§3.7 Homomorphisms

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 10-11, 2020

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G

  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4
- $\mathbf{Z}_n^\times$: *not* always cyclic. $|\mathbf{Z}_n^\times| = \varphi(n) = \#$ of generators of $\mathbf{Z}_n$
- Product of two subgroups: *not* always a subgroup.
- Direct product of 2 groups $\rightsquigarrow$ n groups: $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \cdots \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n)$

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$. ϕ is a group homomorphism. (Check it!) [

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) $[\det(AB) = \det(A)\det(B)\ \checkmark]$
ϕ is *not* an isomorphism. More precisely,

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
It is possible to have different matrices that have the same determinant.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
It is possible to have different matrices that have the same determinant.
Let $n = 2$*. For example,* $A = I_2$ *and* $B = -I_2$ *both have determinant* 1.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
It is possible to have different matrices that have the same determinant.
Let $n = 2$. For example, $A = I_2$ and $B = -I_2$ both have determinant 1.

Is ϕ onto?

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^{\times}$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
It is possible to have different matrices that have the same determinant.
Let $n = 2$. For example, $A = I_2$ and $B = -I_2$ both have determinant 1.

Is ϕ onto? (Yes!) *Let $n = 2$. For example,*

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. A function $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

Note 1

Every isomorphism is a homomorphism, but conversely not true. (Why?)

Example 2 (Determinant of an invertible matrix)

Let $G_1 = \mathrm{GL}_n(\mathbf{R})$ and $G_2 = \mathbf{R}^\times$. Define $\phi : G_1 \to G_2$ by $\phi(A) = \det(A)$.
ϕ is a group homomorphism. (Check it!) [$\det(AB) = \det(A)\det(B)$ ✓]
ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
It is possible to have different matrices that have the same determinant.
Let $n = 2$. For example, $A = I_2$ and $B = -I_2$ both have determinant 1.
Is ϕ onto? (Yes!) *Let $n = 2$. For example,* $C = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, *for any* $a \in \mathbf{R}^\times$.

More Examples, I

Example 3 (Parity of an integer)

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$.

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely,

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer:

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n + m) = [n + m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto?

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

•

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$;
-

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \overset{?}{=} 1 \overset{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma, \tau \in O_n : \phi(\sigma\tau) \overset{?}{=} 1 \overset{?}{=} \phi(\sigma) \cdot \phi(\tau)$
-

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$

- $\sigma \in A_n, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} -1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; •

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$;
- $\sigma, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$
- $\sigma \in A_n, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} -1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$;
- $\sigma \in O_n, \tau \in A_n : \checkmark$ (Why?)

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$
- $\sigma \in A_n, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} -1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma \in O_n, \tau \in A_n : \checkmark$ (Why?)

ϕ is onto (Why?) and

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$;
- $\sigma, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$
- $\sigma \in A_n, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} -1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$;
- $\sigma \in O_n, \tau \in A_n$: ✓(Why?)

ϕ is onto (Why?) and *not* one to one (Why?). (

More Examples, I

Example 3 (Parity of an integer)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_2$ by $\phi(n) = [n]_2$. ϕ is a homomorphism. (Check it!)

$$\phi(n+m) = [n+m]_2 = [n]_2 + [m]_2 = \phi(n) + \phi(m) \text{ for all } n, m \in \mathbf{Z}.$$

ϕ is *not* an isomorphism. More precisely, it is *not* one to one. (Why?)
Parity of an integer: n is even $\Leftrightarrow \phi(n) = [0]_2$ & n is odd $\Leftrightarrow \phi(n) = [1]_2$
Is ϕ onto? (Yes!) (Why?)

Example 4 (Parity of a permutation $\sigma \in S_n$; Theorem 10 in §3.6)

Define $\phi : S_n \to \{\pm 1\}$ by $\phi(\sigma) = 1$ if $\sigma \in A_n$, and $\phi(\sigma) = -1$ if σ is odd.
ϕ is a homomorphism. (Check it!) Consider 4 cases:

- $\sigma, \tau \in A_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} 1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$
- $\sigma \in A_n, \tau \in O_n : \phi(\sigma\tau) \stackrel{?}{=} -1 \stackrel{?}{=} \phi(\sigma) \cdot \phi(\tau)$; • $\sigma \in O_n, \tau \in A_n : \checkmark$ (Why?)

ϕ is onto (Why?) and *not* one to one (Why?). (*similarly as in Example 3*)

More Examples, II

Example 5 (Exponential functions for groups)

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (Check it!)

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:**

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:**

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of* G *is a power of* a).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined:

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

$$\phi([x]+[y]) = \phi([x+y]) = [m(x+y)] = [mx]+[my] = \phi(x)+\phi(y)$$

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

$$\phi([x] + [y]) = \phi([x+y]) = [m(x+y)] = [mx] + [my] = \phi(x) + \phi(y)$$

Is ϕ one-to-one or onto? **A:**

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

$$\phi([x] + [y]) = \phi([x+y]) = [m(x+y)] = [mx] + [my] = \phi(x) + \phi(y)$$

Is ϕ one-to-one or onto? **A:** ϕ is one-to-one and onto $\Leftrightarrow d = (m, n) = 1$.
Thm 10 in Chapter. 1:

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

$$\phi([x]+[y]) = \phi([x+y]) = [m(x+y)] = [mx] + [my] = \phi(x) + \phi(y)$$

Is ϕ one-to-one or onto? **A:** ϕ is one-to-one and onto $\Leftrightarrow d = (m, n) = 1$.
Thm 10 in Chapter. 1: $mx \equiv y \pmod{n}$ has a solution $\Leftrightarrow d = (m, n) | y$.
Moreover,

More Examples, II

Example 5 (Exponential functions for groups)

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (Check it!) $\phi(n+m) = a^{n+m} = a^n a^m = \phi(n) \cdot \phi(m)$
Is ϕ onto? **A:** ϕ is onto $\Leftrightarrow G = \langle a \rangle$ (*every element of G is a power of a*).
Is ϕ one-to-one? **A:** ϕ is one-to-one $\Leftrightarrow o(a) = \infty$ (Why?) (*this ensures that no two powers with different exponents can be equal to each other*).

