11-1-1993

Isomorphisms.

Definition. Let G and H be groups. An **isomorphism** from G to H is a bijective homomorphism $\phi : G \to H$. If there is an isomorphism $\phi : G \to H$, 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.

2. Older works define an isomorphism from G to H to be an injective homomorphism $\phi : G \to H$. That is, ϕ 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 $\phi : G \to H$ is an isomorphism if and only if it is invertible. In this case, ϕ^{-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 $\phi : G \to H$ is an isomorphism. I must show the inverse $\phi^{-1} : H \to G$ is a homomorphism. Let $h_1, h_2 \in H$. I need to show that

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2).$$

Since $\phi : G \to H$ is onto, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$\phi^{-1}(h_1 h_2) = \phi^{-1}\left(\phi(g_1)\phi(g_2)\right) = \phi^{-1}\left(\phi(g_1 g_2)\right) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2).$$

Therefore, ϕ^{-1} is a homomorphism.

Since ϕ^{-1} is invertible — its inverse is ϕ — it is an isomorphism by the first part of the lemma. □

Examples.

1. Consider the exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ given by $\exp(x) = e^x$. By an earlier example, exp is a homomorphism from the reals under addition to the positive reals under multiplication.

The natural logarithm $\ln : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ inverts exp:

$$\ln e^x = x, \quad e^{\ln y} = y \text{ for } x \in \mathbb{R}, y \in \mathbb{R}^+.$$

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

2. Consider the set $G = \{-1, 1\}$. Make G into a group using multiplication as the group operation.

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

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

Clearly, ϕ is invertible: Its inverse is

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

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

a	b	$\phi(a+b)$	$\phi(a)\phi(b)$
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.* $\square$

What does it mean to say that *isomorphic groups have the same group-theoretic properties*?. Here are some examples.

Examples. Suppose G and H are groups and $\phi : G \to H$ is an isomorphism.

1. If G is abelian, so is H.

Proof. Let $h_1, h_2 \in H$. I must show that $h_1 h_2 = h_2 h_1$. Since ϕ is onto, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1.$$

Therefore, H is abelian. $\square$

2. If G is finite, so is H. If G is infinite, so is H. (More specifically, isomorphic groups have the saem cardinality.

Proof. This is trivial, since ϕ puts G and H in 1-1 correspondence. $\square$

Example. $\mathbb{Z}$ and $\mathbb{R}$ cannot be isomorphic, since the integers are countable, while the reals are uncountable. $\square$

3. If G has a subgroup K of order 42, so does H.

Proof. If $K < G$ and $|K| = 42$, then $\phi(K) < H$ and (since ϕ maps K bijectively onto $\phi(K)$) $|\phi(K)| = 42$. $\square$

It should be clear that this can be continued *ad infinitum*. Any property of G *considered as a group* will be mirrored by ϕ in H.

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.

The next theorem is an enormously powerful result that you can use to construct isomorphisms. The idea is simple, and uses the universal property of the quotient. First, I'll prove a very useful lemma.

Lemma. Let $\phi : G \to H$ be a group map. ϕ is injective if and only if $\ker\ \phi = \{1\}$.

Proof. ($\Rightarrow$) Suppose ϕ is injective. Since $\phi(1) = 1$, $\{1\} \subset \ker\ \phi$. Conversely, let $g \in \ker\ \phi$, so $\phi(g) = 1$. Then $\phi(g) = 1 = \phi(1)$, so by injectivity $g = 1$. Therefore, $\ker\ \phi \subset \{1\}$, so $\ker\ \phi = \{1\}$.

