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

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

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 $\forall n_1, n_2 \in \mathbf{Z}$, 有 $a^{n_1}a^{-n_2} \in G$. 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.

推论 0.1

有限群 G 的任一元素 a 的阶是 G 的阶的因子, 即 $\operatorname{ord} a \mid [G:1]$. 进一步, 若 $G = \langle a \rangle$, 则 $\operatorname{ord} a = [G:1]$, 并且 $G = \langle a \rangle = \{1, a, \cdots, a^{\operatorname{ord} a - 1}\}$.

♡

证明 令 $\langle a \rangle = \{a^n | n \in \mathbf{Z}\}$, 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 $n \in \mathbf{Z}$ 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 $\forall r_1, r_2 \in \mathbf{N}$, 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.

若 $G = \langle a \rangle, \operatorname{ord} a = d$, 则由上述证明知 $G = \langle a \rangle = \{1, a, \cdots, a^{d-1}\}$ 是 d 阶群, 故 $d = [G:1]$.

□

定理 0.1

循环群的任何子群也是循环群.

♡

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

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

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.

□

推论 0.2

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

$$d = nu + rv.$$

于是 $a^d = a^{nu+rv} = a^{rv} \in \langle a^r \rangle$. 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 $\langle a^r \rangle = \langle a^d \rangle$.

□

推论 0.3

设 $G = \langle a \rangle$ 为循环群,

(1) 如果 $|G| = \infty$, 则 G 的全部子群为 $\{\langle a^d \rangle \mid d = 0, 1, 2, \cdots\}$, 并且 $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle, \forall d_1, d_2 \in \mathbb{N}_0$ 且 $d_1 \neq d_2$;

(2) 如果 $|G| = n$, 则 G 的全部子群为 $\{\langle a^d \rangle \mid d$ 为 n 的正因子 $\}$, 并且 $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle, \forall d_1, d_2$ 为 n 的正因子.

♡

证明 设 e 为 G 的幺元,G 的所有子群构成的集合为 S. 由定理 0.1知, 循环群的任一子群必形如 $\langle a^r\rangle (r\in\mathbb{Z})$. 显然, 有

$$\langle a^r\rangle = \langle a^{-r}\rangle.$$

因此, 循环群的任一子群必形如 $\langle a^r\rangle (r\in\mathbb{Z}, r\geqslant 0)$. 此即

$$S=\{\langle a^r\rangle \mid r\in\mathbb{Z}, r\geqslant 0\}=\{\langle a^r\rangle \mid r=0,1,2,\cdots\}. \tag{1}$$

(1) 如果 $|G|=\infty$, 由(1)式知

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

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 $a^r\notin\langle a^0\rangle=\langle e\rangle=\{e\}$, 所以有

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

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

(2) 如果 $|G|=n$, 对任意的正整数 r, 存在 n 的正因子 $d=(n,r)$, 由推论 0.2可知

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

故再由(1)式知 $S\subseteq\{\langle a^d\rangle \mid d为n的正因子\}$. 又显然有 $S\supseteq\{\langle a^d\rangle \mid d为n的正因子\}$, 故

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

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 的正因子.

□

推论 0.4

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

(2) 整数加法群 $\mathbf{Z}$ 的任何子群必为 $m\mathbf{Z}(m\geqslant 0$且$m\in\mathbf{Z})$.

♡

证明

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

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

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

(2) 事实上, $\mathbf{Z}=\langle 1\rangle$. 设 G_1 为 $\mathbf{Z}$ 的子群. 于是由定理 0.1有 $m\geqslant 0$且$m\in\mathbf{Z}$, 使得 $G_1=\langle m\rangle=m\mathbf{Z}$.

□

命题 0.1 (素数阶群必为循环群)

设 G 是一个群, 且 $|G|=p$ 为一个素数, 则

(1) G 必是循环群, 并且 $\forall a\in G$ 且 $a\neq e$ 有 $G=\langle a\rangle$.

(2) G 只有平凡子群.

♠

证明

(1) 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.

