变换群与置换群

定义 1 (变换)**.** 设 A 是一个集合，映射 $f : A \to A$ 称为**变换**，即集合到自身的映射.

定义 2 (变换群)**.** 集合 A 上所有的可逆变换组成的集合，关于映射的复合构成群，称为集合 A 的**全变换群**，记作 S_A. 全变换群的一个子群称为 A 的一个**变换群**.

可以依定义验证 S_A 构成群. 可逆变换即双射，要求集合中的元素在变换前后是一一对应的.

定义 3 (对称群)**.** 若集合 A 是含 n 个元素的有限集，S_A 也称为 n 元**对称群**，也记作 S_n. S_n 中的变换称为**置换**.

定义 4 (置换群)**.** 对称群 S_n 中若干置换可以构成一个 S_n 的子群，称为**置换群**.

由定义，对称群是最大的置换群.

定理 1 (Cayley)**.** 任何群都与一个变换群同构.

证明. 设 G 是群，任意 $a \in G$，定义 $\varphi_a : G \to G,\ g \mapsto ag$. g 在 φ_a 下的像 ag 是唯一的，所以 φ 是映射.

由于 $a^{-1}g \in G$，而 $\varphi_a(a^{-1}g) = g$，也就是 G 中任何元素 g 都有原像 $a^{-1}g$，所以 φ_a 是满射.

对任意 $g_1, g_2 \in G$，若 $\varphi_a(g_1) = \varphi_a(g_2)$，则 $ag_1 = ag_2$. 由消去律有 $g_1 = g_2$，于是 φ_a 是单射. φ_a 又是满射，所以是双射，即可逆映射. 故 $\varphi_a \in S_G$.

设 $T = \{\varphi_a \mid a \in G\}$，则 $T \subset S_G$. 又因为 $(\varphi_b)^{-1} = \varphi_{b^{-1}}$，则 $\varphi_a(\varphi_b)^{-1} = \varphi_a\varphi_{b^{-1}} = \varphi_{ab^{-1}} \in T$，于是由子群的充要条件，有 $T < S_G$，则 T 是 G 的一个变换群，下面证明 $T \cong G$.

设 $f : G \to T,\ a \mapsto \varphi_a$，显然 f 是满映射. 对任意 $g_1, g_2 \in G$，若 $f(g_1) = f(g_2)$，则 $\varphi_{g_1} = \varphi_{g_2}$，$\varphi_{g_1}(e) = \varphi_{g_2}(e)$，即 $g_1 = g_2$，所以 f 是单射. 于是 f 是双射.

对任意 $a, b \in G$，$f(ab) = \varphi_{ab} = \varphi_a\varphi_b = f(a)(b)$，所以 f 是同构映射，$G \cong T$. □

推论 1. 任何有限群都与一个置换群同构.

下面介绍置换群相关内容. 设 $\sigma \in S_n$，设 $A = \{a_1, a_2, \cdots, a_n\}$，则置换 σ 可以表示为

$$\sigma(A) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}$$

其中，$\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_n)$ 是 $a_1, a_2, \cdots, a_n$ 的一个排列. 注意到一共有 $n!$ 种不同的排列方式，于是 $|S_n| = n!$. 特别地，若 $\mathrm{id}(a_i) = a_i, i = 1, 2, \cdots, n$，则称 id 为**恒等置换**.

定义 5 (轮换). 设 $I_r = \{i_1, i_2, \cdots, i_r\} \subset \{a_1, a_2, \cdots, a_n\} = A$，置换 σ 满足

$$\sigma(I_r) = \begin{pmatrix} i_1 & i_2 & \cdots & i_r \\ i_2 & i_3 & \cdots & i_1 \end{pmatrix}$$

$$\sigma(A \backslash I_r) = \mathrm{id}(A \backslash I_r),$$

则称 σ 为 ***r*-轮换**，记作 $\sigma = (i_1 i_2 \cdots i_r)$. $i_1, i_2, \cdots, i_r$ 称为轮换中的**文字**，r 称为轮换的**长**.

特别地，当 $r = 2$ 时称为**对换**，$r = 1$ 时为恒等置换.

命题 1. r-轮换的阶为 r.

命题 2. $(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_1) = \cdots (i_r i_1 \cdots i_{r-1})$.

上述两个命题都是显然的.

定义 6. 在 S_n 中，如果若干个轮换间无共同文字，则称它们是**不相交的轮换**.

命题 3. 在 S_n 中不相交轮换的乘积可换.

证明. 对于两个不相交的轮换 σ_1 和 σ_2，σ_1 作用在 σ_2 作用的文字上时是恒等置换，同理 σ_2 作用在 σ_1 作用的文字上时也是恒等置换，而恒等置换与置换的乘积是可换的，于是不相交轮换的乘积可换. 对于多个不相交的轮换，以此类推即可. □

定理 2. S_n 中任一置换都可表为若干不相交轮换的乘积.

