# 第四次作业

先复习置换的一些性质：

1. $(i_1 i_2 \cdots i_k)$：长度为 $k$ 的循环.

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

2. $\forall \sigma \in S_n \setminus \{e\}$，$\sigma$ 是有限个两两互不相交的长度大于 1 的循环之积.

设 $\sigma = \tau_1 \cdots \tau_m$，$\tau_i$ 互不相交的循环

则 $ord(\sigma) = lcm(ord(\tau_1), \cdots, ord(\tau_m)) = lcm(l_1, \cdots, l_m)$. $l_i$ 是 $\tau_i$ 的长度.

$\sigma^{-1} = \tau_m^{-1} \cdots \tau_1^{-1}$

3. 奇偶置换

$(i_1 i_2 \cdots i_k) = \underbrace{(i_k i_{k-1}) \cdots (i_k i_2)(i_k i_1)}$. 长度为 $k$ 的循环可分解成 $k-1$ 个对换之积

分解不唯一，~~但奇偶~~

$\forall \sigma \in S_n$，$\sigma = \lambda_1 \cdots \lambda_k = \mu_1 \cdots \mu_m$，$\lambda_i, \mu_j$ 对换. $k$ 和 $m$ 的奇偶性相同.

如果 $\sigma$ 可以写成奇数个对换之积，则称 $\sigma$ 为奇置换，否则称为偶置换.

置换 $\sigma$ 的符号：$\varepsilon_\sigma = (-1)^k = (-1)^m = \begin{cases} 1, & \text{偶置换} \\ -1, & \text{奇置换} \end{cases}$.

性质：$\forall \sigma, \tau \in S_n$，则 $\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau$

$\forall \sigma_1, \cdots, \sigma_m \in S_n$，则 $\varepsilon_{\sigma_1 \cdots \sigma_m} = \varepsilon_{\sigma_1} \varepsilon_{\sigma_2 \cdots \sigma_m} = \varepsilon_{\sigma_1} \varepsilon_{\sigma_2} \varepsilon_{\sigma_3 \cdots \sigma_m} = \varepsilon_{\sigma_1} \varepsilon_{\sigma_2} \cdots \varepsilon_{\sigma_m}$

以下是作业：

1. 求置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 1 & 6 & 4 & 8 & 7 \end{pmatrix}$ 互不相交的循环分解，阶数和置换符号.

$\sigma = \underbrace{(132564)}_{\tau_1} \underbrace{(78)}_{\tau_2} = (46)(45)(42)(43)(41)(78)$

$ord(\tau_1) = 6$，$ord(\tau_2) = 2 \Rightarrow ord(\sigma) = lcm(ord(\tau_1), ord(\tau_2)) = lcm(6, 2) = 6$

$\tau_1$ 可以分解成 $6-1$ 对换的乘积，$\tau_2$ 可以分解成 $2-1$ 对换的乘积

$\therefore \varepsilon_\sigma = \varepsilon_{\tau_1} \varepsilon_{\tau_2} = (-1)^{6-1} \cdot (-1)^{2-1} = (-1)^{5+1} = 1$.

2. 设 $S_n$ 中置换的互不相交的循环分解为 $\pi=\pi_1\pi_2\cdots\pi_m$，其中 $\pi_k$ 长度为 $l_k$. 令 $m'=n-\sum_{k=1}^{m} l_k$，则 $\pi$ 使集合 $\{1,2,\cdots,n\}$ 中 $m'$ 个元素保持不动. 证明 $\varepsilon_\pi=(-1)^{n-(m+m')}$

证：$\varepsilon_\pi=\varepsilon_{\pi_1}\varepsilon_{\pi_2}\cdots\varepsilon_{\pi_m}=(-1)^{l_1-1}(-1)^{l_2-1}\cdots(-1)^{l_m-1}=(-1)^{\sum_{k=1}^{m}(l_k-1)}$.

