群

2023 年 5 月 26 日

目录

1 置换

这一节我们讲置换。

1.1 定义：排列

我们设X是一个集合，则X中的一个表指的是函数$f:\{1,2,3,\cdots,n\}\to X$，若$X$中的表是双射，则称$f$为$X$的一个排列

若f是一个表，我们记它的值$f(i)$为x_i，其中$1\le i\le n$。所以X中的表是一个$n-$元组$(x_1,x_2,\cdots,x_n)$我们说表f是单射，指的是其中不存在重复的**坐标**[若$i\neq j$，则$x_i=f(i)\neq f(j)=x_j$]。我们说f是满射，指的是每个$x\in X$作为某个坐标出现，那么X的排列是X的所有元数组组成的一个无重复的$n-$元组$(x_1,x_2,\cdots,x_n)$。例如，$X=\{a,b,c\}$有27个表和6个排列

$$abc;acb;bac;bca;cab;cba$$

而对于表，我们数一下不是双射的映射$|X|=3$，则我们的映射从1到3有

$$\begin{aligned}
&f:\{1,2,3\}\to a \quad && f:\{1,2,3\}\to a,b,c\\
&f:\{1,2,3\}\to b && f:\{1,2,3\}\to a,c,b\\
&f:\{1,2,3\}\to c && f:\{1,2,3\}\to b,a,c\\
& && f:\{1,2,3\}\to b,c,a\\
& && f:\{1,2,3\}\to c,a,b\\
& && f:\{1,2,3\}\to c,b,a
\end{aligned}$$

不满足满射的有18个即

$$\begin{aligned}
&f:\{1,2\}\to a \quad && f:\{3\}\to b\\
&f:\{1,2\}\to a && f:\{3\}\to c\\
&f:\{1,2\}\to b && f:\{3\}\to a\\
&f:\{1,2\}\to b && f:\{3\}\to c\\
&f:\{1,2\}\to c && f:\{3\}\to a\\
&f:\{1,2\}\to c && f:\{3\}\to b
\end{aligned}$$

把$f:\{1,2\}$中的$\{1,2\}$换成$\{2,3\}$和$\{1,3\}$就得到了另外12种。所以合起来一共是18种

1.2　定义：置换

设X是一个集合（可能是无限集），X的一个置换指的是双射$\sigma : X \to X$

给定一个有限集X，$|X| = n$，我们设$\psi : (1, 2, 3, \cdots, n) \to X$是一个排列，当然，$\psi$是双射。若$f : \{1, 2, \cdots, n\} \to X$是一个$X$的排列，则$f \circ \psi^{-1} : X \to X$是一个置换，但我们都知道实际上这只是一个排列，其次$a : X \to X$是一个关于X的置换，我们有$a \circ \psi : \{1, 2, \cdots, n\} \to X$是$X$的一个排列。所以，置换和排列其实是同一个东西，但只是描述不一样。若$X = \{1, 2, \cdots, n\}$，我们利用一个二行记号来表示置换α

$$a = \begin{pmatrix} 1 & 2 & \cdots & j & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(j) & \cdots & \alpha(n) \end{pmatrix}$$

底行就是一个排列$\alpha(1), \cdots, \alpha(n)$

1.3　定义：对称群

集合X所有的置换构成的族，记为S_X，称为X上的对称群，S_X通常记为S_n，并称为n次对称群。

注意的是，一个S_3的合成并不交换，我们考虑

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

它们的合成是这样的，例如$\alpha \circ \beta$，我们先把β的一个映射写出来，例如$\beta(2) = 1$，那么$\alpha(\beta(2)) = \alpha(2) = 3$，则$\alpha \circ \beta = \alpha(2, 1, 3) = (3, 2, 1)$，即

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

且用同样的方法，我们得到$\beta \circ \alpha$有

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

这意味着$\alpha \circ \beta \neq \beta \circ \alpha$不满足交换律，但有些置换是可以交换的，例如

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \ \delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

其中$\gamma \circ \delta = (2,1,4,3)$，而$\delta \circ \gamma = (2,1,4,3)$满足交换。

但S_X中的合成是满足消去律的。

> 若$\gamma \circ \alpha = \gamma \circ \beta$，则$\alpha = \beta$

这是因为

$$
\begin{aligned}
\alpha =& 1_X \circ \alpha \\
=& (\gamma^{-1} \circ \gamma) \circ \alpha \\
=& \gamma^{-1} \circ (\gamma \circ \beta) \\
=& (\gamma^{-1} \circ \gamma) \circ \beta \\
=& \beta
\end{aligned}
$$

同样的，我们可以证明$\alpha \circ \gamma = \beta \circ \alpha \Rightarrow \alpha = \beta$，但这个二行记号还是挺恼火的，而且，如果我们想表达一个置换的m次幂为恒等函数的正整数m最少取多少？我们把一个置换分解成一个更简单的置换呢？对于这种问题，我们不能直观的看到，所以我们要用其他的方法解决，**首先我们先简化一些符号，我们把$\beta \circ \alpha$记为$\beta\alpha$，而且1_X记为(1)**

1.4 定义：移动-固定

设$a \in S_n$，$i \in \{1,2,3,\cdots,n\}$，若$a(i) = i$，则称a固定i，若$a(i) \neq i$，则称a移动i

1.5 定义：循环置换

设$a \in S_n$，且$i_1,\cdots,i_r$是$\{1,2,\cdots,n\}$中的不同整数，若

$$a(i_1) = i_2, a(i_2) = i_3, \cdots, a(i_{r-1}) = i_r, a(i_r) = i_1$$

且a固定其他整数（如果还有的话），则称a为$r-$循环置换。我们也可以说a是一个长度为r的循环置换

这意味着，一个循环置换会交换i_r的位置并固定其他数。例如一个$2-$循环置换就会交换i_1和i_2的位置并固定其他的数，所以$2-$循环置换也叫对换。$1-$循环置换则是一个恒等函数，因为固定每个i恒有$(i) = (1)$

我们考虑置换

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

当你直接看的时候你并不能知道这是一个5−循环置换，其中$a(1)=4$, $a(4)=5, a(5)=2, a(2)=3, a(3)=1$。所以我们引入一个新的记号，一个$r$−循环置换$a$被记为

$$a=(i_1 i_2 \cdots i_r)$$

那么我们把刚才的循环记为$a=(1\,4\,5\,2\,3)$一些例如为

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

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

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

注意!

