# ISOMORPHISMS

KEITH CONRAD

## 1. Introduction

Groups that are not literally the same may be structurally the same. An example of this idea is the relation between multiplication and addition via exponentiation:

$$e^x e^y = e^{x+y}. \tag{1.1}$$

Every number in $\mathbf{R}_{>0}$ has the form $e^x$ for exactly one $x \in \mathbf{R}$, and (1.1) tells us that when we write numbers in $\mathbf{R}_{>0}$ as $e^x$ then multiplying in $\mathbf{R}_{>0}$ corresponds to adding the exponents in $\mathbf{R}$. Going the other way, every real number has the form $\ln x$ for exactly one $x > 0$, and addition of logarithm values corresponds to multiplication inside the logarithm:

$$\ln(x) + \ln(y) = \ln(xy).$$

The functions $\exp\colon \mathbf{R} \to \mathbf{R}_{>0}$ and $\ln\colon \mathbf{R}_{>0} \to \mathbf{R}$ make the groups $\mathbf{R}_{>0}$ and $\mathbf{R}$ look the same: they are each a *bijective* way of passing between the two groups that turn the operation in one group into the operation in the other group (*e.g.* doubling in $\mathbf{R}$ is like squaring in $\mathbf{R}_{>0}$).

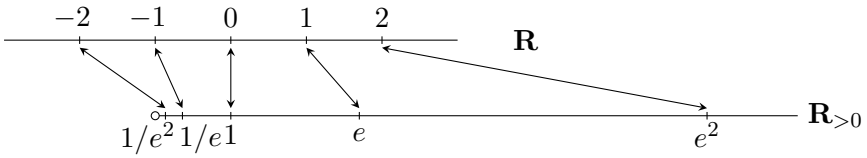



FIGURE 1. The groups $\mathbf{R}$ and $\mathbf{R}_{>0}$, linked by $x \mapsto e^x$ and $y \mapsto \ln y$.

**Definition 1.1.** An *isomorphism* $f\colon G \to \widetilde{G}$ between two groups $G$ and $\widetilde{G}$ is a bijective homomorphism. When there is an isomorphism between $G$ and $\widetilde{G}$, the groups are called *isomorphic* and we write $G \cong \widetilde{G}$.

An isomorphism between two groups is a dictionary that lets us translate elements and operations from one group to the other without losing essential information. For example, we'll see that all cyclic groups of the same size are isomorphic, so if we understand one cyclic group then we can usually transfer that understanding to all the other cyclic groups of the same size. Isomorphisms are the way to express how two groups that are different are nevertheless basically the same.

## 2. Examples of isomorphisms

**Example 2.1.** The exponential function $\exp\colon \mathbf{R} \to \mathbf{R}_{>0}$, sending each $x \in \mathbf{R}$ to $e^x$, is an isomorphism: it is a homomorphism since $e^{x+y} = e^x e^y$ and it is a bijection since it has an inverse function, the natural logarithm.

More generally, for each $b > 0$ with $b \neq 1$ the function $f\colon \mathbf{R} \to \mathbf{R}_{>0}$ given by $f(x) = b^x$ is an isomorphism: it is a homomorphism since $f(x+y) = b^{x+y} = b^x b^y = f(x)f(y)$, and it is a bijection since it has $\log_b x$ as an inverse function. Figure 1 shows some corresponding elements of $\mathbf{R}$ and $\mathbf{R}_{>0}$ under this isomorphism.

Going the other way, $\log_b\colon \mathbf{R}_{>0} \to \mathbf{R}$ is an isomorphism: it is a homomorphism since $\log_b(xy) = \log_b x + \log_b y$, and it is a bijection since it has $b^x$ as an inverse function.

**Example 2.2.** The "exponential-type" function $f\colon \mathbf{Z}/(4) \to (\mathbf{Z}/(5))^\times$ where $f(a \bmod 4) = 2^a \bmod 5$, is an isomorphism: it makes sense since $2^4 \equiv 1 \bmod 5 \Rightarrow 2^{a+4k} = 2^a 2^{4k} \equiv 2^a \mod 5$, and it is a homomorphism since

$$f(a \bmod 4)f(b \bmod 4) = (2^a \bmod 5)(2^b \bmod 5) = 2^{a+b} \bmod 5$$

and

$$f(a \bmod 4 + b \bmod 4) = f((a+b) \bmod 4) = 2^{a+b} \bmod 5,$$

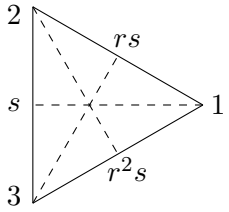
so $f(a \bmod 4)f(b \bmod 4) = f(a \bmod 4 + b \bmod 4)$. This function is a bijection from the data in the table below.

| $a \bmod 4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $2^a \bmod 5$ | 1 | 2 | 4 | 3 |

**Example 2.3.** The function $f\colon \mathbf{Z}/(4) \to (\mathbf{Z}/(5))^\times$ where $f(a \bmod 4) = 4^a \bmod 5$, is *not* an isomorphism: it is a homomorphism by the same argument as in the previous example (just replace $2^a$ with $4^a$), but $f$ is not a bijection since it is not injective, as the table below shows (it is also not surjective, as it misses two values).

| $a \bmod 4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $4^a \bmod 5$ | 1 | 4 | 1 | 4 |

**Example 2.4.** The groups $D_3$ and $S_3$ are isomorphic. Evidence that they resemble each other is that both groups have order 6, three elements of order 2, and two elements of order 3 (and of course one element of order 1: the identity). To create an isomorphism from $D_3$ to $S_3$, label the vertices of an equilateral triangle as 1, 2, and 3 (see picture below) so that each element of $D_3$ permutes the vertices and thus can be turned into an element of $S_3$.




