

3.3 Homomorphisms and Isomorphisms

Section 3.1 named the pattern shared by $(\mathbb{Z}, +)$, the units of a ring and the bijections of a set, and Section 3.2 looked inside one group at a time, at its subgroups. This section compares two groups. A map between groups that respects the two operations is a homomorphism; a bijective one is an isomorphism, and it says that two groups differ only in the names of their elements. The elements a homomorphism sends to the identity form its kernel, a subgroup that measures how much the map forgets.

3.3.1 Maps that respect the operation

Write out the addition table of $\mathbb{Z}/2\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 3.4.2) and the multiplication table of $\{1, -1\} \subseteq \mathbb{Z}$, the group $\mathbb{Z}^\times$ of Proposition 3.1.4:

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	1	-1
1	1	-1
-1	-1	1

Rename [0] as 1 and [1] as -1, and the first table becomes the second, entry for entry. The two groups are the same table with different names. The renaming is a function φ with $\varphi([0]) = 1$ and $\varphi([1]) = -1$, and “entry for entry” says that the entry for a, b is sent to the entry for $\varphi(a), \varphi(b)$: $\varphi(a + b) = \varphi(a)\varphi(b)$. Maps with this property are worth having even when they are not bijections. The map $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, $a \mapsto [a]$, keeps only the parity of an integer, and it still turns sums into sums.

A homomorphism is a map between groups that sends products to products; an isomorphism is a bijective one, a renaming of the elements.

Definition 3.3.1. Group Homomorphism

Let G and H be groups. A function $\varphi: G \rightarrow H$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. A **bijective** homomorphism is an **isomorphism**. The groups G and H are **isomorphic**, written $G \cong H$, if **there exists** an isomorphism $G \rightarrow H$. The **kernel** of φ is

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\},$$

where e_H is the identity of H .

In words: the product ab on the left is taken in G , and the product $\varphi(a)\varphi(b)$ on the right is taken in H . So “ φ respects the operation” compares two different operations, and either group may be written additively. For $\varphi: (\mathbb{Z}/2\mathbb{Z}, +) \rightarrow (\{1, -1\}, \cdot)$ above, the condition reads $\varphi(a + b) = \varphi(a)\varphi(b)$. The kernel is a subset of the **source** G ; the identity it is measured against is that of the **target** H . We write e_G and e_H whenever both groups are in play.

The definition asks for one equation and nothing else. It does not ask that $\varphi(e_G) = e_H$ or that φ respect inverses: both follow, by [Theorem 3.3.1](#) below. This differs from the field homomorphisms of Chapter 2, which must send 1 to 1 by a clause of their own: the map sending every element of a field to 0 respects $+$ and $\cdot$, yet $1 \mapsto 0$. In a group, every element can be canceled, and that is what makes the clause redundant.

Two homomorphisms exist between any two groups, or from any group to itself:

- the **trivial homomorphism** $G \rightarrow H$, $g \mapsto e_H$: since $e_H e_H = e_H$ by (G2), $\varphi(ab) = e_H = \varphi(a)\varphi(b)$. Its kernel is all of G . It forgets everything.
- the **identity** $\text{id}_G: G \rightarrow G$: $\text{id}_G(ab) = ab = \text{id}_G(a)\text{id}_G(b)$. It is bijective (Sets, Relations, and Cardinality, Theorem 1.5.4, with inverse id_G), so it is an isomorphism, and its kernel is $\{e_G\}$. It forgets nothing.

These two extremes are why we say that the kernel measures what φ forgets: the larger $\ker \varphi$, the more elements φ sends to the same place. [Proposition 3.3.3](#) below makes the slogan exact at the end where nothing is forgotten.

The product of two groups. Several examples below have a pair of groups as their target. For groups G and H , take the set $G \times H$ of pairs (Sets, Relations, and Cardinality, Definition 1.3.2) with the operation in each coordinate:

$$(g, h)(g', h') := (gg', hh').$$

This is a binary operation on $G \times H$, since $gg' \in G$ and $hh' \in H$. It makes $G \times H$ a group, the **product** of G and H :

- (G1) For $(g, h), (g', h'), (g'', h'') \in G \times H$, both bracketings give $(gg'g'', hh'h'')$, because (G1) holds in G in the first coordinate and in H in the second.
- (G2) $(e_G, e_H)(g, h) = (e_G g, e_H h) = (g, h)$, and $(g, h)(e_G, e_H) = (g, h)$ in the same way.
- (G3) $(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$, and $(g^{-1}, h^{-1})(g, h) = (e_G, e_H)$ in the same way.

If G and H are abelian, so is $G \times H$, coordinate by coordinate. For abelian groups written additively, the product is written additively too, $(g, h) + (g', h') = (g + g', h + h')$; this is the componentwise sum on $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ of Number Systems: From $\backslash(\backslash n\mathbb{N} \backslash)$ to $\backslash(\backslash n\mathbb{R} \backslash)$, Theorem 3.5.3 (b).

Example. Homomorphisms

Check that each map is a homomorphism, and find its kernel.