(2) 由结论 (1) 知 G 是循环群. 又循环群的任何子群也是循环群, 故 G 的任意子群 H 也是循环群, 若 $H\neq\{e\}, G$,

则可设 $H=\langle a\rangle, a\in G\setminus\{e\}$, 再由结论 (1) 知 $G=\langle a\rangle=H$ 矛盾! 故 $H=\{e\}$或G.

□

命题 0.2

设 $m>0$, 则有

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

♠

证明 由推论 0.4(1)知 $m\mathbf{Z}$ 为 $\mathbf{Z}$ 的子群.

□

定理 0.2

设 $G=\langle a\rangle$ 是一个循环群.

(1) 若 G 是无限阶的, 则 G 与整数加法群 $\mathbf{Z}$ 同构.

(2) 若 G 的阶 m 有限, 则 G 与加法群 $\mathbf{Z}_m$ 同构.

进而两个循环群同构当且仅当它们的阶相同.

♡

证明 作 $\mathbf{Z}$ 到 G 上的映射 $\varphi:\varphi(n)=a^n(n\in\mathbf{Z})$. 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 $\mathbf{Z}$ 到 G 上的同态映射, 故由群的同态基本定理知 $G\cong\mathbf{Z}/\ker\varphi$ 且 $\ker\varphi\lhd\mathbf{Z}$. 由推论 0.4(2)知存在 $m\geqslant 0$且$m\in\mathbf{Z}$, 使得 $\ker\varphi=m\mathbf{Z}$.

若 $m>0$, 则由命题 0.2知, 此时 $G\cong\mathbf{Z}/\ker\varphi=\mathbf{Z}/m\mathbf{Z}=\mathbf{Z}_m$ 且 $|G|=|\mathbf{Z}_m|=m$.

若 $m=0$, 则 $G\cong\mathbf{Z}$ 同构, 此时 G 的阶为无限.

□

推论 0.5

无限循环群的非平凡子群仍为无限循环群.

♡

证明 设 G 为无限循环群, 则由定理 0.2知 $G\cong\mathbf{Z}$. 又由推论 0.4(2)知 $\mathbf{Z}$ 的非平凡子群为 $m\mathbf{Z}(m\neq 0,1)$ 为无限循环群. 故 G 的非平凡子群也为无限循环群.

□

定理 0.3

设 G 是 m 阶循环群,m_1 是 m 的一个因数, 则存在唯一的 m_1 阶子群.

♡

证明 设 $G=\langle a\rangle$. 从推论 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 $0<km/m_1<m$, 因而 $(a^{m/m_1})^k\neq 1$, 但 $(a^{m/m_1})^{m_1}=1$, 故 $\langle a^{m/m_1}\rangle$ 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 0.1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 $0<n<m/k$, 则 $0<kn<m$, 从而 $(a^k)^n=a^{kn}\neq 1$. 另外 $(a^k)^{m/k}=1$, 故 G_1 的阶为 $m/k=m_1$, 因而 $k=m/m_1$, 即 $G_1=\langle a^{m/m_1}\rangle$.

□

命题 0.3

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 0.1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, 由推论**??**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 0.4

一个 m 阶群 G 对 m 的每个因数 m_1 存在唯一的 m_1 阶子群, 则群 G 必是循环群. ♡

证明 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 0.3(3)知 G 必是循环群.

□

定理 0.5

设 G 是一个群,$a, b \in G$. 它们的阶分别为 m, n, 则有下列结论:

(1) a^k 的阶为 $\dfrac{m}{(m,k)}$,(m, k) 是 m 与 k 的最大公因数;

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

♡

证明

(1) 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 $\frac{m}{(m,k)}|q$. 又 $(a^k)^{m/(m,k)} = (a^m)^{k/(m,k)} = 1$, 即得 $q|(\frac{m}{(m,k)})$, 因而

$$q = \frac{m}{(m,k)}.$$

(2) 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 $m_1 = [m, n]$.

□

推论 0.6

(1) 若 a 为 m 阶元素, 则 a^k 为 m 阶元素的充要条件是 $(m, k) = 1$;

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

♡

证明

(1) 这是定理 0.5的自然推论.

(2) 设 m_1 是 $\langle a\rangle \cap \langle b\rangle$ 的阶, 由推论 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 0.5知 ab 的阶为 $[m, n] = mn$.

□