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

不是循环置换，注意到其中$1,2$互相交换，和$3,4$互相交换，而定义告诉我们2的下一个元素应该是3，4的下一个元素应该是1。所以这其实是两个置换，$\beta=(1\,2)(3\,4)$

现在，我们来给出一个算法，把置换分解为一些循环置换的乘积，我们取

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&4&7&2&5&1&8&9&3\end{pmatrix}$$

我们从写(1开始，$a:1\to 6$，那么括号里添6有(1 6，又因为$a:6\to 1$，那么循环关闭，有$(1\,6)$，接下来我们从2继续，$a:2\to 4$且$a:4\to 2$，那么接下来的循环就是$(1\,6)(2\,4)$，我们继续剩下的最小数从3开始，那么$a:3\to 7, a:7\to 8$, $a:8\to 9$, $a:9\to 3$，接下来的循环就是$(1\,6)(2\,4)(3\,7\,8\,9)$剩下最后的$a(5)\to 5$，我们断言

$$a=(1\,6)(2\,4)(3\,7\,8\,9)(5)$$

由于函数中的乘积是合成，所以我们断言对1到n之间的每个i都存在

$$a(i)=[(1\,6)(2\,4)(3\,7\,8\,9)(5)](i)$$

我们验算一下，事实上，对于这个合成，我们不妨记$\beta=(1\,6),\gamma=(2\,4),\delta=(3\,7\,8\,9)$，那么这个合成就是$\beta\gamma\delta$，但我们将忽略(5)，因为这是个恒等函数，将会一直固定。现在$a(1)=6$，我们把置换看成函数然后取合成，假设$i=1$，则

$$\begin{aligned}\beta\gamma\delta(1)=&\beta(\gamma(\delta(1)))\\=&\beta(\gamma(1)) && \text{因为}\delta\text{固定}1\\=&\beta(1) && \text{因为}\gamma\text{固定}1\\=&6\end{aligned}$$

把一个置换分解为多个循环置换的乘法是非常方便的，但是对于一些置换可能需要化简，例如

$$\sigma=(1\,2)(1\,3\,4\,2\,5)(2\,5\,1\,3)=abc$$

先输入1,那么在c有$c(1)=3$，$b(3)=4$，所以循环从$(1,4$开始。然后$b(4)=2,a(2)=1$，为此第一个闭环就是$(1,4)$。接着固定2，因为2是没有考虑的最小数，所以带入2有$c(2)=5,b(5)=1,a(1)=2$，所以2只是一个单循环，所以循环从$(1,4)(2)$开始。然后我们从3开始，4已经在第一个循环里了。$c(3)=2,b(2)=5,a(5)=5$，然后从5开始，$c(5)=1,b(1)=3,a(3)=3$，最后一个循环就是$(3,5)$所以简化后的置换是$\sigma=(1\,4)(2)(3\,5)$

1.6 定义：置换不相交

两个置换$\alpha,\beta\in S_n$是不相交的，若每个i被其中一个固定而另一个移动，若$\alpha(i)\neq i$，则$\beta(i)=i$，或者$\beta(j)\neq j$而$\alpha(j)=j$，一族置换$\beta_1,\cdots,\beta_t$是不相交的，若对每对置换都是不相交的。

考虑一个循环置换的特殊情况，若$a=(i_1\cdots i_r),\beta=(j_1\cdots j_t)$，则$\{i_1,i_2,\cdots,i_r\}\cap\{j_1,j_2,\cdots,j_t\}$指的是被$a$和$\beta$移动。所以，若两个循环置换是不相交的，则$\{i_1,i_2,\cdots,i_r\}\cap\{j_1,j_2,\cdots,j_t\}=\emptyset$

所以，当置换a,β不相交时，对i刚刚好有3种可能，被a移动，被β移动，或者都不动。

1.7 引理

不相交置换$a, \beta \in S_n$是交换的。

证明： 我们只需要证明对$1 \leq i \leq n$，则$a\beta(i) = \beta a(i)$，若β移动i部分设$\beta(i) = j \neq i$，则β也移动j，因为a, β不相交，则$a(i) = i$, $a(j) = j$，所以$\beta a(i) = j = a\beta(i)$

特别的，不相交的循环置换是交换的。

1.8 引理

设$X = \{1, 2, \cdots, n\}$,$a \in S_X = S_n$，$i_1 \in X$，则对所有$j \leq 1$归纳地定义$i_j : i_{j+1} = a(i_j)$，记$Y = \{i_j \mid j \leq 1\}$，并设$Y'$为$Y$的补集

1. 若a移动i_1，则存在$r > 1$使得$i_1, \cdots, i_r$互异，且$i_{r+1} = a(i_r) = i_1$
2. $a(Y) = Y$,$a(Y') = Y'$

证明： 因为X是有限集，所以存在最小的$r > 1$使$i_1, \cdots, i_r$互异，但是$i_{r+1} = a(i_r) \in \{i_1, \cdots, i_r\}$，即对$1 \leq j \leq r$有$a(i_r) = i_j$，若$j > 1$，则$a(i_r) = i_j = a(i_{j-1})$，由于$a$是个单射，所以$i_r = i_{j-1}$。且$j-1 = r$，那么当$r = 1$的时候$j$没有对应的数，所以存在两个数$i_{j_a} = i_{j_b} = i_1$这与$i_1, \cdots, i_r$互异矛盾，所以$i_j = i_1 = a(i_r)$

对于命题2，显然$a(Y) \subseteq Y$，因为$a(i_j) = i_{j+1} \in Y$。若$k \in Y'$，则$a(k) \in Y$或者$a(k) \in Y'$由于Y'是Y的补集，所以$X = Y \cup Y'$，若$a(k) \in Y$，则对某个j有$a(k) = i_j = a(i_{j-1})$，因为a是单射，所以$k = i_{j-1} \in Y$与$Y \cap Y' = \emptyset$矛盾。所以$a(Y') \subseteq Y'$

最后，我们来证明等号，因为$a(X) = a(Y \cup Y') = a(Y) \cup a(Y')$，是两个不相交的集合的并，由于$a$是个单射且$a(Y) \subseteq Y$意味着$|a(Y)| \leq |Y|$和$a(Y') \subseteq Y'$有$|a(Y')| \leq |Y'|$若其中存在严格的不等式，可得$|a(X)| < X$，但$a$是一个满射，$a(X) = X$是矛盾，为此$a(Y) = Y$, $a(Y') = Y'$

