2024–2025 学年第 1 学期抽象代数 I 课程期中考试试卷

参考解答

一, 判断下列论断是否正确, 若正确, 给出简要证明, 否则举反例说明.

1. 若群 G 所有的子群都是正规子群, 则 G 为一个交换群.

2. 任取群 G 有两个子群 K 和 L, 则 $KL = \{kl \in G \mid k \in K, l \in L\}$ 是一个子群当且仅当 $KL = LK$.

3. 任取群 G 和非空集合 X, 都存在至少一个 G 在 X 上的群作用.

4. 阶为21 的群不是单群.

解. 1. 错误. 反例: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

2. 正确. 若 KL 为一个子群, 则对任意 $k \in K$ 和 $l \in L$, 有 $k', k'' \in K$ 和 $l', l'' \in L$, 满足 $klk'l' = e$ 和 $k^{-1}l^{-1}k''l'' = e$. 因此有 $kl = l'^{-1}k'^{-1}$ 和 $k''l'' = lk$. 因此 $KL \subset LK$ 且 $KL \supset LK$, 即 $KL = LK$.

   反之, 设 $KL = LK$. 注意到 KL 非空. 任取 $k, k' \in K$ 和 $l, l' \in L$, 考虑

   $$kl(k'l')^{-1} = k(ll'^{-1})k'^{-1}.$$

   由于 $KL = LK$, 存在 $k'' \in K$ 和 $l'' \in L$, 满足 $(ll'^{-1})k'^{-1} = k''l''$. 因此

   $$kl(k'l')^{-1} = (kk'')l'' \in KL.$$

   所以 KL 为一个子群.

3. 正确. 映射

   $$\begin{aligned} G \times X &\to X \\ (a, x) &\mapsto x \end{aligned}$$

   给出 G 在 X 上的平凡作用.

4. 正确. 设 G 为一个 21 阶群. 考虑 21 的素数分解 3×7. 记 n_7 为 G 的 Sylow 7-子群的个数. 利用 Sylow 定理可知:

   $$n_7 \equiv 1 \mod 7, \quad n_7 \mid 3.$$

   因此 $n_7 = 1$. 由此可知 G 有一个 7 阶正规子群, G 不是单群.

□

二, 考虑群 $\mathrm{SL}(2,\mathbb{Z})$. (群运算为矩阵乘法)

1. **证明 $\mathrm{SL}(2,\mathbb{Z})$ 可以由**

$$\left\{\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}\right\}$$

生成.

证明. 记

$$U=\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} \quad V=\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$$

注意到任取向量 $[m,n]^T\in\mathbb{Z}^2$, 对任意 $k\in\mathbb{Z}$, 我们有

$$U^k\begin{bmatrix}m\\n\end{bmatrix}=\begin{bmatrix}m+kn\\n\end{bmatrix}, \quad V^k\begin{bmatrix}m\\n\end{bmatrix}=\begin{bmatrix}m\\n+km\end{bmatrix}.$$

记 $d=\gcd(m,n)$. 由辗转相除, 我们有

$$\begin{aligned}m&=q_1n+r_1\\n&=q_2r_1+r_2\\&\cdots\\r_{k-2}&=q_kr_{k-1}+r_k\end{aligned}$$

其中 $r_k=0$, $r_{k-1}=d=\gcd(m,n)$. 写为矩阵形式可得

$$V^{-1}UU^{-q_k}\cdots V^{-q_2}U^{-q_1}\begin{bmatrix}m\\n\end{bmatrix}=V^{-1}U\begin{bmatrix}0\\d\end{bmatrix}=\begin{bmatrix}d\\0\end{bmatrix}$$

或者

$$V^{-q_k}\cdots V^{-q_2}U^{-q_1}\begin{bmatrix}m\\n\end{bmatrix}=\begin{bmatrix}d\\0\end{bmatrix}$$

若

$$A=\begin{bmatrix}p & q\\r & s\end{bmatrix}\in\mathrm{SL}(2,\mathbb{Z}).$$

则有 $\gcd(p,r)=\gcd(q,s)=1$. 因此存在 $m_1,...,m_l,n_1,...,n_l\in\mathbb{Z}$, 满足

$$A'=V^{n_l}U^{m_l}\cdots V^{n_1}U^{m_1}A=\begin{bmatrix}1 & q'\\0 & s'\end{bmatrix}$$

由于 $A'\in\mathrm{SL}(2,\mathbb{Z})$, 我们有 $s'=1$. 因此存在 $k'\in\mathbb{Z}$, 满足 $A'=U^{k'}$.
由此可知 $A\in\langle U,V\rangle$. 由于 A 为任意选取, 我们有

$$\mathrm{SL}(2,\mathbb{Z})\subset\langle U,V\rangle\subset\mathrm{SL}(2,\mathbb{Z}).$$

结论成立. □

2. **证明 $\mathrm{SL}(2,\mathbb{Z})$ 可以由**

$$\left\{\begin{bmatrix}0 & 1\\-1 & 1\end{bmatrix}, \quad \begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}\right\}$$

生成.

