群

2023 年 6 月 2 日

目录

1 群

在之前，很多数学家对于求出一个多项式的根而着迷，但对于更高次数的多项式就很难了，在1824年，**阿贝尔(N.H.Abel, 1802-1829)**证明了一般的五次多项式不能用公式求根。但还好我们有天才的伽罗瓦(E.Galois, 1811-1832) 他找到了任意次数的多项式能用公式求根的一般判别方法，这包含了群的思想。

“积”的本质，是指将两种事物结合成第三个同类的事物，例如：普通的乘法，加法、减法将两个结合的数变成了另一个数。而合成把两个置换变成了一个置换。

1.1 定义：二元运算

集合G上的一个二元运算是指函数

$$*: G \times G \to G$$

具体来讲，一个运算是将G中的元素$*(x,y)$分配到每对在G中的其他元素(x,y)，且用$x*y$代替$*(x,y)$的写法看起来会更自然点，因此，函数的复合就是函数$(f,g) \to g \circ f$，而对于乘法、加法和减法来说，它们的函数是$(x,y) \to xy$,$(x,y) \to x+y$, $(x,y) \to x-y$，由合成和减法的例子我们知道为什么需要有序对，因为对于$x*y$和$y*x$来说可能是不同的。对于任何函数，函数和运算都是单值的，具体来说，我们经常把这叫做**替换律**，即

$$若x = x', y = y', \text{则} x*y = x'*y'$$

1.2 定义：群

在集合G上带有运算$*$和一个特殊元（单位元）$e \in G$称为群。若

1. 结合律成立，对于每个$a,b,c \in G$有

$$a*(b*c) = (a*b)*c$$

2. $e*a = a$对每个$a \in G$成立

3. 对每个$a \in G$，有$a' \in G$使得$a'*a = e$

在之前的命题，集合S_X是由X的所有置换构成的集合。而且通过把

合成看作是一个运算且算上恒等置换1_X的话，那么这就是一个群（我们把S_X叫做X上的对称群）。

我们现在处在一些从代数转变为抽象代数的转折点上，与由$X = \{1, 2, \cdots, n\}$的所有置换构成的具体群S_n相比。我们将证明关于群的一般结论不用指定某些元素或者运算。因此，积能不能计算其实也不是显然的，而只是服从某些法则。而且这种方法是富有成效的，对于许多定理也使用于许多不同的群。证明这些定理的时候并不需要对每个群都证明一遍，这使得证明的效率更高了。例如，等一下给出的一个命题和三个引理都说明了一些在群G中成立的性质。除了这种明显的省力的形式外，对于我们在处理一些特定的具体群时，利用抽象的方法来证明通常更加简单。例如，当我们暂时不谈S_n的置换时，它身上有一些性质会更容易处理。

1.3 定义：阿贝尔群

一个群G称为阿贝尔群，若该群满足交换律，即对于任意$x, y \in G$有：

$$x * y = y * x$$

对于群S_n，对$n \geq 3$不是阿贝尔群，因为$(1\ 2), (1\ 3) \in S_n$，但它们不交换：$(1\ 2)(1\ 3) = (1\ 3\ 2)$和$(1\ 3)(1\ 2) = (1\ 2\ 3)$。

我们将在给出更多的例子之前证明一些基本事实。

如何乘三个数，例如表达式$2 \times 3 \times 4$，对于这个例子，我们可以先做$2 \times 3 = 6$，再做$6 \times 4 = 24$，或者先做$3 \times 4 = 12$，或者$2 \times 12 = 24$。当然，这两个答案是一样的，因为数乘满足交换。但并非所有的运算都是交换的，例如减法就不满足，设$c \neq 0$，则

$$a - (b - c) \neq (a - b) - c$$

因为$a - (b - c) = a - b + c$但$(a - b) - c = a - b - c$。

更一般的，如何将三个元素$a * b * c$相乘？因为我们一次只能做一次乘法，一次乘法能乘两个元素，所以我们有一些选择：做$b * c$来得到G中的一个新元素，然后我们再用这个元素去与a相乘得到$a * (b * c)$。或者我们先做$a*b$再乘c，由可交换性可知，这两者的积是一样的。$a*(b*c) = (a*b)*c$，所以我们可以直接去掉括号写$a * b * c$，等一下给出的引理表面，一些结合律性质对含四个因子的积成立。

1.4 引理

如果$*$是一个在G上满足可交换的运算，则对于所有$a,b,c,d \in G$

$$(a*b)*(c*d) = [a*(b*c)]*d$$

证明：记$g = a*b$，则$(a*b)*(c*d) = g*(c*d) = (g*c)*d = [(a*b)*c]*d = [a*(b*c)*d]$

1.5 引理：

若G是一个群和$a \in G$满足$a*a = a$，那么$a = e$

证明：存在$a' \in G$满足$a'*a = e$，然后在要证明的式子两边左乘a'得到等式$a'*(a*a) = a'*a$，等式右边的是e，对于左边就有$(a'*a)*a = e*a$，所以有$a = e$

1.6 命题

设G是一个群，其运算为$*$和单位元是e

1. $a*a' = e$对所有$a \in G$成立
2. $a*e = a$对所有$a \in G$成立
3. 若对所有$a \in G$有$e_0 \in G$满足e_0*a则$e_0 = e$
4. 令$a \in G$，若$b \in G$满足$b*a = e$，则$b = a'$

证明： 已知$a'*a = e$，现在来证明$a*a' = e$ 利用引理1.4有

$$\begin{aligned}(a*a')*(a*a') =& [a*(a'*a)]*a' \\ =& (a*e)*a' \\ =& a*(e*a) \\ =& a*a'\end{aligned}$$

再利用引理1.5就有$a*a' = e$

对于第二个命题，利用命题1就有

$$a*e = a*(a'*a) = (a*a')*a = e*a = a$$

所以$a * e = a$

而命题3是要我们证明每个群只有一个单位元，也就是说，若$e_0 * a = a$对所有$a \in G$成立，尤其是$e_0 * e_0 = e_0$，但利用引理1.5有$e_0 = e$，所以e_0只能是e且G中无第二个单位元。

对于命题4，在命题1中我们证明了若$a' * a = e$，则$a * a' = e$，现在有

$$\begin{aligned} b = b * e =& b * (a * a') \\ =& (b * a) * a' = e * a' = a' \end{aligned}$$

且由命题3可知，单位元是唯一的，所以存在唯一的$a' \in G$有$a' * a = e$

1.7 定义：逆元

设G是一个群和$a \in G$，则存在唯一的元素$a' \in G$使得$a' * a = e$，a'称为a的逆元，记为a^{-1}

接下来我们还有三个关于所有群的性质

1.8 引理

令G是一个群

1. 消去律成立：设$a, b, x \in G$，若$x * a = x * b$或者$a * x = b * x$，则$a = b$
2. 对所有的$a \in G$有$(a^{-1})^{-1} = a$
3. 若$a, b \in G$，则
$$(a * b)^{-1} = b^{-1} * a^{-1}$$
更一般的，对所有的$n \geq 2$有
$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}$$

