0.1 循环群

定义 0.1 (循环群)

设 G 是一个群且 $a \in G$, 我们称

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$$

是**由 a 生成的 G 的子群**, 如果在一个群 G 中存在一个元素 a, 使得 $G = \langle a \rangle$, 即 G 由 a 生成, 则称 G 是**循环群**, a 为 G 的一个**生成元**.

注 对 $\forall n_1, n_2 \in \mathbb{Z}$, 有 $a^{n_1} a^{-n_2} = a^{n_1 - n_2} \in G$. 因此 $\langle a \rangle$ 是 G 的子群. 故由 a 生成的 G 的子群是良定义的.

注 显然若 a 在群 G 中, 则 $\langle a \rangle \subseteq G$.

命题 0.1 (循环群都是 Abel 群)

循环群都是 Abel 群.

证明 设 $G = \langle a \rangle$ 为循环群, 则对任意的 $x, y \in G$, 存在 k, l, 使 $x = a^k$,$y = a^l$, 于是

$$xy = a^k a^l = a^{k+l} = a^l a^k = yx.$$

所以 G 为 Abel 群.

□

命题 0.2 (素数阶群必为循环群)

设 G 是一个群, 且 $|G| = p$ 为一个素数, 则 G 必是循环群, 并且 $\forall a \in G$ 且 $a \neq e$ 有 $G = \langle a \rangle$.

证明 由 $p > 1$ 知 G 中至少存在一个非幺元 $a \neq e$, 则对 $\forall a \in G$ 且 $a \neq e$, 有 $\langle a \rangle$ 是 G 的子群. 由 Lagrange 定理知 $\langle a \rangle$ 的阶是 $|G| = p$ 的因数, 而 p 为素数, 故 $\langle a \rangle$ 的阶为 1 或 p. 由 $a, e \in \langle a \rangle$ 知 $\langle a \rangle$ 的阶必大于 1, 因此 $\langle a \rangle$ 的阶为 p. 又因为 $\langle a \rangle \subseteq G$, 所以 $G = \langle a \rangle$. 故 G 为循环群.

□

定义 0.2

设 a 是群 G 的元素. 若 $\forall k \in \mathbb{N}, a^k \neq 1$, 则称 a 的**阶为无穷**, 记作 $\operatorname{ord} a = \infty$. 若 $\exists k \in \mathbb{N}$, 使得 $a^k = 1$, 则 $r = \min\{k | k \in \mathbb{N}, a^k = 1\}$ 称为 a 的**阶**, 记作 $\operatorname{ord} a = r$.

定理 0.1

有限群 G 的任一元素 a 的阶是 G 的阶的因子, 即 $\operatorname{ord} a \mid |G|$. 特别地, $G = \langle a \rangle \iff \operatorname{ord} a = |G|$.

证明 令 $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$, 容易验证这是 G 的一个子群. 又由于 G 有限, 故 $\langle a \rangle$ 有限, 因而 a 是有限阶的, 设为 d. 对 $n \in \mathbb{Z}$ 有 t_n 与 r_n $(0 \leqslant r_n < d)$, 使 $n = t_n d + r_n$, 于是 $a^n = a^{r_n}$. 因此 $\langle a \rangle$ 中至多只有 d 个元素 $1, a, \cdots, a^{d-1}$.

又对 $\forall r_1, r_2 \in \mathbb{N}$, 且 $r_1 \neq r_2, 0 \leqslant r_1, r_2 < d$, 则 $|r_1 - r_2| < d$, 从而 $a^{r_1 - r_2} \neq 1$, 进而 $a^{r_1} \neq a^{r_2}$. 故 $1, a, \cdots, a^{d-1}$ 互不相同. 由此知 $\langle a \rangle = \{1, a, \cdots, a^{d-1}\}$, 即 $\langle a \rangle$ 是 d 阶群. 故由 Lagrange 定理知 d 为 $[G:1]$ 的因子.

设 $\operatorname{ord} a = d$. 若 $G = \langle a \rangle$, 则由上述证明知 $G = \langle a \rangle = \{1, a, \cdots, a^{d-1}\}$ 是 d 阶群, 故 $d = |G|$. 又若 $d = |G|$, 则由上述证明知 $\langle a \rangle = d = |G|$. 又显然有 $\langle a \rangle \subseteq G$, 故 $\langle a \rangle = G$.

□

定理 0.2 (群元素的阶的基本性质)

设 $(G, \cdot)$ 是一个群,$a, b \in G$, 则

(1) a 的阶为无穷当且仅当 $\forall m, n \in \mathbb{Z}$ 且 $m \neq n$ 时, $a^m \neq a^n$.

(2) 设 a 的阶为 d, 则

$$a^m = a^n \iff m \equiv n \pmod d. \tag{1}$$

特别地, 我们有

$$\operatorname{ord} a = 1 \iff a = 1, \quad a^{-1} = a \iff a = 1 \text{或} \operatorname{ord} a = 2.$$

(3) $\operatorname{ord} a = \operatorname{ord} a^{-1} = \operatorname{ord}(gag^{-1}), \forall g \in G$. 进而 $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

(4) 若 a 为 m 阶元素, 则对 $\forall k \in \mathbb{N}, a^k$ 的阶为 $\dfrac{m}{(m,k)}$, 其中 (m,k) 是 m 与 k 的最大公因数.
进而, a^k 为 m 阶元素的充要条件是 $(m,k) = 1$.