- For $n \in \mathbb{Z}_{>0}$, the map $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$, $a \mapsto [a]$.
- For a group G and $g \in G$, the map $(\mathbb{Z}, +) \rightarrow G$, $k \mapsto g^k$. Find its image as well.
- For a group G and $g \in G$, **conjugation by g** , $c_g: G \rightarrow G$, $c_g(x) := gxg^{-1}$. Show that it is an isomorphism, and that it is the identity map exactly when g commutes with every element of G .
- For an **abelian** group G , the map $G \rightarrow G$, $x \mapsto x^2$.
- For $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$, the map $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $[x]_{mn} \mapsto ([x]_m, [x]_n)$, of additive groups. Show that it is an isomorphism.
- The modulus $(\mathbb{C} \setminus \{0\}, \cdot) \rightarrow (\mathbb{R}_{>0}, \cdot)$, $z \mapsto |z|$, where $\mathbb{R}_{>0} := \{x \in \mathbb{R} : x > 0\}$.

Then show that $x \mapsto x + 1$ is **not** a homomorphism $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$.

Solution.

- (a) $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group by Example (Groups) (a). By Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.1 (c), applied to the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Definition 3.4.2), $[a+b] = [a] + [b]$: a homomorphism. By Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.1 (d), $[a] = [0]$ exactly when $a \in n\mathbb{Z}$, so the kernel is $n\mathbb{Z}$. Every element of $\mathbb{Z}/n\mathbb{Z}$ is a class $[a]$, so the map is surjective.
- (b) By Proposition 3.1.3 (a), $g^{k+l} = g^k g^l$ for all $k, l \in \mathbb{Z}$, which is the homomorphism property with $+$ in the source and the product of G in the target. The kernel is $\{k \in \mathbb{Z} : g^k = e_G\}$. The image is $\{g^k : k \in \mathbb{Z}\} = \langle g \rangle$, by Definition 3.2.2. For instance, for the group $G = (\mathbb{Z}/7\mathbb{Z})^\times$ (Proposition 3.1.4) and $g = [3]$, the image is all of $(\mathbb{Z}/7\mathbb{Z})^\times$: the powers $[3]^0, \dots, [3]^5$ are $[1], [3], [2], [6], [4], [5]$, and $[3]^6 = [1]$, so 6 lies in the kernel.
- (c) For $x, y \in G$, inserting $e = g^{-1}g$ between x and y and dropping brackets (Proposition 3.1.2 (b)),

$$c_g(x)c_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = gxyg^{-1} = c_g(xy).$$

So c_g is a homomorphism. Next, since $(g^{-1})^{-1} = g$ (Theorem 3.1.1 (3)),

$$c_{g^{-1}}(c_g(x)) = g^{-1}gxg^{-1}g = x,$$

and in the same way $c_g(c_{g^{-1}}(x)) = gg^{-1}xgg^{-1} = x$. So $c_{g^{-1}}$ is a two-sided inverse of c_g (Sets, Relations, and Cardinality, Definition 1.5.2), and c_g is bijective (Sets, Relations, and Cardinality, Theorem 1.5.4): an isomorphism. Finally, $c_g = \text{id}_G$ means $gxg^{-1} = x$ for every x (Sets, Relations, and Cardinality, Proposition 1.4.1). Multiplying on the right by g turns $gxg^{-1} = x$ into $gx = xg$, and multiplying $gx = xg$ on the right by g^{-1} turns it back. So $c_g = \text{id}_G$ exactly when $gx = xg$ for every $x \in G$. In an abelian group every conjugation is the identity. The kernel of c_g is $\{e\}$: if $gxg^{-1} = e$, then $x = c_{g^{-1}}(e) = g^{-1}eg = e$.

- (d) Since G is abelian, $xy = yx$, and Proposition 3.1.3 (d) gives $(xy)^2 = x^2y^2$. The kernel is $\{x \in G : x^2 = e\}$. In $(\mathbb{Z}/7\mathbb{Z})^\times$ the squares of $[1], \dots, [6]$ are $[1], [4], [2], [2], [4], [1]$, so the kernel is $\{[1], [6]\}$. In $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$ the squares are $[1], [9], [25], [49]$, all equal to $[1]$, so the kernel is the whole group.
- (e) The target is the product of the groups $(\mathbb{Z}/m\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$, written additively. The rule is the map Φ of Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.5.3 (b), a well-defined bijection, and it satisfies $\Phi([x]_{mn} + [y]_{mn}) = \Phi([x]_{mn}) + \Phi([y]_{mn})$ with the componentwise sum, which is the product operation above. So it is an isomorphism of additive groups, and its kernel is $\{[0]_{mn}\}$. For example, $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, since $1 = 4 - 3$ shows $\gcd(3, 4) = 1$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Corollary 3.2.2).
- (f) $\mathbb{C}$ is a field (Theorem 1.2.4), so $(\mathbb{C} \setminus \{0\}, \cdot)$ is a group by Example (Groups) (b). $(\mathbb{R}_{>0}, \cdot)$ is a group by the rules of the ordered field $\mathbb{R}$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 5.3.3): a product of positive reals is positive by (O4), associativity and the identity law are (F5)–(F7), and $1 > 0$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.5 (e)). For $x > 0$ we have $x \neq 0$ by (O1), so x^{-1} exists by (F8), and it is positive by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.5.2 (a). For $z \neq 0$, $|z| \geq 0$ by its definition as a non-negative square root (Definition 1.2.1) and $|z| \neq 0$ by Theorem 1.2.2 (e), so $|z| \in \mathbb{R}_{>0}$. The homomorphism property is $|zw| = |z||w|$, Theorem 1.2.2 (d). The kernel is $\{z \in \mathbb{C} : |z| = 1\} = \mathbb{T}$, the unit circle of Proposition 1.5.1.

