群论

数62谭泽睿

本书(小册子)的目的是带领读者了解群并理解群。本书希望以原理性的方式讲述，使读者明白基本的原理，并能理解整个理论，而不是完全的平铺直叙。其中穿插了许多练习，可以帮助读者熟悉概念并检查自己的理解。有一定难度的问题我们用难度星级★ 标示出来了，★的个数代表它们的难度(难度分为0,1,2,3,4,5星)。0星的题目都是可以立即想出来的，读者看几眼就能知道答案的那种。看到0星题目时一定要立即想一想，这可以用于检查对概念的理解，想不出来就应该回顾前面的内容。有些练习事实上是简单而有一定重要性或有用的结论，读者通过自己的思考，可以对它们有更好的理解和印象。

可以搭配我们标配的教材姚慕生老师的《抽象代数学》或是中科大冯克勤老师的优秀教材《近世代数引论》一起学习。

最后更新：2017年7月1日

Contents

CHAPTER 1

对称现象与群

1. 认识对称

在浩瀚无边的宇宙中，存在着无数缤纷复杂的对称现象。对称这个词我们不陌生，比如我们常说圆既是个轴对称图形，又是个中心对称图形，它还是“旋转”对称的；（等边）三角形是轴对称的，它有三条对称轴，不仅如此，事实上我们感觉到：三角形从三个不同的方向看过去，是一样的，这似乎也是一种对称性……那么什么是对称呢？

我们需要把对称现象作一个高度的概括。不难发现，可以以一种统一的方式来重新理解上面的几个例子：对圆作对称轴反射变换、旋转变换，或者是中心对称变换，即映射$(x, y) \mapsto (-x, -y)$，整个圆又回到了原来的样子。对（等边）三角形作对称轴反射变换、120度旋转变换，三角形没有发生变化。

于是我们可以说，所谓某个对象的某种对称，就是指某种变换（映射），它保持整个对象不变。但是一般来说，这种变换要有所限制，通常是只考虑从某个大的比较正常/自然的映射空间中选取一些保持它不变的映射。不能是太烂的映射，要不然可选的映射太多了。对于这整个三角形来说，我们所考虑的仅仅是把它看做不可切割的刚体的变换，那些会割裂三角形的映射按照这种说法也可以看成某种对称，但是我们不予考虑。在这种考虑下，一个（等边）三角形的对称事实上只需要看它的三个顶点1,2,3如何运动。比如$(1, 2, 3) \mapsto (2, 3, 1)$的变换就是某种旋转，而$(1, 2, 3) \mapsto (1, 3, 2)$则是某种轴对称。

1.1. 对称的本质属性. 我们现在用数学抽象的记号来书写我们刚才的讨论。我们首先有一个可能具有某些对称性的对象X，在上面有一些对称，也就是一些变换$T_1, T_2, \ldots$。它们作用在X上使整个X不变，也就是说

$$T_i(X) = X.$$

一个自然的道理是任何对象都有一种对称，其实就是啥也不干。这个啥也不干的恒等映射我们记作1。这是对称的本质属性之一。既然是变换（映射）的话，它们之间必然可以复合，复合运算也必然满足结合律。我们很容易发现，对称之间的复合一定也是对称。用稍微抽象一点的语言来说，这个朴素（这是对称的本质属性之二）的道理就是

$$T_i \circ T_j(X) = T_i(T_j(X)) = T_i(X) = X$$

（后面的大部分时间里，我们将省略复合的符号$\circ$，直接写成T_iT_j.）这个简单的式子说明如何用两个对称来“制造”新的对称：把它们复合起来一定还是X 的对称! 作为最简单的例子，我们还是可以考察一下等边三角形。我们知道，旋转120度的变换可以作用两次，即$\sigma\circ\sigma=\sigma^2$，这事实上是某种旋转240 度的变换。作用三次，这事实上就相当于什么也没干。不妨用σ 来表示旋转（不妨说是逆时针）120度的变换，我们已经发现$\sigma\circ\sigma\circ\sigma=1$即单位映射，这也就是

$$\sigma^3=1$$

值得注意的是，就像映射的复合不一定交换一样，没有任何理由表明对称的复合一定会交换，即不一定有$T_iT_j=T_jT_i$。对称还有一种本质属性。那就是每一种对称变换一定可以反过来进行！也就是任意一种对称T，有一种对应于它的反对称，我们把它记作T^{-1}，称它为T 的逆，使得$T^{-1}\circ T=1$。互逆是相互的关系，你是我的逆，我也是你的逆，所以必须也有$T\circ T^{-1}=(T^{-1})^{-1}\circ T^{-1}=1$。比如说$\sigma$ 的反操作就是顺时针旋转120 度。而这事实上与σ^2无异，这一点可以通过对式子$\sigma^3=1$两边同时复合一个σ^{-1}看出来：

$$\sigma^{-1}\sigma^3=\sigma^{-1}=\sigma^2.$$

如果我们用$S(X)$来表示X上的所有对称变换的集合的话，以上讨论就是说：

(1) $1\in S(X)$.
(2) $a,b\in S(X)\Rightarrow ab\in S(X)$.
(3) $a(bc)=(ab)c$.
(4) $a\in S(X)\Rightarrow$存在a的逆$b\in S(X), ab=ba=1$.

事实上，我们把这样一个集合$S(X)$称为**群**，即X的对称群。

2. 等边三角形的对称群

等边三角形的对称，有旋转，也有轴对称，事实上它有三种不同的轴对称，不妨记其中以纵轴为对称轴的反射变换是τ。也有两种不同的旋转$\sigma,\sigma^2=\sigma^{-1}$ （一个逆时针转120度，一个顺时针转120度），还有一个啥也不干的对称1。如前，我们以1,2,3记三角形的三个顶点（不妨把等边三角形平放，上面的顶点定为1，右下的为2，左下的为3）。那么每一个对称事实上都是一个从$\{1,2,3\}$到$\{1,2,3\}$的映射f。别忘了，作为一个对称，f需要有逆，所以f 得是单满射。这样的f有多少个呢？这只需要决定$f(1),f(2),f(3)$的值就好了。一共有6种可能的排列，所以三角形上最多只能有6个对称！那实际上它有多少个呢？每一个这样的f都是三角形的一个对称吗？的确是！我们将用如下记号

$$\begin{pmatrix}1&2&3\\a&b&c\end{pmatrix}$$

来表示把1映到a，把2映到b，把3映到c的映射。很容易发现

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

别忘了我们说过，对称变换可以复合，我们试着复合一下σ与τ，看看会发生什么？通过计算给出

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

有趣的是这次复合没有产生新的东西，$\sigma\tau$这个对称是另一种轴对称，保持顶点2不变的轴对称。值得注意的是$\sigma\tau \neq \tau\sigma$，读者可以验证这一点。我们可以验证，整个三角形的对称群有如下6个不同的元素：（这刚好构成了{1,2,3}到{1,2,3}的所有单满射。）

$$1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$$

这样一个群具有良好的运算性质：有一个恒等元素1、每个元素都有逆、任何两个元素的复合（也称为元素的乘积）仍然属于这个群，也就是乘法运算具有封闭性。事实上，这个群我们一般记作D_3，叫做二面体群。二面体群这个词事实上包括了一整个系列的群D_n，D_n是指作用在正n边形上的所有对称组成的群。（注：有些书上用D_{2n}记我们这里的D_n，这是记号的差别，不幸的是这两种记号都有广泛使用。）

2.1. 另一个简单的但重要的群的例子：置换群. 我们考虑集合$\{1, 2, \ldots, n\}$，我们研究这个集合的对称。作用在上面的变换是啥呢？就是从它到它自身的所有单满射（必须是单满射，因为对称变换要求有逆）。这个群我们记作S_n，叫做n元置换群。其间的元素称为置换

$$S_n = \{\text{单满射} f : \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}\}.$$

容易知道，$|S_n| = n!$。置换群具有基本的重要性，所以对它引入简单而方便的记号是重要的。我们还是以

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

表示置换。特别的，我们把如下置换形状的置换

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n & b_1 & \ldots & b_k \\ a_2 & a_3 & \ldots & a_1 & b_1 & \ldots & b_k \end{pmatrix}$$

称为轮换，把它记为$(a_1 a_2 a_3 \ldots a_n)$。可以有长度小于n的轮换，比如(12)表示把1映到2，把2映到1，其它元素不动的轮换。

2.1.1. 置换的轮换表示. 一个有趣的事实是每个置换事实上都可以用轮换的乘积（复合）表示出来! 为了从一个置换得到它的轮换表示，只需要这样操作：它可能把a_1映到a_2,把a_2映到a_3,……这样下去直到又把某个a_k映回a_1，我们就找到了一个轮换$(a_1a_2\dots a_k)$。再从这个轮换没有包含的某一个元素出发，让f 不停地作用在它身上，直到循环，得到另一个轮换$(b_1b_2\dots b_l)$，以此类推，我们最终能把该置换的所有元素穷尽，得到

$$f=(a_1a_2\dots a_k)(b_1b_2\dots b_l)\dots$$

并且，表达式中所出现的轮换之间没有公共元素(故此时这些轮换复合(乘积)的顺序不重要)。比如，我们可以得到这个置换的轮换表示：

$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(14)(23)=(23)(14)$$

只需要发现$1\mapsto 4\mapsto 1$,$2\mapsto 3\mapsto 2$.

