Visual Group Theory

群论——可视化方法

作者: Nathan Carter

翻译: 333



2018 年 7 月 25 日



微信公众号

前言

别人关心你飞的有多高，我只关心你好不好吃！

目 录

前言 **i**

概览 **vi**

第一章 什么是群？ **1**

1.1 一个著名的玩具 1

1.2 考虑这个方块 2

1.3 对称性的研究 3

1.4 群的规则 4

第二章 群长什么样子？ **6**

2.1 制图 6

2.2 一个不太著名的玩具 9

2.3 给群做一个地图 10

2.4 凯莱图 13

2.5 多一点抽象 14

第三章 为什么要研究群？ **18**

3.1 对称现象的群 18

3.1.1 分子的形状 22

3.1.2 晶体学 24

3.1.3 建筑与艺术 25

3.2 作用的群 28

3.2.1 舞蹈 29

3.2.2 多项式的根 30

3.3 无处不在的群 31

第四章　最后，再来点代数　33
4.1　操作都去哪了？ 33
4.2　复合，复合，复合 36
4.3　乘法表 37
4.4　经典定义 39
4.4.1　结合律 41
4.4.2　逆元 42
4.4.3　全都放到一起 44
4.5　之前，现在，之后 44

第五章　五大家族　46
5.1　循环群 48
5.1.1　旋转 48
5.1.2　乘法表和剩余类加法 49
5.1.3　轨道 51
5.1.4　引入循环图 52
5.2　阿贝尔群 53
5.2.1　凯莱图的非交换特征 53
5.2.2　乘法表的交换特征 55
5.2.3　盘曲的循环图 56
5.3　二面体群 58
5.3.1　翻转与旋转 58
5.3.2　D_n 的凯莱图 59
5.3.3　D_n 的乘法表 60
5.3.4　第七章的一个预告 61
5.3.5　D_n 的循环图 62
5.4　对称群与交错群 63
5.4.1　置换 63
5.4.2　置换群 64
5.4.3　正多面体 66
5.4.4　凯莱定理 69
5.4.5　本章小结 71

第六章 子群 **73**
6.1 乘法表说了什么？ 74
6.1.1 完善之前的定义 75
6.2 初见子群 76
6.3 窥探子群 77
6.4 陪集 78
6.5 拉格朗日定理 82

第七章 积与商 **86**
7.1 直积 87
7.1.1 构建直积 88
7.1.2 更多直积的例子 91
7.1.3 为什么需要直积？ 92
7.1.4 从代数的角度来看 95
7.2 半直积 98
7.3 正规子群与商运算 102
7.4 正规化子 110
7.5 共轭 115

第八章 同态映射的力量 **120**
8.1 嵌入与商映射 120
8.1.1 嵌入映射 127
8.1.2 商映射 127
8.2 群同态基本定理 132
8.3 模的算术 134
8.4 直积与互素 139
8.5 阿贝尔群基本定理 142

概览

这里，我要强调这本书在三个方面有别于寻常的群论书籍，并简单介绍一下它的组织构成。

首先，图片和可视化的例子是本书的灵魂。全书有超过 300 张图片，平均下来每页超过一张。主要的可视化工具是凯莱图 (Cayley digram)，将在第二章定义，因为它们可以如实的、清晰地反映群的结构。但是乘法表 (multiplication table) 以及其他的一些具有对称性的对象也会时不时的出现，比如循环图 (cycle graph)、海色图 (Hasse diagrams), 作用图 (action diagram)，同态图 (homomorphism diagrams) 等等。正如你随手翻开此书都可以看见各种图，可视化是我们这场游戏的名字。

其次，相比于无限群，我将更多地关注有限群。部分原因是有限群更容易作图，不过更重要的原因是它给我们在更一般意义上理解群论奠定了坚实的直觉基础。理解好有限群，会使得无限的情况仅仅只是一种自然的推广。这样的处理几乎不会牺牲掉什么，如果有，那也是不得已，因为有限的乐园里有着太多尚待研究的问题。本书中，我会提及最常见的几种无限群，每一章后的练习也包含了一些关于无限群的题目。

最后，这本书处理群论的手法恰好和许多传统教科书的顺序相反。通常的教科书模式是将群定义为一个带有二元运算的集合，然后证明凯莱定理，即每一个群都是一系列的置换。本书中，直到第四章都不会出现这种传统的定义；我在第一章中将群定义为一系列的作用 (action), 之后证明它们也可以视为带有二元运算的集合。这种非标准形式的定义有助于我在第二章引入凯莱图，一种将群刻画为一系列的作用的图。

本书的结构是线性的，需要按顺序阅读；之后的章节通常依赖于前面的章节。不过，有两个例外。第五章，宽泛地介绍了几种有限群，这对于后续内容是有帮助的但不是必须的。你大可以跳过其中的大部分内容 (除了 5.2 中关于交换性 (Abelian) 的定义)，在有需要的时候再翻过来看一看。另一个例外是第十章，它稍微要用到第九章；9.2 中的柯西定理在 10.7 中有用处。第九章的其余部分可能对于第十章的部分习题有所帮助。

第十章是关于伽罗瓦理论的，旨在展示群论的力量以及它的一些历史根源。这一章包括了一些域论的介绍，但是其中的几个定理只简单陈述不作证明，以让我们充分理解群论跟哪些东西紧密相连，并指导读者进一步探索域论的更多细节。美丽而富有历史传奇色彩的关于高次多项式方程不可解的结果将是这最终章的焦点和终点。

1

什么是群？

1.1 一个著名的玩具

1974 年，匈牙利布达佩斯的 Erno Rubik 发布了他那引人入胜的发明：魔方。它立刻渗入进了流行文化，出现在故事片中，激发了各种比赛，迷住了孩子们和各路英才，数学期刊刊发研究论文。无法复原魔方的人们也可以在各种各样的书籍中习得它的解法。

如图 1.1那样的新式魔方很快出现。正方体的每个面包含了 9 个小正方形面，并被涂了颜色以示区分。你只需先随便旋转这 6 个面，之后你就可以开始玩了。图 1.2展示了相继施加两个不同的旋转是如何打乱魔方的。只需无所事事地瞎拧几分钟，一个天真的家伙 (比如你) 就会发现颜色彻底被打乱了，而且并没有什么明显的方法能将它恢复成原样。挑战就是如何将一个打乱的魔方恢复为原始状态。



Figure 1.1. An untouched Rubik's Cube

图 1.1

魔方在各种拼图玩具和智力游戏中都享有特别的声誉，这其中很大一部分源于它本身内在所具有的数学模式。乍一看这个方块跟数学什么关系都没有，因为玩魔方甚至是

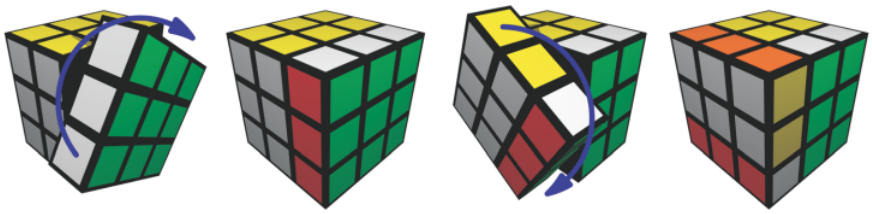


Figure 1.2. The leftmost cube shows the green face rotating 90 degrees clockwise; the next cube shows the result of that move. The third cube shows the white face rotating 90 degrees clockwise; the final cube shows the result of that move.

图 1.2

还原魔方根本用不到任何比如数字啊，方程啊或者数量这些东西。但是，这只是因为我们这本书中涉及的数学，群论，并不是主要跟数字打交道；它是关于模式的数学。群论研究对称性，这种对称性在魔方中不仅体现在这个正方体本身，还存在于它的运动之中。

“Easy to learn, a challenge to master”是 Erno Rubik 发明的好几个智力玩具所采用的市场宣传口号。这句宣传标语非常恰当地描述了魔方。通过考察为何如此将是我们的群论研究之旅的一个很好的开始。在这一章中，我们将会考察是什么使得魔方“Easy to learn”；在第二章中，我们将关注又是什么让它“a challenge to master”。

1.2　考虑这个方块

为了探索为什么魔方很容易上手，让我们先作几个观察。

从部分来看，魔方之所以很容易上手是因为玩家不用事先学习一套复杂的规则。与之相比，想下棋的玩家首先必须得掌握每个棋子的不同的规则，更糟的是，在游戏过程中，有些本来合理的棋子移动会变成不合理。魔方没有这么复杂；我们甚至可以说它只有六种运动——每个面顺时针旋转 90 度 1。通过组合这六种运动，玩家可以探索魔方的全部可能状态。这种易操作导致我们得到了关于魔方的第一个观察。

观察 1.1. *存在事先给定的一系列基本运动，并且这些基本运动永远不会改变。*

另一个我们都同意的事实是，魔方允许你犯错并改正。如果一个玩家旋转了一个面，但是立刻就后悔了，这并没什么大不了的。玩家只需逆着刚才的旋转操作把那一面再转回去就能纠正自己的错误了。这就是我们的第二个观察。

观察 1.2. *每个运动都可逆。*

关于魔方，另一个有帮助的事实可能不那么容易注意到，但是和其它的游戏一比就清楚了：魔方是一个跟机会和运气无关的游戏。一个网球运动员可能全神贯注的击好每

一个球，但是当他们的身体到了极限无法再执行他们的想法时，他就不能再做到这一点。一个扑克牌玩家可能有一个绝妙的策略，但是如果手上发到的牌太烂他们还是会输。不确定性和运气的存在赋予一个游戏别样的风味，但是在魔方中，不存在这样的特点。旋转一个面带来的结果是可预见的，既不靠技术也不靠运气。一个作用 (action)，如果它的结果可以事先确定，不会受到随机性因素的干扰，我们称之为确定性的。

观察 1.3. 每一个运动都是确定性的。

但是我们必须要公平。独立地看，这些观察似乎表明魔方并没有什么复杂性。为了给出一个准确的说法，我们必须承认貌似无限种可能的运动的组合，才使得魔方富有挑战性。

观察 1.4. 运动可以按任何顺序组合。

请注意观察 1.2对于观察 1.4的影响。如果有一个玩家极其得小心谨慎，把他或她所做的每一次运动都列在了纸上，那么不管这一列运动有多少，都可以被一次一个地、仔细地复原。

1.3 对称性的研究

除了上述四条观察以外，我们还可以加入很多别的观察。比如我们可以提及面的颜色，立方体的物理结构，还原所需的步数，或者其他一些关于游戏的方方面面以及你作为玩家的经验等等。但是我们将只关注以上列出来的四条，因为它们所体现出来的方面是最和我们这本书相关的。群论就是研究对称性，我们即将看到这四条观察是如何描述魔方的对称性。

我们称任意两个立方体是对称的，如果它们有完全相同的棱，完全相同的角和完全相同的边缘。不过对于魔方而言，由于可以旋转，这给它增加了额外的复杂性。而且由魔方所有可能的运动和构型所组成的集合也极具对称性。要想清晰地解释这一点，我们得先知道“对称”到底是什么。

这个问题引领我们来到了这本书的门口，因为群论正是能够回答这一问题的一个数学分支，“什么是对称？”本书的前三章会通过引入群这一概念并展示如何用群描述对称，对此问题给出一个很细致耐心的答案。(你都说了好几遍了) 群在哪呢？别急——魔方就是第一个即将展示物体与模式 (pattern) 的对称性的例子。随着分析的进行，我们也会同时学习群论。后面的章节还会带领我们探索其它的关于对称性的实例，包括分子晶体和舞蹈。

但是我们并不会局限于只看一些对称物体的例子。我们的研究也会用到许多别的工具；这本书的目的就是关注那些能够帮助我们可视化的工具。这其中包括常见的群论工具如乘法表 (multiplication table)，还有不那么常见的凯莱图 (Cayley diagram) 和循环图 (cycle graph)。在接下来的章节中，我会一一介绍。

从第二章开始，你会接触一些对称的对象 (object)。有些是客观物体，有些是客观物体的作用 (action) 或行为 (behavior), 还有些纯粹只是我们想象出来的。共同之处就是，它们全部适用1.2到1.4。群论研究那些观察所产生的数学结果，因此它能够帮忙回答一些关于对称对象的有趣问题，比如，魔方有多少种不同的构型？不过在本书中我们不会来计算这个数目，感兴趣的读者可以参考 [21]。

1.4　群的规则

现在让我们重新回到那些观察上来，它们是群论的基石。但是，这里我们不局限于把它们仅仅当作是对魔方的描述。让我们重新组织一下语言，把那些观察变成一条条的规则 (rules) 以明确定义我们的研究范围。这种引入的方式是很典型的数学风格。先给定一堆规则，然后数学家们就着手研究遵循这些规则的事物。这些规则我们有专门的数学术语来称呼，叫作公理 (axiom)。不过只要我们的讨论还是非正式的，我就还将一直叫它们规则。

定下这些规则会带来一些显著的好处。首先，这使得我们的研究范围得以清晰。符合下面即将引入的这些规则的事物就是群论的研究对象，不符合的就不是。其次，由于要在数学社区一起生活一阵子，事先制定一些大家都认同的规则能保证我们以后讨论一个对象时不会产生分歧。换句话说，把我们的想法厘清成规则可以让我们用一种语言说话，最大限度地减少交流障碍。最后，我们可以以这些规则为基础进行逻辑推导，进而挖掘一些新的事实 (这些新的事实往往是单独地考察所无法预料到的)。我们上面提到的计算魔方的构型数量就是这样的一种事实。在本章的练习中你可以自己作一些推导。

现在就让我们把关于魔方的那些观察重新表述为规则。正如上文所说，要把这些规则看成是我们要研究的对象所必须满足的要求。

规则 1.5. 存在一些预先定义的永不发生改变的作用（*action*）。

规则 1.6. 每一个作用都可逆。

规则 1.7. 每个作用都是确定性的。

规则 1.8. 任意的一系列连续的作用仍然是一个作用。

我的重述只有两个变动。第一个，我把“运动 (move)”这个词换成了“作用 (action)”，以便让它看起来不那么像一个游戏。在之前魔方的内容中，用“运动”是合适的，但是我并不想把我们的注意力局限在游戏方面。第二个，在表述规则 1.8时，我把规则 1.4变得更专业了一些；不仅仅是可能的一列作用，更进一步，我把任意的一列作用都一视同仁地称为作用。这并不意味着这些作用必须得出现在规则 1.5所说的那些基本作用里面；而是说1.5中的基本作用是我们的起始出发点，通过运用规则 1.8，把这些基本作用像链条一样一节一节地连在一起来创造新的作用。

在魔方的例子中，尽管我只列出了六个基本作用，然而你可以通过组合它们来得到任何你想要的效果。举个简单的例子，把魔方正前面的面进行两次 90 度旋转就得到了一个新的作用——把正前面旋转 180 度。通过组合基本作用，你可以得到更多更复杂的作用。标准说法是，规则 1.5中的那些作用生成 (generate) 了所有其它的作用, 因此我们称之为生成元。

现在我们准备给出第一个定义，这标志着你正式进入了群论的学习。这并非是通常所见的群的数学定义，但是表达的意思是相同的，以后我们会明白这一点。现在让我们暂时地把它叫作非正式定义。

定义 1.9 (群，非正式的)**.** 一个群就是一个满足规则 *1.5*到规则 *1.8*的作用的集合。

也许你现在想知道除了魔方之外，究竟还有什么东西能满足这个定义？有什么能被称为群？正如我们将在第二章和第三章看到的，任何具有对称性的对象都满足规则 1.5到规则 1.8，这其中包括大量的自然科学、艺术和数学中的对象。

2

群长什么样子？

2.1　制图

第一章通过检查魔方的一些性质引入了群的概念，这可以很好地吸引小白读者的兴趣。让我们现在开始增加点难度。

假设你手里有一个乱掉的魔方，并且你不知道要怎么样才还原它，试验性地快速转动那些面似乎起不了什么作用，因为你是在魔方众多可能的构型中漫无目的地游荡。在这一片又一片混乱贫瘠的荒野中只有一处是你一直在寻找的绿洲——被还原的那个状态。然而，不知道自己身处何方，不知道绿洲又在何处，你甚至都不知道自己走的方向是什么。你所面对的是一个希望渺茫的处境。

对于一个迷失在魔方荒野中的人来说，最有帮助的莫过于一张地图——可以告诉你“你在这”，“答案在那”，并且能明确的指给你到达那个地方的路要怎么走。这样一张地图能解决你所有的导航问题。有了这样一张地图，任何人都可以轻松的还原魔方 (尽管这样会比较没意思)。

有许多关于魔方的书会教读者还原的技巧，也有一些专业的学术文献利用群论对魔方进行仔细的分析 [21]。在这里，我的目标并不是简单重复他人的这些工作来给你们提供一张“魔方荒野地图”。取而代之的是，我想带领读者做一个思想实验，告诉你们这样一张地图应该包含哪些细节，或者说它应该是什么样子的。它不应该只是一种指导你如何还原魔方的技巧，而应是一张包含了魔方所有可能的构型以及这些构型彼此之间的联系的详尽无比的地图。显然一张寻常大小的地图是无法包含这么多信息的，所以让我们编一本“巨大的书”吧！因为这只是一个思想实验，所以我们不妨就把这本书叫作“大书”，接下来就是考虑这本书里需要包含哪些内容。

想象一下，你有一个混乱的魔方以及一本“大书”。“大书”首先应该能够帮助你确定你正处在荒野的哪个位置。为了实现这一点，我们将“大书”编排成一页一个魔方构型的版式，并用类似于字典的方式来排列这些书页。正如首字母为 a 的字在字典中被放在一起，我们也许可以将所有立方体的上面左上角为红色块的魔方构型放在一起。这样排好了之后，再排接下来一小块的颜色，就像在字典中排单词的第二个字母一样，重复这个步骤直到排完所有的构型。其实这种组织方式的细节并不重要，因为毕竟这只是一个思想实验。为了方便“大书”的读者进行查找，我们就采用这样的排版方式吧 (虽然查起来需要极大的耐心和细心)。

现在让我们假设你已经在“大书”中找到了自己魔方所处的位置。那一页应该还提供一些导航帮助，具体细节最好用例子来展示。图 2.1展示了“大书”中的某一页。这一页显示了一个给定构型的所有面，前面和后面，并且告诉读者离还原状态还有多远。然后一张表格提供了一些导航信息；它告诉读者每一步操作会达到什么样的地方。举个例子，表格的第一行告诉我们如果把前面顺时针旋转将到达 36,131,793,510,312,058,964 这些页上的构型状态，它们都比目前的状态更接近还原状态。

你会发现这样一本书能够极大地帮助你还原魔方。一旦你找了魔方当前状态所在页，简单地按照书页上的导航信息操作一下你就能到达一个更接近还原的新状态，再翻到这新的一页。之后在新位置重复这样的步骤。你总是知道自己离还原状态还有多远，你可以把你的魔方和书页上的图仔细比对以确保你没有犯错。

大书”有一个显见的问题，你可能已经从图 2.1中察觉了这一点。魔方有超过 4×10^{19} 个可能的构型，这将让“大书”真的大到突破天际。或许我们可以每页多放几个构型状态，但是事实是，即使我们把每个构型状态压缩为 1 平方英寸 1 个，打印这本书所需的纸张仍可以覆盖地球表面好几次。把“大书”存储为电子书也无济于事；即使使用最高效的编码手段，也没有任何一台现存的计算机能够存储它。所以“大书”只能是一个思想实验，不过这一章的剩余部分将会表明这个思想实验的巨大价值。

“大书”教给我们的最重要的事情是，一张魔方荒野的地图事实上是一个群的地图。让我来解释一下，魔方的操作形成了一个群，因为它们满足定义 1.9（实际上，那些操作是我们接触到的群的第一个例子，正是由此启发了这个定义）。定义 1.9中的规则只涉及了魔方的操作和由此而来的组合操作。而“大书”包含了关于魔方操作和它们彼此间联系的全部信息，因此它就是一张群的地图。

所以，由我们对于“大书”的讨论而引入的造图 (mapmaking) 想法不应仅仅因为群（魔方的操作所构成的群）的规模太大而被简单地丢弃。我们完全可以运用同样的想法 (idea) 来给任意一个群制造“地图”。在下面一节中，我们正是这么做的。

Page 12, 574, 839, 257, 438, 957, 431

Cube front	Cube back
	

You are **15** steps from the solution.

Face	Direction	Destination page	Progress
Front	Clockwise	36, 131, 793, 510, 312, 058, 964	Closer to solved
Front	Counterclockwise	12, 374, 790, 983, 135, 543, 959	Farther from solved
Back	Clockwise	26, 852, 265, 690, 987, 257, 727	Closer to solved
Back	Counterclockwise	41, 528, 397, 002, 624, 663, 056	Farther from solved
Left	Clockwise	6, 250, 961, 334, 888, 779, 935	Closer to solved
Left	Counterclockwise	10, 986, 196, 967, 552, 472, 974	Farther from solved
Right	Clockwise	26, 342, 598, 151, 967, 155, 423	Farther from solved
Right	Counterclockwise	40, 126, 637, 877, 673, 696, 987	Closer to solved
Top	Clockwise	35, 275, 154, 257, 268, 472, 234	Closer to solved
Top	Counterclockwise	33, 478, 478, 689, 143, 786, 858	Farther from solved
Bottom	Clockwise	20, 625, 256, 145, 628, 342, 363	Farther from solved
Bottom	Counterclockwise	7, 978, 947, 168, 773, 308, 005	Closer to solved

Figure 2.1. Sample page from *The Big Book*

图 2.1

2.2 一个不太著名的玩具

让我给你们介绍一个跟魔方很像的小玩具。这个玩具很早就出现了，只不过名字没那么响亮。它叫矩形，我保证在此之前你肯定听说过它！几乎每个人早期的数学教育中都包含矩形的内容。为了方便，我把矩形的四个角标上了数字，如图 2.2. 首先应该注意到的是它要比魔方简单多了，因此有可能利用它来将我们的造图计划付诸实践。

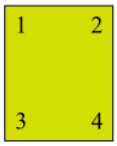


Figure 2.2. A rectangle with its corners numbered

图 2.2

不过首先，为了能完全理解接下来的讨论，你应该给自己做个像图 2.2那样的矩形玩具，。给自己做一个这样的玩具似乎有些多此一举，但是由于我们下面会对矩形进行一些翻转和旋转操作，光凭想象可能有点难以想象出它的形状。所以随便撕一张纸为你自己做一个带标号的矩形吧。

矩形的玩法规则在这儿。把矩形平放在一张桌子或你自己的膝盖上，方便你能看到像图 2.2那样的数字。跟魔方一样，矩形玩具从它的原始状态——你手里现在的形状，开始玩。打乱它的顺序，然后你的工作就是把它还原为原始状态。

我们规定矩形玩具只有两个合法操作。如图 2.3，你可以将它进行翻转，沿水平线或竖直线。在第三章，我会阐明为什么是这两种操作 (而不是别的) 对矩形来说是有意义的。不过现在，我们就权且将其当作游戏规则吧。正如魔方，你可以随心所欲地重复、组合这两个操作 (事实上，你可能已经注意到矩形的操作形成了一个群)。

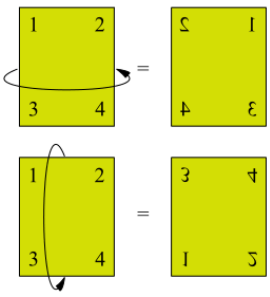


Figure 2.3. The top arrow illustrates a horizontal flip; the upper right rectangle shows the result of such a flip. The bottom arrow illustrates a vertical flip; the lower right rectangle shows the result of such a flip.

图 2.3

现在花点时间弄乱它，然后试着将它还原。这要不了多少时间，不过要保证你没有作弊（没按规定的两种操作进行）！一个典型的错误是，把矩形拿起来观察一番，然后就把它直接摆成了原样。。。注意这是不允许的！这样一个过程其实跟玩魔方很像。始终要记住，不管是在打乱还是在还原的过程中，你都只能使用图 2.3展示的那两种合法操作。

好了，让我们花点时间证明对矩形施加的操作确实形成了一个群，并将其与魔方相比较。规则 1.5要求要有事先给定的一组操作，我们这里已经有了：水平和竖直翻转。规则 1.6要求每个操作都可逆，这对于矩形玩具来说也是对的，因为每个翻转就是本身的逆。举个例子，如果你做了一次水平翻转，现在想将它恢复成翻转前的状态，只需要再做一次水平翻转即可。对于竖直翻转同样如此。规则 1.7要求这些操作都是确定性的，不存在随机性；在这里这些操作完全由你控制，当然是确定的。规则 1.8要求这些操作的任何可能的组合仍是一个合法操作；这也是满足的，因为一个水平或竖直翻转将矩形变到一个物理位置，从这个位置仍可以对矩形施加水平或竖直操作。与之相比，如果我们加入这样一个操作“把矩形撕碎并扔掉”，这会导致游戏终结：因为再也做不了别的操作了。然而我们之前规定的两个操作并不存在这样的问题：它们总是允许进行下一步操作并因此允许我们把它们按任何顺序组合。

在下一节，我们将画出这个矩形群的地图。不过首先，注意比较它和魔方的物理构造。这个矩形玩具要求你把矩形放置在一个平面上来记录它的原始朝向，之后就是试着将其还原为这个状态 (原始朝向)。而魔方不是这样的，你可以在房间里随便扔，把它丢到装袜子的抽屉里，等你再拿起它的时候，它的构型并没有发生改变。因为魔方的运动枢纽藏在了它本身的内部，所以并不需要外部的参照物 (比如桌子，或是一个原始的朝向)。然而我们的矩形玩具仅仅就是一张纸片 diy 出来的，它没有运动枢纽，所以把它当作玩具就需要外界的参照物（比如桌子，或是你能记住的一个朝向）。我们完全可以设计一个跟矩形玩具表现得一模一样的新玩具，而且它也跟魔方一样是自包含 (self-contained) 的；只不过在家里做一个这样的玩具确实不太容易。

2.3　给群做一个地图

造图工作以探索开始。如果我们想给一个地方绘制地图，我们就需要先了解此地的地形地貌。因此让我们首先来探索一下这个矩形玩具的世界，一边走一边画。我们需要确保探索是彻底的——即找到了矩形玩具所有可能的构型——所以应当有条不紊地进行我们的探索研究。

从还原状态开始，如图 2.2，我们能用的工具只有水平和竖直这两种翻转操作。它们是群的生成元，我们的地图会展示这两种操作究竟是如何生成这个群的。

首先做一个水平翻转。由于我们的探索刚刚启程，因此这个操作必然会将我们带往一个还未发现的构型。不过在图 2.3中我们已经介绍过它的样子了。再做一个水平翻转，就又回到了还原状态，利用这个信息，让我们着手绘制地图。图 2.4展示了我们目前为止探索过的“地形”。在图中，我用双向箭头来表明从这两种构型的任一个开始，施加一个水平翻转都可以到达另一个构型。

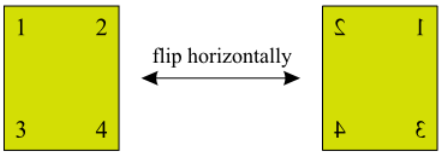


Figure 2.4. Partial map of the configurations of the rectangle puzzle, using only horizontal flips

图 2.4

这些构型是我们只用水平翻转就能获得的状态。继续借用探索这一比喻的说法，可以说我们在矩形玩具的世界中找到了两个地方，从其中任一个地方出发，图 2.4的地图就会告诉我们水平翻转会把我们带到何处。但是目前对于竖直翻转可以带我们去何处，还一无所知。此时的地图还不完整，所以我们得接着探索。

还是回到矩形的还原状态来探索竖直翻转的效果。图 2.3已经告诉我们竖直翻转能干什么，让我们彻底地探索那些状态并将它们添加到我们的地图中。从还原状态，一个竖直翻转带我们到了一个尚未到过的地方，再做一个竖直翻转又可以回到原地。图 2.5展示了我们的论断。

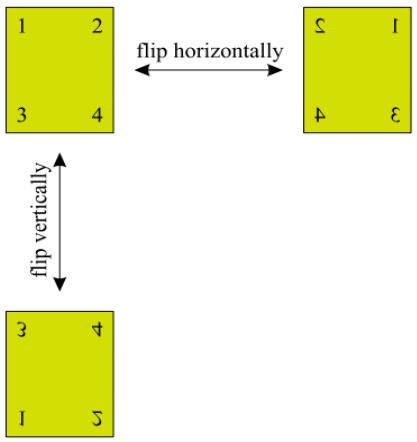


Figure 2.5. Partial map of the configurations of the rectangle puzzle, exploring from the solved state using one type of move at a time

图 2.5

我们的地图还是不完整，因为我们仍然不知道从图 2.5的右上角状态做一个竖直翻转会到达何处。为了能从那个状态开始探索，我们首先要把矩形摆成那个样子。如果你一直都在跟着做，那么只要从初始的还原状态做一个水平翻转就可以变成图 2.5右上角的样子——这正是地图告诉我们的！从那个状态开始，我们做一个竖直翻转，看看它将把我们带到哪里。这个操作的效果是目前为止第一个不能从图 2.3中事先预见的。自己动手试试，看看它把你带到了什么地方。是一个新的、我们必须添加到地图中去的地方？还是一个我们已经知道的？(从图 2.6中你可以找到答案)

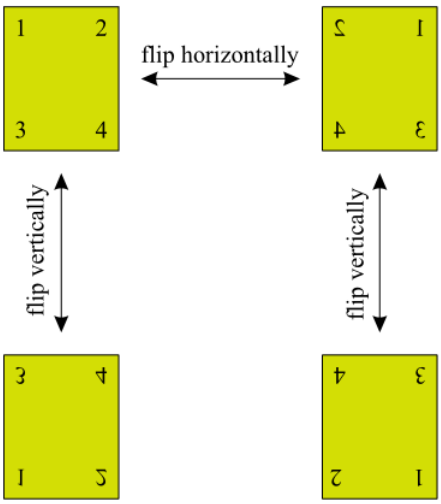


Figure 2.6. Partial map of the configurations of the rectangle puzzle, continuing to explore from Figure 2.5. The lower right state shown in this map does not appear in Figure 2.3.

图 2.6

图 2.6包含了矩形的四个状态，但是下面的两个状态还没有水平翻转的箭头从它们出发或到达它们。因此，我们的地图仍然不完整。举个例子，如果你的矩形是像图 2.6中左下角那样的，那么一个水平翻转将会带你到哪呢？地图没说，我们还得接着工作。

用地图来帮助，把你手边的矩形变成图 2.6左下角的状态，接着做一个水平翻转，看看结果是什么。结果并不是一个新的构型：它与我们刚刚发现的那个构型是一样的。如果再做一个水平翻转，显然你又回到了图 2.6左下角的状态。终极版的地图是图 2.7那样的。现在我们总算可以说，我们的探索是完整无缺的了，因为不会再有尚未被回答的问题。从任何一个位置出发，从地图中都能清楚地看出一个给定的操作会带我们到达何方。

你刚创造了你的第一个群的地图！然而，我们不得不承认图 2.7中的地图有点多此一举，因为即使没有一张地图，这个矩形玩具也很容易恢复原样。不过地图确实精确地向我们展示了矩形玩具的结构，也让我们明白了它为什么如此简单 (举个例子，从地图

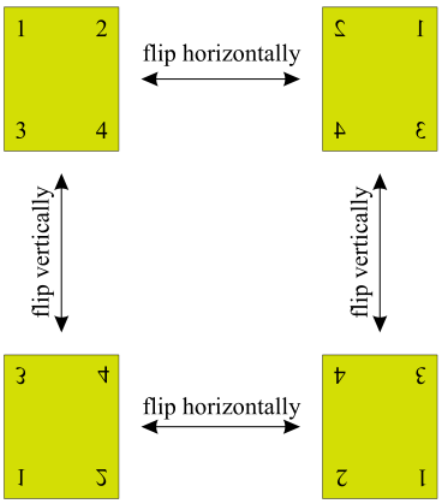


Figure 2.7. Full map of the configurations of the rectangle puzzle

图 2.7

中你可以看出，交替使用水平和竖直翻转可以带你逛遍矩形玩具世界中的每一个地方). 这张地图也是如何给群制作地图的第一个极好的示范；同时在我们即将接触更复杂的群之前，也让我们得以在实践中先练练手。

2.4　凯莱图

像图 2.7那样的图被称为凯莱图，以它们的发明者——19 世纪英国数学家亚瑟 • 凯莱的名字命名。我们将在整本书中广泛地使用凯莱图；这些图是非常强有力的可视化工具。作为开始，我们来说明一些关于凯莱图的重要事实，这对于以后的理解会有帮助。就我们之前的矩形玩具而言，凯莱图的这些事实看起来很显然甚至有点乏味，因为矩形玩具是在是太过简单了。但是我们将会给更多更复杂的群制作凯莱图，这些事实对于这些复杂的群来说仍然成立。

图 2.7给出了矩形玩具世界的详细地图，使得我们能够去往任何地方而不必作出任何主观臆测。举个例子，假设你想从右下角的状态走到还原状态。从地图中可以看出，你有两条路可走（先向上再向左或者先向左再向上）。为了充分利用这张地图，当你用手或眼循着这两条路径的时候，你可以拿出你的矩形，跟着箭头上的指示动手试试。从右下角的状态向上意味着将你的矩形竖直翻转；向左意味着水平翻转。这样的做法能够成功指引你前往你心中想去的任何地方；因为地图已经帮你计划好了旅程。

记得吗？我们费了一番脑筋以确保图 2.7是完整的：矩形世界里的每个地方都出现在了地图中，没有被漏掉的。这一点可以由我们构建地图的过程保证。运用生成元，我

们在开始位置产生岔道，之后再一次运用这些生成元产生新的路。如果玩具足够复杂，我们就可以持续的进行以上过程，探索出更远更宽广的天地，直到我们发现这个世界的每一个角落。如果我们的地图无法回答像“从现在的位置开始，一个水平翻转会把我带到哪里呢？”这样的问题，那我们就知道地图尚不完整。也就是说，如果你的地图中存在一个地方，没能包含所有可能的路径从此开始可以抵达的地方，那么你的地图就是不完整的。当所有问题都能回答时，地图也就完整了。

因此，凯莱图拥有我们刚在上面讨论的两个重要性质：包含所有可能的路径和构型（即上面所说的“地方”）。正如矩形玩具有一张地图，任何一个的群也有属于自己的满足这两条性质的地图。从现在开始，我将用用正式的名字来称呼这些地图：凯莱图。凯莱图最有用的方面就在于它能够清晰地展示一个群的结构。观察一张凯莱图，我们可以直观而完整的获得关于一个群的相关信息，比如它的大小，复杂程度以及结构等，这比枯燥的文字描述要有趣和容易的多。我们此后学习群的过程中会频繁凯莱图，原因也正是如此。

你可以按照我们制作图 2.7的方法给任意一个群画一个凯莱图。随便取定一个构型或位置，从它开始，每次用一个生成元仔细地探索，探索一定要彻底和仔细。随着你的进程，慢慢画图，并在两个状态之间标明过渡操作。一直继续下去，直到包含上面要求中的所有地点和路径。尽管图 2.4到图 2.7画得很漂亮，不过你第一次画凯莱图很可能会搞得一团糟。当你每次探索出一个新的地方，凯莱图就会乱一点，因为你不可能提前知道如何安排这些连线是最简洁美观的。通过探索画出的凯莱图，在探索完成后，往往需要二次美化，以使得它更对称、更美观。

这一章后的习题鼓励你使用这种探索技术来画几张凯莱图。在亲自体验了这种“制作地图”的感觉后，你将对之前的段落有新的领会。你完全可以现在就翻到后面的习题，先做几道练习，再回过来读接下来的内容。

2.5　多一点抽象

对于刚刚学习的“制作地图”的概念，我们来看看它的本质究竟是什么？这一点对于后续学习很重要。定义 1.9阐述得很清楚，对于一个群而言，重要的是它里面那些“作用 (action)”的相互叠加，至于具体导致这些作用的那些具体情境则并不重要。让我用一个例子来解释这一点。我们想象墙上有两个靠在一起的开关。你被允许做两种操作：拨第一个开关和拨第二个开关。由这两个操作叠加出的所有可能的操作生成了一个群；你可以用群的定义来检查一下。这个群的地图如图 2.8所示。

你会注意到，这张地图跟前面矩形玩具的地图，图 2.7，有完全相同的结构。矩形中

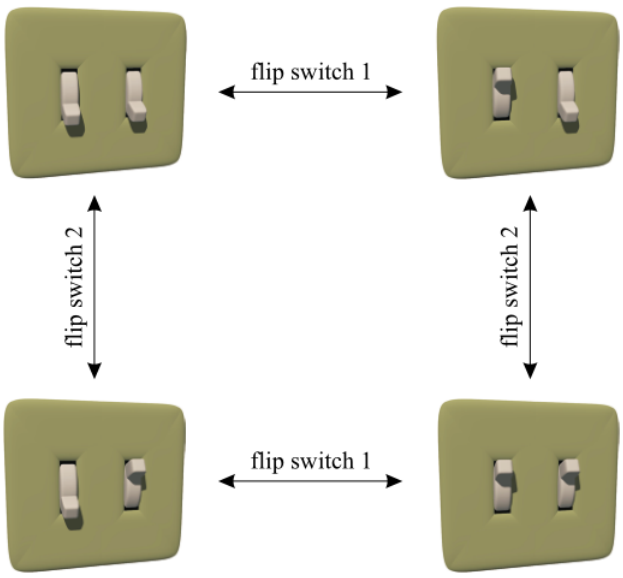


Figure 2.8. Full map of the configurations of the two-light switch group

图 2.8

的四个构型在这里变成了开关的四种状态，而箭头“水平翻转”和“竖直翻转”则变成了箭头“拨开关 1”和“拨开关 2”。但是这些箭头连接四种状态的方式仍与前面一样，这就导致图 2.7和图 2.8几乎是一样的。

所以，尽管这两个群具有表面上的不同，但它们内在的结构却是完全相同。这就启发我们两个不同的群有可能拥有一样的结构，并且这一点是可以从它们的凯莱图清楚地看出来的。因此，为了能够抽象的研究群，我们希望抹去凯莱图的一些细节，也就是说忽略它们所处的具体情境。毕竟，群是一个数学上的结构，数学家们是用抽象的 (纯数学的) 手段来研究群。矩形玩具和开关的例子只是帮助我们用具体的、熟悉的东西来理解抽象事物的一种途径。

所以让我们把图 2.7中的那些矩形用一些没什么具体意义的东西替代，比如说点，我们称之为“节点 (node)”；同时将两种不同的箭头 (由箭头上的标签“水平翻转”“竖直翻转”可以区分) 用不同颜色的连线箭头来替代，这样就不必在箭头上做文字标记了 (事实上还可以进一步简化，把箭头都可以去掉，因为图中所有箭头都是双向的；在以后，我仍会将不带箭头的连线称作“箭头”)。图 2.9所示的结果，一个群的凯莱图，现在以完全没有任何装饰的样子呈现在我们面前。你会发现，图 2.9展示的结构不仅是图 2.7的本质结构，同时也是图 2.8的本质结构。

图 2.9显示的群叫作克莱因四元群 (Klein 4-group). 我之所以选择它作为我们可视化的第一个群，是因为它足够简单，我们能够很快、很容易的画出，同时它还有一些有趣

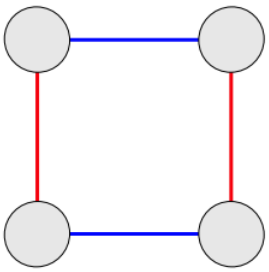


Figure 2.9. Cayley diagram of the Klein 4-group

图 2.9

的结构。图 2.10展示了几个其他的凯莱图，这可以拓宽你对于群的认识，并且给你个机会近距离的瞧瞧它们往往长什么样子。正如你所见，有些非常简单，有些则可能非常复杂。凯莱图的多样性也暗示了它们背后那些群的复杂性。你无须感觉好像你必须现在就要理解图 2.10的每一部分；我们将在以后陆续碰到这些群。

我对于群论可视化的研究兴趣促使我开发了 Group Explorer 这个软件，这是一个可以画凯莱图（以及其他的一些图示工具，在后面我们会陆续介绍）的免费软件包。Group Explorer 可以跟这本书配套使用，你可以从`http://groupexplorer.sourceforge.net`.这个网站下载。它内置了一系列的群以及各个群的拓展知识，每个群都至少有一张凯莱图。Group Explorer 创作凯莱图的算法跟我们之前例子中的步骤非常类似——它使用群的规则来产生箭头，不断探索每一个角落，直到它发现了所有的地方，然后自动的将其重新布置，以使得图能美观漂亮的展示。

这一章教给你了第一个可视化群的技术——凯莱图。在接下来的章节中，我们会进一步探索这一技术的应用，并且凯莱图这一可视化技术将贯穿我们对于群论的研究。首先，花点时间做本章习题来巩固你对于凯莱图的理解。

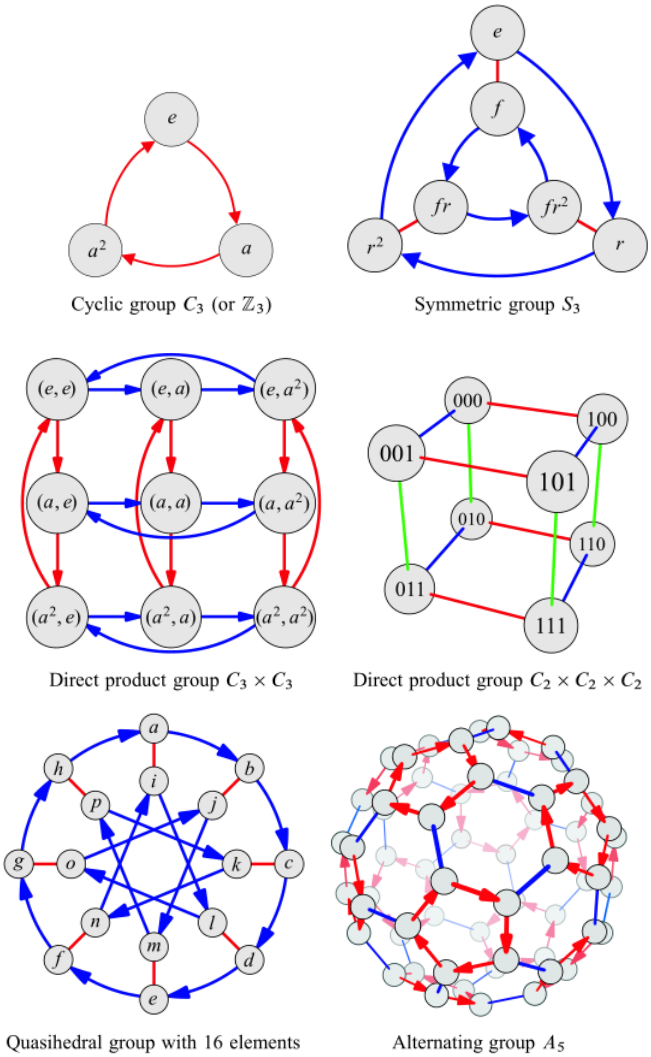


Figure 2.10. Cayley diagrams of some small, finite groups

图 2.10

3

为什么要研究群？

到目前为止，你在本书中见识过的这些群使你不禁想知道群论研究的目的是什么？毕竟，我们之前研究的东西除了在智力方面，似乎别无它用——游戏、玩具以及想象中的情境。如果群论果真只是一堆智力游戏的集合物，那么不管谁质疑道“然而这并没有什么卵用”都可以被原谅和理解。

前两章的学习已经给我们打下了一定基础，可以让我们进一步学习群论的一些更实际的应用。这一章展示了其中一些应用，并给有兴趣的读者做进一步探索提供了参考。在这章之后，我们的群论学习将变得更加深入而抽象，我将回归到选择一些能够深刻而鲜明地阐述这些材料的例子，而不去关心它们在现实世界的具体用处。

我们将会看到群论被应用到三个不同领域：自然科学、艺术和数学。我本来是可以加入更多的例子和内容的，不过这几个对于新手来说会是个好的开始。对称，这一概念将编织起我们全部的示例并贯穿于其中。在读完本章后，你就有了一个强大的工具来帮助你识别并分类周遭世界的各种对称现象。本章的一些习题将鼓励你发现更多的能让群论派上用场的对象和场合。

3.1　对称现象的群

我们说一个东西是对称的，如果从不同的视角看过去它都是相同的话。比如，人体是左右对称的：我们的左半边和右半边看起来是一样的，所以照镜子时看到的像就仿佛有个一模一样的人和你面对面。海星是五角放射对称的：它们有五条相同的手臂，并向外呈现等角度的放射状。你可以把它们旋转一个角度，旋转后的海星和旋转前看起来是一样的 (准确的说，旋转 72ř，五分之一的圆周)。

这又和群有什么关系呢？目前我们见过的群处理的都是对相似物体的重新排放 (re-arrangement)——四角标号的正方形，魔方上涂了颜色的小块，房间墙上装饰画的安排方式 (习题 1.4)——在第五章中，我们会提及群论的一个基本事实：任意一个群都可以视为对一些事物的重新排列方式的集合。正是因为一个物体的对称性可以用这个物体的某些部分的重排来描述，群才和对称产生了奇妙的联系。刚刚我举的那个海星的例子，把海星进行旋转就是将它的手臂重新排放到了一个新的位置，因此这是一个相当简单的关于手臂的重排 (rearrangement of the arms)。

数学家和科学家们使用群来描述客观物体的对称性。这种寻找一个群来描述物体对称性的技术已经在本书中出现过；第二章中，我们在矩形玩具上就已经小试牛刀了，之后的习题 2.8，2.18 和 2.19 都是要你自己动手亲自实践，试着完成跟矩形玩具相同的过程。在这里，我们是时候正式引入这种技术了。定义 3.1详细地描述了这一技术，之后我将解释为什么这一技术是合理有效的。

定义 3.1 (度量对称性的技术)**.** 以下步骤可以从任意的客观物体中提取出一个能够描述此物体对称性的群。

1. 确定物体所有相似的部分 *(similar parts)*，并给每一个部分赋予一个不同的数字标号。*(*矩形有四个相似的角，因此我们将四个角标号。我们也可以选择四条边，给边标号，因为矩形的对边是相同的。*)*
2. 考虑那些你可以用手对物体施加的操作，这些操作须满足：能够重新排列标号但是不改变操作前后物体的空间形状和大小 *(*如果物体太大或太小，无法用手来操作，那就用脑子想象*)*。这些操作形成一个群。
3. 如果你想把这个群可视化，那就照着我们在第二章中的矩形玩具的例子，不断探索并绘图。这个过程如图 *2.2*到图 *2.7*所示。

回顾一下，在第二章中，我们是如何将此技术应用到矩形玩具上的，这有助于你清晰地理解上述定义。图 3.1帮你捋了捋其中的过程。

现在让我们花点时间仔细思考一下这个技术，以便我们能够明白它背后的逻辑。定义 3.1的步骤 1 是给物体的部分标上数字序号，这是为了方便我们在步骤 2 中跟踪那些被允许施加的操作。也就是说，它确保了我们能区分物体的各种不同的状态，并使我们能够看出各个状态之间的联系。注意到，物体的每一个新的状态就对应着数字序号的一个新的排列，即重排 (re-arrangement)。这种标号手段使得我们可以清楚地描述这些重排；否则的话，我们就没办法区分这些状态或排列。

这个技术的核心是步骤 2，它既是自由的，也是有限制的：你应该找出物体所有的满足步骤 2 要求的操作。自由在于寻找这所有的操作，正是这种自由确保了我们能获得

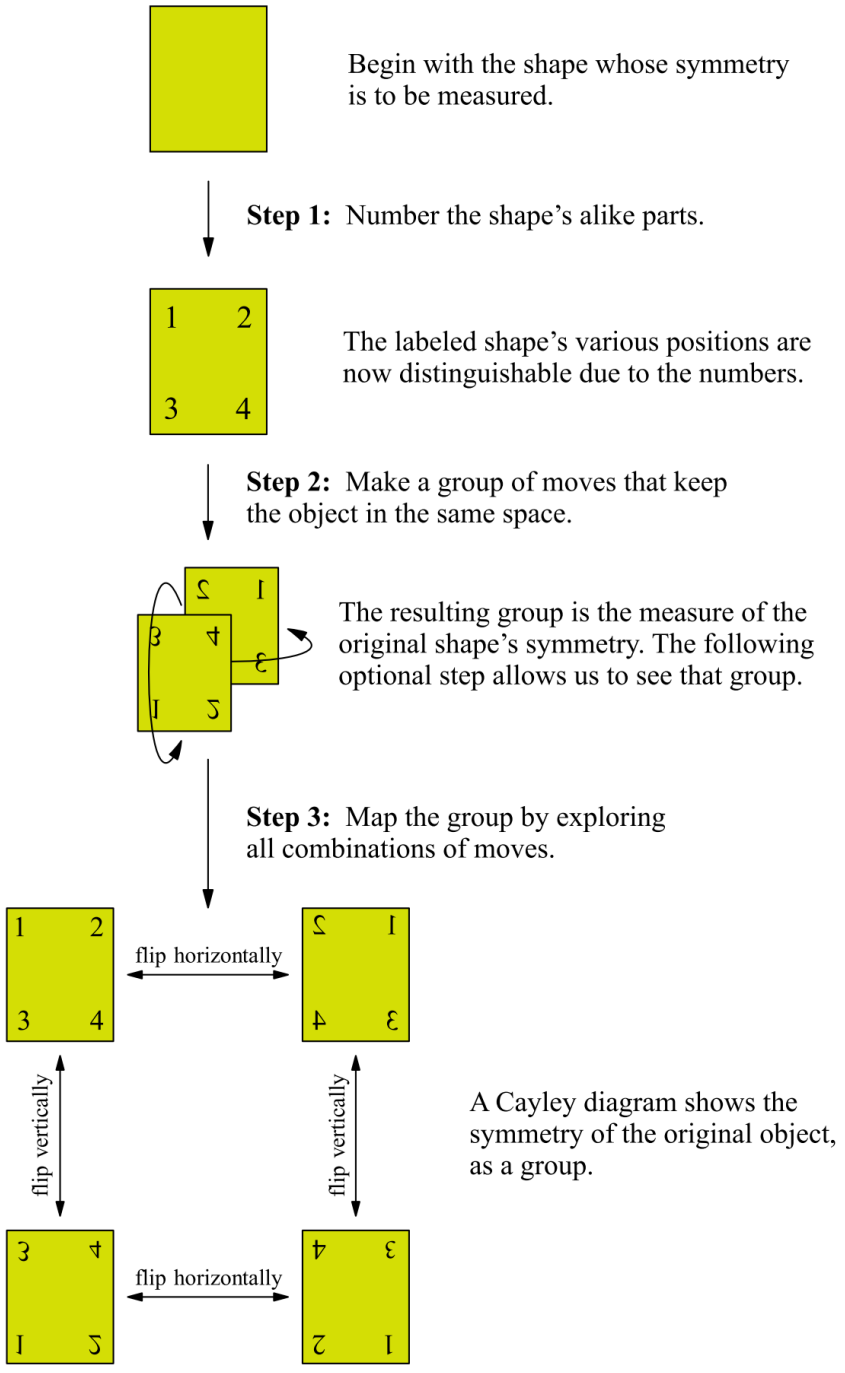


Figure 3.1. In Chapter 2, we applied the technique in Definition 3.1 to the rectangle. A summary of the steps we took is shown here as an example. Clearer illustrations of the rectangle's valid moves and its map appear in Figures 2.3 and 2.7, respectively.

