Homomorphisms and isomorphisms

Juan Patricio Carrizales Torres

May 23, 2023

The notion of an *isomorphism* is that two groups have the same gorup-theoretic structure (any property that can be derived from the axioms of the group holds for both groups). Let $(G, *)$ and $(H, \cdot)$ be groups. A map $\phi : G \to H$ such that $\phi(x*y) = \phi(x)\cdot\phi(y)$ for all $x, y \in G$ is a homomorphism. For this map to be considered an ismorphism, it must be bijective. The symbol $\cong$ represent the equivalence isomorphic relation. Since $\cong$ is an equivalence relation in the set $\mathfrak{G}$ of all groups, it follows that there are equivalence clases that are isomorphic. This is important for the classification of groups using isomorphisms.

Also, one can show isomorphic relationships between sets by looking at their group presentations. Suppose for a group G with generators $\{r_1, \ldots, r_m\}$ and group H with some subset $\{s_1, \ldots, s_m\}$ that every relation in G is fulfilled in H when r_i is changed to s_i. Then there is a unique homomorphism $\varphi : G \to H$ such that $r_i \to s_i$. Furthermore, if $\{s_1, \ldots, s_m\}$ is the set of generators for H, then φ is surjective. Also, if $|G| = |H|$, then φ is injective and so an isomorphism.

1 Excercises

Let G and H be groups.

Problem 1. Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

Proof. We proceed by induction. First, note that $\varphi(e \cdot x) = \varphi(e) \cdot \varphi(x) = \varphi(x)$ for any $x \in G$ and so $\varphi(e) = e'$ (Recall that there is a unique identity element in a group). Since $\varphi : G \to H$ is a homomorphism, it follows that $\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0$ for any $x \in G$. Hence, the result is true for $n = 0$.

Now, assume that $\varphi(x^k) = \varphi(x)^k$ for any $x \in G$ and some nonnegative integer k. We show that $\varphi(x^{k+1}) = \varphi(x)^{k+1}$. Observe that

$$\begin{aligned}\varphi(x^{k+1}) &= \varphi(x^k \cdot x^1) \\ &= \varphi(x^k) \cdot \varphi(x) = \varphi(x)^k \cdot \varphi(x) \\ &= \varphi(x)^{k+1}.\end{aligned}$$

By the Principle of Mathematical Induction, $\varphi(x^n) = \varphi(x)^n$ for any $x \in G$ and any $k \in \mathbb{Z}^+$. □

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Proof. Let $x \in G$. Then $\varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$ and $\varphi(x \cdot x^{-1}) = \varphi(e) = e'$. Since there is a unique inverse for any element of a group, it follows that $\varphi(x) \cdot \varphi(x^{-1}) = e'$ implies that $\varphi(x^{-1}) = \varphi(x)^{-1}$, namely, it is the unique inverse of $\varphi(x)$. Now, consider what happens when we plug the inverse of x^n inside the function, namely, $\varphi(x^{-n})$ for some $n \in \mathbb{N}$. Note that,

$$\begin{aligned}\varphi\left(x^{-n}\right) &= \varphi\left(\left(x^{-1}\right)^n\right) \\ &= \varphi\left(x^{-1}\right)^n = \left(\varphi(x)^{-1}\right)^n \\ &= \varphi(x)^{-n}.\end{aligned}$$

Therefore, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. □

Problem 2. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

Proof. First, we show that $|\varphi(x)| = |x|$. Consider any $x \in G$ with some order $n = |x|$, where $n \in \mathbb{Z}^+$. Then, $\varphi(x^n) = \varphi(e) = e' = \varphi(x)^n$ and so $\varphi(x)$ has a finite order. Let $k = |\varphi(x)| \in \mathbb{Z}^+$. Note that,

$$\varphi(x)^k = e' = \varphi(e) = \varphi(x^k)$$

Then, $k \leq n$ ($\varphi(x)^k = \varphi(x)^n$) and $n \leq k$ ($x^n = x^k$), which implies that $n = k$.
For the previous argument, we only used the results that are derived from the homorphic property of the function and didn't need to assume that φ was bijective. Thus, for any homomorphic function $\varphi : G \to H$, $|\varphi(x)| = |x|$ for all $x \in G$.

