第一章　预备知识

定义 5.13 设 $\sim$ 是 S 上的等价关系. 关于 $\sim$ 的所有等价类的集合称为 S 关于 $\sim$ 的商集. 记为 $S/\sim$. 映射

$$\begin{array}{rccc} \pi: & S & \longrightarrow & S/\sim \\ & x & \mapsto & \bar{x} \end{array}$$

称为关于 $\sim$ 的商映射或自然投射.

注意到商映射是满射. 对于等价关系 $\sim_c$, 其商映射就是判断每位同学是哪个班的. 对于 $\equiv_2$, 其商映射就是判断每个整数的奇偶性.

5.4　集合的划分

定义 5.14 设 S 是非空集, $\mathcal{P}$ 是 S 中一些非空子集组成的集合*(有限或无限)*. 如果

(i) 对任意不相等的 $U, V \in \mathcal{P}$, $U \cap V = \emptyset$,

(ii) $S = \bigcup_{U\in\mathcal{P}} U$,

则称 $\mathcal{P}$ 是 S 的一个划分 *(partition)*.

设 $\sim$ 是 S 上的等价关系. 根据上一讲中命题 5.11 和等价关系的自反性, $S/\sim$ 是 S 的一个划分. 反之, 设 $\mathcal{P}$ 是 S 的一

个划分. 我们定义 S 上的二元关系 $\sim_{\mathcal{P}}$ 如下: 对 $x, y \in S$, 如果存在 $U \in \mathcal{P}$ 使得 $x, y \in U$, 则 $x \sim_{\mathcal{P}} y$.

下面我们来验证 $\sim_{\mathcal{P}}$ 是等价关系. 由定义 5.14 中的条件 (ii) 可知, 对任意 $x \in S$, 存在 $U \in \mathcal{P}$ 使得 $x \in U$. 于是, $x \sim_{\mathcal{P}} x$. 自反性成立. 设 $x \sim_{\mathcal{P}} y$. 则存在 $U \in \mathcal{P}$ 使得 $x, y \in U$. 故 $y, x \in U$. 于是, $y \sim_{\mathcal{P}} x$. 对称性成立. 设 $x \sim_{\mathcal{P}} y$ 和 $y \sim_{\mathcal{P}} z$. 则存在存在 $U, V \in \mathcal{P}$, 使得 $x, y \in U$ 和 $y, z \in V$. 于是, $y \in U \cap V$. 由定义 5.14 中的条件 (ii) 可知, $U = V$. 故 $x, z \in U$. 从而, $x \sim_{\mathcal{P}} z$. 传递性成立. 称 $\sim_{\mathcal{P}}$ 是由划分 $\mathcal{P}$ 诱导的等价关系.

根据命题 5.11, 对于给定的集合 S 上的等价关系 $\sim$, 划分 $S/\sim$ 诱导的等价关系就是 $\sim$.

反之, 对于给定的集合 S 的划分 $\mathcal{P}$, 其诱导等价关系的商集 $S/\sim_{\mathcal{P}}$ 就是 $\mathcal{P}$.

因此, 等价关系通过其商集对集合分类, 而商映射意味着对集合中的元素归类. 另一方面, 对集合元素进行分类(划分)就是在集合上引入一个等价关系.

例 5.15 设 $S = [0, 3] \times [0, 1]$. 令

$$\begin{aligned}\mathcal{P} =& \{\{(x, y)\} \,|\, (x, y) \in S \text{ 且 } 0 < x < 3\} \\ & \cup \{\{(0, y), (3, y)\} \,|\, 0 \leq y \leq 1\}.\end{aligned}$$

则 $S/\sim_{\mathcal{P}}$ 是一个圆柱. 令

$$\begin{aligned}\mathcal{Q} =&\{\{(x,y)\}\,|\,(x,y)\in S \text{ 且 } 0<x<3\}\\ &\cup\{\{(0,y),(3,1-y)\}\,|\,0\le y\le 1\}.\end{aligned}$$

则 $S/\sim_{\mathcal{Q}}$ 是 *Möbius* 带.

5.5 映射分解定理

定义 5.16 设 $f:S\longrightarrow T$ 是映射. 如果 $f(x)=f(y)$, 则记 $x\sim_f y$. 称 $\sim_f$ 是由 f 诱导的等价关系.