练习1. 计算$(12)(34)(13)(24)$,直接将它表为不相交轮换的乘积。

练习2. 将置换

$$\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$$

写为不相交的轮换乘积。

3. 对称的本质框架：群

一个群本质上是指作用在某种对称物件X上的所有对称变换的集合$S(X)$，这集合满足如下性质

(1) $1\in S(X)$.
(2) $a,b\in S(X)\Rightarrow ab\in S(X)$.
(3) 乘法满足结合律，$a(bc)=(ab)c$.
(4) $a\in S(X)\Rightarrow$存在a的逆$b\in S(X), ab=ba=1$.

事实上，抽象地考察群，我们可以发现其运算结构与X并没有什么关系，其所有运算信息完全包含在了乘法运算里。以上条件是所有对称现象都具有的，为了研究宇宙中所有的对称现象的本质结构，我们不妨去繁就简，作出如下定义

定义1.1. 一个**群(Group)**是指一个集合G以及上面附带的一种二元运算$\cdot: G\times G\to G$称为乘法，满足：

(1) $a,b\in G\Rightarrow ab\in G$
(2) 存在一个元素$e\in G$(称为幺元素)，它满足对任意元素$a\in G$都有$ea=ae=a$.
(3) 对任意的$a\in G$，存在$b\in G$，称为a的逆，满足$ab=ba=e$.

(4) 乘法满足结合律，对任意的$a, b, c \in G$有$(ab)c = a(bc)$.

特别地，如果这个运算还满足交换律，$ab = ba$，则称它为**Abel群(Abelian Group)**。

练习3. 验证在一个群中，幺元素是唯一的。一个元素的逆也是唯一的。

在这个群的定义里我们没有提到任何对称变换，甚至只看这个定义的话看不出来这是要干什么[1]，还以为这只是某种运算封闭的集合。群确实也可以代表这种运算封闭的集合，比如说全体整数在加法运算下成群。（事实上，这种运算封闭的集合，比如全体整数在加法下成的群，也是某种对称变换：它是作用在整数集上的所有平移变换。）但请记住群的由来，和群最本质的属性是对称。这样一来，研究了所有群，我们就相当于研究了作用在任何可能的物件/对象上的所有可能的对称。

我们只研究有限群，即元素个数有限的群。我们称一个群的元素个数为这个群的**阶数**。在第二章我们会为大家证明，对于每个有限群，都可以构造一个对象X，使得这个群恰好是该对象的对称群，也即，每个群都是对称群。所以说群的本质是对称：群即对称，对称即群!

3.0.2. *群的一些例子*. 除了我们已经介绍的S_n与D_n以外，还有一些简单的群。最简单的群的例子应该是$\mathbb{Z}$，即全体整数在加法下组成的群，我们可以把这个群想象成全体整数的平移对称群。容易验证，全体偶数在加法下也成群。事实上，全体n的倍数在加法下都能组成群（因为n的倍数在加法下封闭）。

如果我们把D_n中的所有旋转$\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$拿出来单独组成一团，容易验证这也构成一个群（因为旋转之间的复合还是旋转），这种群也是最基本的群之一，我们把它记作$\mathbb{Z}_n$，叫它n 阶循环群[2]，这是一个Abel群。

关于循环群，事实上还有另一种算术的描述：全体整数按照模n分成n 个不同的剩余类，就是按除以n之后的余数分别为$0, 1, 2, \ldots, n-1$划分为n类。剩余类之间可以进行加法运算，比方说在模5下，有$2 + 4 = 1$.这样，这些不同的剩余类按加法就组成了一个群，这个群看起来跟之前的$\mathbb{Z}_n$好像是不同的，因为一个是旋转变换$\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$，一个是剩余类$\{0, 1, 2, 3, \ldots, n-1\}$。但是不难看出这两个群在结构上没有什么本质上的区别，也即如果我们把剩余类k与σ^k等同起来，两边进行的任何群运算都是一样的。这也就是说，在一个对应f下

$$f : \{0, 1, 2, 3, \ldots, n-1\} \to \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$$
$$k \mapsto \sigma^k$$

[1]一般的书从一开始就只写了这个定义，这对初学者来说容易带来困难，初学者会以为群就是一种集合上面带有一种运算，满足一些不知道为什么的定义，他们需要花很长时间才能认识到群代表的实际上是对称。

[2]也记为C_n或$\mathbb{Z}/n\mathbb{Z}$.

左边的各种运算可以与右边对应的元素的对应运算相对应。这时，我们说这两个群**同构**。同构的群没有本质的区别，可以视为同一个。关于同构的具体描述将在下一章给出。

练习4. 考虑由所有n次单位根$\{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\}$，验证它在通常的复数乘法下组成一个群，也即验证它满足群的定义。这个群跟$\mathbb{Z}_n$ 同构吗？

CHAPTER 2

群的基本结构

本章我们用简单的方法探索群[1]的基本结构。

1. 元素上的结构信息

1.1. 元素的阶数. 设$g \in G$，如果有正整数n使得$g^n = 1$，那么我们说g是有限阶的，把最小的这样的正整数n称作g的阶，否则说它是无限阶的。对于有限群G来讲，任一个元素$g \in G$，不停地作乘法，得到序列$g, g^2, g^3, \ldots$ 由于G 有限，这个序列一定会重复，不妨设$g^k = g^l, k > l$，那么有$g^{k-l} = 1$。也即有限群中任何元素都是有限阶的。

练习5. 设g是G中的n阶元素并且$g^N = 1$.证明N是n的倍数。

命题2.1. 设g是群G中的n阶元素，那么g^m的阶数是$\frac{n}{(m,n)}$，其中(m,n)表示m,n的最大公因数。

Proof. 首先由$(g^m)^{\frac{n}{(m,n)}} = g^{\frac{mn}{(m,n)}} = 1$我们知道，$g^m$的阶数$\leq \frac{n}{(m,n)}$.而若有$(g^m)^k = 1 = g^{mk}$，则必有$mk$是$n$的倍数，因此$k$必然是$\frac{n}{(m,n)}$的倍数。这就表明了$g^m$的阶数一定是$\frac{n}{(m,n)}$. □

在Abel群中，如果已知a, b的阶数，那么ab的阶数就被约束住了。

练习6. 设G是$Abel$群，$a, b \in G$阶数分别为m, n，则ab的阶数是$[m, n]$的因数。

练习7 (★)**.** 如上题，若还有m, n互素，证明ab的阶数就是mn.

值得注意的是，对于非Abel群，仅仅已知a, b的阶数是不能得到与ab 阶数有关的任何信息的，可以证明存在群使得ab的阶数取到任意给定的正整数。

练习8 (★)**.** 证明，如果一个群中只有$1, 2$阶元素，那么这个群是$Abel$群。

练习9 (★)**.** 设G是一个偶数阶群，则$g^2 = 1$有偶数个解。由此知群G中一定有二阶元素。

[1]我们基本上只讨论有限群。

2. 子群与商结构

不难发现，D_6，即正六边形的对称群，里面也包含了正三角形的所有对称!比方说旋转120度的对称，这个在正六边形的对称群里也有。三角形的三条轴对称也构成正六边形的三条轴对称，当然正六边形有更多轴对称（反射对称）。这种时候我们说D_3是D_6的子群[2]。数学的历史告诉我们，研究一个结构的子结构是重要的：我们作出如下定义

定义2.1. 设G是一个群，$S \subset G$是一个子集，若它在群G的乘法下仍然满足群的定义性质，则称S是G的一个**子群**。记为$S \leq G$。

我们有很多子群的例子，比方说全体偶数的加法群$2\mathbb{Z}$就是$\mathbb{Z}$的一个子群。再比如说，$\mathbb{Z}_6 = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$有子群$\{1, \sigma^2, \sigma^4\}$ 和子群$\{1, \sigma^3\}$，其实就是$\mathbb{Z}_3$和$\mathbb{Z}_2$.