其中 $\sum_{k=1}^{m}(l_k-1)=\sum_{k=1}^{m}l_k-m=(n-m')-m=n-(m+m')\Rightarrow\varepsilon_\pi=(-1)^{n-(m+m')}$

3. 设 $a_1,\cdots,a_n\in\mathbb{Z}$，不全为0，$g=\gcd(a_1,\cdots,a_n)$. 证明：$\exists u_1,\cdots,u_n\in\mathbb{Z}$ s.t.

$$a_1u_1+\cdots+a_nu_n=g.$$

证明：方法一（归纳法）.

先证 $\gcd(a_1,\cdots,a_k,a_{k+1})=\gcd(\gcd(a_1,\cdots,a_k),a_{k+1})$，$1\le k\le n-1$.

令 $g_1=\gcd(a_1,\cdots,a_k,a_{k+1})$，$g_2=\gcd(\gcd(a_1,\cdots,a_k),a_{k+1})$ 下证 $g_1=g_2$.

一方面：$\because g_1\mid a_1,\cdots,g_1\mid a_k$. $\therefore g_1$ 是 $a_1,\cdots,a_k$ 的公因子 $\therefore g_1\mid\gcd(a_1,\cdots,a_k)$

又因为 $g_1\mid a_{k+1}$，$\therefore g_1\mid\gcd(\gcd(a_1,\cdots,a_k),a_{k+1})$ i.e. $g_1\mid g_2$.

另一方面：$\because g_2\mid\gcd(a_1,\cdots,a_k)$，$g_2\mid a_{k+1}$ $\therefore g_2\mid a_1,\cdots,g_2\mid a_k$，$g_2\mid a_{k+1}$

$\therefore g_2\mid\gcd(a_1,\cdots,a_k,a_{k+1})$ i.e. $g_2\mid g_1$.

综上 $g_1=g_2$.

归纳法：

$n=2$. $\exists u_1,u_2\in\mathbb{Z}$ s.t. $u_1a_1+u_2a_2=g$.

假设 $n=k$ 时成立.

当 $n=k+1$. $g=\gcd(a_1,\cdots,a_k,a_{k+1})=\gcd(\gcd(a_1,\cdots,a_k),a_{k+1})$.

记 $d=\gcd(a_1,\cdots,a_k)$. 由归纳假设 $\exists v_1,\cdots,v_k\in\mathbb{Z}$ s.t.

$$d=v_1a_1+\cdots+v_ka_k$$

$\because g=\gcd(d,a_{k+1})$，已知 $\exists\alpha,\beta\in\mathbb{Z}$，s.t. $\alpha d+\beta a_{k+1}=g$. 即

$$g=\alpha(v_1a_1+\cdots+v_ka_k)+\beta a_{k+1}$$
$$=\alpha v_1a_1+\cdots+\alpha v_ka_k+\beta a_{k+1}$$

取 $u_1=\alpha v_1,\cdots,u_k=\alpha v_k$，$u_{k+1}=\beta$，有 $u_1a_1+\cdots+u_{k+1}a_{k+1}=g$.

方法二：令 $S=\{u_1a_1+\cdots+u_na_n \mid u_i\in\mathbb{Z}\}$，则 $S$ 中有正整数，令 $g$ 是 $S$ 中的最小正整数，则 $\exists u_1,\cdots,u_n\in\mathbb{Z}$ s.t. $u_1a_1+\cdots+u_na_n=g$.

下证 $g=\gcd(a_1,\cdots,a_n)$.

设 $d$ 是 $a_1,\cdots,a_n$ 的公因子，由 $d\mid a_1,\cdots,d\mid a_n$ 可得 $d\mid g$.

设 $a_1=q_1g+r_1$，$r_1\in\{0,1,\cdots,g-1\}$

由 $q_1u_1a_1+\cdots+q_1u_na_n=q_1g=a_1-r_1$

得 $r_1=(1-q_1u_1)a_1+(-q_1u_2)a_2+\cdots+(-q_1u_n)a_n$

由 $g$ 的极小性和 $r_1\in\{0,1,\cdots,g-1\}$ 可知 $r_1=0$，故 $g\mid a_1$，同理可得 $g\mid a_2,\cdots,g\mid a_n$，即 $g$ 是 $a_1,\cdots,a_n$ 的公因子，因此 $g=\gcd(a_1,\cdots,a_n)$.

注：(1) 如何证 $d=\gcd(a,b)$.