(5) 若 a, b 的阶分别为 m, n 且 $\langle a \rangle \cap \langle b \rangle = \{1\}, ab = ba$, 则 ab 的阶为 m, n 的最小公倍数 $[m, n]$.

(6) 若 a, b 的阶分别为 m, n 且 $ab = ba, (m, n) = 1$, 则 ab 的阶为 mn.

(7) 设群 G 中的元 g 的阶 $\operatorname{ord} g = mn, (m, n) = 1$. 则 $g = ab, \operatorname{ord} a = m, \operatorname{ord} b = n$, 且 a, b 均为 g 的幂.

(8) 设 $\operatorname{ord} a = n, r$ 是任一整数. 如果 $(n, r) = d$, 则 $\langle a^r \rangle = \langle a^d \rangle$.

证明

(1) 事实上, 若 a 的阶为无穷, 而有 $m \neq n$, 使 $a^m = a^n$. 设 $m > n$, 于是 $a^m(a^n)^{-1} = 1$, 而 $a^m(a^n)^{-1} = a^{m-n} = 1$, 自然 $m - n \in \mathbb{N}$. 矛盾.
反之, $\forall m, n \in \mathbb{Z}$ 且 $m \neq n$, 有 $a^m \neq a^n$, 则 $a^{m-n} = a^m(a^n)^{-1} = 1$, 即 $\forall k \in \mathbb{N}$ 有 $a^k \neq 1$, 故 a 的阶为无穷.

(2) 设 a 的阶为 d, $m, n \in \mathbb{N}$, 由带余除法知, 一定能找到整数 t_1, t_2, r_1, r_2, 使 $m = dt_1 + r_1 (0 \leqslant r_1 < d)$, $n = dt_2 + r_2 (0 \leqslant r_2 < d)$. 于是 $a^m = (a^d)^{t_1} a^{r_1} = a^{r_1}$, $a^n = (a^d)^{t_2} a^{r_2} = a^{r_2}$, 因而

$$a^m = a^n \iff a^{r_1} = a^{r_2} \iff a^{r_1 - r_2} = a^{r_2 - r_1} = 1.$$

又 $|r_1 - r_2| < d$, 故上式也等价于 $r_1 - r_2 = 0$, 即式 (1) 成立. 特别地, 由 (1) 式可得

$$a^{-1} = a \iff a^2 = 1 = a^0 \iff 2 \equiv 0 \pmod d \iff \operatorname{ord} a = 1 \text{或} 2 \iff a = 1 \text{或} \operatorname{ord} a = 2.$$

(3) 如果 $\operatorname{ord} a$ 或 $\operatorname{ord} a^{-1}$ 有一个为有限的, 记为 n. 则由 $(a^n)^{-1} = (a^{-1})^n$ 知另一个也必是有限的, 这说明 $\operatorname{ord} a$ 与 $\operatorname{ord} a^{-1}$ 必同时有限或同时无限, 故仅需对 $\operatorname{ord} a$ 与 $\operatorname{ord} a^{-1}$ 同时有限的情形加以证明. 再由 $(a^n)^{-1} = (a^{-1})^n$ 知 $a^k = 1$ 当且仅当 $(a^{-1})^k = 1$, 故 a^{-1} 与 a 同阶.
如果 $\operatorname{ord} a$ 或 $\operatorname{ord}(gag^{-1})$ 有一个为有限的, 当 $\operatorname{ord} a = n < \infty$ 时, 则

$$(gag^{-1})^n = ga^n g^{-1} = 1,$$

故 $\operatorname{ord}(gag^{-1}) \leqslant n < \infty$. 当 $\operatorname{ord}(gag^{-1}) < \infty$ 时, 同理可证 $\operatorname{ord} a < \infty$. 这说明 $\operatorname{ord} a$ 与 $\operatorname{ord}(gag^{-1})$ 必同时有限或同时无限, 故仅需对 $\operatorname{ord} a$ 与 $\operatorname{ord}(gag^{-1})$ 同时有限的情形加以证明. 现设 $\operatorname{ord} a = r_1, \operatorname{ord}(gag^{-1}) = r_2$, 则

$$a^{r_2} = g^{-1}(gag^{-1})^{r_2} g = 1,$$
$$(gag^{-1})^{r_1} = ga^{r_1} g^{-1} = 1.$$

由此得 $r_2 \geqslant r_1, r_1 \geqslant r_2$, 从而 $r_1 = r_2$. 所以 gag^{-1} 与 a 有相同的阶.
注意到 $ba = b(ab)b^{-1}$, 故只需取 $g = b$, 则由上述证明知 ab 与 ba 有相同的阶.

(4) 设 a^k 的阶为 q, 即 $a^{kq} = 1$, 因而有 $m | kq$, 故由数论相关结论知 $\dfrac{m}{(m,k)} | q$. 又 $(a^k)^{\frac{m}{(m,k)}} = (a^m)^{\frac{k}{(m,k)}} = 1$, 即得 $q | \dfrac{m}{(m,k)}$, 因而 $q = \dfrac{m}{(m,k)}$.

