§3.4 Isomorphisms

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 27-28, 2020

Review

- Group

Review

- Group
  - abelian vs. nonabelian

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$;   If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$;   If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
    - $o(a)|n$ for any $a \in G$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\Big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$;   If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.
    - $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.
    - $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$
    - If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.
    - $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$
    - If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.
    - $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.
    - $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$
    - If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.
    - $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.
  - Definition of a field & New groups defined over a filed F.

Review

- Group
  - abelian vs. nonabelian
  - finite vs. infinite
- Subgroup
  - cyclic: $o(a) = |\langle a \rangle|$; If $o(a) = n < \infty$, then $a^k = e \Leftrightarrow n|k$.
  - Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic (and so abelian).
- Constructing (sub)groups
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.
    - If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.
  - Direct product: $G_1 \times G_2$ is a group under a new defined operation.
    - $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$
    - If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.
    - $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.
  - Definition of a field & New groups defined over a filed F.
  - Subgroup generated by S: $\langle S \rangle$ is the smallest subgroup that contains S.

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Table: Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Table: Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Table: Addition in $\mathbf{Z}_2$

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

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^{\times}$ and the group $\mathbf{Z}_2$.

Table: Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Table: Addition in $\mathbf{Z}_2$

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

Table: Group table in G with $|G| = 2$

$*$	e	a
e	e	a
a	a	e

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Table: Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Table: Addition in $\mathbf{Z}_2$

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

Table: Group table in G with $|G| = 2$

$*$	e	a
e	e	a
a	a	e

Table: Group table in G with $|G| = 3$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Examples: Motivation

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Table: Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Table: Addition in $\mathbf{Z}_2$

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

Table: Group table in G with $|G| = 2$

$*$	e	a
e	e	a
a	a	e

Table: Group table in G with $|G| = 3$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Upshot: All groups with two (or three) elements must have exactly the same algebraic properties.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Important Note: In every problem that requires you to prove that two groups are **isomorphic**, you need to

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Important Note: In every problem that requires you to prove that two groups are **isomorphic**, you need to

- **define a function** (well-defined) and then

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Important Note: In every problem that requires you to prove that two groups are **isomorphic**, you need to

- **define a function** (well-defined) and then
- **verify** that the function you defined is an **isomorphism**.

Note 1

Definition

Definition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

- ϕ is one-to-one and onto, and
- $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all elements $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Important Note: In every problem that requires you to prove that two groups are **isomorphic**, you need to

- **define a function** (well-defined) and then
- **verify** that the function you defined is an **isomorphism**.

Note 1

Sometimes your first guess for what that function is might not work, so you might need to try several different functions until you find one that satisfies the requirements.

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ *and* $(G_2, \cdot)$ *be groups, and let* $\phi : G_1 \to G_2$ *be an isomorphism. Let* e_1 *and* e_2 *be the identity elements of* G_1 *and* G_2*, respectively. 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* $n \in \mathbf{Z}$.

(a):

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

(a): $\phi(e_1) \cdot \phi(e_1) = \phi(e_1 * e_1) = \phi(e_1) = \phi(e_1) \cdot e_2$

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

(b):

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

(b): $\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} * a) = \phi(e_1) = e_2$

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

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

(c):

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

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

(c): By induction, we have

$$\phi(a_1 * a_2 * \cdots * a_n) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_n),$$

for $a_1, a_2, \ldots, a_n \in G_1$.

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

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

(c): By induction, we have

$$\phi(a_1 * a_2 * \cdots * a_n) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_n),$$

for $a_1, a_2, \ldots, a_n \in G_1$. In particular, $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}^+$.

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

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

(c): By induction, we have

$$\phi(a_1 * a_2 * \cdots * a_n) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_n),$$

for $a_1, a_2, \ldots, a_n \in G_1$. In particular, $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}^+$. It follows that $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}$. (Check it!)

Properties of isomorphisms

Proposition 1

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. 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* $n \in \mathbf{Z}$.