图 3.1

关于物体对称性的完整描述；这个过程也许需要一些探索，就像在矩形玩具那个例子中一样。限制在于这些操作必须是满足要求的，正是这种限制使得我们必须始终注意物体的形状。还记得吗？对称并不仅仅只是一堆相似的部分，还跟它们的布排有关。(海星 ≠ 五条相似的手臂！) 步骤 2 的限制保证了整个技术始终保持物体各个部分的布排方式不变。

由步骤 2 可确定出一个描述物体对称性的群。步骤 3 可以选择做或不做，但是我们最好还是进行步骤 3，这样才能看清这个群长什么样子，而我们整本书的主题正是群论的可视化。在第二章的矩形玩具示例中我们已经体验了这一技术，现在是时候将它运用到一些更有用的东西上了。

3.1.1　分子的形状

在化学研究中，化学家们往往需要对分子的形状进行分类，因为分子的形状会影响分子所具有的化学性质。他们正是使用群论这一工具来做这种分类的！这也给了我们一个机会，把定义 3.1的技术应用到一个实际的东西上。图 3.2展示了一个硼酸分子：红色的球代表硼原子，蓝色的球代表氧原子，绿色的球代表氢原子。下面，让我们做点化学家的工作，度量它的对称性并找出描述其对称性的群。

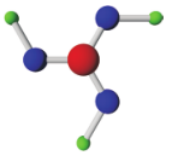


Figure 3.2. A molecule of Boric acid, $B(OH)_3$

图 3.2

根据定义 3.1教给我们的技术，其中第一步要求我们将分子相似的部分——在硼酸分子中即三条“手臂”，标上序号。如图 3.3

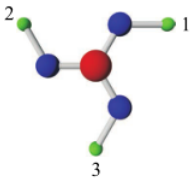


Figure 3.3. The same molecule as in Figure 3.2, but now with each of the three identical arms numbered, to distinguish them, as in Step 1 of Definition 3.1

图 3.3

第二步要求我们找出对于这个分子来说，哪些操作是合理的。想象一下，我们手里有一个此分子的比例模型，现在来转动它。注意到的第一件事是，不管沿顺时针还是逆时针，将分子旋转三分之一个圆周是一个合理的操作，因为转动后的分子与转动前的是一样的，无非是数字标号被重新排列了 (为了帮助你想象，可以参看图 3.4)。另一方面，我们也能找到不被允许的操作，比如说，水平翻转 (见图 2.3) 在矩形玩具中是合理的，不过在这却不被允许。图 3.5展示了水平翻转后的分子的样子，它跟原来的分子有本质上的不同！

如果我们对这个群进行详细而全面的探索，就像画矩形玩具的地图那样，我们将会找到一个三元的循环群 (cyclic group)，如图 3.6所示。一个有着三个分支的、螺旋桨似

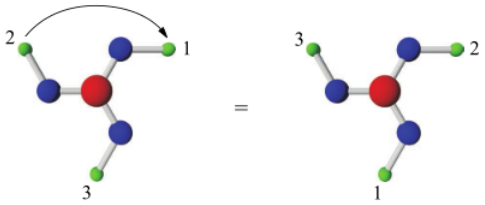


Figure 3.4. Rotating the numbered molecule from Figure 3.3 clockwise one-third of a full rotation rearranges the numbering, but the molecule occupies the same space as before. Thus a one-third turn is part of the group describing this molecule, as per Definition 3.1.

图 3.4

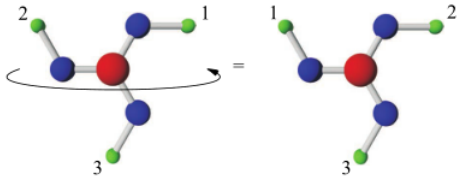


Figure 3.5. Flipping the numbered molecule from Figure 3.3 over horizontally situates the shape differently in space. (The arms do not reach in the same directions as originally.) Thus a horizontal flip is *not* part of the group describing this molecule, as per Definition 3.1.

图 3.5

的分子有一个步长为 3 的循环对称群，这一点相当自然也很让人满意。“循环 (cyclic)”这个词，在这里并不是乱用的；事实上，它是一个正儿八经的专业术语，从图 3.6你也可以明显地看出它的内在含义。在第五章，我们会进一步讨论循环群。

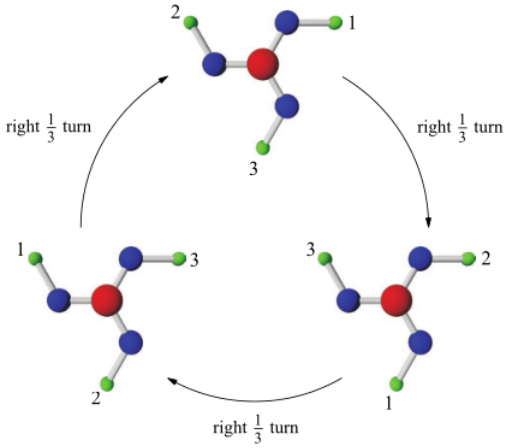


Figure 3.6. A complete map of the group obtained by exploring the symmetry of the labeled molecule from Figure 3.3. If we make this diagram abstract, as we did when creating Figure 2.9, we obtain the top left diagram in Figure 2.10, page 22, the cyclic group C_3.

图 3.6

3.1.2　晶体学

当然，化学家们并不是一个一个分子单独来研究的。对于化学家来说，要想在原子层面了解固体的性质，其中一个最简单的办法是研究那些内部原子排列得很规则的固体。我们把原子或分子在空间按一定规律周期性重复排列的固体称为晶体。研究晶体的学问就称为晶体学。

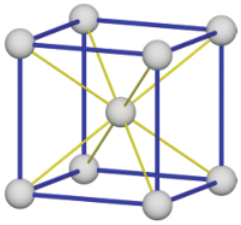


Figure 3.7. One cube from a crystal whose type chemists have named *body-centered cubic*. Each white ball represents an atom (of lithium or sodium, for instance) and each line a bond between atoms. The crystal structure formed by repeating many of these through space is shown in Figure 3.8.

图 3.7

三维晶体的排列模式数不胜数，我们只选择其中一种作为示例。几种较为常见的元素（比如钠和锂）的原子按照立方体网格的排列方式形成固体，且在每个立方体（晶胞）的中心额外分布着一个原子。这种排列方式称为体心堆积，如图 3.7所示。许许多多这样的晶胞聚在一起最终形成一个晶体，如图 3.8. 晶胞在三维空间中一个挨着一个，无限延伸。在彼此重叠的面上，晶胞共享那个面上的四个原子。

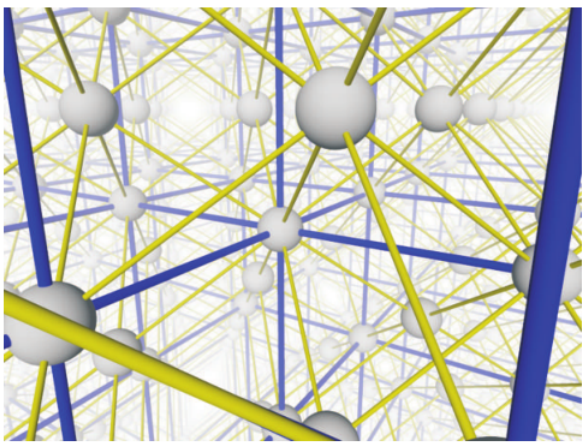


Figure 3.8. The cube from Figure 3.7 repeated to fill three-dimensional space. The different colors of the lines have no chemical significance; they make it easier to distinguish the edges of each cube from the diagonal lines through the cubes' centers.

图 3.8

定义 3.1的技术甚至可以用在此处，来分类这些晶体的对称模式，比如我们上面介绍的那个。我不会在这里来展示这么一个复杂的例子，这其中的复杂性很大程度上源于晶体的一个特性：无限延伸。事实上，化学家在研究的时候确实是把它们当作无限重复的模式，正因为如此，描述晶体对称性的群也是无限的。也许这勾起了你的好奇心，希望我能举个例子。非常好！尽管我并不准备来分类晶体的对称性，不过在下一节，我会举个分类一维无限重复模式的对称性的例子。一个有趣的思考是：我们如何处理无限的对象？无限群又长什么样呢？

从互联网可以找到很多更进一步的关于分子和晶体的群论知识。特别要提一下，由 Jonathan Goss[10] 维护的一个网站帮助产生了本章的一些例子。

3.1.3 建筑与艺术

晶体是一种在三维空间中不断重复的构型，不过我们也可以考虑非三维空间中的情形。这样的重复构型在艺术领域常常出现。首先让我们考虑仅在一个方向上重复的情形，即沿着一条线。也许你在衣服的褶边绣花或者桌布的边缘上已经见过这样一种模式；很多珠宝首饰也是由相同的链环一个连一个组成的；一些建筑的屋檐被雕刻成“饰带(frieze)”，即一维重复的图案。数学家们也采用了这一术语，把所有一维重复模式都称为“饰带构型 (frieze pattern)”，并将描述这种对称模式的群称作“饰带群 (frieze group)”。图 3.9展示了一个简单的饰带构型。也许它不够复杂也不够漂亮，你也不想把它变成你的衣服上或家里房屋上的图案，但是以一个简单的例子开头更有助于我们的理解。尽管在图 3.9中只显示了五片叶子，不过，图两头的省略号表明我们应该将其想象为可以向两端无限延伸的模式。

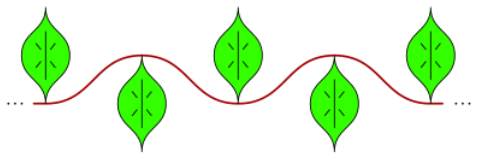


Figure 3.9. A frieze pattern, which can be extended indefinitely to the left or right.

图 3.9

把定义 3.1的技术应用到一个无限的对象上还是头一遭，这将给我们带来新的经验。技术的第一步要求我们给所要研究的那个对象的相似的部分进行标号；当这些相似的部分有无穷多个时，这一步就是一个不小的挑战！我只给在图 3.9中出现的部分图案标了号。在这里，我使用了一个小小的标号技巧，以使得你能够明白，当有更多的叶子被画出来时，你应如何继续给它们标号。但是，这个构型中相似的部分是什么，我到底要

给啥标号呢？你可能会说，每一片叶子是相似的，所以以一整片叶子作为标号单位；然而这只是故事的一半。每一片叶子本身也是对称的：叶子左半边和右半边是一样的。因此，我们应该把半片叶子作为一个标号单位，也就是我们应当给叶子的左右两部分都标上号。图 3.10展示了一种标号方式，将中间一片叶子的右部标为 1，往右方向依次加一。按照镜像对称的方式，我们使用负数来标往左方向的叶子，起点是中间叶子的左部，标为-1，往左方向依次减一。如果这根藤蔓往两边伸展，使得更多的叶子被画了出来，按照这种编号方法，我们很明显地知道应当如何继续给它们标号。

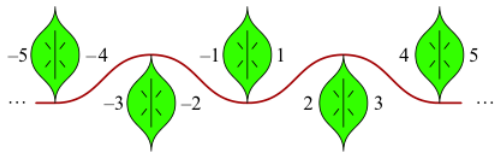


Figure 3.10. The frieze pattern from Figure 3.9, now with all alike parts labeled, as Step 1 of Definition 3.1 requires.

图 3.10

技术的第二步，要求我们找出这条饰带上可以进行的操作，当然这些操作得满足定义3.1中的相关规定。其中一个可行的操作我们之前已经遇到过两次了——水平翻转 (horizontal flip)。正如图 2.3显示的那样，对于一个矩形来说，水平翻转是一个合法操作；又如图 3.5，对于一个硼酸分子来说，水平翻转就不是一个合法操作。在这里，图 3.11告诉我们，对于饰带构型而言，水平翻转确实是一个合法操作。图 3.11中展示的另一种操作在本书中是第一次出现：它叫做平移反射变换 (glide reflection)。平移反射，顾名思义，也就是对一个几何图形, 先按一条直线作镜面反射，然后再沿刚才那条直线作平移（当然先平移再反射也是一样的）。这就是说，将每片叶子向右平移一个位置，再竖直翻转一次，如图 3.11中的箭头所示。一个原本在上面的叶子在操作后变到了和它相邻的右下角的叶子原来所在的位置。

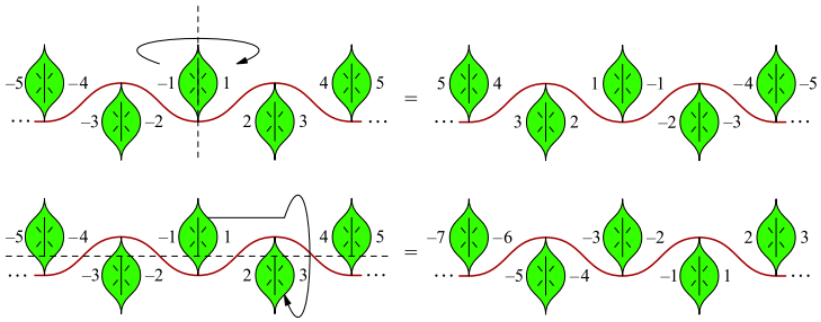


Figure 3.11. The legal moves for the leaf frieze shape from Figure3.9, according to Step 2 of Definition 3.1.

图 3.11

平移反射是我们遇到的第一个将物体同时向各个方向移动的操作。这是因为只有在无限的情况下，我们对物体施加这样的操作后，物体才能和原来的看起来一模一样。这个饰带构型沿着一根轴可以向两端无限重复延伸，所以沿着轴的方向移动并不改变图案的空间形状和体积。(注意到，还有一个合法的操作是将叶子向右平移两个单位，这时并不需要竖直的翻转；但是这实际上和做连续两次平移反射变换的效果相同，所以只要加入平移反射这一操作，我们就能诱导出“将叶子平移两个单位”这个操作。)

如果我们仔细地将这两个操作不断复合叠加，就像定义 3.1中说的那样，最终我们就获得了一张凯莱图，它所对应的群刚好描述了这个饰带构型的对称性。与这个饰带构型相同，凯莱图是一张无限的图，所以我们只能看到它的其中一部分，也就必须要用省略号来表示它可以无限延展。这里，我并不打算详细描述探索出这张凯莱图的历程，这一探索过程类似于我们在第二章的矩形玩具那所做的。图 3.12展示了最终结果图，其抽象版本如图 3.13所示。

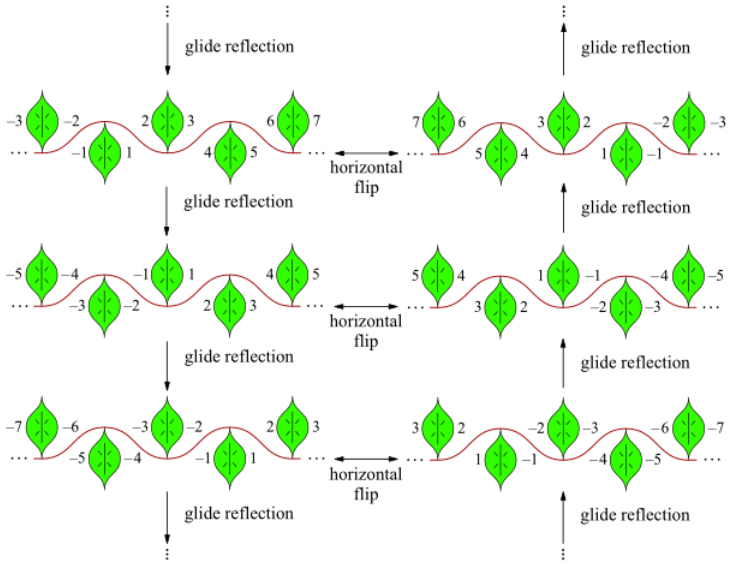


Figure 3.12. A portion of the infinite Cayley diagram of the group of symmetries of the frieze pattern in Figure 3.9.

图 3.12

群论的研究揭示了一个关于饰带构型的很有趣的事实。任意一个饰带构型的对称性都可以用七种不同的无限群之一来描述。也就是说，尽管你可能花了一辈子的时间来创造新的、各不相同的饰带构型，它们本质上所蕴含的对称性却只可能是这七种类型之一。每一种类型都可由一个群描述，我们刚刚看到的图 3.12或图 3.13，展示的就是其中之一。习题 3.11 给出了另外六种饰带构型，用藤-叶模型表示，并要求你画出这六种饰带群的凯莱图 (译注: 感兴趣的读者可以自己查找这一习题，我不打算翻译习题)。

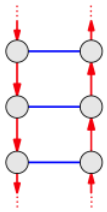


Figure 3.13. The abstract version of Figure 3.12. All the friezes and names of actions have been removed, leaving only nodes representing different states, and two kinds of arrows connecting them. The pattern of such connections, however, remains unchanged from Figure 3.12 to here.

图 3.13

这个饰带的例子表明定义 3.1的技术，其应用范围比我们乍看之下还要广泛的多——它甚至可以应用到无限的对象上！我们使用它度量了一维重复模式的对称性，在这之前，我们也提到化学家使用它来分类出现在晶体中的三维重复模式。就像饰带构型可以用七种不同的饰带群来描述一样，晶体的构型可以用 230 种不同的晶体群 (crystallographic group)[19] 来描述。如你怀疑的，我们当然也能用这一技术来分类二维重复模式，得到的结论是只有 17 种不同的壁纸群 (wallpaper group)。

二维重复模式，就像壁纸上的那些图案。然而我不打算在这里深入讨论它们。尽管原则上，定义 3.1的技术是可以应用到这种模式的分类中的，但是这一过程会花费巨大的耐心和巨量的草稿纸。它们的凯莱图中有几种不同类型的箭头，并且同时可以向两个方向无限延伸，这一点和它们所描述的壁纸构型 (wallpaper patterns) 是一致的。当然咯，这些图看起来也确实让人眼花缭乱。

对我们在可视化过程中用到的那几个特定的、很重要的生成元请予以特别的重视：群的凯莱图能否画出取决于这个群是否拥有一个小集合 (a small set)，它由可以被用作“箭头”的生成元组成。群的凯莱图就是这个群的一张“地图”，箭头就是道路。一方面，如果我们使用的箭头，即那些合法操作，无法产生整个群，那么在凯莱图中就会有一些无法到达的节点，凯莱图也就不连通了；另一方面，如果把所有的合法操作都当做箭头包括在内，就会把图弄得乱七八糟，不具有可读性 (事实上，在无限群里这样的话，你根本无法画图！)。所以，生成元的集合应当取作能够完整连接图中所有节点的最小的那个；这样才有可能画出一张凯莱图。

3.2　作用的群

在本书的开头，我们用了两个例子引入群的概念：魔方和矩形玩具。而在本章中展示的一些应用示例多多少少都跟魔方和矩形玩具有相似之处，因为处理的对象都是具有内在对称性的实际物体。因此，迄今为止我们见到的应用都是使用定义 3.1的技术来寻

找描述物体对称性的群。

但是我们在第一章中学过的群的定义却不只局限于实际物体的对称性。任何一个作用 (actions) 的集合，只要满足定义 1.9的要求，就构成一个群。事实上，群论中一些非常重要的群 (有些也相当有趣) 根本就和实际物体的对称性无关。本章的第二节将给我们展示两个简洁的、这样的例子。

3.2.1 舞蹈

一些传统的乡村舞蹈往往包含几个事先明确的基本舞步，这些舞步使得舞者们在舞厅中翩翩起舞。在方块舞和对跳舞中，舞蹈者通过记舞步的名字和练习学习到这些基本步伐；练习时，指挥者指示舞者在音乐的恰当节点处跳特定的舞步。在这些舞蹈中，舞者双方成对站着，每两对彼此之间站成“箱式”，如图 3.14所示。

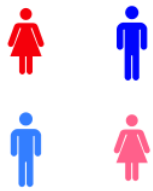


Figure 3.14. The arrangement of two couples in a square, ready to begin a square dance or a contra dance.

图 3.14

每跳一个舞步就将舞者的位置进行了一次重新排列。如果他们严格遵循指挥者的指示，则每一个舞步跳完，他们都会回到刚开始的位置。图 3.15展示了对跳舞中的六个舞步的效果。具体的步伐并没有画出，只显示了每个舞步对舞者的重排效果。

这些效果的集合实际上就形成了一个群。也就是说，定义 1.9的所有要求都被对跳舞中的这些舞步满足了。更有趣的是，这个群和描述正方形对称性的群 (D_4) 有着相同的结构。换句话说，这两种群的凯莱图形状一模一样，只不过图中的顶点和箭头的名称不同而已。当两个群结构相同时，我们称它们是同构 (isomorphic) 的，同构这个话题我们会在第八章中详细介绍。

对舞蹈中的群论有兴趣了解更多的读者可以从本章 3.44 节的习题开始；当然，更进一步的阅读材料在互联网上都可以搜索到。我找到了 Larry Copes 的一个网站 [5] 和 Ivars Peterson 的一篇文章 [15]，可以帮助你长长知识。

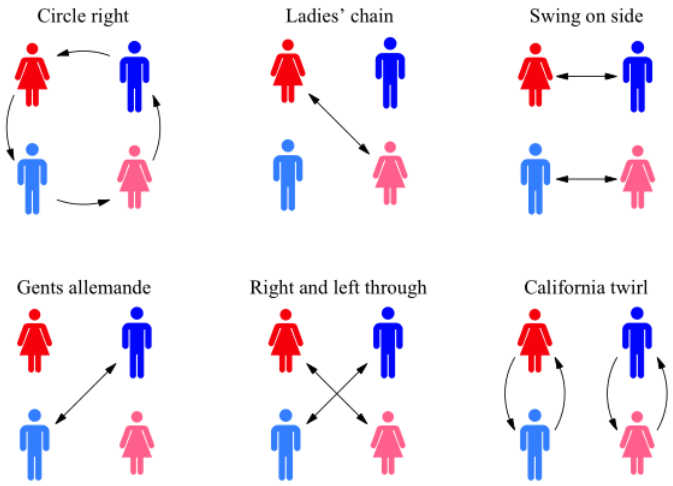


Figure 3.15. How six example contra dance figures rearrange the dancers.

图 3.15

3.2.2　多项式的根

到现在，我们的读者肯定已经确信群论可以在各种场合出现。但是我还想再多举一个应用的例子，这个例子事关群论的起源，要是我连它都不提的话，这对数学的历史会是个不小的伤害！在 19 世纪，两个年轻的数学天才，尼尔斯 • 阿贝尔 (Neils Abel) 和埃瓦里斯特 • 伽罗瓦 (Evariste Galois)，解决了一个几个世纪以来让人们束手无策的数学问题：五次多项式方程不可解。这是数学中最重要的发现之一，当你读到本书的第十章，你就能了解其中的一些具体细节。这一发现依赖于这样一个事实：多项式方程的根彼此之间有着确切的联系，它们实际上形成了一个群。

伽罗瓦并没有将他观察到的这一现象或模式称为群；后辈的数学家们推广了他的工作，并赋予了这一概念以“群”的名字。但他的确是第一个注意到这其中本质并对此进行深入研究的人。伽罗瓦是在研究多项式的根时发现了群，自那之后，数学家们在众多的情境与场合中都发现了群的踪迹，其中一些正是你已经读过的。

正如在对跳舞中一样，伽罗瓦研究的那些群里面的作用并非是对实际物体的操作，却是对一些东西的重新排列。只不过伽罗瓦重排的不是舞者，而是多项式方程的根。他那不朽的伟大发现告诉我们，通过检查由这些重排所构成的群，我们就能够知道解相应的多项式方程的难度如何。他证明了，有些群对应的方程是不可能解的出来的。(译注: “不可解”这个词在数学上有着特殊的含义，通俗说来即为“不可用根式表达出解的样子”，请读者千万莫要带入自己的主观臆测。)

我们之所以在这里提及伽罗瓦的工作，尽管跳过了很多细节 (包括阿贝尔的贡献)，是因为：第一，它提供给诸位读者一些关于这门学问的历史起源，这些事实上正是群论

的首次应用；第二，随着群论学习的不断推进，你现在应该有所期待；这本书的结尾部分描述了一些非常著名而深刻，同时也非常美丽的数学理论。中间的章节是为了让你能够理解这些理论而做的准备。

3.3 无处不在的群

本章中，我们试着将群论应用到了化学、视觉艺术、舞蹈和数学上。从这些应用，我们可以很清楚地看到群论无处不在，而我们所举的例子也只是其中的冰山一角。我们没这么多篇幅也没必要去涉及群论的全面应用，不过以下我会捎带着提一些，以便对某种应用感兴趣的读者知道要从何处着手去查找相关资料和信息。

我们已经知道群论对于化学家的重要意义有两个方面——分子形状和晶体结构。化学家们还常常拿群论去做另一件事——研究并枚举同分异构体 (isomers)，使用一种称为“波利亚 (Polya) 计数”的技术。Kennedy, McQuarrie 和 Brubaker 在 [12] 中对于这一应用做了很棒的综述，还提供了其中更多细节的相关参考文献。理论物理学家在考察基本粒子的时候也经常会用到群论知识 [4,17]。

3.2.2 节揭示了群论诞生于求解一个代数中的著名的数学问题。自那以后，其他数学分支的数学家们也开始使用群论这一工具；我举几个例子。群论和线性代数 (描述的是线性空间中的操作，就像我们知道的一些群当中的操作一样)、数论 (在 8.3 节我们会稍微提到) 有着紧密联系。拓扑学，一门用抽象的手段研究形状和空间的学问，在物理学、天文学以及其他很多领域都有广泛的应用，它同样使用群来分类空间和形状。有一本书叫 *Group Representations in Probability and Statistics*(概率统计中的群表示论)，讲到了群论在概率论与数理统计中的各种应用 [7]。

子群 (subgroup) 与陪集 (coset)(第六章的话题) 可以用来设计纠错码，这种编码可以使得信息在传输过程中产生的错误尽可能少。每当你从互联网上下载一个文件，你的电脑就使用这样的编码来保证你的下载不会被网络传输过程中的各种噪声和干扰淹没。

David Benson 的书 *Music: AMathematical Offering*[2] 包含了一章群论在音乐中的相关应用的内容。其涉及了各种各样的群论结果，从初等的到较为高深的都有。我们在上面提到的 Polya 计数方法，化学家们用来计数同分异构体，而 Benson 在这本书中却用来列举具有特定性质的音级 (pitch class)。

我还可以继续举更多的例子，比如诗歌、杂耍、数独等等。但是我们就到此为止吧。对称性无处不在，群论则是研究对称性的基本工具。我们的眼睛能发现对称，然而这一章教给我们的度量对称性的技术却能使我们看到肉眼所看不见的更本质的东西。凯莱图告诉我们，一个客观物体的对称性并不是一堆混乱模式的集合，而常常是以一种复杂精

美的方式组合在一起。群论以数学的方法研究那其中的联系，也正是因为抽象，所以它才能被用以解决大量的具体问题。

4

最后，再来点代数

到目前为止，你已经按照本书独特的叙述方式了解了不少群论的知识。我们对于群所下的 (非正式)定义 1.9，并不是数学家们广泛采用的定义。尽管使用我的这种定义 (当然，后面还会用这种定义) 有很多方便之处，但是如果不让你熟悉一下其他任何一本群论书籍都会提到的那种正式 (official) 的定义，你的群论学习历程就会是不完整的。

群的标准定义来自于它本身自带的一种可视化技术，我们称之为乘法表 (multiplication table)。由于我们一直聚焦于可视化，因此乘法表将会是带领我们进入群的标准定义的一个重要工具。但是在此之前，我们得先了解一些相关的背景材料，即以下 4.1 节和 4.2 节的内容。

4.1 操作都去哪了？

在第二章我们制作的凯莱图中，群里面的操作 (actions) 以箭头的形式呈现在凯莱图中。但是在一张典型的凯莱图里，我们往往只看得见其中某一些操作的箭头，这些特别的操作叫作生成元 (generators)。乘法表将有效地弥补这一不足之处，它能让我们看到群里面的所有操作以及这些操作彼此之间的交互作用。

为了弄明白为什么凯莱图无法展示出群中的全部操作，让我们回忆规则 1.8。这一规则明确要求，任意操作的复合仍是一个合法的操作。所以，举个例子，即使在第二章中我们说矩形玩具有两个操作 (水平和竖直翻转)，先水平翻转再竖直翻转 (做一次复合) 也仍然是一个合法的操作。更进一步来讲，我们完全可以把这个复合后的操作就当作是一个 (single) 操作。但是矩形玩具的凯莱图 (图 2.7) 并不含有这一复合操作。它只展现了我们最初给矩形玩具引进的两个处于生成元地位的操作：水平和竖直翻转。这其中的微

妙在习题 2.13 有提到：在凯莱图中，生成元要给予特殊待遇，因为它们可由图中的箭头表示。我建议你回过头再去品品图 2.7，想清楚这其中的道理。

尽管凯莱图没有直接地向我们展示群中的所有元素，不过它们确实已经间接地展示了这一点。凯莱图中的每一个节点，例如图 2.7，都自然地关联着一个指向此节点的操作 (箭头)。因此，群中的所有操作事实上已经以这些它们所指向的节点的形式含蓄得呈现在了图中。让我们来更改一下图 2.7，使得它不再那么“含蓄”，而是明白地表明这一点。图 4.1是图 2.1的一个拷贝，在图 4.1中，每一个状态上都标明了从初始状态开始要做怎样的操作能到达当前状态。这使得节点与指向节点的箭头之间的联系得以清晰展现。现在仔细观察一下图 4.1，并将其与图 2.7相比较。注意到，和初始状态关联着的操作是“什么也不做”，因为从初始状态到初始状态，根本就没变啥！

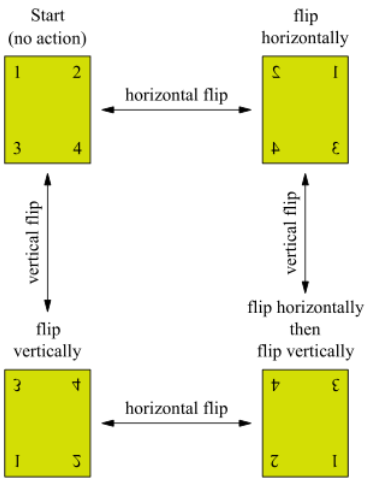


Figure 4.1. An annotated copy of Figure 2.7 from page 18. Above each rectangle in the figure appears a phrase describing an action that leads there from the starting point.

图 4.1

挪走矩形，只留下相关注释，如图 4.2，我们就得到了一张不再跟矩形状态有关，而只是关于操作的图。如果你喜欢，你也可以说是“从关于名词的图变成了关于动词的图”。图 4.2没有包含箭头上的指示文字，因为这明显多此一举。为了能一眼就区分出“水平翻转”和“竖直翻转”，我们用虚线来画代表“竖直翻转”的箭头。我们很容易看出哪种箭头代表哪种操作：因为实线箭头从“开始”指向了“水平翻转”，所以它肯定就表示水平翻转；同理，虚线就表示竖直翻转。

像图 4.2这样的图将在下一节大有用处，所以我们先来仔细观察一下这种图。以下给出的定义总结了将图 2.7变成图 4.2的过程。当你一边读这个定义的时候，你应该一边看着图 2.7、图 4.1和图 4.2，以确保你明白定义中的每一步在刚才那个例子中是如何实

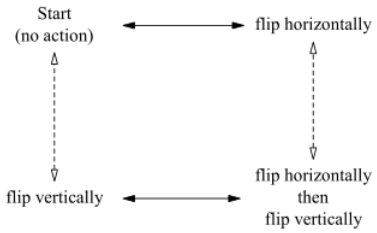


Figure 4.2. A simplified copy of Figure 4.1. The rectangles themselves have been removed, and replaced by the actions that led to them. The labels on the arrows have become superfluous, and were therefore removed. The two types of arrows are now distinguished by dashed vs. solid lines.

图 4.2

现的。

定义 4.1 (作用图)**.** 以下三步可以将一张群的凯莱图转化成关于群的操作的图。

1. 任选一个节点，将其称为“起点”。对于“起点”的比较自然的选择往往是存在的，正如我们在图 *4.1*中做的那样。
2. 将每个节点用一条从起点出发到达此节点的路径重新标上名字。
3. 将箭头上的相关说明去掉，并用其它方式区别图中的箭头 *(*比如，用不同的颜色或者实线、虚线等*)*。

让我们把变换所得的图称为作用图 (diagram of actions)。

定义 4.1所给出的变换，对任意一个凯莱图都可以施行，甚至是一张完全抽象的凯莱图，例如图 2.9所示的克莱因 4 元群 (图 2.9中的“箭头”其实并没有箭头，我们以此来表示双向箭头的意思)。为了能简洁地称呼这些路径以及它们的复合，我们将会需要用一些符号来指代不同颜色的箭头。让我们约定用 R 表示红色箭头，B 表示蓝色箭头，N 表示起点。对图 2.9施行定义 4.1描述的变换，我们就得到了图 4.3. 不妨以此来测验一下你对定义 4.1的理解，仔细检查图 4.3确实是图 2.9经过变化所得的相应的作用图。

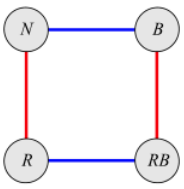


Figure 4.3. The result of labeling nodes according to “actions” (in this case the colors of the diagram’s arrows) in the abstract Cayley diagram from Figure 2.9 on page 21. The group shown is the Klein 4-group V_4, which we first encountered in Chapter 2.

图 4.3

4.2　复合，复合，复合

群的作用图给我们提供了新的信息——关于群里面的操作之间的关系。事实上，我们将会发现像图 4.3那样的作用图，可以当成一种简单的计算器。它能够用来计算群中任意两个操作复合 (combine) 后的效果。

你或许会感到奇怪，为何我会说图 4.3中包含着群里面的操作？怎么看它都只是一张抽象的图而已啊。当然，我们通常期望数学是抽象的，不过有时具体的情境往往能帮助我们更好的理解抽象的事物，因此，回忆一下我们从 2.2 节到 2.5 节中遇到的那些跟图 4.3相关的具体例子。回到这里，所谓的“操作”就体现为图中的红色箭头与蓝色箭头 (分别称为操作 R 和操作 B)。为了将两个操作复合，只须从初始节点 N 依次施加这两个操作即可。这就是图 4.3这种计算器的使用方法.

举个例子，我们可以验证“先 R 再 B”和“先 B 再 R”的作用效果是一样的。怎么验证呢？在图中从初始节点 N 开始先走一个红色箭头 (R)，再走一个蓝色箭头 (B)，然后我们就到达了 RB 这个节点。同样的道理，从初始节点 N 先走一个蓝色箭头（B），再走一个红色箭头（R）将把我们带到相同的节点。因此，两个不同的短句“先 R 再 B”和“先 B 再 R”实际上描述的是两个完全等价的操作，因为它们最终得到的结果完全一样！

用代数中的符号来表达上述这种关系是很常用的手段。（事实上，人们对于群论的研究通常正是以一种相当代数化的方式进行的，因此群论往往被归于抽象代数 (Abstract Algebra) 这一数学分类中。本章内容将会体现这一点）为了表述“先 R 再 B”，我们用代数中类似于两个变量相乘的“RB”来表示；同理，“先 B 再 R”就可以记作“BR”。于是，下述说法

“先 R 再 B”等价于“先 B 再 R”

可以简明地表达为

$$RB = BR$$

这个观察只是很简单的一个，图 4.3还可以计算群中操作之间更复杂的关系。比如，这个长长的序列 RRRBRRBBB. 我们运用代数中很方便的一种记法将这个序列简洁地写成 $R^3BR^2B^3$，这看起来就像把变量乘起来是不是？用图 4.3当然也能计算这个表达式的结果。从初始节点 N 开始，依次施加给定的这些操作（PS: 按右乘顺序）——沿着红色箭头走三次，接着走一次蓝色箭头，再走两次红色箭头，最后走三次蓝色箭头。你应该到达了 R 这个节点，因此这就得到了以下等式

$$R^3BR^2B^3 = R$$

我们将作用图当成一个计算器解决了一个乘法计算的问题：R^3 乘以 B 乘以 R^2 乘以 B^3

等于 R。任何一张作用图 (定义 4.1) 都能以这种方式当成一个计算器使用。(也许你想知道，我能不能就像在普通代数里那样把 $R^3BR^2B^3$ 进一步化简为 R^5B^4 呢？自己试一试，用刚刚教给你的技术去弄明白这两个表达式是否相等。)

现在，你该清楚为什么群论会被划归为代数学的一部分——这些等式像极了代数式。但是我必须要强调，这里的代数式跟你所理解的那种寻常的代数式（比如中学里学的那些）有着本质上的不同。尽管 RB 看起来似乎是 R 和 B 的乘积，而实际上其含义是将这两个操作按顺序复合。我们在这里隐喻地使用了“乘法 (multiplication)”一词。贯穿在这本书，我都将以这种不严格的方式来使用“乘法”这一术语。在数学中，像这样把抽象的运算叫作“乘法”或“加法”是很常见的行为，我们仅仅把这些词语当作一个“占位符 (placeholder)”而已。

等式 $R^3BR^2B^3 = R$(以及其它许多类似的等式) 实际上表明了群中的操作具体是如何进行复合的。而我们用以找到这一等式的方法告诉我们，不必去担心像 $R^3BR^2B^3$ 这样的式子有多么长、多么复杂，因为不管我们写下的式子有多长，作用图（以图 4.3为例）都会帮我们把它最终简化为与 R，B，RB 和 N 其中之一相等价的某个操作。

4.3　乘法表

懂得如何将一个作用图当作计算器使用，就好像使你拥有了一个解码环 (decoder ring)——你能够轻松地读出作用图中所包含的信息，因为你知道这其中的窍门。不过从可视化的角度来说，保守秘密并不是我们的目的：我们的目的恰是让事实清晰可见。因此，让我们来创造一张表格——它包含了关于群中的作用如何复合的所有信息，这样我们就无须再费神从凯莱图中读取这其中的秘密信息。

这样一张能够显示群中每一对作用的复合效果的表格，叫作“乘法表 (multiplication table）)。回忆一下，小学里我们学过的乘法表是什么样子的；如果你忘了的话，可以看一下图 4.4. 我们用群中的作用来替代数字，并将“乘法”重新定义为作用的复合，即依次施加两个相继的作用。

我们还是沿用上面的图 4.3所表示的群作为例子。在这里，我们关心的四个作用是：N, R, B 和 RB. 做一张跟图 4.4相似的表格，不过行头和列头都取作 N, R, B 和 RB，如图 4.5. 接下来只须使用“计算器”(图 4.3) 计算出两两作用复合的效果，就能填完整个表格。举个例子，在 R 所在行与 B 所在列相交的表格处，我们写下“先 R 再 B”的复合结果：RB。在 RB 行与 RB 列相交的表格处，我们写下“先做一次 RB, 再做一次 RB”的结果：N。通过这种方式，我们就能完成这张表，最终结果如图 4.6.

由于 N 表示“什么也不做”，所以将它和其他作用复合就相当于这个作用本身。比

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24
5	5	10	15	20	25	30
6	6	12	18	24	30	36

Figure 4.4. A standard elementary-school multiplication table, in this case only showing how to multiply the numbers 1 through 6.

图 4.4

	N	*R*	*B*	*RB*
N				
R				
B				
RB				

Figure 4.5. Beginning to create a multiplication table for the group ¼, whose Cayley diagram appears in Figure 4.3

图 4.5

如，NB=B. 注意到，图 4.6的第一行和第一列正好就是用 N 去做的乘法，出于此，第一行就是把行头复制了一遍，而第一列也就是把列头复制了一遍。这就使得行头和列头的存在有点多余了，所以我们不妨删去行头和列头，将图 4.6左边的表简化为图 4.6右边的表。这样，行头和列头就成为了乘法表本身的一部分：第一行和第一列。Group Explorer 软件在绘制乘法表时也采用了这一习惯，因为可以使得表格更简洁明晰。但是，行头和列头是天然的“参考系”，有时也很有用，所以在之后的乘法表中我们仍然保留它们。

	N	*R*	*B*	*RB*
N	*N*	*R*	*B*	*RB*
R	*R*	*N*	*RB*	*B*
B	*B*	*RB*	N	*R*
RB	*RB*	*B*	*R*	*N*

N	*R*	*B*	*RB*
R	*N*	*RB*	*B*
B	*RB*	N	*R*
RB	*B*	*R*	*N*

Figure 4.6. On the left, a completed version of the multiplication table begun in Figure4.5. Each entry can be computed using Figure 4.3 as a calculator. On the right, the same table with row and column headings removed, because they appear as the first row and column of the remaining table anyway.

图 4.6

乘法表是一种新的、强有力的可视化工具，因为它能够从群中的作用复合的角度揭示群所描述的模式，这一点凯莱图没有办法明显地展示出来。为了使其更直观，我们可

以将乘法表的格子有条理的涂上颜色。具体做法是：给群中每一个作用分配一个不同的颜色，然后根据格子里出现的是什么作用，再涂上相应的颜色即可。图 4.7展示了已经用这种方法涂好颜色的六种不同的乘法表。这六张乘法表所代表的群与图 2.10中用凯莱刻画六个群是完全一样的。

目前为止，图 4.7中的构型仅仅是一种视觉上的乐趣，但是在接下来的章节中，我们会更深入的研究它们。本章剩余的内容将着力于运用乘法表来引入群的标准定义。

4.4 经典定义

群论传统的介绍方式并不是我们目前接触到的这种形式。大部分的教材只有在花了几章的篇幅絮叨完一些基本概念和定理之后，才会将群看成是一堆作用的集合，也就是之前本书所采用的那种方式。大多数的教科书都采用先陈述群的正式定义，即定义 4.2，再说满足这些定义条件的东西就叫作群。这种方式通常使用非常数学化的语言，好处在于说法极其精确，毫不含糊；然而坏处是对于初学者不太友好，很难洞悉其中的本质。因为那种标准定义比我们的定义 (定义 1.9) 可以更自然而直接地引出乘法表，所以我们也可以反过来，试着利用刚刚熟悉的乘法表这一工具来理解标准定义。

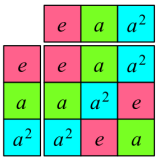
我们一直都将群里的东西称为“作用 (actions)”，因为我们的定义要求一个群得是一堆作用 (满足特定条件) 的集合。但是群的标准定义并不依赖于“作用”，因此我们有必要采用更一般的术语。我们称群里的东西为“元素 (elements)”。“元素”这个词是一个数学术语，数学家们喜欢把一堆放在一起的东西叫作“集合”(事实上，在此之前我们已经不自觉的使用了这一词语) 并把里面的东西叫作“元素”。

随之而来的还有一些常用记号。为了表述“N 是群 V_4 中的元素之一”，我们有标准记法：

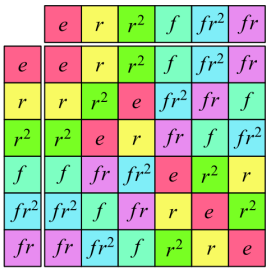
$$N \in V_4$$

记号 $\in$ 看起来像字母“e”，就用来指代“元素 (element)”的意思。读作“N 是群 V_4 中的元素之一”。这样的术语和记号并不只局限于在定义 4.2中使用，在本书的剩余章节以及更广阔的数学领域中都随处可见。

除了这几个新的术语，让我们再回顾一些旧的术语。在前一节中，我们知道乘法表展示了如何将群中的两个元素复合成另一个元素。数学家们把这样一种复合的方法称为“运算 (operation)”，这个词对于熟悉中学数学的读者来说应该不陌生。我们知道普通的运算有所谓的“运算顺序”，比如小学老师教给我们的“先做乘除运算，再做加减运算”。对于算术 (Arithmetic) 而言，有四个基本运算——每种运算都是将两个数字以某种方式组合成一个新的数字（比如，$2+3=5, 6.3\div 7=0.9$）. 由于我们这里提到的运算均是将



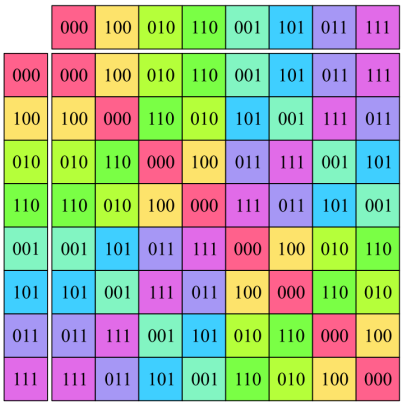
Cyclic group C_3 (or $\mathbb{Z}_3$)



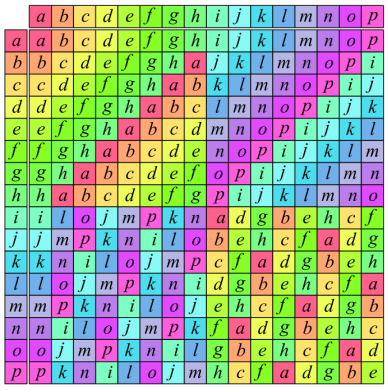
Symmetric group S_3



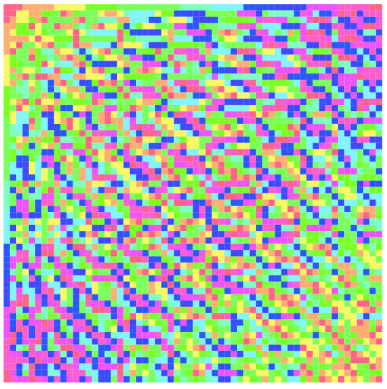
Direct product group $C_3 \times C_3$



Direct product group $C_2 \times C_2 \times C_2$



Quasihedral group with 16 elements



Alternating group A_5

Figure 4.7. Multiplication tables of the same small, finite groups whose Cayley diagrams appear in Figure 2.10 on page 22.

图 4.7

两个元素以某种方式组合成一个新的元素，所以我们给这些运算一个特殊的名字“二元运算 (binary operations)”。

乘法表所描述的群元素的复合也是一种二元运算。当我们说它是群元素上的一个二元运算时，意思就是说它能将群中的任意两个元素对应得到群中的另一个元素。我们往往用“乘法”记号来表示群上的二元运算 (R 跟 B 复合就可以写成 RB)。另一种常见的表示群上的二元运算的方式是用“加法”，如 R+B。当然，还可以用其他的符号，只要你高兴，随你用什么都行，例如 $R*B$，$R\cdot B$. 只要一本书的作者使用的符号能够前后一致，自圆其说，那么采用什么样的符号并不重要。

这两个新术语：元素和运算，是定义 4.2的核心。正确地理解这两个概念能让我们更好地理解那个定义。有兴趣的读者可以参阅任何一本关于离散数学或者传统的群论教科书，从中找到关于集合与运算更正式的定义。

每一张乘法表都描述了一个二元运算：因为所有可能的运算都展示在了表中。乘法表的特点——有两个轴向 (横轴和纵轴)，这也正是二元运算的特点。但是由于我们研究的乘法表是描述群的，所以它肯定具有定义 1.9的典型特征。因此，并不是随便一张填满了符号的表都能成为某个群的乘法表。实际上，有两个显著的特征区分了哪些表是群的乘法表，而哪些则不是。4.4.1 和 4.4.2 节将详述这两个重要特征，这也将使我们能更好地理解定义 4.2. 不过要是你喜欢独立思考，你可以先试着找出图 4.8中哪一个是群的乘法表，以及另一个为什么不是？

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

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

Figure 4.8. Can you figure out which of these two multiplication tables depicts the binary operation for a group? To learn how, read Sections 4.4.1 and 4.4.2 and then try the exercises in Section 4.5.3 on page 55.