(5) 设 ab 的阶为 m_1, 则有 $(ab)^{m_1} = 1$. 由 $ab = ba$ 知 $a^{m_1} b^{m_1} = (ab)^{m_1} = 1$, 即 $a^{m_1} = b^{-m_1} \in \langle a \rangle \cap \langle b \rangle = \{1\}$, 因而 $a^{m_1} = b^{m_1} = 1$, 故 $m | m_1, n | m_1$, 因而 $[m, n] | m_1$. 另有 $(ab)^{[m,n]} = a^{[m,n]} b^{[m,n]} = 1$, 故 $m_1 | [m, n]$, 即 $m_1 = [m, n]$.

(6) 设 m_1 是 $\langle a \rangle \cap \langle b \rangle$ 的阶, 由定理 0.1 知 $\langle a \rangle, \langle b \rangle$ 的阶分别为 m, n. 由于 $\langle a \rangle \cap \langle b \rangle$ 是 $\langle a \rangle, \langle b \rangle$ 的子群, 故由 Lagrange 定理知 $m_1 | m, m_1 | n$. 但 $(m, n) = 1$, 故 $m_1 = 1$, 因而 $\langle a \rangle \cap \langle b \rangle = \{1\}$, 于是由定理 0.2(5) 知 ab 的阶为 $[m, n] = mn$.

(7) 因 $(m, n) = 1$, 故有整数 s, t 使得 $sm + tn = 1$, 而且 $(t, m) = (s, n) = 1$. 令 $a = g^{tn}, b = g^{sm}$, 则 $g = ab$, 并且由

可得

$$\operatorname{ord} a=\operatorname{ord} g^{tn}=\frac{\operatorname{ord} g}{(tn,\operatorname{ord} g)}=\frac{mn}{n(t,m)}=m,$$
$$\operatorname{ord} b=\operatorname{ord} g^{sm}=\frac{\operatorname{ord} g}{(sm,\operatorname{ord} g)}=\frac{mn}{m(s,n)}=n.$$

(8) 因为 $(n,r)=d$, 所以存在 $u,v\in\mathbb{Z}$, 使

$$d=nu+rv.$$

于是 $a^d=a^{nu+rv}=a^{rv}\in\langle a^r\rangle$, 故 $\langle a^d\rangle\subseteq\langle a^r\rangle$. 另一方面, 同样由于 $(n,r)=d$, 所以 $d\mid r$, 从而又有 $a^r\in\langle a^d\rangle$, 于是 $\langle a^r\rangle\subseteq\langle a^d\rangle$. 由此得 $\langle a^r\rangle=\langle a^d\rangle$.

□

例题 0.1 设群 G 中两个元 g,h 可换, $o(g)=m$, $o(h)=n$. 记 $(m,n),[m,n]$ 分别是 m,n 的最大公因子和最小公倍数. 则

(1) $\operatorname{ord}(g^nh^m)=\dfrac{[m,n]}{(m,n)}$;

(2) G 中存在阶为 (m,n) 的元;

(3) G 中存在阶为 $[m,n]$ 的元.

证明

(1) 由定理 0.2(4)知 $\operatorname{ord} g^n=\dfrac{m}{(m,n)}$, $\operatorname{ord} h^m=\dfrac{n}{(m,n)}$, $g^nh^m=h^mg^n$, $\left(\dfrac{m}{(m,n)},\dfrac{n}{(m,n)}\right)=1$, 故由定理 0.2(6)知

$$o(g^nh^m)=\frac{m}{(m,n)}\cdot\frac{n}{(m,n)}=\frac{[m,n]}{(m,n)}.$$

(2) 设 $m=p_1^{m_1}\cdots p_t^{m_t}$, $n=p_1^{n_1}\cdots p_t^{n_t}$, 其中 $p_1,\cdots,p_t$ 是互不相同的素数, m_i,n_i 均为非负整数. 不妨设 $m_i\geqslant n_i, 1\leqslant i\leqslant l$; $m_i<n_i, l+1\leqslant i\leqslant t$. 令

$$a=p_1^{m_1}\cdots p_l^{m_l},\quad b=p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}.$$

则由定理 0.2(4)知

$$\operatorname{ord} g^a=\frac{m}{(a,m)}=p_{l+1}^{m_{l+1}}\cdots p_t^{m_t},\quad \operatorname{ord} h^b=p_1^{n_1}\cdots p_l^{n_l}.$$

这两个阶显然是互素的, 且 g^a 与 h^b 可换, 因此由定理 0.2(6)知

$$\operatorname{ord} g^ah^b=p_1^{n_1}\cdots p_l^{n_l}p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}=(m,n).$$