证明： 对于命题1，有

$$\begin{aligned} a = e * a = (x^{-1} * x) * a =& x^{-1} * (x * a) \\ =& x^{-1} * (x * b) = e * b = b \end{aligned}$$

对另一种情况$(a * x)$的证明类似，利用$x * x^{-1} = e$并在x的右边利用提示就行。

对于命题2，利用命题1.6的1，有$a * a' = e$，但利用1.6的命题4可知逆是唯一的，这么说$(a^{-1})^{-1}$则是$x \in G$中唯一满足$x * a^{-1} = e$的元素，所以$(a^{-1})^{-1} = a$

对于命题3利用引理1.4有

$$(a * b) * (b^{-1} * a^{-1}) = [a * (b * b^{-1})] * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e$$

所以$(a * b)^{-1} = b^{-1} * a^{-1}$。对于推广的命题则通过命题1.6的4并对$n \geq 2$做归纳法即可。

对于$n = 2$的情况成立，现在假设对n的情况成立，则设$g = a_1 * \cdots * a_n$

$$\begin{aligned}(g * a_{n+1}) * (a_{n+1}^{-1} * g^{-1}) =& g * (a_{n+1} * a_{n+1}^{-1}) * g^{-1} \\ =& g * g^{-1} \\ =& e\end{aligned}$$

所以成立。

在我们刚刚给出的证明，我们一直在非常小心的证明每一步的合理性并给出所有的括号。因为我们才刚刚开始学习群论的思想。随着熟练度的增加，我们所需要写入证明的细节会少很多，因为会变得很自然。但这不意味着你就可以变得粗心了，这只是在说我们变得成熟了，当然，在证明的过程中如果有任何让你感到困惑的地方，你必须随时准备好写出被省略的细节。

从现在开始，我们将用ab来表示群中的积$a * b$（因为在对称群中我们已经用ab表示了合成$a \circ b$），我们将用1表示单位元而不是用e。当一个群是阿贝尔群的时候，无论如何，我们将经常使用加法来表示这个。以下是用加法表示群的定义。

一个加法群指的是集合G上带有运算$+$和包含一个单位元0满足

1. 对每个$a, b, c \in G$有$a + (b + c) = (a + b) + c$
2. $0 + a = a$对所有$a \in G$成立
3. 对每个$a \in G$，存在一个$-a \in G$使得$(-a) + a = 0$

注意a的逆元，在加法中，我们一般把a^{-1}写为$-a$。我们将给出很多关于群的例子，可以看看列表，选择一些你喜欢的。

例1

1. 我们一直提醒读者关于S_X其实就是X的所有置换构成的，在合成的运算下构成了一个群。特别的，$X = \{1, 2, \cdots, n\}$所有置换构成的S_n是一个群

2. 整数Z是一个加法群（且是阿贝尔群），其中$a * b = a + b$带有单位元$e = 0$，它的逆元$n^{-1} = -n$，类似的，我们也可以看到集合Q, R, C都是一个加法阿贝尔群

3. 注意到所有的非零有理数集$Q^\times$是一个阿贝尔群，它的运算是乘法，单位元是1它的元素$r \in Q^\times$的逆元是$1/r$对于$R^\times$也是一个阿贝尔群，对于$C^\times$也是一样的

4. 对于正整数n，令

$$\Gamma_n = \{\zeta^k : 0 \leq k < n\}$$

是所有n次单位根构成的集合，有

$$\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$$

利用棣莫佛定理我们可以得知这个集合是一个阿贝尔群，它带有的运算是复数乘法。逆元是它的复共轭。

接下来的讨论具有技巧性，我们要讨论的是一个定理，如果已经懂了这个定理则可以完全跳过。这个定理讲的是：若运算是满足结合律的，则在含有$n \geq 3$的每个因子的积中都不需要添加括号

一个n元表达式指的是一个n元组$(a_1, \cdots, a_n) \in G \times \cdots G$(含有n个因子)，通过以下方法产生许多的G的元素，选择其中两个相邻的元素相乘，得到一个$n-1$元表达式。这个新得到的积里面含有有原表达式的$n-2$个因子，在这个新表达式中，继续选择两个相邻的元素（或者选择一个元素与上一步得到的积做乘法），然后我们重复这一步直到最后只剩下两个元素(W, X)，现在相乘得到G中的元素WX，我们把WX叫做n元表达式的**最终积**，例如考虑一个4–表达式$(a\ b\ c\ d)$，现在把a, b相乘得到一个3元表达式(ab, c, d)，我们选一种情况做乘法就行，把ab, c做乘法得到一个2元表达式$([(ab)c], d)$或者得到(ab, cd)，在最后的表达式中的元素可以通过最终

积$[(ab)c]d$或者$(ab)(cd)$给出。其他的最终积可以由$(a\ b\ c\ d)$先做bc或者cd给出。得到(a,bc,d)或者(a,b,cd)，所以这最后的导出积是相等的，但这不是很明显，即使这些运算是满足结合律的，但在很长的表达式中不是很容易看出来是否相等。

1.9 定义

一个n元表达式不需要加括号，若它的所有的最终积都是相等的，即无论我们如何选择相邻的因子去做乘法，最终所有G中的乘积都相等

1.10 定理：广义结合律

若$n \geq 3$，则所有群G中的n元表达式$(a_1, a_2, \cdots, a_m)$ 都不需要加括号

注意：在证明中我们既不用单位元也不需要逆元来证明。因此定理的假设可以被减弱为G是一个半群，所以，G是一个配备了结合律的非空集。

证明：我们利用第二归纳来证明，对$n = 3$的时候从结合律得到，对归纳步骤，我们考虑G中从n元表达式$(a_1, a_2, \cdots, a_n)$的两个一系列选择得到的2元表达式

$$(W, X) = (a_1 \cdots a_i, a_{i+1} \cdots a_n),\ \ (Y, Z) = (a_1 \cdots a_j, a_{j+1} \cdots a_n)$$

我们的目的是证明$WX = YZ \in G$，对每个元素，设$W = a_1 \cdots a_i$，$X = a_{i+1} \cdots a_n$，和$Y = a_1 \cdots a_j$，$Z = a_{j+1} \cdots a_n$都是从m元表达式$(m < n)$中得到的唯一最终积，不失一般性。我们可以假设$i \leq j$，若$i = j$，则由归纳假设我们可以得到$W = Y$和$X = Z$有$WX = YZ$

若$i < j$，我们设A是从i元表达式$(a_1, \cdots, a_i)$得到的最终积，设B是从$(a_{i+1}, \cdots, a_j)$得到的最终积并设C是从$a_{j+1}, \cdots, a_n$得到的最终积。群的元素A, B, C是明确定义的，对于归纳假设，这是说每个较短的表达式都定义有唯一一个最终积，现在有$W = A$，这俩的最终积从i元表达式$(a_1, \cdots, a_i)$得到。而$Z = C$由$(n-j)$元表达式得到。$X = BC$从$n-i$元表达式$[a_{i+1}, \cdots, a_n]$得到，并$Y = AB$也从j元表达式$(a_1, \cdots, a_j)$得到，由我们的推断得出$WX =$

