第 3 章　多项式的根

对于任意二次, 三次或者四次多项式, 我们都可以通过一个固定的公式, 将多项式的系数进行若干次四则运算和开根号后计算出它的根. 这个公式被称为求根公式. 如果一个公式只涉及四则运算和开根号, 我们会称其为代数公式. 所以二次, 三次或者四次多项式就是代数公式. 但是这样的代数求根公式对于次数更高的多项式来说是不存在的. 要严格证明这个定理, 通常需要半个学期以上的时间专门学习抽象代数理论. 本节给大家提供一种从本质上使用抽象代数的思想, 但实质上不涉及其内容的证明.

3.1　复数的极坐标表示

在开始之前, 我们需要对中学里所学的复数概念做一点回顾与深化. 形如 $z = x + iy$ 的数被称为复数, 其中 x, y 是实数, i 是虚数单位根, 满足 $i^2 = -1$. 特别地, 我们可以以实部 x 为横坐标, 虚部 y 为纵坐标给出平面上的一个点 (x, y). 反过来任意一个平面上的点也可以通过横纵坐标分量给出相应的复数. 所以平面给出了全体复数的一个几何模型, 称为复平面. 同时我们也知道平面上除了直角坐标系以外还有一个常用的坐标系称为极坐标系. 具体来说, 对于平面上任意一个点, 我们将它与原点用直线相连. 这条直线与 x 轴的夹角记为 θ, 长度记为 r, 则有转换关系式

$$x = r\cos\theta, y = r\sin\theta.$$

所以在极坐标下复数可以表示为

$$z = x + iy = r\cos\theta + ir\sin\theta = re^{i\theta}.$$

最后一个等式被称为 Euler 公式. 这个公式的证明需要用到复变函数理论, 因此不在这里具体展示. 为了帮助读者理解, 我们用 Taylor 展开来做诠释:

$$\begin{aligned} e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \cdots \\ &= 1 + ix - \frac{x^2}{2!} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} + \cdots \end{aligned}$$

$$
\begin{aligned}
&= (1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdots)+i(x-\frac{x^3}{3!}+\frac{x^5}{5!}-\cdots)\\
&= \cos\theta + i\sin\theta.
\end{aligned}
$$

注意这并不是一个数学证明. 因为我们其实并不知道 $e^{i\theta}$ 的定义以及这种复变量的指数函数能否 Taylor 展开. 事实上在复变函数的发展过程中, 是先有 Euler 公式, 再以这个公式来定义 $e^{i\theta}$ 的.

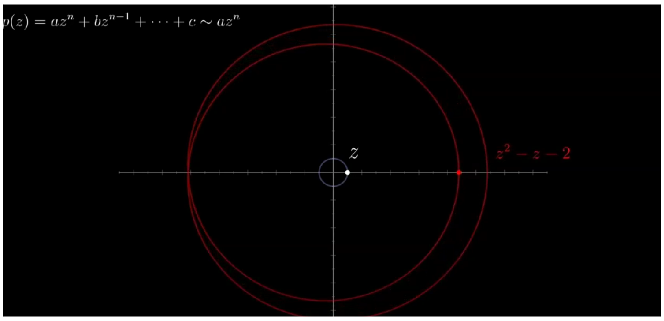
问题 3.1.1 在极坐标表示下复数与复数的乘法是怎样的?

3.2 代数基本定理

接下来我们统一用极坐标来表示复数. 极坐标的好处是, 在这个表示下复数的乘法具有清晰的几何意义. 对任意 $z=re^{i\theta}, z'=r'e^{i\theta'}$, 它们的乘积为 $rr'e^{i(\theta+\theta')}$. 即模长与模长相乘, 辐角与辐角相加. 特别地, 作为热身我们可以用它来证明下面这个代数基本定理.

定理 3.2.1 (代数基本定理) 任何一个 n 次多项式在计算重根的意义下一定恰好有 n 个根.

证明. 首先我们证明任何多项式一定有一个根. 以二次多项式 $z^2-z-2=0$ 为例. 当我们让 z 绕着原点旋转一周时, 这个多项式函数会相应地旋转二周.



