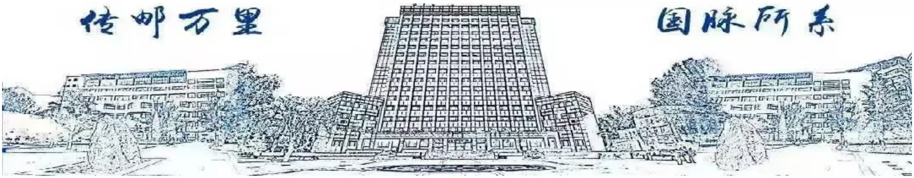
信息安全数学基础

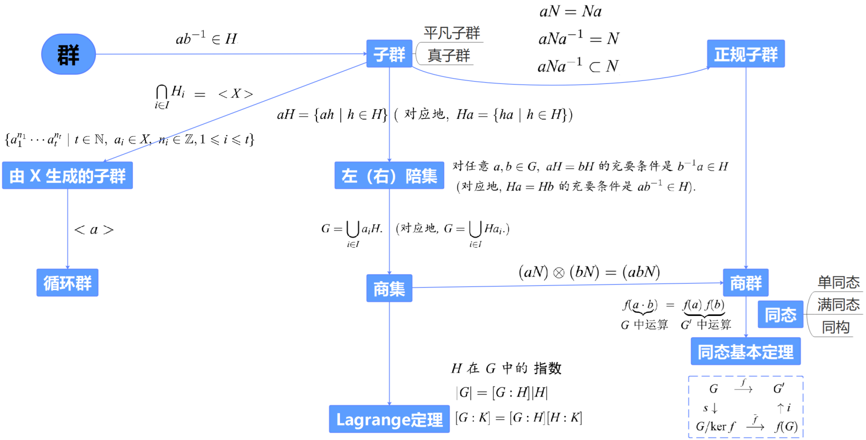
—— 群 (3)

信数课题组

北京邮电大学



上次课回顾



群
$ab^{-1} \in H$
子群
平凡子群
真子群
$aN = Na$
$aNa^{-1} = N$
$aNa^{-1} \subset N$
正规子群
$\bigcap_{i \in I} H_i = \ < X >$
$\{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbb{N},\ a_i \in X,\ n_i \in \mathbb{Z}, 1 \leqslant i \leqslant t\}$
由 X 生成的子群
$aH = \{ah \mid h \in H\}$ (对应地，$Ha = \{ha \mid h \in H\}$)
左（右）陪集
对任意 $a, b \in G$，$aH = bH$ 的充要条件是 $b^{-1}a \in H$
(对应地，$Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).
$< a >$
循环群
$G = \bigcup_{i \in I} a_i H.$ (对应地，$G = \bigcup_{i \in I} Ha_i$.)
$(aN) \otimes (bN) = (abN)$
商集
商群
单同态
满同态
同构
同态
$\underbrace{f(a \cdot b)}_{G\ 中运算} = \underbrace{f(a)\,f(b)}_{G'\ 中运算}$
同态基本定理
H 在 G 中的 指数
$|G| = [G : H]|H|$
$[G : K] = [G : H][H : K]$
Lagrange定理
$G \xrightarrow{f} G'$
$s \downarrow$
$\uparrow i$
$G/\ker f \xrightarrow{\bar{f}} f(G)$

目录

首先讨论加群 $\mathbb{Z}$ 及其子群.

定理 6.4.1

加群 $\mathbb{Z}$ 的每个子群 H 是循环群. 并且, 有

$$H = < 0 > \quad \text{或} \quad H = < m > = m\mathbb{Z},$$

其中 m 是 H 中的最小正整数. 如果 $H \neq < 0 >$, 则 H 是无限的.

首先讨论加群 $\mathbb{Z}$ 及其子群.

定理 6.4.1

加群 $\mathbb{Z}$ 的每个子群 H 是循环群. 并且, 有

$$H =< 0 > \text{ 或 } H =< m >= m\mathbb{Z},$$

其中 m 是 H 中的最小正整数. 如果 $H \neq < 0 >$, 则 H 是无限的.

证：(i) 如果 H 是零子群 $\{0\}$, 只有一个单位元, 则是循环群 $H =< 0 >$.

(ii) 如果 H 是非零子群, 则存在非零整数 $a \in H$. 因为 H 是子群, 所以 $-a \in H$. 这说明 H 中有正整数. 设 H 中的最小正整数为 m, 则一定有 $H =< m >= m\mathbb{Z}$.

