群的结构

- 循环群
- 有限生成交换群
- 循环群
- 应用

9.1 循环群

- **定理1** 加群$\mathbf{Z}$ 的每个子群H 是循环群. 且有$H = \{0\}$ 或$H =< m >= m\mathbf{Z}$, 其中m 是H 中的最小正整数. 如果$H \neq< 0 >$, 则H 是无限的.

  证 如果$H = \{0\}$, 结论成立. 如果$H \neq \{0\}$, 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$H =< m >= m\mathbf{Z}$.

  事实上, 对任意的$a \in H$, 根据欧几里得除法, 存在整数q, r 使得$a = qm + r, \quad 0 \leq r < m$.

  如果$r \neq 0$, 则$r = a - qm \in H$, 这与m 的最小性矛盾.

  因此, $r = 0$, $a = qm \in m\mathbf{Z}$. 故$H \subset m\mathbf{Z}$. 但显然有$m\mathbf{Z} \subset H$. 因此, $H = m\mathbf{Z}$. 证毕.

- **定理2** 每个无限循环群同构于加群$\mathbf{Z}$. 每个阶为m的有限循环群同构于加群$\mathbf{Z}/m\mathbf{Z}$.

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

$$\begin{aligned} f:\mathbf{Z} &\longrightarrow G \\ n &\longmapsto a^n \end{aligned}$$

因为$f(n+m)=a^{n+m}=a^na^m=f(n)f(m)$, 所以$f$是$\mathbf{Z}$到$G$的同态, 而且是满的. 根据§8.3 定理9, 群G同构于$\mathbf{Z}/\ker(f)$. 根据定理1, $\ker(f)=<0>$或$\ker(f)=m\mathbf{Z}$. 前者对应于无限循环群, 后者对应于m阶有限循环群. 证毕.

- **定义1** 设G是一个群, $a\in G$. 则子群$< a >$的阶称为元素a的阶, 记为$\mathrm{ord}(a)$.

- **定理3** 设G 是一个群, $a \in G$. 如果a 是无限阶, 则
(i) $a^k = e \Leftrightarrow k = 0$.
(ii) 元素a^k $(k \in \mathbf{Z})$ 两两不同.
如果a 是有限阶$m > 0$, 则
(iii) m 是使得$a^m = e$ 的最小正整数.
(iv) $a^k = e \Leftrightarrow m|k$.
- **证** 考虑$\mathbf{Z}$ 到群G 映射$f : n \longmapsto a^n$. f 是同态. 有$\mathbf{Z}/\ker f \cong < a >$. 因为$a$ 是无限阶元等价于$\ker f = \{0\}$, 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$\ker f = m\mathbf{Z}$. 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$m|k$.

- **定理3**(续) 设G 是群, $a \in G$. 如果a 是无限阶, 则
  (v) $a^r = a^k \Leftrightarrow r \equiv k \pmod m$.
  (vi) a^k $(k \in \mathbf{Z}/m\mathbf{Z})$ 两两不同.
  (vii) $< a >= \{a, a^2, \ldots, a^{m-1}, a^m = e\}$.
  (viii) $\mathrm{ord}(a^d) = \dfrac{m}{(m,d)}$.
- **证** (v) $a^r = a^k \Longleftrightarrow r-k \in \ker f \Longleftrightarrow r \equiv k \pmod m$.
  (vi) 元素a^k 对应于$\mathbf{Z}/\ker f$ 中不同元素, 两两不同.
  (vii) $< a >= \{a, a^2, a^{m-1}, a^m = e\}$ 与$\mathbf{Z}/\ker f$ 中最小正剩余系相对应.
  (viii) 对任意整数$1 \le d \le m$, 有$\mathrm{ord}(a^d) = \dfrac{m}{(m,d)}$.
  $(a^d)^k = e \Longleftrightarrow dk \in \ker f \Longleftrightarrow m|dk \Longleftrightarrow \dfrac{m}{(m,d)}|\dfrac{d}{(m,d)}k \Longleftrightarrow \dfrac{m}{(m,d)}|k$. 故$\mathrm{ord}(a^d) = \dfrac{m}{(m,d)}$.

- **定理4** 循环群的子群是循环群.
- **证** 考虑映射$\mathbf{Z}$ 到循环群$G = < a >$ 的映射f :

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

f 是同态映射. 根据§8.2 定理1, 对于G 的子群H, 我们有$K = f^{-1}(H)$ 是$\mathbf{Z}$ 的子群. 根据定理1, K 是循环群, 所以$H = f(K)$ 是循环群. 证毕.

- **定理5** 设G 是循环群. 如果G 是无限的, 则G 的生成元为a 和a^{-1}. 如果G 是有限阶m, 则a^k 是G 的生成元为当且仅当$(k,m)=1$.
- **证** 考虑映射$\mathbf{Z}$ 到循环群G 的映射$f:$

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

f 是同态映射. 根据§8.3 定理9, 我们有

$$\mathbf{Z}/\ker f \cong G.$$

因为G 中的生成元对应于$\mathbf{Z}/\ker f$ 中的生成元. 但$\ker f=0$ 时, $\mathbf{Z}/\ker f$ 的生成元是1 和-1; $\ker f = m\mathbf{Z}$, $m>0$ 时, $\mathbf{Z}/\ker f$ 的生成元是k, $(k,m)=1$. 因此, 定理成立. 证毕.

- **引理1** 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

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

- **证** 因为

$$a^{\mathrm{ord}(ab)\mathrm{ord}(b)} = (ab)^{\mathrm{ord}(ab)\mathrm{ord}(b)} = 1,$$

所以$\mathrm{ord}(a) \mid \mathrm{ord}(ab)\mathrm{ord}(b)$. 进而$\mathrm{ord}(a) \mid \mathrm{ord}(ab)$.
同理, $\mathrm{ord}(b) \mid \mathrm{ord}(ab)$. 故$\mathrm{ord}(a)\mathrm{ord}(b) \mid \mathrm{ord}(ab)$.
此外, 显然有

$$\mathrm{ord}(ab) \mid \mathrm{ord}(a)\mathrm{ord}(b).$$

故$\mathrm{ord}(a)\mathrm{ord}(b) \mid \mathrm{ord}(ab)$.
因此, $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$.