方法一：只需证 (i) $d$ 是 $a,b$ 的公因子，即 $d\mid a, d\mid b$.

(ii) 对任意的 $a,b$ 的公因子 $c$，都有 $c\mid d$

方法二：$a=n_1d$，$b=n_2d$，若 $\gcd(n_1,n_2)=1$，则 $d=\gcd(a,b)$.

(2) 若 $d=\gcd(a,b)$，则 $\exists u,v\in\mathbb{Z}$ s.t. $ua+vb=d$.

注意此命题反过来不对，即 $\exists u,v\in\mathbb{Z}$ s.t. $ua+vb=d \not\Longrightarrow d=\gcd(a,b)$.

例：$a=3$，$b=2$，$\gcd(a,b)=1$.

$u=2$，$v=2$，$ua+vb=2\times3+2\times2=10$.

但如果 $d$ 是 $a,b$ 的公因子，且 $\exists u,v\in\mathbb{Z}$ s.t. $ua+vb=d \Longrightarrow d=\gcd(a,b)$

(可验证 $\forall c\mid a, c\mid b \Rightarrow c\mid d$)

4. 求 161, 253 的 gcd, lcm. 并计算 $u, v$ s.t. $161u + 253v = \gcd(161, 253)$.

解：$r_0 = 253$, $u_0 = 1$, $v_0 = 0$, $r_1 = 161$, $u_1 = 0$, $v_1 = 1$

$r_2 = \text{rem}(r_0, r_1) = \text{rem}(253, 161) = q_2$

$q_2 = \text{quo}(r_0, r_1) = \text{quo}(253, 161) = 1$.

$u_2 = u_0 - q_2 u_1 = 1$, $v_2 = v_0 - q_2 v_1 = -1$

$r_3 = \text{rem}(r_1, r_2) = \text{rem}(161, q_2) = 69$

$q_3 = \text{quo}(r_1, r_2) = \text{quo}(161, q_2) = 1$.

$u_3 = u_1 - q_3 u_2 = -1$. $v_3 = v_1 - q_3 v_2 = 2$

$r_4 = \text{rem}(r_2, r_3) = \text{rem}(92, 69) = 23$

$q_4 = \text{quo}(r_2, r_3) = \text{quo}(92, 69) = 1$

$u_4 = u_2 - q_4 u_3 = 2$. $v_4 = v_2 - q_4 v_3 = -3$

$r_5 = \text{rem}(r_3, r_4) = \text{rem}(69, 23) = 0$

$\Rightarrow \gcd(253, 161) = r_4 = 23$ 且 $2 \times 253 - 3 \times 161 = 23$ 即 $\begin{cases} u = -3 \\ v = 2 \end{cases}$

$\text{lcm}(253, 161) = \frac{253 \times 161}{23} = 1771 = 161 \times 11 = 253 \times 7$

注：$(2 + 7k) \times 253 + (-3 - 11k) \times 161 = 2 \times 253 - 3 \times 161 = 23$, $k \in \mathbb{Z}$

即 $\begin{cases} v = 2 + 7k \\ u = -3 - 11k \end{cases}$, $k \in \mathbb{Z}$ 都可以.

5、$a,b,m,r\in\mathbb{Z}^+$，说明：若 $b=am+r$，则 $gcd(a,b)=gcd(a,r)$

说明：方法一：

令 $g_1=gcd(a,b)$，$g_2=gcd(a,r)$，下证 $g_1=g_2$。

$\because g_1|a,\ g_1|b\ \therefore g_1|b-am$，即 $g_1|r$，所以 $g_1$ 是 $a,r$ 的公因子 $\Rightarrow g_1|g_2$

$\because g_2|a,\ g_2|r\ \therefore g_2|am+r$ 即 $g_2|b$，所以 $g_2$ 是 $a,b$ 的公因子 $\Rightarrow g_2|g_1$

因此 $g_1=g_2$

方法二：令 $g=gcd(a,b)$，设 $g=gcd(a,r)$。

$\because g|a,\ g|b\ \therefore g|b-am$ 即 $g|r$，$\therefore g$ 是 $a,r$ 的公因子。

$\forall d$ 是 $a,r$ 的公因子，$d|a,\ d|r\Rightarrow d|ma+r$ 即 $d|b\ \therefore d$ 是 $a,b$ 的公因子。