事实上, 对任意的 $a \in H$, 根据欧几里德除法, 存在正整数 q, r 使得 $a = qm + r,\ 0 \leqslant r < m$. 如果 $r \neq 0$, 则 $r = a + q(-m) \in H$, 这与 m 的最小性矛盾. 因此, $r = 0, a = qm \in m\mathbb{Z}$. 故 $H \subset m\mathbb{Z}$. 但显然有 $m\mathbb{Z} \subset H$. 因此, $H = m\mathbb{Z}$.

例 6.4.1 $\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ 是 $(\mathbb{Z}, +)$ 的子群 (且为正规子群, 因为 $\mathbb{Z}$ 是交换群），而 $3\mathbb{Z} =< 3 >, 4\mathbb{Z} =< 4 >, 6\mathbb{Z} =< 6 >= \{6^0, 6^1, 6^2, 6^3, \cdots\}$.

例 6.4.1 $\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ 是 $(\mathbb{Z}, +)$ 的子群 (且为正规子群, 因为 $\mathbb{Z}$ 是交换群），而 $3\mathbb{Z} =< 3 >, 4\mathbb{Z} =< 4 >, 6\mathbb{Z} =< 6 >= \{6^0, 6^1, 6^2, 6^3, \cdots\}$.

定理 6.4.2

每个无限循环群同构于加群 $\mathbb{Z}$. 每个阶为 m 的有限循环群同构于加群 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

例 6.4.1 $\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ 是 $(\mathbb{Z}, +)$ 的子群 (且为正规子群, 因为 $\mathbb{Z}$ 是交换群）, 而 $3\mathbb{Z} =< 3 >, 4\mathbb{Z} =< 4 >, 6\mathbb{Z} =< 6 >= \{6^0, 6^1, 6^2, 6^3, \cdots\}$.

定理 6.4.2

每个无限循环群同构于加群 $\mathbb{Z}$. 每个阶为 m 的有限循环群同构于加群 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

证：设循环群 $G =< a >= \{a^n \mid n \in \mathbb{Z}\}$. 考虑映射

$$\begin{aligned} f\colon \mathbb{Z} &\to G, \\ n &\mapsto a^n. \end{aligned}$$

则 f 是同态映射, 且为满射. 由群同态基本定理知, 群 G 同构于 $\mathbb{Z}/\ker f$.
根据定理 6.3.3, $\ker f =< 0 >$ 或 $\ker f = m\mathbb{Z}$.
前者对应于无限循环群, 后者对应于 m 阶有限循环群.

例 6.4.1 $\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ 是 $(\mathbb{Z}, +)$ 的子群 (且为正规子群, 因为 $\mathbb{Z}$ 是交换群），而 $3\mathbb{Z} =< 3 >, 4\mathbb{Z} =< 4 >, 6\mathbb{Z} =< 6 >= \{6^0, 6^1, 6^2, 6^3, \cdots\}$.

定理 6.4.2

每个无限循环群同构于加群 $\mathbb{Z}$. 每个阶为 m 的有限循环群同构于加群 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

证：设循环群 $G =< a >= \{a^n \mid n \in \mathbb{Z}\}$. 考虑映射

$$\begin{aligned} f\colon \mathbb{Z} &\to G, \\ n &\mapsto a^n. \end{aligned}$$

则 f 是同态映射, 且为满射. 由群同态基本定理知, 群 G 同构于 $\mathbb{Z}/\mathrm{ker}f$.
根据定理 6.3.3, $\mathrm{ker}f =< 0 >$ 或 $\mathrm{ker}f = m\mathbb{Z}$.
前者对应于无限循环群, 后者对应于 m 阶有限循环群.

定义 6.4.1

设 G 是群, $a \in G$, 则子群 $< a >$ 的阶称为**元素 a 的阶**, 记为 $\mathrm{ord}(a)$.

定理 6.4.2

设 G 是一个群, $a \in G$,

当 a 是无限阶时, 则

(i) $a^k = e$ 当且仅当 $k = 0$.

(ii) 元素 a^k $(k \in \mathbb{Z})$ 两两不同.

当 a 是有限阶 $m > 0$, 则

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 当且仅当 $m \mid k$.

(v) $a^r = a^k$ 当且仅当 $r \equiv k \mod m$.

(vi) 元素 a^k $(k \in \mathbb{Z}/m\mathbb{Z})$ 两两不同.