Now, we show that the homomorphism $\varphi : G \to H$ being a bijection is a sufficient condition for both G and H to have the same number of elements of order n.
If the homomorphism $\varphi : G \to H$ is a bijection, then there is a one-to-one correspondence $x \leftrightarrow \varphi(x)$, where $|x| = |\varphi(x)|$ for any $x \in G$. Hence, both isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

Note that this only applies when we consider any n, including ∞. There can be homomorphic groups such that they have the same quantity of elements with order $n \in \mathbb{Z}^+$. □

Problem 3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi G \to H$ is a homomorphism, what additional condiitons on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

Proof. Since $\varphi : G \to H$ is an isomorphism, there is a one-to-one correspondence $x \leftrightarrow y$, where $x \in G$ and $y \in H$. Basically, we can "translate" one element from a group to the other, and viceversa. We just have to show that the abelian property is maintained throug the isomorphism. Note that,

$$x \cdot y = y \cdot x \implies \varphi(x \cdot y) = \varphi(x) * \varphi(y) = \varphi(y) * \varphi(x) = \varphi(y \cdot x). \forall x, y, \in G$$

$$y * x = x * y \implies \varphi^{-1}(y * x) = \varphi^{-1}(y) \cdot \varphi^{-1}(x) = \varphi^{-1}(x) \cdot \varphi^{-1}(y) = \varphi^{-1}(x * y). \forall x, y, \in H,$$

because the inverse of an isomorphism is homomorphic.
In the case of a homomorphism $\varphi : G \to H$ an additional condition to ensure that if G is abelian, then so is H, is that φ must be surjective. This is so because this implies that the image of φ is H and so the commutativity of G can be trasmitted to all the elements of H through the surjective homomorphism φ. □

Problem I. The homomorphism $\varphi : G \to H$ is injective if and only if there is a one-to-one correspondence between the identities of both groups.

Proof. The direct is clear, since a homomorphism maps the identity of G ot the identity of H. So let's assume the converse. Then, $e \leftrightarrow e'$. Consider some $x, y \in G$ such that $\varphi(y) = \varphi(x)$. Then, $e' = \varphi(x) * \varphi(y)^{-1} = \varphi(x \cdot y^{-1})$, which implies that $x \cdot y^{-1} = e$ and so $x = y$. The homomorphism φ is injective. □

Problem II. Let $\varphi : G \to H$ be a homomorphism. Here we show that any equality relation between binary structures with elements in G, holds between equal structures of the binary operation corresponding to H for all elements in $\varphi(G)$. Namely, for some finite sequences A, B of elements of G, if $g[A, \cdot] = f[B, \cdot]$, then $g[\varphi(A), *] = f[\varphi(B), *]$. Before beginning, we must define what $g[A, \cdot]$ means. For any finite sequence $A = (\pi_1, \pi_2, \pi_3, \ldots, \pi_n)$ of elements of a group G, the binary structure

$$\begin{aligned} g[A, \cdot] &= \pi_1 \cdot \pi_2 \cdot \pi_3 \cdot \ldots \cdot \pi_n \\ &= \prod_{(i \leq n, \cdot)} \pi_i \end{aligned}$$

Proof. Consider some equality relation $g[A, \cdot] = f[B, \cdot]$ in G, where $A = (a_i : i \leq n)$ and $B = (b_i : i \leq m)$ are finite sequences of elements in G. Note that these sequences can contain particular elements and/or general representations for any elements.
Since φ is a homomorphism, it follows that

$$\begin{gathered} \varphi(g[A, \cdot]) = \varphi(f[B, \cdot]) \implies \\ \varphi\left(\prod_{(i \leq n, \cdot)} a_i\right) = \prod_{(i \leq n, *)} \varphi(a_i) = \varphi\left(\prod_{(i \leq m, \cdot)} b_i\right) \\ = \prod_{(i \leq m, *)} \varphi(b_i). \end{gathered}$$

