Group homomorphisms

Definition

Definition 1

A function $\varphi : (G, \star) \to (H, \bullet)$ *between groups is called a* **group homomorphism** *means for every* $g_1, g_2 \in G$*,*

$$\varphi(g_1 \star g_2) = \varphi(g_1) \bullet \varphi(g_2).$$

In other words, a group homomorphism keeps the group operation consistent between the source and the target.

Exercise 1 (cf. Problem 62)

Which of the following are group homomorphisms? (What are the implied operations?)

(a) $\phi_1 : \mathbb{R} \to \mathbb{R}$ via $\phi_1 : a \mapsto a^2$

(b) $\phi_2 : \mathbb{Q} \to \mathbb{Q}$ via $\phi_2 : a \mapsto a + 10$

(c) $\phi_3 : \mathbb{Z} \to \mathbb{Z}$ via $\phi_3 : a \mapsto 6a$.

(d) $\delta : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^\times$ via

$$\delta : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc.$$

Isomorphisms

Recall, from Section **??**, what it means for a function to be one-to-one (injective) or onto (surjective).

When a function is both injective and surjective, it is called **bijective**. We say there is a **one-to-one correspondence** between the source and the target.

Definition 2

A bijective homomorphism is called an **isomorphism***. The source and target are said to be* **isomorphic***.*

Exhibiting a group isomorphism demonstrates that the source and target are really the "same" group, with different names.

Example 1

Define the exponential function

$$E : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$$
$$a \mapsto e^a,$$

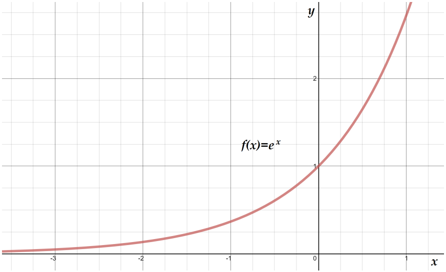
where $\mathbb{R}^+$ denotes the set of positive real numbers and $e \approx 2.71928$ is the Euler number.

Claim. E gives a bijection between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$. In other words, $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ are isomorphic as groups, and we write:

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$$

Proof: When exhibiting an isomorphism, make sure to verify it is well-defined – i.e., is $E : \mathbb{R} \to \mathbb{R}^+$ truly a group homomorphism?

- Recall, from Precalculus courses, the exponential function is always positive and passes the "vertical line test" (see the figure below). So E is a function.



Exponential function drawn using `https://www.desmos.com/calculator`.

- Suppose $a, b \in \mathbb{R}$. Then $e^{a+b} = e^a \cdot e^b$ implies $E(a+b) = E(a) \cdot E(b)$, the requirement for E to be a group homomorphism.

Now we check E is one-to-one. Suppose there exist $a, b \in \mathbb{R}$ such that $E(a) = E(b)$. Then

$$\begin{aligned} e^a &= e^b \\ \implies \ln\left(e^a\right) &= \ln\left(e^b\right) \\ \implies a &= b, \end{aligned}$$

as required.

Finally, we must check E is onto; if $x \in \mathbb{R}^+$ then we must show there exists $a \in \mathbb{R}$ such that $E(a) = x$. One common technique is to define an **inverse** function for E. Define

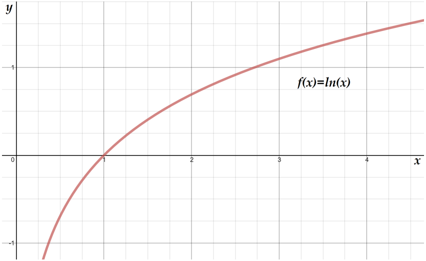
$$\begin{aligned} L : \mathbb{R}^+ &\to \mathbb{R} \\ x &\mapsto \ln x. \end{aligned}$$

If we put $a = \ln x$ for fixed $x \in \mathbb{R}^+$ then

$$E(a) = E(\ln x) = e^{\ln x} = x$$

and we are done – provided L is well-defined.

Again, from Precalculus, we know the natural logarithm function is well-defined (see figure below); log algebra then shows for $x, y \in \mathbb{R}^+$, $\ln(xy) = \ln x + \ln y$, meaning $L(xy) = L(x) + L(y)$ and hence L is a group homormorphism.



Natural logarithm function drawn using `https://www.desmos.com/calculator`.

