第 5 章　集合与运算

在本讲中，我们将打开一扇通往现代数学核心领域的大门——集合论。当我们谈论数学时，无论是数学分析中的连续函数，还是高等代数里的向量空间，这些概念最终都建立在同一个基础之上：集合。

想象一下，数学世界就像一座宏伟的图书馆，而集合论就是支撑整座建筑的钢架结构。从康托尔在 19 世纪用" 确定且可区分的对象构成的整体" 定义集合开始，这个看似简单的概念就像数学的" 基因编码"，既能描述宇宙中最基本的元素（比如自然数 1,2,3），也能通过笛卡尔积构建出多维空间，还能通过映射在完全不同的集合之间架起桥梁。

5.1　集合

集合的概念相信大家都很熟悉，集合是指具有某种特定性质的具体的或抽象的对象汇总而成的集体。不过在集合论诞生之初，人们对集合这一概念认识还不清晰，提出了诸多悖论，其中最著名的就是罗素悖论，这些悖论引发了第三次数学危机。

例 5.1.1　(罗素悖论) 假设有一个集合 A，是由所有不属于自身的集合构成的，那么 A 是否属于 A?

假如 $A \in A$，那么根据定义，A 是一个不属于自身的集合，故 $A \notin A$，矛盾；假如 $A \notin A$，那么 A 就是一个不属于自身的集合，根据定义，$A \in A$，矛盾。

最终人们通过建立公理化的集合论(例如由德国数学家 Zermelo 和以色列数学家 Fraenkel 等提出的 ZF 系统，在此基础上再加上选择公理构成 ZFC 公理系统）避免了悖论，为无限集合的研究提供了一个工具，同时为数学提供了一个严格的基础，几乎所有现代数学都可以在 ZFC 公理化体系的框架内形式化。

问题 5.1.1　如何描述集合？描述集合的方法有哪些?

问题 5.1.2　请举出几个集合的例子。

问题 5.1.3　集合具有怎样的性质?

集合的性质:

1. 确定性：对于一个对象，能够明确判断它是否属于这个集合。
2. 互异性：集合中的元素都是互不相同的，重复的元素只算一个。

3. 无序性：集中中的元素不考虑排列顺序。

问题 5.1.4 由一些集合构成的集体还一定是集合吗?

例 5.1.2 设 $S=1,2,3$，令 P 是由 S 的所有的子集构成的集体，那么

$$P=\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}.$$

P 是一个集合，称为集合 S 的幂集，通常记作 $P(S)$。

回到罗素悖论中，我们发现无法确定集合 A 是否是属于集合 A 的，这和集合的确定性是矛盾的，这也就告诉我们，由所有不属于自身的集合构成的集体并不是一个集合！通常，由一些集合构成的集体我们称为集族，集族可能是集合，也可能不是集合。

在本节的最后，请大家回答下面的问题:

问题 5.1.5 如何衡量一个集合的规模大小?

一个集合的规模大小称为集合的势，很容易我们可以想到通过元素的个数来衡量一个集合的势，但对于元素个数有限的集合这是可以操作的，对于无限的集合怎么办?

问题 5.1.6 对于一些特殊的集合，例如线性空间，还有其他方法来衡量规模大小吗?

5.2 映射

知道了如何衡量一个集合的规模大小之后，自然而然会提出如下的问题:

问题 5.2.1 两个集合之间如何比较它们的规模大小?

为了回答这个问题，我们需要引入集合之间映射的概念。

定义 5.2.1 设 A,B 是两个集合，如果集合 A,B 之间存在某种对应规则 f，使得对任意的 $x\in A$，都存在唯一的 $y\in B$ 与之对应，那么我们就称 f 是一个从 A 到 B 的映射，记作

$$f:A\to B$$

$$x\mapsto y=f(x).$$

有了这样的概念之后，自然而然会有如下的问题:

问题 5.2.2 如果 $f:A\to B$ 是一个集合间的映射，那么

- $\forall y\in B$, 是否存在 $x\in A$，使 $y=f(x)$?
- $\forall x\in A, y=f(x)$，是否存在另一个 $x_0\in A$，使得 $y=f(x_0)$?