- **引理2** 设G 是有限交换群. 对任意元素$a, b \in G$, 存在$c \in G$ 使得$\mathrm{ord}(c) = [\mathrm{ord}(a), \mathrm{ord}(b)]$.
- **证** 由§1.5 例5, 对于$\mathrm{ord}(a)$ 和$\mathrm{ord}(b)$, 存在u, v 满足:

$$u|\mathrm{ord}(a), \quad v|\mathrm{ord}(b), \quad (u, v) = 1$$

使得$[\mathrm{ord}(a),\ \mathrm{ord}(b)] = uv$.
现在令$s = \frac{\mathrm{ord}(a)}{u}, \quad t = \frac{\mathrm{ord}(b)}{v}$,
根据定理3(viii), 我们有

$$\mathrm{ord}(a^s) = \frac{\mathrm{ord}(a)}{(\mathrm{ord}(a), s)} = u, \quad \mathrm{ord}(b^t) = v.$$

再根据引理1, 我们得到

$$\mathrm{ord}(a^s b^t) = \mathrm{ord}(a^s)\mathrm{ord}(b^t) = uv = [\mathrm{ord}(a),\ \mathrm{ord}(b)].$$

因此, 取$c = a^s b^t$. 即为所求. 证毕.

- **定理6** 设G是有限交换群，则G中存在元素$a_1, a_2, \ldots, a_s$使得它们各自的元素阶$m_1, m_2, \ldots, m_s$满足$m_i|m_{i+1}$, $1 \le i \le s-1$, 并且使得$G = < a_1 >< a_2 > \cdots < a_s >$.

- 证 设$G = \{b_1, b_2, \ldots, b_n\}$. 由引理2, 存在元素$c_1$使得$\mathrm{ord}(c_1) = [\mathrm{ord}(b_1), \ldots, \mathrm{ord}(b_n)]$. 令$H_1 = < c_1 >$, 则

$$G/H_1 = \{b_{11}H_1, \ldots, b_{1n_1}H_1\}, \quad n_1 = [G : H_1] < n.$$

同理, 存在c_2使得$\mathrm{ord}(c_2) = [\mathrm{ord}(b_{11}), \ldots, \mathrm{ord}(b_{1n_1})]$. 令$H_2 = < c_2 >$, 则

$$G/(H_1H_2) = \{b_{21}(H_1H_2), \ldots, b_{2n_1}(H_1H_2)\},$$

$$n_2 = [G : H_1H_2] < n_1.$$

- 如此可找到$c_3, \ldots, c_s$ 及$H_3, \ \ldots, \ H_s$, 对于$2 \leq i \leq s$, 有

$$\begin{aligned} &\operatorname{ord}(c_i) = [\operatorname{ord}(b_{i-11}), \ldots, \operatorname{ord}(b_{i-1n_{i-1}})], \\ &G/(H_1H_2\cdots H_i) \\ = \ &\{b_{i1}(H_1H_2\cdots H_i), \ldots, b_{in_1}(H_1H_2\cdots H_i)\}, \\ &n_i = [G : H_1H_2\cdots H_i] < n_{i-1}. \end{aligned}$$

最后, $n_s = 1, \ G = H_1H_2\cdots H_s$.
从元素$c_1, \ c_2, \ldots, \ c_s$ 的构造, 我们有

$$\operatorname{ord}(c_i) \mid \operatorname{ord}(c_{i-1}), \quad 2 \leq i \leq s.$$

现在令$a_i = c_{s-i+1}, \ 1 \leq i \leq s$, 则它们为所求.

- **例1** 设$n = 3\cdot 5 = 15$. 则$(\mathbf{Z}/n\mathbf{Z})^* = \{1,2,4,7,8,11,13,14\}$.
  $H_1 =< 2 >= \{2, 2^2 = 4, 2^3 = 8, 2^4 = 1\}$.
  $7H_1 = \{7\cdot 2 = 14, 7\cdot 2^2 = 13, 7\cdot 2^3 = 11, 7\cdot 2^4 = 7\}$
  令$H_2 =< 7 >= \{7, 7^2 = 4, 7^3 = 13, 7^4 = 1\}$.
  $G = H_1 \cdot H_2 =< 2 >< 7 >$.

- **例2 设**$n = 23 \cdot 41 = 943$. **则**$\varphi(n) = (23-1)(41-1) = 880$. $[\varphi(23), \varphi(41)] = [23-1, 41-1] = 440$. **进一步**,
$\mathrm{order}_n(2) = 220$, $\mathrm{order}_n(3) = 88$, $\mathrm{order}_n(4) = 110$,
$\mathrm{order}_n(5) = 220$, $\mathrm{order}_n(6) = 440$, $\mathrm{order}_n(7) = 440$,
$\mathrm{order}_n(10) = 110$, $\mathrm{order}_n(11) = 440$, $\mathrm{order}_n(14) = 88$.

9.2 有限生成交换群

- 设G 是加法交换群. 设X 是G 的非空子集, 则由X 生成的子群是所有的线性组合

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k, \quad k \in \mathbf{N},\ n_i \in \mathbf{Z},\ x_i \in X$$

组成的集合. 特别, 由一个元生成循环子群

$$< x >= \{nx | n \in \mathbf{Z}\}.$$

- 交换群G 的一个子集X 叫做G 的**基底**, 如果X 是G 的最小生成元, 即

(i) $G =< X >$;

(ii) X 中任意不同元素$x_1, \ldots, x_k$ 在$\mathbf{Z}$ 上线性无关, 即不存在不全为零的整数$n_1, \ldots, n_k$ 使得

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0.$$

- 设G 是乘法交换群. 设X 是G 的非空子集, 则由X 生成的子群是所有的乘性组合

$$x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}, \quad k \in \mathbf{N},\ n_i \in \mathbf{Z},\ x_i \in X$$