$A(BC)$，$YZ = (AB)C$而这个群满足结合律，这意味着这就是从一开始对$n = 3$的归纳步骤得到的$WX = YZ$

1.11 定义

若G是一个群和$a \in G$，对$n \geq 1$归纳的定义a的幂a^n为

$$a^1 = a,\ a^{n+1} = aa^n$$

定义$a^0 = 1$，而且，若n是正整数，定义

$$a^{-n} = (a^{-1})^n$$

特别的，关于$(a^{-1})^n = (a^n)^{-1}$将会在习题中作为特例给出。

这里有个隐藏的问题，一次幂和二次幂其实还好，因为$a^1 = a, a^2 = aa$，但我们这里对三次幂有两种不同的方法去定义：$a^3 = aa^2 = a(aa)$，但这里有另一种合理的备用选项：$(aa)a = a^2a$，若它们是满足结合律的，则这两个选项其实是相等的：

$$a^3 = aa^2 = a(aa) = (aa)a = a^2a$$

而广义结合律展示了所有的幂次的定义都是很清楚的。

1.12 推论

设G是一个群，若$a \in G$且设$m, n \geq 1$，则

$$a^{m+n} = a^m a^n \text{和 } (a^m)^n = a^{mn}$$

a^{m+n}和$a^m a^n$都是从含有$m + n$个等于a的因子的表达式中产生的，在第二个等式中$(a^m)^n$和a^{mn}都是从mn个等于a的因子的表达式产生的，所以群中元素a的任何两个幂都是交换的：

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

对于接下来的命题中的各种证明是简单的，但有点长

1.13 命题：指数律

令G是一个群且令$a, b \in G$，和m, n是整数（不一定是正整数）

1. 若a, b满足交换，则$(ab)^n = a^n b^n$
2. $(a^n)^m = a^{mn}$
3. $a^m a^n = a^{m+n}$

证明：书上原文：**Exercises for the reader.**

真正的证明： 因为a, b交换，则$(ab)^1 = ab = a^1 b^1$是成立的，继而有$a^2 b^2 = aabb = abab = (ab)^2$基础步骤成立，我们对$a^k b$进行归纳，由归纳假设得到对$a^{k-1}$交换是成立的，那么$a^{k-1}ba = a^{k-1}ab = a^k b$归纳完毕。

进一步的，因为$a^n b$是交换的，则对$a^n b^n$归纳，则$a^n b^n = (\underbrace{aa\cdots a}_{\text{n个a}})(\underbrace{bb\cdots b}_{\text{n个b}})$由于对每个$i \in n$都有$a^i b$满足交换，我们先交换$a^{n-1}$和b的位置得到$a\,b\,aa\cdots ab\cdots b$，重复步骤一直到每个$a, b$都有配对到，那么我们就得到了

$$a^n b^n = a\,b\,aa\cdots ab\cdots b = abab\cdots ab = (ab)^n$$

成立

对于第二个命题，$(a^n)^m = a^{nm} = a^{mn}$是显然的。

$$(a^n)^m = (\underbrace{aa\cdots a}_{\text{n个a}})^m = (a^m a^m \cdots a^m) = (a)^{\underbrace{m+m\cdots+m}_{\text{n个m}}} = a^{nm}$$

第三个命题，利用前两个命题得到

$$a^n a^n = a^{2n} = a^{n+n}$$

其中的一个n替换为m则得到

$$a^{m+n} = a^m a^n$$

符号a^n是$a*a*\cdots*a$的自然表示，如果a出现n次，我们把运算选为+，则na是$a+a+\cdots+a$的一自然表示。设G是一个加法群，若$a,b\in G$和m,n是整数（不一定是正的），则由命题1.13我们可以把定理重写为

1. $n(a+b)=na+nb$
2. $m(na)=(mn)a$
3. $ma+na=(m+n)a$

例2

假设一副牌被打乱，这样子牌的顺序就从 $1,2,\cdots,52$ 到 $2,1,4,3,\cdots,52,51$ 。我们再次洗牌，则卡片的顺序就变回原样。但是任何关于52张卡片的置换α都会发生类似的事情：如果我们重复置换α足够多次，那么卡片最终都会变回原样。为了搞清楚这些，你需要用到学到的置换的知识；记α为不相交循环置换的积，则$\alpha=\beta_1\beta_2\cdots\beta_t$，其中$\beta_i$是一个$r_i-$循环置换，一般的，一个元素经过循环节的长度的幂次刚好就是自身（这是一个重复的循环），所以对每个i，$\beta_i^{r_i}=(1)$。一样的，对于$k=r_1r_2\cdots r_t$来说，β_i^k是一个恒等置换，因为：$\beta_i^k=\beta_i^{r_1\cdots r_t}=(\beta_i^{r_i})^{k/r_i}=(1)^{k/r_i}=(1)$ ，这意味着必须有$k=r_1\cdots r_t$。则对于所有的i我们得出

$$\alpha^k=(\beta_1\cdots\beta_t)^k=\beta_1^k\cdots\beta_t^k=(1)$$

这里有更一般的结果和简单的证明（用抽象代数会比代数更简单）：若G是一个有限群和$a\in G$，则对某个$k\geq 1$ 有$a^k=1$。利用置换中的引理1.8的（1）并考虑如下排列

$$1,\alpha,\alpha^2,\cdots,\alpha^n,\cdots$$

由于G是有限群，在无限的循环中肯定会出现重复的元素，则存在正整数$m>n$满足$a^m=a^n$，那么就会有$1=a^ma^{-n}=a^{m-n}$，所以某个a的正幂次得到1，我们最开始讨论对于52张卡牌的置换α的幂$a^k=(1)$不是毫无意义的，接下来的一些定理说明了我们可以选择$k=lcm(r_1,\cdots,r_t)$

1.14　定义：阶

设G是一个群和$a \in G$，若对某个$k \geq 1$有$a^k = 1$，则这样的最小指数$k \geq 1$叫做a的阶。若不存在这样子的幂，那么我们说a是**无限阶**的

例如，刚才的扑克牌的例子告诉我们，这个有限的对称群中的每个置换$a \in G$都是有限阶的。对于任何群G，阶数为1的是单位元，并且这也是群里唯一一个阶数为1的元。而且，一个元素的阶数为2，当且仅当它是自己的逆元。例如(1 2) 的逆元(2 1)，我们有一个非常不错的例子来说明无限阶，矩阵$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$，对所有$k \geq 1$有$A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$，这意味着$A$是无限阶的。

1.15　引理

设G是一个群，假设$a \in G$的阶数k是有限的，若$a^n = 1$，则$k|n$，实际上$\{n \in Z : a^n = 1\}$是k的所有倍数的集合

证明：我们构造集合$I = \{n \in Z : a^n = 1\} \subseteq Z$，则它满足如下定理内容

1. $0 \in I$，因为$a^0 = 1$
2. 若$n, m \in I$，则$a^n = a^m = 1$，所以$a^{n-m} = a^n a^{-m} = 1$为此$n - m \in I$
3. 若$n \in I$和$q \in Z$，则$a^n = 1 = a^{qn} = (a^n)^q = 1^q = 1$，所以$qn \in I$

因为$n - m \in I$并且$n, m \in I$所以这说明$n - m$是最小元d的倍数（由最小元定理可知存在最小元素d满足$a^d = 1$），利用定义1.14。我们知道这种最小数其实就是k，所以$d = k$。所以，若$a^n = 1$，则$n \in I$并且是k的倍数。