因此 $d|g\Rightarrow g=gcd(a,r)$

方法三：令 $g=gcd(a,r)$，设 $a=n_1g$，$r=n_2g$，其中 $gcd(n_1,n_2)=1$。

则 $b=am+r=n_1gm+n_2g=(n_1m+n_2)g$。

由于 ~~所以~~ $gcd(n_1m+n_2,n_1)=1$（~~否则~~：若 $d|n_1m+n_2,\ d|n_1\Rightarrow d|n_2$，即 $d$ 是 $n_1,n_2$ 的公因子，$\because gcd(n_1,n_2)=1,\ \therefore d=1$）

所以 $gcd(a,b)=g$

方法四：用辗转相除法看。

$r_0=b,\ r_1=a,\ r_2=r$。

求 $gcd(r_0,r_1)$：
$$\left.\begin{cases} r_0=q_2r_1+r_2 \\ r_1=q_3r_2+r_3 \\ \vdots \\ r_{k-2}=q_kr_{k-1}+r_k \\ r_{k-1}=q_{k+1}r_k \end{cases}\right\}\text{求 } gcd(r_1,r_2)$$

因此 $gcd(r_0,r_1)=gcd(r_1,r_2)=r_k$，即 $gcd(b,a)=gcd(a,r)$

其实 $gcd(r_0,r_1)=gcd(r_1,r_2)=gcd(r_2,r_3)=\cdots=gcd(r_{k-1},r_k)=r_k$

6. 证明以下结论（下面字母表示正整数）

(1) $\gcd(ma,mb)=m\gcd(a,b)$

(2) 若 $\gcd(a,b)=1$，则 $\gcd(ab,m)=\gcd(a,m)\gcd(b,m)$.

证：(1)

方法一：设 $g=\gcd(a,b)$. $a=n_1g$, $b=n_2g$. 其中 $\gcd(n_1,n_2)=1$.

则 $ma=n_1mg$, $mb=n_2mg$. $\Rightarrow \gcd(ma,mb)=mg=m\gcd(a,b)$

方法二：设 $g=\gcd(a,b)$. $\because g|a$, $g|b$ $\therefore mg|ma$, $mg|mb$.

即 $mg$ 是 $ma$, $mb$ 的公因子.

$\exists u,v\in\mathbb{Z}$ s.t. $ua+vb=g \Rightarrow uma+vmb=mg$.

任取 $ma$, $mb$ 的公因子 $d$. $d|ma$. $d|mb \Rightarrow d|mg$.

$\therefore mg=\gcd(ma,mb)$

(2). 设 $g=\gcd(ab,m)$, $g_1=\gcd(a,m)$, $g_2=\gcd(b,m)$ 下证 $g=g_1g_2$

一方面，$g_1|a$, $g_2|b \Rightarrow g_1g_2|ab$.

$\because \gcd(a,b)=1$ $\therefore \gcd(g_1,g_2)=1$.

$\therefore g_1|m$, $g_2|m \Rightarrow g_1g_2|m$.

即 $g_1g_2$ 是 $ab$, $m$ 的公因子，所以 $g_1g_2|g$.

另一方面，$\exists u_1,u_2,v_1,v_2\in\mathbb{Z}$ s.t. $u_1a+v_1m=g_1$, $u_2b+v_2m=g_2$

$\therefore g_1g_2=u_1u_2ab+(v_1v_2m+v_1u_2b+u_1v_2a)m$

$\because g|ab$, $g|m$ $\therefore g|g_1g_2$.

因此 $g=g_1g_2$

注：① $g_1|m$, $g_2|m \xrightarrow{\gcd(g_1,g_2)=1} g_1g_2|m$. 例：$6|12$, $4|12$ 但 $24\nmid 12$

② 若 $\gcd(a,b)\neq 1$，则 (2) 中等式不一定成立.

例：$a=2$, $b=4$, $m=6$, $\gcd(ab,m)=\gcd(8,6)=2$, $\gcd(a,m)\gcd(b,m)=2\times 2=4$