例2.1. $\{1, (12)(34), (13)(24), (14)(23)\}$构成$S_4$的一个子群，叫做$Klein$ 四元群，有时它记作V或$\mathbb{Z}_2^2$.这个群是$Abel$群，但是跟同阶的$Abel$ 群$\mathbb{Z}_4$不同构。

练习10. 证明，子群的(任意)交仍然是子群。

2.1. 陪集与拉格朗日定理. 设G是一个群，给定了它的一个子群$H \leq G$后，我们可以在群G上规定一个等价关系：

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

由于H本身是个群，容易验证这样确实定义了一个等价关系[3]，按照这个等价关系，整个群G 划分成一些不相交的等价类的并。容易发现，与b等价的元素的全体就是bH，因为$b \sim a \Leftrightarrow b^{-1}a \in H \Leftrightarrow a \in bH$. 这样，所有的等价类都形如$bH$，并且它们的大小相等，都是$|bH| = |H|$. 我们称形如$bH$ 这样的子集叫做G关于H的左陪集，简称陪集[4]。我们以$[G : H]$ 记这个等价关系下，等价类的个数，也即陪集的个数，称它为子群H的**指数(index)**.我们有

$$G = \bigcup_{i=1}^{[G:H]} b_i H$$

由于不同的等价类不相交，那么我们已经得到了

定理2.1 (拉格朗日定理)**.** 设H是群G的子群，那么

$$|G| = [G : H]|H|$$

---

[2]严格来说，是D_3同构于D_6 的一个子群

[3]一个关系$\sim$称作等价关系，如果它满足自反性$a \sim a$，对称性$a \sim b \Leftrightarrow b \sim a$ 和传递性$a \sim b, b \sim c \Rightarrow a \sim c$.

[4]也可以定义右陪集。但为了方便，本书统一使用左陪集。

推论2.1. 设$A \leq B \leq G$.则有$[G:A] = [G:B][B:A]$.

这个定理还表明，子群的阶数一定是$|G|$的因数。比方说，借助拉格朗日定理，我们就能知道12阶群一定没有5阶子群。

例2.2. 对于群

$$D_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

以及它的子群$H = \{1, \sigma, \sigma^2\}$，我们有如下陪集分解：

$$D_3 = H \cup \tau H.$$

此时有$[D_3 : H] = 2$.

练习11. 设$H \leq G$.证明$g \in H \Leftrightarrow gH = H$，从而得知$a \sim b \Leftrightarrow aH = bH$.

定理2.2. 设$g \in G$是有限群G中的一个n阶元素，那么n是$|G|$的因数。

Proof. 由于g是n阶元素，我们很容易验证，$H = \{1, g, g^2, \ldots, g^{n-1}\}$构成$G$的一个$n$阶子群，因而由拉格朗日定理知一定有$n$是$|G|$的因数。 □

2.2. 商群与正规子群. 就像线性空间(向量空间)可以对子空间构作商空间一样，群也存在商结构。

给定$H \leq G$，我们试图把陪集集合$G/H = \{H, b_1H, \ldots, b_{k-1}H\}$ 看成一个群，我们所期望的群运算是这样的：

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

不幸的是，对于某些子群H，这个等式不成立。也就是说，不是所有子群都可以用来构作商群G/H。我们作如下推理：$(aH)(bH) = (ab)H \Leftrightarrow HbH = bH \Leftrightarrow (b^{-1}Hb)H = H \Leftrightarrow b^{-1}Hb \subset H \Leftrightarrow b^{-1}Hb = H$ 所以，若要构作商群G/H，子群H必须满足条件：$\forall b \in G, b^{-1}Hb = H$，这引出如下定义：

定义2.2. 设$N \leq G$，若

$$\forall g \in G \quad g^{-1}Ng = N$$

则称N是G的**正规子群**，记作$N \triangleleft G$.如果一个群G除了1和G以外没有别的正规子群，则称G为**单群**。

例2.3. 若G是$Abel$群，则G的任何子群都是正规子群。

例2.4. 我们有$\mathbb{Z}_3 \triangleleft D_3$，这只需验证$\tau^{-1}\sigma\tau = \sigma^{-1}$.容易看出$\{1, \tau\}$是$D_3$的子群，但$\{1, \tau\}$并不是$D_3$的正规子群，因为$\sigma^{-1}\tau\sigma = \sigma^2\tau \notin \{1, \tau\}$.

例2.5. 我们有$\{1, (12)(34), (13)(24), (14)(23)\} = V \triangleleft S_4$.这一点在我们谈到置换群的共轭概念后大家能马上得到。

值得注意的是，正规子群不具有传递性，即$A \triangleleft B \triangleleft C$推不出$A \triangleleft C$.反例将在后面的学习中给出。

练习12. 设$N \leq H \leq G$并且$N \triangleleft G$.证明$N \triangleleft H$.

练习13. 证明：$N \triangleleft G$等价于说对任意的$g \in G$有$Ng = gN$.

练习14 (★). 设$M, N \triangleleft G$且$M \cap N = \{1\}$，证明M和N之间的元素可交换。即$\forall m \in M, n \in N$有$mn = nm$.

练习15 (★). 设$H \leq G$且$[G : H] = 2$.证明$H \triangleleft G$.

练习16 (★). 找出所有的有限交换单群。

2.3. 子群之间的乘积. 设$N, H \leq G$.我们记集合

$$NH = \{nh | n \in N, h \in H\} \subset G.$$

这个集合在大群G赋予的运算下，能成一个群吗？答案是不一定。但是当N或H至少有一个是正规子群时这是对的。不妨设$N \triangleleft G$，我们计算

$$n_1h_1n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 \in NH$$

$$(n_1h_1)^{-1} = (h_1^{-1}n_1^{-1}h_1)h_1^{-1} \in NH$$

$$1 \in NH$$

而群NH的结合律也以从大群中的结合律遗传过来，因而此时NH构成子群。

另外，就算N,H中没有一个是正规子群，通过运用陪集分解的方法我们仍然能够计算集合NH中的元素个数。

命题2.2. 设$A, B \leq G$,则有

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Proof. 显然，AB可以写成一些不相交的关于B的陪集的并(尽管AB可能不是子群),我们有

$$AB = \bigcup_{a \in A} aB$$

另外，对B作关于子群$A \cap B$的陪集分解有

$$A = \bigcup_{a \in A} aA \cap B$$

我们发现，

$$a_1B = a_2B \Leftrightarrow a_1^{-1}a_2 \in B \Leftrightarrow a_1^{-1}a_2 \in A \cap B \Leftrightarrow a_1A \cap B = a_2A \cap B$$

也就是说，AB关于B的陪集个数等于A关于$A\cap B$的陪集个数，所以有

$$\frac{|AB|}{|B|}=\frac{|A|}{|A\cap B|}.$$

(这个等式与线性代数中的第二同构定理是否很相似？) □

练习17 (★★)**.** 设$A,B\leq G$.证明

$$[G:A\cap B]\leq[G:A][G:B].$$

特别的，如果$[G:A]$与$[G:B]$互素，证明等号一定成立，并且有$G=AB$.

练习18 (★★)**.** 设$A,B\subset G$是子集(注意，没说是子群)，如果$|A|+|B|>|G|$，证明一定有$G=AB$.

3. 群映射

线性空间之间的映射一般只考虑与其线性结构有关的线性映射。而群与群之间的映射也是这样，一般只考虑与其群结构有关的群映射，我们要找的这群映射便是群同态。

定义2.3 (群同态)**.** 设G,H都是群，$f:G\to H$是映射，若

$$f(ab)=f(a)f(b)$$

则称f是**群同态**，简称同态。若f是单射，则称它为单同态。若f是满射，则称满同态。若f既是单同态又是满同态，则称f是一个**同构**，称G和H是**同构**的，记作$G\cong H$.

值得注意的是，在等式$f(ab)=f(a)f(b)$中，ab所用的是群G中的乘法运算，而$f(a)f(b)$处所用的是群H中的乘法运算。

例2.6. 如第一章，通过对三角形顶点编号，我们发现事实上有$S_3\cong D_3$. 对于$n>3$，S_n与D_n并不相同。

例2.7. 一个群同构于它自身。这只需要取$f(g)=g$即可。有趣的是一个群可以有不同于恒等映射的同构映射，比如

$$f:\mathbb{Z}_3\to\mathbb{Z}_3$$
$$g\mapsto g^2$$

就是一个同构映射，但它不同于恒等映射，我们把它称为$\mathbb{Z}_3$的自同构。事实上，这种同构映射的存在说明了群G的结构本身具有某种对称性，而群G的所有自同构，也就是作用在G上的所有对称变换，也构成一个群，称为G的自同构群，记作$\mathrm{Aut}(G)$.

