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: $3, 2, 2$):** $p = (a_1, a_2)(b_1, b_2)(c_1, c_2, c_3)$. In this case, the number of ways to construct p using elements of S_7 is:
$$\binom{7}{3}\frac{3!}{3} \cdot \binom{4}{2}\frac{2!}{2} \cdot \binom{2}{2}\frac{2!}{2} \cdot \frac{1}{2} = 210$$
Essentially, each $\binom{n}{k}$ is the number of unique combinations of elements for a single cycle of length k. We multiply this by $\frac{k!}{k}$ in order to account for all the unique orderings of elements within that cycle. In this case, we must also divide by 2 since the order of either two-cycle does not matter.

- **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:
$$\binom{7}{3}\frac{3!}{3} \cdot \binom{4}{2}\frac{2!}{2} = 420$$

- **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:
$$\binom{7}{6}\frac{6!}{6} = 840$$

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

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 in S_4:

1.	$\begin{array}{cc} 1 & 2 \\ 4 & 3 \end{array}$	$\xrightarrow[e]{\text{identity}}$	$\begin{array}{cc} 1 & 2 \\ 4 & 3 \end{array}$
2.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{\longleftrightarrow} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,2)(4,3)]{\text{horizontal flip}}$	$\begin{array}{cc} 2 & 1 \\ 3 & 4 \end{array}$
3.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{\updownarrow} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,4)(2,3)]{\text{vertical flip}}$	$\begin{array}{cc} 4 & 3 \\ 1 & 2 \end{array}$
4.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{\nearrow} \\ 4 & 3 \end{array}$	$\xrightarrow[(2,4)]{\text{left diagonal flip}}$	$\begin{array}{cc} 1 & 4 \\ 2 & 3 \end{array}$
5.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{\nwarrow} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,3)]{\text{right diagonal flip}}$	$\begin{array}{cc} 3 & 2 \\ 4 & 1 \end{array}$
6.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{\circlearrowright} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,2,3,4)]{\text{clockwise rotation}}$	$\begin{array}{cc} 4 & 1 \\ 3 & 2 \end{array}$
7.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{2} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,3)(2,4)]{\text{clockwise rotation (x2)}}$	$\begin{array}{cc} 3 & 4 \\ 2 & 1 \end{array}$
8.	$\begin{array}{cc} 1 & 2 \\ \multicolumn{2}{c}{3} \\ 4 & 3 \end{array}$	$\xrightarrow[(1,4,3,2)]{\text{clockwise rotation (x3)}}$	$\begin{array}{cc} 2 & 3 \\ 1 & 4 \end{array}$

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

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

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

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

By lemma 1, nr is odd. Since e must equal the product of an even number of two cycles, this is a contradiction. Therefore, r must be even which implies that p is an even permutation. □

Proof. We will provide a counter-example to show that an even permutation is not necessarily of odd order. Consider the even permutation $(1, 2)(3, 4)$. Evidently, $((1, 2)(3, 4))^2 = (1, 2)(3, 4)(1, 2)(3, 4) = (1)(2)(3)(4) = e$. This implies that $(1, 2)(3, 4)$ is of even order. □

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

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

$$\begin{aligned} x \cdot y &= (2b_x + 1) \cdot (2b_y + 1) \\ &= 4b_x b_y + 2b_x + 2b_y + 1 \\ &= 2(2b_x b_y + b_x + b_y) + 1 \end{aligned}$$

Therefore, $2 \nmid x \cdot y \implies x \cdot y$ is odd. □

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

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

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^*:

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

- **Injective:** Let $u, v \in \mathbb{C}^*$ such that $u = a + bi$ and $v = c + di$ where $a, b, c, d \in \mathbb{R}$. $\phi(u) = \phi(v) \implies \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \implies a = c$ and $b = d \implies u = v$.

- **Surjective:**

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

- **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. $\square$

Problem 5. Let G be a group. An isomorphism from G to itself is called an *automorphism* of G. Let $\mathrm{Aut}(\mathsf{G})$ 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 $\mathsf{G} \not\approx \mathsf{H}$ but $\mathrm{Aut}(\mathsf{G}) \approx \mathrm{Aut}(\mathsf{H})$.

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

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

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

  Therefore, the number of distinct automorphisms in $\mathrm{Aut}(G)$ 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 $\alpha_1, \alpha_{-1} \in \mathrm{Aut}(G)$ denote the automorphisms that map 1 to 1 and -1 respectively. Therefore, we have that $\mathrm{Aut}(G) = \{\alpha_1, \alpha_{-1}\}$.

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

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

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

Evidently, $G \not\approx H$ since $|G| \neq |H|$. Additionally, $|\mathrm{Aut}(G)| = |\mathrm{Aut}(H)| = 2$. Since there is only one way to construct a group of order 2 (using an identity and an element that is its own inverse), it must be the case that $\mathrm{Aut}(G) \approx \mathrm{Aut}(H)$. $\square$