证明. 记

$$C=\begin{bmatrix}0&1\\-1&1\end{bmatrix},\quad D=\begin{bmatrix}0&1\\-1&0\end{bmatrix}.$$

只需证明 $U,V\in\langle C,D\rangle$ 即可.

直接计算可得

$$DC=\begin{bmatrix}0&1\\-1&0\end{bmatrix}\begin{bmatrix}0&1\\-1&1\end{bmatrix}=\begin{bmatrix}-1&1\\0&-1\end{bmatrix}=-U^{-1}.$$

考虑

$$CD=\begin{bmatrix}0&1\\-1&1\end{bmatrix}\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}-1&0\\-1&-1\end{bmatrix}=-V$$

注意到

$$D^2=\begin{bmatrix}0&1\\-1&0\end{bmatrix}^2=\begin{bmatrix}-1&0\\0&-1\end{bmatrix},$$

我们有 $D^3C=U^{-1}$ 以及 $CD^3=V$.

由此可知 $U,V\in\langle C,D\rangle$, 因此 $\mathrm{SL}(2,\mathbb{R})=\langle C,D\rangle$. □

3. **记 $\mathbb{Z}^2$ 中的元素为整系数列向量. 任取向量 $[m,n]^T\in\mathbb{Z}^2$ 和矩阵 $A\in\mathrm{SL}(2,\mathbb{Z})$, 记 $[m',n']^T=A[m,n]^T$. 证明 $\gcd(m,n)=\gcd(m',n')$.**

证明. 记

$$\Phi:\mathrm{SL}(2,\mathbb{Z})\times\mathbb{Z}^2\to\mathbb{Z}^2$$
$$\left(\begin{bmatrix}p&q\\r&s\end{bmatrix},\begin{bmatrix}m\\n\end{bmatrix}\right)\mapsto\begin{bmatrix}pm+qn\\rm+sn\end{bmatrix}$$

考虑 $[m,n]^T\in\mathbb{Z}^2$, 记 $\gcd(m,n)=d$. 记

$$U=\begin{bmatrix}1&1\\0&1\end{bmatrix},\quad V=\begin{bmatrix}1&0\\1&1\end{bmatrix}$$

注意到

$$\begin{aligned}U[m,n]^T&=[m+n,n]^T,\\U^{-1}[m,n]^T&=[m-n,n]^T,\\V[m,n]^T&=[m,n+m]^T,\\V^{-1}[m,n]^T&=[m,n-m]^T.\end{aligned}$$

我们有 $\gcd(m+n,n)=\gcd(m-n,n)=\gcd(m,n+m)=\gcd(m,n-m)=\gcd(m,n)$. 因此结论对 U,U^{-1},V,V^{-1} 成立. 由于注意到 $\mathrm{SL}(2,\mathbb{Z})$ 由

$$\left\{\begin{bmatrix}1&1\\0&1\end{bmatrix},\quad\begin{bmatrix}1&0\\1&1\end{bmatrix}\right\}$$

生成. 因此任取 $A\in\mathrm{SL}(2,\mathbb{Z})$, 存在 $k_1,...,k_s,l_1,...,l_s\in\mathbb{Z}$, 满足

$$A=U^{k_1}V^{l_1}\cdots U^{k_s}V^{l_s}.$$

由归纳法可知 $\gcd(m',n')=\gcd(m,n)$. □

4. **该群作用是可递的么? 为什么?**

解. 不是可递的. 任取非零向量 $[m,n]^T\in\mathbb{Z}^2$, 以及 $d\in\mathbb{Z}\setminus\{0,\pm1\}$, 有 $\gcd(m,n)\neq\gcd(dm,dn)$. 因此不存在 $A\in\mathrm{SL}(2,\mathbb{Z})$ 将 $[m,n]^T$ 送到 $[dm,dn]^T$. □

三, 任取两个群 G 和 H, 考虑二者的笛卡尔积 $G \times H$. 映射

$$\begin{aligned}(G\times H)\times(G\times H) &\to G\times H\\ ((g,h),(g',h')) &\mapsto (gg',hh')\end{aligned}$$

给出 $G \times H$ 上一个群结构. 我们称 $G \times H$ 为 G 和 H 的直积.