为什么恰好是二周? 因为当 z 的辐角从 0 变为 2π 时, z^2 的辐角从 0 变到 4π, 旋转了两周. 而一个比较深刻的复变函数结果, 即辐角原理, 告诉我们多项式函数值的辐角变化完全有最高次项决定, 所以 $z^2-z-2=0$ 也旋转了两周. 同理如果是一个 n 次多项式, 当变量 z 绕原点旋转一周之后, 函数值相应地绕原点旋转 n 周.

现在我们缩小 z 旋转的圆周, 那么函数值旋转的闭曲线也会缩小. 当 $z\to 0$ 时, 函数值形成的闭曲线便会缩小成一点. 那么就有两种情况: 一是闭曲线也缩小到原点 (例如: $w=z^3$ 这个多项式函数). 原点就是一个根; 二是闭曲线缩小到了别的点 (例如: $w=z^2-z-2$ 就会缩到 -2). 那么在这个过程中必然会经过原点. 经过原点时所对应的 z 的取值即为一个根. 所以我们证明了任意一个多项式必然会有一个根.

现在任取一个 n 次多项式 $a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0$, 则其存在一个根 z_1. 于是可以做因式分解

$$a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0=(z-z_1)(b_{n-1}z^{n-1}+\cdots+b_0).$$

而对于多项式 $b_{n-1}z^{n-1}+\cdots+b_0$ 来说也会存在一个根 z_2. 所以可以继续做因式分解

$$a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0=(z-z_1)(z-z_2)(c_{n-2}z^{n-2}+\cdots+c_0).$$

以此类推, 最终可以将多项式分解为

$$a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0=a_n(z-z_1)(z-z_2)\cdots(z-z_n).$$

那么 $z_1,...,z_n$ 就是原多项式的 n 个根. □

问题 3.2.1 五次求根公式不存在与代数基本定理矛盾吗?

3.3 二次求根公式

接下来我们进入正题. 作为热身, 我们来说明二次求根公式中开根号运算出现的必然性. 最重要的一个观察在于: 我们无法对多项式的根进行有效排序. 以二次多项式 $z^2=w=4$ 为例. 我们很容易知道它有两个根 $2,-2$. 通常我们会把一个记作 z_1, 另一个记作 z_2. 但问题是我们该把哪个记作 z_1 呢? 或许这个问题没那么重要. 那么姑且先 $z_1=2,z_2=-2$. 那么多项式就可以重新写为

$$z^2-4=(z-z_1)(z-z_2)=0.$$

接下来我们让 4 绕着原点旋转一周后回到原点. 具体来说, 在 z_1,z_2 后面都乘以 $e^{i\theta}$, 并且让 θ 从 0 跑到 π. 那么相应地 $4=z_1z_2$ 的辐角就跑了 2π 因此没发生任何变化. 但是 $z_1e^{i\pi}=-2,z_2e^{i\pi}=2$, 与之前相比互换了位置. 相对于我们之前指定的顺序 $2,-2$, 在多项式未发生任何改变的情况下变成了 $-2,2$. 这说明我们刚才的排序是有问题的! 从这个基本现象出发, 我们可以证明

定理 3.3.1 *二次多项式的求根公式不可能仅仅由系数的四则运算给出. 等价地, 二次求根公式不是有理函数. (一个仅涉及四则运算的函数被称为有理函数.)*

证明. 假设 z_1,z_2 是二次多项式 $z^2+bz+c=0$ 的根, 并且有求根公式 $z_1=R(b,c)$. 其中 $R(b,c)$ 是关于 b,c 的有理函数.

现在互换 z_1 与 z_2 的位置. 一方面由 Vieta 定理知,

$$-b=z_1+z_2,c=z_1z_2.$$

所以改变根的排序不会改变多项式系数, 从而也不会改变 $R(a,b,c)$ 的函数值. 但是现在通过 $R(a,b,c)$ 所求的根从 z_1 变为了 z_2, 函数值应该发生变化. 矛盾. □

问题 3.3.1 为什么在引入开根号以后能避免这个现象?