1.9 命题

每个置换$a \in S_n$或是一个循环置换，或是不相交循环置换的乘积

证明：我们对a移动的点的个数做归纳，基础步骤$k = 0$成立。因为这个时候a是恒等函数。

若$k > 0$，则存在被a移动的点，我们设为i_1，接着定义$Y = \{i_1, i_2, \cdots, i_r\}$，其中$i_1, \cdots, i_r$是互异的，对每个$j < r$，都有$a(i_j) = i_{j+1}$，且$a(i_r) = i_1$，我们设一个循环$\sigma \in S_X$为$r-$循环，它表示为$(i_1 i_2 \cdots i_r)$，所以循环$\sigma$固定$Y'$的每个点（$Y'$为集合$Y$的补集），如果还有的话，若$r = n$，则$a$取$\sigma$就是一个循环置换，如果$r < n$，则$a(Y') = Y'$，为了找出循环置换的乘积，我们定义与$\sigma$不相交的定义$a' = a\sigma^{-1}$，这样子当$\sigma$移动$i$的时候就有$i = i_j \in Y$，但对于$a'$有$a'(i_j) = a(\sigma^{-1}(i_j)) = a(i_{j-1}) = i_j$，说明$a'$对$Y$的元素固定。我们假设$a'$移动其他的点$i'$，则$i' \in Y'$。因为$a'$对$Y$的元素固定，所以$\sigma$固定$i'$，我们得到关于$a$的两个不循环乘积有$a = a'\sigma$，则被$a'$移动的点的个数是$k - r < k$，所以由归纳假设得到$a' = \beta_1\beta_2 \cdots \beta_t$是不相交的循环置换，所以$a = a'\sigma = \beta_1\beta_2 \cdots \beta_t\sigma$是不相交循环置换的乘积，证毕

1.10 定义：完全分解

置换α的一个完全分解指的是：将α分解成不相交循环置换的乘积且含有关于被α固定的每个i的$1-$循环置换(i)

例如，我们给定

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

则我们可以得到一个完全分解$\alpha = (1)(2\ 3\ 4)(5)$，但是，如果我们隐去$1-$循环置换，则分解$\alpha = (2\ 3\ 4) = (1)(2\ 3\ 4) = (2\ 3\ 4)(5)$都不是完全分解，因为一个完全分解$\alpha = \beta_1 \cdots \beta_t$中$1$和$n$的每个符号$i$在这些$\beta$都恰好出现一次。

若$\beta \in S_n, k \geq 0$，我们归纳地定义β的幂为$\beta^0 = (1), \beta^{k+1} = \beta\beta^k$，所以如果我们记$\beta = (i_0 \cdots i_{r-1})$，那么$i_1 = \beta(i_0), i_2 = \beta(i_1) = \beta^2(i_0)$，以此类推，$i_{r-1} = \beta^{r-1}(i_0)$。且对所有的$k \leq r-1$有

$$i_k = \beta^k(i_0)$$

1.11 引理

1. 设$\alpha = \beta\delta$是不相交置换的积，若β移动i，则对所有的$k \geq 1$，存在$a^k(i) = \beta^k(i)$
2. 若β, γ是移动$i = i_0$的循环置换的积，且对所有$k \geq 1$有$\beta^k(i) = \gamma^k(i)$，则$\beta = \gamma$

证明：由于β移动i，所以由不相交可知δ对i固定。所以满足交换，有$(\beta\delta)^k(i) = \beta^k(\delta^k(i)) = \beta^k(i)$，证毕

对命题2，我们设$\beta = (i_0 i_1 \cdots i_{r-1})$，则对所有的$k < r - 1$有$i_k = \beta^k(i_0)$，类似的，设$\gamma = (i_0 j_1 \cdots j_{s-1})$，则对$j < s - 1$有$j_k = \gamma^k(i_0)$，对此，我们假设$r \leq s$使得$i_1 = j_1, \cdots, i_{r-1} = j_{r-1}$，有$j_r = \gamma^r(i_0) = \beta^r(i_0) = i_0$，所以$s - 1 = r - 1$，这意味着对所有的$k$都有$j_k = i_k$，所以$\beta = \gamma = (i_0 i_1 \cdots i_{r-1})$

1.12 定理：算数基本定理的其他表述

设$\alpha \in S_n$，$\alpha = \beta_1\beta_2 \cdots \beta_t$是一个完全分解，若不考虑循环置换出现的顺序，则这个分解是唯一的。

证明：设$\alpha = \gamma_1 \cdots \gamma_s$是关于$\alpha$的另一个分解，由于$\alpha$的每个完全分解对于每个被$\alpha$固定的数$i$都恰好是一个1−循环。所以实际上我们只需要对$t, s$中的较大者做归纳证明长度$l > 1$的循环置换由$\alpha$唯一确定即可。

基础步骤是显然的，对于长度$l = 1$，我们假设$\alpha = \beta_1 = \gamma_1$

现在开始证明归纳步骤，注意到，若β_t移动$i = i_0$，利用引理1.11则对于$\beta_t^k(i_0) = a^k(i_0)$，那么对于置换$\gamma$来说，某个$\gamma_j$也移动$i_0$，由于不相交循环置换交换，则我们只需要重新编排有$\gamma_s$。跟刚才一样，对于每个$k$都有$\gamma_s^k(i_0) = a^k(i_0)$，利用1.11的命题2可知$\gamma_s = \beta_t$利用消去律就剩下

$$\beta_1 \cdots \beta_{t-1} = \gamma_1 \cdots \gamma_{s-1}$$

因为$s = t = 1$是成立的，对此由归纳假设有$s = t$，则重新排列有$\gamma_1 = \beta_1, \cdots, \gamma_{t-1} = \beta_{t-1}$

置换都是一个双射，现在我们得解决如何找到一个置换的逆，在前面我们定义一个逆的时候是针对一个元素的。但面对一整个置换，我们可以

把置换β看成是一个圆周的顺时针旋转，圆周上的点是被置换的元素。而逆β^{-1}是逆时针旋转。

1.13　命题：置换的逆

1. 循环置换$\alpha = (i_1 i_2 \cdots i_r)$的逆为$(i_r i_{r-1} \cdots i_1)$，即

$$(i_1 i_2 \cdots i_r)^{-1} = (i_r i_{r-1} \cdots i_1)$$

2. 若$\gamma \in S_n$ 且$\gamma = \beta_1 \cdots \beta_k$，则

$$\gamma^{-1} = \beta_k^{-1} \cdots \beta_1^{-1}$$

注意γ^{-1}的因子被颠倒过来了

证明： 若$a \in S_n$，我们只需要证明$\alpha\alpha^{-1} = (1)$即可。那么$(i_1 i_2 \cdots i_r)$ $(i_r i_{r-1} \cdots i_1)$固定1到n之间不同于$i_1, \cdots, i_r$的每个整数。而这个合成对$i_j (j \geq 2)$都有$i_j \to i_{j-1} \to i_j$，并且$i_1 \to i_r \to i_1$所以1到n之间的每个整数都被这个合成固定，所以这个置换是(1)。所以

$$(i_1 i_2 \cdots i_r)^{-1} = (i_r i_{r-1} \cdots i_1)$$

对于另一个命题，我们对$k \geq 2$用归纳法，对基础步骤$k = 2$，有

$$(\beta_1\beta_2)(\beta_2^{-1}\beta_1^{-1}) = \beta_1(\beta_2\beta_2^{-1})\beta_1^{-1} = \beta_1\beta_1^{-1} = (1)$$