图 4.8

4.4.1　结合律

回忆一下之前我们化简 $R^3BR^2B^3$ 的例子。尽管我们最后成功的将其化简为一个简单的结果 R，不过实际上我们还可以把它化简成其它的（不彻底）样子，比如下面几个：

$$R^3BR^2B^3 = RBR^2B^3$$

$$R^3BR^2B^3 = R^3BB^3$$

$$R^3BR^2B^3 = R^3BB$$

在上面的第一个化简式中，我们着力于化简 $R^3BR^2B^3$ 开头的 R^3B。添上括号也许看得更清楚些

$$(R^3B)R^2B^3 = (RB)R^2B^3$$

等式左边括号里的内容被化简成了等式右边括号里的内容。添上括号后并没有改变整个式子的意义；括号仅仅表明我们当前的化简聚焦于此处。括号在哪儿都可以添上，然而事实上哪儿都不并需要括号。

由于群的运算允许我们为了看得更清楚而添加括号，但是又不实际需要这些括号，且括号的添加与否并不会改变整个式子的意义，基于这些特点，因此我们称群的运算是可结合的 (associative)。也就是说，对于一串群元素的相乘式，只要不改变原有元素的次序，随你怎么结合其中的部分元素，这个式子的意义都不会改变。上面另外两个等式的带括号版本如下：

$$R^3(BR^2)B^3 = R^3(B)B^3$$

$$R^3B(R^2B^3) = R^3B(B)$$

请注意，并非所有的二元运算都是可结合的！一个简单的例子是，考虑整数的减法:

$$4 - (2 - 5) \neq (4 - 2) - 5$$

因为在上式中，括号所处的位置明显会改变运算的结果，所以减法是非结合的，或者说减法不满足结合律。在做减法的时候就不能像做加法或做群元素运算那样随意添括号了。

群中作用的复合总是满足结合律的，因此这样一种群元素的运算总是可结合的。这是任意一个群上的运算所必须要满足的两大特殊性质中的第一条；至于第二条，就是下一节的内容了。关于运算的这两条性质形成了定义 4.2的核心。本章后面的一些习题将帮助你弄明白乘法表是如何体现群运算是否具有可结合性的，以及群中元素的逆元。

4.4.2　逆元

定义 1.9中的规则 1.6要求群中的每一个元素都可逆。这就是说，任给一个群元素 x，在同一个群中，你也应该能找到与它相对的一个元素 y，我们把这样的一个元素 y 称为 x 的逆元 (inverse)。直观点来讲，如果你施加了某个操作，然后又紧接着施加了它的“逆元”(逆操作)，那么结果就等同于你啥也没做。举个例子，在魔方中，将一个面顺时针旋转 90 度的“逆元”是将同一个面逆时针旋转 90 度；最终效果就等于根本没改变魔方的状态，或者说等同于没做任何操作。为了能用代数的语言写下这一原则，我们需要

一个记号来表示“什么也没做 (no action)”。在我给 V_4 做的乘法表中，我用“N”来表示“什么也不做”的意思；在一般的群论书籍中通常使用 0，1 或者 e 来表示。群里面这样一个特殊的元素我们称之为“恒等元 (identity)”，中文里也常叫作单位元。在本书中，我将使用 e 来表示单位元。(注意，不要将其跟自然对数的底 e 混淆！后者的定义是 $e = \lim_{n\to\infty}(1+\frac{1}{n})^n \approx 2.71828$ 通常用来计算复利、放射性衰减等问题)。

有了这个记号后，我们就能用代数方程表达群中每一个元都有逆元。举个例子，考虑 3 次对称群 S_3，它的乘法表在图 4.7中。把单位元用 e 表示，其余符号沿用乘法表中的符号。我们可以用方程表述 S_3 中每个元都有逆元这一事实。下面的六个方程每一个描述 S_3 中的一个元素。例如，第一个方程的意思是：r 可以用 r^2“逆回去”——所以 r^2 就是 r 的逆元。

$$r(r^2) = e$$

$$(r^2 r) = e$$

$$ff = e$$

$$(fr)(fr) = e$$

$$(fr^2)(fr^2 = e)$$

$$ee = e$$

在这个群中，有些元素比如 f 和 fr 就是它们本身的逆元，也有些不是，比如 r 和 r^2。相反，它们彼此互为逆元。上面所有等式由于结合律的存在其实都可以不写括号，但是我为了清楚起见加上了括号。

V_4 是一个更加不平凡的例子，因为它里面的每个元都是本身的逆元 (想想矩形玩具就明白了——任一个翻转操作只要做两次就回到原来的样子)。

$$NN = N$$

$$RR = N$$

$$BB = N$$

$$(RB)(RB) = N$$

“每一个群元素都有逆元”是定义 4.2要求的两个关键事实中的另一个；第一个是结合性，我们在上一节已经讨论过了。本章的习题也将让你搞清楚怎么从乘法表中读出“逆元”的信息。不过现在，我们要正式开始叙述并分析群的经典定义了。

4.4.3　全都放到一起

定义 4.2 (群). 一个集合 G 称为一个群，如果它满足以下条件：

1. G 上有一个二元运算 $*$
2. 此二元运算具有结合性, 即对于任意 $a, b, c \in G$, 均有等式 $(a * b) * c = a * (b * c)$ 成立
3. 在此运算下，有一个恒等元 $e \in G$. 即对于任意 $g \in G$, 均有等式 $g * e = g = e * g$ 成立
4. 在此运算下, 对于任意 $g \in G$ 都有逆元, 记作 g^{-1}, 且均有等式 $g * g^{-1} = e = g^{-1} * g$ 成立

定义中的第 1 条本质上是说“一个群就是一张乘法表”；定义中的第 2 条则将我们考察的对象限制在那些具有结合性（详见 4.4.1 节）的乘法表上；定义中的第 4 条要求每个元素都得可逆 (详见 4.4.2 节)；而为了说清楚逆元，又需要恒等元 (详见 4.4.2 节) 的概念，这便是定义中的第 3 条所要求的。

注意到我们引进了一个新的记号 g^{-1}, 它表示群元素 g 的逆元。举个例子，在 V_4 中，我们可以写

$$R^{-1} = R$$

在 S_3 中，我们可以写

$$r^{-1} = r^2$$

在任意一个群中，总有 $e^{-1} = e$. 你能根据定义证明这一点吗？

以上的讨论让我们越发清楚地意识到定义 1.9和定义 4.2有莫大关联。但是，它们真的是等价的吗？或者说，如果定义 1.9认为某个东西是群，那么定义 4.2也会这么认为吗？反之是否也成立呢？我们对于第一个问题的回答是肯定的！之前两节的内容其实已经给这个肯定回答提供了一个非正式的论据。在第五章学习置换群 (permutation group) 后，我们还会回到这里，并将明确地回答第二个问题。

4.5　之前，现在，之后

本章给我们一直以来研究的主题提供了一个重要的、新的观点。我们现在可以用两种完全等价的观点来看待群：你既可以把它视为一堆作用 (actions)，也可以把它当做一个带有二元运算的集合。每种观点都有它的好处，并且往往一个群论定理从一个角度来看会比从另一个角度来看更清晰易懂。因此，同时有两种观点供我们自由使用是非常有

益的；尤其当我们进入后面几章的学习时，在那里我们将会遇到更加严肃的群论，也会揭秘一些群论中相当著名而重要的定理。不过现在，你是时候做点习题了，以检测你在本章中学到的知识。

5

五大家族

我们已经学习了两种强力的可视化技术：凯莱图将群以一堆作用的形式呈现在我们面前，而乘法表则通过二元运算的形式展示一个群的样子。本章将充分运用这两种技术，以期能全方面地介绍群论中常见的五种群。当然，在介绍的过程中，我们还会遇到很多新的概念。

我们首先会遇到的是循环群（cyclic group），有很多理由可以让我们把它作为这一旅程的始发点。不仅仅因为循环群是最简单的一类被用来描述对称性的群，更由于循环群将使得本章接下来的内容条理清晰：循环群会以所谓的轨道（orbit）的形式出现在所有的群中，同时我们将学习基于轨道概念的另一种可视化技术，我们称作“循环图（cycle graph）”。循环群也将帮助我们理解之后遇到的群，如阿贝尔群（Abelian group）和二面体群（Dihedral group）。这些群都可以通过对循环群做“积（product）”运算得到。在这一章中，我们会提到“积”这一概念，对于它的深入研究将在第七章中进行。

最后，我们会遇到对称群（symmetric group）和交错群（alternating group），这两种群将揭示群与物体排列（rearranging）之间的联系。本书中很多的例子和练习处理的都是有关物体排列的问题，数学家们习惯称其为“置换（permutation）”。本章的高潮部分是来自群论的两个美丽的结果：五种正多面体（Platonic solid）的对称性以及凯莱定理（Cayley’s Theorem）的一个图解法证明。

在某种意义上，本章是由之前那些很浅显的内容向之后较深入的内容的一个过渡。当然，这里所有的内容都是以可视化的方式叙述的。为了让你明白熟悉掌握本章内容将会有怎样的回报，不妨花点时间想想以下问题：

1. 是否存在两个及两个以上的群，使得它们都具有 10 个元素？
2. 是否存在一个群，其中任意元素（单位元除外）都不是它本身的逆元？

3. 所有的群都可以用来描述某些实际对象的对称性吗？

所以你瞧，为了弄明白这些问题，在你头脑中存放一个资源丰富而条理清晰的“群图书馆”是多么有用而必要。本章的旅程就将带你见识许多种类的群，并将它们分门别类地组织在你的记忆中，同时用可视化的方式突出它们各自具有的关键特征。

5.1　循环群

5.1.1　旋转

第三章已经教给我们如何用群来描述实际物体的对称性。最基本的一类群，循环群，描述的正是那些只有旋转对称性的物体。我们分析过的硼酸分子的对称性群（图3.6）是三个作用的循环。这种循环非常简单，其原因就在于硼酸分子只有一种操作。事实上，对于硼酸分子 $B(OH)_3$，要想保持它的对称性，你所能做的操作只有一个——旋转。你既可以把它逆时针旋转也可以顺时针旋转几次，但是这些其实都可以从一个基本旋转得到，这里我们规定这个基本旋转为“顺时针旋转 120 度”。

硼酸分子的对称性群中有三个元素是因为这个分子有三条旋臂。可以推测，类似的具有更多旋臂的形状就应该用具有更多元素的循环群描述。或许这些形状并没有实际的分子可与之对应，但是我们可以想象啊！还有，一些日常物品也只有旋转对称性——如图 5.1 中的风车和螺旋桨。图 5.2 对螺旋桨的对称性作了简要分析，注意它和我们对硼酸分子所作的分析的相似性，参看图 3.4 和图 3.5。



Figure 5.1. A six-bladed propeller and an eight-foiled pinwheel, whose symmetry groups are the cyclic groups with six and eight elements, respectively.

因为描述硼酸分子的循环群中有 3 个元素，所以我们通常将其记作 C_3. 描述图 5.1 中的螺旋桨和风车的循环群同理可分别记作 C_6 和 C_8. 你也许还听过有人把 C_3 叫作“3 阶循环群”，因为“阶（order）”在群论中是专门用来称呼群所含元素个数的一个术语。当我们需要叙述整个循环群这个家族，或其中某个泛指的循环群时，我们通常用 C_n 来表达，其中 n 可以是任意正整数。

为了表示循环群中的元素，最常用的方法是将恒等元记为 0，顺时针旋转一次的元素记为 1，顺时针旋转两次的元素记为 2，以此类推，直到 $n-1$. 注意到在 C_n 中并没有一个叫 n 的元素，这是因为一个有 n 个桨叶的螺旋桨旋转 n 次就回到了它的初始状态，也就是说，旋转 n 次跟旋转 0 次是一样的。因此，每个数字的意义就是指将基本旋转 1 重复进行的次数。

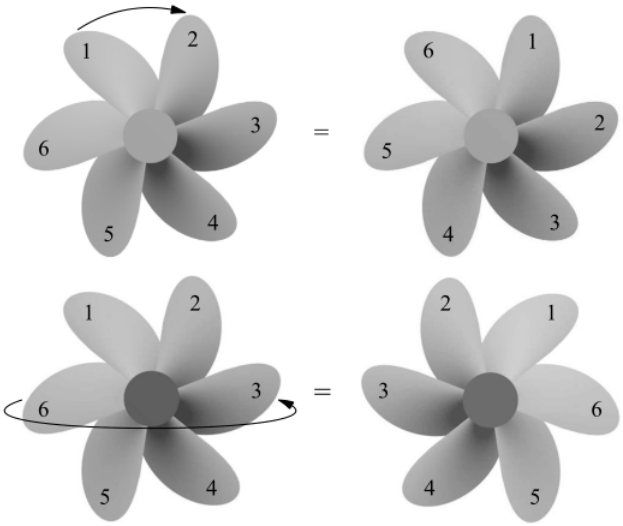


Figure 5.2. Propellers have only rotational symmetry. Rotating them clockwise (as shown in the top row) keeps them occupying the same space, but flipping them over (as in the bottom row) does not. The lower right propeller rotates backwards compared to the other three, and thus doesn't sit the same in space.

图 5.3 展示了 C_3, C_5 和 C_n 的凯莱图，采用我们上面介绍的命名方式。图 5.3 中最右边的图使用了省略号来表示，这一点很容易理解。

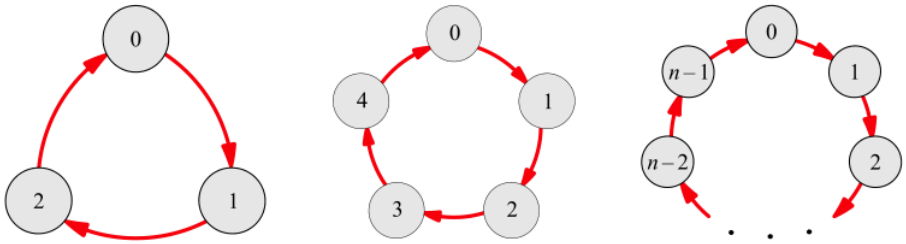


Figure 5.3. Cayley diagrams for the cyclic groups C_3, C_5, and C_n

5.1.2　乘法表和剩余类加法

有时我们也会见到有人用 Z_n 表示循环群 C_n，这种表示法源自于整数集合的记号 Z。由于我们可以把 C_n 看作前 n 个非负整数（凯莱图中标的数字），所以许多书和论文索性就用 Z_n 来表示了。

习题 4.6，要求你用 C_5 的凯莱图做一份它的乘法表，也就是 Z_5 的乘法表。之前我们介绍过怎么用数字来命名作用，所以最终的乘法表如图 5.4 的左图。尽管在这张表中，数字之间的运算看起来很像普通的加法（比如 0+3=3 和 2+2=4），但也有不同之处（比如，2+3=0 和 3+3=1）.

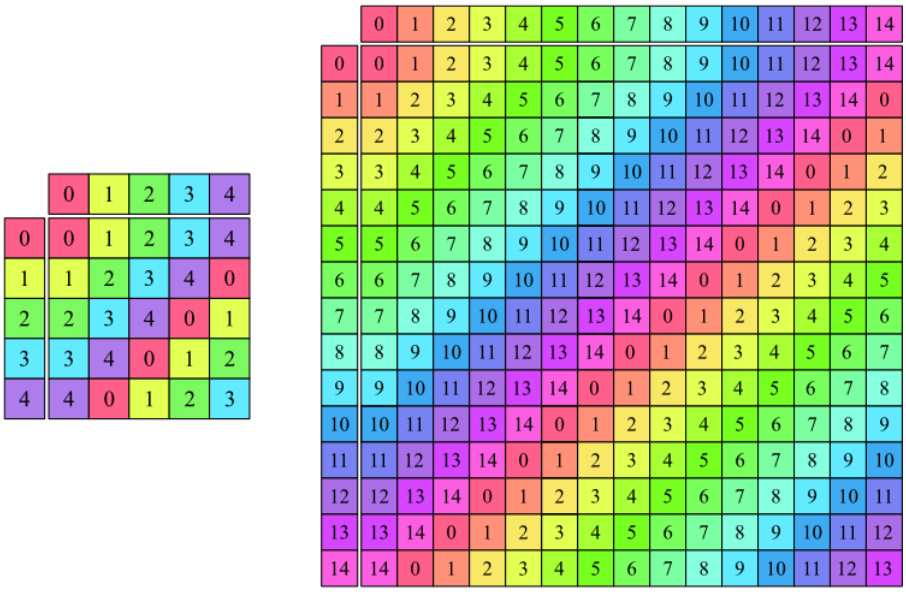


Figure 5.4. Multiplication tables for the groups C_5 and C_{15}

在 C_5 中所做的运算正式名称叫“剩余类加法（modular addition）”，或者通俗点，也叫“时钟加法（clock addition）”。它的原理跟我们观钟识时间的方法很像——数字排成了一个圈，这种加法也是如此。举个例子，假如你在晚上十点（10:00pm）的时候开始看一部时长三个小时的电影，电影的结束时间就是凌晨一点（1:00am），这时你肯定不会说是 13:00pm，因为在你的心底已经自动做了转换。这种转换用数学语言来说就是“将 10 和 3 在模 12 的意义下相加”，也即相加的和再对 12 取余数；因此，当两数相加的和大于 12 时，比如 13，就会重新返回到 1. 你家墙上挂着的钟和 C_{12} 的凯莱图之间唯一的区别只是：钟最上面的数字是 12，而凯莱图中是 0 而已。这并不是什么本质上的不同，纯粹只是习惯问题。

同样的，在 C_5 中，当我们做 3+4 时得到的并不是 7，因为 C_5 只包含 0，1，2，3，4 这五个数字。那怎么加呢？很简单，从 3 出发，走四步（很明显，这不就是 3+4 的意义嘛），我们就得到 $3 \to 4 \to 0 \to 1 \to 2$，所以结果就是 2. 在 C_5 中自己试着算一下 3+2，正确答案是 0，看看自己有没有真正理解。如果你想象不出一个 5 小时进制的时钟，那就参考图 5.3。

剩余类加法在乘法表中的表现形式具有十分美妙的视觉效果：乘法表中任意一行都可由其上面一行中的每个元素往左挪一个位置得到。这种特征在涂了颜色的乘法表中表现为，色谱沿着主对角线方向渐变，产生一种如彩虹般的美丽效果。参看图 5.4 的右图，它是 C_{15} 的乘法表。这张表也代表了循环群的乘法表所具有的一般模式。注意其中的副对角线，即从左下角到右上角的那条对角线。在副对角线的上方，加法都遵循普通加法

的规则，因为任一个和都不超过 14；在副对角线的下方，$mod15$ 的加法就不同了，从格子的颜色可以清晰地看到这一点。图 5.5 展示了一般的循环群 C_n 的乘法表。

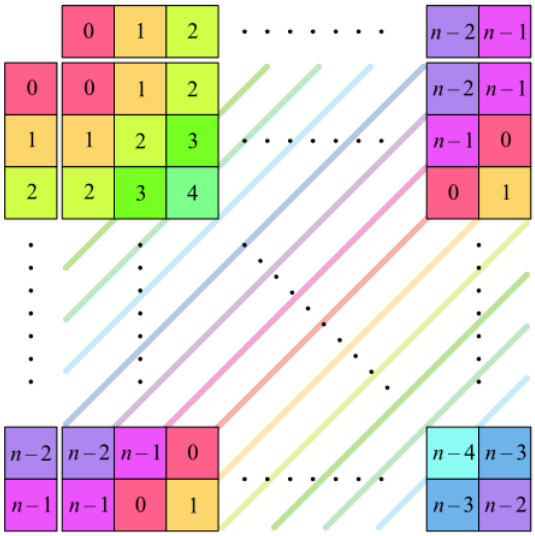


Figure 5.5. The pattern of multiplication tables for cyclic groups. The ellipses indicate linear sequences and the colored diagonal lines connect strips that are numbered (and therefore colored) the same.

5.1.3 轨道

我们之所以从循环群 C_n 切入对各种不同的群的学习研究，部分原因是循环群简单易懂，另一部分原因则是，循环群是研究其他群的基础。之后我们会遇到交换群，再后面是二面体群；尤其是二面体群，它可以由循环群按照一定的规则简单而直接的生成。不过首先还是让我们来看看怎么从任意一个群中辨认出它里面藏着的循环群。

让我们回顾一下本书中的第一个凯莱图，图 2.10，其中右上角的图是 S_3 的凯莱图。考虑 S_3 中的蓝色箭头，它表示的是作用 r. 我们从单位元 e 出发，沿着蓝色的箭头将走出一个圈，这个圈就是 C_3 在 S_3 中的拷贝。用标准术语来表述这个“圈”，我们称之为元素 r 所在的轨道（orbit）。轨道是一个集合，所以我们常用大括号 {} 来表示它；例如此处这个轨道就写作 $\{e, r, , r^2\}$.

群中的每一个元素都有自己所在的轨道。同样是在 S_3 中，如果我们从单位元 e 出发，沿着 f 箭头走，就得到了一个很短的轨道 $\{e, f\}$，这是因为 $f^2 = e$.

从图中我们可以很清楚地看出元素 r 和 f 的轨道：元素 r 所在的轨道就是外围的那个圈；元素 f 所在的轨道则只是一个简单的竖着的双向箭头。其他元素所在的轨道也是存在的，不过没这么明显。例如，要找元素 fr^2 所在的轨道，只需从单位元 e 出发，按照箭头顺序 $f \to r \to r$ 走就是了。注意，每次只有当走完一个完整的 $f \to r \to r$ 时，才

记录下你所在的节点，中间只是路过的节点不需要记下。这样，我们便找到了元素 fr^2 所在的轨道 $\{e, fr^2\}$. 这样的轨道隐藏得很深，没法一眼看出，但它确实是存在的，也确实是一个轨道。第六章将告诉读者，我们有很多方式去重整化一个凯莱图，以凸显其某种结构。因此，S^3 的凯莱图也有另一种表示方式可以将轨道清晰地体现出来，这种图就是我们下一节要讲的循环图。

有时，即使在凯莱图中一眼就能看出的轨道，可能看起来也并不具有一个圈的样子。考虑图 2.10 中的 $C_3 \times C_3$ 的凯莱图，元素 (e, a) 所在的轨道是其凯莱图中最顶上的一个圈，不过这个圈是“横着”排列的，它是循环群 C_3 在这个群中的拷贝。

如果我们依次找出 S_3 中所有元素的轨道，就得到了图 5.6 左边那一列（注意到集合 $\{e, r, r^2\}\{e, r^2, r\}$ 是相同的，因为我们认为轨道是一个集合，而集合中的元素不考虑次序问题）。我们不能给单位元 e 计算轨道，因为在凯莱图中并没有代表 e 的箭头。

Element	Orbit
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
f	$\{e, f\}$
fr	$\{e, fr\}$
fr^2	$\{e, fr^2\}$

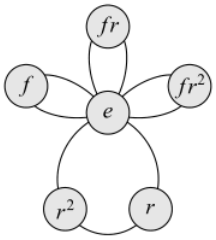


Figure 5.6. The orbits for the group S_3, shown on the left in a table, and on the right as the group's cycle graph.

5.1.4　引入循环图

根据如图 5.6 左边列出来的那张表，我们可以设计一种新的图，这种图能显示一个群的轨道结构。由于每一个轨道都是一个圈，所以我们就把这样的图叫作循环图。S_3 的循环图如图 5.6 的右边，它正是根据左边的表作出来的。

本章后面的部分将会频繁使用循环图，以便来展示各大群的家族是如何从一个个“圈”的基础上发展壮大的。注意到，循环群本身就是一个圈，所以它们的循环图相当显而易见。事实上，循环群的循环图就是它们的凯莱图；只不过在循环图中，我们习惯用不带箭头的线来连接节点。读者可以比较一下图 5.3 中的凯莱图和图 5.7 中与之相应的循环图。

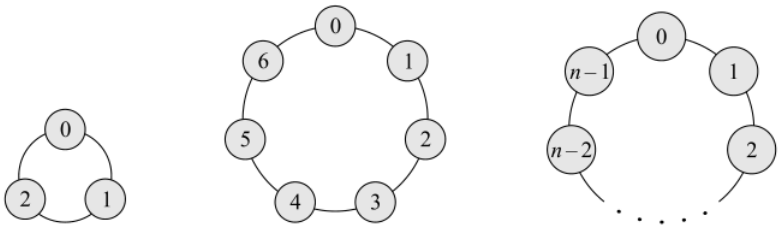


Figure 5.7. Cycle graphs for the cyclic groups C_3, C_5, and C_n, the same groups whose Cayley diagrams appear in Figure 5.3.

5.2 阿贝尔群

循环群可以自然地导出阿贝尔群（Abelian group）的概念。这一点体现在两方面：其一，所有的循环群都是阿贝尔群，阿贝尔群保留了循环群的某些简洁的特性；其二，我们将看到利用循环群可以自然地“拼凑出”阿贝尔群，这一事实被称为阿贝群基本定理（Fundamental Theorem of Abelian Groups），本章我们也会预告这一定理，对于其更深入的讨论留待第八章进行。

阿贝尔群，以尼尔斯·阿贝尔（Neils Abel）——群论的创始人之一的名字命名，它们是这样一种有趣的群：在这种群里面，元素间进行运算的次序不会对结果产生什么影响。也就是说，如果 a 和 b 是一个阿贝尔群里的作用（即元素），那么先进行 a 操作再进行 b 操作和先 b 后 a 的效果是一样的，用代数语言来说就是 a 与 b 可交换（commutative）。因此，阿贝尔群也常称作交换群。等式 $ab = ba$ 就准确表达了这一意思，我们说一个群是阿贝尔群即是说此等式对于该群中任意两个元素均成立。

5.2.1 凯莱图的非交换特征

为了搞清楚交换性会以怎样的方式影响一个凯莱图的样貌，让我们设想手边正好有一个阿贝尔群 G 的凯莱图，并且假设其中的红色箭头代表用 a 去乘，蓝色箭头代表用 b 去乘（我们这里的习惯是采用右乘顺序）。在这样的一张图中，ab 就表示先走一个红色箭头再接着走一个蓝色箭头；同理，ba 就表示先走一个蓝色箭头再接着走一个红色箭头。注意到交换性规定 $ab = ba$，因此，这意味着在阿贝尔群的凯莱图中，无论你从哪一个节点出发，先走一个蓝色箭头再走一个红色箭头与先走一个红色箭头再走一个蓝色箭头，到达的节点是一样的。图 5.8 形象地展示了这一点。

根据图 5.8 中的模式，我们可以很轻松地从凯莱图中识别该群是否为阿贝尔群：观察每一对蓝红-红蓝箭头组合是否呈现如图 5.8 右部中的菱形状。至于是不是构成一个标准的菱形形状并不重要（因为箭头有可能是弯的）——重要的是连接的模式必须得是

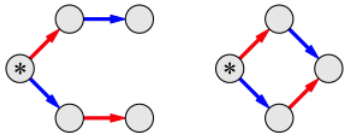


Figure 5.8. On the left is a pattern that never appears in Cayley diagrams for abelian groups: from the node marked $*$, following a red and then blue arrow does not reach the same node as following a blue and then red. The pattern on the right will always appear instead.

“菱形”。举个例子可能更好理解。

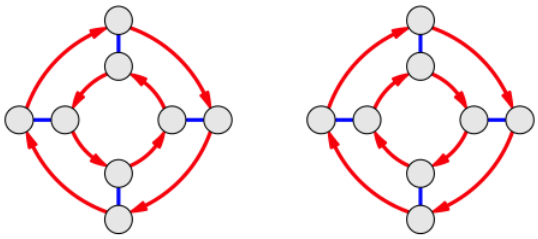


Figure 5.9. Cayley diagrams for two very similar groups, D_4 and $C_2 \times C_4$. Test these groups for commutativity by finding instances of the patterns in Figure 5.8.

图 5.9 展示了两个有细微差别的凯莱图。仔细观察这两张图，如果你能找到如图 5.8 中左边那样的模式，那么可以断言此群不是阿贝尔群。注意，不带箭头的“箭头”是双向的意思。当你仔细检查完后，可以跟图 5.10 对一下答案。

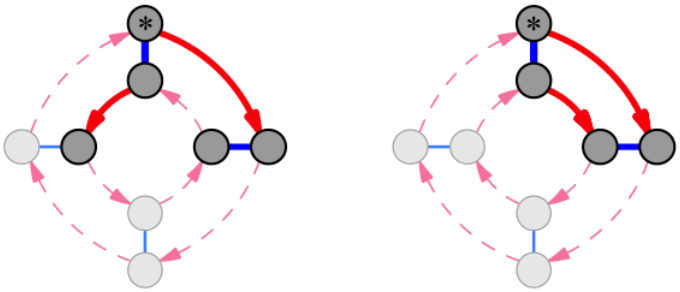


Figure 5.10. The diagrams from Figure 5.9 reappear here, highlighted to show instances of the patterns in Figure 5.8. The left diagram highlights an instance of the pattern that makes it non-abelian: if a stands for red and b for blue, then $ab \neq ba$ because from $*$, ab leads to a different destination than ba does. The right diagram highlights the analogous paths, but the pattern indicates commutativity.

图 5.8 中的箭头都是直的，而在图 5.10 中箭头变成了弯的，但是它们的连接模式本质上是一样的。注意到 $*$ 元素可以取作图中的任一节点，由此得到的模式是都跟高亮部分类似。凯莱图包含了丰富的对称性，在第八章中，我们会看到如图 5.8 那样的模式是如何奠定阿贝尔群基本定理的基础的。

5.2.2　乘法表的交换特征

与凯莱图相比，利用乘法表来识别阿贝尔群显得更加容易。考虑图 5.11，沿着主对角线将乘法表分为上三角和下三角两部分，并给下三角部分打上阴影。任取两个元素 a 和 b，标出它们所在的行和列，交出来的格子中有两个格子就分别是 ab 和 ba，显然 ab 和 ba 所在的格子关于主对角线对称。又因为 $ab = ba$，这意味着这两个格子里所填的元素是相同的，也就是说，格子连同其中的元素都关于主对角线对称。

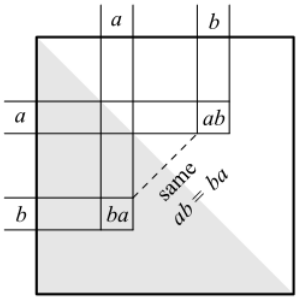


Figure 5.11. The equation $ab = ba$, which defines abelian groups, causes their multiplication tables to be symmetric across the diagonal shown here.

由于 a、b 的任意性，因此阿贝尔群乘法表的特征即为：整个上三角部分与整个下三角部分关于主对角线镜像对称。如果你将一个阿贝尔群的乘法表沿着主对角线折叠起来，那么两两相同的元素就会重合在一起。观察一下图 5.12 中的两个乘法表，根据上述对称性很容易识别出哪一个是阿贝尔群。

	e	r	r^2	f	fr^2	fr
e	e	r	r^2	f	fr^2	fr
r	r	r^2	e	fr^2	fr	f
r^2	r^2	e	r	fr	f	fr^2
f	f	fr	fr^2	e	r^2	r
fr^2	fr^2	f	fr	r	e	r^2
fr	fr	fr^2	f	r^2	r	e

	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,0)	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,1)	(0,1)	(0,2)	(0,3)	(0,0)	(1,1)	(1,2)	(1,3)	(1,0)
(0,2)	(0,2)	(0,3)	(0,0)	(0,1)	(1,2)	(1,3)	(1,0)	(1,1)
(0,3)	(0,3)	(0,0)	(0,1)	(0,2)	(1,3)	(1,0)	(1,1)	(1,2)
(1,0)	(1,0)	(1,1)	(1,2)	(1,3)	(0,0)	(0,1)	(0,2)	(0,3)
(1,1)	(1,1)	(1,2)	(1,3)	(1,0)	(0,1)	(0,2)	(0,3)	(0,0)
(1,2)	(1,2)	(1,3)	(1,0)	(1,1)	(0,2)	(0,3)	(0,0)	(0,1)
(1,3)	(1,3)	(1,0)	(1,1)	(1,2)	(0,3)	(0,0)	(0,1)	(0,2)

Figure 5.12. The symmetry of the table on the right tells us it is abelian. The left table does not have the required diagonal symmetry.

5.2.3　盘曲的循环图

非循环群的阿贝尔群常常拥有一些有趣而赏心悦目的循环图。观察一下图 5.13 中的诸循环图，我们只挑其中最简单的一个，左上角的那张循环图来近距离赏析一下。这是 $C_3 \times C_3$ 的循环图，它表明 $C_3 \times C_3$ 由四个长度为 3 的轨道组成。图 5.14 详细展示了在其凯莱图中的何处能寻找到这些轨道。

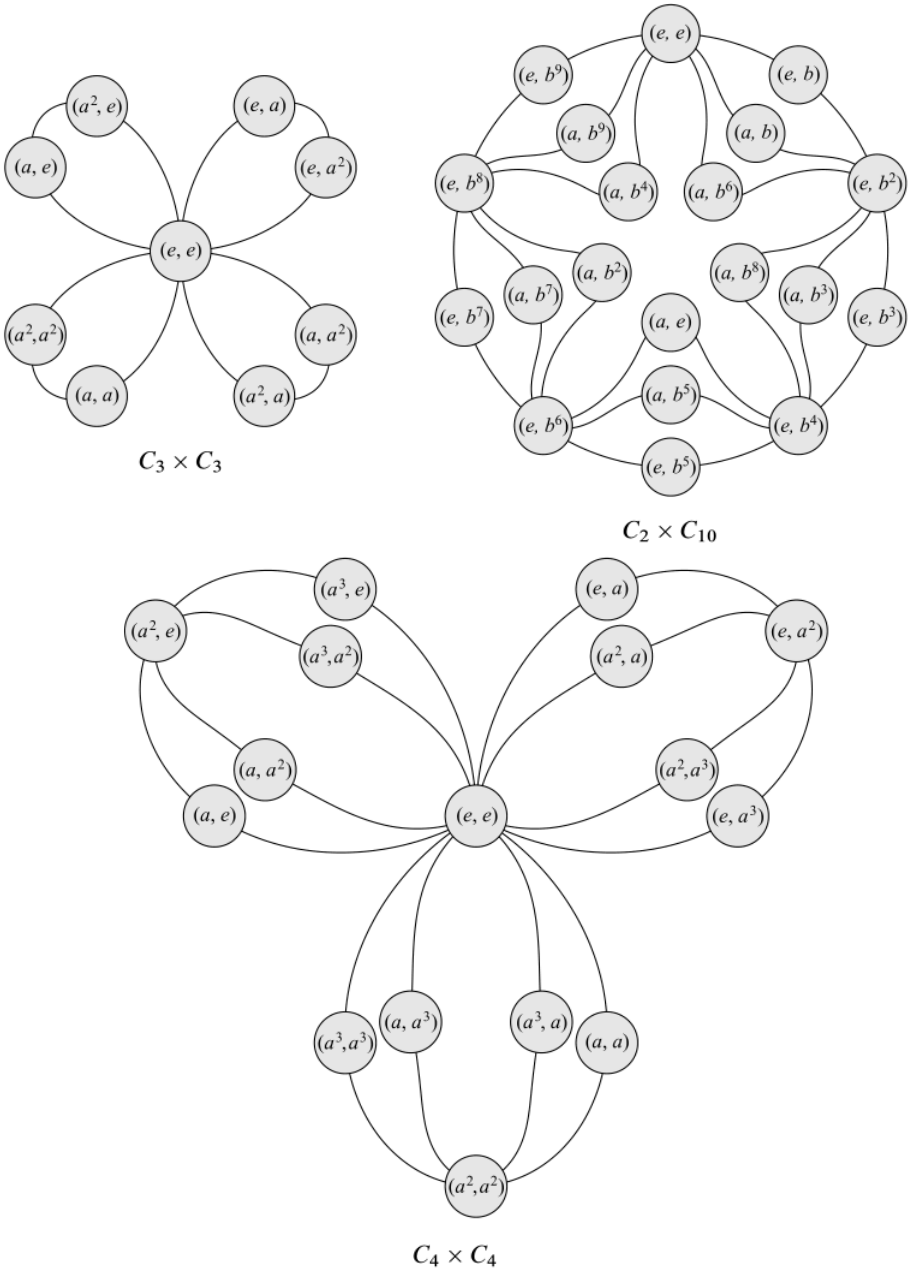


Figure 5.13. Cycle graphs for three abelian groups

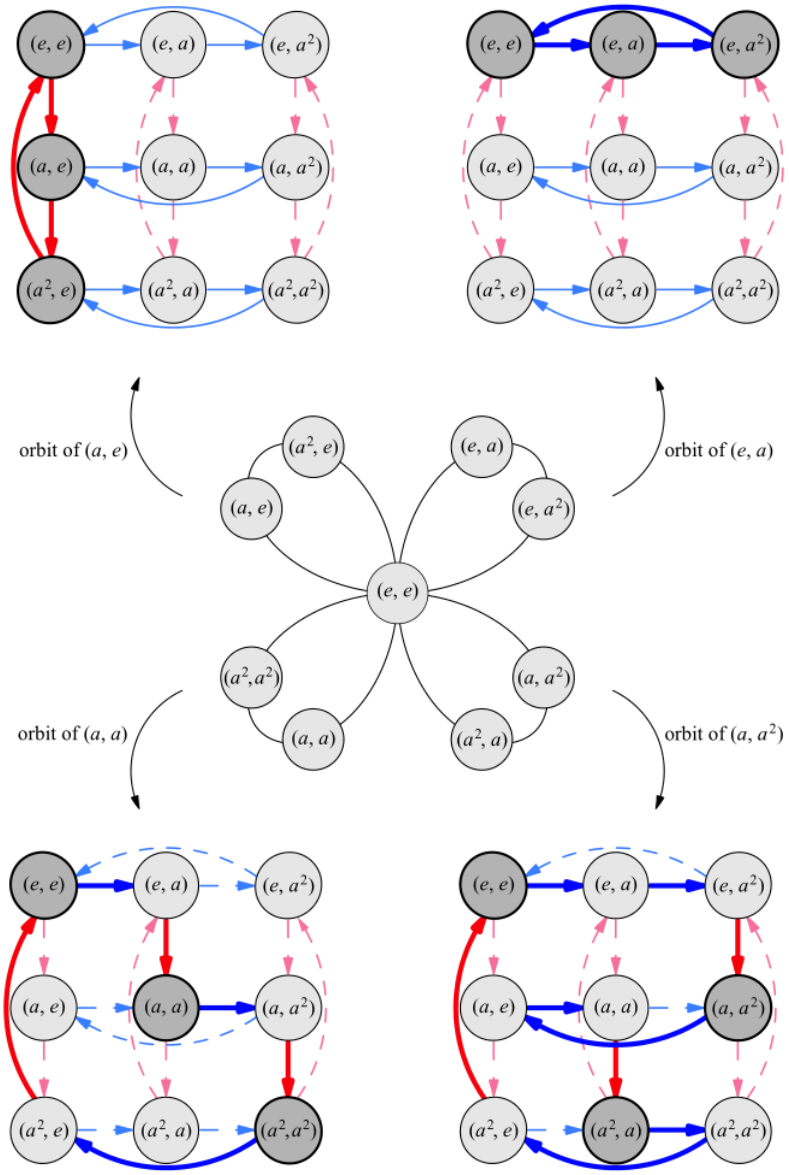


Figure 5.14. In the center is the cycle graph of $C_3 \times C_3$, and next to each of the four orbits is a copy of the Cayley diagram for $C_3 \times C_3$ with the corresponding orbit highlighted. These Cayley diagrams are structured like the original in Figure 2.10 on page 22.

顶上的两个轨道是十分显而易见的，它们分别由完全的红色箭头和完全的蓝色箭头走出来。另外两个轨道则需要红色箭头和蓝色箭头交替走出来，并经过上面两个轨道没到过的节点。

此处我们考虑的这个 $C_3 \times C_3$ 的循环图是某种一般情形的特例。在 8.4 节，我们将会遇到一个著名的定理，利用这个定理我们就能证明一般情形：对任意素数 p，群 $C_p \times C_p$ 的循环图总是含有 $p+1$ 个轨道，每个轨道里有 p 个元素，各个轨道相交于恒等元处。

不过现在我们得离开交换群的领域了，进入稍显复杂（事实上是十分复杂）的非交换群的世界。首先我们访拜的是二面体群（dihedral group），你已经在图 5.9 中的左图见识过二面体群 D_4 了，从那张图中你会发现尽管 D_4 是非交换的，不过它已经很接近交换了。

5.3　二面体群

5.3.1　翻转与旋转

我们知道循环群描述的是只有旋转对称性的物体的对称性，而二面体群（dihedralgroup）则可用来描述既有旋转对称又有轴对称（bilateral symmetry）的物体的对称性。所谓轴对称是指物体沿着某一个方向对折后，两侧的部分完全一样（这一说法等价于沿着某一方向翻转，翻转前后的图形可以完全重合）。图 5.2 表明螺旋桨不具有轴对称性——因为无论沿哪一个方向翻转，都不能使翻转前后的图形完全重合。几何上，同时具有轴对称和旋转对称的最简单的例子是正多边形（regular polygon），如图 5.15. “正（regular）”的意思是图形中所有的边和角都是一样大的。

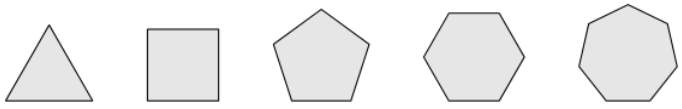


Figure 5.15. Regular polygons, from three- through seven-sided: triangle, square, pentagon, hexagon, and heptagon.

一个有 n 条边的多边形叫作 n 边形。描述正 n 边形对称性的二面体群，我们记作 D_n. 所有 C_n 中的作用也都在 D_n 中，这是因为旋转一个正多边形可以保持它的形状（即旋转对称）。注意到，正多边形还允许翻转（即轴对称），因此 D_n 中显然应具有比 C_n 更多的元素，事实上的确如此。循环群 C_n 中含有 n 个元素，而二面体群 D_n 中含有 $2n$ 个元素。让我们来看看这多出来的 n 个作用都有什么效果。

回想一下，C_3 描述了图 3.6 中硼酸分子的对称性，接下来让我们将其和正三边形，即等边三角形的对称性作个比较。（如果你做过习题 2.18，这和那个习题会很相似；如果没有，你可能就要自己来做一个标号的等边三角形，以保证你能跟上下面的节奏）我们已经知道旋转能够保持硼酸分子或螺旋桨或风车的形状，但是翻转却不行（参看图 3.4，3.5，5.2）。图 5.16 表明对于等边三角形来说，情况发生了变化：旋转和翻转都能保持其形状。

如果我们把如图 5.16 所示的旋转作为基本的旋转操作，并且暂时只做旋转变换，那么由此可得一个 C_3 的拷贝版本，并且我们已经知道这个群肯定位于 D_3 中。不妨把图中

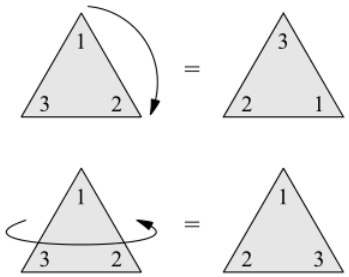


Figure 5.16. Both rotations and horizontal flips respect the shape of the equilateral triangle. The one shown here has its corners labeled to show the effects of those moves, as in Exercise2.18 (page 24).

所示的旋转记为 r，那么我们拷贝的 C_3 就是 r 所在的轨道。我们把图 5.16 中所示的翻转作为基本的翻转操作，并记为 f。接下来让我们瞧瞧，同时使用 f 和 r 的轨道能够产生什么有趣的结果。从初始状态，对三角形做一个翻转将得到一个新的状态，这一状态还不曾在 r 的轨道中出现过，它是一个全新的状态。再从这个新的状态出发，使用 r 操作将得到另外两个新的状态。这样，我们新得到的三个状态加上 C_3 中的三个元素就总共是 6 个了。如果你从另外两个新状态出发，使用 f 操作就会发现又回到了 r 的轨道中去了。因此，D_3 中的全部元素就是 $\{e, r, r^2, f, rf, r^2f\}$。实际上，要是你做过习题 2.18，就会发现这其中具体的步骤和过程就是你制作凯莱图时所经历的那些步骤和过程。

5.3.2 D_n 的凯莱图

图 5.17 中最左边的那张图就是由上面描述所得到的 D_3 的凯莱图。你是不是觉得有点眼熟？因为这张图在本书中已经出现过多次，只不过之前我们提到它总是用“S_3”这个名字。事实上，对于这张图，无论是叫作 S_3 还是叫作 D_3 都可以，也都是常用的名字。不久之后你就会了解“S_3”这个名字的由来了。

二面体群可以有各种大小，但是既然作为一个家族，它们的凯莱图便拥有一些共有的重要结构特征。其他二面体群的凯莱图跟 D_3 的长得很像。图 5.17 中间的是 D_5 的凯莱图，最右边的是一般情形下 D_n 的凯莱图。

这些凯莱图的外面一圈是 r 所在的轨道，即循环群 C_n 的一个拷贝版本。里面是同样大小的一个圈，只不过所指向的方向是逆时针的，正好跟外面那一圈相反。为什么里面跟外面会恰好反向呢？想象一下你手里拿着一个处于初始状态（如图 5.16 的左边）的等边三角形，你的朋友和你面对面站着。那么你看到的是三角形的正面，你的朋友看到的则是三角形的反面；对三角形进行一次 f 操作（即翻转）的效果则是转换你们之间的视角。当你所见的三角形是处于它的初始状态时，你的朋友看到的三角形则是处于它的翻转后的状态，即图 5.16 的右下角的图。

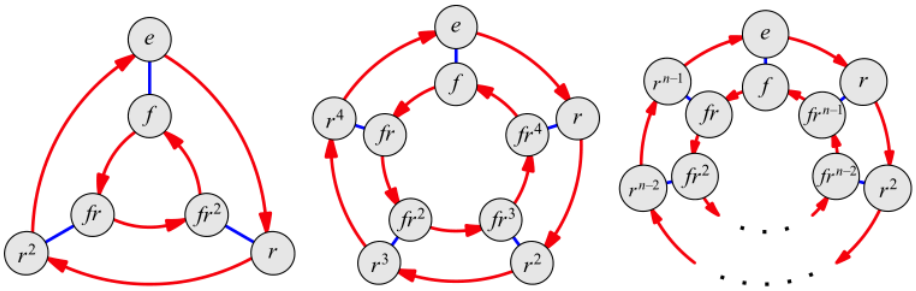


Figure 5.17. Cayley diagrams for the dihedral groups D_3 (left) and D_5 (center), as well as the general scheme for Cayley diagrams of D_n (right).

你给三角形施加一次 r 操作和你的朋友施加 r 操作的效果是不同的。举个例子，不妨假设三角形这时在你朋友手中，如果他将三角形顺时针转了一下，在你看来三角形则是被逆时针旋转了。如果是你在旋转这个三角形，也是同样的道理。你的顺时针旋转在你朋友看来则是逆时针旋转。也就是说，原本旋转的效果经过翻转变换后则变成了完全相反方向的旋转。用代数语言来描述这个道理会非常简洁：$frf = r^{-1}$. 这个式子的实际意义很明确：先一次 f 操作是将你从你的视角转成了朋友所在视角；再一次 r 操作是指你朋友将三角形进行了旋转；最后又一次 f 操作是将你的视角再次切换成自己的。因此式子的左边表示的实际意义正是“从你的角度看你朋友对三角形所做的旋转”，根据我们上面的分析，你看到的将是反向的旋转，即 r^{-1}，因此我们就得到了等式 $frf = r^{-1}$.

所以，图 5.17 的那些凯莱图内部的圈事实上描述的是你朋友看到的旋转效果。由于做一次 f 操作（即翻转）就可以转换你们彼此之间的视角，因此 f 操作连通了外面的圈和里面的圈。这样，我们就能理解为何里面的圈和外面的圈是反方向的了：外面的圈是你看到的旋转效果，里面的圈是你朋友看到的旋转效果，你们之间存在着视角的切换。

5.3.3　D_n 的乘法表

在 D_n 的凯莱图中，我们能明显看出它分成了内外两个部分——这一现象在 D_n 的乘法表中也是可见的。观察图 5.18，这是 D_5 的乘法表。可以直观的感觉到按照水平和竖直对半分，我们能把整张表分成四个区域；实际上，表格的颜色就在暗示我们应该这么分。

这是因为乘法表的表头（表的第一行和第一列）写得很考究：凯莱图中处于外圈位置的元素（(e 至 r^4) 写在了前面，紧接着才写处于内圈位置的元素 (f 至 fr^4)。这就使得乘法表左上角那四分之一块只包含由外圈元素相互作用所得的结果。因此，这一块实际上就是拷贝了一份 C_5 的乘法表，从凯莱图也能看出这一点，因为外圈正好构成了 C_5.

