第八章　群和环

第十五节 循环群(2)

4. 循环群生成元的个数

定理2

设<G,★>是由 g 生成的循环群。

(1) 若 G 为无限循环群，则 G 只有两个生成元 g 和 g^{-1}。

(2) 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$ 个生成元。

对于任何正整数 r，若 $r \leq n$ 且与 n 互素，

则 g^r 是 G 的生成元。

$\phi(n)$ 为欧拉函数，即小于或等于 n 且与 n 互素的正整数的个数。

定理2

设<G,★>是由 g 生成的循环群。

(1) 若 G 为无限循环群，则 G 只有两个生成元 g 和 g^{-1}。

证明(1) 因为 g 是<G,★>的生成元，所以对任意 $a\in G$，均存在 $k\in I$ 使得 $a=g^k$。又 $a=((g^{-1})^{-1})^k=((g^{-1})^k)^{-1}=(g^{-1})^{-k}$，所以 g^{-1} 也是生成元。

再证 G 中只有 g 和 g^{-1} 这两个生成元。

假设 h 也是生成元，对于 $g\in G$，存在整数 s 使得 $g=h^s$。

对于 $h\in G$，由于 g 是<G,★>的生成元，所以存在整数 t 使得 $h=g^t$。于是 $g=h^s=(g^t)^s=g^{ts}$。于是 $e=g\star g^{-1}=g^{ts-1}$。因为<G,★>是无限群，$e=g^0$，所以 $ts-1=0$，即 $ts=1$。于是有 $t=s=1$ 或 $t=s=-1$，因此 $h=g$ 或 $h=g^{-1}$。

定理2

设<G,★>是由 g 生成的循环群。

(2) 若 G 是 n 阶循环群，则 G中 含有 $\phi(n)$ 个生成元。

对于任何小于等于 n 且与 n 互素的正整数 r，g^r 是 G 的生成元。

$\phi(n)$ 为小于或等于 n 且与n 互素的正整数的个数。

证明(2)　只需证明对于任意正整数 r ($r \leq n$),

g^r 是<G,★>的生成元⇔ r 与n 互素。

充分性　设 r 与 n 互素且 $r \leq n$，(往证 g^r 是<G,★>的生成元)

因 r 与 n 互素且 $r \leq n$，　则存在整数 u 和 v 使得　$ur + vn = 1$

因$|G|=n$，　$g^n = e$。　于是　$g = g^{ur+vn} = (g^r)^u(g^n)^v = (g^r)^u$

这就推出　对任意 $g^k \in G$，$g^k = (g^r)^{uk}$，

于是 g^r 是<G,★>的生成元。

设<G,★>是由 g 生成的循环群。

定理2

(2) 若 G 是 n 阶循环群，则 G中 含有 $\phi(n)$ 个生成元。

对于任何小于等于 n 且与 n 互素的正整数 r，g^r 是 G 的生成元。

$\phi(n)$ 为小于或等于 n 且与n 互素的正整数的个数。

证明(2)　只需证明对于任意正整数 r (r ≤n)，

设<G,★>是群，a∈G 且 |a| = k。

设 n 是整数，则 $a^n = e$ 当且仅当 k/n。

必要性　设 g

因 g^r 是 数为 d，则存在正整数 t 使得 r = dt，并且 n/d 为整数。于是

$(g^r)^{n/d} = (g^{dt})^{n/d} = (g^t)^n = (g^n)^t = e$　于是　n/d 是 $|g^r|$ 的整数倍，而 $|g^r| = n$，于是 n 整除 n/d，从而有 d = 1。

因此 r 与n 互素。

一般来说，求一个群的子群并不容易，但对于循环群，
可以直接求出他的所有子群

例1： <G,★>是由 g 生成的循环群， |G|=12,

小于或等于 12 且与 12 互素的正整数有 4 个：

1, 5, 7, 11，即 $\phi(12)=4$。

于是<G,★>有 4 个生成元，分别是 ：g，g^5，g^7，g^{11} 。

例2：设 <G,+>， G={ 3a | a∈I }， “+” 是普通加法运算，

则 <G,+> 为无限循环群，只有 两个生成元：3 和 –3。

第十五节 结束