MATH 3311, FALL 2025: HOMEWORK 4

(1) Decide if the following statements are true or false:

(a) A group of order 6 must contain an element of order 6.

False, D_6 does not contain a group of order 6. If it did, it would be cyclic and thus abelian. D_6 is nonabelian.

(b) If $g \in G$ is an element of a group G with $g^{2025} = e$, then g cannot have order 24.

True: If $g^{2025} = e$, then the order must divide 2025. However, $24 \nmid 2025$.

(c) There is a group action $G \curvearrowright X$ and two elements $x_1, x_2 \in X$ such that $\mathcal{O}(x_1)$ is a proper subset of $\mathcal{O}(x_2)$.

False, $\mathcal{O}(x_1) \subseteq \mathcal{O}(x_2) \implies x_1 \in \mathcal{O}(x_2) \implies \mathcal{O}(x_1) = \mathcal{O}(x_2)$. (We proved the last implication in class: orbits with common elements are the same.) So every orbit that is a subset of another one must be equal to the other one.

(d) If G is a group of order 24 acting on a set X, then there cannot be any orbits of size 10 in X.

True: By corollary of orbit-stabilizer theorem, the size of the orbit must divide the size of the group. However, $10 \nmid 24$.

(e) If $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ acts on a set with an odd number of elements then there must be at least one point whose orbit consists only of itself.

True: By corollary of orbit-stabilizer theorem, the size of each orbit should divide the order of the group, which is 4. Therefore, the possible sizes are 1, 2, and 4. We proceed by trying to pair up all elements with their orbits. Say we are able to pair elements into orbit sizes of 2 and 4 (if we are not, we are done because some orbit size would be one), one element is left (remaining number must be odd since we pair up even numbers from an odd number of elements). We only have one element remaining, and since orbits are disjoint, the orbit of this element must have size 1. Either case (if we cannot pair elements until 1 remaining), we get elements with orbits of size 1. Such an element has an orbit that only consists of itself.
In summary, if we want to partition the elements into orbits of size 1, 2, or 4, we must use an orbit of size 1 because the set has odd number of elements.

(2) Show that every subgroup of a cyclic group is also cyclic. Conclude that every subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z} = \{dm : \ m \in \mathbb{Z}\}$ for some integer d.

Hint: Given a cyclic group $G = \langle g \rangle$ and a subgroup $H \leq G$, look at the smallest positive integer m such that $g^m \in H$.

Part 1: Suppose $|G| = n$ with G generated by $g \in G$. Then as always, $G = \{e, g, g^2, ..., g^{n-1}\}$. Suppose $H \leq G$ is a subgroup with elements of form $g^k : k \in \{0, 1, ..., n-1\}$. We know there must be some g^a with the least power a. Every element must be $g^{j \cdot a}$ for some integer j. Suppose not: $\exists g^b : g^b \neq g^{j \cdot a}$ for some integer j. $0 < \gcd(a, b) < a$ and $\exists s, t \in \mathbb{Z} : as + bt = \gcd(a, b) < a$. Then, $g^{as+bt} \in H$ but $0 < as + bt < a$. This contradicts that we chose a to be the lowest power of g in H.

As demonstrated, $\langle g^a \rangle \subseteq H$. By closure, $H \subseteq \langle g^a \rangle$. Therefore, $H = \langle g^a \rangle$. So for any $H \leq G$, H is a cyclic subgroup.

Part 2: If $G = \langle g \rangle$ is infinite and $H \leq G$ and H does not only contain the identity (If so $H = \langle e \rangle$ anyways), then there is a smallest positive integer m such that $g^m \in H$. If we have a negative power of g in H, we know there is a positive power of g in H given by the inverse of that element (so there are positive powers of g in H). We want to prove that $\forall g^k \in H, g^k = g^{jm}$ for some integer j.

By Bezout's lemma, we know $\gcd(m,k) = am + bk$ for integers a and b. Then, $g^{\gcd(m,k)} = g^{am+bk} = (g^m)^a(g^k)^b \in H$. Therefore, $\gcd(m,k) \geq m$, for $\gcd(m,k) > 0$. Since $0 < \gcd(m,k) \leq m$ because $\gcd(m,k) \mid m$, we know $\gcd(m,k) = m$. Therefore, $m \mid k$ and $k = jm$ for some integer j. Every element in H is therefore a power of g^m, and therefore in $\langle g^m \rangle$. So we have $H \subseteq \langle g^m \rangle$. By closure, we also know $\langle g^m \rangle \subseteq H$, so $H = \langle g^m \rangle$. We have proven that every subgroup of a infinite group is cyclic.