针对这两个问题，人们提出了单射与满射的概念:

定义 5.2.2 设 $f:A\to B$ 是一个集合间的映射，

- 若 $\forall y\in B$, 都存在 $x\in A$，使 $y=f(x)$，则称 f 是一个满射。

- 若 $\forall x, x' \in A$，且满足 $f(x) = f(x')$，都能推出 $x = x'$，则称 f 是一个单射。
- 若 f 既是单射又是满射，则称 f 是一个双射。

问题 5.2.3　请举出如下的例子：

- 一个映射是单射但不是满射。
- 一个映射是满射但不是单射。
- 一个映射是双射。

有了映射的概念后，就可以比较两个集合之间的势了。

定义 5.2.3　设 A, B 是两个集合，若存在双射 $f : A \to B$，那么称这两个集合是等势的。

例 5.2.1　$\{A, B, C\}$, {红，黄，蓝}，{孙悟空，哪吒，二郎神}，$\{1, 2, 3\}$，$\{-1, 0, 1\}$ 这些集合都是等势的。

若是等势的有限集，等势意味着这些集合所含元素个数相等。

问题 5.2.4　请举出 3 个和 $\mathbb{Z}$ 等势的集合。

凡是和 $\mathbb{Z}$ 等势的集合就称为无限可数集。无限可数集的势是所有无限集中势最小的集合，那么怎样的无限集的势是第二小的呢?

德国数学家乔治 · 康托尔在 19 世纪末提出不存在一个集合的势严格介于自然数集的势和实数集的势之间。这就是著名的连续统假设，在 ZFC 公理系统中无法被证明也无法被反驳，有兴趣的同学可以自行了解相关数学历史。

5.3　运算与关系

有了集合的概念后，我们发现仅有集合的概念是与远远不够的。例如，我们最熟悉的集合是数集，而数与数之间存在加法、乘法，数与数之间还可以比较大小，那么我们该如何来用集合论的语言描述这些呢?

5.3.1　运算

首先来看一个例子：

例 5.3.1　两个实数的加法可以看作如下映射：

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

$$(a, b) \mapsto a + b$$

问题 5.3.1　写出两个正实数的幂次，即 a^b，对应的映射。

问题 5.3.2 写出两个 n 阶实矩阵的乘法所对应的映射。

定义 5.3.1 设 A 是一个集合，若 $f: A \times A \to A$ 是一个映射，则称 f 是集合 A 上的一个二元运算。

定义 5.3.2 设 A 是一个集合，$f: A \times A \to A$ 是一个一个二元运算。

1. 若 $f(a,b) = f(b,a)$ 对任意的 $a, b \in A$ 都成立，则称该二元运算满足交换律。
2. 若 $f(f(a,b),c) = f(a,f(b,c))$ 对任意的 $a, b, c \in A$ 都成立，则称该二元运算满足结合律。

这样，我们从集合与映射的角度重新定义了什么是二元运算以及运算的交换律和结合律。

问题 5.3.3 分配律也是一种常见的规律，大家能不能试着给出分配律的定义?

问题 5.3.4 定义 5.3.1还可以进一步的推广吗? 例如不同集合之间的运算的定义。

问题 5.3.5 仿照 5.3.1写出向量的数乘对应的映射。

5.3.2 关系

除了运算之外，集合中两个元素之间通常还具有某些关系，例如，数之间的大小关系，集合的包含关系，矩阵的相似关系等等。那么我们能否像之前给出关系的抽象定义呢?