Example 6 (Linear functions on $\mathbf{Z}_n$)

For a fixed $m \in \mathbf{Z}$, define $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\phi([x]) = [mx]$, for all $[x] \in \mathbf{Z}_n$.
ϕ is well-defined: If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.
ϕ is a homomorphism: (Check it!)

$$\phi([x]+[y]) = \phi([x+y]) = [m(x+y)] = [mx]+[my] = \phi(x)+\phi(y)$$

Is ϕ one-to-one or onto? **A:** ϕ is one-to-one and onto $\Leftrightarrow d = (m,n) = 1$.
Thm 10 in Chapter. 1: $mx \equiv y \pmod{n}$ has a solution $\Leftrightarrow d = (m,n)|y$.
Moreover, if $d|y$, there are d distinct solutions modulo n.

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Proofs of Parts (a), (b), (c) are the same as in the case of an isomorphism.

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Proofs of Parts (a), (b), (c) are the same as in the case of an isomorphism.

(a) $\phi(e_1)\phi(e_1) = \phi(e_1 e_1) = \phi(e_1) \Rightarrow \phi(e_1) = e_2$. (Why?)

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Proofs of Parts (a), (b), (c) are the same as in the case of an isomorphism.

(a) $\phi(e_1)\phi(e_1) = \phi(e_1 e_1) = \phi(e_1) \Rightarrow \phi(e_1) = e_2$. (Why?)

(b) $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_1) = e_2 \Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$. (Why?)

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Proofs of Parts (a), (b), (c) are the same as in the case of an isomorphism.

(a) $\phi(e_1)\phi(e_1) = \phi(e_1 e_1) = \phi(e_1) \Rightarrow \phi(e_1) = e_2$. (Why?)

(b) $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_1) = e_2 \Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$. (Why?)

(c) This can be proved using a simple induction argument. (Check it!)

Properties of homomorphisms

Proposition 1

If $\phi : G_1 \to G_2$ is a group homomorphism, then

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

Proof.

Proofs of Parts (a), (b), (c) are the same as in the case of an isomorphism.

(a) $\phi(e_1)\phi(e_1) = \phi(e_1 e_1) = \phi(e_1) \Rightarrow \phi(e_1) = e_2$. (Why?)

(b) $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_1) = e_2 \Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$. (Why?)

(c) This can be proved using a simple induction argument. (Check it!)

(d) $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. Thus, $o(\phi(a))|n$. (Why?)

$\square$

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?)

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note:

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?)

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k|nm$. (Why?) [

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?)
this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k|nm$. (Why?) [$n \cdot [m]_k = [nm]_k = [0]_k$]

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k|nm$. (Why?) $[n \cdot [m]_k = [nm]_k = [0]_k]$
Thus, $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism if and only if $k|mn$.
Furthermore,

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k|nm$. (Why?) $[n \cdot [m]_k = [nm]_k = [0]_k]$
Thus, $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism if and only if $k|mn$.
Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.
Note that

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g)|n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k)|n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k|nm$. (Why?) $[n \cdot [m]_k = [nm]_k = [0]_k]$
Thus, $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism if and only if $k|mn$.
Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.
Note that $\phi(\mathbf{Z}_n)$ is the cyclic subgroup generated by $[m]_k$ (Why?), and so

Examples

Example 7 (Homomorphisms defined on cyclic groups)

Let $C = \langle a \rangle$ be a cyclic group. Define a homomorphism $\phi : C \to G$ by $\phi(a) = g$. Then $\phi(a^m) = g^m$. (Why?)
Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, (Why?) this implies that ϕ is completely determined by its value on a. (Why?)
Note: If $o(a) = n < \infty$, then $o(g) | n$. (Why?) [Proposition 1 (d)]

Example 8 (Homomorphisms $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$)

Any such homomorphism ϕ is completely determined by $\phi([1]_n)$. (Why?)
Say, $\phi([1]_n) = [m]_k$ with $o([m]_k) | n$. (Why?) So $n \cdot [m]_k = [0]_k$. (Why?)
It follows that $k | nm$. (Why?) $[n \cdot [m]_k = [nm]_k = [0]_k]$
Thus, $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism if and only if $k | mn$.
Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.
Note that $\phi(\mathbf{Z}_n)$ is the cyclic subgroup generated by $[m]_k$ (Why?), and so $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ is onto $\Leftrightarrow$ $[m]_k$ is a generator of $\mathbf{Z}_k$, i.e., $(m, k) = 1$. (Why?)

Kernel and Image of a Homomorphism

Definition 9

Let $\phi : G_1 \to G_2$ be a group homomorphism. The **kernel** of ϕ is the set

$$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\}.$$

The **image** of ϕ is the set

$$\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\}.$$

Note 2

Kernel and Image of a Homomorphism

Definition 9

Let $\phi : G_1 \to G_2$ be a group homomorphism. The **kernel** of ϕ is the set

$$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\}.$$

The **image** of ϕ is the set

$$\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\}.$$

Note 2

- $\ker(\phi)$ *is a subset of* G_1.