(vii) $< a >= \{a, a^2, \cdots, a^{m-1}, a^m = e\}$.

(viii) 对任意的整数 $1 \leqslant d \leqslant m$, 有 $\mathrm{ord}(a^d) = \frac{m}{(d,m)}$.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\mathrm{ker} f \cong < a >$.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\ker f \cong < a >$.

因为 a 是无限阶等价于 $\ker f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\mathrm{ker}f \cong < a >$.

因为 a 是无限阶等价于 $\mathrm{ker}f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\mathrm{ker}f = m\mathbb{Z}$. 因此, 我们有：

(iii) m 是使得 $a^m = e$ 的最小正整数.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\ker f \cong < a >$.

因为 a 是无限阶等价于 $\ker f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\ker f = m\mathbb{Z}$. 因此, 我们有：

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于 $k \in \ker f$, 等价于 $m \mid k$.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\ker f \cong < a >$.

因为 a 是无限阶等价于 $\ker f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\ker f = m\mathbb{Z}$. 因此, 我们有：

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于 $k \in \ker f$, 等价于 $m \mid k$.

(v) $a^r = a^k$ 等价于 $r - k \in \ker f$, 等价于 $r \equiv k \mod m$.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\mathrm{ker} f \cong < a >$.

因为 a 是无限阶等价于 $\mathrm{ker} f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\mathrm{ker} f = m\mathbb{Z}$. 因此, 我们有:

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于 $k \in \mathrm{ker} f$, 等价于 $m \mid k$.

(v) $a^r = a^k$ 等价于 $r - k \in \mathrm{ker} f$, 等价于 $r \equiv k \mod m$.

(vi) 元素 a^k 对应于 $\mathbb{Z}/\mathrm{ker} f$ 中的不同元素, 两两不同.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\mathrm{ker} f \cong < a >$.

因为 a 是无限阶等价于 $\mathrm{ker} f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\mathrm{ker} f = m\mathbb{Z}$. 因此, 我们有：

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于 $k \in \mathrm{ker} f$, 等价于 $m \mid k$.

(v) $a^r = a^k$ 等价于 $r - k \in \mathrm{ker} f$, 等价于 $r \equiv k \mod m$.

(vi) 元素 a^k 对应于 $\mathbb{Z}/\mathrm{ker} f$ 中的不同元素, 两两不同.

(vii) $< a >= \{a, a^2, \cdots, a^{m-1}, a^m = e\}$ 与 $\mathbb{Z}/\mathrm{ker} f$ 中的最小正剩余系相对应.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射. 根据群同态基本定理, 我们有 $\mathbb{Z}/\ker f \cong <a>$.

因为 a 是无限阶等价于 $\ker f = 0$, 后者说明 f 是一对一的. 因此, (i) 和 (ii) 成立.

如果 a 是有限阶 m, 则 $\ker f = m\mathbb{Z}$. 因此, 我们有：

(iii) m 是使得 $a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于 $k \in \ker f$, 等价于 $m \mid k$.

(v) $a^r = a^k$ 等价于 $r - k \in \ker f$, 等价于 $r \equiv k \mod m$.

(vi) 元素 a^k 对应于 $\mathbb{Z}/\ker f$ 中的不同元素, 两两不同.

(vii) $<a> = \{a, a^2, \cdots, a^{m-1}, a^m = e\}$ 与 $\mathbb{Z}/\ker f$ 中的最小正剩余系相对应.

(viii) $(a^d)^k = e$ 等价于 $dk \in \ker f$, 等价于 $m \mid dk$, 等价于 $\frac{m}{(d,m)} \mid \frac{d}{(d,m)}k$, 等价于 $\frac{m}{(d,m)} \mid k$. 因此, $\mathrm{ord}(a^d) = \frac{m}{(d,m)}$.

定理 6.4.4

循环群的子群是循环群.

定理 6.4.4

循环群的子群是循环群.

证：考虑加群 $\mathbb{Z}$ 到循环群 $G =< a >$ 的映射

$$f : n \mapsto a^n.$$

f 是同态映射.

根据定理 6.3.3, 对于 G 的子群 H, 我们有 $K = f^{-1}(H)$ 是 $\mathbb{Z}$ 的子群. 根据定理 6.4.1, K 是循环群, 所以 $H = f(K)$ 是循环群.

定理 6.4.4

循环群的子群是循环群.

证：考虑加群 $\mathbb{Z}$ 到循环群 $G =< a >$ 的映射

$$f : n \mapsto a^n.$$

f 是同态映射.

