Groups and Homomorphisms

Dr. Chuck Rocca

Table of Contents

1. Homomorphisms
2. Isomorphisms
3. Groups and Actions
4. Cayley's Theorem

Homomorphisms of Groups

Definition

A function ϕ from a group G to a group H is a **group homomorphism** provided

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$

Homomorphisms of Groups

Definition

A function ϕ from a group G to a group H is a **group homomorphism** provided

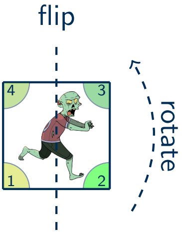
$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$

Definition

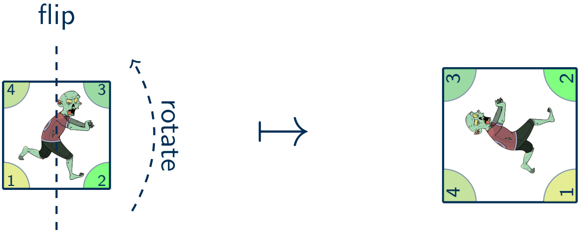
If $\phi : G \to H$ is a homomorphism, then the **kernel of** ϕ is the set

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

D_n to S_n

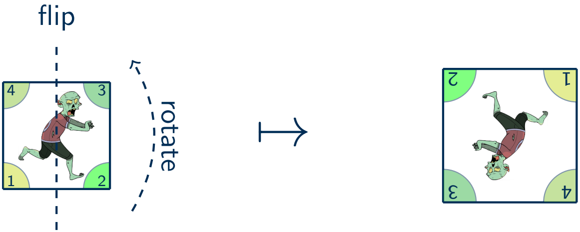


D_n to S_n



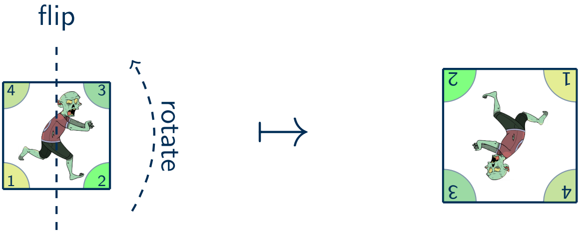
- $r \mapsto (1234)$

D_n to S_n



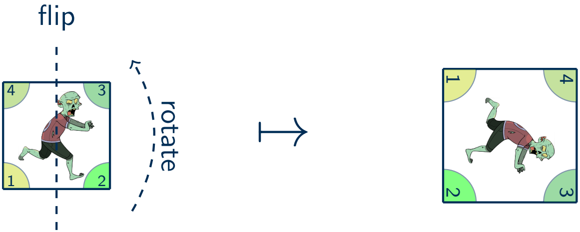
- $r \mapsto (1234)$
- $r^2 \mapsto$

D_n to S_n



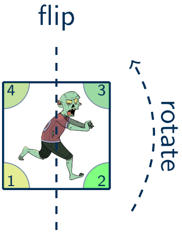
- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$

D_n to S_n

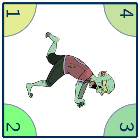


- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto$

D_n to S_n

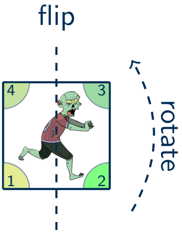


$\mapsto$

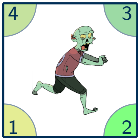


- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$

D_n to S_n

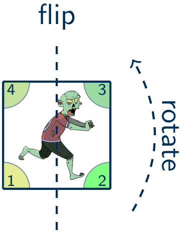


$\mapsto$



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto$

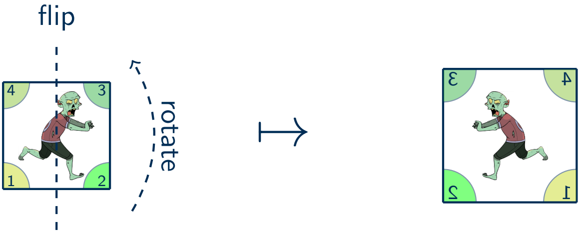
D_n to S_n



$\mapsto$

- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

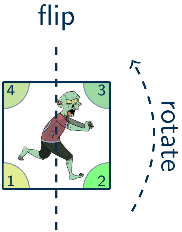
D_n to S_n



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$

D_n to S_n

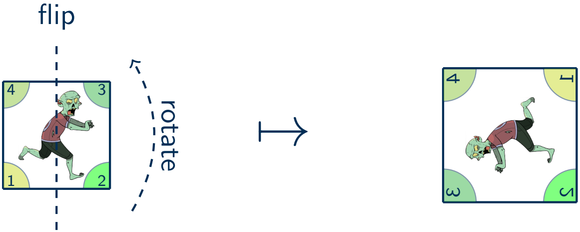


$\mapsto$

- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$
- $rf \mapsto$

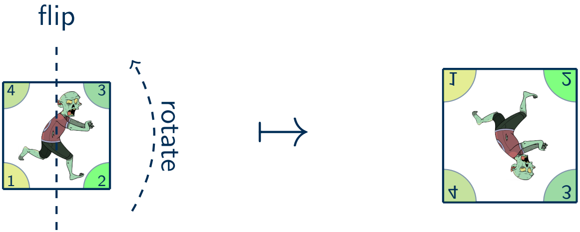
D_n to S_n



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$

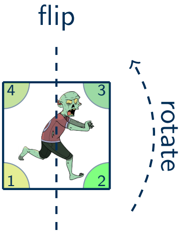
D_n to S_n



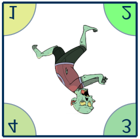
- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$
- $r^2 f \mapsto$

D_n to S_n



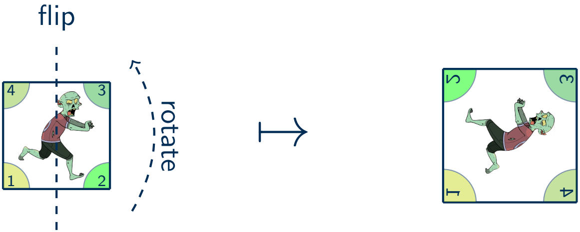
$\longmapsto$



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$
- $r^2 f \mapsto (13)(24)(12)(34) = (14)(23)$

