MATH 3311, FALL 2025: HOMEWORK 2

A **homomorphism** $f : G \to G'$ of a groups is a function satisfying

$$f(g * h) = f(g) * f(h) \in G'$$

for all $g, h \in G$. A homomorphism is an **isomorphism** if it is a bijection. In this case, we will denote it as follows:

$$f : G \xrightarrow{\simeq} G'.$$

Two group G and G' are **isomorphic** if there is some isomorphism $f : G \xrightarrow{\simeq} G'$. In this case, we will write $G \simeq G'$.

(1) Consider the additive group $G_1 = (\mathbb{R}, +)$: this is the set of real numbers equipped with addition. Consider also the multiplicative group $G_2 = (\mathbb{R}^+, \cdot)$: this is the set of *positive* real numbers equipped with multiplication. Construct an explicit isomorphism between the two groups. By this I mean, write down a bijective homomorphism $\varphi : G_1 \to G_2$.
Hint: You need a function that converts addition to multiplication.

$\varphi(x) = e^x$ (e is the irrational number in this problem) is such an isomorphism from G_1 to G_2. It must be that e^x is well defined from its analytic construction. Since e^x passes the horizontal line test, φ is injective (i.e. $e^{x_1} = e^{x_2} \implies x_1 = x_2$). Also, since every positive number is given by an input from the reals by e^x (also $\forall y \in \mathbb{R}^+ \exists x \in \mathbb{R} : e^x = y$ because you may take $x = \ln(y)$), φ is surjective.

Now, $\varphi(a + b) = e^{a+b} = e^a \cdot e^b = \varphi(a) \cdot \varphi(b)$. Therefore, φ is a bijective homomorphism (i.e. an isomorphism) from G_1 to G_2. This is an isomorphism.

A **finite group** is a group G with a finite number of elements. The **order** of a finite group G is the number of elements in G, and is denoted $|G|$.
A group is **abelian** if for all $g, h \in G$, we have $g * h = h * g$; otherwise, it is **non-abelian**.

(2) Let G be a finite abelian group of order n. Show that, for any $g \in G$, we have $g^n = e$.[1] *Hint: This is an exact generalization of the proof of Fermat's little theorem from Homework 1.*

Suppose $G = \{g_1, g_2, \ldots, g_n\}$ with n distinct elements.

Lemma: $\forall g \in G, \tilde{G} = \{g * g_1, g * g_2, ..., g * g_n\} = G$. Proof: Since $*$ is a binary operation closed under G, it is clear that $\{g * g_1, g * g_2, ..., g * g_n\} \subseteq G$. For $i \neq j$ and i and j in $\{1, 2, ..., n\}$, $g * g_i \neq g * g_j$. By way of contradiction, if $g * g_i = g * g_j$, then $g_i * g = g_j * g \implies g_i = g_j$ via right cancellation. However, though $i \neq j$, the elements are not distinct. This is a contradiction.**Q.E.D**

Therefore, by the lemma, $\Pi_{i=1}^n g * g_i = \Pi_{i=1}^n g_i$ (here, the product is using the binary operation $*$). Because G is abelian and associative, we can reorder elements of the product of the left-hand side to match the order of elements on the right-hand side without changing the product.

Notice that

$$\Pi_{i=1}^n g * g_i = (g * g_1) * \Pi_{i=2}^n = (g * g_1) * (g * g_2) * \Pi_{i=3}^n = ((g * g_1) * g) * g_2) * \Pi_{i=3}^n$$

[1] Here, g^n is short-hand for the element $\underbrace{g * g * \cdots * g}_{n\text{-times}}$.

using associativity, and then

$$((g * g_1) * g) * g_2) * \Pi^n_{i=3} = ((g * (g_1 * g)) * g_2) * \Pi^n_{i=3} = ((g * (g * g_1)) * g_2) * \Pi^n_{i=3}$$

by associativity and commutativity. Then, that is equal to

$$((g * g) * g_1)) * g_2) * \Pi^n_{i=3} = ((g^2 * g_1) * g_2) * \Pi^n_{i=3} = (g^2 * (g_1 * g_2)) * \Pi^n_{i=3}$$

Notice this is actually

$$(g^2 * \Pi^2_{i=1} g_i) * \Pi^n_{i=3}(g * g_i)$$

Repeating this process again,

$$\Pi^n_{i=1} g * g_i = (g^2 * \Pi^2_{i=1} g_i) * \Pi^n_{i=3}(g * g_i) = (g^3 * \Pi^3_{i=1} g_i) * \Pi^n_{i=4}(g * g_i)$$

This eventually yields (in finite steps) $\Pi^n_{i=1} g * g_i = g^n \Pi^n_{i=1} g_i$.

Remember that $\Pi^n_{i=1} g * g_i = \Pi^n_{i=1} g_i$. Now, we know $\Pi^n_{i=1} g_i = g^n * \Pi^n_{i=1} g_i$. Then, $e * \Pi^n_{i=1} g_i = g^n * \Pi^n_{i=1} g_i$. Applying right cancellation, we get $g^n = e$.