根据定理 6.3.3, 对于 G 的子群 H, 我们有 $K = f^{-1}(H)$ 是 $\mathbb{Z}$ 的子群. 根据定理 6.4.1, K 是循环群, 所以 $H = f(K)$ 是循环群.

例 6.4.2 若 G 是循环群, G 与 $\overline{G}$ 同态, 则 $\overline{G}$ 是循环群.

证：设 $G =< a >$, G 与 $\overline{G}$ 同态, 所以存在满同态映射 g.

$$g(a^2) = g(a \cdot a) = g(a) * g(a) = g(a)^2 \in \overline{G}.$$

进一步有, 任意 $g(b) = g(a^m) = (g(a))^m$. 所以 $\overline{G}$ 是循环群, 生成元 $g(a)$.

例 6.4.3 找到模 12 的剩余类加群的所有子群.

解：12 的因子有 1, 2, 3, 4 , 6, 12.

模 12 的剩余类加群 $G = \{[0], [1], \cdots, [11]\}$ 是循环群, 生成元为 [1].

根据循环群的所有子群都是循环群知：

1 阶子群 $([0]) = \{[0]\}$,

2 阶子群 $([6]) = \{[6], [0]\}$,

3 阶子群 $([4]) = ([8]) = \{[4], [8], [0]\}$,

4 阶子群 $([3]) = ([9]) = \{[3], [6], [9], [0]\}$,

6 阶子群 $([2]) = ([10]) = \{[2], [4], [6], [8], [10], [0]\}$,

12 阶子群 G.

定理 6.4.5

设 $G=<a>$ 是循环群.

(i) 如果 G 是无限的, 则 G 的生成元为 a 和 a^{-1}.

(ii) 如果 G 是有限阶 m, 则 a^k 是生成元当且仅当 $(k,m)=1$.

定理 6.4.5

设 $G=<a>$ 是循环群.

(i) 如果 G 是无限的, 则 G 的生成元为 a 和 a^{-1}.

(ii) 如果 G 是有限阶 m, 则 a^k 是生成元当且仅当 $(k,m)=1$.

证：考虑加群 $\mathbb{Z}$ 到群 G 的映射 $f: n \mapsto a^n$. f 是同态映射.

根据群同态基本定理, 我们有 $\mathbb{Z}/\ker f \cong G$.

因为 G 中生成元对应于 $\mathbb{Z}/\ker f$ 中生成元, 故有

(i) 当 G 是无限阶, 即 $\ker f=0$ 时, $\mathbb{Z}/\ker f$ 的生成元是 1 和 -1. 这时, G 的生成元是 a 和 a^{-1}.

(ii) 当 G 是有限阶, 即 $\ker f=m\mathbb{Z}$, $m>0$ 时, $\mathbb{Z}/\ker f$ 的生成元是 k, 其中 $(k,m)=1$. 这时, G 的生成元是 $a^k, (k,m)=1$.

因此, 结论成立.

定理 6.4.6

设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

定理 6.4.6

设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

证：因为

$$a^{\mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)} = a^{\mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)} \cdot \left(b^{\mathrm{ord}(b)}\right)^{\mathrm{ord}(a \cdot b)} = \left((a \cdot b)^{\mathrm{ord}(a \cdot b)}\right)^{\mathrm{ord}(b)} = 1,$$

根据定理 6.4.3 (iv), 我们有 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)$.

因为 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 所以 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b)$.

定理 6.4.6

设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

证：因为

$$a^{\mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)} = a^{\mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)} \cdot \left(b^{\mathrm{ord}(b)}\right)^{\mathrm{ord}(a \cdot b)} = \left((a \cdot b)^{\mathrm{ord}(a \cdot b)}\right)^{\mathrm{ord}(b)} = 1,$$

根据定理 6.4.3 (iv), 我们有 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)$.

因为 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 所以 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b)$.

同理, $\mathrm{ord}(b) \mid \mathrm{ord}(a \cdot b)$.

定理 6.4.6

设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

证：因为

$$a^{\mathrm{ord}(a\cdot b)\cdot \mathrm{ord}(b)} = a^{\mathrm{ord}(a\cdot b)\cdot \mathrm{ord}(b)} \cdot \left(b^{\mathrm{ord}(b)}\right)^{\mathrm{ord}(a\cdot b)} = \left((a\cdot b)^{\mathrm{ord}(a\cdot b)}\right)^{\mathrm{ord}(b)} = 1,$$

根据定理 6.4.3 (iv), 我们有 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b) \cdot \mathrm{ord}(b)$.

