

## 第四次习题课

伍文超 MJTDX USTC

1: (1) 证明  $GL_2(2)$  同构于  $S_3$ .

(2) 证明  $PGL_2(3) \cong S_4$ . 从而也有  $PSL_2(3) \cong A_4$  因为它是  $PGL_2(3)$  的指数为 2 的子群.

$GL_n(\mathbb{F}_q)$  简记为  $GL_n(q)$ ,  $q$  是素数的幂.

**证明:** (1): 考虑:

$$GL_2(2) \xrightarrow{\quad} (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \setminus \{(0,0)^T\} \longrightarrow (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \setminus \{(0,0)^T\}$$

上述作用是合理的, 因为  $GL_2(2)$  中任意一个元素给出  $S = (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \setminus \{(0,0)^T\}$  的一个置换 (元素是可逆矩阵). 通过计算可知  $A \in GL_2(2)$  在  $S$  上作用平凡当且仅当  $A = I_2$ . 因此有单射  $GL_2(2) \hookrightarrow S_3$ . 最后由  $|GL_2(2)| = 2 \cdot 3 = 6 = |S_3|$  可知二者同构.

(2) 类似于 (1), 考虑  $\mathbb{Z}_3 \oplus \mathbb{Z}_3$  中的四个子集  $V_i = \{a(i,1) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 | a = 0, 1, 2\}, i = 0, 1, 2, V_\infty = \{a(1,0) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 | a = 0, 1, 2\}$ . 记  $S = \{V_0, V_1, V_2, V_\infty\}$ . 同样的  $GL_2(3)$  中任意一个元素给出  $S$  的一个置换 (合理的), 而且通过计算可知  $A \in GL_2(3)$  在  $S$  上作用平凡当且仅当  $A$  是标量矩阵 (scalar matrices). 因此有单射  $GL_2(3)/Z(GL_2(3)) = PGL_2(3) \hookrightarrow S_4$ . 最后由  $|GL_2(3)| = 24 = |S_4|$  可知二者同构.  $\square$

**Remark:** (1) 类似的, 我们可以取  $\mathbb{F}_q \oplus \mathbb{F}_q$  中的  $q+1$  个子集 (一维子空间)  $V_i = \{a(i,1) \in \mathbb{F}_q \oplus \mathbb{F}_q | a = 0, 1, \dots, q-1\}, i = 0, 1, \dots, q-1, V_\infty = \{a(1,0) \in \mathbb{F}_q \oplus \mathbb{F}_q | a = 0, 1, \dots, p-1\}$ , 记  $S = \{V_0, V_1, V_2, \dots, V_{q-1}, V_\infty\}$ .

同样的  $GL_2(q)$  中任意一个元素给出  $S$  的一个置换 (合理的), 且只有标量矩阵给出平凡作用, 因此我们得到单射  $PGL_2(q) \hookrightarrow S_{q+1}$ .

(2) 在线性代数中, 我们定义射影空间为  $\mathbb{R}^n$  的所有一维子空间 (直线) 构成的集合.  $n=2$  时就是射影直线,  $n=3$  时就是射影平面. 在此处我们可以类似的命名 (1) 中的集合为  $\mathbb{F}_q$  上的射影直线, 不妨记为  $PL(q)$ . 根据我们的定义,  $PL(q) = \{V_0, V_1, V_2, \dots, V_{q-1}, V_\infty\} \leftrightarrow \mathbb{F}_q \cup \{\infty\}$  (将每一个直线视作一个点), 我们将二者视为恒等的. 如果取  $\mathbb{F}_q^3$  的二维子空间构成的集合则是射影平面 (有限射影平面, 有  $q^2 + q + 1$  个点和线, 每条线上  $q+1$  个点, 每个点关联  $q+1$  条线.)

(3) 任意  $A = \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in GL_2(q)$ , 我们有  $A(k(i,1)^T) = k(ai + b, ci + d), A(k(1,0)^T) = k(a, 0)$ . 等价的:

$$GL_2(q) \xrightarrow{\quad} PL(q) \longrightarrow PL(q)$$

$$z \longrightarrow \frac{az+b}{cz+d} = \frac{a+b/z}{c+d/z}$$

2: 旋转群  $SO(3)$  是单群 ( $SO(n)?$ ).

**证明:** 第一次习题课我们证明了  $SU(2)/\{\pm I_2\} \cong SO(3)$ , 第四次作业说明了  $SU(2)$  的包含  $\{\pm I_2\}$  的正规子群和  $SO(3)$  的正规子群是一一对应的, 因此我们只需要说明  $SU(2)$  的真包含  $\{\pm I_2\}$  的正规子群  $G$  等于  $SU(2)$ . 回顾:

$$SU(2) = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \middle| |x|^2 + |y|^2 = 1, x, y \in \mathbb{C} \right\}$$