Therefore, $g[\varphi(A), *] = f[\varphi(B), *]$. Here are some issues. If A and B are sequences of general elements that represent any element in G, then $\varphi(A), \varphi(B)$ are sequences of general elements that represent any element in $\varphi(G)$. However, if one of the sequences contain specific elements in G, one must be sure that this element is mapped to a unique element in $\varphi(G)$, which can be assured if φ is injective. However, some work must be done to define how a structure with specific elements can be maintained through a homomorphism. But for now, we are sure that general structures like $a+b=b+a$ for any $a, b \in G$ are maintained through homomorphism. □

Problem 10. Let's prove the following interesting result:

Consider two sets Ω, Δ. If $|\Omega| = |\Delta|$ then $S_\Delta \cong S_\Omega$.

Proof. Assume that $|\Omega| = |\Delta|$. Then, there is a bijection $\vartheta : \Delta \to \Omega$. Consider the function $\varphi : S_\Delta \to S_\Omega$, defined by

$$\varphi(\sigma) = \vartheta \cdot \sigma_\Delta \cdot \vartheta^{-1}, \ \ \forall \sigma_\Delta \in S_\Delta.$$

We show that φ is an isomorphism.

(a) φ is well-defined.

We have to show that $\varphi(\sigma_\Delta)$ is a permutation of Ω for all σ_Δ. Note that

$$\varphi(\sigma_\Delta) = \vartheta \cdot \sigma_\Delta \cdot \vartheta^{-1} : (\Omega \to \Delta) \to (\Delta \to \Delta) \to (\Delta \to \Omega),$$

and so $\varphi(\sigma_\Delta) : \Omega \to \Omega$. Furthermore, observe that $\varphi(\sigma_\Delta)$ is an association of bijective functions, which is also bijective. Therefore, $\varphi(\sigma_\Delta)$ is a permutation of Ω. Thus, φ is well-defined.

(b) φ is a bijection.

We can show that it is a bijection if we can define a double-inverse φ^{-1}. Let $\varphi^{-1} : S_\Omega \to S_\Delta$ be defined by

$$\varphi^{-1}(\sigma_\Omega) = \vartheta^{-1} \cdot \sigma_\Omega \cdot \vartheta, \ \ \forall \sigma_\Omega \in S_\Omega.$$

With a similar argument from (a), we can show that φ^{-1} is well-defined. Consider any $\sigma_\Omega \in S_\Omega$ and $\sigma_\Delta \in S_\Delta$. Then,

$$\varphi^{-1}(\varphi(\sigma_\Delta)) = \vartheta^{-1} \cdot \left(\vartheta \cdot \sigma_\Delta \cdot \vartheta^{-1}\right) \cdot \vartheta = \sigma_\Delta.$$
$$\varphi\left(\varphi^{-1}(\sigma_\Omega)\right) = \vartheta \cdot \left(\vartheta^{-1} \cdot \sigma_\Omega \cdot \vartheta\right) \vartheta^{-1} = \sigma_\Omega.$$

Thus, $\varphi \cdot \varphi^{-1} = id_{S_\Omega}$ and $\varphi^{-1} \cdot \varphi = id_{S_\Delta}$. This implies that φ^{-1} is the double-inverse of φ and so φ is a bijection.

(c) φ is a homomorhpism.

This is easier to prove. Consider any $\sigma_\Delta, \delta_\Delta \in S_\Delta$. Then,

$$\begin{aligned}\varphi(\sigma_\Delta \cdot \delta_\Delta) &= \vartheta \cdot (\sigma_\Delta \cdot \delta_\Delta) \cdot \vartheta \\ &= \vartheta \cdot \left((\sigma_\Delta \cdot (\vartheta^{-1} \cdot \vartheta)) \cdot \delta_\Delta\right) \cdot \vartheta \\ &= \vartheta \cdot \left(((\sigma_\Delta \cdot \vartheta^{-1}) \cdot \vartheta) \cdot \delta_\Delta\right) \cdot \vartheta \\ &= \vartheta \cdot \left((\sigma_\Delta \cdot \vartheta^{-1}) \cdot (\vartheta \cdot \delta_\Delta)\right) \cdot \vartheta \\ &= (\vartheta \cdot \sigma_\Delta \cdot \vartheta^{-1}) \cdot (\vartheta \cdot \delta_\Delta \cdot \vartheta) = \varphi(\sigma_\Delta) \cdot \varphi(\delta_\Delta).\end{aligned}$$

