1-17-2018

Group Homomorphisms

Here are the operation tables for two groups of order 4:

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

There is an obvious sense in which these two groups are "the same": You can get the second table from the first by replacing 0 with 1, 1 with a, and 2 with a^2.

When are two groups the same?

You might think of saying that two groups are the same if you can get one group's table from the other by substitution, as above. However, there are problems with this. In the first place, it might be very difficult to check — imagine having to write down a multiplication table for a group of order 256! In the second place, it's not clear what a "multiplication table" is if a group is infinite.

One way to implement a substitution is to use a function. In a sense, a function is a thing which "substitutes" its output for its input. I'll define what it means for two groups to be "the same" by using certain kinds of functions between groups. These functions are called **group homomorphisms**; a special kind of homomorphism, called an **isomorphism**, will be used to define "sameness" for groups.

Definition. Let G and H be groups. A **homomorphism** from G to H is a function $f : G \to H$ such that

$$f(x \cdot y) = f(x) \cdot f(y) \quad \text{for all} \quad x, y \in G.$$

Group homomorphisms are often referred to as **group maps** for short.

Remarks. 1. In the definition above, I've assumed multiplicative notation for the operations in both G and H. If the operation in one or both is something else, you must adjust the definition accordingly. For instance:

Operation in G	**Operation in H**	**Group map definition**
$+$	$+$	$f(x+y) = f(x) + f(y)$
$+$	$\cdot$	$f(x+y) = f(x) \cdot f(y)$
$\cdot$	$+$	$f(x \cdot y) = f(x) + f(y)$
$\diamond$	$\star$	$f(x \diamond y) = f(x) \star f(y)$

2. You have seen patterns like this before; for example, "The derivative of a sum is the sum of the derivatives".

Lemma. Let G be a group and let H be a subgroup.

(a) The identity map $\mathrm{id} : G \to G$ defined by $\mathrm{id}(x) = x$ is a group map.

(b) The inclusion map $i : H \to G$ defined by $\subset (x) = x$ is a group map.

Proof. I'll prove (a); the proof of (b) is the same. Let $x, y \in G$. Then

$$\mathrm{id}(x \cdot y) = x \cdot y = \mathrm{id}(x) \cdot \mathrm{id}(y).$$

Hence, id is a group map. $\square$

Example. (**Constant maps are usually not group maps**) For the group $\mathbb{Z}$ under addition, define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(n) = 3 \quad \text{for all} \quad n \in \mathbb{Z}.$$

Show that f is not a group map.

$$f(1+1) = f(2) = 3, \quad \text{but} \quad f(1) + f(1) = 3 + 3 = 6. \quad \square$$

Example. (**Logs and exponentials**) (a) Prove that the exponential function $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ given by $\exp(x) = e^x$ is a group map.

(b) Prove that the natural log function $\ln : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ is a group map.

(a) Let $x, y \in \mathbb{R}$. Then by properties of exponentials,

$$\exp(x+y) = e^{x+y} = e^x \cdot e^y = \exp(y) \cdot \exp(y). \quad \square$$

(b) Let $x, y \in \mathbb{R}^+$. Then by properties of logarithms,

$$\ln(x \cdot y) = \ln x + \ln y. \quad \square$$

Example. (**Checking whether a function is a group map**)

(a) Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = 5x.$$

Prove or disprove: f is a group map.

(b) Define $g : \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x^2.$$

Prove or disprove: f is a group map.

(a) f is a group map: If $x, y \in \mathbb{Z}$, then

$$f(x+y) = 5(x+y) = 5x + 5y = f(x) + f(y). \quad \square$$

(b)

$$g(2+3) = g(5) = 5^2 = 25, \quad \text{but} \quad g(2) + g(3) = 2^2 + 3^2 = 4 + 9 = 13.$$

Since $g(2+3) \neq g(2) + g(3)$, g is not a homomorphism. $\square$

Lemma. Let V and W be vector spaces over a field F, considered as groups under vector addition. Let $T : V \to W$ be a linear transformation. Then T is a group map.

Proof. This follows immediately from one of the axioms for a linear transformation: If $x, y \in V$, then

$$T(x+y) = T(x) + T(y). \quad \square$$

Example. $\mathbb{R}^3$ and $\mathbb{R}^2$ are groups under vector addition. Define $T : \mathbb{R}^3 \to \mathbb{R}^2$ by

$$T(x, y, z) = (2x + 8y - z, x + 5y - 3z).$$

Prove that T is a group map.

