



§ 2.5 循环群

补充参考书：初等数论

[本节主要内容]

- 1) 循环群的定义;
- 2) 循环群的同构;
- 3) 循环群的子群;

一、循环群的定义及生成

定义1 循环群：若群 G 由其中的某个元素 a 生成的，记为 $G = \langle a \rangle$

a 称为 G 的生成元。

例1 1. 整数的加法群 $(\mathbb{Z}, +) = \langle 1 \rangle$

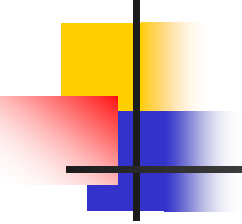
2. 模 n 的同余等价类之集所构成的群

$$(\mathbb{Z}_n, \oplus) = \langle [1] \rangle$$



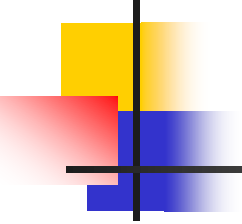
注:

- 1) 循环群必为交换群（类似循环半群必为交换半群）；
- 2) 设 $G = \langle a \rangle$ ，且 a 的阶为无穷，则
$$G = \left\{ \cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, a^1, a^2, \cdots, a^n, \cdots \right\}$$



3) 设 $G = \langle a \rangle$ ，且 a 的阶为 n ，即有
 $a^n = e$ 则

$$G = \{ e, a, a^2, \dots, a^{n-1} \}$$



定理1 循环群 $G = \langle a \rangle$ 为无穷循环群的充要条件是 a 的阶为无穷大；

循环群 $G = \langle a \rangle$ 为 n 阶循环群的充要条件是 a 的阶为 n 。



4) 生成元的唯一性问题

A. 设 $G = \langle a \rangle$, 且 a 的阶为无穷,
则 a 与 a^{-1} 均为 G 的生成元;

B. 设 $G = \langle a \rangle$, 且 a 的阶为 n ,
则其生成元为 a^k ,
且 $(k, n) = 1, k > 1$

例2 若 $n=6$, 则

$$(Z_6, \oplus) = \{ [0], [1], [2], [3], [4], [5], \oplus \} = ([1])$$

此时 $([5]) = ([1])$;

而 $([2]) = \{ [0], [2], [4] \}$; $([3]) = \{ [0], [3] \}$

$$([4]) = \{ [0], [4], [2] \}$$

若 $n=5$ 呢?

$$\text{此时 } ([1]) = ([2]) = ([3]) = ([4])$$

$$= (Z_5, \oplus)$$

二、循环群的同构

1. 无穷循环群

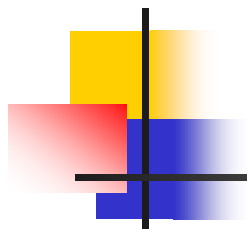
设 $G = \left\{ \cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, \right.$
 $\left. a^1, a^2, \cdots, a^n, \cdots \right\}$
= (a) 为无穷循环群,
($\mathbb{Z}, +$) 为整数加法群, 令 $\varphi: \mathbb{Z} \rightarrow G$
映射, 且对 $\forall m \in \mathbb{Z}, \varphi(m) = a^m$
则 $\varphi: \mathbb{Z} \rightarrow G$ 上的同构

2. 有限循环群

设 $G = \{e, a, a^2, \dots, a^{n-1}\} = \langle a \rangle$
为 n 阶循环群, $a^n = e$, (\mathbb{Z}_n, \oplus) 为

模 n 同余类加法群, 令 $\varphi: G \rightarrow \mathbb{Z}_n$ 映射,
且对 $\forall a^i \in G, \varphi(a^i) = [i]$

则 $\varphi: G \rightarrow \mathbb{Z}_n$ 上的同构

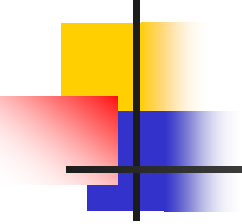


定理2 无穷循环群同构于整数加法群 $(\mathbb{Z}, +)$;
阶为 n 的有限循环群同构于 (\mathbb{Z}_n, \oplus)

三、循环群的子群

1. 设 $G = \langle a \rangle$ 为无穷循环群, H 为 G 的子群, 且 $H \neq \{e\}$, 则

$$H = \langle a^m \rangle = \left\{ \dots, a^{-2m}, a^{-m}, e, a^m, a^{2m}, \dots \right\}$$



2. 设 $G = \langle a \rangle$ 为 n 阶循环群, 且 a 的阶为 n , H 为 G 的子群, 且 $H \neq \{e\}$: 则

$$H = \langle a^m \rangle = \left\{ e, a^m, a^{2m}, \dots, a^{(q-1)m} \right\}$$

$$n = mq, \text{ 即 } m \mid n$$

定理3 设 $G = \langle a \rangle$ 是由 a 生成的循环群，则：

- 1) 循环群的子群仍为循环群；
- 2) 若 G 为无穷循环群，则 G 的子群为 $\{ e \}$ 或为

$$H_m = \langle a^m \rangle = \{ \cdots, a^{-2m}, a^{-m}, e, a^m, a^{2m}, \cdots \}$$

且为无穷循环子群，从而同构于 G 。

3) 若G为n阶循环群, 则其子群的阶必整除n. 对n的任一因子m, 必有一个阶为 $q=n/m$ 的子群。

$$H_m = \langle a^m \rangle = \left\{ e, a^m, a^{2m}, \dots, a^{(q-1)m} \right\}$$

$$m \mid n, \quad n=mq$$