Kernel and Image of a Homomorphism

Definition 9

Let $\phi : G_1 \to G_2$ be a group homomorphism. The **kernel** of ϕ is the set

$$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\}.$$

The **image** of ϕ is the set

$$\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\}.$$

Note 2

- $\ker(\phi)$ *is a subset of* G_1.
- $\mathrm{im}(\phi)$ *is a subset of* G_2.

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (See Example 5)

Question 1

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =$?

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) = ?$

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =$?

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) = ?$

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. (Why?)

Note:

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =?$

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. (Why?)

Note: *In either case,* $\ker(\phi)$ *is a subgroup of* $\mathbf{Z}$*.*

Question 2

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =$?

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. (Why?)

Note: *In either case,* $\ker(\phi)$ *is a subgroup of* $\mathbf{Z}$.

Question 2

What is $\mathrm{im}(\phi) =$?

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$.
ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =$?

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. (Why?)

Note: *In either case,* $\ker(\phi)$ *is a subgroup of* $\mathbf{Z}$.

Question 2

What is $\mathrm{im}(\phi) =$?

By definition, $\mathrm{im}(\phi) = \{a^n \mid n \in \mathbf{Z}\} = \langle a \rangle$.
Note:

Revisit Example 5: Exponential functions for groups

Let G be a group, and let $a \in G$. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. ϕ is a homomorphism. (See Example 5)

Question 1

What is $\ker(\phi) =?$

By definition, $\ker(\phi) = \{n \mid a^n = e\}$. Let $o(a)$ be the order of a in G. So,

- If $o(a) = m < \infty$, then $\ker(\phi) = \langle m \rangle = m\mathbf{Z}$. (Why?)
- If $o(a) = \infty$, then $\ker(\phi) = \{0\}$. (Why?)

Note: *In either case,* $\ker(\phi)$ *is a subgroup of* $\mathbf{Z}$.

Question 2

What is $\mathrm{im}(\phi) =?$

By definition, $\mathrm{im}(\phi) = \{a^n \mid n \in \mathbf{Z}\} = \langle a \rangle$.
Note: $\mathrm{im}(\phi) = \langle a \rangle$ *is a subgroup of* G.

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ *be a group homomorphism. Then*

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1*.*

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2*.*

(a) $\ker(\phi)$ is nonempty:

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$.

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of G_1.*

(b) $\mathrm{im}(\phi)$ *is a subgroup of G_2.*

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty:

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of G_1.*

(b) $\mathrm{im}(\phi)$ *is a subgroup of G_2.*

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty: $e_2 \in \mathrm{im}(\phi)$. (Why?) [

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) $[\phi(e_1) = e_2]$
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty: $e_2 \in \mathrm{im}(\phi)$. (Why?) $[\phi(e_1) = e_2]$
For $x, y \in \mathrm{im}(\phi)$, *to show* $xy^{-1} \in \mathrm{im}(\phi)$.

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of G_1.*

(b) $\mathrm{im}(\phi)$ *is a subgroup of G_2.*

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty: $e_2 \in \mathrm{im}(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $x, y \in \mathrm{im}(\phi)$, *to show* $xy^{-1} \in \mathrm{im}(\phi)$. So $\phi(a) = x$ and $\phi(b) = y$ for some $a, b \in G_1$. Therefore,

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1*.*

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2*.*

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty: $e_2 \in \mathrm{im}(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $x, y \in \mathrm{im}(\phi)$, *to show* $xy^{-1} \in \mathrm{im}(\phi)$. So $\phi(a) = x$ and $\phi(b) = y$ for some $a, b \in G_1$. Therefore,

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}).$$

Theorem 11 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

$\ker(\phi)$ is a subgroup of G_1 & $\mathrm{im}(\phi)$ is a subgroup of G_2

Theorem 10

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

(a) $\ker(\phi)$ *is a subgroup of* G_1.

(b) $\mathrm{im}(\phi)$ *is a subgroup of* G_2.

(a) $\ker(\phi)$ is nonempty: $e_1 \in \ker(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $a, b \in \ker(\phi)$, *to show* $ab^{-1} \in \ker(\phi)$. So $\phi(a) = e_2$ & $\phi(b) = e_2$.

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e_2 e_2^{-1} = e_2.$$

(b) $\mathrm{im}(\phi)$ is nonempty: $e_2 \in \mathrm{im}(\phi)$. (Why?) [$\phi(e_1) = e_2$]
For $x, y \in \mathrm{im}(\phi)$, *to show* $xy^{-1} \in \mathrm{im}(\phi)$. So $\phi(a) = x$ and $\phi(b) = y$ for some $a, b \in G_1$. Therefore,

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}).$$

Theorem 11 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

(a) ϕ *is one-to-one if and only if* $\ker(\phi) = \{e_1\}$.

(b) ϕ *is onto if and only if* $\mathrm{im}(\phi) = G_2$.

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism.

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in** $\S$**3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. $\square$

(b)

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in** $\S$**3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. $\square$

(b) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$.

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in §3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. $\square$

(b) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$. Trivial. (Why?) $\square$

Proposition 1 (d):

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in §3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. □

(b) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$. Trivial. (Why?) □

Proposition 1 (d): If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.

Proposition 2 (More properties that are preserved by homomorphisms)

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in §3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. $\square$

(b) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$. Trivial. (Why?) $\square$

Proposition 1 (d): If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.