Write T as a matrix multiplication:

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 8 & -1 \\ 1 & 5 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

From linear algebra, this defines a linear transformation. Hence, T is a group map by the previous lemma. $\square$

Example. (**A group map on a matrix group**) Let $M(2, \mathbb{R})$ be the group of 2×2 reals matrices under matrix addition. Let $\operatorname{tr} : M(2, \mathbb{R}) \to \mathbb{R}$ denote the **trace map**:

$$\operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d.$$

Show that tr is a group homomorphism.

Now

$$\operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = \operatorname{tr}\left(\begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix}\right) = (a + a') + (d + d'),$$

$$\operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \operatorname{tr}\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = (a + d) + (a' + d').$$

Thus,

$$\operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = \operatorname{tr}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \operatorname{tr}\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right).$$

Therefore, tr is a homomorphism. $\square$

Lemma. Let $f : G \to H$ be a group homomorphism. Then:

(a) $f(1_G) = 1_H$, where 1_G is the identity in G and 1_H is the identity in H.

(b) $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$.

Proof. (a)

$$f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G).$$

If I cancel $f(1_G)$ off both sides, I obtain $f(1_G) = 1_H$.

(b) Let $x \in G$.

$$f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1_G) = 1_H$$

$$f(x^{-1}) \cdot f(x) = f(x^{-1} \cdot x) = f(1_G) = 1_H$$

This shows that $f(x^{-1})$ is the inverse of $f(x)$, i.e. $f(x)^{-1} = f(x^{-1})$. $\square$

Warning. The properties in the last lemma are not part of the *definition* of a homomorphism. To show that f is a homomorphism, all you need to show is that $f(a \cdot b) = f(a) \cdot f(b)$ for all a and b. The properties in the lemma are automatically true of any homomorphism.

On the other hand, if you want to show a function is *not* a homomorphism, do a quick check: Does it send the identity to the identity? If not, then the lemma shows it's *not* a homomorphism. $\square$

Example. (**Group maps must take the identity to the identity**) Let $\mathbb{Z}$ denote the group of integers with addition. Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = x + 1.$$

Prove that f is not a group map.

Note that $f(0) = 1$. Since the identity $0 \in \mathbb{Z}$ is not mapped to the identity $0 \in \mathbb{Z}$, f cannot be a group homomorphism. $\square$

Warning: If a function takes the identity to the identity, it may or may not be a group map. Consider $g : \mathbb{Z} \to \mathbb{Z}$ given by

$$g(x) = \sin x.$$

$g(0) = \sin 0 = 0$, but this doesn't mean that g is a homomorphism. In fact,

$$g\left(\frac{\pi}{2} + \frac{\pi}{2}\right) = g(\pi) = \sin \pi = 0, \quad \text{but} \quad g\left(\frac{\pi}{2}\right) + g\left(\frac{\pi}{2}\right) = \sin \frac{\pi}{2} + \sin \frac{\pi}{2} = 1 + 1 = 2.$$

The point is that simple-looking functions you may have seen in other math classes need not be homomorphisms. When in doubt, check the definition. $\square$

There are several important subsets associated to a group homomorphism $f : G \to H$.

Definition. Let $f : G \to H$ be a group homomorphism.

(a) The **kernel** of f is

$$\ker f = \{g \in G \mid f(g) = 1\}.$$

(b) The **image** of f is (as usual)

$$\operatorname{im} f = \{f(g) \mid g \in G\}.$$

(c) Let $H' < H$. The **inverse image** of H' is (as usual)

$$f^{-1}(H') = \{g \in G \mid f(g) \in H'\}.$$

Warning. The notation $f^{-1}(H')$ *does not imply* that the **inverse** of f exists. $f^{-1}(H')$ is simply the set of inputs which f maps into H'; this *is* f^{-1} applied to the set H' if there is a f^{-1} (but there need not be). $\square$

Lemma. Let $f : G \to H$ be a group map.

(a) $\ker f$ is a subgroup of G.

(b) $\operatorname{im} f$ is a subgroup of H.

(c) If H' is a subgroup of H, then $f^{-1}(H')$ is a subgroup of G.

