Math 307 Abstract Algebra Homework 4 **Sample Solution**

1. Consider $\sigma = (13256)(23)(46512)$.

   (a) Express σ as a product of disjoint cycles. Solution. $\sigma = (1,2,4)(3,5)$.

   (b) Express σ as a product of transpositions. Solution. $\sigma = (1,4)(1,2)(3,5)$.

   (c) (Extra 2 points.) Express σ as a product minimum number of transpositions.

   (Prove that the number is minimum!)

   Note that σ is an odd permutation and moves 5 numbers in $\{1,\ldots,6\}$. So, we cannot use one transpositions to make the moves. So, we need at least three transpositions.

2. (a) Let $\alpha = (1,3,5,7,9,8,6)(2,4,10)$. What is the smallest positive integer n such that $\alpha^n = \alpha^{-5}$?

   Solution. We need to find the smallest n such that $\alpha^{n+5} = \varepsilon$, where ε is the identity permutation. Since $|\alpha| = \text{lcm}(7,3) = 21$, we see that $n = 16$.

   (b) Let $\beta = (1,3,5,7,9)(2,4,6)(8,10)$. If β^m is a 5-cycle, what can you say about m?

   Solution. Note that β^m is a 5-cycle if and only if $(2,4,6)^m = (8,10)^m = \varepsilon$ and $(1,3,5,7,9)^m$ is a five cycle. This happen if and only if m is a multiple of $6 = \text{lcm}(3,2)$ and m is not a multiple of 5. That is $m = 6k$ and k is not a multiple of 5.

3. In S_7 show that $x^2 = (1,2,3,4)$ has no solutions, but $x^3 = (1,2,3,4)$ has at least two.

   Solution. Note that $(x^2)^4 = \varepsilon$, the identity map. So, the order $|x| = 1,2,4$. Clearly, $|x| \neq 1,2$, else $x^2 \neq (1,2,3,4)$. If $|x| = 4$, then x is a 4-cycle, or the product of a 4-cycle and a 2-cycle; in either case, $x^2 \neq (1,2,3,4)$.

   Alternatively, observe that $x^2 = (1,2,3,4) = (1,4)(1,3)(1,2)$ is an odd permutation. But x^2 must be an even permutation for any $x \in S_n$.

   Let $x \in \{(1,4,3,2), (1,4,3,2)(5,6,7), (1,4,3,2)(5,7,6)\}$. Then $x^3 = (1,2,3,4)$. In fact, these are all the solution because in the disjoint cycle decomposition of the solution x, $(1,4,3,2)$ is needed to produce the cycle $(1,2,3,4)$ in x^3. Clearly, either there is no other cycle in the decomposition of x, or there is a 3-cycle using the numbers $5,6,7$, which must be of the form $(5,6,7)$ or $(5,7,6)$.

4. Describe all elements of order 5 in A_6.

   Solution. Note that $\sigma \in A_6$ satisfies $|\sigma| = 5$ must be a 5-cycle $(i_1,\ldots,i_5)$, and that a 5-cycle is an even permutation lying in A_6.

   Although it is not required in this question, one may determine the numbers of such elements. There are 6 ways to choose 5 elements from $\{1,\ldots,6\}$, and $5!/5 = 24$ ways to arrange the five elements in a cycle. Thus, there are $24 \cdot 6 = 144$ such permutations.

5. Let $H \leq S_n$.

   (a) Show that either $H \leq A_n$ or $|H \cap A_n| = |H|/2$.

   Solution. Suppose $H \leq S_n$. Let $S_1 = H \cap A_n$, and $S_2 = H - S_1$.

   Case 1. If $S_2 = \emptyset$, then $H \leq A_n$.

   Case 2. If $S_2 \neq \emptyset$ and $g \in S_2$ is an odd permutation. Then define $\lambda_g : S_1 \to S_2$ by $\lambda_g(x) = gx$.

It is well defined because for every even permutation $x \in H$, $gx \in H$ is an odd permutation and will be in S_2.

