两两不同，因此，b 能生成 C_n 的全体元素。

(3) 一般情况下，记 d 为 k 和 n 的最大公约数，$n = md$，证明：b 的环道长度为 m。

解答：仍然分析 b 的环道长度。

设 b 的环道长度为 j，则 $a^{kj} = e$，故 n 整除 kj。

设 $n = md$，$k = qd$，则 q 与 m 互素。代入，得到 md 整除 qdj，即 m 整除 qj。因为 q 与 m 互素，所以 m 必须整除 j。这说明 j 至少是 m。另一方面，当 $j = m$ 时，

$$b^m = a^{km} = a^{qdm} = a^{qn} = (a^n)^q = e.$$

因此，满足条件的最小正整数 j 就是 m。b 的环道长度为 m。

注：这里我们根据 k 和 n 的公因数，确定了 a^k 的环道长度。后面我们会学到：环道长度总是群势 n 的因数。另一方面，与 n 的公因数为 d 的 k 的个数是可以算出来的：它等价于找到 $1, 2, \cdots, m$ 里所有与 m 互素的数，因此等于 $\varphi(m)$。其中 $\varphi(m)$ 是模 m 简化同余系中同余类的个数，也就是所有与 m 互素的同余类个数。也就是说，这些 a^k 的环道长度都是 m。对不同的 d，也会找到不同的 a^k。于是，按照环道长度，就能不重不漏地把 n 个元素进行划分。环道长度为 m 的 a^k 有 $\varphi(m)$ 个。当 d 遍历 n 的所有因子时，m 也遍历 n 的所有因子。最终得到结论：

$$n = \sum_{m|n} \varphi(m).$$

3. 考虑 k 个二元循环群架积得到的群 C_2^k。它一般记为

$$\mathsf{C}_2^k = \{(n_1, n_2, \cdots, n_k) \,|\, n_1, n_2, \cdots, n_k \in \{0, 1\}\}.$$

其中元素运算为按分量的同余加法：$(n_1, n_2, \cdots, n_k) + (m_1, m_2, \cdots, m_k)$ 的第 i 位是 $n_i + m_i$ 模 2 的余数。

(1) 证明：任何 $x \in \mathsf{C}_2^k$ 都满足 $x + x = (0, 0, \cdots, 0)$。

解答：每个分量 $n_i \in \{0, 1\}$，所以 $n_i + n_i$ 要么是 $0 + 0 = 0$，要么是 $1 + 1 = 2 \equiv 0 \pmod 2$。因此，$x + x$ 的每一个分量都是 0，即 $x + x = (0, 0, \cdots, 0)$。

(2) 说明为何 C_2^k 构成群。说出群的幺元和任何元素的逆元。

解答： **封闭性**：两个分量均为 0 或 1 的元组，按位模 2 相加后，每个分量依然是 0 或 1，结果仍在集合中。**结合律**：因为每个分量的模 2 加法满足结合律，所以整个元组的运算也满足结合律。**幺元**：全 0 元组 $(0, 0, \cdots, 0)$。任何元组加上它，按位模 2 加后保持不变。**逆元**：对于任何元素 $x = (n_1, \cdots, n_k)$，$x + x = e$，因此它的逆元就是它自身。

(3) 设 a, b 为正整数，证明：C_2^{a+b} 与 C_2^a、C_2^b 架积得到的群同构。

解答： $\mathsf{C}_2^a \times \mathsf{C}_2^b$ 中的元素形如 (u, v)，其中 u 是 a 元组，v 是 b 元组。我们可以构造一个映射 f：将 C_2^{a+b} 中的 $(a+b)$ 元组 $(n_1, \cdots, n_a, n_{a+1}, \cdots, n_{a+b})$，拆分成前 a 位和后 b 位，映射为 $\big((n_1, \cdots, n_a), (n_{a+1}, \cdots, n_{a+b})\big)$。这个映射显然是双射(一一对应)。同时，它保持运算：两个 $(a+b)$ 元组相加，等于它们的前 a 位分别相加，后 b 位分别相加。这恰好对应于架积群中分量的运算规则。因此，这两个群同构。

注：这说明“拼接”元组的操作，在代数上完美对应了群的架积。C_2^k 可以看作 k 个独立的“开关”状态。)

4. 考虑两个循环群 C_n、C_m 架积得到的群：$\mathsf{C}_n \times \mathsf{C}_m$。记 C_n、C_m 的幺元分别为 e_1, e_2。设 a, b 分别为 C_n、C_m 的生成元。

(1) 考虑 (a, b)，它的逆元素是什么?

解答： 设 (a, b) 的逆元为 (x, y)。按架积的定义，$(ax, by) = (e_1, e_2)$，于是取 $x = a^{-1}, y = b^{-1}$ 即可。所以 (a, b) 的逆元是 (a^{-1}, b^{-1})。

(2) (a, b) 不断自乘得到 $(a, b), (a^2, b^2), \cdots (a^k, b^k), \cdots$。找出使得 $(a^k, b^k) = (e_1, e_2)$ 的最小正整数 k。k 有什么性质?

解答： 要使 $(a^k, b^k) = (e_1, e_2)$，必须同时满足 $a^k = e_1$ 和 $b^k = e_2$。这意味着 k 必须是 n 的倍数（使 $a^k = e_1$），同时也必须是 m 的倍数（使 $b^k = e_2$）。满足这两个条件的最小正整数 k，就是 n 和 m 的**最小公倍数**。

(3) 证明：如果 m, n 互素，(a, b) 能生成 $\mathsf{C}_n \times \mathsf{C}_m$。

解答： 如果 m, n 互素，它们的最小公倍数就是 mn。由上一问可知，(a, b) 的环道长度为 mn。而架积群 $\mathsf{C}_n \times \mathsf{C}_m$ 的元素个数就是 nm。一个元素的环道长度等于群的总元素个数，说明这个元素不断自乘可以遍历群中所有状态。因此，(a, b) 能生成整个群。

(4) 证明：如果 m, n 不互素，那么没有任何群元素能单独生成整个 $\mathsf{C}_n \times \mathsf{C}_m$。

解答： 如果 m, n 不互素，设它们的最大公约数为 $d > 1$，设 $m = m_1 d, n = n_1 d$，其中 $m_1 < m, n_1 < n$。设 $t = m_1 n_1 d < mn$。t 是 m, n 的公倍数，因此不小于其最小公倍数。这说明：m, n 的最小公倍数小于 mn。而由前问可知，(a, b) 的环道长度是 m, n 的最小公倍数，故 (a, b) 的环道长度小于 mn。这说明它无法单独生

成 $\mathsf{C}_n \times \mathsf{C}_m$。

对于一般的元素 (a^i, b^j)，情况也是类似的。要使得 $(a^{ik}, b^{jk}) = (e_1, e_2)$，就是要 n 整除 ik，m 整除 jk。而如果 k 是 m, n 的最小公倍数，那么必然有 n 整除 ik，m 整除 jk。因此，任何元素的环道长度都不会超过 m, n 的最小公倍数，从而小于 mn。既然任何元素的环道长度都小于 mn，自然没有任何元素能单独生成整个群。

映轮群和置换群

1. 存在恰有 77 个元素的映轮群吗?

解答：不存在。
根据定义，正 n 边形映轮群 D_n 包含 n 个旋转变换和 n 个翻转变换，总元素数为 $2n$。因为 n 是正整数，所以 $2n$ 必然是偶数。而 77 是奇数，不可能等于 $2n$。

2. 研究映轮群 D_4。

(1) D_4 有几个元素？列出 D_4 所有元素，并定性说明它们与 D_3 元素的相似之处。

解答： D_4 有 $2 \times 4 = 8$ 个元素。
4 个旋转变换：逆时针旋转 0°（恒等 e），90°（记为 r），180°（r^2），270°（r^3）。
4 个翻转变换：关于两条对边中点连线的翻转（记为 s_1, s_2），关于两条对角线的翻转（记为 s_3, s_4）。

与 D_3 的相似之处：

1. 都由一半旋转、一半翻转组成。
2. 任何翻转的平方都是幺元（即翻转两次恢复原状，环道长度为 2）。

(2) 如何生成 D_4？研究 D_4 的生成路径图，说明相关的变换如何生成整个群。

解答：我们可以用逆时针 90° 旋转 r 和一个翻转 s（例如关于某条对角线的翻转）来生成整个群。查看其生成路径图，r 不断自乘可以到达 4 个状态。经过翻转后可以到达另外 4 个状态。另外 4 个状态之间也相互通过不断旋转到达，但方向相反。从另外 4 个状态出发，经过翻转也可以对应返回之前纯旋转到达的 4 个状态。

通过不断交替使用 r 和 s，我们可以从 e 出发，到达群中任何一个状态。

(3) 给出 D_4 各个元素的环道。对比 D_4 的环道图，分析哪些元素的环道和环道图上不一样。

解答:

- e，环道长 1：$\{e\}$。
- r, r^3，环道长 4：$\{e, r, r^2, r^3\}$。
- r^2，环道长 2：$\{e, r^2\}$。
- 4 个翻转 $s_i = r^i s$ $(i = 0, 1, 2, 3)$，环道长 2：$\{e, s_i\}$。

环道图中，旋转变换处于同一个四阶环道里，它是 r 生成的环道：$\{e, r, r^2, r^3\}$。这一点与 D_3 一样。不一样的是，这个环道仅仅是 r, r^3 的环道，而不是 r^2 的环道。

(4) 写出 D_4 的乘法表。

解答:

表 一.1: 映轮群（D_4）的乘法表

$\cdot$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

3. 写出 S_1 到 S_{10} 这 10 个全置换群的势。

解答: n 元全置换群 S_n 的势为 $n!$（n 的阶乘）。具体数值如下:

$$|\mathsf{S}_1| = 1! = 1 \qquad |\mathsf{S}_6| = 6! = 720$$
$$|\mathsf{S}_2| = 2! = 2 \qquad |\mathsf{S}_7| = 7! = 5040$$
$$|\mathsf{S}_3| = 3! = 6 \qquad |\mathsf{S}_8| = 8! = 40320$$
$$|\mathsf{S}_4| = 4! = 24 \qquad |\mathsf{S}_9| = 9! = 362880$$

$$|\mathsf{S}_5| = 5! = 120 \qquad |\mathsf{S}_{10}| = 10! = 3628800$$

可以观察到，随着 n 的增加，群的大小呈爆炸式增长。这解释了为什么研究高维对称性如此困难。

4. 研究 S_4。

(1) **解答：** S_4 有 $4! = 24$ 个元素。它的所有元素可见本章正文最后的图 4.25。

(2) **解答：** 本章介绍的写法是用箭头来表示映射关系。两行写法中，如果把上行固定为 $1,2,3,4$，那么把下行的数逐个写出来，就是简单写法的结果。反之，把简单写法作为下行，添上上行 $1,2,3,4$，再在相同的数之间标上箭头连起来，就是本章正文里的写法。

(3) **解答：** $\tau_1 = (2\,3\,4\,1)$ 表示 $1 \to 2, 2 \to 3, 3 \to 4, 4 \to 1$。$\tau_1^2 = (3\,4\,1\,2), \tau_1^3 = (4\,1\,2\,3), \tau_1^4 = e$。它的环道长度为 4。

(4) **解答：** $\tau_2 = (2\,1\,3\,4)$ 表示 $1 \to 2, 2 \to 1, 3 \to 3, 4 \to 4$。这是一个**对换**，它只调转 $1,2$ 的位置。它的环道长度为 2：τ_2, e。

(5) **解答：** $\tau_3 = (2\,1\,4\,3)$ 表示 $1 \to 2, 2 \to 1, 3 \to 4, 4 \to 3$。这是一个**双对换**，它调转 $1,2$ 的位置，也调转 $3,4$ 的位置。它的环道长度为 2：τ_3, e。

(6) **解答：** $\tau_4 = (2\,3\,1\,4)$ 表示 $1 \to 2, 2 \to 3, 3 \to 1, 4 \to 4$。$\tau_4^2 = (3\,1\,2\,4), \tau_4^3 = e$。它的环道长度为 3。

(7) **解答：** 根据上述分析以及穷举所有 24 个置换，环道长度共有 **4 种**：长度为 1：恒等变换（1 个）。长度为 2：对换（6 个）和双对换（3 个），共 9 个。长度为 3：8 个。长度为 4：6 个。

(8) **解答：** 经过计算：

- τ_1 与 τ_2, τ_3, τ_4 均不交换。
- τ_2 和 τ_3 交换：$\tau_2\tau_3 = (1\,2\,4\,3) = \tau_3\tau_2$。
- τ_2 与 τ_4 不交换。
- τ_3 与 τ_4 不交换。

5. (1) **解答：** 观察生成路径图，外圈有 8 个节点，内圈有 8 个节点。总共有 $8+8=16$ 个节点。因为生成路径图中的每个节点代表群的一个唯一状态，所以群 G 有 16

个元素。

(2) **解答**：群 G 由两个变换 a（红边）和 b（蓝边）生成。

- a 的作用：在外圈和内圈对应的节点之间来回翻转。因为红边是双向的，所以 $a^2 = e$。
- b 的作用：在外圈，b 的效果是顺时针旋转一步。但在内圈，b 的作用不是简单的顺时针旋转，而是“跳 3 步”。

与 D_8 的不同：
在 D_8 的生成路径图中，如果外圈 b 是顺时针一步步旋转，那么内圈的 b 作用是逆时针旋转。但在 G 的生成路径图中，内圈的 b 作用是“跳 3 步”。
代数上，D_8 满足关系 $aba = b^{-1}$（即 $aba = b^7$）；而群 G 满足关系 $aba = b^3$。这是一个不同于映轮群的 16 元群。

(3) **解答**：从节点 e 出发，先沿红色箭头进入内圈，然后沿蓝色箭头即到达 x。因此，$x = ba$。

(4) **解答**：图中路径告诉我们，x 的效果就是先红后蓝，先 a 后 b：$a \to b$。因此，不断重复“先红后蓝”，就是 x 不断自乘的结果。从 e 出发，先红后蓝，得到 x；再次“先红后蓝”，得到外圈最下方节点；再次“先红后蓝”，得到内圈左上节点；再次“先红后蓝”，回到 e。
因此，x 不断自乘，4 步后回到 e：$x^4 = e$。

(5) **解答**：由上可知环道长度为 4：$e \to x \to x^2 \to x^3 \to e$。

(6) **解答**：我们需要计算群中所有 16 个元素的环道长度（即元素的阶）。按照以上的做法，先用 a, b 表达从 e 到达该元素对应节点的方法，然后不断重复，看几次后回到 e。
外圈元素（形如 b^i）：

- e：长度是 1。
- b, b^3, b^5, b^7：长度是 8。
- b^2, b^6：$(b^2)^4 = b^8 = e$，长度是 4。
- b^4：$(b^4)^2 = b^8 = e$，长度是 2。

内圈元素（形如 $b^i a$）：

- 如果 i 是偶数（$i = 0, 2, 4, 6$）：长度是 2。

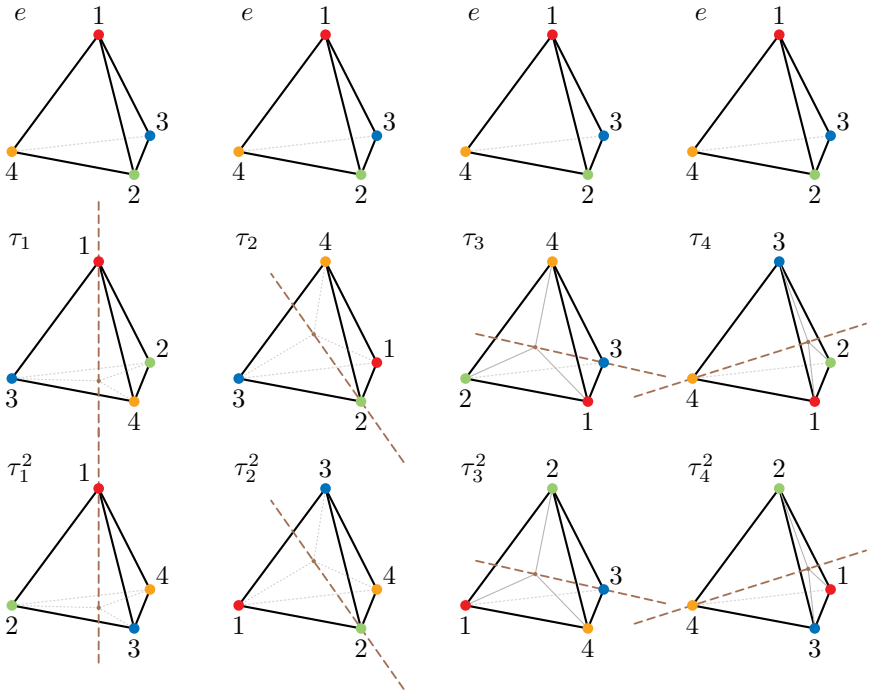
- 如果 i 是奇数（$i=1,3,5,7$）：长度是 4。

分类整理：

- 环道长度为 1 的元素：1 个（e）。
- 环道长度为 2 的元素：5 个（b^4，以及 a, b^2a, b^4a, b^6a）。
- 环道长度为 4 的元素：6 个（外圈的 b^2, b^6，以及 ba, b^3a, b^5a, b^7a）。
- 环道长度为 8 的元素：4 个（外圈的 b, b^3, b^5, b^7）。

注：对比 D_8，D_8 中内圈所有元素的环道长度都是 2。而群 G 中，内圈元素的环道长度有 2 也有 4。这正是 $aba=b^3$ 与 $aba=b^7$ 在代数结构上的表现。