Let $r$ be a counterclockwise rotation by 120 degrees and $s$ be the reflection across the horizontal dashed line. Then $rs$ and $r^2s$ are reflections across the other dashed lines. The vertex labels in the picture lead to the table below turning elements of $D_3$ into elements of $S_3$.

| $D_3$ : | 1 | $r$ | $r^2$ | $s$ | $rs$ | $r^2s$ |
|---|---|---|---|---|---|---|
| $S_3$ : | (1) | (123) | (132) | (23) | (12) | (13) |

The correspondence in the table is compatible with the group laws in $D_3$ and $S_3$, *e.g.*, $r$ has order 3 and (123) has order 3, $s$ has order 2 and (23) has order 2, and $sr = r^{-1}s$ while $(23)(123) = (123)^{-1}(23)$. If we let $f\colon D_3 \to S_3$ by the table above, it is a bijection and a tedious calculation (omitted) can verify that it is a homomorphism. Since $f$ is a bijective homomorphism from $D_3$ to $S_3$, it is an isomorphism.

**Example 2.5.** The group $\mathrm{Aff}(\mathbf{Z}/(4))$ is isomorphic to $D_4$. The idea behind this is that each matrix in $\mathrm{Aff}(\mathbf{Z}/(4))$ can be written as $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ where $a \in \{\pm 1 \bmod 4\}$ and $b \in \mathbf{Z}/(4)$, and we can decompose such a matrix as

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

where $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \bmod 4$ has order 4 in $\mathrm{Aff}(\mathbf{Z}/(4))$, $\left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \bmod 4$ has order 2, and

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

which resembles the rule $sr = r^{-1}s$ in $D_4$. This suggests considering the function $f\colon D_4 \to \mathrm{Aff}(\mathbf{Z}/(4))$ where

$$f(r^k s^\ell) = \begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix} \bmod 4,$$

which makes sense since in $r^k s^\ell$ the exponent $k$ only matters mod 4 and the exponent $\ell$ only matters mod 2, which is also all that matters for $k$ and $\ell$ in the mod 4 matrix on the right. To check $f$ is a homomorphism we compute $f(r^k s^\ell)f(r^{k'} s^{\ell'})$ and $f((r^k s^\ell)(r^{k'} s^{\ell'}))$:

$$f(r^k s^\ell)f(r^{k'} s^{\ell'}) = \begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} (-1)^{\ell'} & k' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} (-1)^{\ell+\ell'} & (-1)^\ell k' + k \\ 0 & 1 \end{pmatrix},$$

and since $s^\ell r^k = r^{(-1)^\ell k} s^\ell$ (check this separately for even $\ell$ and odd $\ell$, trying $\ell = 0$ and 1 first),

$$f((r^k s^\ell)(r^{k'} s^{\ell'})) = f(r^k r^{(-1)^\ell k'} s^\ell s^{\ell'})) = f(r^{k+(-1)^\ell k'} s^{\ell+\ell'}) = \begin{pmatrix} (-1)^{\ell+\ell'} & k + (-1)^\ell k' \\ 0 & 1 \end{pmatrix}.$$

Thus $f$ is a homomorphism. Its kernel is determined by solving $f(r^k s^\ell) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 4$, which says $\left(\begin{smallmatrix} (-1)^\ell & k \\ 0 & 1 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \bmod 4$, so $\ell$ has to be even and $k \equiv 0 \bmod 4$, which makes $r^k s^\ell = 1$. Thus $f\colon D_4 \to \mathrm{Aff}(\mathbf{Z}/(4))$ is injective (kernel is trivial). Since $D_4$ and $\mathrm{Aff}(\mathbf{Z}/(4))$ both have order 8, an injective function between them is surjective, so $f$ is a bijection and thus is an isomorphism.

While there can be infinitely many different cyclic groups of the same size, they all turn out to be isomorphic to each other. This is proved in the following two theorems.

**Theorem 2.6.** *Every infinite cyclic group is isomorphic to* $\mathbf{Z}$.

*Proof.* Let $G = \langle g \rangle$ be an infinite cyclic group, with generator $g$. Each element of $G$ has the form $g^n$ for some $n \in \mathbf{Z}$, and $n$ is unique: if $g^n = g^{n'}$ where $n \neq n'$, then without loss of generality $n' < n$ so $g^{n-n'} = 1$ and $n - n'$ is a positive integer, so $g$ has finite order and that contradicts $\langle g \rangle$ being infinite.

Since $g^n g^{n'} = g^{n+n'}$, the function $f\colon \mathbf{Z} \to G$ where $f(n) = g^n$ is a homomorphism. This function is injective since we showed $g^n \neq g^{n'}$ when $n \neq n'$, and it is surjective since $g$ generates $G$, so every element of $G$ is some $g^n = f(n)$. Thus $f$ is a bijection, so it is an isomorphism from $\mathbf{Z}$ to $G$. □

**Example 2.7.** In $\mathbf{Q}^\times$, the subgroup $\langle 2 \rangle = \{2^n : n \in \mathbf{Z}\}$ is infinite cyclic with generator 2, so it is isomorphic to $\mathbf{Z}$ by the function $f\colon \mathbf{Z} \to \langle 2 \rangle$ where $f(n) = 2^n$.