Proposition 2 (More properties that are preserved by homomorphisms)

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) *If G_1 is abelian, then G_2 is also abelian.*

(b) *If G_1 is cyclic, then G_2 is also cyclic.*

Note 3

Proof of Theorem 11

(a) ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$.
Let $\phi : G_1 \to G_2$ be a group homomorphism. By **Proposition 5 in §3.4:**
ϕ is one-to-one $\Leftrightarrow \phi(x) = e_2 \Rightarrow x = e_1$, i.e., $\ker(\phi) = \{e_1\}$. $\square$

(b) ϕ is onto if and only if $\mathrm{im}(\phi) = G_2$. Trivial. (Why?) $\square$

Proposition 1 (d): If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.

Proposition 2 (More properties that are preserved by homomorphisms)

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) *If G_1 is abelian, then G_2 is also abelian.*

(b) *If G_1 is cyclic, then G_2 is also cyclic.*

Note 3

Proposition 2 (a) & (b) are not necessarily true if ϕ is not onto.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \stackrel{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$:

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \stackrel{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$.
  We can write $y = \phi(b)$ for some $b \in G_1$. (Why?)

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \stackrel{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$. We can write $y = \phi(b)$ for some $b \in G_1$. (Why?) We can also write $b = a^m$ for some $m \in \mathbf{Z}$. (Why?)

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$. We can write $y = \phi(b)$ for some $b \in G_1$. (Why?) We can also write $b = a^m$ for some $m \in \mathbf{Z}$. (Why?) This implies that

$$y = \phi(b) = \phi(a^m) = (\phi(a))^m.$$

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \overset{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$. We can write $y = \phi(b)$ for some $b \in G_1$. (Why?) We can also write $b = a^m$ for some $m \in \mathbf{Z}$. (Why?) This implies that

$$y = \phi(b) = \phi(a^m) = (\phi(a))^m.$$

Thus, $G_2 = \langle \phi(a) \rangle$.

Proof of Proposition 2

Let $\phi : G_1 \to G_2$ be a group homomorphism. And assume that ϕ is onto.

(a) If G_1 is abelian, then G_2 is also abelian.

(b) If G_1 is cyclic, then G_2 is also cyclic.

(a) For any $x, y \in G_2$, there exist $a, b \in G_1$ such that $\phi(a) = x, \phi(b) = y$.

$$xy = \phi(a)\phi(b) = \phi(ab) \stackrel{!}{=} \phi(ba) = \phi(b)\phi(a) = yx.$$

(b) Let $G_1 = \langle a \rangle$ for a generator $a \in G_1$. Claim: $G_2 = \langle \phi(a) \rangle$.

- $\langle \phi(a) \rangle \subseteq G_2$: Trivial. (Why?) [$\phi(a) \in G_2$]
- $G_2 \subseteq \langle \phi(a) \rangle$: *To show* every element y of G_2 is a power of $\phi(a)$. We can write $y = \phi(b)$ for some $b \in G_1$. (Why?) We can also write $b = a^m$ for some $m \in \mathbf{Z}$. (Why?) This implies that

$$y = \phi(b) = \phi(a^m) = (\phi(a))^m.$$

Thus, $G_2 = \langle \phi(a) \rangle$. That is, G_2 is also cyclic.

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore,

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism:

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ *to* $\mathbf{Z}$, *from* $\mathbf{Z}$ *to* $\mathbf{Z}_n$, *and from* $\mathbf{Z}_n$ *to* $\mathbf{Z}$.

Proposition 3

Let m *be a fixed integer. Define a function* $\phi : \mathbf{Z} \to \mathbf{Z}$ *by* $\phi(x) = mx$. *Then* ϕ *is a homomorphism. Every homomorphism must be of this form.*

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ *to* $\mathbf{Z}$*, from* $\mathbf{Z}$ *to* $\mathbf{Z}_n$*, and from* $\mathbf{Z}_n$ *to* $\mathbf{Z}$*.*

Proposition 3

Let m *be a fixed integer. Define a function* $\phi : \mathbf{Z} \to \mathbf{Z}$ *by* $\phi(x) = mx$*. Then* ϕ *is a homomorphism. Every homomorphism must be of this form.*

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) =$

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) =$

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ *to* $\mathbf{Z}$, *from* $\mathbf{Z}$ *to* $\mathbf{Z}_n$, *and from* $\mathbf{Z}_n$ *to* $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) =$

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = x\phi(1) =$

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ *to* $\mathbf{Z}$, *from* $\mathbf{Z}$ *to* $\mathbf{Z}_n$, *and from* $\mathbf{Z}_n$ *to* $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = x\phi(1) = mx$.

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$, from $\mathbf{Z}$ to $\mathbf{Z}_n$, and from $\mathbf{Z}_n$ to $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = x\phi(1) = mx$.
For $x \in \mathbf{Z}^-$, so $x = -|x|$:

Examples: Homorphisms between cyclic groups

Example 8: We define a homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. And $\phi([x]_n) = [mx]_k$ is well-defined if and only if $k|mn$. Furthermore, every homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ must be of this form.

Question 3 (How about the other cases?)

Find all homomorphisms from $\mathbf{Z}$ *to* $\mathbf{Z}$, *from* $\mathbf{Z}$ *to* $\mathbf{Z}_n$, *and from* $\mathbf{Z}_n$ *to* $\mathbf{Z}$.

