# 近世代数 (H) 第九、十周作业

涂嘉乐 PB23151786

2025 年 4 月 30 日

**Exercise 1** 证明群 $G$ 中逆元是唯一的

**Proof** 对 $\forall a \in G$，假设存在 $b_1, b_2 \in G$ 均为 $a$ 的逆元，则

$$b_1 = 1_G \cdot b_1 = (b_2 \cdot a) \cdot b_1 = b_2 \cdot (a \cdot b_1) = b_2 \cdot 1_G = b_2$$

$\square$

**Exercise 2** 证明对 $\forall a \in G, \forall m, n \in \mathbb{Z}, a^{m+n} = a^m \cdot a^n$

**Proof**

Case1. $m, n \geq 0$，则

$$a^{m+n} = \overbrace{a \cdot a \cdots a \cdot a}^{(m+n)\text{个}} = \overbrace{a \cdot a \cdots a \cdot a}^{m\text{个}} \cdot \overbrace{a \cdot a \cdots a \cdot a}^{n\text{个}} = a^m \cdot a^n$$

Case2. $m, n < 0$，则

$$a^{m+n} = \overbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}^{-(m+n)\text{个}} = \overbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}^{-m\text{个}} \cdot \overbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}^{-n\text{个}} = a^m \cdot a^n$$

Case3. $m > 0 > n$

*1.* $m + n = 0$，则

$$a^m \cdot a^n = \overbrace{a \cdot a \cdots a \cdot a}^{m\text{个}} \cdot \overbrace{a^{-1} \cdot a^{-1} \cdots a^{-1} \cdot a^{-1}}^{-m\text{个}}$$

通过不断地在最中间加括号可得 $a^m \cdot a^n = 1 = a^{m+n}$

*2.* $m + n > 0$，则

$$a^m \cdot a^n = a^{m+n+(-n)} \cdot a^n = a^{m+n} \cdot a^{-n} \cdot a^n = a^{m+n}$$

*3.* $m + n < 0$，则

$$a^m \cdot a^n = a^m \cdot a^{-m+(n+m)} = a^m \cdot a^{-m} \cdot a^{n+m} = a^{n+m}$$

$\square$

**Exercise 3** 写出 $\Sigma(\square)$ 的 8 个矩阵

**Solution** 旋转

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

对称

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$$

**Exercise 4** 若 $G=\bigsqcup\limits_{i\in I}Ha_i$，证明 $G=\bigsqcup\limits_{i\in I}a_i^{-1}H$

**Proof** 设 $I$ 为右陪集代表元系的指标集

***Claim:*** $Ha=Hb \iff ab^{-1}\in H, aH=bH \iff b^{-1}a\in H$

Proof Of Claim : 证明第二式，第一式上课证过了（实际上也同理）

$(\Longrightarrow)$ : 若 $aH=bH$，则 $a=ae\in aH=bH$，则 $\exists h\in H, \text{s.t. } a=bh$，故 $b^{-1}a=h^{-1}\in H$

$(\Longleftarrow)$ : 因为 $b^{-1}a\in H$，所以 $a^{-1}b\in H$，故对 $\forall h\in H, \exists h',h''\in H, \text{s.t. } h=a^{-1}bh', h=b^{-1}ah''$，因此

$$\begin{cases}ah=a\cdot a^{-1}bh'=bh'\in bH\Longrightarrow aH\subseteq bH\\ bh=b\cdot b^{-1}ah''=ah''\in aH\Longrightarrow bH\subseteq aH\end{cases}$$

故 $aH=bH$，断言得证，所以

$$Ha=Hb \iff ab^{-1}\in H \iff (a^{-1})^{-1}b^{-1}\in H \iff a^{-1}H=b^{-1}H$$

由 $G=\bigsqcup\limits_{i\in I}Ha_i$ 是无交并知，$\forall i\neq j, a_ia_j^{-1}\notin H\Longrightarrow a_i^{-1}H\neq a_j^{-1}H$，因此 $\bigsqcup\limits_{i\in I}a_i^{-1}H$ 也是无交并，且考虑

$$\sigma: H\longrightarrow aH$$
$$h\longmapsto ah$$

则 $\sigma$ 是双射：若 $\sigma(h_1)=\sigma(h_2)$，则 $ah_1=ah_2\Longrightarrow h_1=h_2$，故为单射；$\forall ah\in aH$，均有原像 $h$，故为满射