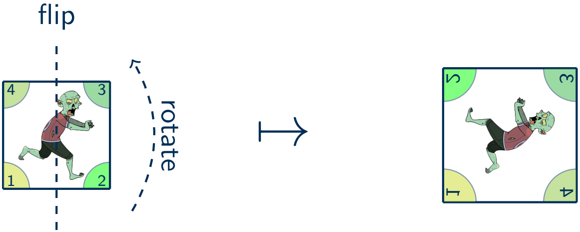
D_n to S_n



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

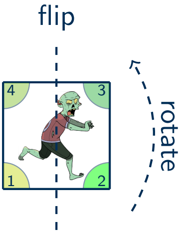
- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$
- $r^2 f \mapsto (13)(24)(12)(34) = (14)(23)$
- $r^3 f \mapsto$

D_n to S_n



- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$
- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$
- $r^2 f \mapsto (13)(24)(12)(34) = (14)(23)$
- $r^3 f \mapsto (1432)(12)(34) = (24)$

D_n to S_n



$\mapsto$

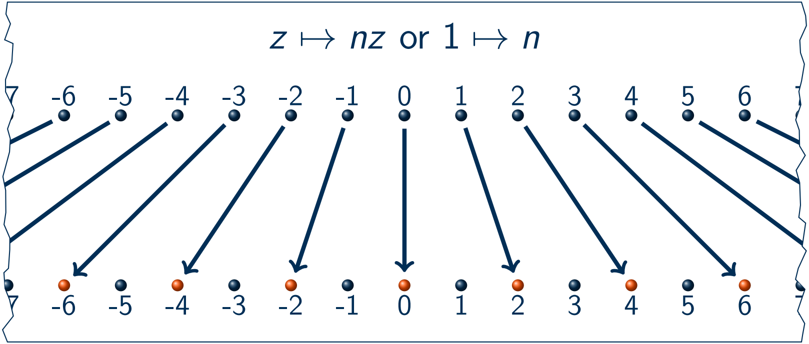
- $r \mapsto (1234)$
- $r^2 \mapsto (1234)^2 = (13)(24)$
- $r^3 \mapsto (1234)^3 = (1432)$
- $r^4 \mapsto (1234)^4 = (1) = e$

- $f \mapsto (12)(34)$
- $rf \mapsto (1234)(12)(34) = (13)$
- $r^2 f \mapsto (13)(24)(12)(34) = (14)(23)$
- $r^3 f \mapsto (1432)(12)(34) = (24)$

In general $\phi : D_4 \to S_4$ is defined by

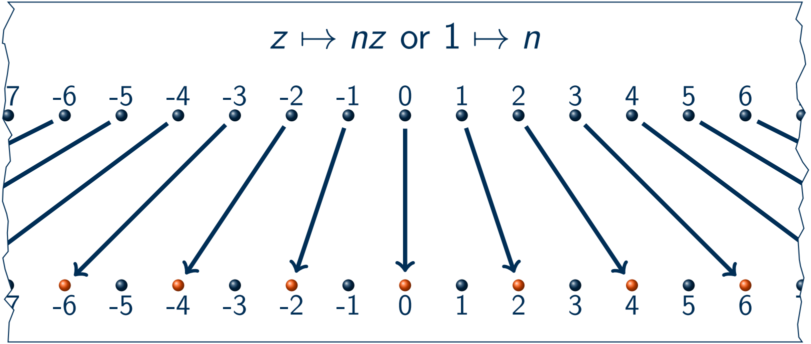
$$\phi(r) = (1234) \text{ and } \phi(f) = (12)(34)$$

$\mathbb{Z}$ to $n\mathbb{Z}$



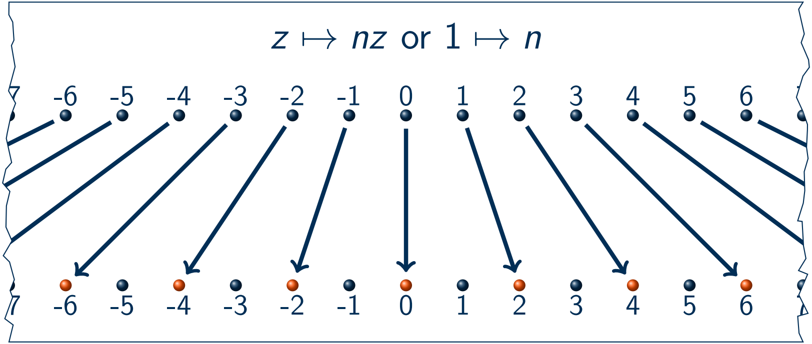
- $z \mapsto nz$ or $1 \mapsto n$

$\mathbb{Z}$ to $n\mathbb{Z}$



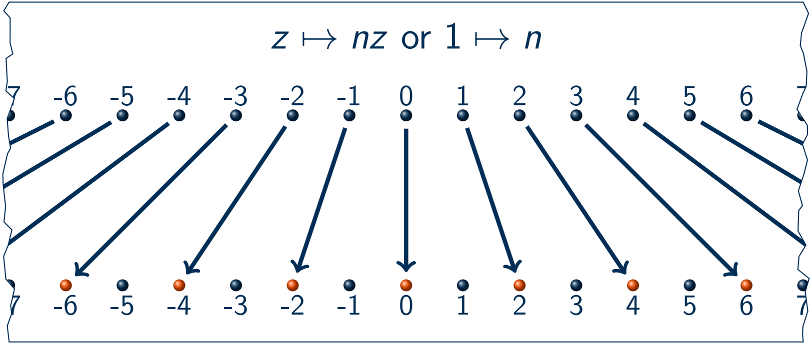
- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$