这张表将会在下一节和习题 5.35 中被进一步讨论。

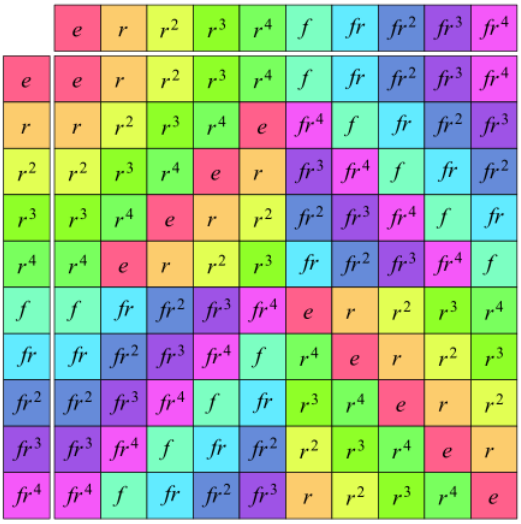


Figure 5.18. Multiplication table for the dihedral group D_5

5.3.4　第七章的一个预告

我们从整体上再来看一下图 5.18. 位于左上角的四分之一块使用的颜色和位于右下角的四分之一块使用的颜色是相同的；同理可发现，位于左下角的四分之一块和右上角，颜色上也是契合的。这种颜色上的特征将乘法表中不含 f 的那些元素所在的两个四分之一块归到了一起，将其中包含 f 的元素所在的两个四分之一块归到了一起。我们不妨把不包含 f 的那些元素统称为 $non-flip$，把含有 f 的那些元素统称为 $flip$，这样我们就会可以发现以下事实：

任意一个 $non-flip$ 乘上一个 $non-flip$，得到的结果是 $non-flip$；

任意一个 $non-flip$ 乘上一个 $flip$，得到的结果是 $flip$；

任意一个 $flip$ 乘上一个 $non-flip$，得到的结果是 $flip$；

任意一个 $flip$ 乘上一个 $flip$，得到的结果是 $non-flip$.

将这一事实用图注释出来就得到了图 5.19，一个覆盖在原有 10×10 表格上的、简洁的 2×2 表格。这个 2×2 的表格事实上正是二阶群（二阶群存在且唯一）的乘法表。

通过观察 D_5 乘法表的颜色特征，我们发现了这张表内部实际上还隐藏一个更小的群 C_2 的结构。依照这种方式“缩小”一个群，我们称为对群“作商（taking a quotient）”。这里，我们对于“商（quotient）”这一概念只是稍稍预告一下。群的商以及它的互补概念，群的积（product），对于群论的研究具有核心重要性，第七章将会详细探讨这两个概念。我们也将学习到：一个二面体群 D_n 可以由 C_n 与 C_2 作“半直积（semidirect product）”得到。从图 5.19 得到的商群正是半直积这一运算的逆运算。

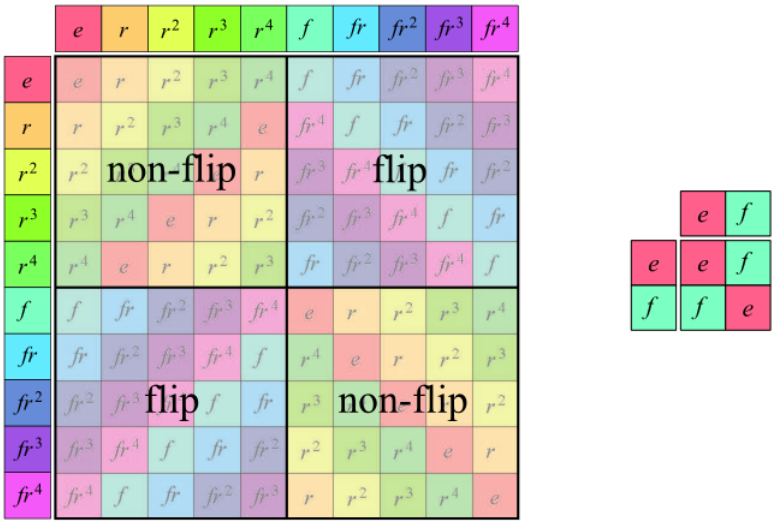


Figure 5.19. Multiplication table for D_5 with annotation that clusters elements according to whether they involve a flip. The resulting two-by-two pattern matches the multiplication table for the group of order two, shown on the right.

5.3.5　D_n 的循环图

在离开二面体群之前，让我们来看看它们的循环图以巩固我们对 D_n 中的元素所扮演的角色的理解。图 5.6 表明，D_3 中元素 r 所在的轨道包含 3 个元素，不在此轨道中的元素都位于一些更小的轨道上，这些小轨道的构成很简单：只包含恒等元和每一个元素自己本身。对于更高阶的二面体群的循环图，也都沿袭了这种模式：D_n 中元素 r 所在的轨道包含 n 个元素，其它的 n 个元素，每一个都位于自己的那个只含两个元素的小轨道上。下面就让我们来看看为何如此。

对于 D_n 中任意一个不在轨道 r（即元素 r 所在的轨道）中元素都可以写成 fr^m 的形式，其中 m 是 0 到 $n-1$ 之间的整数（要是你不懂为什么可以这么写，可以回过去看看图 5.17）。接下来我将说明，为什么做两次 fr^m 的效果跟什么都不做是一样的？回忆一下 5.3.2 节中所描述的情境，你和你的朋友拿着一个三角形。那个例子告诉我们操作 frf 的效果和 r^{-1} 是相同的，之所以是相同的，是因为这个情境让我们意识到将 r 两边用 f “包围”（即 $frf = r^{-1}$），其实就是将角色的视角进行了切换。运用类似的方法，我们会发现将 r^m 两边用 f “包围”（即 $fr^m f$）等效于进行 m 次 r^{-1} 操作（即 r^{-m}）。因此，先做 $fr^m f$ 操作，再来 m 次 r 操作（即 r^m）就回到了初始状态。用代数语言来表达即为：$fr^m f = r^{-m}$ 或者 $fr^m fr^m = e$. 这就表明，连续做两次 fr^m 的效果跟什么都不做是一样的！

我们上述的解释并不依赖于正多边形的形状，你和你的朋友拿的还可以是正五角形、正方形或其它正多边形。所以，在任意一个 D_n 中，不在 r 轨道上的元素都拥有一个

自己的长度为 2 的小轨道。这就揭示了 D_n 循环图的特点：以一个长度为 n 的圈为主体，附带许多长度为 2 的小圈，并且这些小圈都连接在恒等元处。图 5.20 展示了 D_4、D_5 以及一般情形 D_n 的循环图。

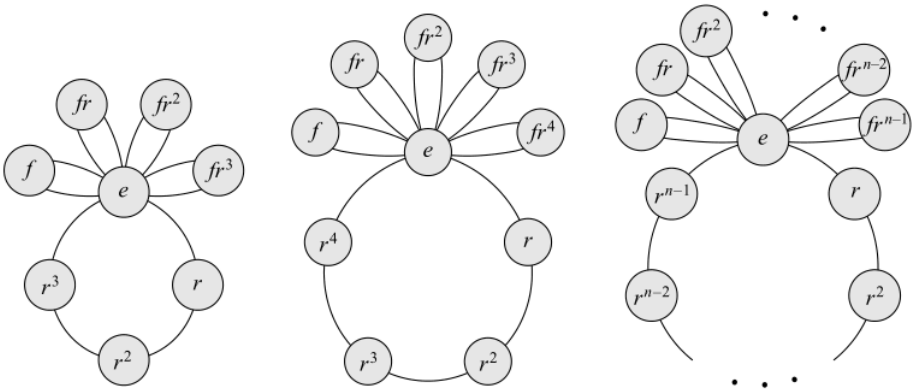


Figure 5.20. Cycle graphs for D_4, D_5, and the general pattern for D_n

这是我们碰到的第一个非交换群大家族，不过现在是时候离开 D_n 了。当你回忆图 5.9 时，你会记起，二面体群从结构上来看已经非常接近交换群，因此它们其实并不太复杂。接下来一节将会打开防洪闸门，让我们充分感受一下群论的复杂程度。

5.4 对称群与交错群

我们在本书中见过的很多群都跟重新排列（rearrange）东西密切相关。第一章的练习题要求你重排桌子上的硬币和墙上的图画，第一章也提到过魔方，这可以看成是对于带色贴纸的重排。在第三章中，我们给具有对称性的物体标上数字，以便于将对这些物体的操作转化为关于对数字的重排。重新排列（rearrangement），数学家们更喜欢称其为“置换（permutation）”，与群论有着紧密联系，这种联系体现在两方面：第一，我们即将拜访两个重要的群族，对称群（symmetric group）与交错群（alternating group），这两大群族可以通过置换概念自然地建立起来；第二，我们将赏味凯莱定理的一个可视化证明，而凯莱定理告诉我们置换是一种足够强有力的工具，利用这一工具我们能构建出任意一个群。

5.4.1 置换

所谓置换就是对物体的重新排列。置换可以用来描述洗牌过程、单词中字母的重新排列，甚至是你架子上那些 CD 分类的方式。不过，数学家们更喜欢去重新排列一些整数数字，因为这样可以方便的将置换写在纸上。

遵循这一习惯，让我们假设我们有四个东西可供排列：数字 1，2，3，4. 图 5.21 展示了几个置换的示例。要说明的是，数学家们用来表示置换的记号五花八门，这里以及接下来的内容，我们都采用如图 5.21 那种方式来表示置换。



Figure 5.21. Three example permutations of the numbers 1, 2, 3, and 4. For example, the leftmost one permutes the elements by moving each one step to the right, but moving 4 all the way to the left. The central permutation does not alter the positions of 1 or 4, but swaps the other two numbers.

5.4.2　置换群

置换，跟我们一开始的群的定义（定义 1.9）契合的非常好。取定一些东西（比如数字 1，2，3，4）进行置换，将所有的置换放在一起，这样我们就有了一组给定的作用（actions），因此符合规则 1.5；显然这些置换每个都是明确的，没有歧义的，因此符合规则 1.7；进一步，图 5.22 展示了如何将两个置换复合，从中可以看出任意两个置换相继作用的效果都与其它某一个置换单独作用等价，这也就是说任意两个置换复合后仍是一个置换，因此符合规则 1.8；如图 5.23 所示，显然每个置换都是可逆的，因此符合规则 1.6。所以，这就解释了为什么本书中有这么多群都跟“重排东西”有关：置换（permutations）本身就符合群的定义，它们是构建群的天然材料和工具。

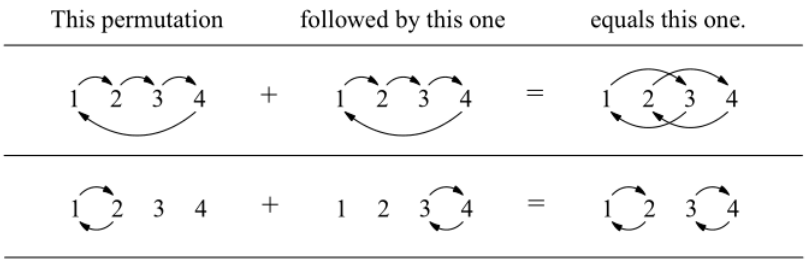


Figure 5.22. Two examples of combining two permutations to form a new one. In the top row, the first permutation moves 1 to 2, which the second permutation moves to 3, so their combination must move 1 to 3. In the bottom row, the first permutation moves 1 to 2, which the second permutation leaves untouched, so in combination, they move 1 to 2. Try following the paths of 2, 3, and 4 through each pair of combined permutations yourself.

举个例子，习题 1.4 要求你计数出在三面墙上排列三幅图画的所有可能的方式，习题 2.5 在习题 1.4 的基础上，进一步要求你画出那个群的凯莱图，同时习题 4.8 要求你再绘制出那个群的乘法表。在本章中，我们知道以上三个习题里涉及到的那个群有一个新颖的名字“D_3”，不过在此之前我们更熟悉它的另一个名字“S_3”。字母 S 表示对

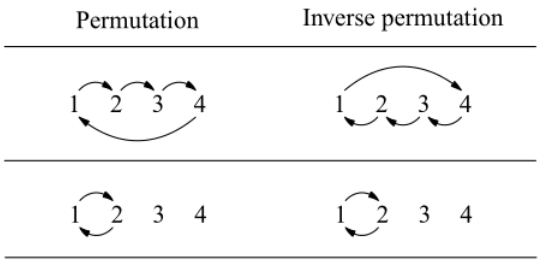


Figure 5.23. Two examples of permutations alongside their inverses. Try combining each permutation shown here with its inverse, in the way Figure 5.22 combines permutations. The result will always be the permutation that moves no numbers.

称（symmetric）的含义，这是因为由给定事物的所有置换所构成的群被称作“对称群（symmetric group）”。因此，S_n 就表示由 n 个东西的所有置换所构成的群。

我们已经见过好多次 S_3 了，不过迄今为止还没有碰到对称群家族中其他的成员。这个家族中的最小成员 S_1 和 S_2 留待读者在习题 5.18 中自行分析。至于更高阶的 S_n 则非常复杂而有趣。它们的阶数增长的极其迅速：群 S_n 的阶为 $n!$（即 1 到 n 的整数之积）。因此，S_4 的阶为 $1\times2\times3\times4=24$，$S_5$ 的阶为 $1\times2\times3\times4\times5=120$. 高阶对称群群，比如 S_5 的凯莱图可以变得极为纠缠混乱，以至于难以画出来。不过 S_4 的规模还不算太大，我们还是有办法将它的凯莱图漂亮的呈现出来，如图 5.24. 它是不是长得很像一个正方体？在下一节中，你就明白这其中自有奥妙，实非偶然！

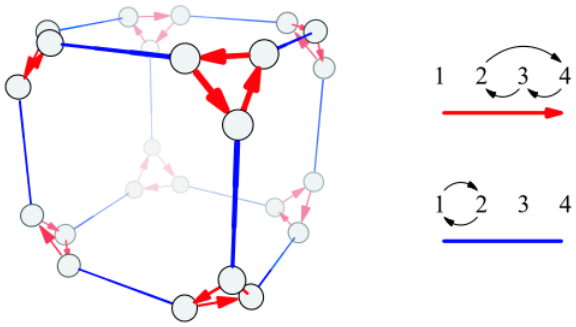


Figure 5.24. A Cayley diagram for S_4 arranged on a cube with clipped corners (usually called a “truncated cube”). The legend on the right shows which permutations in S_4 the arrows represent. Node labels were omitted to eliminate clutter.

现在我们知道，把 n 个东西的全体置换放在一起构成一个群，然而有时却并不需要所有的置换，往往只要取 S_n 中的某些置换就足以构作出一个群。其中一种著名的方法是只取 S_n 中一半的元素来构造所谓的“交错群（alternating group）”。当然，不是随便取出一半的元素都能作成群；实际上你随便取出一半的元素，它们能作成群的概率是很小的。但是，如果你将 S_n 中所有的元素都平方一下，那么平方后得到的元素就会刚刚好是 S_n 的二分之一，这样挑选出的元素构成的就是交错群，通常记为 A_n. 图 5.25 展示

了从 S_3 构造 A_3 的过程。如果你做过并且还记得习题 4.21，那么你就会知道 3 阶群只存在唯一一种结构，因此 A_3 的结构和循环群 C_3 是一模一样的。

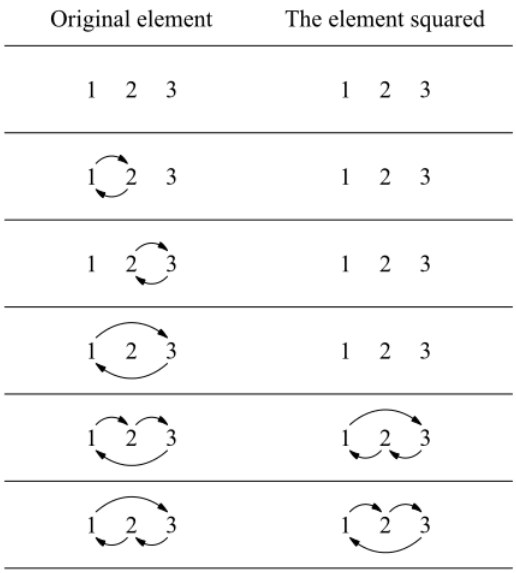


Figure 5.25. The left column shows all the elements of S_3 as permutations, and the right column shows all their corresponding squares. Because four of the six elements square to the identity (the permutation that moves nothing around, the "no action"), the right column contains only three distinct elements. Those three elements comprise the group A_n.

5.4.3　正多面体

在三维空间中，每个面都是正多边形且交角相等的立体图形只有五种，我们称之为正多面体或柏拉图立体（Platonic solids）。在图 5.26 中你可以看到这些正多面体的立体图。我之所以在这里提到正多面体，是为了展现它们与对称群、交错群之间的有趣联系。

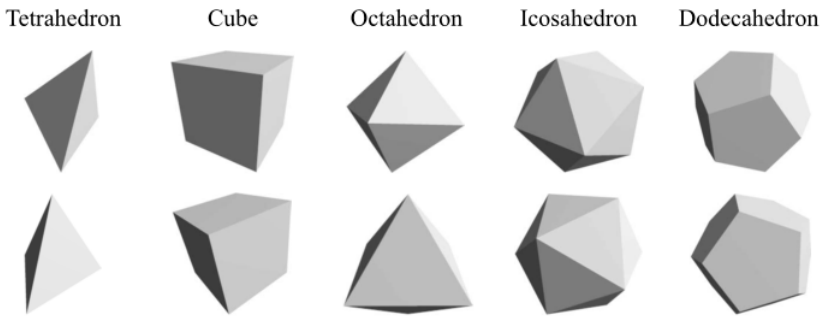


Figure 5.26. The five platonic solids, the only three-dimensional objects that are comprised of faces made of the same regular polygon repeated, connected to one another at the same angle throughout. Each solid is shown from two different angles, to help indicate depth.

回忆一下第三章教给我们的分类三维物体对称性的技术。在那里，我们将此技术应用到了分子、舞蹈者以及一些其他事物上。我们当然也可以用此技术来研究正多面体的对称性。习题 5.25 要求你就正四面体作一个尝试练习。把这一技术应用到其他正多面体上，尤其是正二十面体和正十二面体，是一项艰巨的挑战。这一工作已经有人做过了，我们这里只看结果。

能描述正四面体的对称性的群是 A_4. 我们可以将它的凯莱图画得漂亮一些，如图 5.27，以便能更清晰地展示 A_4 与正四面体之间的联系。正方体和正八面体共享同一个对称性群：S_4. 这就解释了为什么在图 5.24 中展示的 S_4 的凯莱图长得那么像一个正方体。我们也可以将 S_4 的凯莱图画的像一个正八面体，只要调整一下红蓝箭头所分别代表的置换即可，如图 5.28，你可以和图 5.24 对照着看。正十二面体和正二十面体也共享同一个对称性群：A_5——一个 60 阶的群。同样地，A_5 的凯莱图既可以画成类似于正十二面体的形状，也可以画成类似于正二十面体的形状，如图 5.29 所示。

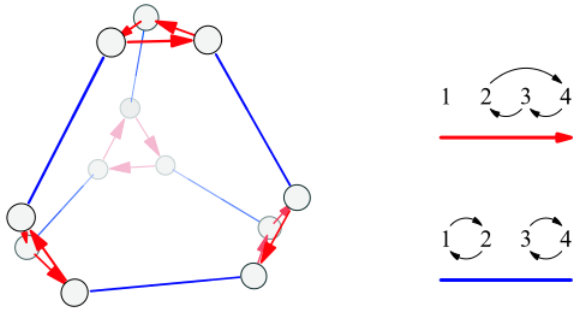


Figure 5.27. A Cayley diagram for A_4 arranged on a truncated tetrahedron. The legend on the right shows which permutations in A_4 the arrows represent. As in Figure 5.24 and Figures 5.28 and 5.29, node labels are omitted to eliminate clutter.

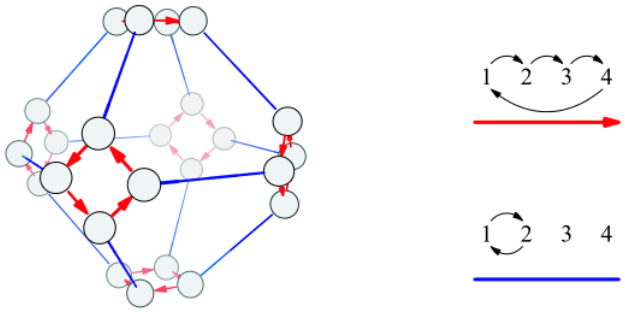


Figure 5.28. A Cayley diagram for S_4 arranged on a truncated octahedron. (Compare to Figure 5.24, a truncated cube.)

因此我们不难看出置换在群论中扮演着重要角色。我们已经了解到置换可以很容易的构成一个群，只需将一个给定大小的所有置换全部放在一起即可。我们将其称为对称群 S_n；然后再取出二分之一个 S_n 中的特定的元素，就构成了交错群 A_n. 我们发现群族 S_n 与群族 A_n 中的某些成员可以用来描述一些美丽的形状——正多面体的对称性。但是

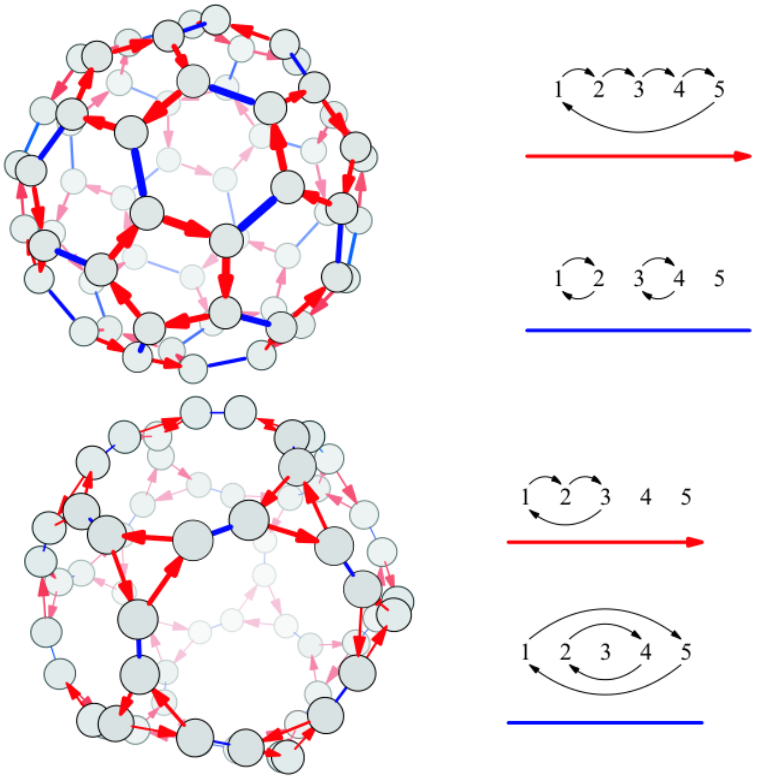


Figure 5.29. Two Cayley diagrams for A_5, one arranged on a truncated icosahedron and the other on a truncated dodecahedron. To make this possible, the arrows represent different elements in the one diagram than in the other.

远不止如此，还有另一个更加重要而深刻的途径能体现置换与群论之间的联系，而凯莱定理正是描述了这种深刻的联系。

5.4.4 凯莱定理

在 5.4 节的开头，我说过可以用置换构造出任意一个有限群，换句话说整个群论都可以由置换构建出来——这就是著名的凯莱定理（Cayley’s theorem）. 作为证明这一定理的先导步骤，让我们首先来看看如何从凯莱图和乘法表中发现隐匿于其中的置换。

考虑如图 5.30 左边的 S_3 的凯莱图。图中的节点已经用 1-6 的数字标好了，以便于我们使用熟悉的记号来表示置换。每一种颜色的箭头都代表一个置换：红色箭头将 1 变为 2，2 变成 3，3 变成 1，4 变成 6 等等。图 5.30 右上部分的图就是红色箭头所表示的置换。蓝色的箭头表示的置换则是对换两个数字，如图 5.30 的右下部分。为了从凯莱图中得到置换，我所做的只是将节点的数字标号依次写成一行，1 到 6，然后依照凯莱图的箭头所示，变换相关数字，并用我们熟悉的符号表示出这一变换过程（即置换），这就从凯莱图中提取出了置换。

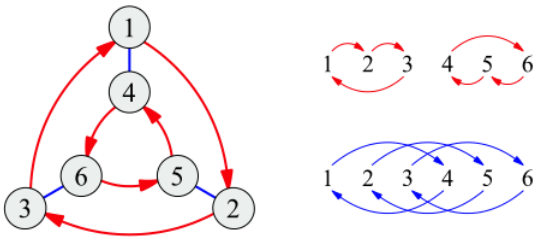


Figure 5.30. A Cayley diagram for the group S_3, with nodes numbered 1 through 6 to facilitate analyzing how the arrows permute the elements (shown to the right)

凯莱定理就是说，这样两个置换所表示的关系就等价于 S_3 中 6 个元素之间的关系。换句话说，如果我们用图 5.30 右边所示的两个置换来构建一个群，我们会发现得到的群是一个有 6 个元素的群且与 S_3 的结构完全一样！更精确的说，红色置换所起的作用和 S_3 中的 r 是一样的，蓝色置换所起的作用则与 S_3 中的 f 是一样的。两个群的结构完全一样，我们称之为“同构（isomorphic）”——这将在第八章中研究，目前我们只是不严格地使用这一术语。我们暂时还没有证明这一点，不过很快了。再让我们来看看置换与乘法表的联系。

在图 5.30 中，我们利用凯莱图的箭头从中提取出了置换，这里所有的乘法都采用的是右乘顺序。那么，对于乘法表呢？考虑图 5.31 所示的 V_4 的乘法表，其中的元素都用 1 到 4 的数字重新标识过了，以便于能简洁得和置换产生联系。

乘法表中每一个格子都是由其所在行元素与列元素相乘得到的结果。因此，乘法表中的每一列就表示用每一个行元素依次去乘上同一个列元素所得到的一列结果。举个例子，图 5.31 所示的乘法表中的第 3 列，就是将每一个行元素都右乘 3 得到的结果，也就等价于将每个群元素都右乘 3。因此，这一列实际上完整记录了群 V_4 中元素右乘 3 后的

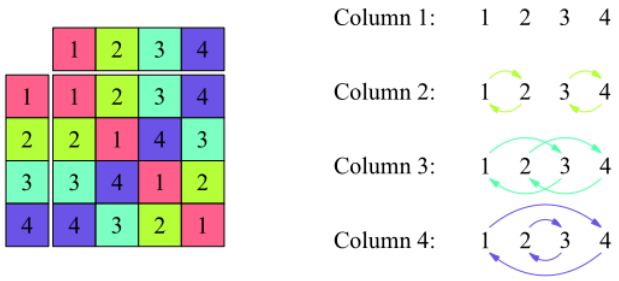
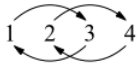


Figure 5.31. A multiplication table for the group V_4, with nodes numbered 1 through 4 to facilitate analyzing how the arrows permute the elements. The permutation for each arrow color is shown on the right.

全部可能效果。注意到行头只是简单的 1，2，3，4 依次排列，而将行头右乘 3 后所得的第三列则是 3，4，1，2；因此这一列就是一个置换：它将 1 变成 3，2 变成 4，3 变成 1，4 变成 2. 我们可以用以下的方式重新表述这一置换。这样我们就找到了从乘法表中



提取置换的方法：一列就是一个置换。图 5.31 中的乘法表所表示的置换就由它的四列所体现，将它们提取出来就如图 5.31 的右部所示。

注意到：对于任意一张凯莱图，我们都可以按照图 5.30 所示的例子中的步骤来提取其中的置换；对于任意一张乘法表，我们则可以按照图 5.31 所示的例子中的步骤来提取其中的置换。这两种方法的不同之处在于，从凯莱图中提取的置换是起到生成元作用的某些的“关键”置换，而从乘法表则可以提取出构成一个群的全部置换。这种差异的原因在于乘法表的表头包含了所有的群元素，而凯莱图的箭头往往只是代表生成元。凯莱定理将这两种情形统一起来，它表明由这些置换（无论是从凯莱图中提取的，还是从乘法表中提取的）所构造出的群与原来的群拥有完全相同的结构。现在，就让我们看看为什么凯莱定理是正确的。我们的证明基于图 5.30 和图 5.31 展示的可视化计算过程，最后将整个证明用图 5.32 展现出来。

定理 5.1 (凯莱定理)**.** *任意一个有限群都同构于某一个置换群*

证明. 我们已经知道乘法表的每一列就是一个置换，因此我们可以给给定群的每个元素都创造一个置换（因为乘法表的表头涵盖了所有群元素），就像图 5.31 所示那样。再考虑给这些置换做一张乘法表。我们的证明将解释为什么这样两张乘法表必须“表现得一模一样”。

假设已经给定了一个有限群，为了简便起见，让我们给这个群的每一个元素重新用数字 1 到 n 进行标识，并让 1 表示单位元。我们也需要给从群的乘法表中得到的置换以一些简便的记号表示，不妨设乘法表第 1 列表示的置换为 P_1，第 2 列表示的置换为 P_2，以此类推。我们用 P_1，P_2，$\cdots P_n$ 再构作一张乘法表，将这张新的表与原来群的乘法表相比较。

设想我们现在考察新的乘法表中的 P_i 行与 P_i 列相交出来的格子，假设这个格子的结果为 P_k，即 $P_i \cdot P_j = P_k$，下面我将证明这些置换以及它们之间的关系“忠实地（faithfully）”反映了原来的群元素及其关系。也就是说在原来的乘法表中必有 $i \cdot j = k$ 成立。

考虑这些置换对于原来群的单位元 1 的作用效果。因为 Pk 在原群中意味着“右乘 k”，将 P_k 作用到 1 上就表示将 1 右乘 k，即 $P_k(1) = 1 \cdot k = k$. 同理，将置换 $P_i \cdot P_j$ 作用到 1 上就表示先用 1 右乘 i，再右乘 j，即

$$P_i \cdot P_j(1) = 1 \cdot i \cdot j = i \cdot j$$

因为 $P_i \cdot P_j = P_k$，所以 $P_k(1)$ 和 $P_i \cdot P_j(1)$ 的作用结果必然是相同的，而前者的结果是 k，后者的结果是 $i \cdot j$，这就表明 $i \cdot j = k$. 由 i, j, k 的任意性，我们便知道，任何来自于置换的乘法表中的 $P_i \cdot P_j = P_k$，都只是相应的原群乘法表中的 $i \cdot j = k$ 的复制版本而已。因此，这个置换群的结构模式与原来给定的群是完全一样的，即证得定理之所述。 □

这个证明可以总结为两步：由群的乘法表得到每一列所表示的置换，然后检查这些置换对群的单位元的作用效果。图 5.32 阐明了这两步，它展示了由图 5.31 的例子所得到的置换的乘法表。每一个格子里，彩色高亮的部分表示的是将相应置换作用在单位元 1 上得到的结果。图 5.31 与图 5.32 之间的联系十分清楚：当我们只看图 5.32 中彩色高亮的部分，而忽略其它的时候，图 5.32 就变成了图 5.31 中的乘法表。

5.4.5 本章小结

想想看，在本章中你学到了多少新知识！你见识了群论世界中著名的五大家族，它们的大小、凯莱图以及乘法表。你学习了循环图，置换，还有一个非常基础而重要的群论定理的证明。正如我在前面所承诺的，你目前拥有的“群-图书馆”馆藏资源应该能让你回答我在本章开始所列举出的三个问题。在下面的习题中不断练习巩固你新学会的知识吧，尤其是那些 5.5.5 节的习题。

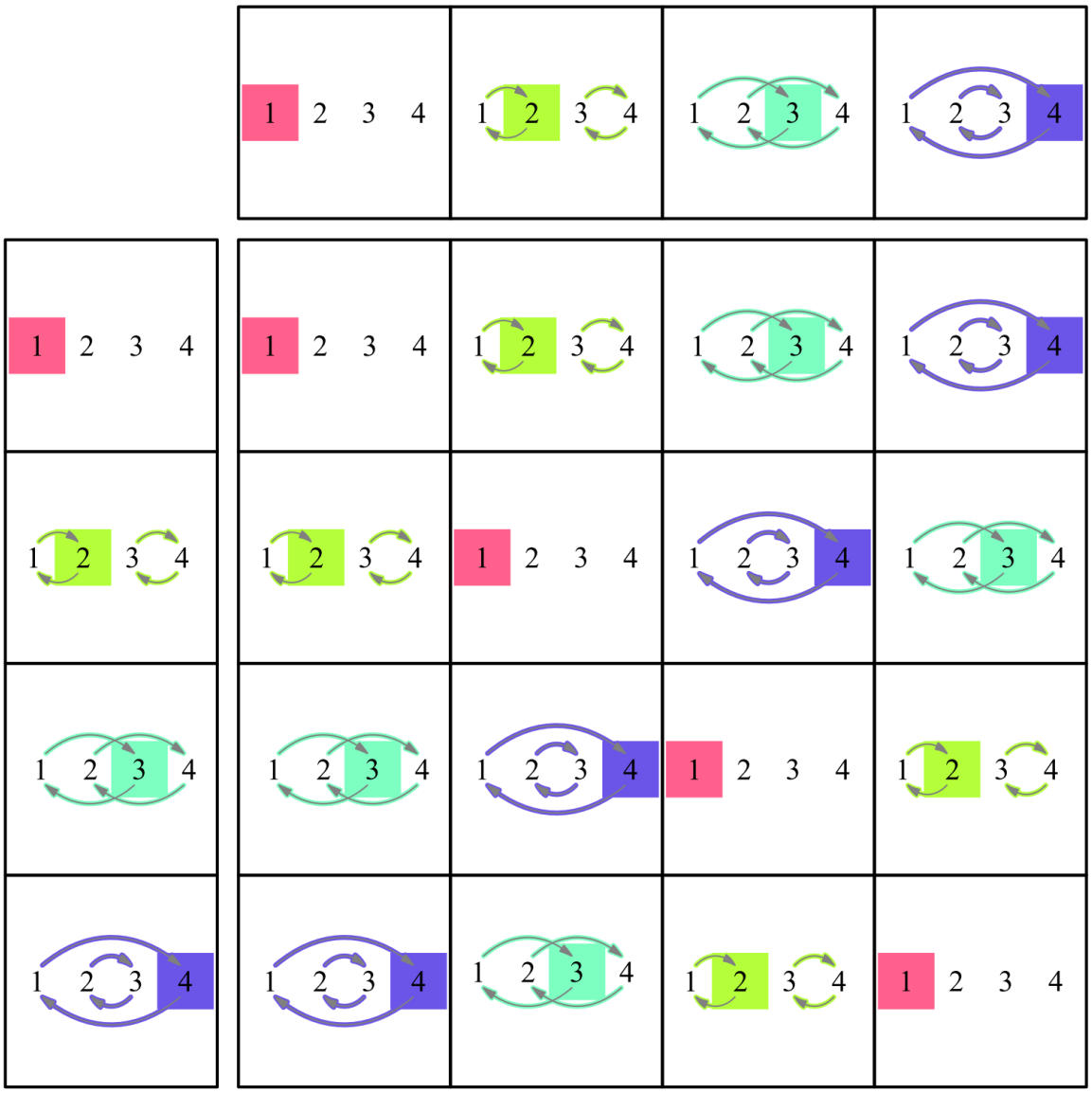


Figure 5.32. A multiplication table made up of the permutations created in Figure 5.31. Each cell highlights the destination to which the permutation sends 1, using the corresponding color from Figure 5.31, emphasizing what the colors of the arrows already showed: The two tables contain the same pattern.

6

子群

尽管本章的标题平平无奇，但实际上你已经来到了本书一个很 exciting 的部分！我用了半本书的篇幅让读者对群论有了足够的熟悉和了解，现在开始我们准备进行一些深入的探讨。从这一章开始，我们将要更多地开动大脑来分析问题，也会频繁遇到新的专业术语，但是这不意味着我会抛弃一直以来秉持的可视化原则。进入更高级的层面并不是说就非要将可视化的工具弃之不用；它仍然可能与在入门阶段时一样有用，甚至更甚。事实上，可视化极大地帮助了我更好地理解本书后半部分的材料内容，这也是我当初决定写这本书的一大动机。我之所以说本章很 exciting，是因为这章开始，我们将利用可视化的工具来揭示一些群论中的定理及其证明——定理与证明将会贯穿后半本书。

想要更深入地研究群论，这意味着我们需要提出更多的问题：群的结构都有哪些？群与群之间的联系如何？怎么样利用小阶群来构建大阶群？如何剖析大阶群以使其中的小阶群得以暴露出来？本章以及接下来的章节将会回答所有这些问题。这一章我们的主题是“往里看（look inside）”，搜寻一个群里面藏着的更小的群（subgroup），这将是其它进阶内容的基础，同时也将加深我们对于群的构成与所熟悉的可视化方法的理解。

我将用 6.1 节的内容来奠定基础，融合我们一直以来对于群的两套观点。我们知道，可以将群视为一堆作用的集合（a collection of actions），也可以看成是带了一个二元运算的集合。前者是基于作用（action-based）的观点，这可由凯莱图进行可视化；后者是基于代数的观点，可由乘法表进行可视化。代数的观点将教给我们关于凯莱图的一个最重要的事实，即所谓的凯莱图的“正则性（regularity）”。本章其余的小节将运用这种正则性的概念来简化子群的有关分析。

6.1　乘法表说了什么？

乘法表是群的代数观点的一部分，它使得我们可以运用等式来描述群中元素之间的关系。正如我们已经知道的，这些等式在凯莱图中是通过箭头之间的关系来体现的。考虑 S_3 的凯莱图，如图 5.17 的左边。等式 $frf = r^{-1}$ 在 S_3 中成立的原因是，路径 frf 与路径 r^{-1} 是完全相同的。这里“路径相同”的含义是指，走一个 f 箭头，接着走一个 r 箭头，然后再走一个 f 箭头到达的目标节点与从出发处走一个 $r-1$ 箭头到达的目标节点相同。

这一“路径相同”的性质对于凯莱图中的节点来说处处成立：不管你从哪一个节点出发。从单位元节点出发，路径 frf 与路径 r^{-1} 都最终到达相同的目标节点 r^2；从任意一个节点出发，这两条路径总是会到达相同的目标节点。我们可以把等式 $frf = r^{-1}$ 描绘的模式从 S_3 的凯莱图中抽取出来，如图 6.1 所示。

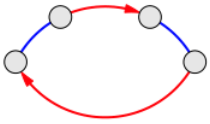


Figure 6.1. A Cayley diagram fragment representing the equation $frf = r^{-1}$. The top path, followed left-to-right, is frf, and the bottom path, followed left-to-right, is r^{-1}. This diagram indicates their equality by giving them common starting and ending points.

代数等式的成立意味着，由此等式所描绘的模式并不只对于凯莱图的某一部分成立，而是在图中处处成立。比如图 6.1 所示的模式并不只在 S_3 的凯莱图中某一处出现，而是对于 S_3 的每一个节点都有此性质。你现在应该明白了我为什么没给图 6.1 中的节点标上具体的符号，这是为了说明此图展示的模式在 S_3 的凯莱图中到处都是适合的。

注意，像这样无孔不入地渗入 S_3 的凯莱图的模式并不是唯一的。事实上，由 S_3 写出的任何一个等式都具有这样一种“无孔不入”、遍布凯莱图的性质。因此，任何一张凯莱图总是具有十分美妙的均匀对称性（uniform symmetry）：图的每一部分结构上都跟另一些部分相同。我们不能指望 $frf = r^{-1}$ 对于凯莱图的某些部分是成立的，而对于另一些部分则是不成立的；要么是处处成立，要么是处处不成立！

定义 6.1 (正则性). 我们称一个图是正则的（*regular*），如果此图内部的任一模式在整张图中，（以我们上面所讨论的意义）处处成立。特别地，任意一张凯莱图都是正则图。如果一张图不具有正则性，那么它一定不是群的图，因而我们也不把它称作凯莱图。

举个例子，请看图 6.2，我们把红箭头记作 r。在节点 $4-5$ 与 $6-7$ 之间，均有 $r^2 = 0$

成立；然而在 0 – 1 – 2 – 3 这一部分，事情发生了变化：$r^2 \neq 0$. 于是，这张图不具有正则性，也因此不是一张凯莱图，从而也不能描述一个群。

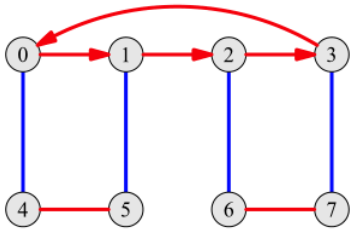


Figure 6.2. A diagram that satisfies many of the criteria for being a Cayley diagram, but violates one: equations about relationships among the generators change from one part of the diagram to another.

凯莱图的正则性向我们展示了群究竟是如何表现对称性的。我们之前就知道可以用群来度量对称性，并且我还说过凯莱图可以忠实地（faithfully）表示一个群：正则性正是这种忠实表示（faithful representation）的产物。群中任意部分都与其它部分看起来相同，群本身就具有满到快要溢出的对称性！

6.1.1 完善之前的定义

在习题 4.16 中，我要求你检查那两张图是否能成为凯莱图，其中一张正如图 6.2 所示。而早在习题 2.14 到 2.17 中，我便让读者试着建立一个判别准则，来确定一个满足了定义 1.9 所有要求的图是否能够表示一个群。你仔细验证的话，会发现图 6.2 所示的图满足了定义 1.9 的全部条件！因此，我们会想当然地认为这样一张图确实代表了一个群——这个结论却是错的！在前面，为了使第一章内容尽可能简单，我给出了所谓的定义 1.9；而我同时也强调过，此定义是非正式的（unofficial），我故意遗漏了一个重要的技术要点。正是这个技术要点的遗漏，使得我们仅仅从定义 1.9 出发，得到了一个似是而非的结论。

现在我们已经有能力来理解这个被遗忘的关键细节，其实就是 6.1 节中所述的：一张图不是凯莱图（换句话说不能表示一个群）——除非它具有正则性（regularity）。在第一章中，我一点也没提到图的正则性的概念，因为要说清这个概念需要用方程的语言，这一点不适合一开始就拿出来讲。在 4.4 节中，我们还有一个非正式（unofficial）的断言：任何一个由定义 1.9 确定出的群，也都可由定义 4.2 确定；现在来看，这一断言也是有瑕疵的。严格的表述只须再加入正则性的要求。

但其实也没必要：从对正则性的介绍当中，我们已经得到了想要的东西——即对凯莱图的更好的理解，这为接下来的小节做好了准备。在本书后面的内容中，我将把凯莱

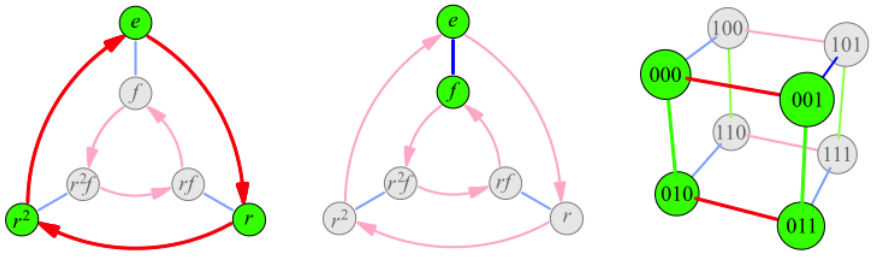
图作为我们首选的可视化工具（当乘法表更有用的时候，也偶尔会用到乘法表）。下面几节，我们就来充分利用“正则性”这一新观点来证明一些关于子群的基本定理。

6.2　初见子群

通过第五章的学习，我们已经熟悉了很多种类的群。关于它们的内部结构，下面让我们来多谈一点。由前面的内容，每一个群里面都蕴藏着一个或更多的循环群，我们把这些叫作“轨道（orbit）”。现在，让我们把这个想法加以推广，并不仅仅局限于循环群。

定义 6.2 (子群). *当一个群被完全包含在另一个群中时，我们把前者叫作后者的一个子群。若群 H 是群 G 的子群，标准记号记为 $H < G$.*

在第五章中，我们见到的所有轨道都是子群。举个例子，S_3 中元素 r 所在的轨道 $\{e, r, r^2\}$，是一个 3 阶循环子群，或者说是 C_3 的一个拷贝（a copy of C_3），我们就可以记作 $\{e, r, r^2\} < S_3$；当然啦，随意一点的话，也可以记为 $C_3 < S_3$. 这也是图 6.3 中第一张图所展示的例子。图 6.3 中第二张图展示的是 $\{e, f\} < S_3$，这个子群也是一个轨道。但是第三张图就不再是轨道了，因为高亮部分所表示的子群不是由同一种颜色的箭头构成的圈。利用从习题 4.25 处学到的关于生成元的记号，我们可以更方便的表示这些子群。比如，$\{e, r, r^2\}$ 是由 r 生成的，因此可以简洁地记为 $< r >$; 同理, 图 6.3 中展示的另外两个示例子群可以分别记为 $< f >$ 和 $< 001, 010 >$.



A copy of C_3 in the group S_3　　A copy of C_2 in the group S_3　　A copy of V_4 in the group $C_2 \times C_2 \times C_2$

Figure 6.3. Three Cayley diagrams highlighting easy-to-spot subgroups.

每一个群都必存在子群，理由如下：单位元 e 本身是任意一个群的子群，我们称其为平凡子群（trivial subgroup）；每一个群本身也是自身的子群（比如 $S_3 < S_3$），我们称其为非真子群（non-propersubgroup）。

图 6.3 展示的三个子群是很容易辨认出来的。因为从之前的章节中，我们已经很熟悉这些小群的样子了，所以就算是藏匿在大群中，也一眼就能辨识它们的凯莱图。倘若

图 6.3 没有给我们用高亮的色彩表示出来，我相信读者也能看出。但是，并非每一张凯莱图中的子群都是那么明显就能让你看出来的。图 6.4 展示了两个不那么明显的例子，然而这也不代表它们就完全毫无踪迹可循。因此，为了实现子群的可视化，我们还需要一些手段把它们从隐身之处揪出来。

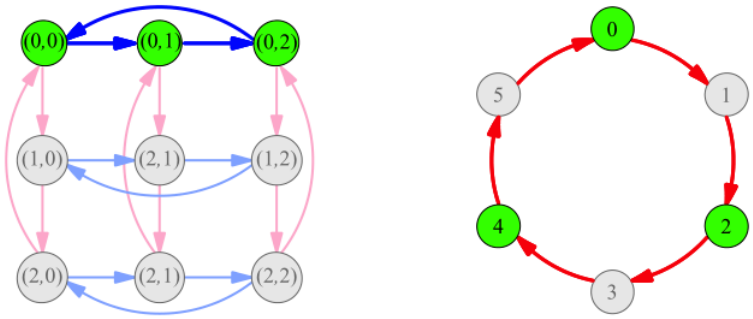


Figure 6.4. Two Cayley diagrams highlighting less obvious subgroups. The left diagram shows a copy of C_3 in $C_3 \times C_3$; the pattern is easy to spot, but it is not the familiar circular pattern of C_3. The right shows a copy of C_3 in C_6; each step in the copy of C_3 is *two* steps in the C_6 cycle.