因为 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 所以 $\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b)$.

同理, $\mathrm{ord}(b) \mid \mathrm{ord}(a \cdot b)$.

再由 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 我们得到 $\mathrm{ord}(a) \cdot \mathrm{ord}(b) \mid \mathrm{ord}(a \cdot b)$.

定理 6.4.6

设 G 是有限交换群. 对任意元素 $a, b \in G$, 若 $\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

证：因为

$$a^{\mathrm{ord}(a\cdot b)\cdot\mathrm{ord}(b)} = a^{\mathrm{ord}(a\cdot b)\cdot\mathrm{ord}(b)} \cdot \left(b^{\mathrm{ord}(b)}\right)^{\mathrm{ord}(a\cdot b)} = \left((a\cdot b)^{\mathrm{ord}(a\cdot b)}\right)^{\mathrm{ord}(b)} = 1,$$

根据定理 6.4.3 (iv), 我们有 $\mathrm{ord}(a) \mid \mathrm{ord}(a\cdot b) \cdot \mathrm{ord}(b)$.

因为 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 所以 $\mathrm{ord}(a) \mid \mathrm{ord}(a\cdot b)$.

同理, $\mathrm{ord}(b) \mid \mathrm{ord}(a\cdot b)$.

再由 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 我们得到 $\mathrm{ord}(a)\cdot\mathrm{ord}(b) \mid \mathrm{ord}(a\cdot b)$.

此外, 显然有 $\mathrm{ord}(a\cdot b) \mid \mathrm{ord}(a)\cdot\mathrm{ord}(b)$. 事实上,
由 $(ab)^{\mathrm{ord}(a)\mathrm{ord}(b)} = a^{\mathrm{ord}(a)\mathrm{ord}(b)} b^{\mathrm{ord}(a)\mathrm{ord}(b)} = e$ 及阶的定义立得.

故 $\mathrm{ord}(a\cdot b) = \mathrm{ord}(a)\cdot\mathrm{ord}(b)$.

例 6.4.4 设 $(G,+)$ 是 6 阶循环群, a,b 分别是 2, 3 阶的元素, 则 $a+b$ 是 6 阶的, 恰是 G 的生成元.

具体举例如下：$\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$, 生成元为 $[1]$, $(\mathbb{Z}_6,\oplus_6)$ 是循环群. 其中, $[2]$ 是 3 阶, $[3]$ 是 2 阶, 则 $[2]\oplus_6[3]=[5]$ 是 $2*3=6$ 阶元素, 是生成元.

定义 6.5.1

设 S 是一个非空集合, G 是 S 到自身的所有一一对应的映射组成的集合, 则对于映射的复合运算, G 构成一个群, 叫做 **对称群**.

定义 6.5.1

设 S 是一个非空集合, G 是 S 到自身的所有一一对应的映射组成的集合, 则对于映射的复合运算, G 构成一个群, 叫做 **对称群**.

注：单位元：恒等映射.

G 中的元素叫做 S 的一个**置换**.

当 S 是 n 元有限集时, G 叫做 n **元对称群**, 记作 S_n.

设 $S=\{1,2,\cdots,n-1,n\}$, σ 是 S 上的一个置换, 即 σ 是 S 到自身的一一对应的映射.

$$\begin{aligned}\sigma: \quad S &\longrightarrow S\\ k &\longmapsto \sigma(k)=i_k\end{aligned}$$

将 σ 表示成:

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n)\end{pmatrix}.$$

例 6.5.1 对 $S=\{1,2,3,4,5,6\}$, 有

置换 $\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 1 & 2 & 4 \end{pmatrix}$.

置换 $\tau=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$.

单位置换 $I=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$.

例 6.5.2 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$，$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$.

计算 $\sigma\tau, \tau\sigma, \sigma^{-1}$.

例 6.5.2 设 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}$, $\tau=\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}$.

计算 $\sigma\tau,\tau\sigma,\sigma^{-1}$.

解:

$$\begin{aligned}
\sigma\cdot\tau&=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}\\
&=\begin{pmatrix}5&6&4&2&3&1\\1&3&2&5&4&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}\\
&=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&5&4&6\end{pmatrix}.\\
\tau\cdot\sigma&=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&5&4\end{pmatrix}.\\
\sigma^{-1}&=\begin{pmatrix}1&2&3&4&5&6\\5&4&6&3&2&1\end{pmatrix}.
\end{aligned}$$

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，且 $|S_n| = n!$.