(3) 设 $m=p_1^{m_1}\cdots p_t^{m_t}$, $n=p_1^{n_1}\cdots p_t^{n_t}$, 其中 $p_1,\cdots,p_t$ 是互不相同的素数, m_i,n_i 均为非负整数. 不妨设 $m_i\geqslant n_i, 1\leqslant i\leqslant l$; $m_i<n_i, l+1\leqslant i\leqslant t$. 令

$$a=p_{l+1}^{m_{l+1}}\cdots p_t^{m_t},\quad b=p_1^{n_1}\cdots p_l^{n_l}.$$

则由定理 0.2(4)知

$$\operatorname{ord} g^a=\frac{m}{(a,m)}=p_1^{m_1}\cdots p_l^{m_l},\quad \operatorname{ord} h^b=p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}.$$

这两个阶显然是互素的, 且 g^a 与 h^b 可换, 因此由定理 0.2(6)知

$$\operatorname{ord} g^ah^b=p_1^{m_1}\cdots p_l^{m_l}p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}=[m,n].$$

□

定理 0.3

循环群的任何子群也是循环群. 进而循环群 $\langle a\rangle$ 的所有子群构成的集合为

$$\{\langle a^r\rangle\mid r=0,1,2\cdots\}.$$

♡

证明 设 G_1 是循环群 $G=\langle a\rangle$ 的一个非平凡子群. 令

$$k=\min\{m'\in\mathbb{N}|a^{m'}\in G_1\},$$

于是 G 中由 a^k 生成的子群 $\langle a^k\rangle \subseteq G_1$. 又若有 $a^{m'} \in G_1$, 则有整数 q, r 满足

$$m' = kq + r, \quad 0 \leqslant r < k,$$

因而 $a^r = a^{m'}(a^k)^{-q} \in G_1$, 由 k 的取法知 $r = 0$, 否则与 k 的最小值取法矛盾! 因而 $a^{m'} = (a^k)^q \in \langle a^k\rangle$, 故 $G_1 \subseteq \langle a^k\rangle$, 所以 $G_1 = \langle a^k\rangle$ 为循环群. 于是 $G_1 \subseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$. 因此记 $\langle a\rangle$ 的所有子群构成的集合为 S, 则 $S \subseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$. 又显然有 $S \supseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$, 故

$$S = \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}.$$

□

推论 0.1

(1) 设 $m \in \mathbb{Z}$, 则 $m\mathbb{Z} \triangleq \{mx | x \in \mathbb{Z}\}$ 是整数加法群 $\mathbb{Z}$ 的子群.

(2) 整数加法群 $\mathbb{Z}$ 的任何子群必形如 $m\mathbb{Z}(m \in \mathbb{N}_0)$.

♡

证明

(1) 对 $\forall x_1, x_2 \in \mathbb{Z}$, 有

$$mx_1 - mx_2 = m(x_1 - x_2) \in m\mathbb{Z}.$$

故 $m\mathbb{Z}$ 是整数加法群 $\mathbb{Z}$ 的子群.

(2) 事实上, $\mathbb{Z} = \langle 1\rangle$. 设 G_1 为 $\mathbb{Z}$ 的子群. 于是由定理 0.3有 $m \geqslant 0$且$m \in \mathbb{Z}$, 使得 $G_1 = \langle m\rangle = m\mathbb{Z}$.

□

命题 0.3

设 $m > 0$, 则有

$$m\mathbb{Z} \lhd \mathbb{Z}, \quad \mathbb{Z} = \bigcup_{k=0}^{m-1}(k + m\mathbb{Z}), \quad \mathbb{Z}_m \triangleq \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}, \quad |\mathbb{Z}_m| = [\mathbb{Z} : m\mathbb{Z}] = m.$$

♠

证明 由推论 0.1(1)知 $m\mathbb{Z}$ 为 $\mathbb{Z}$ 的子群.

□

定理 0.4

设 $G = \langle a\rangle$ 为循环群, 则有以下结论.

(1) $\langle a^{-1}\rangle = \langle a\rangle$.

(2) 如果 $|G| = \infty$, 则

(i) $G = \{1, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \cdots\}$, 且对 $\forall k, l \in \mathbb{Z}$, 有 $a^k = a^l \iff k = l$.

(ii) a 与 a^{-1} 是 G 的两个仅有的生成元.

(iii) G 的全部子群为 $\{\langle a^d\rangle \mid d = 0, 1, 2, \cdots\}$, 并且对 $\forall d_1, d_2 \in \mathbb{N}_0$且$d_1 \neq d_2$, 有 $\langle a^{d_1}\rangle \neq \langle a^{d_2}\rangle$.

(iv) $G \cong (\mathbb{Z}, +)$.

(3) 如果 $|G| = n < \infty$, 则

(i) $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$, 且对 $\forall k, l \in \mathbb{Z}$, 有 $a^k = a^l \iff n \mid k - l$.

(ii) G 恰有 $\phi(n)$ 个生成元, 且 a^r 是 G 的生成元的充分必要条件是 $(n, r) = 1$, 其中,$\phi(n)$ 是欧拉函数.

(iii) G 的全部子群为 $\{\langle a^d\rangle \mid d$ 为 n 的正因子 $\}$, 并且对 $\forall d_1, d_2$ 为 n 的不同正因子, 有 $\langle a^{d_1}\rangle \neq \langle a^{d_2}\rangle$. 若还有正整数 n 的标准分解式为

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s},$$

其中 $p_1, p_2, \cdots, p_s$ 是 n 的不同素因子. 则 n 阶循环群 G 的子群的个数为

$$r = (r_1 + 1)(r_2 + 1) \cdots (r_s + 1).$$

(iv) $G \cong \mathbb{Z}_n$.