The non-example. Let $\varphi(x) := x + 1$. Then $\varphi(0 + 0) = 1$, while $\varphi(0) + \varphi(0) = 2$. So $\varphi(0 + 0) \neq \varphi(0) + \varphi(0)$, and φ is not a homomorphism. It is a minimal change of the identity map $x \mapsto x$, which is one: the shift keeps the map bijective and destroys only the equation.

Part (b) says that every element g of every group is the image of 1 under a homomorphism out of $\mathbb{Z}$. Part (c) gives the first isomorphisms of a group with itself that can differ from the identity: $c_g \neq \text{id}_G$ exactly when g fails to commute with some element of G , as for the two swaps of the fold after Example (Groups) (c), there called f, g : writing h for the second, $c_f(h) = f \circ h \circ f^{-1} \neq h$ because $f \circ h \neq h \circ f$. Part (f) shows a kernel that is not a set of integers.

3.3.2 Basic properties of homomorphisms

The definition asks only for products. Identities, inverses and powers come with them, and kernels and images are subgroups.

Theorem 3.3.1. Basic Properties of Homomorphisms

Let $\varphi: G \rightarrow H$ be a homomorphism of groups, and let $a \in G$.

- (a) $\varphi(e_G) = e_H$.
- (b) $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- (c) $\ker \varphi$ is a subgroup of G .
- (d) $\varphi(a^n) = \varphi(a)^n$ for every $n \in \mathbb{Z}$.
- (e) The image $\varphi(G)$ is a subgroup of H .

Idea. For (a), apply φ to $e_G e_G = e_G$: the equation $\varphi(e_G)\varphi(e_G) = \varphi(e_G)$ has the shape $gg = g$, and **multiply by the inverse** of $\varphi(e_G)$ leaves $\varphi(e_G) = e_H$. For (b), $\varphi(a^{-1})$ undoes $\varphi(a)$, and inverses are unique. Then (c) and (e) are the subgroup test, and (d) is induction along the definition of powers.

Proof.

- (a) Since $e_G e_G = e_G$ by (G2) in G , and $\varphi(e_G) = \varphi(e_G)e_H$ by (G2) in H ,

$$\varphi(e_G)\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) = \varphi(e_G)e_H.$$

Canceling $\varphi(e_G)$ on the left (Theorem 3.1.1 (4)) gives $\varphi(e_G) = e_H$.

- (b) By the homomorphism property, (G3) in G and (a),

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H,$$

and in the same way $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = e_H$. So $\varphi(a^{-1})$ is an inverse of $\varphi(a)$, and since inverses are unique (Theorem 3.1.1 (2)), $\varphi(a^{-1}) = \varphi(a)^{-1}$.

- (c) By (a), $e_G \in \ker \varphi$, so $\ker \varphi \neq \emptyset$. Let $x, y \in \ker \varphi$. By the homomorphism property and (b),

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H,$$

where $e_H^{-1} = e_H$ because $e_H e_H = e_H$ and inverses are unique. So $xy^{-1} \in \ker \varphi$, and $\ker \varphi$ is a subgroup by the subgroup test (Theorem 3.2.1).

- (d) First let $n \in \mathbb{N}$; we use induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, $\varphi(a^0) = \varphi(e_G) = e_H = \varphi(a)^0$ by Definition 3.1.3 and (a). If $\varphi(a^n) = \varphi(a)^n$, then by the recursion $a^{n+1} = a^n a$ of Definition 3.1.3, in G and in H ,

$$\varphi(a^{n+1}) = \varphi(a^n a) = \varphi(a^n) \varphi(a) = \varphi(a)^n \varphi(a) = \varphi(a)^{n+1}.$$

Now let $n < 0$, and write $n = -m$ with $m \in \mathbb{N}$. By Definition 3.1.3, $a^n = (a^{-1})^m$ and $\varphi(a)^n = (\varphi(a)^{-1})^m$. By the case just proved, applied to a^{-1} , and by (b),

$$\varphi(a^n) = \varphi((a^{-1})^m) = \varphi(a^{-1})^m = (\varphi(a)^{-1})^m = \varphi(a)^n.$$

- (e) By Sets, Relations, and Cardinality, Definition 1.6.1, $\varphi(G) = \{\varphi(x) : x \in G\} \subseteq H$. It contains $\varphi(e_G)$, so it is non-empty. For two of its elements $\varphi(x)$ and $\varphi(y)$, with $x, y \in G$, the homomorphism property and (b) give

$$\varphi(x) \varphi(y)^{-1} = \varphi(x) \varphi(y^{-1}) = \varphi(xy^{-1}) \in \varphi(G).$$

