10.3 循环群与置换群

① 循环群

定义 1： 设 G 是群。若$\exists a \in \mathrm{G}$，使得

$$\mathrm{G} = \langle a \rangle = \left\{a^k \middle| k \in \mathbb{Z}\right\},$$

则称 G 为循环群，称 a 为 G 的生成元。

注 1： 设$\mathrm{G} = \langle a \rangle$。若 a 是 n 阶有限元，则

$$\mathrm{G} = \langle a \rangle = \{\mathrm{e}, a, a^2, \cdots a^{n-1}\}$$

是 n 阶循环群。若 a 是无限阶元，则

$$\mathrm{G} = \langle a \rangle = \{\cdots a^{-n}, \cdots, a^{-2}, a^{-1}, \mathrm{e}, a, a^2, \cdots a^n, \cdots\}$$

是无限循环群。

- 例如， $<\mathbb{Z}, +>$是无限循环群，且

$$\langle \mathbb{Z}, + \rangle = \langle 1 \rangle = \langle -1 \rangle。$$

定理 1： 设$\mathrm{G} = \langle a \rangle$是循环群。

(1) 若 G 是无限循环群，则 G 只有两个生成元 a 和a^{-1}。

(2) 若 G 是 n 阶循环群，则 G 含有$\varphi(n)$个生成元，其中$\varphi(n)$表示 0，1，2，$\cdots, n-1$中与 n 互素的数的个数。对于任何小于 n 且与 n 互素的自然数 r，a^r是 G 的生成元。

例 1： (1) 设$\mathrm{G} = \langle a \rangle = \{\mathrm{e}, a, a^2, \cdots a^{11}\}$是 12 阶循环群。小于 12 且与

12 互素的数自然数是 1，5，7，11。故$\varphi(12)=4$。由定理 1，G 的生成元是a, a^5, a^7和a^{11}。

(2) 设$\mathrm{G}=\langle 3\mathbb{Z},+\rangle$，则 G 的生成元是 3 和$-3$。

例 2： 设 G 是一个有限群，且$|\mathrm{G}|=p$，其中 p 是一个素数。证明 G 是一个循环群。

例 3： 任何一个四阶群只可能是四阶循环群，或者是 Klein 四元群。

注 2：一般说来，求一个有限群的子群不是一件容易的事。但对于循环群来讲，可以直接求出它的所有的子群。请看下面的定理。

定理 2： (1) 设$\mathrm{G}=\langle a\rangle$是循环群，则它的子群仍是循环群。

(2) 设$\mathrm{G}=\langle a\rangle$是无限循环群，则它的子群除$\{\mathrm{e}\}$以外都是无限循环群。

(3) 设$\mathrm{G}=\langle a\rangle$是 n 阶循环群，则对 n 的每个正因子 d，G 恰好含有一个 d 阶子群。

注 3：定理 2 给出了求循环群子群的方法。

(1) 若$\mathrm{G}=\langle a\rangle$是无限循环群，那么对$\forall m\in\mathbb{N}$，$\langle a^m\rangle$是 G 的子群，且$m\neq n\in\mathbb{N}$时，$\langle a^m\rangle\neq\langle a^n\rangle$。

(2) 设$\mathrm{G}=\langle a\rangle$是 n 阶循环群，则对 n 的每个正因子 d，$\left\langle a^{\frac{n}{d}}\right\rangle$是 G 的唯一的 d 阶子群。

- 例如：对于群 $\langle\mathbb{Z},+\rangle=\langle 1\rangle=\langle -1\rangle$，它的所有子群是

$$m\mathbb{Z},\ m\in\mathbb{N}。$$

例 4： 设 $G=<\mathbb{Z}_{12},\oplus>$，其中 $\mathbb{Z}_{12}=\{0,1,2,\cdots,11\}$，$x\oplus y=(x+y)\bmod 12$。则 $G=\langle 1\rangle$是 12 阶循环群。求它的所有子群。

例 5： 证明偶数阶群必含二阶元。

例 6： 设 G 为非阿贝尔群。证明 G 中存在非单位元 a 和 b，a 不等于 b，且 $ab=ba$。

例 7： 设 $G=\langle a\rangle$是 15 阶循环群。

(1) 求出 G 的所有生成元。

(2) 求出 G 的所有子群。

② 置换群

定义 2: 有限集$S=\{1,2,\dots,n\}$到其自身的双射称为 S 上的一个 n 元置换。

例如：$S=\{1,2,3,4,5\}$，下面为 5 元置换。

$$\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix},\ \tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix}。$$

定义 3： 设σ，τ是 n 元置换，σ和τ的复合$\sigma\circ\tau$也是 n 元置换，称为σ与τ的乘积，记作$\sigma\tau$。

例如：对上述两个 5 元置换，有

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix},\ \sigma\tau=\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}。$$

定义 4： 设$S=\{1,2,\ldots,n\}$上有如下置换

$$f=\begin{pmatrix}a_1&a_2&\ldots&a_{i-1}&a_i&a_{i+1}&\ldots&a_n\\a_2&a_3&\ldots&a_i&a_1&a_{i+1}&\ldots&a_n\end{pmatrix}$$

称该置换为 i 价轮换，记为$(a_1, a_2, \ldots, a_i)$，i 为循环长度。当 i =2 时称为对换。恒等映射也视为轮换，记为（1）。

例 8： 设$S=\{1,2,\ldots,8\}$，

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

是 8 元置换。考虑σ的分解式。观察到

$\sigma(1)=5$，$\sigma(5)=2$，$\sigma(2)=3$，$\sigma(3)=6$，$\sigma(6)=1$；$\sigma(4)=4$；$\sigma(7)=8$，$\sigma(8)=7$。

于是，可以写出σ的轮换表示式

$$\sigma=(15236)(4)(78)。$$

为了使得轮换表示式更为简洁，通常省略其中的一阶轮换。于是，置换σ可以写作

$$\sigma=(15236)(78)。$$

定义 5： 有限集$S=\{1,2,\ldots,n\}$上所有的置换所组成的集合 S_n 及其复合运算∘构成群，称为 n 次对称群，而 $\langle S_n, \circ\rangle$ 的任意子群称为 n 次置换群。

例 9： 假设 $S=\{1,2,3\}$，写出 S 的 3 次对称群和所有的 3 次置换群。