(3) Write down a list of groups of order 4 such that every other group order 4 is isomorphic to exactly one group on this list. Are any of them non-abelian?

Every group of order 4 is isomorphic to one of $(\mathbb{Z}/4\mathbb{Z}, +, 0)$ and $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0,0))$ where $(a, b) + (c, d) = (a + c, b + d)$. Both of these are abelian.

Lemma 0: $e^k = e$ for $k \in \mathbb{Z}$. $e^k = e * e^{k-1} = e$. **Q.E.D**

Part 1: If a group G of order 4 is cyclic with generator g (i.e. $G = \{e, g, g^2, g^3\}$), it is isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +, 0)$ through $\varphi : \mathbb{Z}/4\mathbb{Z} \xrightarrow{\simeq} G$ via $\varphi(k) = g^k$.

Lemma 1: $g^4 = e$. We may prove G is abelian because by number 2, we know that then $g^4 = e$. Any two elements can be represented by g^k and g^j. $g^k * g^j = g^{k+j} = g^{j+k} = g^j * g^k$. We already see that G is abelian without using isomorphism properties. **Q.E.D**

Proving well defined ness, and injectivity, we may demonstrate $i = j \iff \varphi(k) = \varphi(j)$. For $\implies$ direction we must show that different representatives for the equivalence class does not change the result. Using the Euclidean algorithm, we know $i = q_1 \cdot 4 + r$ and $j = q_2 \cdot 4 + r$ (same remainder). Then, $g^i = g^{q_1 \cdot 4 + r} = (g^4)^{q_1} * g^r = e^{q_1} * g^r = e * g^r = g^r$. Similarly, $g^j = g^r$. So $g^i = g^j$.

For the $\impliedby$ direction, we use the contrapositive. $i \neq j \implies g^i \neq g^j$ Without loss of generality, assume $i > j$ (we also assume here that i and j are the least nonnegative representatives). Then, as always, $g^i = g^j \implies g^{i-j} = e$. However, $i - j < 4$ and this means the group generated by G would have size less than 4 (again, as always).Therefore, $i \neq j \implies g^i \neq g^j$ and this means $\varphi(i) \neq \varphi(j)$, proving the $\impliedby$ direction.

To prove surjectivity, every element $g^k \in \{e = g^0, g, g^2, g^3\}$ is hit by $\varphi(k) = g^k$.

Now, $\varphi(a + b) = g^{a+b} = g^a * g^b = \varphi(a) * \varphi(b)$. If $a + b$ goes over 4, not that the result still stands. For extra clarity, $\varphi(a + b) = \varphi(a) * \varphi(b) \in G$ by closure. Furthermore, applying the Euclidean algorithm to $a + b$ yields $a + b = q \cdot 4 + r$ with $r \in \{0, 1, 2, 3\}$, so $g^{a+b} = (g^4)^q * g^r = e^q * r = e * q^r = q^r \in G$.

Thus cyclic groups of order 4 are thus isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +, 0)$.

Part 2: If a group G of order 4 is not cyclic, choosing any non-identity element $g \in G$ must have a least positive number k such that $g^k = e$. If there is no such number that yields $g^k = e$, then

$\{g^n : n \in \mathbb{Z}\}$ is a subset of the set of the group, but that subset is infinite.

Furthermore, k must actually be equal to 2. If $k > 4$, the subset generated by g would have size greater than 4. If $k = 4$, the group would be generated by g. If $k = 3$, $\{g, g^2, e\} \subset G$. Then, there is an element remaining in G that is not a power of g. Call this element h. Then, $gh \in G$ but $g * h \neq h$ and $g * h \notin \{g, g^2, e\}$. The former is true because otherwise $g = e$ via right cancellation. The latter wouldn't work either, because via left cancellation, h is a power of g. But then, we have more elements than 4. Then, the remaining positive number is 2 (1 cannot work because $g^1 = e \implies g = e$). Since we chose any arbitrary non-identity element, this is true for all such non-identity elements.

For convenience, we now label the elements of G: $G = \{e, a, b, c\}$. We know $a^2 = b^2 = c^2 = e$. Also, it must be true that $a * b = b * a = c$, $b * c = c * b = a$, $c * a = a * c = b$. Otherwise, if we take an example of $a * b$, if $a * b = e$, b is the inverse of a, but a is the inverse of itself. so $a = b$. In addition, if $a * b = b$, via right cancellation, $a = e$. Similarly, $a * b \neq a$. Therefore, any product of distinct non-identity elements must be the other one. We also know that by the identity property, anything multiplied by the identity regardless of order is itself. Therefore, we know the multiplication table of the binary operation of G. Also notice that all the elements commute with each other. We already know that G is abelian.