现在，对称群S_n中的置换阶是什么呢

1.16 命题

设$\alpha \in S_n$

1. 若α是$r-$循环置换，则α阶数是r
2. 令$\alpha = \beta_1 \cdots \beta_t$是不相交$r_i-$循环置换$\beta_i$的乘积，则$\alpha$的阶数是$m = \text{lcm}(r_1, \cdots, r_t)$
3. 设p是素数，若α阶数是p当且仅当它是一个$p-$循环置换或者是不相交$p-$循环置换的乘积

证明： 对于命题1,α是$r-$循环，则对于每个元素$k \in \alpha$，都有$\alpha^r(k) = k$，所以有$\alpha^r = 1$这意味着α的阶是r

命题2，每个β_i的阶数都是r_i，假设$a^M = (1)$，因为β_i是交换的，则$(1) = \alpha^M = (\beta_1 \cdots \beta_t)^M = \beta_1^M \cdots \beta_t^M$

现在引入一个命题：

若 $\alpha, \beta \in S_n$是不相交的，且$\alpha\beta = (1)$，则$\alpha = (1)$和$\beta = (1)$

证明中的证明：

设i是一个元素，由于α, β不相交，那么$\alpha \neq \beta^{-1}$，我们不妨设i被α移动，则$\alpha\beta(i) = \alpha(i) = i$，但$i$由假设可知被$\alpha$移动，但$\alpha\beta = (i)$，所以$i$不是$\alpha, \beta$的元素。这意味着$\alpha, \beta$不移动元素，且不存在逆运算，所以$\alpha = (1), \beta = (1)$。现在回到外面的证明上来

所以β的不相交暗示了对每个i有$\beta_i^M = (1)$利用引理1.15，我们知道$r_i | M$，所以$M = r_1 \cdots r_t$，但对于$m = \text{lcm}(r_1, \cdots, r_t)$，不难看出$a^m = (1)$。所以$\alpha$的阶数就是$m$。

对于第三个命题，只需要将α写成不相交的循环置换乘积，再利用命题2。若α是一个$p-$循环置换，利用命题1就知道α的阶为p。若$\alpha = \beta_1 \cdots \beta_t$是一系列不相交$p-$循环置换的乘积，则对于每个$\beta_t$都是$p-$循环置换，则对于每个$i$有$\beta_i^p = (1)$所以$\alpha$的阶是$\text{lcm}(p, \cdots, p) = p$

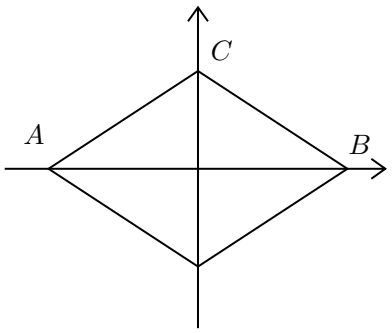
例如，S_n中的2阶置换当且仅当它是对换或者是对换的乘积。

为此我们适当的拓宽在置换中得到的表，在S_5中有

循环置换	置换个数	阶	奇偶性
(1)	1	1	偶
(1 2)	10	2	奇
(1 2 3)	20	3	偶
(1 2 3 4)	30	4	奇
(1 2 3 4 5)	24	5	偶
(1 2)(3 4 5)	20	6	奇
(1 2)(3 4)	$\frac{15}{120}$	2	偶

2 对称

现在我们给出群和对称之间的关系（利用R上的一些线性代数），当我们谈论一个等腰三角形的对称性说是什么意思？例如下图：



等腰三角形$\triangle = \triangle ABC$，它的底$AB$在$x$上，且$y$轴是$AB$的垂直平分线，如果在图上作出三角形关于$y$的反射（令顶点$A, B$互换），我们发现反射后和反射前的图形重合了，所以$\triangle$关于$y$轴对称，一样的。若$\triangle$关于$x$轴对称，那么应该是重合的图形，但这明显不会发生（因为这个菱形下面的三角形是没被定义的），所以$\triangle$关于x轴不对称，这意味着反射是一种特殊的等距同构。

2.1 定义：等距同构

一个平面上的等距同构指的是函数$\varphi : R^2 \to R^2$保持距离：对R^2中的所有点$P = (a, b)$和$Q = (c, d)$有

$$\|\varphi(P) - \varphi(Q)\| = \|P - Q\|$$

其中$\|P - Q\| = \sqrt{(a-c)^2 + (b-d^2)}$是$P$到$Q$的距离

$P \cdot Q$是一个点积，那么

$$P \cdot Q = ac + bd$$

则

$$\begin{aligned}(P-Q)\cdot(P-Q) =& P\cdot P - 2(P\cdot Q) + Q\cdot Q\\ =& a^2 + b^2 - 2(ac+bd) + (c^2+d^2)\\ =& (a^2 - 2ac + c^2) + (b^2 - 2bd + d^2)\\ =& (a-c)^2 + (b-d)^2\\ =& \|P-Q\|^2\end{aligned}$$

这意味着，对于每个等距同构φ都保持点积不变：

$$\varphi(P)\cdot\varphi(Q) = P\cdot Q$$

因为

$$\varphi(P)\cdot\varphi(Q) = \|\varphi(P) - \varphi(Q)\| = \|P - Q\| = P\cdot Q$$

我们回顾点积公式的几何形式：

$$P\cdot Q = \|P\|\|Q\|\cos\theta$$

其中θ是P, Q之间的角度，所以这意味在几何上等距同构保持角度不变，其次，若P, Q正交，这意味着$P \cdot Q = 0$，所以等距同构保持垂直，反过来说，若φ保持点积运算，即，若$\varphi(P)\cdot\varphi(Q) = P\cdot Q$，则$(P-Q)\cdot(P-Q) = \|P-Q\|^2$有 φ是一个等距同构

我们把所有平面上的等距同构的集合表示为$\mathbf{lsom}(R^2)$，它存在一个满足$\varphi(O) = O$的等距同构构成的子集，叫平面上的正交群，且记为$O_2(R)$，等一下我们将证明$\mathrm{lsom}(R^2)$和$O_2(R)$对合成运算构成一个群

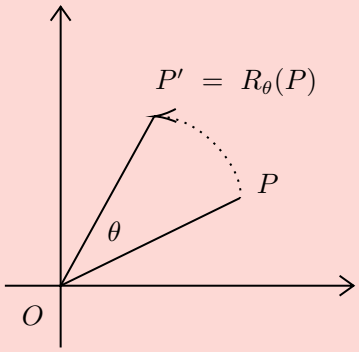
现在引入一些符号来帮助我们分析等距同构。

记号：若P,Q是平面上的不同点，则$L[P,Q]$表示由这两个点确定的直线，用PQ表示带端点的线段

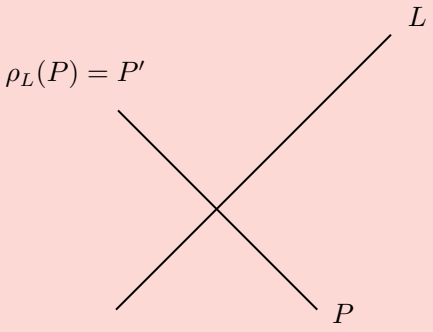
下面是一些等距同构的例子：

例

1. 给定角度θ，绕点O的旋转R_θ定义如下：$R_\theta(O) = O$，若$P \neq O$，我们绘制线PO，并旋转θ得到OP'（若θ为正，则逆时针旋转，否则顺时针旋转）并定义$R_\theta(P) = P'$，当然，绕平面任何点旋转都是没问题的。