6.3 窥探子群

任何一个子群都可以通过适当调整群的凯莱图使其得以显现出来。举个例子，回忆一下图 5.29，在这张图中展示了 A_5 的两种不同组织方式的凯莱图。一种凸显的是 A_5 中的 5 阶循环子群，另一种则凸显了 A_5 中的 3 阶循环子群；5-循环和 3-循环的圈在这两种图里显然可见。本节内容就来揭示，如何重组（reorganize）一个凯莱图以凸显其中某个特定的子群；在习题 6.26 中我还介绍了乘法表版本的重组方法。

使用生成元的符号语言可以大大简化关于凯莱图和乘法表构成形式的讨论。考虑 6 阶循环群 $C_6 = \{0, 1, 2, 3, 4, 5\}$，这个群可以用好几种不同的方式来生成，比如平凡的 $C_6 =< 1 >$ 以及 $C_6 =< 5 >$。还可以更出乎意料一点，我们可以写成 $C_6 =< 2, 3 >$；要是你真的为此感到惊奇的话，我建议你稍微想想，为什么在 *mod*6 的意义下，只用 2 和 3 就能得到 C_6 中的所有成员？（译注：考虑 *Bezout* 定理即可）单独的 2 或者 3 都不能生成 C_6，但是把它们放在一起就能生成 C_6 了！C_6 的这几种不同的生成方式也带来了相应的、各不相同的凯莱图画法，如图 6.5 所示。（不太熟悉的读者可以回过去参考习题 2.9）

图 6.5 中左边两幅图很明显就能看出来代表的是一个 6 阶循环群，而右边的两幅图则似乎看不出哪里像一个“圈”。左边两幅图凸显的子群都是非真子群 $< 1 >= C_6$；右边两张图凸显的则是子群 $< 2 >$ 和子群 $< 3 >$。你不妨花点时间，从右边两张图里找出子群 $< 2 >$ 和子群 $< 3 >$ 在哪儿。

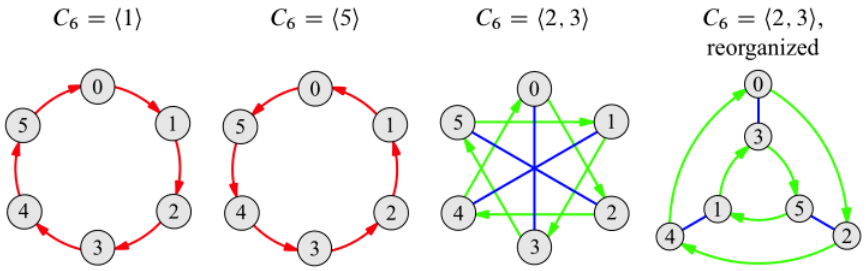


Figure 6.5. Four ways to connect a Cayley diagram of C_6, based on different choices of generators. Note how similar the rightmost diagram is to the familiar Cayley diagram of S_3. Can you spot the difference?

以上讨论带给我们的启发是，我们可以给群挑选合适的生成元，那么借由这些生成元就可以找到群中的子群并将其可视化展现出来；有时候为了使图的箭头不会纠缠在一起，我们还有必要重新排布一下凯莱图的布局。这也就是我用来找出 C_6 中的子群 $< 2 >$ 和 $< 3 >$ 的方法：首先我用 $< 2, 3 >$ 生成了 C_6，由此得到图 6.5 中的第三幅图；接着我重新排布了一下这张图使其看起来更清晰简洁，这就得到了图 6.5 中最右边的那张图。注意到，怎么重新排布凯莱图的方式并不唯一，所以并不存在什么“完美的”、“正确的”图的样式，只要能看得清晰，全凭你自己的喜好来排布就行了。

合理地选择箭头，恰当的排布方式都有帮于我们揭示出隐藏的子群，比如 $< 2 >< C_6$. 通过使用 Group Explorer 这一软件并参考它的相关说明文件，你可以很容易地进行自己的尝试，实验凯莱图不同的生成方式与箭头的组织安排方式。

6.4　陪集

迈向更深入研究的第一步是注意到：与子群完全相似的结构模式，或者叫“子群的恒同拷贝（identical copies of each subgroup）”遍布了凯莱图的其余部分。举个例子，考虑群 S_3 中子群 C_3 的拷贝，如图 6.3 最左边那张图；其中，一个结构上完全一样的 3 元循环圈也出现在了凯莱图的内部（尽管循环的方向反向了）。类似的，群 S_3 中子群 C_2 的拷贝在剩下的凯莱图中又出现了两次，如图 6.6 所示。

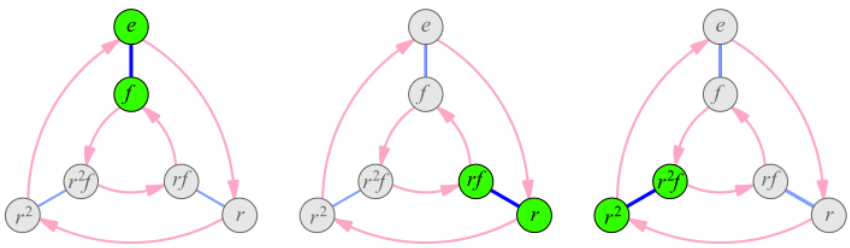


Figure 6.6. Copies of the subgroup $\langle f \rangle$ in S_3

但是这些拷贝版本却不再是子群了。一个子群，正由于它是一个群，就必须包含单位元。在图 6.6 中，只有最左边的 e, f 包含了单位元 e；而对于另外两张图，比如 $\{r, rf\}$，因为将 r 与 rf 相乘得到的 $r^2 f$ 已经不在这个集合内了，所以它就作不成群。因此，我们给集合 $\{r, rf\}$ 和 $\{r^2, r^2\}f$ 一个不同的名字：把它们叫作子群的“陪集（cosets）”，以表明它们仅仅只是在结构上拷贝了某一个子群（copies of a subgroup structurally），但是本身却不是群。

了解子群及其陪集将会揭示出群的一些重要的结构性质。让我们首先对陪集作一些观察，我将这些称为“观察（observations）”而不是定理，是因为这些事实非常简单，以至于我能够用一些非正式的语言来确证其正确性。在下面的内容中，凯莱图的“正则性（regularity）”概念将广泛使用，这在 6.1 节中我们已经介绍过。第一个观察指出，陪集并不局限于图 6.6 中的示例。

观察 6.3. *每一个子群都有陪集，子群与其陪集彼此不相交的覆盖该群的凯莱图。*

让我们看看为什么这个观察是对的。在图 6.3 中，我们之所以能把 e, f 写作 $< f >$，把 000,001,010,011 写作 $< 001, 010 >$，是因为任意一个有限群都存在有限个生成元，即使这个群本身还是另外一个群的子群。我们只需从凯莱图的单位元节点出发，用相应的生成元来探索，就可以找到并可视化一个子群。

但是实际上，这样的探索（exploration）可以从任何一个节点出发进行。我们考虑用群 G 的子群 H 的生成元来进行一场探索，如果从群 G 的单位元节点出发，我们不会得到什么别的，得到的正是子群 H；但是如果从 G 中的其它任意一个节点 g 出发呢？凯莱图所具有的正则性告诉我们，这样的探索将得到和子群 H 完全相同的模式结构，该结构只取决于子群 H，而与从哪个节点出发无关。因此，这样的探索就勾勒出了一个从节点 g 出发的子群 H 的拷贝版本。由正则性，群 G 的凯莱图就遍布了子群 H 的拷贝版本，或者说子群及其陪集可以完全覆盖整个凯莱图。

观察 6.4. *我们可以用代数的方法描述陪集。以节点 a 拷贝 H 得到的陪集有一个“代数的名字” aH.*

“名字” aH 可不是乱取的。回忆一下之前的内容，在凯莱图中做乘法 ab，其含义是指从节点 a 出发走一个路径 b 所到达的节点；因此，aH 也就有类似的含义：每次都从节点 a 出发，遍历 H 中的所有路径所到达的节点的集合。这就给出了以节点 a 拷贝 H 得到的陪集，其可视化的描述，因此，这样的命名方式是有意义的。遵循这一命名习惯，图 6.6 中，中间的陪集就可以叫作 $r < f >$，右边的陪集就可以叫作 $r^2 < f >$.

上面我们说的是利用凯莱图来形象地计算陪集 aH，不过我们也可以直接用代数的

方式来计算：只需用元素 a 依次去左乘（正如名字 aH 暗示的那样）子群 H 中的每一个元素。例如我们用这种方法来计算陪集 $r<f>$：

$$r<f>=r\{e,f\}=\{r\cdot e,r\cdot f\}=\{r,rf\}$$

正是由于这种左乘的方式，我们遇到的这种陪集实际上又被称为“左陪集（left coset）”。在下面两个观察之后，我还会介绍与之互补的一个概念“右陪集（right coset）”。

观察 6.5. 每一个陪集的名字并不唯一。

举个例子，$r<f>$ 是我们赋予图 6.6 中间那个陪集的名字，因为它是以节点 r 拷贝 $<f>$ 得来的陪集；然而事实上，我们也可以说它是以节点 rf 拷贝 $<f>$ 得来的陪集。再举一个例子，考虑图 6.3 中群 $C_2\times C_2\times C_2$ 高亮表示的子群（不妨就记作 H）。在 H 后面的那个陪集我们就有四种记法，$100H$,$101H$,$110H$ 和 $111H$，这是因为不管你从这四个节点中的哪一个出发，由 H 中的生成元进行探索得到的都是完全相同的陪集。其中更本质的原因则是凯莱图的正则性。

只要一个左陪集 aH 含有一个元素 b，我们就可以简单得将这个陪集也叫作 bH. aH 表示一个包含元素 a 的陪集，bH 表示一个包含元素 b 的陪集，由于它们意指同一个陪集，所以就让我们把这一点作为最后一个观察。

观察 6.6. 若 $b\in aH$, 则 $aH=bH$.

因此，在图 6.6 中，我们也可以把 $r<f>$ 叫作 $rf<f>$，把 $r^2<f>$ 叫作 $r^2f<f>$. 你所选的那个用来命名陪集的元素，我们称之为“代表元（representative）”。（译注：稍微熟悉等价分类概念的读者，看到这里就会意识到，实际上陪集正是用子群对大群进行分类后得到的一个个等价类！）

现在让我们稍稍冷落一下左陪集，把目光聚焦到其互补概念“右陪集（rig coset）”上——之前我就已经提到，但还没有正式展示过。从代数角度来看，你可以很自然地猜到我将会怎样来描述右陪集：一个右陪集 Ha 的计算方法与左陪集类似，只需用 a 依次去右乘 H 中的元素。比如，S_3 中子群 $<f>$ 的右陪集如下：

$$<f>r=\{e,f\}r=\{e\cdot r,f\cdot r\}=\{r,r^2f\}$$

$$<f>r^2=\{e,f\}r^2=\{e\cdot r^2,f\cdot r^2\}=\{r^2,rf\}$$

这些右陪集与我们所见的 $<f>$ 的左陪集没一个是相同的。因此，它们在凯莱图中势必又是另一番模样，让我们瞧瞧它们长什么样，这就涉及到如何在凯莱图上计算右陪集。

为了能形象的计算一个右陪集，我们只需要将处理左陪集时的方法反过来：每次从 $< f >$ 中挑一个节点出发，都走路径 r，当出发点遍历 $< f >$ 中所有节点后，所到达的节点集合就是右陪集 $< f > r$. 这一方法与代数计算方法是一致的；用 r 右乘了该子群中的所有元素。

图 6.7 比较了同一张凯莱图中的左陪集 $r < f >$ 与右陪集 $< f > r$。图 6.8 则展示了在一般情形下，左陪集和右陪集之间的区别。要着重说明的一点是，之所以在本书中左陪集长得像子群而右陪集中的元素似乎显得有些零散，看起来完全不像是“拷贝”子群而来的，其中的根本原因是我的“习惯”导致的——在书中，我默认凯莱图的箭头表示右乘。倘若我采用另一种习惯，用箭头代表左乘，那么这时候右陪集就会长得像子群了，而左陪集的元素则会分布得比较零散。

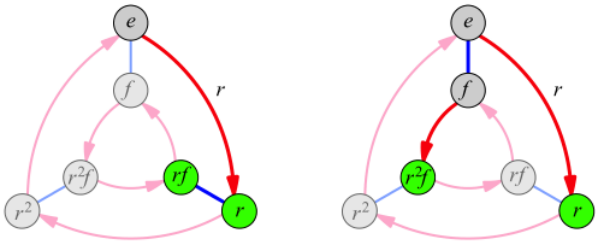


Figure 6.7. The left diagram shows the left coset $r\langle f\rangle$ in S_3, the nodes that f arrows can reach after the path to r has been followed. The right diagram shows the right coset $\langle f\rangle r$ in S_3, the nodes that r arrows can reach from the elements in $\langle f\rangle$.

子群 $< f >< S_3$ 是第一个很好的示例，因为它充分展示了左陪集与右陪集之间往往有着很大的不同。然而，左、右陪集也并非总是完全不同的，考虑这种情形具有非常的重要性，因此，来看一看这样的例子也很有价值。图 6.9 使用子群 $H =< (0,1) >< C_3 \times C_3$ 展示了当左陪集与右陪集相同时的状况。尽管这张图只描述了，对于 $g = (1,0)$，有 $gH = Hg$ 成立。然而实际上，$gH = Hg$ 对于任意的 $g \in C_3 \times C_3$ 均是成立的，具有这种性质的子群 H 由于其重要性，我们赋予其另外的特别称呼“正规子群（normal subgroup）”，在第七章我们会学习到它的重要作用。

利用乘法表来计算左陪集与右陪集也很方便，如图 6.10 展示的那样。我根据所给

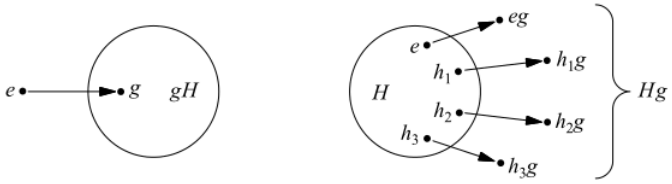


Figure 6.8. Each left coset gH is where H arrows can reach from g, which looks like a copy of H based at g, as in the left illustration. Each right coset Hg is the set of nodes to which the g arrows take the elements of H, as in the right illustration.

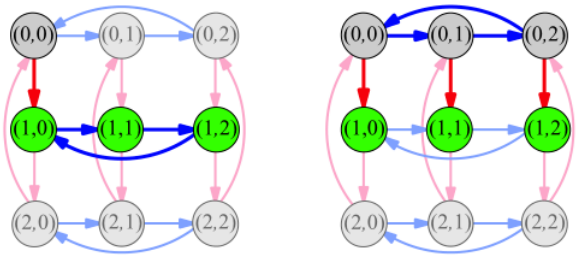


Figure 6.9. A left and right coset pair that are equal. Here $H = \langle (0,1) \rangle$ in the group $C_3 \times C_3$ and $g = (1,0)$; on the left we see the computation of gH and on the right Hg. The result is $\{(1,0),(1,1),(1,2)\}$ in both cases.

子群 $< f >$ 中的元素重新排列了一下乘法表的行头与列头。左陪集 $r^2 < f >$ 的元素一定出现在 r^2 行与 e、f 列的相交处，因为这些格子就表示乘积 $r^2 \cdot e$ 与 $r^2 \times f$. 在任何一张乘法表中，你都可以按这种方法来计算左陪集：左陪集 gH 中的元素位于 g 行与 H 诸列的相交格子处。另一方面，右陪集 Hg 也可以用类似方法计算，只不过要把计算左陪集时的“行”、“列”交换一下，即：右陪集 Hg 中的元素位于 g 列与 H 诸行的相交格子处。

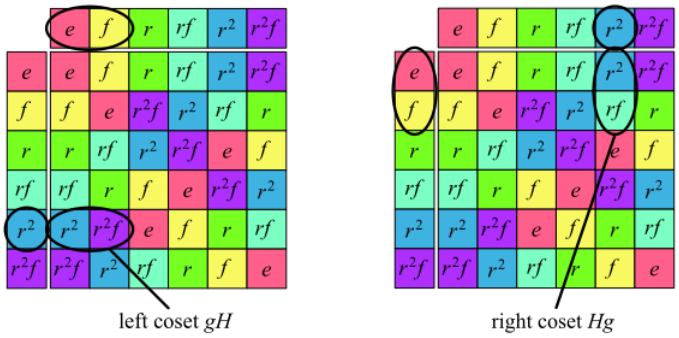


Figure 6.10. The visual computation of left and right cosets in multiplication tables. The computations of gH and Hg are exemplified for $H = \{e, f\}$ and $g = r^2$ in the group S_3.

6.5　拉格朗日定理

在迄今为止看过的子群及其陪集的例子中，有一个显著的共同特征值得我们予以特别关注，下面就让我们来具体谈谈这一点。观察 6.3 告诉我们，一个子群的左陪集可以完全覆盖整个大群。事实上，在上面见过的所有例子中，观察 6.3 不仅是对的，而且更进一步，我们还会发现大群中的每个元素都有且只有一个陪集作为其容身之处。图 6.6 形象地展示了这一点：子群 $< f >$ 的左陪集覆盖了 S_3，且不存在一个元素同时处于两个陪集，或者说任意两个陪集都不相交。这一点对于子群 $< f >$ 的右陪集来说也是成立

的，尽管我们没有用图把它画出来。

因为子群 $< f >$ 的陪集不会相交，所以我们可以把图 6.6 的三张图合并为一张图，只需用不同颜色加以区分不同的陪集即可，如图 6.11 的左边; 图 6.11 的右边展示的则是右陪集的情形。之所以用颜色区分能奏效，是因为不存在一个元素同时属于两个陪集，因此每个节点只要一种颜色就足够了。

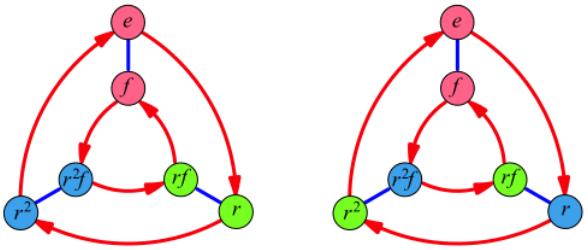


Figure 6.11. The left Cayley diagram for S_3 shows how the group is partitioned by the left cosets of the subgroup $\{e, f\}$; the right diagram shows how S_3 is partitioned by the right cosets of $\{e, f\}$.

当一个集合被像这样分成了好几个类，每一个元素属于且只属于一个类，数学上将其称为一个“划分（partition）”。图 6.11 表明子群 $< f >$ 的左陪集构成了群 S_3 的一个划分；$< f >$ 的右陪集也构成一个划分，只是划分方式有所不同。仔细观察一下图 6.9，你会发现子群 $< (0, 1) >$ 的陪集也一样划分了群 $C_3 \times C_3$.

我们很自然地就想问这样的问题：以上所说的这种划分现象是否只是某种巧合？子群的陪集是不是真的总能构成大群的一个划分？下面的定理将给出明确的回答。要说明的一点是，为了简便起见，在以下的叙述与证明中我只处理左陪集；至于右陪集的情形，我放在了习题 6.16 中，让读者自己思考。

定理 6.7. *若 H 是群 G 的子群，则 G 中每个元素属于 H 的某一个唯一确定的左陪集。*

证明. 设 G 中存在一个元素 g 同时属于两个左陪集，不妨设为 aH 与 bH。那么我们必可以断定，aH 与 bH 实际上就是同一个陪集的不同“名字”。理由如下：

因为 $g \in aH$，根据观察 6.6，我们得到 $gH = aH$；同理，因为 $g \in bH$，就有 $gH = bH$. 因此，我们就有 $aH = bH(= gH)$. □

定理 6.7 告诉我们，可以将群视作由其任意一个子群的不相交“拷贝”组成的。在图 6.11 中我们已经见过一个直观的例子了；根据图 6.9，你也可以很容易地为 $C_3 \times C_3$ 做一个类似的划分图示。在这两个例子中，划分的具体表现形状截然不同，然而其背后抽

象的想法原理（abstract idea）确是完全相同的，即可以用陪集来划分群。这样的抽象想法可以用图 6.12 中的几张图来表示。

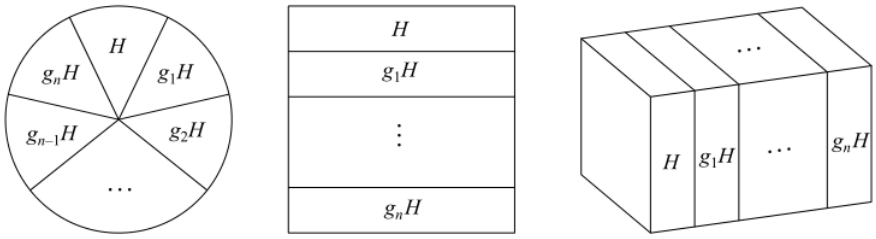


Figure 6.12. Several ways to picture the idea that cosets partition a group. The appearance of cosets in a diagram differs based on the layout of the diagram, so each of these illustrations represents the same idea, but for a different type of Cayley diagram layout.

用这种方式图示化一个群，将揭示群与其子群之间的一个重要关系。这就是下面这个，以意大利出生的法国著名数学家约瑟夫 • 路易斯 • 拉格朗日的名字命名的重要定理，所要表达的内容。在下面的叙述中，我将使用标准记号 $|G|$ 来表示群 G 的大小（阶）。尽管拉格朗日定理还有一个无限群的版本，不过这里我们总假设 G 是一个有限群。

定理 6.8 (拉格朗日定理)**.** *若 $H < G$，则 $|H|$ 整除 $|G|$.*

在这里我用了一个词“整除”，这是一个具有特定数学意义的词语。我们称一个较小的整数整除一个较大的整数，如果这个较小的整数是较大的整数的某个因子。比如，6 整除 12，但不整除 20，因为 $20 \div 6$ 有余数。

证明. 定理 6.7 证明了群 G 可以用子群 H 的“拷贝”进行划分，所以要想知道 G 的大小，只要去计数有多少个 H 的拷贝，再乘以每一个拷贝的大小 $|H|$ 即可。（注：因为既然是 copies of H，那么每一个拷贝的大小都跟 H 的大小相同）。因此，不妨设 H 的左陪集有 n 个（包括 H 本身），我们就可以写出如下等式：

$$|G| = \overbrace{|H| + |H| + \cdots + |H|}^{n\text{个}} = n|H|$$

□

上面证明中的数字 n 在群论关于子群的研究中出现的是如此频繁，以至于我们有必要赋予它一个专有名称。

定义 6.9 (指标)**.** *若 $H < G$，定义子群 H 在 G 中的指标 (index) 为 $[G : H]$，其中*

$$[G : H] = \frac{|G|}{|H|}$$

指标的实际意义是很明显的，就是子群 H 的左陪集个数，当然我们得把 H 本身也算做它的一个左陪集。要说明的一点是，在绝大多数情况下，当我们使用到“陪集”这个词时，都默认子群本身既是左陪集也是右陪集，因为 $H = eH = He$.

你也许也注意到了，$[G : H]$ 必定整除 $|G|$，这是由于上述等式也可以写作

$$|H| = \frac{|G|}{[G : H]}$$

让我们再回到具体的例子 $< f >< S_3$ 中来看看这些概念。S_3 的阶为 6，在图中可以清楚的看出是由 3 个 2 元陪集构成的。因此子群 $< f >$ 在 S_3 中的指标为 3，因为 $< f >$ 正好有 3 个陪集.

$$[S_3 :< f >] = \frac{|S_3|}{|< f >|} = \frac{6}{2} = 3$$

由于拉格朗日定理被冠以了一个非常著名的数学家的名号，所以你有理由去怀疑这个定理有很多深远而有趣的应用。事实上，你的怀疑是对的！这个定理的一个重要意义在于它显著地缩小了一个群可能拥有的子群数目。举个例子，对于一个 8 阶群，你根本不必费神去寻找它的 3 阶、5 阶、6 阶或 7 阶子群，因为这些数都不整除 8. 更一般地，对于任意一个有限群 G，你都不需要去费神寻找 $|H| > \frac{|G|}{2}$ 的子群 H，这是因为比 $|G|$ 的二分之一大的数都不能整除 $|G|$ 当然，唯一的例外只有非真子群 $H = G$）。当你开始做本章的习题时，把这些小窍门记在心里。

此定理另一个重要的意义在于，我们问这样一个很自然的问题：拉格朗日定理的逆命题是否成立？由此而来的讨论可谓是硕果累累，精彩纷呈。拉格朗日定理说的是，如果存在一个子群 H，那么它的阶整除 G 的阶。“逆命题”是说，是否对于任意 n 整除 $|G|$，我们都能够找到一个 n 阶子群 $H < G$？答案是否定的。在习题 6.31 中将会指导你找出为何如此。但是，如果给这样的逆命题进行适当的调整与修改，得到的命题则可能不仅是正确的，而且会非常有用。在这些“不完全的”逆命题中，最著名的是三条西罗定理（Sylow Theorems），这将在第九章学习到。

要提醒各位的是，记得要去做 6.6.3 节关于海色图（Hasse diagram）的习题，因为在第十章我们将会用到这种图，通过它可以帮助我们理解子群之间的关系。

7

积与商

第六章的内容是向群的内部探寻子群，由此我们获得了一些关于群的内部结构的信息。本章则往与之相反的方向前进，将展示如何把不同的群集聚在一起来构建更大的群。在这里我们将学到两种构建方式，每一种都是一个不同的群的“积运算”（product operation）。注意到我用了“积（product）”这个词，正如它通常的数学意义那样，在此处也表示某种乘法运算。我们也将学习到，某种特定的子群将成为上述运算之逆运算的关键，即所谓的“商运算”（quotien operation）。实施一个商运算将解构任何一种积，这可以揭示出一个大群是如何由小群构建出来的。这使得我们有能力清晰而简洁地图示出很多大群（large groups），并将许多原本极为巨大而复杂的对象纳入我们智力所能企及的范围之内。

因此，本章将教给读者三个方面的知识：如何实施两种积运算以及如何实施商运算。每一个运算的具体流程都会由一些例子以图示的形式展示出来，本章的习题也是要求读者多多练习这三种运算。“亲自动手（get your hands dirty）”是很重要的，因为这样才能加强你对这三种运算的直观感觉，并且加深你对手里所操作的那些群的熟悉程度。

本章的习题已经被我仔细整理设计好了，以帮助读者在每学完一个新的话题后都能得到及时的巩固。这一章的每一小节内容都有对应的一小节习题。所以，当你读完 7.1 节后，如果你觉得在进行下一节内容的学习前自己有必要做点练习以加深对所学概念的理解，你大可以直接跳到习题 7.6.1，这节的习题也只跟 7.1 节所学的材料内容相关。本章其余小节内容与习题的搭配也是这个模式，这样你就可以细嚼慢咽，好好消化每一节的内容了。

我们首先以较简单的一种积运算开始，即所谓的“直积（direct product）”。

7.1　直积

其实在本书中，你已经见过一些直积群了。每一个名字里带有乘积符号 × 的群都是直积群，它们可以通过“直积（direct product）”这一道“工序流程”构建出来。我们见到的第一批直积群是图 2.10 中的 $C_3 \times C_3$ 和 $C_2 \times C_2 \times C_2$，此后我们也遇见了一些其他的直积群，比如图 5.9 中的 $C_2 \times C_4$. 为了方便起见，我把这些直积群的凯莱图都重新画在了图 7.1 中。符号“×”在英文中通常读作“cross”或者“times”，所以如果你要用英文表达 $C_2 \times C_4$，就可以读作“cee two cross cee four”。这里的例子中都含有循环群 C_n，但这在作直积时并不是必须的，只是在一些小例子中时常会涉及到 C_n. 就在不远的后面，我们很快就会遇到一个较大的例子 $S_3 \times C_2$.

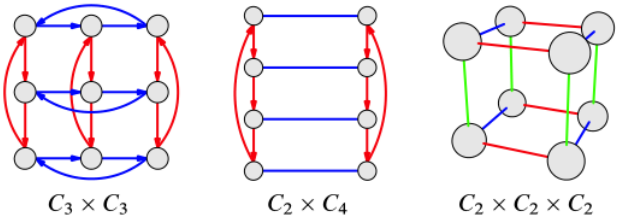


Figure 7.1. Three example direct product groups

在 7.1.1 节我将解释具体要如何建造直积群，并将在几个例子上详细展示这一构建过程。在初步了解直积群之后，我们就做好准备来学习究竟直积群会给我们的群论学习之旅带来怎样的好处？（这是 7.1.3 节的内容了）

在学习直积运算的具体细节之前，让我们先来观察图 7.1 中的三个示例，看看其中一些“显然的”特征。这三张图可以告诉我们为何我们即将学习的这一运算会被称为“积”，还用了 × 符号？明显的理由有两个：其一，$C_3 \times C_3$ 的凯莱图显然是一个 3×3 的网格，这也使得名字 $C_3 \times C_3$ 有那么点名副其实；其二，$C_3 \times C_3$ 显然是一个有 9 个元素的群，毕竟，$3 \times 3 = 9$. 这两个基本的特征对于 $C_2 \times C_4$（一个 2×4 的网格）和 $C_2 \times C_2 \times C_2$（一个 $2 \times 2 \times 2$ 的网格）也是成立的，从图中即可看出。

7.1.1　构建直积

在这一节里，我将把构建直积的过程用图例的方式教给读者。从两个给定的群的凯莱图 A 和 B 出发，我们将利用定义 7.1 所述的步骤来得到直积群 $A \times B$。正如图 7.2 所示的那样，这里我把 A 取作了 C_2，把 B 取作了 C_4，并于图 7.2 中详尽展示了构建过程；所得到的结果正是图 7.1 中间的那张直积群的凯莱图。之后，我还会将这种构建方法推广到乘法表上，由此我们又可以从代数的观点来理解直积。

定义 7.1 (由凯莱图构建直积的技术)**.** 使用凯莱图 A 与 B 来构造直积 $A \times B$，其构建步骤如下：

1. 画出 A 的凯莱图。在图 7.2 的示例中，$A = C_2$，即其中最左边的图。
2. “吹胀” A 中的所有节点，并于每一个“吹胀了的”节点中放置一个 B 的凯莱图。如图 7.2 中间那张图所示，C_2 的两个节点都被“吹胀”得足够大，以使其中放得下一个 C_4 的凯莱图。
3. 把 A 中节点被“吹胀”的外轮廓擦去，同时使用 A 中的箭头去连接各个 B 凯莱图中彼此相关的节点；也就是说，移走凯莱图 A，只把它的箭头留给诸凯莱图 B，并以其为连接模式的样本，来连接各个凯莱图 B 的节点。在图 7.2 的示例中，我们放置了两个 C_4，每个都有四个节点。最顶上的两个是彼此相关的，我们在它们中间用 C_2 的红箭头连接起来，这样连接后就成为了 C_2 的一个小小拷贝；对于剩下的那些节点做相同处理；在完成四对节点的连接工作后，我们就得到了 $C_2 \times C_4$ 的凯莱图。由于这一步比之前两步更加复杂，所以我另外画了一张图 7.3 来单独细说这一步是如何进行的。

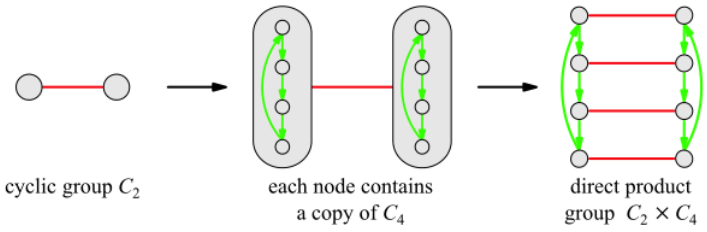


Figure 7.2. The construction of a Cayley diagram for the group $C_2 \times C_4$, using Cayley diagrams of C_2 and C_4, as described in Definition 7.1

根据定义 7.1 的步骤得到的群 $A \times B$，称为群 A 与群 B 的直积（the direct product of A and B），并把 A 与 B 称为它的因子（factor）。请注意，在进行第 2 步时，务必使用不同的颜色来标记 A、B 中的箭头，这样才能保证由第 3 步画出的图是一个合理的凯莱图。

注意到，$C_2 \times C_4$ 中含有 C_2 的拷贝版作为它的“行”，同时含有 C_4 的拷贝版作为它的“列”。按照定义 7.1 描述的步骤，我们使用了两个 C_4 的拷贝版并将其放置于“吹胀”

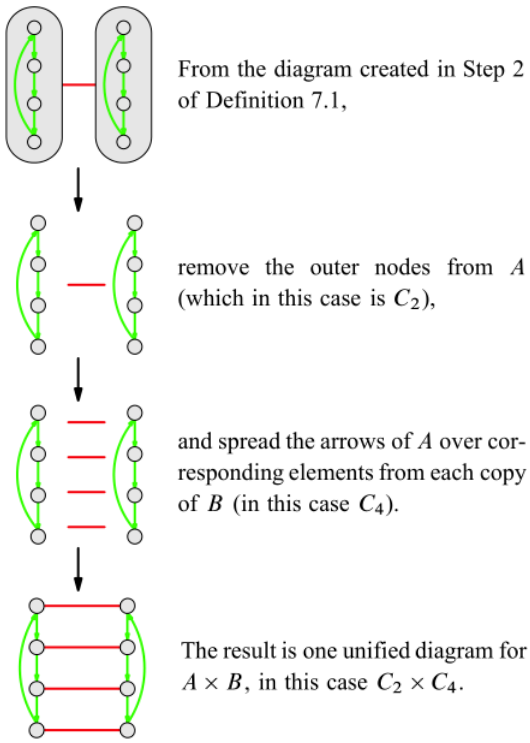


Figure 7.3. An example execution of Step 3 of Definition 7.1, illustrated in greater detail than Figure 7.2 shows. As in Figure 7.2, in this example, $A = C_2$ and $B = C_4$.

了的 C_2 中，然后将每一对节点连接起来，使每一对都变成 C_2 的拷贝版。然而我们也可以换一个顺序作这个积，得到相同的结果。图 7.4 展示了直积 $C_4 \times C_2$ 的效果，并且实际上 $C_4 \times C_2$ 同构于 $C_2 \times C_4$，这个同构是很容易看出来的，只要把 $C_2 \times C_4$ 凯莱图转个方向就得到了 $C_4 \times C_2$ 的图。我们可以证明，对于任意的群 A 与群 B，$A \times B$ 总是与 $B \times A$ 有着完全相同的结构。因此，我们称在同构意义下，直积运算可交换（commutative）；在习题 8.36 中，会要求你证明这一命题。现在，我只把其作为现成结论来使用。

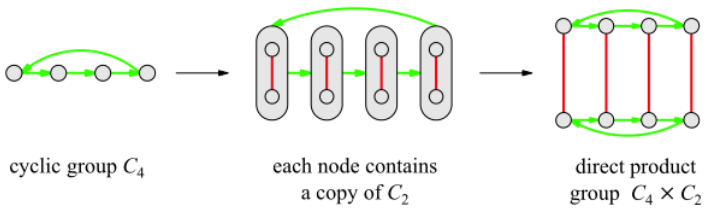


Figure 7.4. Constructing a Cayley diagram for the group $C_4 \times C_2$, using Cayley diagrams of C_4 and C_2 and following the procedure in Definition 7.1. The result is a group that is equivalent to $C_2 \times C_4$, as constructed in Figure 7.2.

我们所制作出的直积群的凯莱图，其节点并没有标注上符号“名字”，但是如果我们想方便的引用这些节点的话，给它们赋予标记将会大有裨益。事实上，我们有一个标准方式来命名直积群中的元素。高中学习的代数课程教给我们用坐标如 $(1, 3)$ 与 $(10, 6)$

来表示平面上的点。因此平面上的点都有像这样的名字 (x, y)，x 用以标明点所在的水平位置，y 用来标明点所在的竖直位置。类似的，在 $A \times B$ 中，我们给其中的元素以这样的一个元素对 (a, b)，其中 $a \in A$，$b \in B$。在上面的两个例子中，我们就可以按这种方式来命名直积群中的节点，如图 7.5 所示。一般来说，对于一个直积群凯莱图中的任意一个节点而言，其名字的各个分量都是在进行定义 7.1 中的步骤 2 时获得的。一个节点从“被吹胀了的”A 的节点（即它被放置于其中的那个 A 的节点）中获取它的第一个名字分量 a；再从 B 的节点（即它曾经所代表的那个 B 中的节点）中获取它的第二个名字分量 b。在图 7.5 所示的简单例子中，这分别就与行、列相关。

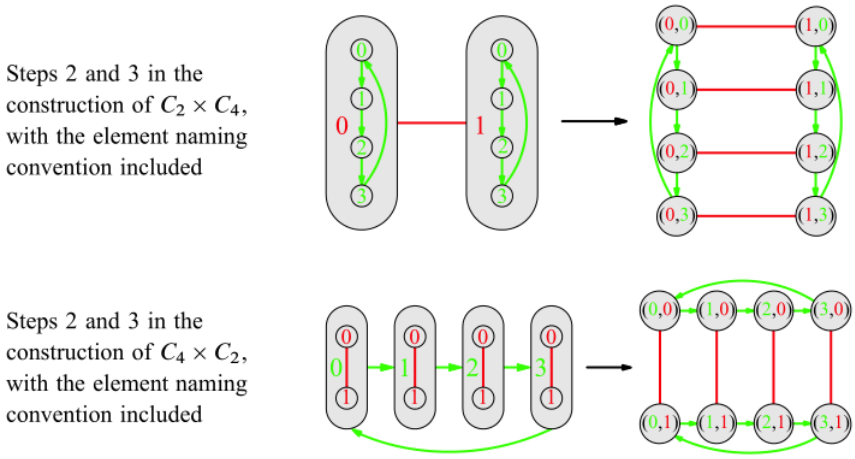


Figure 7.5. An element (a, b) in $A \times B$ gets its name from the a in A and b in B that gave rise to it in Step 2 of Definition 7.1. Colored numbers are used to make it easier to see that the names of the inflated A nodes go on the left of each pair, and the names of the inner B nodes on the right.

联系上我们最近学习的子群的内容，你也许注意到了 C_2 是 $C_2 \times C_4$ 的一个子群，实际上 C_2 正是子群 $< (1,0) >$，而 $< (1,0) >$ 的陪集也清晰可见，就是 $C_2 \times C_4$ 的各行。它们既是左陪集也是右陪集，这就使得 C_2 称为了所谓的“正规子群（normal subgroup）”。在第六章中我提到过正规子群的概念，那时并未加以详细阐述，但是在本章中，正规子群将起到重要作用，因此是时候给出正式定义了。

定义 7.2 (正规子群). 一个子群 $H < G$ 是正规的（*normal*），如果 H 的每一个左陪集同时也是一个右陪集（反之亦是）我们用 $H \triangleleft G$ 来表示 H 是 G 的正规子群。

用上新记号，我们就可以将之前的观察表述为 $< (1,0) > \triangleleft C_2 \times C_4$；类似的，$C_4$ 也是 $C_2 \times C_4$ 的正规子群，且 C_4 正是子群 $< (0,1) >$，它的陪集也就是 $C_2 \times C_4$ 的各列。我们将会发现，在任意一个直积中，它的因子都是正规子群（习题 7.12）；也就是说，对于任意的群 A 与群 B，我们总是有 $A \triangleleft A \times B$ 且 $B \triangleleft A \times B$.

7.1.2 更多直积的例子

让我们离开 $C_2 \times C_4$ 这个过于简单的例子，来看看 $C_2 \times C_2 \times C_2$——这个我们首次于图 2.10 见到的群，以此充实我们对于直积的理解。从图上来看 $C_2 \times C_2 \times C_2$ 是一个三维的直积群，我们可以将其视为相继进行了两次直积运算，即 $(C_2 \times C_2) \times C_2$. 括号告诉我们要先计算 $C_2 \times C_2$，然后将结果再次和 C_2 做直积，这就需要使用两次定义 7.1 中所述的步骤，如图 7.6 所示。注意到每一次都将相应凯莱图的节点“吹胀”以容纳一个 C_2 的拷贝；而为了清晰起见，每次都应换一个新的方向来画图。在第一次给吹胀的节点填入 C_2 时，我将这两个 C_2 竖直放置，第二次时，则将需要填入的四个 C_2 垂直纸面放置，从而营造出一种立体感。结果就是一张 $2 \times 2 \times 2$ 的网状图，这也与其名 $(C_2 \times C_2) \times C_2$ 相吻合。

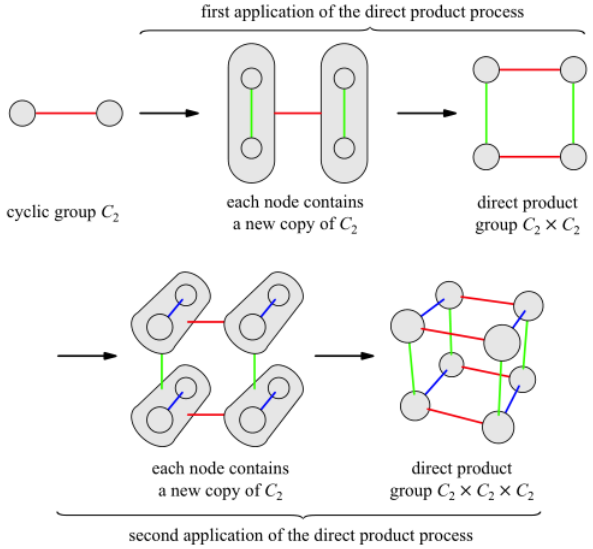


Figure 7.6. An example direct product with three factors, $C_2 \times C_2 \times C_2$. Constructing such a product involves applying Definition 7.1 twice, as marked in the figure.

既然我们是以 $(C_2 \times C_2) \times C_2$ 来计算该直积的，很自然地，我们也会以这样的方式来给其节点命名，比如 ((01)0)；不过这样未免太显笨拙，通常的习惯是只用一对括号，即将节点命名为 $(0, 1, 0)$。名字中的第一个分量来自于第一个 C_2，第二个分量来自于第二个 C_2，第三个分量来自于第三个 C_2。类似的，对于直积 $C_2 \times C_2 \times C_2 \times C_2$，它的节点名字将是如 $(1, 0, 1, 1)$ 这样的形式；对于更大的直积，同理可知。有时为了使凯莱图更美观、更具有可读性，我甚至会扔掉括号和逗号，直接将节点名由 $(0, 1, 0)$ 缩写为 010，就像我在图 2.10 中展示的那样。这样的简写只要不引起歧义，就可以更方便地用于标注凯莱图的节点。

这一节的最后一个例子，$S_3 \times C_2$，是一个比较大而且不可交换的群。如图 7.7 左边

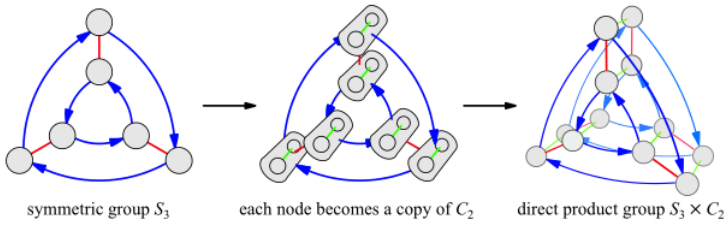


Figure 7.7. The direct product construction for $S_3 \times C_2$

那样画出 S_3 的凯莱图，然后将 S_3 的各个节点吹胀，放入 C_2. 注意这里放置时又使用刚刚那个技巧：将 C_2 垂直纸面放置，造成一种立体感，如图 7.7 中间的图所示。最终结果就是图 7.7 右边的效果图，一个“三明治”。这是我们碰到的第一个非交换的直积。遵循之前的命名传统，$S_3 \times C_2$ 中的各元素名如下：

“三明治”的前面一层：$(e,0)$　$(r,0)$　$(r^2,0)$　$(f,0)$　$(rf,0)$　$(r^2f,0)$

“三明治”的后面一层：$(e,1)$　$(r,1)$　$(r^2,1)$　$(f,1)$　$(rf,1)$　$(r^2f,1)$

7.1.3　为什么需要直积？

我们已经知道如何构建直积，却还不清楚这样一种技术究竟有什么价值？这一节我们就来看看它的价值所在。直积是几种常见而简单的构造大阶群的技术之一，如果我们能理解这一技术，我们也就可以更容易的理解一些大阶群。本节我们将使用这样一个事实——直积的因子相互独立，来具体解释。注意到，在 $A \times B$ 的凯莱图中，沿着 A 中的箭头既不会影响 B，也不会被 B 影响。

举个例子，在图 7.4 所示的 $C_4 \times C_2$ 的凯莱图中，沿着一个水平箭头 (C_4) 将导航至新的一列，但是仍然在同一行。另一种等价表述是，绿色箭头 (C_4) 只影响每一个节点名字的第一个分量。沿着 $C_4 \times C_2$ 中绿色箭头所得到的轨道如下：

$$(0,0) \longrightarrow (1,0) \longrightarrow (2,0) \longrightarrow (3,0) \longrightarrow (0,0) \longrightarrow \cdots$$

同理，沿着一个竖直箭头 (C_2) 会改变节点所在的行，或者说节点名字的第二个分量；但是仍然处于同一列并因此保持节点名字的第一个分量不变。

$$(0,0) \longrightarrow (0,1) \longrightarrow (0,0) \longrightarrow \cdots$$

从上例可以看出，在直积 $A \times B$ 中，A 中的箭头只会带着你在 A 中移动而不会踏足 B；B 中的箭头只会带着你在 B 中移动也不会到 A 里面。在一定意义上，直积的两个因

子之间存在着某种“独立性”，这导致了看待直积群的一个十分有用的新方式，即我下面要介绍的内容。

我们将凯莱图中的节点想象为一个一个地点，其中的箭头想象为连接两个地方的道路。每一次，你把自己置身于其中某一个节点，再沿着路径走向另一个。想象你在群的世界中徒步旅行，当你需要停下来检查一下路边地图时，那会是什么样？这样的地图理应是这个群的凯莱图，并在你所身处的那个节点处标注着“你现在在这里 (You are here)”的字样，如图 7.8 所示：

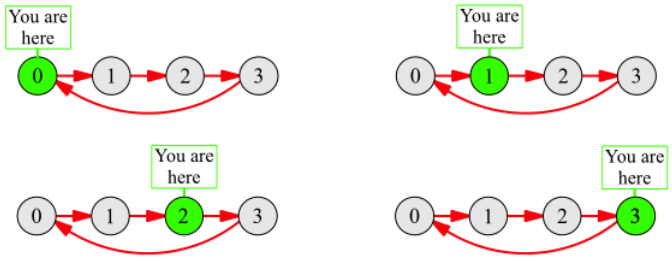


Figure 7.8. Four example roadside maps for a Cayley diagram of the group C_4, one map for each node

为一个直积群作导航可以视为在两个不同的群里同时且独立地作导航，下面就来具体说说这句话的含义。图 7.9 展示了与图 7.8 相类似的导航地图，只不过在图 7.9 中，每一幅地图都包含两个群且每个里面都有一个高亮标注的地点。也许让你想象自己同时在两个世界中旅行有点难，现在让我们这样来想：假设你在远程指挥两个别的什么人的行动。有时你需要对在 C_4 世界中前进的那个人发出指令，告诉他要往哪走；而有时则又需对另一个在 C_2 世界中的人发出行进指令。像这样指挥两个人在两幅凯莱图中同时且独立地前进，与你自己身处直积群世界中为自己导航，这两者之间是一种绝妙的类比，或者说等价的情形。回到具体例子中，直积 $C_4 \times C_2$ 中每一个节点的名字都得名于 C_4 中的一个节点和一个 C_2 中的节点，如果采用“让你自己身处直积世界为自己导航”的观点，那就是以水平坐标和竖直坐标的想法（如图 7.5）来阐释这些直积群中节点名字的含义。但是，我们事实上也可以用另一种方式来解释，就像让一个人在 C_4 世界中，另一个人在 C_2 世界中一样，我们考虑分开的两张凯莱图，让一个节点位于 C_4，另一个位于 C_2 中，让它们同时且独立地分别在两幅图中运动。用这种方式来理解直积，比如 $C_4 \times C_2$ 中的节点 $(1,0)$ 就可以解释为图 7.9 中上面一行里的第二幅图。因此到目前为止，我们就拥有了两种不同但本质上等价的理解直积的方式。我们可以将直积群 $A \times B$ 视为由一根绳子牵连着的 A 和 B。

让我来清楚地解释一下，什么叫指挥两个人“同时且独立”地运动？这就是说，这两个人之间不管哪一个的运动，对另一个人所处的位置和运动情况都不会产生影响。说

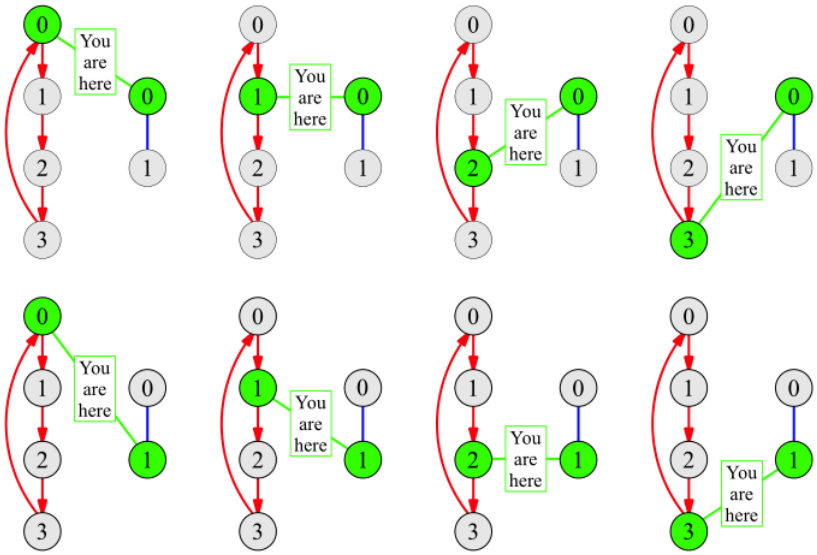


Figure 7.9. Each of these maps depicts a two-part location as you simultaneously navigate the two groups C_4 and C_2.