Taking parts 1 and 2 together, every subgroup of a cyclic group is cyclic.

Part 3: We have previously shown that $\mathbb{Z}$ is an infinite cyclic group with generator 1. By part 2, every subgroup of $\mathbb{Z}$ is cyclic. Any cyclic group is defined by the generator. If we have a subgroup of the integers, it has a generator d for some integer d. Then the described subgroup is $\langle d \rangle = \{dm : m \in \mathbb{Z}\}$. Therefore, every subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z} = \{dm : m \in \mathbb{Z}\}$.

A **(left) coset** for a subgroup $H \leq G$ is a subset of G of the form $gH = \{gh : h \in H\}$ for some $g \in G$. We call g a **representative for the coset**.

(3) Consider the element $\sigma \in S_7$ given by

$$\sigma(1) = 2\ ; \sigma(2) = 5\ ; \sigma(3) = 1\ ; \sigma(4) = 3\ ; \sigma(5) = 4\ ; \sigma(6) = 7\ ; \sigma(7) = 6.$$

Let $H \leq S_n$ be the subgroup consisting of powers of σ (the subgroup *generated* by σ).

(a) Compute the orbits and stabilizers of H acting on $\{1, 2, \ldots, 7\}$.

Finding all the elements that share the orbit with 1: $\sigma^0(1) = 1, \sigma(1) = 2, \sigma^2(1) = \sigma(2) = 5, \sigma^3(1) = \sigma(5) = 4, \sigma^4(1) = \sigma(4) = 3, \sigma^5(1) = \sigma(3) = 1$. Continuing, everything will be repeated again. So one orbit is $\{1, 2, 3, 4, 5\}$

The remaining elements are 6, 7. They are in each other's orbits: $\sigma^0(6) = 6, \sigma(6) = 7$, $\sigma^2(6) = \sigma(7) = 6$. So the orbits are $\{1, 2, 3, 4, 5\}$ and $\{6, 7\}$

Lemma 1. *The order of σ is 10. As such, $H = \langle \sigma \rangle$ has order 10.*

Proof. By the orbit stabilizer theorem, since the orbits were of size 2 and 5, $2 \mid |\langle \sigma \rangle| = |\sigma|$ and $5 \mid |\langle \sigma \rangle| = |\sigma|$. Therefore, $10 \mid |\sigma|$. Now we just need to confirm $\sigma^{10} = \mathrm{Id}$. We proceed by checking for elements in each orbit.

$$\sigma^{10}(1) = \sigma^5\sigma^5(1) = \sigma^5(1) = 1$$
$$\sigma^{10}(2) = \sigma^{10}(\sigma(1)) = \sigma(\sigma^{10}(1)) = \sigma(1) = 2$$
$$\sigma^{10}(3) = \sigma^{10}(\sigma^4(1)) = \sigma^4(\sigma^{10}(1)) = \sigma^4(1) = 3$$
$$\sigma^{10}(4) = \sigma^{10}(\sigma^3(1)) = \sigma^3(\sigma^{10}(1)) = \sigma^3(1) = 4$$
$$\sigma^{10}(5) = \sigma^{10}(\sigma^2(1)) = \sigma^2(\sigma^{10}(1)) = \sigma^2(1) = 5$$

$$\sigma^{10}(6) = \sigma^2\sigma^2\sigma^2\sigma^2\sigma^2(6) = \sigma^2\sigma^2\sigma^2\sigma^2(6) = \cdots = \sigma^2(6) = 6$$
$$\sigma^{10}(7) = \sigma^9\sigma^1(6) = \sigma^9(6) = \sigma\sigma^2\sigma^2\sigma^2\sigma^2(6) = \cdots = \sigma(6) = 7$$

We proved 10 divides the order (meaning 10 is the least possibility for the order), and that powering σ by 10 does yield the identity. Therefore, $|\sigma| = 10$. So $|H| = |\langle \sigma \rangle| = |\sigma| = 10$.