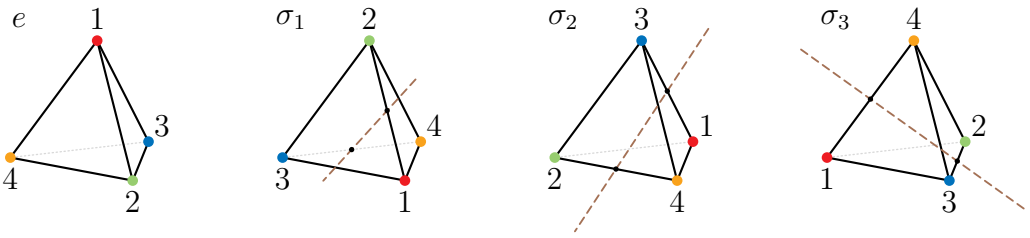
6. (1) **解答**：绕一顶点中线的旋转变换一共有 3 个，分别是不变、旋转 120° 和旋转 240°（或反方向旋转 120°）。按任何方向旋转 3 次都得到恒等变换。我们把顶点按 $1,2,3,4$ 编号，把过顶点 1 且按某个方向的旋转 120° 记为 τ_1，则 τ_1^2 就是按相反方向的旋转 120°。同理，绕顶点 $2,3,4$ 中线的旋转变换分别记为 τ_2, τ_3, τ_4 和 $\tau_2^2, \tau_3^2, \tau_4^2$。



注：和正三角形的情况一样，一旦我们命名并固定了这些变换，它们就不再和正四面体的顶点绑定了。否则我们旋转了正四面体之后再来谈“绕顶点 1 中线的旋转”，就不知道在谈哪个了。为此，我们假设这样的初始情景：正四面体放置在

水平的桌面上，顶点 1 在上方，顶点 2,3,4 在下方和桌面接触。其中顶点 2 在前（更靠近我们），顶点 3,4 靠后，顶点 4 在左，顶点 3 在右（见上图上起第一排的图形）。因此，我们说的 τ_1 变换更详细地定义为：以上方顶点（初始状态的顶点 1）到下面中心的连线（过顶点 1 的中线）为轴的旋转（见上图第二排左起第一个图形）。它把初始状态的顶点 2 旋转到顶点 3 的位置，把顶点 3 旋转到顶点 4 的位置，把顶点 4 旋转到顶点 2 的位置。τ_1^2 则是把顶点 2 旋转到顶点 4 的位置，把顶点 4 旋转到顶点 3 的位置，把顶点 3 旋转到顶点 2 的位置（见上图上起第三排左起第一个图形）。其他 $\tau_i, \tau_i^2 (i = 2, 3, 4)$ 类似（见上图其他图形）。

(2) **解答**：正四面体有 3 条对棱中线。绕任一条对棱中线旋转，就是让相关的两条棱绕其中点旋转。因此，该棱的两顶点总在同一平面内，不会旋转到另两顶点。要使得顶点重合，就必须旋转 180°。因此，绕一条对棱中线的旋转变换只有 2 个：不变和旋转 180°。我们把过棱 1,2 和 3,4 的中线旋转 180° 记为 σ_1，把过棱 1,3 和 2,4 的中线旋转 180° 记为 σ_2，把过棱 1,4 和 2,3 的中线旋转 180° 记为 σ_3。



(3) **解答**：完全不变对应于恒等变换 e。绕顶点中线的旋转变换保持该顶点不变，其他三个顶点变换，因此对应 3 元轮换：

$$\begin{aligned} \tau_1 &= (1\,3\,4\,2), & \tau_1^2 &= (1\,4\,2\,3), \\ \tau_2 &= (3\,2\,4\,1), & \tau_2^2 &= (4\,2\,1\,3), \\ \tau_3 &= (2\,4\,3\,1), & \tau_3^2 &= (4\,1\,3\,2), \\ \tau_4 &= (2\,3\,1\,4), & \tau_4^2 &= (3\,1\,2\,4). \end{aligned}$$

绕对棱中线的旋转变换让两棱分别对应的两对顶点互换位置，因此对应双对换：

$$\sigma_1 = (2\,1\,4\,3), \quad \sigma_2 = (3\,4\,1\,2), \quad \sigma_3 = (4\,3\,2\,1).$$

不难验证它们满足前面提到的性质：

$$\begin{aligned} \tau_1^3 = \tau_2^3 = \tau_3^3 = \tau_4^3 = e, \\ \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = e. \end{aligned}$$

(4) **解答：**

第一个等式：从右到左验证右边三个置换的复合效果。

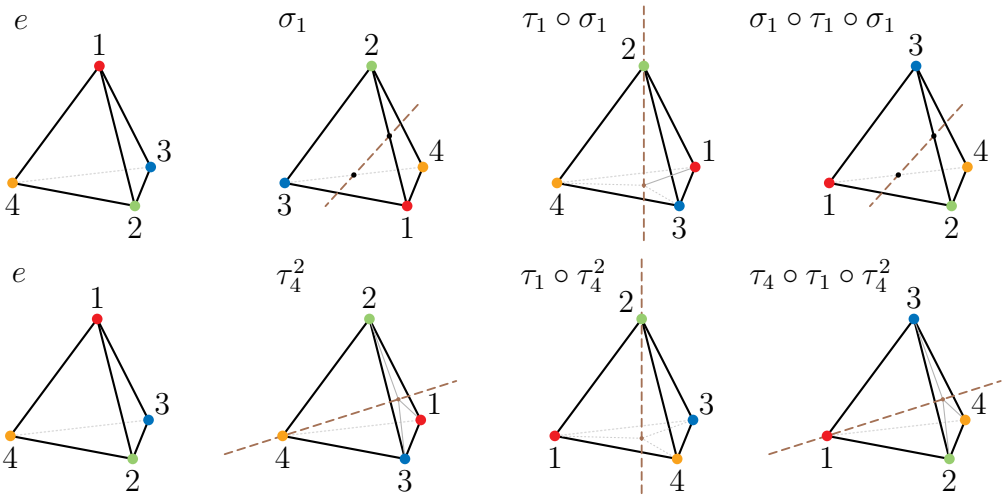
- 1 被映射到 2，然后被映射到 3，再被映射到 4，所以 $1 \mapsto 4$。
- 2 被映射到 1，然后被映射到 1，再被映射到 2，所以 $2 \mapsto 2$。
- 3 被映射到 4，然后被映射到 2，再被映射到 1，所以 $3 \mapsto 1$。
- 4 被映射到 3，然后被映射到 4，再被映射到 3，所以 $4 \mapsto 3$。

因此，右边的复合置换效果是 (4 2 1 3)，与左边相同。

第二个等式：从右到左验证右边三个置换的复合效果。

- 1 被映射到 3，然后被映射到 4，再被映射到 4，所以 $1 \mapsto 4$。
- 2 被映射到 1，然后被映射到 1，再被映射到 2，所以 $2 \mapsto 2$。
- 3 被映射到 2，然后被映射到 3，再被映射到 1，所以 $3 \mapsto 1$。
- 4 被映射到 4，然后被映射到 2，再被映射到 3，所以 $4 \mapsto 3$。

因此，右边的复合置换效果是 (4 2 1 3)，与左边相同。



从正四面体的角度来看，这两个等式说明了绕过顶点 1 中线的旋转与绕过顶点 2 中线的旋转之间如何转换。第一个等式的含义是：首先绕交换 1, 2 顶点和 3, 4 顶点的对棱中线旋转 180°，然后绕顶点 1 中线旋转 120°，最后再绕交换 1, 2 顶点和 3, 4 顶点的对棱中线旋转 180°，最终效果等同于绕顶点 2 中线旋转 120°。第二个等式的含义是：首先绕过顶点 4 的中线旋转 120°，然后绕过顶点 1 的中线旋转 120°，最后绕过顶点 4 的中线反向旋转 120°，最终效果等同于绕顶点 2 中线旋转 120°。

(5) **解答：**

空间中的旋转总绕着一个轴线进行。如果一个旋转交换两个顶点，那么轴线必然经过两顶点的中点，也就是对应棱的中点。然而，该旋转要保持正四面体的位置形状不变，因此必然经过其中心。于是自然经过对棱的中点，成为对棱中线，于是也交换另两个顶点。因此，旋转不可能只交换两个顶点，而是要么不交换顶点，要么交换两对顶点。

(6) **解答：**

用反证法证明。上一问已经说明旋转无法得到对换。假设能得到 4 元轮换，我们可以通过将它与 A_4 的某个变换组合，得到对换，从而违反群的封闭性，得到矛盾。

作为例子，考虑 4 元轮换 $(2\,3\,4\,1)$，它把顶点映射到下一个编号（最后返回顶点 1）。我们希望再经过一次变换后得到 $1,2$ 的对换。据此倒推该变换：

- 1 被映射到 2，所以该变换必须把 2 映射到 2。
- 2 被映射到 3，所以该变换必须把 3 映射到 1。
- 3 被映射到 4，所以该变换必须把 4 映射到 3。
- 4 被映射到 1，所以该变换必须把 1 映射到 4。

于是这个变换应该是 $(4\,2\,1\,3)$ 验证：计算 $(4\,2\,1\,3)\circ(2\,3\,4\,1)$，得到

$$(4\,2\,1\,3)\circ(2\,3\,4\,1)=(2\,1\,3\,4).$$

确实得到 $1,2$ 的对换。而 $(4\,2\,1\,3)$ 是绕顶点 2 中线旋转 120° 的变换，确实在 A_4 中。

(7) **解答：**

所有 24 个 4 元置换，可以分为：恒等变换、对换、双对换、3 元轮换和 4 元轮换。其中，4 元轮换有 6 个，3 元轮换有 8 个，双对换有 3 个，对换有 6 个。

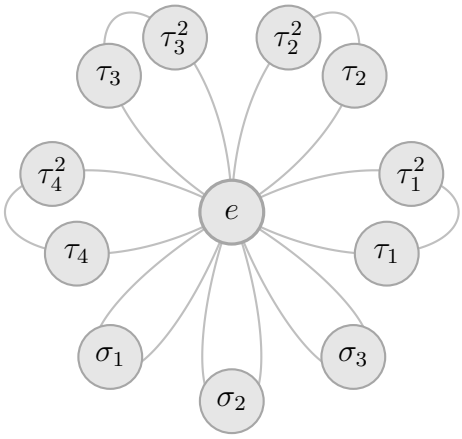
前面已经证明：恒等变换、双对换和 3 元轮换在 A_4 中，而对换和 4 元轮换不在 A_4 中。因此，A_4 一共有：

$$1+3+8=12$$

个元素。它同构于 12 个 4 元置换构成的置换群：

$$\begin{aligned}\{&(1\,2\,3\,4),(1\,3\,4\,2),(1\,4\,2\,3),(3\,2\,4\,1),\\&(4\,2\,1\,3),(2\,4\,3\,1),(4\,1\,3\,2),(2\,3\,1\,4),\\&(3\,1\,2\,4),(2\,1\,4\,3),(3\,4\,1\,2),(4\,3\,2\,1)\}\end{aligned}$$

(8) **解答**：A_4 中有 4 个长度为 3 的环道，3 个长度为 2 的环道。环道图如下：



(9) **解答**：

我们把第 4 问中的等式写成：

$$\tau_2^2 = \sigma_1 \circ \tau_1 \circ \sigma_1^{-1},$$

继续计算 τ_1, σ_1 其他的组合方式，得到：

$$\sigma_1 \circ \tau_1 = \tau_3$$
$$\tau_1 \circ \sigma_1 = \tau_4^2$$

因此 $\tau_4 = \tau_4^4 = \tau_2^2 \circ \tau^2 = \tau_1 \circ \sigma_1 \circ \tau_1 \circ \sigma_1$。

(10) **解答**：

从 $e, \tau_1, \tau_2, \tau_3, \tau_4$ 等不同元素出发，不断复合 τ_1。每得到一个三元循环就将其记录起来，在剩余的元素里再挑一个，继续不断复合 τ_1。比如，从 τ_3 出发，可得：$\tau_1 \circ \tau_3 = \tau_2$，$\tau_1 \circ \tau_2 = \sigma_3$，$\tau_1 \circ \sigma_3 = \tau_3$。记录这个循环。然后从循环中没出现过的元素比如 τ_4 开始，继续计算 $\tau_1 \circ \tau_4$，$\tau_1 \circ \tau_1 \circ \tau_4$ 等等。直到不再有剩余元素。最终得到四个三元循环：

$$e \xrightarrow{\tau_1} \tau_1 \xrightarrow{\tau_1} \tau_1^2 \xrightarrow{\tau_1} e,$$
$$\tau_3 \xrightarrow{\tau_1} \tau_2 \xrightarrow{\tau_1} \sigma_3 \xrightarrow{\tau_1} \tau_3,$$
$$\tau_4^2 \xrightarrow{\tau_1} \tau_3^2 \xrightarrow{\tau_1} \sigma_1 \xrightarrow{\tau_1} \tau_4^2,$$
$$\tau_4 \xrightarrow{\tau_1} \sigma_2 \xrightarrow{\tau_1} \tau_2^2 \xrightarrow{\tau_1} \tau_4.$$

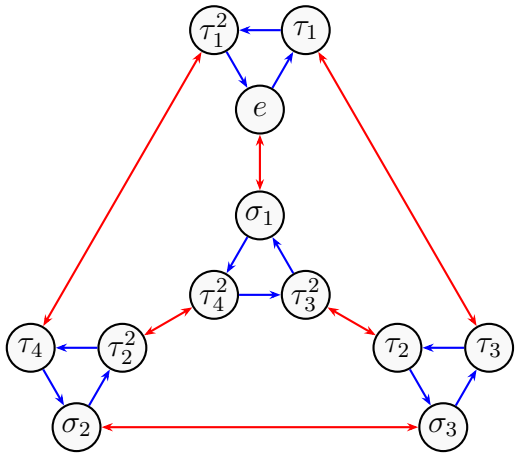
它们完整覆盖了 A_4 的所有 12 个元素。

(11) **解答：**

$\sigma_1^2 = e$，所以“通路”就是按同样的方法得到的二元循环。经计算得到：

$$
\begin{aligned}
e &\xrightarrow{\sigma_1} \sigma_1 \xrightarrow{\sigma_1} e,\\
\tau_1 &\xrightarrow{\sigma_1} \tau_3 \xrightarrow{\sigma_1} \tau_1,\\
\tau_1^2 &\xrightarrow{\sigma_1} \tau_4 \xrightarrow{\sigma_1} \tau_1^2,\\
\tau_2^2 &\xrightarrow{\sigma_1} \tau_4^2 \xrightarrow{\sigma_1} \tau_2^2,\\
\tau_2 &\xrightarrow{\sigma_1} \tau_3^2 \xrightarrow{\sigma_1} \tau_2\\
\sigma_2 &\xrightarrow{\sigma_1} \sigma_3 \xrightarrow{\sigma_1} \sigma_2.
\end{aligned}
$$

于是最终可以画出 A_4 的生成路径图如下：



变换图例：

σ_1

τ_1

1.5 第五章参考解答

1. (1) 正确。C_3 同构于 $\{e, r, r^2\}$

(2) 正确，D_3 同构于 S_3（是其自身的子群）。

(3) 正确，C_3 同构于 $\{e, a^2, a^4\}$。

(4) 错误。可以验证 C_8 的子群大小为 $1, 2, 4, 8$，不包含三元群。

(5) 正确。C_3 同构于 $\{(x, e) \mid x \in \mathsf{C}_3\}$。

(6) 正确。C_6 同构于 $\langle (a, b^2) \rangle$。

(7) 正确。$n\mathbb{Z}$ 同构于 $\{(nk, 0) \mid k \in \mathbb{Z}\}$。

(8) 错误。$\mathbb{Z}_n$ 中有 n 阶元素，但 $\mathbb{Z}$ 中没有 n 阶元素。

2. **证明**:
设 G 有两个子群 H_1, H_2。按照定义，$\forall a, b \in H_1 \cap H_2$，$ab^{-1} \in H_1$ 且 $ab^{-1} \in H_2$。因此 $ab^{-1} \in H_1 \cap H_2$。因此按照子群判断标准，$H_1 \cap H_2$ 也是 G 的子群。

子群的并集一般不是子群。比如，D_3 的子群 $\{e, r, r^2\}$ 和 $\{e, s\}$ 的并集有 4 个元素，不是 $|\mathsf{D}_3|$ 的因数，因此不是其子群。

3. **证明**:
任取 gHg^{-1} 中两个元素，可以写为 gag^{-1}, gbg^{-1}，其中 $a, b \in H$。计算:

$$\begin{aligned} gag^{-1}\left(gbg^{-1}\right)^{-1} &= gag^{-1}\left(g^{-1}\right)^{-1}b^{-1}g^{-1} \\ &= gag^{-1}gb^{-1}g^{-1} = g(ab^{-1})g^{-1}. \end{aligned}$$

由于 H 是子群，$ab^{-1} \in H$，所以 $g(ab^{-1})g^{-1} \in gHg^{-1}$。因此按照子群判断标准，$gHg^{-1}$ 也是 G 的子群。

4. 考虑正四面体的旋转群 A_4。

(1) A_4 同构于以下元素构成的 4 元置换群：

$$\{(1\,2\,3\,4),(1\,3\,4\,2),(1\,4\,2\,3),(3\,2\,4\,1),\\ (4\,2\,1\,3),(2\,4\,3\,1),(4\,1\,3\,2),(2\,3\,1\,4),\\ (3\,1\,2\,4),(2\,1\,4\,3),(3\,4\,1\,2),(4\,3\,2\,1)\}$$

具体证明见第四章练习题 6。

(2) 以上的群由 4 元置换构成，故而是 S_4 的子群。

(3) J_4 的元素（除了幺元）都是 2 阶的，因此需要在 A_4 中找 2 阶的元素。A_4 只有 3 个 2 阶元素，所以只能是：

$$G=\{(1\,2\,3\,4),(2\,1\,4\,3),(3\,4\,1\,2),(4\,3\,2\,1)\}.$$

其中 $(1\,2\,3\,4)$ 是幺元，另外三个都是 2 阶元素，且

$$(2\,1\,4\,3)=(3\,4\,1\,2)(4\,3\,2\,1).$$

不难验证 G 是群。列出其乘法表可知其与 J_4 同构。

(4) C_6 有阶为 6 的元素，即需要重复 6 次才变成恒等变换。A_4 中没有这样的元素。

(5) D_3 有 3 个 2 阶元素。反设 A_4 有子群 H 同构于 D_3，那么 H 也会有 3 个 2 元素。由上一题知必然是 $(2\,1\,4\,3),(3\,4\,1\,2),(4\,3\,2\,1)$。它们和幺元一起构成子群，而且是 H 的子集。这说明 H 有 4 元子集 G，违反群势定理，矛盾！