$\mathbb{Z}$ to $n\mathbb{Z}$



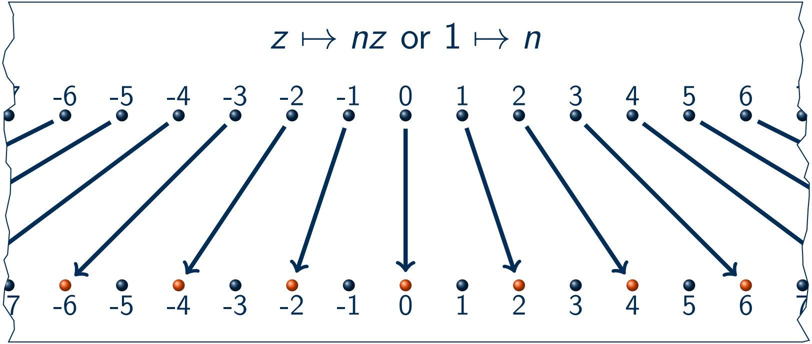
- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$
- $z + w \mapsto n(z + w) = nz + nw$

$\mathbb{Z}$ to $n\mathbb{Z}$



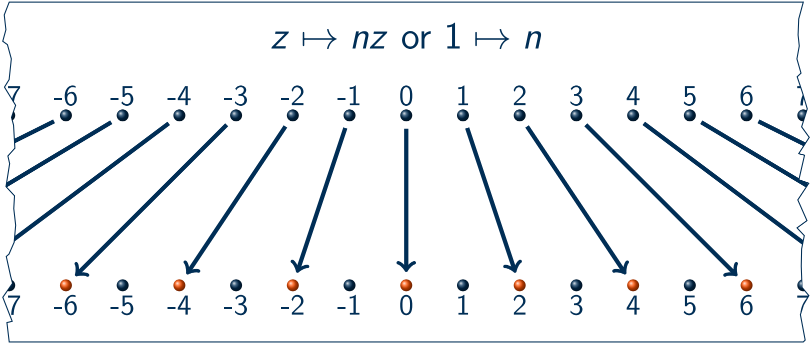
- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$
- $z + w \mapsto n(z + w) = nz + nw$
- $-z \mapsto n(-z) = -nz$

$\mathbb{Z}$ to $n\mathbb{Z}$



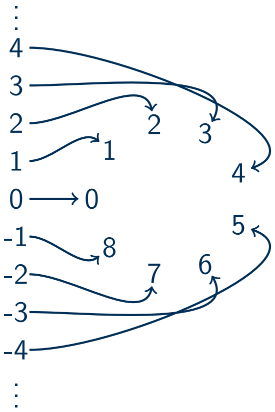
- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$
- $z + w \mapsto n(z + w) = nz + nw$
- $-z \mapsto n(-z) = -nz$
- $0 \mapsto n(0) = 0$

$\mathbb{Z}$ to $n\mathbb{Z}$



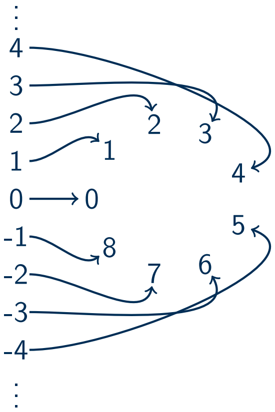
- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$
- $z + w \mapsto n(z + w) = nz + nw$
- $-z \mapsto n(-z) = -nz$
- $0 \mapsto n(0) = 0$
- $ker\phi = \{0\}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



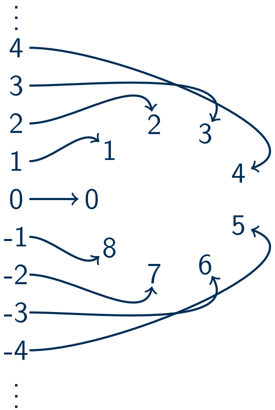
- $z \mapsto z \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



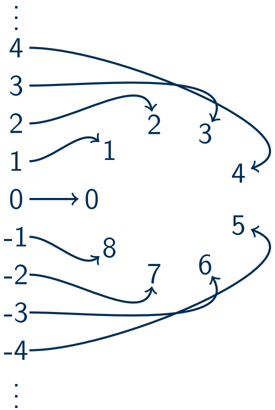
- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



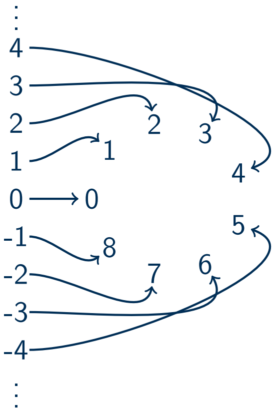
- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



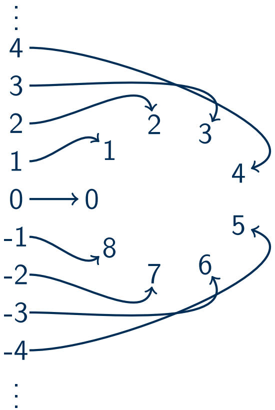
- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



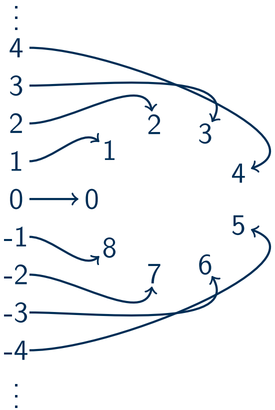
- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$
- $(z + w) \pmod{n} = z \pmod{n} + w \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



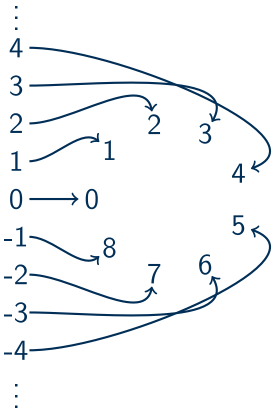
- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$
- $(z + w) \pmod{n} = z \pmod{n} + w \pmod{n}$
- $-z \mapsto -z \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$
- $(z + w) \pmod{n} = z \pmod{n} + w \pmod{n}$
- $-z \mapsto -z \pmod{n}$
- $0 \mapsto 0 \pmod{n}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$
- $(z + w) \pmod{n} = z \pmod{n} + w \pmod{n}$
- $-z \mapsto -z \pmod{n}$
- $0 \mapsto 0 \pmod{n}$
- $\ker \phi = \{nz | z \in \mathbb{Z}\} = n\mathbb{Z}$