练习19. 验证同态一定把G中的1对应到H中的1，把g^{-1}对应到$f(g)^{-1}$，也就是说$f(1)=1$以及$f(g^{-1})=f(g)^{-1}$.

练习20. 验证$\mathbb{Z}_4$有一个二阶子群，并证明它对这个二阶子群的商群同构于$\mathbb{Z}_2$.

练习21. 设g是n阶元素，证明$f(g)$必是有限阶元素，而且阶数是n的因数。

练习22. 求出$\mathrm{Aut}(\mathbb{Z}_4)$.

定义2.4 (核与像)**.** 设有群同态$f:G\to H$，我们称集合

$$\ker f=f^{-1}(1)=\{g\in G|f(g)=1\}$$

为f的核，集合

$$\mathrm{Im}f=\{f(g)|g\in G\}$$

为f的像。

值得注意的是$\ker f$和$\mathrm{Im}f$分别是G和H的子群，而且事实上有$\ker f\triangleleft G$.

练习23. 证明

(1) $\ker f=\{1\}\Leftrightarrow f$是单射。
(2) $\ker f\triangleleft G$.

练习24 (★)**.** 找出所有的阶数≤ 5的群。包含只有一个元素的平凡群在内，阶数不超过5的群一共有6个。*(同构的群视为同一个)*

3.1. 简单重要而典型的群映射.

3.1.1. 单同态. 最简单的群映射应该属于单同态。一个单同态$f:H\to G$本质上是把H 给对应到了G中的一个子群$f(H)\leq G$，而$f(H)$与H是同构的。换而言之，单同态就是把H以同构的方式“塞”进了G.

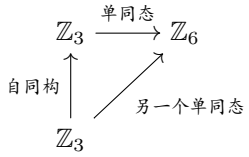
例2.8. 考虑群的单同态

$$f:\mathbb{Z}_3=\{1,a,a^2\}\to\mathbb{Z}_6=\{1,b,b^2,b^3,b^4,b^5\}$$

容易发现，这个同态完全被$f(a)$的值确定下来了，因为$f(1)=1$而$f(a^2)=f(a)^2$.由于a是3阶元素，$f(a)$必须是1或3阶元素。$\mathbb{Z}_6$中的三阶元素只有b^2,b^4。因此我们知道，$f(a)$只可能取$1,b^2,b^4$。由于我们只考虑单同态，可能的选择只剩下两个：$f(a)=b^2$或$f(a)=b^4$.

如果$f(a)=b^2$，那么就有$f(a^2)=b^4$，整个群$\mathbb{Z}_3=\{1,a,a^2\}$被映射成了$\{1,b^2,b^4\}$。如果选择$f(a)=b^4$，那么就有$f(a^2)=(b^4)^2=b^8=b^2$，整个群$\mathbb{Z}_3=\{1,b^4,b^2\}$.我们知道$\{1,b^2,b^4\}$是$\mathbb{Z}_6$的同构于$\mathbb{Z}_3$的子群，但是却有两种不同的将$\mathbb{Z}_3$嵌入到$\mathbb{Z}_6$的方式。但在任何一种方式下，这个单同态都建立了$H$与$f(H)$的同构。尽管$G=\mathbb{Z}_6$中只有一个子群同构于$H=\mathbb{Z}_3$，但之所以会有多种不同的将$H$ 嵌入到$f(H)$ 的方式，

是因为存在从H 到H 的自同构$(1, a, a^2) \mapsto (1, a^2, a)$.换而言之，这种现象发生是因为$H$自身具有的对称性导致的。



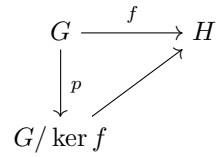
3.1.2. 投射与同态的分解. 另一种简单而重要的映射是投射。我们说过，对于群G的正规子群N，可以构作商群G/N.我们可以考虑一种把G中的元素g对应到G/N中g所在的陪集的自然的映射

$$p : G \to G/N$$
$$g \mapsto gN$$

这个映射显然是同态，因为$p(ab) = abN = aNbN = p(a)p(b)$.而且还是满同态。那它的核是什么呢？回忆商群$G/N$中的单位元素就是$N$，也即$G$ 中的单位元素所在的陪集，因此$p(a) = aN = N \Leftrightarrow a \in N$，我们得出$\ker p = N$.

投射的重要性和基本性在于，对于任何同态$f : G \to H$ 我们去考虑这个同态的$\ker f$.一件值得注意的事情是，$a^{-1}b \in \ker f$等价于说$f(a^{-1}b) = 1 \Leftrightarrow f(a) = f(b)$.换而言之，若是把$G$对$\ker f$作商群(也即陪集分解)，每个陪集$b\ker f$的中的元素都被$f$映射到同一个$f(b)$，而不同的陪集一定被映射到了不同的元素(因为只要两个陪集$a\ker f$和$b\ker f$被映射到了相同的元素，就有$f(a^{-1}b) \in \ker f \Leftrightarrow a\ker f = b\ker f$).既然$a\ker f$中所有元素都被映为同一个$f(a)$(给我们一种浪费的感觉)，不如定义一个新映射，把$a\ker f$视为商群中$G/\ker f$的一个元素，让它对应到$f(a)$.

换而言之，我们发现，任何具有$\ker f$的同态$f : G \to H$都可以分解成两个映射的复合：



这个图的意思就是我们可以将映射$a \mapsto f(a)$对应成两步：$a \mapsto a\ker f \mapsto f(a)$.第一步是将$a$对应到它所在的陪集$a\ker f$(即从$G$向$G/\ker f$ 的自然投射)，第二步是将$a\ker f$ 映射到$f(a)$.唯一可能存在的问题是第二部映射是不是一个同态？答案是是。验证这一点是极为容易的。任何群映射可以分解成两种基本映射的复合：即一个投射，和一个单同态的复合。顺便，事实上我们可以在这个基础上再加一步，也是最水的一步：$a \mapsto a\ker f \mapsto f(a) \mapsto f(a)$,也即先将$f(a)$映入$H$的子群$\mathrm{Im} f$，再

将$\mathrm{Im}f$通过平凡单射对应到H.

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow{\cong} & \mathrm{Im}f \end{array}$$

这样，第二步$G/\ker f \to a\ker f \mapsto f(a)$就是一个同态且是单满射，因此是同构。于是我们得出，我们得出了如下重要的定理：

定理2.3 (同态基本定理)**.** *若$f : G \to H$是同态，那么$\ker f \lhd G$,$\mathrm{Im}f \leq H$且有同构*

$$G/\ker f \cong \mathrm{Im}f$$

Proof. 如上，构作映射

$$h : G/\ker f \to \mathrm{Im}f$$
$$a\ker f \mapsto f(a)$$

易验证这个映射的定义是良好的，因为只要$b\ker f = a\ker f$就有$f(b) = f(a)$. 现在来证明这是同态：

$$h((a\ker f)(b\ker f)) = h(ab\ker f) = f(ab) = f(a)f(b)$$

第一个等号是因为$\ker f$正规。h是单射，因为$h(a\ker f) = f(a) = 1 \Leftrightarrow a \in \ker f$. 另外，$h$显然是满射，故$h$是同构。 □

4. 同构定理

同态基本定理又叫第一同构定理。由同态基本定理我们很容易导出许多同构定理，它们和我们在线性代数中学过的同构定理是类似的。

定理2.4 (第二同构定理)**.** *设$N \lhd G$且$H \leq G$.则有$N \lhd NH$且$N \cap H \lhd H$并且有*

$$NH/N \cong H/N \cap H$$

Proof. 由于$N \lhd G$以及$N \leq NH \leq G$容易得出$N \lhd NH$.现在对任意的$n \in N \cap H, h \in H$有

$$h^{-1}nh \in N \cap H$$

故$N \cap H \lhd H$. 现在，构作映射

$$f : H \to NH/N$$
$$h \mapsto hN$$

先证明这个映射是同态。因为$N \lhd NH$,我们有

$$f(ab) = abN = aNbN = f(a)f(b).$$

这显然是个满同态。现在我们计算$\ker f$，设$h \in \ker f$，则

$$hN = N \Leftrightarrow h \in N \Leftrightarrow h \in N \cap H$$

故$\ker f = N \cap H$.现在同态基本定理给出

$$H/N \cap H \cong NH/N.$$

□

5. 循环群，生成元与群的表现

循环群是最简单、最基本的一类群，但仍然十分重要。循环群$\mathbb{Z}_n$有多种描述方法，比如可以描述成正n边形的旋转变换群，也可以描述成模n的余数类的加法群。循环群的本质特点是，它可以仅由一个元生成。这就是说，可以找到其中一个元素a，通过不断的作逆a^{-1}和乘法$1, a, a^2, a^3, \ldots$可以得到群G 中的所有元素。我们把话说得更明白一点：

定义2.5. 设G是一个群，$S \subset G$是G的一个子集。则G中所有包含S的子群的交，也即包含S的最小子群，称为由S生成的子群，记为$\langle S \rangle$. 如果$G = \langle S \rangle$ ，则称G是由S生成的群，称S是G的一组**生成元**。若一个群可由其中一个元素生成，即存在$a \in G$使得$G = \langle a \rangle$，就称G是**循环群**。

按照这个定义，除了有限循环群$\mathbb{Z}_n$以外，可以有无限循环群，而那本质上就是$\mathbb{Z}$.