5. 生成的子群为：

(1) $\mathbb{Z}_{12}$

(2) $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\}$

(3) $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10},\overline{12},\overline{14},\overline{16}\}$

(4) $\{\overline{0},\overline{6},\overline{12},\overline{18},\overline{24},\overline{30}\}$

(4) $4\mathbb{Z}$

(5) $6\mathbb{Z}$

(6) $3\mathbb{Z}$

(7) $\{e,r^2,s,r^2s\}$

6. **证明**：这个群就是映轮群 D_n。考虑 D_n 中两个翻转变换 a,b，其对称轴夹角为 $\frac{\pi}{n}$。如果这样的变换存在，那么 ab 就是 $\frac{2\pi}{n}$ 的旋转变换，因此它和 a（或 b）就生成整个映轮群 D_n。

下面说明 a, b 总存在。我们知道正多边形的对称轴要么经过顶点，要么经过边的中点。考虑某条经过顶点的对称轴，它旁边的边的中点也在某条对称轴上。这两条对称轴夹角就是 $\frac{\pi}{n}$。

7. 考虑 D_4 的生成元。它可由一个旋转 r 和一个翻转 s 生成。在 S_4 中，我们可以找到两个很像的置换：4 元轮换 $\tau = (2\,3\,4\,1)$ 和对换 $\sigma = (2\,1\,3\,4)$。这两个置换可以生成一个 8 元群，而且其结构和 D_4 相同。我们可以通过计算 $\tau\sigma, \tau^2\sigma, \tau^3\sigma, \tau^4\sigma$ 以及 $\sigma\tau$ 来验证。前者可以验证生成路径图。后者可以得到关系：

$$\tau\sigma = \sigma\tau^{-1}.$$

据此可以计算乘法表。它们的生成路径图和乘法表都一样，因此同构。

8. 子群的往集为：

(1) $\{6n + k \,|\, n \in \mathbb{Z}\}$，其中 $k = 1, 2, 3, 4, 5$。左右往集相等。

(2) $\{6n + k \,|\, n \in \mathbb{Z}\}$，其中 $k = 2, 4$。左右往集相等。

(3) $\{\overline{1}, \overline{4}, \overline{7}, \overline{10}\}$ 和 $\{\overline{2}, \overline{5}, \overline{8}, \overline{11}\}$。左右往集相等。

(4) **解答**：
不难推出 r 是 4 阶旋转，s 是翻转。$\langle r^2 \rangle = \{e, r^2\}$，记为 H。H 的左往集为 $rH = \{r, r^3\}$，$sH = \{s, r^2 s\}$，$rsH = \{rs, rsr^2\} = \{rs, r^3 s\}$。$H$ 的右往集为 $Hr = \{r, r^3\}$，$Hs = \{s, sr^2\} = \{s, r^2 s\}$，$Hrs = \{rs, r^3 s\}$。左右往集相等。原因是 $sr^2 = r^2 s$。这让 r^2 和 $s, rs, r^2 s, r^3 s$ 都交换，从而和所有群元素交换。

9. 设群 G 有子群 H。$a, b \in G$，使得 $aH = bH$。以下说法是否正确?

解答：

(1) $Ha = Hb$ 不正确。考虑 $\mathsf{D}_3 = \langle r, s \rangle$ 的子群 $H = \{e, s\}$。其中 r 为旋转，s 为翻转。$rH = \{r, rs\} = \{rs, rss\} = rsH$。但 $Hr = \{r, sr\} = \{r, r^2 s\}$，$Hrs = \{rs, srs\} = \{rs, r^2\}$。$Hr \neq Hrs$。

(2) $Ha^{-1} = Hb^{-1}$ 正确。$aH = bH$，说明有 $h \in H$，使得 $a = bh$，于是 $b^{-1} = ha^{-1} \in Ha^{-1}$。这说明 $Hb^{-1} \subseteq Ha^{-1}$。同理可证 $Ha^{-1} \subseteq Hb^{-1}$。于是 $Ha^{-1} = Hb^{-1}$。

(3) $a^2 H = b^2 H$ 不正确。用第一问的例子，$rH = rsH$，但 $(rs)^2 = e$，于是 $(rs)^2 H =$

$eH = \{e, s\}$。而 $r^2H = \{r^2, r^2s\}$。$r^2H \neq (rs)^2H$。

10. **证明**:

设群 G 满足 $|G| = p$，p 是素数。考虑 G 非幺元素 x 的阶。依照群势定理，它的阶整除 p，于是要么是 1，要么是 p。但 1 阶元素只能是幺元，所以只能是 p。于是 $G = \langle x \rangle$ 是循环群。

11. **解答**:

(1) $\forall x, y \in H_a$，$y(a) = a$，说明 $y^{-1}(a) = a$。因此

$$\left(xy^{-1}\right)(a) = x\left(y^{-1}(a)\right) = x(a) = a.$$

这说明 $xy^{-1} \in H_a$。于是按照子群的判定方法，H_a 是 S_X 的子群。

(2) 考虑 X 到自身的恒等变换 e。$e(a) = a \neq b$，于是 $e \notin H_a^b$。这说明 H_a^b 不是 S_X 的子群。

(3) 取一个把 a 映射到 b 的置换 $\sigma_0 \in \mathsf{S}_X$。按 S_X 的定义，这样的置换必然存在。于是，$\forall h \in H_a$，$(\sigma_0 h)(a) = \sigma_0(h(a)) = \sigma_0(a) = b$，即 $\sigma_0 h \in H_a^b$，因此 $\sigma_0 H \subseteq H_a^b$。另一方面，$\forall g \in H_a^b$，$g(a) = b$，而 $\sigma_0^{-1}(b) = a$。于是

$$\left(\sigma_0^{-1} g\right)(a) = \sigma_0^{-1}\left(g\left(a\right)\right) = \sigma_0^{-1}(b) = a.$$

即 $\sigma_0^{-1} g \in H_a$，于是 $g \in \sigma_0 H_a$。这说明 $H_a^b \subseteq \sigma_0 H_a$。

综上有 $H_a^b = \sigma_0 H_a$。

1.6 第六章参考解答

1. **解答**:

(1) 这个表达式是说 $12\mathbb{Z}$ 是 $\mathbb{Z}$ 的往合子群，$2+12\mathbb{Z}$ 是其商群的元素。

(2) 这个表达式是说 $16\mathbb{Z}$ 是 $2\mathbb{Z}$ 的往合子群，$10+16\mathbb{Z}$ 是其商群的元素。

(3) 这个表达式是说 $6\mathbb{Z}\times12\mathbb{Z}$ 是 $\mathbb{Z}\times\mathbb{Z}$ 的往合子群，$(5,9)+6\mathbb{Z}\times12\mathbb{Z}$ 是其商群的元素。

(4) 这个表达式是说 $12\mathbb{Z}\times6\mathbb{Z}$ 是 $4\mathbb{Z}\times2\mathbb{Z}$ 的往合子群，$(4,4)+12\mathbb{Z}\times6\mathbb{Z}$ 是其商群元素。

(5) 这个表达式是说 $\langle\overline{3}\rangle$ 是 $\mathbb{Z}_{12}$ 的往合子群，$\overline{2}+\langle\overline{3}\rangle$ 是其商群的元素。

(6) 这个表达式是说 $\langle\overline{4}\rangle$ 是 $\mathbb{Z}_{12}$ 的往合子群，$\overline{5}+\langle\overline{4}\rangle$ 是其商群的元素。

(7) 这个表达式是说 $\langle(\overline{0},\overline{2})\rangle$ 是 $\mathbb{Z}_3\times\mathbb{Z}_4$ 的往合子群，$(\overline{2},\overline{1})+\langle(\overline{0},\overline{2})\rangle$ 是其商群的元素。

(8) 这个表达式是说 $\langle(\overline{2},\overline{0})\rangle$ 是 $\mathbb{Z}_8\times\mathbb{Z}_4$ 的往合子群，$(\overline{1},\overline{3})+\langle(\overline{2},\overline{0})\rangle$ 是其商群的元素。

2. **解答**:

(1) 小明的问题在于没有理解商群的元素到底是什么，长什么样子，把商群当作普通的群。商群的性质与其形式密切相关。当小明写出 $a,b\in G\!\!\diagup_{H}$，就说明他不知道自己在写什么。他应该写 $aH,bH\in G\!\!\diagup_{H}$。

(2) 任取 $aH,bH\in G\!\!\diagup_{H}$（由于左右往集相等，所以不妨写左往集。用右往集结果不变)。按照商群的运算规则：$(aH)(bH)=(ab)H$。由于 G 是交换群，$ab=ba$，所以 $(aH)(bH)=(ab)H=(ba)H=(bH)(aH)$. 这就说明商群也是交换群。

3. **解答**:

(1) 子怡的问题首先在于没有理解往合的概念，把往合的定义和交换的定义混淆了。往合子群的左往集总等于右往集，和群元素交换的定义是不一样的。左往集等于右往集，说明两者是同一个对象，而不是交换关系。而交换性则是两个不同的往集之间的运算的性质。实际上，如果子群的左往集不等于右往集 $aH\neq Ha$，那么两个左往集 aH,bH 之间就无法定义群运算了，根本谈不上交换不交换。她混淆了结构兼容的问题和运算性质的问题。

另外，子怡认为非交换群无法分解为两个交换群，混淆了群的架积和商群分解。通过往合子群分解为商群，并不代表往合子群和商群的架积是原来的群。实际上，非交换群可以同时拥有交换的往合子群和商群，比如 D_3 就通过同构于交换群 C_3 的往合子群得到同构于 C_2 的商群，后两个群都是交换群。

(2) S_4 中同构于 C_3 的子群就是 3 阶元素生成的子群。S_4 有 8 个 3 阶元素，即 3 元轮换。它们构成 4 个三元群，都同构于 C_3。但它们都不往合。例如，取子群 $H = \{(1\,2\,3\,4), (2\,3\,1\,4), (3\,1\,2\,4)\}$，用 $a = (4\,2\,3\,1)$ 左乘它，得到 $aH = \{(4\,2\,3\,1), (2\,3\,4\,1), (3\,4\,2\,1)\}$，右乘则得到 $Ha = \{(4\,2\,3\,1), (4\,3\,1\,2), (4\,1\,2\,3)\}$。于是 $aH \neq Ha$。其他群可类似验证。

4. **解答**:

(1) 设题目中给出的 12 个置换构成的群为 H（A_4 同构于 H），考察它的往集。H 左乘对换 $\tau = (2\,1\,3\,4)$，得到以下 12 个元素:

$$\begin{aligned}\tau H &= \{\tau\sigma \,|\, \sigma \in H\} \\ &= \{(2\,1\,3\,4), (2\,3\,4\,1), (2\,4\,1\,3), (3\,1\,4\,2), \\ &\quad (4\,1\,2\,3), (1\,4\,3\,2), (4\,2\,3\,1), (1\,3\,2\,4), \\ &\quad (3\,2\,1\,4), (1\,2\,4\,3), (3\,4\,2\,1), (4\,3\,1\,2)\}\end{aligned}$$

窍门是把其中的 $1, 2$ 对换即可。
我们知道左往集 τH 和 H 不相交且等势，构成 S_4 的分划。同理，右往集 $H\tau$ 也和 H 不相交且等势，构成 S_4 的分划。这说明 $\tau H = H\tau$，因此 $H \trianglelefteq \mathsf{S}_4$。

(2) 如果有限群 G 的子群 H 拥有 G 的一半元素，取另一半元素中任一个: a。那么根据往集的性质，aH 和 Ha 都是另一半元素构成的往集，于是 $aH = Ha$。这说明 $H \trianglelefteq G$。

(3) 反设 A_4 有 6 元子群 H，则 H 除自身外只有一个往集，因此左往集等于右往集。这说明 H 是往合子群，可以定义商群 Q。Q 是二元群，因此同构于 C_2。H 则是从 A_4 到 C_2 的同态 φ 的核。
考察 A_4 中的 3 元轮换，它们都是 3 阶元素。因此任意 3 元轮换 x 都有 $x^3 = e_1 \in \mathsf{A}_4$。$x$ 经 φ 映射变成 $\varphi(x) \in \mathsf{C}_2$，于是 $e_2 = \varphi(e_1) = \varphi(x^3) = \varphi(x)^3$，其中 e_2 是 C_2 的幺元。然而 C_2 中没有 3 阶元素。$\varphi(x)^3 = e_2$，说明 $\varphi(x) = e_2$。因此 A_4 中所有 3 元轮换都映射到 e_2，即都在同态核 H 中。但 A_4 中有 8 个 3 元轮换，H

只有 6 个元素，矛盾!

(4) 按定义，$\mathsf{H}_0 = \{\sigma \in \mathsf{S}_{\mathbb{N}} \,|\, \sigma(0) = 0\}$。如果 $a \in \mathsf{H}_0$，那么 $a(0) = 0$，于是 $a^{-1}(0) = 0$。因此，$\forall a, b \in \mathsf{H}_0$，$(ab^{-1})(0) = a(b^{-1}(0)) = a(0) = 0$。这说明 $ab^{-1} \in \mathsf{H}_0$。因此 $\mathsf{H}_0 \lhd \mathsf{S}_{\mathbb{N}}$。

(5) 考虑 $\mathbb{N}$ 上的置换 σ，它只交换 1 和 2。$\sigma(0) = 0$，因此 $\sigma \in \mathsf{H}_0$。计算 $\sigma\tau \in \mathsf{H}_0\tau$：$(\sigma\tau)(0) = 2$，$(\sigma\tau)(1) = 0$，$(\sigma\tau)(2) = 1$，其他情况下 $(\sigma\tau)(n) = n$。考虑左往集 $\tau\mathsf{H}_0$。$\forall \tau h \in \tau\mathsf{H}_0$，总有 $(\tau h)(0) = \tau(h(0)) = \tau(0) = 1$。所以 $\sigma\tau \notin \tau\mathsf{H}_0$。这说明 $\tau\mathsf{H}_0 \neq \mathsf{H}_0\tau$。左往集不等于右往集，因此 H_0 不是往合子群。（**注意**：通过证明 $\sigma\tau \neq \tau\sigma$ 来证明 H_0 不是往合子群是不行的。）

(6) $\forall \sigma \in \mathsf{H}_0$，$(\tau_n\sigma)(0) = \tau_n(\sigma(0)) = \tau(0) = n$，所以 $\tau_n\mathsf{H}_0 \subseteq \mathsf{H}_n$。反之，$\forall \sigma \in \mathsf{H}_n$，$\left(\tau_n^{-1}\sigma\right)(0) = \tau_n^{-1}\left(\sigma(0)\right) = \tau_n^{-1}(n) = 0$。所以 $\tau_n^{-1}\sigma \in \mathsf{H}_0$，即 $\sigma \in \tau_n\mathsf{H}_0$。于是 $\mathsf{H}_n \subseteq \tau_n\mathsf{H}_0$。综合有 $\mathsf{H}_n = \tau_n\mathsf{H}_0$。这说明 $|\mathsf{H}_0| = |\tau_n\mathsf{H}_0| = |\mathsf{H}_n|$。

(7) 按定义显然 $\mathsf{H}_0^{(i)}$ 两两不相交。由于 H_0 中元素不可能把 1 映射到 0，所以只能映射到正整数，于是必然恰好属于一个 $\mathsf{H}_0^{(i)}$（只要 $\sigma(1) = i$，σ 就属于 $\mathsf{H}_0^{(i)}$）。因此 $\{\mathsf{H}_0^{(i)}, \,|\, i \in \mathbb{Z}^+\}$ 构成 H_0 的分划。另一方面，仿照前一问的方法可证明 $\mathsf{H}_0^{(i)} = \rho_i\mathsf{H}_0^{(1)}$，其中 ρ_i 是只交换 1 和 i 的对换。因此 $|\mathsf{H}_0^{(i)}| = |\mathsf{H}_0^{(1)}|$。

(8) $\forall \sigma \in \mathsf{H}_0^{(1)}$，双射 σ 固定 0 和 1，因此只变动大于 1 的正整数。考虑 $f : x \mapsto \sigma(x+1) - 1$，$\forall x \in \mathbb{Z}^+$，$x + 1 \geqslant 2$，$f(x) = \sigma(x+1) - 1 \geqslant 1$。根据 σ 的性质，它是正整数集上的双射，因此可以补充定义 $f(0) = 0$。这样就定义了一个属于 H_0 的置换 f。于是我们构建了从 $\mathsf{H}_0^{(1)}$ 到 H_0 的映射：

$$\Phi : \sigma \mapsto \left(x \mapsto \begin{cases} \sigma(x+1) - 1 & x \in \mathbb{Z}^+ \\ 0 & x = 0 \end{cases} \right)$$

反之，给定 $\sigma \in \mathsf{H}_0$，定义 $g : x \mapsto \sigma(x-1) + 1$。正整数 $x > 1$ 时，$x - 1 > 0$，于是 $g(x) = \sigma(x-1) + 1 > 1$。根据 σ 的性质，它在大于 1 的正整数集上是双射。补充定义 $g(0) = 0$，$g(1) = 1$。这样就构造出属于 $\mathsf{H}_0^{(1)}$ 的置换 g。我们把这个从 H_0 到 $\mathsf{H}_0^{(1)}$ 的映射记作 Ψ：

$$\Psi : \sigma \mapsto \left(x \mapsto \begin{cases} \sigma(x-1) + 1 & x \in \mathbb{Z}^+,\ x > 1 \\ 1 & x = 1 \\ 0 & x = 0 \end{cases} \right)$$