$\square$

Proposition 1

Let $\varphi : G \to H$ denote a group homomorphism where the identities of G and H, respectively, are 1_G and 1_H. Then $\varphi(1_G) = 1_H$.

$\square$

Exercise 2

Verify Proposition 1 for Example 1.

Proposition 2

Let p and q be relatively prime numbers. Then

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

$\square$

Exercise 3

Prove Proposition 2.

Exercise 4 (cf. Problem 64)

Prove $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/8\mathbb{Z}$.

Kernels and images

One can show (see Exercise 5) that the image of a group homomorphism is a subgroup of the target. The source also has an important related subgroup.

Definition 3

Let $\varphi : G \to H$ denote a group homomorphism where 1_G and 1_H are the respective identity elements in G and H.

(a) *The* **kernel** *of φ, denoted $\ker(\varphi)$, is the set of all elements in G mapped to the identity in H:*

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\}$$

(b) *The* **image** *of φ is the set of all elements in H of the form $\varphi(g)$ for some $g \in G$:*

$$\operatorname{image}(\varphi) := \{h \in H \mid h = \varphi(g) \text{ for some } g \in G\}.$$

Exercise 5 (cf. Problem 65)

Let $\varphi : G \to H$ denote a group homomorphism. Prove $\ker \varphi < G$ and $\operatorname{image} \varphi < H$.

Example 2

This example motivates the content of Section **??**. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}_n \\ m &\mapsto m \pmod{n} \end{aligned}$$

where $m \pmod{n}$ is the remainder of m upon division by n.

Question

Why is φ a well-defined function?

Claim. φ is a (group) homomorphism.

Proof: Suppose $m_1, m_2 \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers q and r, with $0 \leq r < n$, such that

$$\begin{aligned} (m_1 + m_2) &= nq + r \\ \implies r &= (m_1 + m_2) - nq \\ &\equiv (m_1 + m_2) \pmod{n} \\ &= \varphi(m_1 + m_2). \end{aligned}$$

Apply the Division Algorithm to m_1, m_2 as well, so that there exist unique integers q_1, q_2 and r_1, r_2, with $0 \leq r_1, r_2 < n$, such that

$$\begin{aligned} m_1 &= nq_1 + r_1 \\ \implies r_1 &= m_1 - nq_1 \\ &\equiv m_1 \pmod{n} \\ &= \varphi(m_1). \end{aligned}$$

$$\begin{aligned} m_2 &= nq_2 + r_2 \\ \implies r_2 &= m_2 - nq_2 \\ &\equiv m_2 \pmod{n} \\ &= \varphi(m_2). \end{aligned}$$

Now apply the Division Algorithm to get unique integers p, s, with $0 \leq s < n$ such that

$$\begin{aligned} np + s &= (\varphi(m_1) + \varphi(m_2)) \equiv s \pmod{n} \\ &= (m_1 - nq_1) + (m_2 - nq_2) \\ &= (m_1 + m_2) - n(q_1 + q_2) \end{aligned}$$

by associativity. Rearranging,

$$m_1 + m_2 = s + n(p + q_1 + q_2).$$

The uniqueness condition of the Division Algorithm says that $s = r$, because $0 \leq s < n$. Therefore

$$\varphi(m_1 + m_2) = r = s \equiv s \pmod{n} = \varphi(m_1) + \varphi(m_2).$$

$\square$

Claim. φ is not injective.

Proof: We exhibit two distinct elements in $\mathbb{Z}$ with the same image. Take $n-1 \in \mathbb{Z}$ and $(n-1)+n \in \mathbb{Z}$. Note, from Definition **??**, $n \neq 0$, so $n-1 \neq (n-1)+n$. Since $n-1 < n$, we have

$$\varphi(n-1) = n-1 \pmod{n} = n-1.$$

By the uniqueness condition in the Division Algorithm, we have

$$\begin{aligned}\varphi((n-1)-n) &= (n-1)+n(-1)\\ &= (n-1) \pmod{n}\\ &= n-1.\end{aligned}$$

$\square$

Claim. φ is surjective.

Proof: $\mathbb{Z}/n\mathbb{Z}$ consists of non-negative integers strictly less than n, which are also in $\mathbb{Z}$. If $m \in \mathbb{Z}/n\mathbb{Z}$, then

$$m = m \pmod{n} = \varphi(m).$$

$\square$

Question

What are $\ker(\varphi)$ and $\operatorname{image}(\varphi)$?