Adding a Morphism Theorem to Abstract Algebra

P. Reany

March 5, 2025

Abstract

This morphism will facilitate proving that a set with a binary operation on it and having an identity element is a group. Some improvements in the paper have been added.[1]

Introduction

First, some useful definitions.

Groupoid — a set with binary operation.

Semigroup — a set with associative binary operation.

Monoid — a semigroup with identity element.

Group — a monoid with inverses.

Say we are tasked with proving that a given set with binary operation defined on it has more structure on it, such as having inverses or that the binary operation is actually associative, or both. The usual way to accomplish this is to use the defining rules of the binary operation and brute force a demonstration of the required task.

The point of this paper is to investigate an alternative approach to proving the above tasks. The method demonstrated below may, in some cases, be simpler than the 'direct approach.'

The Group Morphism Theorem: Let $(S, *)$ be a set with binary operation *. If a group G and an onto function f from G to S can be found such that f satisfies the morphism $f(gh) = f(g) * f(h)$, then $(S, *)$ is a group. (The gist of our proof is to show that, via the morphism f, $(S, *)$ inherits the group structure of G. Specifically, we need to show that $(S, *)$ has an identity element, that all its elements have inverses, and that * is associative.)

[1] This paper was first written in its near present form about the time of July 1998. Since then some corrections have been added.

Proof:
1) Given: S has an identity element, which we'll call e', such that for all $s \in S$

$$e' * s = s * e' = s' \,. \tag{1}$$

It's easy to show that the map f must take the identity e of G to e': $f(e) = e'$. Since f is onto, every s in S can be written as $f(g)$ for some g in G. Now in G: $g = eg = ge$, so $f(g) = f(eg) = f(ge)$, implying that

$$\begin{aligned} f(g) &= f(e) * f(g) = f(g) * f(e) = f(e) * s \\ &= s * f(e) = e' * s = s * e' = s \,, \end{aligned} \tag{2}$$

where we have used our morphism property.

2) S has inverses. Since every g in G has an inverse: $e = gg^{-1} = g^{-1}g$ then $e' = f(gg^{-1}) = f(g^{-1}g)$. So

$$e' = f(g) * f(g^{-1}) = f(g^{-1}) * f(g) = s * f(g^{-1}) = f(g^{-1}) * s. \tag{3}$$

Therefore, if $s = f(g)$, $s^{-1} = f(g^{-1})$ for arbitrary s in S.

3) S's binary operator $*$ is associative. We wish to show that $s*(t*v) = (s*t)*v$ for all s, t, v in S. Once again, this structure can be pulled back onto G. Let $s = f(g)$, $t = f(h)$, and $v = f(k)$. Since $g(hk) = (gh)k$ in G, then $f(g(hk)) = f((gh)k)$, or $f(g) * f(hk) = f(gh) * f(k)$, or

$$f(g) * (f(h) * f(k)) = (f(g) * f(h)) * f(k) \,. \tag{4}$$

And from our morphism f we get $s * (t * v) = (s * t) * v$ as needed.

We have proven that to show that a groupoid $(S, *)$ is a group, it is sufficient to find a morphism from some group G onto S. But what if we didn't want to prove that much? Say we are tasked with showing that a groupoid's binary operator is associative? The groupoid may be a group or it may not be. In this case, a safer thing to try is to find a morphism from a semigroup onto the groupoid, and that will suffice. The proof of this is contained in the above proof, since to prove associativity, we did not need to invoke either identity element or inverses.

Applications:

A few applications of this theorem should help to demonstrate the power of this theorem in certain circumstances. We begin with a typical problem in first-year abstract algebra.

Problem 1: Let $\mathbb{R}\backslash\{0\}$ be the group of real numbers under multiplication. Let $S = \mathbb{R}\backslash\{1\}$ be a set with binary operation $*$ given by,

$$a * b = a + b - ab \tag{5}$$

for all a, b in S. Show that $(S, *)$ is a group.

