近世代数 (H) 第十二周作业

涂嘉乐 PB23151786

2025 年 5 月 16 日

Exercise 1 $G \curvearrowright X$ 给出群同态 $\rho : G \to S(X)$, 证明 $\mathrm{Ker}\rho = \bigcap_{x\in X} G_x$

Proof

$$\begin{aligned} g \in \mathrm{Ker}\rho &\iff \rho(g) = \mathrm{Id}_X \\ &\iff \forall x \in X, \rho(g)(x) = x \\ &\iff \forall x \in X, g.x = x \\ &\iff \forall x \in X, g \in G_x \\ &\iff g \in \bigcap_{x\in X} G_x \end{aligned}$$

$\square$

Exercise 2 证明 $Z(G) = \bigcap_{x\in G} Z(x)$

Proof 因为共轭作用给出群同态

$$\begin{aligned} \rho : G &\longrightarrow G \\ g &\longmapsto \rho(g) : a \mapsto gag^{-1} \end{aligned}$$

又因为

$$\begin{aligned} \mathrm{Ker}\rho &= \{g|\rho(g) = \mathrm{Id}_G\} = \{g|\rho(g)(a) = a, \forall a \in G\} \\ &= \{g|gag^{-1} = a, \forall a \in G\} = \{g|ag = ga, \forall a \in G\} \\ &= Z(G) \end{aligned}$$

且 $G_x = Z(x)$, 由 $Ex1$ 即证 $\square$

Exercise 3 设 G 是 p^2 阶群,p 是素数,$H = (g), g \in Z(G), \mathrm{Ord}(g) = p$, 取 $g_1 \in G\backslash H$, s.t. $\mathrm{Ord}(g_1) = p$, 记 $K = (g_1)$, 验证

$$\begin{aligned} \Phi : H \times K &\longrightarrow G \\ (h, k) &\longmapsto hk \end{aligned}$$

是群同态

Proof 首先 H, K 中元素可写为 g^m, g_1^n 的形式，且 $g \in Z(G)$，故 $gg_1 = g_1 g$

$$\begin{aligned}\Phi\big((g^{m_1}, g_1^{n_1})\big)\Phi\big((g^{m_2}, g_1^{n_2})\big) &= g^{m_1} g_1^{n_1} g^{m_2} g_1^{n_2} \\ &= g^{m_1+m_2} g_1^{n_1+n_2} \\ &= \Phi(g^{m_1+m_2} g_1^{n_1+n_2})\end{aligned}$$

所以 Φ 是群同态 □

Exercise 4 考虑共轭作用

$$S_4 \curvearrowright X = \{(12)(34), (13)(24), (14)(23)\}, \quad g.x = gxg^{-1}$$

则有群同态 $S_4 \xrightarrow{\rho} S(X) \simeq S_3$，计算 $\mathrm{Ker}\rho$

Proof 记 $X = \{(12)(34), (13)(24), (14)(23)\} = \{A, B, C\}$，因为

$$\mathrm{Ker}\rho = \{\sigma \in S_4 | \sigma x \sigma^{-1} = x, \forall x \in X\} = \bigcap_{x \in X} Z(x) = Z(A) \cap Z(B) \cap Z(C)$$

考虑 $A = (12)(34)$，设 $\sigma \in S_4$，解如下方程

$$\sigma(12)(34)\sigma^1 = (\sigma(12)\sigma^{-1})(\sigma(34)\sigma^{-1}) = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) = (12)(34)$$

即有如下八种情况

$$\begin{cases}\sigma(1)=1\\ \sigma(2)=2\\ \sigma(3)=3\\ \sigma(4)=4\end{cases}, \begin{cases}\sigma(1)=2\\ \sigma(2)=1\\ \sigma(3)=3\\ \sigma(4)=4\end{cases}, \begin{cases}\sigma(1)=1\\ \sigma(2)=2\\ \sigma(3)=4\\ \sigma(4)=3\end{cases}, \begin{cases}\sigma(1)=2\\ \sigma(2)=1\\ \sigma(3)=4\\ \sigma(4)=3\end{cases}$$

$$\begin{cases}\sigma(1)=3\\ \sigma(2)=4\\ \sigma(3)=1\\ \sigma(4)=2\end{cases}, \begin{cases}\sigma(1)=3\\ \sigma(2)=4\\ \sigma(3)=2\\ \sigma(4)=1\end{cases}, \begin{cases}\sigma(1)=4\\ \sigma(2)=3\\ \sigma(3)=1\\ \sigma(4)=2\end{cases}, \begin{cases}\sigma(1)=4\\ \sigma(2)=3\\ \sigma(3)=2\\ \sigma(4)=1\end{cases}$$