A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

0	0
1	1
2	2
	3
	4
	5

A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

- $e \mapsto 0$

$$\begin{array}{ccc} 0 & \longrightarrow & 0 \\ 1 & & 1 \\ 2 & & 2 \\ & & 3 \\ & & 4 \\ & & 5 \end{array}$$

A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

- $e \mapsto 0$
- $1 \mapsto 1$

$$\begin{array}{ccc}
0 & \longrightarrow & 0 \\
1 & \longrightarrow & 1 \\
2 & & 2 \\
 & & 3 \\
 & & 4 \\
 & & 5
\end{array}$$

A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

- $e \mapsto 0$
- $1 \mapsto 1$
- $2 \mapsto 2$

$$\begin{array}{ccc} 0 & \longrightarrow & 0 \\ 1 & \longrightarrow & 1 \\ 2 & \longrightarrow & 2 \\ & & 3 \\ & & 4 \\ & & 5 \end{array}$$

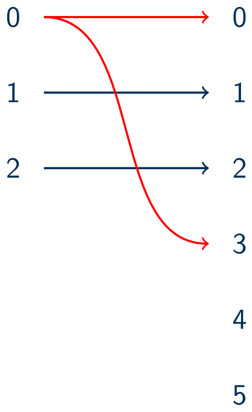
A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

- $e \mapsto 0$
- $1 \mapsto 1$
- $2 \mapsto 2$
- $3 = 1 + 2 \mapsto 1 + 2 = 3$

$$\begin{array}{ccc} 0 & \longrightarrow & 0 \\ 1 & \longrightarrow & 1 \\ 2 & \longrightarrow & 2 \\ & & 3 \\ & & 4 \\ & & 5 \end{array}$$

A Non-Example: $\mathbb{Z}_3$ into $\mathbb{Z}_6$

- $e \mapsto 0$
- $1 \mapsto 1$
- $2 \mapsto 2$
- $3 = 1 + 2 \mapsto 1 + 2 = 3$
- But $3 \equiv 0 \pmod 3 \mapsto 0$



A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$

e	0
r	1
r^2	2
f	3
rf	4
$r^2 f$	5

A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$

$$
\begin{array}{ccc}
e & \longrightarrow & 0 \\
r & & 1 \\
r^2 & & 2 \\
f & & 3 \\
rf & & 4 \\
r^2 f & & 5
\end{array}
$$

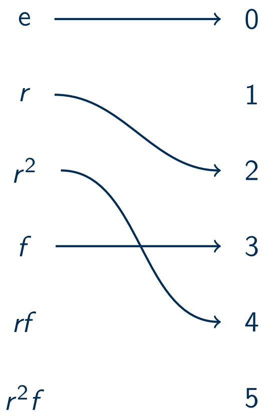
A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$

$$\begin{tikzcd}
e \arrow[r] & 0 \\
r \arrow[dr, bend left] & 1 \\
r^2 \arrow[ddr, bend left] & 2 \\
f & 3 \\
rf & 4 \\
r^2 f & 5
\end{tikzcd}$$

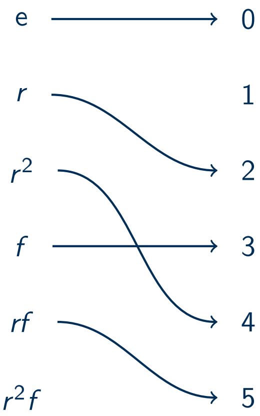
A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$
- $f \mapsto 3$



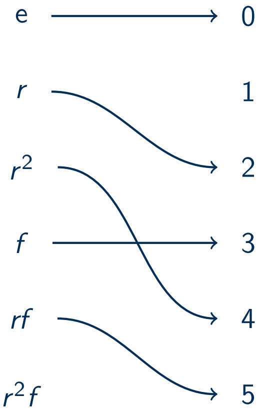
A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$
- $f \mapsto 3$
- $rf \mapsto 2 + 3 = 5$



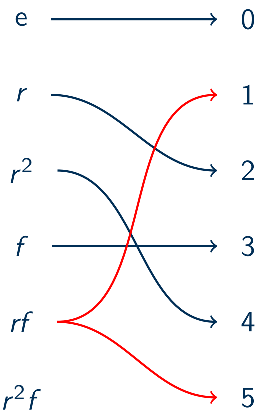
A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$
- $f \mapsto 3$
- $rf \mapsto 2 + 3 = 5$
- $fr^2 \mapsto 3 + 4 = 7 \pmod 6 = 1$



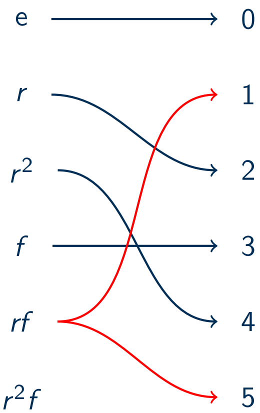
A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$
- $f \mapsto 3$
- $rf \mapsto 2 + 3 = 5$
- $fr^2 \mapsto 3 + 4 = 7 \pmod 6 = 1$
- But $rf = fr^2$



A Non-Example: D_3 to $\mathbb{Z}_6$

- $|D_3| = |\mathbb{Z}_6| = 6$
- $e \mapsto 0$
- $r^i \mapsto 2i$
- $f \mapsto 3$
- $rf \mapsto 2 + 3 = 5$
- $fr^2 \mapsto 3 + 4 = 7 \pmod 6 = 1$
- But $rf = fr^2$
- D_n is non-abelian and $\mathbb{Z}_n$ is abelian



Properties of Homomorphisms

Theorem

If $\phi : G \to H$ is a homomorphism, then:

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}$
3. $\phi(g^n) = \phi(g)^n$
4. $|\phi(g)|$ *divides* $|g|$
5. $\phi(G)$ *is a subgroup of* H

Proof of Order Property

Proof.