最后，计算 $\Phi(\Psi(\sigma))$。首先按 Φ 的定义，$\Phi(\Psi(\sigma))(0)=0$；其次，

$$\forall\, x\in\mathbb{Z}^+,\ \ \Phi(\Psi(\sigma))(x)=\Psi(\sigma)(x+1)-1=\sigma(x+1-1)+1-1=\sigma(x).$$

因此 $\Phi(\Psi(\sigma))=\sigma$。同理可验证 $\Psi(\Phi(\sigma))=\sigma$。这说明 Φ 和 Ψ 互为逆映射，即 Φ 是可逆的双射。我们建立了 H_0 和 $\mathsf{H}_0^{(1)}$ 之间的双射。

(9) 通过 τ_n 可建立 H_0 到 H_n 的双射 $\phi_n: x\mapsto\tau_n x$。注意到 $\{\mathsf{H}_n|n\in\mathbb{N}\}$ 构成 $\mathsf{S}_\mathbb{N}$ 的分划，因此 H_0 的补集就是 H_n（$n\in\mathbb{Z}^+$）的不交并集 K。只要证明 $\mathsf{H}_0^{(n)}$ 到 H_n 之间有双射 ψ_n。那么把所有 ψ_n 拼接起来，就构成 H_0 到 K 的双射。
下面构建双射 ψ_n。前一问证明了 H_0 和 $\mathsf{H}_0^{(1)}$ 之间有双射，记为 $\Phi_0^{(1)}$。考虑只交换 1 和 n 的置换 τ_1^n，$\sigma\mapsto\tau_1^n\circ\sigma$ 是 $\mathsf{H}_0^{(1)}$ 到 $\mathsf{H}_0^{(n)}$ 的双射。于是对任意正整数 n，H_0 和 $\mathsf{H}_0^{(n)}$ 之间总有双射，记为 $\Phi_0^{(n)}$。而 H_0 和 H_n 之间也有双射 ϕ_n，因此 H_n 和 $\mathsf{H}_0^{(n)}$ 就有双射，这就是我们要找的 ψ_n。
H_0 和它在 $\mathsf{S}_\mathbb{N}$ 的补集 K 之间有双射。按集合的性质，两者等势。我们可以说“K 和 H_0 的往集一样大”，但这不说明“H_0 占了 $\mathsf{S}_\mathbb{N}$ 的一半元素”或“H_0 是 $\mathsf{S}_\mathbb{N}$ 的往合子群”。在有限群上成立的结论，对无限群则不成立了。

5. **解答**:

(1) 可以验证，e, r^2 都与 D_4 中所有元素交换，因此，$\forall a\in\mathsf{D}_4$，都有 $a\langle r^2\rangle=\langle r^2\rangle a$。于是 $H\lhd\mathsf{D}_4$。

(2) D_4 的其他二元子群 K 都是翻转变换生成的子群。可以验证 $rK\neq Kr$。

(3) $\langle r^2\rangle$ 的所有往集为:

$$\begin{aligned}\langle r^2\rangle &= r^2\langle r^2\rangle,\\ r\langle r^2\rangle &= r^3\langle r^2\rangle,\\ s\langle r^2\rangle &= sr^2\langle r^2\rangle = r^2s\langle r^2\rangle,\\ rs\langle r^2\rangle &= sr^3\langle r^2\rangle = sr\langle r^2\rangle = r^3s\langle r^2\rangle.\end{aligned}$$

其运算律和 D_4 不同。首先是:

$$\left(r\langle r^2\rangle\right)\left(r\langle r^2\rangle\right)=\left(r^2\right)\langle r^2\rangle=\langle r^2\rangle,$$

即 r 对应的往集是 2 阶元素。其次是:

$$\left(r\langle r^2\rangle\right)\left(s\langle r^2\rangle\right)=(rs)\langle r^2\rangle=(sr)\langle r^2\rangle=\left(s\langle r^2\rangle\right)\left(r\langle r^2\rangle\right),$$

r, s 对应的往集交换。最后：

$$\begin{aligned}
\left(r\langle r^2\rangle\right)\left(rs\langle r^2\rangle\right) &= \left(r^2 s\right)\langle r^2\rangle = s\langle r^2\rangle,\\
\left(rs\langle r^2\rangle\right)\left(r\langle r^2\rangle\right) &= (rsr)\langle r^2\rangle = s\langle r^2\rangle,\\
\left(s\langle r^2\rangle\right)\left(rs\langle r^2\rangle\right) &= (srs)\langle r^2\rangle = \left(r^3\right)\langle r^2\rangle = r\langle r^2\rangle,\\
\left(rs\langle r^2\rangle\right)\left(s\langle r^2\rangle\right) &= (rss)\langle r^2\rangle = r\langle r^2\rangle,
\end{aligned}$$

r, s 对应的往集，分别和 rs 对应的往集交换。

综上可知，$\langle r^2\rangle, r\langle r^2\rangle, s\langle r^2\rangle, rs\langle r^2\rangle$ 是含有三个 2 阶元素的四元群，同构于 $\mathsf{C}_2\times\mathsf{C}_2$。

(4) $\langle r^2, s\rangle = \{e, s, r^2, r^2 s\}$。这个群同构于矩群。

(5) M_1 的势是 D_4 的一半。因此它的左往集等于右往集，从而往合。D_4/M_1 有两个元素，因此同构于 C_2。

(6) 另外的两个往合真子群都是四元群，分别记为 $M_2 = \langle r\rangle$，$M_3 = \langle r^2, rs\rangle$。前者同构于 C_4，后者同构于矩群。对应的商群都是二元群，同构于 C_2。

(7) $\langle r^2\rangle$ 对应的商群同构于矩群。矩群有三个不同的二元子群。而 $\langle r^2\rangle$ 可继续添加元素生成三个四元往合子群。我们可以画出表示 D_4 往合子群与对应商群各自的对应关系图。把有直接包含关系的群连线，用箭头从子群指向母群。从包含（子群）关系来看，往合子群网格和商群网格有相同的结构（见下页图）。

不过，除了包含关系，我们并不能推出更多的东西。比如，第二“层”的商群都是 C_2，但第二“层”的 M_1, M_2, M_3 并不是同一个构造，$M_2 = \langle r\rangle$ 和其他两个群不同构。

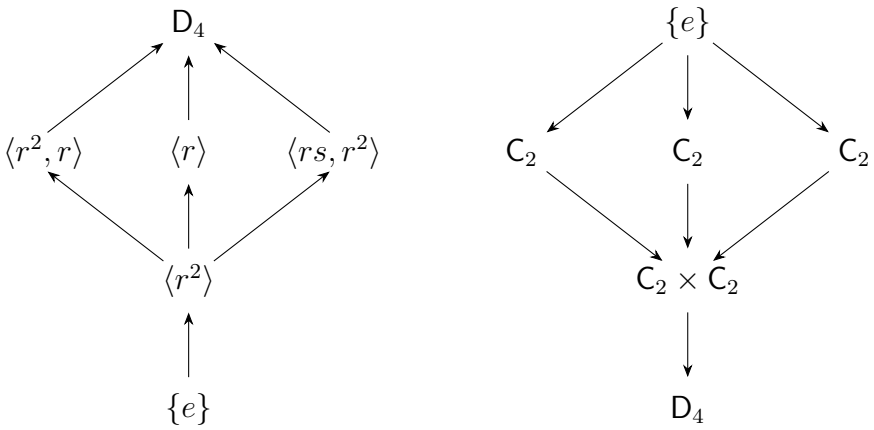


图 一.2: D_4 的各个往合子群以及对应商群之间的关系网格

1.7 第七章参考解答

1. **解答**:

(1) **不是**。
理由: 不封闭（如 $\gamma(-1,-1) = -2 \notin X$）；与幺元不相容（群的幺元是 1，但 $\gamma(1,0) = 1+0 = 1 \neq 0$）。

(2) **是**。
理由: 结果仍在 X 中(封闭); 幺元 1 作用为 $1{\cdot}x = x$; 与结合律相容 $a(bx) = (ab)x$。

(3) **不是**。
理由: 虽然封闭（整数加平方仍为整数），且与幺元相容（$\gamma(0,x) = x + 0^2 = x$），但与结合律不相容。$\gamma(a,\gamma(b,x)) = \gamma(a, x+b^2) = x + b^2 + a^2$；而 $\gamma(a+b,x) = x + (a+b)^2 = x + a^2 + 2ab + b^2$。两者不相等。

(4) **不是**。
理由: $\gamma(a,\gamma(b,x)) = (xb)a = x(ba) \neq x(ab) = \gamma(ab,x)$。与结合律不相容。**注意**: 这是因为本书只定义了**左观群** ($G \times X \to X$)。群论中还会定义**右观群**: $X \times G \to X$。对应的条件是满足幺元相容性以及 $\gamma(x,ab) = \gamma(x,\gamma(x,b))$。在右观群时本题定义的 γ 就是观群法了，称为**右乘观**。左观群和右观群是观群的两种定义，并无对错。本书采取较为常用的左观群。两种观群定义是对称的，左观群得到的结论都能对称地写成右观群的相应结论，只是写法不同。

(5) **是**。
理由: 可以验证它与幺元、结合律都相容: $\gamma(e,x) = xe^{-1} = xe = x$。$\gamma(a,\gamma(b,x)) = (xb^{-1})\,a^{-1} = x(b^{-1}a^{-1}) = x(ab)^{-1} = \gamma(ab,x)$。**注意**: 这是在左观群时模拟右乘观的方法。由于 a 遍历群时 a^{-1} 也遍历群，所以我们可以讨论以右乘方式观群的性质。

(6) **不是**。
理由: 群的幺元是 0，但 $\gamma(0,x) = 0 \cdot x = 0 \neq x$，不相容。此外，群的运算是模 5 加法，而映射依赖普通整数乘法，导致不容结合律: $\gamma(a,\gamma(b,x)) = (ab)x$，但 $\gamma(a+b,x) = (a+b)x$。

(7) **不是**。

理由：不满足封闭性。D_3 包含旋转 120° 的变换，将正方形顶点旋转 120° 后，顶点将落在非顶点位置（不在集合 X 中）。

(8) **是**。

理由：D_4 的变换（旋转 90° 倍数及翻转）作用于整数格点 (m,n)，结果总在 $(1\pm m, 1\pm n)$、$(1\pm n, 1\pm m)$、$(\pm m, \pm n)$ 或 $(\pm n, \pm m)$ 之中。结果必为整数格点，故封闭。变换的复合天然与幺元、结合律相容。

2. **解答**：

按轨定定理，轨迹长度是 35 的因数，但按条件大于 1 且不超过 19，因此要么是 5，要么是 7。这些轨迹构成 X 的分划。设有 m 个长度为 5 的轨迹，n 个长度为 7 的轨迹，则有以下的整数不定方程：

$$5m + 7n = 19.$$

m, n 都是非负整数。于是 $n < 3$。用 $n = 0, 1, 2$ 测试，得到 $n = 2, m = 1$。因此一共有 3 个轨道，1 个长度为 5，2 个长度为 7。

3. **解答**：

记 H 为 $g(x)$ 的定子群。按定义，$G_x = \{a \in G \,|\, a(x) = x\}$。于是 $\forall a \in G_x$，$(gag^{-1})(g(x)) = g(a(g^{-1}(g(x)))) = g(a(x)) = g(x)$。这说明 gag^{-1} 是 $g(x)$ 的定子。这说明 $gG_xg^{-1} \subseteq H$。另一方面，如果 $a \in G$ 使得 $a(g(x)) = g(x)$，那么 $(g^{-1}ag)(x) = x$，即 $g^{-1}ag \in G_x$，于是 $a \in gG_xg^{-1}$。这说明 $H \subseteq gG_xg^{-1}$。综上，$H = gG_xg^{-1}$。

4. **解答**：

往复观群 G 于自身，则 $x \in G$ 的定子群为其交心群。按照轨定定理，x 的交心群势乘以 x 的轨道长度等于群势 p^n。因此，x 的轨道长度是 $|G|$ 的因数，于是总是 p 的乘方。要么是 1，要么是 p 的倍数。按定义，x 的轨道长度为 1，当且仅当其与群里所有元素交换，即 x 为 G 的心元。按照 G 显于 G 的轨道将 G 划分，得到：

$$|G| = \sum_{\mathcal{O}_G(x) \in \mathcal{O}_G(G)} |\mathcal{O}_G(x)| = \sum_{x \in G^{\text{心}}} |\mathcal{O}_G(x)| + \sum_{x \notin G^{\text{心}}} |\mathcal{O}_G(x)|.$$

我们将轨道 $\mathcal{O}_G(x)$ 按长度为 1 和大于 1 分成两类。后一类都是 p 的倍数。而前一类都是 1，加起来就是 $G^{\text{心}}$ 的势。也就是说：

$$|G| = \sum_{x \in G^{\text{心}}} |\mathcal{O}_G(x)| + \sum_{x \notin G^{\text{心}}} |\mathcal{O}_G(x)| = \sum_{x \in G^{\text{心}}} 1 + \sum_{x \notin G^{\text{心}}} p\text{的倍数} = |G^{\text{心}}| + p\text{的倍数}.$$

这说明：

$$|G| \equiv |G^{\text{心}}| \ \ (\text{模 } p)\,.$$

但 $|G| = p^n$ 也是 p 的倍数，所以

$$|G^{\text{心}}| \equiv |G| \equiv 0 \ \ (\text{模 } p)\,.$$

即 G 的中心的元素个数也是 p 的倍数，不可能只有幺元 e。

5. **解答**：

(1) 根据往集定理，H 有 p 个左往集。

(2) 记 $X = \{aH \,|\, a \in G\}$，它有 p 个元素。考虑映射

$$\begin{aligned} \gamma :\ (G,\, X) &\longrightarrow X \\ (x,\, A) &\longmapsto xA \end{aligned}$$

下面逐个验证它满足显相映射的两个条件。首先，$\forall A = aH \in X$，其中 $c \in G$，$\gamma(e, A) = eaH = aH = A$。其次 $\forall x, y \in G$，$\forall A = aH \in X$，$\gamma(x, \gamma(y, A)) = \gamma(x, yaH) = xyaH = (xy)aH = \gamma(xy, A)$，于是兼容结合律。

(3) $\varphi(x) = \gamma_x = A \mapsto xA$。$\gamma_x$ 是 S_X 中元素（X 上的置换）。S_X 的幺元是恒等变换，即 $aH \mapsto aH$，所以 φ 的核 N 里的元素 x 对应的是令 $\forall a \in G,\ x(aH) = aH$ 都成立的 γ_x。即 $\gamma_x = \varphi(x)$ 要使得 $\forall a \in G,\ x(aH) = aH$。令 $a = e$，就得到 $xH = H$。于是至少要有 $x \in H$。因此 $N \subseteq H$。

(4) 按照群同态基本定理，同态 φ 满足：$|N| \times |\varphi(G)| = |G|$。因此 $|\varphi(G)|$ 是 $|G|$ 的因数。

另一方面，$\varphi(G)$ 是 G 通过群同态在 S_X 中的像，因此是 S_X 的子群。按照群势定理，它的群势整除 S_X 的群势。X 有 p 个元素，所以 S_X 为 p 元置换的全置换群，群势为 $p!$。因而 $|\varphi(G)|$ 是 $p!$ 的因数。

$p!$ 的素因数最大是 p。作为 $p!$ 的因数，$|\varphi(G)|$ 的素因数要么是 p，要么比 p 更小。但 $|\varphi(G)|$ 的素因数也是 $|G|$ 的素因数，而 p 按定义是 $|G|$ 最小的素因数。所以，$|\varphi(G)|$ 不能有比 p 更小的素因数，$|\varphi(G)|$ 只能是 p 的乘方：$p, p^2, p^3, \cdots$

但 p 作为素数，只在 $p!$ 中出现一次（比 p 小的正整数不会有 p 作为因数），所以 $p^2 \nmid p!$。这说明 $|\varphi(G)| = p$。于是

$$|N| = \frac{|G|}{|\varphi(G)|} = \frac{n}{p} = |H|.$$

这与 $N \subseteq H$ 一起，可推出 $N = H$。

N 作为群同态 φ 的核，是 G 的往合子群，所以 $H = N$ 就是 G 的往合子群。

正方体和正四面体的旋转群

1. **解答**：两组顶点的坐标分别为：

$$T^+ = \{(1,1,1),\ (-1,-1,1),\ (-1,1,-1),\ (1,-1,-1)\},$$
$$T^- = \{(1,1,-1),\ (1,-1,1),\ (-1,1,1),\ (-1,-1,-1)\}.$$

这两组顶点构成正方体顶点的分划。每组内 4 个顶点之间两两距离都是 $2\sqrt{2}$。正方体的同一条顶心对角线的两个端点（下称对顶点）必然分属两组（坐标互为相反数）。同一条棱的两端点必然分属两组。

2. **解答**：以上分出的 T^+, T^- 两个集合，每个集合中的顶点恰好是一个正四面体的顶点。由于正方体所有顶点到原点等距，可知两个正四面体的中心都是坐标原点。

3. **解答**：通过面心的 90° 旋转有三类，分别以 x, y, z 轴为旋转轴。不妨设旋转轴为 z 轴，该旋转分别旋转 $z = 1$ 和 $z = -1$ 两个面上的顶点。在平面上该旋转体现为 90° 旋转，因此把 x, y 坐标转到下一个象限。于是乘积 xy 变号而 z 不变。这说明 T^+ 中所有点都会变为 T^- 中点，反之亦然。

4. **解答**：通过体心的旋转以顶心对角线为旋转轴。它固定一个顶点与其对顶点，而置换其相邻顶点的位置。观察可知：任何顶点相邻三顶点都属于 T^+, T^- 中同一个子集，因此经过置换仍然在其中。这说明该旋转把 T^+, T^- 变为自身。

5. **解答**：通过对棱中线的 180° 旋转把相关两条棱中每条棱的顶点对调，而把其他棱上的所有顶点都变为其对顶点，因此所有顶点都改变归属 T^+, T^- 的情况。