进而 $|H|=|aH|$，由 $\bigsqcup\limits_{i\in I}Ha_i$ 知，$|G|=|H|\cdot|I|$，故

$$\bigsqcup_{i\in I}a_i^{-1}H\subseteq G,\quad \sum_{i\in I}|a_i^{-1}H|=|I|\cdot|H|=|G|$$

两边元素个数相等，故 $\bigsqcup\limits_{i\in I}a_i^{-1}H=G$ □

**Exercise 5** $f:G\to H$ 为群同态，$G,H$ 为有限群，$a\in G$，则 $\mathrm{Ord}(f(a))\mid\mathrm{Ord}(a)$；若 $f$ 为群同构，则 $\mathrm{Ord}(a)=\mathrm{Ord}(f(a))$

**Proof** 设 $\mathrm{Ord}(a)=d, \mathrm{Ord}(f(a))=d'$，则 $a^d=1$，所以

$$1_H=f(1_G)=f(a^d)=f(a)^d$$

则 $\mathrm{Ord}(f(a)) = d' \mid d = \mathrm{Ord}(a)$，若 $f$ 为群同构，则对 $f^{-1}: H \to G$ 重复上述过程得

$$1_G = f^{-1}(1_H) = f^{-1}(f(a)^{d'}) = \left[f^{-1}(f(a))\right]^{d'} = a^{d'}$$

则 $\mathrm{Ord}(a) = d \mid d' = \mathrm{Ord}(f(a))$，故 $d, d'$ 相互整除，由它们都是正数知 $d = d'$ □

**Exercise 6** 考察求逆映射

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

则 $(-)^{-1}$ 是群同态 $\iff$ $G$ 是 *Abel* 群

**Proof** $(\Longrightarrow)$：若 $(-)^{-1}$ 是群同态，则 $\forall a, b \in G$

$$b^{-1}a^{-1} = (-)^{-1}(ab) = (-)^{-1}(a)(-)^{-1}(b) = a^{-1}b^{-1}$$

所以

$$b = a^{-1}ba \Longrightarrow ab = aa^{-1}ba = ba$$

$(\Longleftarrow)$：若 $G$ 是 *Abel* 群，则 $\forall a, b \in G, ab = ba$，所以

$$(-)^{-1}(ab) = b^{-1}a^{-1} = a^{-1}b^{-1} = (-)^{-1}(a)(-)^{-1}(b)$$

故 $(-)^{-1}$ 是群同态 □

**Exercise 7** 定义 $G$ 的反群 $G^{\mathrm{op}} = \{a^{\mathrm{op}} | a \in G\}$，乘法定义为 $a^{\mathrm{op}}b^{\mathrm{op}} = (ba)^{\mathrm{op}}$，求证 $G$ 同构于 $G^{\mathrm{op}}$

**Proof** 考虑映射

$$\begin{aligned}\sigma: G &\longrightarrow G^{\mathrm{op}}\\ a &\longmapsto (a^{-1})^{\mathrm{op}}\end{aligned}$$

则 $\sigma$ 是同构：

1. 同态：$\sigma(ab) = ((ab)^{-1})^{\mathrm{op}} = (b^{-1}a^{-1})^{\mathrm{op}} = (a^{-1})^{\mathrm{op}}(b^{-1})^{\mathrm{op}} = \sigma(a)\sigma(b)$
2. 单射：由群同态知，$1_{G^{\mathrm{op}}} = 1_G^{\mathrm{op}}$，先证明 $(a^{-1})^{\mathrm{op}} = (a^{\mathrm{op}})^{-1}$，即取 op 和取逆可以交换，因为

$$a^{\mathrm{op}} \cdot (a^{-1})^{\mathrm{op}} = (a^{-1}a)^{\mathrm{op}} = 1^{\mathrm{op}} = 1_{G^{\mathrm{op}}}$$