So $\varphi(G)$ is a subgroup by Theorem 3.2.1. This proves the theorem. ■

So a homomorphism carries the whole structure of Section 3.1, identity, inverses and powers, and not just the products it was defined by. In additive notation, (a), (b) and (d) read $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$ and $\varphi(n \cdot a) = n \cdot \varphi(a)$. Conversely to [Example \(Homomorphisms\) \(b\)](#), every homomorphism $\varphi: (\mathbb{Z}, +) \rightarrow G$ is $k \mapsto \varphi(1)^k$: $k = k \cdot 1$ (Proposition 3.1.3 (e)), so $\varphi(k) = \varphi(1)^k$ by (d). Part (c) gives a supply of subgroups: the unit circle $\mathbb{T}$ is a subgroup of $\mathbb{C} \setminus \{0\}$ because it is the kernel of the modulus ([Example \(Homomorphisms\) \(f\)](#)), and $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ because it is the kernel of $a \mapsto [a]$.

Quick check. Is $a \mapsto 3a$ a homomorphism $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$? What is its kernel? Is it an isomorphism?

Solution. Yes: $3(a + b) = 3a + 3b$ by distributivity in $\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Theorem 2.3.1). The kernel is $\{0\}$, since $3a = 0$ with $3 \neq 0$ forces $a = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 2.3.5 (f)). It is injective, since $3a = 3b$ gives $3(a - b) = 0$ and so $a = b$ by the same rule, but **not** surjective: 1 is not of the form $3a$, since $3 \nmid 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 3.1.1 (g)). So it is not an isomorphism.

Homomorphisms compose, and the inverse of an isomorphism is again one. These are the facts that let “isomorphic” behave like “equal up to renaming”.

Proposition 3.3.2. Composites and Inverses of Homomorphisms

Let G , H and K be groups.

- (a) If $\varphi: G \rightarrow H$ and $\psi: H \rightarrow K$ are homomorphisms, then so is $\psi \circ \varphi: G \rightarrow K$.

- (b) If $\varphi: G \rightarrow H$ is an isomorphism, then its inverse function $\varphi^{-1}: H \rightarrow G$ is an isomorphism.
- (c) id_G is an isomorphism. Consequently $G \cong G$; if $G \cong H$, then $H \cong G$; and if $G \cong H$ and $H \cong K$, then $G \cong K$.

Idea. Part (a) is the homomorphism property applied twice. For (b), we cannot compute φ^{-1} directly, but we can compare $\varphi^{-1}(xy)$ with $\varphi^{-1}(x)\varphi^{-1}(y)$ after applying φ , which is injective.

Proof.

- (a) For $a, b \in G$, by Sets, Relations, and Cardinality, Definition 1.4.2 and the homomorphism property of φ and then of ψ ,

$$(\psi \circ \varphi)(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).$$

- (b) Since φ is bijective, it has a two-sided inverse φ^{-1} (Sets, Relations, and Cardinality, Theorem 1.5.4), which is bijective by the same theorem, with inverse φ . Let $x, y \in H$. Then, since φ is a homomorphism and $\varphi \circ \varphi^{-1} = \text{id}_H$,

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

Since φ is injective, $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$. So φ^{-1} is a homomorphism, and being bijective, an isomorphism.

- (c) id_G is an isomorphism (the second of the two homomorphisms listed after Definition 3.3.1), so $G \cong G$. If $\varphi: G \rightarrow H$ is an isomorphism, so is $\varphi^{-1}: H \rightarrow G$ by (b). If $\varphi: G \rightarrow H$ and $\psi: H \rightarrow K$ are isomorphisms, then $\psi \circ \varphi$ is a homomorphism by (a) and bijective by Sets, Relations, and Cardinality, Theorem 1.4.4 (c). This proves the proposition. ■

The kernel was introduced to measure what a homomorphism forgets. At the end where it forgets nothing, the measurement is exact:

Proposition 3.3.3. Injective Exactly When the Kernel Is Trivial

A homomorphism $\varphi: G \rightarrow H$ is injective **if and only if** $\ker \varphi = \{e_G\}$.

Idea. Injectivity compares two elements a, b with the same image; the kernel looks at one element with the image e_H . The quotient ab^{-1} turns the first question into the second: $\varphi(a) = \varphi(b)$ says exactly that ab^{-1} lies in the kernel.

Proof. ($\Rightarrow$) Suppose φ is injective. By Theorem 3.3.1 (a), $e_G \in \ker \varphi$. If $g \in \ker \varphi$, then $\varphi(g) = e_H = \varphi(e_G)$, so $g = e_G$ by injectivity. Hence $\ker \varphi = \{e_G\}$.

($\Leftarrow$) Suppose $\ker \varphi = \{e_G\}$, and let $a, b \in G$ with $\varphi(a) = \varphi(b)$. By the homomorphism property and [Theorem 3.3.1](#) (b),

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_H.$$

So $ab^{-1} \in \ker \varphi$, that is, $ab^{-1} = e_G$. **Multiply by the inverse:** multiplying on the right by b and using (G1)–(G3), $a = ab^{-1}b = e_G b = b$. So φ is injective. This proves the proposition. ■

To decide injectivity we now check one equation, $\varphi(g) = e_H$, instead of all pairs a, b . Linear maps in linear algebra satisfy the same statement, with the same proof read additively: *Spaces and Maps*, the chapter “Linear Maps”, proves that a linear map is injective exactly when its kernel is $\{0\}$.