1. $|g| = l$ implies $e_H = \phi(e_G) = \phi(g^l) = \phi(g)^l$

$\square$

Proof of Order Property

Proof.

1. $|g| = l$ implies $e_H = \phi(e_G) = \phi(g^l) = \phi(g)^l$
2. $|\phi(g)| = k \leq l$

$\square$

Proof of Order Property

Proof.

1. $|g| = l$ implies $e_H = \phi(e_G) = \phi(g^l) = \phi(g)^l$
2. $|\phi(g)| = k \leq l$
3. By previous theorem $k|l$

$\square$

Proof of Order Property

Proof.

1. $|g| = l$ implies $e_H = \phi(e_G) = \phi(g^l) = \phi(g)^l$
2. $|\phi(g)| = k \leq l$
3. By previous theorem $k|l$
4. $\therefore |phi(g)|$ divides $|g|$

□

Properties of Homomorphisms

Theorem

If $\phi : G \to H$ is a homomorphism, then:

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}$
3. $\phi(g^n) = \phi(g)^n$
4. $|\phi(g)|$ *divides* $|g|$
5. $\phi(G)$ *is a subgroup of* H

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$

$\square$

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$
2. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$

$\square$

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$
2. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$
3. $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) \in \phi(G)$

$\square$

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$
2. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$
3. $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) \in \phi(G)$
4. $h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \phi(G)$

$\square$

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$
2. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$
3. $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) \in \phi(G)$
4. $h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \phi(G)$
5. $\phi(G)$ is closed under the operation and inverses

$\square$

Proof of Subgroup Property

Proof.

1. $h_1, h_2 \in \phi(G) \subseteq H$
2. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$
3. $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) \in \phi(G)$
4. $h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \phi(G)$
5. $\phi(G)$ is closed under the operation and inverses
6. $\therefore \phi(G)$ is a subgroup by the two-step subgroup test

$\square$

Properties of Homomorphisms

Theorem

If $\phi : G \to H$ is a homomorphism, then:

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}$
3. $\phi(g^n) = \phi(g)^n$
4. $|\phi(g)|$ *divides* $|g|$
5. $\phi(G)$ *is a subgroup of* H

A Couple Special Maps

Theorem

Given a group G the map $\phi(g) = g$ is called the **identity map** *and is always a homomorphism.*

A Couple Special Maps

Theorem

Given a group G the map $\phi(g) = g$ is called the **identity map** *and is always a homomorphism.*

Theorem

Given groups G and H the map $\phi(g) = e_H$ is called the **trivial map** *and is always a homomorphism.*

Table of Contents

1. Homomorphisms
2. Isomorphisms
3. Groups and Actions
4. Cayley's Theorem

Isomorphisms

Definition (Surjective)

A homomorphism $\phi : G \to H$ is **surjective** if for all $h \in H$ there exists $g \in G$ such that $\phi(g) = h$.

Isomorphisms

Definition (Surjective)

A homomorphism $\phi : G \to H$ is **surjective** if for all $h \in H$ there exists $g \in G$ such that $\phi(g) = h$.

Definition (Injective)

A homomorphism $\phi : G \to H$ is **injective** if $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$.

Isomorphisms

Definition (Surjective)

A homomorphism $\phi : G \to H$ is **surjective** if for all $h \in H$ there exists $g \in G$ such that $\phi(g) = h$.

Definition (Injective)

A homomorphism $\phi : G \to H$ is **injective** if $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$.

Definition (Isomorphism)

An **isomorphism of groups** is a homomorphism which is injective and surjective.

Sample Isomorphism

Example

Let

$$G = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$$

which is a group with the operation of vector addition. Then define $\phi : G \to G$ by

$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 3a + 2b \\ 4a + 3b \end{pmatrix}.$$

Since the matrix has determinant 1, $3 \cdot 3 - 2 \cdot 4 = 1$, the matrix is invertible, and in general $M(\vec{v} + \vec{w}) = M\vec{v} + M\vec{w}$. Therefore, this is an isomorphism.

Sample Non-Isomorphism

Non-Example

Let

$$G = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$$

which is a group with the operation of vector addition. Then define $\phi : G \to G$ by

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}.$$

All vectors of the form $(0, b)^T$ map to $(0, 0)^T$, so this map is not injective. Similarly, it is "clearly" not surjective. Thus ϕ is not an isomorphism. However, it is still a homomorphism. Note that

$$ker\phi = \left\{ \begin{pmatrix} 0 \\ b \end{pmatrix} \middle| b \in \mathbb{Z} \right\},$$

in linear algebra this is called the **Null Space** of the linear transformation.

Kernels, Injective Maps, and Isomorphisms

Theorem

Given a homomorphism $\phi : G \to H$, $\ker\phi = \{e\}$ if and only if ϕ is injective.

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker \phi = \{e\}$

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker \phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker\phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker\phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker\phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

If.

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker \phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

If.

1. Assume ϕ is an injective homomorphism

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker \phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

If.

1. Assume ϕ is an injective homomorphism
2. $a \in ker\phi$ implies $\phi(a) = e$ and $\phi(a) = \phi(e)$

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker \phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

If.

1. Assume ϕ is an injective homomorphism
2. $a \in ker\phi$ implies $\phi(a) = e$ and $\phi(a) = \phi(e)$
3. $\phi(a) = \phi(e)$ implies $a = e$

$\square$

Kernels and Injections

Only If.

1. Assume ϕ is a homomorphism and $\ker\phi = \{e\}$
2. $\phi(a) = \phi(b)$ implies $\phi(a)\phi(b)^{-1} = e$
3. $\phi(ab^{-1}) = e$ and $ab^{-1} \in ker\phi$
4. $\therefore ab^{-1} = e$, $a = b$, and ϕ is injective

$\square$

If.