We are now in the position to construct the isomorphism $\phi : G \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ via $\phi(e) = (0, 0)$, $\phi(a) = (1, 0)$, $\phi(b) = (0, 1)$, and $\phi(c) = (1, 1)$. This is well defined as we gave explicit answers for each input. It is injective because the output of our function can only be same when the input is same. It is surjective because every element in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is hit by one of the elements in G.

Also, it satisfies the property that $\forall g, h \in G, \phi(g * h) = \phi(g) + \phi(h)$. We prove this by actually doing all the computations (through some casework to simplify). When operating with the same element to itself, $\forall g \in G$, $\phi(g*g) = \phi(e) = (0, 0)$. Also, $\phi(g)+\phi(g) = 2\phi(g)$ but any element in $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, when multiplied by 2, is $(0, 0)$, as $2(a, b) = (2a, 2b)$ and since $2 \mid 2a$ and $2 \mid 2b$, $(2a, 2b) = (0, 0)$. Therefore, $\phi(g * g) = \phi(g) + \phi(g)$. When operating with the identity and a non-identity element $\tilde{g}$,

$$\phi(e * \tilde{g}) = \phi(\tilde{g} * e) = \phi(\tilde{g}) = \phi(\tilde{g}) + (0, 0) = \phi(\tilde{g}) + \phi(e) = \phi(e) + \phi(\tilde{g})$$

(both the starting group and ending group are abelian). So $\phi(e * \tilde{g}) = \phi(e) + \phi(\tilde{g})$ and $\phi(\tilde{g} * e) = \phi(\tilde{g}) + \phi(e)$. Lastly, when operating on different nonidentity elements, $\phi(a * b) = \phi(c) = (1, 1) = (1, 0) + (0, 1) = \phi(a) + \phi(b)$. $\phi(b * c) = \phi(a) = (1, 0) = (0, 1) + (1, 1) = \phi(b) + \phi(c)$. $\phi(c * a) = \phi(b) = (0, 1) = (1, 1) + (1, 0) = \phi(c) + \phi(a)$. Remember that the groups are abelian so changing the order of operands do not destroy this property.

Therefore, we have a bijective homomorphism. This group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, +, (0, 0))$.

A group G is **cyclic** if there exists an element $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$. In this case, we say that g **generates** G.

(4) Show that the groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ (under addition) are cyclic.

$\mathbb{Z}$ is cyclic because $\mathbb{Z} = \{n1 : n \in \mathbb{Z}\} = \{n : n \in \mathbb{Z}\}$, so the created set is the same as listing every element of $\mathbb{Z}$. Therefore, $1 \in \mathbb{Z}$ generates $\mathbb{Z}$ and $\mathbb{Z}$ is cyclic.

Similarly, $\mathbb{Z}/n\mathbb{Z}$ is cyclic because $\mathbb{Z}/n\mathbb{Z} = \{n1 : n \in \mathbb{Z}\}$. This is actually the same as $\{n : n \in \mathbb{Z}/n\mathbb{Z}\}$ because each integer belongs to precisely one equivalence class modulo n (remember, $n1$ is under modulo n addition and not the "regular" addition as the set above). Again, the created list is the same as listing every element of $\mathbb{Z}/n\mathbb{Z}$. Thus, $1 \in \mathbb{Z}/n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is cyclic.

(5) Show that any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$, depending on whether the group is infinite or finite.

Hint: If G is a cyclic group with $G = \{g^n : n \in \mathbb{Z}\}$, you want to write down a homomorphism from either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ to G depending on whether G is finite or infinite. If G is finite, then what should n be?

Part 1: If the group G is infinite and generated by the element $g \in G$, $\varphi : \mathbb{Z} \xrightarrow{\simeq} G$ given by $\varphi(k) = g^k$ is an isomorphism.

To prove well-defined ness and injectivity, we may prove $i = j \iff \varphi(i) = \varphi(j)$. The $\implies$ direction is clear, as $i = j \implies g^i = g^j \implies \varphi(i) = \varphi(j)$. For the $\impliedby$ direction, by way of contradiction, assume $g^i = g^j$ but $i \neq j$. Also, without loss of generality, assume $i > j$. Then,

$$g^i * (g^j)^{-1} = g^j * (g^j)^{-1} \implies g^i * g^{-j} = e \implies g^{i-j} = e$$

Then, $G = \{g^k : k \in \mathbb{Z}\} = \{g^k : k \in \{0, 1, ..., i-j-1\}\}$, because applying the Euclidean algorithm on k yields $k = q(i-j) + r$, and $g^k = g^{q(i-j)+r} = (g^{(i-j)})^q * g^r = e^q * g^r = g^r$ and $r \in \{0, 1, ..., i-j-1\}$. Clearly, G is finite here. We have reached a contradiction.

Now we want to prove surjectivity. For any $\tilde{g} \in G$, $\tilde{g} = g^k$ for some integer k. Then, $\varphi(k) = g^k = \tilde{g}$.