我们来验证 $\sim_f$ 是等价关系. 对任意 $x\in S$, $f(x)=f(x)$. 于是, $x\sim_f x$. 自反性成立. 设 $x\sim_f y$. 则 $f(x)=f(y)$. 故 $f(y)=f(x)$. 于是, $y\sim_f x$. 对称性成立. 设 $x\sim_f y$ 和 $y\sim_f z$. 则 $f(x)=f(y)$ 且 $f(y)=f(z)$. 故 $f(x)=f(z)$. 于是, $x\sim_f z$. 传递性成立. 验证完毕.

例 5.17 设

$$\begin{array}{ccccc} f & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x,y) & \mapsto & \sqrt{x^2+y^2} \end{array}.$$

则 $\mathbb{R}^2$ 中两点关于 $\sim_f$ 等价当且仅当这两点在以原点为圆心的同心圆上. 而 $\mathbb{R}^2/\sim_f$ 是以原点为圆心的所有圆构成的集合.

定理 5.18 设 $f : S \longrightarrow T$ 是映射, π 是关于 $\sim_f$ 的商映射. 则存在唯一的映射 $\bar{f} : S/\sim_f \longrightarrow T$ 使得 $f = \bar{f} \circ \pi$, 且该映射是单射.

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & T \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\bar{f}} & \\ & (S/\sim_f) & \end{array}$$

证明. 设:

$$\begin{array}{rccc} \bar{f}: & S/\sim_f & \longrightarrow & T \\ & \bar{x} & \mapsto & f(x). \end{array}$$

因为 $\bar{x}$ 可能有不同的代表元, 所以我们需要验证 $\bar{f}$ 是良定义的. 设 $\bar{x} = \bar{y}$. 根据命题 5.11, $x \sim_f y$. 即 $f(x) = f(y)$. 故 $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. 于是, $\bar{f}$ 是良定义的.

对任意 $x \in S$, $\bar{f} \circ \pi(x) = \bar{f}(\bar{x}) = f(x)$. 故 $f = \bar{f} \circ \pi$. 存在性成立.

再设 $g : S/\sim_f \longrightarrow T$ 是映射使得 $f = g \circ \pi$. 则对于任意 $x \in S$, $f(x) = g \circ \pi(x) \implies g(\bar{x}) = f(x) = \bar{f}(\bar{x})$. 即 $g = \bar{f}$. 唯一性成立.

设 $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. 则 $f(x) = f(y)$. 故 $x \sim_f y$. 根据命题 5.11 (i), $\bar{x} = \bar{y}$. 故 $\bar{f}$ 是单射. □

例 5.19 设 S 是某中学全体学生的集合, T 是该中学全体老师的集合. 定义:

$$\begin{aligned} f:\ S &\longrightarrow T \\ x &\mapsto x \text{ 的班主任.} \end{aligned}$$

则 $\sim_f$ 是关于同学的等价关系 $\sim_c$. 商集 $S/\sim_f$ 是该中学所有的班. 而诱导映射 $\bar{f}$ 把班映到班主任, 它显然是单射. □

例 5.20 设 $m \in \mathbb{Z}^+$. 定义:

$$\begin{aligned} r:\ \mathbb{Z} &\longrightarrow \quad \mathbb{Z} \\ x &\mapsto \ \mathrm{rem}(x, m). \end{aligned}$$

则 $\sim_r$ 是关于 m 的同余关系. 商集 $S/\sim_r$ 是集合

$$\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

而诱导映射 $\bar{r}$ 把 $\bar{x}$ 映到 $\bar{x}$ 最小的非负代表元 $\mathrm{rem}(x, m)$, 它显然是单射. □

5.6 序关系

定义 5.21 设 $\preceq$ 是集合 S 上的二元关系. 如果

(i) 对任意 $x \in S$, $x \preceq x$ *(自反性)*,

(ii) 如果 $x, y \in S$ 且 $x \preceq y$ 和 $y \preceq x$, 则 $y = x$ *(反对称性)*,

(iii) 如果 $x, y, z \in S$, $x \preceq y$ 且 $y \preceq z$, 则 $x \preceq z$ *(传递性)*,

则称 $\preceq$ 是偏序. 进而, 设 $\preceq$ 是 S 上的偏序. 如果对任意 $x, y \in S$, 我们有 $x \preceq y$ 或 $y \preceq x$. 则称 $\preceq$ 是全序.