原因在于, $z=\sqrt{w}$ 是一个多值函数. 当 z 的辐角从 0 跑到 π, $w=z^2$ 未发生改变. 但是它的平方根从一个单值分支跑到了另一个.

这个证明的本质, 在于有理函数的单值性与互换两个根的位置所产生的多值性之间的矛盾, 从而给出了在求根公式中引入开根号运算的必要性. 而证明五次以上求根公式不存在的想法也是如此. 区别在于, 允许在求根公式中引入了开根号运算这个多值函数后, 仅仅互换两个根的位置所产生的多值性不足以排除其可能性, 我们需要用一种更加微妙的方式来改变根的分布顺序.

3.4 五次求根公式

我们先来排除掉仅仅使用一次根号运算给出求根公式的可能性.

定理 3.4.1 *五次多项式的求根公式不可能仅仅由系数进行一次根式运算给出.*

证明. 假设 z_1,z_2,z_3,z_4,z_5 是五次多项式 $z^5+bz^4+cz^3+dz^2+ez+f=0$ 的根, 并且 $z_1=\sqrt[n]{R(b,c,d,e,f)}$. 其中 $R(b,c,d,e,f)$ 是关于 b,c,d,e,f 的有理函数.

现在我们交换第一个与第二个根的位置. 此时 z_2,z_1,z_3,z_4,z_5 仍然是这个多项式的五个根, 所以这个多项式未发生变化. 另一方面, 假设

$$\sqrt[n]{R(b,c,d,e,f)}$$

的函数值在交换后辐角增加了 $2\pi m$. 接下来我们交换第二个与第三个根:

$$(z_2,z_1,z_3,z_4,z_5)\mapsto(z_2,z_3,z_1,z_4,z_5).$$

对 $\sqrt[n]{R(b,c,d,e,f)}$ 函数值所产生的影响为辐角增加 $2\pi l$. 然后我们交换第一个与第二个根:

$$(z_2,z_3,z_1,z_4,z_5)\mapsto(z_3,z_2,z_1,z_4,z_5).$$

对 $\sqrt[n]{R(b,c,d,e,f)}$ 函数值所产生的影响为辐角减少 $2\pi m$. (因为这是第一个操作的逆操作.) 最后交换第二个与第三个根:

$$(z_3,z_2,z_1,z_4,z_5)\mapsto(z_3,z_1,z_2,z_4,z_5).$$

对 $\sqrt[n]{R(b,c,d,e,f)}$ 函数值所产生的影响为辐角减少 $2\pi l$. (因为这是第二个操作的逆操作.) 四步操作完后,

$$(z_1,z_2,z_3,z_4,z_5)$$

的排序变为了

$$(z_3,z_1,z_2,z_4,z_5).$$

特别地, 原来 z_1 所在的位置换成了 z_3. 但是这四步操作对求根公式 $z_1 = \sqrt[n]{R(b,c,d,e,f)}$ 的综合影响为零. 所以在求根公式下算出来的仍然应该是 z_1. 矛盾. □

这种先进行一次操作 σ, 再进行一次操作 τ, 再进行一次逆操作 σ^{-1}, 最后进行一次逆操作 τ^{-1} 的行为被称为交换子 (Commutator). 而定理 3.4.1 可以简述为通过一个交换子可以排除掉一次根式运算给出求根公式的可能性. 特别地注意到, 交换子的定义只涉及到三个根, 所以我们其实顺便证明了三次求根公式不可能仅仅由系数进行一次根式运算给出. 事实上在三次求根公式中会出现下面这种根式套根式, 即两次根式运算的部分:

$$\sqrt[3]{\frac{2b^3 - 9abc + 27a^2d + \sqrt{2b^3 - 9abc + 27a^2d^2 - 4(b^2 - 3ac)^3}}{2}}.$$