所以 $(a^{-1})^{\mathrm{op}} = (a^{\mathrm{op}})^{-1}$，若 $\sigma(a) = \sigma(b)$，则

$$(a^{-1})^{\mathrm{op}} = (b^{-1})^{\mathrm{op}} \Longrightarrow (a^{\mathrm{op}})^{-1} = (b^{\mathrm{op}})^{-1} \Longrightarrow a^{\mathrm{op}} = b^{\mathrm{op}} \Longrightarrow a = b$$

3. 满射：对 $\forall a^{\mathrm{op}} \in G^{\mathrm{op}}$，它的原像为 $a$

故 $\sigma$ 是群同构 □

**Exercise 8** $\forall n \geq 2, \mu_n = \{z \in \mathbb{C} | z^n = 1\} \leq \mathbb{C}^\times$，证明 $(\mu_n, \cdot)$ 同构于 $(\mathbb{Z}_n, +)$

**Proof** 考虑映射

$$\begin{aligned} \sigma : \mu_n &\longrightarrow \mathbb{Z}_n \\ \xi^k &\longmapsto \overline{k} \end{aligned}$$

则 $\sigma$ 是同构：

1. 同态：$\sigma(\xi^k \xi^l) = \sigma(\xi^{k+l}) = \overline{k+l} = \overline{k} + \overline{l} = \sigma(\xi^k)\sigma(\xi^l)$
2. 单射：$\sigma(\xi^k) = \sigma(\xi^l)$，则 $\overline{k} = \overline{l}$，即 $k = l + mn, m \in \mathbb{Z}$，所以 $\xi^k = \xi^l \cdot (\xi^n)^m = \xi^l$
3. 满射：$\forall \overline{k} \in \mathbb{Z}_n$，均有原像 $\xi^k$

□

**Exercise 9** 回忆 $\mu_2 = \{1, -1\}$，记 $\mu_2 \times \mu_2 = V_4$，称为 *Klein* 四群，证明 $V_4 \simeq U(\mathbb{Z}_8)$

**Proof** 因为 $U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}, V_4 = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$，考虑映射

$$\begin{aligned} \sigma : U(\mathbb{Z}_8) &\longrightarrow V_4 \\ (1,1) &\longmapsto \overline{1} \\ (1,-1) &\longmapsto \overline{3} \\ (-1,1) &\longmapsto \overline{5} \\ (-1,-1) &\longmapsto \overline{7} \end{aligned}$$

则 $\sigma$ 是双射，且容易验证 $\sigma$ 确实保乘法，故 $V_4 \simeq U(\mathbb{Z}_8)$ □

**Exercise 10** 证明 $\mathbb{Q}^\times$ 不是循环群

**Proof** 假设 $\mathbb{Q}^\times$ 是循环群，由于 $|\mathbb{Q}^\times| = \infty$，所以 $\exists a \in \mathbb{Q}^\times, \text{s.t. } \mathbb{Q}^\times = (a)$，由 $a \in \mathbb{Q}^\times$ 可设 $a = \frac{n}{m}$ 即约，取素数 $p \nmid m, p \nmid n$，则 $p \notin (a)$，否则 $\exists k \in \mathbb{Z}, \text{s.t. } \left(\frac{n}{m}\right)^k = p$，若 $k > 0$，则 $p \mid n^k$；若 $k < 0$，则 $p \mid m^k$，显然矛盾！ □

**Exercise 11** 证明群 $G$ 的中心 $Z(G)$ 是正规子群，其中

$$Z(G) = \{g \in G | gh = hg, \forall h \in G\}$$

**Proof** 即证明 $\forall a \in G, aZ(G)a^{-1} = Z(G)$，因为 $\forall g \in Z(G), a \in G, ga = ag$，所以

$$\begin{aligned} aZ(G)a^{-1} &= \{aga^{-1} | g \in Z(G)\} \\ &= \{gaa^{-1} | g \in Z(G)\} \\ &= \{g | g \in Z(G)\} = Z(G) \end{aligned}$$