Solution: Note: G has identity element 1. Now, we need a function f that takes 1 to the identity element of S. Does S even have an identity element? It does, namely 0. Proof: Let $a = 0$ in (5)

$$0 * b = 0 + b - 0b = b \quad \text{and} \quad b * 0 = b + 0 - b0 = b\,. \tag{6}$$

So, 0 is the identity element of S. Now we need a function f that takes 1 in G to 0 in S. Let the ansatz function be given by

$$f(g) = 1 - g\,, \tag{7}$$

which clearly satisfies $f(1) = 0$. Furthermore, the function is clearly onto, since for every a in S, we can find an element of G, namely, $1 - a$, that maps to it:

$$f(1 - a) = 1 - (1 - a) = a\,. \tag{8}$$

Since a in S is never 1, $1 - a$ in G is never zero. But is f a morphism? To show that, we need to show that for all $g, h \in G$, $f(gh) = f(g) * f(h)$. So,

$$\begin{aligned} f(gh) &= 1 - gh \\ &= 2 - (g + h) - [1 - (g + h) + gh] \quad \text{(by Vir. Empl.)} \\ &= (1 - g) + (1 - h) - (1 - g)(1 - h) \\ &= (1 - g) * (1 - h) \\ &= f(g) * f(h)\,. \end{aligned} \tag{9}$$

Thus f is a morphism and $(S, *)$ is indeed a group. But how did I know how to make that tricky virtual emplacement in line 2? Easy. I started on the last line and 'worked backwards'.

For the purpose of finding Equation (7), we went to the trouble of finding the identity element of S, but if we had had this function first, we could have found this identity of S by using the fact that the identity of G gets mapped to the identity of S by $f(1) = e' \in S$:

$$e' = f(1) = 1 - 1 = 0\,. \tag{10}$$

Lastly, does S have inverses? Yes, and we can show this the direct way by solving for the inverse of an arbitrary element a of S by finding element b satisfying

$$a * b = a + b - ab = 0\,, \tag{11}$$

yielding

$$a^{-1} = b = \frac{a}{a - 1}\,, \tag{12}$$

and since $a * b = b * a$ for all elements in S, the above equation does provide the true inverse.

Since f is one-to-one, we can pull back the calculation of finding the inverse of $a \in S$ to finding it in G by the following trick:

$$a * b = 0\,, \tag{13}$$

produces, with the help of (8),

$$f(1-a) * f(1-b) = f(1)\,, \tag{14}$$

which, on applying the morphism rule (7), yields

$$f((1-a)(1-b)) = f(1)\,, \tag{15}$$

which yields

$$(1-a)(1-b) = 1\,, \tag{16}$$

which is algebraically the same as (11).

Comments: Of course, this 'morphism technique' requires some skill in choosing a suitable group G and a suitable onto function f. The clear advantage of this morphism version of a proof is that we avoided the direct and sometimes tedious calculations involved in showing that $*$ is associative.

Problem 2: Our second use of the Morphism Theorem is to show that addition on the integers mod m under addition mod m is associative. In other words, is the binary operator $\oplus$ on $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ associative? Note that for all a, b in $(\mathbb{Z}/m\mathbb{Z}, \oplus)$, the binary operator $\oplus$ is defined by

$$a \oplus b \equiv a + b \bmod m \tag{17}$$

We define the function f from the group $(\mathbb{Z}, +)$ onto $(\mathbb{Z}/m\mathbb{Z}, \oplus)$, given by

$$f(x) = x \bmod m \tag{18}$$

for all x in $\mathbb{Z}$. (We choose $\mathbb{Z}$ since its addition $+$ is associative.)

Question: Is f onto? The elements of $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ are cosets with canonical representatives $S = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. We simply map by f the integers from 0 to $m-1$ onto their counterparts in S. That is, for all $a \in [0, 1, \ldots, m-1]$ $f(a) = \overline{a}$.

