Groups1stIso

Kai Ogden Hongyu Wang

June 25, 2025

The First Isomorphism Theorem for Groups: A Formal Proof from Axioms

0.1 Fundamental Definitions

Definition 1 (Group)**.** A **group** is an ordered pair $(G, \cdot)$, where G is a set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. **Associativity:** For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. **Identity Element:** There exists an element $e \in G$, called the identity element, such that for all $a \in G$, we have $a \cdot e = e \cdot a = a$.
3. **Inverse Element:** For each $a \in G$, there exists an element $a^{-1} \in G$, called the inverse of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 2 (Subgroup)**.** Let $(G, \cdot)$ be a group. A subset H of G is a **subgroup** of G, denoted $H \leq G$, if $(H, \cdot)$ is itself a group. This is equivalent to the following conditions:

1. H is non-empty.
2. For all $a, b \in H$, $a \cdot b \in H$ (closure).
3. For all $a \in H$, $a^{-1} \in H$ (closure under inverses).

Definition 3 (Group Homomorphism)**.** Let $(G, \cdot_G)$ and $(H, \cdot_H)$ be groups. A function $\phi : G \to H$ is a **group homomorphism** if for all $a, b \in G$, we have:

$$\phi(a \cdot_G b) = \phi(a) \cdot_H \phi(b)$$

Definition 4 (Kernel of a Homomorphism)**.** Let $\phi : G \to H$ be a group homomorphism. The **kernel** of ϕ, denoted $\ker(\phi)$, is the set of elements in G that are mapped to the identity element in H.

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$$

Definition 5 (Image of a Homomorphism)**.** Let $\phi : G \to H$ be a group homomorphism. The **image** of ϕ, denoted $\operatorname{im}(\phi)$, is the set of elements in H that are the image of some element in G.

$$\operatorname{im}(\phi) = \{h \in H \mid \exists g \in G, \phi(g) = h\}$$

Definition 6 (Normal Subgroup)**.** A subgroup N of a group G is a **normal subgroup**, denoted $N \trianglelefteq G$, if for all $g \in G$ and for all $n \in N$, we have $gng^{-1} \in N$.

Definition 7 (Coset)**.** Let H be a subgroup of a group G. For any $g \in G$, the **left coset** of H in G with respect to g is the set $gH = \{gh \mid h \in H\}$.

Definition 8 (Quotient Group)**.** Let N be a normal subgroup of a group G. The **quotient group** (or factor group) of G by N, denoted G/N, is the set of all left cosets of N in G, with the binary operation defined by:

$$(aN)(bN) = (ab)N$$

for all $a, b \in G$.

0.2 Preliminary Lemmas

Lemma 9 (Properties of Homomorphisms)**.** *Let $\phi : G \to H$ be a group homomorphism. Then:*

1. $\phi(e_G) = e_H$.
2. $\phi(g^{-1}) = (\phi(g))^{-1}$ *for all* $g \in G$.

Proof.
1. We have $\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) \cdot \phi(e_G)$. Multiplying by $(\phi(e_G))^{-1}$ on the right in H, we get $\phi(e_G)(\phi(e_G))^{-1} = (\phi(e_G)\phi(e_G))(\phi(e_G))^{-1}$, which simplifies to $e_H = \phi(e_G)$.
2. For any $g \in G$, we have $e_H = \phi(e_G) = \phi(g \cdot g^{-1}) = \phi(g) \cdot \phi(g^{-1})$. Multiplying on the left by $(\phi(g))^{-1}$, we get $(\phi(g))^{-1} \cdot e_H = (\phi(g))^{-1} \cdot (\phi(g) \cdot \phi(g^{-1}))$, which simplifies to $(\phi(g))^{-1} = \phi(g^{-1})$.

□

Lemma 10 (The Kernel is a Subgroup)**.** *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker(\phi)$ *is a subgroup of G.*

Proof. We verify the three conditions from Definition 2.

1. By Lemma 9, $\phi(e_G) = e_H$, so $e_G \in \ker(\phi)$. Thus, $\ker(\phi)$ is non-empty.
2. Let $a, b \in \ker(\phi)$. Then $\phi(a) = e_H$ and $\phi(b) = e_H$. Using the homomorphism property from Definition 3, we have $\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H$. Thus, $ab \in \ker(\phi)$.
3. Let $a \in \ker(\phi)$. Then $\phi(a) = e_H$. By Lemma 9, $\phi(a^{-1}) = (\phi(a))^{-1} = (e_H)^{-1} = e_H$. Thus, $a^{-1} \in \ker(\phi)$.