组成的集合. 特别, 由一个元生成循环子群

$$< x >= \{x^n \mid n \in \mathbf{Z}\}.$$

- 交换群G 的一个子集X 叫做G 的**基底**, 如果X 是G 的最小生成元, 即

(i) $G =< X >$;

(ii) X 中任意不同元素$x_1, \ldots, x_k$ 都是**乘性无关**, 即不存在不全为零的整数$n_1, n_2, \ldots, n_k$ 使得

$$x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} = e.$$

- 设$H_1,\ldots,H_k$ 是交换群G 的k 个子群. 我们称和子群$H_1+\cdots+H_k$ 是$H_1,\ldots,H_k$ 的直和, 如果

$$(H_1+\cdots+H_{i-1}+H_{i+1}+\cdots+H_k)\cap H_i=\{0\},\ 1\le i\le k.$$

记作$H_1\oplus\cdots\oplus H_k$.
- 写作乘法时, 我们称$H_1\cdots H_k$ 是$H_1,\ldots,H_k$ 的直积, 如果$(H_1\cdots H_{i-1}H_{i+1}\cdots H_k)\cap H_i=\{e\},\ 1\le i\le k$. 记作$H_1\otimes\cdots\otimes H_k$.

- **定理1** 设交换群G 有一组非空基底, 则G 是一组循环群的直和.
- 定理1中的群叫做自由交换群.

- **证** 设$X = \{x_i \mid i \in \mathrm{I}\}$ 是G 的非空基底. 根据基底的定义, $G = \sum\limits_{i\in \mathrm{I}} < x_i >$.

  现在只需证明: 对任意$x_j \in X$,

$$< x_j > \cap (\sum_{i\in \mathrm{I},\ i\neq j} < x_i >) = \{0\}.$$

- 反证法. 若存在$y \in < x_j > \cap (\sum_{i\in \mathrm{I},\ i\neq j} < x_i >)$, $y \neq 0$, 则存在$n_j \in Z \setminus \{0\}$及$n_1, \ldots, n_{j-1}, n_{j+1}, \ldots, n_k \in \mathbf{Z}$使得

$$\begin{aligned} y &= n_j x_j \\ &= n_1 x_1 + \cdots + n_{j-1} x_{j-1} + n_{j+1} x_{j+1} + \cdots + n_k x_k. \end{aligned}$$

从而

$$n_1x_1+\cdots+n_{j-1}x_{j-1}+(-n_j)x_j+n_{j+1}x_{j+1}+\cdots+n_kx_k = 0.$$

因为$x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_k$ 是X 中的不同元, 所以根据基底的定义, 有

$$n_1 = \cdots = n_{j-1} = -n_j = n_{j+1} = \cdots = n_k = 0.$$

因此, $y = n_j x_j = 0$. 这与$y \neq 0$ 矛盾. 证毕.

- **定理2** 自由交换群的任意两个基底所含元素个数相同.

  证 仅考虑基底所含元素个数为有限的情形. 设

$$G =< x_1, x_2, \ldots, x_k >=< y_1, y_2, \ldots, y_m > .$$

- 考虑子群$H = 2G =< 2x_1, 2x_2, \ldots, 2x_k >$, 则商群

  $G/H = \{(n_1x_1 + n_2x_2 + \cdots + n_kx_k)H \mid n_i \in \mathbf{Z}/2\mathbf{Z}.\}$

  因此, $[G : H] = 2^k$.

- 又有$H = 2G =< 2y_1, 2y_2, \ldots, 2y_m >$, 同样有$[G : H] = 2^m$. 故$k = m$. 证毕.

- 自由交换群G 的基底的元素个数叫做群G 的秩.

- **定理3** 每个交换群G 都是一个秩为$|X|$ 的自由交换群的同态象子群, 其中X 为G 的生成元集.
- **证** 设G 的生成元集$X = \{x_1,\ x_2,\ \ldots\} = \{x_i\}_{i\in I}$. 考虑集合

$$\mathbf{Z}^I = \{(n_1, n_2, \ldots, n_i, \ldots) \mid n_i \in \mathbf{Z}, i \in I.\}$$

易知, $\mathbf{Z}^I$ 是秩为$|I| = |X|$ 的自由交换群, 且映射

$$f:\ (n_1, n_2, \ldots, n_k, \ldots) \longmapsto n_1x_1 + n_2x_2 + \cdots + n_kx_k$$

是$\mathbf{Z}^I$ 到G 的满同态. 所以$G = f(\mathbf{Z}^I)$. 证毕.
- **注** 表达式$(n_1, n_2, \ldots, n_i, \ldots)$ 中只有有限项不为零.

- **定理4** 每个有限生成交换群G 都是有限个循环群的直和, 并且有限循环群的阶$m_1, \ldots, m_s$ 满足$m_1|m_2, \ldots, m_{s-1}|m_s$.
- **证** 设G 的生成元集$X = \{x_1, x_2, \ldots, x_k\}$.
- 如果G 有无限阶元, 不妨设为x_1,令$H_1 =< x_1 >$, 考虑商群G/H_1, 其生成元为

$$X_1 = \{x_2 + H_1, \ldots, x_k + H_1\}.$$

- 如果G/H_1 中有无限阶元, 不妨设为$x_2 + H_1$, 则x_1, x_2 在$\mathbf{Z}$ 上线性无关. 令$H_2 =< x_2 >$,
考虑商群$G/(H_1 + H_2)$, 其生成元为

$$X_2 = \{x_3 + (H_1 + H_2), \ldots, x_k + (H_1 + H_2)\}.$$

- 如此继续下去, 可找到线性无关元$x_1, \ldots, x_t$及$H_1, \ldots, H_t$使得商群$G/(H_1 + \cdots + H_t)$ 为有限交换群.
- 根据§9.1 定理6, 存在有限阶循环群$H_{t+1}, \ldots, H_{t+s}$其阶$|H_{t+1}| = m_1, \ldots, |H_{t+s}| = m_s$ 满足

$$m_1 | m_2, \ \ldots, \ m_{s-1} | m_s,$$

并使得

$$G = H_1 + \cdots + H_t + H_{t+1} + \cdots + H_{t+s}.$$

9.3 置换群

- 进一步研究对称群S_n. 设$S=\{1,\ 2,\ \ldots,\ n-1,\ n\}$, σ 是S 上的一个置换, 即σ 是S 到自身的一一对应的映射:

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

因为k 在σ 下的象是i_k, 所以我们将σ 表示成

$$\sigma=\begin{pmatrix} 1 & 2 & \ldots & n-1 & n\\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n)\end{pmatrix}=\begin{pmatrix} 1 & 2 & \ldots & n-1 & n\\ i_1 & i_2 & \ldots & i_{n-1} & i_n\end{pmatrix}.$$

当然可写成

$$\sigma=\begin{pmatrix} n & n-1 & \ldots & 2 & 1\\ i_n & i_{n-1} & \ldots & i_2 & i_1\end{pmatrix}=\begin{pmatrix} j_1 & j_2 & \ldots & j_{n-1} & j_n\\ i_{j_1} & i_{j_2} & \ldots & i_{j_{n-1}} & i_{j_n}\end{pmatrix},$$

其中$j_1,\ j_2,\ \ldots,\ j_{n-1},\ j_n$ 是$1,\ 2,\ \ldots,\ n-1,\ n$ 的一个排列.

- **例1** 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$\sigma\tau$, $\tau\sigma$, σ^{-1}.

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

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

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

- **定理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, 其阶是$n!$.
- **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$e = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 1 & 2 & \ldots & n-1 & n \end{pmatrix}$ 是单位元.
- 置换$\sigma = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}$ 有逆元$\sigma^{-1} = \begin{pmatrix} i_1 & \ldots & i_n \\ 1 & \ldots & n \end{pmatrix}$.

  因此, S_n 对置换的乘法构成一个群.
- 因为$(1, 2, \ldots, n-1, n)$ 在置换σ 下的象$(\sigma(1), \sigma(2), \ldots, \sigma(n-1), \sigma(n)\xi)$ 是$(1, 2, \ldots, n-1, n)$ 的一个排列, 这样的排列共有$n!$ 个, 所以S_n 的阶为$n!$. 证毕.

- 如果n 元置换σ 使得$\{1,\ 2,\ \ldots,\ n-1,\ n\}$ 中的一部分元素$\{i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k\}$ 满足

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

又使得余下的元素保持不变, 则称该置换为$k-$轮换, 简称轮换, 记作

$$\sigma=(i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k).\ \left(=\begin{pmatrix} i_1 & \ldots & i_{k-1} & i_k & j_1 & \ldots & j_{n-k} \\ i_2 & \ldots & i_k & i_1 & j_1 & \ldots & j_{n-k} \end{pmatrix}\right.$$

k 称为轮换的长度.

- $k=1$时, 1-轮换为恒等置换;
- $k=2$ 时, 2-轮换(i_1,i_2)叫做对换.
- 两个轮换

$$\sigma=(i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k),\ \tau=(j_1,\ j_2,\ \ldots,\ j_{l-1},\ j_l)$$

叫做不相交, 如果$k+l$ 个元素都是不同的.

- **定理2** 任意一个置换都可以表示为不相交轮换的乘积. 在不考虑乘积次序的情况下, 该表达式是惟一的.
- **证** 设σ 是$S=\{1,\ 2,\ \ldots,\ n-1,\ n\}$ 上的一个置换. 在S中任取一个元素, 设为$i_1^{(1)}$. 因为$n+1$ 个元素

$$i_1^{(1)},\ \sigma^1(i_1^{(1)}),\ \ldots,\ \sigma^n(i_1^{(1)})$$

都落在n 元集S 中, 必有$k\neq l$ 使得$\sigma^k(i_1^{(1)})=\sigma^l(i_1^{(1)})$.
不妨设$k>l$, 得到$\sigma^{k-l}(i_1^{(1)})=i_1^{(1)}$.
取$k_1\leq n$ 为使得

$$\sigma^{k_1}(i_1^{(1)})=i_1^{(1)}$$

的最小正整数, 并令

$$i_2^{(1)}=\sigma^1(i_1^{(1)}),\ \ldots,\ i_{k_1}^{(1)}=\sigma^{k_1-1}(i_1^{(1)}).$$

则$\sigma_1=(i_1^{(1)},\ i_2^{(1)},\ \ldots,\ i_{k_1}^{(1)})$ 就是一个k_1-轮换.
如果$k_1=n$, 则$\sigma=\sigma_1$. 结论成立.

- 如果$k_1 < n$, 在$S \setminus \{i_1^{(1)}, i_2^{(1)}, \ldots, i_{k_1}^{(1)}\}$ 中任取一个元素, 设为$i_1^{(2)}$. 取$k_2 \le n$ 为使得

$$\sigma^{k_2}(i_1^{(2)}) = i_1^{(2)}$$

的最小正整数, 并令

$$i_2^{(2)} = \sigma^1(i_1^{(2)}), \ldots, i_{k_2}^{(2)} = \sigma^{k_2-1}(i_1^{(2)}).$$

则$\sigma_2 = (i_1^{(2)}, i_2^{(2)}, \ldots, i_{k_2}^{(1)})$ 是一个与σ_1 不相交的k_2–轮换.

- 如此下去,..., 可找到与$\sigma_1, \ldots, \sigma_{r-1}$ 不相交的k_r–轮换σ_r 使得$k_1 + k_2 + \cdots + k_r = n$. 因为对任意$i \in S$, 有

$$\sigma_1\sigma_2\cdots\sigma_r(i) = \sigma(i),$$

所以定理成立. 证毕.

- **例2** $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2,5,4)(1,6,3).$
- 对于轮换$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k)$, 有

$$\begin{aligned} \sigma &= (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k) \\ &= (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2) \\ &= (1, i_1)(1, i_k)(1, i_{k-1}) \cdots (1, i_3)(1, i_2)(1, i_1) \end{aligned}$$

.

