Abstract algebra

Krisztián Szabó

Source: Contemporary Abstract Algebra by Joseph A. Gallian

Content

6 Isomorphisms

6.1 Definition and Examples

In this chapter, we give a formal method for determining whether two groups defined in different terms are the same. When this is the case, we say that there is an isomorphism between the two groups. This notion was first introduced by Galois about 175 years ago. The term *isomorphism* is derived from the Greek words *isos*, meaning "same" or "equal", and *morphe*, meaning "form".

6.1.1 Group isomorphism

Definition. An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a,\, b \in G.$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.

It is implicit in the definition of isomorphism that the operation on the left side of the equal sign is that of G, whereas the operation on the right side is that of $\overline{G}$. The four cases involving $\cdot$ and $+$ are shown in the table below.

G operation	$\overline{G}$ operation	Operation preservation
$\cdot$	$\cdot$	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
$\cdot$	$+$	$\phi(a \cdot b) = \phi(a) + \phi(b)$
$+$	$\cdot$	$\phi(a + b) = \phi(a) \cdot \phi(b)$
$+$	$+$	$\phi(a + b) = \phi(a) + \phi(b)$

There are four separate steps involved in proving that a group G is isomorphic to a group $\overline{G}$.

Step 1. "Mapping". Define a candidate for the isomorphism; that is, define a function ϕ from G to $\overline{G}$.
Step 2. "1-1". Prove that ϕ is one-to-one; that is, assume that $\phi(a) = \phi(b)$ and prove that $a = b$.
Step 3. "Onto". Prove that ϕ is onto; that is, for any element $\overline{g} \in \overline{G}$, find an element $g \in G$ such that $\phi(g) = \overline{g}$. **Step 4.** "O.P." Prove that ϕ is operation-preserving; that is, show that $\phi(ab) = \phi(a)\phi(b)$ for all a and b in G.

None of these steps are unfamiliar to you. The only one that may appear novel is the fourth one. It requires that one be able to obtain the same result by combining two elements and then mapping, or by mapping two elements and then combining them. Roughly speaking, this says that the two processes-operating and mapping-can be done in either order without affecting the result. This same concept arises in calculus when we say

$$\lim_{x\to a}\big(f(x)\cdot g(x)\big)=\lim_{x\to a}f(x)\lim_{x\to a}g(x)$$

or

$$\int\limits_a^b\big(f(x)+g(x)\big)\,dx=\int\limits_a^b f(x)\,dx+\int\limits_a^b g(x)\,dx.$$

Let us consider some examples.

Example. Let $G=\mathbb{R}$ under addition and let $\overline{G}=\mathbb{R}^+$ under multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\phi(x)=2^x$. Certinly, ϕ is a function from G to $\overline{G}$. To prove that it is one-to-one, suppose that $2^x=2^y$. Then $\log_2 2^x=\log_2 2^y$, and therefore $x=y$. For "onto", we must find for any positive real number y some real number x such that $\phi(x)=y$; that is $2^x=y$. Well, solving for x gives $\log_2 y$. Finally,

$$\phi(x+y)=2^{x+y}=2^x\cdot 2^y=\phi(x)\phi(y).$$

Example. Any infinite cyclic group is isomorphic to Z. Indeed, if a is a generator of the cyclic group, the mapping $a^k\to k$ is an isomorphism. Any finite cyclic group $\langle a\rangle$ of order n is isomorphic to Z_n under the mapping $a^k\to k \bmod n$. That these correspodences are functions and are one-to-one is the essence of Theorem 4.1.

Example. The mapping from $\mathbb{R}$ under addition to itself given by $\phi(x)=x^3$ is not an isomorphism. Although ϕ is one-to-one and onto, it is not operation-preserving, since it is not true that $(x+y)^3=x^3+y^3$ for all x and y in $\mathbb{R}$.

Example. $U(10)\approx Z_4$ and $U(5)\approx Z_4$. To verify this, one need only observe that both $U(10)$ and $U(5)$ are cyclic of order 4.

6.1.2 Cayley's theorem (1854)

Theorem. Every group is isomorphic to a group of permutations.