定义 5.3.3 设 A 是一个集合，R 是集合 $A \times A$ 的一个子集，那么称集合 R 是 A 上的一个关系。若 $(x,y) \in R$，记作 xRy。

例 5.3.2 设 $R = \{(x,y) | x, y \in \mathbb{R}, x < y\}$，则 R 是实数集 $\mathbb{R}$ 上的小于关系。

例 5.3.3 设 $R = \{(A,B) | A, B \in M_n(\mathbb{R}), \text{且存在可逆阵 } P \text{ 使得} B = P^{-1}AP\}$，则 R 是 n 阶实矩阵的相似关系。

例 5.3.4 设 $R = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} | m - n \text{是 3 的倍数}\}$，则 R 是整数上的两个数除以 3 后余数相同的关系。

问题 5.3.6 请写出相等关系对应的集合 R。

对于一个集合，我们通常希望能根据一些特性将集合划分成若干个不相交的部分，例如将一个国家划分成省进行管理，这样我们就不需要对集合中的每一个元素单独进行研究，只需要对具有代表性的元素研究就可以了。

问题 5.3.7 满足怎样的性质的关系才能成为一个划分的依据?

定义 5.3.4 设 $\sim$ 是集合 A 上的一个关系，若满足如下性质，则称 $\sim$ 是集合 A 上的一个等价关系：

- 反身性：对任意 $a \in A$，$a \sim a$；
- 对称性：若 $a \sim b$，则 $b \sim a$；
- 传递性：若 $a \sim b, b \sim c$，则 $a \sim c$。

问题 5.3.8 请列出三个等价关系的例子。

等价关系是相等关系的一个推广，有了等价关系后就可以对集合进行划分了。

定义 5.3.5　设 A 是一个集合，$\sim$ 是 A 上的一个等价关系，对任意的 $a \in A$，令 $[a] = \{b \in A | a \sim b\}$，则称 $[a]$ 是集合 A 中元素 $[a]$ 所在的等价类。集合 A 关于关系 $\sim$ 的所有等价类的全体记作 $A/\sim$。

性质　若 $[a] \cap [b] \neq \emptyset$，则 $[a] = [b]$。

问题 5.3.9　$A/\sim$ 是一个集合吗?

例 5.3.5　设 n 是一个给定的大于 1 的正整数，在整数集上定义如下关系：

$$a \equiv b \pmod{n} \text{ 当且仅当 } n | a - b。$$

称为模 n 的同余关系。

这是一个等价关系，因为除以 n 得到的余数只有 $0, 1, 2, \cdots, n-1$，因此一共有 n 个等价类：$[0], [1], [2], \cdots, [n-1]$，也记作

$$\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}.$$

这些等价类通常被称为模 n 的剩余类，在数论的相关研究中扮演了十分重要的角色。我们可以定义这些等价类之间的加法与乘法，同学们有兴趣的可以在课后做进一步了解。

第 6 章　置换

6.1　刚性变换

刚性变换是描述物体在空间中位置和方向变化的一种数学工具，广泛应用于机器人学、计算机图形学和物理学等领域。它能够保持物体的形状和大小不变，也就是使每个几何图形的像与原像是全等的变换，例如在三维空间中，平移、旋转以及关于某个平面的镜像反射都是刚性变换。通过刚性变换，我们可以精确地描述物体从一个状态到另一个状态的转换过程，为建模、仿真和控制提供重要基础。

最基础的刚性变换有三类：平移、旋转、镜像反射。事实上，这三类变换都可以通过矩阵来表示出来。

问题 6.1.1　请写出二维平面上逆时针旋转 θ、以及关于 x 轴对称和关于原点对称这三类变换所对应的矩阵。

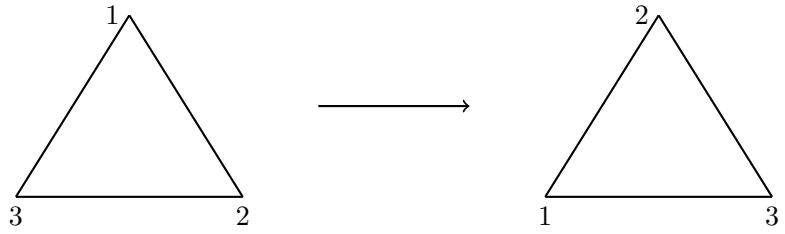
在某些情况下，一些特殊形状的物体可能存在经过刚体变换后还保持不动，例如圆在绕圆心旋转的变换中，无论旋转多少度，仍然还是那个圆。通过分析这些特殊形状在刚体变换下的不变性，可以更好地理解刚体的性质，例如在化学中，通常会用来描述分子的对称性。

