10 Group Homomorphisms

■ Definition: Group Homomorphism

Let G and $\bar{G}$ be groups. A mapping $\varphi : G \to \bar{G}$ is called a **group homomorphism** if for all $a, b \in G$: $\varphi(ab) = \varphi(a)\varphi(b)$.

Terminology:

- If φ is both a homomorphism and **one-to-one**, it is a **monomorphism**
- If φ is both a homomorphism and **onto**, it is an **epimorphism**
- If φ is both a homomorphism and **bijective**, it is an **isomorphism**
- A homomorphism from a group to itself is called an **endomorphism**
- An isomorphism from a group to itself is called an **automorphism**

■ Definition: Kernel of a Homomorphism

Let $\varphi : G \to \bar{G}$ be a group homomorphism. The **kernel** of φ, denoted $\mathrm{Ker}\ \varphi$, is the set: $\mathrm{Ker}\ \varphi = \{g \in G \mid \varphi(g) = \bar{e}\}$. where $\bar{e}$ is the identity element of $\bar{G}$.

Interpretation:

- The kernel consists of all elements in G that map to the identity in $\bar{G}$
- The kernel measures "how far" φ is from being one-to-one
- $\mathrm{Ker}\ \varphi = \{e\}$ if and only if φ is a monomorphism (one-to-one)

Notation: $\mathrm{Ker}\ \varphi$ (most common). $\mathbf{ker}\ \varphi$ (lowercase also used). Sometimes $\mathbf{ker}(\varphi)$ or $\mathrm{kernel}(\varphi)$.

■ EXAMPLE 1: Every Isomorphism is a Homomorphism

Explanation: By definition, an isomorphism $\varphi : G \to \bar{G}$ satisfies $\varphi(ab) = \varphi(a)\varphi(b)$

- This is precisely the homomorphism property
- Additionally, isomorphisms are bijective (one-to-one and onto)

Kernel Analysis: For any isomorphism $\varphi : G \to \bar{G}$

- $\text{Ker}\ \varphi = \{e\}$ where e is the identity of G
- **Proof:** If $\varphi(g) = \bar{e}$, and φ is one-to-one, then $g = e$

Key Insight: A homomorphism is an isomorphism $\iff$ it is bijective $\iff$ $\text{Ker}\ \varphi = \{e\}$ and φ is onto.

■ EXAMPLE 2: The Determinant Homomorphism:

The determinant mapping $\varphi : GL(2,\mathbb{R}) \to \mathbb{R}^*$: $\varphi(A) = \det(A)$ for any matrix $A \in GL(2,\mathbb{R})$ is a group homomorphism. **Where:**

- $G = GL(2,\mathbb{R}) = \{2 \times 2 \text{ invertible real matrices}\}$ under matrix multiplication
- $\bar{G} = \mathbb{R}^* = \{\text{nonzero real numbers}\}$ under multiplication

Verification of Homomorphism Property: For any matrices $A, B \in GL(2,\mathbb{R})$:
$\varphi(AB) = \det(AB) = \det(A) \cdot \det(B) = \varphi(A)\varphi(B)$, This is a fundamental property from linear algebra.

Kernel Calculation: $\mathrm{Ker}(\det) = \{A \in GL(2,\mathbb{R}) \mid \det(A) = 1\} = SL(2,\mathbb{R})$. This is the **special linear group.**

Properties:

- $\det$ is **onto** (surjective): every nonzero real number is the determinant of some matrix
- $\det$ is **not one-to-one**: many matrices have the same determinant
- The kernel $SL(2,\mathbb{R})$ is a normal subgroup of $GL(2,\mathbb{R})$

■ EXAMPLE 3: Absolute Value Homomorphism

The absolute value mapping $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $\varphi(x) = |x|$ is a group homomorphism.

