信息安全数学基础

第三章 群

陈大江

信息与软件工程学院

3.5 循环群

定义3.5.1 设G是一个群，若存在一个元素a，使得$G=\langle a\rangle$，则称G为**循环群**。元素a称为G的生成元。若$o(a)=\infty$，G称为**无限循环群**；若$o(a)=n$, n 是某个正整数，则G称为**有限循环群**。

例3.5.1

（1）整数加法群Z是循环群，其生成元为1或-1。

（2）模整数m剩余类加群Z_m是循环群，其生成元为[1]。

3.5 循环群

循环群的生成元

定理3.5.1 设$G=\langle a\rangle$是无限循环群，则G只有两个生成元为a和a^{-1}。

证明 因为$a=(a^{-1})^{-1}\in\langle a^{-1}\rangle$，故$a$和 a^{-1}都是G的生成元。假设$k\in Z$, a^k是G的生成元，即$G=\langle a^k\rangle$，则$a\in G=\langle a^k\rangle$，这样存在整数$m$，使得$a=(a^k)^m=a^{mk}$，而$o(a)=\infty$，所以$mk=1, k=\pm 1$。因此, G只有两个生成元为a和a^{-1}。

3.5 循环群

设$G=\langle a\rangle$是n阶循环群，则群G中的元素都是a^k 的形式，其中$\gcd(k,n)=1$。

定理3.5.2 设$G=\langle a\rangle$是n阶循环群，a^k是G的生成元的充要条件是$\gcd(k,n)=1$。

证明思路 证明满足是$\gcd(k,n)=1$的 a^k的阶为n，注意要抓住阶的定义中的“最小正整数”。

定理3.5.2的证明

引理3.5.1 设a是群G中的一个有限阶元素，$o(a)=n$，则对于任意正整数m，$a^m=e$当且仅当$n\mid m$。

引理3.5.2 设a是群G中的一个有限阶元素，$o(a)=n$，则对于任意正整数k，a^k的阶为$\frac{n}{\gcd(k,n)}$。

3.5 循环群

引理3.5.1的证明

充分性：假设$n \mid m$，则存在整数t，使得$m = nt$，所以

$$a^m = a^{nt} = (a^n)^t = e^t = e$$

必要性:$a^m = e$。不妨设$m = nq + r$，其中q, r为非负整数，$0 \le r < n$，那么有

$$e = a^m = a^{nq+r} = (a^n)^q a^r = a^r$$

但是由于$0 \le r < n$，根据定义3.3.5有$r = 0$。因此有$n \mid m$。

引理3.5.2的证明

令$d=\gcd(k,n)$。显然有

$$(a^k)^{\frac{n}{d}}=a^{\frac{nk}{d}}=(a^n)^{\frac{k}{d}}=e$$

设l是a^k的阶，那么由引理3.5.1可知

$$l \mid \frac{n}{d} \qquad (1)$$

另一方面，又有

$$a^{kl}=(a^k)^l=e$$

由引理3.5.1可知$n\mid kl$，且$d\mid n, d\mid k$，

故

$$\frac{n}{d} \mid \frac{k}{d}l$$

又

$$\gcd(\tfrac{n}{d},\tfrac{k}{d})=1$$

所以有

$$\tfrac{n}{d}\mid l \qquad (2)$$

由（1）（2）可得$l=\frac{n}{d}$，即$l=\frac{n}{\gcd(k,n)}$。

根据引理3.5.2的结论，很容易得出定理3.5.1的结论。

根据定理3.5.1, n 阶循环群$G=\langle a\rangle$的生成元的个数为$\psi(n)$。

根据定理3.5.1可知，模整数m的剩余类加群Z_m中的生成元有$\psi(m)$，其生成元a满足$\gcd(a,m)=1$。

3.5 循环群

定义3.5.2 设$\alpha \in Z_m^*$，若 α 的阶为 $\varphi(m)$ ，则 α 称为Z_m^* 的生成元或原根。

如果Z_m^* 有一个生成元 α ，则 Z_m^* 是循环群，且

$$Z_m^* = \{\alpha^i \pmod{m} | 0 \le i \le \varphi(n) - 1\}$$

根据定理3.5.2，α 为 Z_m^* 的一个生成元，则 $\beta = \alpha^i \pmod{m}$ 为 Z_m^* 的生成元当且 仅当 $(i, \varphi(m)) = 1$ 。