即 $Z(A) = \{\mathrm{Id}, (12), (34), (12)(34), (13)(24), (1324), (1423), (14)(23)\}$，同理可以解得

$$\begin{cases}Z(B) = \{\mathrm{Id}, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1423)\}\\ Z(C) = \{\mathrm{Id}, (14), (23), (14)(23), (12)(34), (13)(24), (1243), (1342)\}\end{cases}$$

观察可得

$$\begin{aligned}\mathrm{Ker}\rho &= Z(A)\cap Z(B)\cap Z(C)\\ &= \{\mathrm{Id},(12)(34),(13)(24),(14)(23)\} = K_4\end{aligned}$$

□

Exercise 5 补充证明 35 阶群是循环群的细节. 根据 *Sylow* 定理, 设 P,Q 是 G 的唯一的 5,7 阶子群, 则有群同态

$$\begin{aligned}\phi: P\times Q &\longrightarrow G\\ (g,h) &\longmapsto gh\end{aligned}$$

且 $P\cap Q=\{1_G\}$, 因此 35 阶群是循环群

Proof 因为 P,Q 是唯一的 5,7 阶子群, 所以 $P\lhd G, Q\lhd G$, 且素数阶群是循环群, 即 $\exists p\in P, q\in Q, \text{s.t. } P=(p), Q=(q)$

首先证明 $P\cap Q=\{1_G\}$, 假设 $\exists a\in (P\cap Q)\backslash\{1_G\}$, 则 $1<\mathrm{Ord}(a)\mid 5, 1<\mathrm{Ord}(a)\mid 7$, 但显然不存在这样的 $\mathrm{Ord}(a)$, 因此 $P\cap Q=\{1_G\}$

设 $a\in P, b\in Q$, 则 $b^{-1}ab\in b^{-1}Pb=P, aba^{-1}\in aQa^{-1}=Q$

$$\begin{cases} b^{-1}aba^{-1}=(b^{-1}ab)a^{-1}\in P\\ b^{-1}aba^{-1}=b^{-1}(aba^{-1})\in Q\end{cases} \Longrightarrow b^{-1}aba^{-1}\in P\cap Q=\{1_G\}$$

进而 $ab=ba, \forall a\in P, b\in Q$

所以

$$\begin{aligned}\phi\big((g_1,h_1)\big)\phi\big((g_2h_2)\big) &= g_1h_1g_2h_2 = g_1g_2h_1h_2\\ &= \phi\big((g_1g_2)\big)\phi\big((h_1,h_2)\big)\end{aligned}$$

故 ϕ 是群同态, 若 $g\in P, h\in Q, gh=1_G$, 则 $h=g^{-1}\in P$, 所以 $h\in P\cap Q=\{1_G\}$, 故 $g=h=1_G$, 即 $\mathrm{Ker}(\phi)=\{(1_G,1_G)\}$, 所以 ϕ 是单射, 且 $|P\times Q|=|G|=35$, 所以 ϕ 是满射, 故是群同构

又因为 $P\times Q=\big((p,q)\big)$ 为循环群, 所以 G 是 35 阶循环群 □

Exercise 6 设 $|G|=p_1^{s_1}\cdots p_t^{s_t}$, 其中 p_i 为两两不同的素数, 若 G 是 *Abel* 群, 则存在唯一 *Sylow* p_i-子群 P_i, 证明存在群同构

$$\begin{aligned}\phi: P_1\times P_2\times\cdots\times P_t &\xrightarrow{\sim} G\\ (a_1,a_2,\cdots,a_t) &\longmapsto a_1a_2\cdots a_t\end{aligned}$$

Proof 因为

$$\begin{aligned}\phi\big((a_1,a_2,\cdots,a_t)\big)\phi\big((b_1,b_2,\cdots,b_t)\big) &= (a_1a_2\cdots a_t)(b_1b_2\cdots b_t) = (a_1b_1)(a_2b_2)\cdots(a_tb_t)\\ &= \phi\big((a_1b_1,a_2b_2,\cdots,a_tb_t)\big)\end{aligned}$$