6. **解答**：前三问中的旋转都把 T^+, T^- 整体变换，即同属一个子集的顶点变换后要么都属于原子集，要么都属于另一个子集。这些旋转变换能生成正方体的任何旋转变换（具体见第四章习题 5）。因此，$\forall \tau \in \mathsf{T}_6$，作为它们的复合，也把 T^+, T^- 整体变换。用 ϕ 和 τ 来描述，就是：$\phi \circ \tau$ 在 T^+, T^- 上各自都是常数。

7. **解答**：由上一问可知 $\sigma(t) \in \{T^+, T^-\} = \mathsf{T}$。由于 γ 用旋转作为映射来自然定义，只要契义，就自然满足显相映射的条件。而前面可以看到把 T^+, T^- 变为对方的旋转变换，所以它们的轨迹都是 T，即群显通相。

8. **解答**：$H = \{\sigma \in \mathsf{T}_6 \,|\, \sigma(T^+) = T^+\}$，根据轨定定理，$|H|$ 乘以 T^+ 的轨迹长度就是

$|\mathsf{T}_6| = 24$。T^+ 的轨迹长度为 2，所以 $|H| = 12$。由于 H 的势是 $|\mathsf{T}_6|$ 的一半，它的另一个左往集等于另一个右往集，因此左右往集相等，为往合子群。

9. **解答**：如果 $\sigma(T^+) = T^+$，那么 $\sigma(T^-) = T^-$，即 γ_σ 为恒等变换。否则不然。因此群同态 $\sigma \mapsto \gamma_\sigma$ 的核就是 H，它的像是 T 上的置换群 S_T，同构于 C_2。

10. **解答**：根据群同态基本定理，由于 H 是 $\sigma \mapsto \gamma_\sigma$ 的核，H 除 T_6 的商群就同构于它的像：置换群 S_T，即同构于 C_2。

11. **解答**：我们用顶心对角线的置换来描述正方体的旋转，从而建立 T_6 与 S_4 中的置换的对应。按定义 H 保持 T^+ 中的顶点，包括通过面心的 180° 旋转（3 个）、通过体心的 120° 旋转（8 个）以及恒等变换。它们分别对应 S_4 中双对换、3 元轮换和恒等变换。

12. **解答**：考虑 H 中的旋转如何具体变换正四面体 T^+ 中的顶点：通过正方体体心的 8 个 120° 旋转对应绕过正四面体顶点和中心的轴线的旋转；通过正方体面心的 3 个 180° 旋转则对应绕正四面体对棱中线的旋转（注意对 T^- 也是如此）。因此 H 包含于正四面体的旋转群 A_4。考虑到两者等势，$H = \mathsf{A}_4$。

13. **解答**：S_4 中的对换对应绕对棱中线的 180° 旋转：它恰好调换相关两棱所在截面的顶心对角线，而保持另外两条不变。它把 T^+ 变为 T^-，因此不属于 $H = \mathsf{A}_4$。

14. **解答**：经过尝试可以发现：取某个顶点 V 相邻的三条棱及其对棱，绕这三对棱的中线分别旋转 180°，效果恰好就是绕通过正方体面心的轴线的 90° 旋转。用置换来表示，可以举例写为：$(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2)$，其中“1”就是顶点 V 及其对顶点代表的顶心对角线。

15. **解答**：根据第四章的习题，我们知道绕面心的旋转能生成整个 T_6，即对应的置换能生成整个 S_4。而这些置换本身又能通过对换复合生成，所以对换可以生成整个 S_4。

16. **解答**：A_4 中元素对应 T_6 中通过面心的 180° 旋转（3 个）、通过体心的 120° 旋转（8 个）以及恒等变换。通过面心的 180° 旋转是通过面心的 90° 旋转两次，通过体心的 120° 旋转是同轴反方向旋转两次，恒等变换等价于自身重复两次。

17. **解答**：A_4 中的元素总能表示为 S_4 中元素的平方，而后者总能表示为对换的复合。所

以作为其平方，A_4 中的元素总能表示偶数个对换的复合。而其余元素就是 $\mathsf{A}_4 = H$ 作为往合子群的另一个往集。由于对换交换 T^+, T^-，所以另一个往集可以写为 τH，其中 τ 是某个对换。因此其中元素都可以写为奇数个对换的复合。

18. **解答**：$\{\pm 1\}$ 作为二元群同构于 C_2，又同构于 $\mathsf{S_T}$。记 f 为从 $\mathsf{S_T}$ 到 $\{\pm 1\}$ 的同构映射，g 是 S_4 到 T_6 的同构映射。考虑映射 $\Join = f \circ \varphi \circ g$。$\Join$ 从 S_4 映射到 $\{\pm 1\}$：

$$\forall \sigma \in \mathsf{S}_4,\ \Join(\sigma) = f(\gamma_{g(\sigma)}).$$

由于 $\varphi : \sigma \mapsto \gamma_\sigma$ 是群同态，所以 $\forall \sigma, \tau \in \mathsf{S}_4$，

$$\begin{aligned} \forall t \in \mathsf{T},\ \Join(\sigma\tau) &= f\left(\gamma_{g(\sigma\circ\tau)}\right) = f\left(\gamma_{g(\sigma)g(\tau)}\right) \\ &= f\left(\gamma_{g(\sigma)}\gamma_{g(\tau)}\right) = f\left(\gamma_{g(\sigma)}\right) f\left(\gamma_{g(\tau)}\right) \\ &= \Join(\sigma)\Join(\tau). \end{aligned}$$

所以 $\Join$ 是群同态。它的核是令 $\gamma_{g(\sigma)}$ 为恒等变换的 σ 集合，也就是 A_4。

19. **解答**：对换总把 T^+, T^- 调换，所以任何对换经 $\Join$ 映射到 -1。考虑 $\sigma \in \mathsf{S}_4$ 某种表示为对换复合的方法：$\sigma = \tau_1\tau_2\cdots\tau_k$，其中 k 是正整数，$\tau_1, \tau_2, \cdots, \tau_k$ 是对换，则 $\Join(\sigma) = \Join(\tau_1)\Join(\tau_2)\cdots\Join(\tau_k) = (-1)^k$。而 $\Join$ 是良好定义的群同态，所以 $\Join(\sigma)$ 的值是定值。反设 σ 既能表示为偶数个对换的复合，又能表示为奇数个对换的复合，那么按两种方法分别计算 $\Join(\sigma) = (-1)^k$，就得出 $\Join(\sigma)$ 既是 1 又是 -1，矛盾!

★ ★ ★ ★ ★

对称差积与置换的符号

1. **解答**：先说明契义：把 p 的各个变元换成另一些变元，所得仍是 n 元实系数整式，故 $\gamma(\sigma,p)\in\mathbb{R}[x_1,\cdots,x_n]$。

验证 γ 满足显相映射的条件：

- 设 e 是恒等置换，$x_{e(i)}=x_i$，所以 $\gamma(e,p)=p$。
- 记 $q=\gamma(\tau,p)$，即 $q(y_1,\cdots,y_n)=p(y_{\tau(1)},\cdots,y_{\tau(n)})$。把 y_i 代换为 $x_{\sigma(i)}$，得

$$\begin{aligned}\gamma(\sigma,\gamma(\tau,p)) &= q\big(x_{\sigma(1)},\cdots,x_{\sigma(n)}\big)\\ &= p\big(x_{\sigma(\tau(1))},\cdots,x_{\sigma(\tau(n))}\big)=\gamma(\sigma\tau,\,p).\end{aligned}$$

2. **解答**：$\Delta_2=x_1-x_2$，而

$$(1\,2)\cdot\Delta_2=x_2-x_1=-\Delta_2.$$

$\mathsf{S}_2=\{e,(1\,2)\}$，故 Δ_2 的轨迹为 $\{\Delta_2,\,-\Delta_2\}$，长度为 2；定子群为 $\{e\}$。用轨定定理核对：$|\mathsf{S}_2|=2=2\times1$，相符。

3. **解答**：$\Delta_3=(x_1-x_2)(x_1-x_3)(x_2-x_3)$。逐个代入：

σ	$\sigma\cdot\Delta_3$	结果
e	$(x_1-x_2)(x_1-x_3)(x_2-x_3)$	Δ_3
$(1\,2)$	$(x_2-x_1)(x_2-x_3)(x_1-x_3)$	$-\Delta_3$
$(1\,3)$	$(x_3-x_2)(x_3-x_1)(x_2-x_1)$	$-\Delta_3$
$(2\,3)$	$(x_1-x_3)(x_1-x_2)(x_3-x_2)$	$-\Delta_3$
$(1\,2\,3)$	$(x_2-x_3)(x_2-x_1)(x_3-x_1)$	Δ_3
$(1\,3\,2)$	$(x_3-x_1)(x_3-x_2)(x_1-x_2)$	Δ_3

例如 $(1\,3)$ 一行：三个因子分别为 $-(x_2-x_3)$、$-(x_1-x_3)$、$-(x_1-x_2)$，三个负号相乘得 -1。而 $(1\,2\,3)$ 一行出现两个负号，相乘得 $+1$。

因此保持 Δ_3 的是 $e,(1\,2\,3),(1\,3\,2)$；把它变号的是三个对换。

4. **解答**：猜想：任何置换施于 Δ_n，结果要么仍是 Δ_n，要么是 $-\Delta_n$，即 $\sigma\cdot\Delta_n=\pm\Delta_n$。换言之，$\Delta_n$ 的轨迹只有两个元素，置换按”保持”与”变号”分成两类。

5. **证明**：把 Δ_n 的因子按二元子集编号。记

$$\Gamma_n = \{\{i,j\} \mid 1 \leqslant i < j \leqslant n\}, \qquad \Delta_n = \prod_{\{a,b\}\in\Gamma_n,\ a<b} (x_a - x_b).$$

由于 σ 是双射，映射 $\{i,j\} \mapsto \{\sigma(i),\sigma(j)\}$ 是 Γ_n 到自身的双射：首先，若 $\{\sigma(i),\sigma(j)\} = \{\sigma(i'),\sigma(j')\}$，则 $\{i,j\} = \{i',j'\}$，再由 $i<j$、$i'<j'$ 得 $(i,j) = (i',j')$。其次，$\{i,j\}$ 显然可以由 $\{\sigma^{-1}(i),\sigma^{-1}(j)\}$ 映射得到，因此是满射。

6. 按定义

$$\sigma\cdot\Delta_n = \prod_{1\leqslant i<j\leqslant n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right).$$

对每个 $i<j$，令 a 为 $\sigma(i),\sigma(j)$ 中较小者，b 为较大者，则

$$x_{\sigma(i)} - x_{\sigma(j)} = \epsilon_{ij}\,(x_a - x_b), \qquad \epsilon_{ij} = \begin{cases} 1, & \sigma(i) < \sigma(j), \\ -1, & \sigma(i) > \sigma(j). \end{cases}$$

当 $\{i,j\}$ 遍历 Γ_n 时，$\{a,b\}$ 也恰好遍历 Γ_n 一次。把所有因子相乘，

$$\sigma\cdot\Delta_n = \Big(\prod_{i<j}\epsilon_{ij}\Big) \prod_{\{a,b\}\in\Gamma_n,\ a<b} (x_a - x_b) = \varepsilon(\sigma)\,\Delta_n, \qquad \varepsilon(\sigma) = \prod_{i<j}\epsilon_{ij} \in \{1,-1\}.$$

再说明 $\varepsilon(\sigma)$ 是唯一的：$\mathbb{R}[x_1,\cdots,x_n]$ 中非零整式之积非零，故 Δ_n 不恒等于零。若 $\varepsilon\Delta_n = \varepsilon'\Delta_n$，则 $(\varepsilon-\varepsilon')\Delta_n$ 恒等于零，从而推出 $\varepsilon=\varepsilon'$。

7. **证明**：按定义 $\curlywedge(\sigma) = \varepsilon(\sigma)$，即 $\sigma\cdot\Delta_n = \curlywedge(\sigma)\Delta_n$。显然 $\curlywedge(e) = 1$。

注意代入变元不改动实系数，故对任意实数 c 有 $\sigma\cdot(c\,p) = c\,(\sigma\cdot p)$。于是由显相映射的性质，

$$\begin{aligned}(\sigma\tau)\cdot\Delta_n = \sigma\cdot(\tau\cdot\Delta_n) &= \sigma\cdot\big(\curlywedge(\tau)\Delta_n\big) \\ &= \curlywedge(\tau)\,(\sigma\cdot\Delta_n) = \curlywedge(\tau)\curlywedge(\sigma)\,\Delta_n.\end{aligned}$$

另一方面 $(\sigma\tau)\cdot\Delta_n = \curlywedge(\sigma\tau)\Delta_n$。由第 6 问中说明的唯一性，并注意 $\{1,-1\}$ 中数的乘法可交换，得

$$\curlywedge(\sigma\tau) = \curlywedge(\sigma)\curlywedge(\tau).$$

故 $\curlywedge$ 是群同态。

8. **证明**：设 $\tau = (a\,b)$，$a < b$。它交换 x_a, x_b，其余变元不动。把 Δ_n 的因子分成三部分：

$$\Delta_n = (x_a - x_b) \cdot A \cdot B,$$

其中 A 是两端下标都不属于 $\{a, b\}$ 的因子之积，B 是恰有一个下标属于 $\{a, b\}$ 的因子之积。可以把 B 中的项配对写为：

$$B = \prod_{k \neq a,b} (x_k - x_a)(x_k - x_b)$$

交换 x_a, x_b 时：

- A 完全不变；
- B 中 $(x_k - x_a)(x_k - x_b)$ 变为 $(x_k - x_b)(x_k - x_a)$，整体不变。
- 唯有 $(x_a - x_b)$ 变为 $(x_b - x_a) = -(x_a - x_b)$。

因此 $\tau \cdot \Delta_n = -\Delta_n$，即 $\operatorname{sgn}(\tau) = -1$。

9. **解答**：

(1) 由第 8 问，任一对换把 Δ_n 变为 $-\Delta_n$，故 $-\Delta_n$ 在轨迹中。又 $\Delta_n \neq -\Delta_n$。结合第 6 问可知，Δ_n 的轨迹恰为 $\{\Delta_n, -\Delta_n\}$，长度为 2。由轨定定理，

$$|\mathsf{S}_n| = |\mathcal{O}(\Delta_n)| \cdot |H_n| \quad \Longrightarrow \quad n! = 2\,|H_n| \quad \Longrightarrow \quad |H_n| = \frac{n!}{2}.$$

(2) 两条理由皆可。其一：按定义 $H_n = \{\sigma \mid \sigma \cdot \Delta_n = \Delta_n\} = \{\sigma \mid \operatorname{sgn}(\sigma) = 1\} = \operatorname{Ker}\operatorname{sgn}$，而群同态的核总是往合子群。其二：$H_n$ 的左往集只有两个，即 H_n 与其补集；右往集也只有这两个，故对一切 σ 有 $\sigma H_n = H_n \sigma$。

(3) 由第 8 问，sgn 能取到 -1，故 sgn 是满同态，像为 $\{1, -1\}$。由群同态基本定理，

$$\mathsf{S}_n \big/ H_n \;\cong\; \{1, -1\} \;\cong\; \mathsf{C}_2,$$

即二元循环群。

10. **解答**：

(1) 由承认结论，σ 可写成对换的复合 $\sigma = \tau_1 \tau_2 \cdots \tau_k$。反复使用第 7 问的同态性与第 8 问的结论：

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1)\operatorname{sgn}(\tau_2) \cdots \operatorname{sgn}(\tau_k) = (-1)^k.$$

(2) 关键在于：$\curlywedge$ 是由第 6 问的等式 $\sigma\cdot\Delta_n=\curlywedge(\sigma)\Delta_n$ 定义的，这个定义只用到 σ 与 Δ_n，没有用到任何对换分解。因此 $\curlywedge(\sigma)$ 是由 σ 唯一确定的一个数。由上一问，任何分解都给出 $(-1)^k=\curlywedge(\sigma)$，所以 k 的奇偶不依赖分解方式：同一个置换不可能既写成偶数个对换的复合，又写成奇数个对换的复合。

(3) 按定义，偶置换即 $\curlywedge(\sigma)=1$ 者，也就是 $\sigma\cdot\Delta_n=\Delta_n$ 者，故全体偶置换恰为定子群 $H_n=\mathrm{Ker}\curlywedge$，记为 A_n，且 $|\mathsf{A}_n|=n!/2$。取任一对换 τ，则 $\curlywedge(\tau)=-1$，故 $\tau\notin\mathsf{A}_n$。由于只有两个往集，另一个往集就是 $\tau\mathsf{A}_n$；而对其中任一元素 τh（$h\in\mathsf{A}_n$）有 $\curlywedge(\tau h)=-1$，反之奇置换 σ 满足 $\tau^{-1}\sigma\in\mathrm{Ker}\curlywedge$，即 $\sigma\in\tau\mathsf{A}_n$。故全体奇置换恰构成另一个往集。

11. **证明**：在

$$\sigma\cdot\Delta_n=\prod_{1\leqslant i<j\leqslant n}\left(x_{\sigma(i)}-x_{\sigma(j)}\right)$$

中逐个考察因子。若 $\sigma(i)<\sigma(j)$，该因子就是 Δ_n 中对应子集 $\{\sigma(i),\sigma(j)\}$ 的那个因子；若 $\sigma(i)>\sigma(j)$，则它等于该因子的相反数，贡献一个负号。由第 5 问已知，当 $\{i,j\}$ 遍历所有二元子集时，$\{\sigma(i),\sigma(j)\}$ 也恰好遍历所有二元子集一次，因此这些因子的绝对部分之积恰为 Δ_n，而负号的个数恰为集合

$$\{(i,j)\mid i<j,\ \sigma(i)>\sigma(j)\}$$

的势，也就是逆序数。于是 $\sigma\cdot\Delta_n=(-1)^{\mathrm{inv}(\sigma)}\Delta_n$，即 $\curlywedge(\sigma)=(-1)^{\mathrm{inv}(\sigma)}$。