- **例3**

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

.

- **定义1** n 元排列$i_1,\ \ldots,\ i_k,\ \ldots,\ i_l,\ \ldots,\ i_n$ 的一对有序元素$(i_k,\ i_l)$ 叫做**逆序**, 如果 $k < l$ 时, $i_k > i_l$. 排列中逆序的个数叫做该排列的**逆序数**, 记为$[i_1,\ \ldots,\ i_n]$.

- 对于例2 的置换σ, 有$[\sigma] = 5 + 4 + 0 + 0 + 1 + 0 = 10$.
- $[(1, 2, \ldots, n-1, n)] = 0$.
- $[(n, n-1, \ldots, 2, 1)] = (n-1)+(n-2)+\cdots+1 = \frac{(n-1)n}{2}$.

- **定 理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$[\sigma(1),\ \ldots,\ \sigma(n)]$ 的奇偶性相同.
- **证** 设$\tau = (\sigma(k),\ \sigma(l))$, 其对排列

$$\sigma(1),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(n)$$

作用得到新排列

$$\sigma(1),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(n)$$

则发生改变的有序对为

$$\underbrace{(\sigma(k),\ \sigma(k+1)),\ \ldots,\ (\sigma(k),\ \sigma(l))}_{l-k\ \text{对}},\ \underbrace{(\sigma(k+1),\ \sigma(l)),\ \ldots,\ (\sigma(l-1),\ \sigma(l))}_{l-k-l\ \text{对}},$$

共$2(l-k)-1$ 对. 因此, 对换改变排列的逆序数$[\sigma(1),\ldots,\sigma(n)]$ 的奇偶性.

- 再设$\sigma = \tau_k \cdots \tau_1$ 为m 个对换的乘积, 那么排列
$$1, \ldots, n$$
经过m 个对换变为排列
$$\sigma(1), \ldots, \sigma(n).$$
因此, 逆序数$[\sigma(1), \ldots, \sigma(n)]$ 的奇偶性与
$$[1, \ldots, n] + m = m$$
的奇偶性相同. 证毕.

- **定义2** 一个置换σ 叫做偶置换, 如果它可以表示为偶数个对换的乘积; σ 叫做奇置换, 如果它可以表示为奇数个对换的乘积.

  记A_n 为n 元偶置换全体组成的集合.

- **定理4** A_n 对置换的乘法构成一个群, 其阶是$n!/2$.
- **证** 因为偶置换与偶置换的乘积是偶置换, 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$\tau$是任一给定的奇置换. 因此, 取定一个奇置换$\tau$, 我们有$S_n = A_n \cup \tau A_n$ 以及$|S_n| = |A_n| + |\tau A_n| = 2A_n$. 故$|A_n| = n!/2$. 证毕.
- A_n 叫做**交错群**.
- 由n 元置换构成的群叫做n 元**置换群**.

- **例3** 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4** 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.

- G_1 与G_2 不是同构的四元群.

- **定理5** 设G 是一个n 元群. 则G 同构一个n 元置换群.
- **证** 任取$a \in G$,并令$\tau_a : x \mapsto ax \ (x \in G)$,则易知$\tau_a$是$G$的一个双射变换.现令$n$元置换群