Proof. To prove this, let G be a group. We must find a group $\overline{G}$ of permutations that we believe is isomorphic to G. Since G is all we have to work with, we will have to use it to construct $\overline{G}$.

For any g in G, define a function T_g from G to G by

$$T_g(x) = gx \quad \forall\, x \in G.$$

(In words, T_g is just a multiplication by g on the left.) We prove that T_g is a permutation on the set of elements G. T_g is one-to-one, because

$$\forall\, x,\, y \in G : T_g(x) = T_g(y) \quad \Longleftrightarrow \quad gx = gy \quad \Longleftrightarrow \quad (g^{-1}g)x = (g^{-1}g)y$$

T_g is onto. Let $y \in G$. We have to find $x \in G$, that satisfies

$$T_g(x) = y \quad \Longleftrightarrow \quad gx = y$$

$x := g^{-1}y$ shows that T_g is onto, so we proved that T_g is a permutation.

Now let $\overline{G} := \{T_g \mid g \in G\}$. Then, $\overline{G}$ is a group under the operation of function composition. To verify this, we first observe that for any g and h in G we have $T_gT_h(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$, so that $T_gT_h(x) = T_{gh}(x)$. From this it follows that T_e is the identity and $(T_g)^{-1} = T_{g^{-1}}$. Since function composition is associative, we have verified all the conditions for $\overline{G}$ to be a group. The isomorphism ϕ between G and $\overline{G}$ is now ready-made. For every g in G, define $\phi(g) = T_g$. If $T_g = T_h$, then $T_g(e) = T_h(e)$ or $ge = he$. Thus, $g = h$ and ϕ is one-to-one. By the way $\overline{G}$ was constructed, we see that ϕ is onto. The only condition that remains to be checked is that ϕ is operation-preserving. To this end, let a and b belong to G. Then

$$\phi(ab) = T_{ab} = T_aT_b = \phi(a)\phi(b).$$

The group $\overline{G}$ constructed above is called the *left regular representation of* G.

Example. For concreteness, let us calculate the left regular representation $\overline{U(12)}$ for $U(12) = \{1,\, 5,\, 7,\, 11\}$.

$$\phi : U(12) \to \overline{U(12)}, \quad \phi(x) = T_x : U(12) \to U(12)$$

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \quad T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix},$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \quad T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}.$$

It is instructive to compare the Cayley table for $U(12)$ and its left regular representation $\overline{U(12)}$.

$U(12)$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\overline{U(12)}$	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

6.2 Properties of isomorphisms

Our next two theorems give a catalog of properties of isomorphisms and isomorphic groups.

6.2.1 Properties of isomorphisms acting on elements

Theorem. Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. For every integer n and for every group element a in G, $\phi(a^n) = \big(\phi(a)\big)^n$.
3. For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).
6. For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Proof. We will restrict ourselves to proving only properties 1, 2, and 4, but observe that property 5 follows from properties 1 and 2, property 6 follows from property 2, and property 7 follows from property 5. For convenience, let us denote the identity in G by e and the identity in $\overline{G}$ by $\overline{e}$. Then, since $e = ee$, we have

$$\phi(e) = \phi(e)\phi(e).$$

Also, because $\phi(e) \in \overline{G}$, we have $\phi(e) = \overline{e}\phi(e)$, as well. Thus, by cancellation, $\overline{e} = \phi(e)$. This proves property 1.

For positive integers, property 2 follows from the definition of an isomorphism and mathematical induction: if $n = 1$, $\phi(a^1) = \big(\phi(a)\big)^1$.

Suppose that $\phi(a^{n-1}) = \big(\phi(a)\big)^{n-1}$. Then $\phi(a^n) = \phi(a^{n-1}a) = \phi(a^{n-1})\phi(a) = \big(\phi(a)\big)^{n-1}\phi(a) = \big(\phi(a)\big)^n$. So it is true for positive n values. If n is negative, then $-n$ is positive, and we have from property 1 and the observation about the positive integer case that $e = \phi(e) = \phi(g^n g^{-n}) = \phi(g^n)\phi(g^{-n}) = \phi(g^n)\big(\phi(g)\big)^{-n}$. Thus, multiplying both sides on the right by $\big(\phi(g)\big)^n$, we have $\big(\phi(g)\big)^n = \phi(g^n)$. Property 1 takes care of the case $n = 0$.