**Theorem 2.8.** *Every cyclic group of order* $m$ *is isomorphic to* $\mathbf{Z}/(m)$.

*Proof.* Let $G = \langle g \rangle$ be a cyclic group of order $m$, with generator $g$. Since the order of $g$ is the size of $\langle g \rangle$, $g$ has order $m$. Let $f\colon \mathbf{Z}/(m) \to G$ by $f(a \bmod m) = g^a$. We want to show this is a bijective homomorphism.

First we need to show $f(a \bmod m)$ makes sense: it is defined in terms of a representative $a$ from a congruence class, so we need to check that if $a \equiv a' \bmod m$ then $g^a = g^{a'}$. We can write $a = a' + mk$ for some $k \in \mathbf{Z}$, so

$$g^a = g^{a'+mk} = g^{a'}(g^m)^k = g^{a'}1^k = g^{a'}.$$

To see $f$ is a homomorphism,

$$f(a \bmod m)f(b \bmod m) = g^a g^b = g^{a+b} = f((a+b) \bmod m) = f(a \bmod m + b \bmod m).$$

To prove $f$ is a bijection, since $|\langle g \rangle| = m = |\mathbf{Z}/(m)|$ it suffices to prove just that $f$ is injective or just that $f$ is surjective. Surjectivity is simpler: by the definition of a cyclic group with $g$ being a generator, every element of $G$ is $g^a$ for some $a \in \mathbf{Z}$, so $f(a \bmod n) = g^a$. Thus $f$ is a bijection.[1] □

**Example 2.9.** The groups $\mathbf{Z}/(6)$, $U(7)$, and $U(9)$ are all cyclic: $\mathbf{Z}/(6)$ has generator 1 mod 6, $U(7)$ has generator 3 mod 7 and $U(9)$ has generator 2 mod 9. So there are isomorphisms $f\colon \mathbf{Z}./(6) \to U(7)$ and $f'\colon \mathbf{Z}./(6) \to U(9)$ where $f(a \bmod 6) = 3^a \bmod 7$ and $f'(a \bmod 6) = 2^a \bmod 9$.

The way we constructed an isomorphism from $\mathbf{Z}$ or $\mathbf{Z}/(m)$ to a cyclic group depended on a choice of a generator, since $f(1) = g$ is the generator we used. If we use a different generator then $f$ becomes a different isomorphism. Thus you should be careful not to confuse the statement that two groups are isomorphic (there is *some* bijective homomorphism between them) and the statement that a specific function between the groups is an isomorphism.

**Example 2.10.** In $U(7)$ two generators are 3 and 5. They each lead to separate isomorphisms $\mathbf{Z}/(6) \to U(7)$, as shown in the table below.

| $a \bmod 6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $3^a \bmod 7$ | 1 | 3 | 2 | 6 | 4 | 5 |
| $5^a \bmod 7$ | 1 | 5 | 4 | 6 | 2 | 3 |

**Corollary 2.11.** *For a prime $p$, every group of order $p$ is isomorphic to $\mathbf{Z}/(p)$.*

*Proof.* Let $G$ be a group of order $p$. Pick a nonidentity element $g$ in $G$. Then the order of $g$ divides $|G| = p$ and is not 1, so the order of $g$ is $p$. Thus $\langle g \rangle = G$, so $G$ is cyclic. By Theorem 2.8, there is an isomorphism $\mathbf{Z}/(p) \to G$ by $a \bmod p \mapsto g^a$. □

**Example 2.12.** Focusing on visualization, consider the quotient groups $\mathbf{R}/\mathbf{Z}$ and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$. In $\mathbf{R}/\mathbf{Z}$, all *integers* are treated like 0 and the group is represented by $[0, 1)$ or any half-open interval $[x, x+1)$ for $x \in \mathbf{R}$. In $\mathbf{R}_{>0}/2^{\mathbf{Z}}$, all *integral powers of* 2 are treated like 1 and the group is represented by $[1, 2)$ or any half-open interval $[x, 2x)$ for $x > 0$.

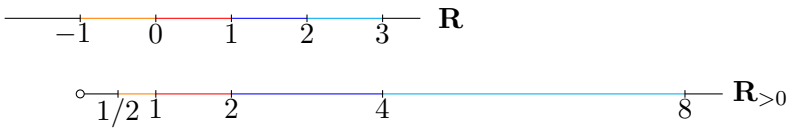



FIGURE 2. Different sets of representatives for $\mathbf{R}/\mathbf{Z}$ and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$.

The pictures in Figure 2, with matching representatives in $\mathbf{R}$ and $\mathbf{R}_{>0}$ for $\mathbf{R}/\mathbf{Z}$ and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ colored the same (using $x \mapsto 2^x$), suggest how $\mathbf{R}/\mathbf{Z}$ and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ are isomorphic to $S^1$: both

[1] If instead we wanted to show $f$ is injective we check its kernel is trivial: if $f(a \bmod m) = 1$ then $g^a = 1$ so $m \mid a$ (because $g$ has order $m$) and thus $a \equiv 0 \bmod m$.

quotient groups have a "wraparound" aspect that is similar to the unit circle $S^1$. A detailed algebraic description of isomorphisms between $S^1$, $\mathbf{R}/\mathbf{Z}$, and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ is in Section 5.