($\Leftarrow$) Suppose $\ker\ \phi = \{1\}$. I want to show that ϕ is injective. Suppose $\phi(a) = \phi(b)$. I want to show that $a = b$.

$$\phi(a) = \phi(b), \quad \phi(a)\phi(b)^{-1} = 1, \quad \phi(a)\phi(b^{-1}) = 1, \quad \phi(ab^{-1}) = 1.$$

Hence, $ab^{-1} \in \ker\ \phi = \{1\}$, so $ab^{-1} = 1$, and $a = b$. Therefore, ϕ is injective. $\square$

Theorem. (The First Isomorphism Theorem) Let $\phi : G \to H$ be a group map, and let $\pi : G \to G/\ker\ \phi$ be the quotient map. There is an isomorphism $\tilde{\phi} : G/\ker\ \phi \to \operatorname{im}\ \phi$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "\phi"] & \\ G/\ker\ \phi \arrow[r, "\tilde{\phi}"'] & \operatorname{im}\ \phi \end{tikzcd}$$

Proof. Since ϕ maps G onto im ϕ and ker $\phi \subset$ ker ϕ, the universal property of the quotient yields a map $\tilde{\phi} : G/\ker\ \phi \rightarrow \text{im}\ \phi$ such that the diagram above commutes. Since ϕ is onto, so is $\tilde{\phi}$; in fact, if $\phi(g) \in \text{im}\ \phi$, by commutativity $\tilde{\phi}(\pi(g)) = \phi(g)$.

It remains to show that $\tilde{\phi}$ is injective.

By the previous lemma, it suffices to show that ker $\tilde{\phi} = \{1\}$. Since $\tilde{\phi}$ maps out of $G/\ker\ \phi$, the "1" here is the identity element of the group $G/\ker\ \phi$, which is the subgroup ker ϕ. So I need to show that ker $\tilde{\phi} = \{\ker\ \phi\}$.

However, this follows immediately from commutativity of the diagram. For $g \ker\ \phi \in \ker\ \tilde{\phi}$ if and only if $\tilde{\phi}(g \ker\ \phi) = 1$. This is equivalent to $\tilde{\phi}(\pi(g)) = 1$, or $\phi(g) = 1$, or $g \in \ker\ \phi$ — i.e. ker $\tilde{\phi} = \{\ker\ \phi\}$. □

The results that follow are really examples of homomorphisms and isomorphisms, though some of the results are stated as theorems.

The content of the next two results is roughly that a homomorphism out of a cyclic group is determined by where you send a generator.

Lemma. Let $G = \langle g \rangle$ be infinite cyclic, let H be an arbitrary group, and let $h \in H$. There is a unique homomorphism $\phi : G \rightarrow H$ such that

$$\phi(g) = h.$$

Proof. To show that ϕ is unique, if it exists, observe that every element of G has the form g^k for some $k \in \mathbb{Z}$. Then

$$\phi(g^k) = \phi(g)^k = h^k.$$

That is, if I know $\phi(g) = h$ then I know the value of ϕ at every element of G.

To show that such a map ϕ exists, *define*

$$\phi(g^k) = h^k, \qquad k \in \mathbb{Z}.$$

(Note that since G is *infinite cyclic*, every element can be *uniquely* written as g^k for $k \in \mathbb{Z}$. Hence, the map is well defined.)

Then

$$\phi(g^i g^j) = \phi(g^{i+j}) = h^{i+j} = h^i h^j = \phi(g^i) \cdot \phi(g^j).$$

This shows that ϕ is a homomorphism. □

Now I will prove a similar result for finite cyclic groups. First, observe that if $\phi : G \rightarrow H$ is a homomorphism and $g \in G$ has order n, then

$$1 = \phi(1) = \phi(g^n) = \phi(g)^n.$$

It follows that the order of $\phi(g)$ must divide n, the order of g.

Going the other way, if I want to define a map by sending $g \in G$ somewhere, I must send it to an element which is killed by n.

