

MATH 1530 Problem Set 5

Tanish Makadia

(Collaborated with Esmé and Kazuya)

March 2023

Problem 1. How many elements of order 6 are in S_7 ?

Proof. By (Gallian, 5.1), every permutation of a finite set can be expressed as a product of disjoint cycles. Additionally, by (Gallian, 5.3), the order of a permutation in disjoint cycle form is the **lcm** of lengths of the disjoint cycles.

Let $P = \{s \in S_7 \mid |s| = 6\}$. We must find the cardinality of P . Let $p \in P$. From above, p must have a disjoint cycle form in which the **lcm** of the disjoint cycle lengths equals 6. Therefore, the disjoint cycle form of p must fall under one of the following cases: (note that the order of the disjoint cycles does not matter since they are commutative)

- **Case 1 (lengths: 2, 2, 3):** $p = (a_1, a_2)(b_1, b_2)(c_1, c_2, c_3)$. In this case, the number of ways to construct p using elements of S_7 is:

$$\frac{1}{2} \left(\frac{7!}{5! \cdot 2} \cdot \frac{5!}{3! \cdot 2} \cdot \frac{3!}{3} \right) = 210$$

- **Case 2 (lengths: 3, 2, 1, 1):** $p = (a_1, a_2, a_3)(b_1, b_2)(c_1)(d_1)$. In this case, the number of ways to construct p is:

$$\frac{7!}{4! \cdot 3} \cdot \frac{4!}{2! \cdot 2} = 420$$

- **Case 3 (lengths: 6, 1):** $p = (a_1, a_2, a_3, a_4, a_5, a_6)(b_1)$. In this case, the number of ways to construct p is:

$$\frac{7!}{1! \cdot 6} = 840$$

Therefore, the number of elements of order 6 in S_7 is $\text{card}(P) = 210 + 420 + 840 = 1470$. \square

Problem 2. Let D_4 denote the rigid operations on a square taking the square back to itself (i.e., the symmetries of the square). For example, rotating the square by π is a rigid operation taking the square back to itself. This is called the *dihedral group*, and it is a group under composition.

Label the vertices of the square from 1 to 4. Use this to represent the elements of D_4 a subgroup of S_4 (that is, list the elements of D_4 using cycle notation). What is the order of D_4 ? Is D_4 isomorphic to S_4 ?

Proof. The elements of D_4 are the following permutations:

1.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 4 3</div>	$\xrightarrow[\text{e}]{\text{identity}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 4 3</div>
2.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ↔ 4 3</div>	$\xrightarrow[(1,2)(4,3)]{\text{horizontal flip}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">2 1 3 4</div>
3.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ↕ 4 3</div>	$\xrightarrow[(1,4)(2,3)]{\text{vertical flip}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">4 3 1 2</div>
4.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ↗ 4 3</div>	$\xrightarrow[(2,4)]{\text{left diagonal flip}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 4 2 3</div>
5.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ↖ 4 3</div>	$\xrightarrow[(1,3)]{\text{right diagonal flip}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">3 2 4 1</div>
6.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ↻ 4 3</div>	$\xrightarrow[(1,2,3,4)]{\text{clockwise rotation}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">4 1 3 2</div>
7.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ② 4 3</div>	$\xrightarrow[(1,3)(2,4)]{\text{clockwise rotation (x2)}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">3 4 2 1</div>
8.	<div style="border: 1px solid black; padding: 5px; display: inline-block;">1 2 ③ 4 3</div>	$\xrightarrow[(1,4,3,2)]{\text{clockwise rotation (x3)}}$	<div style="border: 1px solid black; padding: 5px; display: inline-block;">2 3 1 4</div>

Evidently, $|D_4| = 8$. Since $|S_4| = 4! = 24 \neq 8$, by (Gallian, 6.2.7), we have that $D_4 \not\cong S_4$. \square

Problem 3. Prove that a permutation with odd order must be an even permutation. Show that the converse is false.

Proof. Let \mathbf{p} be a permutation such that $|\mathbf{p}| = \mathbf{n}$ where \mathbf{n} is odd. We have that, $\mathbf{p}^{\mathbf{n}} = \mathbf{e}$. By (Gallian, 5.4), $\mathbf{p} = \beta_1 \cdots \beta_r$ where each β_i is a two-cycle. Combining these two equations, we obtain $(\beta_1 \cdots \beta_r)^{\mathbf{n}} = \mathbf{e}$. For contradiction, suppose r is odd. Thus, we have that

$$\begin{aligned} \mathbf{e} &= (\beta_1 \cdots \beta_r)^{\mathbf{n}} \\ &= (\beta_1 \cdots \beta_r)^{\mathbf{n} \text{ times}} (\beta_1 \cdots \beta_r) \\ &= \beta_1 \cdots \beta_{\mathbf{n}r} \end{aligned}$$

By lemma 1, $\mathbf{n}r$ is odd. Since \mathbf{e} must equal the product of an even number of two cycles, this is a contradiction. Therefore, r must be even which implies that \mathbf{p} is an even permutation. \square