□

Recall $\sigma^0(1) = \sigma^5(1) = 1$. Then, $H_1 = \{e, \sigma^5\}$. There are no more elements, because by the orbit stabilizer theorem, $|H| = |\mathcal{O}(1)||H_1|$, and thus $|H_1| = 10/5 = 2$. Similarly, $\sigma^0(2) = \sigma^5(2) = 2$ so $H_2 = \{e, \sigma^5\}$. For the very same reasons, $H_1 = H_2 = H_3 = H_4 = H_5 = \{\mathrm{Id}, \sigma^5\}$.

Now, $\sigma^0(6) = \sigma^2(6) = \sigma^4(6) = \sigma^8(6) = 6$. So $H_6 = \{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}$ without any more elements because $|H_6| = |H|/|\mathcal{O}(6)| = 10/2 = 5$. Similarly, $H_6 = H_7 = \{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}$.

(b) Find five *distinct* cosets of H in S_7.
Let $\tau \in S_7$ be the permutation such that $\tau(1) = 2, \tau(2) = 3, \tau(3) = 4, \tau(4) = 5, \tau(5) = 6, \tau(6) = 7, \tau(7) = 1$. Notice that each number gets moved via addition of 1 modulo 7 (except the representatives are 1 through 7). Then, $\tau^7 = \mathrm{Id}$ as each one moved seven times will go back to itself. Now, $|\tau| = 7$ because $|\tau| \mid 7$ by HW#3 3b. Then the possible orders of τ are 1 and 7, but $\tau \neq \mathrm{Id}$ forces $|\tau| = 7$.

Now consider $\tau, \tau^2, \tau^3, \tau^4, \tau^5$. None of these are alike, as if for $i, j \in \{1, 2, 3, 4, 5\}$, $\tau^i = \tau^j$ means $\tau^{i-j} = \mathrm{Id} \implies 7 \mid i - j$, so $7 \mid |i - j|$, forcing $i = j$.

By HW#3 4a, we know that τ^k has order $\frac{7}{\gcd(7,k)}$. For each of 1 through 5 (which are the powers we are considering, $\gcd(7, k) = 1$. Therefore, $|\tau| = |\tau^2| = |\tau^3| = |\tau^4| = |\tau^5| = 7$.

Lemma 2. $g_1H = g_2H \iff g_2^{-1}g_1 \in H$

Proof. Suppose $g_1H = g_2H$, then $\forall h_1 \in H \exists h_2 \in H : g_1h_1 = g_2h_2 \implies g_2^{-1}g_1 = h_2h_1^{-1} \in H$.

Suppose $g_2^{-1}g_1 \in H$. Then, $\exists h \in H : g_2^{-1}g_1 = h \implies g_1 = g_2h$. Now, $\forall \tilde{h} \in H, g_1\tilde{h} = g_2h\tilde{h}$. Since $h\tilde{h} \in H$ by closure, $g_1\tilde{h} \in g_2H$. Therefore, $g_1H \subseteq g_2H$ by repeating the same thing or noticing that g_1H and g_2H are orbits with common elements, we thereby conclude $g_1H = g_2H$.

□

Now, we claim that $\tau H, \tau^2H, \tau^3H, \tau^4H, \tau^5H$ are all distinct cosets. Suppose $\tau^iH = \tau^jH$ with $i, j \in \{1, 2, 3, 4, 5\}$. Then, $\tau^{-j}\tau^i = \tau^{i-j} \in H$. Remember that $\tau^{i-j} \in \langle\tau\rangle$ and $|\langle\tau\rangle| = \langle\tau\rangle = 7$. By Lagrange's theorem, τ^{i-j} has order dividing 7.

On the other hand, remember $|H| = |\langle\sigma\rangle| = |\sigma| = 10$. Again, by Lagrange's theorem, each element in H has order dividing 10.

Now, τ^{i-j} has order dividing both 7 and 10. Therefore, τ^{i-j} must have order 1. So $(\tau^{i-j})^1 = \tau^{i-j} = \tau^i\tau^{-j} = \mathrm{Id}$. Multiplying τ^j on both sides, we obtain $\tau^i = \tau^j$. So we demonstrated that for $i, j \in \{1, 2, 3, 4, 5\}$, $\tau^iH = \tau^jH \implies \tau^i = \tau^j$. This means $\tau^i \neq \tau^j \implies \tau^iH \neq \tau^jH$, therefore proving that $\tau H, \tau^2H, \tau^3H, \tau^4H, \tau^5H$ are all distinct cosets.