于是，循环群$\mathbb{Z}_n$可以想象成一个由抽象字母a生成的，满足关系$a^n = 1$的群，这种用生成元与约束关系描述群的方法叫做**群的表现**，这个例子我们记作

$$\mathbb{Z}_n = \langle a | a^n = 1 \rangle.$$

例2.9. 类似的，我们容易想象，群D_3可以抽象地描述成由抽象字母σ和τ生成，满足约束关系$\sigma^3 = \tau^2 = 1$以及$\sigma\tau = \tau\sigma^{-1}$ 的群。我们可以试试列出一系列这两个字母生成的元素

$$1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$$

在群D_3这个特例中，任何抽象字母生成的元素，比如$\sigma\tau\sigma^2$，都可以写成上面的形式，也即$\tau^i\sigma^j$的形式。这是因为

$$\sigma\tau\sigma^2 = \tau\sigma^{-1}\sigma^2 = \tau\sigma.$$

我们把这记为

$$D_3 = \langle \sigma, \tau | \sigma^3 = \tau^2 = (\sigma\tau)^2 = 1 \rangle$$

(条件$\sigma\tau = \tau\sigma^{-1}$可以简化为$(\sigma\tau)^2 = 1$).这容易推广成一般的$D_n$的定义

$$D_n = \langle \sigma, \tau | \sigma^n = \tau^2 = (\sigma\tau)^2 = 1 \rangle.$$

这个定义是抽象的，它完全没有涉及对称，却把群的结构简单明了地确定下来了!

练习25. 接上例，请计算

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

本节的描述算是启发性，非正式的。我们今后会严格地对待这种群的表示方法。

n阶循环群有多少个生成元？问题的答案是明显的，设a是一个生成元，则a^i是生成元当且仅当i与n互质。也就是说，一共有$\varphi(n)$个生成元，这里$\varphi(n)$表示$1,2,3,\ldots,n$中与n互素的数的个数，也即数论中的欧拉函数。关于这个欧拉函数，有一个有趣的恒等式

$$\sum_{d|n}\varphi(d)=n$$

其中求和号$\sum_{d|n}$表示对n的所有正因数d求和。这个等式可以由如下观察得出：对于每一个$d|n$,循环群$\mathbb{Z}_n$中有且仅有一个d阶子群，而这d阶子群的生成元有$\varphi(d)$个。每个$g\in\mathbb{Z}_n$都恰好是某一个$\mathbb{Z}_d$的生成元。

关于循环群，有一个刻画了循环群的性质的重要命题：

定理2.5. 设G是有限群。若对$n=|G|$的任何因数d，G中至多只有一个d阶子群，则G是循环群，反之显然也成立。

Proof. 注意到，任何$g\in G$都有一个由它生成的循环子群$\langle g\rangle$。由假设，这个阶数的子群至多只有一个。对于$d|n$若有一个d阶循环子群，则记它的生成元集合为$\mathrm{gen}(d)$，若没有，则令$\mathrm{gen}(d)$表空集。由于任何$g\in G$都是某个d阶循环群的生成元，我们有

$$G=\bigcup_{d|n}\mathrm{gen}(d)$$

而d阶循环群有$\varphi(d)$个生成元，因此

$$n\le\sum_{d|n}|\mathrm{gen}(d)|\le\sum_{d|n}\varphi(d)=n$$

我们发现等号成立，故对每个$d|n$它恰有一个d阶循环子群，这对$d=n$也是对的，因此它是循环群。 □

练习26 (★). *(没有听说过域的可以跳过)*证明，域F的乘法群$F^\times=F\backslash\{0\}$的任何有限子群必是循环群。

6. 置换群与共轭

置换群是有限群中最重要的一类群，说是最基本也不为过，原因是：置换群事实上包含了所有的有限群，即任何有限群都是置换群的某个子群！(这一点我们将在后面给出)

6.1. 置换的结构与共轭. 置换群的基本要素当然是置换。对于置换来说，置换的(不相交的)轮换分解最能体现出它的结构。我们知道，每个置换都有一个不相交轮换的乘积分解，而且可以有很多轮换分解，但事实上，其中那个置换的不相交轮换分解在不记轮换之间的次序之下是唯一的。这一点比较直觉，证明只需用归纳法，没有太多可说的。

命题2.3. *每个$\alpha \in S_n$都有不相交的轮换$\beta_1, \ldots, \beta_k$使得*

$$\alpha = \beta_1 \ldots \beta_k.$$

而且这种分解是唯一的，在不记次序的情况下。

Proof. 设α有两个不相交的轮换分解

$$\alpha = (\alpha_{11} \ldots \alpha_{1k_1})(\alpha_{21} \ldots \alpha_{2k_2}) \ldots$$

$$\alpha = (\beta_{11} \ldots \beta_{1l_1})(\beta_{21} \ldots \beta_{2l_2}) \ldots$$

如果α移动了α_{11},那么α_{11}就会出现在另一个轮换分解式中的某个轮换中，不妨设$\beta_{11} = \alpha_{11}$. 让α不停地作用在α_{11}上，依次得到$\alpha_{11} = \beta_{11}$,$\alpha_{12} = \beta_{12} \ldots$显然必然有这两个分解式的第一个轮换相等。两个式子同时乘以该轮换的逆，我们得到一个轮换个数更少的式子。重复这个过程，不难得到命题。 □

于是每个置换都有一种唯一的轮换结构，比如说(123)(45)和(234)(15)具有相同的轮换结构，只是数字不同而已。我们说它们的轮换结构是$2 \cdot 3$.类似的，设α的轮换分解中长度为k的轮换有m_k个，则我们说它的轮换结构是$2^{m_2} \cdot 3^{m_3} \ldots k^{m_k}$.

具有相同的轮换结构就像是矩阵具有完全相同的约当块一样，可以通过“换基”来实现“相似”，比如

$$(123)(45) = \sigma^{-1}(234)(15)\sigma$$

其中$\sigma = (14)$.这种现象我们称之为共轭：

定义2.6. 对于$a, b \in G$,若有$g \in G$使得

$$a = g^{-1}bg$$

我们称a与b在G中共轭。易验证共轭是一个等价关系。只与自己共轭的元素[5]我们称为中心元素，所有中心元素记为$C(G)$ 或$Z(G)$,称为群G的中心.

练习27. *证明群G的共轭类个数等于$|G|$当且仅当G是Abel群。*

练习28. *设$g \in G$是某个固定的元素，验证，共轭映射*

$$f_g(a) = g^{-1}ag.$$

是群G的自同构。

[5]也即与其它所有元素都交换的元素

练习29 (★). 接上一题，我们于是有从G到$\mathrm{Aut}(G)$的映射

$$i : G \to \mathrm{Aut}(G)$$

$$g \mapsto f_g$$

验证这也是一个群同态。证明$\ker i = Z(G)$从而得知$Z(G)$是G的正规子群。
记$\mathrm{Im}i = \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$,称它为群$G$的内自同构群，于是由同态基本定理

$$\mathrm{Inn}(G) \cong G/Z(G).$$

作为给大家看的一个例子，我们证明一个有用的命题。

命题2.4. 若$G/Z(G)$是循环群，则G是*Abel*群。

Proof. 设a是循环群$G/Z(G)$的一个生成元在G中的原象，可作G关于$Z(G)$的陪集分解

$$G = \bigcup_{i=0}^{n-1} a^i Z(G)$$

故每个元素形如$a^i z$，显然有$a^i z_1 a^j z_2 = a^j z_2 a^i z_1$. □

练习30 (★). 证明，若$\mathrm{Aut}(G)$是循环群，则G是*Abel*群。

练习31 (★). 设$|G| = p^2$,其中p是素数，证明G是*Abel*群。

练习32 (★★★★). 设$\alpha \in \mathrm{Aut}(G)$，令$I = \{g \in G | \alpha(g) = g^{-1}\}$.证明：若

$$|I| > \frac{3}{4}|G|$$

则G是*Abel*群。

那么，既然共轭是一个群上的等价关系，群中的元素自然就会划分为一些等价类，这些等价类就称作共轭类。一般来说，群的共轭类的情况比较复杂，但是对于S_n 情况比较简单。