这么多，不如来看一个不具有这样的“独立性”的例子，如图 7.10 是 D_4 的凯莱图。在这张图中，竖直的运动有可能改变水平的位置，因此水平运动与竖直运动并不独立。比如，从 $(1,0)$ 竖直移动下去，并没有到达 $(1,1)$，而是到达了 $(3,1)$. 对比一下，在 $C_4 \times C_2$ 的凯莱图中，从 $(1,0)$ 竖直移动后到达的正是 $(1,1)$，并没有带来水平位置上的改变。也许你会想这可能是节点命名的问题，可以把原来的 $(3,1)$ 强行命名为 $(1,1)$，并对凯莱图作适当的调整以修正这个问题；然而事实上你这么做是徒劳无功的，D_4 本身就不是一个由直积构造得到的群，这样的本质特性决定了，你修补好这里，那么必然在其他地方又会出现类似的问题。

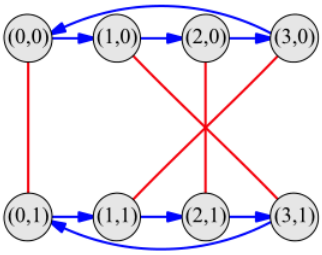


Figure 7.10. A rectangular layout of D_4, with elements named according to their row and column, as if it were a direct product group (which it is not).

其实我们第一次见到像这样把两个群独立地“粘”在一起的例子是图 2.8. 在这个“双开关”群中，每一个开关都不会影响另一个，即你对其中之一做开灯、关灯操作，对另一个的开、关状态根本不产生影响。每一个开关单独地来看可由群 C_2 来描述，当把它们独立地“粘”在一起时，便是由直积群 $C_2 \times C_2$ 来描述；而群 $C_2 \times C_2$ 更常见的名字

是 V_4，或者说群 $C_2 \times C_2 = V_4$.

将直积视为两个“独立的”粘在一起的群，其中之一个好处是一些高阶的群将能简洁地被可视化。举个例子，我们用不着去画一个有 56 个元素的群 $D_4 \times C_7$ 的凯莱图——要是真这么画出来，那会相当的杂乱繁复；我们只需分别画出 D_4 的凯莱图和 C_7 的凯莱图，再用一根线连着它们，以表示在做“同时且独立地导航”。比如元素 $(r^2, 5)$ 分别代表了两个位置，一个在 D_4 中，一个在 C_7 中，如图 7.11 所示。这样就大大减轻了我们画图和读图的工作量，因为不需要画那么多的节点和箭头；并使得我们不用去看多于 8 个节点的结构了。更进一步，这样的可视化方式不仅可以忠实地表示这个 56 阶群（尽管不那么直观），而且通过观察像图 7.11 那样的可视化图像，能更好得帮助我们全面理解这个 56 阶群的结构是如何由直积的构建过程给构造出来的。因此，直积是一种将大阶群变得更容易理解的手段——它形象地展现给我们一个大阶群是怎样由小阶群经过一个简单的过程构建得到的。

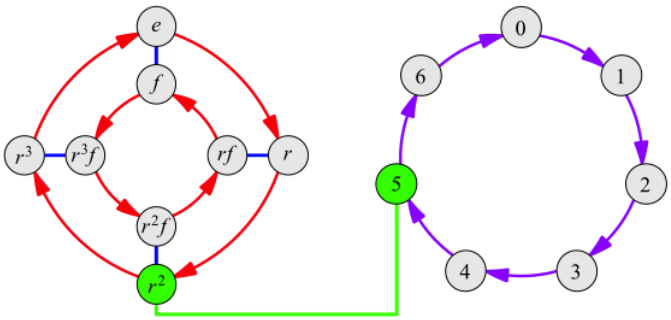


Figure 7.11. The element $(r^2, 5)$ from the group $D_4 \times C_7$, viewed as a pair of elements, one in a Cayley diagram from D_4 and one in a Cayley diagram of C_7.

7.1.4 从代数的角度来看

我们这本书在介绍群论概念的时候，一直以来都在试图教会读者“用两条腿走路”：一条“腿”是基于作用（action-based）的观点，而另一条“腿”则是基于代数（algebraic）的观点；这两套观点在理解群论的相关概念时都十分有帮助。前面我们是从作用的观点（凯莱图）理解直积，接下来就让我们试着从代数的角度——即将群视为一个带二元运算的集合，来理解直积。由于乘法表能很好地反映这种代数的观点，所以我们就从如何制作直积群的乘法表开始吧。幸运的是，正如直积群的凯莱图有可视化的制作过程（即定义 7.1），对于直积群的乘法表我们也有相应的可视化制作步骤。

定义 7.3 (由乘法表构建直积的技术). 给定群 A 与群 B 的乘法表，为了制作直积 $A \times B$ 的乘法表，我们只需按照如下三个步骤进行。读者可以将其与前面的定义

7.1 对比来看，就会发现这两种技术步骤的相似之处。这里我取 $A = C_4$，$B = C_2$ 作为示例，图 *7.12* 则展示了示例 $A \times B$ 的构建过程。

1. 画出 A 的乘法表。在图 *7.12* 的示例中，C_4 的乘法表由蓝色的元素表示。
2. “吹胀”A 中的所有格子，并于每一个“吹胀了的”格子中放置一个 B 的乘法表。为了避免原来的表 A 中的信息丢失，将 A 中的元素名仍然保留，并悬浮在相应位置处。在图 *7.12* 中间那张图中，蓝色的大号数字代表原来的 C_4 乘法表中的元素，它们悬浮于填充了 C_2 的原本自己所在的位置处。
3. 将所得新表中的元素以有序对的形式重新命名，将 A 中的元素作为名字的左分量，B 中的元素作为名字的右分量。图 *7.12* 最右边的图便是直积 $C_4 \times C_2$ 的乘法表，其中每一个元素名字都是有序对，我保留了各个分量元素的原始颜色，以方便读者看出该分量原本是来自于的哪一个群。

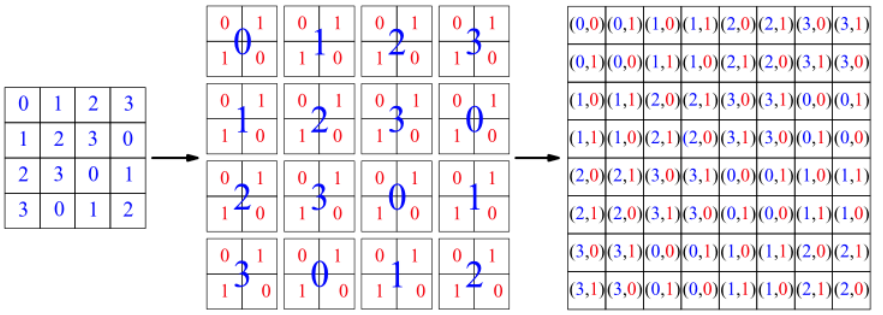


Figure 7.12. Constructing a multiplication table for $C_4 \times C_2$ from multiplication tables for C_4 and C_2, following the technique in Definition 7.3. Row and column headings could easily be added, but the process is more clearly illustrated without them.

这一构建过程，如图 7.12 所示，可以告诉我们关于直积群 $C_4 \times C_2$ 中二元运算的很多信息。对于初学者来说，一个简单的应用就是把图 7.12 中最后那张图当作计算工具。比如，为了计算 $(2,1)\cdot(3,1)$，我们可以先找到元素 $(2,1)$ 的所在行，再找到元素 $(3,1)$ 的所在列，两者相交的地方就是结果，即 $(1,0)$. 然而我们真正感兴趣的是，为什么这张表能够像这样给出运算结果呢？它的原理是什么？事实上，仔细回顾一下直积群乘法表的构建过程，我们就能找到这一问题的答案。

图 7.12 中最后一幅图中乘法表的结构是由图 7.12 中间那张上下交叠的乘法表所决定的。直积乘法表中蓝色数字所表现出来的行为模式完全拷贝自图 7.12 中间的交叠乘法表中的大号蓝色数字，或者说白了就是拷贝自原始的 C_4. 因此，直积乘法表中每个元素的左分量（蓝色数字）的运算规则完全取决于 C_4 的乘法表；即是说，左分量之间的运算只跟它们在 C_4 中的位置有关，而与该元素的右分量（红色数字）毫不相关。所以，

$(2,1)\cdot(3,1)$ 的结果中左分量是 1 的原因就不难解释了：因为在 C_4 中，$2+3=1$. 在计算直积的左分量时，右分量可以遮住不看，因为与它完全没关系。这一点被展示在图 7.13 左边的那幅图，在直积乘法表中，那些左分量为 2 的元素乘以那些左分量为 3 的元素，所得到的结果是那些左分量为 1 的元素。

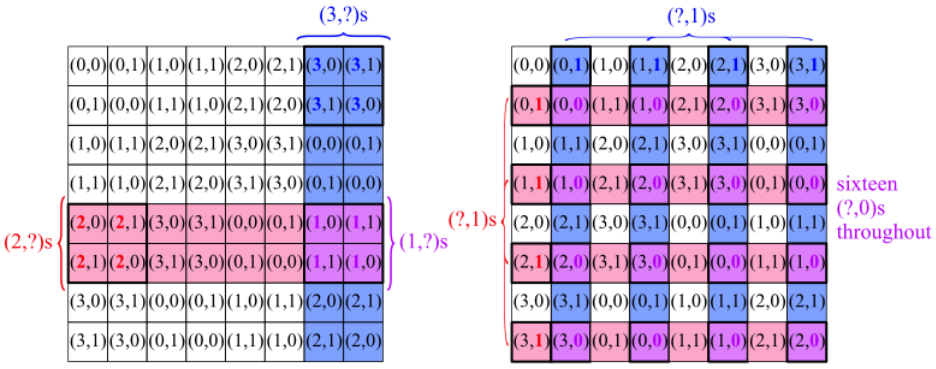


Figure 7.13. The multiplication table for $C_4 \times C_2$ constructed in Figure 7.12, used to show the independence of the factors in a direct product. The left table shows that any element $(2,?)$ times any element $(3,?)$ results in some element $(1,?)$. The right table shows that any element $(?,1)$ times any element $(?,1)$ results in some element $(?,0)$.

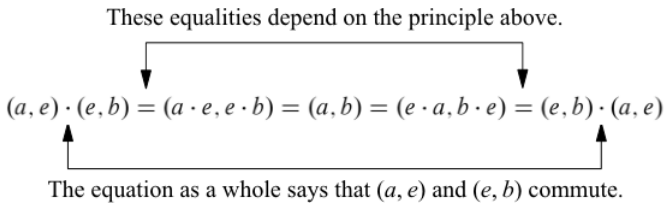
对于直积乘法表中的右分量（红色数字）来说，道理是相同的，它们的运算模式拷贝自 C_2。当右分量之间进行运算时，左分量又被冷落一旁了，且完全不影响右分量的运算。因此，$(2,1)\cdot(3,1)$ 的结果中右分量是 0 的原因也就容易解释了：因为在 C_2 中，$1+1=0$. 这一点被展示在图 7.13 右边那幅图，在直积乘法表中，那些右分量为 1 的元素乘以那些右分量为 1 的元素，所得到的结果是那些右分量为 0 的元素。

综上所述，为了在 $C_4 \times C_2$ 中计算 $(2,1)\cdot(3,1)$，我们只需知道如何在 C_4 中计算 $2+3$ 以及如何在 C_2 中计算 $1+1$ 即可；每个分量在进行各自的运算时，相互独立，互不干扰。我们总结为下面这个等式：

$$(2,1)\cdot(3,1)=(2+3,1+1)=(1,0)$$

在前面的凯莱图中，我们已经见识过了直积因子之间的这种独立性；以上的原理则是这一独立性在乘法表中的具体表现。

现在让我们试着用代数语言来表达这种独立性。任取 $a\in A, b\in B$，我们用 e 表示每个群中的单位元（译注：读者应当注意，虽然这里都用的 e 来表示单位元，但是 A 中的单位元未必就和 B 中的单位元相同；实际上应该区分为 e_A 和 e_B），则原来的元素 a 反映到直积 $A\times B$ 中就是 (a,e)，原来的元素 b 反映到直积 $A\times B$ 中就是 (e,b)。下面这个等式链表明：在 $A\times B$ 中，(a,e) 和 (e,b) 是可交换的。这种可交换性正是我们上面所讨论的因子之间的独立性所导致的结果。



因此，直积因子之间的这种独立性告诉我们，如果我们把 A 中的元素 a 和 $A\times B$ 中的元素 (a,e)，以及 B 中的元素 b 和 $A\times B$ 中的元素 (e,b) 分别等同起来看待，那么我们可以在这种意义下直接简洁地称“a 和 b 是可交换的”。让我们带着这个新的、有趣的认识再次暂时回到凯莱图的世界。“a 和 b 是可交换的”意味着在直积 $A\times B$ 的凯莱图中，来自于 A 中的箭头与来自于 B 中的箭头是可交换的，图 7.14 用两个不同的示例图来阐明了这一想法。(译注：在原作中，图 7.14 下面的文字说明有点错误，由于没办法修改图片，故在此提醒读者注意一下：$a^3\cdot b^2=b^2\cdot a^3$ 应该为 $a^2\cdot b^3=b^3\cdot a^2$)

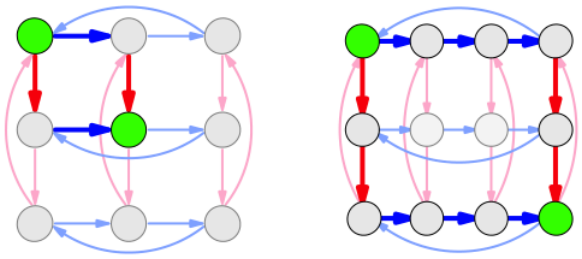


Figure 7.14. The left Cayley diagram illustrates the equation $a\cdot b=b\cdot a$ in $C_3\times C_3$, and the right Cayley diagram illustrates the equation $a^3\cdot b^2=b^2\cdot a^3$ in $C_4\times C_3$. In each case, a is the red generator and b is the blue generator.

现在，对于直积我们有了较为全面的认识，既从作用的观点考虑了，也从代数的观点考虑了。是时候给读者介绍一下另外一种常见且常用的积运算——半直积（semidirect product）。尽管半直积比直积要更复杂一些，它们却也有很多相同之处。其中之一个相同之处便在于，只要我们理解了构建半直积所需的基本原料（小阶群）与构建的过程，那么我们就可以理解由此创造出的大阶群，即使这样的大阶群复杂到难以画出来。

7.2　半直积

清晰简洁的直积运算还有两个情况较为复杂的表兄弟。在这里我只准备介绍其中的半直积（semidirect product），不打算涉及更加复杂的 knit product（译注：不确定这个词在中文数学术语里是如何翻译的，欢迎知道的读者在文末留言）。即使是半直积也要依赖于一些较为抽象复杂的概念——这些概念直到第八章我们都不会学习到。所以在这里谈及的半直积只是为了给读者一些初步的印象，剩余的细节我们得到下一章才能进一步

学习。正如研究直积是为了弄清楚大阶群的结构，研究半直积的理由同样是为了发展一套能够让我们更简单地去描述大阶群の结构的方法。

我们已经知道，直积是将其中一个因子进行恒同拷贝（identical copies），拷贝得到的那些再按照另一个因子的连接方式将相关元素连接起来而形成的。半直积的构建过程与此十分类似。它也有两个因子，一个因子用来“拷贝”，另一个用来决定连接方式。不同之处在于，半直积中所做的“拷贝”并非通常意义上的" 完全一模一样的复制"，我们允许拷贝时发生一些“扭折 (twisting)”，由此产生更多可能的复杂情形。为了能够更好地叙述半直积所允许的这种“扭折”，我将引进下面这个词条。这并非标准的群论术语；实际上，我们将在后面使用更专业的词语来取代下面的不正规说法。不过目前来说，使用一个形象化的非正式术语更为合适。

定义 7.4 (rewiring)**.** 我们称一张凯莱图是另一张的 *rewiring*，如果满足以下所有条件：

1. 两张凯莱图有完全相同的节点位置
2. 两张凯莱图的箭头布置可以不相同
3. 两张凯莱图中的群元素之间的代数关系必须保持一致

条件 (b) 并非真正的限制条件，它出现在以上三条中是为了强调“rewiring”这一操作的主要特点——同一张凯莱图的不同箭头排布方式。而至于条件 (c)，另一种更好理解的说法是：尽管两张凯莱图不同，它们的乘法表却是一样的，也因此它们描述的是同一个群（某种意义上）。

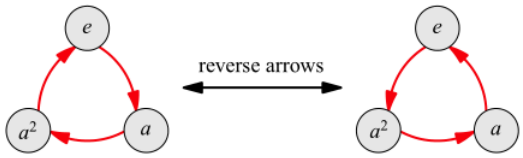


Figure 7.15. The left diagram is a familiar Cayley diagram for C_3, and the right is a rewiring of it. Reversing either diagram's arrows yields the other diagram.

图 7.15 展示了 C_3 以及它的一个 rewiring. 让我们来仔细想想为什么它们满足了上述定义 7.4 的三个要求。条件 (a) 要求两张图中的节点位置是一模一样的，这可以从图中明显的看出来。条件 (b) 是说两张图中的箭头连接方式可以不同，这也是显然的：一个里面的箭头按顺时针方向构成圈连接了节点，另一个是按逆时针方向连接节点。验证条件 (c) 意味着要去验证在其中一张图中成立的等式关系在另一个里面也要成立（此即“代数关系保持一致”的含义）。比如，左图中成立 $a \cdot a = a^2$，这是因为从单位元节点出发走两条红箭头 a 将到达节点 a^2. 所以我们必须去验证在右图里，此等式关系仍然成

立。它确实是成立的，不过其中缘由你可能乍一看没看出来。注意到，从右图中我们会发现：两个相继的红箭头才表示 a！因此，在右图中，$a \cdot a$ 其实代表的是从单位元出发走四条红箭头所到达的节点！从而在绕了一整圈之后到达的确实是节点 a^2，也即等式 $a \cdot a = a^2$ 在右图中成立。我们还可以去验证诸如 $a^3 = e$ 等许多等式。为了彻底地验证所有等式，我们可以将每一张凯莱图各自转化为相应的乘法表，你会发现所得到的两张乘法表是一样的（同构意义下），因此，这两个凯莱图描述的是相同的群。从而，图 7.15 满足定义 7.4 中的所有条件。

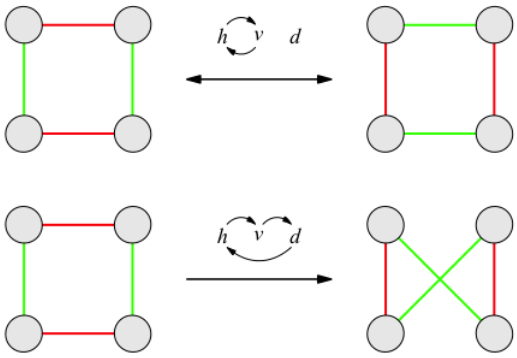


Figure 7.16. Two ways to rewire a Cayley diagram for V_4, described as permutations of horizontal (h), vertical (v), and diagonal (d). The permutations refer to diagonal (d) arrows even though the original diagram has only horizontal and vertical arrows, because they can be rearranged to diagonal positions.

图 7.16 展示了一个稍微大点的例子——重新排布 V_4 中箭头的两种方式，每一个都代表了 V_4 箭头的一种置换方式。顶上的那种 rewiring 方式连续施加两次就又回到了原始状态，因为它只是简单的交换水平箭头与竖直箭头。底下的 rewiring 方式，却要连续施加三次才能回到原始状态，因此它可由一个 3 阶置换描述。

也许将刚刚见过的两个 rewiring 例子和下图 7.17 中的两个非 rewiring 的例子作下比较会有助于加深我们的理解。图 7.17 顶上的例子展示的是经过一次重新布线后，得到的不是凯莱图，也因此就不能称之为 rewiring；底部的例子展示的是经过变换后却不再保持代数关系，比如，在右下角的图中，$2 + 2 = 1$，然而为了满足定义 7.4 的条件 (c)，$2 + 2$ 应当等于 0. 因此也不是 rewiring.

你可能也察觉到了，在图 7.16 中我们用置换来描述 rewirings；事实上，正如你所怀疑的那样，我们可以将所有的 rewirings 放在一起形成一个群。最简单的例子是图 7.15，不仅仅因为这张图展示了一种重新给 C_3 布线的方式，更重要的是倘若我们把图 7.15 中的凯莱图当作节点来看的话，那么在更大的视角层面上它们所形成的结构正是 C_2，而此时扮演着连接 C_2 中两个节点の箭头的角色者正是图 7.15 中那个上面写着“reverse arrows”字样的黑色箭头。另一个更加有趣的例子是 V_4 的所有 rewirings 形成的群，这个

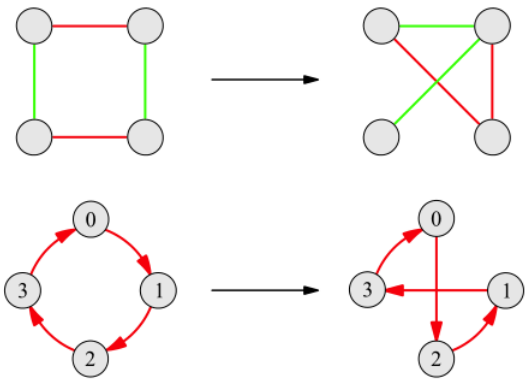


Figure 7.17. Two rearrangements of Cayley diagram arrows that are *not* rewirings.

群由两个基本的 rewiring 生成，而图 7.16 中所展示的就是这两个生成元。这个 rewiring 群具有的结构与 S_3 相同，如图 7.18 所示。

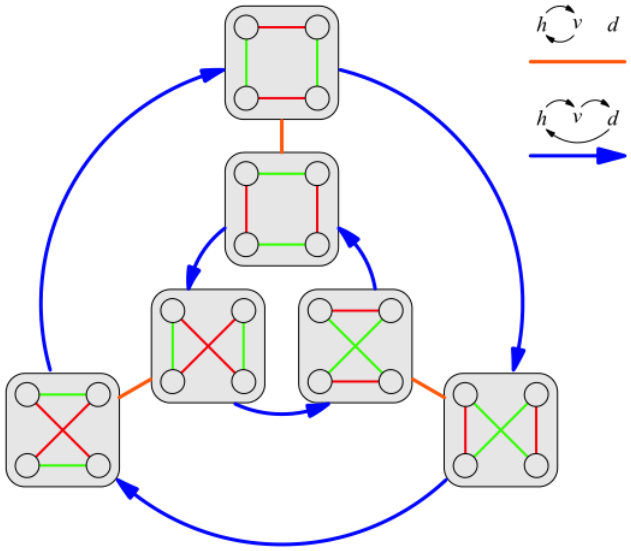


Figure 7.18. The group of all rewirings of V_4, generated by the two in Figure 7.16. The meanings of the arrows are given by the legend in the upper right.

图 7.15 与图 7.18 这样的图让我们想起了直积群的构造过程。因为这两张图也是把凯莱图当作节点，然后连接起来；这就跟定义 7.1 的步骤 2 十分相似了。不同之处在于，对于直积，我们在凯莱图的节点里拷贝了一模一样的另外一个群；而此处，我们在节点里放置的群却是彼此各不相同，因为它们的布线方式不同。如果进一步，把图 7.15 和图 7.18 再按照直积构造过程定义 7.1 的步骤 3 连接各个相应节点，就得到了所谓的半直积群（semidirect product group）。图 7.19 展示了如何如上所述把图 7.15 中的各个节点连接起来。我们将得到的结果称为 C_3 与 C_2 的半直积，因为其中的小群是 C_3 的两个 rewirings，而整体的结构却是遵循 C_2 的结构。C_3 与 C_2 的半直积用符号记为: $C_3 \rtimes C_2$

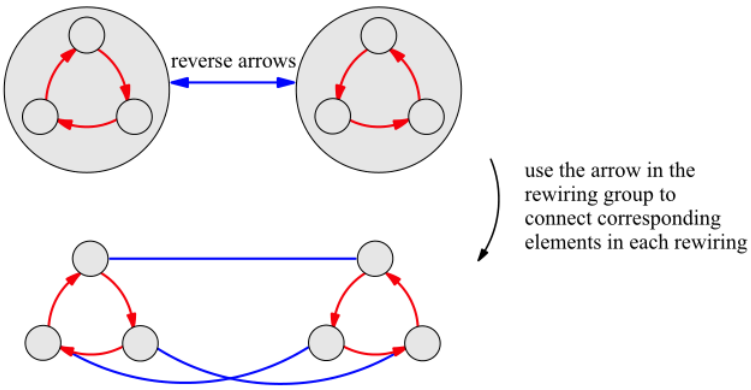


Figure 7.19. Applying Step 3 of Definition 7.1 to Figure 7.15 yields this semidirect product of C_3 and C_2, structurally identical to S_3.

半直积群的构造可以更一般地叙述如下：从任一个群 G 开始，画出它的各个 rewirings，并将凯莱图视为节点以此画出这些 rewirings 所形成的群的凯莱图 $(*)$，然后按照定义 7.1 步骤 3 中的规则，给所得凯莱图 $(*)$ 中的所有节点连接好箭头。你可以用这一方法并根据图 7.18，来画出 $V_4 \rtimes S_3$ 的一个凯莱图。但是，用我们这里所说的这种方法构建的半直积，只是诸多可能的半直积中的某一些，并不能得到全部的半直积。为了能更好的描述并构建出所有的半直积，我们需要群同态（homomorphism）的语言来描述这里的“rewirings”及其复合。我们将在第八章实现这一点，并将全面展示如何从任意给定的两个群 A 与群 B 出发构建出各种各样的半直积 $A \rtimes B$

7.3　正规子群与商运算

在 7.1.3 节中我们看到，我们可以使一些大阶群更容易理解，如果我们将其表述为直积群。只要理解了其中的因子和直积的构建过程，我们就可以用一种简单的方式来描绘一个否则将非常复杂的大阶群。同理可以设想，我们也需要一个类似的可以用来解构半直积的技术。因此，我们很自然地就想知道，当看见一个群时，如何才能将其重新审视为一个关于直积的凯莱图呢？也就是说，倘若一张凯莱图并非是你自己亲手用直积或半直积过程构建出来的，那你怎么辨识出它究竟是不是直积或半直积？是的话，你又怎么知道 A 和 B 具体是什么呢？

将大阶群解构为两个因子的最一般的方式叫作“取商（take a quotient）”. 这一运算不仅能揭示出直积，也能找出半直积。如果作了一次商运算后，你发现目标群暴露出了直积或半直积的样子，这就表明我们有机会能清楚地洞悉此群的结构。（当我们在第 8 章中学到更多关于半直积的知识后，这一点将显得更加明白）。商运算甚至还可以用来重新组织那些并非由直积或半直积构建出来的群的结构，而且由此揭示的结构常常有助

于我们进一步理解这些本身非直积也非半直积的群。群的积运算是将群相乘起来，而群的商运算则是对群做“除法”。我们选用群的某个合适的子群来“商掉”这个群（译注：以后将“商”这个词做动词使用，希望读者理解）。与本章介绍其他运算过程时一样，我在下面给出的定义中，同时也举了一个例子来具体说明整个流程操作。

定义 7.5 (商运算). 为了用 G 的某个子群 H 来商掉 G，请遵循以下步骤:

1. 将群 G 的凯莱图用 H 进行重组（如我们第一次在 *6.3* 节中所做的那样）图 *7.20* 最上方的图展示的示例是 $G = C_6$，$H =< 2 >$. 注意到，G 中 H 的陪集已经被我按行组织好了，这是为了给下面的步骤做准备。
2. 将 H 的每一个陪集缩并为一个节点，并将此时有着相同出发点与终点的箭头合并。这一步形成一个新的凯莱图，其中的节点数与箭头数都大大减少了。图 *7.20* 的中间与下方的图展示了这一步的操作。
3. 如果新得到的凯莱图是一个群，那么你就已经获得了 H 商掉 G 后的商群, 且这个新得到的凯莱图便是此商群的凯莱图；否则的话，则表明 G 不能用所选取的 H 作商运算。图 *7.20* 的最下方那张图表示的是 C_2，符合群的凯莱图的要求，也因此 C_3 商掉 C_6 得到 C_2.

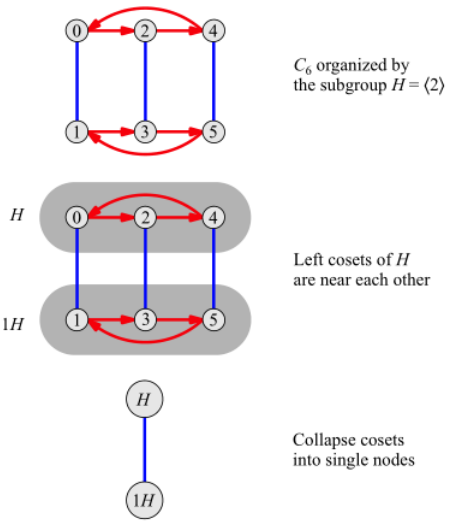


Figure 7.20. Application of the quotient process of Definition 7.5 to the group $G = C_6$ and subgroup $H = \langle 2 \rangle$, isomorphic to C_3. Notice that organizing the Cayley diagram of G by the subgroup H facilitates collapsing of the cosets of H.

显然，我们可以看出商运算在某种意义上同时是直积与半直积的“逆运算”。因为我们前面学到的两种积运算的操作流程都是拷贝节点、重连箭头；而进行商运算的过程则是缩并了这些拷贝和箭头。在这个例子以及以后的诸多例子中，特别要注意和理解的另一个重要的细节是，商群中的元素都是原来的那个子群 H 的陪集。图 7.20 底部图中

的节点名称表明了这一点。

但是在作商运算之前，这个群的原始结构是什么呢？比如说，C_6 究竟是直积呢，还是半直积？亦或是其它的什么积？我们可以看出，C_6 其实是一个直积，因为从图 7.20 顶部所示的 C_6 的凯莱图可以看出，它可由直积的构建过程得到：取 C_3 的两个拷贝，再辅以 C_2 的连接模式来连接相应节点。定义 7.5 中的第 1 步是必不可少的，因为它实际上起到了重新组织凯莱图的作用，以提取并显现出一个可能被其它画图方式所掩盖的结构。因此群 C_6 是直积群 $C_3 \times C_2$，尽管我们已经从上一章（特别是图 6.5）中知道了这一点。如果你想知道还有哪些像 C_6 这样具有隐藏着的直积结构的循环群，我们将会在 8.4 节回答这个问题！

使用商过程来解构任意一个直积群，我们按照如下所述就可以明确地找出直积 $A \times B$ 的两个因子：左因子 A 就是我们在施行定义 7.5 中的第 1 步时所用的那个子群 H，而右因子 B 则是在做商运算后所得的结果表示的那个群。

我们知道 S_3 是一个与 C_6 长得很像的群，其实在 S_3 中也有一个与 C_3 同构的子群。现在就让我们试着用 C_3 来商掉 S_3，并将其与前面的例子相比较。图 7.21 详细展示了 C_3 商掉 S_3 的三个步骤。可以发现 $\frac{C_6}{C_3} = \frac{S_3}{C_3}$ 所得结果均为 C_2，但是我们知道 C_6 和 S_3 显然是两个不同的群——这表明在商运算后，它们之间的差异被抹平了！事实上，“商”这一运算的特点与精髓正在与此：它是一种从“较为宏观”的大视角来审视原来的群的手段，而不去在意细枝末节上的差异，更关注于整体的结构。

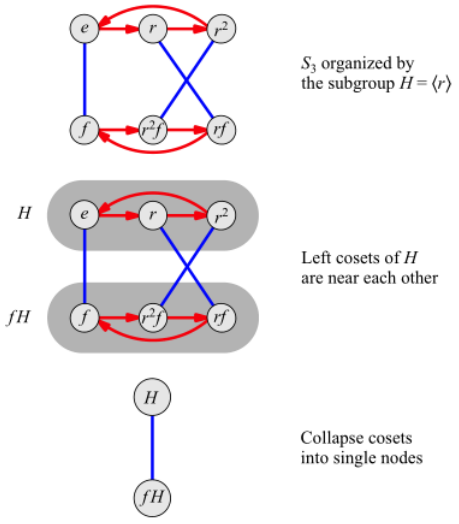


Figure 7.21. Application of the quotient process of Definition 7.5 to the group $G = S_3$ and subgroup $H = \langle r \rangle$, isomorphic to C_3. The result is the same as when we divided C_6 by a subgroup isomorphic to C_3, because the differences in the original groups have been removed by the quotient process.

之前我提到过，$\frac{C_6}{C_3}$ 拆解的是一个直积；所以很自然地，我们会问 $\frac{S_3}{C_3}$ 是否也是对某

个直积的解构？注意到图 7.21 顶部所示的 S_3 的凯莱图，其蓝色箭头并非如 C_6 一样是将 C_3 子群中的元素与 C_3 陪集中的相应元素按 C_2 的模式对应连接的（如图 7.20 顶部所示），而是发生了交叉。因此，S_3 并不是 C_3 与 C_2 的直积。我想你仍然会对这个理由有所怀疑，我们是否可以通过调整交叉的蓝色箭头来避免这样的问题出现呢？好的，那我们就来试试看！假如我们对 S_3 凯莱图的节点位置进行适当调整，以使得蓝色箭头不会发生像之前那样的交叉，如图 7.22；尽管此时的确是相应的元素都对应连接了，但是新的问题又出现了：图 7.22 中第二行用红色箭头连接的元素将不再是第一行的恒同拷贝（identital copy）！实际上，第二行此时是第一行的一个 rewiring. 这下就清楚了，无论我们如何调整，都不可能使 S_3 是 C_3 与 C_2 的直积；其实，S_3 虽然做不了直积，但它确实一个货真价实的半直积，即 S_3 是 C_3 与 C_2 的一个半直积。事实上，图 7.22 就是图 7.19，只不过画的时候布局方式有所不同而已。

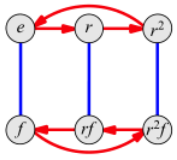


Figure 7.22. A rearrangement of the bottom row of S_3 from Figure 7.20 to uncross the vertical arrows.

因此，我们已经看到了商运算是如何揭示这两种积结构的：当做一个商运算产生的结果是恒同拷贝且其中相应的元素被对应着连接，则它揭示的是一个直积结构；当做一个商运算产生的结果不是恒同拷贝而是一些 rewirings 且其中相应元素被对应着连接，则它揭示的是一个半直积结构。我们也将看到做了商之后揭示的既非直积模式也非半直积模式的一些情形，尽管如此，这些商仍能帮助我们了解一个大阶群的结构（例如，习题 7.18）。

上面举的这些例子已经蕴含了丰富的信息，但是所用的群规模比较小。一个富有启发性的更大一点的例子是群 A_4，我们已经在图 5.27 中看到过它的样子。这张图强调了 A_4 与四面体的对称性之间的关系，但它并没有告诉我们太多关于这个群的内部结构的信息。我们来试试给 A_4 取商，以发现其中可能存在的更简单的结构。让我们用 A_4 中同构 V_4 的那个子群来作这个商运算。

按照定义 7.5 的第一步，图 7.23 展示了用子群 $< x, z >$ 重新组织后的 A_4 的凯莱图。这种重组需要用到生成元 x 和 z 所表示的箭头（图中红色与绿色箭头），以及另一个生成元所表示的箭头，用以连接 $< x, z >$ 的诸陪集，此处即是元素 a 表示的箭头（蓝色）. 定义 7.5 的第二步要求我们将重组后显露出来的 $< x, z >$ 的三个陪集分别缩并为单个节点，同时将连接陪集的冗余箭头都合为一个箭头。完成后，我们就得到了一个三阶的循

环群，如图 7.23 的底部。因此在 A_4 中隐藏着 C_3 的结构，或者说 $\dfrac{A_4}{V_4}$ 同构于 C_3.

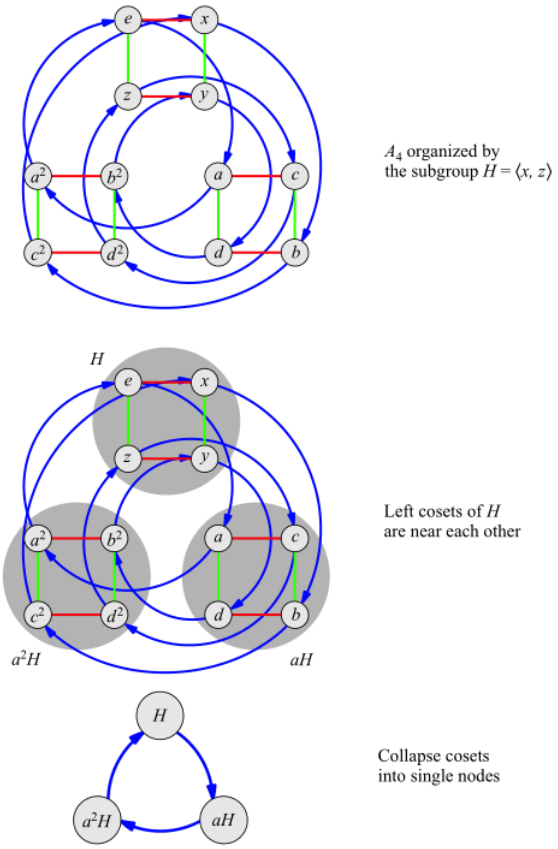


Figure 7.23. The quotient process computing $\frac{A_4}{V_4}$. All blue arrows from H lead to aH, and all blue arrows from aH lead to a^2H, and then back to H.

这个商是哪种积运算的逆呢？我们可以看出它不可能是直积，因为在图 7.23 上方所示的凯莱图中，连接 H 的各个陪集的箭头并不是严格按照对应元素来连接的。例如，子群 H 中的右上方节点并没有与其陪集 aH 中的右上节点相连。正如上面所举的 S_3 的例子，这里也并非是一个由图的布局所导致的简单问题。尽管我们可以重新排布图的节点，以使箭头能连接每个陪集中的相应元素，但这又将改变这些陪集本身的布局，如图 7.24 所示。这种取舍是不可避免的，原因就在于 A_4 本身的复杂结构；你可以把箭头排列相同的模式，或者是把陪集排成相同的模式，但却无法同时达到这两个要求，你最多只能达成其中之一。

因此，$A_4 \neq V_4 \times C_3$，但是确有可能是一个半直积。在图 7.24 中，经过对陪集布置方式的重新安排，蓝色箭头成功连接着对应元素。注意到，此时这张图就是半直积 $V_4 \rtimes S_3$ 的外围一圈，参看图 7.18。图 7.25 进一步展示了这种模式。因此，群 A_4 便是那个大的半直积群的一个子群。当我们在第八章全面学习半直积的知识后，我们就会知道如何将

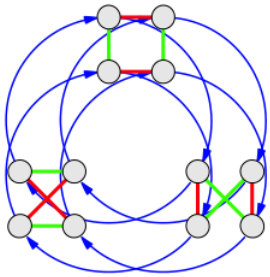


Figure 7.24. The cosets of V_4 in A_4 rewired to demonstrate its semidirect product structure.

A_4 表达为 C_3 和 V_4 的半直积。不过目前，我们只需知道商过程给我们揭示出了 A_4 的一个简单结构，如图 7.25 所示。

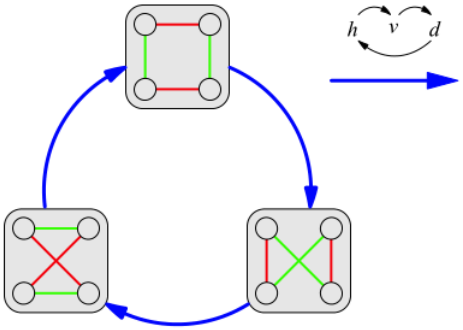


Figure 7.25. The pattern in A_4 as a subgroup of a rewiring group. To create A_4, connect the corresponding nodes in each rewiring with arrows in the three-cycle shown.

正如定义 7.5 步骤 3 中的措词所表明的那样，在某些情况下，尝试进行一个商操作可能不太顺利，甚至会得到一个无效的凯莱图。因此，来看看这样一个导致无效的凯莱图的例子，对于加深我们的理解是非常重要的。恰好 A_4 就可以提供一个这样的例子，而这个例子也将帮助我们导出一个用于判别商操作何时会成功，何时会失败的定理。

当我们最初在图 5.27 中见到 A_4 时，它的结构是用三阶子群 $< a >$ 来组织的。图 7.26 显示了当我们试图用这个子群来划分 A_4，却发现所得结果不是有效的凯莱图。这其中有几个原因，但最明显的就是图 7.26 中那唯一的箭头（蓝色箭头）的指向是有歧义的、不明确的。例如，从顶上节点出发，蓝色箭头并不是只有唯一一个节点作为其终点，而是有三个终止节点。因此，这个图不能用来描述一个群，也就不是凯莱图。（回忆一下习题 2.14 到 2.17 中的那些可视化原则，在 6.1 节也有提到）

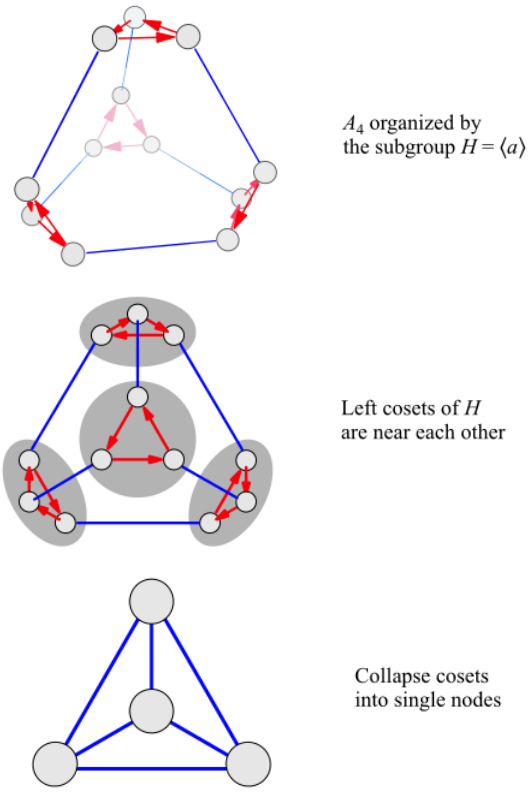


Figure 7.26. An organization of A_4 by a subgroup that is not normal, and therefore does not allow us to take a quotient.

所以我们看到，商运算对于某些子群来说是可行的，而对于另一些则不可行。为了说明我们真正理解了商的过程，我们需要知道这其中的原因。究竟是什么决定了一个群或子群能否成功地商掉别的群？正如我们这一节的标题所示，决定因素就在于这个子群是否是正规的（normal）.

定理 7.6. 设 $H < G$. $\dfrac{G}{H}$ 能构成一个商群当且仅当 $H \triangleleft G$.

证明. 定义 7.5 中规定的商过程，只有当其所得的结果是一个有效的（valid）凯莱图时，我们才能说此商操作是成功的。实际上，商过程已经足以保证一个图能成为凯莱图所需的绝大多数条件。例如，因为我们是从一个每个节点都有箭头相连的图开始的，所以我们所得的结果图也仍然具有这个性质，即图的连通性是得到保证的；又因为我们是从一个正则图（参见定义 6.1）开始进行商运算的，并且整个整合的过程是针对那些散布在图中但具有完全相同结构的部分（也就是子群与其陪集），因此我们最终得到的结果图也具有正则性。

不过可能会出现另一个问题。回想一下图 7.26 中我们得到的那个结果图所违反的

规定：对于任意一个给定的节点，每一种箭头只能进入或离开此节点一次。我们的图已经用颜色来区分了每种箭头，因此，也可以直观的来看，即一种颜色的箭头只能进入或离开任一节点一次；或者简单地说，“箭头指向须无歧义（unambiguous）”。这是因为在我们的操作中，是将原来许多不同的节点合并成一个节点，且还将这些节点之间原有的箭头都“强行拆掉了”，在这样略显“粗暴”的操作中，我们很难再保证所得图中的箭头指向是无歧义的，从而导致得到的结果图可能不满足上述“箭头指向无歧义”的要求。所以，这个定理实际上又可归结为以下事实（目前我还没有提供证明）：要想在合并左陪集后得到箭头指向无歧义的图，当且仅当所挑选的子群是正规的。我将通过比较那些在合并后变得指向不明确的箭头所具有的样子，与那些仍然保持明确指向的箭头的样子，来说明这一点的正确性。

考虑同种箭头（也就是颜色相同的箭头），如果从一个左陪集射出的该种颜色箭头，分别指向了两个或更多个不同的左陪集中的节点时，此时合并诸陪集将产生出“指向有歧义（ambiguous）”的箭头；图 7.27 中的左图形象地展示了这一点，并且借助于这张图，我们也因此能更清晰地看出导致图 7.26 中问题的症结所在。另一方面，如果从一个左陪集中射出的所有同色箭头都一致地指向另一个左陪集中的各个节点时，就不会出现“指向有歧义”的情况；这一点如图 7.27 中的右图例证所示，并且我们在前面看过的三个例子，如图 7.20，图 7.21 和图 7.23，正好就于它们的商过程中体现了这一点。

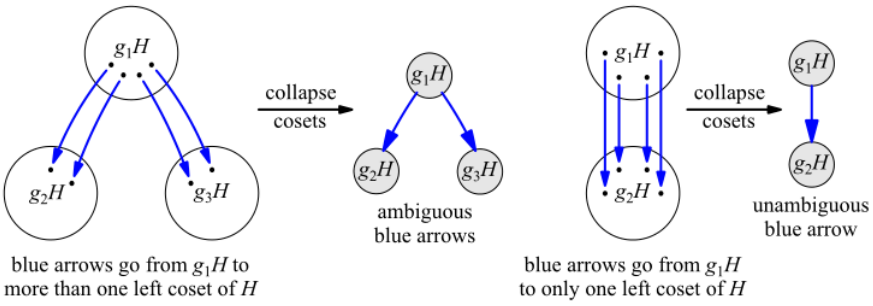


Figure 7.27. Arrows sending a left coset to several others cause ambiguity when the cosets are collapsed. Arrows unanimously sending a coset to one other coset do not create ambiguity after collapsing.

之所以只有当所选取的子群是正规子群时，才能使左陪集之间的箭头指向一致，个中缘由就在于我们最初于第六章中讲到的左陪集和右陪集的可视化技术。重新再回过头来瞧瞧图 6.8，这张图告诉我们，可以将左陪集 gH 可视化为：每次都从节点 g 出发，遍历 H 中的所有路径所能到达的节点的集合。图 6.8 也告诉我们可以将右陪集 Hg 可视化为：每次从 H 中挑一个节点出发，都走路径 g，当出发点遍历 H 中所有节点后，所能到达的节点集合就是此右陪集。这两种可视化技术实际上已经揭露了正规子群满足的条件“对任意 $g \in G, gH = Hg$”所具有的特征。我们将其重述如下：

如果存在一根从 H 中射出的 g 箭头指向了 H 的某个左陪集 gH，那么从 H 中射出的其他所有 g 箭头都会一致地指向此左陪集。（因为 $Hg = gH$）.

说的更详细点，即从 H 中的任意一个节点出发，沿着箭头 g 走到的终点恰好就是左陪集 gH 中的节点；再换句话说，即所有从 H 射出的 g 箭头都全体一致地指向了 gH. 注意到 $g \in G$ 还得是任意的，不同的 g 反映在图中就是不同颜色的箭头，因此，一个子群是正规子群当且仅当从 H 中射出的任意一种颜色的箭头都具有一致的朝向。

图 7.28 展示了这一点，它将图 6.8 中的两幅图示结合在了一起。此外，由于凯莱图是正则的，所以连接 H 与其每个左陪集之间的箭头所遵循的这一模式，也将在 H 的任意两个拷贝（即任意两个左陪集）之间重复出现，并遍及整张凯莱图。因此，一个子群是正规的也当且仅当陪集之间每一种颜色的连接箭头都具有一致朝向，此时在合并所有的左陪集后，就得到了一个箭头指向无歧义的图，也就是商运算能成功进行的时候。 □

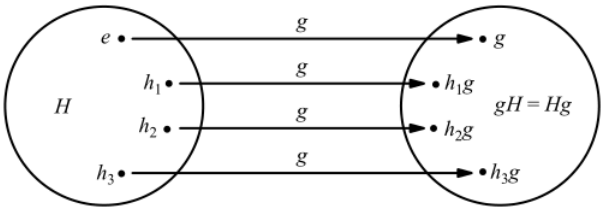


Figure 7.28. When H is normal, $gH = Hg$, and thus the illustrations in Figure 6.8 on page 104 lead us to picture g arrows as unanimously connecting H to gH.