Verification: The absolute value preserves multiplication: $|xy| = |x| \cdot |y|$

Kernel: $\operatorname{Ker} \varphi = \{x \in \mathbb{R}^* \mid |x| = 1\} = \{-1, 1\}$

Note: If we consider $\mathbb{R}$ under **addition**, then $\varphi(x) = |x|$ is **NOT** a homomorphism because:

- $\varphi(2 + (-3)) = \varphi(-1) = 1 \neq \varphi(2) + \varphi(-3) = 2 + 3 = 5$

■ EXAMPLE 4: The Derivative Operator

Let $G = \{f \mid f : \mathbb{R} \to \mathbb{R} \text{ is a differentiable function}\}$ under function addition.
The derivative mapping $\varphi(f) = f'$ is a group homomorphism from G to itself.

Verification: For any differentiable functions f, g:
$\varphi(f+g) = (f+g)' = f' + g' = \varphi(f) + \varphi(g)$. This is the **sum rule** from calculus.

Kernel Calculation: $\mathrm{Ker}\ \varphi = \{f \in G \mid f' = 0\}$

These are precisely the **constant functions**: $\mathrm{Ker}\ \varphi = \{f(x) = c \mid c \in \mathbb{R}\}$

Additional Properties:

- This homomorphism is **onto** (every function is the derivative of some function)
- This homomorphism is **not one-to-one** (many functions have the same derivative)
- The kernel (constant functions) forms a normal subgroup.

Generalization:

- This extends to polynomial rings: $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$
- For polynomials, $\mathrm{Ker}\ \varphi = \{\text{constant polynomials}\} \cong \mathbb{R}$

■ EXAMPLE 8: The Squaring Function

The mapping $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $\varphi(x) = x^2$ is a group homomorphism when $\mathbb{R}^*$ has multiplication as its operation.

Verification: For $\varphi(xy) = \varphi(x)\varphi(y)$ because $(xy)^2 = x^2 \cdot y^2$.

Where Squaring Fails: If we consider $(\mathbb{R}, +)$ under addition:

- $\varphi(x + y) = (x + y)^2 = x^2 + 2xy + y^2$
- $\varphi(x) + \varphi(y) = x^2 + y^2$
- These are NOT equal (unless $xy = 0$)
  - $\varphi(x) = x^2$ IS a homomorphism from $(\mathbb{R}^*, \cdot)$ to $(\mathbb{R}^*, \cdot)$
  - $\varphi(x) = x^2$ is NOT a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$
  - The group operation determines whether a map is a homomorphism

Well-Defined Mappings

Caution: When defining a homomorphism from a group with multiple element representations, ensure the correspondence is a function.

Example: The mapping $x + \langle 3 \rangle \to 3x$ from $Z/\langle 3 \rangle$ to Z is NOT well-defined:

- $0 + \langle 3 \rangle = 3 + \langle 3 \rangle$ in $Z/\langle 3 \rangle$
- But $3 \cdot 0 \neq 3 \cdot 3$ in Z

Linear Algebra Connection: Every linear transformation is a group homomorphism.

Theorem 10.1: Properties of Homomorphisms w.r.t elements

Let ϕ be a homomorphism from G to G' and let $g \in G$. Then:

1. ϕ carries the identity of G to the identity of G' **(If e is the identity in G, then $\phi(e)$ is the identity in G')**
2. $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$ **(Homomorphisms preserve powers)**
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$ **(The order of an image divides the order of the element)**
4. Ker ϕ is a subgroup of G **(The kernel forms a subgroup)**
5. $\phi(a) = \phi(b)$ if and only if $a \text{ Ker } \phi = b \text{ Ker } \phi$ **(Elements have the same image if and only if they're in the same coset of Ker ϕ)**
6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \text{ Ker } \phi$ **(The inverse image of an element is a coset of the kernel)**

Theorem 10.2: Properties of Subgroups Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ *is a subgroup of* $\overline{G}$.
2. *If H is cyclic, then $\phi(H)$ is cyclic.*
3. *If H is Abelian, then $\phi(H)$ is Abelian.*
4. *If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.*
5. *If $|\text{Ker } \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.*
6. *If H is finite, then $|\phi(H)|$ divides $|H|$.*
7. $\phi(Z(G))$ *is a subgroup of* $Z(\phi(G))$.
8. *If $\overline{K}$ is a subgroup of $\overline{G}$ then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.*
9. *If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.*
10. *If ϕ is onto and $\text{Ker } \phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.*

Corollary: Kernels Are Normal

Let ϕ be a group homomorphism from G to G'. Then:

Ker ϕ is a normal subgroup of G.