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

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

(c): By induction, we have

$$\phi(a_1 * a_2 * \cdots * a_n) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_n),$$

for $a_1, a_2, \ldots, a_n \in G_1$. In particular, $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}^+$.
It follows that $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}$. (Check it!)
If $n < 0$, then $n = -|n|$: $\phi(a^n) = \phi((a^{-1})^{|n|}) = (\phi(a^{-1}))^{|n|} = ((\phi(a))^{-1})^{|n|}$

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

- one-to-one:

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

- one-to-one: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 - x_2 = 0 \Rightarrow x_1 = x_2$. (Why?)

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

- one-to-one: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 - x_2 = 0 \Rightarrow x_1 = x_2$. (Why?)
- onto:

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

- one-to-one: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 - x_2 = 0 \Rightarrow x_1 = x_2$. (Why?)
- onto: For any $y \in \mathbf{R}^+$, take $x = \ln y \in \mathbf{R}$ and then $\phi(x) = e^{\ln y} = y$.

Example

Upshot: Any group isomorphism preserves general products, the identity element, and inverses of elements.

Example 2

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to **positive** real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

Try $\phi(x) = e^x$:

(i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

(ii) $\phi(x) = e^x$ is

- one-to-one: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 - x_2 = 0 \Rightarrow x_1 = x_2$. (Why?)
- onto: For any $y \in \mathbf{R}^+$, take $x = \ln y \in \mathbf{R}$ and then $\phi(x) = e^{\ln y} = y$.

(iii) $\phi(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = \phi(x_1) \cdot \phi(x_2)$.

More properties of isomorphisms

Proposition 2

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a):

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$,

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b):

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms.

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?)

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?) *To show* $\psi\phi$ preserves products. If $a, b \in G_1$, $\Rightarrow \psi\phi(a * b) =$

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?) *To show* $\psi\phi$ preserves products. If $a, b \in G_1$,

$\Rightarrow \psi\phi(a * b) = \psi(\phi(a * b)) =$

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?) *To show* $\psi\phi$ preserves products. If $a, b \in G_1$,
$\Rightarrow \psi\phi(a * b) = \psi(\phi(a * b)) = \psi(\phi(a) \cdot \phi(b)) =$

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?) *To show* $\psi\phi$ preserves products. If $a, b \in G_1$, $\Rightarrow \psi\phi(a * b) = \psi(\phi(a * b)) = \psi(\phi(a) \cdot \phi(b)) = \psi(\phi(a)) \star \psi(\phi(b)) =$

More properties of isomorphisms

Proposition 2

(a) *The inverse of a group isomorphism is a group isomorphism.*

(b) *The composite of two group isomorphisms is a group isomorphism.*

(a): Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. (Why?) [ϕ is one-to-one and onto]

- For each $g_2 \in G_2$ there exists a unique $g_1 \in G_1$ such that $\phi(g_1) = g_2$, and then $\theta(g_2) = g_1$.
- By definition of θ, we have $\theta\phi = 1_{G_1}$ and $\phi\theta = 1_{G_2}$.
- The definition also implies that θ is one-to-one and onto.

To show θ preserves products. Let $a_2, b_2 \in G_2$. Let $\theta(a_2) = a_1$ and $\theta(b_2) = b_1$. Then $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$, so $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2$.

$$\theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2).$$

(b): Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group isomorphisms. Then $\psi\phi$ is one-to-one and onto. (Why?) *To show* $\psi\phi$ preserves products. If $a, b \in G_1$,
$\Rightarrow \psi\phi(a * b) = \psi(\phi(a * b)) = \psi(\phi(a) \cdot \phi(b)) = \psi(\phi(a)) \star \psi(\phi(b)) = \psi\phi(a) \star \psi\phi(b)$.

