

循环群与生成组

定义 1 (循环群). 由一个元素 a 反复运算得到的群称为**循环群**, 记作 $\langle a \rangle$. 这个元素称为群的**生成元**.

定理 1. 循环群都是交换群.

证明. 对任意 $a^m, a^n \in \langle a \rangle$, $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$. □

定理 2. 循环群的子群仍是循环群.

证明. 设 $G_1 < \langle a \rangle$, 设 $k = \min \{m \in \mathbb{N}^+ \mid a^m \in G_1\}$, 则 $\langle a^k \rangle \subset G_1$.

对任意 $a^n \in G_1$, 设 $n = qk + r$, 则 $a^n = a^{qk} a^r \in G_1$, 于是 $a^r \in G_1$, $0 \leq r < k$, 则 $r = 0$. 于是 $a_n \in \langle a^k \rangle$, 则 $G_1 \subset \langle a^k \rangle$. □

定理 3. 设循环群 $G = \langle a \rangle$. 若 $|G| = m$, 则 $G \cong (\mathbb{Z}_m, +)$; 若 $|G| = \infty$, 则 $G \cong (\mathbb{Z}, +)$.

证明. 设 $f: \mathbb{Z} \rightarrow G, n \rightarrow a^n$. 显然 f 是映射. 任意 a^n 都有 n 对应, 故 f 是满射. 对任意 $m, n \in \mathbb{Z}$,

$$f(m+n) = a^{m+n} = a^m a^n = f(m)f(n),$$

故 f 是满同态. 由群同态基本定理,

$$\mathbb{Z}/\ker f \cong G.$$

而 $\ker f \triangleleft \mathbb{Z} = m\mathbb{Z}$, 这里存在 $m \in \mathbb{N}$. 当 $m = 0$ 时, $\ker f = \{0\}$, 则 $\mathbb{Z} \cong G$. 当 $m > 0$ 时, $\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \cong G$. □

定理 4. 设 $|G| = m$, 则 G 是循环群的充要条件是对每一个正整数因子 $m_1|m$, 都存在唯一的 m_1 阶子群.

命题 1. 有限群 G 中元素的阶是 $|G|$ 的因子.

证明. 显然有限群中元素的阶有限, 设 $a \in G, |a| = d$, 则

$$\langle a \rangle = \{e, a, a^2, \dots, a^{d-1}\},$$

而 $\langle a \rangle < G, |\langle a \rangle| = d$, 由 Lagrange 定理得证. □

命题 2. 素数阶群必为循环群.

证明. 设有限群 $|G| = p$, p 是素数, 则由命题1, 对任意 $g \in G, |g| = 1$ 或 p . 当 $|g| = 1$ 时, $g = e$. 当 $|g| = p$ 时, $|\langle g \rangle| = p = |G|$, 而 $\langle g \rangle < G$, 于是 $\langle g \rangle = G$, 即 G 是由 g 生成的循环群. □

定义 2 (生成的子群). 设 S 是群 G 的非空子集, 包含 S 的最小子群称为 S 生成的子群, 记作 $\langle S \rangle$. 等价定义为包含 S 的所有子群的交.

定理 5. 设 S 是群 G 的非空子集, $S^{-1} = \{a^{-1} \mid a \in S\}$, 则

$$\langle S \rangle = \{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}\}$$

证明. 设 $T = \{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}\}$. 由于 $S \subset \langle S \rangle$, $S^{-1} \subset \langle S \rangle$, 于是 $S \cup S^{-1} \subset \langle S \rangle$, 则 $T \subset \langle S \rangle$. 下面证明 T 是子群.

设 $x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m \in T$, 则 $y_i^{-1} \in S \cup S^{-1}$, 于是

$$x_1 x_2 \cdots x_n (y_1 y_2 \cdots y_m)^{-1} = x_1 x_2 \cdots x_n y_m^{-1} y_{m-1}^{-1} \cdots y_1^{-1} \in T.$$

故 $T < \langle S \rangle$, 而 $\langle S \rangle$ 是包含 S 的最小子群, 故 $T = \langle S \rangle$. □

定义 3 (生成组). 若 $G = \langle S \rangle$, 则称 S 为 G 的生成组.

定义 4 (有限生成群). 若存在群 G 的有限个元素的生成组, 则称 G 是有限生成群. 若 G 还是交换群, 则称为有限生成 Abel 群.

注意到有限群是有限生成群, 但有限生成群不一定是有限群, 例如 $(\mathbb{Z}, +) = \langle 1 \rangle$.