## 3. Properties of isomorphisms

The relation of being isomorphic is an equivalence relation on groups: it is reflexive ($G \cong G$), symmetric (if $G \cong \widetilde{G}$ then $\widetilde{G} \cong G$), and transitive (if $G_1 \cong G_2$ and $G_2 \cong G_3$ then $G_1 \cong G_3$). Reflexivity is easy to see: for every group $G$, the identity function $G \to G$ is an isomorphism from $G$ to itself. To show symmetry and transitivity, use the following two theorems.

**Theorem 3.1.** *If $f\colon G \to \widetilde{G}$ is an isomorphism its inverse function $f^{-1}\colon \widetilde{G} \to G$ is also an isomorphism.*

*Proof.* First we show $f^{-1}$ is a homomorphism. For $y \in \widetilde{G}$, the definition of $f^{-1}(y)$ is the unique $x \in G$ such that $f(x) = y$. For any $y$ and $y'$ in $\widetilde{G}$, we can write $y = f(x)$ and $y' = f(x')$ for unique $x$ and $x'$ in $G$. Then $yy' = f(x)f(x') = f(xx')$, so

$$f^{-1}(yy') = xx' = f^{-1}(y)f^{-1}(y').$$

To show $f^{-1}\colon \widetilde{G} \to G$ is a bijection we appeal to the meaning of an inverse function.

Surjectivity: for each $x \in G$, let $y = f(x) \in \widetilde{G}$. Then $f^{-1}(y) = x$, so each element of $G$ is a value of $f^{-1}$ and thus $f^{-1}$ is surjective.

Injectivity: since $f^{-1}$ is a homomorphism, if suffices (and is equivalent) to show $f^{-1}$ has trivial kernel. If $f^{-1}(y) = e_G$ then by the definition of an inverse function $y = f(e_G)$, which is $e_{\widetilde{G}}$ since homomorphisms send the identity to the identity. Thus $f^{-1}$ has trivial kernel, so it is injective. □

**Theorem 3.2.** *A composition of isomorphisms is an isomorphism.*

*Proof.* Let $f_1\colon G_1 \cong G_2$ and $f_2\colon G_2 \cong G_3$ be group isomorphisms. We'll show the composition $f_1 \circ f_2\colon G_1 \to G_3$ is also an isomorphism:

(1) The composition of homomorphisms is a homomorphism, so $f_1 \circ f_2$ is a homomorphism.
(2) The composition of bijective functions is bijective (exercise), so $f_1 \circ f_2$ is a bijection. □

**Example 3.3.** From the isomorphisms $f\colon \mathbf{Z}/(6) \to U(7)$ and $f'\colon \mathbf{Z}/(6) \to U(9)$ by $f(a \bmod 6) = 3^a \bmod 7$ and $f'(b \bmod 9) = 2^b \bmod 9$, we get an isomorphism $U(7) \to U(9)$ by composing $f^{-1}$ with $f'$: $f' \circ f^{-1}\colon U(7) \to U(9)$ by $3^a \bmod 7 \mapsto 2^a \bmod 9$.

More generally, if $G = \langle g \rangle$ and $\widetilde{G} = \langle \widetilde{g} \rangle$ are cyclic groups of the same size (possibly infinite) then there is an isomorphism $\langle g \rangle \to \langle \widetilde{g} \rangle$ by $g^k \mapsto \widetilde{g}^k$.

Properties of groups that are described purely in terms of the group operation (and not based on what elements explicitly look like) transfer from a group to any isomorphic group. Here is an example of two such properties.

**Theorem 3.4.** *If $G$ and $\widetilde{G}$ are isomorphic groups then one is abelian if and only if the other is, and one is cyclic if and only if the other is.*

*Proof.* Suppose $G$ is abelian and $G \cong \widetilde{G}$. Let $f\colon G \to \widetilde{G}$ be an isomorphism from $G$ to $\widetilde{G}$. For all $x, x' \in G$ we have

$$xx' = x'x \Longrightarrow f(xx') = f(x'x) \Longrightarrow f(x)f(x') = f(x)f(x),$$

so every pair of values of $f$ commute in $\widetilde{G}$. Since $f$ is surjective, every element of $\widetilde{G}$ is a value of $f$, and thus all pairs of elements in $\widetilde{G}$ commute, so $\widetilde{G}$ is abelian.

Conversely, if $\widetilde{G}$ is abelian then for $x$ and $x'$ in $G$ we have $f(x)f(x') = f(x')f(x)$, so $f(xx') = f(x'x)$. Since $f$ is injective, $xx' = x'x$, so all pairs of elements in $G$ commute, and thus $G$ is abelian. (Alternatively, using the inverse isomorphism $\widetilde{G} \to G$, from Theorem 3.1, lets us deduce by reasoning similar to that in the previous paragraph that $\widetilde{G}$ being abelian makes $G$ abelian.)