Suppose that we have a group action $G \curvearrowright X$. The **set of fixed points** for the action is the subset

$$X^G = \{x \in X : \ g \cdot x = x \text{ for all } g \in G\}.$$

If G is a group, two elements $g, h \in G$ **commute** if $gh = hg$. The **center** of G, denoted $Z(G)$ is defined by

$$Z(G) = \{g \in G : \text{ for all } h \in G, hg = gh\}.$$

In other words, it is the set of the elements of G that commute with every other element of G.

(4) Show that the assignment

$$G \times G \xrightarrow{(g,h)\mapsto ghg^{-1}} G.$$

is a group action of G on itself and that the set of fixed points in G for this action is the center $Z(G)$.
Remark: This is the ***conjugation action*** *of G on itself.*

We need to show $\forall g_1, g_2 \in G \forall h \in G, g_1 \cdot (g_2 \cdot h)) = g_1 g_2 \cdot h$ and $\forall h \in G, e \cdot h = h$.

"Associativity": $\forall g_1, g_2 \in G \forall h \in G, g_1 \cdot (g_2 \cdot h)) = g_1 g_2 \cdot h$: $g_1 \cdot (g_2 \cdot h) = g_1 \cdot g_2 h g_2^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) h (g_1 g_2)^{-1} = g_1 g_2 \cdot h$.

Identity: $\forall h \in G, e \cdot h = h$: $e \cdot h = ehe^{-1} = ehe = eh = h$.
Therefore, the assignment is a group action.

Now, $G^G = \{g \in G : g \cdot h = h, \forall h \in G\} = \{g \in G : ghg^{-1} = h, \forall h \in G\} = \{g \in G : gh = hg, \forall h \in G\} = Z(G)$. Therefore, the set of fixed points in G for this action is the center $Z(G)$.

Fix a prime p. A p-**group** is a finite group G whose order is p^m for some $m \geq 1$.

(5) Suppose that we have a group action $G \curvearrowright X$ with G a p-group and X a finite set. Show that we have

$$|X^G| \equiv |X| \pmod{p}.$$

Hint: What is the size of the orbits that don't *consist of fixed points?*

Lemma 3. *$x \in X^G \iff \mathcal{O}(x) = \{x\}$. This means also means $|\mathcal{O}(x)| = 1 \iff x \in X^G$ because an orbit of x necessarily contains x.*

Proof. $x \in X^G \implies \forall g \in G, g \cdot x = x \implies G_x = G$. Since $|G| = |G_x||\mathcal{O}(x)|$, $\mathcal{O}(x)$ consists of one element, which must be x. So $\mathcal{O}(x) = \{x\}$.

For the other direction, we prove the contrapositive. If $\mathcal{O}(x)$ has another element called y, it means that $\exists g \in G : g \cdot x = y \neq x$. So $x \notin X^G$.

□

So if $x \notin X^G$, $|\mathcal{O}(x)| \mid |G| = p^m$ and since the order is not 1, the order of the orbit must be some power of p that isn't 1, meaning $p \mid |\mathcal{O}(x)|$. This means that $|\mathcal{O}(x)| = kp$ for some $k \in \mathbb{N}$.

Recall that if G and X are finite, then $|X| = \sum_{\text{distinct orbits}} |\mathcal{O}(x)|$. Then, $|X| = \sum_{\text{distinct orbits}} |\mathcal{O}(x)| = \sum_{x \in X^G} 1 + \sum_{\text{orbits without size 1}} k_i p = |X^G| + \sum_{\text{orbits without size 1}} k_i p$. We can split the sum like this because each element in X^G has size 1 and the remaining orbits, as shown, have their sizes as multiples of p.

We now apply modulo p on both sides, yielding $|X| \equiv |X^G| + \sum_{\text{orbits without size 1}} k_i p \pmod{p}$, so $|X| \equiv |X^G| \pmod{p}$.

Recall the following setup from Homework 3: Let Y be any set, and let

$$X = \underbrace{Y \times \cdots \times Y}_{p \text{ times}}$$

be the p-fold Cartesian product of Y with itself. So X consists of p-tuples $(a_1, \ldots, a_p)$, where $a_i \in Y$.
Let $\alpha \in \mathrm{Bij}(X)$ be the cyclic permutation:

$$\alpha \cdot (a_1, \ldots, a_p) = (a_p, a_1, \ldots, a_{p-1}).$$

We saw that this gives an *action* $C_p \curvearrowright X$ of the cyclic group of order p on X.