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive:

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric:

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [Take the inverse $\theta = \phi^{-1}$]

(iii) Transitive:

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [Take the inverse $\theta = \phi^{-1}$]

(iii) Transitive: $G_1 \cong G_2$ and $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ [

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [Take the inverse $\theta = \phi^{-1}$]

(iii) Transitive: $G_1 \cong G_2$ and $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ [The composite $\psi\phi$]

Example 3

$(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$. Here, $\langle i \rangle = \{1, i, -1, -i\}$ and $\mathbf{Z}_4 = \{[0], [1], [2], [3]\}$.

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [Take the inverse $\theta = \phi^{-1}$]

(iii) Transitive: $G_1 \cong G_2$ and $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ [The composite $\psi\phi$]

Example 3

$(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$. Here, $\langle i \rangle = \{1, i, -1, -i\}$ and $\mathbf{Z}_4 = \{[0], [1], [2], [3]\}$.

Table: Multiplication in $\langle i \rangle$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Example

Upshot: The isomorphism $\cong$ is an equivalence relation.

(i) Reflexive: $G \cong G$ [$\phi =$the identity mapping 1_G]

(ii) Symmetric: $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ [Take the inverse $\theta = \phi^{-1}$]

(iii) Transitive: $G_1 \cong G_2$ and $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ [The composite $\psi\phi$]

Example 3

$(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$. Here, $\langle i \rangle = \{1, i, -1, -i\}$ and $\mathbf{Z}_4 = \{[0], [1], [2], [3]\}$.

Table: Multiplication in $\langle i \rangle$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i \rangle$.

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i \rangle$.

Define a function $\phi : \mathbf{Z}_4 \to \langle i \rangle$ by $\phi([n]) = i^n$.

- Well-defined:

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i \rangle$.

Define a function $\phi : \mathbf{Z}_4 \to \langle i \rangle$ by $\phi([n]) = i^n$.

- Well-defined:If $[n] = [m]$, i.e., $n \equiv m \pmod 4$, then $i^n = i^m$. (Why?)

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i \rangle$.

Define a function $\phi : \mathbf{Z}_4 \to \langle i \rangle$ by $\phi([n]) = i^n$.

- Well-defined:If $[n] = [m]$, i.e., $n \equiv m \pmod 4$, then $i^n = i^m$. (Why?)
- The function ϕ defines a one-to-one correspondence. (Check it!)
- ϕ preserves the respective operations:

Example cont.: $(\langle i \rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i \rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i \rangle$.

Define a function $\phi : \mathbf{Z}_4 \to \langle i \rangle$ by $\phi([n]) = i^n$.

- Well-defined:If $[n] = [m]$, i.e., $n \equiv m \pmod 4$, then $i^n = i^m$. (Why?)
- The function ϕ defines a one-to-one correspondence. (Check it!)
- ϕ preserves the respective operations:

$$\phi([n] + [m]) = \phi([n + m]) = i^{n+m} = i^n \cdot i^m = \phi([n]) \cdot \phi([m]).$$

Example cont.: $(\langle i\rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\ ]_4})$

Table: Multiplication in $\langle i\rangle$

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

Table: Addition in $\mathbf{Z}_4$

$+_{[\ ]_4}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i\rangle$.

Define a function $\phi : \mathbf{Z}_4 \to \langle i\rangle$ by $\phi([n]) = i^n$.

- Well-defined:If $[n] = [m]$, i.e., $n \equiv m \pmod 4$, then $i^n = i^m$. (Why?)
- The function ϕ defines a one-to-one correspondence. (Check it!)
- ϕ preserves the respective operations:

$$\phi([n] + [m]) = \phi([n + m]) = i^{n+m} = i^n \cdot i^m = \phi([n]) \cdot \phi([m]).$$

We conclude that ϕ is a group isomorphism.