问题 6.1.2　哪些变换可以保持平面上的正三角形不变？如何描述它们？若是正 n 边形呢？平面上共有多少种刚性变换可以保持正 n 边形不变？

我们发现对一般的正 n 边形，要写出对应满足条件的矩阵很困难，所以我们要用新的方式来描述它们。

6.2　置换

以正三角形为例，绕中心逆时针旋转 120 度后，三角形保持不变，但如果我们对顶点进行标号，会发现顶点的位置发生了改变：

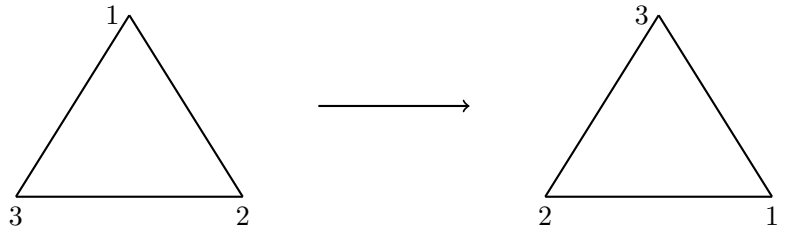


注意到在这个过程中，顶点 1 到了 3 号位，顶点 2 到了 1 号位，顶点 3 到了 2 号位，那么我们可以用顶点的变化关系来表示这个过程：

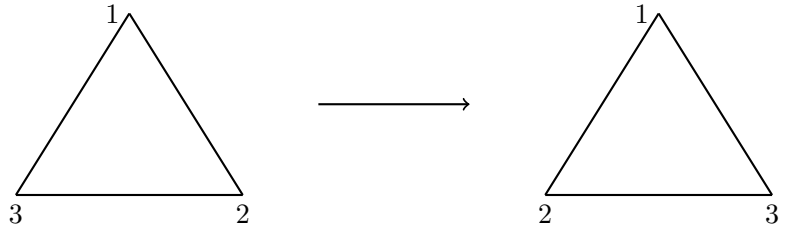
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

其中，第一行代表第一个图形中的顶点标号，第二行代表第一行中对应顶点变换后的位置。

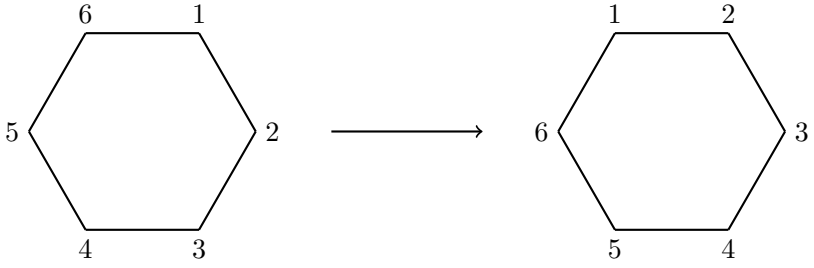
类似的，可以用 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 来表示如下的变换：



用 $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 来表示如下的变换：



问题 6.2.1　可以用上述表示方法来表示一个正 6 边形逆时针旋转 60 度的变换吗？



更进一步，可以用上述方法表示保持正 n 边形不变的变换吗?

观察上述表示方法，我们发现第一行是自然数 $1,2,\cdots,n$ 的自然排列，第二行则是自然数 $1,2,\cdots,n$ 的一个 n 阶排列，于是给出如下定义:

定义 6.2.1 设 n 是一个自然数，从集合 $\{1,2,\cdots,n\}$ 到其自身的一个双射称为 n 个文字的一个置换。

通常，我们可以用列表法给出一个一般的置换 σ: $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$。

将 n 个文字的置换全体记作 S_n，那么 S_n 中有 $n!$ 个元素。

问题 6.2.2 S_n 上能否定义一个二元运算?