Proposition 3

Let m be a fixed integer. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

ϕ is a homomorphism: $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$.
This is a special case of **Example 7** since $\mathbf{Z}$ is an infinity cyclic group.
In particular, let $\phi(1) = m$ for some integer m since 1 is a generator of $\mathbf{Z}$.
For $x \in \mathbf{Z}^+, \phi(x) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = x\phi(1) = mx$.
For $x \in \mathbf{Z}^-$, so $x = -|x| : \phi(x) = \phi(-|x|) = -\phi(|x|) = -m|x| = mx$. $\square$

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. *Define a function* $\phi : \mathbf{Z} \to \mathbf{Z}_n$ *by* $\phi(x) = [mx]_n$. *Then* ϕ *is a homomorphism. Every homomorphism must be of this form.*

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. $\square$

Proposition 5

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$*. Define a function* $\phi : \mathbf{Z} \to \mathbf{Z}_n$ *by* $\phi(x) = [mx]_n$*. Then* ϕ *is a homomorphism. Every homomorphism must be of this form.*

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. □

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ *is the function defined by* $\phi([x]_n) = 0$ *for all* $[x]_n \in \mathbf{Z}_n$*.*

Proof.

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. $\square$

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is the function defined by $\phi([x]_n) = 0$ for all $[x]_n \in \mathbf{Z}_n$.

Proof.

In $\mathbf{Z}_n, o([x]_n) = m|n$. And so

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. $\square$

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is the function defined by $\phi([x]_n) = 0$ for all $[x]_n \in \mathbf{Z}_n$.

Proof.

In $\mathbf{Z}_n, o([x]_n) = m|n$. And so $o(\phi([x]_n))|m$ in $\mathbf{Z}$. (Why?) [

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. $\square$

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is the function defined by $\phi([x]_n) = 0$ for all $[x]_n \in \mathbf{Z}_n$.

Proof.

In $\mathbf{Z}_n, o([x]_n) = m|n$. And so $o(\phi([x]_n))|m$ in $\mathbf{Z}$. (Why?) [Prop. 1 (d)]

Example cont.: Homomorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. □

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is the function defined by $\phi([x]_n) = 0$ for all $[x]_n \in \mathbf{Z}_n$.

Proof.

In $\mathbf{Z}_n, o([x]_n) = m|n$. And so $o(\phi([x]_n))|m$ in $\mathbf{Z}$. (Why?) [Prop. 1 (d)]
However, in $\mathbf{Z}$, only 0 has a finite order ($o(0) = 1$).

Example cont.: Homorphisms between $\mathbf{Z}$ and $\mathbf{Z}_n$

Proposition 4

Let $[m]_n \in \mathbf{Z}_n$. Define a function $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$. Then ϕ is a homomorphism. Every homomorphism must be of this form.

Proof.

The proof is the same as for homomorphisms $\mathbf{Z} \to \mathbf{Z}$. $\square$

Proposition 5

The only homomorphism $\mathbf{Z}_n \to \mathbf{Z}$ is the function defined by $\phi([x]_n) = 0$ for all $[x]_n \in \mathbf{Z}_n$.

Proof.

In $\mathbf{Z}_n, o([x]_n) = m|n$. And so $o(\phi([x]_n))|m$ in $\mathbf{Z}$. (Why?) [Prop. 1 (d)]
However, in $\mathbf{Z}$, only 0 has a finite order ($o(0) = 1$). Thus, $\phi([x]_n) = 0$. $\square$

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note:

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

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

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

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

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} =$

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} =$

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_2$ □

Definition 12

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_2$ □

Definition 12

A subgroup H of the group G is called a **normal** subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Example 13 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_2$ □

Definition 12

A subgroup H of the group G is called a **normal** subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Example 13 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(1) $\ker(\phi)$ is a normal subgroup of G_1; see Proposition 6.

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_2$ □

Definition 12

A subgroup H of the group G is called a **normal** subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Example 13 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(1) $\ker(\phi)$ is a normal subgroup of G_1; see Proposition 6.

(2) If $H = G$ or $H = \{e\}$, then H is normal.

Normal subgroup

Proposition 6 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Let g be any element in G_1. Then $gkg^{-1} \in \ker(\phi)$ for all $k \in \ker(\phi)$.

Note: We have shown that $\ker(\phi)$ is a subgroup of G_1 in Theorem 10 (a).

Proof.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_2\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_2$ $\square$

Definition 12

A subgroup H of the group G is called a **normal** subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Example 13 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(1) $\ker(\phi)$ is a normal subgroup of G_1; see Proposition 6.

(2) If $H = G$ or $H = \{e\}$, then H is normal.

(3) Any subgroup of an abelian group is normal.

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty:

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?)} \checkmark$$

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$.

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \stackrel{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty:

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)
For any $a, b \in \phi^{-1}(H_2), ab^{-1} \in \phi^{-1}(H_2)$ since

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?)} \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)
For any $a, b \in \phi^{-1}(H_2), ab^{-1} \in \phi^{-1}(H_2)$ since $\phi(ab^{-1}) \in H_2$. (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \ \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?)} \ \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)
For any $a, b \in \phi^{-1}(H_2)$, $ab^{-1} \in \phi^{-1}(H_2)$ since $\phi(ab^{-1}) \in H_2$. (Why?)
Let $g \in G_1$ and $a \in \phi^{-1}(H_2)$. *To show $gag^{-1} \in \phi^{-1}(H_2)$.* (Why?)

