Math 307 Abstract Algebra Homework 5 **Sample solution**

1. Let $(\mathbb{R}^+, \cdot)$ be the group of positive real number under multiplication. Show that $\phi : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $\phi(x) = \sqrt{x}$ is an group isomorphism.

   Solution. Note that ϕ is well-defined from $\mathbb{R}^+$ to $\mathbb{R}^+$. If $\sqrt{x} = \sqrt{y}$, then $x = y$ so that ϕ is 1-1. If $z \in \mathbb{R}^+$ then $x = z^2$ satisfies $\phi(x) = z$. Thus, ϕ is surjective. Furthermore, $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$ for all $x, y \in \mathbb{R}^+$. So, ϕ is operation preserving. Combining the above arguments, we see that ϕ is a group isomorphism.

2. Show that the following pair of groups are not isomorphic.

   (a) $(\mathbb{Q}, +), (\mathbb{R}, +)$. (b) $(\mathbb{R}^+, \cdot), (\mathbb{R}^*, \cdot)$. (c) $(\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$.

   Solution. (a) $\mathbb{Q}$ and $\mathbb{R}$ have different cardinality. So, there is no bijection between the two sets, and thus no group isomrophism.

   (b) Note that $\{x \in \mathbb{R}^* : x^2 = 1\}$ has two elements; $\{x \in \mathbb{R}^+ : x^2 = 1\}$ has only one element. Thus, $\mathbb{R}^*$ and $\mathbb{R}^+$ are not isomorphic.

   (c) Note that $\{x \in \mathbb{C}^* : x^4 = 1\}$ has 4 elements; $\{x \in \mathbb{R}^* : x^4 = 1\}$ has 2 elements. Thus, $\mathbb{R}^*$ and $\mathbb{C}^*$ are not isomorphic.

3. Show that $G = \{e^{it} : t \in [0, 2\pi)\}$ under multiplication contains subgroups isomorphic to $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$ for any $n \in \mathbb{N}$, and show that G is not a cyclic group.

   Solution. For each $n \in \mathbb{N}$, the element $z_n = e^{i2\pi/n} \in G$ has order n. Thus, $\langle z_n \rangle$ is isomorphic to $(\mathbb{Z}_n, +)$.

   Let $z = e^{it\sqrt{2}\pi}$. Then there is no $m \in \mathbb{N}$ such that $\sqrt{2}\pi m$ is a multiple of 2π. Hence, $(e^{it\sqrt{2}\pi})^m \neq 1$ for any $m \in \mathbb{N}$, so that $\langle z \rangle$ is an infinite cyclic group isomorphic to $(\mathbb{Z}, +)$.

   If G is a cyclic group, then $|G| = |\mathbb{Z}_n| = n$ for some $n \in \mathbb{N}$ or $|G| = |\mathbb{Z}|$. But $|G| = |[0, 2\pi)|$ is uncountable. Thus, G is not cyclic.

4. Suppose ϕ_1, ϕ_2 are automorphisms of a group G. Show that $H = \{g \in G : \phi_1(g) = \phi_2(g)\}$ is a subgroup of G.

   Solution. Because $\phi_1(e) = e = \phi_2(e)$, $e \in H$. Suppose $x, y \in H$. Then $\phi_1(x) = \phi_2(x)$ and $\phi_1(y) = \phi_2(y)$. Hence, $\phi_1(xy) = \phi_1(x)\phi_1(y) = \phi_2(x)\phi_2(y) = \phi_2(xy)$. Thus, $xy \in H$. Furthermore, by the fact that $\phi_j(x)^{-1} = \phi_j(x^{-1})$ for $j = 1, 2$, we see that $\phi_1(x^{-1}) = \phi_1(x)^{-1} = \phi_2(x)^{-1} = \phi_2(x^{-1})$. Thus, $x^{-1} \in H$. Combining the above arguments, we see that H is a subgroup of G.

5. Let G be a group and $a \in G$. Suppose $|a| = n$ and the inner automorphism $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ has order m in $\mathrm{Aut}(G)$. Show that $m|n$.

   Give an example of G and a so that $1 < m < n$.

   Solution. Since $a^n = e$, we see that $(\phi_a)^n = \phi_{a^n} = \phi_e = \varepsilon$. Now, ϕ_a has order m, we see that $m|n$. (Here we use the fact that if an element g in a group has order m, and $g^n = e$, then $m|n$.)