$$\overline{G} = \{\tau_a | a \in G\},$$

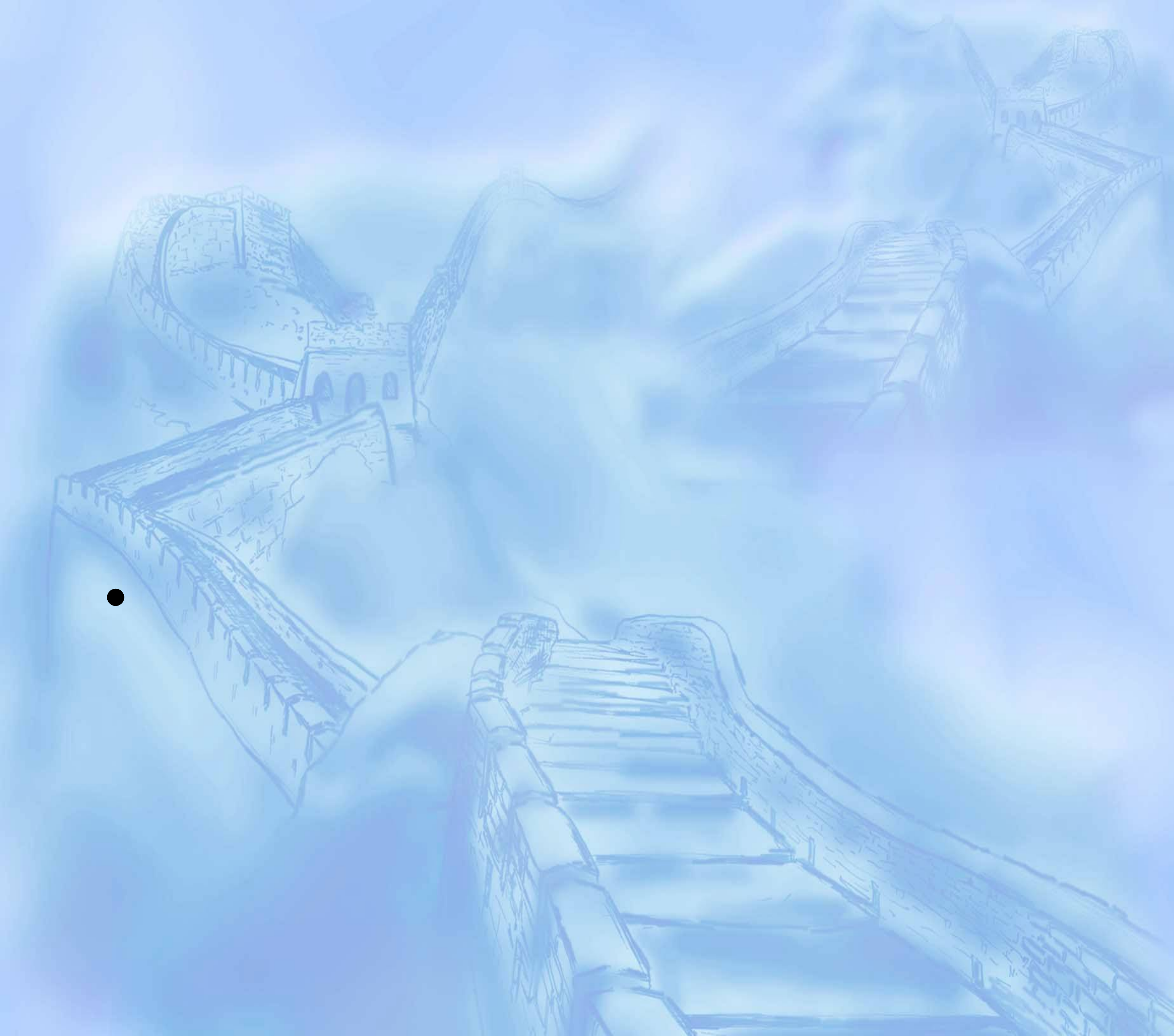
则显然

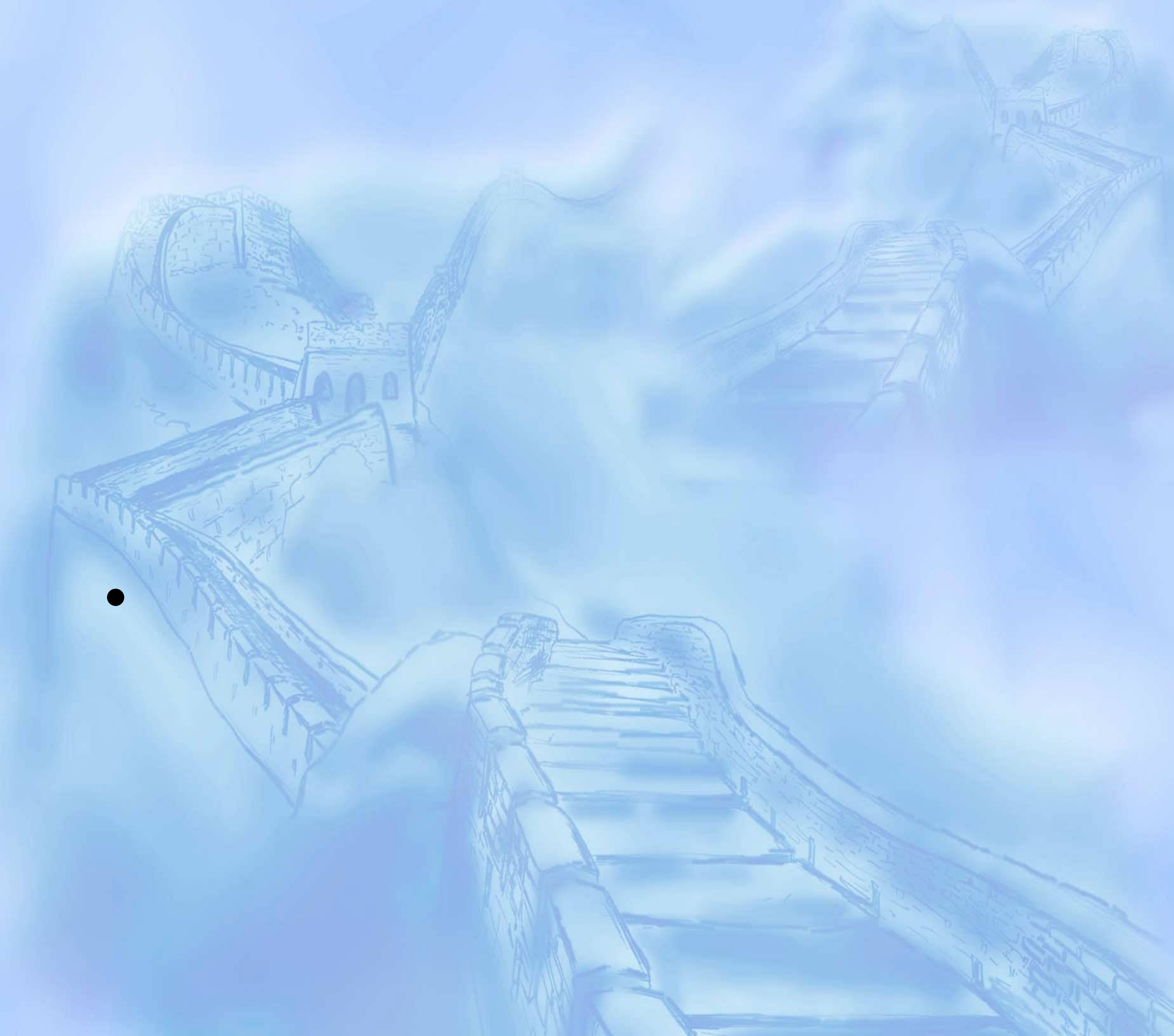
$$\varphi : a \mapsto \tau_a, \qquad \varphi(a) = \tau_a$$

是G到$\overline{G}$的一个双射, 又由于对G中任意元素x来说,有

$$\tau_{ab}(x) = ab(x) = a(bx) = a\tau_b(x) = \tau_a\tau_b(x)$$

故$\tau_{ab} = \tau_a\tau_b$,即有$\varphi_{ab} = \varphi_a\varphi_b$,因此$G \cong \overline{G}$.定理成立.证毕.





1. 设$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 6 & 1 \end{pmatrix}$. 计算$\sigma_1\sigma_2$, $\sigma_2\sigma_1$, σ_1^{-1}.

2. 求4 阶对称群S_4 的所有3 阶子群.

3. 求4 阶对称群S_4 的所有4 阶子群.

4. 素数阶群一定是循环群.