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群, 且 $|S_n| = n!$.

证：因为一一对应的映射的乘积仍是一一对应的, 且该乘积满足结合律, 所以置换的乘法满足结合律.

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，且 $|S_n| = n!$.

证：因为一一对应的映射的乘积仍是一一对应的，且该乘积满足结合律，所以置换的乘法满足结合律.

又 n 元恒等置换 $e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$ 是单位元.

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，且 $|S_n| = n!$.

证：因为一一对应的映射的乘积仍是一一对应的，且该乘积满足结合律，所以置换的乘法满足结合律.

又 n 元恒等置换 $e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$ 是单位元. 置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}$ 有逆元 $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$.

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群, 且 $|S_n| = n!$.

证：因为一一对应的映射的乘积仍是一一对应的, 且该乘积满足结合律, 所以置换的乘法满足结合律.

又 n 元恒等置换 $e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$ 是单位元. 置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}$ 有逆元 $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$.

因此, S_n 对置换的乘法构成一个群.

定理 6.5.1

n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，且 $|S_n| = n!$.

证：因为一一对应的映射的乘积仍是一一对应的，且该乘积满足结合律，所以置换的乘法满足结合律.

又 n 元恒等置换 $e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$ 是单位元. 置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}$ 有逆元 $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$.

因此，S_n 对置换的乘法构成一个群.

因为 $(1, 2, \cdots, n-1, n)$ 在置换 σ 下的像 $(\sigma(1), \sigma(2), \cdots, \sigma(n-1), \sigma(n))$ 是 $(1, 2, \cdots, n-1, n)$ 的一个排列，这样的排列共有 $n!$ 个，所以 S_n 的阶为 $n!$.

为了更好地研究置换, 先考虑特殊的置换.

定义 6.5.2 (k-轮换)

如果 n 元置换 σ 使得 $\{1, 2, \cdots, n-1, n\}$ 中一部分元素 $\{i_1, i_2, \cdots, i_{k-1}, i_k\}$ 满足 $\sigma(i_1) = i_2, \cdots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$, 又使得其他元素保持不变, 则称该置换为 **$k$-轮换**, 简称轮换, 记作 $\sigma = (i_1, i_2, \cdots, i_{k-1}, i_k)$. k 称为轮换的长度.

为了更好地研究置换, 先考虑特殊的置换.

定义 6.5.2 (k-轮换)

如果 n 元置换 σ 使得 $\{1, 2, \cdots, n-1, n\}$ 中一部分元素 $\{i_1, i_2, \cdots, i_{k-1}, i_k\}$ 满足 $\sigma(i_1) = i_2, \cdots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$, 又使得其他元素保持不变, 则称该置换为 **$k$-轮换**, 简称轮换, 记作 $\sigma = (i_1, i_2, \cdots, i_{k-1}, i_k)$. k 称为轮换的长度.

例 6.5.3 (1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix} = (2, 5, 4)$.

(2) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (1, 6, 3)$.

定义 6.5.3

对于定义 6.5.2 中,

$k=1$ 时, 1-轮换为恒等置换;

$k=2$ 时, 2-轮换 (i_1, i_2) 叫作**对换**.

任意两个轮换 $\sigma=(i_1, i_2, \cdots, i_{k-1}, i_k)$, $\tau=(j_1, j_2, \cdots, j_{l-1}, j_l)$, 如果这 $k+l$ 个元素都不同, 则称 σ 和 τ **不相交**.

定义 6.5.3

对于定义 6.5.2 中,

$k=1$ 时, 1-轮换为恒等置换;

$k=2$ 时, 2-轮换 (i_1, i_2) 叫作**对换**.

任意两个轮换 $\sigma=(i_1, i_2, \cdots, i_{k-1}, i_k)$, $\tau=(j_1, j_2, \cdots, j_{l-1}, j_l)$, 如果这 $k+l$ 个元素都不同, 则称 σ 和 τ **不相交**.

例 6.5.4 $\sigma=(2,5,4)$ 与 $\tau=(1,6,3)$ 是不相交的 3-轮换.

定义 6.5.3

对于定义 6.5.2 中，

$k=1$ 时，1-轮换为恒等置换；

$k=2$ 时，2-轮换 (i_1, i_2) 叫作**对换**.