Lemma. Let $G = \langle g \rangle$ be cyclic of order n, let H be a group, and let $h \in H$ satisfy $h^n = 1$. Then there is a unique homomorphism $\phi : G \rightarrow H$ such that

$$\phi(g) = h.$$

Proof. Everything works exactly as in the previous proof, except that I must verify that the map is well defined. I want to set

$$\phi(g^k) = h^k.$$

However, because g has order n, it's possible that $g^i = g^j$ for $i \neq j$. In this situation, I must show $h^i = h^j$. Suppose, then, that $g^i = g^j$. Then $g^{i-j} = 1$, so $n \mid i - j$. Write $i - j = dn$, where $d \in \mathbb{Z}$. Then

$$\phi(g^i) = \phi(g^{j+dn}) = h^{j+dn} = h^j h^{dn} = h^j \cdot 1 = h^j = \phi(g^j).$$

Thus, the map is well defined. Existence and uniqueness are proved exactly as in the preceding lemma. $\square$

Example. If I want to define a map from $\mathbb{Z}_6$ to $\mathbb{Z}_4$, I can send the generator $1 \in \mathbb{Z}_6$ to any element in $\mathbb{Z}_4$ whose order divides 6.

1 and 3 in $\mathbb{Z}_4$ have order 4, and $4 \nmid 6$, so these are ruled out.

I can send 1 to $0 \in \mathbb{Z}_4$ (which has order 1) or to $2 \in \mathbb{Z}_4$ (which has order 2). Therefore, there are exactly two homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_4$.

In more detail, consider the homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_4$ given by $\phi(1) = 2$. Then

$$\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 2 + 2 = 0.$$

Likewise, $\phi(3) = 3 \cdot 2 = 2$, $\phi(4) = 4 \cdot 2 = 0$, $\phi(5) = 5 \cdot 2 = 2$, and of course $\phi(0) = 0$. Notice that once I know where 1 goes, I know where everything goes! $\square$

Example. What are the possible homomorphisms $\mathbb{Z}_4 \to \mathbb{Z}_{12}$?

A homomorphism is determined by where I send the generator $1 \in \mathbb{Z}_4$. Now 1 has order 4, so I must send it to an element of order 1, 2, or 4 in $\mathbb{Z}_{12}$. The possibilities are 0, 3, 6, or 9. Each of these choices gives rise to a homomorphism.

Look at the map given by $\phi(1) = 3$. As in the previous example, you can verify that

$$\phi(2) = 6, \quad \phi(3) = 9, \quad \phi(0) = 0.$$

The kernel of ϕ is $\{0\}$; the image of ϕ is $\{0, 3, 6, 9\}$, which is the subgroup $\langle 3 \rangle$ of $\mathbb{Z}_{12}$.

On the other hand, $\phi(1) = 6$ produces a homomorphism with kernel $\{0, 2\} < \mathbb{Z}_4$ and image $\{0, 6\} < \mathbb{Z}_{12}$.

Finally, note that the formula $\phi(x) = 2x$ *does not* define a homomorphism $\mathbb{Z}_4 \to \mathbb{Z}_{12}$. This may seem puzzling, since formally

$$\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y).$$

The problem is that the map is not well defined. Note that $\phi(1) = 2 \cdot 1 = 2$, and $2 \in \mathbb{Z}_{12}$ is not in the set $\{0, 3, 6, 9\}$ of allowable targets. $\square$

Example. Define $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$\phi(m, n) = m - 3n.$$

ϕ is a homomorphism:

$$\phi\left[(m_1, n_1) + (m_2, n_2)\right] = \phi(m_1 + m_2, n_1 + n_2) =$$

$$(m_1 + m_2) - 3(n_1 + n_2) = (m_1 - 3n_1) + (m_2 - 3n_2) = \phi(m_1, n_1) + \phi(m_2, n_2).$$

$\operatorname{im} \phi = \mathbb{Z}$, because $\phi(m, 0) = m$ for all $m \in \mathbb{Z}$.

$\ker \phi = \langle (3, 1) \rangle$. First,

$$\phi\left[k \cdot (3, 1)\right] = \phi(3k, k) = 3k - 3k = 0.$$

Thus, $\langle (3, 1) \rangle \subset \ker \phi$.

Conversely, if $(m, n) \in \ker \phi$, then $\phi(m, n) = 0$, so $m - 3n = 0$, or $m = 3n$. Then $(m, n) = (3n, n) = n \cdot (3, 1)$, and the latter is an element of $\langle (3, 1) \rangle$. Thus, $\ker \phi \subset \langle (3, 1) \rangle$, so $\ker \phi = \langle (3, 1) \rangle$.

