

CSCI 124/224

Discrete Structures II: Homomorphisms and Isomorphisms

Poorvi L. Vora

In this module, we look at functions on groups, that preserve structure.

1 Homomorphisms

Definition 1 A homomorphism *between groups*:

- G_1 with operation \diamond and
- G_2 with operation \circ

is a function f from G_1 to G_2 such that, $\forall x, y, \in G_1$,

$$f(x \diamond y) = f(x) \circ f(y)$$

Notice that $f(x \diamond y)$ need not always be equal to $f(x) \circ f(y)$. For example, suppose $G_1 = G_2 = \mathbb{R}$, the set of real numbers under addition. That is, \diamond and \circ both correspond to addition. Suppose $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$. Then $f(x \diamond y) = (x + y)^2$ and $f(x) \circ f(y) = x^2 + y^2$. In general, $f(x \diamond y) \neq f(x) \circ f(y)$ and f is not a homomorphism.

The following are example of homomorphisms.

Example 1 Let $G_1 = G_2 = \mathbb{R}$, the set of real numbers under addition. That is, \diamond and \circ both correspond to addition. Let $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = kx$ for any $k \in \mathbb{R}$. Then f is a homomorphism because:

$$\begin{aligned} f(x \diamond y) &= k(x + y) \\ &= kx + ky \\ &= f(x) + f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

Example 2 Let $G_1 = G_2 = \mathbb{R} \setminus \{0\}$, the set of non-zero real numbers under multiplication. That is, \diamond and \circ both correspond to multiplication. Let $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^n$ for any $n \in \mathbb{Z}^+$, the positive integers. Then f is a homomorphism because:

$$\begin{aligned} f(x \diamond y) &= (x.y)^n \\ &= x^n.y^n \\ &= f(x).f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

Example 3 Let $G_1 = G_2 = \mathbb{Z}_m$, the set of integers modulo m . Let \diamond and \circ both correspond to addition mod m . Let $f : G_1 \rightarrow G_2$, $f(x) = kx \text{ mod } m$ for any $k \in \mathbb{Z}_m$. Then f is a homomorphism because:

$$\begin{aligned} f(x \diamond y) &= k(x + y) \text{ mod } m \\ &= (kx \text{ mod } m) + (ky \text{ mod } m) \\ &= f(x) + f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

Example 4 Let $G_1 = G_2 = \mathbb{Z}_p^*$, the set of non-zero integers modulo p where p is prime. Recall that this is a group under multiplication modulo p . Let \diamond and \circ both correspond to multiplication modulo p . Let $f : G_1 \rightarrow G_2$, $f(x) = x^n \text{ mod } p$ for any $n \in \mathbb{Z}^+$, the positive integers. Then f is a homomorphism because:

$$\begin{aligned} f(x \diamond y) &= (x \cdot y)^n \text{ mod } p \\ &= (x^n \text{ mod } p) \cdot (y^n \text{ mod } p) \\ &= f(x) \cdot f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

In the examples we've seen so far, \diamond and \circ are the same operation. We now see an example where \diamond and \circ are different operations.

Example 5 Let G_1 be the group of integers, \mathbb{Z} , with \diamond being the addition operation. Let G_2 be the infinite group $\{\dots, \rho^{-2}, \rho^{-1}, 1, \rho^1, \rho^2, \dots\} = \{\rho^n | n \in \mathbb{Z}\}$ with \circ the multiplication operation. $f : G_1 \rightarrow G_2$, $f(n) = \rho^n$ is a homomorphism because:

$$\begin{aligned} f(x \diamond y) &= \rho^{x+y} \\ &= \rho^x \cdot \rho^y \\ &= f(x) \cdot f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

2 Properties of Homomorphisms

The following are properties of homomorphism f :

1. $f(e) = \bar{e}$ where e is the identity in G_1 , and \bar{e} that in G_2 .

This is because:

$$\begin{aligned} f(x) &= f(x \diamond e) \\ &= f(x) \circ f(e) \end{aligned}$$

Hence $f(e)$ is the identity in G_2 .

2. $f(x^{-1}) = (f(x))^{-1}$ This is to be shown for the HW.

3 Isomorphisms

An isomorphism is a homomorphism that is one-to-one. For example, the following are isomorphisms:

Example 6 Let $G_1 = G_2 = \mathbb{R}$, the set of real numbers under addition. That is, \diamond and \circ both correspond to addition. Let $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = kx$ for any $k \in \mathbb{R}$. Then f is a isomorphism because, first, it is a homomorphism as shown in example 1 above. Second, it is one-to-one. This can be proved by contradiction. Suppose f is not one-to-one. Then there are two values x_1 and x_2 , $x_1 \neq x_2$, such that $f(x_1) = f(x_2)$. That is:

$$\begin{aligned} f(x_1) &= f(x_2) \\ \Rightarrow kx_1 &= kx_2 \\ \Rightarrow k^{-1}kx_1 &= k^{-1}kx_2 \\ \Rightarrow x_1 &= x_2 \end{aligned}$$

which provides a contradiction. Hence f is one-to-one, and an isomorphism.

Example 7 The identity is an isomorphism. Consider any group G with any operation \diamond . Let $G_1 = G_2 = G$. Let f be the identity on G . That is, $f : G_1 \rightarrow G_2$, $f(x) = x$. Then f is an isomorphism because, first, it is a homomorphism:

$$\begin{aligned} f(x \diamond y) &= x \diamond y \\ &= f(x) \diamond f(y) \\ &= f(x) \circ f(y) \end{aligned}$$

Further, it is one-to-one. This can be proved by contradiction. Suppose f is not one-to-one. Then there are two values x_1 and x_2 , $x_1 \neq x_2$, such that $f(x_1) = f(x_2)$. That is:

$$\begin{aligned} f(x_1) &= f(x_2) \\ \Rightarrow x_1 &= x_2 \end{aligned}$$

which provides a contradiction. Hence f is one-to-one, and an isomorphism.