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one:

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1}$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto:

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

  $\phi(hk) =$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

$$\phi(hk) = ahka^{-1} =$$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

  $\phi(hk) = ahka^{-1} = ah(a^{-1}a)ka^{-1} =$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

  $\phi(hk) = ahka^{-1} = ah(a^{-1}a)ka^{-1} = (aha^{-1})(aka^{-1}) =$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

$$\phi(hk) = ahka^{-1} = ah(a^{-1}a)ka^{-1} = (aha^{-1})(aka^{-1}) = \phi(h)\phi(k).$$

Example: $aHa^{-1} \cong H$

Let G be a group, and let H be a subgroup of G. If a is any element of G, then the subgroup aHa^{-1} is isomorphic to H.

(i) The identity element $e = aea^{-1} \in aHa^{-1}$. So aHa^{-1} is nonempty.✓

(ii) For $x, y \in aHa^{-1}$, we have $xy^{-1} \in aHa^{-1}$. (Check it!)

Define $\phi : H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$, for all $h \in H$.

- It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. (Why?)
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$, so $\phi(h) = y$.
- ϕ respects multiplication in H: Let $h, k \in H$.

$$\phi(hk) = ahka^{-1} = ah(a^{-1}a)ka^{-1} = (aha^{-1})(aka^{-1}) = \phi(h)\phi(k).$$

Thus, ϕ is an isomorphism.

Another way to show that ϕ is one-to-one and onto

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism.

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto,

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$.

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

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

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓

Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) =$$

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1}: G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi: \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1}: \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism.

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓

Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto,

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1}: G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi: \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1}: \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓

Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi: H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto, we define $\phi^{-1}: aHa^{-1} \to H$ by $\phi^{-1}(b) = a^{-1}ba$ for all $b \in aHa^{-1}$.

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : aHa^{-1} \to H$ by $\phi^{-1}(b) = a^{-1}ba$ for all $b \in aHa^{-1}$. ✓

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓

Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : aHa^{-1} \to H$ by $\phi^{-1}(b) = a^{-1}ba$ for all $b \in aHa^{-1}$. ✓

Verify that this is the inverse function of ϕ:

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

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : aHa^{-1} \to H$ by $\phi^{-1}(b) = a^{-1}ba$ for all $b \in aHa^{-1}$. ✓
Verify that this is the inverse function of ϕ:

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

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1} : G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

Example 4

We prove $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$ by showing that $\phi : \mathbf{R} \to \mathbf{R}^+$ is an isomorphism. In particular, we define $\phi(x) = e^x$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$ for all $y \in \mathbf{R}^+$. Well-defined ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Example 5

We prove $aHa^{-1} \cong H$ by showing that $\phi : H \to aHa^{-1}$ is an isomorphism. Define $\phi(h) = aha^{-1}$ for all $h \in H$. To show that ϕ is one-to-one and onto, we define $\phi^{-1} : aHa^{-1} \to H$ by $\phi^{-1}(b) = a^{-1}ba$ for all $b \in aHa^{-1}$. ✓
Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(b)) = \phi(a^{-1}ba) = a(a^{-1}ba)a^{-1} = b$$
$$\phi^{-1}(\phi(h)) = \phi^{-1}(aha^{-1}) = a^{-1}(aha^{-1})a = h$$

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ *be an isomorphism of groups.*

Proposition 3

Let $\phi : G_1 \to G_2$ *be an isomorphism of groups.*

(a) *If* a *has order* n *in* G_1, *then* $\phi(a)$ *has order* n *in* G_2.

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a):

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$.

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$.

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$.

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$,

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.
(b):

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 =$$

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.
(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) =$$

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.
(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=}$$

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) =$$

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.
(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) =$$

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c):

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \stackrel{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c): Suppose that G_1 is cyclic, with $G_1 = \langle a \rangle$.

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.
(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c): Suppose that G_1 is cyclic, with $G_1 = \langle a \rangle$. For any element $y \in G_2$, we have $y = \phi(x)$ for some $x \in G_1$. (Why?)

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \stackrel{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c): Suppose that G_1 is cyclic, with $G_1 = \langle a \rangle$. For any element $y \in G_2$, we have $y = \phi(x)$ for some $x \in G_1$. (Why?) We write $x = a^n$ for some $n \in \mathbf{Z}$.