类似的我们有$(\beta_2^{-1}\beta_1^{-1})(\beta_1\beta_2) = (1)$，现在由于基础步骤成立，我们做归纳，设$\delta = \beta_1 \cdots \beta_k$，那么有$\beta_1 \cdots \beta_k\beta_{k+1} = \delta\beta_{k+1}$

$$\begin{aligned}(\beta_1 \cdots \beta_k\beta_{k+1})^{-1} =&(\delta\beta_{k+1})^{-1}\\ =&\beta_{k+1}^{-1}\delta^{-1}\\ =&\beta_{k+1}^{-1}(\beta_1 \cdots \beta_k)^{-1}\\ =&\beta_{k+1}^{-1}\beta_k^{-1} \cdots \beta_1^{-1}\end{aligned}$$

所以，$(1\,2\,3\,4)^{-1} = (4\,3\,2\,1)$，化简一下就是$(1\,4\,3\,2)$，同样的$(1\,2)^{-1} = (2\,1)$化简有$(1\,2)$，所以它的对换都等于自身。

例2

特别的，若因子是不相交的循环置换，则对命题1.13的结果也成立，因为不相交置换满足交换律。若

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&4&7&2&5&1&8&9&3\end{pmatrix}$$

则$\alpha=(1\,6)(2\,4)(3\,7\,8\,9)(5)$且有

$$\begin{aligned}\alpha^{-1}=&(5)(9\,8\,7\,3)(4\,2)(6\,1)\\=&(1\,6)(2\,4)(3\,9\,8\,7)\end{aligned}$$

1.14 定义：相同结构

设$\alpha,\beta\in S_n$，若它们有相同循环结构，当且仅当对每个$r\geq 1$，完全分解具备相同数量的$r-$循环置换。

现在给出一个例子，对于S_n中存在

$$(1/r)[n(n-1)\cdots(n-r+1)]$$

个$r-$循环置换。如果某种置换分解为几个相同长度的循环置换的积，则我们可以用这个公式计算这种置换的个数。例如，S_4中形如$(a\;b)(c\;d)$的置换个数为

$$(1/2)[(1/2)(4\times 3)]\times[1/2(2\times 1)]=3$$

对$(a\,b)$，a有4种选法，b是三种，所以就是4×3，因为$(a\,b)(c\,d)=(c\,d)(a\,b)$，为此我们在$1/2[4\times 3]$外乘上$1/2$避免计算了两次次数。类似的，我们还可以计算$S_n$中形如$(a\;b)(c\;d)(e\;f)$的循环个数，一共有

$$\frac{1}{3!2^3}[n(n-1)(n-2)(n-3)(n-4)(n-5)]$$

其中2^3是一开始给的定义，而3!是为了去除类似$(c\,d)(a\,b)(e\;f)$这类重复的排列。则

循环结构	个数
(1)	1
(1 2)	6
(1 2 3)	8
(1 2 3 4)	6
(1 2)(3 4)	3
总计：	24

1.15　引理：

设$\alpha, \gamma \in S_n$，对于所有的i，如果$\gamma : i \to j$，则$\alpha\gamma\alpha^{-1} : \alpha(i) \to \alpha(j)$

这个证明非常简单，

$$\alpha\gamma\alpha^{-1}(a(i)) = \alpha\gamma(i) = \alpha(j)$$

1.16　命题：

1. 若$\gamma, \alpha \in S_n$，则γ和$\alpha\gamma\alpha^{-1}$具有相同结构
2. 若$\gamma, \gamma' \in S_n$，则γ和γ'具有相同循环的结构当且仅当存在$a \in S_n$使得$\gamma' = \alpha\gamma\alpha^{-1}$

证明：假设γ和γ'具有相同的结构，记$\gamma = \beta_1 \cdots \beta_t$和$\gamma' = \sigma_1 \cdots \sigma_t$是完全分解，其中对所有$\lambda \le t$，$\beta_\lambda$和$\sigma_\lambda$具备相同长度，我们设$\beta_\lambda = (i_1^\lambda, \cdots, i_{r(\lambda)}^\lambda)$，和$\sigma_\lambda = (j_1^\lambda, \cdots, j_{r(\lambda)}^\lambda)$，且对所有$\lambda$定义

$$\alpha(i_j^\lambda) = j_1^\lambda, \alpha(i_2^\lambda) = j_2^\lambda, \cdots, \alpha(i_{r(\lambda)}^\lambda) = j_{r(\lambda)}^\lambda$$

现在，因为$\beta_1 \cdots \beta_t$是一个完全分解，则对每个$i \in X = \{1, 2, \cdots, n\}$中均只在某个$\beta_\lambda$出现，所以$a(i)$对每个$i \in X$存在定义。而且$a : X \to X$是个单值函数。又由于$\sigma_1 \cdots \sigma_t$是一个完全分解，所以每个$j \in X$在某个$\delta_\lambda$出现，所以$a$是一个满射。因为$a$又单射也是满射，所以$a$是一个双射。并且$a \in S_n$

第二步，我们来证明γ'中的每个循环都可以表示为$\alpha\gamma\alpha^{-1}$。任取γ中一个循环置换，设为$(i\ j\ \cdots)$，假设γ移动其中的i，设$\gamma(i) = j$，那么定义σ为α作用于循环γ上每个符号的的一个置换(即把每个循环内的元素变成$a(i)$，但是不改变循环结构)，那么根据定义，这个循环置换为$(\alpha(i)\,\alpha(j) \cdots)$，即$\sigma : a(i) \to a(j)$，且对于我们的$\alpha\gamma\alpha^{-1}$也有$\alpha\gamma\alpha^{-1} : a(i) \to a(j)$，所