□

**Exercise 12** 设 $N \leq G$，若 $[G : N] = 2$，证明 $N \trianglelefteq G$

**Proof** 任取 $a \in G\backslash N$，则有陪集分解

$$\begin{cases} G = N \sqcup aN \\ G = N \sqcup Na \end{cases}$$

则 $aN = Na = G\backslash N$；若 $a \in N$，则 $aN = N = Na$，因此 $N \trianglelefteq G$ $\square$

**Exercise 13** 设 $A \leq G, B \leq G$，求证

$$AB \leq G \iff AB = BA$$

**Proof** $(\Longrightarrow)$ : 若 $AB \leq G$, 对 $\forall x \in AB$, 由 $AB \leq G$ 知, $x^{-1} \in AB \Longrightarrow \exists a \in A, b \in B, \text{s.t. } x^{-1} = ab$, 所以 $x = (ab)^{-1} = b^{-1}a^{-1} \in BA$，即 $AB \subseteq BA$；反之设 $x \in BA$，则 $\exists b \in B, a \in A, \text{s.t. } x = ba$，因此 $x^{-1} = a^{-1}b^{-1} \in AB \leq G$，所以 $x \in AB$，即 $BA \subseteq AB$，综上 $AB = BA$

$(\Longleftarrow)$ : 首先 $1_G = 1_G 1_G \in AB$；若 $AB = BA$，则 $\forall a_1b_1, a_2b_2 \in AB$，下面证明 $a_1b_1a_2b_2 \in AB$，即 $AB$ 保乘法。因为 $b_1a_2 \in BA = AB$，所以可设 $b_1a_2 = a_3b_3$，因此

$$a_1b_1a_2b_2 = a_1a_3b_3b_2 = (a_1a_3)(b_3b_2) \in AB$$

对 $\forall ab \in AB$，因为 $b^{-1}a^{-1} \in BA = AB$，所以 $AB$ 保逆元。综上 $AB \leq G$ $\square$

**Exercise 14** 设 $a, b \in G$，求证 $\text{Ord}(a) = \text{Ord}(a^{-1}), \text{Ord}(ab) = \text{Ord}(ba)$

**Proof** 若 $\text{Ord}(a) = \infty$，则 $\forall k \in \mathbb{N}, a^k \neq 1_G$，所以 $\forall k \in \mathbb{N}^*, a^{-k} = (a^{-1})^k \neq 1_G$，即 $\text{Ord}(a^{-1}) = \infty$

若 $\text{Ord}(a) = d < \infty$，则 $a^d = 1_G$，因此 $(a^{-1})^d = (a^d)^{-1} = 1_G$，因此 $\text{Ord}(a^{-1}) \mid d = \text{Ord}(a)$，交换 $a^{-1}$ 与 $a$ 的位置，同理有 $\text{Ord}(a^{-1}) \mid \text{Ord}(a)$，即 $\text{Ord}(a) = \text{Ord}(a^{-1})$

若 $\text{Ord}(ab) = \infty$，则 $\forall k \in \mathbb{N}^*, (ab)^k \neq 1_G$，若 $\text{Ord}(ba) = n < \infty$，则

$$(ab)^n = (ab)(ab)\cdots(ab) = a(ba)^{n-1}b = a(ba)^{-1}b = aa^{-1}b^{-1}b = 1_G$$

这将导致 $\text{Ord}(a) \leq n$，矛盾！所以 $\text{Ord}(ba) = \infty$

若 $\text{Ord}(ab) = d < \infty$，则由上可知 $(ba)^d = 1_G$，所以 $\text{Ord}(ba) \mid \text{Ord}(ab)$，交换 $a, b$ 的位置，同理可得 $\text{Ord}(ab) \mid \text{Ord}(ba)$，所以 $\text{Ord}(ab) = \text{Ord}(ba)$ $\square$