因此 ϕ 确实是群同态

下证 $P_1 \cap P_2P_3\cdots P_t = \{1_G\}$, 先证 $P_2P_3\cdots P_t \le G$

对 $\forall a_2\cdots a_t, b_2\cdots b_t \in P_2\cdots P_t$, 因为

$$(a_2\cdots a_t)(b_2\cdots b_t)^{-1} = (a_2b_2^{-1})\cdots(a_tb_t^{-1}) \in P_2\cdots P_t$$

所以 $P_2\cdots P_t \le G$

假设 $\exists a \in (P_1 \cap P_2P_3\cdots P_t)\backslash\{1_G\}$, 则

$$\begin{cases} 1 < \mathrm{Ord}(a) \mid |P_1| = p_1^{s_1} \\ 1 < \mathrm{Ord}(a) \mid |P_2\cdots P_t| = p_2^{s_2}\cdots p_t^{s_t} \end{cases} \Longrightarrow \mathrm{Ord}(a) \mid \gcd(p_1^{s_1}, p_2^{s_2}\cdots p_t^{s_t}) = 1$$

这与 $\mathrm{Ord}(a) > 1$ 矛盾.

所以若 $(a_1,\cdots,a_t) \in \mathrm{Ker}\phi$, 即 $a_1\cdots a_t = 1_G \Longrightarrow a_1^{-1} = a_2\cdots a_t \in P_1 \cap P_2\cdots P_t$, 所以 $a_1^{-1} = 1_G$, 即 $a_1 = 1_G$, 同理可证 $a_2 = \cdots = a_t = 1_G$, 即 $\mathrm{Ker}\phi = \{(1,\cdots,1)\}$, 故 ϕ 是单射

又因为 $|P_1\times\cdots\times P_t| = p_1^{s_1}\cdots p_t^{s_t} = |G|$, 所以为满射, 进而 ϕ 是群同构 □

Exercise 7 设 G 是 n 阶群,p 是 n 的一个素因子, 证明 $x^p = 1$ 在群 G 中解的个数是 p 的倍数

Proof 由 *Sylow* 定理,$|G|$ 的 p 阶子群个数为 $pk+1$, 对任意 p 阶子群 P, 它是循环群, 故 $\exists a \in G, \text{s.t.}\ (a) = P$, 且 $\mathrm{Ord}(a^k) = \frac{\mathrm{Ord}(a)}{\gcd(k,p)} = p$, 因此 $\forall b \in (a)\backslash\{1_G\}, \mathrm{Ord}(b) = p$, 此时 b 也是生成元, 即任意两个 p 阶子群, 若相交则相等. 此外 1_G 也是 $x^p - 1 = 0$ 的根, 故

$$\mathrm{Root}_G(x^p - 1) = (p-1)\cdot(pk+1) + 1 = p(pk+1-k)$$

□

Exercise 8 证明 200 阶群必有正规的 *Sylow* 子群

Proof 因为 $200 = 2^3 5^2$, 所以

$$|Sylow\ 5\text{-子群}| = \begin{cases} 8\text{的因子} \\ 5k+1 \end{cases} = 1$$

因此 200 阶群 G 只有 1 个 *Sylow* 5-子群 P, 即它是正规子群, 由 *25* 阶子群的唯一性知 $\forall g \in G, gPg^{-1} = P$ □

Exercise 9 设 N 是有限群 G 的一个正规子群, 如果 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有 *Sylow* p-子群

Proof 由拉格朗日定理 $|G| = |N|\cdot|G/N|$, 且 $\gcd(p, |G/N|) = 1$, 设 $|G| = p^r m$, 则 $\frac{m}{|G/N|} \in \mathbb{Z}$, 所以 $|N| = \frac{p^r m}{|G/N|} = p^r \cdot \frac{m}{|G/N|}$, 设 $P \le G$ 为 G 的 *Sylow* p-子群,Q 为 N 的 *Sylow* p-子群, 则 $Q \le N \le G$, 故 Q 也是 G 的一个 *Sylow* p-子群, 由 *Sylow* 定理,$\exists g \in G, \text{s.t.}\ P = gQg^{-1} \le gNg^{-1} = N$, 即 P 也是 N 的 *Sylow* p-子群 □

Exercise 10 设 G 是有限群,$N \lhd G$,P 是 G 的 *Sylow* p-子群, 证明

1. $N \cap P$ 是 N 的 *Sylow* p-子群
2. PN/N 是 G/N 的 *Sylow* p-子群
3. $(N_G(P)N)/N \simeq N_{G/N}(PN/N)$