♡

证明

(1) 由循环群的定义易得.

(2) (i) 由循环群的定义知 $G = \{1, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \cdots\}$. 因为这个集合中的元素互不相同, 所以

$$a^k = a^l \iff a^{k-l} = 1 \iff k - l = 0 \iff k = l.$$

(ii) 由定理 0.4(1)知 a 与 a^{-1} 都是 G 的生成元. 又如,a^k 是 G 的任一生成元, 则存在 $n \in \mathbb{Z}$, 使

$$(a^k)^n = a^{kn} = a.$$

由定理 0.4(2)(i)得 $kn = 1$, 从而 $k = \pm 1$.

(iii) 如果 $|G| = \infty$, 由定理 0.3知 G 的所有子群构成的集合为

$$S = \{\langle a^r \rangle \mid r = 0, 1, 2, \cdots\}.$$

只需证这个集合中的元素两两不同即可. 因为对任意的 $r_1 > r_2 > 0$, 有 $r_1 \nmid r_2$, 所以 $a^{r_2} \notin \langle a^{r_1} \rangle$, 于是

$$\langle a^{r_1} \rangle \neq \langle a^{r_2} \rangle.$$

另一方面, 对任意的 $r > 0$, 显然 $a^r \notin \langle a^0 \rangle = \langle 1 \rangle = \{1\}$, 所以有

$$\langle a^r \rangle \neq \langle 1 \rangle.$$

故 $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle, \forall d_1, d_2 \in \mathbb{N}_0$且$d_1 \neq d_2$.

(iv) 证法一:令

$$\begin{aligned} \phi : \mathbb{Z} &\to G, \\ k &\mapsto a^k, \quad \forall k \in \mathbb{Z}. \end{aligned}$$

显然 ϕ 是 $\mathbb{Z}$ 到 G 的良定义的映射;
设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由定理 0.2(4)得,$k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射;
对任意的 $a^k \in G$, 有 $k \in \mathbb{Z}$, 使 $\phi(k) = a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射;
对任意的 $k, l \in \mathbb{Z}$,

$$\phi(k + l) = a^{k+l} = a^k \cdot a^l = \phi(k) \cdot \phi(l),$$

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此,$G \cong (\mathbb{Z}, +)$.

证法二:作 $\mathbb{Z}$ 到 G 上的映射 $\varphi : \varphi(n) = a^n (n \in \mathbb{Z})$. 于是有

$$\varphi(n_1 + n_2) = a^{n_1+n_2} = a^{n_1} \cdot a^{n_2} = \varphi(n_1)\varphi(n_2),$$

因而 φ 是 $\mathbb{Z}$ 到 G 上的同态映射, 故由群的同态基本定理知 $G \cong \mathbb{Z}/\ker\varphi$ 且 $\ker\varphi \lhd \mathbb{Z}$. 由推论 0.1(2)知存在 $m \in \mathbb{N}_0$, 使得 $\ker\varphi = m\mathbb{Z}$. 因此 $G \cong \mathbb{Z}/m\mathbb{Z}$.
若 $m \neq 0$, 则由命题 0.3知

$$G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

从而 $|G| = |\mathbb{Z}_m| = m < \infty$, 这与 $|G| = \infty$ 矛盾! 故此时 $m = 0$, 因此 $G \cong \mathbb{Z}$.

(3) (i) 由定理 0.1知 $\operatorname{ord} a = n$, 故 $a^n = 1$. 注意到对 $\forall m \in \mathbb{Z}$, 有

$$m \equiv 0 \text{ or } 1 \text{ or } \cdots \text{ or } n-1 \pmod{n}.$$

故由定理 0.2(2)知

$$a^m = 1 \text{ or } a \text{ or } \cdots \text{ or } a^{n-1}.$$

因此 $\langle a \rangle \subseteq \{1, a, \cdots, a^{n-1}\}$. 又显然有 $\langle a \rangle \supseteq \{1, a, \cdots, a^{n-1}\}$, 故 $\langle a \rangle = \{1, a, \cdots, a^{n-1}\}$.
对 $\forall k, l \in \mathbb{Z}$, 由定理 0.2(2)知

$$a^k = a^l \iff k \equiv l \pmod{n} \iff n \mid k - l.$$

(ii) 由定理 0.2(4)可得 $\operatorname{ord} a^r = \dfrac{n}{(n,r)}$. 再由定理 0.1可得

$$a^r \text{为} G \text{的生成元} \iff \operatorname{ord} a^r = n \iff \frac{n}{(n,r)} = n \iff (n,r) = 1,$$

故由欧拉函数的定义知 G 的生成元的个数为 $\phi(n)$.