Quick check. Use the proposition to show that $k \mapsto [3]^k$, from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/7\mathbb{Z})^\times$, is not injective.

Solution. It is a homomorphism by [Example \(Homomorphisms\)](#) (b). Its kernel contains 6, since $[3]^6 = [729] = [1]$ ($729 = 104 \cdot 7 + 1$). So the kernel is not $\{0\}$, and by [Proposition 3.3.3](#) the map is not injective; indeed $[3]^0 = [3]^6$.

3.3.3 Isomorphic and non-isomorphic groups

An isomorphism is a renaming, so we expect two isomorphic groups to agree on every property that is stated with the operation alone. For the three properties used here this is a one-line check; let $\varphi: G \rightarrow H$ be an isomorphism. A bijection preserves the number of elements. If G is abelian, then any two elements of H are $\varphi(a), \varphi(b)$, and $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. And $x^2 = e_G$ exactly when $\varphi(x)^2 = e_H$, by the homomorphism property, [Theorem 3.3.1](#) (a) and injectivity, so φ maps the solutions of $x^2 = e$ in G bijectively onto those in H . This gives a method in both directions. To show $G \cong H$, write down a bijection and check the homomorphism property. To show $G \not\cong H$, find such a property that one group has and the other lacks.

Example. Isomorphic and Non-Isomorphic Small Groups

- (a) Show that $(\mathbb{Z}/2\mathbb{Z}, +) \cong (\{1, -1\}, \cdot)$.
- (b) Show that $(\mathbb{Z}/4\mathbb{Z}, +) \cong ((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$, by $[k] \mapsto [2]^k$.
- (c) Show that $(\mathbb{Z}/4\mathbb{Z}, +)$ and $((\mathbb{Z}/8\mathbb{Z})^\times, \cdot)$ are **not** isomorphic.
- (d) Show that $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$, by $x \mapsto 2x$.

Solution.

- (a) By Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, [Theorem 3.4.3](#) (b), each element of $\mathbb{Z}/2\mathbb{Z}$ is $[r]$ for exactly one $r \in \{0, 1\}$, so $\varphi([0]) := 1$, $\varphi([1]) := -1$ defines a function. It is bijective, since it pairs off the two elements. The homomorphism property is the

comparison of the two tables at the start of the section, four equations:

$$\begin{aligned}\varphi([0] + [0]) &= \varphi([0]) = 1 = 1 \cdot 1, & \varphi([0] + [1]) &= \varphi([1]) = -1 = 1 \cdot (-1), \\ \varphi([1] + [0]) &= \varphi([1]) = -1 = (-1) \cdot 1, & \varphi([1] + [1]) &= \varphi([0]) = 1 = (-1)(-1),\end{aligned}$$

using $[1] + [1] = [2] = [0]$ and $(-1)(-1) = 1$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (c)).

- (b) The target is a group by Proposition 3.1.4. Its elements are the four non-zero classes $[1], [2], [3], [4]$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (b), (c)): each is a unit, since $[1][1] = [1]$, $[2][3] = [6] = [1]$ and $[4][4] = [16] = [1]$, while $[0]$ is not, since $[0][v] = [0] \neq [1]$.

Well defined. The rule must not depend on the representative k . The powers $[2]^0, [2]^1, [2]^2, [2]^3, [2]^4$ are $[1], [2], [4], [8] = [3], [16] = [1]$. If $[k] = [k']$ in $\mathbb{Z}/4\mathbb{Z}$, then $k' - k \in 4\mathbb{Z}$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.1 (a)), so $k' = k + 4q$ for some $q \in \mathbb{Z}$, and by Proposition 3.1.3 (a) and (c),

$$[2]^{k'} = [2]^k ([2]^4)^q = [2]^k [1]^q = [2]^k,$$

where $[1]^q = ([2]^0)^q = [2]^{0 \cdot q} = [1]$, again by (c).

Homomorphism. $[k] + [l] = [k + l] \mapsto [2]^{k+l} = [2]^k [2]^l$, by Proposition 3.1.3 (a).

Bijective. The four distinct classes $[0], [1], [2], [3]$, which are all of $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (b)), go to $[1], [2], [4], [3]$: four different elements, which are all of $(\mathbb{Z}/5\mathbb{Z})^\times$. So the map is injective and surjective.

- (c) Both groups have four elements (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (b)). In $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$ (the even classes are not units: $[0]$, and $[2][4] = [4][2] = [6][4] = [0]$ with $[4], [2] \neq [0]$, and a unit is not a zero divisor, the paragraph after Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Definition 3.5.1), every element y has $y^2 = [1]$: the squares are $[1], [9] = [1], [25] = [1], [49] = [1]$. Suppose $\varphi: \mathbb{Z}/4\mathbb{Z} \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ were an isomorphism. Then, by the homomorphism property and Theorem 3.3.1 (a),

$$\varphi([2]) = \varphi([1] + [1]) = \varphi([1])^2 = [1] = \varphi([0]).$$

Since $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$, this contradicts injectivity. So no isomorphism exists.