2. 定义直线L上的反射ρ_L，若我们说其是轴，则固定直线L上的每个点，若$P \notin L$，则$\rho_L(P) = P'$，若我们假设轴是一面镜子，则P'是P的镜像（因为L是$P'P$的垂直平分线），现在$\rho_L \in \mathbf{Isom}(R^2)$，若$l$过原点，则$\rho_L \in O_2(R)$



3. 给定一点V，通过V的平移指的是函数$\tau_V : R^2 \to R^2$并定义$\tau_V(U) = \text{U+V}$，并且平移属于$\mathbf{Isom}(R^2)$，若平移τ_V固定原点，当且仅当$V = O$，所以恒等变换是既是旋转又是平移

2.2 引理

若φ是平面上的一个等距同构，则R^2上的点P,Q,R是共线的，当且仅当$\varphi(P),\varphi(Q),\varphi(R)$是共线的

证明：设P,Q,R是共线的，选择符号R在P,Q中间，因此有$\|P-Q\| = \|P-R\| + \|R-Q\|$，若$\varphi(P),\varphi(Q),\varphi(R)$不共线，则构成三角形的三个顶点。由三角不等式有

$$\|\varphi(P)-\varphi(Q)\| < \|\varphi(P)-\varphi(R)\| + \|\varphi(R)-\varphi(Q)\|$$

这与等距矛盾，类似的讨论反过来也成立。若P,Q,R是不共线的，则它们是三角形的三个顶点，若变换后共线，则上述严格不等式是等号，这与不等距矛盾。

每个等距同构φ是单射的，若$P \neq Q$，则$\|P-Q\| \neq 0$则$\|\varphi(P)-\varphi(Q)\| = \|P-Q\| \neq 0$，所以$\varphi(P) \neq \varphi(Q)$，但等距同构是满射这点不太明显，我们等一下会看到是一个满射。

2.3 命题：

R^2中每个φ固定原点的旋转是线性变换

设$C_d = \{Q \in R^2 : \|Q-0\| = d\}$是一个半径$d>0$并以原点$O$为圆心的圆。我们声称$\varphi(C_d) \subseteq C_d$，若点$P \in C_d$则$\|P-O\| = p$，而由于$\varphi$保持距离，则$d = \|\varphi(P)-\varphi(O)\| = \|\varphi(P)-O\|$，因此$\varphi(P) \in C_d$

若R^2中的点$P \neq O$，$r \in R$，若$\|P-O\| = p$，那么$\|rP-O\| = |r|p$，则$rP \in L[O,P] \cap C_{|r|p}$，其中$L[O,P]$是一条由两个点$O,P$确定的直线（不是线段），直线上满足数乘，所以$r$倍的$P$点也在这根线上。且其中$C_{|r|p}$是半径为$|r|p$，圆心在$O$的圆。由于$\varphi$保持共线性，利用引理2.2，$\varphi(L[O,P] \cap C_{|r|p}) \subseteq L[O,\varphi(P)] \cap C_{|r|p}$，因为保持共线，所以任意的$rP \in L[O,P] \cap C_{|r|p}$，所以$\varphi(L[O,P] \cap C_{|r|p})$就是对$rP$做线性变换，那么线性变换共线。所以变换后的点就和由$L[O,\varphi(P)]$确定的点共线，这意味着这个点要么在点$\varphi(P)$上边，要么下边(因为一根直线和圆的交点有两个)，即$\varphi(rP) = \pm\varphi(P)$。

我们排除$\varphi(rP) = -r\varphi(P)$的可能性，则$\varphi(rP) = r\varphi(P)$，在$r>0$的情况中，则原点$O$在$-rP$和$P$之间，所以实际的距离是$rp+p$。另一方面，从$rP$到$P$的距离为$|rp-p|$，所以对于任意常数$r$，都不会有$r+rp = |rp-p|$的

情况，这意味着不会出现$\varphi(rP) = -r\varphi(P)$的情况（因为等距同构保距），所以一个正数不会因为变换而变成负数。

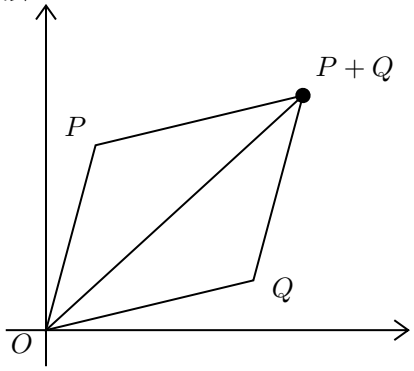
对$r < 0$也有类似的讨论，从$-rP$到$-P$上的距离也是$|rp-p|$，也有$rp+r \neq |rp-p|$，这意味着$\varphi(-rP) \neq r\varphi(P)$ 所以保持数乘。

现在我们只要证明满足加法就行，即$\varphi(P+Q) = \varphi(P)+\varphi(Q)$，若$O, P, Q$共线，我们选择$L[O, P]$上的一点$U$使他到原点的距离为1。因此，$P = pU,\ Q = qU$，那么$P + Q = (p + q)U$，因为$O = \varphi(O)$，$\varphi(U),\ \varphi(P), \varphi(Q)$是共线的。并且$\varphi$满足标量乘法，我们有

$$\begin{aligned}\varphi(P) + \varphi(Q) =& \varphi(pU) + \varphi(qU)\\ =& p\varphi(U) + q\varphi(U)\\ =& (p + q)\varphi(U)\\ =& \varphi((p + q)U)\\ =& \varphi(P + Q)\end{aligned}$$

所以满足加法。

若O, P, Q不是共线的，那么$P+Q$可以由平行四边形法则给出，令$O, P, Q, P+Q$为四边形的顶点，因为φ保距，那么变换后依然是一个平行四边形，所以$\varphi(O) = \varphi(U)$和$\varphi(P), \varphi(Q), \varphi(P+Q)$是顶点，则$\varphi(P+Q) = \varphi(P)+\varphi(Q)$，这意味着变换满足加法



证毕

2.4 推论：

每个等距同构$\varphi : R^2 \to R^2$是双射，以及每个固定原点的等距同构是一个非奇异线性变换。

证明：首先，我们假设φ固定原点有$\varphi(O)=O$，通过命题2.3我们知道这个等距同构是一个线性变换，因此是一个单射。那么$P=\varphi(e_1)$，$Q=\varphi(e_2)$是R^2中的一个基。其中$e_1=(1,0),e_2=(0,1)$是R^2的标准基。因此，函数$\psi:R^2\to R^2$定义为$\psi:aP+bQ\to ae_1+be_2$是一单值函数（单射），并且φ,ψ互为反函数，反函数是双射的。所以φ是一个双射，并且是非奇异的（因为$\varphi(\psi)=1$）。