12. **解答**：按环圈形态分类。注意**同一环圈形态的逆序数未必相同，但奇偶相同**。

$n=2$:

环圈型	个数	$\curlywedge$	逆序数奇偶	代表元的逆序数
幺元	1	1	偶	$e:\ 0$
对换	1	-1	奇	$(1\,2):\ 1$

$\mathsf{A}_2=\{e\}$。

$n=3$:

环圈型	个数	χ	逆序数奇偶	代表元的逆序数
幺元	1	1	偶	$e:\ 0$
对换	3	-1	奇	$(1\,2):1,\ (1\,3):3,\ (2\,3):1$
3 元轮换	2	1	偶	$(1\,2\,3):2,\ (1\,3\,2):2$

$\mathsf{A}_3=\{e,\ (1\,2\,3),\ (1\,3\,2)\}$，同构于 C_3。

$n=4$:

环圈型	个数	χ	逆序数奇偶	代表元的逆序数
幺元	1	1	偶	$e:\ 0$
对换	6	-1	奇	$(1\,2):1,\ (1\,3):3,\ (1\,4):5$
双对换	3	1	偶	$(1\,2)(3\,4):2,\ (1\,3)(2\,4):4,\ (1\,4)(2\,3):6$
3 元轮换	8	1	偶	$(1\,2\,3):2,\ (1\,2\,4):4$
4 元轮换	6	-1	奇	$(1\,2\,3\,4):3,\ (1\,3\,2\,4):5$

A_4 共 $1+3+8=12$ 个元素:

$$\begin{aligned}\{&e,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3),\\ &(1\,2\,3),\ (1\,3\,2),\ (1\,2\,4),\ (1\,4\,2),\\ &(1\,3\,4),\ (1\,4\,3),\ (2\,3\,4),\ (2\,4\,3)\}.\end{aligned}$$

★ ★ ★ ★ ★

1.8 第八章参考解答

1. **解答**：本题的核心是将“本质不同的染色方案数”转化为“对称群显于状态集合的轨迹数”。底座集合 X 为正方体的 6 个面，$|X| = 6$。颜色集合为 C。我们使用**染色计数定理**：轨迹数等于群中各元素对应的环圈数 $c(g)$ 的函数 $|C|^{c(g)}$ 的平均值。

(1) **不考虑对称性**。用 2 种颜色染色，染色方案数为 $2^6 = 64$。

(2) **只允许绕某一条特定的顶心对角线旋转**。顶心对角线连接两个相对的顶点。绕此轴旋转 120° 和 240° 可保持正方体不变，加上恒等变换，构成 3 元循环群 $G_2 \cong \mathsf{C}_3$，群势 $|G_2| = 3$。分析各元素在 6 个面上的环圈：

- 恒等变换 e：$c(e) = 6$。
- 旋转 120° 和 240°：顶心对角线穿过两个顶点，每个顶点连接 3 个面。这 3 个面在旋转下轮换，形成 1 个 3 元环圈。两端共形成 2 个 3 元环圈。因此 $c(r) = c(r^2) = 2$。

用 2 种颜色染色，染色方案有

$$\begin{aligned}\frac{1}{3}\left(1 \times 2^6 + 2 \times 2^2\right) &= \frac{64 + 8}{3} \\ &= \frac{72}{3} = 24 \text{ 种}\end{aligned}$$

(3) **允许保持某一对特定对面（如上下底面）作为集合不变的所有旋转**。要保持“上下底面”这个集合不变，旋转轴必须是垂直轴（连接上下底面中心），或者是水平面内的轴（连接左右/前后侧面中心，或连接侧棱中点）。这些旋转构成一个 8 元群 G_3（同构于映轮群 D_4），群势 $|G_3| = 8$。分析这 8 个元素在 6 个面上的环圈：

- 恒等变换 e（1 个）：$c(e) = 6$。
- 绕垂直轴旋转 $90°, 270°$（2 个）：上下底面各自不动（2 个 1 元环圈），4 个侧面轮换（1 个 4 元环圈）。$c = 3$。
- 绕垂直轴旋转 180°（1 个）：上下底面不动（2 个 1 元环圈），4 个侧面两两互换（2 个 2 元环圈）。$c = 4$。
- 绕水平面心轴（如左右面中心连线）旋转 180°（2 个）：上下底面互换（1 个 2 元环圈），两个侧面不动（2 个 1 元环圈），另两个侧面互换（1 个 2 元环圈）。$c = 1 + 2 + 1 = 4$。
- 绕对棱中线（如左右面与前后面交棱的中点连线）旋转 180°（2 个）：上下底

面互换（1 个 2 元环圈），4 个侧面两两互换（2 个 2 元环圈）。$c = 1+2 = 3$。

用 2 种颜色染色，染色方案有

$$\frac{1}{8}\left(1\times 2^6 + 2\times 2^3 + 1\times 2^4 + 2\times 2^4 + 2\times 2^3\right) = \frac{64+16+16+32+16}{8} = \frac{144}{8} = 18 \text{ 种}$$

(4) **允许正方体的所有旋转**。此时对称群为完整的旋转群 $G_4 = \mathsf{T}_6$，群势 $|G_4| = 24$。分析 24 个元素在 6 个面上的环圈：

- 恒等变换 e（1 个）：$c = 6$。
- 绕面心轴旋转 $90°, 270°$（3 条轴 $\times 2 = 6$ 个）：$c = 3$。
- 绕面心轴旋转 $180°$（3 条轴 $\times 1 = 3$ 个）：$c = 4$。
- 绕顶心对角线旋转 $120°, 240°$（4 条轴 $\times 2 = 8$ 个）：$c = 2$。
- 绕对棱中线旋转 $180°$（6 条轴 $\times 1 = 6$ 个）：$c = 3$。

用 2 种颜色染色，染色方案有

$$\frac{1}{24}\left(1\times 2^6 + 6\times 2^3 + 3\times 2^4 + 8\times 2^2 + 6\times 2^3\right) = \frac{64+48+48+32+48}{24} = \frac{240}{24} = 10 \text{ 种}$$

(5) **颜色变为 3 种（红、蓝、绿）**。只需将上述各问公式中的底数 2 替换为 3 即可：

- 第 (1) 问：$3^6 = 729$ 种。
- 第 (2) 问（3 元群）：$\frac{1}{3}(1\times 3^6 + 2\times 3^2) = \frac{729+18}{3} = 249$ 种。
- 第 (3) 问（8 元群）：$\frac{1}{8}(1\times 3^6 + 2\times 3^3 + 1\times 3^4 + 2\times 3^4 + 2\times 3^3) = \frac{729+54+81+162+54}{8} = \frac{1080}{8} = 135$ 种。
- 第 (4) 问（24 元群）：$\frac{1}{24}(1\times 3^6 + 6\times 3^3 + 3\times 3^4 + 8\times 3^2 + 6\times 3^3) = \frac{729+162+243+72+162}{24} = \frac{1368}{24} = 57$ 种。

(6) **对比与直观解释。变化规律**：

- **对称操作增多**：无论是 2 色（$64 \to 24 \to 18 \to 10$）还是 3 色（$729 \to 249 \to 135 \to 57$），随着允许的对称群势增大，本质不同的染色方案数**严格递减**。
- **颜色种类增多**：在相同的对称群下，3 色的方案数都远大于 2 色的方案数。

直观解释：

- **从“群势与轨迹合并”的角度**：本质不同的方案数，就是状态集合被群分划的**轨迹数**。群势越大，意味着群中有更多的变换可以用来“搬运”状态。更

多的搬运手段，会把原本在较小群下不等价的状态合并到同一个轨迹中。因此，对称性越高（群势越大），分类就越“粗”，轨迹数（方案数）就越少。

- **从“对称轴数量”的角度**：第 (2) 问只有 1 条对称轴，合并能力最弱；第 (3) 问包含了 1 条垂直轴和 4 条水平/对角轴（共 5 条），合并能力中等；第 (4) 问包含了 3 条面心轴、4 条顶心对角线、6 条对棱中线（共 13 条），合并能力最强。对称轴的数量直观地反映了群势的大小，决定了对称操作“抹平”差异的能力。
- **颜色增多的影响**：颜色增多，使得不考虑对称性时的总状态数 $|C|^{|X|}$ 呈指数级爆炸（从 64 到 729）。虽然对称操作合并了一部分状态，但状态池的“基数”变大了，因此最终剩下的本质不同的方案数也随之大幅增加。这体现了代数结构（群）对组合数量（状态数）的约束与化归作用。

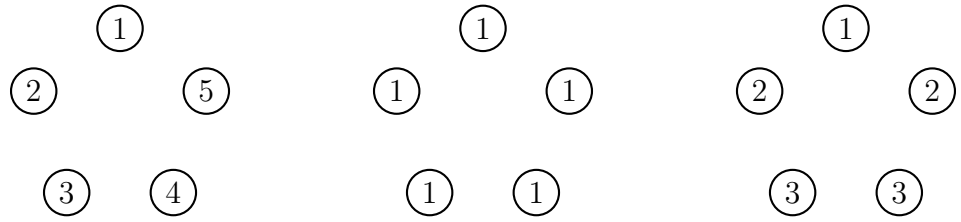
2. **解答**：本题的底座集合 X 为正五边形的 5 个顶点。颜色集合为 C。本质不同的染色方案数，即为对称群显于状态集合 $S = C^X$ 的**轨迹数**。我们将使用本章的**染色计数定理**进行计算：

$$\text{轨迹数} = \frac{1}{|G|}\sum_{g\in G}|C|^{c(g)}$$

其中 $|G|$ 为对称群的势，$|C|$ 为颜色数，$c(g)$ 为群元素 g 作用于 5 个顶点时形成的**环圈数**。

首先，分析正五边形对称群中各元素作用于 5 个顶点时的环圈结构：

- **恒等变换 e（1 个）**：每个顶点各自形成一个 1 元环圈，共 $c(e) = 5$ 个环圈。
- **非平凡旋转（4 个）**：每个旋转将 5 个顶点整体轮换，形成 1 个 5 元环圈，共 $c(g) = 1$ 个环圈。
- **翻转（5 个）**：每个翻转的对称轴过 1 个顶点和 1 条对边中点。该顶点形成 1 个 1 元环圈，其余 4 个顶点两两交换，形成 2 个 2 元环圈。共计 $c(g) = 1 + 2 = 3$ 个环圈。



各类变换形成的环圈：相同数字表示属于同一个环圈。

(1) **解答**：不考虑对称性，状态集合 S 的大小为 $|C|^{|X|} = 2^5 = 32$。所以有 32 种染色方法。

(2) **解答**：允许旋转和翻转，对称群为正五边形的映轮群 D_5，群势 $|\mathsf{D}_5| = 10$。颜色数 $|C| = 2$。根据染色计数定理，轨迹数为：

$$\frac{1}{10}\left(1 \times 2^5 + 4 \times 2^1 + 5 \times 2^3\right) = \frac{32 + 8 + 40}{10} = \frac{80}{10} = 8 \text{ 种}$$

(3) **解答**：对称群仍为映轮群 D_5，群势为 10。颜色数 $|C| = 3$。根据染色计数定理，轨迹数为：

$$\frac{1}{10}\left(1 \times 3^5 + 4 \times 3^1 + 5 \times 3^3\right) = \frac{243 + 12 + 135}{10} = \frac{390}{10} = 39 \text{ 种}$$

(4) **解答**：只允许旋转，对称群为 5 元循环群 C_5，群势 $|\mathsf{C}_5| = 5$。颜色数 $|C| = 2$。分析 C_5 中各元素的环圈数：恒等变换 e（1 个）$c(e) = 5$；非平凡旋转（4 个）$c(g) = 1$。根据染色计数定理，轨迹数为：

$$\frac{1}{5}\left(1 \times 2^5 + 4 \times 2^1\right) = \frac{32 + 8}{5} = \frac{40}{5} = 8 \text{ 种}$$

(5) **解答**：对称群仍为循环群 C_5，群势为 5。颜色数 $|C| = 3$。根据染色计数定理，轨迹数为：

$$\frac{1}{5}\left(1 \times 3^5 + 4 \times 3^1\right) = \frac{243 + 12}{5} = \frac{255}{5} = 51 \text{ 种}$$

(6) **解答**：对比第 (2)、(3) 问（允许翻转，映轮群 D_5）与第 (4)、(5) 问（只允许旋转，循环群 C_5）的答案：

- 用 2 种颜色时，允许翻转（8 种）与只允许旋转（8 种）的答案**相同**。
- 用 3 种颜色时，允许翻转（39 种）的答案**小于**只允许旋转（51 种）。

理由：引入翻转操作（从 C_5 扩大到 D_5）增加了系统的对称性。通常，更大的对称群会将原本在较小群下不等价的轨迹合并，从而减少总轨迹数。

- **为何 2 色时没有减少**：对于 2 色 5 顶点的所有 8 个旋转轨迹，每一个轨迹在翻转操作下都是“自对称”的。也就是说，任何一个 2 色图案翻转后得到的镜像图案，总可以通过某种旋转操作变回它自己。翻转并没有把两个不同的旋转轨迹合并成一个，而只是在每个旋转轨迹内部进行置换。因此，轨迹总数保持不变。

- **为何 3 色时减少了**：3 色增加了状态空间的复杂度。在 3 色的 51 个旋转轨迹中，存在“手性”图案（即翻转后得到的镜像图案，无法通过任何旋转操作与自身重合）。翻转操作将这些互为镜像的旋转轨迹两两合并。因此，总轨迹数从 51 减少到了 39。

六氟化硫的立体异构体

1. **解答**：底座集合 X 是正八面体的六个顶点，也就是六个可以安放原子的位置，$|X| = 6$。颜色集合 $C = \{\text{氟}, \text{氯}\}$，$|C| = 2$。一种原子排布，就是给每个位置指定一种原子，因此它是一个映射 $f : X \to C$。所有排布构成 $S = C^X$，于是

$$|S| = |C|^{|X|} = 2^6 = 64.$$

这里要注意：六个位置是空间中固定的六个点，不随分子转动而改名。转动改变的是“哪个位置上放着哪种原子”，而不是位置本身。

2. **解答**：以旋转群 G 观于 S。两种排布能通过转动重合，就是说存在 $g \in G$ 把其中一种变成另一种，也就是它们属于同一条轨迹。因此本题要求的答案，就是 G 显于 S 的轨迹数 $|\mathcal{O}_G(S)|$。这正是本章第一节把染色问题化为轨迹计数的做法。

3. **解答**：苯环的六个取代位置共面。把这样一个平面分子在空间中绕平面内的一条直线转 180°，是真正的空间旋转；它对六个位置的效果，恰好等同于把平面正六边形沿该直线作轴对称。所以苯环的对称群写成映轮群 D_6，其中并没有混入非旋转的操作。正八面体的六个顶点不共面，镜面反射不是空间旋转，一般不能靠转动实现，因此本题只取旋转构成的群。本题也只讨论旋转异构，不讨论镜像带来的对映异构。

4. **解答**：任取一个顶点，比如“上”。旋转可以把它送到六个顶点位置中的任意一个，共 6 种可能。一旦“上”的去处确定，比如仍留在上方，赤道上的四个顶点就只能在这四个位置之间轮换，共 4 种（转 0°、90°、180°、270°）。因此

$$|G| = 6 \times 4 = 24.$$

这与第一章数正方体旋转的办法完全平行：先把某个面转到朝上，有 6 种；再把某个侧面转到朝前，有 4 种。

5. **解答**：

(1) 六个顶点两两相对，共 3 对，故有 3 条顶点轴；八个面两两相对，共 4 对，故有 4 条面心轴；十二条棱两两相对，共 6 对，故有 6 条棱中轴。

(2) 绕顶点轴转动时，赤道上的四个顶点构成正方形，转 90°、180°、270° 都能复原，非恒等旋转 3 个。绕面心轴转动时，该面的三个顶点轮换，转 120°、240° 复原，非恒等旋转 2 个。绕棱中轴转动时，只有 180° 复原，非恒等旋转 1 个。

(3) 合计

$$1+3\times 3+4\times 2+6\times 1=1+9+8+6=24,$$

与第 4 问一致。作为对照，正方体有 3 条面心轴、4 条顶心对角线、6 条对棱中线，条数完全相同，只是“顶点”与“面”的角色互换。本题不需要追究这一对应关系的缘由，只要会用这 24 个旋转就够了。

6. **解答**：绕上下轴从上往下看逆时针转 90° 时，上与下各自不动，右到前、前到左、左到后、后到右。写成环圈分解：

$$(\text{上})(\text{下})(\text{右 前 左 后}).$$

两个 1 元环圈加一个 4 元环圈，故 $c(g)=3$。

7. **解答**：

(1) g 定住 f，意思是搬家之后每个位置上的原子种类都与原来相同，即

$$\forall a\in X,\quad f(g(a))=f(a).$$

(2) 反复施用 g，从 a 出发依次得到 $a,\ g(a),\ g^2(a),\cdots$，它们恰好遍历 a 所在的环圈。上式说明这些位置上的原子种类必须全部相同。反过来，只要每个环圈内部同色，上述条件就处处成立。不同环圈之间没有任何约束。

(3) 每个环圈独立地有 2 种选择，共有 $c(g)$ 个环圈，因此

$$|S^g|=2^{c(g)}.$$

8. **解答**：上与下不动，右与左互换，前与后互换：

$$(\text{上})(\text{下})(\text{右 左})(\text{前 后}),\qquad c(g)=4.$$

9. **解答**：绕这条面心轴转 120° 时，上到右、右到前、前到上；同时下到左、左到后、后到下：

$$(\text{上 右 前})(\text{下 左 后}),\qquad c(g)=2.$$

转 240° 是它的逆，也是它的平方，环圈的划分方式相同，仍有 $c(g)=2$。

10. **解答**：这条轴穿过“上前”棱的中点，转 180° 把该棱的两个端点对调；相对棱“下后”同理；剩下的左与右被对调：

$$(\text{上 前})(\text{下 后})(\text{左 右}), \qquad c(g) = 3.$$

11. **解答**：汇总如下。

旋转类别	个数	环圈形态	$c(g)$	$2^{c(g)}$
恒等变换	1	1^6	6	64
顶点轴 $90^\circ, 270^\circ$	6	$1^2\,4$	3	8
顶点轴 180°	3	$1^2\,2^2$	4	16
面心轴 $120^\circ, 240^\circ$	8	3^2	2	4
棱中轴 180°	6	2^3	3	8

