Solutions: Homework 3

February 14, 2020

Problem 1. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$
(a) Compute $\tau\sigma$.
(a) Compute $\tau^2\sigma$.
(a) Compute $\sigma^{-2}\tau$.

Proof. The cycle decomposition of σ is $\sigma = (134562)$ and of τ is $\tau = (1243)(56)$.
(a) $\tau\sigma = (46)$.
(b) $\tau^2 = (14)(23)$. $\tau^2\sigma = (124563)$.
(c) $\sigma^2 = (146)(235)$. $\sigma^{-2} = (164)(253)$. $\sigma^{-2}\tau = (1542)(36)$. □

Problem 2. For σ and τ as in Problem 1, compute the following:
(a) $|\langle\sigma\rangle|$
(b) $|\langle\tau^2\rangle|$
(c) σ^{100}

Proof. (a) σ is a cycle of length 6. So $|\langle\sigma\rangle| = 6$.
(b) τ^2 is the product of two disjoint cycles of length 2. So $|\langle\sigma\rangle| = \mathrm{lcm}(2, 2) = 2$.
(c) $\sigma^{100} = \sigma^{102-2} = (\sigma^6)^{17}\sigma^{-2} = \sigma^{-2} = (164)(253)$. □

Problem 3. (a) Find the number of elements in the set $\{\sigma \in S_4 | \sigma(3) = 3\}$.
(b) Show that the set from part (a) is a subgroup of S_4.

Proof. (a) Let us denote this set by S. Then, we can think of S as the set of bijections of $\{1, 2, 4\}$. So, $|S| = 3! = 6$.
(b) Let $\sigma, \tau \in S$. Then $\sigma(3) = 3$ and $\tau(3) = 3$. So, $\sigma\tau(3) = \sigma(\tau(3)) = \sigma(3) = 3$. So, $\sigma\tau \in S$. So, S is closed under composition. Let e denote the identity of S_4. Then $e(3) = 3$. So, $e \in S$. Let $\sigma \in S$. Since $\sigma(3) = 3, \sigma^{-1}(3) = 3$. So, $\sigma^{-1} \in S$. So, S is a subgroup of S_4. □

Problem 4. Consider the permutation $\sigma = (145)(78)(257) \in S_8$. Write σ in cycle notation.

Proof. Let $\sigma_1 = (145)(78)$ and $\sigma_2 = (257)$. Then $\sigma = \sigma_1 \circ \sigma_2$.

$$\sigma(1) = \sigma_1(\sigma_2(1)) = \sigma_1(1) = 4.$$

$$\sigma(2) = \sigma_1(\sigma_2(2)) = \sigma_1(5) = 1.$$
$$\sigma(3) = \sigma_1(\sigma_2(3)) = \sigma_1(3) = 3.$$
$$\sigma(4) = \sigma_1(\sigma_2(4)) = \sigma_1(4) = 5.$$
$$\sigma(5) = \sigma_1(\sigma_2(5)) = \sigma_1(7) = 8.$$
$$\sigma(6) = \sigma_1(\sigma_2(6)) = \sigma_1(6) = 6.$$
$$\sigma(7) = \sigma_1(\sigma_2(7)) = \sigma_1(2) = 2.$$
$$\sigma(8) = \sigma_1(\sigma_2(8)) = \sigma_1(8) = 7.$$

Then $\sigma = (145872)$. □

Problem 5. (a) Find the maximum possible order for an element of S_5.
(b) Find the maximum possible order for an element of S_6.

Proof. (a) Any element in S_5 other than the identity is of the form

(a_1a_2) of order 2

$(a_1a_2)(a_3a_4)$ of order 2

$(a_1a_2a_3)$ of order 3

$(a_1a_2a_3)(a_4a_5)$ of order 6

$(a_1a_2a_3a_4)$ of order 4

$(a_1a_2a_3a_4a_5)$ of order 5

So, the maximum possible order for an element of S_5 is 6.
(b) Any element in S_6 other than the identity is of the form

(a_1a_2) of order 2

$(a_1a_2)(a_3a_4)$ of order 2

$(a_1a_2)(a_3a_4)(a_5a_6)$ of order 2

$(a_1a_2a_3)(a_4a_5)$ of order 6

$(a_1a_2a_3)(a_4a_5a_6)$ of order 3

$(a_1a_2a_3a_4)(a_5a_6)$ of order 4

$(a_1a_2a_3a_4a_5)$ of order 5

$(a_1a_2a_3a_4a_5a_6)$ of order 6

So, the maximum possible order for an element of S_6 is 6.

□

Problem 6. Show that S_n is not cyclic for any $n \geq 3$.

Proof. Let $n \geq 2$. Let $\sigma = (12) \in S_n$ and $\tau = (13) \in S_n$. Then $\sigma\tau = (132)$ and $\tau\sigma = (123)$. So, $\sigma\tau \neq \tau\sigma$, and so S_n is not abelian for $n \geq 3$. Since cyclic groups are baelian, S_n is not cyclic for $n \geq 3$. □

Problem 7. Is A_3 an abelian group? Prove yes or no.

Proof. $A_3 = \{e, (123), (132)\}$. Note that $(132) = (123)^2$. So, $A_3 = \langle (123) \rangle$, and hence is abelian. □

Problem 8. Show that for very subgroup H of S_n for $n \geq 2$, either all of the permutations in H are even or exactly half of them are even.