Lemma 1. *The product of two odd integers is odd*

Proof. Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}$ such that \mathbf{x} and \mathbf{y} are odd. By the division algorithm, we have that $\mathbf{x} = 2\mathbf{b}_x + 1$ and $\mathbf{y} = 2\mathbf{b}_y + 1$ where $\mathbf{b}_x, \mathbf{b}_y \in \mathbb{Z}$. Now consider the product of \mathbf{x} and \mathbf{y} :

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= (2\mathbf{b}_x + 1) \cdot (2\mathbf{b}_y + 1) \\ &= 4\mathbf{b}_x\mathbf{b}_y + 2\mathbf{b}_x + 2\mathbf{b}_y + 1 \\ &= 2(2\mathbf{b}_x\mathbf{b}_y + \mathbf{b}_x + \mathbf{b}_y) + 1 \end{aligned}$$

Therefore, $2 \nmid \mathbf{x} \cdot \mathbf{y} \implies \mathbf{x} \cdot \mathbf{y}$ is odd. \square

Problem 4. Let \mathbb{C} be the complex numbers and

$$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}.$$

prove that \mathbb{C}^* and M^* (the nonzero elements of M), viewed as groups with multiplication, are isomorphic.

Proof. We will prove that the following function is an isomorphism from \mathbb{C}^* to M^* :

$$\begin{aligned} \phi : \mathbb{C}^* &\rightarrow M^* \\ a + bi &\mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \end{aligned}$$

- **Injective:** Let $u, v \in \mathbb{C}^*$ such that $u = a + bi$ and $v = c + di$ where $a, b, c, d \in \mathbb{R}$.

$$\phi(u) = \phi(v) \implies \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \implies a = c \text{ and } b = d \implies u = v.$$

- **Surjective:**

$$\begin{aligned} \text{range}(\phi) &= \{\phi(u) \mid u \in \mathbb{C}^*\} \\ &= \{\phi(a + bi) \mid a, b \in \mathbb{R}\} \\ &= \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \\ &= M^* \end{aligned}$$

- **Preserves Group Operation:** Let $u, v \in \mathbb{C}^*$ such that $u = a + bi$ and $v = c + di$ where $a, b, c, d \in \mathbb{R}$.

$$\begin{aligned} \phi(u \cdot v) &= \phi((a + bi) \cdot (c + di)) \\ &= \phi(ac + adi + bci + bdi^2) \\ &= \phi((ac - bd) + (ad + bc)i) \\ &= \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix} \\ &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \phi(u) \cdot \phi(v) \end{aligned}$$

Therefore, we have proven that \mathbb{C}^* and M^* are isomorphic. □

Problem 5. Let G be a group. An isomorphism from G to itself is called an *automorphism* of G . Let $\text{Aut}(G)$ denote the set of all automorphisms of G . This is a group under the operation of function composition. Find two groups G and H such that $G \not\cong H$ but $\text{Aut}(G) \cong \text{Aut}(H)$.

Proof. Let $G = (\mathbb{Z}, +)$ and let $H = \mathbb{Z}_4$. We will now determine $\text{Aut}(G)$ and $\text{Aut}(H)$.

- $\text{Aut}(G)$: Let $k \in G$ and let $\alpha \in \text{Aut}(G)$. We have that

$$\begin{aligned}\alpha(k) &= \alpha(1 + \overset{k \text{ times}}{\dots} + 1) \\ &= \alpha(1) + \overset{k \text{ times}}{\dots} + \alpha(1) \\ &= k\alpha(1)\end{aligned}$$

Therefore, the number of distinct automorphisms in $\text{Aut}(G)$ is equal to the number of distinct elements that 1 can be mapped to. Since

$$(\mathbb{Z}, +) = \{1^n \mid n \in \mathbb{Z}\} = \{(-1)^n \mid n \in \mathbb{Z}\}$$

we have that $G = \langle 1 \rangle = \langle -1 \rangle$. Since 1 is a generator of G , by (Gallian, 6.2.4) it must be the case that $\langle \alpha(1) \rangle$ is also a generator of G . Thus, $\alpha(1) = 1$ or -1 . Let $\alpha_1, \alpha_{-1} \in \text{Aut}(G)$ denote the automorphisms that map 1 to 1 and -1 respectively. Therefore, we have that $\text{Aut}(G) = \{\alpha_1, \alpha_{-1}\}$.

- $\text{Aut}(H)$: Let $\bar{\alpha} \in \text{Aut}(H)$. A similar process can be used to show that the number of distinct automorphisms in $\text{Aut}(H)$ is equal to the number of distinct elements that 1 can be mapped to. Since

$$H = \{0, 1, 2, 3\} \quad \text{and} \quad |1| = 4$$

we have that $|\bar{\alpha}(1)| = 4$. Hence, $\bar{\alpha}(1) = 1$ or 3. Let $\bar{\alpha}_1, \bar{\alpha}_3 \in \text{Aut}(H)$ denote the automorphisms that map 1 to 1 and 3 respectively. Therefore, we have that $\text{Aut}(H) = \{\bar{\alpha}_1, \bar{\alpha}_3\}$.

Evidently, $G \not\cong H$ since $|G| \neq |H|$. Additionally, $|\text{Aut}(G)| = |\text{Aut}(H)| = 2$ and there is only one unique way to form a group of order 2, $\text{Aut}(G) \cong \text{Aut}(H)$. \square