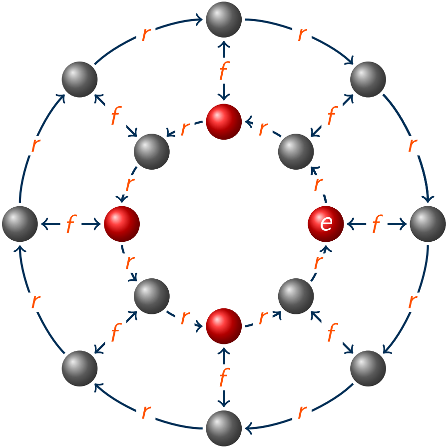
# Quotients and Homomorphisms

Dr. Chuck Rocca

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

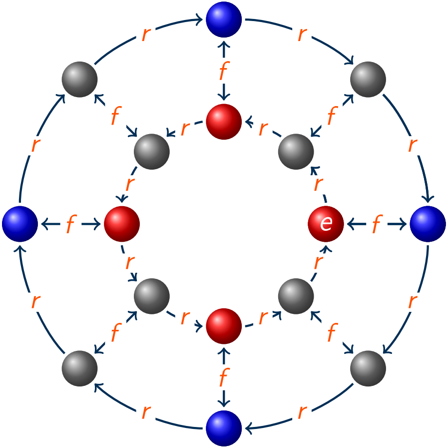
# Table of Contents

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



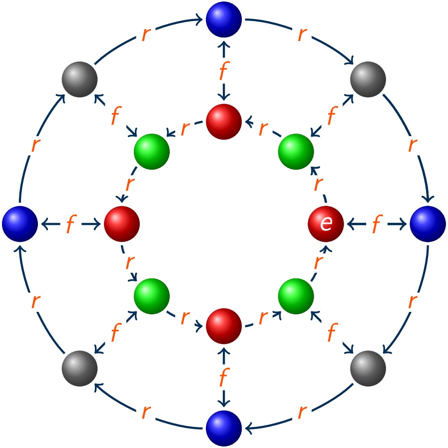

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$

## $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



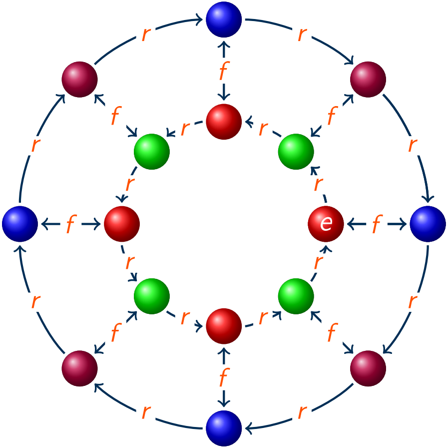

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



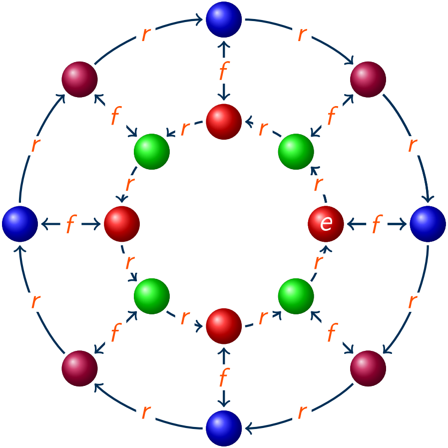

- $\left\langle r^2 \right\rangle = \left\{ r^2, r^4, r^6, e \right\}$
- $f \left\langle r^2 \right\rangle = \left\{ fr^2, fr^4, fr^6, f \right\}$
- $r \left\langle r^2 \right\rangle = \left\{ r^3, r^5, r^7, r \right\}$

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$




- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

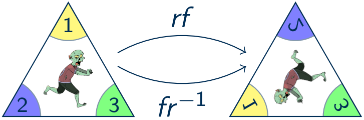
# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$




- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r \langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr \langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{r^2 f, r^4 f, r^6 f, f\}$

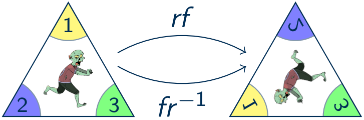
# Calculating in $D_n$

$$D_n = \left\langle r, f \,\middle|\, r^n = f^2 = e, rf = fr^{-1} \right\rangle$$



# Calculating in $D_n$

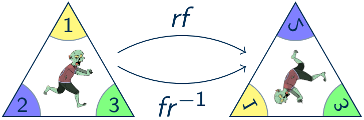
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$




