第十四周作业参考解答及补充

作业

1. (习题 4.2.2)

证明:

(1) $S_n = \langle (1\,2),\ (1\,3),\ \cdots,\ (1\,n)\rangle$, 即 S_n 由对换 $(1\,2),\ (1\,3),\ \cdots,\ (1\,n)$ 生成;

(2) S_n 可由 $(1\,2)$ 和 $(1\,2\,3\cdots n)$ 生成, 即

$$S_n = \big\langle (1\,2), (1\,2\,3\cdots n)\big\rangle.$$

proof

(1) 这是教材推论 4.2.2 的直接结果, 任意置换总能写成有限个对换的乘积, 而 $(i\,j) = (1\,i)(1\,j)(1\,i)$.

(2) 由 (1), 只需证明 $(1\,3), \cdots, (1\,n)$ 都可以被 $(1\,2)$ 和 $(1\,2\cdots n)$ 生成. 事实上 $(1\,n) = (1\,2\cdots n)^{-1}(1\,2)(1\,2\cdots n)$, $(1\,i) = (1\,(i+1))(i\,(i+1))(1\,(i+1))$, 且 $(i\,(i+1)) = (1\,2\cdots n)^{-(n-i+1)}(1\,2)(1\,2\cdots n)^{n-i+1}, 2 < i < n$(其实就是把 i 和 $i+1$ 先移到 1 和 2 的位置上, 用 $(1\,2)$ 对换, 再移回去).

$\square$

2. (习题 4.2.4)

设 $A_n = \{\pi \in S_n \mid \varepsilon_\pi = 1\} \subseteq S_n$, 证明:

(1) $A_n \lhd S_n$ (即 A_n 是 S_n 的正规子群);

(2) A_n 由 3-循环生成, 事实上, $A_n = \langle (1\,2\,3),\ (1\,2\,4),\ \cdots (1\,2\,n)\rangle$.(提示: 利用 $(a\,b)\cdot(b\,c) = (a\,b\,c)$, $(a\,b)\cdot(c\,d) = (a\,b)\cdot(b\,c)\cdot(b\,c)\cdot(c\,d)$.)

proof

(1) $\pi \mapsto \varepsilon_\pi$ 实际上是一个群同态 $S_n \to \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$. 而 A_n 恰好是这个同态的 kernel.

(2) 根据提示有 $(a\,b)(c\,d) = (abc)(bcd)$, 因此所有的 3-循环能生成 A_n, 只需说明任意 3-循环在 $\langle (1\,2\,3),\ (1\,2\,4),\ \cdots (1\,2\,n)\rangle$ 中. 我们可以做拆解, 对

$i, j, k \neq 1, 2$, 反复用上面的等式凑出来 $(1\,2\,m)$.

$$\begin{aligned}(1\,j\,k) &= (k\,1)(1\,j) = (k\,1)(1\,2)(1\,2)(2\,k)(2\,k)(1\,j) = (1\,2\,k)(1\,2\,k)(1\,j)(2\,k)\\ &= (1\,2\,k)(1\,2\,k)(1\,j)(1\,2)(1\,2)(2\,k) = (1\,2\,k)(1\,2\,k)(1\,2\,j)(1\,2\,k)\end{aligned}$$

同样的可以凑出

$$(i\,j\,k) = (i\,j)(1\,j)(1\,j)(j\,k) = (1\,i\,j)(1\,j\,k)$$

□

3. (习题 4.2.5)

群 G 中的两个元素 x, y 称为在 G 中共轭, 如果存在 $a \in G$, 使 $axa^{-1} = y$. 试证明:

(1) $\forall \pi \in S_n\, \alpha = (i_1\, i_2 \cdots i_r) \in S_n$ 有公式

$$\pi \cdot \alpha \cdot \pi^{-1} = (\pi(i_1)\, \pi(i_2) \cdots \pi(i_r)).$$

(2) 所有 3-循环在 S_n 中相互共轭. (所以 S_n 中包含 3-循环的正规子群必包含 A_n.)

(3) 如果 $n \geqslant 5$, 则所有 3-循环在 A_n 中相互共轭, 即对于任意 3-循环 $x, y \in A_n$, 存在 $a \in A_n$, 使 $axa^{-1} = y$.

proof

(1) 按定义验证, 若 $\pi \cdot \alpha \cdot \pi^{-1}(i) = \pi(\alpha(\pi^{-1}(i)))$. 若 $i \notin \{\pi(i_1), \pi(i_2), \cdots, \pi(i_r)\} \iff \pi^{-1}(i) \notin \{i_1, i_2, \cdots, i_r\}$, 则 $\pi(\alpha(\pi^{-1}(i))) = \pi(\pi^{-1}(i)) = i$. 反之 $i \in \{\pi(i_1), \pi(i_2), \cdots, \pi(i_r)\}$, 有 $\pi(\alpha(\pi^{-1}(i))) = \pi(\alpha(i_k)) = (\pi(i_1)\, \pi(i_2) \cdots \pi(i_r))(i)$.