Next suppose $G$ is cyclic and $f\colon G \to \widetilde{G}$ is an isomorphism from $G$ to another group $\widetilde{G}$. Write $G = \langle g\rangle = \{g^a : a \in \mathbf{Z}\}$. Every $y \in \widetilde{G}$ has the form $y = f(x)$ for some $x \in G$. Since $g$ generates $G$, $x = g^a$ for some integer $a$, so $y = f(g^a) = f(g)^a$. Thus every element of $\widetilde{G}$ is a power of $f(g)$, so $\widetilde{G}$ is cyclic and the isomorphism $f$ sends any generator of $G$ to a generator of $\widetilde{G}$.

Conversely, if $\widetilde{G}$ is cyclic with generator $\widetilde{g}$, we will show $G$ is cyclic. We can write $\widetilde{g} = f(g)$ for some $g \in G$ since $f$ is surjective, and we'll show $g$ is a generator of $G$. For each $x \in G$ we can write $f(x) = \widetilde{g}^n$ for some integer $n$, so $f(x) = f(g)^n = f(g^n)$. Since $f$ is injective, $x = g^n$, so every element of $G$ is a power of $g$ and thus $G = \langle g\rangle$ is cyclic. (Alternatively, using the inverse isomorphism $\widetilde{G} \to G$, from Theorem 3.1, we can use the reasoning from the previous paragraph to show a generator of $\widetilde{G}$ is mapped by that inverse isomorphism to a generator of $G$, so $\widetilde{G}$ being cyclic implies $G$ is cyclic.) □

Being isomorphic is a relation between groups, not a property (like being abelian or cyclic) of a single group. Gerry Myerson[2] once asked on a homework assignment if two specific groups $G_1$ and $G_2$ are isomorphic and got a paper saying "$G_1$ is, but $G_2$ isn't." That is as absurd as asking if two triangles $T_1$ and $T_2$ are congruent and hearing that $T_1$ is congruent and $T_2$ is not.

When classifying all groups that have a particular property, we don't distinguish between isomorphic groups, since one group has the property if and only if the other does. For example, Corollary 2.11 says that every group of prime order $p$ is isomorphic to $\mathbf{Z}/(p)$, and thus all groups of order $p$ are isomorphic to each other. We say they are "the same up to isomorphism." Classification questions about groups are concerned not with finding all groups that have some particular property, but rather with finding all the groups *up to isomorphism* that have the property.

Consider counting count how many essentially different groups there are with a particular order. Some groups of order 4 are

$$\mathbf{Z}/(4),\quad (\mathbf{Z}/(2))^2,\quad U(5),\quad U(8),\quad U(10),\quad U(12),\quad \langle i\rangle,\quad \{(1), (12)(34), (13)(24), (14)(23)\}$$

and some groups of order 6 are

$$\mathbf{Z}/(6),\quad S_3,\quad D_3,\quad \mathbf{Z}/(2)\times\mathbf{Z}/(3),\quad U(7),\quad U(9),\quad U(14),\quad U(18),\quad \mathrm{GL}_2(\mathbf{Z}/(2)),\quad \mathrm{Aff}(\mathbf{Z}/(3)).$$

The number of nonisomorphic groups of order 4 or order 6 is far less than these lists suggest. For order 4 it turns out that

$$\mathbf{Z}/(4) \cong U(5) \cong U(10) \cong \langle i\rangle,\qquad (\mathbf{Z}/(2))^2 \cong U(8) \cong U(12) \cong \{(1), (12)(34), (13)(24), (14)(23)\}$$

and for order 6

$$\mathbf{Z}/(6) \cong \mathbf{Z}/(2)\times\mathbf{Z}/(3) \cong U(7) \cong U(9) \cong U(14) \cong U(18),\quad S_3 \cong D_3 \cong \mathrm{GL}_2(\mathbf{Z}/(2)) \cong \mathrm{Aff}(\mathbf{Z}/(3)).$$

It can be shown that every group of order 4 is isomorphic to $\mathbf{Z}/(4)$ or $(\mathbf{Z}/(2))^2$ (and these are not isomorphic to each other since one is cyclic and the other isn't), and every group of order 6 is isomorphic to $\mathbf{Z}/(6)$ or $S_3$ (and these are not isomorphic to each other since one is abelian and the other isn't).

The Online Encyclopedia of Integer Sequences (https://oeis.org/) is a massive database of numerical sequences that have arisen in mathematics. If you ever meet a sequence and want to

[2]See https://mathoverflow.net/questions/53122/mathematical-urban-legends/62749.

know if it has been studied before, do a search on that website of the first 5-10 terms. The very first entry, on https://oeis.org/A000001, is a count of the number of groups of each (small) order up to isomorphism. The first ten entries, starting with groups of order 0 (there are no such groups), are 0, 1, 1, 1, 2, 1, 2, 1, 5, 2. The first 2 means there are only 2 groups of order 4 up to isomorphism, which was mentioned above: a group of order 4 is isomorphic to $\mathbf{Z}/(4)$ or to $\mathbf{Z}/(2))^2$. The 5 means there are 5 groups of order 8 up to isomorphism.

Although isomorphic groups can be treated as "the same group," that point of view does not apply to subgroups of a group: if two subgroups are isomorphic to each other it does **not** generally mean they behave in the same way *as subgroups* of the larger group. For example, in $D_4$ the subgroups $\{1, s\}$ and $\{1, r^2\}$ are isomorphic to each other (both are cyclic of order 2), but these subgroups are quite different *as subgroups*. For instance, $r^2$ is in the center of $D_4$ and $s$ is not.

