

第六讲循环群

陈建文

October 30, 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 $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ 。

例. 整数加法群 $(\mathbb{Z}, +)$ 为循环群, 其生成元为1。

例. 模 n 同余类加群 $Z_n = \{[0], [1], \dots, [n-1]\}$ 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 $G = \langle a \rangle$ 为无穷循环群的充分必要条件是 a 的阶为无穷大, 此时 $G = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$;

(2) 循环群 $G = \langle a \rangle$ 为 n 阶循环群的充分必要条件是 a 的阶为 n , 此时 $G = \{e, a, a^2, \dots, a^{n-1}\}$ 。 $\forall m \in \mathbb{Z}, a^m = a^{m \bmod n}$ 。

证明. $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$

分两种情况讨论:

(1) a 的阶为无穷大

以下证明 $\forall i, j \in \mathbb{Z}, i \neq j \rightarrow a^i \neq a^j$ 。

用反证法。不妨设 $j > i$ 。假设 $a^i = a^j$, 则 $a^{j-i} = e$, 与 a 的阶为无穷大矛盾。

(2) a 的阶为 n

要证 $G = \{e, a, a^2, \dots, a^{n-1}\}$ 。

$\forall m \in \mathbb{Z}, \exists i, 0 \leq i \leq n-1, a^m = a^i$

$m = qn + r, 0 \leq r < n, a^m = a^{qn+r} = (a^n)^q a^r = a^r, \forall m \in \mathbb{Z}, a^m = a^{m \bmod n}$ 。

$\forall i, j, 0 \leq i \leq n-1, 0 \leq j \leq n-1, a^i \neq a^j$ 。

用反证法。假设 $a^i = a^j$, 不妨设 $j > i$, 则 $a^{j-i} = e, 0 < j-i \leq n-1$, 这与 a 的阶为 n 矛盾。 \square

定理2. (1) 无穷循环群同构于整数加群 $(\mathbb{Z}, +)$, 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。

证明. (1) 设 $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$

$\phi: G \rightarrow \mathbb{Z}, \forall i \in \mathbb{Z}, \phi(a^i) = i$

$\phi(a^i \circ a^j) = \phi(a^{i+j}) = i+j = \phi(a^i) + \phi(a^j)$

(2) 设 $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

$$\begin{aligned}\phi: G \rightarrow Z_n, \quad \forall i \in Z, 0 \leq i \leq n-1, \phi(a^i) &= [i] \\ \forall i, j, 0 \leq i \leq n-1, 0 \leq j \leq n-1, \phi(a^i \circ a^j) &= \phi(a^{i+j}) = \phi(a^{(i+j) \bmod n}) = \\ [(i+j) \bmod n] &= [i+j] = [i] + [j] = \phi(a^i) \circ \phi(a^j).\end{aligned}$$

□

定理3. 设 $G = \langle a \rangle$ 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 $H_0 = \{e\}, H_m = \langle a^m \rangle, m = 1, 2, \dots$ 为 G 的所有子群, 这里 $H_m, m = 1, 2, \dots$ 都同构于 G ;
- (3) 如果 G 为 n 阶循环群, 则 $H_0 = \{e\}, H_m = \langle a^m \rangle, m|n$, 为 G 的所有子群。每个子群 H_m 的阶为 $\frac{n}{m}$ 。

证明. (1) 设 H 为循环群 $G = \langle a \rangle$ 的子群, 令 $m = \min\{i \in Z^+ | a^i \in H\}$, 以下证明 $H = \langle a^m \rangle$. $\forall j \in Z$, 如果 $a^j \in H, j = qm + r, 0 \leq r < m$, 则 $a^j = a^{qm+r} = (a^m)^q a^r$, 从而 $a^r = a^j (a^m)^{-q} \in H$, 此时必有 $r = 0$, 于是 $a^j = (a^m)^q$, 从而 $H \subseteq \langle a^m \rangle$. $\langle a^m \rangle \subseteq H$ 显然成立, 于是 $H = \langle a^m \rangle$.

(2) 显然 $H_0, H_m, m = 1, 2, \dots$ 都为 G 的子群。设 H 为 G 的任意一个子群, 由 (1) 知 H 为循环群, 从而 $\exists m \in Z$, 使得 $H = \langle a^m \rangle = \langle a^{-m} \rangle$.

(3) 由 (2) 知, $H_0 = \{e\}, \langle a^k \rangle, k = 1, 2, \dots$ 为 G 的所有子群。

$\forall k, k = 1, 2, \dots$, 令 $m = \min\{i \in Z^+ | a^i \in \langle a^k \rangle\}$. 由 (1) 的证明过程知 $\langle a^k \rangle = \langle a^m \rangle$, 以下证明 $m|n$.

设 $n = qm + r, 0 \leq r < m$, 则 $a^n = a^{qm+r} = (a^m)^q a^r$, 由 a 的阶为 n 知 $a^n = e$, 从而 $e = (a^m)^q a^r$, 于是 $a^r = (a^m)^{-q} \in \langle a^m \rangle = \langle a^k \rangle$, 此时必有 $r = 0$, 否则与 m 的定义矛盾, 所以 $m|n$.

由 $(a^m)^{\frac{n}{m}} = e$, 当 $0 < k < \frac{n}{m}$ 时, $(a^m)^k \neq e$ 知 a^m 的阶为 $\frac{n}{m}$, 此时 $\langle a^m \rangle = \{e, a^m, a^{2m}, \dots, a^{\frac{n}{m}-1}m\}, |\langle a^m \rangle| = \frac{n}{m}$. □

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 $H = \langle d \rangle$. 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 $a, b \in Z, a$ 和 b 不全为 0, 则 $\exists m, n \in Z$ 使得 $(a, b) = ma + nb$.

定理5. 设 $a, b \in Z, b > 0, a = qb + r, 0 \leq r < b$, 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。

证明. n 次单位根之集对数的通常乘法构成的群为 $(\cos(\frac{\theta}{n}) + i\sin(\frac{\theta}{n}))$ 。

□

练习2. 找出模12的同余类加群的所有子群。

解. $([0]) = \{[0]\}$, $([1]) = Z_{12}$, $([2]) = \{[0], [2], [4], [6], [8], [10], [12]\}$, $([3]) = \{[0], [3], [6], [9]\}$, $([4]) = \{[0], [4], [8]\}$, $([6]) = \{[0], [6]\}$ 。

□

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

证明. 由 $(r, n) = 1$ 知存在 $s, t \in Z$, 使得 $1 = sr + tn$, 从而 $a^1 = a^{sr+tn} = (a^r)^s (a^n)^t = (a^r)^s e^t = (a^r)^s$, 于是 $a \in \langle a^r \rangle$, 从而 $\langle a^r \rangle = G$ 。

□

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 。

证明. 以下证明 $\langle a^d \rangle = \langle a^r \rangle$, 而 $|\langle a^d \rangle| = n/d$, 于是 $|\langle a^r \rangle| = n/d$, 从而 a^r 的阶为 n/d 。

由 $(r, n) = d$ 知存在 $s, t \in Z$ 使得 $d = sr + tn$, 从而 $a^d = a^{(sr+tn)} = (a^r)^s (a^n)^t = (a^r)^s e^t = (a^r)^s$, 于是 $a^d \in \langle a^r \rangle$, 由此可得 $\langle a^d \rangle \subseteq \langle a^r \rangle$ 。

设 $r = kd$, 这里 $k \in n$, 于是 $a^r = (a^d)^k$, 从而 $a^r \in \langle a^d \rangle$, 由此可得 $\langle a^r \rangle \subseteq \langle a^d \rangle$ 。

□