假设φ是任意等距同构，使得$\varphi(O)=O$，现在$\tau_{-U}\circ\varphi:O\to U\to O$，有$\tau_{-U}\circ\varphi=\theta$是一个非奇异线性变换，因此$\varphi=\tau_U\circ\theta$是双射，并且是双射的复合。

我们将在第六章学习更多关于$\mathbf{Isom}(R^2)$的知识，尤其是，我们将看到所有的等距同构要么是选择、反射、平移或者是第四类，滑动反射。

2.5 定义：正交群

一个正交群$O_2(R)$是平面上固定原点的所有等距同构构成的集合。

2.6 引理

在合成运算下的$\mathbf{Isom}(R^2)$和$O_2(R)$构成一个群

我们先证明$\mathbf{Isom}(R^2)$是一个群，明显的，1_R是一个等距同构，所以$1_R\in\mathbf{Isom}(R^2)$，设φ',φ是等距同构，那么对于所有点P,Q，我们有

$$\begin{aligned}\|(\varphi'\varphi)(P)-(\varphi'\varphi)(Q)\|=&\|\varphi'(\varphi(P))-\varphi'(\varphi(Q))\|\\=&\|\varphi(P)-\varphi(Q)\|\\=&\|P-Q\|\end{aligned}$$

所以$\varphi'\varphi$是等距同构，所以合成是$\mathbf{Isom}(R^2)$中的运算，若$\varphi\in\mathbf{Isom}(R^2)$，那么$\varphi$是一个双射，利用推论2.4，每个等距同构存在一个逆φ^{-1}并且逆元也是等距同构

$$\|P-Q\|=\|\varphi(\varphi^{-1}(P))-\varphi(\varphi^{-1}(Q))\|=\|\varphi^{-1}(P)-\varphi^{-1}(Q)\|$$

利用推论2.4，因为双射是满足结合律的，所以等距同构满足结合律，为此$\mathbf{Isom}(R^2)$是一个群

2.7 推论：

若O,P,Q不是共线的，并且φ,ψ是一个平面上的等距同构且满足$\varphi(P)=\psi(P)$，$\varphi(Q)=\psi(Q)$，那么$\varphi=\psi$

证明：因为O,P,Q是不共线的，所以向量空间R^2上的P,Q是线性无关的。因此$\dim(R^2)=2$，且是一组基，那么任意选择$P=(a,b)$的一个线性变换$\varphi(P)=ka+tb$对于ψ则$\psi=la+sb$因为$\varphi(P)=\psi(P)$，那么$ka+tb=la+sb$有$a(k-l)+b(t-s)=0$当且仅当$k=l,t=s$成立，因为P,Q任意选择，那么$\varphi=\psi$

最后回到对称性上来

例4

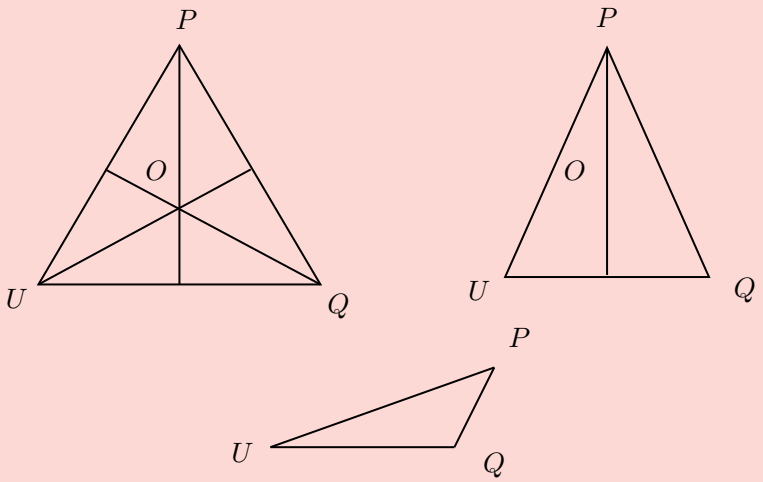
若△是一个三角形且顶点为P,Q,U。并设φ是一个等距同构，则$\varphi(\triangle)$是一个顶点为$\varphi(P).\varphi(Q),\varphi(U)$的三角形。如果我们假设$\varphi(\triangle)=\triangle$，则$\varphi$置换顶点$P,Q,U$。

假设△的中心是O，设△是等腰三角形，并且设ρ_l是一个反射，其中轴$l=L[O,P]$，则$\rho_l(\triangle)=\triangle$（因为中心点在$P$上，这意味着他只是固定点$P$交换$Q,U$）。

另一方面，若△不是等腰三角形，则$\rho_{l'}(\triangle)\neq\triangle$，其中$l'=L[O,Q]$

若△是等边的，并且有$\rho_{l''}(\triangle)=\triangle$，其中$l''=L[O,U]$，那么我们可以把对$l'$和$l''$的反射描写为置换$(P\,U),(P\,Q)$，当△是等腰三角形的时候，反射并没有把△变回自身。因为关于$L[O,Q]$或者$L[O,U]$的变换没有发生跟$L[O,P]$一样对称的情况。

更多的，我们看到等边三角形比等腰三角形是更对称的，因为对于一个等边三角形，我们可以利用关于O的120°和240°度的旋转把每个点归回原位（对于这个旋转，我们可以用一个3–循环置换$(P\ Q\ U)$和$(P\ U\ Q)$描述）。并且用这种关系可知，等腰三角形比一般的三角形更对称（因为有一个反射），因此对于一般的三角形等距同构$\varphi(\triangle)=\triangle$当且仅当$\varphi=1$，即恒等变换



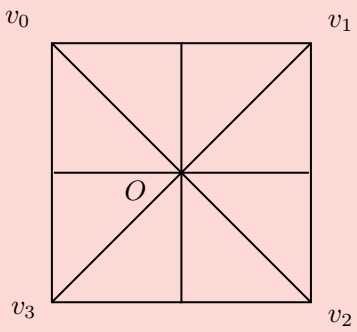
2.8　定义：对称群

平面上的图形Ω的一个对称群$\Sigma(\Omega)$是满足平面上$\varphi(\Omega) = \Omega$的等距同构φ组成的集合，$\Sigma(\Omega)$中的元素称为Ω的对称

所以，对称其实就是一种置换，并且$\Sigma(\Omega)$是一个群

例

- 例如刚才的例子中等边三角形π_3的一个对称群$\Sigma(\Omega)$由其三个顶点P,U,Q组成，且这些顶点的置换个数是群内元素，那么因为置换的排列一共是$n!$中，所以是$3! = 6$个意味着群存在6个元素。分别是三个关于中心轴的反射，$120, 240$的旋转，注意360其实就是恒等置换。所以一共是6个。
- 设π_4是一个边为1的正方形，顶点为$\{v_0, v_1, v_2, v_3\}$，设其中心在原点O，边与坐标轴平行，那么每个$\varphi \in \Sigma(\pi_4)$置换四个顶点。这意味着这个对称$\varphi$由$\{\varphi(v_i) : 0 \leq i \leq 3\}$确定，所以$\pi_4$至多可能存在$24 = 4!$个对称。实际上，若$v_i, v_j$相邻，则$\|v_i - v_j\| = 1$但$\|v_0 - v_2\| = \sqrt{2}$，所以由等距同构可知$\varphi$保持相邻点的位置。但其实只有8个对称是关于$\pi_4$的。除去原点$O$的对称，还有三个关于$90, 180, 270$度的旋转，并带上4个反射，其轴分别为：$x, y$和$L[v_0, v_2], L[v_1, v_3]$。