Proof. (a) First,

$$f(1) = 1, \quad \text{so} \quad 1 \in \ker f.$$

Suppose $x, y \in \ker f$. Then

$$f(xy) = f(x)f(y) = 1 \cdot 1 = 1.$$

Hence, $xy \in \ker f$.

Finally, suppose $x \in \ker f$. Then

$$f(x^{-1}) = f(x)^{-1} = 1^{-1} = 1.$$

Hence, $x^{-1} \in \ker f$. Therefore, $\ker f$ is a subgroup of G.

(b) $1 \in \operatorname{im} f$ since $f(1) = 1$.

Suppose $f(x), f(y) \in \operatorname{im} f$. Then

$$f(x)f(y) = f(xy) \in \operatorname{im} f.$$

Finally, suppose $f(x) \in \operatorname{im} f$. Then

$$f(x)^{-1} = f(x^{-1}) \in \operatorname{im} f.$$

Therefore, $\operatorname{im} f$ is a subgroup of H. □

(c) Let H' be a subgroup of H. I want to show that f^{-1} is a subgroup of G. Reminder: The criterion for membership in $f^{-1}(H')$ is that f takes the element into H'.

Since $1 \in H'$ and $f(1) = 1$, it follows that $1 \in f^{-1}(H')$.

Suppose $x, y \in f^{-1}(H')$. This means that $f(x)$ and $f(y)$ are in H'. Since H' is a subgroup, $f(x)f(y)$ is in H' as well. But

$$f(x)f(y) = f(xy).$$

Therefore, $f(xy)$ is in H', which means that $xy \in f^{-1}(H')$.

Finally, suppose $x \in f^{-1}(H')$, so $f(x) \in H'$. Since H' is a subgroup, $f(x)^{-1} \in H'$. But $f(x)^{-1} = f(x^{-1})$, so $f(x^{-1}) \in H'$. This means that $x^{-1} \in H'$.

Hence, $f^{-1}(H')$ is a subgroup of G. □

Example. (**Finding the kernel and image**) (a) Let

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Show that S^1 is a group under multiplication of complex numbers.

(b) Define $f : \mathbb{R} \to S^1$ by

$$f(t) = e^{2\pi i t}.$$

Show that f is a group map, and find its kernel and image.

(a) Each element $z \in S^1$ can be uniquely written in the form

$$z = e^{2\pi i t} = \cos(2\pi t) + i \sin(2\pi t) \quad \text{for} \quad 0 \le t < 1.$$

Note that

$$e^{2\pi i s} e^{2\pi i t} = e^{2\pi i (s+t)}.$$

This shows that multiplication is closed (hence a binary operation) on S.

Complex number multiplication is associative. The identity element is 1; the inverse of $e^{2\pi i t}$ is $e^{-2\pi i t}$. □

(b) To see that f is a homomorphism, note that

$$f(s+t) = e^{2\pi i (s+t)} = e^{2\pi i s} e^{2\pi i t} = f(s)f(t).$$

From the representation of elements of S as $e^{2\pi it}$, I have $\operatorname{im} f = S^1$.
The kernel of f is

$$\ker f = \{t \in \mathbb{R} \mid e^{2\pi it} = 1\}.$$

Using $e^{2\pi it} = \cos(2\pi t) + i\sin(2\pi t)$, you can see that $\ker f = \mathbb{Z}$. $\square$

Example. (**Kernel, image, and inverse image**) $f : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ is defined by

$$f(x) = 3x \pmod{12}.$$

Take for granted that f is a group map. Find $\ker f$, $\operatorname{im} f$, and $f^{-1}(H)$, where H is the subgroup $\{0, 6\}$ of $\mathbb{Z}_{12}$.

The kernel consists of elements of $\mathbb{Z}_8$ which f takes to 0. Since 0 "is" 12 in $\mathbb{Z}_{12}$, and since f multiplies inputs by 3, I'll get multiples of 12 out if I feed multiples of 4 in:

$$f(0) = 0, \quad f(4) = 0.$$

Hence, $\ker f = \{0, 4\}$.