## 4. First isomorphism theorem

There is a fundamental theorem about group isomorphisms that lets us show when a quotient group is isomorphic to another (possible more concrete) group. It is traditionally called the *first isomorphism theorem*.[3]

**Theorem 4.1.** *Let $f\colon G \to \widetilde{G}$ be a group homomorphism with kernel $K$. The "induced function" $\overline{f}\colon G/K \to \widetilde{G}$ where $\overline{f}(gK) = f(g)$ is an injective homomorphism, it has the same image as $f$, and $\overline{f}$ is an isomorphism of $G/K$ with $f(G)$. In particular, if $f$ is surjective then $G/\ker f \cong \widetilde{G}$.*

**Example 4.2.** Let $f\colon \mathbf{Z} \to \mathbf{C}^\times$ by $f(n) = i^n$. Then $f$ is a homomorphism ($i^{n+n'} = i^n i^{n'}$), its image is $\{1, i, -1, -i\} = \langle i\rangle$, and its kernel is $4\mathbf{Z}$ since $i$ has order 4 ($i^n = 1$ if and only if $4 \mid n$). Then the first isomorphism theorem says $\mathbf{Z}/4\mathbf{Z} \cong \langle i\rangle$ by $a \bmod 4 \mapsto i^a$.

**Example 4.3.** Let $f\colon \mathbf{Z} \to U(7)$ by $f(n) = 2^n \bmod 7$. Then $f$ is a homomorphism ($2^{n+n'} \equiv 2^n 2^{n'} \bmod 7$), its image is $\{1, 2, 4 \bmod 7\}$ since $2 \bmod 7$ has order 3, and its kernel is $3\mathbf{Z}$ since $2 \bmod 7$ has order 3. The first isomorphism theorem says $\mathbf{Z}/3\mathbf{Z} \cong \{1, 2, 4 \bmod 7\} = \langle 2 \bmod 7\rangle$ by $a \bmod 3 \mapsto 2^a \bmod 7$.

**Example 4.4.** Let $f\colon \mathbf{Z} \to U(7)$ by $f(n) = 3^n \bmod 7$. Then $f$ is a homomorphism ($3^{n+n'} \equiv 3^n 3^{n'} \bmod 7$), its image is $U(7)$ since $3 \bmod 7$ is a generator, and its kernel is $6\mathbf{Z}$ since $3 \bmod 7$ has order 6. The first isomorphism theorem says $\mathbf{Z}/6\mathbf{Z} \cong U(7)$ by $a \bmod 6 \mapsto 3^a \bmod 7$.

**Example 4.5.** The function $f\colon \mathbf{R} \to S^1$ where $f(x) = \cos x + i \sin x$ is a homomorphism that is surjective (every point on $S^1$ is $\cos x + i \sin x$ for an $x \in \mathbf{R}$) and its kernel is $2\pi\mathbf{Z}$, so $\mathbf{R}/2\pi\mathbf{Z} \cong S^1$.

**Example 4.6.** The determinant $\det\colon \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$ is a homomorphism ($\det(AB) = \det A \det B$ for all $A, B \in \mathrm{GL}_2(\mathbf{R})$, and invertible matrices have nonzero determinant) that is surjective since each $\delta \in \mathbf{R}^\times$ is the determinant of $\left(\begin{smallmatrix} \delta & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and the kernel of det is, by definition, the group $\mathrm{SL}_2(\mathbf{R})$ of $2 \times 2$ real matrices with determinant 1. The first isomorphism theorem says $\mathrm{GL}_2(\mathbf{R})/\mathrm{SL}_2(\mathbf{R}) \cong \mathbf{R}^\times$ by $\overline{A} \mapsto \det A$, where $\overline{A}$ is the coset $A\,\mathrm{SL}_2(\mathbf{R})$.

By similar reasoning, $\mathrm{GL}_2(\mathbf{Z}/(m))/\mathrm{SL}_2(\mathbf{Z}/(m)) \cong U(m)$.

Here are two ways to think about what the first isomorphism theorem is saying.

(1) Collapsing a group $G$ modulo the kernel of a homomorphism out of $G$ lets us identify the quotient group of $G$ by the kernel with the image of the homomorphism.

[3]There are also traditional results called the second and third isomorphism theorems, which we don't discuss here.

(2) If you want to show a quotient group $G/N$ is isomorphic to some other group $\widetilde{G}$, write down a homomorphism $f\colon G \to \widetilde{G}$ that's *surjective* with *kernel* $N$. Then the induced function $\overline{f}\colon G/N \to \widetilde{G}$ where $\overline{f}(gN) = f(g)$ is a homomorphism that's surjective (it has the same image as $f$, which is $f(G) = \widetilde{G}$) and injective (part of the first isomorphism theorem), so $\overline{f}$ is an isomorphism from $G/N$ to $\widetilde{G}$.

With examples and some viewpoints laid out, we now prove the first isomorphism theorem. Pay close attention to each step and try to understand what the ideas mean.