It is 1-1 because $\lambda_g(x_1) = \lambda_g(x_2)$ implies $gx_1 = gx_2$ so that $x_1 = x_2$ by cancellation.

If is onto because for every $y \in S_2$, we can let $x = g^{-1}y \in H \cap A_n = S_1$ so that $\lambda_g(x) = y$.

Since there is a bijection from S_1 to S_2, it follows that $|S_1| = |S_2|$, and $|H \cap A_n| = |H|/2$.

(b) If $|H|$ is odd, show that $H \leq A_n$.

Solution. Since $|H|$ is odd, it cannot be the case that $|H \cap A_n| = |H|/2$. So, $H \leq A_n$.

6. Let G be a group. Show that $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is an isomorphism if and only if G is Abelian.

   Solution. Suppose G is Abelian. First, we show that ϕ is bijective. Clearly, if $\phi(a) = \phi(b)$, then $a^{-1} = b^{-1}$. Taking inverse on both sides, we see that $a = b$; so ϕ is 1-1. If $a \in G$, then $\phi(a^{-1}) = a$; so ϕ is onto. Now, by commutativity, for any $a, b \in G$. $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$. Thus, ϕ is a group isomorphism.

   Conversely, suppose ϕ is an isomorphism. Then for any $a, b \in G$, $a^{-1}b^{-1} = \phi(a)\phi(b) = \phi(ab) = (ab)^{-1} = b^{-1}a^{-1}$. Taking inverse on both sides, we see that $ba = ab$.

7. Recall that $U(n)$ is group containing the elements in Z_n that are relatively prime to n such that $a * b = ab \pmod{n}$.

   Show that $\phi : U(16) \to U(16)$ defined by $\phi(x) = x^3$ is an isomorphism (automorphism). What about the maps $x \mapsto x^5$ and $x \mapsto x^7$?

   Solution. Note that $(\phi(1), \ldots, \phi(15)) = (1, 11, 13, 7, 9, 3, 5, 15)$ so that ϕ is a bijection. For any $a, b \in U(16)$, we have $\phi(ab) = (ab)^3 = a^3b^3 = \phi(a)\phi(b)$. Thus, ϕ is a group isomorphism.

   Here is a more general argument for the fact that ϕ is a bijection:

   If $\phi(x) = \phi(y)$ for $x, y \in U(16)$, then x and y are odd numbers such that $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ is a multiple of 16. Note that $x^2 + xy + y^2$ is odd. So, $x - y$ is a multiple of 16 by the Fundamental Theorem of Arithmetic. So, $x = y$ in $U(16)$. Hence, ϕ is one-one. Because $U(16)$ is finite, we see that ϕ is also onto.

   Note that $|U(16)| = 8$. If $x \in U(16)$, then $|x| \in \{1, 2, 4, 8\}$. Hence, $x^8 = e$.

   As a result, $x \mapsto x^7 = x^{-1}$ is an isomorphism by the previous exercise.

   For $x \mapsto x^5 = x^{-3}$, because $f(x) = x^{-1}$ is a group isomorphism by the previous exercise, and $\phi(x) = x^3$ is a group isomorphism, so is $\phi \circ f(x) = x^5$.

8. Show that every isomorphism (automorphism) $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}, +)$ has the form $\phi(x) = qx$ for $q = \phi(1)$.

   Solution. Let $\phi(1) = q$. Note that $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$ so that $\phi(0) = 0 = q0$.

   For any $n \in \mathbb{N}$, $\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = nq$.

   For any $m, n \in \mathbb{N}$, $\phi(m/n) = \phi(1/n) + \cdots + \phi(1/n) = m(q/n) = q(m/n)$.

   Since $\phi(m/n) + \phi(-m/n) = \phi(m/n - m/n) = 0$,

   $\phi(-m/n) = -\phi(m/n) = -(m/n)q = q(-m/n)$.

   Hence for any rational number x, $\phi(x) = qx$. Of course, if ϕ is an automorphism, $q \neq 0$.