(6) Suppose that $Y = G$ is a group.

(a) Show that the subset

$$Z = \{(g_1, \ldots, g_p) : \; g_1 g_2 \cdots g_p = e\} \subset X$$

is *stable* under the action of C_p. That is, show that, if $(g_1, \ldots, g_p) \in Z$ then $\alpha \cdot (g_1, \ldots, g_p) \in Z$.

We want to show $\alpha \cdot (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}) \in Z$.

Demonstration: we have $g_1 g_2 \cdots g_p = e$. Then, $g_1 g_2 \cdots g_{p-1} = g_p^{-1} \implies g_p g_1 g_2 \cdots g_{p-1} = g_p g_p^{-1} = e$. Therefore, $\alpha \cdot (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}) \in Z$. We have shown that Z is stable under the action of C_p.

(b) Show that, if G is a finite group, then $|Z| = |G|^{p-1}$.

For the first $p-1$ elements of any element $(g_1, \ldots, g_p)$ in Z, we have $|G|^{p-1}$ choices. However, for the last element, namely g_p, there is only one choice to have $g_1 g_2 \cdots g_p = e$, as there is a unique inverse of $g_1 g_2 \cdots g_{p-1}$. g_p must be that unique inverse. Notice that we did not have any restrictions on the first $p-1$ elements, as we can always force $(g_1, \ldots, g_p) \in Z$ by setting g_p as we did.

(c) Deduce that, if $p \mid |G|$, then Z^{C_p} is has size at least p.

$(e, e, e, \ldots, e) \in Z^{C_p}$ as this is invariant under powers of σ and also $ee \cdots e = e$ so our p-tuple is in Z.

C_p is a p group as $|C_p| = p$ is a power of p. Then, C_p is a p-group acting on Z. By problem 5, we know $|Z| \equiv |Z^{C_p}| \pmod{p}$. Since $|X| = |G|^{p-1}$ and $p \mid |G|$, $p \mid |Z|$. Therefore, $0 \equiv |Z^{C_p}| \pmod{p}$, meaning $p \mid |Z^{C_p}|$.

Since we showed $(e, e, \ldots, e) \in Z^{C_p}$, $|Z^{C_p}| \neq 0$. Now, to satisfy $p \mid |Z^{C_p}|$, $|Z^{C_p}|$ must now be a positive multiple of p. Therefore, Z^{C_p} has at least p elements.

(d) Conclude that there exists an element $g \in G$ of order p.

Now, these elements must look like $(g, g, \ldots, g)$. If any adjacent elements g_i, g_{i+1} are different (position number modulo p), Then, $\sigma(g_1, g_2, \ldots, g_i, g_{i+1}, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_i, g_{i+1}, \cdots, g_{o-1})$. Here, the new $i+1$th position has $g_i \neq g_{i+1}$, so $(g_1, g_2, \ldots, g_i, g_{i+1}, \ldots, g_p) \neq \sigma(g_1, g_2, \ldots, g_i, g_{i+1}, \ldots, g_p)$. This means that such an element is not in Z^{C_p}.

So now we have $(g, g, \ldots, g) \in Z^{C_p}$ where $g \neq e$. Since $(g, g, \ldots, g) \in Z$, $gg \cdots g = g^p = e$. Therefore, $|g| \mid p$, meaning $|g|$ is 1 or p. Since $g \neq e$, $|g| = p$. We have found an element with order p.

*Remark: This problem proves something called **Cauchy's theorem**: If p is a prime dividing the order of a finite group G, then G contains an element of order p.*

(7) Let G be a non-abelian group of order 6.

(a) Show that the subset $X \subset G$ of elements of order 2 is non-empty.

By problem 6d, since 2 is a prime number that divides the $|G| = 6$, there is an element of order 2. Therefore, X is non=empty.

(b) Show that, X is *stable* under the conjugation action of G on itself.

Suppose $x \in X$. Then, we need to prove $\forall g \in G, gxg^{-1} \in X$. First, $(gxg^{-1})^1 \neq e$. This is because $(gxg^{-1})^1 = e \implies gxg^{-1} = e \implies gx = g \implies x = e \implies |x| = 1 \implies x \notin X$. Now, we prove $(gxg^{-1})^2 = e$. $(gxg^{-1})^2 = gxg^{-1}gxg^{-1} = gx^2g^{-1} = gg^{-1} = e$.