*Proof.* Define $\overline{f}\colon G/K \to \widetilde{G}$ by $\overline{f}(gK) = f(g)$. This is *well-defined* because

$$gK = g'K \Longrightarrow g = g'k \text{ for some } k \in K \Longrightarrow f(g) = f(g'k) = f(g')f(k) = f(g')$$

since $k \in K = \ker f$. The function $\overline{f}$ is a homomorphism since

$$\overline{f}(g_1K)\overline{f}(g_2K) = f(g_1)f(g_2) = f(g_1g_2)$$

and

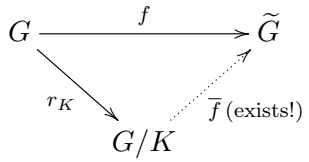
$$\overline{f}(g_1K \cdot g_2K) = \overline{f}(g_1g_2K) = f(g_1g_2).$$

The values of $\overline{f}$ are $\{\overline{f}(gK) : g \in G\} = \{f(g) : g \in G\}$, which is the image of $f$, so $\overline{f}$ and $f$ have the same image in $\widetilde{G}$.

Finally, $\overline{f}\colon G/K \to \widetilde{G}$ is injective since its kernel is trivial: if $\overline{f}(gK) = 1$ then $f(g) = 1$ so $g \in \ker f = K$, and thus $gK = K$, which is the identity in $G/K$.

The function $\overline{f}\colon G/K \to \widetilde{G}$ has image $f(G)$, so if we shrink the target group from $\widetilde{G}$ to $f(G)$ then this makes $\overline{f}\colon G/K \to f(G)$ surjective (same formula as before: $\overline{f}(gK) = f(g)$), and it is also injective (its kernel is trivial), so $G/K \cong f(G)$ by using the function $\overline{f}$. □

A visual way to describe the first isomorphism theorem is through a *commutative diagram*. Starting with the homomorphism $f\colon G \to \widetilde{G}$ having kernel $K$, the reduction map $r_K\colon G \to G/K$ (a generalization of mod $m$ reduction $\mathbf{Z} \to \mathbf{Z}/(m)$) is a homomorphism with kernel $K$, and what the first isomorphism theorem says is that the diagram of groups and homomorphisms $f$ and $r_K$ below can be filled in with a homomorphism $\overline{f}$ so that both ways of going around the diagram from $G$ to $\widetilde{G}$ are the same function (the diagram "commutes"). That is, $\overline{f} \circ r_K = f$ as functions $G \to \widetilde{G}$, since $\overline{f}(r_K(g)) = \overline{f}(gK) = f(g)$ for all $g \in G$.




## 5. Two isomorphisms with the circle group

Returning to the groups in Figure 2, let's relate them to the unit circle $S^1$, a subgroup of $\mathbf{C}^\times$.

**Theorem 5.1.** *The groups $S^1$, $\mathbf{R}/\mathbf{Z}$, and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ are all isomorphic.*

In trigonometry, we treat the circle like $\mathbf{R}/360\mathbf{Z}$ when using degrees ($360 = 0$ and $-180 = 180$) and $\mathbf{R}/2\pi\mathbf{Z}$ when using radians ($2\pi = 0$ and $-\pi = \pi$). Theorem 5.1 uses $\mathbf{R}/\mathbf{Z}$ just to emphasize that algebraically there is nothing special about degrees or radians.

*Proof.* We're going to build isomorphisms $\mathbf{R}/\mathbf{Z} \to S^1$ and $\mathbf{R}/\mathbf{Z} \to \mathbf{R}_{>0}/2^{\mathbf{Z}}$. This doesn't directly include an isomorphism between $S^1$ and $\mathbf{R}_{>0}/2^{\mathbf{Z}}$, but we can get one by composing one of the indicated isomorphisms with the inverse of the other (see Theorems 3.1 and 3.2).

**Part 1: Create an isomorphism $\mathbf{R}/\mathbf{Z} \to S^1$.**

Let $f\colon \mathbf{R}/\mathbf{Z} \to S^1$ by $f(\overline{x}) = \cos(2\pi x) + i\sin(2\pi x)$. (Where does this formula come from? We use $2\pi x$, not $x$, because the identity element $\overline{0}$ in $\mathbf{R}/\mathbf{Z}$ has to go to the identity element 1 in $S^1$ and the cosine and sine functions are $2\pi$-periodic, not $\mathbf{Z}$-periodic, so we want integers to turn into integral multiples of $2\pi$ before taking their cosines and sines.)

Since the domain of $f$ is a quotient group and it's defined by a formula in terms of representatives of $\mathbf{R}/\mathbf{Z}$, we need to check first that $f$ is well-defined. Then we'll check it's a homomorphism and bijective.

$f$ is well-defined. If $\overline{y} = \overline{x}$ in $\mathbf{R}/\mathbf{Z}$ then $y = x + k$ for some $k \in \mathbf{Z}$, so

$$\begin{aligned}\cos(2\pi y) + i\sin(2\pi y) &= \cos(2\pi(x+k)) + i\sin(2\pi(x+k)) \\ &= \cos(2\pi x + 2\pi k) + i\sin(2\pi x + 2\pi k) \\ &= \cos(2\pi x) + i\sin(2\pi x)\end{aligned}$$

since the cosine and sine functions are $2\pi$-periodic.