Proof (1). 设 $|G| = p^r m, p \nmid m$, 则 $|P| = p^r$, 由第二群同构定理

$$(N \cap P) \lhd P, \quad N \lhd NP \le G, \quad NP/N \simeq P/(P \cap N)$$

所以 $|N \cap P| \mid |P| = p^r$, 可设 $|N \cap P| = p^s, 1 \le s \le r$, 又因为 $P \le NP \le G$, 所以 $p^r \mid |NP|$, 设 $|NP| = p^r v, |N| = p^t u$, 由第三式得

$$[P : P \cap N] = [NP : N] \Longrightarrow \frac{p^r}{p^s} = \frac{p^r v}{p^t u} \Longrightarrow v = u, t = s$$

所以 $|N| = p^s u, N \cap P = p^s$, 故 $N \cap P$ 是 N 的 *Sylow* p-子群

(2). 由 $N \lhd G$ 知 $NP = PN$, 由第一问知 $|PN/N| = p^{r-s}$, 且 $|G/N| = \frac{p^r m}{p^s u} = p^{r-s}\frac{m}{u}$, 且由子群对应关系知 $PN/N \le G/N$, 故 PN/N 是 G/N 的 *Sylow* p-子群

(3). 一方面对 $\forall g \in N_G(P), n \in N, (gn)^{-1}P(gn) = n^{-1}(g^{-1}Pg)n = n^{-1}Pn$, 且 $gnN = gN$, 所以

$$(gnN)^{-1}(PN/N)(gnN) = g^{-1}N(PN/N)gN$$

下证 $g^{-1}N(PN/N)gN = PN/N$, 其中 $g \in N_G(P)$

首先对 $\forall pnN = pN \in PN/N, (g^{-1}N)(pN)(gN) = (g^{-1}pg)N$, 因为 $g \in N_G(P)$, 所以 $gPg^{-1} = P$, 故 $\exists p' \in P, \text{s.t.}\ gpg^{-1} = p'$, 故 $(g^{-1}pg)N = p'N \in PN/N$, 即 $LHS \subset RHS$

其次对 $\forall pnN = pN \in PN/N$, 由 $g \in N_G(P)$ 知 $\exists p' \in P, \text{s.t.}\ p' = g^{-1}p'g$, 所以 $pN = (g^{-1}N)(p'N)(gN) \in g^{-1}N(PN/N)gN$, 即 $RHS \subset LHS$

因此 $(gnN)^{-1}(PN/N)(gnN) = g^{-1}N(PN/N)gN = PN/N$, 即 $(N_G(P)N)/N \subseteq N_{G/N}(PN/N)$

另一方面, 对 $\forall gN \in N_{G/N}(PN/N)$, 有 $(gN)^{-1}(PN/N)(gN) = PN/N$, 即 $\forall p \in P, g^{-1}pgN \in PN/N$, 即 $g^{-1}pg \in PN$, 进而

$$g^{-1}Pg \subset PN$$

故 $g^{-1}Pg, P$ 均为 $PN = NP$ 的 *Sylow* p-子群, 由 *Sylow* 定理知它们共轭, 即 $\exists p_2 \in P, n \in N, \text{s.t.}$

$$(np_2)^{-1}g^{-1}Pg(np_2) = P \Longrightarrow p_2^{-1}(gn)^{-1}P(gn)p_2 = P \Longrightarrow (gn)^{-1}P(gn) = P$$

即 $gn \in N_G(P)$, 所以 $gN = gnN \in (N_G(P)N)/N$, 即 $N_{G/N}(PN/N) \subseteq (N_G(P)N)/N$ 综上有 $(N_G(P)N)/N = N_{G/N}(PN/N)$, 所以它们同构 $\square$

Exercise 11 设 P 是 G 的 *Sylow* p-子群, 且 $N_G(P) \lhd G$, 证明 $P \lhd G$

Proof 设 $G=p^rm, p\nmid m$, 则 $|P|=p^r$, 且显然有 $P\le N_G(P)\le G$, 设 $N_G(P)=p^rn$, 则 $n\mid m$, 所以

$$|G/N_G(P)|=\frac{p^rm}{p^rn}=\frac{m}{n}\nmid p$$

故 $\gcd(p,|G/N_G(P)|)=1$, 由练习 9 知 $N_G(P)$ 包含了 G 的所有 *Sylow* p-子群, 且所有 *Sylow* p-子群相互共轭, 由 $N_G(P)$ 的定义知,$\forall g\in N_G(P), g^{-1}Pg=P$, 故只有 P 这一个 *Sylow* p-子群, 因此 $P\lhd G$ □