练习33 (★). 求D_5的共轭类个数。

练习34 (★★★). 设$p > 2$是素数，求D_p的共轭类个数。

定理2.6. 两个置换$\alpha, \beta \in S_n$在S_n中是共轭的，当且仅当它们具有相同的轮换结构。

Proof. 设有两个具有相同轮换结构的置换

$$\alpha = (\alpha_{11} \dots \alpha_{1k_1})(\alpha_{21} \dots \alpha_{2k_2}) \dots$$

$$\beta = (\beta_{11} \dots \beta_{1k_1})(\beta_{21} \dots \beta_{2k_2}) \dots$$

显然可作置换σ使得$\sigma(\alpha_{ij}) = \beta_{ij}$.则有

$$\alpha = \sigma^{-1}\beta\sigma.$$

这等式可用下图[6]表示(其中若$j = k_i$，下标$i(j+1)$应理解为$i1$.)

$$\begin{array}{ccc} \alpha_{ij} & \xrightarrow{\alpha} & \alpha_{i(j+1)} \\ {\scriptstyle\sigma}\downarrow & & \uparrow{\scriptstyle\sigma^{-1}} \\ \beta_{ij} & \xrightarrow{\beta} & \beta_{i(j+1)} \end{array}$$

由共轭推出轮换结构相同也是简单的，设α定义如上，则有

$$\gamma\alpha\gamma^{-1} = (\gamma(\alpha_{11})\dots\gamma(\alpha_{1k_1}))(\gamma(\alpha_{21})\dots\gamma(\alpha_{2k_1}))\dots.$$

□

容易看出，一个群G的子群H若是正规子群的话，那H一定是由一些完整的共轭类拼成的。反之，把一些共轭类拼起来，如果恰好也成一个子群的话，这个子群就是正规子群。

练习35. 好好想一想上面那句话，并证明

$$\{1, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4.$$

练习36 (★). 设p是$|G|$的最小素因子。证明若有p阶子群$A \triangleleft G$,则必有$A \leq Z(G)$.

6.2. 置换的奇偶性. 置换有奇置换和偶置换之分，用符号$\mathrm{sgn}\sigma$来表示：奇置换是-1,偶置换是1.置换的符号$\mathrm{sgn}\sigma$我们并不陌生，在线性代数中已经碰过了，它可以定义为-1 的逆序数次方，也可以定义为使如下等式成立的函数。

$$\prod_{1\leq i\leq j\leq n}(X_{\sigma(j)} - X_{\sigma(i)}) = \mathrm{sgn}\sigma \prod_{1\leq i\leq j\leq n}(X_j - X_i).$$

任何置换都可以分解成对换的乘积，这是因为任何轮换都能分解成对换的乘积，即$(12\dots k) = (1k)(1, k-1)\dots(13)(12)$，我们还可以定义为可分解成的对换的个数的奇偶性，可以证明，置换的任何对换分解的对换的个数的奇偶性不变。按照这种说法，一个对换(12)是奇置换，奇数长度的对换如$(123), (12345)$都是偶置换。

我们将给出另外一种定义，我们先解释一下这个定义是怎么来的。我们知道，每个置换$\sigma \in S_n$都有一个唯一的不相交轮换分解，如果把被它固定的元素c 视为长度为1 的轮换(c)，我们以t记该置换的不相交轮换分解中轮换的个数，包括长度1的轮换。那么定义

$$\mathrm{sgn}\sigma = (-1)^{n-t}.$$

[6]这种用交换图来表达等式的方式非常直观，在代数学中会经常用到。

首先，对恒等置换，$t = n$，因此$\mathrm{sgn}1 = 1$.对于轮换$(12\ldots k)$，$t = n - k + 1$, 故$\mathrm{sgn}(12\ldots k) = (-1)^{k-1}$.而$n - t$事实上是对每一个轮换的长度$l$ 减去1后再求和，其奇偶性将与轮换分解中奇置换的个数有关。麻烦的地方是，我们需要证明这是一个同态。直接证明并不容易，所以我们走稍微简单一点的路线：即证明对任意对换τ有$\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\sigma)$.

引理2.1. 对任何对换τ有$\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\sigma)$.

Proof. 若$\tau = (ab)$与σ的不相交轮换分解的任何一个轮换不相交，等式是显然的。否则若有一个相交元素，容易计算出

$$(ab)(ac..d) = (ac..db)$$

$(ac..db)$的长度相对$(ac..d)$增加了1，故符号改变了。若有两个相交元素，考虑

$$(ab)(abc..d) = (ac..d)$$

计算轮换的长度减1之和，右边比左边的$(abc..d)$少1

$$(ab)(ac..dbe..f) = (ac..d)(be..f)$$

计算轮换的长度减1之和，右边比左边的$(ac..dbe..f)$少1. 故我们立即得出命题。
□

定理2.7. $\mathrm{sgn} : S_n \to \{1, -1\} \cong \mathbb{Z}_2$是一个同态。

Proof. 由第一章，可设$\alpha = \tau_1\tau_2\ldots\tau_k$是$\alpha$的对换分解，则

$$\begin{aligned}
\mathrm{sgn}(\alpha\beta) &= \mathrm{sgn}(\tau_1\tau_2\ldots\tau_k\beta) \\
&= \mathrm{sgn}(\tau_1)\mathrm{sgn}(\tau_2\ldots\tau_k\beta) \\
&\ldots \\
&= \mathrm{sgn}(\tau_1)\ldots\mathrm{sgn}(\tau_{k-1})\mathrm{sgn}(\tau_k)\mathrm{sgn}(\beta) \\
&= \mathrm{sgn}(\tau_1)\ldots\mathrm{sgn}(\tau_{k-1}\tau_k)\mathrm{sgn}(\beta) \\
&\ldots \\
&= \mathrm{sgn}(\tau_1\tau_2\ldots\tau_k)\mathrm{sgn}(\beta) \\
&= \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).
\end{aligned}$$

□

同态sgn的核我们记作A_n,称作n元**交错群**，也就是全体偶置换组成的群。作为一个推论，$A_n \triangleleft S_n$.

练习37. 确定置换(132)(421)(12345)和置换

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$$

的奇偶性。

练习38. 证明一个置换的阶等于它的不相交轮换分解中的所有轮换长度的最小公倍数。

练习39 (★). 对S_4中所有的元素进行共轭类分类，并找出它所有的正规子群。

练习40 (★★). 证明A_{2n}有子群同构于S_n.

7. 直积

我们可以用老群来构造新的群，一种非常简单的构造就是直积。设G_1, G_2都是群，我们要赋予笛卡尔乘积$G_1 \times G_2$群的结构，最简单的方法就是把它的乘法定义为分量乘法，即

$$(g_1, g_2)(h_1, h_2) := (g_1h_1, g_2h_2).$$

这样一来群中的幺元素就是$(1,1)$,(g,h)的逆就是(g^{-1}, h^{-1}).这个群我们就记作$G_1 \times G_2$.如果G_1, G_2都是Abel群，有时这个构造记为直和$G_1 \oplus G_2$，群运算用加号代替。

练习41. 研究群$\mathbb{Z}_2 \times \mathbb{Z}_2$(也即群$\mathbb{Z}_2 \oplus \mathbb{Z}_2$)并证明它同构于

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

.