例 5.22 在实数集上, $\leq$ 和 $\geq$ 都是全序. 设 S 是非空集合, T 是 S 中所有子集的集合. 则 $\subset$ 和 $\supset$ 是 T 上的偏序关系.

定义 5.23 设 $\preceq$ 是集合 S 上的偏序关系, $z \in S$. 如果不存在 $x \in S \setminus \{z\}$ 使得 $z \preceq x$, 则称 z 是 S 中关于 $\preceq$ 的极大元. 如果对于任意 $x \in S$, 我们都有 $x \preceq z$. 则称 z 是 S 中关于 $\preceq$ 的最大元. 类似地, 我们可以定义关于偏序的极小元和最小元.

注解 5.24 极小元意味着集合 S 中没有其它元素比它更小. 最小元意味着集合 S 中的其它元素都比它大. 对极大元和最大原有类似的直观描述.

注解 5.25 设 $\preceq$ 是集合 S 上的偏序关系, z_1 和 z_2 是关于 $\preceq$ 的两个最大元. 则 $z_1 \preceq z_2$ 和 $z_2 \preceq z_1$. 根据反对称性 $z_1 = z_2$. 故当最大元存在时, 它是唯一的. 此时它也是唯一的极大元. 类似的结论也适用于最小元和极小元.

例 5.26 设 $S = \{1, 2, 3\}$, T 是 S 的所有真子集组成的集合. 则 $\subset$ 是 T 上的偏序. 关于该偏序的极大元是

$$\{1, 2\}, \{2, 3\}, \{1, 3\},$$

没有最大元. 关于该偏序的最小元是 $\emptyset$, 也是唯一的极小元. $\square$

6 置换

6.1 置换的定义和乘法

令

$$[n] = \{1, 2, \ldots, n\},$$

S_n 是从 $[n]$ 到 $[n]$ 的所有双射的集合. 则 $\mathrm{card}(S_n) = n!$.

设 $\sigma \in S_n$ 使得 $\sigma(k) = i_k$, $k = 1, 2, \ldots, n$. 我们可以把 σ 表示为

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

其中 $i_1, i_2, \ldots, i_n \in [n]$, 两两不同. 我们称 σ 是关于 $1, 2, \ldots, n$ 的置换. 设 e 是 $[n]$ 上的恒同映射, 即

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix},$$

因为双射的复合仍是双射, 所以, 对任意 $\sigma, \tau \in S_n$, $\sigma \circ \tau \in S_n$. 我们把 $\sigma \circ \tau$ 简记为 $\sigma\tau$, 并简称为 σ 和 τ 的积. 由映射复合的性质可知, 对任意 $\sigma, \tau, \delta \in S_n$,

$$(\sigma\tau)\delta = \sigma(\tau\delta) \quad \text{和} \quad e\sigma = \sigma e = \sigma.$$

又因为 σ 是双射, 所以 $\sigma^{-1} \in S_n$ 且

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = e.$$

例 6.1 设在 S_4 中

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{和} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

计算 $\sigma\tau$ 和 $\tau\sigma$,

解. 根据映射复合的定义可知:

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

和

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

注解 6.2 在上例中, $\sigma\tau \neq \tau\sigma$. 故 S_n 中的乘法不满足交换律. 特别地,

$$(\sigma\tau)^2 = \sigma\tau\sigma\tau$$

一般不等于 $\sigma^2\tau^2$.

设 $k \in \mathbb{Z}, \sigma \in S_n$. 如果 $k > 0$, 则

$$\sigma^k := \underbrace{\sigma \circ \cdots \circ \sigma}_{k}.$$

当 $k=0$ 时, $\sigma^k := e$. 当 $k<0$,

$$\sigma^k := \underbrace{\sigma^{-1}\circ\cdots\circ\sigma^{-1}}_{-k}.$$

可直接验证, 对任意 $i,j\in\mathbb{Z}$,

$$\sigma^i\sigma^j=\sigma^{i+j},\quad \sigma^{ij}=(\sigma^i)^j=(\sigma^j)^i.$$

根据穿衣脱衣规则, 对任意 $\tau\in S_n$,

$$(\sigma\tau)^{-1}=\tau^{-1}\sigma^{-1}.$$

引理 6.3 设 $\sigma\in S_n$. 则存在 $k\in\mathbb{Z}^+$ 使得 $\sigma^k=e$.