1. Assume ϕ is an injective homomorphism
2. $a \in ker\phi$ implies $\phi(a) = e$ and $\phi(a) = \phi(e)$
3. $\phi(a) = \phi(e)$ implies $a = e$
4. $\therefore ker\phi = \{e\}$

$\square$

Kernels, Injective Maps, and Isomorphisms

Theorem

Given a homomorphism $\phi : G \to H$, *ker*$\phi = \{e\}$ *if and only if* ϕ *is injective.*

Theorem

Given a homomorphism $\phi : G \to H$, $\phi : G \to \phi(G)$ *is always surjective.*

Kernels, Injective Maps, and Isomorphisms

Theorem

Given a homomorphism $\phi : G \to H$, $\ker\phi = \{e\}$ if and only if ϕ is injective.

Theorem

Given a homomorphism $\phi : G \to H$, $\phi : G \to \phi(G)$ is always surjective.

Theorem

Given a homomorphism $\phi : G \to H$, ϕ is injective if and only if G is isomorphic to $\phi(G)$.

Kernels, Injective Maps, and Isomorphisms

Theorem

Given a homomorphism $\phi : G \to H$, $\ker\phi = \{e\}$ if and only if ϕ is injective.

Theorem

Given a homomorphism $\phi : G \to H$, $\phi : G \to \phi(G)$ is always surjective.

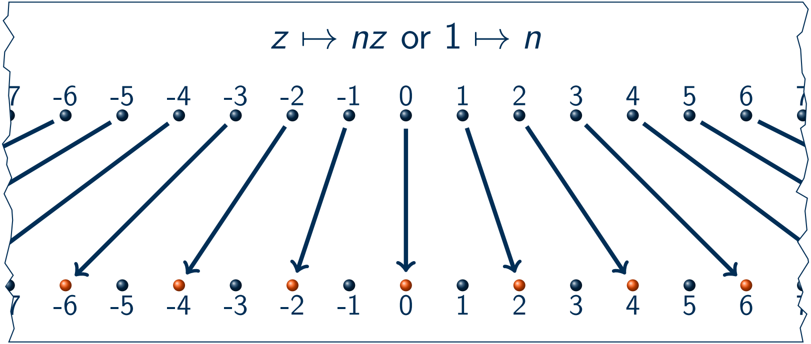
Theorem

Given a homomorphism $\phi : G \to H$, ϕ is injective if and only if G is isomorphic to $\phi(G)$.

Corollary

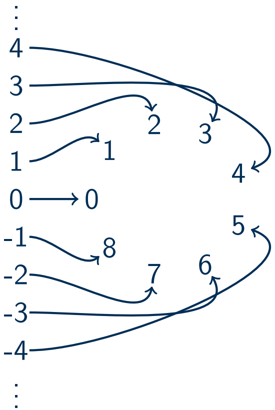
Given a homomorphism $\phi : G \to H$, $\ker\phi = \{e\}$ if and only if G is isomorphic to $\phi(G)$.

$\mathbb{Z}$ to $n\mathbb{Z}$



- $z \mapsto nz$ or $1 \mapsto n$
- $w \mapsto nw$
- $z + w \mapsto n(z + w) = nz + nw$
- $-z \mapsto n(-z) = -nz$
- $0 \mapsto n(0) = 0$
- $ker\phi = \{0\}$

$\mathbb{Z}$ to $\mathbb{Z}_n$



- $z \mapsto z \pmod{n}$
- or $1 \mapsto 1 \pmod{n}$
- $w \mapsto w \pmod{n}$
- $z + w \mapsto (z + w) \pmod{n}$
- $(z + w) \pmod{n} = z \pmod{n} + w \pmod{n}$
- $-z \mapsto -z \pmod{n}$
- $0 \mapsto 0 \pmod{n}$
- $\ker \phi = \{nz | z \in \mathbb{Z}\} = n\mathbb{Z}$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Theorem

If $G = \langle a \rangle$ is a cyclic group, then

1. $G \cong \mathbb{Z}$ *when* $|G| = \infty$, *and*
2. $G \cong \mathbb{Z}_n$ *when* $|G| = n$.

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$

□

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$

$\square$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod n$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod n = i \pmod n + j \pmod n = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism

$\square$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i+j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism
5. $\forall i \in \mathbb{Z}_n : \ \phi(a^i) = i$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism
5. $\forall i \in \mathbb{Z}_n : \ \phi(a^i) = i$
6. $\therefore \phi$ is onto

$\square$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism
5. $\forall i \in \mathbb{Z}_n : \ \phi(a^i) = i$
6. $\therefore \phi$ is onto
7. $\phi(a^i) = 0$ implies $i \equiv 0 \pmod{n}$, i.e. $i = qn$

$\square$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism
5. $\forall i \in \mathbb{Z}_n : \ \phi(a^i) = i$
6. $\therefore \phi$ is onto
7. $\phi(a^i) = 0$ implies $i \equiv 0 \pmod{n}$, i.e. $i = qn$
8. $a^i = a^{qn} = (a^n)^q = e^q = e$

$\square$

Cyclic Groups, $\mathbb{Z}$, and $\mathbb{Z}_n$

Part 2.

1. $G = \langle a \rangle$ and $|G| = n$
2. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(a^i) = i \pmod{n}$, (or by $\phi(a) = 1$)
3. $\phi(a^i a^j) = (i + j) \pmod{n} = i \pmod{n} + j \pmod{n} = \phi(a^i) + \phi(a^j)$
4. $\therefore \phi$ is a homomorphism
5. $\forall i \in \mathbb{Z}_n : \ \phi(a^i) = i$
6. $\therefore \phi$ is onto
7. $\phi(a^i) = 0$ implies $i \equiv 0 \pmod{n}$, i.e. $i = qn$
8. $a^i = a^{qn} = (a^n)^q = e^q = e$
9. $\therefore ker\phi = \{e\}$ and ϕ is 1-1

$\square$

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism
- $a = g(g^{-1}ag)g^{-1}$; conjugation is surjective

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism
- $a = g(g^{-1}ag)g^{-1}$; conjugation is surjective
- $gag^{-1} = e$ implies $a = g^{-1}eg = e$; conjugation is injective

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism
- $a = g(g^{-1}ag)g^{-1}$; conjugation is surjective
- $gag^{-1} = e$ implies $a = g^{-1}eg = e$; conjugation is injective
- $\therefore$ Conjugation is an isomorphism.