Is f a morphism? We need to show that $f(x+y) = f(x) \oplus f(y)$. Let x, y be arbitrary integers, then

$$\begin{aligned} f(x+y) &= x + y \bmod m \\ &= (x \bmod m) + (y \bmod m) \bmod m \\ &= (x \bmod m) \oplus (y \bmod m) \\ &= f(x) \oplus f(y)\,, \end{aligned} \tag{19}$$

where the third line followed from (17). So $f(x+y) = f(x) \oplus f(y)$, making f a morphism, and making $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ a group, and thus associativity follows.

Problem 3: Our third use of our Morphism Theorem is to show that the (projection) map of a group G onto the right cosets of some appropriate subgroup H in G is a morphism under appropriate definition of the binary operation on these cosets, and thereby that the set of cosets forms a group of their own. The

first time through this we will not presume a knowledge of *normal* subgroups, allowing us the opportunity to "invent" this concept as the opportunity arises. Remember that as yet we do not assume a well-defined binary operation on these right cosets, and we will invent that definition along the way.

Let the set of right cosets of H in G be given by $C = \{Hg \mid g \in G\}$.[2] Let $f : G \to C$ given by

$$f(g) = Hg\,. \tag{20}$$

Clearly, f is onto, but can we define a binary operation $*$ on the right cosets in such a way as to make f a morphism? Let $*$ be our candidate binary operator on the right cosets in C. So, we wish to find the condition on $*$ such that the following holds:

$$f(g) * f(g') = Hg * Hg' = Hgg' = f(gg')\,. \tag{21}$$

In our effort to define $*$, we need to establish how it relates to the binary operation on the elements of C. One obvious and natural way to do this is by the following definition:

$$Hg * Hg \equiv HgHg' = H(gH)g'\,, \tag{22}$$

where associativity is given by the fact that G is a group, and that all the products are of elements of G.

Thus, to make $(C, *)$ into a group, it is sufficient have H satisfy the property

$$H(gH)g' = H(Hg)g'\,. \tag{23}$$

In other words, we need H to be special in that the left coset of H by g is equal to the right coset of H by g (for all $g \in G$).[3] Such a subset is said to be *normal* in G.

Next, we need

$$H(Hg)g' = (HH)gg' = Hgg'\,, \tag{24}$$

where $HH = H$ because H is a subgroup of G and thus is closed under multiplication by any element from H. That is, given any element $h \in H$, h acting on H maps H back onto itself. So, think of HH as the set of all elements that can be formed by the union of elements of H by left (or right) multiplication by each element of H. When we remove all the duplications out of this set, the result is just H.

Thus, $*$ is a (closed) binary operation on C because Hgg' is an element of C since gg' is an element of G. The group $(C, *)$ is called the *quotient group* of G by its (normal) subgroup H, and it usually denoted as G/H. By the way, the identity element of this quotient group is the coset H.

Notation: The right cosets of H in G is sometimes denoted as $[G, H]$. This set of coset exists even when H is not normal, although in that case $[G, H]$ does not form a quotient group.

[2] For a given $g \in G$, the right coset of g on H is $\{hg | h \in H\}$.

[3] Not all subgroups have this property.

Alternatively, one could define the concept of the normal subgroup, making the quotient group theorem an immediate consequence of the Morphism Theorem.

Theorem on Quotient Groups: Let G be a group and H be a normal subgroup of G. Then the set of right (left) cosets of H in G forms a group.

Proof: Let f be a function from G onto the right cosets of H in G, given by $f(g) = Hg$. Then

$$f(g) * f(g') = Hg * Hg' = HgHg' = Hgg' = f(gg') \,. \tag{25}$$

Thus, by the Morphism Theorem the cosets of H in G form a quotient group.

ACKNOWLEDGMENTS: I thank John Vahey for showing me the "Morphism Theorem" in 1987.