个数之和为 $1+6+3+8+6=24$，与 $|G|$ 相符。

12. **解答**：由染色计数定理，

$$\begin{aligned} |\mathcal{O}_G(S)| &= \frac{1}{|G|}\sum_{g\in G} 2^{c(g)} \\ &= \frac{1}{24}\left(1\times 64 + 6\times 8 + 3\times 16 + 8\times 4 + 6\times 8\right) \\ &= \frac{64+48+48+32+48}{24} = \frac{240}{24} = 10. \end{aligned}$$

即一共有 10 种本质不同的空间结构。

13. **解答**：

(1) 从六个位置中选两个，共 $\binom{6}{2} = 15$ 种选法。

(2) 两个氯原子要么位于相对顶点，要么位于相邻顶点，没有第三种可能。相对的情形对应三条顶点轴，共 3 种；相邻的情形共 $15-3=12$ 种，也可以直接数：每个顶点与 4 个顶点相邻，$6\times 4\div 2 = 12$。相对型的三种可以通过旋转互相得到，因为旋转能把任一条顶点轴转到任另一条。相邻型的十二种也可以：先把其中一个氯原子转到“上”（群贯通六个顶点），此时另一个氯原子在赤道四个位置之一，再绕上下轴转 90° 的倍数即可互相得到。

(3) 于是恰好两条轨迹，SF_4Cl_2 恰有两种立体异构体。相对型是反式，相邻型是顺式。

14. **解答**：反式的轨迹长为 3，由轨定定理，其定子群有 $24 \div 3 = 8$ 个元素；顺式的轨迹长为 12，定子群有 $24 \div 12 = 2$ 个元素。反式的定子群由保持 {上, 下} 这个集合不变的旋转组成：绕上下轴的 4 个旋转（含恒等），绕左右轴与前后轴各一个 180° 旋转（它们把上下对调），以及赤道平面内两条棱中轴（“右前—左后”与“右后—左前”）各一个 180° 旋转，共 8 个。顺式的定子群由保持 {上, 前} 的旋转组成：只有恒等变换，以及绕“上前棱中点—下后棱中点”连线的 180° 旋转，共 2 个。两者都与轨定定理的计算相符。

15. **解答**：三个氯原子的选法共 $\binom{6}{3} = 20$ 种。若三个氯原子两两相邻，它们必围成正八面体的一个面，而正八面体有 8 个面，故这样的情形有 8 种。若其中有一对相对顶点，则先选一条顶点轴（3 种），再从其余 4 个顶点中任选一个（4 种），共 $3 \times 4 = 12$ 种；每个这样的三元组恰含一对相对顶点，不会重复计数。两类相加 $8 + 12 = 20$，核对无误。面可以转到面，故第一类自成一条轨迹；第二类中，先把所含的顶点轴转到上下，再把第三个氯原子转到赤道任一位置，故也自成一条轨迹。于是 SF_3Cl_3 恰有两种立体异构体：两两相邻型称为面式，含相对对型称为经式。由轨定定理，它们的定子群分别有 $24 \div 8 = 3$ 个与 $24 \div 12 = 2$ 个元素。

16. **解答**：各配比的结果如下。

氯原子个数 k	0	1	2	3	4	5	6
异构体数目	1	1	2	2	2	1	1

总和为 $1+1+2+2+2+1+1 = 10$，与第 12 问一致。$k = 0$ 与 $k = 6$ 时六个位置放同一种原子，只有一种排布。$k = 1$ 时只有一个位置是氯，而群贯通六个顶点，任何两个这样的排布都能互相转到，故只有一种；$k = 5$ 同理，只不过孤立的换成氟。$k = 3$ 见第 15 问。$k = 2$ 与 $k = 4$ 数目相同，原因是对称的：把每个位置上的氟与氯互换，得到 S 上的一个双射，它与旋转的作用可交换（旋转只搬位置，不改原子种类），因此把 $k = 2$ 的轨迹一一对应到 $k = 4$ 的轨迹。

17. **解答**：记 a 为氯，b 为氟，长度 n 的环圈对应 $p_n = a^n + b^n$。按第 11 问的环圈形态逐个搭建整式，并取 a^2b^4 的系数：

- 恒等变换：$P_e = (a+b)^6$，系数为 $\binom{6}{2} = 15$，小计 $1 \times 15 = 15$。
- 顶点轴 $90°, 270°$：$P_g = (a+b)^2(a^4+b^4)$，只有 $a^2 \cdot b^4$ 一项合乎要求，系数为 1，小计 $6 \times 1 = 6$。
- 顶点轴 $180°$：$P_g = (a+b)^2(a^2+b^2)^2 = (a^2+2ab+b^2)(a^4+2a^2b^2+b^4)$，取 $a^2 \cdot b^4$ 与 $b^2 \cdot 2a^2b^2$，系数为 $1+2=3$，小计 $3 \times 3 = 9$。
- 面心轴：$P_g = (a^3+b^3)^2$，各项次数都是 3 的倍数，凑不出 a^2b^4，小计 0。
- 棱中轴：$P_g = (a^2+b^2)^3$，其中 $3a^2b^4$ 的系数为 3，小计 $6 \times 3 = 18$。

求和取平均：

$$\frac{15+6+9+0+18}{24} = \frac{48}{24} = 2,$$

与第 13 问的直接分类结果一致。

★ ★ ★ ★ ★

同构的简单无向图

1. 3 元图最多 3 条边；4 元图最多 6 条边；5 元图最多 10 条边。最少都是 0 条边。

2. n 元简单无向图最多有 C_n^2 条边。E 是 V 的所有二元子集的集合，$|E| = \mathrm{C}_n^2$。任何简单无向图的边集 B 都是 E 的子集。

3. 设 $V = V' = \{v_1, \cdots, v_n\}$，$f : V \to V$ 是双射。定义 E 上的映射：

$$p_f : \{v_i, v_j\} \longmapsto \{f(v_i), f(v_j)\}.$$

由于 f 是双射，若 $\{v_i, v_j\} \neq \{v_k, v_l\}$，则 $\{f(v_i), f(v_j)\} \neq \{f(v_k), f(v_l)\}$，所以 p_f 是单射。反之，由于 f 是双射，从任何 $\{v'_i, v'_j\}$ 都能得到 $\{f^{(-1)}(v'_i), f^{(-1)}(v'_j)\} \in E$，因此 p_f 是满射。综上可知 p_f 是 E 上的置换。唯一性由定义显然。

4. 给定 $\sigma \in \mathsf{S}_n$，任取 4 元简单无向图 $\Omega = (V, B)$。定义 $\Omega' = (V, B')$，其中 $B' = p_\sigma(B) = \{\{\sigma(v_i), \sigma(v_j)\} \,|\, \{v_i, v_j\} \in B\}$。则 σ 是从 Ω 到 Ω' 的同构（按题 3 的定义）。特别地，若 $\Omega' = \Omega$（即 $p_\sigma(B) = B$），则 σ 是 Ω 到自身的同构（自同构）。σ 改变边的方式：将边 $\{v_i, v_j\}$ 变为 $\{\sigma(v_i), \sigma(v_j)\}$。

5.〔1〕 左图有 8 个顶点 7 条边，右图有 8 个顶点 8 条边，不同构。

〔2〕 左右图都有 7 个顶点 6 条边，但右图 v_1 连出 4 条边，左图顶点最多连出 3 条边，所以不同构。

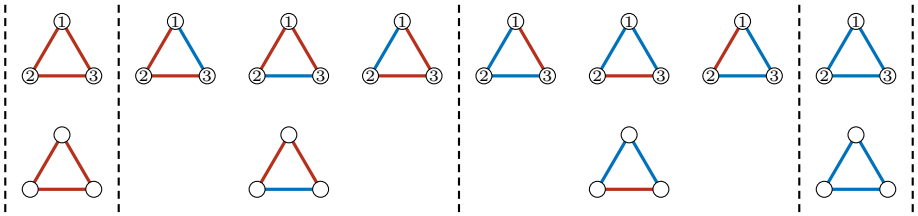
〔3〕 左右图同构。可以看到都由某个顶点连出 4 条“道路”，其中两条由两条边组成，两条由一条边组成。可以写出左图到右图的双射 f：

$$\begin{aligned} f: \quad & v_1 \mapsto v_2, && v_2 \mapsto v_7, \\ & v_3 \mapsto v_6, && v_4 \mapsto v_5, \\ & v_5 \mapsto v_1, && v_6 \mapsto v_3, && v_7 \mapsto v_4. \end{aligned}$$

注：f 并不是唯一的，比如，把 $v_6 \mapsto v_3, v_7 \mapsto v_4$ 换为 $v_6 \mapsto v_4, v_7 \mapsto v_3$，也是合格的双射。但把 $v_3 \mapsto v_6, v_4 \mapsto v_5$ 换为 $v_3 \mapsto v_5, v_4 \mapsto v_6$ 就不行了。

6. 完全图 K_n 每对顶点都有边，共 C_n^2 条边。完全图的自同构：由于完全图每对顶点都有边，V 上的任何双射都保持边集不变。因此完全图的自同构群就是 S_n，有 $n!$ 个元素。

7. K_3 有 3 条边。**顶点标号 $1,2,3$ 时**：每条边独立选红或蓝，共 $2^3 = 8$ 种。**顶点没有区别时**：S_3（6 个元素）作用于 3 条边上。枚举：全红（1 种）、全蓝（1 种）、1 红 2 蓝（1 种）、2 红 1 蓝（1 种），共 4 种。



8. 验证显相映射的相容条件：

(1) $\gamma(e, \{v_i, v_j\}) = \{e(v_i), e(v_j)\} = \{v_i, v_j\}$。

(2) $\gamma(\sigma, \gamma(\tau, \{v_i, v_j\})) = \gamma(\sigma, \{\tau(v_i), \tau(v_j)\}) = \{\sigma\tau(v_i), \sigma\tau(v_j)\} = \gamma(\sigma\tau, \{v_i, v_j\})$。

因此 γ 是观 S_n 于 E 的显相映射。$\sigma \mapsto \gamma_\sigma$ 是群同态：$\gamma_{\sigma\tau} = \gamma_\sigma \circ \gamma_\tau$，由上述第二条直接得出。$\gamma$ 令 S_n 显通相：对 E 中任意两条边 $\{v_i, v_j\}$ 和 $\{v_k, v_l\}$，总存在 $\sigma \in \mathsf{S}_n$ 使得 $\sigma(v_i) = v_k$，$\sigma(v_j) = v_l$（或反之），因此 $\gamma_\sigma(\{v_i, v_j\}) = \{v_k, v_l\}$。所以 E 只有一条轨迹，γ 显通相。

9. $S = 2^E$，$p_\sigma(B) = \{p_\sigma(e) \,|\, e \in B\} = \{\{\sigma(v_i), \sigma(v_j)\} \,|\, \{v_i, v_j\} \in B\}$。验证群观公理：$p_e(B) = B$；$p_\sigma(p_\tau(B)) = p_{\sigma\tau}(B)$。因此 γ' 是观 S_n 于 S 的显相映射。γ' **不令** S_n 显通相：S 中元素（边子集）的势不同，而群作用保持势不变。例如 $\varnothing$ 和 E 不在同一轨迹。因此 S 有多条轨迹。

γ 和 γ' 的关系：对 $\forall \sigma \in \mathsf{S}_n$，$\forall B \in S$，$\forall b \in E$，

$$b \in B \iff \gamma(\sigma, b) \in \gamma'(\sigma, B).$$

即：B 中每条边 b，经 γ 变换后，恰好落在 $\gamma'(\sigma, B)$ 中。γ' 的效果完全由 γ 决定：逐条搬运 B 中的边，搬运规则就是 γ。

10. 设两种染色方案分别对应边集 $B_1, B_2 \subseteq E$。“本质相同”指存在顶点置换 $\sigma \in \mathsf{S}_n$，使得经 σ 变换后，B_1 变为 B_2，即 $p_\sigma(B_1) = B_2$。按题 9，$p_\sigma(B_1) = \gamma'_\sigma(B_1)$。因此 B_1 和 B_2 本质相同，当且仅当存在 σ 使得 $\gamma'_\sigma(B_1) = B_2$，当且仅当 B_1 和 B_2 在 γ' 下属于同一条轨迹。

11. 一个简单无向图由其边集 $B \subseteq E$ 完全决定。而 $B \subseteq E$ 等价于给 E 中每条边染 0（无边）或 1（有边）两种颜色之一。因此，n 元简单无向图与 K_n 的边的二染色方案一一对应。两个简单无向图同构，当且仅当对应的染色方案在 S_n 诱导的群观下属于同一条轨迹。因此，本质不同的简单无向图的种数，等于 C^E 在 S_n 诱导群观下的轨迹个数。

以 $n = 4$ 的情况为例。$V = \{1,2,3,4\}$，$E = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$，$|E| = 6$。按本章正文的术语，底座集合 $X = E$，$|X| = 6$。颜色集合 $C = \{0,1\}$，$|C| = 2$。染色方案集合 $S = C^E = \{0,1\}^E$。E 的每个子集 B 通过函数 $\chi_B : E \to \{0,1\}$ 与 C^E 中元素一一对应。$|C^E| = 2^6 = 64$。群 $G = \mathsf{S}_4$，$|G| = 24$，通过群观 γ 作用于底座集合 X，通过群观 γ' 作用于染色方案集合 $S = C^E$。4 元简单无向图的同构类个数等于 C^E 在 γ' 下的轨迹个数。

12. S_4 按环圈形态（环圈数和长度）分类：

类型	环圈数	代表元	置换个数
恒等	4	$(1)(2)(3)(4)$	1
对换	3	$(1\,2)(3)(4)$	6
3 元轮换	2	$(1\,2\,3)(4)$	8
双对换	2	$(1\,2)(3\,4)$	3
4 元轮换	1	$(1\,2\,3\,4)$	6

总计 $1+6+8+3+6 = 24$ 个置换。

各类的代表元在 $E = \{\overline{12},\overline{13},\overline{14},\overline{23},\overline{24},\overline{34}\}$ 上的轨迹分划：

- **恒等**：每条边不动。因此共有 6 条轨迹，长度是 1。
- **对换** $(1\,2)$：$\overline{12} \to \overline{12}$，$\overline{34} \to \overline{34}$，$\overline{13} \leftrightarrow \overline{23}$，$\overline{14} \leftrightarrow \overline{24}$。共 4 条轨迹：

$$\{\overline{12}\},\ \{\overline{34}\},\ \{\overline{13},\overline{23}\},\ \{\overline{14},\overline{24}\}$$

- 3 **元轮换** $(1\,2\,3)$：$\overline{12} \to \overline{23} \to \overline{13} \to \overline{12}$；$\overline{14} \to \overline{24} \to \overline{34} \to \overline{14}$。共 2 条轨迹：

$$\{\overline{12},\overline{23},\overline{13}\},\ \{\overline{14},\overline{24},\overline{34}\}$$

- **双对换** $(1\,2)(3\,4)$：$\overline{12} \to \overline{12}$，$\overline{34} \to \overline{34}$，$\overline{13} \leftrightarrow \overline{24}$，$\overline{14} \leftrightarrow \overline{23}$。共 4 条轨迹：

$$\{\overline{12}\},\ \{\overline{34}\},\ \{\overline{13},\overline{24}\},\ \{\overline{14},\overline{23}\}$$

- 4 **元轮换** $(1\,2\,3\,4)$：$\overline{12}\to\overline{23}\to\overline{34}\to\overline{14}\to\overline{12}$；$\overline{13}\to\overline{24}\to\overline{13}$。共 2 条轨迹：

$$\{\overline{12},\overline{23},\overline{34},\overline{14}\},\ \{\overline{13},\overline{24}\}$$

13. 对于每个 $\sigma\in\mathsf{S}_4$，γ_σ 都是 E 上的置换，把 E 中的边换到另一条边。$n=4$ 时 $|E|=6$，所以 γ_σ 对应 6 元置换，也就是说，我们通过 $\sigma\mapsto\gamma_\sigma$，建立了 S_4 到 S_6 子群的同构。各类的代表元对应的 6 元置换的环圈结构：

- **恒等**：对应 6 元恒等变换，有 6 个环圈，每个长度为 1。
- **对换** $(1\,2)$：对应 4 个环圈，两个长度为 1，两个长度为 2。
- 3 **元轮换** $(1\,2\,3)$：对应 2 个环圈，每个长度为 3。
- **双对换** $(1\,2)(3\,4)$：对应 4 个环圈，两个长度为 1，两个长度为 2。
- 4 **元轮换** $(1\,2\,3\,4)$：对应 2 个环圈，长度分别是 2 和 4。

14. 设 $\sigma\in\mathsf{S}_4$ 在 X 上划分的轨迹为 $\mathcal{O}_1,\cdots,\mathcal{O}_k$。染色方案 $\varphi\in C^X$ 是 σ 的定元，即 $\gamma'_\sigma(\varphi)=\varphi$，意味着 $\forall x\in X$，$\varphi(x)=\varphi(\sigma(x))$。由于同一轨迹内的元素经 σ 循环置换，这要求同一轨迹内所有边染相同颜色。反之，若同一轨迹内所有边同色，则 φ 经 σ 不变。