这一定理给我们展示了正规子群在群论中所扮演的重要角色。最开始，我们将正规子群描述为其任一左陪集同时也是其右陪集的子群，这在那时似乎并不是什么很重要的特征。但是现在，我们知道它的重要意义了：一个正规子群是一个我们可以用之来对大阶群作商运算的工具，并由此揭示大阶群的整体结构，以使我们能更好地理解一个大阶群。因此，我将利用本章剩下的两节篇幅来增加我们关于正规子群和商群的经验，并为随后第九章与第十章中更进一层的内容做好准备。

7.4　正规化子

让我们再次来研究正规子群的问题，并问一个简单的问题：能否找到某种方式来衡量一个子群的“正规程度”？或者说它距离成为一个正规子群还有多远？这个问题的答案将揭示一些十分有趣的模式结构，而这些结构也将进一步帮助我们理解正规子群。

我们知道一个子群是正规的，如果任一个元素 $g \in G$ 都满足等式 $gH = Hg$，因此一个十分自然的想法便是去检查大群 G 中有多少元素能够满足上述等式，以此来衡量一个子群 H 的“正规程度”。打个比方，我们把大群 G 视为一个民主团体，每个元素

$g \in G$ 都拥有投票的权利，现在大家通过投票来决定内部的一个小团体——某个子群 H 是否应该被推举为“正规子群”，最后统计有多少赞成的票。只有那些能赢得全体一致赞成票的子群 H，才会被授予梦寐以求的“正规 (normal)”的头衔。

至少我们知道，对于 H 中的每一个元素都肯定会投赞成票，这是因为对任意 $g \in G$，均有 $gH = H = Hg$（这就像总统竞选人通常总是先得到自己故乡人民的支持一样）。另一种极端情况则是当 H 恰好就是正规子群时，此时所有的 $g \in G$ 都投了赞成票。但很多时候，投票结果往往介于这两种特殊情形之间，此时我们就可以用赞成票的数目来衡量 H 距离当选为“正规子群”还有多远。我们称，G 中支持 H 正规的那些元素所组成的集合，为 H 在 G 中的“正规化子（normalizer）”，记作 $N_G(H)$.

我们规定 G 中的这种民主制度遵循“民主集中制”原则：对于 H 的陪集，总是投集体票。即若某个 $g \in G$ 投了赞成票（g$H = Hg$），那么陪集 gH 的其他成员元素将毫无异议的全部投赞成票。这种“民主”规定是有它的道理的，因为观察 6.5 告诉我们，任意一个 $k \in gH$ 都可作为这个陪集的代表（对于右陪集也是如此），即 $gH = kH$，且 $Hg = Hk$；所以 k 投赞成票（k$H = Hk$）当且仅当 g 投赞成票 ($gH = Hg$)。这种“民主集中制”的投票模式大大简化了正规化子 $N_G(H)$ 可能的样子，尤其是对“计票工作”来说（正规化子的大小），大大减轻了负担。因为 $N_G(H)$ 是由整个的一些陪集组成的，所以 $N_G(H)$ 的大小总是子群 H 的大小 $|H|$ 的整数倍。

更进一步，决定一个左陪集作为一个团体是否会投赞成票的关键在于它是否也是一个右陪集。因为从定义可以知道，gH 集体支持 H 正规当且仅当 $gH = Hg$。因此正规化子 $N_G(H)$ 是由那些同时为左陪集和右陪集的陪集组成的，这就给我们提供了一种从凯莱图中可视化正规化子的方法。根据上一节，我们可以将这种方法描述的更直白些：所谓正规化子，是由一些陪集组成的集合，其中这些陪集满足射出的箭头可以全体一致的指向子群 H 这一条件。让我们举几个例子。

为了简单起见，我先举一个正规子群的例子。我们在图 7.23 中能够看出 $< x, z > \triangleleft A_4 >$, 因此它的三个左陪集也都同时是右陪集，它们通过无歧义的箭头彼此相连，因此正规化子 $N_{V_4}(A_4) = A_4$。图 7.26 提供了另一个极端情况的例子。我们已经知道 $< a >$ 不是 A_4 的正规子群，它有 4 个左陪集 ($< a >$ 本身也算一个)，但是从上一节我们知道，它的左陪集并非也是右陪集，因此除了 $< a >$ 本身以外，没有人支持它成为正规子群，即 $N_{A_4}(< a >) =< a >$.

当然啦，更有趣的例子并非是这些极端情形，而是那些“有点正规（somewhat-normal）”但实际上并不正规的子群。图 7.29 展示了群 D_6——用它的子群 $< f >$ 及左陪集重新组织后的凯莱图。我们考虑左陪集 $r < f >$，从图中可以看出不存在连接 $< f >$ 和 $r < f >$ 且保持一致性的箭头：因为从子群 $< f >$ 中节点 e 出发的 r 箭头指向

了 $r < f >$ 中的节点 r（正是这一点使得 $r < f >$ 成为一个左陪集），但是从子群 $< f >$ 中节点 f 出发的 r 箭头却指向了另外的左陪集 $r^5 < f >$，而不是一致的指向 $r < f >$ 中的节点。同样的情况也发生在了左陪集 $r^2 < f >$，$r^4 < f >$ 和 $r^5 < f >$ 身上，它们都没有能和 $< f >$ 一致相连的箭头，这一点请读者自行验证。有趣的是，左陪集 $r^3 < f >$ 与之前提到的各个陪集又有所不同：你会发现路径 r^3（连续走三个 r 箭头）却是实实在在地连接了 $< f >$ 和 $^3 < f >$，而且是一致的！尽管在凯莱图中看来，一条是沿顺时针方向，另一条是沿逆时针方向。类似的，如果你从 $r^3 < f >$ 中的节点出发，沿着 r^3 路径前进，也能够一致的、无歧路的走回到子群 $< f >$ 中。因此，正规化子 $N_{D_6}(< f >)$ 并不是只包含 $< f >$ 这一个团体，还包含了它的一个陪集 $r^3 < f >$. 这表明，尽管子群 $< f >$ “正规 (normal)”无望，不过它确实是有除了自己“家乡人民”之外的支持者的。

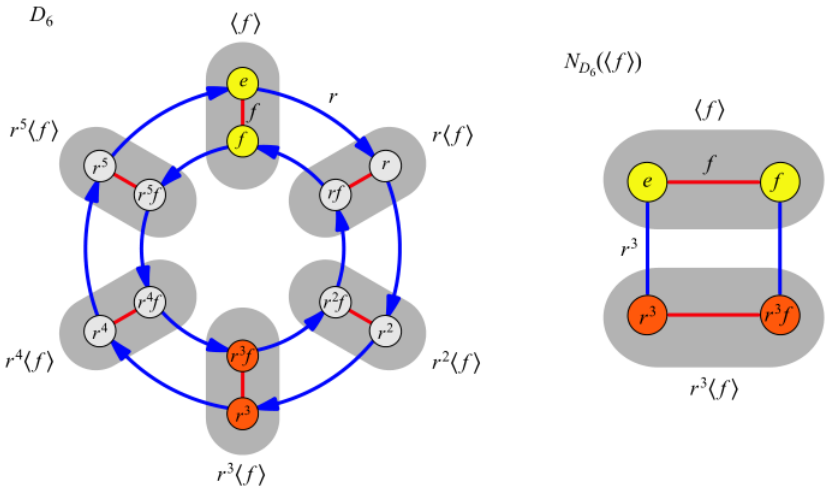


Figure 7.29. The subgroup $\langle f \rangle$ in D_6 is not normal, but neither is it its own normalizer. The normalizer $N_{D_6}(\langle f \rangle)$ is $\langle f, r^3 \rangle$, a group isomorphic to V_4, as shown on the right.

图 7.29 右边展示的是从左图中摘取出的正规化子 $N_{D_6}(< f >)$。正如你所见，它并非只是一些节点的集合，而是一个群！并且 $< f >$ 在其中是正规的。这两个事实并非巧合，或许你没想到正规化子能构成一个群；但是你应该很容易想到，原本的子群在它的正规化子中能够正规，这一事实。毕竟，所谓正规化子就是由那些支持该子群正规的元素组成的，是它的盟友！所以原子群在正规化子中正规也就是理所当然的了（在支持你的人中获得支持，理所应当！）。因此，我们着重来探讨前一个事实，为何每一个正规化子本身也是一个群？

定理 7.7. 设 G 为一个群，对于任意 $H < G$，均有 $N_G(H) < G$.

证明. 在此前，我们用过记号 $< a, b, c >$ 来表示一个由元素 a，b，c 生成的子群。所谓

生成一个子群，是指将 a,b,c 及其逆元 a^{-1},b^{-1},c^{-1} 以各种方式组合在一起（按乘法）。我们很清楚这将产生一个群，因为这正是我们在第二章中用来构建群的方法。

设 $N_G(H)$ 中的元素为 $\{g_1, g_2, \cdots g_n\}$，考虑由这些元素生成的子群 $< g_1, g_2, \cdots g_n >$. 我们来证明 $N_G H =< g_1, g_2, \cdots g_n >$，从而说明 $N_G(H)$ 是一个子群。作为集合来说，后者包含前者是显然的；因此只需去证明前者同样包含后者。为此，首先我们证明 $N_G(H)$ 中任意两个元素的乘积任然在 $N_G(H)$ 中，其次证明 $N_G(H)$ 中任意一个元素的逆也仍然在 $N_G(H)$ 中（译注：熟悉抽象代数的读者，会发现其实这正是证明子群的一般方法）。

考虑 $N_G(H)$ 中任意两个元素 g_1 和 g_2。每一个元素都代表 G 凯莱图中的某条路径，并且这些路径一定无歧义的连接了子群 H 的诸陪集，这是因为 $g_1, g_2 \in N_G(H)$. 图 7.30 形象地展示了复合路径 $g_1 \cdot g_2$ 仍然保持箭头的指向一致性。因此 $g_1 \cdot g_2 \in N_G(H)$，这进一步表明 $N_G H$ 中的元素 $g_1, g_2, \cdots g_n$ 之间按任意方式组合（乘法）在一起得到的元素仍在 $N_G H$ 中。（译注：由于这本书的特点就是尽量的可视化，所以有些证明的说法不太严谨。此处用符号语言来说更好理解。因为 $g_1 \cdot g_2 \in N_G(H)$，所以 $g_1 H = H g_1$, $g_2 H = H g_2$，所以 $(g_1 \cdot g_2)H = g_1 H g_2 = H(g_1 \cdot g_2)$，所以 $g_1 \cdot g_2 \in N_G(H)$）

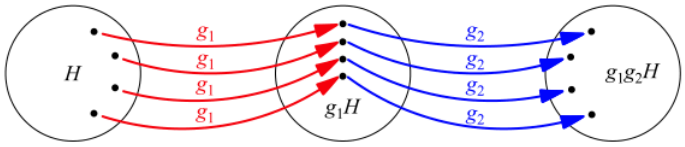


Figure 7.30. Following sequentially from H g_1 and g_2 arrows, two different sets of arrows that connect the cosets of H unanimously, shows that the product $g_1 g_2$ must also connect the cosets of H unanimously.

我们接着来说明 $N_G(H)$ 中每一个元素的逆也仍然在 $N_G(H)$ 中。任取 $g \in N_G(H)$，则 g 表示 G 凯莱图中的某条路径，并且路径 g 一定无歧义的连接了子群 H 的诸陪集。取两个左陪集 aH 和 bH，满足路径 g 从 aH 中射出，一致地终止于 bH。那么，除了从 aH 中射出的 g 箭头外，不可能再有别的 g 箭头能够终止于 bH，这是因为在 bH 中已不再有这些“外来客”的落脚之处，都被来自 aH 的箭头占满了位置 ($|aH| = |bH| = |H|$) 且任意两个 g 箭头不能终止于 bH 中同一节点 (g 箭头的指向具有一致性)。因此，落入 bH 中的箭头只能全部来自于 aH，从而当我们从 bH 出发沿着相反的箭头，也能够一致的回到 aH 中，也即 g^{-1} 为从 bH 指向 aH 的无歧义的箭头，也就是说，$g^{-1} \in N_G(H)$. （译注：还是给出符号语言的证明以供参考。任取 $g \in N_G(H)$，则 $gH = Hg$，左乘 g^{-1} 得 $H = g^{-1}Hg$，再右乘 g^{-1} 即得 $Hg^{-1} = g^{-1}H$，所以 $g^{-1} \in N_G(H)$）

由以上证明我们就知道，$g_1, g_2, \cdots g_n$ 及其逆元之间按任意方式组合（乘法）在一起得到的元素仍在 $N_G(H)$ 中，所以 $< g_1, g_2, \cdots g_n >= N_G(H)$，这就证明了 $N_G(H)$ 是 G 的一个子群。 □

这一定理表明 $N_G(H)$ 是一个群，之前我还提到，它同时也是一个能够让 H 在其中正规的群。我们之所以称 $N_G(H)$ 为“正规化子 (normalizer)”，也是由于这个定理，它告诉我们至少要从 G 中刨除多少个元素才能使得 H 成为一个正规子群。

图 7.31 形象地展示了关系式 $H \triangleleft N_G(H) < G$ 的一些重要方面。首先，集合 $N_G(H)$ 的大小是 $|H|$| 的整数倍，而 G 的大小又是 $|N_G(H)|$ 的整数倍，所以如果想要明显地区分 H, $N_G(H)$, G 这三者，就需要 H 相对于 G 的大小足够小 (最多占比 $\frac{1}{4}$) 才行。其次，$N_G(H)$ 中的元素分界线为子群 H 的左陪集，或者更直白的说，$N_G(H)$ 要么一整个陪集都包含，要么一整个陪集都不包含。最后，更精确的说，$N_G(H)$ 只包含那些本身既是左陪集也是右陪集的陪集。尽管整个大群 G 都充斥着子群 H 的拷贝 (即 H 的左陪集)，但是 $N_G(H)$ 的边界只要在保持关系式 $H \triangleleft N_G(H) < G$ 成立的前提下，就可以尽可能的大。第九章我们将更深入地探讨子群，于其时，正规化子将成为我们的有力工具。

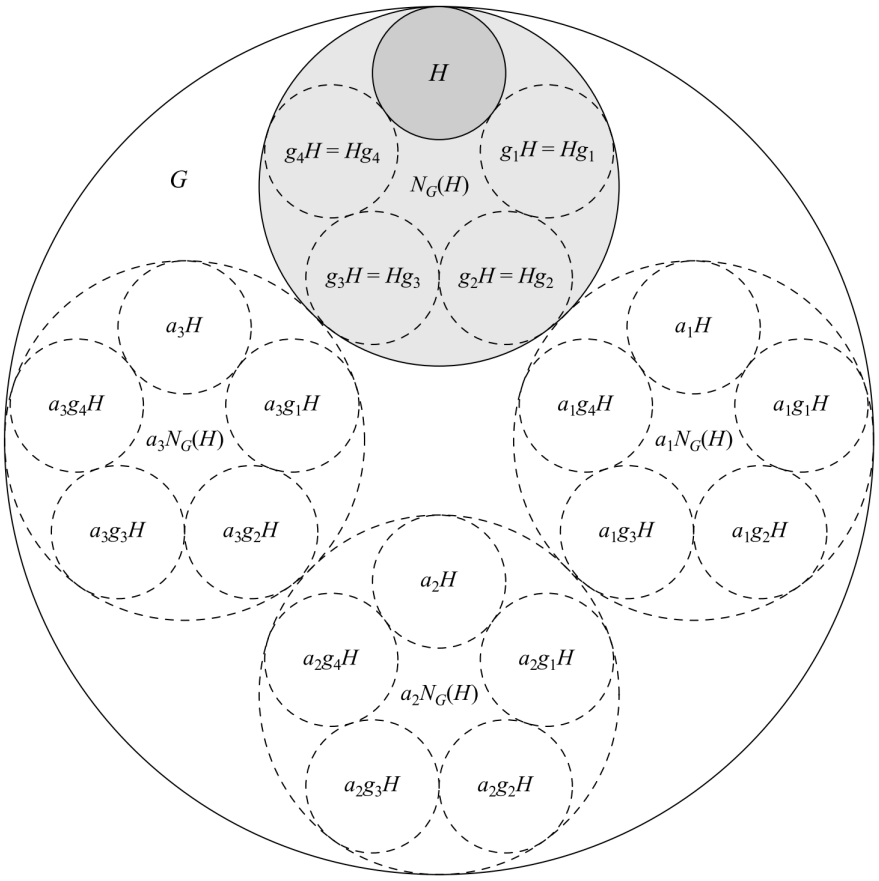


Figure 7.31. Abstract visualization of the relationships $H \triangleleft N_G(H) < G$. Cosets of H are labeled g_1H, g_2H, etc., while cosets of $N_G(H)$ are labeled $a_1N_G(H)$, $a_2N_G(H)$, etc.

7.5 共轭

到目前为止，我们都在使用正规子群最常见的一种定义，即 $H < G$ 是正规子群当且仅当对任意 $g \in G$ 均有 $gH = Hg$. 另一种常见 (当然也是等价的) 的方式是将等式 $gH = Hg$ 重新表达为 $gHg^{-1} = H$，后一形式是将 $gH = Hg$ 左右两边同时右乘 g^{-1} 得到的，具体如下：

$$\text{原本的等式:} gH = Hg$$

$$\text{两边右乘 } g^{-1}\text{:} gHg^{-1} = Hgg^{-1}$$

$$\text{右边可以消去:} gHg^{-1} = H$$

这一等式表达了与原等式相同的信息，因此也可以用它来等价地描述子群正规的条件。

正如等式 $gH = Hg$ 两边表示的都是群中元素的集合，等式 $gHg^{-1} = H$ 也是如此。后面这个新的等式告诉我们，如果你将任意 $h \in H$ 左乘 g 再右乘 g^{-1}，得到元素 ghg^{-1}，当 h 遍历 H 时，这样的元素组成一个集合就记为 gHg^{-1}，那么这个集合 gHg^{-1} 其实就是子群 H。从可视化的角度来看，这就是说以左陪集 gH 中的节点为箭头 g^{-1} 的出发点，则箭头 g^{-1} 全体一致地指向子群 H。

我们将等式 $gH = Hg$ 重新写成 $gHg^{-1} = H$ 的动机 (motivation)，是为了展现正规子群与一种称之为“共轭 (conjugation)”的运算之间的联系。将元素 h 两边用另一元素 g 及其逆元 g^{-1} 包围住 (得到元素 ghg^{-1})，我们称这种运算为用 g 共轭 h，同时所得到的结果称为 h 关于 g 的共轭元，简称“共轭”。同理，集合 gHg^{-1} 称为 H 关于 g 的共轭。由开头的介绍我们已经知道，正规子群可以用共轭来定义，因此这两个概念之间有着深刻的联系。本节就来探索一些正规子群与共轭之间的联系。

表达式 ghg^{-1} 似乎显得有点随意，所以我打算先解释一下，为什么用一个群元素 g 共轭另一个群元素 h 这一操作往往具有十分自然而实用的意义？我们将 ghg^{-1} 视为一连串的作用或操作 (actions)，那么共轭式 ghg^{-1} 就表示先施加操作 g，再施加操作 h，接着施加操作 g 的逆操作。我们身边许多的日常事件都可由这种模式描述。举个例子，我们假设 h 表示开瓶子这一简单的操作。有时瓶盖盖得太紧了，你施加操作 h 就很困难，这时你也许就会先用热水冲淋瓶盖将其稍微加热 (将加热操作记为 g)，然后打开瓶子 (操作 h)，再让盖子冷却 (操作 g^{-1})。这样，操作 h 就被你用操作 g 暂时置于另外一种情境 (context) 中去了，因此得到的结果就会跟你单独施加 h 操作有所不同了。

再举一个例子，假设操作 h 表示一个乐队在演奏他们的歌曲，操作 g 表示这个乐队驱车前往他们的演出场地。在平常排练时，这支乐队会多次进行操作 h；但在音乐会之夜，事情就稍有不同了：他们用操作 g 共轭了平日常常进行的操作 h，从而将演奏这一行为“搬”到了一个新的环境——演出场地 (当然这也是更赚钱、更令人兴奋的环境)。

也就是说，乐队先驱车到达演出场地 (操作 g)，进行演出 (操作 h)，然后开车返回 (操作 g^{-1})。因此，理解共轭 ghg^{-1} 的一个好方法是将其想象为，用操作 g 将操作 h “搬” 到了一个新的情境或场合。正因为如此，一个操作与其共轭常常有许多共同点。

前两个例子很容易理解，但它们并不是来自群论中的例子。我们再来举一个群论中的例子来理解共轭。考虑群 A_4---正四面体的对称性群。与前面一样，我用字母 a, b, c, d 来分别表示在正四面体四个不同顶点处所作的四种顺时针 120 度旋转操作 (详见图 7.32 的文字说明)，显然 a, b, c, d 均为群 A_4 中的元素。在图 7.32 中，我将正四面体的四个顶点标上了大写字母，相应的小写字母就表示该顶点处的旋转操作。我们在前面说过 “一个操作与其共轭常常有许多共同点”；这里，这四个旋转操作中的任意一个都是其余的共轭，因为每一个旋转操作除了所处的情境不同 (具体来说即所处顶点不同) 之外，基本上都是相同的。让我们来具体看看它们为何彼此共轭。

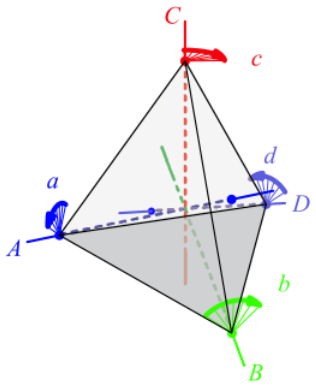
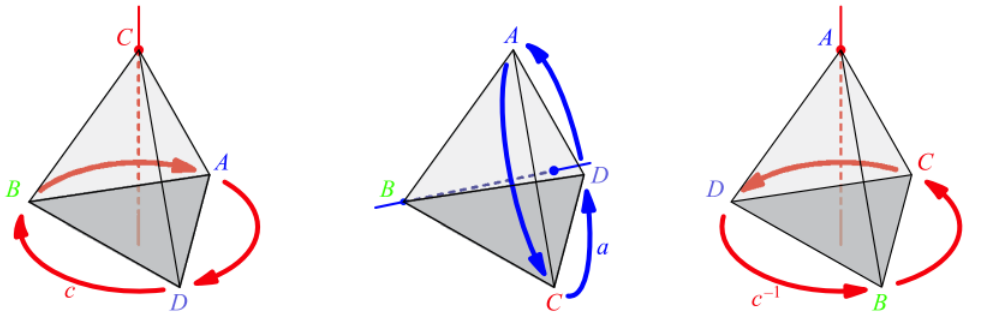


Figure 7.32. A tetrahedron with vertices A, B, C, and D. From each vertex a line through the opposite face is drawn, and the actions of rotating the entire object 120 degrees clockwise around each such line are labeled a, b, c, and d, respectively. (Here “clockwise” is interpreted from the point of view that looks toward the vertex from outside the tetrahedron.)

我将展示如何用群 A_4 中的某个别的元素来共轭 a，从而得到 b；当然，这里只是用 a, b 作示范，其他任意两个旋转操作之间的共轭循例亦可得。我们知道，操作 a 表示关于顶点 A 作一个顺时针旋转，操作 b 表示关于顶点 B 作一个顺时针旋转；因此我们首先需要一个能够将正四面体重新定向 (reorient) 操作，从而使得操作 a 转变为关于顶点 B 的顺时针旋转。这很容易做到，只要在群 A_4 中随便找一个能够实现将 B 顶点的位置变到图 7.32 中最左边顶点位置 (即 A 的位置) 的操作即可，这样我们就可以 “麻痹” 操作 a，让它 “误认为” 还是在作关于顶点 A 的旋转，从而实现将其变成关于顶点 B 的旋转操作这一目标。比如，操作 c 就是一个满足我们以上设想的操作。

图 7.33 详细展示了当我们用 c 来共轭 a 时所发生的情况，其中每一幅图代表作共轭运算时的一个步骤且展示了每一次操作完成后正四面体的朝向 (假设正四面体的初始

朝向如图 7.32)。最后的结果是，顶点 A, C, D 相比于初始状态各顺时针旋转了一个位置，这就使得我们所做的这一系列操作等价于做一个操作 b。因此，用 c 来共轭 a 确实得到结果 b，代数语言来表达即为 $cac^{-1} = b$。仿照这个例子，我们容易知道，在正四面中任意两个绕着顶点的 120 度顺时针旋转操作之间都是共轭关系。



After doing c, we find that B has taken the place of A.

Therefore, the a action now rotates about the point B.

The c^{-1} action puts the vertex B back where it began.

Figure 7.33. Conjugating a by c results in b, written $cac^{-1} = b$. This figure assumes the tetrahedron began in the configuration shown in Figure 7.32. Thus you can verify the equation $cac^{-1} = b$ by picturing the effect of b on the tetrahedron in Figure7.32; your result should be the result of the conjugation shown here.

因为共轭的两个元素之间常常有一些共性，因此，很自然的想法便是依据共轭关系来划分群，以期从中获取一些有用的信息。但是在作这样的划分之前，我们还需要检查一下共轭关系是否具有三个关键的特性——这也是所有可以用来进行划分的关系所必须满足的性质。在本章习题 7.36 中，我要求各位读者自己证明共轭关系确实满足那三个性质，此处按下不表。因此，事实上，群元素间的共轭关系也是一种等价关系，从而我们可以放心大胆的来用共轭关系对群进行等价划分。另外我们注意到，在那三个性质中有一条是说“若元素 a 是元素 b 的共轭，则 b 也是 a 的共轭”(对称性)，因此像“a 与 b 是共轭的”这样的简单表述也就显得十分自然而常见了。

表格 7.1 将群 A_4 中的元素依据共轭关系作了划分。其中属于同一行的元素彼此共轭，不属于同一行的任意两个元素则不共轭。注意到这样划分后，每一行的共轭元素之间所具有的共性就被简洁而有意义的描述出来了。像表格 7.1 中这样的每一行，我们称之为“共轭类 (conjugacy class)”。

一个常见的用来提取共轭类表格中信息的方法是，将每一个共轭类的大小或阶 (size) 加起来写成一个等式，得到的和就是该群的大小。比如说我们上面看到的表格 7.1，各个共轭类的大小分别是 $1, 3, 4, 4$，我们将其相加写成

$$1 + 3 + 4 + 4 = 12$$

Elements	Description
e	the identity element
x, y, z	180-degree flips (illustrated in Exercise 5.25)
a, b, c, d	120-degree clockwise rotations about vertices
a^2, b^2, c^2, d^2	120-degree counterclockwise rotations about vertices

Table 7.1. Conjugacy classes of A_4 described.

其中 12 就是群 A_4 的大小。像这样的一个等式我们称之为“类方程 (class equation)，因此 $1+3+4+4=12$ 就是群 A_4 的类方程。在类方程中，等号左边加数的个数即为该群拥有的共轭类的个数，且每个加数表示一个共轭类的大小，等号右边的数字表示群的大小。尽管类方程看起来十分简单而平凡，但其却携带着令人惊讶的丰富信息。现在，我要将你们的注意力重新拉回到本节所思考的共轭概念的出发点——正规子群上来了，因为类方程的一个重要应用便源自于它与正规子群之间的联系。

在本节开头，我指出正规子群的决定性特征 $gH = Hg$ 也可以表达为 $gHg^{-1} = H$，由此引出后文关于共轭的探讨。因此回过头来，我们可以用共轭的语言重新表述正规子群的这一特征，即正规子群 H 中的任意一个元素 h，它的所有共轭元也必在 H 中；这是因为 h 的任意一个共轭元 $ghg^{-1} \in gHg^{-1}$，而对于正规子群 H 而言，$gHg^{-1} = H$，因此 $ghg^{-1} \in H$。再换句话说，对于正规子群中的任意一个元素，该元素所在的共轭类整个包含于该正规子群。因此一个正规子群实际上是由一些共轭类组成的 (正规子群的“内部构造”)。

类方程的一个重要应用就是帮助我们高效的寻找一个群可能的正规子群，它可以极大的缩小我们的搜索范围；下面还是用群 A_4 来举例说明。从群 A_4 的类方程 $1+3+4+4=12$，我们可以知道群 A_4 有四个共轭类，大小分别为 $1, 3, 4, 4$，那么 A_4 的正规子群只可能是这些共轭类的组合；这是因为根据上一段内容，我们不能只把“半个”共轭类放进正规子群中，要放必须是一整个共轭类都放进去！因此，为了找出 A_4 所有的正规子群，我们将数字 $1, 3, 4, 4$ 进行不同的组合并加以验证，从而用共轭类先构造出可能成为正规子群的“候选”子群。注意，在对数字进行组合时，有两条限制条件：第一，由于我们是在试着构建子群，所以必须得有单位元，即要先选出含有单位元的共轭类；第二，组合的结果须满足拉格朗日定理，即子群的阶 (大小) 整除大群的阶。在群 A_4 的例子中，当把这两个限制条件考虑在内时，我们发现只有三种可能的组合方式：

群 A_4 本身:$1+3+4+4$

单位元与 180 度翻转操作的组合:1 + 3

平凡子群:1

没有其他的 1, 3, 4, 4 的组合能满足加起来等于 12 的某个因子了。群本身以及平凡子群是任意一个群的正规子群，所以它们两个出现在上述清单上并不让人感到意外。真正有趣的是中间那个组合，利用表格 7.1 我们知道这就是表中前两行的组合 $\{e, x, y, z\}$。

仅仅只从上述工作来看，我们还不能断言 $\{e, x, y, z\}$ 就是一个正规子群；还需要考察一下它的凯莱图或乘法表来进一步判断 $\{e, x, y, z\}$ 是否是群 A_4 的一个子群而非仅仅只是子集。由于群 A_4 已经被我们用作过很多次例子了，所以验证 $\{e, x, y, z\}$ 是正规的只需回顾一下图 7.23 就知道了。总而言之，将共轭类组合到一起并不总是能得到子群；这种方法的真正威力在于缩小我们对于正规子群的搜索范围，减少不必要实验与验证。

因此，当我们寻找正规子群时，类方程提供了一种有效的“缩小包围圈”的手段。我们不必对所有的子群尝试用商过程 (quotient process) 去检验它的正规性而仅仅只需检查一小部分的子群 (在上面的例子中，只需去检查一个即可)。尽管共轭与正规子群的这种紧密联系十分有用，但这并不是我们能从共轭这个概念中获得的唯一价值。本节配套习题 7.6.5 给出了共轭的几个其他的应用之处，这些应用也将在本书余下的章节中再次出现。

8

同态映射的力量

在这本书中，我已经多次使用过类似“这个群与那个群有着相同的结构”或者“在那个群里存在一个这个群的拷贝版”这样的说法。在第一次使用这样的表述时 (关于图 2.7 与 2.8 的等价性)，我仔细解释了这两种结构之所以等价的原因。但那之后，当再提到两个结构是一样的时，我都没有啰嗦其中的细节原因，而是相信读者有能力看出其中的结构模式究竟是如何相互匹配的。本章的目的正是为此，即创造一种能够精确描述两个结构之间关系的语言并加以研究。这将极大地推进我们对于群论的研究。

为了描述两个有着一样结构的群，在第三章时，我提到一个术语“同构 (isomorphic)”，但是那时并没有给出一个正式的定义。还有与之相关的一个词“同态 (homomorphism)”，也是用来描述两个群之间的关系的术语。词根“homo”和“morph”源出希腊语，意指“相同的形状 (same shape)。同构 (isomorphism) 是一种特殊的同态，它们两个都将在本章被加以研究。8.1 节通过之前我们已经深究过的两个主题引入了同态的概念。余下的章节则带领我们领略群论中四个非常重要的观点，用同态的语言能帮助我们更好的描述、理解并可视化这四个主题。

8.1　嵌入与商映射

同态就隐藏在我们已经研究过的两个重要内容里，现在是时候将这一概念大白于众，并且我们还要进一步看看能从这一概念中学到些什么。其一，当一个群是另一个群的子群时，其中就有同态的踪迹；其二，当我们做商运算时也有同态隐匿于其中。

我们先来看第一种情况。考虑 $C_3 < S_3$，这是我们第一次在图 6.3 的左图中遇见的。图 6.3 的高亮部分显示在群 S_3 中包含一个三阶循环子群，该子群在结构上且仅在结构

上与 C_3 一模一样，也就是说，C_3 的诸元素 $(0, 1, 2)$ 其实并不真正是群 S_3 中的元素。而当我们说“C_3 是 S_3 的一个子群”时，真正想表达的意思则是“C_3 的结构出现在了群 S_3 中，即使元素并不真的是 0，1 或 2”。

在第六章时，我便期望读者能够辨认出图 6.3 中的这种结构之间的关联——也的确是很明显的联系。既然我们本章的主题就是来研究这样的联系，所以我们首先就把上述的例子来进行精确描述。图 8.1 将 C_3 和 S_3 的凯莱图并排展现了出来，这将给我们以下，关于 C_3 与 S_3 中轨道 $< r >$ 之间的结构性联系的阐释，带来帮助。

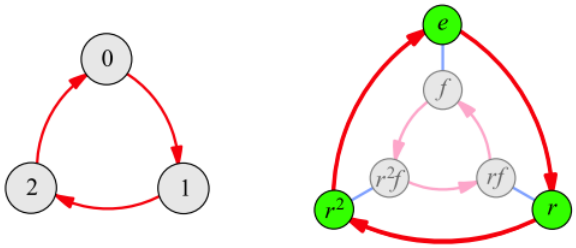


Figure 8.1. The diagrams for C_3 and S_3 side-by-side, to make it clear that the highlighted pattern in S_3 is the pattern of C_3, and to make it possible to describe the element-by-element correspondence

观察图 8.1，元素 $0 \in C_3$ 与元素 $e \in S_3$ 对应，倘若我们在两张图中都沿着红色箭头顺时针方向前进，元素间类似的对应性质仍得以保持。具体来说，当沿着红色箭头走一个步长时，在 C_3 中到达的节点 1 与在 S_3 中走一个步长到达的节点 r 相对应；继续走下去，就使得 $2 \in C_3$ 与 $r^2 \in S_3$ 对应，然后同时回到各自的出发点。因此，在 C_3 中进行的这种 3-步长的遍历便与遍历 S_3 中元素 r 所在的轨道（也是 3-步长）相对应。

像上面这样的解释，就已经能很精确地描述“C_3 为 S_3 的一个子群”这句话的内在意思；但实在是太啰嗦了！仅仅为了精确描述一个简单的、显而易见的对应关系，却要搞成长篇大论，这不是数学家们想要的。同态正是这样一种可以简洁而精确地描述对象之间结构上的联系的数学工具。我们上面那一段冗长的解释如果用同态的语言来表述就如图 8.2 所示。图中虚线箭头连接了 C_3 与 S_3 中相互对应的元素，这也可以从右边的图例看出。比如图例中 $0 \to e$ 表示 $0 \in C_3$ 与 $e \in S_3$ 对应，其它的同理。

因为同态描述了两个群中元素的对应方式，所以你可以把它们当成一种“函数 (function)”。在数学里，我们经常画函数的图像，并且研究各种各样的函数。函数是一种对应法则，它把一个独立变量 (自变量)x 的值唯一对应到另一个变量 (因变量)y 的值上去；通常我们认为这里的 x 与 y 均为数 (numbers)，当然广义上来说，却也不必拘泥于此。比如在群论里的函数，就不是关于数的。图 8.2 即展示了一个从群 C_3(一个元素是数字的群) 对应到群 S_3(其中的元素并非数字) 的函数。我们称，这个函数将 C_3 中的元素映射 (map) 到 S_3 中的元素。

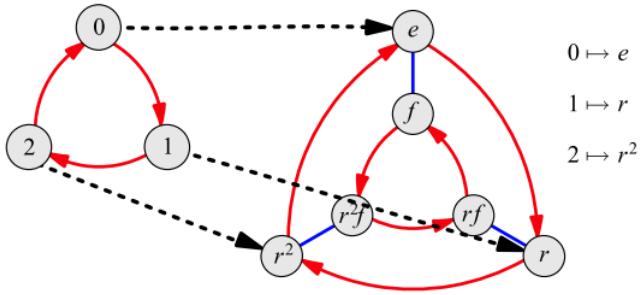


Figure 8.2. A diagram that spells out the correspondence between C_3 and the $\langle r \rangle$ orbit in S_3 by showing which element from S_3 corresponds to each element in C_3. The correspondence is shown using dashed lines and described using the legend on the right.

按照习惯，我们通常用希腊字母来表示群之间的映射，所以我就用 ϕ 来表示图 8.2 中的映射。更进一步，我可以使用数学符号 $\phi : C_3 \to S_3$ 来表述 ϕ 将 C_3 映射到 S_3. 正如通常标准的函数记号 $f(2)$ 表示 2 在 f 的对应之下的得到的结果，在群论中我们记作 $\phi(2)$. 以图 8.2 为例，$\phi(2) = r^2$. 同样地，正如我们用类似 $f(x) = x^2 + 1$ 这样的符号来定义一个函数，我们可以用 $\phi(n) = r^n$ 这个的表达式来简明地定义图 8.2 中的映射；这一定义对任意 $n \in C_3$ 都成立 (如果我们记 $r^0 = e$)，而且这个表达式也突出了 C_3 与 S_3 中元素 r 所在轨道之间的联系。

函数开始出发的那个群我们称为定义域 (domain)，比如 C_3；函数映射进的那个群我们称为值域 (codomain)，比如 S_3。值域中被函数箭头打到的元素称为该函数的像 (image)。符号 $Im(\phi)$ 表示同态 ϕ 的像。

在前面，我对于同态 ϕ 的描述，给出了一个很清晰的事实，ϕ 在它的值域 S_3 中仿制了一个定义域 C_3 的结构。群论很大程度上只关注这种具有“保持结构”性质的函数或者说映射。正式定义如下：

定义 8.1 (同态映射). 一个同态是两个群之间的映射，它在值域中复制了其定义域的结构模式。以下两个说法是等价的，它们都表达了上述的“保持结构”的意思，并且我用图 8.3 展示了这两种说法。

1. 用凯莱图的方式来说：如果定义域中的一个箭头 b 从节点 a 出发，指向了节点 c，那么值域中的 $\phi(b)$ 箭头必须从节点 $\phi(a)$ 出发指向节点 $\phi(c)$.
2. 用乘法表的方式来说：如果在定义域乘法表中成立关系式 $a \cdot b = c$，那么在值域乘法表中必须成立关系式 $\phi(a) * \phi(b) = \phi(c)$. 其中“$\cdot$”为定义域乘法表中的乘法运算规则，“$*$”为值域乘法表中的乘法运算规则。

上述两种说法须对定义域中的任意 a, b, c 元素均成立。好了，现在仔细想想，为什么以上两种定义都意指“保持结构”，或者说“在值域中复制了其定义域的结构模式”

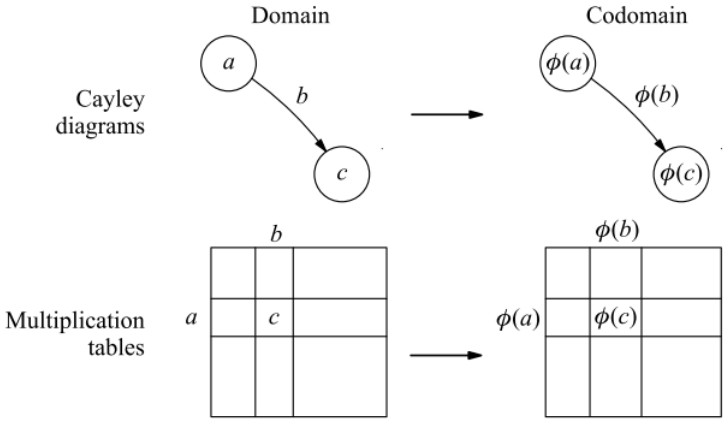


Figure 8.3. The criteria in Definition 8.1 illustrated. On the top left is a portion of the domain Cayley diagram, in which b connects a to c. Therefore somewhere in the codomain Cayley diagram, $\phi(b)$ connects $\phi(a)$ to $\phi(c)$ (top right). On the bottom left, the domain multiplication table includes $a \cdot b = c$, so the codomain multiplication table must include $\phi(a) \cdot \phi(b) = \phi(c)$ (bottom right).

这个意思呢？

另一个例子能帮助我们更好的理解这个定义。回忆一下，我们知道 C_3 也是 C_6 的一个子群，如图 6.4 中的右图和 6.5 所示。我们可以用 C_3 到 C_6 的同态映射 $\theta(n) = 2n$ 来表达 $C_3 < C_6$，如图 8.4 所示。以下几段的篇幅，都将以这个同态 θ 为例，来指出一般情况下关于同态映射的一些重要事实。

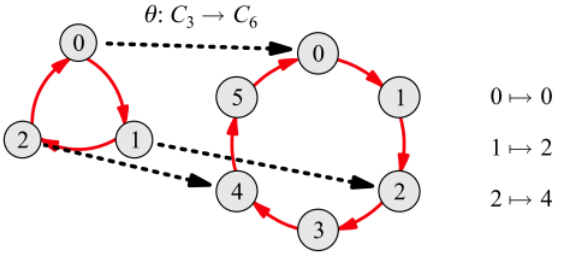


Figure 8.4. A diagram that spells out the correspondence between C_3 and the $\langle 2 \rangle$ orbit in C_6 by showing which element from C_6 corresponds to each element in C_3.

正如 θ 将 C_3 中的节点 1 映到 C_6 中的节点 2，它也将 C_3 中的箭头 1 映到 C_6 中的一个长为 2 的路径——即相应的 C_6 中路径 $\theta(1)$。箭头 1 串起了 C_3 中的轨道 $\{0, 1, 2\}$，而 $\theta(1)$ 则串起了在 C_6 中与之对应的轨道 $\{\theta(0), \theta(1), \theta(2)\}$，即轨道 $\{0, 1, 2\}$。因此一个同态映射并不仅仅将定义域凯莱图中的节点映射到值域凯莱图中的节点，同时也将定义域凯莱图中的路径 (path) 映射到了值域凯莱图中的路径。定义 8.1 中的第二种表述就是要求在定义域中从节点 a 到节点 b 的路径要对应到值域中从节点 (a) 到节点 (b) 的路径。在图 8.4 中，群 C_6 的凯莱图并没有明显包含一条代表 $\theta(1)$ 的箭头；但我们可以将箭头 $\theta(1)$ 视为两个相继的红色箭头的合成。因此，同态 θ 将节点与箭头同时“扩大了两倍”。我

们把 C_6 中相继的两个红色箭头合成并视为一个箭头，则这个合成的箭头连接的节点跳过了 C_6 中奇数标号的节点，在此视角下，我们就在群 C_6 中找出了群 C_3 的结构。

所以，当我们用凯莱图来可视化群的同态映射时，我们就可以从两个层面来看待同态：一是将节点映到节点，另一则是将路径映到路径。更进一步，如果我们已知一个同态是如何将定义域中的路径映到值域中的路径，这事实上也就告诉了我们该同态映射是如何将定义域中的节点与值域中的节点对应起来的。原因就在于，凯莱图中的箭头表示的是相应的群的生成元（(generators)。就像这些生成元生成了群一样，它们被对应到的结果，实际上也生成了这个同态映射。举个例子，设有另一个不同于图 8.4 中 的同态 $\theta' : C_3 \to C_6$，假定我们只知道 $\theta'(1) = 4$，那么其实这已经足够确定余下的对应方式了。

我们使用定义 8.1 中的 (2)，比如因为在 C_3 中成立 $1 + 1 = 2$，我们在 C_6 中就必须有 $\theta'(1) + \theta'(1) = \theta'(2)$ 成立，因此我们就确定出了 $\theta'(2)$

$$\theta'(2) = \theta'(1) = \theta'(1) = 4 + 4 = 2$$

同理，从 C_3 中的等式 $1 + 2 = 0$ 我们就能确定 $\theta'(0)$ 一定等于 0. 所以关于 θ' 的所有信息就由 $\theta'(1) = 4$ 这一已知事实生成了。你可以自己试着动手画一下 θ' 的图示，并将其与图 8.4 作比较。

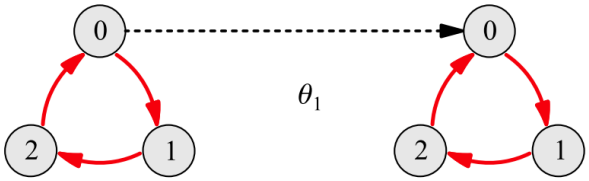
类似的步骤可以用来生成任何一个群同态 $\phi : G \to H$，当然我们得知道群的生成元以及生成元的像。比如已知 $G =< a, b >, \phi(a)\phi(b)$ 的值。具体来说，我们可以按如下方式来确定任意元素 $g \in G$ 对应的值 $\phi(g)$.

因为 a, b 是群 G 的生成元，所以任意元素 g 都可以表示为 a, b 的一些乘积组合，假设 $g = a \cdot b \cdot a \cdot a \cdot b$，多次使用定义 8.1 的 (2), 我们得到

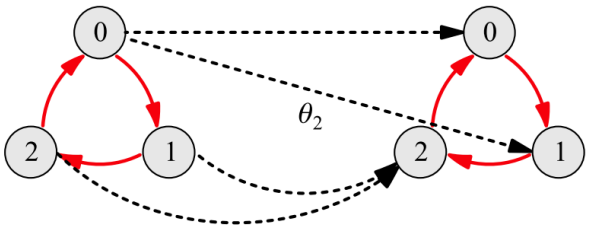
$$\phi(g) = \phi(a) \cdot \phi(b) \cdot \phi(a) \cdot \phi(a) \cdot \phi(b)$$

因为我们已经知道 $\phi(a)$ 与 $\phi(b)$ 的值，所以就可以按照群 H 中的乘法运算计算出 $\phi(g)$ 的值。按这样的方式我们就知道，一个同态映射可以由群的生成元在此同态下的像完全确定。我们举的例子中，群 G 只有两个生成元，这是无关紧要的，对于更多生成元的情况，做类似的推导即可。习题 8.7 要求你解释为何这也表明同态必须将定义域中的恒等式映射为值域中的恒等式。以后我将不加证明的使用这一事实。

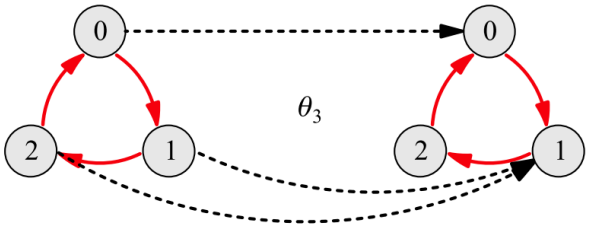
为了更好的理解定义 8.1，我们再来看一些不是同态映射的例子，建议读者将这些例子与我们此前看到的同态的例子做对比，这将会有很大裨益。图 8.5 展示了四个不是同态映射的例子，因为它们不符合定义 8.1. 其中两个由于连映射（或者说函数）都算不上，所以不是同态；另外两个则是由于不具有“保持结构”的性质，因此也不是同态。花点时间仔细想想图 8.5 中的例子。



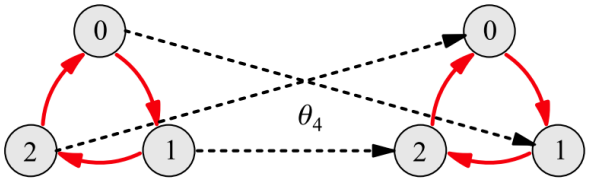
A function maps *each* element of the domain to some element of the codomain. But θ_1 ignores two elements of the domain, and thus is not a function.



A function maps each element of the domain to *one* element of the codomain. But θ_2 maps 0 to two different elements of the domain, and thus is not a function.



Although θ_3 is a function, it is not a homomorphism. In the domain, $1 + 1 = 2$, but in the codomain, $\theta_3(1) + \theta_3(1) \neq \theta_3(2)$.



Although θ_4 is a function, it is not a homomorphism. Although the image is a 3-cycle like the domain, θ_4 does not map the domain identity element to the codomain identity element. For example, $\theta_4(0) + \theta_4(1) \neq \theta_4(1)$.

Figure 8.5. Four example maps that are not homomorphisms, with the corresponding reasons. For simplicity, I kept the domain and codomain C_3 the same in each case, but similar examples could be created for many domains and codomains.

尽管我认为用凯莱图来可视化群的同态映射是最方便的，我们也要来看看一些别的可视化方法，比如用乘法表或者循环图 (circle graph)。举个例子，图 8.6 展示的同态使用的是乘法表的技术，它们与图 8.2 和图 8.4 中所展示的同态完全一样；而图 8.7 则是用循环图的技术展示的这两种同态

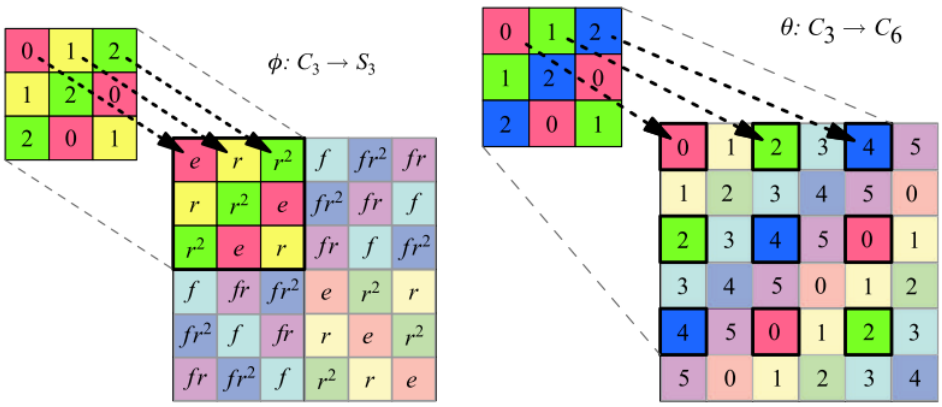


Figure 8.6. Multiplication tables representing the same homomorphisms from Figures 8.2 and 8.4.