任意两个轮换 $\sigma=(i_1, i_2, \cdots, i_{k-1}, i_k)$, $\tau=(j_1, j_2, \cdots, j_{l-1}, j_l)$, 如果这 $k+l$ 个元素都不同，则称 σ 和 τ **不相交**.

例 6.5.4 $\sigma=(2,5,4)$ 与 $\tau=(1,6,3)$ 是不相交的 3-轮换.

定理 6.5.2

任意一个置换都可以表示为一些不相交轮换的乘积. 在不考虑乘积次序的情况下，该表达式是唯一的.

定义 6.5.3

对于定义 6.5.2 中,

$k=1$ 时, 1-轮换为恒等置换;

$k=2$ 时, 2-轮换 (i_1, i_2) 叫作**对换**.

任意两个轮换 $\sigma=(i_1, i_2, \cdots, i_{k-1}, i_k)$, $\tau=(j_1, j_2, \cdots, j_{l-1}, j_l)$, 如果这 $k+l$ 个元素都不同, 则称 σ 和 τ **不相交**.

例 6.5.4 $\sigma=(2,5,4)$ 与 $\tau=(1,6,3)$ 是不相交的 3-轮换.

定理 6.5.2

任意一个置换都可以表示为一些不相交轮换的乘积. 在不考虑乘积次序的情况下, 该表达式是唯一的.

例 6.5.5 $\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix}=(2,5,4)(1,6,3)$.

对于轮换来说, 可以写成对换.

例 6.5.6 $(2,5,4)=(2,4)(2,5),\ (1,6,3)=(1,3)(1,6).$

对于轮换来说, 可以写成对换.

例 6.5.6 $(2,5,4)=(2,4)(2,5)$, $(1,6,3)=(1,3)(1,6)$.

一般地, 对于轮换 $\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)$, 有

$$\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)=(i_1,i_k)(i_1,i_{k-1})\cdots(i_1,i_3)(i_1,i_2).$$

对于轮换来说, 可以写成对换.

例 6.5.6 $(2,5,4)=(2,4)(2,5)$, $(1,6,3)=(1,3)(1,6)$.

一般地, 对于轮换 $\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)$, 有

$$\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)=(i_1,i_k)(i_1,i_{k-1})\cdots(i_1,i_3)(i_1,i_2).$$

定义 6.5.4

对于 n 元排列 $i_1,\cdots,i_k,\cdots,i_l,\cdots,i_n$ 的一对有序元素 (i_k,i_l), 如果 $k<l$ 时, $i_k>i_l$, 则称 (i_k,i_l) 为**逆序**. 排列中逆序的个数叫作该排列的**逆序数**, 记为 $[i_1,\cdots,i_n]$.

对于轮换来说, 可以写成对换.

例 6.5.6 $(2,5,4)=(2,4)(2,5)$, $(1,6,3)=(1,3)(1,6)$.

一般地, 对于轮换 $\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)$, 有

$$\sigma=(i_1,i_2,\cdots,i_{k-1},i_k)=(i_1,i_k)(i_1,i_{k-1})\cdots(i_1,i_3)(i_1,i_2).$$

定义 6.5.4

对于 n 元排列 $i_1,\cdots,i_k,\cdots,i_l,\cdots,i_n$ 的一对有序元素 (i_k,i_l), 如果 $k<l$ 时, $i_k>i_l$, 则称 (i_k,i_l) 为**逆序**. 排列中逆序的个数叫作该排列的**逆序数**, 记为 $[i_1,\cdots,i_n]$.

例 6.5.7 $[1,5,3,2,4,6]=0+0+1+2+1+0=4$.

定理 6.5.3

任意一个置换 σ 都可以表示为一些对换的乘积, 且对换个数的奇偶性与排列的逆序数 $[\sigma(1), \cdots, \sigma(n)]$ 的奇偶性相同.

定理 6.5.3

任意一个置换 σ 都可以表示为一些对换的乘积, 且对换个数的奇偶性与排列的逆序数 $[\sigma(1),\cdots,\sigma(n)]$ 的奇偶性相同.

例 6.5.8 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix} = (2,5,4) = (2,4)(2,5).$

定理 6.5.3

任意一个置换 σ 都可以表示为一些对换的乘积, 且对换个数的奇偶性与排列的逆序数 $[\sigma(1), \cdots, \sigma(n)]$ 的奇偶性相同.