我们考虑群 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 和群 $\mathbb{Z}_9$.

(任取 $n \in \mathbb{Z}$, 记 n 模 k 同余类为 n_k.)

1. **分别给出两个群所有的子群. 比较两个群子群的信息证明 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 和 $\mathbb{Z}_9$ 不同构.**

解. 群 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 的子群有

$$\{(0_3,0_3)\}, \langle(1_3,0_3)\rangle, \langle(0_3,1_3)\rangle, \langle(1_3,1_3)\rangle, \langle(1_3,2_3)\rangle, \mathbb{Z}_3\times\mathbb{Z}_3.$$

群 $\mathbb{Z}_9$ 的子群有

$$\{0_9\}, \langle 3_9\rangle, \mathbb{Z}_9.$$

注意到二者子群数目不同, 因此不同构.

二者的 3 阶子群数目不同, 也可以说明不同构. □

2. **设 G 为一个 9 阶群.**

   a) **证明 G 是一个交换群.**

证明. 注意到 $|G| = 9 = 3^2$.

考虑 G 在 G 上的伴随作用可知, $|Z(G)| = 3$ 或 9. 若为 9, 则结论成立. 若为 3, 则考虑商群 $G/Z(G)$. 注意到 $Z(G)$ 和 $G/Z(G)$ 都为循环群. 因此存在 $a, b \in G$, 满足

$$Z(G) = \langle a\rangle, \quad G/Z(G) = \langle bZ(G)\rangle.$$

因此 $G = \{b^i a^j \mid i, j \in \mathbb{Z}\}$. 任取 $i_1, i_2, j_1, j_2 \in \mathbb{Z}$, 由中心的定义我们有

$$b^{i_1}a^{j_1}b^{i_2}a^{j_2} = b^{i_1}b^{i_2}a^{j_1}a^{j_2} = b_2^{i}b^{i_1}a^{j_2}a^{j_1} = b^{i_2}a^{j_2}b^{i_1}a^{j_1}.$$

因此 G 交换, 即 $|Z(G)| = 9$. 所以不存在 $Z(G) = 3$ 的情形. 综上所述 G 交换. □

   b) **证明 G 或者同构于 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 或者同构于 $\mathbb{Z}_9$.**

证明. 设 G 为一个交换群. 考虑 G 中是否有 9 阶元素. 若有, 则 G 有一个 9 阶循环子群. 由于 G 为一个 9 阶群, 因此 G 就是该循环子群, 有 $G \cong \mathbb{Z}_9$.

若 G 没有 9 阶元素, 则元素的阶只能是 1 或者 3. 设 a 为一个 3 阶元, 则存在 $b \in G \setminus \langle a\rangle$, 也为 3 阶元. 考虑 a 和 b 生成的子群 $\langle a, b\rangle$. 直接验证可知

$$\begin{aligned} f : \langle a, b\rangle &\to \mathbb{Z}_3\times\mathbb{Z}_3\\ a^i b^j &\mapsto (i_3, j_3)\end{aligned}$$

是一个群同构. 注意到该子群中有 9 个元素, 因此等于 G. □

3. **给出所有 $\mathbb{Z}_9$ 到 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 的群同态.**

解. 注意到 $\mathbb{Z}_9$ 是一个循环群. 取生成元 1_9. 由于 $o(1_9)=9$, 因此任取 $f\in \mathrm{Hom}(\mathbb{Z}_9, \mathbb{Z}_3\times\mathbb{Z}_3)$, 都有 $o(f(1_9))\mid 9$, 即 $o(f(1_9))\in\{1,3,9\}$. 反之, 任取 $a\in\mathbb{Z}_3\times\mathbb{Z}_3$, 满足 $o(a)\in\{1,3,9\}$, 都有唯一的一个从 $\mathbb{Z}_9$ 到 $\mathbb{Z}_3\times\mathbb{Z}_3$ 的群同态.

因此

$$\mathrm{Hom}(\mathbb{Z}_9, \mathbb{Z}_3\times\mathbb{Z}_3)=\{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8,f_9\}$$

分别将 1_9 送到 $(0_3,0_3)$, $(1_3,0_3)$, $(2_3,0_3)$, $(0_3,1_3)$,$(0_3,2_3)$, $(1_3,1_3)$,$(1_3,2_3)$, $(2_3,1_3)$,$(2_3,2_3)$. $\square$

四, 记 G 为一个群. 对任意 $a,b\in G$, 记二者的换位子为

$$[a,b]:=aba^{-1}b^{-1}.$$

我们称 G 所有换位子生成的群为 G 的换位子群, 并记作

$$[G,G]:=\langle\{[a,b]\in G\mid a,b\in G\}\rangle.$$

1. 证明 $[G,G]$ 为 G 的一个正规子群

证明. 只需证明对任意 $c\in G$, 都有

$$c[G,G]c^{-1}\subset[G,G],$$

即可.