以σ和$\alpha\gamma\alpha^{-1}$的循环内所有符号一样。并且因为a是一个双射，对每个$k \in X$都有$\alpha(i)=k$，所以$\sigma=\alpha\gamma\alpha^{-1}$，而因为$\sigma$具备与$\gamma$相同的循环结构（由定义可得我们只是在循环中改变元素），而且$\sigma=\alpha\gamma\alpha^{-1}$，所以$\alpha\gamma\alpha^{-1}$和$\gamma$具备相同的循环结构。

那么对每个λ，第λ个循环置换是

$$(a(i_1^\lambda)\ a(i_2^\lambda)\cdots a(i_{r(\lambda)}^k))=\sigma_\lambda=\sigma(\beta_\lambda)=\alpha\beta_\lambda\alpha^{-1}$$

所以$\alpha\gamma\alpha^{-1}=\gamma'$，证毕。

例如，我们给出$\gamma=(1\ 3)(2\ 4\ 7)(5)(6)$和$\alpha=(2\ 5\ 6)(1\ 4\ 3)$，则

$$\alpha\gamma\alpha^{-1}=(\alpha1\ \alpha3)(\alpha2\ \alpha4\ \alpha7)(\alpha5)(\alpha6)=(4\ 1)(5\ 3\ 7)(6)(2)$$

例3

若

$$\gamma=(1\ 2\ 3)(4\ 5)(6),\quad \gamma'=(2\ 5\ 6)(3\ 1)(4)$$

则$\gamma'=\alpha\gamma\alpha^{-1}$，为了解出$\alpha$，我们用这么一个记号

$$\begin{pmatrix}\gamma\\ \gamma'\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\2&5&6&3&1&4\end{pmatrix}$$

现在只需要从1走下去就能得到循环

$$(1\ 2\ 5)(3\ 6\ 4)$$

而$\alpha=(1\ 2\ 5)(3\ 6\ 4)$

对于分解，我们有其他有用的形式

1.17　命题：

若$n\geq 2$，则对于每个$\alpha\in S_n$都是一些对换的乘积。方法如下：若$r=1$

证明：我们考虑一个恒等变换(1)，可以分解为$(1\ 2)(1\ 2)$，对于每个置换$(i\ j)=(i\ j)(1\ 2)(1\ 2)$，根据命题1.9，我们只需要将一个$r-$循环置换$\beta$分解为一些对换的乘积。若$r=1$，则$\beta$是一个恒等函数，且$\beta=(1\ 2)(1\ 2)$，若$r\geq 2$，则$\beta$可以分解为

$$\beta=(1\ 2\ \cdots\ r)=(1\ r)(1\ r-1)\cdots(1\ 3)(1\ 2)$$

当$\beta(1)$的时候，$1 \to 2$并且在后面的循环跟$(1\ 2)$不一样则$\beta(1) = 2$，以此类推可以得到下个循环。

所以每个置换都可以通过这种方法变成一系列的置换乘积，但这种方法没有分解为不相交置换乘积那么好，首先，对换不需要满足交换。因为$(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$，其次，无论是因子本身或者因子的数量都不是唯一决定的，例如，我们对S_4下的置换$(1\ 2\ 3)$做分解有

$$\begin{aligned}(1\ 2\ 3) =& (1\ 3)(1\ 2)\\ =& (2\ 3)(1\ 3)\\ =& (1\ 3)(4\ 2)(1\ 2)(1\ 4)\\ =& (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3)\end{aligned}$$

问题是，这些分解是否具备唯一性，我们现在要证明的是，在置换α的所有这样子的分解中，因子个数的奇偶性是相同的，即对换的个数总是偶数个或者奇数个。

例4

一个15−谜题游戏是由一个起始位置构成的游戏，它是由数字$1-15$和空白符号#组成的一个4×4表格，其中包括简单的移动，例如：

3	15	4	12
10	11	1	8
2	5	13	9
6	7	14	#

一个简单的移动便是将#与旁边的符号做交换，例如，这里有两个存在对于起始位置的简单移动。我们交换14和#，或者交换9和#，如果在一系列的简单移动之后，我们把起始位置转化为标准数组$(1, 2, \cdots, 15, \#)$，那么我们就赢得了这个游戏。

我们要分析这个游戏，首先注意到其实这就是一个关于集合$\{1, 2, 3, \cdots, 15, \#\}$的置换。即存在置换$\alpha \in S_{16}$，进一步讲，如果这些格子标上1到$15, \#$，则我们记$a(i)$为实际上占据了第$i$个格子中的数字。那么根据我们给出的例子，我们可以从例子中的起始单位写出置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \# \\ 3 & 15 & 4 & 12 & 10 & 11 & 1 & 8 & 2 & 5 & 13 & 9 & 6 & 7 & 14 & \# \end{pmatrix}$$

其中，每一个简单的移动都是一种特殊的对换，即对#的移动的对换。此外，我们执行从一个位置（对应一个置换β）的简单移动（对应一个特殊的置换τ），结果产生一个对应于置换$\tau\beta$的新位置。例如，若α是上边的位置，而τ是一个关于14和#的对换。则$\tau(\alpha(\#)) = \tau(\#) = 14$和$\tau(\alpha(15)) = \tau(14) = \#$，而对于其他的$i$都有$\tau\alpha(i) = i$，即在原有的构造上除了14和#被互换外，其他的数字都在原有的位置上。为了赢得这个游戏，我们需要一些特殊的变换$\tau_1, \cdots, \tau_m$使得

$$\tau_m \cdots \tau_2\tau_1\alpha = (1)$$

这意味着我们可以通过有限的置换，把每个元素给归回原位。但详细的在等一下我们会继续。

通过刚才的例子，我们选择一些α可以帮助我们赢得比赛，而其他的不行，例如把刚才例子中的#或者14换成其他的数字，则不会发生什么事情。

我们继续来给出一些东西研究15−字谜游戏

1.18 引理

若$k, l \geq 0$且a, b, c_i, d_j是互异的数，则

$$(a\ b)(a\ c_1 \cdots c_k\ b\ d_1 \cdots\ d_l) = (a\ c_1 \cdots\ c_k)(b\ d_1 \cdots d_l)$$

和

$$(a\ b)(a\ c_1 \cdots c_k)(b\ d_1 \cdots\ d_l) = (a\ c_1 \cdots c_k\ b\ d_1 \cdots d_l)$$

证明：第一个我们要证明的等式左边有

$$\begin{aligned}
&a \to c_1 \to c_1; \\
&c_i \to c_{i+1} \to c_{i+1} \quad \text{如果} i < k \\
&c_k \to b \to a \\
&b \to d_1 \to d_1 \\
&d_j \to d_{j+1} \to d_{j+1} \quad \text{如果} j < l \\
&d_l \to a \to b
\end{aligned}$$