This follows from property 8 of Theorem 10.2, with $K = \{e\}$.

Example 8: Complex Numbers

Consider the mapping ϕ from $\mathbb{C}^*$ to $\mathbb{C}^*$ given by $\phi(x) = x^4$:

- Since $(xy)^4 = x^4y^4$, ϕ is a homomorphism
- Ker $\phi = \{x \mid x^4 = 1\} = \{1, -1, i, -i\}$
- By Theorem 10.2 (5), ϕ is a 4-to-1 mapping
- Elements mapping to 2: $\phi^{-1}(2) = \sqrt[4]{2} \cdot \mathrm{Ker}\ \phi = \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$

Verifying Theorem 10.1 (3): $H = \langle \cos 30^\circ + i \sin 30^\circ \rangle$ has $|H| = 12$, but $|\phi(H)| = 3$

Example 9: Modular Arithmetic

Define $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $\phi(x) = 3x$:

- ϕ is a homomorphism since $3(a+b) = 3a + 3b$ in $\mathbb{Z}_{12}$
- Ker $\phi = \{0, 4, 8\}$
- By Theorem 10.2 (5), ϕ is a 3-to-1 mapping
- $\phi^{-1}(6) = 2 + \text{Ker } \phi = \{2, 6, 10\}$
- $|\langle 2 \rangle| = 6$ and $|\phi(2)| = |6| = 2$, so $|\phi(2)|$ divides $|2|$
- For $K = \{0, 6\}, \phi^{-1}(K) = \{0, 2, 4, 6, 8, 10\}$

Example 10: Homomorphisms Between Cyclic Groups

Determining all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$:

- A homomorphism is specified by the image of 1
- If 1 maps to a, then x maps to xa
- By Theorem 10.1 (3), $|a|$ must divide both 12 and 30
- So $|a| = 1, 2, 3,$ or 6
- This means $a = 0, 15, 10, 20, 5,$ or 25
- Each of these six possibilities yields a valid homomorphism
- Note: $\gcd(12, 30) = 6$ (not a coincidence)

Theorem 10.3: First Isomorphism Theorem (Jordan, 1870)

Let ϕ be a group homomorphism from G to G'. Then: $G/\mathrm{Ker}\ \phi \cong\ \phi(G)$

The mapping from $G/\mathrm{Ker}\ \phi$ to $\phi(G)$ given by: $g\ \mathrm{Ker}\ \phi \mapsto \phi(g)$ is an isomorphism.

Proof of First Isomorphism Theorem

Let ψ denote the correspondence $g\ \mathrm{Ker}\ \phi \mapsto \phi(g)$

1. ψ is well-defined by Theorem 10.1 (5)
   - If $g\ \mathrm{Ker}\ \phi = h\ \mathrm{Ker}\ \phi$, then $\phi(g) = \phi(h)$
2. ψ is one-to-one by Theorem 10.1 (5)
   - If $\phi(g) = \phi(h)$, then $g\ \mathrm{Ker}\ \phi = h\ \mathrm{Ker}\ \phi$
3. ψ is operation-preserving:

$$\psi(x\mathrm{Ker}\ \phi \cdot y\mathrm{Ker}\ \phi) = \psi(xy\mathrm{Ker}\ \phi) = \phi(xy) = \phi(x)\phi(y) = \psi(x\mathrm{Ker}\ \phi)\psi(y\mathrm{Ker}\ \phi)$$

Corollary 1: If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|G|/|\text{Ker } \phi| = |\phi(G)|$.