Since both S_Δ, S_Ω use function association as binary operation, it follows that φ is a homomorphism and, by (b), φ is an isomorphism. This implies that $S_\Delta \cong S_\Omega$.

□

Problem 11. Let A and B be groups. Prove that $A \times B \cong B \times A$.

Proof. Let $\varphi : A \times B \to B \times A$ be defined by

$$\varphi((a,b)) = (b,a) \;\; \forall (a,b) \in A \times B.$$

Clearly, this is a bijection from $A \times B$ to $B \times A$. We just have to show that it is an homorphism, where the binary operation $\circ$ on a cartesian product $A \times B$ of two groups is defined by

$$(a,b) \circ (c,d) = (a \circ_A c, b \circ_B d).$$

Then,

$$\begin{aligned}\varphi((a_1,b_1) \circ (a_2,b_2)) &= \varphi((a_1 \circ_A a_2, b_1 \circ_B b_2)) \\ &= (b_1 \circ_B b_2, a_1 \circ_A a_2) = (b_1,a_1) \circ (b_2,a_2) \\ &= \varphi((a_1,b_1)) \circ \varphi((a_2,b_2)).\end{aligned}$$

Hence, $A \times B \cong B \times A$. □

Problem 12. Let G and H be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

Proof. Let $\varphi : (A \times B) \times C \to A \times (B \times C)$ be defined by

$$\varphi(((a,b),c)) = (a,(b,c)).$$

Clearly, φ is a bijection. We just have to show that it is a homomorphism using the previously defined binary operation between cartesian products of groups. Then,

$$\begin{aligned}\varphi(((a_1,b_1),c_1) \circ ((a_2,b_2),c_2))) &= \varphi(((a_1 \circ_A a_2, b_1 \circ_B b_2), c_1 \circ_C c_2)) \\ &= (a_1 \circ_A a_2, (b_1 \circ_B b_2, c_1 \circ c_2)) = (a_1,(b_1,c_1)) \circ (a_2,(b_2,c_2)) \\ &= \varphi(((a_1,b_1),c_1)) \circ \varphi(((a_2,b_2),c_2)).\end{aligned}$$

□

From the previous excercises we can conclude that cartesian product is commutative and associative with respect to the equivalence relation $\cong$ isomorphism. Hence, one can prove inductively that for any sequence of groups $(A_i : i \leq n)$,

$$A_1 \times A_2 \times A_3 \times \cdots \times A_n \cong A_n \times \cdots \times A_3 \times A_2 \times A_1$$
$$A_1 \times (A_2 \times A_3 \times \cdots \times A_n) \cong (A_1 \times A_2 \times A_3 \times \ldots A_{n-1}) \times A_n.$$

Some important aspects we proved (notebook) in 13 and 14 is that for any homomorphism $\varphi : G \to H$,

(a) $\varphi(G)$ and kernel(G) are subgroups.

(b) $G \cong \varphi(G) \iff \varphi$ is injective $\iff \{e\} \cong$ kernel(G)

Problem IV. Let $A_1, \ldots, A_n$ be a sequence of groups. Then, $A_1 \times A_2 \times \cdots \times A_n = G$ is also a group. Show that the function $\pi : G \to A_i$ for some positive integer $i \leq n$, defined by

$$\pi\left((a_1, \ldots, a_n)\right) = a_i$$

is a homomorphism and find the kernel.