对任意 $g\in[G,G]$, 存在 $a_1,...,a_k,b_1,...,b_k\in G$, 满足

$$g=[a_1,b_1]\cdots[a_k,b_k].$$

任取 $c\in G$, 我们有

$$cgc^{-1}=c[a_1,b_1]\cdots[a_k,b_k]c^{-1}=c[a_1,b_1]c^{-1}\cdots c[a_k,b_k]c^{-1}.$$

因此 $c[G,G]c^{-1}$ 由

$$\Omega=\{c[a,b]c^{-1}\mid a,b\in G\},$$

生成.

下证 $\Omega\subset[G,G]$. 对任意 $a,b,c\in G$, 我们有

$$c[a,b]c^{-1}=c(aba^{-1}b^{-1})c^{-1}=(cac^{-1})(cbc^{-1})(ca^{-1}c^{-1})(cb^{-1}c^{-1})=[cac^{-1},cbc^{-1}]\in[G,G].$$

因此 $\Omega\subset[G,G]$, 进而有 $c[G,G]c^{-1}=\langle\Omega\rangle\subset[G,G]$.

因此有

$$[G,G]\lhd G.$$

$\square$

2. 证明商群 $G/[G,G]$ 交换.

证明. 考虑商群 $G/[G,G]$. 任取 $a,b\in G$, 有

$$a[G,G]b[G,G]=ab[G,G]=ba(a^{-1}b^{-1}ab)[G,G]=ba[G,G]=b[G,G]a[G,G].$$

因此 $G/[G,G]$ 交换. $\square$

3. 记 $\pi:G\to G/[G,G]$ 为自然同态. 任取交换群 H 和群同态 $\varphi:G\to H$, 证明存在唯一的一个同态

$$\overline{\varphi}:G/[G,G]\to H$$

满足 $\varphi=\overline{\varphi}\circ\pi$.

证明. 任取 $a, b \in G$, 注意到

$$\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = [\varphi(a), \varphi(b)] = e_H \in H,$$

因此任取 $b, c \in a[G,G]$, 都有

$$\varphi(b) = \varphi(c).$$

因此我们有以下映射

$$\begin{aligned} \overline{\varphi} : G/[G,G] &\to H \\ a[G,G] &\mapsto \varphi(a) \end{aligned}$$

任取 $a, b \in G$, 我们有

$$\overline{\varphi}(ab[G,G]) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a[G,G])\overline{\varphi}(b[G,G]).$$

因此 $\overline{\varphi}$ 是一个群同态, 且对任意 $a \in G$, 满足 $\varphi(a) = (\overline{\varphi} \circ \pi)(a)$.

下证唯一性. 设群同态 $\psi : G/[G,G] \to H$ 也满足 $\varphi = \psi \circ \pi$, 注意到任取 $a[G,G] \in G/[G,G]$, 我们都有

$$\psi(a[G,G]) = \varphi(a) = \overline{\varphi}(a[G,G]),$$

因此 $\psi = \overline{\varphi}$, 该同态唯一. □

五,

1. **给出 S_5 上一个 Sylow 5-子群的例子, 并求 S_5 中 Sylow 5-子群的个数.**

解. 注意到 $|S_5| = 120 = 2^3 \times 3 \times 5$. 因此 S_5 的 Sylow 5-子群是一个 5 阶循环群.

例子 $\langle(12345)\rangle$.

记 n_5 为 Sylow 5-子群的个数, 我们有 $n_5 \mid 24$ 且 $n_5 \equiv 1 \mod 5$. 因此 $n_5 = 5k+1 \mid 24$. 所有 k 的可能取值为 $0, 1$. 注意到 $\langle(13245)\rangle \neq \langle(12345)\rangle$, 因此 $k = 1$, 即有 6 个 Sylow 5-子群. □

2. **记 P 为 S_5 的一个 Sylow 5-子群. 证明 P 的正规化子**

$$N := \{\sigma \in S_5 \mid \sigma P \sigma^{-1} = P\}$$

满足 $|N| = 20$.