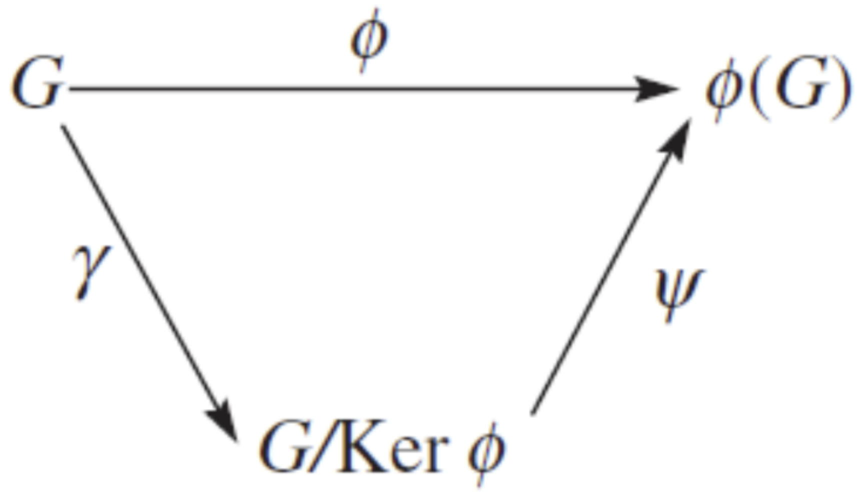
Proof: follows directly from Theorem 10.3.

Corollary 2: If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

Proof: follows directly from Theorem 10.3, property 1 of Theorem 10.2, and Lagrange's Theorem.

Corollary: If ϕ is a homomorphism from a finite group G to G', then $|\phi(G)|$ divides $|G|$ and $|G'|$.

Commutative Diagram for First Isomorphism Theorem



Where:

- $\gamma : G \to G/\text{Ker } \phi$ is the natural mapping $\gamma(g) = g \text{ Ker } \phi$
- $\psi\gamma = \phi$
- This diagram is commutative

Examples Using First Isomorphism Theorem

Example 15: $\mathbb{Z}/(n) \cong \mathbb{Z}_n$

- Consider the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(m) = m \mod n$
- Kernel is (n) (multiples of n)
- By Theorem 10.3, $\mathbb{Z}/(n) \cong \mathbb{Z}_n$

Example 16: Wrapping Function

- $W : \mathbb{R} \to$ circle group, where $W(x) = \cos x + i \sin x$
- This is a homomorphism: $W(x + y) = W(x)W(y)$
- Ker $W = \langle 2\pi \rangle$
- Therefore, $\mathbb{R}/\langle 2\pi \rangle \cong$ circle group

EXAMPLE 15 Determinant-induced quotient isomorphisms

- Quotient by $SL(2, \mathbb{R})$
  - Normal subgroup: $SL(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) \mid \det A = 1\}$.
  - Homomorphism: $\phi : GL(2, \mathbb{R}) \to \mathbb{R}^*$, $\phi(A) = \det A$ (surjective: $\det \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = t$ for any $t \in \mathbb{R}^*$).
  - Kernel: $\operatorname{Ker} \phi = SL(2, \mathbb{R})$.
  - Conclusion (Thm. 10.3): $GL(2, \mathbb{R})/SL(2, \mathbb{R}) \approx \mathbb{R}^*$.
- Quotient by $SL^{\pm}(2, \mathbb{R})$
  - Normal subgroup: $SL^{\pm}(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) \mid \det A = \pm 1\}$.
  - Homomorphism: $\psi : GL(2, \mathbb{R}) \to \mathbb{R}^+$, $\psi(A) = (\det A)^2$ (surjective: for $r > 0$, choose A with $\det A = \pm\sqrt{r}$).
  - Kernel: $\operatorname{Ker} \psi = SL^{\pm}(2, \mathbb{R})$.
  - Conclusion (Thm. 10.3): $GL(2, \mathbb{R})/SL^{\pm}(2, \mathbb{R}) \approx \mathbb{R}^+$.

EXAMPLE 16 Let G be Abelian and $k \in \mathbb{Z}^+$.

- Notation: $G^k := \{x^k \mid x \in G\}$; $G(k) := \{x \in G \mid x^k = e\}$.
- Map: $\phi : G \to G^k$ defined by $\phi(x) = x^k$.
- Homomorphism: $\phi(xy) = (xy)^k = x^k y^k$ (since G is Abelian).
- Surjectivity: By definition, the image of ϕ is G^k.
- Kernel: $\mathrm{Ker}\,\phi = \{x \in G \mid x^k = e\} = G(k)$.
- Conclusion (Thm. 10.3): $G/G(k) \approx G^k$.