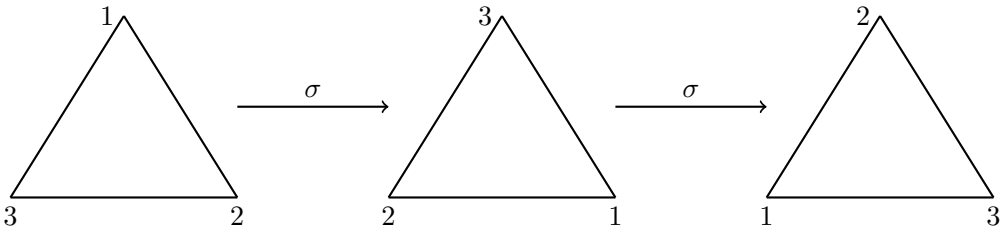
注意到置换的本质是集合间的双射，而双射的复合仍是一个双射，因此我们可以通过映射的复合定义置换的乘法，即:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}=\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

例 6.2.1 设 $\sigma=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$，即 $\sigma(1)=2,\sigma(2)=3,\sigma(3)=1$，那么

$$\sigma^2=\begin{pmatrix} 1 & 2 & 3 \\ \sigma(\sigma(1)) & \sigma(\sigma(2)) & \sigma(\sigma(3)) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ \sigma(2) & \sigma(3) & \sigma(1) \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

上述例子中 σ 代表的是顺时针旋转 120 度，σ^2 的结果是顺时针旋转 240 度，恰好就是做了两次顺时针旋转 120 度!



这告诉我们，置换的乘法对应了变换的乘法!

6.3 轮换

对于列表法，我们发现在实际使用中很不经济，假如说有一个 100 个文字的置换，但就只是将 1 映为 2，2 映为 1，并保持其他不变，那么用列表法表示的时候就会出现很多冗余的信息，而且第一行也很多余，那么有没有更简单的表达方式呢?

定义 6.3.1　设 $i_1, i_2, \cdots, i_d$ 是 $[1,n]$ 中 d 个两两不同的文字。作 $\sigma \in S_n$，满足

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_d) = i_1,$$

并且 $\sigma(i) = i$ 对 $[1,n]$ 中其他文字 i 都成立，则称 σ 是一个 d 轮换，或长度为 d 的轮换，记作 $(i_1 i_2 \cdots i_d)$。

请注意，上述轮换的表示方式是不唯一的，$(i_1 i_2 \cdots i_d)$ 和 $(i_2 \cdots i_d i_1)$ 表示的都是同一个轮换。如果是恒等变换，我们就写作 (1) 或 id 或 1。

例 6.3.1　在 S_4 中，$(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$。

在 S_3 中，$(123) = (231) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$。

注意到用轮换来表示可能会存在一些模糊的情形，例如上述例子中 (123) 可以看作 S_3 中元素，也可以看作 S_4 中元素，但通常都可以通过上下文来判断，因此这个不足之处是可以容忍的。

习题 6.3.1　请用轮换的方式表示置换 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 7 & 6 & 5 \end{pmatrix}$。

对 S_n 中的两个轮换，如果第一轮换中的文字在第二个轮换中没有出现，那么我们称这两个轮换是不相交的。

例 6.3.2　S_6 中，(125) 和 (36) 就是两个不相交的轮换。

用轮换的方式又该如何计算两个置换的乘积呢？我们以下面例子来说明：

例 6.3.3　设 $\sigma = (123), \tau = (243)$，注意到

$$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2, \qquad 2 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 4,$$

$$4 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 1, \qquad 3 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3.$$

因此 $\sigma\tau = (123)(243) = (124)$。

习题 6.3.2　请计算 $(123)(321)$，$(12)(34)$，$(34)(12)$.