**Exercise 15** 证明：$(\mathbb{Q}, +)$ 不是循环群，但是它的任意有限生成的子群都是循环群

**Proof** 假设 $(\mathbb{Q}, +)$ 是循环群，则 $\exists \frac{n}{m} \in \mathbb{Q}, \text{s.t. } \mathbb{Q} = \left(\frac{n}{m}\right)$，设 $\frac{n}{m}$ 即约，取素数 $p, \text{s.t. } p \nmid m$，则 $\frac{1}{p} \notin \left(\frac{n}{m}\right)$，否则 $\exists k \in \mathbb{Z}, \text{s.t. } \frac{1}{p} = \frac{kn}{m}$，故 $knp = m$，这与 $p \mid m$ 矛盾！

对生成元的个数 $n$ 做归纳，若 $n = 1$，显然为循环群

若 $n = 2$，生成元有一个为零时退化到 $n = 1$ 的情形，假设生成元非零，设为 $\frac{p_1}{q_1}, \frac{p_2}{q_2}$（即约），记 $d = \gcd(p_1q_2, p_2q_1)$

***Claim:*** $\left(\frac{d}{q_1q_2}\right) = \left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$

一方面设 $x\in\left(\frac{d}{q_1q_2}\right)$，则 $\exists k\in\mathbb{Z},\text{s.t. } x=\frac{kd}{q_1q_2}$，由 *Bezout* 等式，$\exists u,v\in\mathbb{Z},\text{s.t. } d=up_1q_2+vp_2q_1$，因此 $x=\frac{k(up_1q_2+vp_2q_1)}{q_1q_2}=ku\cdot\frac{p_1}{q_1}+kv\frac{p_2}{q_2}\in\left(\frac{p_1}{q_1},\frac{p_2}{q_2}\right)$

另一方面设 $x\in\left(\frac{p_1}{q_1},\frac{p_2}{q_2}\right)$，则 $\exists a,b\in\mathbb{Z},\text{s.t. } x=a\cdot\frac{p_1}{q_1}+b\cdot\frac{p_2}{q_2}=\frac{ap_1q_2+bp_2q_1}{q_1q_2}=\left(\frac{ap_1q_2}{d}+\frac{bp_2q_1}{d}\right)\cdot\frac{d}{q_1q_2}\in\left(\frac{d}{q_1q_2}\right)$，即 $\left(\frac{p_1}{q_1},\frac{p_2}{q_2}\right)$ 有生成元 $\frac{d}{q_1q_2}$

设 $n=k$ 时，命题成立，下面证明 $n=k+1$ 时，设 $S=\left(\frac{p_1}{q_1},\cdots,\frac{p_{k+1}}{q_{k+1}}\right)$ 由归纳假设，$\exists a\in\mathbb{Q},\text{s.t. }\left(\frac{p_1}{q_1},\cdots,\frac{p_k}{q_k}\right)=(a)$，因此 $S=\left(a,\frac{p_{k+1}}{q_{k+1}}\right)$，由 $n=2$ 时的情形知，$S$ 为循环群

综上 $(\mathbb{Q},+)$ 的任意有限生成子群均为循环群 $\square$

**Exercise 16** 设 $p$ 是素数，$G$ 是方程 $x^p=1,x^{p^2}=1,\cdots,x^{p^n}=1,\cdots$ 的所有根在复数乘法下的群，试证明 $G$ 的任意真子群都是有限阶循环群

**Proof** 首先 $\forall a\in G,\exists n_a\in\mathbb{N}^*,\text{s.t. Ord}(a)=p^{n_a}$；设 $H\le G$ 是真子群，则 $\exists g\in G\backslash H$，则 $\exists n\in\mathbb{N}^*,\text{s.t. Ord}(g)=p^n$；其次我们有事实，若 $x\le y$，则作为 $G$ 的子群，$\mu_{p^x}\le\mu_{p^y}\le G$

***Claim***: $\forall h\in H$，若 $\text{Ord}(h)=p^m$，则 $m<n$

Proof Of Claim : 若 $\exists h\in H,\text{s.t. Ord}(h)=m\ge n$，则 $(h)=\mu_{p^m}$，因此 $(h)=\mu_{p^m}\le H$，因为 $\text{Ord}(g)=p^n$，所以 $g\in\mu_{p^n}\le\mu_{p^m}\le H$，这与 $g\notin H$ 矛盾！