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism
- $a = g(g^{-1}ag)g^{-1}$; conjugation is surjective
- $gag^{-1} = e$ implies $a = g^{-1}eg = e$; conjugation is injective
- $\therefore$ Conjugation is an isomorphism.

Theorem

Given a group G, subgroup $H \subseteq G$, and $g \in G$,

$$gHg^{-1} = \left\{ ghg^{-1} \middle| h \in H \right\}$$

is also a subgroup of G.

Conjugation

Conjugation Isomorphism

Given a group G and $g \in G$, conjugation by g is the map defined by $a \mapsto gag^{-1}$. Note that:

- $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$; conjugation is a homomorphism
- $a = g(g^{-1}ag)g^{-1}$; conjugation is surjective
- $gag^{-1} = e$ implies $a = g^{-1}eg = e$; conjugation is injective
- $\therefore$ Conjugation is an isomorphism.

Theorem

Given a group G, subgroup $H \subseteq G$, and $g \in G$,

$$gHg^{-1} = \left\{ ghg^{-1} \middle| h \in H \right\}$$

is also a subgroup of G.(Proved using the 2-step subgroup test.)

Centralizers and Center

Definition (Centralizer)

Given a group G and element $g \in G$, the **centralizer of g** is the set of all elements $a \in G$ which commute with g:

$$C(g) = \{a | ga = ag\} = \left\{ a \middle| gag^{-1} = a \right\}.$$

Definition (Center)

Given a group G, the **center of G** is the set of all elements $a \in G$ which commute with all elements in G:

$$Z(G) = \{a | \forall g \in G : ga = ag\} = \left\{ a \middle| \forall g \in G : gag^{-1} = a \right\}.$$

Notes on Centralizers and Center

Notes

- The 2-step subgroup test can show that $C(g)$ and $Z(G)$ are subgroups.
- $C(g)$ is fixed when conjugating by g, $gC(g)g^{-1} = C(g)$.
- $\langle g \rangle \subseteq C(g)$ and $Z(G) \subseteq C(g)$ so centralizers are never empty
- $Z(G)$ is fixed when conjugating by any $g \in G$, $gZ(G)g^{-1} = Z(G)$
- $Z(G) = \bigcap_{g \in G} C(g)$
- $\{e\} \subset Z(G)$ so the center is never empty

Table of Contents

1. Homomorphisms
2. Isomorphisms
3. Groups and Actions
4. Cayley's Theorem

Groups Acting on Themselves

Theorem

Let G be a group, then for all $g \in G$ the map $T_g : G \to G$ defined by $T_g(h) = gh$ is a bijection.

Groups Acting on Themselves

Theorem

Let G be a group, then for all $g \in G$ the map $T_g : G \to G$ defined by $T_g(h) = gh$ is a bijection.

Injective.

Given $h, k \in G$:

$$\begin{aligned} T_g(h) = T_g(k) &\Rightarrow gh = gk \\ &\Rightarrow g^{-1}gh = g^{-1}gk \\ &\Rightarrow h = k, \end{aligned}$$

therefore, T_g is injective. □

Groups Acting on Themselves

Theorem

Let G be a group, then for all $g \in G$ the map $T_g : G \to G$ defined by $T_g(h) = gh$ is a bijection.

Surjective.

Given $h \in G$:

$$\begin{aligned} h &= gg^{-1}h \\ &= T_g(g^{-1}h) \end{aligned}$$

therefore, T_g is surjective. □

Groups Acting on Themselves

Theorem

Let G be a group, then for all $g \in G$ the map $T_g : G \to G$ defined by $T_g(h) = gh$ is a bijection.

Not a Homomorphism

Note $T_g(e) = ge = g$, so T_g is not a homomorphism. However, since it is a bijective map from G to its self, it is a permutation of the elements of G.

Example

$\mathbb{Z}_n$ acting on its self

For a set S and element a recall that $aS = \{as | s \in S\}$. This may be written $a + S$ if addition is the appropriate operation. For example, if we add 2 to the set of equivalence classes in $\mathbb{Z}_6$ we get

$$\begin{aligned} 2 + \mathbb{Z}_6 &= 2 + \{0, 1, 2, 3, 4, 5\} \\ &= \{2 + 0, 2 + 1, 2 + 2, 2 + 3, 2 + 4, 2 + 5\} \\ &= \{2, 3, 4, 5, 0, 1\} \end{aligned}$$

Example

$\mathbb{Z}_n$ acting on its self

For a set S and element a recall that $aS = \{as | s \in S\}$. This may be written $a + S$ if addition is the appropriate operation. For example, if we add 2 to the set of equivalence classes in $\mathbb{Z}_6$ we get

$$\begin{aligned} 2 + \mathbb{Z}_6 &= 2 + \{0, 1, 2, 3, 4, 5\} \\ &= \{2+0, 2+1, 2+2, 2+3, 2+4, 2+5\} \\ &= \{2, 3, 4, 5, 0, 1\} \end{aligned}$$

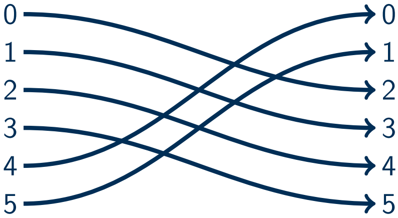


Table of Contents

1 Homomorphisms

2 Isomorphisms

3 Groups and Actions

4 Cayley's Theorem

Cayley's Theorem: Statement

Theorem (Cayley's Theorem)

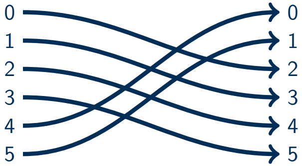
Every group is isomorphic to a group of permutations.