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \stackrel{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c): Suppose that G_1 is cyclic, with $G_1 = \langle a \rangle$. For any element $y \in G_2$, we have $y = \phi(x)$ for some $x \in G_1$. (Why?) We write $x = a^n$ for some $n \in \mathbf{Z}$. Then $y = \phi(x) = \phi(a^n) = (\phi(a))^n$.

Several structural properties preserved by group isomorphisms

Proposition 3

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian, then so is G_2.*

(c) *If G_1 is cyclic, then so is G_2.*

(a): Assume that $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. This shows that $o(\phi(a))|n$. Since ϕ is an isomorphism, there exists ϕ^{-1} such that $\phi^{-1}(\phi(a)) = a$, and a similar argument shows that $n|o(\phi(a))$.

(b): Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2.$$

(c): Suppose that G_1 is cyclic, with $G_1 = \langle a \rangle$. For any element $y \in G_2$, we have $y = \phi(x)$ for some $x \in G_1$. (Why?) We write $x = a^n$ for some $n \in \mathbf{Z}$. Then $y = \phi(x) = \phi(a^n) = (\phi(a))^n$. Thus G_2 is cyclic, generated by $\phi(a)$.

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic**.

Example 6 ($(\mathbf{R}, +) \not\cong (\mathbf{R}^\times, \cdot)$)

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic***.*

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic**.

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic***.*

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic***.*

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic***.*

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e.,

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic***.*

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e., $o(1) = 1$ and $o(-1) = 2$.

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic**.

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e., $o(1) = 1$ and $o(-1) = 2$.
In $(\mathbf{C}^\times, \cdot)$, there are other elements of finite orders.

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic**.

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e., $o(1) = 1$ and $o(-1) = 2$.
In $(\mathbf{C}^\times, \cdot)$, there are other elements of finite orders. For example, $o(i) = 4$.

Examples

Note 2

The previous proposition gives us a technique for proving that two groups are **not isomorphic**.

Example 6 ($(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (Why?) [If so, $2x = 0 \Rightarrow x = 0$.]
Thus there cannot be an isomorphism between the two groups. (Why?)

Example 7 ($(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$)

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e., $o(1) = 1$ and $o(-1) = 2$.
In $(\mathbf{C}^\times, \cdot)$, there are other elements of finite orders. For example, $o(i) = 4$.
Thus there cannot be an isomorphism between the two groups. (Why?)

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic.

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic.

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4.

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

Which of the groups $S_3, \mathrm{GL}_2(\mathbf{Z}_2), \mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ are isomorphic?

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

Which of the groups $S_3, \mathrm{GL}_2(\mathbf{Z}_2), \mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ are isomorphic?

- The first two groups (S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$) we know to be nonabelian.

More examples

Example 8 ($\mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

Which of the groups $S_3, \mathrm{GL}_2(\mathbf{Z}_2), \mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ are isomorphic?

- The first two groups (S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$) we know to be nonabelian.
- Any cyclic group is abelian.

More examples

Example 8 ($\mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \not\cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

Which of the groups $S_3, \mathrm{GL}_2(\mathbf{Z}_2), \mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ are isomorphic?

- The first two groups (S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$) we know to be nonabelian.
- Any cyclic group is abelian. So $\mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ (Why?) are abelian.

More examples

Example 8 ($\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$)

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. (Why?)

Example 9 ($\mathbf{Z}_4 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$)

In the second group, any non-identity element must have order 2. (Why?)
In the first group, there are elements of order 4. For example, $([1]_4, [1]_4)$ has order 4. (Why?) [If $(x, y) \in G_1 \times G_2$, so $o((x, y)) = \mathrm{lcm}[o(x), o(y)]$.]

Question 1 (Groups of order 6)

Which of the groups $S_3, \mathrm{GL}_2(\mathbf{Z}_2), \mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ are isomorphic?