同一轨迹内的边必须染相同颜色，不同轨迹之间独立选择。$|C|=2$，k 条轨迹各有 2 种选择，故 $|S^\sigma|=2^k$。

S_4 中各类置换的相关结果：

类型	个数	γ_σ 轨迹数（k）	定元数（2^k）
恒等	1	6	64
对换	6	4	16
3 元轮换	8	2	4
双对换	3	4	16
4 元轮换	6	2	4

15. 由定元分轨定理：

$$\begin{aligned}\mathcal{O}_G(S)&=\frac{1}{|\mathsf{S}_4|}\sum_{\sigma\in\mathsf{S}_4}|S^\sigma|=\frac{1\cdot64+6\cdot16+8\cdot4+3\cdot16+6\cdot4}{24}\\&=\frac{64+96+32+24+48}{24}=\frac{264}{24}\\&=11.\end{aligned}$$

4 元简单无向图的同构类个数为 **11**。

16. 按边数 k 分类枚举：

- $k=0$：无边图（也就是点集）。1 种。
- $k=1$：一条边 + 两个孤立顶点。1 种。
- $k=2$：两边相邻（路径 P_3 加孤立点）或两边不相邻（$2K_2$）。2 种。
- $k=3$：三角形 K_3 加孤立点、路径 P_4、星形 $K_{1,3}$。3 种。
- $k=4$：由互补性，与 $k=2$ 对应。2 种。
- $k=5$：与 $k=1$ 对应。1 种。
- $k=6$：完全图 K_4。1 种。

总计 $1+1+2+3+2+1+1=11$ 种，与上一题结果一致。

17. 对任意正整数 n，基本多项式为：

$$p_n = a^n + b^n.$$

p_n 代表一个长度为 n 的环圈：该环圈内所有底座元素必须染同色，要么全染颜色 0（贡献 a^n），要么全染颜色 1（贡献 b^n）。逐类搭建 P_σ：

- **恒等**（1 个）：6 条长度 1 的环圈。

$$P = p_1^6 = (a+b)^6.$$

- **对换**（6 个）：2 条长度 1、2 条长度 2 的环圈。

$$P = p_1^2\, p_2^2 = (a+b)^2(a^2+b^2)^2.$$

- 3 **元轮换**（8 个）：2 条长度 3 的环圈。

$$P = p_3^2 = (a^3+b^3)^2.$$

- 4 **元轮换**（6 个）：1 条长度 4、1 条长度 2 的环圈。

$$P = p_4\, p_2 = (a^4+b^4)(a^2+b^2).$$

- **双对换**（3 个）：2 条长度 1、2 条长度 2 的环圈。

$$P = p_1^2\, p_2^2 = (a+b)^2(a^2+b^2)^2.$$

注意对换与双对换的 P_σ 相同，合并后系数为 $6+3=9$。

18. 汇总得：

$$P=\frac{1}{24}\Big[(a+b)^6+9(a+b)^2(a^2+b^2)^2+8(a^3+b^3)^2+6(a^4+b^4)(a^2+b^2)\Big].$$

逐项展开：

$$\begin{aligned}
(a+b)^6 &= a^6+6a^5b+15a^4b^2+20a^3b^3+15a^2b^4+6ab^5+b^6,\\
(a+b)^2(a^2+b^2)^2 &= a^6+2a^5b+3a^4b^2+4a^3b^3+3a^2b^4+2ab^5+b^6,\\
9(a+b)^2(a^2+b^2)^2 &= 9a^6+18a^5b+27a^4b^2+36a^3b^3+27a^2b^4+18ab^5+9b^6,\\
(a^3+b^3)^2 &= a^6+2a^3b^3+b^6,\\
8(a^3+b^3)^2 &= 8a^6+16a^3b^3+8b^6,\\
(a^4+b^4)(a^2+b^2) &= a^6+a^4b^2+a^2b^4+b^6,\\
6(a^4+b^4)(a^2+b^2) &= 6a^6+6a^4b^2+6a^2b^4+6b^6.
\end{aligned}$$

按次数汇总各项系数：

项	a^6	a^5b	a^4b^2	a^3b^3	a^2b^4	ab^5	b^6
恒等	1	6	15	20	15	6	1
对换 + 双对换	9	18	27	36	27	18	9
3 元轮换	8	0	0	16	0	0	8
4 元轮换	6	0	6	0	6	0	6
合计	24	24	48	72	48	24	24

各项除以 24：

$$P=a^6+a^5b+2a^4b^2+3a^3b^3+2a^2b^4+ab^5+b^6.$$

各系数为 $1,1,2,3,2,1,1$。其中 $a^{6-k}b^k$ 的系数就是恰有 k 条边的 4 元简单无向图的同构类个数。与之前枚举的结果完全一致。

★ ★ ★ ★ ★

附录二　本书符号记法常例

$a = b$	a 等于 b
$a \neq b$	a 不等于 b
$\{x \mid x$是偶数$\}$	偶数的集合
$x \in A$	x 属于集合 A
$x \notin A$	x 不属于集合 A
$A \subseteq B$	A 是 B 的子集
$A \subset B$	A 是 B 的真子集
$\varnothing$	空集
$\lvert A \rvert$	集合 A 的势

$\mathbb{N}$	自然数集
$\mathbb{Z}$	整数集
$\mathbb{Q}$	有理数集
$\mathbb{R}$	实数集
$\mathbb{Z}^+$	正整数集
$n\mathbb{Z}$	n 的倍数集合
$\mathbb{R}_0^+$	非负实数集

$(G,*)$	关于运算 $*$ 的群 G
$A \cong B$	A 同构于 B
$H \trianglelefteq G$	H 是 G 的子群
$H \triangleleft G$	H 是 G 的真子群
$H \trianglelefteqslant G$	H 是 G 的往合子群
$H \trianglelefteqslant G$	H 是 G 的真往合子群
$\mathrm{Ker}\,(\phi)$	群同态 ϕ 的核
$G\!\!\diagup\!\!_{H}$	H 除 G 的商群
$\langle x \rangle$	x 生成的群
aH, Ha	以 a 左乘、右乘集合 H
$a+H, H+a$	以 a 左加、右加集合 H
C_n	n 元循环群
D_n	正 n 边形的映轮群
S_n	n 元全置换群
S_X	X 上的全置换群
J_4	矩群
T_6	正方体旋转群
$A \times B$	A 与 B 的架积
$\mathsf{C}_m \times \mathsf{C}_n$	C_m 与 C_n 的架积
U_4	四元数群
$\mathbb{Z}_n$	模 n 同余系

$A \cap B$	A 和 B 的交集
$A \cup B$	A 和 B 的并集
$f : \mathbb{Z} \to \mathbb{R}$	f 是从 $\mathbb{Z}$ 到 $\mathbb{R}$ 的映射
$x \mapsto x + 1$	把 x 对应到 $x + 1$ 的映射
$f(x)$	x 经 f 映射的值
$f(A)$	集合 A 经 f 映射的像
$f \circ g$	函数 f 复合 g, $(f \circ g)(x) = f(g(x))$
$f^{(-1)}$	f 的逆映射
$\forall x \in A$	对集合 A 的任一元素 x
$\exists x \in A$	集合 A 中至少有一元素 x
a^{-1}	a 的（乘法）逆元
$\sum_{x \in S}$	当 x 遍历集合 S 的求和
$[a; b]$	闭区间
$a \mid b$	a 整除 b
$a \nmid b$	a 不整除 b
$a \equiv b \pmod{n}$	a, b 模 n 同余
$\overline{k}$	同余类 k
$\triangle(a, b, c)$	a, b, c 的最大公约数
$\triangledown(a, b, c)$	a, b, c 的最小公倍数
$n!$	n 的阶乘

$\mathcal{O}_G(X)$	群 G 显于 X 的轨迹集合
$\mathcal{O}_G(x)$	群 G 在 x 的轨迹
G_x	群 G 关于 x 的定子集
X^g	群元素 g 在 X 上的定元集
$G^{\text{心}}$	群 G 的中心
$\text{大}(x,y)$	x 和 y 的较大者
$\text{小}(x,y)$	x 和 y 的较小者
$\mathbb{K}[x]$	$\mathbb{K}$ 系数整式的集合
$\mathbb{K}_n[x]$	次数不超过 n 的 $\mathbb{K}$ 系数整式
$\imath$	虚数单位[①]
$\mathbb{C}$	复数域
$\square$	证明完毕

[①]读作“埃”。

附录三　术语对照表

以下是本书涉及的核心术语及其与主流中文、英文、法文术语的对照，并附上部分术语的命名释义。

术语	**中文**	**英文**	**法文**
群	群	group	groupe
子群	子群	subgroup	sous-groupe
往合子群	正规子群	normal subgroup	sous-groupe normal
往集	陪集	coset	coset
往集定理、群势定理	拉格朗日定理	Lagrange's theorem	théorème de Lagrange
往复、同轨	共轭（群）	conjugate	conjugué
同轨类	共轭类	conjugacy class	classe de conjugaison
群的架积	群的直积	direct product of groups	produit direct des groupes
轨迹	轨道	orbit	orbite
轨道	轨道	orbit	orbite
环道	轨道	orbit	orbite

续下页

表 三.1 – 续前页

术语	中文	英文	法文
环圈	轮换	cycle of a permutation	cycle d'une permutation
群观、群相	群作用	group action	action de groupe
有效、显明相	忠实的	faithful, effective	fidèle, effective
行健、显行相	自由的	free	libre
贯通、显通相	传递的	transitive	transitive
得宜、显实相	正则的	regular, sharply transitive	simplement transitive
全置换群	对称群	symmetric group	groupe symétrique
对称群	对称变换群	symmetry transformation group, symmetry group	groupe de symétrie
置换群定理	凯莱定理	Cayley's theorem	théorème de Cayley
轨定定理	轨道-稳定化子定理	orbit-stabilizer theorem	relation orbite-stabilisateur
定元分轨定理	伯恩赛德引理	Burnside's lemma	formule de Burnside
染色计数定理	波利亚计数定理	Pólya's enumeration theorem	théorème de dénombrement de Pólya
映轮群	二面体群	dihedral group	groupe diédral
组架坐标系	笛卡尔坐标系	Cartesian coordinate system	système de coordonnées cartésiennes

续下页

表 三.1 – 续前页

术语	中文	英文	法文
架积	笛卡尔积	Cartesian product	produit cartésien
契义	是良定义的	to be well-defined	être bien défini
契义	良定义的	well-defined	bien défini
保距映射	等距映射	isometry	isométrie

部分术语命名解释

- **“对称群”和“置换群”**：这些名称的指代关系在英语、法语等语言中也有些模糊。Symmetric group 指某个集合上所有置换（到自身的双射）的集合，代表了该集合的对称性。permutation group 或 group of permutation(s) 则指“由置换构成的群”。所以 symmetric group 是一种 permutation group；permutation group 一般是 symmetric group 的子群。为了顾名思义，我们将 symmetric group 命名为“全置换群”，这样“全置换群就是全部置换构成的群”，“置换群是全置换群的子群”就容易理解了。“对称群”则被用来作两种称呼，一种保留为全置换群的别称，一种对应保持某个几何对象性质的变换群的称呼，即对应 symmetry (transformation) group，group of symmetry(ies) 等。
- **“群观”和“群相”**：随着中文重命名程度加深，我们认识到单单建立术语之间的映射表已经不够了。因为术语背后是使用者对数学概念的观念和理解。主流中文术语只是单纯地、机械地翻译个别名词术语，所以不需要考虑这一点。但如果从整体系统的认知开始用中文命名数学概念，就会发现：动词、形容词也应该随之匹配，才能一致地、系统地表达整个思想。比如我们把群作用（group action）这个概念用中文重新审视，就会发现 group action 的实质是通过把群元素视为在另一个集合上的变换，来显示、体现群的结构和功能。通过观察群的各个元素作用在集合上的现象，而理解群的本质。因此，我们要在整体上把这个观念、思想表达出来，就不能满足于把“群作用”改掉，而是要从各个方面着手，整个改掉相关的表达方式。详细内容见第七章“观群”。
- **“往复”、“同轨”和“共轭”**：群论中的“共轭”是字面翻译“conjugate”。因为在复数中用“共轭”来翻译“conjugate”，所以这里也沿用“共轭”了。但实际上无论是英文的“conjugate”，还是“共轭”，都没有准确表示群论中“gxg^{-1}”的意

涵。英文的“conjugate”仅仅是表示“这几个东西经过同一种变换相互得到，地位平等”，有一种“连襟”、“同袍”这样的含义。而法语则直接用“conjugué”，和法语中的“动词变位”一样，更为直白，表示“这几个东西隶属于同一类，通过变换而来，地位平等”。“共轭”也仅仅是试图翻译这一层意思：所谓“轭”，指的是古代牛车上放在并行的牛脖颈上的曲木，比喻像共轭的牛一样地位相等，但已经少了“通过变换可以互相得到”的一层意思。而由于没有像法语一样的使用场景，到了别的地方就更让人难以理解。毕竟复数的共轭只有一个，这里突然有好几个。而我们用牛耕田时一般共轭的牛马不会超过两头（【疏】服馬有二，一馬有一軶。軶者，厄馬領不得出也）。所以“共轭”有过强的二元对应意味，用在这里已经不太适合了。“往复”是直接从“gxg^{-1}”的本身角度命名。我们从群作用的角度来看，x 到 gx 其实可以看作“往左偏一步”，而右边再乘其逆元，就是试图“回来”（复）。如果 x 和 g 交换，那么就变回 x。但由于 x 和 g 未必交换，所以不一定能回到 x。而回不到 x 的情况下，就产生了一系列与 x 相关的元素，构成轨道。这就是这个作用的本质，所以命名为“往复”。一个群元素往复后，不再是自己，而“走出”了一条轨道。这就是群轨道的特性：它是同一个元素经过不同方式“往复”得到的集合。而经过往复得到的等价关系叫做同轨关系，其等价类就是同轨类。因此群论的这个地方，用“同轨”代替“共轭”。

- **“往集”、“往复”和“往合”**：群论中的这几个词都是根据其对象的内在关联而命名的。“往”就是强调“走出”、“离开原位”，“往某个地方走”。而从 x 到 gx，就是通过 g 的左乘往 gx 走了。所以我们可以说“x 往左乘 g 得到 gx”。而对某个子集的所有元素都这么“往左乘 g”，就得到了其往集。“往复”则是在“往”之后试图“恢复”、“复原”，也就是往右乘 g 的逆元。但由于群元素未必交换，所以不一定能复原，而得到了轨道。“往合”则是说往左乘 g 和往右乘 g 的效果在总体上对合了。之所以用“合”而不是“等”、“同”，就是因为只是整体效果相同（$aH = Ha$，同一个集合），而不是严格地对等（$ax = xa$）。比“往合”更强的是条件是中心，即严格有 $ax = xa$。
- **“明相”、“行相”、“通相”和“实相”**：这些名词用来形容群作用的性质，对应选择的形容词（表语）为“有效”、“行健”、“贯通”、“得宜”。英语中只有形容词，分别是“faithful/effective”、“free”、“transitive”、“regular/sharply transitive”。要注意的是外语用词已经用了譬喻和类比手法，使用了有带感情或价值含义的用词如“faithful”、“free”。中文主流用语分别是“忠实的”、“自由的”、“传递的”、“正则的”，基本是字面翻译，导致词不达意，难以顾名思义。比如“transitive”照字面翻译成“传递的”，中文的“传递”一般并不用作形容词，导致“传递的”到底

想表达什么性质让人费解。而“贯通”则直接说明“transitive”的本义，即从一个元素出发不断变换就能贯通整个集合，名词“通相”的“通”就概括了其本质。又比如“free”本身就过于空泛，照字面翻译翻译为“自由”更恶化了这个问题。而“行健”取自“天行健”出自《周易 · 乾卦 · 象传》，表示整个天球永恒运动，所有星辰都一刻不息，恰到好处地说明了“除了最核心的幺元以外所有的群元素都在变动所有的集合元素，没有止息”这个性质。同理“regular”这个本就空泛的词被字面翻译为“正则”，再次让人费解。而“得宜”和“实相”的“实”则说明每个集合元素恰被一个群元素变为另一个集合元素的性质，即“适宜而确实”。《说文》:“宜，所安也”,《左传》:“宜，和顺之意也”。“faithful”这个词本来就不太恰当，词义过强，更适合用来描述 regular action。字面翻译为“忠实”更是容易让人误解。我们采用“有效”（来自“effective”）和“明”来命名，强调所有群元素都至少有一点效果，能通过群作用被观察到，整个群都被摆在明处，没有藏在暗处完全不起效果的元素。

- **“轨迹”和“轨道”**：两者都是我们给群论中“orbit”的中文对应新命名。前者是群作用于一般集合时，不同群元素作用于同一个集合元素得到的集合。后者是群以（共轭）作用于自身时，群元素的 orbit。因此我们决定把两者分开命名。把前者称为“轨迹”，表示群在另一个集合里留下的痕迹；而把后者（一种特殊而重要的群自身的 orbit）继续称为轨道，因为它是属于群自身的结构。“群的轨迹”指一般在某个集合留下的痕迹，通过这个痕迹可以理解群的性质。而“群元素的轨道”指这个群元素在共轭作用下得出的结构，是群自身的结构。“轨道”这个名字更偏重实体存在，而“轨迹”则有“留在别的东西上的痕迹”的意义。
- **“环道”和“轨道”**：两者都是我们给群论中“orbit”的中文对应新命名。前者是群元素生成的循环子群的形象说法，后者是群以（共轭）作用于自身时，群元素的 orbit。因此我们决定把两者分开命名。
- **“环圈”和“轮换”**：“轮换”是中文用来称呼置换性质的名词，通常有两个含义。一个是某个 i 经置换重复映射得到的所有值，即 n 元置换群自然作用于 $1, 2, ..., n$ 集合时，置换生成的循环子群作用于集合中元素的轨道。另一个含义是只有一个这样的非平凡轨道的置换。因此我们决定把两者分开命名，前者称为“环圈”，后者称为“轮换”。一个轮换恰有一个（非平凡的）环圈。一般的置换则可以有多个环圈，由多个轮换复合而成。在充分理解其关系后，在不至于混淆的情况下，才能以修辞手法的方式，把轮换称为环圈或反过来。