Example

$\mathbb{Z}_n$ acting on its self

For a set S and element a recall that $aS = \{as|s \in S\}$. This may be written $a + S$ if addition is the appropriate operation. For example, if we add 2 to the set of equivalence classes in $\mathbb{Z}_6$ we get

$$\begin{aligned} 2 + \mathbb{Z}_6 &= 2 + \{0, 1, 2, 3, 4, 5\} \\ &= \{2+0, 2+1, 2+2, 2+3, 2+4, 2+5\} \\ &= \{2, 3, 4, 5, 0, 1\} \end{aligned}$$



$$2 \longrightarrow T_2(g) = 2 + g \longrightarrow (024)(135) \in S_6$$

Cayley's Theorem: Proof

Lemma

For each $g \in G$ define $T_g(x) = gx$ for all $x \in G$, the set

$$T_G = \{T_g | g \in G\}$$

is a group with the operation of composition.

Proof.

1. Closure: $T_g \circ T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = T_{gh}(x)$

□

Cayley's Theorem: Proof

Lemma

For each $g \in G$ define $T_g(x) = gx$ for all $x \in G$, the set

$$T_G = \{T_g | g \in G\}$$

is a group with the operation of composition.

Proof.

1. Closure: $T_g \circ T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = T_{gh}(x)$
2. Associative: $T_g \circ (T_h \circ T_k) = T_{g(hk)} = T_{(gh)k} = (T_g \circ T_h) \circ T_k$

$\square$

Cayley's Theorem: Proof

Lemma

For each $g \in G$ define $T_g(x) = gx$ for all $x \in G$, the set

$$T_G = \{T_g | g \in G\}$$

is a group with the operation of composition.

Proof.

1. Closure: $T_g \circ T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = T_{gh}(x)$
2. Associative: $T_g \circ (T_h \circ T_k) = T_{g(hk)} = T_{(gh)k} = (T_g \circ T_h) \circ T_k$
3. Identity: $T_g \circ T_e(x) = T_g(T_e(x)) = T_g(x)$

□

Cayley's Theorem: Proof

Lemma

For each $g \in G$ define $T_g(x) = gx$ for all $x \in G$, the set

$$T_G = \{T_g | g \in G\}$$

is a group with the operation of composition.

Proof.

1. Closure: $T_g \circ T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = T_{gh}(x)$
2. Associative: $T_g \circ (T_h \circ T_k) = T_{g(hk)} = T_{(gh)k} = (T_g \circ T_h) \circ T_k$
3. Identity: $T_g \circ T_e(x) = T_g(T_e(x)) = T_g(x)$
4. Inverse: $T_g \circ T_{g^{-1}}(x) = gg^{-1}x = x = T_e(x)$

□

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self

□

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G

$\square$

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G
3. Define $\phi : G \to A(G)$ by $g \mapsto T_g$

$\square$

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G
3. Define $\phi : G \to A(G)$ by $g \mapsto T_g$
4. By the lemma, $T_G = \{T_g | g \in G\}$ is a subgroup of $A(G)$

$\square$

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G
3. Define $\phi : G \to A(G)$ by $g \mapsto T_g$
4. By the lemma, $T_G = \{T_g | g \in G\}$ is a subgroup of $A(G)$
5. $\phi(gh) = T_{gh} = T_g \circ T_h = \phi(g) \circ \phi(h)$ so ϕ is a homomorphism

$\square$

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G
3. Define $\phi : G \to A(G)$ by $g \mapsto T_g$
4. By the lemma, $T_G = \{T_g | g \in G\}$ is a subgroup of $A(G)$
5. $\phi(gh) = T_{gh} = T_g \circ T_h = \phi(g) \circ \phi(h)$ so ϕ is a homomorphism
6. $\phi(g) = T_g = T_e$ implies $g = e$ so that $ker\phi = \{e\}$ and ϕ is 1-1

$\square$

Cayley's Theorem: Proof

Cayley's Theorem.

1. A permutation of a set is any bijection from the set to its self
2. Let $A(G)$ be the set of all possible permutations of the elements of G
3. Define $\phi : G \to A(G)$ by $g \mapsto T_g$
4. By the lemma, $T_G = \{T_g | g \in G\}$ is a subgroup of $A(G)$
5. $\phi(gh) = T_{gh} = T_g \circ T_h = \phi(g) \circ \phi(h)$ so ϕ is a homomorphism
6. $\phi(g) = T_g = T_e$ implies $g = e$ so that $ker\phi = \{e\}$ and ϕ is 1-1
7. $\therefore$ G is isomorphic to $\phi(G) = T_G \subseteq A(G)$

$\square$

Cayley's Theorem: Statement

Theorem (Cayley's Theorem)

Every group is isomorphic to a group of permutations.

Corollary

Every group of order n is isomorphic to a subgroup of the symmetric group S_n.

Cayley's Theorem: Proof

Corollary.

1. Let $A(G)$ be the set of all possible permutations of the elements of G

$\square$

Cayley's Theorem: Proof

Corollary.

1. Let $A(G)$ be the set of all possible permutations of the elements of G
2. $|G| = n$ means $A(G)$ is a set of permutations of n elements

$\square$

Cayley's Theorem: Proof

Corollary.

1. Let $A(G)$ be the set of all possible permutations of the elements of G
2. $|G| = n$ means $A(G)$ is a set of permutations of n elements
3. By "definition" $A(G)$ is isomorphic to S_n

$\square$

Cayley's Theorem: Statement

Theorem (Cayley's Theorem)

Every group is isomorphic to a group of permutations.

Corollary

Every group of order n is isomorphic to a subgroup of the symmetric group S_n.

Groups and Homomorphisms

Dr. Chuck Rocca