如果我们想排除两次根式运算的可能性该怎么做? 使用交换子的交换子! 即选取四种交换根之间位置的操作 σ, τ, χ, ρ, 然后定义

$$(\sigma\tau\sigma^{-1}\tau^{-1})(\chi\rho\chi^{-1}\rho^{-1})(\sigma\tau\sigma^{-1}\tau^{-1})^{-1}(\chi\rho\chi^{-1}\rho^{-1})^{-1}.$$

可以直接验证, 这个操作不会改变形如 $\sqrt[n]{R_1 + \sqrt[m]{R_2}}$ 的函数值, 其中 R_1, R_2 是有理函数. 但是它确实会改变根原来的顺序, 从而给出矛盾. 注意到交换子的交换子定义涉及到四个根, 所以对四次以上的求根公式我们都可以排除只做两次根式运算的可能. 但是使用根式套根式再套根式的运算是可以给出四次求根公式的!

而到了五次多项式, 这个现象发生了颠覆性的变化. 注意到

$$\chi : (z_1, z_2, z_3) \mapsto (z_3, z_1, z_2)$$

这个置换事实上是可以写成一个交换子的样子的.

问题 3.4.1　试着验证这个命题.

借助另外两个根 z_4, z_5, 我们做如下变换:

$$(z_1, z_2, z_3, z_4, z_5) \overset{\sigma}{\mapsto} (z_4, z_1, z_3, z_2, z_5) \overset{\tau}{\mapsto} (z_4, z_3, z_5, z_2, z_1) \overset{\sigma^{-1}}{\mapsto}$$
$$(z_3, z_2, z_5, z_4, z_1) \overset{\tau^{-1}}{\mapsto} (z_3, z_1, z_2, z_4, z_5).$$

注意到从起始到结束, z_4, z_5 的位置未发生改变, 但是借助它们我们同样完成了

$$\chi : (z_1, z_2, z_3) \mapsto (z_3, z_1, z_2)$$

这个置换. 所以可以记作

$$\chi = \sigma\tau\sigma^{-1}\tau^{-1}.$$

更多地, χ, σ, τ 有一个共同的性质, 即 $\chi^3 = \sigma^3 = \tau^3 = id$. 这里 id 指代恒等置换, 即 $(1,2,3) \mapsto (1,2,3)$. 这样的置换被称为 3 阶循环置换. 所以这个观察可以总结为: 涉及

到五个根及以上的三阶循环置换总是可以分解成两外两个三阶循环置换所组成的交换子. 那么 σ, τ 又可以继续拆成交换子. 不断重复这个过程, 我们可以将

$$\chi : (z_1, z_2, z_3) \mapsto (z_3, z_1, z_2)$$

分解成交换子的交换子的交换子的交换子的... 交换子. 所以无论事先假设五次求根公式是多少次的根式运算, 我们总可以用相同次数的交换子来得出矛盾. 综上, 五次及以上的求根公式不存在!

3.5 群论补充

最后我们做一些补充. 已知三次和四次多项式求根公式确实是存在的. 那么这种交换子套交换子的论证方法为什么不会对它们产生矛盾? 事实上, 对于三个根之间的置换总共有六种, 即 $(z_1, z_2, z_3) \mapsto (z_1, z_2, z_3)$, $(z_1, z_2, z_3) \mapsto (z_1, z_3, z_2)$, $(z_1, z_2, z_3) \mapsto (z_2, z_1, z_3)$, $(z_1, z_2, z_3) \mapsto (z_2, z_3, z_1)$, $(z_1, z_2, z_3) \mapsto (z_3, z_1, z_2)$, $(z_1, z_2, z_3) \mapsto (z_3, z_2, z_1)$. 直接验证可知, 无论取其中哪两种组成交换子, 必然会得到 $(z_1, z_2, z_3) \mapsto (z_1, z_2, z_3)$, $(z_1, z_2, z_3) \mapsto (z_2, z_3, z_1)$, $(z_1, z_2, z_3) \mapsto (z_3, z_1, z_2)$ 的其中之一. 也就是说涉及三个根的交换子一定是 3 阶循环置换. 接着还可以直接验证, 两个 3 阶循环置换的交换子一定是恒等置换.

问题 3.5.1 试着验证这个命题.