To prove property 4, let $G = \langle a \rangle$ and note that, by closure, $\big\langle \phi(a) \big\rangle \subseteq \overline{G}$. Because ϕ is onto, for any element $b \in \overline{G}$, there is an element $a^k \in G$ such that $\phi(a^k) = b$. Thus, $b = \big(\phi(a)\big)^k$ so $b \in \big\langle \phi(a) \big\rangle$. This proves that $\overline{G} = \big\langle \phi(a) \big\rangle$.

Now suppose that $\overline{G} = \big\langle \phi(a) \big\rangle$. Clearly, $\langle a \rangle \subseteq G$. For any element $b \in G$, we have $\phi(b) \in \big\langle \phi(a) \big\rangle$. So, for some integer k we have $\phi(b) = \big(\phi(a)\big)^k = \phi(a^k)$. Because ϕ is one-to-one, $b = a^k$. This proves that $\langle a \rangle = G$.

When the group operation is addition, property 2 of Theorem 6.2 is $\phi(na) = n\phi(a)$; property 4 says that an isomorphism between two cyclic groups takes a generator to a generator.

Property 6 is quite useful for showing that two groups are not isomorphic. Often b is picked to be the identity. For example, consider $\mathbb{C}^*$ and $\mathbb{R}^*$. Because the equation $x^4 = 1$ has four solutions in $\mathbb{C}^*$ but only two in $\mathbb{R}^*$, no matter how one attempts to define an isomophism from $\mathbb{C}^*$ to $\mathbb{R}^*$, property 6 cannot hold.

6.2.2 Properties of isomorphisms acting on groups

Theorem. Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.
2. G is Abelian if and only if $\overline{G}$ is Abelian.
3. G is cyclic if and only if $\overline{G}$ is cyclic.
4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

Theorem. Properties 1 and 4 are left as exercises. Property 2 is a direct consequence of property 3 of Theorem 6.2. Property 3 follows from property 4 of Theorem 6.2 and property 1 of Theorem 6.3.

Theorems 6.2 nad 6.3 show that isomorphic groups have many properties in common. Actually, the definition is precisely formulated so that isomorphic groups have all group-theoretic properties in common. By this we mean that if two groups are isomorphic, then any property that can be expressed in the language of group theory is true for one if and only if it is true for the other. This is why algebraists speak of isomorphic groups as "equal" or "the same". Admittedly, calling groups equivalent, rather than the same, might be more appropriate, but we bot to long-standing tradition.

6.3 Automorphisms

Certain kinds of isomorphisms are referred to so often that they have been given special names.

6.3.1 Automorphism

Definition. An isomorphism from a group G onto itself is called in *automorphism* of G.

Example. Let $\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$. Then $\phi(a, b) = (b, a)$ is an automorphism of the group $\mathbb{R}^2$ under componentvise addition. Geometrically, ϕ reflects each point in the plane across the line $y = x$. More generally, any reflection across a line passing through the origin or any rotation of the plane about the origin is an automorphism of $\mathbb{R}^2$.

6.3.2 Inner automorphism induced by a

Definition. Let G be a group, and let $a \in G$. The function $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is called the *inner automorphism of G induced by a.*

6.3.3 ϕ_a is an automorphism

Theorem. Every inner automorphisms of G are automorphisms.

Proof. (personal) Let G be a group and $a \in G$ an arbitrary element. The inner automorphism of G induced by a:

$$\phi_a : G \to G, \quad \phi_a(x) = axa^{-1} \quad (x \in G).$$

It is certainly a **function**:

$$x = y \quad \Longleftrightarrow \quad axa^{-1} = aya^{-1} \quad (x, y \in G)$$

Let us prove that ϕ_a is **one-to-one**.