Proof. We will keep using the previously binary operation defined for cartesian products of groups. Then,

$$\begin{aligned}\pi((y_1, \ldots, y_n) \circ (x_1, \ldots, x_n)) &= y_i \circ x_i \\ &= \pi((y_1, \ldots, y_n)) \circ \pi((x_1, \ldots, x_n)),\end{aligned}$$

which completes the proof. Clearly, the kernel of π is

$$\ker(\pi) = \{g \in G | \text{ ith element is } 1_{A_i}\}.$$

□

Problem 17. Let G be any group. Prove that the map from G to itself defined by $g \to g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. First, assume that G is abelian, then

$$\begin{aligned}\pi(g_1 \circ g_2) &= (g_1 \circ g_2)^{-1} \\ &= g_2^{-1} \circ g_1^{-1} \\ &= g_1^{-1} \circ g_2^{-1} = \pi(g_1) \circ \pi(g_2),\end{aligned}$$

since G is abelian.

For the converse, suppose that π is a homomorphism. Then,

$$\pi(g_1 \circ g_2) = \pi(g_1) \circ \pi(g_2),$$

which implies that $g_2^{-1} \circ g_1^{-1} = g_1^{-1} \circ g_2^{-1}$. Because, by definition, all elements of groups are inverses of some elements, it follows that G is abelian. □

Problem 18. Let G be any group. Prove that the map from G to itself defined by $g \to g^2$ is a homomorphism if and only if G is abelian.

Proof. First, assume that G is abelian, then

$$\begin{aligned}\pi(g_1 \circ g_2) &= (g_1 \circ g_2)^2 \\ &= (g_1 \circ g_2) \circ (g_1 \circ g_2) = g_1 \circ (g_2 \circ g_1) \circ g_2 \\ &= g_1 \circ (g_1 \circ g_2) \circ g_2 = g_1^2 \circ g_2^2 \\ &= \pi(g_1) \circ \pi(g_2),\end{aligned}$$

since G is abelian.

For the converse, suppose that π is a homomorphism. Then,

$$\begin{aligned}\pi(g_1 \circ g_2) = \pi(g_1) \circ \pi(g_2) \implies \\ g_1 \circ g_2 \circ g_1 \circ g_2 = g_1 \circ g_1 \circ g_2 \circ g_2\end{aligned}$$

which implies that $g_2 \circ g_1 = g_1 \circ g_2$. It follows that G is abelian. □

Problem 19. Let $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \to z^k$ is a surjective homomorphism but is not an isomorphism.

Proof. Clearly, G is the group of all complex numbers with finite order. First we show that the map $\pi : G \to G$ defined by $z \to z^k$ for some fixed integer $k > 1$ is a homomorphism. Note that

$$\begin{aligned}\pi(z_1 \cdot z_2) &= (z_1 \cdot z_2)^k \\ &= z_1^k \cdot z_2^k = \pi(z_1) \cdot \pi(z_2),\end{aligned}$$

since multiplication is commutative in $\mathbb{C}$. Furthermore, note that if $z \in G$, then $z^{1/k} \in G$. However, it is not injective.

Observe that $w = e^{2\pi i/k} \neq 1$ is equal to 1 when raised to k. Hence, $\ker(\pi) \neq \{1\}$ and so the function is not injective. In fact, there are k unity roots of the form $w, w^1, w^2, \ldots, w^{k-1}$. □

Problem 24. Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$.

Proof. Since G is finite, it follows that every element has a finite order. Thus, $|xy| < \infty$. Furthermore, by excercise 1.2.6, $|x| = |y| = 2$ and $|xy| < \infty$ imply that xy and y satisfy the same relations in G as r, s do in D_{2n}, where $n = |xy|$.
Also, note that $(xy)y^{-1} = x$, hence xy and y generate x. Thus, xy and y are generators of G. All this means that G and D_{2n} have the same group representations, namely, same generators that fulfill same relations. Then, if we define a homomorphism $\varphi : D_{2n} \to G$ by

$$\varphi(r) = xy \text{ and } \varphi(s) = y,$$

it follows that φ is an isomorphism. □