$r^3 f$

# Calculating in $D_n$

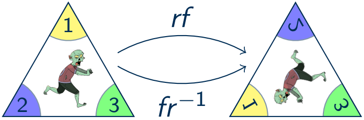
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$




$$r^3 f = r^2(rf)$$

# Calculating in $D_n$

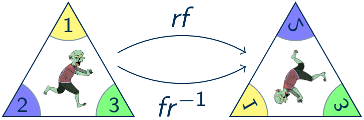
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \end{aligned}$$

# Calculating in $D_n$

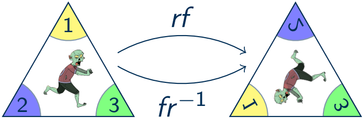
$$D_n = \left\langle r, f \,\middle|\, r^n = f^2 = e, rf = fr^{-1} \right\rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \end{aligned}$$

# Calculating in $D_n$

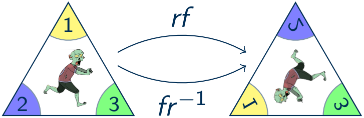
$$D_n = \left\langle r, f \,\middle|\, r^n = f^2 = e, rf = fr^{-1} \right\rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \end{aligned}$$

# Calculating in $D_n$

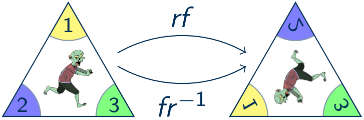
$$D_n = \langle r, f \mid r^n = f^2 = e, rf = fr^{-1} \rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \end{aligned}$$

# Calculating in $D_n$

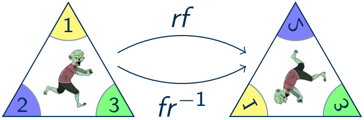
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \end{aligned}$$

# Calculating in $D_n$

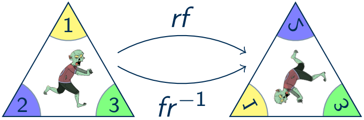
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$




$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \\ &= fr^{n-3} \end{aligned}$$

# Calculating in $D_n$

$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$

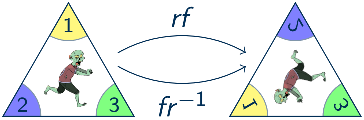



$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \\ &= fr^{n-3} \end{aligned}$$

$$r^k f = fr^{-k} = fr^{n-k}$$

# Calculating in $D_n$

$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$

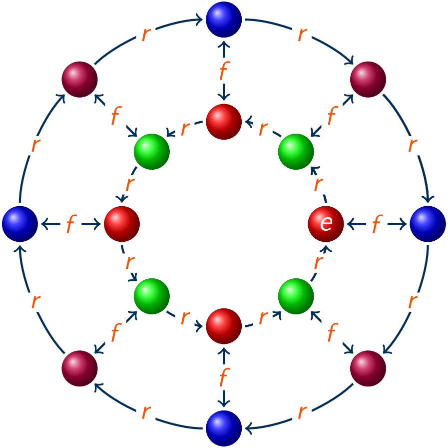



$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \\ &= fr^{n-3} \end{aligned}$$

$$r^k f = fr^{-k} = fr^{n-k}$$

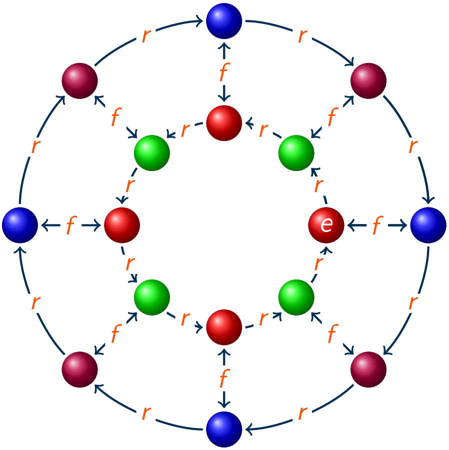
$$fr^k = r^{-k} f = r^{n-k} f$$

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



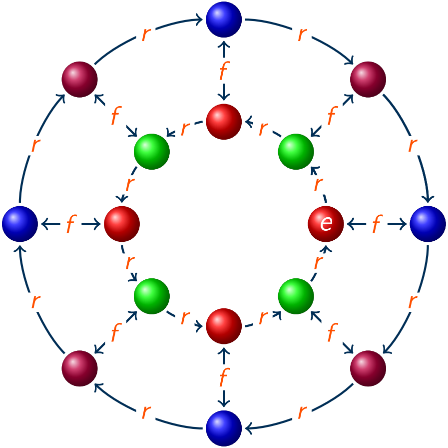

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r \langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr \langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{r^2 f, r^4 f, r^6 f, f\}$