For all x, $y \in G$:

$$\phi_a(x) = \phi_a(y) \quad \iff \quad axa^{-1} = aya^{-1}$$

By left- and right-hand side cancellation we get $x = y$. Now proove that ϕ_a is **onto**; that is, for every $y \in G$, there exists $x \in G$, such that

$$\phi_a(x) = y \quad \iff \quad axa^{-1} = y \quad (x := a^{-1}ya)$$

The only thing left is to proove that ϕ_a is operation-preserving, such that for every x, $y \in G$:

$$\phi_a(xy) = axya^{-1} = ax(aa^{-1})ya^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_a(y)$$

6.3.4 Aut(G) and Inn(G)

Definition. Let G be a group. Aut(G) denotes the set of all automorphisms of G and Inn(G) denotes the set of all inner automorphisms of G, so

$$\mathrm{Aut}(G) := \{\phi : G \to G \mid \phi \text{ is an automorphism of } G\}$$

$$\mathrm{Inn}(G) := \{\phi_g : G \to G \mid g \in G\}$$

6.3.5 Aut(G) and Inn(G) are groups

Theorem. The set of all automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

Proof. (personal) Let G be a group. We prove that Aut(G) is also a group under function composition. We see that closure holds. Let α, $\beta \in \mathrm{Aut}(G)$. $\alpha\beta \in \mathrm{Aut}(G)$ means that $\alpha\beta$ is also an automorphism, so let us prove that:

1. **Function**: Because α and β are clearly functions, we get $x = y \implies \beta(x) = \beta(y) \implies \alpha\beta(x) = \alpha\beta(y)$ for all x, $y \in G$.

2. **One-to-one**: Because α and β are one-to-one functions we get $\alpha\big(\beta(x)\big) = \alpha\big(\beta(y)\big) \implies \beta(x) = \beta(y) \implies x = y$.

3. **Onto**: We have to proove that for all $y \in G$, there is an $x \in G$ such that $\alpha\beta(x) = y$. Because α is onto, there is a $z \in G$ such that $\alpha(z) = y$. Because β is onto, there is a $w \in G$ such that $\beta(w) = z$. We get $\alpha\big(\beta(x)\big) = y$ $(x := w)$.

4. **O.P.**: Finally, for all x, $y \in G$:

$$\alpha\beta(xy) = \alpha\big(\beta(x)\beta(y)\big) = \alpha\big(\beta(x)\big)\alpha\big(\beta(y)\big) = \alpha\beta(x)\alpha\beta(y).$$

We proved that closure holds. The associativity comes from the fact that function composition is associative.

Now let us prove that the identity $\gamma \in \mathrm{Aut}(G)$ exists, such that for all $\alpha \in \mathrm{Aut}(G) : \alpha\gamma(x) = \gamma\alpha(x) = \alpha(x)$ for all $x \in G$. The function $\gamma : G \to G$, $\gamma(x) = x$ is certainly an automorphism, and we get $\alpha\big(\gamma(x)\big) = \gamma\big(\alpha(x)\big) = \alpha(x)$.

We know that if $\alpha \in \mathrm{Aut}(G)$ is an automorphism, then α^{-1} is also an automorphism, but let us proove the O.P. part of it:

$$\alpha^{-1}(xy) = \alpha^{-1}\Big(\alpha\big(\alpha^{-1}(x)\big)\alpha\big(\alpha^{-1}(y)\big)\Big) = \alpha^{-1}\Big(\alpha\big(\alpha^{-1}(x)\alpha^{-1}(y)\big)\Big) = \alpha^{-1}(x)\alpha^{-1}(y).$$

We proved that $\mathrm{Aut}(G)$ is indeed a group.