而对等式右边的计算类似，对a, b和所有的$c_i\ d_j$这两个置换是一致的。

对第二个等式，我们翻转第一个等式，有

$$(a\ c_1 \cdots\ c_k)(b\ d_1 \cdots d_l) = (a\ b)(a\ c_1 \cdots c_k\ b\ d_1 \cdots\ d_l)$$

然后我们在两边的左侧同乘$(a\ b)$有

$$(a\ b)(a\ c_1 \cdots c_k)(b\ d_1 \cdots\ d_l) = (a\ b)(a\ b)(a\ c_1 \cdots c_k\ b\ d_1 \cdots d_l)$$

我们知道$(a\ b)(a\ b)$是恒等函数，所以就得到了第二个等式。

而关于该引理的一个例子有

$$(1\ 2)(1\ 3\ 4\ 2\ 5\ 6\ 7) = (1\ 3\ 4)(2\ 5\ 6\ 7)$$

1.19 定义

若$\alpha \in S_n$和$\alpha = \beta_1 \cdots \beta_t$是不相交的完全分解，则符号$\alpha$被定义为

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

因为t是由α的循环个数所决定的，而每个不完全相交的乘积是唯一确定的，这意味着$\mathrm{sgn}(\alpha)$是单值函数。若ϵ是1−循环置换，则$\mathrm{sgn}(\epsilon) = 1$，因为这里1−循环置换是$S_1$，且只有一个置换$(i)$这意味着$n = t = 1$，所以$\mathrm{sgn}(\epsilon) = (-1)^{n-t} = (-1)^0 = 1$，若$\tau$是一个对换，则移动两个数字和固定$n-2$个其他数字中的每个数，这意味着对于这$n-2$个数，每个数都是一个1−循环置换。那么对于这个对换，$\tau = (a\ b)$有一个对换，所以$t = 1 + (n-2) = n-1$有$\mathrm{sgn}(\tau) = (-1)^{n-(n-1)} = -1$

1.20 引理

设$\alpha, \tau \in S_n$，其中τ是一个对换，则

$$\mathrm{sgn}(\tau\alpha) = -\mathrm{sgn}(\alpha)$$

证明：我们设$\alpha = \beta_1 \cdots \beta_t$是一个$\alpha$的完全分解，且令$\tau = (a\ b)$，如果$a, b$出现在同一个$\beta$中，则$\beta_1 = (a\ c_1 \cdots c_k\ b\ d_1 \cdots\ d_l)$那么根据引理1.18，$\tau\beta_1 = (a\ c_1 \cdots c_k)(b\ d_1 \cdots\ d_l)$。

这是$\tau\alpha = (\tau\beta_1)\beta_2 \cdots \beta_t$的完全分解，对于其中的循环置换都是俩俩不相交且对于每个数$\{1, 2, \cdots, n\}$都只在一个循环置换中出现。因为$\tau\beta$有2个不相交置换,所以$\tau\beta$存在t+1个循环置换。则$\mathrm{sgn}(\tau\alpha) = (-1)^{n-(t+1)} = -\mathrm{sgn}(\alpha)$

对于a, b不包含在β中的情况，我们设$\beta_1 = (a\, c_1 \cdots\ c_k)$，和$\beta_2 = (b\, d_1 \cdots\ d_l)$，其中$k, l \geq 0$，那么$\tau\alpha = (\tau\beta_1\beta_2) \cdots \beta_t$ ，由我们刚才证明的引理1.18有

$$\tau\beta_1\beta_2 = (a\ c_1 \cdots c_k\ b\ d_1 \cdots d_l)$$

那么$\tau\beta_1\beta_2\cdots\beta_t$有$t-1$个循环置换。则$\mathrm{sgn}(\tau\alpha)=(-1)^{n-t+1}=-\mathrm{sgn}(\alpha)$

1.21 定理

对于任意$\alpha,\beta\in S_n$有

$$\mathrm{sgn}(\alpha\beta)=\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$$

证明：假设$\alpha\in S_n$且可以分解为m个对换$\alpha=\tau_1\cdots\tau_m$的乘积。我们通过对$m$的归纳，对每个$\beta\in S_n$都有$\mathrm{sgn}(\alpha\beta)=\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$，归纳的基础步骤是$m=1$就是我们的引理1.20，对$m=1$我们说$\alpha$是一个对换，当$m>1$的时候，我们设当$\alpha=\tau_2\cdots\tau_m$成立并应用归纳法有

$$\begin{aligned}\mathrm{sgn}(\alpha\beta)=&\mathrm{sgn}(\tau_1\cdots\tau_m\beta)\\=&-\mathrm{sgn}(\tau_2\cdots\tau_m\beta) && \text{利用引理1.20}\\=&-\mathrm{sgn}(\tau_2\cdots\tau_m)\mathrm{sgn}(\beta) && \text{由归纳假设得到}\\=&\mathrm{sgn}(\tau_1\cdots\tau_m)\mathrm{sgn}(\beta)\\=&\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)\end{aligned}$$

成立。

以此类推，我们对$k\geq 2$使用归纳法有

$$\begin{aligned}\mathrm{sgn}(\alpha_1\alpha_2\cdots\alpha_k)=&\mathrm{sgn}(\alpha_1)\mathrm{sgn}(\alpha_2)\cdots\mathrm{sgn}(\alpha_{m-2})\mathrm{sgn}(\alpha_{m-1}\alpha_m)\\=&\mathrm{sgn}(\alpha_1)\mathrm{sgn}(\alpha_2)\cdots\mathrm{sgn}(\alpha_{m-2})\mathrm{sgn}(\alpha_{m-1})\mathrm{sgn}(\alpha_m)\end{aligned}$$

成立

1.22 定义

设置换$\alpha\in S_n$，我们说α是偶置换当且仅当$\mathrm{sgn}(\alpha)=1$，若是奇置换，则有$\mathrm{sgn}(\alpha)=-1$，我们说置换α,β具有相同的奇偶性，当且仅当两者是偶置换或者是奇置换

现在让我们回到置换分解为一些对换乘积上来，在前面的章节中我们看到了很多关于置换的分解(例如：$(1)=(1\ 2)(1\ 2)$)，但似乎这些不同的因子唯一的相似之处在于它们的分解中的奇偶性，为了证明这一明显的说法，我们要证明的是，一个置换不可能既是奇置换又是偶置换的积。