Hence, the First Isomorphism Theorem says that

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (3, 1) \rangle} \approx \mathbb{Z}.$$

A coset of $\langle (3, 1) \rangle$ in $\mathbb{Z} \times \mathbb{Z}$ consists of the lattice points on the line $y = \dfrac{1}{3}x + b$, where b is an integer. The isomorphism essentially maps this coset to the y-intercept $b \in \mathbb{Z}$. $\square$

Lemma. If $\phi : G \to H$ is a surjective group map and $K \lhd G$, then $\phi(K) \lhd H$.

Proof. $1 \in K$, so $1 = \phi(1) \in \phi(K)$, and $\phi(K) \neq \emptyset$.

Let $a, b \in K$, so $\phi(a), \phi(b) \in \phi(K)$. Then

$$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(K), \text{ since } ab^{-1} \in K.$$

Therefore, $\phi(K)$ is a subgroup.

(Notice that this does not use the fact that K is normal. Hence, I've actually proved that the image of a subgroup is a subgroup.)

Now let $h \in H$, $a \in K$, so $\phi(a) \in \phi(K)$. I want to show that $h\phi(a)h^{-1} \in \phi(K)$. Since ϕ is surjective, $h = \phi(g)$ for some $g \in G$. Then

$$h\phi(a)h^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi\left(gag^{-1}\right).$$

But $gag^{-1} \in K$ because K is normal. Hence, $\phi\left(gag^{-1}\right) \in \phi(K)$. It follows that $\phi(K)$ is a normal subgroup of H. □

Theorem. (**The Second Isomorphism Theorem**) Let $K, H \triangleleft G$, $K < H$. Then

$$\frac{\dfrac{G}{K}}{\dfrac{H}{K}} \approx \frac{G}{H}.$$

Proof. Note that a typical element of the left side looks like $(gK)(H/K)$, where $g \in G$.

If $\phi : G \to G/K$ is the quotient map, $\phi(H) = H/K$. Since $H \triangleleft G$, it follows that $H/K \triangleleft G/K$, by the preceding lemma. Therefore, the left side *really is* a quotient group!

I will construct maps going both ways which are inverses. The construction will make heavy use of the Universal Property of the Quotient.

First, the quotient map $\pi : G \to G/H$ sends $K < H$ to the identity. By the Universal Property of the Quotient, there is an induced map $\phi : G/K \to G/H$ defined by

$$\phi(gK) = gH.$$

Now if $g \in H$, then $\phi(gK) = gH = H$, which is the identity coset in G/H. Since ϕ kills H, the Universal Property of the Quotient implies the existence of a map $\psi : (G/K)/(H/K) \to G/H$ defined by

$$\psi\left[(gK)(H/K)\right] = gH.$$

Thus, I've constructed a map from the left side to the right side.

Next, consider the composite $\sigma : G \to G/K \to (G/K)/(H/K)$ made up of two quotient maps. It is $\sigma(g) = (gK)(H/K)$. If $g \in H$, then $\sigma(g) = (gK)(H/K) = H/K$, which is the identity coset in $(G/K)/(H/K)$. Hence, σ kills H, and the Universal Property of the Quotient implies the existence of a map $\tau : G/H \to (G/K)/(H/K)$ given by

$$\tau(gH) = (gK)(H/K).$$

Now I have a map from the right side to the left side.

ψ and τ are visibly inverses, so they are isomorphisms. □

Notice the ease with which the Universal Property of the Quotient allowed me to construct the maps. Nowhere did I need to check that a map was well defined, or that a map was a homomorphism! All the work was done in the proof of the Universal Property.

There is a Third Isomorphism Theorem (sometimes called the Modular Isomorphism, or the Noether Isomorphism). It asserts that if $H < G$ and $K \triangleleft G$, then

$$\frac{H}{H \cap K} \approx \frac{HK}{K}.$$