Example. To compute $\mathrm{Aut}(Z_{10})$, we try to discover enough information about an element α of $\mathrm{Aut}(Z_{10})$ to determine how α must be defined. To begin with, observe that once we know $\alpha(1)$, we know $\alpha(k)$ for any $k \in Z_{10}$, because

$$\boxed{\alpha(k)} = \underbrace{\alpha(1+1+\cdots+1)}_{k \text{ terms}} = \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{k \text{ terms}} = \boxed{k\alpha(1)}.$$

So, we need only determine the choices for $\alpha(1)$ that make α an automorphism of Z_{10}. Since property 5 of Theorem 6.2 tells us that $|\alpha(1)| = |1| = 10$, there are four candidates for $\alpha(1)$:

$$\alpha(1) = 1; \quad \alpha(1) = 3; \quad \alpha(1) = 7; \quad \alpha(1) = 9.$$

To distinguish among the four possiblitities, we refine our notation by denoting the mapping that sends 1 to 1 by α_1, and so on. Clearly α_1 is the identity. Let us check α_3. Since $x \bmod 10 = y \bmod 10 \Longrightarrow 3x \bmod 10 = 3y \bmod 10$, α_3 is a function indeed. Moreover, because $\alpha_3(1) = 3$ is a generator of Z_{10}, for all $y \in Z_{10}$, there should be $x \in Z_{10}$ such that $\alpha_3(x) = y$, therefore $3x = 3k$ for some k. $3x - 3k = 0 \Longrightarrow 3(x-k) = 0$, $x := k$, so α_3 is onto. We know if S is a finite set, then $f : S \to S$ is onto if and only if f is one-to-one, so α_3 is one-to-one. Finally, since $\alpha_3(a+b) = 3(a+b)/3a+3b = \alpha_3(a)+\alpha_3(b)$ for all a, $b \in Z_{10}$, we see that α_3 is operation-preserving as well. Thus, $\alpha_3 \in \mathrm{Aut}(Z_{10})$. The same argument shows that α_7 and α_9 are also automorphisms.

This gives us the elements of $\mathrm{Aut}(Z_{10})$ but not the structure. For instance, what is $\alpha_3\alpha_3$?. Direct calculations show that $|\alpha_3| = 4 = |\mathrm{Aut}(Z_{10})|$, thus $\mathrm{Aut}(Z_{10})$ is cyclic. Actually, the following Cayley tables reveal that $\mathrm{Aut}(Z_{10})$ is isomorphic to $U(10)$.

$U(10)$	1	3	7	9
1	1	3	7	9
7	7	1	9	3
9	9	7	3	1

$\text{Aut}(Z_{10})$	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_7	α_7	α_1	9	α_3
α_9	α_9	α_7	α_3	α_1

With example above as a guide, we are now ready to tackle the group $\text{Aut}(Z_n)$. The result is particularly nice, since it relates the two kinds of groups we have most frequently encountered thus far-the cyclic groups Z_n and the U-groups $U(n)$.

6.3.6 Aut$(Z_n) \approx U(n)$

Theorem. For every positive integer n, $\text{Aut}(Z_n)$ is isomorphic to $U(n)$.

Proof. As in the example above, any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspodence from $\text{Aut}(Z_n)$ to $U(n)$ given by

$$T : \text{Aut}(Z_n) \to U(n), \quad T(\alpha) = \alpha(1) \quad (\alpha \in \text{Aut}(Z_n)).$$

The fact that $\alpha(k) = k\alpha(1)$ implies that T is a one-to-one mapping, becaues if α, $\beta \in \text{Aut}(Z_n)$ we get:

$$T(\alpha) = T(\beta) \iff \alpha(1) = \beta(1)$$

We have to show that $\alpha(k) = \beta(k)$ for all $k \in Z_n$.

$$\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k) \Longrightarrow \alpha = \beta.$$

To prove that T is onto, let $r \in U(n)$ and consider the mapping $\alpha : Z_n \to Z_n$ defined by $\alpha(s) = sr \pmod{n}$ for all $s \in Z_n$. *It is an automorphism of* Z_n. Then, since $T(\alpha) = \alpha(1) = 1r$, T is onto $U(n)$.

Finally, we establish the fact that T is operation-preserving. Let α, $\beta \in \text{Aut}(Z_n)$. We then have

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha\big(\beta(1)\big) = \underbrace{\alpha(1 + 1 + \cdots + 1)}_{\beta(1)\text{ terms}} = \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)\text{ terms}}$$

$$= \alpha(1)\beta(1) = T(\alpha)T(\beta).$$

This completes the proof.