所以交换子套交换子必然是恒等置换. 那么再这个基础上套更多的交换子就失去意义了. 从另一个角度来说, 之前我们将一个涉及三个根的置换分解成无限交换子的过程需要借助另外两个根, 这本身也是一个映证.

四次多项式也有类似的现象. 我们只列出具体性质, 把验证留给有兴趣的读者. 对于涉及四个根的置换, 交换子的交换子会改变根的位置; 交换子的交换子的交换子是恒等置换. 相应地, 仅仅两次根号运算无法给出四次多项式求根公式, 但是三次根号运算可以.

问题 3.5.2 试着验证这个命题.

从本质上说, 我们通过说明根的位置分布所具有的" 对称性" 与求根公式所具有的" 对称性" 应该相匹配, 从而给出多项式求根公式的具体描述. 而这种研究" 对称性" 的理论其实就是群论. 区别在于, 群论会把这些现象抽象出来做更加一般的讨论. 这种抽象对于初学者来说虽然痛苦, 但是对于解放我们的数学思想, 减轻思维负担具有重要意义. 回到求根公式问题. 我们可以利用群语言把整个事情说得非常干净简洁.

涉及 n 个根的置换全体记作 S_n, 被称为 n 阶对称群. 涉及 n 个根的循环置换全体记作 C_n, 被称为 n 阶循环群. n 阶对称群中全体偶置换组成的群记作 A_n, 被称为 n 阶交错群. 所以我们刚才论证过程用群论的语言来描述就是: 二、三、四次多项式有求根公式, 是因为 $S_n (n \leqslant 4)$ 可以写成某些素数阶循环群的直和. 什么叫直和? 比如 S_3 里面有六个成员, 而 C_3 是其中三个成员. 但是剩下三个成员其实可以通过对 C_3 中的成员做相同的变化

得到. 具体来说, 交换前两个位置就可以:

$$(1,2,3) \mapsto (2,1,3), (2,3,1) \mapsto (3,2,1), (3,1,2) \mapsto (1,3,2).$$

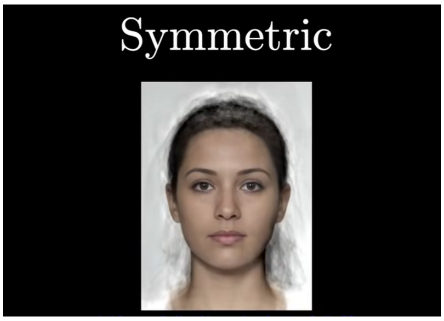
所以 S_3 是 C_3 与 C_2 的直和. 另一方面, S_n 一定可以写成 A_n 与 C_2 的直和. 因为置换可以均分为奇置换和偶置换, 并且将所有偶置换交换前两个位置就可以得到所有奇置换. 但是 A_5 无法再写成更小的直和, 因此五次多项式没有求根公式.

第 4 章　群论简述

在上一节的证明中, 我们其实用到了很多群论的基本内容, 例如交换子的定义、直和分解等等. 群 (group) 是抽象代数学的研究对象. 通常我们需要花费一个学期的时间专门学习抽象代数这门学科. 因此这里仅仅提供一个简单叙述.

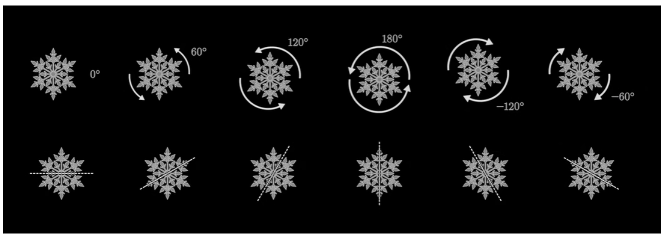
4.1　群成员

从本质上来说, 群论研究的是自然世界中的对称性 (Symmetry). 例如下面这张照片, 即使我们不学习数学也能凭常识判断其对称性. 不过我们依赖的" 常识" 究竟是什么?