- The first two groups (S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$) we know to be nonabelian.
- Any cyclic group is abelian. So $\mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$ (Why?) are abelian. In fact, the element $([1]_2, [1]_3)$ of $\mathbf{Z}_2 \times \mathbf{Z}_3$ has order 6. (Why?)

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3 we described S_3 by letting $e = (1), a = (123)$ and $b = (12)$, which allowed us to write

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2b.$$

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3 we described S_3 by letting $e = (1), a = (123)$ and $b = (12)$, which allowed us to write

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2b.$$

Also recall that those 6 elements in $\mathrm{GL}_2(\mathbf{Z}_2)$ are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3 we described S_3 by letting $e = (1), a = (123)$ and $b = (12)$, which allowed us to write

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2b.$$

Also recall that those 6 elements in $\mathrm{GL}_2(\mathbf{Z}_2)$ are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

To establish the connection between S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$, let

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \text{and} \qquad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3 we described S_3 by letting $e = (1), a = (123)$ and $b = (12)$, which allowed us to write

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2 b.$$

Also recall that those 6 elements in $\mathrm{GL}_2(\mathbf{Z}_2)$ are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

To establish the connection between S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$, let

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \text{and} \qquad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then direct computations show that $a^3 = e, b^2 = e$ and $ba = a^2 b$.

Example: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3 we described S_3 by letting $e = (1)$, $a = (123)$ and $b = (12)$, which allowed us to write

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2b.$$

Also recall that those 6 elements in $\mathrm{GL}_2(\mathbf{Z}_2)$ are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

To establish the connection between S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$, let

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \text{and} \qquad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then direct computations show that $a^3 = e$, $b^2 = e$ and $ba = a^2b$. Furthermore, each element of $\mathrm{GL}_2(\mathbf{Z}_2)$ can be expressed uniquely in one of the following forms:

$$e, a, a^2, b, ab, a^2b.$$

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$.

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$. Let

$$\phi((123)) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \phi((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$. Let

$$\phi((123)) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \phi((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and then extend this to all elements by letting

$$\phi((123)^i(12)^j) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^j$$

for $i = 0, 1, 2$ and $j = 0, 1$.

Proposition 4

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$. Let

$$\phi((123)) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \phi((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and then extend this to all elements by letting

$$\phi((123)^i(12)^j) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^j$$

for $i = 0, 1, 2$ and $j = 0, 1$.

Proposition 4

Let $\phi : S_3 \to \mathrm{GL}_2(\mathbf{Z}_2)$ be defined as above. Then ϕ is an isomorphism.

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$. Let

$$\phi((123)) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \phi((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and then extend this to all elements by letting

$$\phi((123)^i(12)^j) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^j$$

for $i = 0, 1, 2$ and $j = 0, 1$.

Proposition 4

Let $\phi : S_3 \to \mathrm{GL}_2(\mathbf{Z}_2)$ be defined as above. Then ϕ is an isomorphism.

Our remarks about the unique forms of the respective elements show that ϕ is a one-to-one correspondence.✓

Example cont: $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

This indicates how to define an isomorphism from S_3 to $\mathrm{GL}_2(\mathbf{Z}_2)$. Let

$$\phi((123)) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \phi((12)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and then extend this to all elements by letting

$$\phi((123)^i(12)^j) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^j$$

for $i = 0, 1, 2$ and $j = 0, 1$.

Proposition 4

Let $\phi : S_3 \to \mathrm{GL}_2(\mathbf{Z}_2)$ be defined as above. Then ϕ is an isomorphism.

Our remarks about the unique forms of the respective elements show that ϕ is a one-to-one correspondence.✓

The fact that the multiplication tables are identical shows that ϕ respects the two operations. (Check it!)