$\operatorname{im} f$ consists of the set of outputs of f. Since f multiplies its inputs by 3, the outputs are the multiples of 3:

$$\operatorname{im} f = \{0, 3, 6, 9\}.$$

Finally, $f^{-1}(\{0, 6\})$ consists of elements of $\mathbb{Z}_8$ which are mapped by f to either 0 or 6. So you need to find the elements in $\{0, 1, 2, 3, 4, 5, 6, 7\}$ which give 0 or 6 when multiplied by 3. Obviously, an "odd" input will give an "odd" output, and I already know 0 and 4 are mapped by f to 0, so I just try 2 and 6:

$$f(2) = 6, \quad f(6) = 6.$$

Hence, $f^{-1}(\{0, 6\}) = \{0, 2, 4, 6\}$. $\square$

Definition. Let G and H be groups. An **isomorphism** from G to H is a bijective homomorphism $f : G \to H$. If there is an isomorphism $f : G \to H$, G and H are **isomorphic**; notation: $G \approx H$.

Remarks. 1. To say that two groups are isomorphic is to say that they are the same *as groups*. The elements of the two groups and the group operations may be different, but the two groups have the same structure. This means that if one has a certain group-theoretic property, the other will as well.

What is a *group-theoretic property*? Well, it's a bit circular: a group-theoretic property is a property preserved by isomorphism. For this to be a useful concept, I'll have to provide specific examples of properties that you can check.

2. Some older books define an isomorphism from G to H to be an injective homomorphism $f : G \to H$. That is, f need not map G onto H. One then says G and H are isomorphic if there is an isomorphism from G *onto* H. Unfortunately, one then has the odd situation that there may be an isomorphism from G to H, yet G and H may not be isomorphic! I'll always use the word *isomorphism* to mean a bijective map.

Here is an easy way to tell that a group map is an isomorphism.

Lemma. A group map $f : G \to H$ is an isomorphism if and only if it is invertible. In this case, f^{-1} is also a homomorphism, hence an isomorphism.

Proof. The first statement is trivial, since a map of sets is bijective if and only if it has an inverse.

Now suppose that $f : G \to H$ is an isomorphism. I must show the inverse $f^{-1} : H \to G$ is a homomorphism. Let $x, y \in H$. I need to show that

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y).$$

Since $f: G \to H$ is onto, there exist $x, y \in G$ such that $f(x) = x$ and $f(y) = y$. Then

$$f^{-1}(xy) = f^{-1}\left(f(x)f(y)\right) = f^{-1}\left(f(xy)\right) = xy = f^{-1}(x)f^{-1}(y).$$

Therefore, f^{-1} is a homomorphism.
Since f^{-1} is invertible — its inverse is f — it is an isomorphism by the first part of the lemma. $\square$

Example. (**A group isomorphism**) Show that the exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ given by $\exp(x) = e^x$ is a group isomorphism.

I showed earlier that exp and the natural log function $\ln : \mathbb{R}^+ \to \mathbb{R}$ are group maps. They're also inverses:

$$\ln(\exp(x)) = \ln e^x = x \quad \text{for} \quad x \in \mathbb{R}.$$
$$\exp(\ln x) = e^{\ln x} = x \quad \text{for} \quad x \in \mathbb{R}^+.$$

By the lemma, exp is an isomorphism (as is ln). The groups $(\mathbb{R}, +)$ and $\mathbb{R}^+$ are isomorphic. $\square$

Example. (**A group isomorphism on the integers mod 2**) Consider the set $G = \{-1, 1\}$. Make G into a group using multiplication as the group operation. Show that G is isomorphic to $\mathbb{Z}_2$.

Define a map $f : \mathbb{Z}_2 \to G$ by

$$f(0) = 1, \quad f(1) = -1.$$

Clearly, f is invertible: Its inverse is

$$f^{-1}(1) = 0, \quad f^{-1}(-1) = 1.$$

I'll show f is a homomorphism, hence an isomorphism, by simply checking cases:

a	b	$f(a+b)$	$f(a)f(b)$
0	0	1	$1 \cdot 1 = 1$
0	1	-1	$1 \cdot (-1) = -1$
1	0	-1	$(-1) \cdot 1 = -1$
1	1	1	$(-1) \cdot (-1) = 1$

The brute force approach above can be used to construct an isomorphism from $\mathbb{Z}_2$ to any group of order 2. *There is only one group of order* 2*, up to isomorphism.* $\square$

Here are some examples of "group-theoretic properties". Thus, if two groups are isomorphic and one of the groups has such a property, the other must as well. On the other hand, if one of two groups has one of these properties but the other group does not, then the two groups cannot be isomorphic.