证明. 考虑无穷序列: $\sigma,\sigma^2,\ldots$. 则存在 $i,j\in\mathbb{Z}^+$ 且 $i<j$ 使得 $\sigma^j=\sigma^i$. 于是, $\sigma^{j-i}=e$. □

定义 6.4 设 $\sigma\in S_n$. 使得 $\sigma^k=e$ 的最小正整数称为 σ 的阶, 记为 $\mathrm{ord}(\sigma)$.

例 6.5 设

$$\sigma=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\in S_4.$$

求 $\mathrm{ord}(\sigma)$.

解. 直接计算得

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

进而,

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

于是, $\mathrm{ord}(\sigma) = 3$.

命题 6.6 设 $\sigma \in S_n$ 且 $k = \mathrm{ord}(\sigma)$. 则对任意 $m \in \mathbb{Z}$, $\sigma^m = e \iff k|m$.

证明. 设 $q = \mathrm{quo}(m,k), r = \mathrm{rem}(m,k)$. 则

$$\sigma^m = \sigma^{qk+r} = (\sigma^k)^q \sigma^r = \sigma^r.$$

于是, $\sigma^m = e \iff \sigma^r = e$. 因为 $0 \le r < k$, 所以

$$\sigma^m = e \iff r = 0. \quad \square$$

6.2 循环分解

定义 6.7 设 $\sigma \in S_n$. 如果存在 $i_1, i_2, \ldots, i_k \in [n]$ 两两不同使得

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

且对任意 $m \in [n] \setminus \{i_1, \ldots, i_k\}$,

$$\sigma(m) = m,$$

则称 σ 是长度为 k 的循环. 我们把这样的循环记为 $(i_1 i_2 \ldots i_k)$.

注意到

$$(i_1 i_2, \ldots, i_k) = (i_2 i_3 \ldots i_k i_1) = (i_3 i_4 \ldots i_k i_1 i_2) = \cdots .$$

此外, 长度为 1 的循环只有 e.

例 6.8 可直接验证循环 $(i_1 i_2 \ldots i_k)^{-1} = (i_k i_{k-1} \ldots i_2 i_1)$.

引理 6.9 设 $\sigma \in S_n$ 是长度为 k 的循环. 则 $\mathrm{ord}(\sigma) = k$.

证明. 设 $\sigma = (i_1 i_2 \ldots i_k)$ 且 $m \in \{1, 2, \ldots, k-1\}$, 则

$$\sigma^m(i_1) = i_{1+m}.$$

故 $\sigma^m \neq e$. 而 $\sigma^k(i_1) = i_1$. 注意到对任意 $\ell \in \{2, \ldots, k\}$,

$$\sigma = (i_\ell i_{\ell+1} \ldots i_k i_1 \ldots i_{\ell-1}).$$

故 $\sigma^k(i_\ell) = i_\ell$. 于是, $\sigma^k = e$. 我们得到 $\mathrm{ord}(\sigma) = k$. □

恒同映射也称为长度等于 1 的循环, 它是平凡的.

例 6.10 把

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 4 & 5 & 7 & 6 & 1 & 8 \end{pmatrix}$$

写成循环之积.

解. $\sigma = (198)(23)(67)$.

设 $\sigma \in S_n$. 定义 $M_\sigma = \{i \in [n] \,|\, \sigma(i) \neq i\}$.

例 6.11 我们有 $M_e = \emptyset$ 和 $M_{(i_1,\ldots,i_k)} = \{i_1, \ldots, i_k\}$.

引理 6.12 设 $\sigma \in S_n$ 且 $i \in M_\sigma$. 则 $\sigma(i) \in M_\sigma$.

证明. 假设设 $\sigma(i) \notin M_\sigma$. 则 $\sigma^2(i) = \sigma(i)$. 两边同时作用 σ^{-1} 得 $\sigma(i) = i$, 矛盾. □

定义 6.13 设 $\sigma, \tau \in S_n$. 如果 $M_\sigma \cap M_\tau = \emptyset$, 则称 σ 和 τ 是两个互不相交的置换.

引理 6.14 设 $\sigma, \tau \in S_n$ 互不相交. 则 $\sigma\tau = \tau\sigma$.

证明. 如果 $\sigma = e$ 或 $\tau = e$, 则结论显然成立.

