§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＝（a）

a称为G的生成元。

例1 1. 整数的加法群（Z, +）=（1）

2. 模n的同余等价类之集所构成的群

$$(Z_n, \oplus) = ([1])$$

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＝（a），且a的阶为无穷，则

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

3）设G＝（a），且a的阶为n，即有 $a^n = e$ 则

$$G = \left\{ e, a, a^2, \cdots, a^{n-1} \right\}$$

定理1 循环群G＝（a）为无穷循环群的充要条件是a的阶为无穷大；

循环群G＝（a）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＝（a），且a的阶为无穷，则 a 与 a^{-1} 均为G的生成元；

B. 设G＝（a），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？

此时 $([1])=([2])=([3])=([4]))$

$$=(Z_5,\oplus)$$

二、循环群的同构

1. 无穷循环群

设 $G=\{\cdots,a^{-n},\cdots,a^{-2},a^{-1},e,a^{1},a^{2},\cdots,a^{n},\cdots\}$ ＝（a）为无穷循环群，

（Z，＋）为整数加法群，令φ：$Z\to G$ 映射，且对$\forall\, m\in Z$，$\varphi(m)=a^{m}$

则 φ：$Z\to G$ 上的同构

2．有限循环群

设 $G=\left\{e,a,a^2,\cdots,a^{n-1}\right\}=$（a）为n阶循环群，$a^n=e$，（Zn，$\oplus$）为模n同余类加法群，令$\varphi$：$G\rightarrow \mathrm{Zn}$ 映射，且对

$$\forall a^i\in G,\varphi(a^i)=[i]$$

则φ：$G\rightarrow \mathrm{Zn}$ 上的同构

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

三、循环群的子群

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

$$H = \left(a^{m}\right) = \left\{ \begin{array}{c} \cdots, a^{-2m}, a^{-m}, e, \\ a^{m}, a^{2m}, \cdots \end{array} \right\}$$

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

$$H = (a^m) = \{e, a^m, a^{2m}, \cdots a^{(q-1)m}\}$$

$n = mq$, 即 $m \mid n$

定理3 设G＝（a）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

$$H_m=\left(a^m\right)=\left\{\cdots,a^{-2m},a^{-m},e,a^m,a^{2m},\cdots\right\}$$

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。

$$H_m = (a^m) = \{e, a^m, a^{2m}, \cdots a^{(q-1)m}\}$$

$m \mid n$ ， n=mq