1.23 定理

1. 设$\alpha \in S_n$若α是偶置换，则α可以分解为偶数个对换的乘积。若α是一个奇置换，则它可以分解为奇数个对换的乘积

2. 若$\alpha = \tau_1 \cdots \tau_q = \tau_1' \cdots \tau_p'$是一些对换的积，则$p, q$具有一样的奇偶性。

证明：若$\alpha = \tau_1 \cdots \tau_q$是一些对换的乘积，则由引理1.12有$\mathrm{sgn}(\alpha) = \mathrm{sgn}(\tau_1) \cdots \mathrm{sgn}(\tau_q) = (-1)^q$，因为$\alpha$的对换只移动$2q$个数，并且固定$n-2q$个数，对于这$n-2q$个数，每个数都是一个固定的1−循环置换。所以$\mathrm{sgn}(\tau) = (-1)^{n-(n-2q+q)} = (-1)^q$，所以$q$是偶数，那么$\mathrm{sgn}(\alpha) = 1$，如果是奇的，那么$\alpha = -1$

对于第二个命题，若有两个关于α的分解，我们设一个有奇数个对换，另一个有偶数个对换。若两个分解，则由命题1我们知道，奇置换的符号函数是-1，偶置换的符号函数是1，那么

$$\mathrm{sgn}(\alpha) = -1 = 1$$

是一个矛盾，所以对于两个置换只能是同奇或者同偶

1.24 推论

设$\alpha, \beta \in S_n$，若α和β具备相同的奇偶性，那么$\alpha\beta$是偶置换，反之$\alpha\beta$是奇置换。

证明：若$\mathrm{sgn}(\alpha) = (-1)^q$, $\mathrm{sgn}(\beta) = (-1)^p$，那么由引理1.21可知$\mathrm{sgn}(\alpha\beta) = (-1)^{q+p}$当$q, p$是奇数，设分解$q = 2k_1 + 1$, $p = 2k_2 + 1$，有$q + p = 2(k_1 + k_2 + 1)$是偶数，对于偶数同样显然，则若$q = 2k$, $p = 2k + 1$，则$q + p = 4k + 1$是奇数。

现在让我们回到15−字谜游戏上来，若$\alpha \in S_{16}$是一个起始位置。我们能赢得这个游戏当且仅当α是一个偶置换且固定#，为了证明这个，我们推荐阅读**McCoy 和Janusz**的《近世代数导引》(Intrroduction to Modern Algebra)，而我们对游戏一个方向上的证明是很明显的，不管怎样，空白符号#从格子16开始，每个简单的移动都使得#向上、下、左、右移动。因此对于移动的总次数m，可以被分解为四个整数u, d, l, r的和$u + d + l + r$，其中u指的是向上的运动，d是向下，l是向左，r是向右。若把#移动到原

地，则每个移动都会和另一个移动的次数相消。也就是$u = d$，$l = r$，所以总次数m是偶数$m = 2u + 2r$，就是说，若$\tau_m \cdots \tau_1 \alpha = (1)$，则$m$的次数是偶数。所以我们就得到$\alpha = \tau_1 \cdots \tau_m$，例如$1, 2, 3$，我们有$3, 2, 1$，当我们对换$1, 3$用了6步，由于我们的定理1.17告诉我们置换都是一些对换的乘积，对于这个游戏，我们对换回去再回来要做偶次的对换，且一整个步骤下来只改变了2个数并且固定其他数，这意味着这个置换是偶次的（利用定理1.23因为偶次的置换只能被分解为偶数个对换，因为m是对换的总次数）

$$\alpha = (1\ 3\ 4\ 12\ 9\ 2\ 15\ 14\ 7)(5\ 10)(6\ 11\ 13)(8)(\#)$$

每个数要换回去必须做偶次的对换，因为只有m是偶数的时候可以换回来。但$\mathrm{sgn}(\alpha) = (-1)^{16-5} = -1$是奇数次的置换，而奇数次的置换不能分解为偶次的对换，所以这个游戏如果从α开始则不可能赢。

2 习题

2.1 判断

1. n次对称群是由n个元素构成的集合(错)
   n次对称群的元素是表中的一个双射，考虑一个$S_3 = \{1, 2, 3\}$，他有$3! = 6$种方法，所以一个3次对称群含有6个元素，实际上n次对称群的元素一共有$n!$个。

2. 若$\alpha, \beta \in S_n$，则$\alpha\beta$是$\alpha \circ \beta$的一个缩写。（对）
   一个置换指的是一个双射，则$\alpha\beta$指的是两个置换的乘积，而$\alpha \circ \beta$是指两个置换的合成。一个置换都可以分解成不相交置换的乘积。所以我们对相交的置换化简再分解就可以得到一系列不相交置换的乘积。而对于合成，我们在不相交置换上有，一个置换移动i则另一个固定，为此这个合成最后得到的排列就等于置换的乘积。

3. 若α, β是S_n中的循环置换，则$\alpha\beta = \beta\alpha$ (对)
   首先，对命题1.9，我们设$\alpha\beta = \alpha_1 \cdots \alpha_n$和$\beta\alpha = \beta_1 \cdots \beta_m$是两个关于置换的完全分解，由于置换分解的唯一性（定理1.12）给出，重新排列就有每个$m = n$。而不相交置换满足交换律，所以$\alpha\beta = \beta\alpha$

4. 若$\alpha, \beta \in S_n$是$r-$循环置换，则$\alpha\beta$也是一个$r-$循环置换。（错）
   $(1\ 2)(1\ 3) = (1\ 3\ 2)$是一个反例。

2.2 计算题

1 求出$\mathrm{sgn}(\alpha)$和α^{-1}其中

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

我们先写出置换，一样的，从1开始有$1 \to 9 \to 1$第一个置换为$(1\ 9)$那么我们从2继续有$2 \to 8 \to 2$，那么第二个是$(2\ 8)$，第三个最小的是3，重复步骤就得到了置换

$$\alpha = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5) = (1\ 9)(2\ 8)(3\ 7)(4\ 6)$$