- (d) $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (Example (Subgroups) (b)), so a group. The map $x \mapsto 2x$ is a homomorphism by distributivity, $2(x + y) = 2x + 2y$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 2.3.1). It is surjective onto $2\mathbb{Z}$ by the definition of $2\mathbb{Z}$, and injective because its kernel is $\{0\}$: $2x = 0$ forces $x = 0$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.5 (f)), and Proposition 3.3.3 applies. So $\mathbb{Z} \cong 2\mathbb{Z}$: a group can be isomorphic to a subgroup of itself other than itself.

The square of Section 3.1, turned by quarter turns, gives another group with four elements; once its rotations are written as permutations, Exercise B3 of Section 3.4 matches them with $\mathbb{Z}/4\mathbb{Z}$.

Warning. Two groups with the same number of elements need not be isomorphic. $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/8\mathbb{Z})^\times$ both have four elements, yet part (c) shows that no isomorphism exists between them. Equal counts decide nothing by themselves: different counts prove $G \not\cong H$, but equal counts never prove $G \cong H$. To prove $G \not\cong H$, find a property that an isomorphism would carry over and that one group has and the other lacks; in (c) it was “some element x has $x^2 \neq e$ ”, which holds in $\mathbb{Z}/4\mathbb{Z}$ (in additive form, $[1] + [1] \neq [0]$) and fails in $(\mathbb{Z}/8\mathbb{Z})^\times$.

Remark (Where homomorphisms go next). In linear algebra, a linear map is in particular a homomorphism of the additive groups, and its kernel is the kernel of this section (*Spaces and Maps*, the chapter “Linear Maps”). The determinant will be a homomorphism from the invertible matrices to $F^\times$ (*Determinants and the Structure of Operators*, the chapter “Determinants”). Quotient groups and the isomorphism theorems are in *Groups*, the chapter “Normal Subgroups, Quotient Groups, and the Isomorphism Theorems”.

Remark (Field homomorphisms as group homomorphisms). In the terms of Chapter 2 (no proof in this chapter rests on this remark): a field homomorphism $\varphi: F \rightarrow L$ (Definition 2.4.1) is a homomorphism of the additive groups $(F, +) \rightarrow (L, +)$; it sends $F^\times$ into $L^\times$, and is a homomorphism of these multiplicative groups (Proposition 2.4.1 (a)–(c)). The automorphisms of F form a group under composition (Proposition 2.4.1 (e)), a subgroup of the group of bijections of F (Example (Groups) (c)). And the multiplicative group $\mathbb{F}_p^\times$ of the field with p elements is the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of Proposition 3.1.4.

3.3.4 Exercises

3.3.4.1 A. Check your understanding

Exercise. A1

- (a) In the proof of $(\Leftarrow)$ of Proposition 3.3.3, where is it used that φ is a homomorphism?
- (b) The map $\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $a \mapsto ([a], [a])$, is a homomorphism of additive groups. Find its kernel.
- (c) True or false: a homomorphism $\varphi: G \rightarrow H$ sends every subgroup K of G onto a subgroup $\varphi(K)$ of H . Justify your answer.
- (d) The map $x \mapsto x + 1$ on $(\mathbb{Z}, +)$ sends 0 to 1. Could it become a homomorphism $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ if 1 were declared the identity of the target, keeping its operation $+$? Explain.

Solution.

- (a) In the first displayed step, $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$: the homomorphism property gives $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1})$, and Theorem 3.3.1 (b), itself a consequence of the homomorphism property, gives $\varphi(b^{-1}) = \varphi(b)^{-1}$. Without it, $\varphi(a) = \varphi(b)$ says nothing about ab^{-1} .
- (b) The map is a homomorphism into the product group, coordinate by coordinate (Example (Homomorphisms) (a) in each coordinate). Its kernel is $\{a : [a]_6 = [0]_6 \text{ and } [a]_4 = [0]_4\} = 6\mathbb{Z} \cap 4\mathbb{Z}$, by Number Systems: From $\mathbb{N}$ to $\mathbb{N}$, Theorem 3.4.1 (d). This is a subgroup of $\mathbb{Z}$ (Proposition 3.2.2), so it is $d\mathbb{Z}$ with d its least positive element (Theorem 3.2.4). The positive multiples of 6 are 6, 12, $\dots$, and $4 \nmid 6$, $4 \mid 12$; so $d = 12$ and the kernel is $12\mathbb{Z}$.
- (c) True. A subgroup K is a group with the operation of G (the paragraph after Definition 3.2.1), and the restriction of φ to K is a homomorphism $K \rightarrow H$, since the homomorphism property for $a, b \in K$ is a special case of that for $a, b \in G$. Its image is $\varphi(K)$, a subgroup of H by Theorem 3.3.1 (e).