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic,

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one:

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) =$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) = \phi([n + m]_6) =$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) = \phi([n + m]_6) = ([n + m]_2, [n + m]_3) =$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) = \phi([n + m]_6) = ([n + m]_2, [n + m]_3) = ([n]_2 + [m]_2, [n]_3 + [m]_3) =$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. Thus, $6|(n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) = \phi([n + m]_6) = ([n + m]_2, [n + m]_3) = ([n]_2 + [m]_2, [n]_3 + [m]_3) = ([n]_2, [n]_3)([m]_2, [m]_3) =$

Example: $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

Since we have already observed that both groups are cyclic, we can let a be a generator for $\mathbf{Z}_6$ and b be a generator for $\mathbf{Z}_2 \times \mathbf{Z}_3$. In particular,

$$\mathbf{Z}_6 = \langle [1]_6 \rangle \qquad \text{and} \qquad \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle.$$

Define the function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by letting

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

- If $[n_1]_6 = [n_2]_6$, i.e., $n_1 \equiv n_2 \pmod 6$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$, and so ϕ is well-defined.
- one-to-one: If $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, then $n_1 \equiv n_2 \pmod 2$ and $n_1 \equiv n_2 \pmod 3$. That is to say, $2 | (n_1 - n_2)$ and $3 | (n_1 - n_2)$. Thus, $6 | (n_1 - n_2)$ since $(2, 3) = 1$. It follows that $n_1 \equiv n_2 \pmod 6$.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto.
- $\phi([n]_6 + [m]_6) = \phi([n+m]_6) = ([n+m]_2, [n+m]_3) =$ $([n]_2 + [m]_2, [n]_3 + [m]_3) = ([n]_2, [n]_3)([m]_2, [m]_3) = \phi([n]_6)\phi([m]_6)$.

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one,

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

$\Leftarrow$: If $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, then

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

$\Leftarrow$: If $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, then

$$\phi(x_1 * x_2^{-1}) = \phi(x_1) \cdot \phi(x_2^{-1}) = \phi(x_1) \cdot (\phi(x_2))^{-1} = \phi(x_2) \cdot (\phi(x_2))^{-1} = e_2,$$

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

$\Leftarrow$: If $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, then

$$\phi(x_1 * x_2^{-1}) = \phi(x_1) \cdot \phi(x_2^{-1}) = \phi(x_1) \cdot (\phi(x_2))^{-1} = \phi(x_2) \cdot (\phi(x_2))^{-1} = e_2,$$

and hence $x_1 * x_2^{-1} = e_1$, and thus

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

$\Leftarrow$: If $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, then

$$\phi(x_1 * x_2^{-1}) = \phi(x_1) \cdot \phi(x_2^{-1}) = \phi(x_1) \cdot (\phi(x_2))^{-1} = \phi(x_2) \cdot (\phi(x_2))^{-1} = e_2,$$

and hence $x_1 * x_2^{-1} = e_1$, and thus

$$x_1 = x_2.$$

An easier way to check that ϕ which preserves products is one-to-one

Proposition 5

Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

Proof.

$\Rightarrow$: If ϕ is one-to-one, then only e_1 can map to e_2. (Why?) On the other hand, suppose that $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$.

$\Leftarrow$: If $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, then

$$\phi(x_1 * x_2^{-1}) = \phi(x_1) \cdot \phi(x_2^{-1}) = \phi(x_1) \cdot (\phi(x_2))^{-1} = \phi(x_2) \cdot (\phi(x_2))^{-1} = e_2,$$

and hence $x_1 * x_2^{-1} = e_1$, and thus

$$x_1 = x_2.$$

This shows that ϕ is one-to-one.

$\square$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) =$ $f_{m_1,b_1}(m_2x + b_2) =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) =$ $f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) = f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 = m_1m_2x + (m_1b_2 + b_1)$.

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) = f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 = m_1m_2x + (m_1b_2 + b_1)$.

It follows that $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) = f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 = m_1m_2x + (m_1b_2 + b_1)$.

It follows that $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1m_2,m_1b_2+b_1}) =$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) = f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 = m_1m_2x + (m_1b_2 + b_1)$.