Proposition. Suppose G and H are isomorphic groups. If G is abelian, so is H.

Proof. Let $x, y \in H$. I must show that $xy = yx$. Since f is surjective, there exist $x', y' \in G$ such that $f(x') = x$ and $f(y') = y$. Then

$$\begin{array}{rcll} xy & = & f(x')f(y') & \\ & = & f(x'y') & (f \text{ is a group map}) \\ & = & f(y'x') & (G \text{ is abelian}) \\ & = & f(y')f(x') & (f \text{ is a group map}) \\ & = & yx & \end{array}$$

Therefore, H is abelian. □

Example. (**Non-isomorphic groups**) D_3 is the group of symmetries of an equilateral triangle. D_3 and $\mathbb{Z}_6$ are both groups of order 6. Why aren't they isomorphic?

$\mathbb{Z}_6$ is abelian, while S_3 is nonabelian. Therefore, S_3 and $\mathbb{Z}_6$ are not isomorphic. □

Proposition. Suppose G and H are isomorphic groups. If G is finite, so is H. If G is infinite, so is H.
In other words, isomorphic groups have the same cardinality.

Proof. Since G and H are isomorphic, there is a bijective (group map) $f : G \to H$. Since f is bijective, $|G| = |H|$ (since that's what it means for two sets to have the same cardinality). □

Example. (**Groups of different cardinalities aren't isomorphic**) Why can't $\mathbb{Z}$ and $\mathbb{R}$ be isomorphic?

Both groups are infinite, but the integers are countable, while the reals are uncountable. Since they don't have the same cardinality, they can't be isomorphic. □

Proposition. Suppose G and H are isomorphic groups. If G has a subgroup K of order 42, so does H.

Proof. If $K < G$ and $|K| = 42$, then $f(K) < H$ and (since f maps K bijectively onto $f(K)$) $|f(K)| = 42$. □

Obviously, there's nothing special about "42". If G has a subgroup of order 117, so does H. If G has a subgroup of order 91, so does H. And so on. This proposition is not very useful as is, and is just here to show you a property shared by isomorphic groups.

There are clearly infinitely many properties that will be shared by isomorphic groups. However, the earlier examples show that some properties are *not* shared by isomorphic groups. For example, the elements of one group may be letters, while the elements of the other are numbers. "Having the same kind of elements" is *not* a group-theoretic property. Likewise, the operation in one group may be addition of numbers, while the operation in the other could be composition of functions. "Having the same kind of binary operation" is *not* a group-theoretic property.

Example. (**Showing groups aren't isomorphic by considering orders of elements**)

(a) Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are *not* isomorphic.

(b) Show that $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$ are not isomorphic.

(a) Both groups have 4 elements; however, every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 1 or 2. If $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, then

$$2 \cdot (x, y) = (2x, 2y) = (0, 0).$$

Therefore, the order of (x, y) divides 2, and the only positive divisors of 2 are 1 and 2.

On the other hand, $\mathbb{Z}_4$ has two elements of order 4 (namely 1 and 3). Having different numbers of elements of a given order is a group property. Since these groups differ in this respect, they aren't isomorphic.

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$ are all abelian groups of order 8. However, their elements have different orders.

Every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 1 or 2. For if $(x, y, z) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, then

$$2 \cdot (x, y, z) = (2x, 2y, 2z) = (0, 0, 0).$$

Therefore, the order of (x, y, z) divides 2, and the only positive divisors of 2 are 1 and 2.

Every element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ has order 1, 2, or 4. For if $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$4 \cdot (x, y) = (4x, 4y) = (0, 0).$$

Therefore, the order of (x, y) divides 4, and the only positive divisors of 2 are 1, 2, and 4. Note that $(0, 1)$ is an element of order 4. This means that $\mathbb{Z}_2 \times \mathbb{Z}_4$ can't be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, since the latter has no elements of order 4.

$\mathbb{Z}_8$ has elements of order 8. (1 has order 8, for example.) Therefore, it can't be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_2 \times \mathbb{Z}_4$, since these two groups have no elements of order 8.

Therefore, the three groups aren't isomorphic. $\square$
