第一章　预备知识

6.3　偶置换和奇置换

长度等于 2 的循环称为对换(transposition). 对换的逆就是其本身.

引理 6.20 任何一个置换都是若干个对换之积.

证明. 根据循环分解定理, 只要证明任何一个循环可以写成若干个对换之积即可. 我们验证:

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

其中 $k > 2$. 令 $\sigma = (i_k i_{k-1}) \cdots (i_k i_2)(i_k i_1)$.

对于任意 $j \in \{1, 2, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$, $(i_1, \ldots, i_k)$ 和 σ 都把 j 映成 j. 设 $\ell \in \{1, 2, \ldots, k-2\}$. 则

$$\begin{aligned}
\sigma(i_\ell) &= \underbrace{(i_k i_{k-1}) \cdots (i_k i_{\ell+2})}\underbrace{(i_k i_{\ell+1})(i_k i_\ell)}\,(i_\ell) \\
&= \underbrace{(i_k i_{k-1}) \cdots (i_k i_{\ell+2})}\,(i_{\ell+1}) \\
&= i_{\ell+1}.
\end{aligned}$$

而

$$\sigma(i_{k-1}) = (i_k i_{k-1})(i_{k-1}) = i_k \quad \text{和} \quad \sigma(i_k) = i_1.$$

等式 (1) 成立. □

例 6.21 把

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

写成对换之积.

解. 由循环分解和上述引理可知:

$$\sigma = (124)(56) = (42)(41)(56).$$

引理 6.22 设 $\sigma, \tau \in S_n$ 两个对换, $\sigma = (st)$ 且 $\sigma \neq \tau$. 则 S_n 中存在两个对换 σ' 和 τ' 满足

$$\sigma'(s) = s,\ \tau'(s) \neq s \text{ 且 } \tau\sigma = \tau'\sigma'.$$

证明. 设 $\tau = (uv)$.

情形 *1.* 如果 $\{s,t\} \cap \{u,v\} = \emptyset$, 则令 $\tau' = \sigma$ 和 $\sigma' = \tau$. 由第三讲引理 6.14 可知, $\tau\sigma = \tau'\sigma'$.

情形 *2.* 设 $\tau = (su)$. 则 $u \neq t$. 取 $\sigma' = (tu)$, $\tau' = (st)$ 即可.

情形 *3.* 设 $\tau = (tu)$. 则 $u \neq s$. 取 $\sigma' = \tau$, $\tau' = (su)$ 即可. □

引理 6.23 设 $\tau_1, \ldots, \tau_k \in S_n$ 是对换. 如果 $\tau_1 \cdots \tau_k = e$, 则 k 是偶数.

证明. 我们先证明下列断言:

断言. 设 $k > 2$. 则 e 可以写成 $k-2$ 个对换之积.

断言的证明. 如果 $\tau_{k-1} = \tau_k$, 则 $\tau_{k-1}\tau_k = e$. 我们有 $\tau_1 \cdots \tau_{k-2} = e$. 断言成立.

否则 $\tau_{k-1} \neq \tau_k$. 设 $s \in \{1, 2, \ldots, n\}$ 满足 $\tau_k(s) \neq s$. 根据引理 6.22, 存在对换 $\tau'_{k-1}, \tau'_k \in S_n$ 满足 $\tau'_k(s) = s$, $\tau'_{k-1}(s) \neq s$ 且 $\tau'_{k-1}\tau'_k = \tau_{k-1}\tau_k$. 于是 $e = \tau_1 \cdots \tau_{k-2}\tau'_{k-1}\tau'_k$. 特别地, 最右侧的对换不移动 s.

下面考虑 τ_{k-2}, τ'_{k-1}. 如果 $\tau_{k-2}\tau'_{k-1} = e$, 则 e 是 $k-2$ 个对换之积. 否则, 引理 6.22 蕴含存在对换 τ^*_{k-2} 和 τ^*_{k-1} 满足 $\tau^*_{k-1}(s) = s$, $\tau^*_{k-2}(s) \neq s$ 和 $\tau_{k-2}\tau'_{k-1} = \tau^*_{k-2}\tau^*_{k-1}$. 于是

$$e = \tau_1 \cdots \tau^*_{k-2}\tau^*_{k-1}\tau'_k.$$

特别地, 最右侧的两个对换都不移动 s, 但 τ^*_{k-2} 移动 s.

以此类推, 我们要么证明 e 是 $k-2$ 个对换之积; 要么得出 $e = \lambda_1\lambda_2 \cdots \lambda_k$, 其中 $\lambda_1, \ldots, \lambda_k \in S_n$ 是对换, 满足

$$\lambda_1(s) \neq s, \text{ 且 } \lambda_2(s) = \cdots \lambda_k(s) = s.$$

但这意味着 $e(s) \neq s$. 矛盾. 断言成立.

反复利用断言可知, k 是偶数. □

定理 6.24 设 $\sigma \in S_n$. 设 $\sigma = \lambda_1 \cdots \lambda_k = \mu_1 \cdots \mu_m$, 其中 $\lambda_1, \ldots \lambda_k, \mu_1, \ldots, \mu_m$ 都是对换. 则 k 和 m 的奇偶性相同.

证明. 由穿衣脱衣规则可知, $e = \lambda_1 \cdots \lambda_k\mu_m^{-1} \cdots \mu_1^{-1}$. 因为对换的逆是其本身, 所以引理 6.23 蕴含 $k+m$ 是偶数. 于是, k 和 m 的奇偶性相同. □

定义 6.25 设 $\sigma \in S_n$. 如果 σ 可以写成奇数个对换之积, 则称 σ 是奇置换. 否则称为 偶置换. 特别地, e 是偶置换. 奇置换的符号定义为 -1, 偶置换的符号为 1. 置换 σ 的符号记为 ε_σ.

上述定理说明置换的符号是良定义的.

推论 6.26 设 $\sigma \in S_n$ 且 $\sigma = \tau_1 \cdots \tau_k$, 其中 $\tau_1, \ldots, \tau_k$ 是循环. 则 σ 的奇偶性与整数 $\sum_{i=1}^{k}(\mathrm{ord}(\tau_i) - 1)$ 相同. 即 $\epsilon_\sigma = (-1)^{\sum_{i=1}^{k}(\mathrm{ord}(\tau_i)-1)}$.

证明. 设 $\tau = (i_1 \ldots i_m)$. 根据引理 6.20, $\tau = (i_m i_{m-1}) \cdots (i_m i_1)$. 于是, $\epsilon_\tau = (-1)^{m-1}$. 再根据第三讲引理 6.9 可知,

$$m = \mathrm{ord}(\tau) \implies \epsilon_\tau = (-1)^{\mathrm{ord}(\tau)-1}.$$

由上述引理和注解可知

$$\epsilon_\sigma = (-1)^{\sum_{i=1}^{k}(\mathrm{ord}(\tau_i)-1)}. \quad \square$$

例 6.27 确定下列置换的阶数并判定其奇偶性:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 8 & 6 & 10 & 7 & 4 & 5 & 9 & 2 & 1 \end{pmatrix}.$$

解. 计算得 $\pi = (136410)(289)(57)$. 于是

$$\mathrm{ord}(\pi) = \mathrm{lcm}(5, 3, 2) = 30.$$

进而 $\epsilon_\pi = (-1)^{4+2+1} = -1$. 故 π 是奇置换.

引理 6.28 设 $\sigma, \tau \in S_n$. 则 $\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau$.

证明. 注意到两个同号置换之积是偶置换, 而两个异号置换之积是奇置换. □

注解 6.29 反复应用上述定理可知, 对 $\sigma_1, \ldots, \sigma_k \in S_n$,

$$\epsilon_{\sigma_1 \cdots \sigma_k} = \epsilon_{\sigma_1} \cdots \epsilon_{\sigma_k}.$$

记号. 所有 S_n 中偶置换的集合记为 A_n.

命题 6.30 令 A_n 是 S_n 中所有偶置换的集合. 证明: 当 $n > 1$ 时, $\mathrm{card}(A_n) = n!/2$.

证明. 设 B_n 是 S_n 中所有奇置换的集合. 定义:

$$\begin{array}{ccccc} \phi: & A_n & \longrightarrow & B_n \\ & \sigma & \mapsto & (12)\sigma \end{array} \quad \text{和} \quad \begin{array}{ccccc} \psi: & B_n & \longrightarrow & A_n \\ & \tau & \mapsto & (12)\tau \end{array}.$$

由注解 6.29 可知, ϕ 和 ψ 都是良定义的. 注意到:

$$\psi \circ \phi(\sigma) = (12)(12)\sigma = \sigma \quad \text{且} \quad \phi \circ \psi(\tau) = (12)(12)\tau = \tau.$$

故 $\psi \circ \phi = \mathrm{id}_{A_n}$ 且 $\phi \circ \psi = \mathrm{id}_{B_n}$. 由第二讲命题 4.14 可知, ϕ 是双射. 故 $\mathrm{card}(A_n) = \mathrm{card}(B_n)$. 又因为

$$S_n = A_n \cup B_n \quad \text{且} \quad A_n \cap B_n = \emptyset.$$

于是, $\mathrm{card}(A_n) = n!/2$. □

7 整数的算数

7.1 最大公因子和最小公倍数

以下引理是整除的一个基本性质.

引理 7.1 设 $m, n, d \in \mathbb{Z}$ 且 $d \neq 0$. 如果 $d|m$ 且 $d|n$, 则对于任意 $u, v \in \mathbb{Z}$, $d|(um + vn)$.

证明. 设 $a, b \in \mathbb{Z}$ 使得 $m = ad$ 和 $n = bd$. 则

$$um + vn = uad + vbd = (ua + vb)d.$$

于是, $d|(um + vn)$. □

设 $m, n, c \in \mathbb{Z}$ 且 $c \neq 0$. 如果 $c|m$ 且 $c|n$, 则称 c 是 m, n 的公因子. 设 g 是 m, n 的正公因子. 如果任何 m, n 的公因子都整除 g, 则称 g 是 m, n 的最大公因子.

如果 $m = n = 0$, 则 m, n 的最大公因子不存在. 如果 $m \neq 0$ 且 $n = 0$, 则 m, n 的最大公因子是 $|m|$.

下面我们描述两个计算正整数的最大公因子算法–辗转相除（*Euclidean*）算法.

定理 7.2 设 $m, n \in \mathbb{Z}^+$. 则下列算法在有限步内输出正整数 g, 和整数 u, v 使得

(i) g 是 m 和 n 的最大公因子;

(ii) $um + vn = g$.

扩展的辗转相除法(Extended Euclidean Algorithm)

输入: $m, n \in \mathbb{Z}^+$

输出: $g \in \mathbb{Z}^+$, $u, v \in \mathbb{Z}$ 使得 $g = \gcd(m, n)$ 和 $um + vn = g$.

1. *[初始化]* $r_0 \leftarrow m$, $r_1 \leftarrow n$, $i \leftarrow 1$,
   $u_0 \leftarrow 1, v_0 \leftarrow 0$, $u_1 \leftarrow 0, v_1 \leftarrow 1$

2. *[循环]* *while* $r_i \neq 0$ *do*

   (a) $i \leftarrow i + 1$

   (b) $q_i \leftarrow \mathrm{quo}(r_{i-2}, r_{i-1})$, $r_i \leftarrow \mathrm{rem}(r_{i-2}, r_{i-1})$

   (c) $u_i \leftarrow u_{i-2} - q_i u_{i-1}$, $v_i \leftarrow v_{i-2} - q_i v_{i-1}$

   end do

3. *[准备返回]* $g \leftarrow r_{i-1}$, $u \leftarrow u_{i-1}$, $v \leftarrow v_{i-1}$
   return g, u, v

特别地, 最大公因子存在且唯一.

证明. 首先验证该算法在有限步内必然终止. 注意到算法中的循环产生一个关于余数的严格递减序列

$$r_1 > r_2 > \cdots .$$

因为余数都非负, 所以该余数序列有限步必然终止. 此时最后一项一定是零. 由此可知, 算法终止.

设算法终止于 $r_{k+1} = 0$. 则算法输出为 $g = r_k$ 且 $\mathrm{rem}(r_{k-1}, r_k) = 0$. 事实上, 算法产生的商序列

$$q_2, \ldots, q_k, q_{k+1}.$$

两序列之间的关系如下

$$r_{i-2} = q_i r_{i-1} + r_i, \quad i = 2, 3, \ldots, k+1. \tag{2}$$

断言 *1*. 对 $i = 2, 3, \ldots, k$, r_{i-2} 和 r_{i-1} 的公因子是 r_{i-1} 和 r_i 的公因子, 反之亦然.

断言 *1* 证明. 根据 (2), $r_{i-2} = q_i r_{i-1} + r_i$. 引理 7.1 蕴含 r_{i-2}, r_{i-1} 的公因子都是 r_{i-1}, r_i 的公因子, 反之也一样. 断言 1 成立.

下面证明: r_k 是 m 和 n 的最大公因子. 因为 r_k 是 r_{k-1} 和 r_k 的公因子, 所以断言 1 蕴含它是 m 和 n 的公因子. 设 d 是 m 和 n 的公因子. 则断言 1 蕴含 d 是 r_{k-1} 和 r_k 的公因子. 故 $d | r_k$. 由此可知, r_k 是 m, n 的最大公因子.

令 $g = r_k$. 验证 $um + vn = g$.

断言 *2*. 对 $i = 0, 1, \ldots, k$, $u_i m + v_i n = r_i$.

断言 *2* 的证明. 对 i 归纳. $i = 0, 1$ 时, 根据 u_0, v_0, r_0 和 u_1, v_1, r_1 初始值的设定可知,

$$u_0 m + v_0 n = r_0 \quad \text{和} \quad u_1 m + v_1 n = r_1.$$

设 $i > 2$ 且结论对 $2, 3, \ldots, i-1$ 都成立. 由归纳假设可知:

$$u_{i-2} m + v_{i-2} n = r_{i-2} \quad \text{和} \quad u_{i-1} m + v_{i-1} n = r_{i-1}.$$

于是, $q_i u_{i-1} m + q_i v_{i-1} n = q_i r_{i-1}$. 由此得出,

$$(u_{i-2} - q_i u_{i-1})m + (v_{i-2} - q_i v_{i-1})n = r_{i-2} - q_i r_{i-1}.$$

根据扩展 Euclid 算法循环中第 (c) 步和 $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$ 可知: $u_i m + v_i n = r_i$. 断言 2 成立.

取 $i = k$ 得 $u_k m + v_k n = r_k$, 即 $um + vn = g$.

设 g 和 g' 是 m 和 n 的最大公因子. 则 $g|g'$ 和 $g'|g$. 因为 $g, g' \in \mathbb{Z}^+$, 所以 $g = g'$. □

注解 7.3 设 $m, n \in \mathbb{Z}$ 不全为零. 则它们的最大公因子是 $|m|$ 和 $|n|$ 的最大公因子. 记之为 $\gcd(m, n)$.

注解 7.4 如果我们只计算整数的最大公因子, 则在扩展的辗转相除法中无需计算序列 $q_2, q_3, \ldots$, $u_0, u_1, u_2, u_3, \ldots$, 和 $v_0, v_1, v_2, v_3, \ldots$.

例 7.5 计算 $\gcd(95, 57)$.

解. 设 $r_0 = 95, r_1 = 57$. 则

$$\begin{cases} r_2 = \mathrm{rem}(r_0, r_1) = \mathrm{rem}(95, 57) = 38, \\ r_3 = \mathrm{rem}(r_1, r_2) = \mathrm{rem}(57, 38) = 19, \\ r_4 = \mathrm{rem}(r_2, r_3) = \mathrm{rem}(38, 19) = 0. \end{cases}$$

于是, $r_3 = \gcd(95, 57) = 19$.

例 7.6 计算 $u, v \in \mathbb{Z}$ 使得 $u \times 95 + v \times 57 = \gcd(95, 57)$.

解. 设 $r_0 = 95, u_0 = 1, v_0 = 0, r_1 = 57, u_1 = 0, v_1 = 1$. 则

$$\begin{cases} r_2 = \mathrm{rem}(r_0, r_1) = \mathrm{rem}(95, 57) = 38, \\ q_2 = \mathrm{quo}(r_0, r_1) = \mathrm{quo}(95, 57) = 1 \\ u_2 = u_0 - q_2 u_1 = 1,\ v_2 = v_0 - q_2 v_1 = -1 \\ \\ r_3 = \mathrm{rem}(r_1, r_2) = \mathrm{rem}(57, 38) = 19, \\ q_3 = \mathrm{quo}(r_1, r_2) = \mathrm{quo}(57, 38) = 1 \\ u_3 = u_1 - q_3 u_2 = -1,\ v_3 = v_1 - q_3 v_2 = 2 \\ \\ r_4 = \mathrm{rem}(r_2, r_3) = \mathrm{rem}(38, 19) = 0. \end{cases}$$

于是, $\underbrace{(-1)}_{u} \times 95 + \underbrace{2}_{v} \times 57 = 19$.

例 7.7 定理 *7.2* 的另一个证明. 令:

$$S = \{am + bn | a, b \in \mathbb{Z}\}.$$

则 S 中有正整数. 令 g 是 S 中的最小正整数. 则存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = g$.

下面我们验证 $g = \gcd(m, n)$. 设 d 是 m, n 的公因子. 根据上一讲引理 *7.1* 可知 $d | g$. 于是, $d \leq g$.

设 $r = \mathrm{rem}(m, g)$. 则存在 $q \in \mathbb{Z}$ 使得 $m = qg + r$. 故

$$qum + qvn = qg \ \Rightarrow\ qum + qvn = m - r \ \Rightarrow\ (1 - qu)m + (-qv)n = r.$$

由 g 的极小性和 $r \in \{0, 1, \ldots, g-1\}$ 可知, $r = 0$. 故 $g|m$. 同理 $g|n$. □

定义 7.8 设 $m, n \in \mathbb{Z}$. 如果 $\gcd(m, n) = 1$, 则称 m 和 n 互素.

定理 7.9 设 $m, n \in \mathbb{Z}$ 不全为零. 则 m, n 互素当且仅当存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$.

证明. 设 m, n 互素. 则 $\gcd(m, n) = 1$. 由定理 7.9 可知, 存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$. 反之, 设存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$ 和 $g = \gcd(m, n)$. 因为 $g|m$ 和 $g|n$, 所以 $g|1$ (上一讲引理 7.1). 故 $g = 1$. □

设 $m, n \in \mathbb{Z}^+$ 且 $h \in \mathbb{Z}$. 如果 $m|h$ 且 $n|h$, 则称 h 是 m 和 n 的公倍数. 设 $\ell \in \mathbb{Z}^+$ 是 m 和 n 的公倍数. 如果对 m 和 n 的公倍数 h 都有 $\ell|h$, 则称 ℓ 是 m 和 n 的最小公倍数.

注解 7.10 最小公倍数存在且唯一. 验证如下:

显然, mn 是 m 和 n 的正公倍数. 设 ℓ 是 m 和 n 的正公倍式中最小者. 对于 m 和 n 的任意公倍数 h, 我们有

$$h = \mathrm{quo}(h, \ell)\ell + \mathrm{rem}(h, \ell).$$

则 $m|\mathrm{rem}(h, \ell)$ 和 $n|\mathrm{rem}(h, \ell)$ *(引理 7.1)*. 由 ℓ 的极小性可知, $\mathrm{rem}(h, \ell)$ 等于 0. 故 ℓ 是最小公倍数.

由整除性可知, 最小公倍数唯一.

记非零整数 m 和 n 的最小公倍数为 $\mathrm{lcm}(m,n)$.

命题 7.11 设 $m,n\in\mathbb{Z}^+$. 则

$$\mathrm{lcm}(m,n)=\frac{mn}{\gcd(m,n)}.$$

证明. 断言. 设 $a,b\in\mathbb{Z}^+$ 互素满足 $an=bm$. 则 an 是 m,n 的最小公倍数.

断言的证明. 设 $\ell=an$. 则 $\ell=bm$. 故 ℓ 是 m,n 的公倍数. 再设 s 是 m,n 的另一个公倍数. 则存在整数 a',b' 使得 $s=a'n=b'm$. 因为 a,b 互素, 所以定理 7.9 蕴含存在 $u,v\in\mathbb{Z}$ 使得

$$\begin{aligned}ua+vb=1 &\Longrightarrow uas+vbs=s\\ &\Longrightarrow ua'an+vb'bm=s \quad (\because a'n=b'm=s)\\ &\Longrightarrow \ell(ua'+vb')=s \quad (\because an=bm=\ell)\\ &\Longrightarrow \ell|s.\end{aligned}$$

于是, ℓ 是最小公倍数. 断言成立.

设 $g=\gcd(m,n)$. 则存在正整数 p,q 使得 $m=pg$ 和 $n=qg$. 因为存在 $s,t\in\mathbb{Z}$ 使得 $sm+tn=g$, 所以

$$spg+tqg=g\Longrightarrow sp+tq=1.$$

由此可知, $sp+tq=1$. 根据定理 7.9, $\gcd(p,q)=1$. 而

$$\frac{mn}{g}=pqg=pn=qm.$$

由断言可知, mn/g 是最小公倍数. □

7.2 素数

定义 7.12 设 p 是大于 1 的整数. 如果 p 不能写成两个大于 1 的整数之积, 则称 p 是素数*(prime).*

例 7.13 证明*:* 任何大于 1 的整数都是有限个素数之积.

证明. 设 n 是大于 1 的整数. 我们对 n 归纳. 当 $n = 2$ 时显然. 设 $n > 2$ 且结论对大于 1 且 小于 n 的整数都成立. 如果 n 是素数, 则结论显然成立. 否则存在两个大于 1 且小于 n 的整数 i, j 使得 $n = ij$, 由归纳假设, i 和 j 都是素数的乘积. 故 n 也是. □

素数包括: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

例 7.14

$$24 = 2^3 \times 3, \quad 10969629647 = 104729 \times 104743.$$

例 7.15 证明*:* 素数有无穷多个.

证明. 假设素数只有有限个*:* $p_1, \ldots, p_k$. 令 $n = p_1 \cdots p_k + 1$. 由上例可知, 存在某个素数整除 n. 不妨设该素数是 p_1. 根据第一章第四讲引理 *7.1*, $p_1|1$, 矛盾. □

引理 7.16 设 p 是素数, $a, b \in \mathbb{Z}$. 如果 $p|(ab)$, 则 $p|a$ 或 $p|b$.

证明. 设 $p \nmid a$. 则 $\gcd(p, a) = 1$. 由定理 7.9 可知, 存在 $u, v \in \mathbb{Z}$ 使得 $up + va = 1$. 于是, $upb + v(ab) = b$. 根据上一讲引理 7.1, $p|b$. □

例 7.17 设 p 是素数, k 是小于 p 的正整数. 证明:

$$p|\binom{p}{k}.$$

证明. 由 $\binom{p}{k}=\frac{p!}{k!(p-k)!}$ 可知 $p!=\binom{p}{k}k!(p-k)!$. 两次应用上述引理可知, $p|\binom{p}{k}$ 或 $p|k!$ 或 $p|(p-k)!$. 反复应用上述引理得出: $p|\binom{p}{k}$ 或 $p|i$ 或 $p|j$, 其中 $1\leq i\leq k$ 和 $1\leq j\leq p-k$. 因为后两种情形不可能发生, 所以 $p|\binom{p}{k}$. □