练习42 (★★). 证明有

$$D_6 \cong D_3 \times \mathbb{Z}_2.$$

事实上，当n是奇数时都有

$$D_{2n} \cong D_n \times \mathbb{Z}_2.$$

练习43 (★). 证明当m, n互质时有

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

CHAPTER 3

群的作用

1. 基本术语

群本质上是对称群/变换群/作用群的抽象结构。本章我们就来研究群的作用，即将抽象的群的元素实现为具体的变换/作用。比方说，循环群这种对称结构如何作用在各种对象上？我们知道，它可以实现为正多边形的旋转，即有群同态

$$\mathbb{Z}_n \to \{\text{正}n\text{边形的旋转群}\}$$

其中$\mathbb{Z}_n$的生成元被映射到某个单位旋转。也可以这样描述这种作用：将正n边形的旋转理解为顶点集$\{1,2,\ldots,n\}$上的一个置换，从而得到(单)同态

$$\mathbb{Z}_n \to S_n$$

其中$\mathbb{Z}_n$的生成元被映射到轮换$(123\ldots n)$. 我们研究群的尽可能广泛的作用，就是考虑群G到尽可能大的一类变换群的同态。一般考虑的大的一类变换群主要是两类：置换群和矩阵群。研究到矩阵群的同态的是群的线性表示论(简称群表示论)。我们研究群在集合上的作用时，就主要是研究的到置换群的同态。以$\mathrm{Sym}(X)$ 记集合X 上的所有置换[1]，即所有单满映射，称之为X 的对称群。那么我们称群G 在集合X 上的一个作用就是指一个同态(不要求是单同态或满同态)

$$\alpha : G \to \mathrm{Sym}(X).$$

这也称为群G的一个置换表示，简称表示。也就是说，$\alpha(g)$将成为集合X上的一个变换(置换)，单满射，即$\alpha(g) : X \to X$.这个变换可以作用在$x \in X$上得到$\alpha(g)(x)$。这种记号比较严格，但过于冗长，给定了同态α后不妨把G想象为一堆“算子”，直接用gx表示$\alpha(g)(x)$.

我们先来给出群作用基本的术语。如果α是单同态，就称这个作用是**忠实的(faithful)**，也就是说，这个作用不会把群中的两个不同元素变成相同的变换。对于$x \in X$，集合

$$Gx = \{gx | g \in G\}$$

称为x的**轨道(Orbit)**。容易证明，a, b属于同一个轨道，也就是存在g使得$a = gb$,是一个等价关系，这一点与G是群密切相关。如此而来，X中的元素划分为一些不相交的等价类的并，也就是不相交的轨道的并。如果X只有一个轨道，我们就称这个

[1]有些书也记为S_X

作用是**传递的(transitive)**，这也就是说，任何一个x 都可以被G 中的某一个作用映到任何一个给定的y.

1.1. 轨道公式.

定义3.1. 给定了群G在集合X上的作用，我们用

$$\mathrm{Stab}(x) = \{g \in G | gx = x\}$$

记G中所有保持x不动的变换。这是G的一个子群，称之为x的**稳定化子(Stabilizer)**.

练习44 (★). 有一个比传递更强的概念，叫**双传递(doubly-transitive)**，它是指对任意的$x \neq y, z \neq w$,存在$g \in G$使得

$$(gx, gy) = (z, w).$$

证明：G在X上是双传递的当且仅当对所有的$x \in X$都有$\mathrm{Stab}(x)$在$G\backslash\{x\}$上是传递的。

既然$\mathrm{Stab}(x)$是个子群，我们就可以作陪集分解

$$G = \bigcup_i g_i \mathrm{Stab}(x)$$

其中，每个陪集在x上的作用全部一致，都是$g_i x$.并且不同的陪集显然给出在x上不同的作用，否则$ax = bx \Leftrightarrow a^{-1}b \in \mathrm{Stab}(x) \Leftrightarrow a\mathrm{Stab}(x) = b\mathrm{Stab}(x)$.我们立马得到了如下简单而基本的轨道公式(计算轨道长度)

定理3.1 (轨道公式).

$$|Gx| = [G : \mathrm{Stab}(x)]$$

由于X划分为一些轨道，我们以x_i记每个轨道的代表元素，则显然必须有

$$|X| = \sum |\text{轨道}| = \sum_i [G : \mathrm{Stab}(x_i)].$$

不要小瞧这个轨道公式，有了它，我们就有了计算一些对称群的阶数的方法，因为$|G| = |Gx||\mathrm{Stab}(x)|$.

例3.1. 我们计算$|D_n|$.取正n边形的某一个顶点x,由于作用是传递的，$|Gx| = n$.而D_n中只有两个变换保持x不变，平凡变换和某个反射(轴对称)变换。故

$$|D_n| = |Gx||\mathrm{Stab}(x)| = 2n.$$

练习45 (★). 计算正四面体的对称群的阶数。

另外，我们马上能得到如下计算轨道个数的公式[2]

[2]据说Cauchy 早在Burnside 之前发现了这个结果

定理3.2 (Burnside)**.** 轨道的个数N有如下公式

$$N = \frac{1}{|G|}\sum_{g\in G}(\text{被}g\text{固定的元素}x \in X\text{的个数}).$$

Proof.

$$N = \sum_{x\in X}\frac{1}{|Gx|} = \sum_{x\in X}\frac{|\mathrm{Stab}(x)|}{|G|} = \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G}1_{gx=x} = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X}1_{gx=x}.$$

□

1.2. 表示的核. 我们来求$\ker\alpha$，这一般是重要的，因为这样，由同态基本定理，$G/\ker\alpha$同构于置换群$\mathrm{Sym}(X)$的某个子群。

$\ker\alpha$是什么呢？就是那些固定所有元素的g,因此

$$\ker\alpha = \bigcap_{x\in X}\mathrm{Stab}(x).$$

如果这个作用是传递的，就有

$$\ker\alpha = \bigcap_{g\in G}\mathrm{Stab}(gx).$$

$\mathrm{Stab}(x)$与$\mathrm{Stab}(gx)$有自然的关系。固定x的那些变换，稍微改一改，也可以拿去固定gx.这只需要先复合一个g^{-1},再施加$\mathrm{Stab}(x)$,再复合g.换而言之我们发现

$$g\mathrm{Stab}(x)g^{-1} \subset \mathrm{Stab}(gx).$$

反过来一样有

$$g^{-1}\mathrm{Stab}(gx)g \subset \mathrm{Stab}(x).$$

因此我们发现

$$\mathrm{Stab}(gx) = g\mathrm{Stab}(x)g^{-1}.$$

因而，在作用是传递的时，有

$$\ker\alpha = \bigcap_{g\in G}g\mathrm{Stab}(x)g^{-1}.$$

这是一个正规子群。这事实上也启示我们如下平凡的命题：设$H \le G$，则

$$\bigcap_{g\in G}gHg^{-1} \triangleleft G$$

2. 常见的作用(表示)

群不光可以作用在其它对象上，它很多时候可以自然地作用在自己的某些结构上。在群论的研究中，这是一种极为重要，朴素而强大的方法。我们举几个简单的例子。

2.1. 共轭作用. 群G以共轭作用作用在群G上，也即

$$\alpha : G \to \mathrm{Sym}(G)$$
$$x \mapsto (g \mapsto x^{-1}gx)$$

关于这个作用的轨道就是共轭类，容易看出，作用的核$\ker\alpha = Z(G)$.对于$g \in G$,其稳定化子$\mathrm{Stab}(g)$我们记作$C_G(g) = \{h \in G | gh = hg\}$[3],这是$G$ 的一个子群。我们把这个情形下的轨道方程

$$|G| = \sum_i [G : C_G(g_i)]$$

称之为群G的**类方程**。值得注意的是，有些元素$g \in G$可能轨道长度为1，也就是只与自己共轭的，中心元素，$Z(G)$.如果设$|G| = p^n$，其中p是某个素数，则有

$$p^n = |Z(G)| + \sum_{i, g_i \notin Z(G)} [G : C_G(g_i)]$$

易知$[G : C_G(g_i)]$必是p的倍数。故此时的$|Z(G)|$必须是p的倍数，因此$|Z(G)| > 1$.换而言之我们得到了结论

命题3.1. *设$|G| = p^n, n > 1$，则G有非平凡的中心$Z(G)$.*

练习46 (★). *若以$c(G)$记群G的共轭类的个数，证明，有*

$$c(G \times H) = c(G) \cdot c(H).$$

练习47 (★★★★). *记号如上，本题中设G是非$Abel$群，证明有*

$$c(G) \leq \frac{5}{8}|G|$$

等号能取到吗？进一步，证明，若p是$|G|$最小的素因子，则有

$$c(G) \leq \frac{p^2 + p - 1}{p^3}|G|$$

我就不问你等号能不能取到了，因为我也不知道。

2.2. 正则表示(作用). 群G以(左)[4]乘法作用在群G上，也即

$$\alpha : G \to \mathrm{Sym}(G)$$
$$g \mapsto (a \mapsto ga)$$

即将g自然地视为一个G上的置换$\alpha(g)$.这是一个忠实表示。

---

[3]对于$S \subset G$,我们以记号$C_G(S)$表示$\{g \in G | gs = sg, \forall s \in S\}$,称为$S$的**中心化子**。