(2) (1) 的推论. 若 α 是 3-循环, 任意的 $\pi \in S_n$, $\pi\alpha\pi^{-1}$ 仍是 3-循环. 具体来说, 对两个 3-循环 $\alpha_1 = (a_1\, b_1\, c_1)$ 和 $\alpha_2 = (a_2\, b_2\, c_2)$, 则令 $\pi = \begin{pmatrix} a_1 & b_1 & c_1 & \cdots \\ a_2 & b_2 & c_2 & \cdots \end{pmatrix}$ 即可.

(3) 设 $x = (i_1\, i_2\, i_3), y = (j_1\, j_2\, j_3)$. 当 $n \geqslant 5$ 时, 由 (2), 考虑

$$a_1 = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & \cdots \\ j_1 & j_2 & j_3 & j_4 & j_5 & \cdots \end{pmatrix}, a_2 = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & \cdots \\ j_1 & j_2 & j_3 & j_5 & j_4 & \cdots \end{pmatrix}$$

则由 (2) 可知 $k = 1, 2$ 都满足 $a_k x a_k^{-1} = y$, 但是 $a_2 = a_1(j_4, j_5)$, 即刚好差一个对换, 那么 a_1, a_2 必然一奇一偶, 因此存在 $a \in A_n$ 使得 $axa^{-1} = y$.

□

4. (习题 4.2.7)

证明: 所有 4 阶群 G 都是交换群. 在同构意义下, G 要么是循环群, 要么同构于下述克莱因 4 元群:

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \subseteq S_4.$$

(提示: 如果 $x^2 = 1$ 对 G 中所有元成立, 则 $\forall a, b \in G$, 有 $abab = 1 \implies ab = b^{-1}a^{-1} = b(b^{-1})^2 \cdot (a^{-1})^2 a = ba$.)

proof

对于这种阶很小的群, 我们可以直接分析 4 阶群的乘法表, 这其实和数独有点像. 乘法表的每一行或每一列是不能有相同元素的, 因为左乘映射是单的 $ga = gb \implies a = b$, 右乘也一样.

设 $G = \{e, a, b, c\}$, e 是单位元. 那么首先有

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

由 1.3.10, G 有 2 阶元, 不妨设 $a^2 = e$, 则 $ab \neq e, a, b$, 只能是 c, ac, ba, ca 同理, 得到

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

此时若 $b^2 = e$, 则得到

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

否则 $b^2 = a$, 得到

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

第二种实际上是 $\mathbb{Z}/4\mathbb{Z}$ 是循环群, 生成元是 b 或者 c, 自然是交换群. 第一种就是题干中的克莱因 4 元群. $\square$

注:

对于阶很大的群这种方法便不适用了. 事实上若 $|G| = p^2$, 则 G 一定是 Abel 群, 其中 p 是素数. 这是共轭作用得到的分类公式的直接推论. 即教材引理 4.2.2 证明的中间结果

$$|G| = C(G) + \sum_{O(x)>1} |O(x)|, \quad |O(x)| = [G : H_x]$$

这里的 H_x 是在共轭作用 $g \cdot x = gxg^{-1}$ 下的稳定子, 又称做 x 的中心化子 (所有和 x 交换的元素构成的子群), 和 1.2.4 是类似, 一般记作 $C(x)$. 这个等式的每一项都是 $|G|$ 的因子, 因此若 G 不是 Abel 群, 即 $C(G) \neq G$, 那么只能是 $|C(G)| = p$. 但这是不可能的. 因为对 $x \notin C(G)$, $|C(x)|$ 也是 p^2 的因子, 而按定义 $C(G)$ 是严格包含于 $C(x)$ 的, $C(G) \subsetneq C(x)$, 这意味着 $|C(x)| > |C(G)| = p$, 那么 $|C(x)| = p^2$, 这就矛盾了, 因为 $x \notin C(G)$, 所以 $C(x)$ 不可能等于 G.
对一般的群作用 $G \times X \to X$, X 是有限集, 教材的引理 4.5.2 事实上可以表示为分类公式 (class formula)

$$|S| = |Z| + \sum_{|O(x)|>1} [G : \mathrm{stab}(x)] = |Z| + \sum_{|O(x)|>1} |O(x)|.$$

其中 Z 称为该群作用下的不动点集, $x \in Z \iff \mathrm{stab}(x) = G \iff O(x) = \{x\}$. 若 G 是 p-群, 则有

$$|Z| \equiv |S| \mod p$$