证明. 设 $a \in \{1, 2, \cdots, n\}$，置换 σ 作用到 a 上得到一些不同的文字.

$$a = \sigma^0(a), \sigma(a), \sigma^2(a), \cdots,$$

假设 $\sigma^m(a)$ 与前面某一文字 $\sigma^k(a)$ 重复，那么 $k = 0$，否则 $\sigma^{k-1}(a) = \sigma^{m-1}(a)$ 从而矛盾. 于是置换 σ 在 a 上的作用等同于轮换

$$\sigma_1 = (a\sigma(a)\sigma^2(a) \cdots \sigma^m(a)),$$

下面考虑 $b \in \{1, 2, \cdots, n\} \setminus \{a, \sigma(a), \cdots \sigma^m(a)\}$，得到轮换

$$\sigma_2 = (b\sigma(b) \cdots \sigma^l(b)),$$

这里 σ_1 和 σ_2 是不相交的轮换. 以此类推，可以通过有限次操作取遍 $\{1, 2, \cdots, n\}$ 中的元素. 于是任一置换可以表为若干不相交轮换的乘积. □

命题 4. 任一个 r-轮换都可以写成 $r - 1$ 个对换的乘积.

证明. $(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2)$. □

命题 5. 任一置换都可以表为一些对换的乘积，这些对换的表示不一定唯一，但对换个数的奇偶性不变.

证明. 由定理2，任一置换可以表示为若干不相交轮换的乘积，而任一轮换可以写成对换的乘积，因此任一置换都可以表为一些对换的乘积. 对换的表示不唯一，因为对任一对换的乘积，乘以 $(i_ji_k)(i_ki_j)$ 之后仍然不变. 对换的表示改变了，但对换个数的奇偶性没有变. □

对换的表示并不是置换的本质，对换个数的奇偶性才是，于是有奇置换与偶置换的概念.

定义 7 (奇置换与偶置换)**.** 可以表为奇数个对换的乘积的置换称为**奇置换**，可以表为偶数个对换的乘积的置换称为**偶置换**.

下面是奇置换与偶置换的一些简单性质，这与整数的奇偶性可以类比.

性质 1. 两个奇置换之积是偶置换，两个偶置换之积是奇置换. 奇置换与偶置换之积是奇置换，偶置换与奇置换之积是奇置换. 置换的逆不改变置换的奇偶性.

定义 8 (交错群)**.** 按照群的定义可以验证，n 元偶置换全体对置换的乘法构成群，称为 n 元**交错群**，记作 A_n.

命题 6. $A_n \lhd S_n$，$|A_n| = n!/2$.

证明. 对任意 $\sigma \in A_n$，$\varphi \in S_n$，$\varphi\sigma\varphi^{-1} \in A_n$，因此 $A_n \lhd S_n$. 而 A_n 中不是奇置换就是偶置换. 对任意 $\sigma \in S_n$，映射 $\sigma \to (1,2)\sigma$ 建立了一个奇置换与偶置换之间的双射，于是 $|A_n| = n!/2$. □

命题 7. 设置换 $\sigma = \sigma_1\sigma_2\cdots\sigma_n$ 表示为 n 个不相交的轮换的乘积，其中 σ_i 是 r_i-轮换，则 σ 的阶为 $[r_1, r_2, \cdots, r_n]$.

证明. 设 $|\sigma| = d$，$m = [r_1, r_2, \cdots, r_n]$，则通过展开即可得 $\sigma^m = \mathrm{id}$，于是 $d \mid m$.

已知 $\sigma^d = \mathrm{id}$，所以对每个 i，有 $\sigma_i^d = \mathrm{id}$. 而 σ_i 是一个 r_i-轮换，其阶为 r_i，因此 $r_i \mid d$. 所以 d 是 r_i 的公倍数，所以 $m \mid d$. □

定义 9 (自同构群)**.** 群 G 到自身的同构映射称为它的一个**自同构**，全体自同构组成的集合对映射的复合作成群，称为 G 的**自同构群**，记作 $\mathrm{Aut}G$.

同构映射是双射，因此 $\mathrm{Aut}G < S_G$.

定义 10 (内自同构群)**.** 设 G 是群，给定 $a \in G$，定义映射 $\sigma_a : G \to G,\ g \mapsto aga^{-1}$，则映射 $\sigma_a \in \mathrm{Aut}G$，称为由 a 决定的**内自同构**. 记

$$\mathrm{Inn}G = \{\sigma_a \mid a \in G\},$$

则 $\mathrm{Inn}G \lhd \mathrm{Aut}G$，称为 G 的**内自同构群**.

证明. 对任意 $g \in G$，$(\sigma_{a^{-1}})\sigma_a(g) = a^{-1}aga^{-1}a = g$. 因此 $\sigma_{a^{-1}}$ 是 σ_a 的逆映射，σ_a 是双射. 又对任意 $g_1, g_2 \in G$，

$$\sigma_a(g_1g_2) = ag_1g_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = \sigma_a(g_1)\sigma_a(g_2),$$

于是 σ_a 是同构，$\sigma_a \in \mathrm{Aut}G$.

于是 $\mathrm{Inn}G \subset \mathrm{Aut}G$. 对任意 $a, b \in G$，任意 $g \in G$，有

$$\sigma_a\sigma_b(g) = \sigma_a(bgb^{-1}) = abgb^{-1}a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g) \in \mathrm{Inn}G,$$

于是 $\mathrm{Inn}G < \mathrm{Aut}G$. 对任意 $\sigma_a \in \mathrm{Inn}G$，$\varphi \in \mathrm{Aut}G$，有

$$\varphi\sigma_a\varphi^{-1}(g) = \varphi(a\varphi^{-1}(g)a^{-1}) = \varphi(a)\varphi\varphi^{-1}(g)\varphi(a^{-1}) = \sigma_{\varphi(a)}(g) \in \mathrm{Inn}G,$$

故 $\mathrm{Inn}G \lhd \mathrm{Aut}G$. □