且，群$\Sigma(\pi_4)$称为有8个元素的二面体群并记为D_8

- 正五边形π_5 有顶点$v_0, \cdots, v_4$和一个原点O，且它的一个对称群$\Sigma(\pi_5)$有10个元素,其中包括关于原点O的5个旋转：$(72j)°$，$1 \leq j \leq 4$，还有5个关于轴$L[O, v_k]$，$0 \leq k \leq 4$的反射，类似上面的，我们也把这个有10个对称的群$\Sigma(\pi_5)$也叫做二面体群并记为D_{10}

2.9　定义：二面体群

一个有$2n$个元素的群D_{2n}叫二面体群，若它含有一个阶数为n的元素a和阶数为2的元素b满足$bab = a^{-1}$

若$n = 2$，是一条线,两个顶点为A, B，那么有旋转180度。恒等变换和两个反射。设旋转为a，而以线段中点为轴的反射为b，那么$a(AB) = BA$在$b(BA) = AB$，并且$b(AB) = BA$且$a(BA) = AB$满足交换，所以D_4是一个阿贝尔群。

当$n \geq 3$的时候，D_{2n}其实不是一个阿贝尔群（可以用等边三角形验算）。且实际上只存在一个含$2n$个元素的二面体群。或者说任意两个这样子的二面体群同构。

2.10　定理：二面体群

正n边形π_n的对称群$\Sigma(\pi_n)$是一个有$2n$个元素的二面体群

证明：设平面π_n有顶点$v_0, \cdots, v_{n-1}$和原点O，定义a是一个饶点O转$(360/n)°$的旋转。

$$a(v_i) = \begin{cases} v_{i+1} & 0 \leq i < n-1 \\ v_0 & i = n-1 \end{cases}$$

根据这个定义，我们可以很清楚的看到a的阶数为n，现在我们定义b是一个以轴$L[O, v_0]$的反射，那么

$$b(v_i) = \begin{cases} v_0 & i = 0 \\ v_{n-i} & 1 \leq i \leq n-1 \end{cases}$$

而反射的阶为2，且存在n个不同的对称$1, a, a^2, \cdots, a^{n-1}$(因为$a$的阶数是$n$)，并且$b, ab, a^2b \cdots, a^{n-1}b$都是不同的（利用消去律）。那么$a, b$加起来有$2n$个运算，若存在$a^s = a^r b$，则说明不存在$2n$个，为此我们要证明的就是这两种运算除了恒等变换以外是不存在相等的元素的。

那么只需要证明$a^r \neq b$即可。当取v_0的时候b是恒等置换，而$a^r(v_0) = v_r \neq v_1$。当取v_1时，交换v_1, v_{n-1}，由于旋转保持相邻性而v_1被v_{n-2}和v_0夹着，这意味着无论如何旋转都无法使得$a^r = b$所以，因为要验证思路，那么这意味着我们有$a^s = a^r b$这种变换是不存在的就行。

不妨假设$a^s = a^r b$其中$0 \leq r \leq n-1$且有$s = 0, 1$，当$s = 0$的时候是恒等变换。那么有

$$a(v_i) = a^r b(v_i) = v_0$$

当$i = n-1$的时候变换a满足条件，但对于变换b则需要v_0而$a^r b(v_{n-1}) = a^r(v_0) = a_r$，所以对于任何的$r, s$，这样子的变换是不存在的。所以这样子的变换只可能有$2n$个并且我们已经展示出来了。

第二种证明：

由消去律得到

$$a^{r-s} = b$$

那么对于v_0有$a^{r-s}(v_0) = v_{r-s} \neq v_0 = b$，由于旋转保持相邻性，所以任意选的点都不满足我们的假设条件，所以对称一共有$2n$个

现在来证明唯一性：设π_n的中心O在原点，并且对没每个对称φ都固定原点，那么φ是一个线性变换（利用推论2.4），顶点v_0相邻的是v_1和v_{n-1}，且是最靠近v_0的顶点。因此，若$2 \leq 2 \leq n-2$都有$\|v_i - v_0\| > \|v_1 - v_0\|$，因此若$\varphi(v_0) = v_j$，那么$\varphi(v_1) = v_{j+1}$或者$v_{j-1}$。对于第一种情形，利用推论2.7，若$\varphi$对$v_0, v_1$有$a^j(v_0) = \varphi(v_0)$，和$a^j(v_1) = \varphi(v_1)$，那么$a^j = \varphi$，第二种情况，如果$a^j b(v_0) = v_j$，$a^j b(v_1) = v_{j-1}$，利用推论2.7依然有$a^j b = \varphi$，所以$|\Sigma(\Omega)| = 2n$

我们已经证明了$\Sigma(\Omega)$是一个有$2n$个元素的群，且包含有n阶和2阶的元素a, b。最后我们只需要证明$bab = a^{-1}$就行。依然是利用推论2.7，我们只需要计算v_0和v_1的值就行了，其中$bab(v_0) = ba(v_0) = b(v_1) = v_{n-1} = a^{-1}(v_0)$，并且$bab(v_1) = v_0 = a^{-1}(v_0)$

对称是在微积分中描述平面中的几何图形产生的，我们用有一些对称的例子，这些可能是关于曲线$f(x, y) = 0$的对称

1. 关于x轴的对称：当y替换为$-y$的时候曲线的方程不变
2. 关于y轴的对称：当x替换为$-x$且$-x$的时候曲线的方程不变
3. 关于原点的对称：当x替换为$-x$且y替换为$-y$时曲线的方程不变
4. 关于直线$y = x$的对称：当x, y互换的时候方程不变。

用我们自己的话来说：第一个对称是p_x即关于x轴的反射，第二个是p_y，即关于y轴的反射，第三个是R_{180}，即180度的旋转。第四个是p_L，L是45°的直线。

3 习题

3.1 计算题

1. 计算阶数、逆、和置换的奇偶性

$$\alpha = (1\ 2)(4\ 3)(1\ 3\ 5\ 4\ 2)(1\ 5)(1\ 3)(2\ 3)$$

为了计算阶数，我们需要知道满足$\alpha^k = 1$的最小的k是多少，对于这个分解，我们知道若$k = 5$则可以很好的保证$\alpha^5 = 1$，但第一件事，我们先分解这个置换$1 \to 3 \to 5$所以第一个括号写上(1 5，以此类推输入5有$5 \to 1 \to 3 \to 4$，那么有(1 5 4有$4 \to 2 \to 1$ 那么就是(1 5 4)，现在剩下有$2, 3$继续有$2 \to 3 \to 1 \to 5 \to 4 \to 3$，写下(2 3最后有$3 \to 2 \to 1 \to 2$有(2 3)，最后的结果就是

$$\alpha = (1\ 5\ 4)(2\ 3)$$

所以它的阶是6，它的一个逆是(2 3)(4 5 1)，因为$\text{sgn}\alpha = (-1)^{5-2} = -1$，所以是奇置换。

1. S_5和S_6中含有多少个阶数为2的元素
2. S_n中含有多少个2阶的元素

首先S_5中的对换有$\frac{5\times4}{2} = 10$，并且利用命题1.16的3可知，$(a\ b)(c\ d)$的阶数也是2，所以$(a\ b)(c\ d)$的个数有$\frac{5\times4\times3\times2}{2^3} = 15$，所以一共是25个。