5. 设p 是奇素数. 证明: 乘群$\mathbf{F_p}^* = \mathbf{F}\{0\}$ 是同构于加群$\mathbf{Z}/(p-1)\mathbf{Z}$ 的循环群.

6. 设$p = 7$. 构造乘群$\mathbf{F_p}^* = \mathbf{F}\{0\}$ 中的乘法表和加群$\mathbf{Z}/(p-1)\mathbf{Z}$ 的加法表. 并说明习题5中的对应关系.

7. 设p 是奇素数. 证明: $\mathbf{Z}/p^2\mathbf{Z}$ 中的可逆元对乘法构成一个循环群, 并求其阶.

8. 求$(\mathbf{Z}/49\mathbf{Z})^*$ 中的所有生成元.

9. 求6 阶对称群S_4 的所有5 阶子群.

10. 分别求出$(\mathbf{Z}/31\mathbf{Z})^*$ 中的一个2 阶元a, 3 阶元b, 5 阶元c, 并证明abc 是生成元.

11. 求$(\mathbf{Z}/(31\cdot 43)\mathbf{Z})^*$ 中的所有元素的阶, 并计算各阶元的个数.

12. 求正整数n, 使得$(\mathbf{Z}/n\mathbf{Z})^*$ 为3 个循环群的乘积群$< a_1 >< a_2 >< a_3 >>$, 其中

$$|< a_{i+1} >| \mid |< a_i >|, \quad 1 \leq i \leq 2.$$

- 13. 求正整数n, 使得$(\mathbf{Z}/n\mathbf{Z})^*$ 为4 个循环群的乘积群$< a_1 >< a_2 >< a_3 >< a_4 >$, 其中