一个有趣的事实 任何一个轮换都可以写作有限多个对换（即 2 轮换）的乘积，例如 $(123) = (12)(23)$。

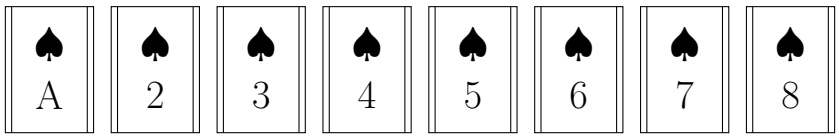
一个轮换 σ 的**阶**是指最小的正整数 n 满足 $\sigma^n = (1)$。

习题 6.3.3　求对换和 3 轮换的阶。

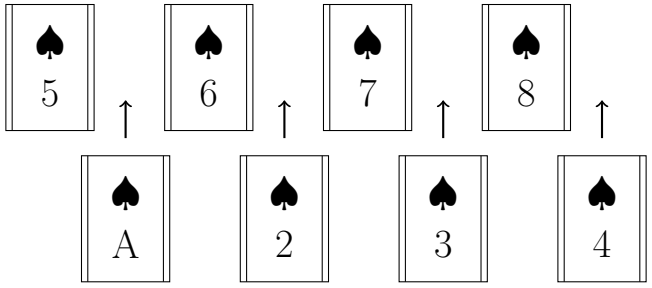
6.4　置换与洗牌

下面请大家思考这样一个问题：洗牌的次数一定是越多越好吗？

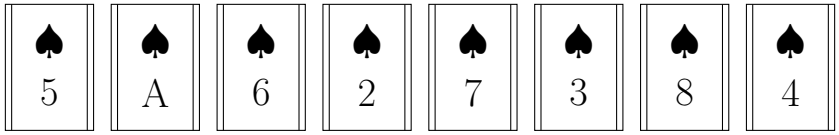
我们以 8 张牌为例。



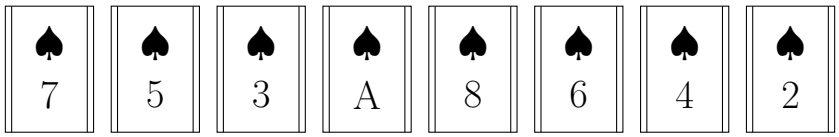
我们不妨假设洗牌是均匀的，即每次洗牌先将前 4 张牌分成第一组，后 4 张牌分成第二组，然后再将第一组的每张牌分别插入第二组对应的位置。例如第一次洗牌过程为：



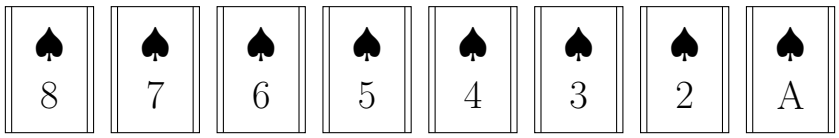
因此洗完一次后得到的顺序为：



我们接着继续按照上述方法洗牌，第二次：



第三次洗牌后：



我们发现，在 8 张牌的时候，洗牌三次后牌堆的顺序和最初顺序刚好完全相反！因此再如此洗 3 次牌后就能回到最初的顺序。这意味着并不是洗的次数越多牌洗的越匀。下面我们来分析下其中的数学原理。

事实上，在上述过程中，我们可以认为每次洗牌给出了一个 8 个文字之间的双射 σ，具体表示为：

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 6 & 2 & 7 & 3 & 8 & 4 \end{pmatrix} = (157842)(36).$$

经计算可以知道 $\sigma^2 = (157842)(157842) = (174)(582)$，注意到 (174) 和 (582) 是不相交的两个 3 轮换，阶为 3，故

