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 necessary and 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 $n \in \mathbb{Z}^+$.

For the converse, assume that the homomorhpism $\varphi : G \to H$ is not a bijection. Then, $\varphi : G \to H$ is not surjective and so there is at least one $a \in H$ with order n such that no element $x \in G$ can be mapped to it. Since every element of G with some order can be mapped to a unique element of H with the same order, it follows that the number of elements with order n in G is lower than the number of elements with order n in H.

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 $n \in \mathbb{Z}^+$. □