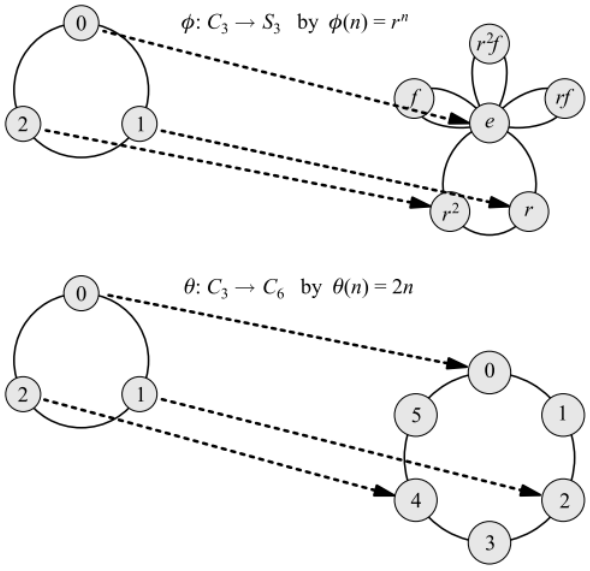


Figure 8.7. Cycle graphs representing the same homomorphisms from Figures 8.2 and 8.4. The homomorphism θ does not look much different than in Figure 8.4 because the cycle graphs of cyclic groups are almost the same as their Cayley diagrams.

8.1.1　嵌入映射

8.1 节开头我曾提到在此之前我们就已经在两种场合见过同态。第一种就是同态帮助我们具体了解究竟一个群是如何成为另一个群的子群的原理，也就是上面刚刚举的例子。我们把这样一种同态映射称为“嵌入映射 (embedding)”，名字很形象，因为它展示的正是如何把一个群“镶嵌”到另一个群中。

因为每一个嵌入映射的功能都是在值域中拷贝了一个定义域的结构，所以它的像与其定义域的大小一样。正如此，嵌入映射有一个很有趣的性质，它不会把定义域中两个不同的元素映到值域中的同一个值上（译注：即嵌入映射是单的同态映射）；不然的话，像的大小 (size) 一定比定义域来得小，这就不是“拷贝 (copy)”了！这一性质在具体的图中来看的话，很容易验证。

如果一个嵌入映射还是满射的话，则表明它的定义域和值域具有完全相同的结构模式。在这种情况下，它就不仅仅只是一个同态映射了，而是一个同构映射 (isomorphism)。图 8.8 展示了一个简单的例子。我们称两个群是同构的 (isomorphic)，如果在它们之间存在一个同构映射。这是“同构 (isomrphic)”这个词的正式定义，此前从第三章开始我一直都在非正式地使用这个词。两个同构的群，它们的元素、凯莱图与乘法表也许看起来长得完全不一样，但是这些只是表面上的不同。起名字的方式、凯莱图和乘法表排布方式所带来的这些表面差异无法掩盖它们内在的本质结构是完全一样的，这一点正是由同构映射所确保。当群 G 与群 H 同构时，我们记作“$G \cong H$”，读作“G 同构于 H”。

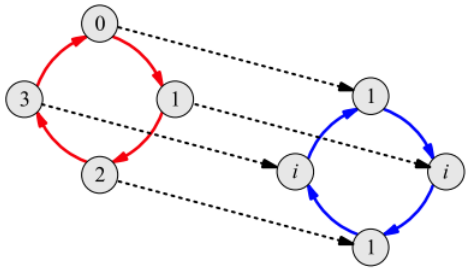


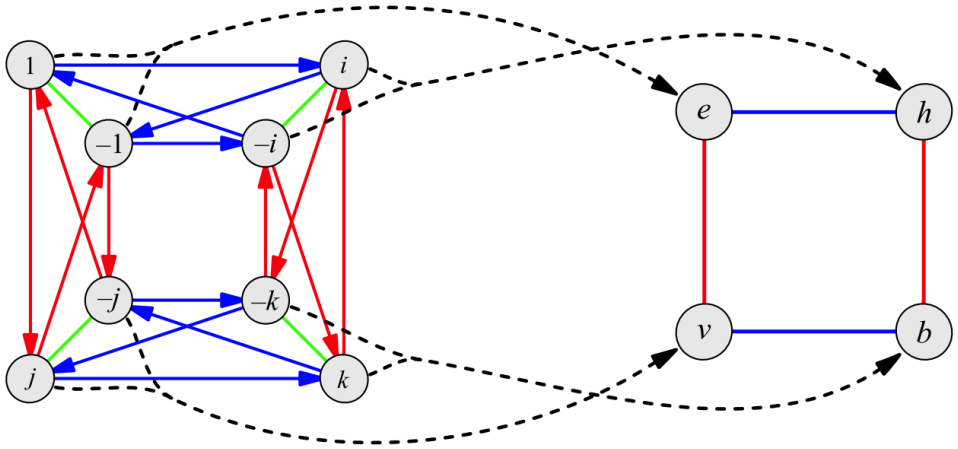
Figure 8.8. The domain of this isomorphism is C_4, and the codomain is a group of complex numbers $\{1, -1, i, -i\}$ under the operation of multiplication. The isomorphism points out that despite their different elements and operations, these groups have the same structure.

8.1.2　商映射

图 8.9 展示了两个非嵌入映射的同态映射的例子。它们满足定义 8.1 的所有要求，因此确实是同态映射；但是它们把定义域中不同的元素映到了同一个值域中的元素上，因此不是嵌入映射。如此一来，它们的像就是其定义域的一个缩小的简化版。图 8.9 中

的凯莱图显得有些交错复杂，花点时间仔细研究一下。你应该去验证它们满足定义 8.1，并试着找出它们的共同之处。

$$\tau_1 : Q_4 \to V_4$$



$$\tau_2 : C_{10} \to C_6 \text{ by } \tau_2(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases}$$

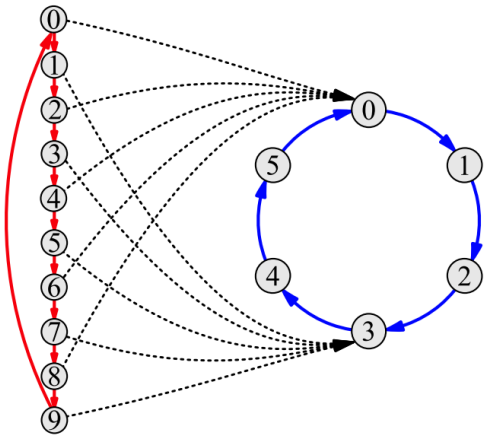


Figure 8.9. Two example homomorphisms that do not have the defining characteristic of embeddings. Each of these homomorphisms maps more than one domain element to the same codomain element.

有几个有用的事实值得注意，这些事实实际上并非为上述两个例子所独有，而是所有非嵌入映射的同态映射所具有的共同特征。我在下面以观察的形式给出这些事实，并给出相应的推导证明。当你一边读着观察 8.2 到 8.4 时，你应该用图 8.9 中展示的那两个例子来验证看看。这可以帮助你获得一些关于这些观察及其证明背后的具体直觉。

观察 8.2. 定义域中凡是被映射到同一个值的元素所组成的集合在定义域中都有着相同的结构。

换句话说，每一个非嵌入的同态映射都依循着一个不断重复的模式结构。举个例子，在图 8.9 所示的同态映射 τ_1 中，值域里的每一个元素都被来自定义域中一个类似 C_2 的拷贝版所映到，也就是 (-1) 箭头（即绿色箭头）连接的那些个元素。而在同态映射 τ_2 中，值域中的元素 0 和 3 都各自被定义域中的五个由红色双箭头连接成环状的元素所映到。下面就让我们来证明观察 8.2 对于任意一个非嵌入的同态映射都成立。

证明. 设 ϕ 是一个同态映射，在它的像中任取两个元素 a 和 b，再设定义域的某个子集 A 满足 $\phi(A) = \{a\}$，某个子集 B 满足 $\phi(B) = \{b\}$。我将解释为什么 A 与 B 必然有相同的结构。也许用一个具体例子来可视化以下的论证会更好地帮助我们理解。比如我们把 ϕ 取作图 8.9 中的 τ_2，并相应的把 a 取作 0，b 取作 3，因此相应的就有，$A = \{0, 2, 4, 6, 8\}$，$B = \{1, 3, 5, 7, 9\}$。

A 与 B 的结构由其中的路径所组成。分别在 A 与 B 中取两个起始点 a_1 和 b_1，如图 8.10 所示。我将解释为什么在 A 中，任意一条从点 a_1 出发到达 A 中另一点的路径，也将在 B 中从点 b_1 出发到达 B 中某一点。

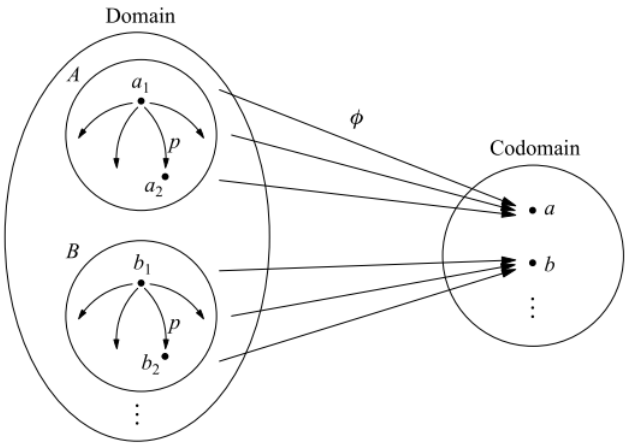


Figure 8.10. A non-embedding homomorphism ϕ and the sets of elements A and B that it maps to the elements a and b. This illustrates the reasoning following Observation 8.2.

设 p 是 A 中一条从节点 a_1 到 A 中另一个节点 a_2 的路径，定义 8.1 的第一条告诉我们 $\phi(p)$ 是一条从节点 $\phi(a_1)$ 到节点 $\phi(a_2)$ 的路径。注意到 $\phi(a_1) = \phi(a_2) = a$，因此 $\phi(p)$ 是一条从节点 a 到节点 a 的路径，这是一条长度为 0 的路径 (或者你也可以把它看成是一条绕了一圈又回到起点的路径)。倘若我们让 p 从点 b_1 出发，它会终止在哪呢？假设这时候的终点为 b_2，我们面临一个很重要的问题，是否 $b_2 \in B$? 注意到此时 $\phi(p)$ 也是一

条从节点 $\phi(b_1)$ 到节点 $\phi(b_2)$ 的路径，而在上面我们已经知道路径 $\phi(p)$ 具有这样的性质**绕一圈回到起点**，这就导致 $\phi(b_1) = \phi(b_2) = b$，于是 $b_2 \in B$.

这表明 A 中任意一条从点 a_1 出发的路径都与 B 中一条从点 b_1 出发的路径相对应；同理，B 中任意一条从点 b_1 出发的路径都与 A 中一条从点 a_1 出发的路径相对应。因此，A 与 B 有着完全相同的结构。再由 A 与 B 的任意性即知，所有这样的集合都有着相同的结构，从而观察 8.2 对于任一个非嵌入映射都成立。 □

正如图 8.10 所示，这就带来了对定义域的一种等价划分——划分为都具有相同结构的小部分。这让我们想起了当初在第六章中用子群的陪集来划分群的场景，事实上，这里的划分也是同样的原理。

观察 8.3. *在观察 8.2 中描述的那些集合事实上就是定义域的一个子群以及它的各个左陪集。*

从第六章我们知道，一个子群的所有左陪集都和该子群享有相同的结构，并且它们等价划分了一个群。因此如果在观察 8.2 中所说的那些集合中有一个是子群，那么其它的集合必是它的左陪集。而能够成为子群的集合必须要包含有单位元，因此观察 8.2 所述的那些集合中只有包含了定义域中单位元的那个集合才有可能是定义域的子群，更进一步，它也必定是那个将其元素都映到值域中单位元的集合。下面我将解释这一点并以此说明观察 8.3 的正确性。

我们使用定理 7.7 证明中的那种论证方法来推导。设 C 表示定义域中那些被映射到值域中单位元的元素所组成的集合。我将说明由集合 C 生成的子群恰好就是 C 自身。显然，由 C 生成的子群必然至少包含 C 本身，所以我们只要说明除此以外再没有别的元素生成了。任取 C 中两个元素 a 和 b，它们的乘积 ab 也一定在 C 中的吗？

因为元素 ab 表示从节点 a 出发的 b 箭头所到达的节点，因此元素 $\phi(ab)$ 表示从节点 $\phi(a)$ 出发的 $\phi(b)$ 箭头所到达的节点。但是注意到 b 在集合 C 中，所以在映射 ϕ 之下，b 被映到了值域中的单位元，故 $\phi(ab) = \phi(a)$，同样由于 a 在集合 C 中，所以 $\phi(a)$ 等于值域中的单位元，因此 ab 也被 ϕ 映到了值域中的单位元，这表明 ab 也在 C 中。

所以由集合 C 生成的子群恰好就是 C 自身，这就是说定义域中那些被映到值域中单位元的元素组成的集合 C 形成了定义域的一个子群，同时它的每一个左陪集都被映射到值域中一个互不相同的单点集。这个子群 C 我们称为同态映射 ϕ 的**核**，记作 $Ker(\phi)$.

观察 8.4. *在观察 8.3 中提到的那些左陪集同时也是右陪集，因此，上述的子群 C 是一个正规子群。*

在第七章中我们已经知道所谓正规子群，是指其诸陪集之间不存在有歧义的连接箭

头的子群，如图 7.27 所示。倘若 $Ker(\phi) = C$ 不是正规的，不妨设箭头 g 同时连接了 $Ker(\phi)$ 和 $gKer(\phi)$，$kKer(\phi)$，如图 8.11 所示，那么根据定义 8.1 的第一个要求，就有箭头 $\phi(g)$ 要在值域中连接着节点 $\phi(e)$ 与节点 $\phi(g)$，节点 $\phi(k)$，这与值域是一个群相矛盾(群的定义)！因此，核 $Ker(\phi)$ 是一个正规子群。

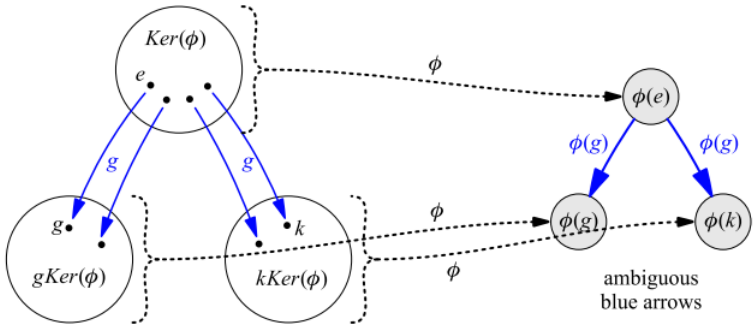


Figure 8.11. The pattern depicted here never happens because the ambiguity of blue arrows in the codomain is impossible; the codomain is a group.

把观察 8.2 到观察 8.4 放到一起，我们可以发现图 8.9 中所示的同态映射在功能上与定义 7.5 中的商过程似乎很像。商过程把一个正规子群的各个陪集缩并为一个个的节点；另一方面，使用同态映射将它的核的各个陪集映射为值域中的一个个节点也能达到同样的效果。举个例子，在图 8.9 中的同态映射 τ_1 把 Q_4 中的每一个 C_2 拷贝版浓缩为 V_4 中的每一个节点；这跟用子群 $< -1 >$——同构于 C_2，来商掉 Q_4 的效果是一样的！图 8.12 就展示了这一商过程。

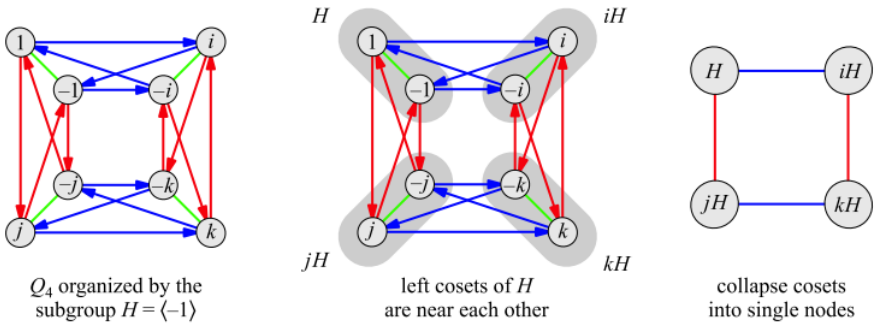


Figure 8.12. The quotient of Q_4 by C_2 corresponding to the homomorphism τ_1 in Figure 8.9. It follows the quotient procedure from Chapter 7, as depicted in Figure 7.20 (and others).

同态映射与商过程的这种关系将是下一节 8.2 的主题，在 8.2 节的开头，我们用一个著名的定理来正式叙述这一联系。由于这种关系，我把非嵌入的同态映射称为“商映射 (quotient maps)”。这是有关同态映射的最为关键的事实之一：同态映射只有两种，一是嵌入映射，一是商映射。嵌入映射的特点是绝不会把定义域中的两个不同的元素映成

值域中的同一个元素，而商映射的特点是它跟商过程实现的效果一样。所以在这一节中，我们学习了嵌入映射与商映射这两种同态映射，也是仅有的两种同态映射。

8.2　群同态基本定理

接下来的这个定理可以说是大名鼎鼎，当然也确实名副其实。它总结了我们此前关于同态映射的一些观察与探索。首先，我将简单地叙述定理内容，然后讨论它的意义并给出证明。

定理 8.5 (群同态基本定理)**.** 若 $\phi : G \to H$，则 $Im(\phi) \cong \frac{G}{Ker(\phi)}$.

在我们给出此定理的证明之前，先来看看它的一些简单的含义。首先考虑嵌入映射，由于嵌入映射 ϕ 是单射，因此它的核就是平凡子群 $\{e\}$，此时定理 8.5 告诉我们 $Im(\phi)$ 同构于 $\frac{G}{\{e\}}$，也即同构于 G 本身。所以定理 8.5 表明，嵌入映射确实名副其实，因为它们的像恰好是定义域的一个拷贝！

当 ϕ 不是嵌入映射时，那它一定把定义域中的某两个元素映到了值域中同一个元素上。事实上，由于商映射而带来的重复性模式的出现，每一个 $Ker(\phi)$ 的陪集都至少有两个元素。因此，商过程 $\frac{G}{Ker(\phi)}$ 把一些元素“粘”起来，从而得到一个更小的群 (而不像 $\frac{G}{\{e\}}$ 那样)。所以，定理 8.5 告诉我们商映射，名副其实，因为它们所做的并非是平凡的商过程。实际上，在证明了此定理之后，我们将使用这个定理来看看商过程与商映射究竟有着怎样的联系。

证明. 对于任意的同态映射 $\phi : G \to H$, 通过观察 8.2 到 8.4，我们知道 $Ker(\phi) \lhd G$，因此我们确实可以做商运算 $\frac{G}{Ker(\phi)}$ 并获得一个新的群。现在，我必须得解释为什么那样得到的群同构于 $Im(\phi)$，后者是 H 的一个子群。我们已经学过如何计算像 $\frac{G}{Ker(\phi)}$ 这样的商，只要把 G 中 $Ker(\phi)$ 的各个陪集分别缩并成一个个点。另一方面，观察 8.2 到 8.4 则展示了用同态映射来缩并 $Ker(\phi)$ 的各个陪集的过程：即每一个映射到 $Im(\phi)$ 中的一个节点。

现在的问题是，ϕ 是否也像用 $Ker(\phi)$ 来做商过程那样给箭头做缩并？让我们回忆一下做商运算的时候陪集之间的箭头是怎样变化的。假设群 G 中的**一族**箭头 b 从陪集 $aKer(\phi)$ 出发指向陪集 $cKer(\phi)$，则当商过程把每个陪集缩并成节点时，这族箭头 b 也会被拧在一起，形成在商群中的**一根**连接着节点 $aKer(\phi)$ 与节点 $cKer(\phi)$ 的箭头。也就是说，商过程变化前后的箭头连接方式要保持一致，并把多根箭头拧成一根就行了。这与同态映射干的活非常类似！定义 8.1 的第一条要求是说，只要在群 G 中有一个连接节点 a 与节点 c 的箭头 b，那么在 H 中也必须得有 $\phi(b)$ 是连接节点 $\phi(a)$ 与 $\phi(c)$ 的箭头。更进一步，因为 H 是一个群，则在它的两个节点之间不可能出现多于一根的连接箭头。

因此，任意一个同态映射 ϕ 都是同时把陪集与箭头进行缩并，就像用 $Ker(\phi)$ 来做商运算那样，因此用这两种方法得到群有着完全一样的结构。

如果 $\frac{G}{Ker(\phi)}$ 与 $Im(\phi)$ 有着相同的结构，那么它俩之间就只是元素名字不同而已。换句话说，你应该能给 $Ker(\phi)$ 的各个陪集与 $Im(\phi)$ 各个元素之间找到一个合适“名字转换器”——同构映射。图 8.13 把这种关系画了出来，并把这个同构映射用 $i:\frac{G}{Ker(\phi)}\to Im(\phi)$ 表示了出来。一个具体的例子是考虑群 A_4，把这些关系反应在 A_4 上就是图 8.14. 其中同态映射 $\phi: A_4\to C_3$ 与用 $Ker(\phi)$ 商掉 A_4 的商过程 q 实现的效果相同，它们之间的“名字转换器”即同构映射 i.

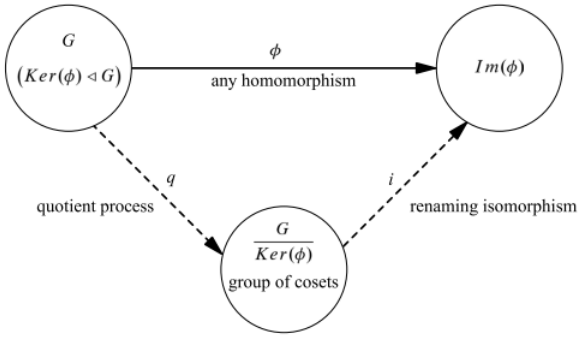


Figure 8.13. The Fundamental Homomorphism Theorem (Theorem 8.5) illustrated

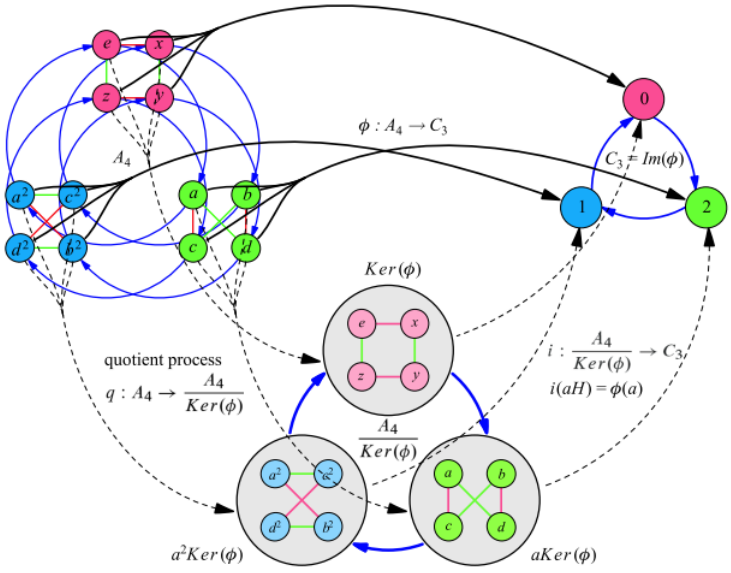


Figure 8.14. The Fundamental Homomorphism Theorem (Theorem 8.5) exemplified using the group A_4 and the quotient map ϕ whose kernel is the subgroup $\{e, x, y, z\}$ of A_4

但是 i 的表达式究竟是什么呢？如图 8.14 所示，i 必须将 $\frac{G}{Ker(\phi)}$ 中的一个陪集映到该陪集里的元素被 ϕ 所映射到的那个元素。还有一点别忘了，我们自然希望 q 与 i 的复合能够等价于 ϕ. 因此，这个同构映射 i 应当把任意一个陪集 $gKer(\phi)$ 映到 H 中的元素

$\phi(g)$，这里并不存在歧义，或者说 i 是良定的 (well-defined)，因为不管你选择用哪个元素来代表这个陪集，ϕ 都将它们映到 H 中同一个节点上。因此，同构映射 i 便使 $\frac{G}{Ker(\phi)}$ 同构于 $Im(\phi)$. □

我们可以把定理 8.5 解释为：任意一个同态映射都能够用一个商过程搭配一个合适的“名字转换器”同态映射来实现。你也许也发现了，在这些图中，商过程本身就是一个同态映射。它是从一个群到一个商群的映射，并且保持群的运算。正因此，在图 8.13 与图 8.14 中的商过程都用 q 表示并且展示的也跟图中其他同态映射无异。事实上，“商映射”这个词语有点被滥用了。之前我用它指代那些非嵌入的同态映射，它们表现得跟商过程十分类似，就像图 8.9 中的 τ_1，表现得跟图 8.12 中的商过程一样。因为商过程本身便是一个同态映射，因此，我们把它也叫做商映射。

现在，我们使用同态映射来研究群论就有了坚实的基础。在本章剩余的内容中，我们将探索同态映射与定理 8.5 的一些具体应用。当然，用处很多，我只挑选了最为重要且十分有名的其中四个应用，每一个话题对应本章 8.3 到 8.6 的一个小节。

8.3　模的算术

在 5.1.2 节中，我们了解到群 C_n 中的二元运算是 mod n 剩余类加法。当时我是通过将 C_{12} 与时钟类比来介绍这个概念的。时钟和 C_{12} 凯莱图的数字标号几乎完全相同，除了时钟上数字 12 的位置，在凯莱图中是用 0 来代替。这一点就引出了一个用来思考群 C_{12} 的非常有用的方法。具体来说就是，我们可以把 C_{12} 看作是整数群 Z“粘合了 12 与 0”得到的群。定理 8.5 可以帮助我们做到这一点。

我们从 Z 的一个凯莱图开始 (使用 1 作为生成元)，如图 8.15 所示。前面关于定理 8.5 的讨论告诉我们, 将 Z 用一个包含 12 的正规子群作商，对应于一个将 12 映成 0 的同态映射。这都代表了应该把 0 和 12 视为相同的这一想法。让我们来做这个商运算。

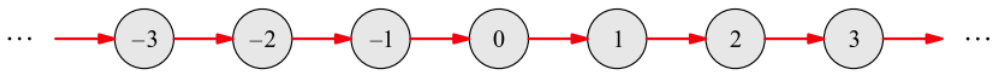


Figure 8.15. The infinite cyclic group $\mathbb{Z}$ of integers

为了避免一下粘合了太多的元素，让我们使用包含 12 的最小的子群来做这个运算。显然，在 Z 中包含 12 的最小子群当然是 $< 12 >$，其中的元素恰好都是 12 的倍数。

$$< 12 >= \{..., -36, -24, -12, 0, 12, 24, 36, ...\}$$

由于 Z 是交换群，它的所有子群 (当然也包括这个子群) 都是正规子群，因此我们的确可以进行 $\frac{Z}{<12>}$ 这个运算。下面我将使用第七章中的商过程来具体展示。

首先，我必须把 Z 的凯莱图重新组织成 $< 12 >$ 及其陪集的形状。要做到这一点，我们必须知道那些陪集究竟是什么样子。因为 Z 是一个群，其上的二元运算是加法 (注：Abel 群通常又称为加群，它上面的运算通常叫加法)。我们将用符号 $k+ < 12 >$(而不是 $k < 12 >$) 来表示 $< 12 >$ 的陪集。图 8.16 展示了一些陪集的例子；正如我们预计的那样，它们的确与 $< 12 >$ 有完全相同的结构。陪集 $1+ < 12 >$ 包含了所有 12 的倍数加一的数字，即当这些数字除以 12 时，余数都为 1。陪集 $2+ < 12 >$ 则包含了所有除以 12 余 2 的数字，以此类推。

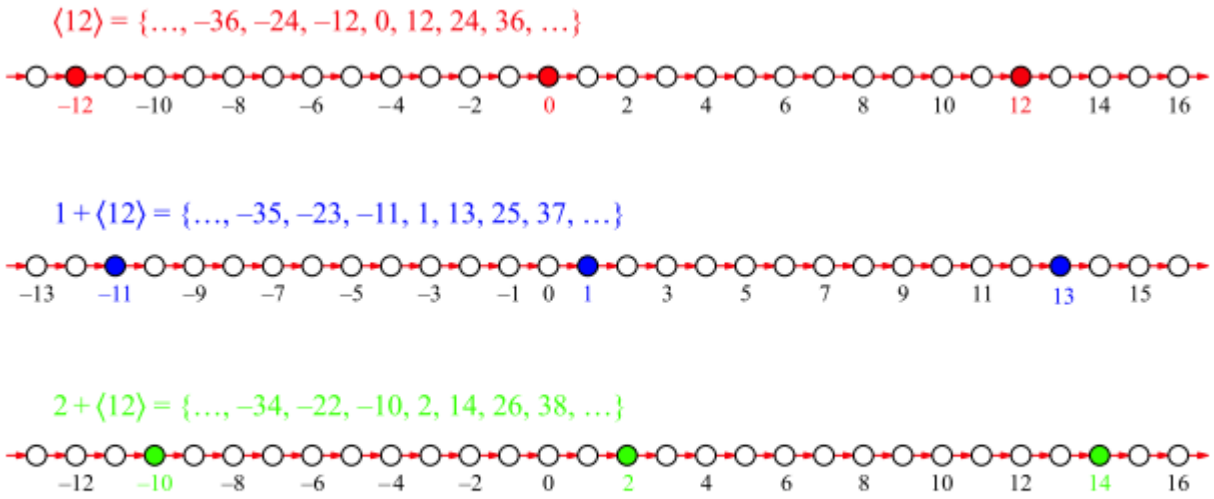


Figure 8.16. Segments of $\mathbb{Z}$ with a few cosets of $\langle 12 \rangle$ highlighted. Other cosets follow the pattern suggested here.

这些陪集被称为 mod 12 的同余类 (或剩余类)。我们称两个元素是 mod 12 同余的，如果它们在同一个同余类中——此时它们被 12 除的余数都相同。当 a 与 $b$mod 12 同余时，记作 $a \equiv_{12} b$. 因此下面的几个说法都是对的：

$$6 \equiv_{12} 18 \qquad 1 \equiv_{12} 25 \qquad 12 \equiv_{12} 1200 \equiv_{12} 0$$

由这些陪集重新组织的 Z 呈无限螺旋的形状，如图 8.17 所示。陪集的这种排布表明 $\frac{Z}{<12>} \cong C_{12}$.

但从这个例子中还可以学到更多东西。图 8.18 依循图 8.13 与图 8.14 描述的模式展示了 $\frac{Z}{<12>} \cong C_{12}$. 图中还标出了同态映射 $\phi : Z \to C_{12}$，商过程 q 以及同构映射 $i : \frac{Z}{<12>} \to C_{12}$.

对于任意整数 k，$q(k)$ 表示所有被 12 除余 k 的数组成的陪集。然后 i 把这个陪集映射到 C_{12} 中的相应节点。因为 ϕ 等同于 q 与 i 的复合，而我们已经知道 ϕ 把陪集 $k+ < 12 >$ 映到 C_{12} 中的元素 k，这也就是 i 映射的结果。注意到，C_{12} 中的元素都是

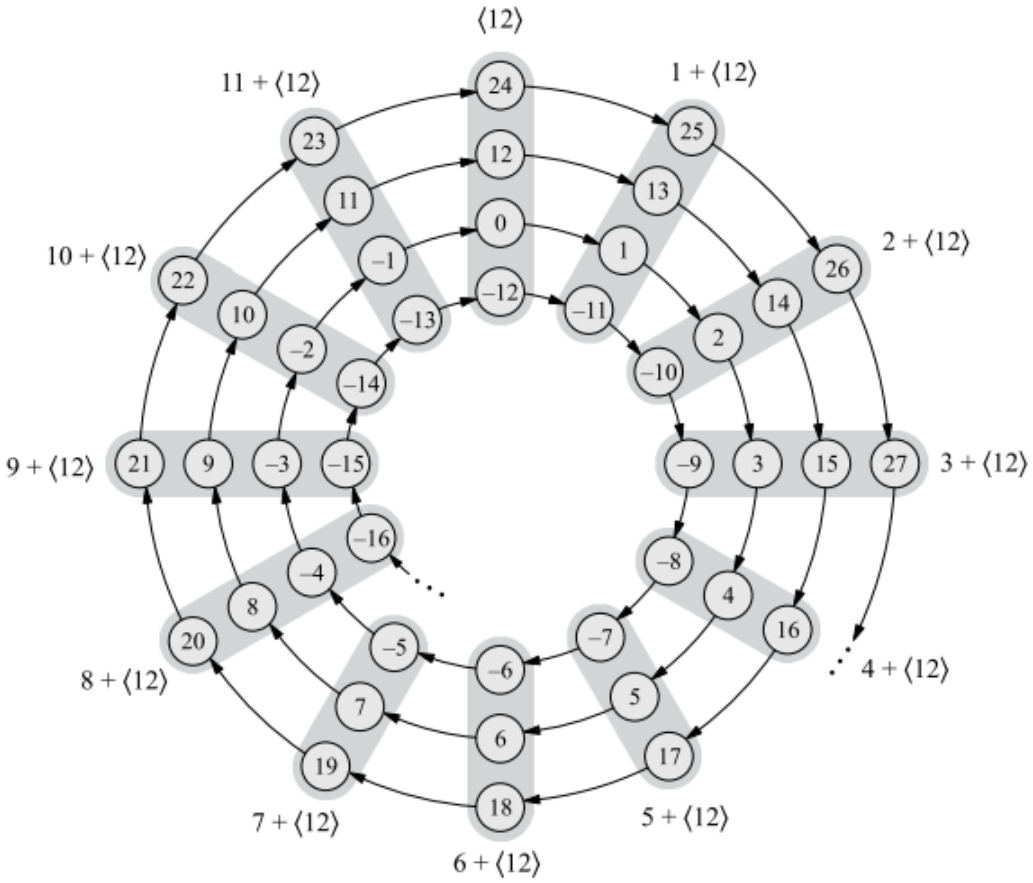


Figure 8.17. A Cayley diagram of the group $\mathbb{Z}$ organized by cosets of $\langle 12 \rangle$. The quotient group structure becomes clear; we can see that the cosets form C_{12}.

mod 12 的余数，因此，对于任意整数 k，$\phi(k)$ 表示的实际意义就是数 k 被 12 除所得的余数，或者说同态映射 ϕ 是一个求余数的算数运算。

以上分析方法可以类似地运用于任意的 $\frac{Z}{<n>}$，从而得到类似的结论，比如 C_n 同构于 $\frac{Z}{<n>}$，同态映射 ϕ 计算的是 mod n 的余数。两个数关于 mod n 同余 ($a \equiv_n b$) 当且仅当 ϕ 将它们映到 C_n 中相同的元素。

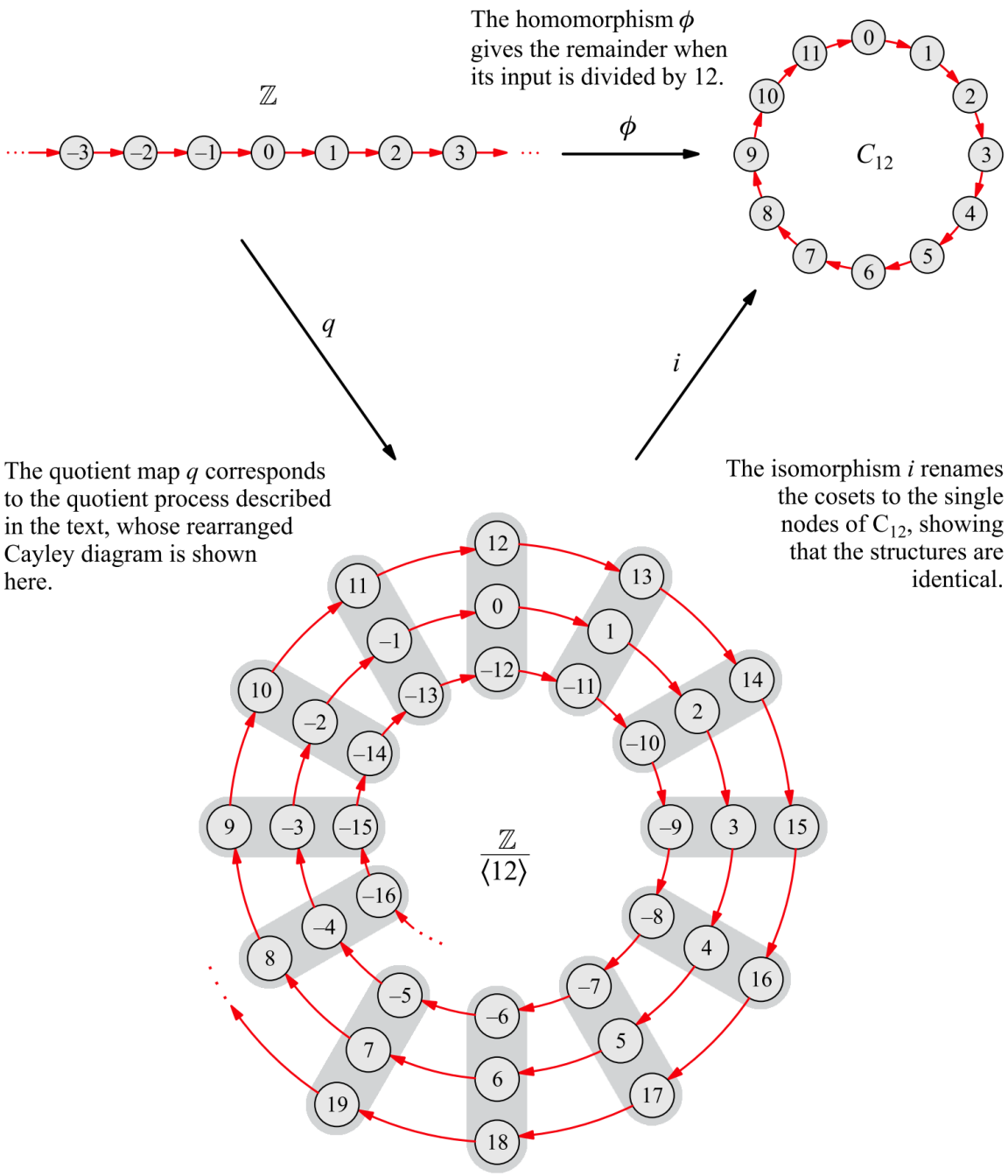
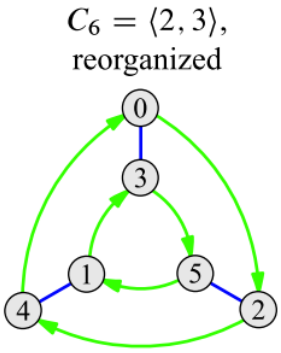


Figure 8.18. The combination of a quotient map and renaming isomorphism yields the map ϕ. For any integer k, $\phi(k)$ is the remainder when k is divided by 12.

8.4　直积与互素

有些循环群可以伪装成直积的样子，有些却不能。在本书之前的内容中，我曾用 C_6 的生成元 2 和 3 作为箭头将其伪装成 C_2 与 C_3 的直积，从而展示了它的另一种形式。(7.3 节的图 6.5 最右边，即下图)



与之相比，你绝不可能把 C_8 表示成除了循环形式外的其他形式。你也许会想着添加或剔除一些箭头以期能将它伪装成别的样子，但是这样做必然会破坏整个图的连通性，从而无法表示 C_8. 但是对于 C_8 的一个有效的凯莱图而言，必然得有一个长度为 8 的箭头 (因为 C_8 中存在 8 阶的元素)，这就导致 C_8 凯莱图的任意一种形式都可识别为**循环**的样子。为什么会有这样的差异呢？为何有的 C_n 能伪装成别的样子有的却不行？答案可以用同构映射来表述。在此之前，我们需要了解**互素 (relatively prime numbers)** 这一概念。

两个整数 a 与 b 互素，可以用好几种不同的方式来定义。我们这里为了方便起见采用公倍数 (common multiples) 来定义。任意两个整数 a 与 b 的乘积 ab 是它们的一个公倍数。但是它们也可能有更小的公倍数，比如 30 是 6 和 15 的一个公倍数，它比乘积 $6 \cdot 15 = 90$ 要来的更小。

> **定义 8.6** (互素[1]). *我们称整数 a 与 b **互素 (relatively prime)**，若它们的最小公倍数 (least common multiple) 等于它们的乘积 ab.*

让我们来看看如何将这个定义应用到循环群的凯莱图及其直积上。我们知道整数 3 与 4 互素，下面的图 8.19 展示了 $C_3 \times C_4$ 的凯莱图，其中 $(1, 1)$ 所在轨道的开始一部分被高亮表示。元素 $(1, 1)$ 的阶是多少？你可以花点时间继续追踪图中剩下没标出的轨道

[1] 另一种等价定义则是利用公因数。任意两个整数 a 与 b 有至少有 1 作为它们的一个公因数，但是它们也许还有更大的公因数，比如，6 与 15 有一个公因数 3。你也可以这样定义 a 与 b 互素，若它们的最大公因数为 1。这两种定义的等价性是初等数论中的一个简单事实，当然在这里我并不打算证明这一点。

来确定答案。

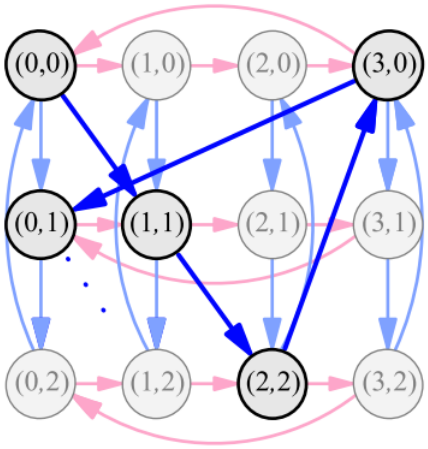


Figure 8.19. Tracing the orbit of $(1,1)$ in the group $C_3 \times C_4$

当你在追踪 $(1,1)$ 的轨道时，你或许也注意到了，每走一步 $(1,1)$ 都会向右移动一列，最后在第四步时又从最右边一列回到了最左边一列，这种“回归”也会出现在第八步，第十二步等等。这种每四步就返回第一列的现象当然是因为图中只有四列。当 $(1,1)$ 的轨道回到初始出发点 $(0,0)$，一个位于第一列的元素，就完成一次追踪。因此，轨道的长度必定是 4 的倍数。对于行，也有类似的事实。每走一步 $(1,1)$ 都会向下移动一行，每三步就会返回第一行。注意到出发点 $(0,0)$ 也位于第一行，因此，轨道的长度也必定是图中行数 3 的倍数。也就是说，元素 $(1,1)$ 所在轨道同时是 3 和 4 的倍数，即它们的一个公倍数。由于 3 与 4 的最小公倍数是 12，所以，元素 $(1,1)$ 所在轨道的长度至少是 12. 因此，$(1,1)$ 的轨道**遍历**了整个 $C_3 \times C_4$，使得 $C_3 \times C_4$ 可以看成是一个由 $(1,1)$ 生成的循环群！从而图 8.19 这样一个缠绕交织的凯莱图可以重新“抖擞”成一个简单的由 $(1,1)$ 生成的长度 12 的圆环形状。

以上推理过程中只用到了 3 与 4 互素这一假设，所以你可以将上一段的推理过程无障碍地进一步推广为 $C_n \times C_m$ 的情形，其中 m 与 n 互素，得到的结论同样是对的。这就证明了下面这个十分重要的定理的一部分。我们将使用这个定理来回答本节开头所提的问题。

定理 8.7. *$C_n \times C_m \cong C_{nm}$ 当且仅当 n 与 m 互素.*

“当且仅当”这个词语是一个很常见的数学术语，其含义是由这个词语连接的两部分总是同时发生。在此处也就是说，若 n 与 m 互素，则群同构；反过来，若群同构，则 n 与 m 互素。我已经在定义 8.6 下面的那几段中解释了其中半个命题的正确性，即“若

n 与 m 互素，则 $C_n \times C_m$ 同构于循环群 C_{nm}”.

更进一步，上面的探讨实际上也给出了显式地确定该同构映射所需的信息。$C_n \times C_m$ 中元素 $(1,1)$ 所在的轨道遍历了整个群，因此 $C_n \times C_m$ 和 C_{nm} 都是包含了 nm 个元素的“圆圈”。C_{nm} 中的每一个元素可以按照一下这个同构映射对应于 $C_n \times C_m$ 中元素 $(1,1)$ 所在轨道中的一步:

$$\theta : C_{nm} \to C_n \times C_m \qquad \text{其中} \qquad \theta(k) = (1,1)\text{所在轨道中的第}k\text{步}.$$

现在我们来证明定理的另一半。

证明. 由于 $C_n \times C_m \cong C_{nm}$，即 $C_n \times C_m$ 是一个循环群，则它必定由它的某个元素生成。我们把这个生成元记作 (a,b)，因为我们不知道 $a \in C_n$ 或 $b \in C_m$ 具体是多少。注意到 (a,b) 的轨道包含了整个 $C_n \times C_m$，因此元素 $a \in C_n$ 所在的轨道必定包含了 C_n 的所有元素，同样地，元素 $b \in C_m$ 所在的轨道必定也包含了 C_m 的所有元素 (用反证法容易说明)。因此，a 生成了 C_n(故 a 的阶为 n) 且 b 生成了 C_m(故 b 的阶为 m). 这样图 8.20 便是 $C_n \times C_m$ 的一个可能的凯莱图的形式，其中生成元是元素 (a,e)(即图中红色箭头) 与元素 (e,b)(即图中蓝色箭头)。**此时，元素 (a,b) 所在的轨道就具有跟图 8.19 中的 $(1,1)$ 所在轨道一样的模式**。

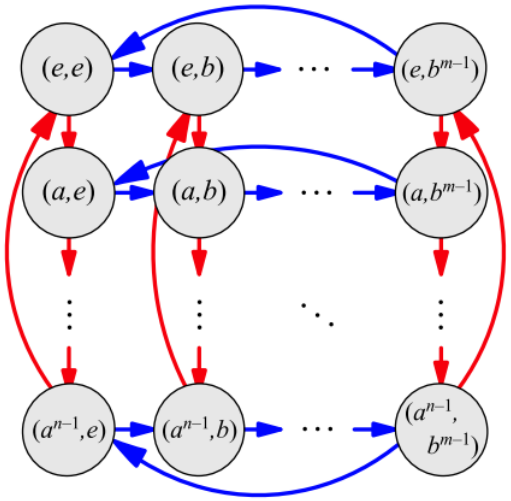


Figure 8.20. A Cayley diagram for the group $C_n \times C_m$, for some n and m

接下来我们来说明为什么元素 (a,b) 的阶一定等于 n 和 m 的最小公倍数。注意到元素 (a,b) 所在的轨道经过 m 步，$2m$ 步，$3m$ 步 $\cdots$ 后返回到第一列，即每经过列数 m 的整数倍就回到第一列；类似地，该轨道每经过行数 n 的整数倍就回到第一行。又因为初始出发点 (e,e) 位于第一行第一列，因此**轨道的长度必定既是 n 的倍数，也是 m 的倍数，**

即 m 与 n 的公倍数。另外我们知道，元素 (a,b) 的阶被定义为从单位元节点 (e,e) 出发首次回到单位元节点时 (a,b) 的轨道的长度，由以上分析便可知，元素 (a,b) 的阶必为 n 与 m 的最小公倍数。另一方面，因为 (a,b) 生成了 $C_n \times C_m$，而 $C_n \times C_m$ 含有 nm 个元素，所以元素 (a,b) 的阶 $= |< (a,b) >| = |C_n \times C_m| = nm$. 综上所述，我们有：

$$n\text{与}m\text{的最小公倍数} = \text{元素}(a,b)\text{的阶} = nm$$

这就证明了 n 与 m 互素。 □

定理 8.7 完美回答了我们开始提的问题，什么时候能将一个循环群伪装成一个直积？如果一个循环群的阶可以分解为两个互素的数的乘积，比如 $6 = 2 \cdot 3$，则它可以图示为直积的形式，即 $C_6 \cong C_2 \times C_3$. 而数字 8 无论如何也不能分解为互素的两个数的乘积 (注:$8 = 1 \cdot 8$ 这种平凡分解不考虑)，所以 C_8 不能伪装成直积，比如 $C_8 \ncong C_2 \times C_4$. 定理 8.7 还有一些别的应用，你将在本章的习题中遇到。它可以帮助我们确定某些特定的循环图的形状 (习题 8.23) 以及如何将 C_n 高效嵌入 S_m(习题 8.27)。它也将应用于下一节内容及相关习题中。

8.5 阿贝尔群基本定理