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)
For any $a, b \in \phi^{-1}(H_2)$, $ab^{-1} \in \phi^{-1}(H_2)$ since $\phi(ab^{-1}) \in H_2$. (Why?)
Let $g \in G_1$ and $a \in \phi^{-1}(H_2)$. *To show $gag^{-1} \in \phi^{-1}(H_2)$.* (Why?)
This is true since

How subgroups are related via a homomorphism

Proposition 7 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

(a) Nonempty: $e_2 \in \phi(H_1)$. (Why?) For any $x, y \in \phi(H_1)$, there exist $a, b \in H_1$ with $\phi(a) = x$ and $\phi(b) = y$, and

$$xy^{-1} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H_1). \ \checkmark$$

Let $x \in G_2$ and $y \in \phi(H_1)$. *To show $xyx^{-1} \in \phi(H_1)$.* (Why?)
There exist $g \in G_1$ and $a \in H_1$ with $\phi(g) = x$ (Why?) and $y = \phi(a)$.

$$xyx^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(gag^{-1}) \overset{?}{\in} \phi(H_1) \text{ (Why?) } \checkmark$$

(b) $\phi^{-1}(H_2) = \{a \in G_1 \mid \phi(a) \in H_2\}$. Nonempty: $e_1 \in \phi^{-1}(H_2)$. (Why?)
For any $a, b \in \phi^{-1}(H_2)$, $ab^{-1} \in \phi^{-1}(H_2)$ since $\phi(ab^{-1}) \in H_2$. (Why?)
Let $g \in G_1$ and $a \in \phi^{-1}(H_2)$. *To show $gag^{-1} \in \phi^{-1}(H_2)$.* (Why?)
This is true since $\phi(gag^{-1}) = \phi(g)\phi(a)(\phi(g))^{-1} \in H_2$. (Why?) □

Equivalence relation on G_1 associated with ϕ

Definition 14 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Equivalence relation on G_1 associated with ϕ

Definition 14 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Natural equivalent relation on G_1 : $a \sim_\phi b$ if $\phi(a) = \phi(b)$, where $a, b \in G_1$.

Notation:

Equivalence relation on G_1 associated with ϕ

Definition 14 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Natural equivalent relation on $G_1 : a \sim_\phi b$ if $\phi(a) = \phi(b)$, where $a, b \in G_1$.

Notation: The set of equivalence classes of this relation: $G_1/\phi = \{[a]_\phi\}$, where $[a]_\phi$ is the equivalence class of $a \in G_1$. (Think about $[r]_n$ in $\mathbf{Z}_n$)

Proposition 8 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Equivalence relation on G_1 associated with ϕ

Definition 14 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Natural equivalent relation on $G_1 : a \sim_\phi b$ if $\phi(a) = \phi(b)$, where $a, b \in G_1$.

Notation: The set of equivalence classes of this relation: $G_1/\phi = \{[a]_\phi\}$, where $[a]_\phi$ is the equivalence class of $a \in G_1$. (Think about $[r]_n$ in $\mathbf{Z}_n$)

Proposition 8 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

The multiplication of equivalence classes in the set G_1/ϕ is well-defined, and G_1/ϕ is a group under this multiplication.

Equivalence relation on G_1 associated with ϕ

Definition 14 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

Natural equivalent relation on G_1 : $a \sim_\phi b$ if $\phi(a) = \phi(b)$, where $a, b \in G_1$.

Notation: The set of equivalence classes of this relation: $G_1/\phi = \{[a]_\phi\}$, where $[a]_\phi$ is the equivalence class of $a \in G_1$. (Think about $[r]_n$ in $\mathbf{Z}_n$)

Proposition 8 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

The multiplication of equivalence classes in the set G_1/ϕ is well-defined, and G_1/ϕ is a group under this multiplication. The natural projection

$$\pi : G_1 \to G_1/\phi$$

defined by $\pi(a) = [a]_\phi$ is a group homomorphism.

(Recall the multiplication of congruence classes in $\mathbf{Z}_n$: $[a]_n[b]_n = [ab]_n$)

Proof of Proposition 8

(i) Multiplication is well-defined:

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ if $a \sim_\phi b$ and $c \sim_\phi d$.

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!)

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ and $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,

$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity:

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,

$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,
$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:
$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses:

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ and $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,
$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:
$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ and $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,
$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:
$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since
$$[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi \quad \text{and} \quad [a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$$

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,
$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:
$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since
$$[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi \quad \text{and} \quad [a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$$

Thus, G_1/ϕ is a group under the multiplication of equivalence classes.

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,

$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \stackrel{!}{=} [(ab)c]_\phi \stackrel{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:

$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since

$$[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi \quad \text{and} \quad [a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$$

Thus, G_1/ϕ is a group under the multiplication of equivalence classes.

Define the natural projection $\pi : G_1 \to G_1/\phi$ by $\pi(a) = [a]_\phi$.

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ *and* $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,

$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:

$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since

$$[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi \quad \text{and} \quad [a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$$

Thus, G_1/ϕ is a group under the multiplication of equivalence classes.