Therefore, 2 is the lowest possible positive power that yields the identity. So $|gxg^{-1}| = 2$, meaning $gxg^{-1} \in X$. Therefore, X is stable under the conjugation action of G on itself.

(c) Deduce that X has exactly 3 elements, and use this to write down an *isomorphism* $G \xrightarrow{\simeq} S_3$.

Let $g \in G$ be an element such that $|g| = 3$. This exists because $3 \mid |G| = 6$ and by problem 6d. Then, $G = \{e, g, g^2, x, gx, g^2x\}$. No two are alike: the first three elements are distinct because $|g| = 3$ (ex. $g = g^2 \implies g = e \implies |g| \neq 3$. The other half of the elements are distinct because of the same reason, after canceling x (ex. $x = xg \implies g = e \implies |g| \neq 3$. No element from the first half is equal to the second half, else x is a power of g and would not have order 2 (ex. $x = g \implies |x| = 3 \neq 2$.

Claim: if $x \in X$, x, gxg^{-1}, g^2xg^{-2} are all distinct elements of order 2. By way of contradiction, suppose two of these are equal (we would see that if any two are equal, the other two are equal through a series of iff statements). First note that $g^{-1} = g^3g^{-1} = g^2$ and $g^{-2} = g^3g^{-2} = g$. Now,

$$x = g^2xg^{-2} \iff gxg^{-1} = x \iff gx = xg \iff x = g^{-1}xg \iff$$

$$x = g^2xg^{-2} \iff g^2xg^{-2} = g^4xg^{-4} \iff g^2xg^{-2} = gxg^{-1}$$

Therefore, $g^kxg^{-k} = x$ and this means $g^kx = xg^k$, so powers of g and x commute. Using this fact, we want to show that G is abelian.

Case 1: $g^kg^j = g^{k+j} = g^{j+k} = g^jg^k$ Case 2: $g^k(g^jx) = g^jg^kx = g^jxg^k = (g^jx)g^k$. Note that we used a result from case 1. Case 3: $(g^kx)g^j = g^kxg^j = g^kg^jx = g^jg^kx = g^j(g^kx)$. Case 4: $(g^kx)(g^jx) = g^kxg^jx = g^jg^kxx = g^jxg^kx = (g^jx)(g^kx)$.

So G is abelian. This is a contradiction.

Now, there are no more elements of order 2. We know e has order 1, g has order 3, and g^2 has order 3 ($g^2 \neq e$, $(g^2)^2 = g^4 = g \neq e$, and $(g^2)^3 = (g^3)^2 = e^2 = e$). Therefore, we have only three elements remaining that can be of order 2. These must correspond to what we have.

We label/index the elements x as 1, gxg^{-1} as 2, g^2xg^{-2} as 3. We then have a group action $G \curvearrowright \{1,2,3\}$, meaning we have a homomorphism $\rho : G \times \{1,2,3\} \to S_3$ via $\forall h \in G \forall y \in \{1,2,3\}, \rho(h)(y) = hyh^{-1}$.

Now, for each $\{1,2,3\}$, their orbits have three elements. To confirm this, we only need to check for each case. If we have $\mathcal{O}(1) = \{1,2,3\}$, it automatically follows that $\mathcal{O}(2)$ and $\mathcal{O}(3)$ are the same. Now, $\rho(e)(1) = 1, \rho(g)(1) = g1g^{-1} = gxg^{-1} = 2, \rho(g^2)(1) = g^21g^{-2} = g^2xg^{-2} = 3$. Therefore, $\mathcal{O}(1) = \mathcal{O}(2) = \mathcal{O}(3) = \{1,2,3\}$.

Now, we wish to find the stabilizers of 1 and 2 respectively. We know that $|G|/|\mathcal{O}(1)| = |G_1| = |G_2| = 2$.

Now, $\rho(e)(1) = 1$ and $\rho(x)(1) = x1x^{-1} = xxx^{-1} = x = 1$. So $G_1 = \{e, x\}$.

Remember that since $|g^2x| = 2$, $(g^2x)^{-1} = g^2x$, as $(g^2x)(g^2x) = e$. Similarly, $|gx| = 2$ and $(gx)^2 = e$, so gx is its own inverse. Then, $gx = (gx)^{-1} = x^{-1}g^{-1} = xg^{-1}$. (Last step is from the fact that $x^2 = e$ and x is its own inverse again.)