$$\sigma^6 = (\sigma^2)^3 = ((174)(582))^3 = (174)^3(582)^3 = (1).$$

这意味着洗 6 次牌后一定能回到最初的牌型。

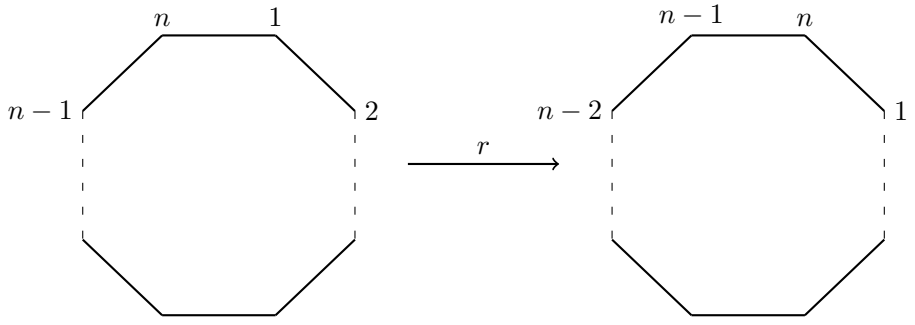
习题 6.4.1　对 8 张扑克还是按照上述方式洗牌，只不过每次洗完牌后再切一次牌，将洗好后的前 4 张放在后 4 张的下面，请问洗多少次牌可以回到最初的顺序?

6.5　二面体群

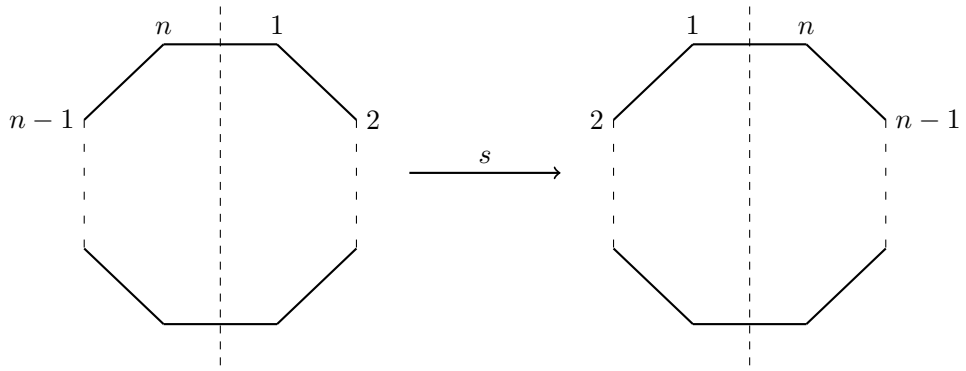
最后，我们回到本章最初的问题，来看看正多边形的刚性变换。

我们假设经过刚性变换，顶点 1 到了 i 号位，此时顶点 2 在变换后的位置只有两种选择，$i-1$ 号位或 $i+1$ 号位（假设 0 号位就是 n 号位，$n+1$ 号位就是 1 号位）。故一共有 $2n$ 种刚性变换。

如果顶点 1 在 i 号位，顶点 2 在 $i+1$ 号位，那么只需要顺时针旋转 $i-1$ 次，每次旋转 $\dfrac{2\pi}{n}$，就可以得到所需图形。也就是说这个刚性变换可以用 r^{i-1} 来表示，其中 $r = (12\cdots n)$。



如果顶点 1 在 i 号位，顶点 2 在 $i-1$ 号位，那我们可以先做一次对称 s，即以顶点 1 和顶点 n 之间的边的垂直平分线为对称轴做一次镜像对称，如下图所示：



因此可以知道

$$s=\begin{cases}(1n)(2,n-1)\cdots(\dfrac{n-1}{2},\dfrac{n+3}{2}) & \text{当 } n \text{ 为奇数时;}\\ (1n)(2,n-1)\cdots(\dfrac{n}{2},\dfrac{n+2}{2}) & \text{当 } n \text{ 为偶数时.}\end{cases}$$

此时，我们再将图形顺时针旋转 i 次就可以了。

通过上述讨论，我们知道所有的刚性变换可以表示为:

$$D_{2n}=\{r^i,r^is|i=0,1,\cdots,n-1\}.$$

事实上，上述集合在置换的乘法下构成一个群，被称作二面体群。

习题 6.5.1 验证所定义的旋转 r 与镜像对称 s 满足关系式 $rs=sr^{n-1}$.