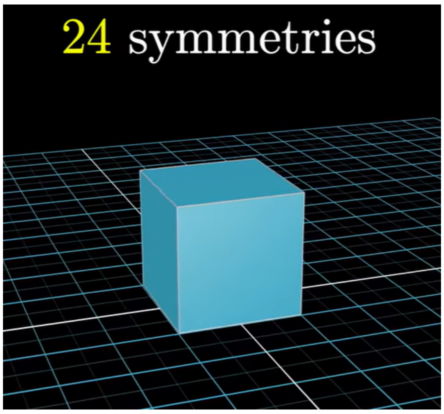
问题 4.1.1　如何描述这张照片的对称性?

具体来说, 我们将照片翻转 180° 之后, 它没有发生任何改变. 因此我们判断它关于中轴线对称. 所以这就是对称性的本质, 即物体在某些操作之后不发生改变的性质. 那么我们将这些操作放在一起组成一个团体, 就称为群. 再来看下面这个雪花, 我们总共有 12 种不同的操作, 可以使其不发生改变.



所以相较于照片, 它有更丰富的对称性. 特别在这些操作中, 我们尤其注意有一个操作叫作" 什么也不做 (Do nothing)"! 什么也不做当然不会改变这个雪花. 我们特意把这个操作也放在里面从而组成十二个成员, 这个群就记为 D_6. 同样的, 之前的照片其实也有两种操作: 一是" 什么也不做"; 二是" 翻转". 这两个成员组成的群就记为 C_2.

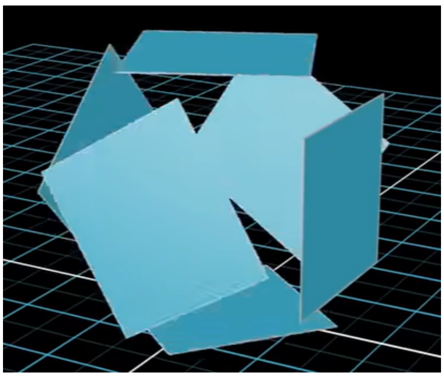
同样需要注意的是, 就算是同一个几何体, 当我们关注的重点不同时, 对称性所反映的群也不一样. 例如一个正六面体. 如果要求在变换的过程中不能改变它的整体结构, 那么我们就只能做翻转变换. 总共就只有 24 种不同的翻转.



当我们允许做镜面对称变换时, 群成员就增加到了 48 种. 特别地, 在镜面对称前后正六面体的定向其实发生了改变. (我们都知道右手在镜子中是左手, 这就是定向发生了变化.) 更多的, 如果还允许在变化过程中将六个表面拆出来做旋转, 又或是交换其中几个正方形的位置后再拼回去, 那群成员就多了很多, 总共有

$$8^6 \cdot 6! = 188743680$$

那么多.

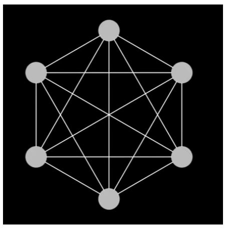


问题 4.1.2　试着验证这个公式.

所以结构越简单对称性就会越丰富. 那么最简单的结构有哪些呢? 例如我们将六个一模一样的小球等距放置. 那么可以随意交换其中某些小球的位置而不产生改变. 为了区分

不同的交换方式, 可以给小球依次标号为 $1,2,3,4,5,6$. 所以现在可以用 $1,2,3,4,5,6$ 所有可能的排列顺序来描述所有可能的置换小球方式. 总共就会有 $6!$ 中不同的排列方式, 也就对应了 $6!$ 种不同的交换方式. 这些交换方式被称为置换 (permutation). 那么 n 个小球的对称性就会产生一个具有 $n!$ 个成员的群, 称为对称群, 记作 S_n.

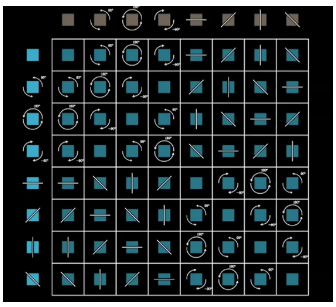
对称群就是一类最为简单的群. 通过给对称群施加限制, 可以得到很多其它群. 例如现在我们额外要求置换的过程中不能改变小球之间的相对位置, 也就是说 1 号球必须在 2 号和 6 号之间, 3 号球必须在 2 号和 5 号之间, 那么我们能做的就只有旋转和翻转两类操作总计 12 种, 与之前雪花的对称性产生的是同一个群.