证明一. 考虑

$$P = \langle(12345)\rangle = \{e, (12345), (13524), (14253), (15432)\}.$$

注意到这是一个循环群, 因此 (12345) 的像决定 P 到共轭子群 $\sigma P \sigma^{-1}$ 的同构.

令任取 σ 满足 $P = \sigma P \sigma^{-1}$, 注意到 $\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))$ 为 P 的生成元, 因此有 4 个可能的取值. 每个取值有 5 种写法:

$$(i_1 i_2 i_3 i_4 i_5) = (i_2 i_3 i_4 i_5 i_1) = (i_3 i_4 i_5 i_1 i_2) = (i_4 i_5 i_1 i_2 i_3) = (i_5 i_1 i_2 i_3 i_4).$$

因此 $|N| = 4 \times 5 = 20$. □

证明二. 考虑 N 在 P 上的伴随作用. 注意到任取 5 轮换 $(i_1 i_2 i_3 i_4 i_5) \in P$, 记 $\sigma \in S_5$, 满足

$$\sigma(1) = i_1, \quad \sigma(2) = i_2, \quad \sigma(3) = i_3, \quad \sigma(4) = i_4, \quad \sigma(5) = i_5$$

都有 $\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)) = (i_1 i_2 i_3 i_4 i_5)$. 因此 N 在 P 上的作用有两个轨道

$$\{e\}, \quad \{(12345), (13524), (14253), (15432)\}.$$

利用轨道稳定化子之间的关系, 我们有

$$|4| = [N : \mathrm{Stab}(12345)].$$

任取 $\sigma \in \mathrm{Stab}(12345)$, 有 σ 与 (12345) 交换, 因此 $\mathrm{Stab}(12345)$ 为 (12345) 的中心化子 $Z(12345)$. 由于 $\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)) \in P$, 因此 $\sigma \in P$. 反之 P 为交换群, 因此 P 在 (12345) 的中心化子中, 综上所述我们有 $P = Z(12345)$.

我们有

$$4 = \frac{|N|}{Z(12345)} = \frac{|N|}{|P|}.$$

因此 $|N| = 4 \times 5 = 20$.

□

证明三. 记所有 S_5 的 5 阶子群 (Sylow 5-子群) 的集合为

$$\Omega = \{P = P_1, P_2, ..., P_6\},$$

并考虑 S_5 在 Ω 上的共轭作用. 注意到 $N = \mathrm{Stab}(P_1)$.
由 Sylow 第二定理知道该作用可递, 因此只有一个轨道. 由轨道稳定化子之间的关系可知

$$|\Omega| = [S_5 : \mathrm{Stab}(P_1)] = [S_5 : N].$$

因此

$$|N| = \frac{|S_5|}{|\Omega|} = \frac{120}{6} = 20.$$

□

3. **考虑 S_5 在 $X = S_5/N$ 上的左平移作用**

$$\begin{aligned} \Phi : S_5 \times X &\to X \\ (\sigma, \tau N) &\mapsto \sigma(\tau N) := (\sigma\tau)N. \end{aligned}$$

证明该作用是可递的.

证明. 任取 $\sigma N \in S_5/N$, 我们有 $\sigma(N) = \sigma N$, 因此 S_5/N 为 N 的轨道, 作用可递. □

4. **对任意 $\sigma \in S_5$, 记**

$$\begin{aligned} \Phi_\sigma : X &\to X \\ \tau N &\mapsto \Phi(\sigma, \tau N) \end{aligned}$$

证明

$$\begin{aligned} \varphi : S_5 &\to S_X \\ \sigma &\mapsto \Phi_\sigma \end{aligned}$$

为一个单同态.

证明. 映射 φ 为作用 Φ 诱导的群同态. 下证 φ 为单射, 即 $\ker\varphi = \{e\}$. 注意到

$$\ker\varphi \lhd S_5 \text{ 且 } \ker\varphi \lhd \mathrm{Stab}(N).$$

利用轨道稳定化子的关系可知

$$|S_5/N| = [S_5 : \mathrm{Stab}(N)].$$

因此

$$|\ker\varphi| \,\Big|\, |\mathrm{Stab}(N)| = \frac{|S_5|}{|S_5/N|} = \frac{120}{6} = 20.$$

也可以直接证明 $\mathrm{Stab}(N) = N$. 任取 $\sigma \in S_5$, 则有 $\sigma N = N$ 当且仅当 $\sigma \in N$. 因此有 $\mathrm{Stab}(N) = N$.
由于 S_5 的正规子群的阶为 1, 60 和 120. 因此 $|\ker\varphi| = 1$, 即 φ 为单射. □