Additionally, $\forall a, b \in \mathbb{Z}, \varphi(a+b) = g^{a+b} = g^a * g^b = \varphi(a) * \varphi(b)$, proving the property required for homomorphisms.

Since we have a homomorphism with bijectivity, it is an isomorphism. Cyclic group G (with an infinite amount of elements) is isomorphic to $\mathbb{Z}$.

Part 2: If the group G is finite (i.e. $|G| = n$ for some positive integer n) and generated by $g \in G$, then $\phi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} G$ where $\phi(k) = g^k$ is an isomorphism.

Lemma 1: $G = \{g, g^2, ..., g^n\}$. Clearly, $\{g, g^2, ..., g^n\} \subseteq G$ because $G = \{g^k : k \in \mathbb{Z}\}$. To demonstrate the opposite subset relation, we may show that $\{g, g^2, ..., g^n\}$ has n elements (so same number of elements as G). By way of contradiction, suppose not. Then, two elements in the set must be alike. $i \neq j$ but $g^i = g^j$. Without loss of generality, assume $i > j$. Then,

$$g^i * (g^j)^{-1} = g^j * (g^j)^{-1} \implies g^i * g^{-j} = e \implies g^{i-j} = e$$

. Then, $G = \{g^k : k \in \mathbb{Z}\} = \{g^k : k \in \{0, 1, ..., i-j-1\}\}$, because applying the Euclidean algorithm on k yields $k = q(i-j) + r$, and $g^k = g^{q(i-j)+r} = (g^{(i-j)})^q * g^r = e^q * g^r = g^r$ and $r \in \{0, 1, ..., i-j-1\}$. Clearly, $|G| \leq i-j$ but $i - j < n$. So $|G| < n$. We have reached a contradiction. **Q.E.D**

Lemma 2: $g^n = e$. By Lemma 1, one of $\{g, g^2, ..., g^n\}$ should be the identity, e. However, that cannot be the case for g^i for which $i < n$. Then, through the same argument as lemma 1 (except using just i instead of $i-j$), $|G| < n$. Therefore, it has to be $g^n = e$. **Q.E.D**

To prove well-defined ness and injectivity, we again prove $i = j \iff \phi(i) = \phi(j)$ (note that the equality in the left side refers to having same equivalence classes modulo n).
$\implies$ direction: $i = j$ means $i = q_1 n + r$ and $j = q_2 n + r$. Then, $\phi(i) = g^{q_1 n + r} = (g^n)^{q_1} * g^r = e^{q_1} * g^r = e * g^r = g^r$. Similarly, $\phi(j) = g^r$. Therefore, $\phi(i) = \phi(j)$.
$\impliedby$ direction: $\phi(i) = \phi(j)$ means $g^i = g^j$. Then, $g^i * (g^j)^{-1} = g^j * (g^j)^{-1}$. We get $g^i * g^{-j} = g^{i-j} = e$. Claim: $n \mid i - j$ i.e. $i \equiv j \pmod{n}$. Proof: By way of contradiction, suppose not. Applying the Euclidean algorithm yields $i - j = qn + r$. Then, by a similar reason given in lemma 1 (this time with r instead of $i - j$), we get a contradiction that $|G| < n$. Therefore it must be that $i \equiv j \pmod{n}$.

Now we have surjectivity remaining. We know that by lemma 1, $G = \{g, g^2, ..., g^n\}$. Then to get $g^k \in G = \{g, g^2, ..., g^n\}$, we can simply do $\phi(k) = g^k$, and we know $k \in \mathbb{Z}/n\mathbb{Z}$.

To verify ϕ is a homomorphism, $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, \phi(a+b) = g^{a+b} = g^a * g^b = \phi(a) * \phi(b)$.

We again have a homomorphism that is bijective. Any finite cyclic group with order n is thus isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Combining parts 1 and 2, we get the conclusion that any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$, depending on the size of the group.

(6) We will soon see that the conclusion of Problem 2 holds for *any* finite group (not just abelian ones). Use this to show that any finite group of order p with p prime must be isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In particular, any such group will be abelian.

Let G be a finite group of prime order p. By the given statement, we know that any element to the pth power is the identity element e. We will choose any non-identity element $g \in G$ (this must exist because the least prime number is 2, so there must be at least one non-identity element).

Claim: $G = \{e, g, g^2, ..., g^{p-1}\}$. Obviously, $\{e, g, g^2, ..., g^{p-1}\} \subseteq G$ because the binary operation is closed under G. To show that the two sets are actually equal, we may show that they have the same size p. For $\{e, g, g^2, ..., g^{p-1}\}$ to not have p elements, two of them must be the same. This means for some $i \neq j$ and $0 \leq i, j \leq p-1$, $g^i = g^j$. Without loss of generality, assume $i > j$. Then, as always, $g^{i-j} = e$. However, $i - j < p$. Note that $\gcd(i-j, p) = 1$ because $p \nmid i - j$ for 0 is the only nonnegative multiple of p less than p, but $i - j > 0$ as $i \neq j$ and $i > j$. By Bezout's identity, we know that there are integers a and b where $a(i-j) + bp = 1$. Then, $g = g^{a(i-j)+bp} = (g^{i-j})^a * (g^p)^b = e^a * e^b = e * e = e$. However, we chose g to not be the identity element. Therefore, $\{e, g, g^2, ..., g^{p-1}\}$ must have p elements, establishing $G = \{e, g, g^2, ..., g^{p-1}\}$.

