

§ 1.5 循环群

定义 1.5.1 设 G 为群，若存在 $a \in G$ ，使 $G = \{a^n \mid n \in \mathbb{Z}\}$ ，则 G 为循环群。
记为 $G = \langle a \rangle$ ，称 a 为生成元。

例 1. ① $\{\mathbb{Z}; +\}$ 为循环群， 1 为生成元。

② $U_m = \{c \in \mathbb{C}^* \mid c^m = 1\}$ 对乘法成群，为循环群。本原根为生成元。

命题 1.5.1：循环群为 Abel 群

命题 1.5.2：循环群的子群为循环群。

推论 1.5.3： $\{\mathbb{Z}; +\}$ 的任何子群，形如 $m\mathbb{Z}$ ， $m \geq 0$ 。

定理 1.5.4 设 G 为循环群，若 $|G| = \infty$ ，则 $G \cong \{\mathbb{Z}; +\}$ 。



若 $|G| = m > 0$ ，则 $G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m (\cong U_m)$

两个循环群同构 \Leftrightarrow 它们的阶相同。

命题 1.5.5 设 $G = \langle a \rangle$ ， $|G| = m$ ， $n \in \mathbb{N}$ ， $n \mid m$ ，则 G 中有唯一的一个子群。

定理 1.5.6. 设 G 为有限群， $|G| = M$ ，则 G 为循环群 \Leftrightarrow 对 M 的任何正整数因子 n ，有惟一的一个 n 阶子群。

命题1.5.7. 设 $|G|=m$, $a \in G$, 则 a 的阶 $d|m$.

循环群与生成元: $\langle a \rangle = \{ma \mid m \in \mathbb{Z}\}$

$$G_1 = \langle a \rangle$$

G 任一子群, $S \subseteq G$ 非空子集

生成子群如何定义:

$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, 令 $S_1 = \{a, a^{-1}\}$, $\langle a \rangle$ 可看成为 S_1 中有限个元素之积
组成的集合. 令 $S^{-1} = \{a^{-1} \mid a \in S\}$.

令 $\langle S \rangle = \{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}, m \in \mathbb{N}\}$ 为 G 的子群

称为由 S 生成的子群. 若 $G = \langle S \rangle$, 称 S 为一组生成元.

$\langle S \rangle = G$ 中包含 S 的最小子群 = G 中包含 S 的子群的交.

若 G 中存在有限集合 S , 使 $G = \langle S \rangle$, 称 G 为有限生成群.

有限群为有限生成群, 反之不对. (eg. $\{\mathbb{Z}, +\}$)