$$|< a_{i+1} >|\,|\,|< a_i >|, \;\; 1 \le i \le 3$$

- 14. 证明: 置换群S_4 的一组生成元为

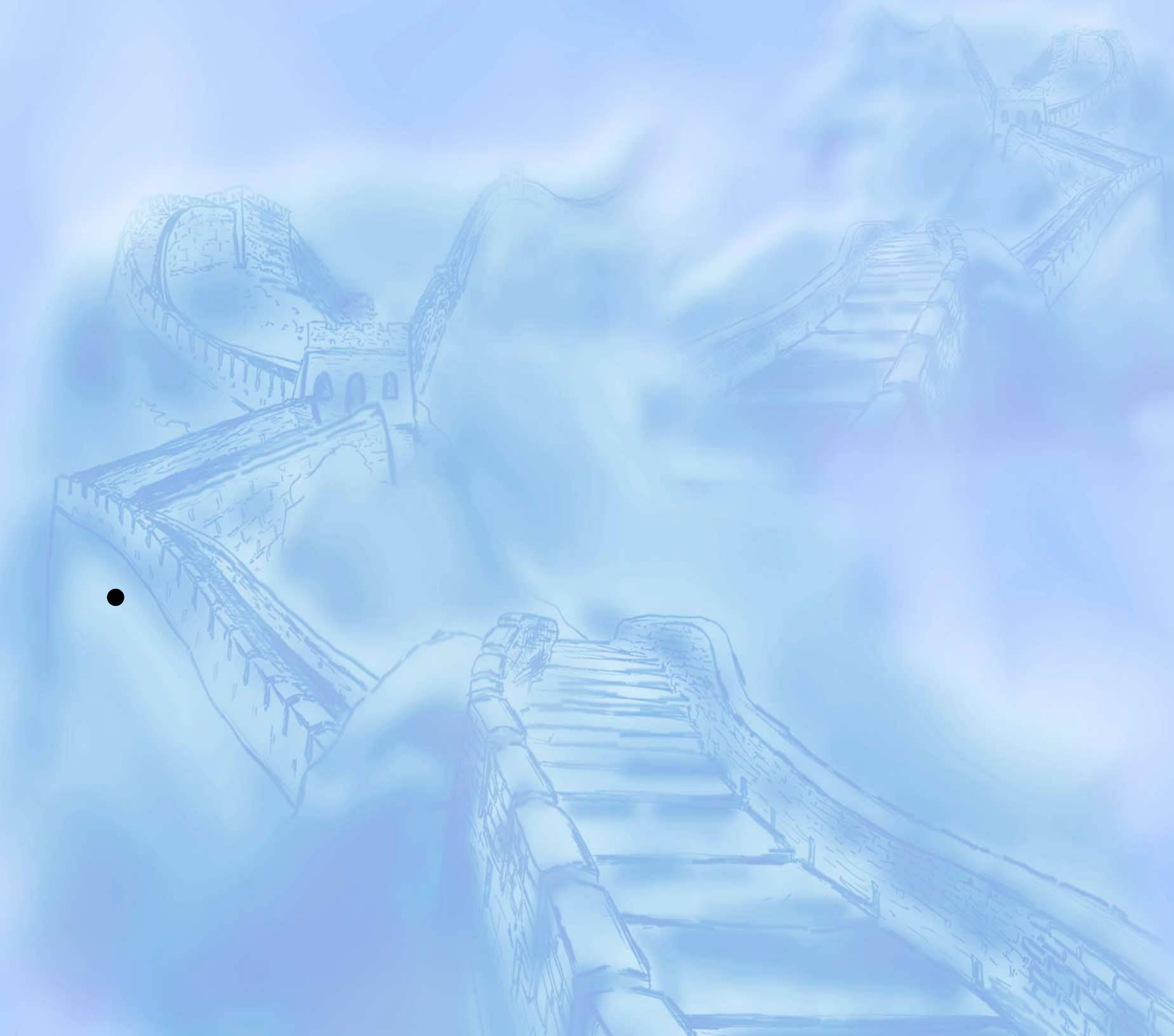
$$(1,2), (1,3), (1,4).$$

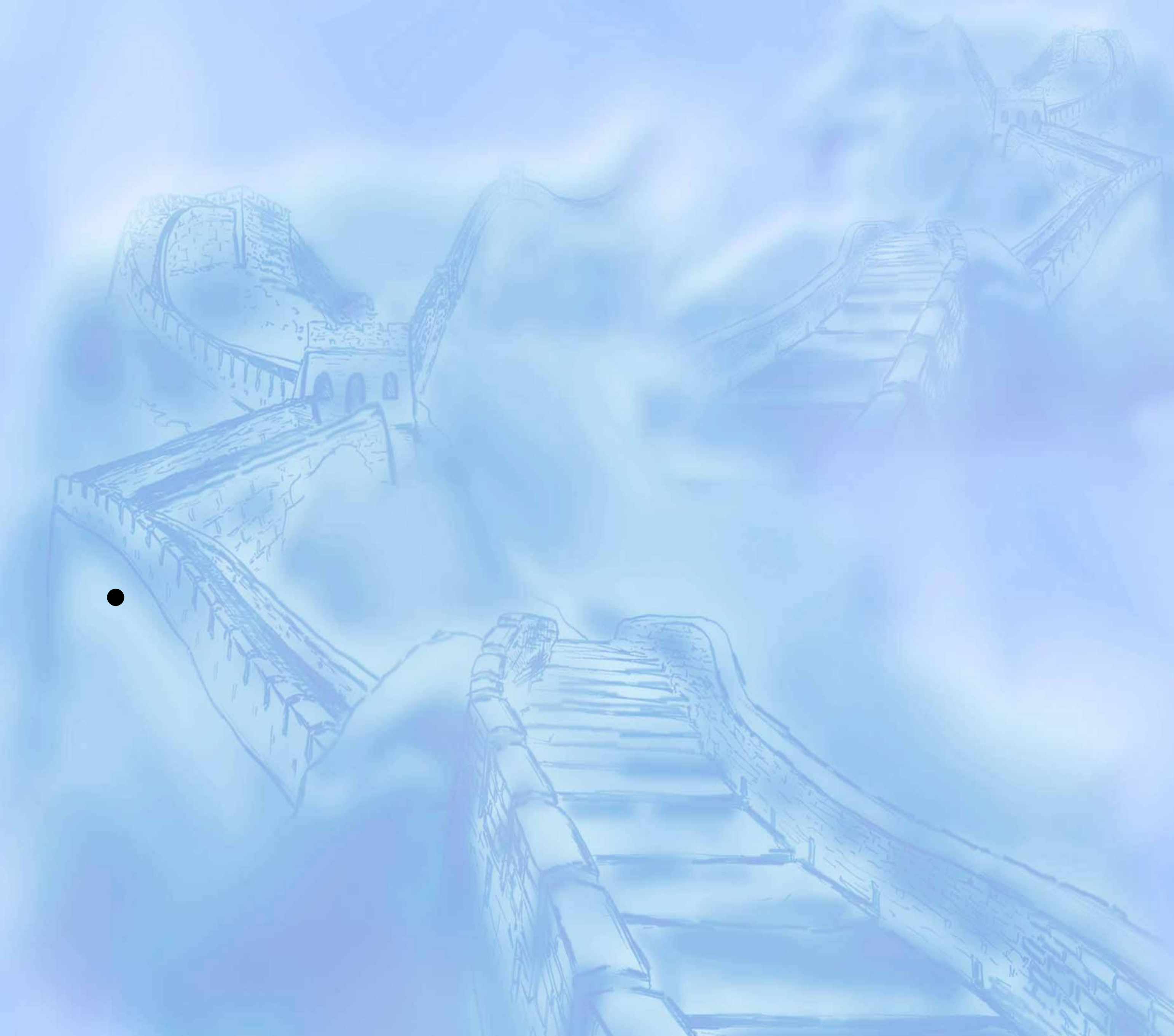
进一步, 用该组生成元来给出S_4 的所有子群.

- 15. 证明: $GL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z},\; ad - bc = 1 \right\}$

对于矩阵乘法构成群. 且 $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

是$GL_2(\mathbf{Z})$ 的一组生成元.





1. 证明: 如果a, b 是群G 的任意元素, 则

$$(ab)^{-1} = b^{-1}a^{-1}.$$

2. 证明: 群G 是交换群的充要条件是对任意$a, b \in G$,
有$(ab)^2 = a^2b^2$.

3. 证明: 群G 是交换群的充要条件是对任意$a, b \in G$,
有

$$(ab)^3 = a^3b^3, \quad (ab)^4 = a^4b^4, \quad (ab)^5 = a^5b^5.$$

4. 设G 是n 阶有限群. 证明: 对任意元$a \in G$, 有$a^n = e$.

5. 证明: 群G 中元素a 与其逆元a^{-1} 有相同的阶.

6. 设G 是一个群. 记

$$\mathrm{cent}(G) = \{a \in G \mid ab = ba \ \ \forall\, b \in G\}.$$

证明: $\mathrm{cent}(G)$ 是G 的正规子群.

7. 设a 是群G 的一个元素. 证明: 映射$\sigma: \ x \longmapsto axa^{-1}$ 是G 到自身的自同构.

8. 设H 是群G 的子群. 在G 中定义关系R: aRb 如果$b^{-1}a \in H$. 证明:

(i) R 是等价关系.

(ii) aRb 的充要条件是$aH = bH$.

9. 每个循环群都是交换群.

10. 给出$\mathbf{F}_7$ 中的加法表和乘法表.

11. 证明$\mathbf{F}_{23}$ 的非零元对于乘法构成一个循环群, 并求出其生成元.

12. 证明: $\mathbf{Z}/n\mathbf{Z}$ 中的可逆元对乘法构成一个群, 记作$\mathbf{Z}/n\mathbf{Z}^*$.

13. 证明: $\mathbf{Z}/26\mathbf{Z}$ 对乘法不构成一个群.

14. 构造26 元的一个乘法群.

10. 证明: $SL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}$ 是一个乘法群, 其生成元为

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

证

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$ 当$|c| > |d|$ 时, 利用此式交换c, d 的位置.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & aq + b \\ c & cq + d \end{pmatrix}$ 当$|c| \le |d|$ 时, 利用此式降低d 的绝对值.