Therefore, g generates G, and $G = \{e, g, g^2, ..., g^{p-1}\} = \{g^k : k \in \mathbb{Z}\}$ as for any $k \in \mathbb{Z}$, applying the Euclidean algorithm yields $k = qp + r$, and as always, $g^k = g^r$.

Note: as always means as done in a previous problem or section.

Also any such group will be abelian because any two elements are in the form of g^k and g^j. Then, $g^k * g^j = g^{k+j} = g^{j+k} = g^j * g^k$.

(7) Can you find two non-abelian groups of order 6 that are *not* isomorphic to each other?

Lemma 0: In a finite group, any non-identity element g must have the least positive number k (let's call this the powering number) where $g^k = e$. (This is the same proof done in number 3 but for general, finite groups.) Suppose not: then, $\{g^k : k \in \mathbb{Z}\} \subseteq G$ but that set is infinite. This yields a contradiction. Also note that the powering number cannot be 1. If so, that element would be the identity, though we chose a non-identity element. **Q.E.D**

Lemma 1: In a non-cyclic finite group G with $|G| = 2n$, the powering number of each non-identity element must be less than or equal to n. First, if the powering number is n for $\tilde{g}$, then $\{e, \tilde{g}, \tilde{g}^2, ..., \tilde{g}^{2n-1}\}$ is a subset of G with equal number of elements (or else two different elements are equal with $i > j$ and $\tilde{g}^i = \tilde{g}^j$, then $i - j$ is a number such that $\tilde{g}^{i-j} = e$ but $i - j < 2n$ contradicts the definition of the powering number). Therefore, it is actually G, meaning G is cyclic, generated by $\tilde{g}$ ($G = \{e, \tilde{g}, \tilde{g}^2, ..., \tilde{g}^{2n-1}\} =$

$\{\tilde{g}^n : n \in \mathbb{Z}\}$). Now, we know the powering number is less than $2n$. **Q.E.D**

Now we want to prove that every powering number between (exclusive) n and $2n$ are unobtainable. By way of contradiction, suppose not: the powering number K for g is greater than n. Then, $\{e, g, g^2, \dots, g^{k-1}\} \subset G$ is the set of all the powers of g. (Again, there are k elements in that set.) Since that set has at most $2n-1$ elements, we are guaranteed at least one non-identity element h that is not a power of g. Then, consider $\{h, hg, hg^2, ..., hg^{k-1}\}$. None of the elements in the set can be a power of g (else h would be one as well). There are k elements in the set by the same argument as before after canceling out the hs. We now have $2k$ distinct elements in G. However, $|G| = 2n < 2k$. We have reached a contradiction. **Q.E.D**

Assume we have a non-abelian group G of order 6. Then for each non-identity element $g \in G$, by lemma 1, it must be true that either $g^2 = e$ or $g^3 = e$.

Lemma 2: We have at least one element with powering number of 3. We prove this by arriving at a contradiction if we have non-identity elements to all have powering number of 2.
$\forall j, k \in G, j * k = l$ for some $l \in G$. Then,

$$j * j * k = j * l \implies e * k = j * l \implies k = j * l \implies k * l = j * l * l \implies k * l = j * e$$

$$\implies k * l = j \implies k * k * l = k * j \implies e * l = k * j \implies l = k * j \implies j * k = k * j$$

But this means the group is abelian. **Q.E.D**

Lemma 3: There is at most two non-identity elements with powering number of 3. Note that if g has powering number 3, then g^2 has powering number 3 as well ($(g^2)^3 = (g^3)^2 = e^2 = e$). It cannot have powering number 2 as $(g^2)^2 = e \implies g^4 = e \implies g * g^3 = e \implies g * e = e \implies g = e$. Since powering 3 yields e and there is no less powerings that work, 3 must be the powering number. By Lemma 2, we know that there is one element $s \in G$ where the powering number of that element is 3. Now we know s^2 also has powering number 3. Suppose we have more that isn't a power of s: $h \in G$ has powering number 3. Then, we know h^2 has powering number 3, and not equal to any of s, s^2, or h. Then, sh and sh^2 are other elements not equal to any previous elements (if equal, it would cause h to be a power of s). Then, $\{e, s, s^2, h, h^2, sh, sh^2\} \subseteq G$ but that set has seven elements, which is greater than six. **Q.E.D**

So from Lemma 3, we know s, s^2, and e are elements of G, and any remaining elements now must have powering number of 2. Call one of these elements t. Then, $s * t$ and $s^2 * t$ are the other elements. Again, each element is different from the previous elements because otherwise t would be a power of s (which would cause it to be either the identity or have powering number 3). In summary, $G = \{e, s, s^2, t, s * t, s^2 * t\}$.