由此可知，若 Z_m^* 为循环的，则生成元的个数为 $\varphi(\varphi(m))$ 。

定理3.5.3 Z_m^*有生成元当且仅当 $m=2,4,p^k,2p^k$ 时，这里 p 为一个奇素数，且$k \geq 1$。特别地，如果p 为一素数，则 Z_p^* 有生成元。

该定理的证明超出了本文的范围，有兴趣的话可以参阅相关文献。

例3.5.2

（1）Z_{21}^*不是循环的，因为 Z_{21}^* 中没有一个元素的阶为 $\varphi(21)=12$ ，注意到**21**不满足定理**3.5.3**的条件。

（2）Z_7^* 是循环的，$\varphi(7)=6$ 有生成元$\alpha=5$ 。

$$Z_7^* = \{1=5^6, 2=5^4, 3=5^5, 4=5^2, 5=5^1, 6=5^3\} \mod 7$$

3.5 循环群

循环群的子群和商群

定理3.5.4 循环群的子群是循环群。循环群的商群也是循环群。

证明思路 寻找生成元。

证明 设$G=\langle a\rangle$是循环群，H是G的子群，不妨设$H\neq\{e\}$。在自然数N的子集

$$S=\{s\in N\mid a^s\in H\}$$

中，注意到$a^s\in H\Leftrightarrow(a^s)^{-1}=a^{-s}\in H$，可知$S$是非空集合。取$S$中的最小元素$d$，可断言$H=\langle a^d\rangle$。

循环群的子群和商群（续）

事实上，任取$a^t \in H$，不妨设$t > 0$ 。令$t = dq + r, 0 \leq r < d$, $q \in Z$。于是有

$$a^r = a^{t-dq} = a^t(a^d)^{-q} \in H$$

根据d的极小性, $r = 0$。因此有$t = dq$,$a^t = (a^d)^q \in \langle a^d \rangle$，故$H = \langle a^d \rangle$是个循环群。

容易验证 aH 是商群G/H的生成元，证明作为作业。

循环群的结构

定理3.5.5 设$G=\langle a\rangle$是循环群，有

若a的阶是无限，则G与整数加群Z同构；

若a的阶是某个正整数m，则G与整数模m的剩余类加群同构。

证明思路：构造同态映射，然后再利用群同态基本定理。

定理3.5.5的证明

定义$f:Z\rightarrow G$为$f(k)=a^k$，则f是个满射。又对于任意整数$l,n\in Z$，有

$$f(l+n)=a^{l+n}=a^la^n=f(l)f(n)$$

故f是个群同态。

（1） 若$o(a)=\infty$,$n\in\ker(f)$，则$f(n)=a^n=e$，故$n=0$，即$\ker(f)=\{0\}$。根据定理3.4.4，有

$$Z=Z/\{0\}\cong G$$

定理3.5.5的证明（续）

若 $o(a)=m$,$n\in\ker(f)$，则 $f(n)=a^n=e$。设

$$n=qm+r, 0\le r<m$$

则 $e=a^n=(a^m)^q a^r=a^r$。

由阶的定义,$r=0$，所以$m\mid n$。反之，若$m\mid n$，则有$a^n=e$

故$\ker(f)=\{mk\mid k\in Z\}=mZ$。由定理3.4.4，有

$$Z_m=Z/mZ\cong G$$

3.5 循环群

群中的离散对数问题

定义3.5.3 设$G=\langle a\rangle$是循环群。群G中的离散对数问题是指：给定G中一个元素h，找到正整数k，使得

$$h=a^k$$

我们把k称为h相对于生成元的离散对数，记作

$$k=\log_a h$$

离散对数的例子

例3.5.3 $(Z,+)$
离散对数问题是平凡的

例3.5.4 Z_m，模m剩余类组成的加法群，a 为Z_m 的一个生成元，离散对数问题为：给定$h \in Z_m$，求解x，使得

$$ax \equiv h \pmod{m}$$

用扩展的欧几里得算法很容易求解。

$$\log_a h = x \equiv ha^{-1} \pmod{m}$$