(iii) 如果 $|G| = n$, 对任意的正整数 r, 存在 n 的正因子 $d = (n,r)$, 由定理 0.2(8)可知

$$\langle a^r \rangle = \langle a^d \rangle \in \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}.$$

记 G 的所有子群构成的集合为 S, 则由定理 0.3知 $S \subseteq \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}$. 又显然有 $S \supseteq \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}$, 故

$$S = \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}.$$

若 $d_1 > d_2$ 为 n 的两个不同的正因子, 则 $d_1 \nmid d_2$, 于是 $a^{d_2} \notin \langle a^{d_1} \rangle$, 从而

$$\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle.$$

故 $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle, \forall d_1, d_2$ 为 n 的不同正因子.

由上述证明知,n 阶循环群 G 的子群的个数恰为 n 的不同正因子的个数. 而 n 的不同正因子的个数等于

$$(r_1+1)(r_2+1)\cdots(r_s+1),$$

即得所证.

(iv) 证法一:作 $\mathbb{Z}$ 到 G 上的映射 $\varphi : \varphi(n) = a^n (n \in \mathbb{Z})$. 于是有

$$\varphi(n_1+n_2) = a^{n_1+n_2} = a^{n_1} \cdot a^{n_2} = \varphi(n_1)\varphi(n_2),$$

因而 φ 是 $\mathbb{Z}$ 到 G 上的同态映射, 故由群的同态基本定理知 $G \cong \mathbb{Z}/\ker\varphi$ 且 $\ker\varphi \lhd \mathbb{Z}$. 由推论 0.1(2)知存在 $m \in \mathbb{N}_0$, 使得 $\ker\varphi = m\mathbb{Z}$. 因此 $G \cong \mathbb{Z}/m\mathbb{Z}$.

若 $m \neq n$, 则当 $m = 0$ 时, 有 $G \cong \mathbb{Z}$, 从而 $|G| = \infty$ 矛盾! 当 $m \neq 0, n$ 时, 有

$$G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

从而 $|G| = |\mathbb{Z}_m| = m \neq n$ 矛盾! 故 $m = n$. 因此

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

证法二:令

$$\begin{aligned} \phi : \mathbb{Z}_n &\to G, \\ \bar{k} &\mapsto a^k, \quad \forall \bar{k} \in \mathbb{Z}_n. \end{aligned}$$

设 $\bar{k} = \bar{l}$, 则 $n \mid k-l$, 于是 $a^{k-l} = e$, 从而 $a^k = a^l$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的良定义的映射;

设 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 如果 $\phi(\bar{k}) = \phi(\bar{l})$, 即 $a^k = a^l$, 则 $n \mid k-l$, 从而 $\bar{k} = \bar{l}$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的单映射;

对任意的 $a^k \in G$, 有 $\bar{k} \in \mathbb{Z}_n$, 使 $\phi(\bar{k}) = a^k$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的满映射;

对任意的 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 有

$$\phi(\bar{k}+\bar{l}) = \phi(\overline{k+l}) = a^{k+l} = a^k \cdot a^l = \phi(\bar{k}) \cdot \phi(\bar{l}),$$

所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的同构映射. 因此 $G \cong (\mathbb{Z}_n, +)$.

□

推论 0.2

两个循环群同构当且仅当它们的阶相同.

证明 设 G_1, G_2 为两个循环群, 则由定理 0.4(2)(iv)和定理 0.4(3)(iv)以及命题 0.3知

$$\begin{aligned} G_1 \cong G_2 &\iff G_1 \cong G_2 \cong \mathbb{Z}\text{或}G_1 \cong G_2 \cong \mathbb{Z}_m (m \in \mathbb{N}) \\ &\iff |G_1| = |G_2| = \infty\text{或}|G_1| = |G_2| = |\mathbb{Z}_m| = m (m \in \mathbb{N}). \end{aligned}$$

□

推论 0.3

(1) 群 G 仅有平凡子群的充分必要条件是 $G=\{1\}$ 或 G 是素数阶循环群.

(2) 无限循环群的非平凡子群仍为无限循环群.

♡

证明

(1) **必要性**: 设 G 仅有平凡子群. 如果 $G=\{1\}$, 则结论成立. 如果 $G\neq\{1\}$, 则存在 $a\in G$, 使 $a\neq 1$, 从而 $\langle a\rangle\neq\{1\}$, 于是由 G 仅有平凡子群知 $\langle a\rangle=G$. 由定理 0.4(2)(iii)可知,G 不可能是无限循环群. 否则, 由定理 0.4(2)(iii)知 G 有无穷多个非平凡子群矛盾! 设 $|G|=n$, 由于 G 仅有平凡子群, 所以再由定理 0.4(3)(iii)知 n 无真因子, 因此 n 为素数.

充分性: 如果 $G=\{1\}$, 则 G 显然只有平凡子群. 如果 G 是素数阶循环群, 则 $|G|$ 的仅有的正因子为 1 及 $|G|$, 由这两个因子得到的都是 G 的平凡子群, 所以再由定理 0.4(3)(iii)知 G 仅有平凡子群.

(2) 设 G 为无限循环群, 则由定理**??**知 $G\cong\mathbb{Z}$. 又由推论 0.1(2)知 $\mathbb{Z}$ 的非平凡子群为 $m\mathbb{Z}(m\in\mathbb{Z}且m\neq 0,1)$ 为无限循环群. 故 G 的非平凡子群也为无限循环群.

□

例题 0.2

(1) 任一偶数阶群必含有阶为 2 的元素.