设 $\sigma \neq e$ 和 $\tau \neq e$. 令 $i \in M_\sigma$. 则 $i \notin M_\tau$. 故 $\tau(i) = i$. 从而, $\sigma\tau(i) = \sigma(i)$. 另一方面, 引理 6.12 蕴含 $\sigma(i) \in M_\sigma$. 故 $\sigma(i) \notin M_\tau$. 我们有 $\tau\sigma(i) = \sigma(i)$. 于是, 对任意 $i \in M_\sigma$,

$$\sigma\tau(i) = \tau\sigma(i).$$

类似地, 对任意 $j \in M_\tau$, $\sigma\tau(j) = \tau\sigma(j)$.

而对任意 $k \in [n] \setminus (M_\sigma \cup M_\tau)$,

$$\sigma\tau(k) = k = \tau\sigma(k)$$

显然成立. 综上所述, $\sigma\tau = \tau\sigma$. □

命题 6.15 设 $\sigma \in S_n \setminus \{e\}$. 则 σ 是有限个两两互不相交的长度大于 1 的循环之积.

证明. 我们对 $\mathrm{card}(M_\sigma)$ 归纳.

根据引理 6.12, $\mathrm{card}(M_\sigma) > 1$. 如果 $\mathrm{card}(M_\sigma) = 2$, 则设 $M_\sigma = \{i_1, i_2\}$. 再利用引理 6.12 可知 $\sigma = (i_1 i_2)$. 设对 $2 \leq \mathrm{card}(M_\sigma) < m$ 结论都成立. 考虑 $\mathrm{card}(M_\sigma) = m$ 的情形. 设 $i_1 \in M_\sigma$ 且 $p = \mathrm{ord}(\sigma)$. 则 $\sigma^p(i_1) = i_1$. 于是, 存在最小正整数 k 使得 $\sigma^k(i_1) = i_1$. 则

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

两两不同. 否则, 存在 $r, s \in \{0, 1, \ldots, k-1\}$ 使得 $r < s$ 且 $\sigma^s(i_1) = \sigma^r(i_1)$. 则 $\sigma^{s-r}(i_1) = i_1$. 但 $0 < s - r < k$, 矛盾. 由 (1) 和 $\sigma(i_k) = \sigma^k(i_1) = i_1$ 可知, 循环 $\tau = (i_1 i_2, \ldots i_k)$ 满足 $\tau(i_1) = \sigma(i_1), \ldots, \tau(i_{k-1}) = \sigma(i_{k-1}), \tau(i_k) = i_1 = \sigma(i_k)$. 换言之,

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

令 $\lambda{=}\tau^{-1}\sigma$. 则 $i_1, \ldots, i_k \notin M_\lambda$. 设 $j \in [n] \setminus M_\sigma$. 则 $j \notin \{i_1, \ldots, i_k\}$. 故 $\lambda(j) = \tau^{-1}\sigma(j) = \tau^{-1}(j) = j$. 于是,

$$M_\lambda \subset M_\sigma \setminus \{i_1, \ldots, i_k\} \Longrightarrow \mathrm{card}(M_\lambda) < m.$$

如果 $M_\lambda = \emptyset$, 则 $\lambda = e$. 故 $\sigma = \tau$ 是循环. 否则, 归纳假设蕴含 $\lambda = \lambda_1 \cdots \lambda_s$, 其中 $\lambda_1, \ldots, \lambda_s$ 是两两互不相交的循环. 又因为 $i_1, \ldots, i_k \notin M_\lambda$, 所以每个循环 $\lambda_1, \ldots, \lambda_s$ 与 τ 都不相交. 从而 $\sigma = \tau\lambda = \tau\lambda_1 \cdots \lambda_s$ 即为所求. □

下面来证明上述定理中循环分解的唯一性.

定理 6.16 设 $\sigma \in S_n \setminus \{e\}$. 则在不计循环出现顺序的前提下, σ 可以唯一地写成有限个两两互不相交的(长度大于 1 的)循环之积.

证明. 分解的存在性见命题 6.15. 下面证明唯一性. 设

$$\sigma = \tau_1 \cdots \tau_p = \lambda_1 \cdots \lambda_q,$$

其中 $\tau_1, \ldots, \tau_p$ 是一组两两互不相交的循环, $\lambda_1, \ldots, \lambda_q$ 是另一组互不相交的循环. 我们要证明 $p = q$ 且适当调整下标后, $\tau_1 = \lambda_1, \ldots, \tau_p = \lambda_p$.

我们对 p 归纳. 设 $\tau_1 = (i_1 i_2 \ldots i_k)$. 则 $i_1 \in M_\sigma$, 故 i_1 会被唯一的一个第二组的循环移动. 由引理 6.14 可知, 不妨设 λ_1 移动 i_1. 则

$$\sigma(i_1) = \tau_1 \tau_2 \cdots \tau_p(i_1) = \tau_1(i_1) = i_2$$

且

$$\sigma(i_1) = \lambda_1 \lambda_2 \cdots \lambda_p(i_1) = \lambda_1(i_1).$$

故 $\lambda_1(i_1) = i_2$. 特别地, i_2 在循环 λ_1 中出现且不在其它循环中出现. 利用上述推理方式可得 $\lambda_1(i_2) = i_3$. 进而

$$\lambda_1(i_j) = i_{j+1},\ j \in \{3, \ldots, k-1\} \quad \text{且} \quad \lambda_1(i_k) = i_1.$$

于是, $\lambda_1 = \tau_1$. 特别地, 当 $p = 1$ 时, $\sigma = \tau_1 = \lambda_1$.

设 $p>1$ 且结论对 $p-1$ 成立. 则根据 $\tau_1=\lambda_1$, 我们有 $\tau_2\cdots\tau_p=\lambda_2\cdots\lambda_q$. 由归纳假设可知, $p=q$ 且在适当调整下标后, $\tau_2=\lambda_2,\ldots,\tau_p=\lambda_p$. □

推论 6.17 设 $\sigma\in S_n\setminus\{e\}$ 是互不相交的循环 $\tau_1,\ldots,\tau_m$ 之积. 则 $\mathrm{ord}(\sigma)=\mathrm{lcm}(\mathrm{ord}(\tau_1),\ldots,\mathrm{ord}(\tau_m))$.

证明. 设 $\ell_i=\mathrm{ord}(\tau_i)$, $i=1,\ldots,m$, $\ell=\mathrm{lcm}(\ell_1,\ldots,\ell_m)$. 令

$$\ell=k_i\ell_i,$$

其中 $k_i\in\mathbb{Z}^+$, $i=1,2,\ldots,m$. 第三讲引理 6.11 蕴含

$$\sigma^\ell=\tau_1^\ell\cdots\tau_m^\ell=\tau_1^{\ell_1k_1}\cdots\tau_m^{\ell_mk_m}=e.$$

设 $k=\mathrm{ord}(\sigma)$. 根据第三讲命题 6.6, $k|\ell$. 我们有

$$\sigma^k=\tau_1^k\cdots\tau_m^k=e.$$

不妨设 $\tau_1(1)\neq 1$. 因为 τ_1 与 $\tau_2,\ldots,\tau_m$ 都不相交, 所以 $\tau_2(1)=\cdots=\tau_m(1)=1$. 于是, $\tau_1^k(1)=1$. 故 $\tau_1^k=e$. 根据第三讲命题 6.6, 我们得到 $\ell_1|k$. 同理, $\ell_2|k$, …, $\ell_m|k$. 故 k 也是 $\ell_1,\ldots,\ell_k$ 的公倍数. 再根据 $k|\ell$ 可知, $k=\ell$. □

例 6.18 计算 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&5&4&6&10&8&2&9&1&7\end{pmatrix}$ 的阶.

解. $\sigma=(134689)(25\underline{10}7)\Longrightarrow\mathrm{ord}(\sigma)=\mathrm{lcm}(6,4)=12.$

命题 6.19 设 $\sigma, (i_1, \ldots, i_k) \in S_n$. 则

$$\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

证明. 只要验证: $\sigma(i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k))\sigma$. 设 $a \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. 则

$$\sigma(i_1, \ldots, i_k)(a) = \sigma(a) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(a) = \sigma(a).$$

设 $j \in \{1, \ldots, k-1\}$. 则

$$\sigma(i_1, \ldots, i_k)(i_j) = \sigma(i_{j+1}) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(i_j) = \sigma(i_{j+1}).$$

进而,

$$\sigma(i_1, \ldots, i_k)(i_k) = \sigma(i_1) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(i_k) = \sigma(i_1).$$

综上所述, $\sigma(i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k))\sigma$. □