第 14 次习题课 (对称群)

设 $A=\{a_1,\cdots,a_n\}$ 是一个 n 元集合, σ 是 A 上的一个置换。若 $\sigma(a_i)=b_i$, $i=1,\cdots,n$, 则可记

$$\sigma=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}.$$

若把 A 中的元素记为 $1,2,\cdots,n$, 则 σ 可表示为 $\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$, 其中 $k_1,\cdots,k_n$ 为 $1,\cdots,n$ 的一个排列。

定义 1 (轮换)**.** (1) 设 σ 是 $A=\{1,\cdots,n\}$ 上的一个置换，如果存在互不相同的整数 $i_1,\cdots,i_r$ 使得

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \to \cdots \to i_{r-1} \xrightarrow{\sigma} i_r \xrightarrow{\sigma} i_1$$

并且 $\sigma(k)=k$, $\forall k\in A\backslash\{i_1,\cdots,i_r\}$, 则称 σ 是 A 上的一个**轮换**, 记为 $\sigma=(i_1,i_2,\cdots,i_r)$, 称 r 为该轮换的长度。
(2) 设 $\sigma=(i_1,\cdots,i_r)$, $\tau=(j_1,\cdots,j_s)$ 是 $A=\{1,\cdots,n\}$ 上的两个轮换，称 σ 和 τ 是**不相交的**，如果 $\{i_1,\cdots,i_r\}\cap\{j_1,\cdots,j_s\}=\emptyset$。

$A=\{1,\cdots,n\}$ 上的恒等置换 id，可视为长度为 1 的轮换，记为

$$id=(1)=(2)=\cdots=(n).$$

题 1. 设 $\sigma=(i_1,\cdots,i_r)$, $\tau=(j_1,\cdots,j_s)$ 是 $A=\{1,\cdots,n\}$ 上的两个不相交的轮换，则在 A 的对称群 S_n 中，$\sigma\tau=\tau\sigma$。

证明. 由于 σ 和 τ 不相交，$\forall k\in\{i_1,\cdots,i_r\}$，有 $k,\sigma(k)\notin\{j_1,\cdots,j_s\}$。从而 $\sigma\tau(k)=\sigma(k)=\tau\sigma(k)$。同理，$\forall k\in\{j_1,\cdots,j_s\}$，可验证 $\sigma\tau(k)=\tau\sigma(k)$。
$\forall k\in A\setminus\{i_1,\cdots,i_r,j_1,\cdots,j_s\}$，有 $\sigma\tau(k)=k=\tau\sigma(k)$。
因此，$\forall k\in A=\{1,\cdots,n\}$，有 $\sigma\tau(k)=\tau\sigma(k)$。故 $\sigma\tau=\tau\sigma$。 □

定理 1 (置换的轮换分解)**.** 设 $A=\{1,\cdots,n\}$ 上的任意置换 σ 可写成一些互不相交的轮换的乘积。

证明. 任取 $i_1\in A$，令 $E_1=\{i_1,\sigma(i_1),\sigma^2(i_1),\cdots\}$，定义

$$\sigma_1(j):=\begin{cases}\sigma(j), & j\in E_1\\ j, & j\notin E_1\end{cases}$$

显然 σ_1 是一个轮换。若 $E_1=A$，则 $\sigma_1=\sigma$，结论成立。
不妨设 $E_1\subsetneq A$，则存在 $i_2\in A\setminus E_1$。令 $E_2=\{i_2,\sigma(i_2),\sigma^2(i_2),\cdots\}$，定义

$$\sigma_2(j):=\begin{cases}\sigma(j), & j\in E_2\\ j, & j\notin E_2\end{cases}$$

显然 σ_2 是一个轮换且 $\sigma=\sigma_1\sigma_2$ 在 $E_1\cup E_2$ 上成立。
若 $E_1\cup E_2=A$，则结论成立。故不妨设 $E_1\cup E_2\subsetneq A$，则存在 $i_3\in A\setminus(E_1\cup E_2)$。令 $E_3=\{i_3,\sigma(i_3),\sigma^2(i_3),\cdots\}$，定义

$$\sigma_3(j):=\begin{cases}\sigma(j), & j\in E_3\\ j, & j\notin E_3\end{cases}$$

显然 σ_3 是一个轮换且 $\sigma=\sigma_1\sigma_2\sigma_3$ 在 $E_1\cup E_2\cup E_3$ 上成立。如此继续下去，可将 σ 写成互不相交的轮换的乘积。 □

注. 本质想法是考虑循环群 $H=\langle\sigma\rangle\le S_n$ 在集合 $A=\{1,\ldots,n\}$ 上的作用，然后对集合 A 进行轨道分解 $A=E_1\sqcup E_2\sqcup\ldots$。

定义 2 (对换)**.** 长度为 2 的轮换称为**对换**，例如 $\sigma=(1,2)=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ 2 & 1 & 3 & \cdots & n\end{pmatrix}$。