Proof. Suppose that not all the permutations in H are even. Let $\sigma \in H$ be an odd permutation. Let $E \subset H$ denote the set of all even permutations in H. Let us define by σE the set $\{\sigma \circ \tau | \tau \in E\}$. Now, we claim that H is the disjoint union of E and σE. Since σ is odd, $\sigma \circ \tau$ is odd for all $\tau \in E$. So, $E \cap \sigma E = \emptyset$. Now, suppose that $\tau \in H$. If τ is even, then $\tau \in E$. If τ is odd, then $\sigma^{-1}\tau$ is even, hence $\sigma^{-1}\tau \in E$ and so $\tau \in \sigma E$. So, $H = E \cup \sigma E$. This proves that H is the disjoint union of E and σE. Also, note that $|\sigma E| = |E|$. So, $|H| = |E| + |\sigma E| = |E| + |E| = 2|E|$. So, $|E| = |H|/2$. So exactly half of the permutations are even. □

Problem 9. Let G be a group. Define the **center** of G, denoted $Z(G)$, to be the following subset:

$$Z(G) = \{x \in G | xy = yx \forall y \in G\}.$$

(a) Show that $Z(G)$ is a subgroup of G.
(b) What is the center of D_3?
(b) What is the center of D_4?

Proof. (a) Let $a, b \in Z(G)$. Then $ay = ya$ for all $y \in G$, and $by = yb$ for all $y \in G$. Then $(ab)y = aby = a(by) = a(yb) = ayb = (ay)b = (ya)b = yab = y(ab)$ for all $y \in G$. So, $(ab)y = y(ab)$ for all $y \in G$. So, $ab \in Z(G)$. Clearly, $e \in G$ as $ey = y = ye$ for all $y \in G$. So, $e \in Z(G)$. Now, suppose that $a \in G$. Then $ay = ya$ for all $y \in G$. Multiplying both sides by a^{-1} on the left and the right, we get $a^{-1}(ay)a^{-1} = a^{-1}(ya)a^{-1}$ for all $y \in G$. But this just implies that $a^{-1}y = ya^{-1}$ for all $y \in G$. So, $a^{-1} \in Z(G)$. So, $Z(G)$ is a subgroup of G.
(b) Let f denote the flips of a triangle and let r denote the rotations (counter-clockwise) of a triangle. Then $D_= \{e, r, r^2, f, fr, fr^2\}$. Note that we have $r^3 = e, f^2 = e$ and $rf = fr^2$. The fact that $rf = fr^2$ implies that r does not commute with f and hence r and f both lie outside $Z(D_3)$. Similarly, r^2 does not commute with f as $fr^2 = rf \neq r^2 f$. So, $r^2 \notin Z(D_3)$. Now, $(fr)r = fr^2 = rf \neq rfr = r(fr)$. So, fr does not commute with r, and hence $fr \notin Z(D_3)$. Also, $f(fr^2) = f^2r^2 = r^2$, while $(fr^2)f = (rf)f = rf^2 = r$. Hence $f(fr^2) \neq (fr^2)f$, so fr^2 does not commute with f. So, $fr^2 \notin Z(D_3)$. Hence $Z(D_3) = \{e\}$.
(c) Let f denote the flips of a square and let r denote the rotations (counter-clockwise) of a square. Then $D_4 = \{e, r, r^2, r^3, f, fr, fr^2, fr^3\}$. Note that we have $r^4 = e, f^2 = e$ and $rf = fr^3$. The fact that $rf = fr^3$ implies that r does not commute with f and hence r and f both lie outside $Z(D_4)$. Similarly, r^3 does not commute with f as $fr^3 = rf \neq r^3 f$. So,

$r^3 \notin Z(D_4)$. Let $0 \le i \le 3$. Then $r^2(fr^i) = r(rf)r^i = r(fr^3)r^i = (rf)r^{i+3} = (fr^3)r^{i+3} = fr^{i+6} = fr^{i+2}r^4 = fr^{i+2} = (fr^i)r^2$. So, r^2 commutes with fr^i for all $0 \le i \le 3$. Obviously, r^2 commutes with r^i for all $0 \le i \le 3$. This implies that r^2 commutes with all the elements of D_4. So, $r^2 \in Z(D_4)$. If $fr^2 \in Z(D_4)$, then $f = (fr^2)r^2 \in Z(D_4)$, a contradiction. Hence, $fr^2 \notin Z(D_4)$. Now, $r(fr) = (rf)r = (fr^3)r = fr^4 = f \ne fr^2 = (fr)r$. So, fr doesn't commute with r, hence $fr \notin Z(D_4)$. If $fr^3 \in Z(D_4)$, then $fr = fr^5 = (fr^3)r^2 \in Z(D_4)$, a contradiction. Hence, $fr^3 \notin Z(D_4)$. So, $Z(D_4) = \{e, r^2\}$.

□

Problem 10. Let G be a finite group. Prove that there exists a positive integer N such that, for any $x \in G, x^N = e$.

Proof. Take $N = |G|$. By the corollary to Lagrange's theorem, for any $x \in G$, the order of x divides $|G|$. Hence, $x^N = x^{|G|} = e$. □