- (d) No. The identity of a group is not chosen; it is the element with (G2), and it is unique (Theorem 3.1.1 (1)). In $(\mathbb{Z}, +)$ it is 0, since $1 + 1 \neq 1$. Every homomorphism into $(\mathbb{Z}, +)$ must send 0 to 0 (Theorem 3.3.1 (a)), and $x \mapsto x + 1$ does not. Changing the operation does change the identity: with $a * b := a + b - 1$, the check of Exercise (A1) (b) with -1 in place of $+1$ shows that $(\mathbb{Z}, *)$ is a group: both bracketings of $a * b * c$ equal $a + b + c - 2$, the identity is 1, and the inverse of a is $2 - a$. The map $x \mapsto x + 1$ is a bijection $\mathbb{Z} \rightarrow \mathbb{Z}$ (its inverse is $x \mapsto x - 1$), and $(a + 1) * (b + 1) = (a + b) + 1$, so it is an isomorphism $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, *)$. But that is a different group.

3.3.4.2 B. Practice

Exercise. B1

Find all homomorphisms $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}/6\mathbb{Z}, +)$, and the kernel of each.

Hint: Theorem 3.3.1 (d), applied to $k = k \cdot 1$.

Solution. Let φ be a homomorphism and write $\varphi(1) = [c]$ with $c \in \{0, \dots, 5\}$ (Number Systems: From $(\mathbb{N})$ to $(\mathbb{N})$, Theorem 3.4.3 (b)). For $k \in \mathbb{Z}$, $k = k \cdot 1$ in $(\mathbb{Z}, +)$ (Proposition 3.1.3 (e)), so Theorem 3.3.1 (d), in additive notation, gives

$$\varphi(k) = \varphi(k \cdot 1) = k \cdot \varphi(1) = k \cdot [c].$$

So φ is determined by c . Conversely, for each c , the map $k \mapsto k \cdot [c]$ is a homomorphism by Example (Homomorphisms) (b) with $g = [c]$. So there are exactly six homomorphisms, one for each class $[c]$.

Kernels. The quotient map $a \mapsto [a]$ is a homomorphism (Example (Homomorphisms) (a)), so Theorem 3.3.1 (d) and Proposition 3.1.3 (e) give $k \cdot [c] = [k \cdot c] = [kc]$. Hence, since $[kc] = [0]$ exactly when $kc \in 6\mathbb{Z}$ (Number Systems: From $(\mathbb{N})$ to $(\mathbb{N})$, Theorem 3.4.1 (d)), the kernel is $\{k \in \mathbb{Z} : 6 \mid kc\}$, a subgroup of $\mathbb{Z}$, so it is $d\mathbb{Z}$ with d the least positive k with $6 \mid kc$ (Theorem 3.2.4). Running through $k = 1, 2, \dots$:

c	0	1	2	3	4	5
least k with $6 \mid kc$	1	6	3	2	3	6
kernel	$\mathbb{Z}$	$6\mathbb{Z}$	$3\mathbb{Z}$	$2\mathbb{Z}$	$3\mathbb{Z}$	$6\mathbb{Z}$

For instance, for $c = 4$: 4, 8 are not multiples of 6, and 12 is. For $c = 5$: 5, 10, 15, 20, 25 are not, and 30 is.

Exercise. B2

- (a) Let G and H be groups. Show that $G \rightarrow G \times H$, $g \mapsto (g, e_H)$, is an injective homomorphism into the product group.
- (b) Show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ (additive groups) are not isomorphic.

Solution.

- (a) For $g, g' \in G$, $(gg', e_H) = (gg', e_H e_H) = (g, e_H)(g', e_H)$, by (G2) in H and the definition of the product operation. The kernel is $\{g : (g, e_H) = (e_G, e_H)\} = \{e_G\}$, since two pairs are equal exactly when their coordinates are. By Proposition 3.3.3 the map is injective.
- (b) The invariant is that of Example (Isomorphic and Non-Isomorphic Small Groups) (c). In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, every element satisfies $x + x = 0$: $([a], [b]) + ([a], [b]) = ([2a], [2b]) = ([0], [0])$. Suppose $\varphi: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ were an isomorphism. Then

$$\varphi([2]) = \varphi([1] + [1]) = \varphi([1]) + \varphi([1]) = ([0], [0]) = \varphi([0])$$

by Theorem 3.3.1 (a), against injectivity, since $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$. An isomorphism in the other direction would have an inverse that is an isomorphism (Proposition 3.3.2 (b)), so it cannot exist either.

Exercise. B3

Give an example of a homomorphism from $(\mathbb{Q} \setminus \{0\}, \cdot)$ **onto** $(\{1, -1\}, \cdot)$, and find its kernel.

Solution. *What any answer must have.* A function $\varphi: \mathbb{Q} \setminus \{0\} \rightarrow \{1, -1\}$ with $\varphi(xy) = \varphi(x)\varphi(y)$ for all non-zero x, y , taking **both** values 1 and -1 . Its kernel is then a subgroup (Theorem 3.3.1 (c)) that is not the whole group.

One answer: the sign. Let $\varphi(x) := 1$ if $x > 0$ and $\varphi(x) := -1$ if $x < 0$. This defines a function on $\mathbb{Q} \setminus \{0\}$, since the order of $\mathbb{Q}$ is total (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1; Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (i)). By the rules of the ordered field $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (c), (d)), the product of two positives is positive, of a positive and a negative is negative, and of two negatives is positive. In each of the four cases $\varphi(xy) = \varphi(x)\varphi(y)$: for example, if $x > 0 > y$, then $xy < 0$ and $\varphi(xy) = -1 = 1 \cdot (-1)$. Both values are taken, at 1 and -1 . The kernel is $\mathbb{Q}_{>0}$.