题 2. 设 $A=\{1,\ldots,n\}$, S_n 为 A 上的对称群。则

(1) $(a_1,\cdots,a_r)=(a_1,a_2)(a_2,a_3)\cdots(a_{r-1},a_r)$。

(2) 任意置换 $\sigma\in S_n$ 可写为若干对换的乘积。

(3) 设 $\sigma=(a_1,\cdots,a_r)$ 是一个轮换，$\tau\in S_n$，则

$$\tau\sigma\tau^{-1}=(\tau(a_1),\tau(a_2),\cdots,\tau(a_r)).$$

(4) 令 $s_i=(i,i+1)$，则 $(i,i+2)=s_is_{i+1}s_i=s_{i+1}s_is_{i+1}$。

(5) 任意对换 (i,j) 可写成形如 $s_i=(i,i+1)$（其中 $1\le i\le n-1$）的对换的乘积。

提示： 设 $i<j$，可证明：$(i,j)=s_is_{i+1}\cdots s_{j-2}s_{j-1}s_{j-2}\cdots s_{i+1}s_i$。

(6) $s_1,\cdots,s_{n-1}$ 构成对称群 S_n 的一组生成元，并且它们满足:

$$s_i^2=id,\ s_is_{i+1}s_i=s_{i+1}s_is_{i+1},\ s_is_j=s_js_i,\quad \text{其中}|i-j|\ge 2.$$

证明. (1) 任取 $x\in A$, 只需证明置换 $f:=(a_1,a_2,\cdots,a_r)$ 和 $g:=(a_1,a_2)(a_2,a_3)\cdots(a_{r-1},a_r)$ 在 x 上的效果相同。若 $x\notin\{a_1,\ldots,a_r\}$，则 $f(x)=x=g(x)$。若 $x\in\{a_1,\ldots,a_r\}$, 可设 $x=a_i$。以下分三种情况。情况 (i): $x=a_1$。则 $g(x)=g(a_1)=(a_1,a_2)(a_1)=a_2=f(a_1)=f(x)$。情况 (ii): $x=a_i$ $(1<i<r)$。则 $g(x)=g(a_i)=(a_{i-1},a_i)(a_i,a_{i+1})(a_i)=a_{i+1}=f(a_i)=f(x)$。情况 (iii): $x=a_r$。此时可验证 $g(x)=a_1=f(x)$。因此，$f=g$。
(2) 任意置换 $\sigma\in S_n$ 可以写成不相交轮换的乘积:

$$\sigma=\gamma_1\gamma_2\cdots\gamma_k.$$

由 (1) 可知，每个轮换 γ_i 可以写成对换的乘积。因此 σ 可以写成对换的乘积。
(3) 任取 $x \in A$，只需验证置换 $f := \tau\sigma\tau^{-1}$ 与 $g := (\tau(a_1), \tau(a_2), \cdots, \tau(a_r))$ 在 x 上的效果相同。
如果 $x = \tau(a_k)$ $(1 \le k \le r-1)$，则:

$$f(x) = \tau\sigma\tau^{-1}(\tau(a_k)) = \tau\sigma(a_k) = \tau(a_{k+1}) = g(\tau(a_k)) = g(x).$$

如果 $x = \tau(a_r)$，则:

$$f(x) = \tau\sigma\tau^{-1}(\tau(a_r)) = \tau\sigma(a_r) = \tau(a_1) = g(\tau(a_r)) = g(x).$$

如果 $x \notin \{\tau(a_1), \ldots, \tau(a_r)\}$，则 $\tau^{-1}(x) \notin \{a_1, \ldots, a_r\}$，于是:

$$f(x) = \tau\sigma\tau^{-1}(x) = \tau(\tau^{-1}(x)) = x = g(x).$$

因此, 总有 $f = g$，即 $\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \cdots, \tau(a_r))$。
(4) 可直接进行验证。
(5) 设 $i < j$。记 $\tau = s_i s_{i+1} \cdots s_{j-2}$，易知 $\tau(j-1) = i$, $\tau(j) = j$。由 (3) 知,

$$s_i s_{i+1} \cdots s_{j-2} s_{j-1} s_{j-2} \cdots s_{i+1} s_i = \tau s_{j-1} \tau^{-1} = \tau(j-1, j)\tau^{-1} = (\tau(j-1), \tau(j)) = (i, j).$$

(6) 由 (2) 知任意置换可写为对换的乘积，由 (5) 知任意对换可写为 $s_i = (i, i+1)$ 的乘积，因此 $\{s_1, \ldots, s_{n-1}\}$ 生成整个对称群 S_n。 □

定义 3 (奇、偶置换)**.** 在对称群 S_n 中，如果一个置换可以写成偶数个对换的乘积，则称其为**偶置换**；如果可以写成奇数个对换的乘积，则称其为**奇置换**。

注. 由于一个置换可以有多种方式写成对换的乘积，因此需要证明奇偶性不依赖于分解方式的选择。

题 3 (置换的符号)**.** 设 $\sigma \in S_n$ 是一个置换，定义 $\mathrm{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j)-\sigma(i)}{j-i}$。证明:

(1) 若 σ 是一个对换，则 $\mathrm{sgn}(\sigma) = -1$。

(2) $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$。从而 $\mathrm{sgn} : S_n \to \{\pm 1\}$, $\sigma \mapsto \mathrm{sgn}(\sigma)$ 是一个群同态。

定理 2. 置换 $\sigma \in S_n$ 的奇偶性（偶置换或奇置换）是良好定义的。

证明. 假设 σ 有两种对换分解:

$$\sigma = \tau_1\tau_2 \ldots \tau_r = \gamma_1\gamma_2 \ldots \gamma_s,$$

其中每个 τ_i, γ_j 都是对换。从而

$$\mathrm{sgn}(\sigma) = (-1)^r = (-1)^s.$$

因此 r 与 s 的奇偶性相同。从而奇置换与偶置换的定义是良好的。 □