Lemma 4: $(g * h)^{-1} = h^{-1} * g^{-1}$. Proof: $(g * h) * (h^{-1} * g^{-1}) = g * ((h * h^{-1}) * g^{-1}) = g * (e * g^{-1}) = g * g^{-1} = e$. **Q.E.D**

Now, we want to develop a multiplication table. For convenience, we separate G into two disjoint sets: $G = \{s^0 = e, s, s^2\} \cup \{t, s * t, s^2 * t\}$. First, we remember that by Lemma 3, all the elements in the second set has powering number 2. Then, $(s^k * t)^2 = e \implies (s^k * t)(s^k * t) = e$. Therefore, $s^k * t$ is its own inverse. We know that $(s^k * t)^{-1} = t^{-1} * (s^k)^{-1} = t^{-1} * s^{-k}$. Since $t^2 = t * t = e$, t is its own inverse. Therefore, $t^{-1} * s^{-k} = t * s^{-k}$. In summary, $s^k * t = t * s^{-k}$

We are now ready to develop our multiplication table. There are four cases.

Case 1: element from first set operated with another one from the first set. Then,

$$s^k * s^j = s^{k+j}$$

Case 2: element from first set operated with an element from the second set. Then,

$$s^k * (s^j * t) = (s^k * s^j) * t = s^{k+j} * t$$

Case 3: element from the second set operated with an element from the second set:

$$(s^j * t) * s^k = s^j * (t * s^k) = s^j * (s^{-k} * t) = s^{j-k} * t$$

Case 4: an element from the second set operated with another element from the second set:

$$(s^j * t) * (s^k * t) = s^j * ((t * s^k) * t) = s^j * ((s^{-k} * t) * t)$$

$$= s^j * (s^{-k} * (t * t)) = s^j * (s^{-k} * e) = s^j * s^{-k} = s^{j-k}$$

We now construct an isomorphism from $(G, *, e)$ to $(D_6, \circ, \mathrm{Id})$. $\phi : G \xrightarrow{\simeq} D_6$. We define this isomorphism as following. $\phi(e) = \mathrm{Id}$, $\phi(s^k) = \sigma^k$ for any integer k, and $\phi(s^j * t) = \sigma^j * \tau$.

More explicitly (computationally), $\phi(e) = \mathrm{Id}$, $\phi(s) = \sigma$, $\phi(s^2) = \sigma^2$, $\phi(t) = \tau$, $\phi(s * t) = \sigma \circ \tau$, and $\phi(s^2 * t) = \sigma^2 \circ \tau$.

If we want to compute $\phi(s^k)$ generally, we use the Euclidean algorithm to find $k = q * 3 + r$ with $0 \leq r \leq 2$. $\phi(s^k) = \phi(s^{q \cdot 3} * s^r) = \phi(e^q * s^r) = \phi(e * s^r) = \phi(s^r)$. Since $0 \leq r \leq 2$, we have the result of computation. $\phi(s^k * t)$ is computed in a similar fashion. Also, $\phi(s^k) = \sigma^k = \sigma^{q \cdot 3 + r} = \mathrm{Id}^q \circ \sigma^r = \mathrm{Id} \circ \sigma^r = \sigma^r$. Similarly, $\phi(s^k * t) = \sigma^r \circ \tau$. These results are in fact in our result list, and match up to their respective inputs. So whenever $s^k = s^r$ or $s^k * t = s^r * t$, we don't need to worry about them having different calculations. Therefore, this function is well defined.

As seen from the explicit calculations, it is also injective, as different inputs always give different outputs. It is finally also surjective, as every element in D_6 is given by a certain element in G.

We now prove that the given function is a homomorphism. Again there are the same four cases.

Case 1: $\phi(s^k * s^j) = \phi(s^{k+j}) = \sigma^{k+j} = \sigma^k \circ \sigma^j = \phi(s^k) \circ \phi(s^j)$.
Case 2: $\phi(s^k * (s^j * t)) = \phi(s^{k+j} * t) = \sigma^{k+j} \circ \tau = \sigma^k \circ (\sigma^j \circ \tau) = \phi(s^k) \circ \phi(s^j * t)$.
Case 3: $\phi((s^k * t) * s^j) = \phi(s^{k-j} * t) = \sigma^{k-j} \circ \tau = \sigma^k \circ \sigma^{-j} \circ \tau = \sigma^k \circ \tau \circ \sigma^j = \phi(s^k * t) \circ \phi(s^j)$
Case 4: $\phi((s^k * t) * (s^j * t)) = \phi(s^{k-j}) = \sigma^{k-j} = \sigma^k \circ \tau \circ \sigma^j \circ \tau = \phi(s^k * t) \circ \phi(s^j * t)$

Therefore, any non-abelian group of order 6 must be isomorphic to D_6.