Define the natural projection $\pi : G_1 \to G_1/\phi$ by $\pi(a) = [a]_\phi$.
π is a group homomorphism: (Check it!) For all $a, b \in G_1$,

Proof of Proposition 8

(i) Multiplication is well-defined: *show* $ac \sim_\phi bd$ *if* $a \sim_\phi b$ and $c \sim_\phi d$.
If $\phi(a) = \phi(b)$ and $\phi(c) = \phi(d)$, then
$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd).$$

(ii) Associativity: (Check it!) For all $a, b, c \in G_1$,
$$[a]_\phi([b]_\phi[c]_\phi) = [a]_\phi[bc]_\phi = [a(bc)]_\phi \overset{!}{=} [(ab)c]_\phi \overset{\checkmark}{=} ([a]_\phi[b]_\phi)[c]_\phi$$

(iii) Identity: The class $[e]_\phi$ is an identity element since for all $a \in G_1$:
$$[e]_\phi[a]_\phi = [ea]_\phi = [a]_\phi \quad \text{and} \quad [a]_\phi[e]_\phi = [ae]_\phi = [a]_\phi$$

(iv) Inverses: For any equivalence class $[a]_\phi$, its inverse is $[a^{-1}]_\phi$ since
$$[a^{-1}]_\phi[a]_\phi = [a^{-1}a]_\phi = [e]_\phi \quad \text{and} \quad [a]_\phi[a^{-1}]_\phi = [aa^{-1}]_\phi = [e]_\phi$$

Thus, G_1/ϕ is a group under the multiplication of equivalence classes.

Define the natural projection $\pi : G_1 \to G_1/\phi$ by $\pi(a) = [a]_\phi$.
π is a group homomorphism: (Check it!) For all $a, b \in G_1$,
$$\pi(ab) = [ab]_\phi = [a]_\phi[b]_\phi = \pi(a)\pi(b).$$

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, *where* $\overline{\phi}$ *is defined by*

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined:

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one:

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto:

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) =$

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} =$

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} =$

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \mathrm{im}(\phi) =$

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \mathrm{im}(\phi) = \phi(G_1)$

(iv) $\overline{\phi}$ is a group homomorphism:

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \mathrm{im}(\phi) = \phi(G_1)$

(iv) $\overline{\phi}$ is a group homomorphism: For any $[a]_\phi, [b]_\phi \in G_1/\phi$,

An extremely important theorem

Theorem 15 (Let $\phi : G_1 \to G_2$ be a homomorphism.)

There exists a group isomorphism $\overline{\phi} : G_1/\phi \to \phi(G_1)$, where $\overline{\phi}$ is defined by

$$\overline{\phi}([a]_\phi) = \phi(a), \text{ for all } [a]_\phi \in G_1/\phi.$$

Note $G_1 \xrightarrow{\pi} G_1/\phi \xrightarrow{\overline{\phi}} \phi(G_1) \xrightarrow{\iota} G_2$: $\phi = \iota\overline{\phi}\pi$, ι is the inclusion mapping

Proof.

(i) well-defined: If $[a]_\phi = [b]_\phi$, then $\phi(a) = \phi(b)$. So $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$.

(ii) one-to-one: If $\overline{\phi}([a]_\phi) = \overline{\phi}([b]_\phi)$, then $\phi(a) = \phi(b)$. So $[a]_\phi = [b]_\phi$.

(iii) onto: $\mathrm{im}(\overline{\phi}) = \{\overline{\phi}([a]_\phi) \mid a \in G_1\} = \{\phi(a) \mid a \in G_1\} = \mathrm{im}(\phi) = \phi(G_1)$

(iv) $\overline{\phi}$ is a group homomorphism: For any $[a]_\phi, [b]_\phi \in G_1/\phi$,

$$\overline{\phi}([a]_\phi[b]_\phi) = \overline{\phi}([ab]_\phi) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}([a]_\phi)\overline{\phi}([b]_\phi).$$

$\square$

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?)

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?)

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.
- If $o(a) = n$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod{n}$.

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.
- If $o(a) = n$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod{n}$. Thus, $\phi(m) = \phi(k)$ if and only if $m \equiv k \pmod{n}$.

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.
- If $o(a) = n$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod{n}$. Thus, $\phi(m) = \phi(k)$ if and only if $m \equiv k \pmod{n}$. This shows that $\mathbf{Z}/\phi$ is the additive group of congruence classes modulo n.

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.
- If $o(a) = n$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod{n}$. Thus, $\phi(m) = \phi(k)$ if and only if $m \equiv k \pmod{n}$. This shows that $\mathbf{Z}/\phi$ is the additive group of congruence classes modulo n. Therefore, $G \cong \mathbf{Z}_n$. (Why?)

Example: Characterization of cyclic groups

Theorem 16 (Theorem 2 in §3.5)

Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, for some $n \in \mathbf{Z}^+$.

Another proof: (Using Theorem 15).

Given $G = \langle a \rangle$, define $\phi : \mathbf{Z} \to G$ by $\phi(m) = a^m$. (Example 5: ϕ is onto)

- If $o(a) = \infty$, then ϕ is one-to-one. (Why?) So $\mathbf{Z} \cong \phi(\mathbf{Z}) = G$(Why?) Since ϕ is one-to-one, the equivalence classes of the factor set $\mathbf{Z}/\phi$ are just the subsets of $\mathbf{Z}$ consisting of single elements, and thus $\mathbf{Z}$ itself.
- If $o(a) = n$, then $a^m = a^k \Leftrightarrow m \equiv k \pmod n$. Thus, $\phi(m) = \phi(k)$ if and only if $m \equiv k \pmod n$. This shows that $\mathbf{Z}/\phi$ is the additive group of congruence classes modulo n. Therefore, $G \cong \mathbf{Z}_n$. (Why?)

By Theorem 15, $\mathbf{Z}/\phi \cong \phi(\mathbf{Z}) = G$ & $\mathbf{Z}/\phi = \mathbf{Z}_n$.

$\square$

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism:

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b)$.

one-to-one:

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a \, (\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$.