(2) 设 $n>2$, 则有限群 G 中有偶数个阶为 n 的元.

证明

(1) 设 S 为 G 的所有阶大于 2 的元素的集合,T 为 G 的所有阶小于等于 2 的元素的集合. 如果 S 为空集, 则 $|S|=0$; 如果 S 非空, 则对任意的 $x\in S$, 有 $\operatorname{ord}x^{-1}=\operatorname{ord}x>2$, 所以 $x^{-1}\in S$ 且 $x^{-1}\neq x$, 由此得 $|S|$ 必为偶数. 因为已知 G 的阶为偶数, 所以 G 中阶小于等于 2 的元素的个数 $|T|$ 为偶数. 由于 G 中有且仅有一个阶为 1 的元素, 即 1, 所以 $|T|\neq 0$, 从而 $|T|\geqslant 2$ 且 T 中除 1 外其余元素的阶都是 2. 因此 G 必含有阶为 2 的元素.

(2) 若 G 无 n 阶元, 则结论成立. 若 G 有 n 阶元 g, 设 A 是 G 中所有 n 阶元构成的集合, 则对 $\forall x\in A$, 由定理 0.2(2)有 $\operatorname{ord}a^{-1}=\operatorname{ord}a=n$ 且 $a\neq a^{-1}$, 故 $a^{-1}\in A$. 又因为 $n>2$, 所以 $1\notin A$. 因此 A 中元素都成对出现, 故 $|A|$ 必是偶数.

□

命题 0.4

设 G 为有限交换群,$|G|=n$. 证明: 对 n 的任一素因子 p,G 必有阶为 p 的元素.

♠

证明 对 n 应用数学归纳法. 首先, 当 $n=2$ 时, 结论显然成立. 假设结论对所有阶小于 n 的交换群成立. 考察阶为 n 的交换群 G, 设 p 为 n 的任一素因子. 任取 $a\in G,a\neq e$, 设 $\operatorname{ord}a=r$.

(a) 如果 $r=pk$, 则由定理 0.2(4)知 $\operatorname{ord}a^k=\dfrac{r}{(r,k)}=p$, 结论成立.

(b) 如果 $p\nmid r$, 令 $H=\langle a\rangle$, 则由命题**????**知 H 为 G 的正规子群, 且商群 G/H 为交换群. 而 $|G/H|=\dfrac{n}{r}<n$, 且因 $p\nmid r$, 所以 $p\mid\left(\dfrac{n}{r}\right)$. 从而由归纳假设知, 存在 $bH\in G/H$, 使 $\operatorname{ord}bH=p$, 则 $b^p\in H$. 于是 $b^{pr}=e$. 由于 $p\nmid r$, 所以 $(bH)^r\neq H$, 即 $b^r\notin H$, 于是 $b^r\neq e$. 而 $(b^r)^p=e$, 所以 $\operatorname{ord}b^r=p$.

从而由归纳法原理知结论成立.

□

命题 0.5

设 G 是 n 阶群且其不同的子群有不同的阶. 试证:

(1) G 的任何子群都是正规子群;

(2) G 的子群与商群的不同子群也有不同的阶;

(3) G 是循环群.

♠

证明

(1) 设 H 为 G 的子群, $g \in G$. 对 $\forall h_1, h_2 \in H$, 有

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

故 gHg^{-1} 是 G 的子群. 又由命题**??**知 gHg^{-1} 与 H 有相同的阶. 因此由条件知 $gHg^{-1} = H$, 故 H 是正规子群.

(2) 设 H_1, H_2 是 G 的子群 H 的子群, 自然也是 G 的子群, 于是由条件知 $H_1 = H_2$ 当且仅当 $|H_1| = |H_2|$.

设 $\overline{H_1}, \overline{H_2}$ 是商群 G/H 的子群. 记 π 为 G 到商群 G/H 上的自然同态,G 中包含 H 的子群的集合为 Σ,G/H 的子群的集合为 Γ, 由推论**????**知有 G 的子群 $H_1 \supseteq H, H_2 \supseteq H$ 使得

$$\overline{H_1} = \pi(H_1) = H_1/H, \quad \overline{H_2} = \pi(H_2) = H_2/H.$$

因为 π 是 $\Sigma \to \Gamma$ 的双射, 所以 $\overline{H_1} = \overline{H_2}$ 当且仅当 $H_1 = H_2$. 而 $H_1 = H_2$ 当且仅当 $|H_1| = |H_2|$. 注意

$$|H_i| = [H_i : H]|H| = |\overline{H_i}||H|, \quad i = 1, 2.$$

于是 $\overline{H_1} = \overline{H_2}$ 当且仅当 $|\overline{H_1}| = |\overline{H_2}|$.

(3) 设 $|G| = p_1p_2\cdots p_s$, 其中 $p_i(1 \leqslant i \leqslant s)$ 是素数.