[4]也可以定义右正则表示

$$\alpha : G \to \mathrm{Sym}(G)$$
$$g \mapsto (a \mapsto ag^{-1})$$

练习48. 证明这是一个忠实、传递的作用。

我们马上得出Cayley定理：每个群都同构与某个置换群的子群。这看起来似乎弱智无比，但是就是这样朴素的观点我们可以得到非平凡的结论，我们举一个例子。

命题3.2. 设G是$4k+2$阶群，那么它一定有一个指数为2的正规子群。

Proof. 考虑群的左正则作用

$$\alpha : G \to \mathrm{Sym}(G)$$

由于这是忠实表示，我们可以把G与$\alpha(G)$等同起来。那么，每个$\alpha(g)$都是一个G上的置换，由于群乘法具有逆的原因，除非$g=1$,这个置换不可能固定任何群中的元素($ga=a \Leftrightarrow g=1$.) 因此可以将$\alpha(g)$写为一些长度大于1的不相交轮换的乘积。现取g为群中的一个二阶元素，由前面的习题我们知道在偶数阶群中这是一定可以取到的。因此，$\alpha(g)$分解成$2n+1$个不相交的对换的乘积，因而是奇置换。于是我们证明了G中有奇置换，因而G中的所有偶置换构成一个指数为2的正规子群。 □

推论3.1. 设$k \geq 1$,则$4k+2$阶群一定不是单群。

2.3. 诱导表示(陪集上的表示/作用). 给定了群G的一个子群H后，有(左)陪集集合G/H，群G可以自然地作用在G/H上。

$$\alpha : G \to \mathrm{Sym}(G/H)$$

$$g \mapsto (aH \mapsto gaH)$$

这称为(左)诱导表示。它显然是传递的。它的核是

$$\ker \alpha = \bigcap_{g \in G} gHg^{-1}$$

并注意事实上有$\ker \alpha \lhd H$.运用这个表示可以得到很多厉害(其实很简单)的结论。

命题3.3. 设p是$|G|$最小的素因子，那么若$H \leq G$且$[G:H]=p$则有$H \lhd G$.

Proof. 考虑在陪集集合G/H上的诱导表示

$$\alpha : G \to \mathrm{Sym}(G/H)$$

由于有$G/\ker\alpha$同构于$\mathrm{Sym}(G/H)$的一个子群，因而必须有$|G/\ker\alpha|$是$[G:H]!$的因数。现在由于$\ker\alpha \leq H$,我们有

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

是$[G:H]=p$的倍数。由于p是$|G|$的最小素因子，我们知道$[H:\ker\alpha]$是1或p的倍数。若不是1，必有$p^2|p!$，这不可能，故

$$H = \ker\alpha \lhd G.$$

□

练习49 (★★)**.** 设G是大于3阶的单群，$H \leq G$,证明$[G:H] > 4$.

2.4. 循环群的作用：Cauchy定理. 本节我们看一个群作用的强大威力的例子，我们证明如下的柯西定理：

定理3.3 (Cauchy)**.** 设p是$|G|$的一个因数，则G中有p阶元素。

在开始看证明之前我们来理解一下思路。$p = 2$的情形已经作为一道练习题做过了，还记得做法吗？大家的做法，估计就是对G中的元素配对，g和g^{-1}配一对，二阶元素g和g^{-1}是相同的，就无法配对，最后因为群的阶数是2的倍数，配了对的元素个数也是2的倍数，我们得出满足$x^2 = 1$的元素个数有偶数个。由于$1^2 = 1$，我们知道一定有二阶元素。

不过，这个证明初看起来似乎并不能推广到$p > 2$的情形。但是，如果你用群与对称的观点重新叙述上面的证明，你马上就可以看出如何作推广。我们要将上述证明中出现的现象理解为一种对称性，那么就一定要有对称变换。我们观察到的现象是什么呢？那就是在所有的有序对$X = \{(g, g^{-1})|g \in G\}$集合上，有一种对称变换$(x, y) \mapsto (y, x)$.这就是群$\mathbb{Z}_2$在该集合上的作用。那么$X$拆分为一些轨道的并。而在该作用下轨道的长度为1等价于说$g = g^{-1}$也就是$g^2 = 1$,由轨道方程

$$|X| = |\{(g, g)|g^2 = 1\}| + \sum |\text{其它长为2的轨道}|$$

轨道公式表明轨道的长度只能是1或2,我们立刻得出$|\{g|g^2 = 1\}|$是2的倍数。现在，我想，如何推广这个证明已经至为显然。

Proof. 设$X = \{(g_1, g_2, \ldots, g_p)|g_1 g_2 \ldots g_p = 1\}$,并设$a$是群$\mathbb{Z}_p$的生成元，考虑群$\mathbb{Z}_p$在$X$上的如下作用

$$\alpha : \mathbb{Z}_p \to \mathrm{Sym}(X)$$
$$a \mapsto f$$

其中$f : X \to X$是把$(g_1, g_2, \ldots, g_p)$映到$(g_2, g_3, \ldots, g_p, g_1)$的映射。

我们需要验证$g_2 g_3 \ldots g_p g_1 = 1$,这可由$ab = 1 \Leftrightarrow ba = 1$得到。现在由轨道方程

$$|G|^{p-1} = |X| = |\{g \in G|g^p = 1\}| + \sum |\text{其它长为}p\text{的轨道}|$$

我们立得$|\{g \in G|g^p = 1\}|$是p的倍数，由$1^p = 1$立即知道群G中存在p阶元素，而且至少有$p - 1$个。事实上，可以得到更强的结论：(p阶元素个数+1)是p的倍数。 □

练习50 (★★)**.** 设$|G| = mp, 1 < m < p$,其中p是素数。证明$\mathbb{Z}_p \triangleleft G$.

练习51 (★)**.** 设G是6阶$Abel$群，按如下提示，证明$G \cong \mathbb{Z}_6$.*(*由柯西定理，G中有$2, 3$阶元素。从而$G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.*)*

练习52 (★★★). 设G是6阶非$Abel$群。按如下提示，证明有$G \cong S_3$,从而只有两个6阶群：$\mathbb{Z}_6$和S_3.

(1) 先证明$Z(G) = 1$.
(2) 证明G中必恰有3个2阶元素。
(3) 考虑G在集合$X = \{a, b, c\}$上的共轭作用，其中a, b, c都是2阶元素。*(需先证明这是X上的作用。)*
(4) 证明$\{a, b, c\}$能生成群G，由此证明上述作用是忠实的。同态基本定理给出$G \cong S_3$.

2.5. 在子群上的共轭作用. 设$A \leq G$是一个子群，容易发现，$g^{-1}Ag$也是一个子群。因为映射$x \mapsto g^{-1}xg$是自同构，而自同构限制在子群上还是同构，其像必然为群。我们称子群A与B共轭，如果$A = g^{-1}Bg$.那么容易看出，G可以以共轭作用作用在它的一些子群上。容易看出，一个子群可以有很多个共轭子群，而G的正规子群就是那些在G 的共轭作用下不变的子群，也就是只与自己共轭的子群，这时它单独组成一个共轭类。

对于$S \subset G$,我们以记号$N_G(S)$表示$\{g \in G | gS = Sg\}$,称为S的**正规化子**。容易看出，$A \leq G$的稳定化子是$N_G(A)$，从而有共轭类的大小为

$$[G : N_G(A)].$$

练习53 (★). 设$|G| = p^n$，证明G的非正规子群个数是p的倍数。

3. 群在组合计数问题中的应用(Under Construction)

如果要给一个立方体的两个面涂上红色，有多少种涂法呢？初看起来似乎有

$$\binom{6}{2} = \frac{6 \times 5}{2} = 15$$

种涂法，但是事实上很多种涂法都是相同的，它们之间只是差一个旋转而已。换而言之我们发现在对称的物件上涂色，只需考虑该物件的对称群，并让这个群作用在所有可能的涂色集合上。想知道两种涂法是不是一样的，只需看它们在不在一个轨道里。故，若要知道本质上不同的涂色有多少种，只需数轨道的个数就可以了! 而Burnside定理提供了一种方案。

4. Sylow定理(Under Construction)

Sylow(西罗)定理可能是初等群论中最重要的一个定理，它也是群的作用的一个精妙的应用。

定理3.4 (Sylow). 设G是群，$|G| = mp^n$,素数$p \nmid m$.那么有：

(1) 存在p^n阶的子群$P \leq G$,称为G的$Sylow\text{-}p$子群。

(2) 以$N(p^n)$记G的*Sylow-p*子群的个数，有

$$N(p^n) \equiv 1 \mod p.$$

(3) 所有*Sylow-p*子群互相共轭。

PROOF. 我们将群G作用在G的所有p^n元子集上，即

$$\begin{aligned} \alpha : G &\to \mathrm{Sym}(\Sigma) \\ g &\mapsto (A \mapsto gA). \end{aligned}$$

□