Since all three conditions are satisfied, $\ker(\phi)$ is a subgroup of G. □

Lemma 11 (The Kernel is a Normal Subgroup)**.** *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker(\phi)$ *is a normal subgroup of G.*

Proof. By Lemma 10, we know that $K = \ker(\phi)$ is a subgroup of G. We now show it is normal. Let $k \in K$ and $g \in G$. We need to show that $gkg^{-1} \in K$. By the definition of the kernel (Definition 4), $\phi(k) = e_H$. Using the homomorphism property (Definition 3) and Lemma 9:

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_H(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e_H$$

Thus, $gkg^{-1} \in K$. Therefore, $\ker(\phi)$ is a normal subgroup of G. □

Lemma 12 (The Image is a Subgroup)**.** *Let $\phi : G \to H$ be a group homomorphism. Then im(ϕ) is a subgroup of H.*

Proof. We verify the three conditions from Definition 2.

1. By Lemma 9, $\phi(e_G) = e_H$, so $e_H \in \mathrm{im}(\phi)$. Thus, $\mathrm{im}(\phi)$ is non-empty.
2. Let $h_1, h_2 \in \mathrm{im}(\phi)$. By Definition 5, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$. Since $g_1 g_2 \in G$, $h_1 h_2 \in \mathrm{im}(\phi)$.
3. Let $h \in \mathrm{im}(\phi)$. Then there exists $g \in G$ such that $\phi(g) = h$. By Lemma 9, $h^{-1} = (\phi(g))^{-1} = \phi(g^{-1})$. Since $g^{-1} \in G$, $h^{-1} \in \mathrm{im}(\phi)$.

Since all three conditions are satisfied, $\mathrm{im}(\phi)$ is a subgroup of H. □

0.3 The First Isomorphism Theorem

Theorem 13 (First Isomorphism Theorem for Groups)**.** *Let $\phi : G \to H$ be a group homomorphism. Then the quotient group $G/\ker(\phi)$ is isomorphic to the image of ϕ, im(ϕ).*

$$G/\ker(\phi) \cong im(\phi)$$

Proof. Let $K = \ker(\phi)$. By Lemma 11, K is a normal subgroup of G, so the quotient group G/K is well-defined. By Lemma 12, $\text{im}(\phi)$ is a subgroup of H.

We define a map $\psi : G/K \to \text{im}(\phi)$ by $\psi(gK) = \phi(g)$ for any coset $gK \in G/K$. To prove the theorem, we must show that ψ is well-defined, is a homomorphism, is injective, and is surjective.

1. ψ is well-defined: We need to show that if $aK = bK$ for $a, b \in G$, then $\psi(aK) = \psi(bK)$. If $aK = bK$, then $b^{-1}a \in K$. By the definition of the kernel (Definition 4), $\phi(b^{-1}a) = e_H$. Using the homomorphism properties (Definition 3 and Lemma 9), we have:

$$\phi(b^{-1})\phi(a) = e_H$$

$$(\phi(b))^{-1}\phi(a) = e_H$$

Multiplying on the left by $\phi(b)$ gives:

$$\phi(a) = \phi(b)$$

By our definition of ψ, this means $\psi(aK) = \psi(bK)$. Thus, ψ is well-defined.

2. ψ is a homomorphism: We need to show that for any two cosets $aK, bK \in G/K$, we have $\psi((aK)(bK)) = \psi(aK)\psi(bK)$. Using the definition of the operation in a quotient group (Definition 8) and the definition of a homomorphism (Definition 3):

$$\psi((aK)(bK)) = \psi((ab)K) = \phi(ab) = \phi(a)\phi(b) = \psi(aK)\psi(bK)$$

Thus, ψ is a group homomorphism.

3. ψ is injective (one-to-one): We need to show that if $\psi(aK) = \psi(bK)$, then $aK = bK$. Suppose $\psi(aK) = \psi(bK)$. By the definition of ψ, this means $\phi(a) = \phi(b)$. Multiplying on the left by $(\phi(a))^{-1}$:

$$(\phi(a))^{-1}\phi(b) = e_H$$

Using the homomorphism properties (Lemma 9):

$$\phi(a^{-1})\phi(b) = e_H$$

$$\phi(a^{-1}b) = e_H$$

By the definition of the kernel (Definition 4), this implies $a^{-1}b \in K$. This is the condition for the cosets to be equal: $aK = bK$. Thus, ψ is injective.

4. ψ is surjective (onto): We need to show that for any element $h \in \text{im}(\phi)$, there exists a coset $gK \in G/K$ such that $\psi(gK) = h$. Let $h \in \text{im}(\phi)$. By the definition of the image (Definition 5), there exists some $g \in G$ such that $\phi(g) = h$. Consider the coset $gK \in G/K$. Then $\psi(gK) = \phi(g) = h$. Thus, for any $h \in \text{im}(\phi)$, we have found a coset in G/K that maps to it. Therefore, ψ is surjective.

Since ψ is a well-defined, bijective homomorphism, it is an isomorphism. We have thus shown that $G/\ker(\phi) \cong \text{im}(\phi)$. $\square$