Week 6 摘要

本周研究的主要内容是置换，包括两方面的内容：

(1) 置换的运算，包括置换间的乘法运算（即复合）与置换的求逆。随后我们较详细地研究了 S_3 的结构。

(2) 置换的分解。我们研究的分解方式有如下两种：

* 任意置换分解为不相交的轮换之积。这是一种在交换意义下唯一的分解。值得注意的是，这种将较复杂对象标准地分解为相同类型的处理在各个领域中广泛存在。例如素数的唯一分解定理、向量分解到标准正交基上。
  利用置换的不相交轮换分解，我们可以给出置换的阶的一个表达式。
* 任意置换分解为对换之积。在这种分解下，每一个"单元"都更加简单，但无法保证不相交性、可交换性，也没有唯一性。我们基于此引入了奇偶置换的概念（需要注意这个概念引入的合理性讨论），随后引入了 n 阶交代群的概念。

置换的复合、求逆运算（简单，略去）

三次对称群 S_3

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$

（最小的非交换群是 6 阶群，所有非交换的 6 阶群同构于 S_3）

回顾：轮换　轮换 $(a_1,a_2,\dots,a_m)$（$a_1,\dots,a_m$ 两两不同）定义为：

$$\sigma(a_1)=a_2,\ \sigma(a_2)=a_3,\ \dots,\ \sigma(a_m)=a_1.\ \forall a\notin\{a_1,\dots,a_m\},\ \sigma(a)=a.$$

那么元素 $\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 就是轮换 $(1,2,3)$

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

τ 生成的子群 $H:=\langle\tau\rangle=\{(1,2,3),(1,3,2),id\}$（我们将说明 $H\lhd S_3$）

我们可以看到，H 外的元素恰好是 3 个对换。记 $\eta=(1,2)$

$\eta^2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$o(\eta)=2$.　$\eta=\eta^{-1}$

$\eta\tau\eta^{-1}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\tau^2\in H.$　（体现了非交换性）

其余的共轭变换均可类似地论证。则有 $H\lhd S_3$.　（我们可以用这样的关系式简化很多运算）

$|H|=3$.　$|\eta H|=3$ 且 $\eta H\cap H=\phi$

$\Rightarrow S_3=\{\langle\tau,\eta\rangle\}$（即 S_3 可由一个三轮换和一个对换生成）

附：S_3 的所有子群。（由 Lagrange Thm.，S_3 仅可能有 1, 2, 3, 6 阶子群）

1 阶：$\{id\}$

2 阶：$\{(1,2),id\}$，$\{(2,3),id\}$，$\{(1,3),id\}$.

3 阶：$\{(1,2,3),(1,3,2),id\}$.

6 阶：S_3.

置换的轮换分解

轮换是置换的最简单形式。我们希望将一般的置换分解为这些更简单的形式

Def. 考虑 X 上的对称群 $Sym(X)$。$a_1,\dots,a_m$ 是 X 上两两不同的元素，$b_1,\dots,b_k$ 是 X 上两两不同的元素，不存在 i, j 使 $a_i=b_j$。则称轮换 $(a_1,\dots,a_m)$，$(b_1,\dots,b_k)$ 不相交

不相交轮换的乘法是可交换的，这是我们引入不相交性的重要原因。

例如，在 S_7 上：

$(1,2,3)\circ(4,5,6)=(4,5,6)\circ(1,2,3)$

直观来看，在一个置换中"变动"的元素，在不相交的另一个置换中不会"变动"。

$$(1,2,3)\circ(4,5,6)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&6&4&7\end{pmatrix}$$

也就是说，两层置换分别作用于不同的元素，它俩"各管各"，则顺序当然没有关系。

附：

$M(\sigma):=\{x\mid\sigma(x)\neq x\}$. 对 $\sigma_1,\sigma_2\in Sym(X)$，若 $M(\sigma_1)\cap M(\sigma_2)=\phi$，则 $\sigma_1\sigma_2=\sigma_2\sigma_1$.

Thm. S_n 中的任一置换都是两两不相交的若干轮换之积。且不考虑次序时，该分解是唯一的。

类似的考虑我们在很多分支中都见过——素数的唯一分解定理，向量分解为基的线性组合……

证明不做要求，我们通过几个例子展示这种分解的方法。

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

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

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&5&1&4&8&10&9&2&7&6\end{pmatrix}$$

$=(1,3)\circ(2,5,8)\circ(6,10)\circ(7,9)$

将上述的步骤稍作抽象。

对 $\sigma\in Sym(X)$，任取 $x\in X$，

$\exists k\in\mathbb{Z}^+$，$\sigma^{(k)}(x)=x$。取最小的 k，则 x 所在的轮换为

$(x,\sigma(x),\sigma^{(2)}(x),\dots,\sigma^{(k-1)}(x))$。再取在 $x,\sigma(x),\dots,\sigma^{(k-1)}(x)$ 中未出现的 x，

重复操作，直至没有未出现过的 x.

换句话说，如果我们定义等价关系 ~：$x\sim y\Leftrightarrow\exists k\in\mathbb{Z}^+$ s.t. $\sigma^{(k)}(x)=y$

则每一个轮换的所有元素无非是 ~ 诱导的一个等价类

置换的对换分解

对换的形式更为简单，但这里无法再确保不相交。

由于我们已经将置换写成轮换，接下来只要说明轮换可写成对换。

例子.