Exercise 12 验证 $|\mathrm{GL}_n(\mathbb{F}_p)|=\prod\limits_{k=1}^{n}(p^n-p^{k-1})$

Proof 对 $\forall A\in \mathrm{GL}_n(\mathbb{F}_p)$,$A$ 与它的线性无关的行向量组 $\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_n\}$ 一一对应, 因此讨论在 $\mathbb{F}_p^n$ 中, 能有多少种线性无关的行向量组.

首先 $\boldsymbol{e}_1$ 共有 p^n-1 种选择, 排除的那一种为 $(0,\cdots,0)$

对于 $\boldsymbol{e}_2$, 它不能与 $\boldsymbol{e}_1$ 线性相关, 即它不等于 $\boldsymbol{e}_1,2\boldsymbol{e}_1,\cdots,(p-1)\boldsymbol{e}_1,p\boldsymbol{e}_1=\boldsymbol{0}$, 共有 p^n-p 种选择

对于 $\boldsymbol{e}_3$, 它不能与 $\boldsymbol{e}_1,\boldsymbol{e}_2$ 线性相关, 因为线性子空间 $<\boldsymbol{e}_1,\boldsymbol{e}_2>=\{x\boldsymbol{e}_1+y\boldsymbol{e}_2|0\le x,y\le p-1\}$, 共有 p^2 个元素, 因此 $\boldsymbol{e}_3$ 共有 p^n-p^2 种选择

依此类推, 故 $|\mathrm{GL}_n(\mathbb{F}_p)|=\prod\limits_{k=1}^{n}(p^n-p^{k-1})$ □

Exercise 13 设 $H\le K, U\le K$ 是 K 的 *Sylow* p-子群, 则 $\exists g\in K, \text{s.t. } H\cap gUg^{-1}$ 为 H 的 *Sylow* p-子群

Proof 考虑左诱导作用 $H\curvearrowright(K/U)$

$$H\times K/U\longrightarrow K/U$$
$$(h,kU)\longmapsto hkU$$

设 $|K|=p^rm, p\nmid m$, 因为 U 是 *Sylow* p-子群, 所以 $p\nmid |K/U|=\frac{|K|}{|U|}=m$, 故

$$p\nmid |K/U|,\quad K/U=\bigsqcup_{k\in K}|\mathcal{O}_{kU}|$$

因此一定存在 $gU\in K/U, \text{s.t. } p\nmid|\mathcal{O}_{gU}|$, 由轨道-稳定化子公式知

$$|H|=|\mathcal{O}_{gU}|\cdot|H_{gU}|$$

其中 H_{gU} 为 U 的稳定化子, 则 $|H_{gU}|,|H|$ 中 p 的幂次相等, 故 H_{gU} 即为 H 的 *Sylow* p-子群, 且

$$H_{gU}=\{h\in H|hgU=gU\}=\{h\in H|g^{-1}hg\in U\}=\{h\in H|h\in gUg^{-1}\}=H\cap gUg^{-1}$$

□

Exercise 14 任意字可以化为唯一的即约字

Proof 对字中元素的个数 n 使用数学归纳法

当 $n=1$ 时, 显然是即约, 且表达唯一

当 $n=k-1$ 时命题成立, 下面证明 $n=k$ 时. 首先证明可以化为即约的字: 设 $\omega=x_1\cdots x_{k-1}x_k$, 由数学归纳法,$x_1\cdots x_{k-1}$ 可以化为唯一的即约字, 设为 $\omega_1=y_1\cdots y_j, 1\le j\le k-1$

Case 1. 若 $j<k-1$, 则 $\omega=\omega_1 x_k=y_1\cdots y_j x_k$, 由数学归纳法知它可以化为即约的字

Case 2. 若 $j=k-1$, 假设 $x_k=y_j^{-1}$, 则它可以与 y_j 消去, 得到 $y_1\cdots y_{j-1}$, 它是即约的; 假设 $x_k\ne y_j^{-1}$, 则 $y_1\cdots y_j x_k$ 是即约的