接下来，S_6中的二阶置换有$(a\ b)(a\ b)(c\ d)$ $(a\ b)(c\ d)(e\ f)$三种，那么就有$15 + 45 + 15 = 75$个

若n是一个偶数，那么就含有

$$\sum_{i=1}^{n} \frac{n(n-1)\cdots(n-i+1)}{(n/2)!2^{(n/2)}}$$

个，其中k是含有置换的个数。若是奇数，只需要把n变成$n-1$再利用上述

公式则有

$$\sum_{i=1}^{n} \frac{n(n-1)\cdots(n-i+1)}{[(n-1)/2]!2^{[(n-1)/2]}}$$

设y是群G内一个阶数为m的元素，若对于一个素数p有$m = pt$，证明y^t阶数为p

证明： 由于y的阶数为m，则有$y^m = 1$。对于一个幂次p，因为有$m = pt$其中p是素数，那么利用命题1.13的2有$(y^t)^p = y^{pt} = y^m = 1$，所以$y^t$的阶为$p$

设G是一个群，对于素数p有$a \in G$是一个阶数为pk的元素，对$k \geq 1$证明若$x \in G$且$x^p = a$，则x的阶为p^2k，并以此可知x比a有更大的阶

证明： 因为$a^{pk} = 1$，而$x^p = a$意味着$(x^p)^{pk} = 1$由命题1.13的2可知$x^{p^2k} = 1$，所以x是一个阶数为p^2k的元素。所以x的阶是比a要大的。

设$G = GL[2, Q]$(在Q域上的2阶可逆矩阵)令

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

证明$A^4 = I = B^6$，但对任何$n > 0$有$(AB)^n \neq I$，并得到结论：两个有限阶的因子A, B可以得到一个无限阶AB的元素（但在有限群中不可能发生）

$$A^4 = A^3A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

而

$$B^6 = B^5B = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = I$$

但

$$(AB)^n = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^n$$

那么有

$$(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

对n进行归纳有

$$(AB)^{n-1}(AB) = \begin{pmatrix} 1 & 1-n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

对任意n成立，所以$(AB)^n$是无限阶的。

对每个群G中的元素$x \in G$有$x^2 = 1$，证明G是一个阿贝尔群。

证明：要证对$y \in G$有$xy = yx$，那么设$(xy)^2 = (xy)(xy) = 1$，因为群是满足结合律的，那么$(xy)^2 = x(yx)y = 1$，只能有$xy(yx) = 1$否则矛盾，这意味着xy是可交换的，所以有$xy = yx$

设G是一个有限群，G中的每个元素x都有一个平方根，即对每个$x \in G$都有$y \in G$使得$y^2 = x$，证明里面每个G中的元素都有唯一的平方根

令$f : G \to G$是一个函数，其中$f(x) = x^2$，由于每个元素都有一个平方根，这说明$f(x) = x^2$是一个满射。

现在证明函数是一个单射，由于G是有限群，并且$f(x)$是一个满射，则G中的每个元素x至多有一个对应的。所以$f(x)$是一个单射，f是满射又是单射，所以是一个双射，这意味着G中元素的都有唯一的平方根。

设G是一个群，其元素个数为偶数，证明G中阶为2的元素个数是奇数，特别的，G一定含有阶为2的元素。

由于G是一个具有偶数个元素的群，则对每个G中元素$a \in G$都有一个相应的逆元a^{-1}对应满足$g^2 = 1$，利用上述关系配对并去除$a = e$的情况，则a, a^{-1}是俩俩存在的

另外，对于阶数大于2的元（若存在），因为逆元是唯一的，由于单位元是唯一的，所以每个阶数大于2的元都是成对出现的。所有：单位元+二

阶+大于二阶的元素是偶数，其中有单位元加二阶的总个数也是偶数的，但1只有一个，所以二阶元的个数是奇数的。

对$n=1,2,\cdots,10$中S_n中元素最大的阶数为多少

利用命题1.16首先，对于一个S_n，我们可以假设是由任意的不相交置换得到的。由于置换简化后和简化前的阶是一样的，那么我们的任务就是分解n为k个数相加，然后乘起来就是最大的阶。

$n=1$时，最大阶是1，$n=2$为2，$n=3$的时候有$1+3$然后乘起来有3，对于4，注意$(a\ b)(c\ d)$的阶是2不是4，所以我们排除这种有相同元素的。所以$4=1+2+1,2+2$是2，$n=5$有$2+3=1+2+3=2+2+1=1+1+1+1+1$所以最大的阶是6，对于$n=6$则有$6=4+2$所以是8，$n=7=3+4$有12，$n=8=3+5=15$，对于$n=9$有$4+5$为20，当$n=10$的时候有$4+6$有24，所以它们各自最大的阶为：

$$S_1:1$$
$$S_2:2$$
$$S_3:3$$
$$S_4:4$$
$$S_5:6$$
$$S_6:8$$
$$S_7:12$$
$$S_8:15$$
$$S_9:20$$
$$S_10:24$$

设$e_1=(1,0)$，$e_2=(0,1)$，若φ是一个平面上固定点O的等距同构，并设$\varphi(e_1)=(a,b)$，$\varphi(e_2)=(c,d)$，且$A=\begin{bmatrix}a & c\\ b & d\end{bmatrix}$，证明$det(A)=\pm1$

e_1,e_2是一个基向量，且

$$\varphi(e_1)=(1,0)A$$
$$\varphi(e_2)=(0,1)A$$

并且两个向量都是距离为1的正方形的两条相邻边。因此变换后依然是一个正方形，因为$\|\varphi(e_1)-\varphi(e_2)\|=\|e_1-e_2\|$ 且变换固定原点

这意味着$\varphi(e_1)\cdot\varphi(e_2)=0$，即$(a,b)\cdot(c,d)=0$有$ac+bd=0$，那其中$c,b\neq 0$，否则有$a/b=d/c$的矛盾式子，所以要么$a=b=0$或者其他的数，但若$a=b=1$，则$\sqrt{(1,1)}=\sqrt{2}$或者其他数都不满足等距(因为这是在说$\sqrt{a^2+b^2}=1$有其他解)，并且有$b=c\neq 0$，所以$b=c=1$，并且每种都有两个可能，$b=\pm 1=c$，我们应用到矩阵上有

$$A=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

所以此情况下$det(A)=-1$，当其中有一个是-1的时候，$det(A)=0-(-1)=1$，所以这个矩阵的行列式值只能是± 1，对另一种$a=b\neq 0$但$b=c=0$的情况也是如法炮制。