$(1,2,3)=(1,2)(2,3)$

$(1,2,3,4)=(1,2,3)(3,4)=(1,2)(2,3)(3,4)$

一般情形：$(a_1,a_2,\dots,a_m)=(a_1a_2)(a_2,a_3),\dots,(a_{m-1},a_m)$

该结论用归纳法是容易证明的。

命题.

任一置换都可写成若干对换的乘积.

S_n 可由以下 $(n-1)$ 个对换生成：

$(1,2),(2,3),\dots,(i,i+1),\dots,(n-1,n)$.

可由以下 2 个轮换生成：

$(1,2)(1,2,\dots,n)$

奇置换与偶置换

称可写成奇数个对换之积的置换为奇置换，

可写成偶数个对换之积的置换为偶置换。

刚引入这个定义时，似乎会引入疑虑：每个置换都能以多种方式写成对换之积，如何保证所有的分解的奇偶性相同？

我们有如下的定理解决上述的问题.

定义映射 $f:S_n\to M_{n\times n}$

$\forall\sigma\in S_n$，$f(\sigma)$ 定义为如下的 n 阶矩阵，其 (i, j) 元 $a_{ij}=\begin{cases}1 & i=\sigma(j)\\0 & i\neq\sigma(j)\end{cases}$

容易验证 f 为 S_n 到 $M_{n\times n}$ 的同态，即

$f(\sigma)f(\tau)=f(\sigma\tau)$

对 $\sigma=(a_1,b_1)(a_2,b_2)\cdots(a_n,b_n)$

$=(a_1',b_1')(a_2',b_2')\cdots(a_m',b_m')$

则有 $f(\sigma)=f(a_1,b_1)f(a_2,b_2)\cdots f(a_n,b_n)$

$=f(a_1',b_1')f(a_2',b_2')\cdots f(a_m',b_m')$

两边取行列式，有 $(-1)^m=(-1)^n$，故 m、n 奇偶性相同.

$A_n:=\{\sigma:\sigma\in S_n,\sigma\text{ 为偶置换}\}$

则 $A_n\leq S_n$，称为 n 次交代群.

Pf：设 $\sigma,\tau\in A_n$

则 $\sigma=(a_1,b_1)\cdots(a_m,b_m)$，m 偶

$\tau=(c_1,d_1)\cdots(c_k,d_k)$，k 偶

则 $\sigma\tau=(a_1,b_1)\cdots(a_m,b_m)(c_1,d_1)\cdots(c_k,d_k)$，$(m+k)$ 偶

$\Rightarrow\sigma\tau\in A_n$

$\sigma^{-1}=(a_m,b_m)\cdots(a_1,b_1)$　（因为群中 $(xy)^{-1}=y^{-1}x^{-1}$，而 $(a_i,b_i)(a_i,b_i)=id$，即 $(a_i,b_i)^{-1}=(a_i,b_i)$）

$S_n\ (n\geq2)$ 中奇、偶置换个数相同.

考虑对换 $(1,2)$。$\forall\sigma\in A_n$，$(1,2)\sigma$ 为奇置换.

$\forall\tau$ 为奇置换，$(1,2)\tau$ 为偶置换

$\Rightarrow S_n=A_n\cup(1,2)A_n\quad(n\geq2)$

（注意，$\sigma\to(1,2)\sigma$ 为双射，它的逆映射是 $\tau\to(1,2)\tau$）

当 $n\geq5$ 时，A_n 的正规子群仅有平凡子群（或 A_n 为有限单群）

（事实上，该结果导致了一元五次及以上的方程无根式解）

置换的阶

注：在有限阶群中，元素一定是有限阶的。

（因为无限阶蕴含不存在 $k,l\in\mathbb{Z}_+$，$k>l$，$a^k=a^l$。否则 $a^{k-l}=e$）

$(1,2)^2=id\Rightarrow o(1,2)=2$.

$$\left.\begin{aligned}&(1,2,3)^2=(1,3,2)\\&(1,2,3)^3=(1,3,2)(1,2,3)=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=id\end{aligned}\right\}\Rightarrow o(1,2,3)=3.$$

一般地，$o(a_1,a_2,\dots,a_m)=m$

证明思路：$(a_1,a_2,\dots,a_m)^k$ 将 a_i 置换到 a_{i+k}（$i=1,2,\dots,m$，下标模 m 考虑）

对于更一般的置换：

将置换作不相交轮换分解：$\sigma=\tau_1\tau_2\dots\tau_k$

设 $\tau_i=d_i$　$i=1,2,\dots,k$.　则 $o(\sigma)=lcm(d_1,d_2,\dots,d_k)$

（σ 在复合时，各个轮换也仍然是"各管各"，因此只需找最小的让各个轮换都回到 id 的复合次数即可，即最小公倍数）

要求"不相交"。

（或者如此证明：$\tau_1,\dots,\tau_k$ 两两不相交 ⇒ 乘法可交换。

$\Rightarrow\sigma^m=(\tau_1\cdots\tau_k)^m=\tau_1^m\tau_2^m\cdots\tau_k^m$

则 $\sigma^m=id\Leftrightarrow\tau_i^m=id$，$i=1,\dots,k$

（注意这里仍用到不相交性。由不相交，一个轮换中换住的元素不可能在另一个置换中换回来，故每一个都必须是 id）

则 $\sigma^m=id\Leftrightarrow d_i\mid m$，$i=1,\dots,k$. 又 m 最小，

则 $m=lcm(d_1,\dots,d_k)$）

至此我们需要掌握的计算：置换的乘积，不相交轮换分解，置换的阶.