问题 4.1.3 这是不是说明两者是同一种对称性?

4.2 群运算

我们现在有了初步认识, 群成员就是反映某种几何体对称性的所有操作. 不过群这个数学对象的精彩之处在于, 它除了成员还有结构. 以一个正方形为例, 它的对称性对应于八种操作: 什么也不做, 逆时针旋转 $90°$, 逆时针旋转 $180°$, 顺时针旋转 $90°$, 沿着横轴翻转, 沿着纵轴翻转以及沿着两条对角线翻转. 而这八种操作之间并不是完全独立的. 比如, 我们先逆时针旋转 $90°$, 再逆时针旋转 $180°$, 效果等同于顺时针旋转 $90°$; 先逆时针旋转 $90°$, 再沿着横轴翻转, 效果等同于沿着对角线翻转. 施加任何两个操作, 效果都会恰好等同于另一个操作. 我们甚至可以将这些关联列为一个表格.



问题 4.2.1 验证这个表格.

这像不像我们熟悉的九九乘法表? 事实上这个现象在任何一个群里都有, 暗示着我们其实可以像做数与数之间的乘法一样, 将任意两个群成员" 乘" 在一起得到另一个群成员. 特别地, 有一个特殊的成员" 什么也不做", 它与任何成员做" 乘法" 都不会改变那个成员. 所有其扮演的角色就像是数的乘法中的"1", 又或是数的加法中的"0".

所以群是" 反映对称性的操作"+" 操作之间的乘法" 所给出的一个代数结构. 将这些朴素的语言深化就得到如下定义:

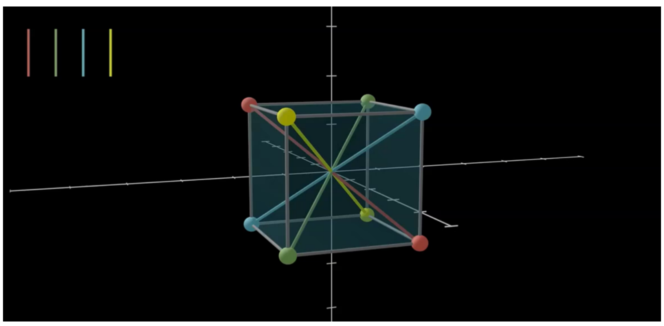
定义 4.2.1　假设 G 是一个非空集合, 在其上定义了一个二元映射记为 $\cdot$, 满足

1. (结合律) 任意 $a, b, c \in G$, 都有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. (幺元) 存在一个元素 $e \in G$, 使得对任意 $a \in G$ 都有 $e \cdot a = a \cdot e = a$;
3. (逆元) 任意 $a \in G$, 都可以找到另一个元素 $b \in G$ 使得 $a \cdot b = b \cdot a = e$.

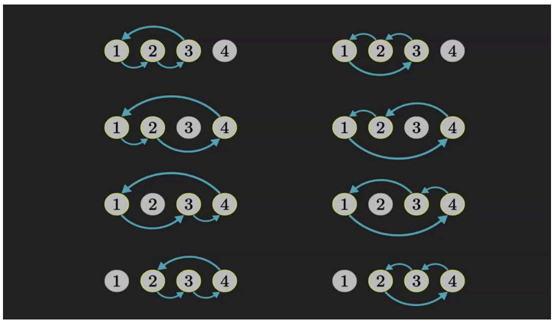
则 $(G, \cdot)$ 被称为是一个群.

