循环群的生成元

2008-2010 by Li Weigang. All RightS ReSeRved.

循环群的生成元

*定理6.18 设$G=\langle a\rangle$是循环群.

(1) 若G是无限循环群，则G只有两个生成元，即a和a^{-1}.

(2) 若G是 n 阶循环群，则G含有$\phi(n)$个生成元. 对于任何小于n且与 n 互质的数$r\in\{0,1,\ldots,n-1\}$, a^r是G的生成元.

$\phi(n)$称为欧拉函数，例如 $n=12$，小于12且与12互质的正整数有4个:

1, 5, 7, 11，

所以$\phi(12)=4$.

证明

证 (1) 先证a^{-1}是G的生成元, 再证G只有a和a^{-1}这两个生成元.

先证: 显然$\langle a^{-1}\rangle \subseteq G$. $\forall a^k \in G$，$a^k=(a^{-1})^{-k} \in \langle a^{-1}\rangle$，因此$G\subseteq \langle a^{-1}\rangle$，$a^{-1}$是$G$的生成元.

再证:

假设 b 也是G 的生成元，则 $G=\langle b\rangle$. 由$a\in G$ 可知存在整数 t 使得$a = b^t$. 由$b\in G = \langle a\rangle$ 知存在整数 m 使得 $b = a^m$. 从而得到

$$a = b^t = (a^m)^t = a^{mt}$$

由G中的消去律得

$$a^{mt-1} = e$$

因为G是无限群，必有$mt-1 = 0$. 从而证明了$m = t = 1$或 $m = t = -1$，即 $b = a$ 或 $b = a^{-1}$

证明

(2) 只须证明：对任何正整数 r ($r \le n$)，

a^r是G的生成元 $\Leftrightarrow$ n与r互质.

充分性(证$\langle a^r\rangle = G$). 设r与n互质，且$r \le n$，那么存在整数 u 和 v 使得

$$ur + vn = 1$$（数论中的重要定理）

从而 $a = a^{ur+vn} = (a^r)^u(a^n)^v = (a^r)^u$

这就推出$\forall a^k \in G$，$a^k = (a^r)^{uk} \in \langle a^r\rangle$，即$G \subseteq \langle a^r\rangle$.

另一方面，显然有$\langle a^r\rangle \subseteq G$. 从而$G = \langle a^r\rangle$.

必要性. 设a^r是G的生成元，则 $|a^r| = n$. 令r与n的最大公约数为d，则存在正整数 t 使得 $r = dt$. 因此 $(a^r)^{n/d} = (a^{dt})^{n/d} = (a^n)^t = e$

所以$|a^r|$ 是n/d的因子，即n整除n/d. 从而证明了$d = 1$，所以n与r互质.

实例

***例6**

(1) 设$G=\{e, a, \ldots, a^{11}\}$是12阶循环群，则$\phi(12)=4$. 小于12且与12互素的数是1, 5, 7, 11, 由定理6.18可知 a, a^5, a^7 和 a^{11}是G的生成元.

(2) 设$G=\langle Z_9, \oplus \rangle$是模9的整数加群，则$\phi(9)=6$. 小于9且与9互素的数是 1, 2, 4, 5, 7, 8. 根据定理6.18，G的生成元是1, 2, 4, 5, 7和8.

(3) 设$G=3Z=\{3z \mid z \in Z\}$, G上的运算是普通加法. 那么G只有两个生成元：3和-3.

THE END