It follows that $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1m_2,m_1b_2+b_1}) = \begin{bmatrix} m_1m_2 & m_1b_2 + b_1 \\ 0 & 1 \end{bmatrix}$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

First, for any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = f_{m_1,b_1}(f_{m_2,b_2}(x)) = f_{m_1,b_1}(m_2x + b_2) = m_1(m_2x + b_2) + b_1 = m_1m_2x + (m_1b_2 + b_1)$.

It follows that $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1m_2,m_1b_2+b_1}) = \begin{bmatrix} m_1m_2 & m_1b_2 + b_1 \\ 0 & 1 \end{bmatrix}$

And also $\phi(f_{m_1,b_1})\phi(f_{m_2,b_2}) = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1m_2 & m_1b_2 + b_1 \\ 0 & 1 \end{bmatrix}$

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) $[m \neq 0]$
- one-to-one:

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$,

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $m = 1, b = 0$.

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $m = 1, b = 0$. It is easy to check that $f_{1,0} = e_1$. (Check it!) (

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $m = 1, b = 0$.
  It is easy to check that $f_{1,0} = e_1$. (Check it!) (By Proposition 5 ✓1-1)
- onto:

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $m = 1, b = 0$.
  It is easy to check that $f_{1,0} = e_1$. (Check it!) (By Proposition 5 ✓1-1)
- onto: It is obvious by definition of ϕ.

Example cont.

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\} \text{ under matrix multiplication.}$$

Define a function $\phi : G_1 \to G_2$ by

$$\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}.$$

Verify: ✓ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$ for all $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$.

- well-defined: ✓(Why?) [$m \neq 0$]
- one-to-one: If $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $m = 1, b = 0$.
  It is easy to check that $f_{1,0} = e_1$. (Check it!) (By Proposition 5 ✓1-1)
- onto: It is obvious by definition of ϕ.

Thus, ϕ is an isomorphism.

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$*, then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$,

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$*, then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$,

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x + y]_{mn}) = ([x + y]_m, [x + y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$*, then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x+y]_{mn}) = ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?)

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x+y]_{mn}) = ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?)

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x+y]_{mn}) = ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?) It follows that $[x]_{mn} = [0]_{mn}$,

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x+y]_{mn}) = ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?) It follows that $[x]_{mn} = [0]_{mn}$, and so ϕ is one-to-one. (Why?)

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m,n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m,n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m,n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x+y]_{mn}) = ([x+y]_m, [x+y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?) It follows that $[x]_{mn} = [0]_{mn}$, and so ϕ is one-to-one. (Why?)
- Since $|\mathbf{Z}_{mn}| = |\mathbf{Z}_m \times \mathbf{Z}_n|$,

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$, *then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x + y]_{mn}) = ([x + y]_m, [x + y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?) It follows that $[x]_{mn} = [0]_{mn}$, and so ϕ is one-to-one. (Why?)
- Since $|\mathbf{Z}_{mn}| = |\mathbf{Z}_m \times \mathbf{Z}_n|$, any one-to-one mapping must be onto.

Example: $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$ if $\gcd(m, n) = 1$.

Note 3 (Proposition 3 in §3.3)

$\mathbf{Z}_m \times \mathbf{Z}_n$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proposition 6

If $m, n \in \mathbf{Z}^+$ *such that* $\gcd(m, n) = 1$*, then* $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.

Define $\phi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$.

- If $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and so ϕ is well-defined.
- $\phi([x]_{mn} + [y]_{mn}) = \phi([x + y]_{mn}) = ([x + y]_m, [x + y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$
- If $\phi([x]_{mn}) = ([0]_m, [0]_n)$, then $m|x, n|x$. (Why?) So $mn|x$. (Why?) It follows that $[x]_{mn} = [0]_{mn}$, and so ϕ is one-to-one. (Why?)
- Since $|\mathbf{Z}_{mn}| = |\mathbf{Z}_m \times \mathbf{Z}_n|$, any one-to-one mapping must be onto.

Thus, ϕ is an isomorphism.