对 s 作归纳证明 G 是循环群. 若 $s = 0$, 则 $|G| = 1$, 显然 G 是循环群. 若 $s = 1$, $|G| = p_1$ 是素数, 由命题 0.2知 G 是循环群. 假定 $s-1$ 时结论成立. 以 e 表示 G 的幺元, 取 $a_1 \in G, a_1 \neq e$. 若 a_1 的阶为 n, 则 G 是循环群. 不妨设 a_1 的阶为 $p_sp_{s-1}\cdots p_k \neq n$, 于是 $a = a_1^{p_{s-1}\cdots p_k}$ 的阶为 p_s. 由结论 (1), $\langle a \rangle$ 是 G 的正规子群. 由结论 (2), 商群 $G/\langle a \rangle$ 的不同子群有不同的阶, 由推论**??**知 $G/\langle a \rangle$ 的阶为 $n_1 = p_1p_2\cdots p_{s-1}$. 由归纳假设, $G/\langle a \rangle$ 是循环群. 于是存在 $b \in G$ 使得 $G/\langle a \rangle$ 的元素为 $\langle a \rangle, b\langle a \rangle, \cdots, b^{n_1-1}\langle a \rangle$. 从而由 $(b\langle a \rangle)^{n_1} = \langle a \rangle$ 知对 $0 \leqslant k < p_s$, 有 $k_0(0 \leqslant k_0 < p_s)$ 使得

$$(ba^k)^{n_1} = a^{k_0}.$$

下面证明 $b\langle a \rangle$ 中有元素 c 使得 $c^{n_1} \neq e$. 若 $b^{n_1} \neq e$, 则可取 $c = b$. 故设 $b^{n_1} = e$. 注意 $G/\langle a \rangle$ 的阶为 n_1, 于是当 $0 < r < n_1$ 时, $b^r \neq e, (ba)^r \neq e$. 如果 $(ba)^{n_1} = e$, 则 $\langle b \rangle$ 与 $\langle ba \rangle$ 均为 n_1 阶群, 因而由条件知 $\langle b \rangle = \langle ba \rangle$, 于是有 $ba = b^m, 0 < m < n_1$. 由于 $ba \in b\langle a \rangle, b^m \in b^m\langle a \rangle$, 而 $m \neq 1$ 时, 由定理**????**知 $b\langle a \rangle \cap b^m\langle a \rangle = \varnothing$, 于是 $m = 1$, 即 $ba = b$, 从而 $a = e$, 这就得到矛盾. 由此可知 $(ba)^{n_1} \neq e$. 取 $c = ba$. 由 $c \in b\langle a \rangle$, 知 $b\langle a \rangle = c\langle a \rangle$, 于是 $G/\langle a \rangle = \langle c\langle a \rangle \rangle$. 因为 $G/\langle a \rangle$ 的阶为 n_1, 所以 $(c\langle a \rangle)^{n_1} = c^{n_1}\langle a \rangle = \langle a \rangle$. 因而 $c^{n_1} \in \langle a \rangle$. 注意 $c^{n_1} \neq e$, 于是

$$c^{n_1} = a^m \neq e, \quad 1 \leqslant m < p_s.$$

因为 p_s 是素数, 所以有 $(m, p_s) = 1$. 进而 $a \in \langle c \rangle, \langle a \rangle \subset \langle c \rangle$. 于是有

$$\langle c \rangle / \langle a \rangle = G/\langle a \rangle.$$

因此 $G = \langle c \rangle$ 为循环群.

□

定理 0.5

设 G 是一个 m 阶群, 则 G 是循环群的充要条件是对 m 的每个因数 m_1 存在唯一的 m_1 阶子群.

证明 **必要性**: 设 $G = \langle a \rangle$. 从定理 0.1知 G 的阶 m 也就是元素 a 的阶. 由 $m_1|m$ 知当 $0 < k < m_1$ 时有 $0 < \dfrac{km}{m_1} < m$, 因而 $(a^{\frac{m}{m_1}})^k \neq 1$, 但 $(a^{\frac{m}{m_1}})^{m_1} = 1$, 故 $\langle a^{\frac{m}{m_1}} \rangle$ 是 G 的 m_1 阶子群.

下面证 m_1 阶子群的唯一性. 设 G_1 是 G 中的 m_1 阶子群, 由定理 0.3知 $G_1 = \langle a^k \rangle$, 其中,$k \geqslant 0$, 并且当 $a^{m'} \in G_1$ 时,$k|m'$. 由 $a^m = 1 \in G_1$ 知 $k|m$, 若 $0 < n < \dfrac{m}{k}$, 则 $0 < kn < m$, 从而 $(a^k)^n = a^{kn} \neq 1$. 另外 $(a^k)^{\frac{m}{k}} = 1$, 故 G_1 的阶为 $\dfrac{m}{k} = m_1$, 因而 $k = \dfrac{m}{m_1}$, 即 $G_1 = \langle a^{\frac{m}{m_1}} \rangle$.

充分性: 设 G_1, G_2 是 G 的两个不同子群, 则由 Lagrange 定理知 $[G_1 : 1], [G_2 : 1]$ 都是 m 的因数. 若 $[G_1 : 1] = [G_2 : 1]$, 则由条件知 $G_1 = G_2$ 矛盾! 故 $[G_1 : 1] \neq [G_2 : 1]$. 因此 G 的不同的子群有不同的阶. 于是由命题 0.5(3)知 G 必是循环群.

□