第八章　群和环

第十四节 循环群(1)

1. 定义：设<G,★>是群，如果存在一个元素 $g \in G$，对任意 $x \in G$，都存在整数 i，使得 $x=g^i$，则称 <G,★>是循环群。并称 g 是 G 的生成元。

例1：$N_4=\{0,1,2,3\}$，$<N_4,+_4>$是群，$<N_4,+_4>$是否是循环群？

解：$<N_4,+_4>$是以 1 为生成元的循环群，

因为显然 $2=1+_4 1=1^2$，$3=1+_4 1+_4 1=1^3$，

$0=2+_4 2=1^4$

所以 N_4 可表示成 $N_4=\{1^4,1,1^2,1^3\}$。

例2： I={…-3, -2, -1, 0, 1, 2, 3, ...}， <I,+>是群，

因为 $-1=1^{-1}$， $-2=(-1)+(-1)=1^{-1}+1^{-1}=(1^{-1})^2=1^{-2}$ ， ……

$0=1^0$ ， $1=1^1$ ， $2=1^2$ ， ……

所以 I 可以写成：$I=\{\ldots 1^{-3},1^{-2},1^{-1},1^0,1^1,1^2,1^3 \ldots\}$，

即 <I,+> 是以 1 为生成元的循环群。

思考

-1 是否是生成元？

答：-1 是生成元，

$0=(-1)^0$ ， $1=(-1)^{-1}$ ， $1=(-1)^{-2}$ ……

$-1=(-1)^1$ ， $-2=(-1)^2$ ……

2. 循环群的类别：

根据生成元 g 的阶，循环群<G,★>可以分成两类：

(1) 若g的阶是 n，则<G,★>为 n 阶循环群，

$G=\{g^1,g^2,..., g^n=e\}$，并且称<G,★>的循环周期为 n。

(2) 若g是无限阶元，则<G,★>是无限循环群，

$G=\{\dots, g^{-3},g^{-2}, g^{-1},g^0=e, g^1, g^2, g^3\dots\}$

并且称<G,★>的循环周期是无限的。

例：$<N_4,+_4>$，$N_4=\{0,1,2,3\}=\{1^4,1,1^2,1^3\},1^4=0$，循环周期为4。

$<I,+>$，$I=\{\dots -3, -2, -1, 0, 1, 2, 3, \dots\}$

$=\{\dots 1^{-3},1^{-2},1^{-1},1^0,1^1,1^2,1^3 \dots\}$，循环周期是无限的。

3. 循环群的生成元

定理1 设<G,★>是以 g 为生成元的有限循环群。则 $|G|=n$ 当且仅当 $|g|=n$ 。

证明：必要性 若 $|G|=n$，(往证$|g|=n$) 设 $|g|=m$，根据拉格朗日定理的推论，群中元素的阶一定是群阶的因子，所以有 $m \le n$。

设 $|g|=m<n$，因为<G,★>是以 g 为生成元的有限循环群，所以对任意 $a\in G$，均存在 $s\in I$ 使得 $a=g^s$。

令 $s=mq+r$ $(q,r\in I,\ 0\le r<m)$，则有

$$a = g^s = g^{mq+r} = g^{mq}\star g^r = (g^m)^q \star g^r = e^q \star g^r = g^r$$

即 G 中任意元素均具有 g^r 的形式且 $0\le r<m$。因而 G 中至多有 m 个元素 $g^1,g^2,\ldots, g^m$，于是 $|G| \le m< n$，与 $|G|=n$ 矛盾。因此 $m \ge n$ 。

于是有 $m=n$，即 $|g|=n$。

定理1 设$<G,\star>$是以 g 为生成元的有限循环群。则 $|G|=n$ 当且仅当 $|g|=n$ 。

证明：充分性 若 $|g|=n$，（往证$|G|=n$ ）

因 $|g|=n$， 则 $g^n=e$。因 g 是$<G,\star>$的生成元，所以对任意 $a\in G$，均存在 $k\in I$ 使得 $a=g^k$。令 $k=nq+r$ $(q,r\in I, 0\leq r<n)$，则有 $a=g^k = g^{nq+r} = g^{nq}\star g^r = (g^n)^q \star g^r = e^q \star g^r = g^r$

即 G 中任意元素均具有 g^r 的形式且 $0\leq r<n$。因而 G 中至多有 n 个元素 $g^1,g^2,\ldots, g^n$，于是 $|G|\leq n$。

再证明 $g^1,g^2,\ldots, g^n$ 互不相同。

若不然， 则有 $1\leq i<j\leq n$ 使得 $g^i = g^j$，于是

$g^{j-i} = g^j\star(g^{-1})^i = g^i\star(g^i)^{-1}=e$ 且 $j-i<n$，与 $|g|=n$ 矛盾。

所以 $g^1,g^2,\ldots, g^n$ 互不相同。 综上 $|G|=n$ 。

第十四节 结束