从线性代数我们知道任意  $A \in SU(2)$  酉相似于对角矩阵, 特征多项式有共轭复根或都为  $\pm 1$ , 记为  $B_\varphi = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}$ ,  $\varphi \in [0, 2\pi)$ . 因此  $SU(2)$  的每个共轭类都含有对角矩阵, 而由于正规子群是共轭类的无交并, 因此  $G$  包含一个对角矩阵 ( $\neq \pm I_2$ ), 记为  $B_{\alpha_0}$ ,  $\alpha_0 \neq 0, \pi$ . 自然的  $B_{\alpha_0}^{-1} = B_{2\pi-\alpha_0} \in G$ , 故设  $0 < \alpha_0 < \pi$ . 考虑  $B_{\alpha_0}$  和  $\forall A \in G$  的换位子:

$$\begin{aligned} [B_{\alpha_0}, A] &= B_{\alpha_0} A B_{\alpha_0}^{-1} A^{-1} \\ &= \begin{pmatrix} e^{i\alpha_0} & 0 \\ 0 & e^{-i\alpha_0} \end{pmatrix} \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \begin{pmatrix} e^{-i\alpha_0} & 0 \\ 0 & e^{i\alpha_0} \end{pmatrix} \begin{pmatrix} \bar{x} & -y \\ \bar{y} & x \end{pmatrix} \\ &= \begin{pmatrix} |x|^2 + |y|^2 e^{i2\alpha_0} & (e^{i2\alpha_0} - 1)xy \\ (1 - e^{-i2\alpha_0})\bar{x}\bar{y} & |x|^2 + |y|^2 e^{-i2\alpha_0} \end{pmatrix}. \end{aligned}$$

$tr([B_{\alpha_0}, A]) = 2|x|^2 + |y|^2(e^{i2\alpha_0} + e^{-i2\alpha_0}) = 2(1 - |y|^2) + 2|y|^2(-2\sin^2\alpha_0 + 1) = 2(1 - 2|y|^2\sin^2\alpha_0)$ . 设  $[B_{\alpha_0}, A]$  和  $B_{\alpha_1}$  共轭, 故  $e^{i\alpha_1} + e^{-i\alpha_1} = 2\cos\alpha_1 = 2 - 4|y|^2\sin^2\alpha_0 \Rightarrow \cos\alpha_1 = 1 - 2|y|^2\sin^2\alpha_0 \in [1 - 2\sin^2\alpha_0, 1] = [\cos 2\alpha_0, 1]$ , 因为  $0 \leq |y|^2 \leq 1$ .

不妨设  $2\alpha_0 \leq 2\pi - 2\alpha_0$  (另一边类似), 则有  $\alpha_1$  可以取遍  $[0, 2\alpha_0], [2\pi - 2\alpha_0, 2\pi]$ . 也就是说  $B_{\alpha_1} \in G, \forall \alpha_1 \in [0, 2\alpha_0]$ . 因为对于任意的  $\alpha > 0$ , 存在  $n \in \mathbb{Z}_{\geq 0}$  使得  $0 < \alpha/n \leq 2\alpha_0$ , 因此  $B_\alpha \in G, \forall \alpha$ , 即  $G = SU(2)$ .  $\square$

**Remark:** 一般的,  $SO(2n+1)$  是单群,  $SO(2n)/\{\pm I_{2n}\}$  是单群.

3: 如果域  $F$  有至少四个元素, 则  $SL_2(F)/\{\pm I_2\}$  是单群 (一般的,  $PSL_n(F_p)$  呢?).

**证明:** 我们先给出一些需要用到的子群:

$$\begin{aligned} U &= \left\{ u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in F \right\} \\ V &= \left\{ v(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \mid x \in F \right\} \\ D &= \left\{ d(x) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in F^* \right\} \\ B &= DU = UD = \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \mid x \in F^*, y \in F \right\} \end{aligned}$$

取  $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ , 断言  $G = SL_2(F)$  有双陪集分解  $G = B \cup BwB$ . 实际上:

- (a)  $\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ , 若  $c = 0$ , 则  $A \in B$ ; 若  $c \neq 0$ , 则  $\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} f & g \\ 0 & f^{-1} \end{pmatrix} = \begin{pmatrix} -yf & -yg + xf^{-1} \\ -x^{-1}f & -x^{-1}g \end{pmatrix}$ , 总是可以取到  $x, y, f, g$  使得其乘积为  $A$ .
- (b)  $A \in B \cap BwB \Rightarrow -x^{-1}f = 0$ , 矛盾.

再考虑  $[G, G] = \{ABA^{-1}B^{-1} \in G | A, B \in G\}$ , 容易证明  $[G, G]$  是  $G$  的正规子群.  $d(a)u(b)d(a)^{-1}u(b)^{-1} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b(a^2 - 1) \\ 0 & 1 \end{pmatrix}$  因此只需要  $a^2 \neq 1$ , 则可以得到  $U \subset [B, B] \subset U$ , 故  $U = [B, B] \leq [G, G]$ . 进而  $wUw^{-1} = V \leq [G, G] \Rightarrow w = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in [G, G] \Rightarrow [G, G] = G$ .

设  $K$  是  $G$  的正规子群, 则  $B \leq KB$ . 若  $B = KB \Rightarrow K \in B \Rightarrow K = CKC^{-1} \subset \bigcap_{A \in G} ABA^{-1} = \{\pm I_2\}$ .

若  $B \neq KB$ , 则存在  $h \in KB \setminus B$  且  $h = b_1wb_2 \Rightarrow w \in KB \Rightarrow KB = G$ . 从而  $w = kb, k \in K, b \in B \Rightarrow V = wUw^{-1} = kbUb^{-1}k^{-1} = kUk^{-1} = kk_1U \subset KU \Rightarrow KU = G$ , 故  $G/K = KU/K \cong U/U \cap K$  是交换群, 因此  $G = [G, G] \leq K \Rightarrow K = G$ .

□

**Remark:** 一般的, 若  $n \geq 3$ , 则  $PSL_n(q)$  是单群 (利用 Iwasawa 定理).