因此断言得证，考虑集合 $O=\{\text{Ord}(h):h\in H\}$，则 $O$ 为非空正整数集，且有上界 $n$，因此可以取得最大值，取 $h\in H,\text{s.t. Ord}(h)$ 最大，记 $\text{Ord}(h)=p^s$，则 $\forall h'\in H,\text{Ord}(h')=p^t,t\le s$，因此 $h'\in\mu_{p^t}\le\mu_{p^s}=(h)$，即 $H=(h)$ $\square$

**Exercise 17** 设 $M,N\trianglelefteq G$，如果 $M\cap N=\{1_G\}$，则对任意 $a\in M,b\in N$，有 $ab=ba$

**Proof** 由 $M,N\trianglelefteq G$ 知，$M=bMb^{-1},N=aNa^{-1}$，因此

$$\begin{cases}aba^{-1}b^{-1}=(aba^{-1})b^{-1},aba^{-1}\in aNa^{-1}=N\Longrightarrow aba^{-1}b^{-1}\in N\\ aba^{-1}b^{-1}=a(ba^{-1}b^{-1}),ba^{-1}b^{-1}\in bMb^{-1}=M\Longrightarrow aba^{-1}b^{-1}\in M\end{cases}$$

由 $M\cap N=\{1_G\}$ 知，$aba^{-1}b^{-1}=1_G$，即 $ab=ba$ $\square$

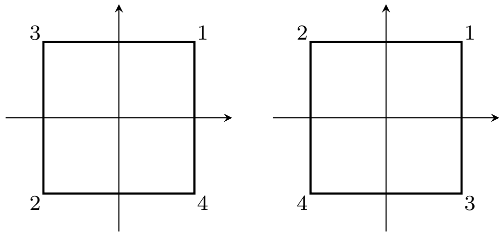
**Exercise 18** 若 $G/Z(G)$ 是循环群，则 $G$ 是 *Abel* 群

**Proof** 设 $G/Z(G)=gZ(G),g\in G$，则 $\forall a,b\in G,\exists m,n,\text{s.t. } aZ(G)=g^mZ(G),bZ(G)=g^nZ(G)$，所以

$$\begin{cases}a=a\cdot 1_G\in aZ(G)=g^mZ(G)\Longrightarrow\exists c\in Z(G),\text{s.t. } a=g^mc\\ b=b\cdot 1_G\in bZ(G)=g^nZ(G)\Longrightarrow\exists d\in Z(G),\text{s.t. } b=g^nd\end{cases}$$

因此 $ab=g^mc\cdot g^nd=g^nd\cdot g^mc=ba$，由 $a,b$ 的任意性知 $G$ 是 *Abel* 群 $\square$

**Exercise 19** 若正方形顶点的编号变为




分别计算 $\Sigma(\square)$ 到 $S_4$ 的嵌入同态的像集 $H', H''$，并且计算 $H \cap H' \cap H''$

**Solution**

$H'$ 包含八个元素

1. 四个旋转：$\mathrm{Id}, (1324), (12)(34), (1423)$
2. 四个对称：$(14)(23), (13)(24), (12), (34)$

$H''$ 包含八个元素

1. 四个旋转：$\mathrm{Id}, (1243), (14)(23), (1342)$
2. 四个对称：$(13)(24), (12)(34), (14), (23)$

上课求过 $H$ 包含八个元素

1. 四个旋转：$\mathrm{Id}, (1234), (13)(24), (1432)$
2. 四个对称：$(14)(23), (12)(34), (24), (13)$

因此，观察发现

$$H \cap H' \cap H'' = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$$

**Exercise 20** 证明 $H$ 为由 $(13), (1234)$ 生成的子群

**Proof** 因为 $\mathrm{Ord}(1234) = 4$, 且 $(13)$ 无法被 $(1234)$ 生成, 所以 $\big((13),(1234)\big) \geq 5$, 且 $\big((13),(1234)\big) \leq H$，$|H| = 8$，由拉格朗日定理知，$\big|\big((13),(1234)\big)\big| \;\Big|\; 8$，因此它的阶为 8，即 $H = \big((13),(1234)\big)$ $\square$