例 6.5.8 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix} = (2,5,4) = (2,4)(2,5).$

定义 6.5.5

如果一个置换 σ 可以表示为偶数个对换的乘积, 则称其为**偶置换**; 如果可以表示为奇数个对换的乘积, 则称其为**奇置换**.

根据定理 6.5.3, 有

$$\begin{array}{rcrcl} & & \text{偶置换} \times \text{偶置换} & = & \text{偶置换} \\ \text{偶置换} \times \text{奇置换} & = & \text{奇置换} \times \text{偶置换} & = & \text{奇置换} \end{array}$$

根据定理 6.5.3, 有

	偶置换 $\times$ 偶置换	$=$ 偶置换
偶置换 $\times$ 奇置换	$=$ 奇置换 $\times$ 偶置换	$=$ 奇置换

记 A_n 为 n 元偶置换全体组成的集合.

根据定理 6.5.3, 有

		偶置换 × 偶置换	=	偶置换
偶置换 × 奇置换	=	奇置换 × 偶置换	=	奇置换

记 A_n 为 n 元偶置换全体组成的集合.

定理 6.5.4

A_n 对置换的乘法构成一个群, 其阶是 $n!/2$.

根据定理 6.5.3, 有

		偶置换 × 偶置换	=	偶置换
偶置换 × 奇置换	=	奇置换 × 偶置换	=	奇置换

记 A_n 为 n 元偶置换全体组成的集合.

定理 6.5.4

A_n 对置换的乘法构成一个群, 其阶是 $n!/2$.

证：封闭性：偶置换与偶置换的乘积是偶置换. 易验证结合律. 单位元 I 恒等置换是偶置换, 偶置换的逆置换是偶置换, 所以 A_n 对置换的乘法构成一个群.

根据定理 6.5.3, 有

		偶置换 × 偶置换	=	偶置换
偶置换 × 奇置换	=	奇置换 × 偶置换	=	奇置换

记 A_n 为 n 元偶置换全体组成的集合.

定理 6.5.4

A_n 对置换的乘法构成一个群, 其阶是 $n!/2$.

证：封闭性：偶置换与偶置换的乘积是偶置换. 易验证结合律. 单位元 I 恒等置换是偶置换, 偶置换的逆置换是偶置换, 所以 A_n 对置换的乘法构成一个群.

因为奇置换与偶置换的乘积是奇置换, 所以 n 元奇置换全体组成的集合为 $\tau A_n = \{\tau\sigma \mid \sigma \in A_n\}$, 其中 τ 是任已给定的奇置换. 因此, 取定一个奇置换 τ, 有 $S_n = A_n \cup \tau A_n$ 以及 $|S_n| = |A_n| + |\tau A_n| = 2|A_n|$, 故 $|A_n| = n!/2$.

定义 6.5.6

A_n 叫作**交错群**. 由 n 元置换构成的群叫作 n 元**置换群**.

定义 6.5.6

A_n 叫作**交错群**. 由 n 元置换构成的群叫作 n **元置换群**.

例 6.5.9 设 $\sigma = (1,2,3)$, 则循环群 $G =< \sigma >= \{e, (1,2,3), (1,3,2)\}$ 是 3 元置换群.

定义 6.5.6

A_n 叫作**交错群**. 由 n 元置换构成的群叫作 n 元**置换群**.

例 6.5.9 设 $\sigma=(1,2,3)$, 则循环群 $G=<\sigma>=\{e,(1,2,3),(1,3,2)\}$ 是 3 元置换群.

例 6.5.10 设 $\sigma_1=(1,2,3,4),\sigma_2=(1,3,2,4)$, 则循环群
$G_1=<\sigma_1>=\{e,(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}$ 和
$G_2=<\sigma_2>=\{e,(1,3,2,4),(1,2)(3,4),(1,4,2,3)\}$ 都是 4 元置换群.

本课作业

1. 证明：循环群是交换群.

2. 把下列置换写成不相交轮换的乘积, 并计算置换的奇偶性.

(1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$.　　(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 6 & 7 & 2 & 4 \end{pmatrix}$.

3. 下列各题中的置换 σ 和 τ, 计算 $\tau\sigma\tau^{-1}$.

(1) $\sigma = (1, 2, 4, 3)$, $\tau = (1, 3, 2)$.

(2) $\sigma = (1, 3, 5, 2)(4, 6)$, $\tau = (1, 3, 6)(2, 4, 5)$.

4. 设 σ 是一个置换, 且 $\operatorname{ord} \sigma$ 是奇数, 证明: σ 是偶置换.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn