第五周习题课

李文桥

2023 年 10 月 20 日

1 置换的奇偶性

回忆: 置换的奇偶性

- 任何置换都能写成若干个不相交循环的乘积.
- 任何置换都能写成若干个对换的乘积, 且个数的奇偶性唯一.
- 定义奇置换与偶置换: 如果置换 σ 可以写成奇数个对换的乘积, 则称 σ 为奇置换, 否则称为偶置换. 定义置换 σ 的符号 ϵ_σ :

$$\epsilon_\sigma = \begin{cases} 1, & \text{如果 } \sigma \text{ 为偶置换;} \\ -1, & \text{如果 } \sigma \text{ 为奇置换.} \end{cases}$$

- $\epsilon_{\sigma\tau} = \epsilon_\sigma \epsilon_\tau$.
- 设 $\sigma = (i_1 i_2 \cdots i_l)$ 是一个循环, 则 $\mathrm{ord}(\sigma) = l$, $\epsilon_\sigma = (-1)^{l-1}$.
- 设置换 σ 的不相交循环分解为 $\sigma = \tau_1 \tau_2 \cdots \tau_k$, 则:

$$\epsilon_\sigma = (-1)^{\sum\limits_{i=1}^{k}(\mathrm{ord}(\tau_i)-1)}.$$

- 单位置换(即恒同) e 是偶置换.

习题1: (a) 题给置换即为 $(125)(368)(47)$, 是 2 个偶置换与 1 个奇置换的乘积, 故为奇置换;

(b) 题给置换是 1012 个对换的乘积, 故为偶置换;

(c) 题给置换是 1 个奇置换与 1 个偶置换的乘积, 故为奇置换.

习题2: (a) 我们给出两种证明:

法1: 设 σ 的不相交循环分解为 $\sigma = \tau_1 \tau_2 \cdots \tau_k$, 并设 τ_i 的阶为 $l_i, i = 1, 2, \cdots, k$. 则:

$$\mathrm{ord}(\sigma) = \mathrm{lcm}(l_1, l_2, \cdots, l_k).$$

由于 $\mathrm{ord}(\sigma)$ 为奇数, 故 $\mathrm{lcm}(l_1, l_2, \cdots, l_k)$ 为奇数, 从而 l_i 为奇数, $i = 1, 2, \cdots, k$. 则 $\sum\limits_{i=1}^{k}(l_i - 1)$ 为偶数, 从而 $\epsilon_\sigma = (-1)^{\sum\limits_{i=1}^{k}(l_i-1)} = 1$, σ 为偶置换.

法2: 设 $\mathrm{ord}(\sigma) = m$, 则 $\sigma^m = e$ 为偶置换, 由 m 为奇数知 σ 只能是偶置换.

(b) 不一定. 比如 $(12)(34)$ 的阶为 2, 但它是偶置换.

习题3: (a) 验证等式两端的置换作用在任何一个正整数 s 上相等即可. 注意 s 可能不属于 $\{i,j,k,l\}$.

(b) 设 σ 为偶置换, 则根据定义, σ 可写为偶数个对换的乘积, 根据置换乘积的结合律, 我们只需证明任意两个对换的乘积可写为一些三轮换的乘积即可. 设 $(ij),(kl)$ 为两个对换, $i \neq j$, $k \neq l$. 则有如下三种情况:

1. i,j,k,l 互不相同. 此时, 根据 (a) 中公式, $(ij)(kl) = (ikj)(ikl)$ 可写成两个三轮换的乘积;
2. $\{i,j\}$ 和 $\{k,l\}$ 有一个元素相同, 不妨设 $i = k$, 则根据 (a) 中公式, $(ij)(kl) = (kj)(kl) = (jk)(kl) = (jkl)$ 是一个三轮换;
3. $\{i,j\} = \{k,l\}$. 此时 $(ij)(kl) = (ij)(ij) = e = (123)^3$ 仍能写成一些三轮换的乘积.

从而命题得证.

补充: 关于置换的表示.

引理 1.1 *对任意互不相同的正整数 i,j,k, $(ij) = (ik)(jk)(ik)$.*

证明. 直接验证, 或者

$$(ij) = (ij)(ik)(ik) = (ji)(ik)(ik) = (jik)(ik) = (ki)(kj)(ik).$$

□

定理 1.2 *设 S_n 是 n 元置换全体构成的集合, 则以下结论成立:*

(1) S_n 中的置换都可写成 $(12),(13),\cdots,(1n)$ 的乘积;

(2) S_n 中的置换都可写成 $(12),(23),\cdots,(\underline{n-1}\,n)$ 的乘积;

(3) S_n 中的置换都可写成 $(12),(12\cdots n)$ 的乘积;

证明: 关于(1): 由于 S_n 中的置换都能写成一些对换的乘积, 所以只需证明任何一个对换可以写成 $(12),(13),\cdots,(1n)$ 的乘积. 任取对换 (ij), $i,i \in \{1,2,\cdots,n\}$, 并不妨设 i,j 都不是 1, 则由前引理:

$$(ij) = (1i)(1j)(1i)$$

从而命题成立.

关于(2): 只要证明 $(12),(13),\cdots,(1n)$ 都可以写成 $(12),(23),\cdots,(\underline{n-1}\,n)$. (12) 当然满足上述命题, 我们对 k 归纳证明 $(1k)$ 均满足命题. 假设 $k-1$ 时命题成立, 即 $(1\,\underline{k-1})$ 可以写为 $(12),(23),\cdots,(\underline{n-1}\,n)$ 的乘积, 则由引理:

$$(1k) = (1\,\underline{k-1})(k\,\underline{k-1})(1\,\underline{k-1}).$$

从而 $(1k)$ 可以写成 $(12),(23),\cdots,(\underline{n-1}\,n)$ 的乘积. 命题得证.

关于(3): 只需注意到: 若设 $\tau = (12\cdots n)$, 则:

$$\tau(\underline{i-1}\,i)\tau^{-1} = (i\,\underline{i+1}) \text{ 且 } \tau^{-1} = \tau^{n-1},$$

从而 $(12),(23),\cdots,(\underline{n-1}\,n)$ 均可写成 $(12),\tau$ 的乘积. □

2 辗转相除法

习题4: (a) 如下表所示.

i	q_i	r_i	u_i	v_i
0	-	62	1	0
1	-	51	0	1
2	1	11	1	-1
3	4	7	-4	5
4	1	4	5	-6
5	1	3	-9	11
6	1	1	14	-17

(b) 根据(a), $-17\times 51+14\times 62=1$, 则$-17m\times 51+14m\times 62=m$. $-17m, 14m$ 满足要求.

补充: 给定正整数 a, b, m, 形如 $ua+vb=m$ 的方程的整数解.

引理 2.1 设 a, b, c 为整数, 且 a, b 互素. 则 $a\mid bc \Rightarrow a\mid c$.

证明: 存在整数 u, v 使得 $ua+vb=1$. 则$uac+vbc=c$, 由 $a\mid bc$ 知 $a\mid c$. □

先假设 $\gcd(a,b)=1$, 则根据习题 4, 可以用辗转相除法求出一组解, 记为 (u_0, v_0). 如果 (u_1, v_1) 是方程的整数解, 则:

$$u_0a+v_0b=m; \tag{1}$$

$$u_1a+v_1b=m. \tag{2}$$

两式作差:

$$(u_0-u_1)a=(v_1-v_0)b.$$

则由引理 (2.1) 知 $a\mid(v_1-v_0)$, $b\mid(u_0-u_1)$. 所以存在整数 s, t, 满足:

$$u_1=u_0+sb;$$

$$v_1=v_0+ta.$$

代入 (2), 结合 (1) 可得:

$$0=(s+t)ab.$$

从而 $s+t=0$, u_1, v_1 具有形式:

$$u_1=u_0+sb;$$

$$v_1=v_0-sa.$$

其中 s 为整数. 反之, 若存在整数 s, 使得 u_1, v_1 具有上述形式, 则容易验证 u_1, v_1 是方程 $ua+vb=m$ 的解. 所以方程的全体整数解为:

$$\{(u_0+sb, v_0-sa)\mid s\in\mathbb{Z}\}.$$

一般地, 若 $\gcd(a,b)=d>1$, 则方程有整数解 $\Rightarrow\ d\,|\,m$. 此时可将方程两边同除 m, 方程化为:

$$u(\frac{a}{d})+v(\frac{b}{d})=\frac{m}{d},$$

并且 $\gcd(\frac{a}{d},\frac{b}{d})=1$(见习题5中的引理(2.3)). 这样就转化为先前讨论的情形.

习题5: 我们在课上定义的最大公因子: 设 m,n 为整数, 若 d 为 m,n 的正公因子, 且任意的 m,n 的公因子 d', 有 $d'\,|\,d$, 则称 d 为 m,n 的最大公因子. 从定义可以看出: d 是 m,n 的最大的公因子. 而本题在定义多个正整数的最大公因子时, 只是取了 $a_1,\cdots,a_n$ 的最大的公因子, 没有要求其它公因子整除这个最大的公因子. 所以要想严格地完成本题的证明, 我们首先需要让本题所给出的定义与课上的定义一致起来.

下面仍然记 $a_1,a_2,\cdots,a_n$ 的最大的公因子为 $\gcd(a_1,a_2,\cdots a_n)$. 最终的目标是证明如下定理:

定理 2.2 设 $d=\gcd(a_1,a_2,\cdots,a_n)$, 则对于任何一个 $a_1,\cdots,a_n$ 的公因子 d', 都有 $d'\,|\,d$.

在证明之前, 我们需要一个引理:

引理 2.3 设 $d=\gcd(a_1,a_2,\cdots,a_n)$, 并设 $a_i=b_id,\ i=1,2,\cdots,n$. 则 $\gcd(b_1,b_2,\cdots,b_n)=1$.

证明: 记 $u=\gcd(b_1,b_2,\cdots,b_n)$, 且 $b_i=c_iu,\ i=1,2,\cdots,n$.则 $a_i=c_iud,\ i=1,2,\cdots,n$. 则 ud 为 $a_1,\cdots,a_n$ 的一个公因子. 根据 d 的最大性知 $u=1$. □

定理的证明: 设 $a_i=b_id$, 则 $\gcd(b_1,b_2,\cdots,b_n)=1$. 任取 d' 为 $a_1,\cdots,a_n$ 的一个正公因子, 令 d 对 d' 做带余除法: $d=qd'+r,\ q,r\in\mathbb{Z},\ 0\le r<d'$. 则有:

$$a_i=b_iqd'+b_ir,\ \ i=1,\cdots,n.$$

从而 $d'\,|\,b_ir,\ i=1,\cdots,n$. 令 $c_i=\gcd(b_i,d')<b_i$.

如果对任意的$i=1,\cdots,n,\ c_i=b_i$, 则 $d'\,|\,b_i,\ i=1,\cdots,n$, 因而是 $b_1,\cdots,b_n$ 的公因子. 由 $\gcd(b_1,b_2,\cdots,b_n)=1$ 知 $d'=1$.

如果存在 $i_0\in\{1,2,\cdots,n\}$, 使得 $c_{i_0}<b_{i_0}$. 由引理 (2.3) 知 $\gcd(\frac{b_i}{c_i},\frac{d'}{c_i})=1$, 且由 $d'\,|\,b_ir$ 可得 $\frac{d'}{c_i}\,|\,\frac{b_i}{c_i}r$. 再由引理 (2.1) 知 $\frac{d'}{c_i}\,|\,r$, 从而 $d'\,|\,c_ir,\ i=1,2,\cdots,n$. 我们可以令 $e_i=\gcd(c_i,d')$, 重复以上过程, 就会得到: $d'=1$ 或者存在 $i_1\in\{1,2,\cdots,n\}$ 使得 $e_{i_1}<c_{i_1}$, 且$d'\,|\,e_ir,\ i=1,2,\cdots,n$.