由于$(1\ 9)(2\ 8)(3\ 7)(4\ 6)$都是不相交的置换乘积，那么满足交换且数都是俩俩交换，则它的逆还是自身。所以

$$\alpha^{-1} = \alpha = (1\ 9)(2\ 8)(3\ 7)(4\ 6)$$

对于$\mathrm{sgn}(\alpha) = (-1)^{9-5} = 1$

2.3 证明题

一 设$\sigma \in S_n$固定某个j，其中$1 \le j \le n$(即$\sigma(j) = j$)，定义$\sigma' \in S_X$其中$X : \{1, 2, \cdots, \hat{j}, \cdots, n\}$并且$i \neq j$有$\sigma'(i) = \sigma(i)$，证明

$$\mathrm{sgn}(\sigma') = \mathrm{sgn}(\sigma)$$

证明： 对于每个$i \neq j$置换$\sigma'(i) = \sigma(i)$，并且$\sigma' : \{1, 2, \cdots, j, \cdots, n\} \to X$，则设它们的完全分解为$\sigma = \alpha_1 \cdots \alpha_n$和$\sigma' = \beta_1 \cdots \beta_m$由于$\sigma$除了$j$每个置换的值都相等，且每个置换都是一个双射，则对于σ, σ'的完全分解，对于每个$i \neq j$存在相同的循环结构。那么由归纳法可知循环中都是互异的数，为此σ'中不可能存在和σ不一样的置换分解。所以$\sigma'(j) = \hat{j}$。对于每个λ都有$\alpha_\lambda = \beta_\lambda$，则$\sigma = \sigma'$ 所以

$$\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma')$$

二

1. 若$1 < r \leq n$，证明S_n中存在

$$\frac{1}{r}[n(n-1)\cdots(n-r+1)]$$

个$r-$循环置换

2. 若$kr \leq n$，其中$1 < r \leq n$，证明置换$\alpha \in S_n$的个数是

$$\frac{1}{k!}\frac{1}{r^k}[n(n-1)\cdots(n-r+1)]$$

其中α是k个不相交$r-$循环置换的积。

证明： S_n中存在n个元素的各种排列，而且我们允许$(a\,b) = (b\,a)$是一个排列，但它们其实是一样的置换。为此对于一个长度为r置换首先有第一个元素有n种选择，第二个是$n-1$一直到$n-r+1$上，所以我们允许一个S_n出现$[n(n-1)\cdots(n-r+1)]$个置换。为了去除重复的置换，例如置换$(1\,2\,3\,4)$，我们只需要把每个数字往前推一位，有$(2\,3\,4\,1)$, $(3\,4\,1\,2)$, $(4\,1\,2\,3)$，所以当一个$4-$循环置换我们能通过这种方法改变顺序但不改变置换的映射，所以一个长度为r的置换存在r个这样子的置换，所以去除重复的置换得到的置换个数为

$$\frac{n(n-1)\cdots(n-r+1)}{r}$$

对于第二个命题只是第一个命题的拓展，那么对于每个分解的不相交$r-$置换，则利用命题1的结论可知这样子的置换个数一共有$\frac{1}{r^k}[n(n-1)\cdots(n-r+1)]$，因为一共有$n$个数，然后把$n$个数平分到每个$r-$循环置换上，能选择的个数依然是$n(n-1)\cdots(n-r+1)$个。所以这个置换形如$(1\,2\,\cdots\,r)(r+1\cdots\,r+k)\cdots(r+l\,\cdots\,n)$其中每个置换各有$1/r$个一样的排列，而且也是乘积，则这种可能是$1/r^k$，最后，对于整个置换的分解，我们把一个置换看成是排列中的一个元素，则一共有k个元素，k个元素有$k!$个排列，所以我们还需要除去$k!$最终的式子就是

$$\frac{1}{k!}\frac{1}{r^k}[n(n-1)\cdots(n-r+1)]$$

三

1. 证明，若α, β都是置换（不一定相交）且交换，则对所有$k \geq 1$有$(\alpha\beta)^k = \alpha^k\beta^k$

2. 给出满足$(\alpha\beta)^2 \neq \alpha^2\beta^2$的$\alpha, \beta$的例子

若α, β是不相交置换，设α移动i_0，则对于任意的k都有$\beta^k(i) = i$和$\alpha^k(i) = i_k$，则$(\alpha\beta)^k(i) = \alpha^k(i) = i_k = \alpha^k\beta^k(i)$。

若α, β有可能相交，且由题设对$k = 1$存在$\alpha\beta = \beta\alpha$成立，则$(\alpha\beta)^2 = (\alpha\beta)(\alpha\beta) = (\beta\alpha)(\beta\alpha) = (\beta\alpha)^2$成立，且$\alpha^2\beta^2 = \alpha\alpha\beta\beta = \alpha\beta\alpha\beta = (\alpha\beta)^2$则由归纳法得到对$k-1$成立有

$$(\alpha\beta)^k = (\alpha\beta)^{k-1}(\alpha\beta) = \alpha^{k-1}\beta^{k-1}(\alpha\beta) = \alpha^{k-1}\alpha\beta^{k-1}\beta = \alpha^k\beta^k$$

所以若α, β可交换，则$(\alpha\beta)^k = \alpha^k\beta^k$

对于第二个命题，则有$\alpha = (2\ 3\ 4\ 5)\beta = (1\ 3\ 4\ 5)$，则$(\alpha\beta)^2(3) = 1$但$\alpha^2\beta^2(3) = 3$。

四　若$n \geq 2$，证明S_n中的偶置换的个数是$\frac{1}{2}n!$

证明：设$\tau = (1\ 2)$且定义$f : A_n \to O_n$，其中A_n为所有偶置换构成的集合，O_n是奇置换构成的集合。且$f : \alpha \to \tau\alpha$，则任取一个$o \in O_n$有$\tau(\tau o) = o$，但是$\tau o$是一个$A$中的元素(因为$\tau o$是偶置换)，以此类推我们也可以证明$\tau a, a \in A_n$是一个奇置换，所以$A_n, O_n$是一个满射。并且每个$o \in O$至少对应着一个$A$，但$o_1 \neq o_2$，则有$\tau\tau o_1 = o_1 \neq o_2$，所以这是一个单射。为此$f : A_n \to O_n$是双射。所以$|A_n| = |O_n|$并且由于$S_n$的置换要么是奇置换要么是偶置换，则$|S_n| = n!$，所以奇置换的个数 = 偶置换的个数 $= \frac{1}{2}n!$

五　这个15−字谜游戏能赢吗？

4	10	9	1
8	2	15	6
12	5	11	3
7	14	13	#

我们先写出这个S_{16a}置换

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 4 & 10 & 9 & 1 & 8 & 2 & 15 & 6 & 12 & 5 & 11 & 3 & 7 & 14 & 13 & \# \end{pmatrix}$$

则一个分解为

$$\alpha = (1\ 4)(2\ 10\ 5\ 8\ 6)(3\ 9\ 12)(7\ 15\ 13)(11)(14)(\#)$$

且$\operatorname{sgn}(\alpha) = (-1)^{16-7} = -1$，所以这个游戏赢不了