EXAMPLE 17: The N/C Theorem

Let H be a subgroup of a group G. Define:

- $N(H) = \{g \in G \mid gHg^{-1} = H\}$, the **normalizer** of H in G
- $C(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$, the **centralizer** of H in G

Key Facts:

1. $C(H) \subseteq N(H) \subseteq G$
2. $C(H)$ is a normal subgroup of $N(H)$
3. H is a normal subgroup of $N(H)$ (by definition of normalizer)

The Homomorphism: Define $\phi : N(H) \to \mathrm{Aut}(H)$ (the group of automorphisms of H) by

$$\phi(g)(h) = ghg^{-1} \quad \text{for all } h \in H.$$

For $g \in N(H)$, the map $\phi(g) : H \to H$ is indeed an automorphism of H (it's the restriction of the inner automorphism of G by g to the subgroup H).

Kernel: $\mathrm{Ker}\ \phi = \{g \in N(H) \mid ghg^{-1} = h \text{ for all } h \in H\} = C(H).$

Application of First Isomorphism Theorem: $N(H)/C(H) \cong \phi(N(H)) \subseteq \mathrm{Aut}(H).$

This is called the **N/C Theorem**.

Interpretation: The quotient $N(H)/C(H)$ measures "how many distinct ways" elements of $N(H)$ can act on H by conjugation. Elements in the same coset of $C(H)$ act on H in the same way.

Theorem 10.4: Normal Subgroups Are Kernels

Every normal subgroup of a group G is the kernel of a homomorphism of G.

In particular, a normal subgroup N is the kernel of the mapping: $g \mapsto gN$ from G to G/N.

Proof

Define $\psi : G \to G/N$ by $\psi(g) = gN$ (the natural homomorphism)

1. ψ is a homomorphism:
   $\psi(xy) = (xy)N = xN \cdot yN = \psi(x)\psi(y)$
2. $g \in \mathrm{Ker}\ \psi$ if and only if $gN = \psi(g) = N$
   - This is true if and only if $g \in N$

Therefore, $\mathrm{Ker}\ \psi = N$

Using Homomorphisms to Simplify Problems

Problem Find an infinite group that is the union of three proper subgroups

Strategy: Simplify First

1. **Start with a finite case** — easier to analyze
2. **Use homomorphisms** to lift the solution to the infinite case

Step 1: Find a Finite Solution

- No cyclic group works (cannot be unin of proper subgroups)
- Try smallest noncyclic group: order 4
- **Solution:** $U(8) = \{1, 3, 5, 7\}$
  - $U(8) = H \cup K \cup L$ where: $H = \{1, 3\}$, $K = \{1, 5\}$, $L = \{1, 7\}$

Step 2: Lift to Infinite Group

- Define $\phi : U(8) \oplus \mathbb{Z} \rightarrow U(8)$ by $\phi(a, b) = a$
- **Answer:** $U(8) \oplus \mathbb{Z} = \phi^{-1}(H) \cup \phi^{-1}(K) \cup \phi^{-1}(L)$

■ **EXAMPLE 21** Claim: $\mathbb{Z} \oplus \mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.

Proof: Assume (for contradiction): There exists an isomorphism

- $\alpha : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.

- Reduce mod 2:
  - Define $\beta : \mathbb{Z}^3 \to \mathbb{Z}_2^3$ by
    - $\beta(x, y, z) = (x \bmod 2,\ y \bmod 2,\ z \bmod 2)$.
- Compose:
  - $\gamma = \beta \circ \alpha : \mathbb{Z}^2 \to \mathbb{Z}_2^3$ is a homomorphism.
  - Since α is onto and β is onto, γ would be onto.
- Generator count:
  - $\mathbb{Z}^2$ is generated by $(1, 0)$ and $(0, 1)$.
  - Hence $\operatorname{Im} \gamma$ is generated by $\gamma(1, 0)$ and $\gamma(0, 1)$ (at most 2 generators).
- Key fact: Any subgroup of $\mathbb{Z}_2^3$ generated by 2 elements has order at most 4.
- Contradiction: $\mathbb{Z}_2^3$ has order 8, so γ cannot be onto.
- Conclusion: No such α exists. Therefore, $\mathbb{Z} \oplus \mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.