$f$ is a homomorphism. For $\overline{x}$ and $\overline{x'}$ in $\mathbf{R}/\mathbf{Z}$,

$$\begin{aligned}f(\overline{x})f(\overline{x'}) &= (\cos(2\pi x) + i\sin(2\pi x))(\cos(2\pi x') + i\sin(2\pi x')) \\ &= (\cos(2\pi x)\cos(2\pi x') - \sin(2\pi x)\sin(2\pi x')) + i(\cos(2\pi x)\sin(2\pi x') + \sin(2\pi x)\cos(2\pi x')). \quad (5.1)\end{aligned}$$

The addition formulas for cosine and sine are

$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta), \quad \sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta).$$

Comparing this to (5.1), we have

$$f(\overline{x})f(\overline{x'}) = \cos(2\pi x + 2\pi x') + i\sin(2\pi x + 2\pi x') = f(2\pi(x+x')),$$

so $f$ is a homomorphism.

$f$ is injective. Since $f$ is a homomorphism, it suffices to check $\ker f$ is trivial: we want to show if $f(\overline{x}) = 1$ then $\overline{x} = \overline{0}$, *i.e.*, $x \in \mathbf{Z}$.

The condition $f(\overline{x}) = 1$ says $\cos(2\pi x) + i\sin(2\pi x) = 1$, so $\boxed{\cos(2\pi x) = 1}$ and $\boxed{\sin(2\pi x) = 0}$. The solutions of $\sin t = 0$ in $\mathbf{R}$ are the integral multiples of $\pi$, so $2\pi x = \pi n$ for $n \in \mathbf{Z}$. Thus $x = n/2$, so $x$ is an integer (if $n$ is even) or a half-integer (if $n$ is odd). We want $x$ to be an integer, so we want $n$ to be even.

To $n$ is even, we'll show it's not odd. If $n$ were odd, so $n = 2m+1$ for an integer $m$, then

$$\cos(2\pi x) = \cos(2\pi(n/2)) = \cos(\pi n) = \cos(\pi(2m+1)) = \cos(2\pi m + \pi) = \cos(\pi) = -1,$$

but recall above that $\cos(2\pi x) = 1$. We have a contradiction, so $n$ is even. Thus $x = n/2 \in \mathbf{Z}$, so $\overline{x} = \overline{0}$.

$f$ is surjective. Let $z \in S^1$, so $z \in \mathbf{C}^\times$ with $|z| = 1$. Write $z$ in polar coordinates: $z = r(\cos\theta + i\sin\theta)$ where $r > 0$ and $\theta \in [0, 2\pi)$. Then $|z| = \sqrt{r^2\cos^2\theta + ^2\sin^2\theta} = \sqrt{r^2} = r$, so $r = 1$, and that leaves us with $z = \cos\theta + i\sin\theta = f(\theta/2\pi)$.

**Part 2: Create an isomorphism $\mathbf{R}/\mathbf{Z} \to \mathbf{R}_{>0}/2^{\mathbf{Z}}$.**

Let $f\colon \mathbf{R}/\mathbf{Z} \to \mathbf{R}_{>0}/2^{\mathbf{Z}}$ by $f(\overline{x}) = \overline{2^x}$, meaning $f(x+\mathbf{Z}) = 2^x 2^{\mathbf{Z}}$. (Where does this formula come from? We want to convert addition into multiplication, so the function should involve exponentiation. The real numbers that are trivial in $\mathbf{R}/\mathbf{Z}$ are integers and the positive real numbers that

are trivial in $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ are the integral powers of 2, we want to use an exponential function sending integers to integral powers of 2. The nicest such function is $x \mapsto 2^x$.)

$f$ is well-defined. If $\overline{y} = \overline{x}$ in $\mathbf{R}/\mathbf{Z}$ then $y = x + k$ for some $k \in \mathbf{Z}$, so

$$2^y = 2^{x+k} = 2^x 2^k \in 2^x 2^{\mathbf{Z}} \Longrightarrow \overline{2^y} = \overline{2^x} \text{ in } \mathbf{R}_{>0}/2^{\mathbf{Z}}.$$

$f$ is a homomorphism. For $\overline{x}$ and $\overline{x'}$ in $\mathbf{R}/\mathbf{Z}$,

$$f(\overline{x})f(\overline{x'}) = \overline{2^x}\,\overline{2^{x'}} = \overline{2^x 2^{x'}} = \overline{2^{x+x'}} = f(\overline{x+x'}),$$

so $f$ is a homomorphism.

$f$ is injective. Since $f$ is a homomorphism, it suffices to check $\ker f$ is trivial. If $f(\overline{x}) = \overline{1}$ then $\overline{2^x} = \overline{1}$ in $\mathbf{R}_{>0}/2^{\mathbf{Z}}$, so $2^x \in 2^{\mathbf{Z}}$. Thus $2^x = 2^k$ for some $k \in \mathbf{Z}$, so $x = k$. In $\mathbf{R}/\mathbf{Z}$, $\overline{x} = \overline{k} = \overline{0}$ since $k$ is an integer.

$f$ is surjective. Each element of $\mathbf{R}_{>0}/2^{\mathbf{Z}}$ has the form $\overline{t}$ for some $t > 0$. Every positive real number is a power of 2: $t = 2^x$ some $x \in \mathbf{R}$, so $\overline{t} = \overline{2^x} = f(\overline{x})$. □

**Remark 5.2.** By similar arguments, the group $S^1$ is isomorphic to $\mathbf{R}/a\mathbf{Z}$ for each nonzero real number $a$ and to $\mathbf{R}_{>0}/b^{\mathbf{Z}}$ for each positive number $b \neq 1$.