Lemma 5: If $(G, *, e_G)$ has an isomorphism to $(K, \cdot, e_K)$ given by $\psi : G \xrightarrow{\simeq} K$, then K has an isomorphism to G given by the inverse of ψ. By HW1#9 bullet 4, we know such a bijective function exists.
$\forall a, b \in K \exists \tilde{a}, \tilde{b} \in G : \psi(\tilde{a}) = a$ and $\psi(\tilde{b}) = b$. Then, $\psi(\tilde{a} * \tilde{b}) = \psi(\tilde{a}) \cdot \psi(\tilde{b}) = a \cdot b$. Now, we know that $\psi^{-1}(a \cdot b) = \psi^{-1}(a) * \psi^{-1}(b)$ because they both evaluate to $\tilde{a} * \tilde{b}$.
Therefore, ψ^{-1} is a bijective homomorphism (so an isomorphism) from K to G. **Q.E.D**

Lemma 6: If $(G, *, e_G)$ has an isomorphism β to $(H, \circ, e_H)$ and the latter has an isomorphism α to $(K, \cdot, e_K)$, then $(G, *, e_G)$ has an isomorphism to $(K, \cdot, e_K)$ via $\alpha \circ \beta$.

Proof: First, we demonstrate that $\alpha \circ \beta$ is injective.

$$\forall g_1, g_2 \in G : (\alpha \circ \beta)(g_1) = (\alpha \circ \beta)(g_2) \implies \alpha(\beta(g_1)) = \alpha(\beta(g_2)) \implies \beta(g_1) = \beta(g_2) \implies g_1 = g_2$$

This follows from the injectivity properties of each α and β.

Now, we demonstrate that $\alpha \circ \beta$ is surjective. This means $\forall k \in K \exists g \in G : (\alpha \circ \beta)(g) = \alpha(\beta(g)) = k$. Because α is surjective, $\exists h \in H$ where $\alpha(h) = k$. Because β is surjective, $\exists g \in G$ where $\beta(g) = h$. Then, $\alpha(h) = \alpha(\beta(g)) = k$.

Now it remains to prove that $\alpha \circ \beta$ is a homomorphism. $\forall g_1, g_2 \in G, (\alpha \circ \beta)(g_1 * g_2) = (\alpha \circ \beta)(g_1) \cdot (\alpha \circ \beta)(g_2)$. In other words, $\alpha(\beta(g_1 * g_2)) = \alpha(\beta(g_1)) \cdot \alpha(\beta(g_2))$. We may demonstrate this by using the homomorphism properties of β and then α.

$$\alpha(\beta(g_1 * g_2)) = \alpha(\beta(g_1) \circ \beta(g_2)) = \alpha(\beta(g_1)) \cdot \alpha(\beta(g_2))$$

Q.E.D

Now, take any two groups X and Y (with their binary operators and identity elements with the property that the group has order 6 and is nonabelian). We know that X is isomorphic to D_6. Also, Y is isomorphic to D_6. Using lemma 5, we see that D_6 is isomorphic to Y. Finally, using lemma 6, we see that X is isomorphic to Y. We chose arbitrary non-abelian groups of order 6. Therefore, there does not exist two non-abelian groups of order 6 that are not isomorphic to each other.

(8) (*Read the problem very carefully! There is a new level of abstraction here that you might not have grappled with before, but will be very useful as we go ahead in the course.*) Let G be a group equipped with an operation $*$. Then every element $g \in G$ gives a function

$$m_g : G \to G$$
$$m_g(h) = g * h.$$

In other words, we are considering the function given by *left* multiplication by g.

Show that the function $m : G \to \mathrm{Fun}(G)$ given by $m(g) = m_g$ (*it's a function whose output is a function!*) has the following properties:

- m is *injective* (that is, one-to-one);
- $m(g_1 * g_2) = m(g_1) \circ m(g_2)$ (as functions! *What axiom is essential here?*);
- $m(g)$ lies in $\mathrm{Bij}(G)$. (*Hint: Apply the third bullet point from Problem 9 on HW 1 to both $m(g)$ and $m(h)$, where $g * h = e$.*)

Conclude that m gives an *injective homomorphism of groups* from G to $\mathrm{Bij}(G)$.

First bullet point: m is injective, meaning $\forall g, h \in G, m(g) = m(h)$. $m(g) = m(h)$ means $m_g = m_h$. Consider the input e for both m_g and m_h. Since $m_g = m_h$, $m_g(e) = m_h(e) \implies g*e = h*e \implies g = h$, proving that m is injective.