其次证明表达唯一, 假设 $\omega=x_1\cdots x_m=y_1\cdots y_n$ 为两个即约字, 则

$$y_n^{-1}\cdots y_1^{-1}x_1\cdots x_m=1$$

考虑 x_1, 因为 $x_1\cdots x_m$ 是即约的, 所以 $x_2\ne x_1^{-1}$, 但是上式最终要化为 1, 一定只能是 $y_1^{-1}=x_1^{-1}$, 即 $y_1=x_1$. 同理可以说明 $x_j=y_j$, 进而 $m=n$, 故表达唯一 $\square$

Exercise 15 证明 $N(r_1,\cdots,r_m)=\big(\omega r_j\omega^{-1}\mid 1\le j\le m,\omega\in F(x_1,\cdots,x_n)\big)$

Proof 一方面, 对 $\forall\omega\in F(x_1,\cdots,x_n)$, 由 $N(r_1,\cdots,r_m)$ 为正规子群知 $\omega N(r_1,\cdots,r_m)\omega^{-1}=N(r_1,\cdots,r_m)$, 所以 $\exists y_i\in N(r_1,\cdots,r_m)$, s.t. $y_i=\omega r_i\omega^{-1}$, 即 $RHS\subset LHS$

另一方面, 要证 $LHS\subset RHS$, 只需证明 RHS 是正规子群, 且包含 $r_1,\cdots,r_m$, 再由最小性即得证, 因为对 $\forall y\in F(x_1,\cdots,x_n),\omega r_j\omega^{-1}\in RHS$, 有

$$y(r\omega r_j^{-1})y^{-1}=(yr)\omega(yr)^{-1}\in RHS$$

因此 $RHS\lhd F(x_1,\cdots,x_n)$

综上 $N(r_1,\cdots,r_m)=\big(\omega r_j\omega^{-1}\mid 1\le j\le m,\omega\in F(x_1,\cdots,x_n)\big)$ $\square$

Exercise 16 证明 $G=<s,t\mid s^2,t^2,(st)^6>\simeq D_6$

Proof 考虑满同态

$$f:G\longrightarrow D_6$$
$$st\longmapsto a$$
$$s\longmapsto b$$

因为 $f(t)=f(s^2t)=f(s)f(st)=ba$, 故 $f(t^2)=(ba)^2=1$

Claim: $G=\{(st)^i s^j|0\le i\le 5,0\le j\le 1\}$

因为 $s^2=t^2=1$, 所以 G 中元素一定形如 $ststststs\cdots$ 或 $tstststst\cdots$.

若为前者, 则结合 $(st)^6=1$ 知它一定形如 $(st)^i s$ 或 $(st)^i$, 其中 $0\le i\le 5$

若为后者, 因为 $(st)^6=1$, 所以 $t(st)^6t=t^2=1$, 即 $(ts)^6=1$, 因此它一定可化为 $(ts)^i t$ 或 $(ts)^i$, 其中 $0\le i\le 5$, 又因为 $(st)^6=1$, 所以

$$(ststst)(ststst)=1\Longrightarrow ststst=tststs$$

因此 $(ts)^4=(ts)^3(ts)=(st)^3(st)=(st)^2$, 同理 $(ts)^5=st,(ts)^2=(st)^4,ts=(st)^5$, 所以 $(ts)^i$ 均可化为 $(st)^{6-i}$, 对于 $(ts)^it=(st)^{6-i}t=(st)^{5-i}(st)t=(st)^{5-i}s$, 再说明 $\{(st)^is^j|0\leq i\leq 5,0\leq j\leq 1\}$ 没有重复的元素, 假设 $0\leq i,m\leq 5,0\leq j\leq 1$, 且

$$(st)^is^j=(st)^ms^n\Longrightarrow s^j=(st)^{6+m-i}s^n$$

若 $j=0$, 则 $1=(st)^{6+m-i}s^n$, 故 $6+m-i=6,n=0$, 所以 $i=m,j=n;$ 若 $j=1$, 两边同时右乘 s, 则 $1=(st)^{6+m-i}s^{n+1}$, 所以 $6+m-i=6,n+1=2$, 即 $m=i,n=j=1$, 因此表达唯一, 即断言得证

所以 $|G|\leq 12$, 且由满射知,$|G|=12$ 且 f 是双射, 所以 f 是群同构, 即 $G\simeq D_6$ $\square$