   Consider the dihedral group $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, where r is the rotation of the square by an angle of $\pi/2$ radians, and s is the reflection about the horizontal axis. Then r has order 4 and $r^2 g = gr^2$ for all $g \in D_4$. Thus, $(\phi_r)^2(g) = r^2 g r^{-2} = g$ for all $g \in G$, i.e., $(\phi_r)^2 = \phi_{r^2} = \varepsilon$ is the identity map. Now, $\phi_r \neq \varepsilon$. We see that $|r| = 4$ and $|\phi_r| = 2$.

6. Suppose G is a group of order n, and $k \in \mathbb{N}$ is relatively prime to n. Show that $g : G \to G$ defined by $g(x) = x^k$ is one-one. If G is Abelian, show that g is an automorphism.

   Solution. If $\gcd(k, n) = 1$, then $an + bk = 1$ for some integers a, b. Observe that $|x|$ and $|y|$ are factors of n so that $x^n = y^n = e$. Suppose $x^k = y^k$. Then $x = x^{an+bk} = x^{an}x^{bk} = y^{an}y^{bk} = y^{an+bk} = y$.

7. Suppose $1 \leq i < j \leq n$.

   (a) Show that $(i, j) = (j, j-1)(j-1, j-2)\cdots(i+1, i)(i+1, i+2)\cdots(j-1, j)$.

   (b) Show that every element $\sigma \in S_n$ is a product of transpositions of the form

   $$(1, 2), (2, 3), \ldots, (n-1, n).$$

   Solution. (a) Let $\sigma = (j, j-1)(j-1, j-2)\cdots(i+1, i)(i+1, i+2)\cdots(j-1)$. We consider $\sigma(x)$ for $x = 1, \ldots, n$. If $x = i$, then $(i+1, i+2)\cdots(j-1, j)$ has no effect on x, and $(j, j-1)(j-1, j-2)\cdots(i+1, i)$ will take x to j so that $\sigma(i) = j$. If $x = j$, then $(i+1, i)(i+1, i+2)\cdots(j-1, j)$ will take x to i, then $(j, j-1)(j-1, j-2)\cdots(i+2, i+1)$ will have no effect on i so that $\sigma(j) = i$. If $x < i$ or $x > j$, then σ will have no effect on x so that $\sigma(x) = x$. If $i < x < j$, then $(i+1, i+2)\cdots(j-1)$ will take x to i and then $(j, j-1)(j-1, j-2)\cdots(i+1, i)$ will take i back to x so that $\sigma(x) = x$. By the above arguments, we see that $\sigma = (i, j)$.

   (b) Note that every $\sigma \in S_n$ is a product of transpositions. By (a) every transposition is product of transpositions chosen from the set $\{(1, 2), \ldots, (n-1, n)\}$. The result follows.

8. (a) Show that every $\sigma \in S_n$ is a product of the n-cycle $\alpha = (1, 2, \ldots, n)$ and $\tau = (1, 2)$.

   Solution. Note that $\alpha^n = \varepsilon$ so that $\alpha^{-j} = \alpha^{n-j}$. By the previous question, it suffices to show that for $i = 1, \ldots, n-1$, the transposition $(i, i+1)$ can be generated by α and τ. We show that $(i+1, i+2) = \alpha^i\tau\alpha^{-i}$ for $i = 1, \ldots, n-2$. To this end, let $f = \alpha^i\tau\alpha^{-i}$ for $i = 1, \ldots, n-2$. Let $x \in \{1, \ldots, n-1\}$. If $x = i+1$, then $\alpha_{-i}(x) = 1$, $\tau\alpha_{-i}(x) = 2$ and $f(x) = i+2$. If $x = i+2$, then $\alpha_{-i}(x) = 2$, $\tau\alpha_{-i}(x) = 1$ and $f(x) = i+1$. If $x \notin \{i+1, i+2\}$, then $\alpha^{-i}(x) \notin \{1, 2\}$. Thus, $\alpha^i\tau\alpha^{-i}(x) = \alpha^i\alpha^{-i}(x) = x$. Hence, $f = (i+1, k+2)$ as asserted.

   (b) Determine the minimum number of α and τ needed for a given σ.

   (c) For $n \geq 4$, every σ can be written as the product of no more than $n(n-1)/2$ permutations from the set $\{\alpha, \alpha^{-1}, \tau\}$.

   See http://arxiv.org/pdf/1303.3776.pdf for related results.