第六讲循环群

陈建文

October 8, 2022

定义1. 群G称为循环群，如果G是由其中的某个元素a生成的，即$G = (a) = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}$。

例. 整数加法群$(Z,+)$为循环群，其生成元为1。

例. 模n同余类加群$Z_n = \{[0],[1],\cdots,[n-1]\}$为一个阶为$n$的有限循环群，其生成元为$[1]$。

定理1. （*1*）循环群$G = (a)$为无穷循环群的充分必要条件是a的阶为无穷大，此时$G = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}$；

（*2*）循环群$G = (a)$为n阶循环群的充分必要条件是a的阶为n，此时$G = \{e, a, a^2, \cdots, a^{n-1}\}$。

定理2. （*1*）无穷循环群同构于整数加群$(Z,+)$，即如果不计同构，无穷循环群只有一个，就是整数加群；

（*2*）阶为n的有限循环群同构于模n同余类加群$(Z_n,+)$，即如果不计同构，n阶循环群只有一个，就是模n同余类加群。

定理3. 设$G = (a)$为由a生成的循环群，则

（*1*）循环群的子群仍为循环群；

（*2*）如果G为无限循环群，则$H_0 = \{e\}, H_m = (a^m), m = 1, 2, \cdots$为$G$的所有子群，这里$H_m, m = 1, 2, \cdots$都同构于$G$；

（*3*）如果G为阶为n的循环群，则$H_0 = \{e\}, H_m = (a^m), m|n$为$G$的所有子群。每个子群$H_m, m = 1, 2, \cdots$的阶为$n/m$。

例. 设$a \in Z$，$b \in Z$，a和b不全为0，则在整数加群$(Z,+)$中集合$\{a,b\}$的生成子群为$H = \{ma + nb | m \in Z, n \in Z\}$。由于循环群$(Z,+)$的每个子群都为循环群，因此存在正整数$d$,使得$H = (d)$。这里$d$为$a$和$b$的最大公约数$(a,b)$。这是因为由$a \in H$知存在$p \in Z$，使得$a = pd$，即$d|a$；由$b \in H$知存在$q \in Z$，使得$b = qd$，即$d|b$；又因为$d \in H$，从而存在$m \in Z, n \in Z$，使得$d = ma + nb$，从而$\forall d' \in Z$，由$d'|a$并且$d'|b$，可以得到$d'|d$。

定理4. 设$a, b \in Z$，$b > 0$，$a = qb + r$，$0 \le r < b$，则$(a,b) = (b,r)$。

证明. 设$A = \{x \in Z | x > 0, x|a, x|b\}$，$B = \{x \in Z | x > 0, x|b, x|r\}$,以下证明$A = B$，从而集合$A$中最大的数等于集合$B$中最大的数，即$(a,b) = (b,r)$。

$\forall x \in A$，则$x > 0$,$x|a$并且$x|b$，由$a = qb + r$知$x|r$，从而$x > 0$，$x|b$且$x|r$，即$x \in B$；$\forall x \in B$，则$x > 0$,$x|b$并且$x|r$，由$a = qb + r$知$x|a$，从而$x > 0$，$x|a$且$x|b$，即$x \in A$。 □

例. 计算$(266,112)$，并将其表示成$m\cdot 266+n\cdot 112$的形式。

解. 由

$$\begin{aligned}266&=2*112+42\\112&=2*42+28\\42&=1*28+14\\28&=2*14+0\end{aligned}$$

可得$(266,112)=14$。

由

$$\begin{aligned}42&=266+(-2)*112\\28&=112+(-2)*42\\&=112+(-2)*(266+(-2)*112)\\&=(-2)*266+5*112\\14&=42+(-1)*28\\&=(266+(-2)*112)+(-1)*((-2)*266+5*112)\\&=3*266+(-7)*112\end{aligned}$$

得$(266,112)=3*266+(-7)*112$。 □

课后作业题:

练习1. 证明：n次单位根之集对数的通常乘法构成一个循环群。

练习2. 找出模12的同余类加群的所有子群。

练习3. 设$G=(a)$为一个n阶循环群。证明：如果$(r,n)=1$，则$(a^r)=G$。

练习4. 设群G中元素a的阶为n，$(r,n)=d$。证明：a^r的阶为n/d。