So, $\rho(e)(2) = 2$ and $\rho(g^2x)(2) = g^2xgxg^{-1}(g^2x)^{-1} = g^2xgxg^{-1}g^2x = g^2xgxgx = g^2x(gx)^2 = g^2x = ggx = gxg^{-1} = 2$. Therefore, $G_2 = \{e, g^2x\}$.

Now we are ready to prove injectivity. $\rho(k_1) = \rho(k_2)$. This means k_1 and k_2 takes every element in $\{1,2,3\}$ to the same place: $\forall t \in \{1,2,3\}, \rho(k_1)(t) = k_1 \cdot t = \rho(k_2)(t) = k_2 \cdot t$. So, $k_1 \cdot t = k_2 \cdot t \implies k_2^{-1} \cdot (k_1 \cdot t) = k_2^{-1} \cdot (k_2) \cdot t \implies k_2^{-1}k_1 \cdot t = e \cdot t = t$. Therefore, $k_2^{-1}k_1 \in G_t \forall t \in \{1,2,3\}$. So $k_2^{-1}k_1 \in G_1 \cap G_2$.

Recall $G_1 = \{e, x\}$ and $G_2 = \{e, g^2x\}$, so $G_1 \cap G_2 = \{e\}$. Therefore, $k_2^{-1}k = e \implies k_1 = k_2$. We have proven that $\forall k_1, k_2 \in G, \rho(k_1) = \rho(k_2) \implies k_1 = k_2$, showing injectivity.

Because $|G| = |S_3| = 6$ is finite, injectivity automatically means surjectivity holds.

Therefore, if we label/index the elements x as 1, gxg^{-1} as 2, g^2xg^{-2} as 3. We have a isomorphism $\rho : G \times \{1, 2, 3\} \to S_3$ via $\forall h \in G \forall y \in \{1, 2, 3\}, \rho(h)(y) = hyh^{-1}$.

(8) Suppose that G is a p-group. Use problem 4 to show that $Z(G) \neq \{e\}$ is non-trivial.

Note that we need to know that G itself is non-trivial, for its order to be a multiple of p. We will assume this.

Suppose we have the conjugation action of G on itself. ($G \curvearrowright G$ via $g \cdot x = gxg^{-1}$)We demonstrated $Z(G) = G^G$. By problem 5, we know $|G| \equiv |G^G| \pmod p$. So $|G| \equiv |Z(G)| \pmod p$. Since G is a p-group with size greater than 1, $p \mid |G|$. Therefore, $|Z(G)| \equiv 0 \pmod p$, meaning $p \mid |Z(G)|$. Since $e \in Z(G)$ ($\forall g \in G, eg = ge = g$), $|Z(G)|$ is a positive multiple of p, meaning $|Z(G)| \geq p$. This means that there must be other elements in the center of G, showing $Z(G)$ is non-trivial.

A subgroup $H \leq G$ is **normal** if, for all $h \in H$, $g \in G$, we have $ghg^{-1} \in H$. In other words, $H \leq G$ is *stable* for the conjugation action.

(9) Prove the following:

(a) $Z(G)$ is a *normal* subgroup of G;

We prove $Z(G)$ is a group.

Closure: $\forall a, b \in Z(G), ab \in Z(G)$ because $\forall g \in G, abg = agb = gab$. Identity: $e \in Z(G)$ as $\forall g \in G, eg = ge$ Inverses: $\forall a \in Z(G), a^{-1} \in Z(G)$ because $\forall g \in G, a^{-1}g = (g^{-1}a)^{-1} = (ag^{-1})^{-1} = ga^{-1}$.

Now we prove $Z(G)$ is normal.

$\forall z \in Z(G), g \in G, gzg^{-1} = zgg^{-1} = ze = z \in Z(G)$. (We used the fact that z commutes with g.) Therefore, $Z(G)$ is a normal subgroup of G.

(b) $Z(G) = G$ if and only if G is abelian.

If $Z(G) = G$, $\forall g_1, g_2 \in G, g_1, g_2 \in Z(G)$ and this means $g_1g_2 = g_2g_1$, so G is abelian.

If G is abelian, $\forall g \in G, h \in H, gh = hg \implies g \in Z(G)$, meaning $G \subseteq Z(G)$. We know $Z(G) \subseteq G$ by definition (and because $Z(G)$ is a subgroup), so $Z(G) = G$.

Therefore, $Z(G) = G \iff G$ is abelian.