Other answers exist. For instance, writing a non-zero rational as $\pm 2^k a/b$ with a, b odd, the parity of k gives another one; we do not prove that this is well defined here.

3.3.4.3 C. Going deeper

Exercise. C1

- (a) Let $\varphi: G \rightarrow H$ be a homomorphism, with G abelian. Prove that the subgroup $\varphi(G)$ of H is abelian.
- (b) Deduce that there is no homomorphism from $\mathbb{Z}/6\mathbb{Z}$ **onto** the group of bijections of $\{1, 2, 3\}$.

Solution.

- (a) Let $u, v \in \varphi(G)$, say $u = \varphi(a)$ and $v = \varphi(b)$ with $a, b \in G$ (Sets, Relations, and

Cardinality, Definition 1.6.1). Then

$$uv = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = vu,$$

using that G is abelian in the middle step.

- (b) $\mathbb{Z}/6\mathbb{Z}$ is abelian (Example (Groups) (a)). If φ were a homomorphism from it onto the group of bijections of $\{1, 2, 3\}$, then that group would be $\varphi(\mathbb{Z}/6\mathbb{Z})$, abelian by (a). It is not: the bijections f swapping 1, 2 and g swapping 2, 3 satisfy $(f \circ g)(1) = f(1) = 2$ and $(g \circ f)(1) = g(2) = 3$, as in the fold after Example (Groups) (c). So no such homomorphism exists. (Size alone could not decide this: Section 3.4 shows that both groups have six elements.)

Marking scheme. (10 points) - 2: (a) writes arbitrary $u, v \in \varphi(G)$ as $\varphi(a), \varphi(b)$. - 3: (a) the chain $uv = \varphi(ab) = \varphi(ba) = vu$, with the homomorphism property and commutativity of G named. - 1: (b) notes that $\mathbb{Z}/6\mathbb{Z}$ is abelian. - 1: (b) “onto” makes the target equal to $\varphi(\mathbb{Z}/6\mathbb{Z})$, so (a) applies. - 3: (b) exhibits two bijections of $\{1, 2, 3\}$ that do not commute, with a point where the two composites differ. Fatal errors (0 for the step): (a) takes u, v in all of H rather than in the image; (b) argues from the number of elements alone.

Exercise. C2

Let $\varphi: G \rightarrow H$ be a homomorphism and $a, b \in G$.

- Prove that the following are equivalent: (i) $\varphi(a) = \varphi(b)$; (ii) $ab^{-1} \in \ker \varphi$; (iii) $a^{-1}b \in \ker \varphi$.
- Deduce that the set of elements with the same image as a , the **fiber** $\varphi^{-1}(\{\varphi(a)\})$, equals $\{ak : k \in \ker \varphi\}$.
- For the quotient map $\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$, $x \mapsto [x]$, write out the fiber of 7.

Solution.

- $\Rightarrow$ (ii): as in the proof of [Proposition 3.3.3](#), $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_H$.
 - $\Rightarrow$ (i): if $\varphi(ab^{-1}) = e_H$, then $\varphi(a)\varphi(b)^{-1} = e_H$; multiplying on the right by $\varphi(b)$, $\varphi(a) = \varphi(b)$.
 - $\Leftrightarrow$ (iii): the same two arguments with $a^{-1}b$: $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$ ([Theorem 3.3.1](#) (b)), which is e_H exactly when $\varphi(b) = \varphi(a)$, multiplying on the left by $\varphi(a)$ or by $\varphi(a)^{-1}$.
- ($\subseteq$) Let b lie in the fiber, so $\varphi(b) = \varphi(a)$. By (a), $k := a^{-1}b \in \ker \varphi$, and $b = a(a^{-1}b) = ak$. ($\supseteq$) If $k \in \ker \varphi$, then $\varphi(ak) = \varphi(a)e_H = \varphi(a)$.
- The kernel is $5\mathbb{Z}$ ([Example \(Homomorphisms\)](#) (a)), so by (b) the fiber of 7 is $\{7 + 5j : j \in \mathbb{Z}\} = \{\dots, -3, 2, 7, 12, \dots\}$, the class $[7] = [2]$ itself. The sets $\{ak : k \in \ker \varphi\}$ are the **cosets** of the kernel, which *Groups*, the chapter “Cosets and Lagrange’s Theorem”, studies for every subgroup.

Marking scheme. (10 points) - 2: (a) (i) $\Rightarrow$ (ii), using $\varphi(b^{-1}) = \varphi(b)^{-1}$, cited. - 2: (a) (ii) $\Rightarrow$ (i), multiplying by $\varphi(b)$ on the right. - 2: (a) (i) $\Leftrightarrow$ (iii), both directions, by the mirror argument. - 2: (b) both inclusions, with $k := a^{-1}b$ for ($\subseteq$). - 2: (c) kernel $5\mathbb{Z}$, and the fiber

$\{7 + 5j : j \in \mathbb{Z}\}$. Fatal errors (0 for the step): (a) “divides” by $\varphi(b)$, or uses commutativity of H ; (b) proves one inclusion and calls it equality.