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a \, (\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a \, (\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus G itself. Thus,

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a \, (\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus G itself. Thus,

$$G \cong \phi(G). \text{ (Why?) [}$$

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a \, (\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus G itself. Thus,

$$G \cong \phi(G).$$ (Why?) [Theorem 15!]

And

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus G itself. Thus,

$$G \cong \phi(G).$$ (Why?) [Theorem 15!]

And $\phi(G)$ is a permutation group.(Why?) [

Example: Another proof of Cayley's theorem (use Thm 15)

Cayley's theorem: *Every group is isomorphic to a permutation group.*

Given any group G, define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(a) = \lambda_a$, for any $a \in G$, where $\lambda_a\,(\in \mathrm{Sym}(G))$ is the function defined by $\lambda_a(x) = ax$ for all $x \in G$.

ϕ is a homomorphism: For all $a, b \in G$, $\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b)$.

one-to-one: λ_a is the identity permutation only if $a = e$. So $\ker(\phi) = \{e\}$.

Since ϕ is one-to-one, the equivalence classes of the factor set G/ϕ are just the subsets of G consisting of single elements, and thus G itself. Thus,

$$G \cong \phi(G).\ \text{(Why?) [Theorem 15!]}$$

And $\phi(G)$ is a permutation group.(Why?) [$\phi(G)$ is a subgroup of $\mathrm{Sym}(G)$]

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2)

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow$

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow$

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ *for some* $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ *for some* $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3)

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1)

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1) If $a = kb$, then $\phi(a) = \phi(kb) = \phi(k)\phi(b) = e_2\phi(b) = \phi(b)$.

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1) If $a = kb$, then $\phi(a) = \phi(kb) = \phi(k)\phi(b) = e_2\phi(b) = \phi(b)$.
Similarly it can be shown that (1) implies (4) implies (5) implies (1). $\square$

Lemma 17 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ *for some* $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ *for some* $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1) If $a = kb$, then $\phi(a) = \phi(kb) = \phi(k)\phi(b) = e_2\phi(b) = \phi(b)$.
Similarly it can be shown that (1) implies (4) implies (5) implies (1). $\square$

Lemma 17 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ *define* $a \sim b$ *if* $ab^{-1} \in H$. *Then* $\sim$ *is an equivalence relation.*

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1) If $a = kb$, then $\phi(a) = \phi(kb) = \phi(k)\phi(b) = e_2\phi(b) = \phi(b)$.
Similarly it can be shown that (1) implies (4) implies (5) implies (1). $\square$

Lemma 17 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

By Proposition 9, we let $H = \ker(\phi)$.

$G/\ker(\phi)$: The more standard notation for G/ϕ

Proposition 9 (Let $\phi : G_1 \to G_2$ be a homomorphism, and $a, b \in G_1$.)

The following conditions are equivalent:

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

(2) $ab^{-1} \in \ker(\phi)$;

(3) $a = kb$ for some $k \in \ker(\phi)$;

(4) $b^{-1}a \in \ker(\phi)$;

(5) $a = bk$ for some $k \in \ker(\phi)$;

(1) $\Rightarrow$ (2) $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = \phi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker(\phi)$
(2) $\Rightarrow$ (3) If $ab^{-1} = k \in \ker(\phi)$, then $a = kb$.
(3) $\Rightarrow$ (1) If $a = kb$, then $\phi(a) = \phi(kb) = \phi(k)\phi(b) = e_2\phi(b) = \phi(b)$.
Similarly it can be shown that (1) implies (4) implies (5) implies (1). $\square$

Lemma 17 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

By Proposition 9, we let $H = \ker(\phi)$. Then, we write $G/\ker(\phi)$ for G/ϕ.

Some remarks

Remark 1 (Restate Theorem 15)

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ *be a homomorphism. Then* $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form:*
For $a, b \in G_1$, *the following conditions are equivalent:*

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form:*
For $a, b \in G_1$, the following conditions are equivalent:

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. Then ϕ is a homomorphism.

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form:*
For $a, b \in G_1$, the following conditions are equivalent:

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. Then ϕ is a homomorphism.
What is the $\ker(\phi) =$? **A:**

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form: For $a, b \in G_1$, the following conditions are equivalent:*

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. Then ϕ is a homomorphism. What is the $\ker(\phi) =$? **A:** $\ker(\phi) = n\mathbf{Z} = \langle n \rangle$. So

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form:*
For $a, b \in G_1$, the following conditions are equivalent:

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. Then ϕ is a homomorphism.
What is the $\ker(\phi) =$? **A:** $\ker(\phi) = n\mathbf{Z} = \langle n \rangle$. So $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$.

Some remarks

Remark 1 (Restate Theorem 15)

Let $\phi : G_1 \to G_2$ *be a homomorphism. Then* $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Remark 2 (Let $\phi : G_1 \to G_2$ be a homomorphism of abelian groups.)

With operations denoted additively, then **Prop. 9** *has the following form: For* $a, b \in G_1$, *the following conditions are equivalent:*

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

(2) $a - b \in \ker(\phi)$;

(3) $a = b + k$ *for some* $k \in \ker(\phi)$.

Example 18 (A special case of Proposition 4: $m = 1$)

Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [x]_n$. Then ϕ is a homomorphism.
What is the $\ker(\phi) =$? **A:** $\ker(\phi) = n\mathbf{Z} = \langle n \rangle$. So $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$.

$$\phi(x) = \phi(y) \Leftrightarrow [x]_n = [y]_n \Leftrightarrow x \equiv y \pmod{n} \Leftrightarrow x - y = mn \text{ for } m \in \mathbf{Z}$$