$$\cdots\cdots$$

如此, 如果 $d'\neq 1$, 则以上过程会在有限步后终止, 即会存在某个指标 $i_N\in\{1,2,\cdots,n\}$, 使得序列 $b_{i_N}\ge c_{i_N}\ge e_{i_N}\ge\cdots$ 最终递降为 $\eta_{i_N}=1$. 那么就有 $d'\,|\,\eta_{i_N}r=r$. 而 $0\le r<d'$, 所以只能是 $r=0,\ d'\,|\,d$. □

接下来证明原题:

(a) 记 $d=\gcd(a_1,a_2,\cdots,a_n)$, $h=\gcd(\gcd(a_1,a_2,\cdots,a_{n-1}),a_n)$. 首先由 $h\,|\,\gcd(a_1,a_2,\cdots,a_{n-1})$ 知 $h\,|\,a_i,\ i=1,2,\cdots,n-1$. 并且 $h\,|\,a_n$. 从而 h 为 $a_1,a_2,\cdots,a_n$ 的一个公因子, 从而 $h\,|\,d$.
另一方面, 由于 $d\,|\,a_i,\ i=1,2,\cdots,n$, 从而是 $a_1,\cdots,a_{n-1}$ 的一个公因子, $d\,|\,\gcd(a_1,a_2,\cdots,a_{n-1})$, 进而 $d\,|\,h$.

(b) 我们给出两种方法.

法1. 对 n 进行归纳. $n=2$ 时已经成立. 设 $n-1$ 时成立, 则存在整数 $v_1, v_2, \cdots, v_{n-1}$ 使得:

$$v_1a_1 + v_2a_2 + \cdots + v_{n-1}a_{n-1} = \gcd(a_1, a_2, \cdots, a_{n-1}).$$

而根据 (a), 我们有:

$$\begin{aligned}\gcd(a_1, a_2, \cdots, a_n) =& \gcd(\gcd(a_1, a_2, \cdots, a_{n-1}), a_n)\\ =& \gcd(v_1a_1 + v_2a_2 + \cdots + v_{n-1}a_{n-1}, a_n).\end{aligned}$$

根据 $n=2$ 的情形, 存在整数 v_n, u_n 使得:

$$\begin{aligned}v_n(v_1a_1 + v_2a_2 + \cdots + v_{n-1}a_{n-1}) + u_na_n =& \gcd(v_1a_1 + v_2a_2 + \cdots + v_{n-1}a_{n-1}, a_n)\\ =& \gcd(a_1, a_2, \cdots, a_n).\end{aligned}$$

令 $u_i = v_nv_i$, $i = 1, 2, \cdots, n-1$, 命题得证.

法2. 设集合 $S = \{v_1a_1 + v_2a_2 + \cdots + v_na_n \,|\, v_i \in \mathbb{Z},\ i = 1, 2, \cdots, n\}$, 则 S 包含一个最小的正整数, 将其记为 L, 并设 $L = u_1a_1 + \cdots + u_na_n$. 首先证明 L 是 $a_1, \cdots, a_n$ 的公因子.

令 a_1 对 L 作带余除法, 则存在 $q, r \in \mathbb{Z}$, $0 \le r < L$, 使得 $a_1 = qL + r$. 则:

$$a_1 = qu_1a_1 + \cdots + qu_na_n + r.$$

从而:

$$r = (1 - qu_1)a_1 - qu_2a_2 - \cdots - qu_na_n.$$

则 $r \in S$ 且小于 L, 所以只能为 0. 从而 $L \,|\, a_1$. 同理可证 $L \,|\, a_i$, $i = 2, \cdots, n$, L 为 $a_1, \cdots, a_n$ 的公因子.

此外, 任取 $a_1, \cdots, a_n$ 的公因子 g, 易见 $g \,|\, L$. 这说明 L 是 $a_1, a_2, \cdots, a_n$ 的最大公因子. $\square$