Second bullet point: $m(g_1 * g_2) = m(g_1) \circ m(g_2)$ if and only if $\forall g \in G, m_{g_1 * g_2}(g) = (m_{g_1} \circ m_{g_2})(g)$. Therefore, we proceed to prove the latter. $\forall g \in G, m_{g_1*g_2}(g) = (g_1*g_2)*g = g_1*(g_2*g) = g_1*(m_{g_2}(g)) = m_{g_1}(m_{g_2}(g)) = (m_{g_1} \circ m_{g_2})(g)$ (by associativity, of course).

Third bullet point: Let h be the element such that $g * h = e$.
$m_g \circ m_h(x) = (g * h)(x) = x \forall x \in G$, so $m(g) \circ m(h) = \mathrm{Id}$. From the third bullet point from problem 9 on HW 1, $m(g)$ is surjective and $m(h)$ is injective. Since our choice of $g \in G$ doesn't matter for this fact, it is also true that $m(h)$ is surjective. Therefore, $m(h)$ is bijective. By the next bullet point from problem 9, we know that there is a unique bijective function $(m(h))^{-1}$ that satisfies $(m(h))^{-1} \circ m(h) = \mathrm{Id}$. Since that function is unique, $m(g) = (m(h))^{-1}$ is bijective.

Conclusion: Finally, m is an injective homomorphism of groups from G to $\mathrm{Bij}(G)$ because we proved injectivity via bullet one, homomorphism via bullet two, and that the output is a bijective function from G to G via bullet three.

(9) Use the previous problem to verify the following assertions about groups:

(a) A left identity is also a right identity: If $e * g = g$, for all $g \in G$, then $g * e = g$, for all $g \in G$.

(b) There is a unique identity element $e \in G$. That is, if $e' \in G$ is another element such that $e' * g = g$ for all $g \in G$, then $e' = e$.

(c) Inverses in groups are unique and agnostic to order of multiplication. More precisely, for every $g \in G$ there is a unique element $h \in G$ such that $g * h = e$, and it also satisfies $h * g = e$.

Hint: The previous problem shows that it is enough to do this for the group $\mathrm{Bij}(G)$*; that is, for functions, rather than abstract group elements.*

Fact 1 from previous problem set: If $\mathrm{Id} : X \to X$ is the identity transformation $\mathrm{Id}(x) = x$, then $\mathrm{Id} \circ f = f \circ \mathrm{Id} = f$, for all $f \in \mathrm{Fun}(X)$

Fact 2 from previous problem set: If $f \in \mathrm{Bij}(X)$, then there exists a unique $f^{-1} \in \mathrm{Bij}(X)$ such that $f \circ f^{-1} = \mathrm{Id}$. Moreover, it also satisfies $f^{-1} \circ f = \mathrm{Id}$.

First bullet point: $m_e = \mathrm{Id}$ because $\forall g \in G$, $m_e(g) = e * g = g$. Therefore, by fact 1, $\forall g \in G$, $m_e \circ m_g = m_g \circ m_e = m_g$. Then, by bullet point two from the previous question,$m_{g*e} = m_g$. By bullet one from the previous question, since m is injective, $m_{g*e} = m_g \implies m(g * e) = m(g) \implies g * e = g$. Thus, if $e * g = g$, for all $g \in G$, then $g * e = g$, for all $g \in G$.

Second bullet point: From the previous bullet point's proof, we know that $m_e = \mathrm{Id}$. Similarly $m_{e'} = \mathrm{Id}$ because $\forall g \in G$, $m_{e'}(g) = e' * g = g$. Therefore, $m_e = m_{e'}$. By bullet one from the previous question, since m is injective, $m_e = m_{e'} \implies m(e) = m(e') \implies e = e'$. Therefore, there is a unique identity element $e \in G$.

Third bullet point: Choose an arbitrary $g \in G$. Then, by the third bullet point of the previous problem, m_g is a bijective function. By fact 2, there is a unique $(m_g)^{-1}$ such that $m_g \circ (m_g)^{-1} = \mathrm{Id}$ and also $(m_g)^{-1} \circ m_g = \mathrm{Id}$. We know that g has a right inverse through properties of groups. We label this h. Also, $(m_g \circ m_h) = m_{g*h} = m_e = \mathrm{Id}$. Therefore, $m_h = (m_g)^{-1}$ as such a function is unique. Additionally, h is the unique inverse of g because if h' is also an inverse of g, it should also be true that $m_g \circ m_{h'} = \mathrm{Id}$ by similar fashion, and therefore $(m_g)^{-1} = m_h = m_{h'}$. Then, by injectivity of m, $h = h'$. Now, we show that h is also the left inverse. We know that $(m_g)^{-1} \circ m_g = \mathrm{Id}$, so $(m_g)^{-1} \circ m_g = m_h \circ m_g = m_{h*g} = \mathrm{Id} = m_e$. By injectivity, $m_{h*g} = m_e \implies m(h * g) = m(e) \implies h * g = e$.