4.3　群同构

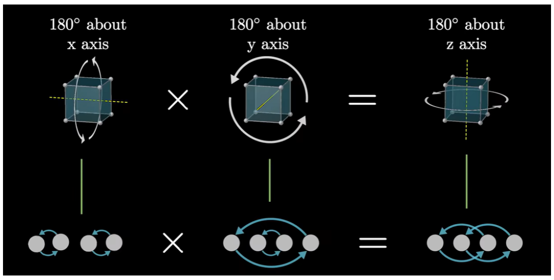
接下来一个很重要的问题是, 这样的抽象是否真有必要? 依然以正六面体为例, 诚然我们不需要借助群就可以凭借几何直观了解其对称性. 但是当我们将其抽象成群以后, 可极大地减少思维上的负担从而发现一些新东西. 另一方面, 高维空间在现实生活中无法实现, 我们的几何直观失效了, 这时候也势必要借助群完成正确的探究. 那么正六面体的对称性对应的群是什么呢? 将正六面体的四条斜对角线取出来, 则任意一种翻转其实就等同于交换其中几条斜对角线.



所以翻转正六面体的对称性给出的群就是四条直线之间的置换群, 即 S_4. 所以我们现在可以将对正六面体对称性的思考, 转换为对 S_4 的思考. 后者当然比前者更加直观. 例如我们可以发现, 有六种置换是很特殊的, 它们自己与自己" 相乘" 三次后, 就相当于" 什么也不做".



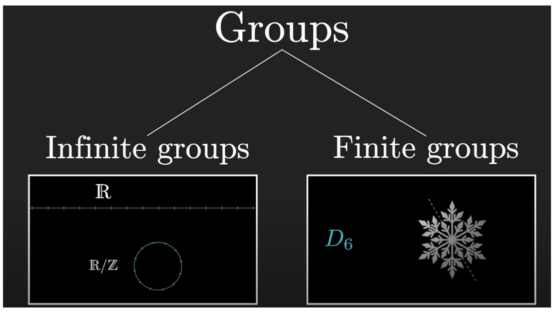
而这六种置换其实对应的就是将正方体以斜对角线为轴旋转 120°. 再比如说先沿着 x-轴旋转 180° 再沿着 y-轴旋转 180°, 效果等同于沿着 z-轴旋转 180°. 这样的乘法关系在置换中也有对应.



所以正方体的对称性所产生的群不仅仅与 S_4 之中的成员一一对应, 而且两个群之间的乘法结构还被完美的保持下来. 这样的对应关系在群论中尤为重要, 称为群同构. 在群论中, 两个同构的群通常就被认为是同一个.

4.4 群分类

群论的一个基本问题是, 如何在同构意义下对所有的群进行分类? 首先可以根据群成员的数量进行一个划分.



为简单起见, 我们这里只介绍有限群的分类. 就像整数理论从素数开始研究一样, 群论也从最基本最不可分解的群——单群 (simple group) 开始研究. 著名的 Jordan–Hölder 定理确保了每一个有限群都可以分解成若干单群.

因此有限群分类问题被细分为: 1. 对所有单群分类; 2. 找出所有单群可能的组合方式.

第一个问题已经被完全解决. 简单来说, 所有单群的种类为 18 个无限族以及 26 个散在群. 这 18 个无限族中包括所有的素数阶循环群, 所有的偶置换群等等, 相对来说比较清楚. 而 26 个散在群又可细分为 20 个成员组成的" 快乐家族" 和 6 个孤儿群. 为什么叫" 快乐家族" 呢? 是因为其余 19 个群都是由一个大家长" 魔群 (Monster group)" 衍生而来. 这个群为什么叫魔群呢? 首先它的阶数很大, 足有 8×10^{53} 之多. 其次, 它所描述的是一个出现于 196,884 维空间中几何体的对称性. 那么 196,884 这个数字就出现的莫名其妙.

后来, J. Mckay 这位数学家在研究模函数 (解析数论中的重要函数) 时, 发现其展开项中出现了这个系数. 他将这个现象告诉了 J.Conway, 并且共同提出了著名的魔群月光猜想. 这一猜想后来被 R.Borcherds 所证明. 而这些数学家们的故事已经远远超出我们的课程范围. 将来同学们的积累足够深厚, 或许有可能再次碰见他们.