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



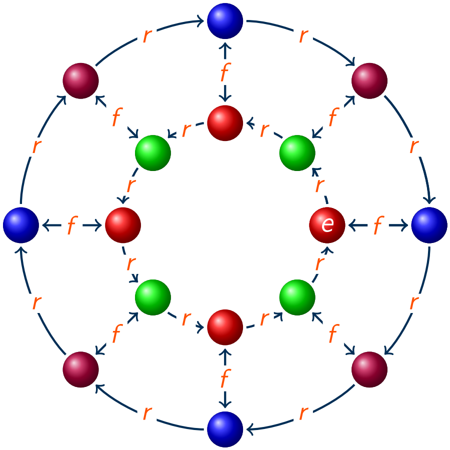

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r \langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr \langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$

# $D_8 = \left\langle r, f \,\middle|\, r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



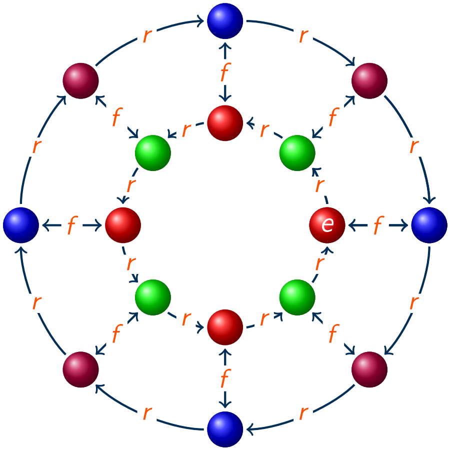

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$
- $\langle r^2 \rangle r = \{r^3, r^5, r^7, r\}$

# $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$




- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$
- $\langle r^2 \rangle r = \{r^3, r^5, r^7, r\}$
- $\langle r^2 \rangle fr = \{r^2 fr, r^4 fr, r^6 fr, fr\}$

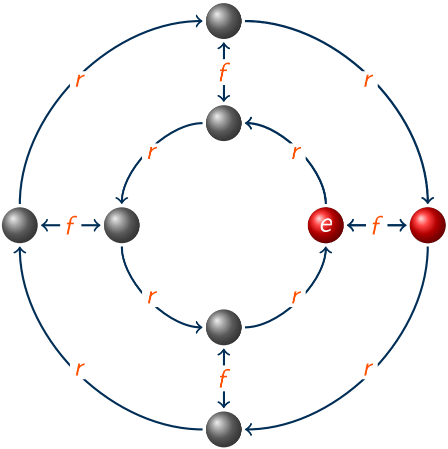
## $D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$




- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$
- $\langle r^2 \rangle r = \{r^3, r^5, r^7, r\}$
- $\langle r^2 \rangle fr = \{fr^7, fr^5, fr^3, fr\}$

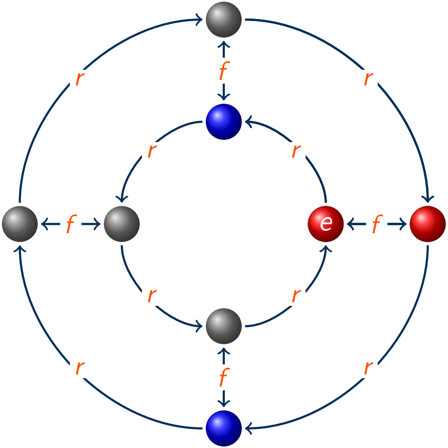
$$D_8 = \langle r^2 \rangle \cup f\langle r^2 \rangle \cup r\langle r^2 \rangle \cup fr\langle r^2 \rangle$$

# $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



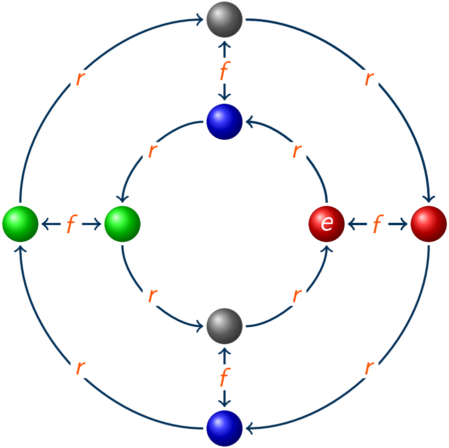

- $\langle f \rangle = \{f, e\}$

## $D_4 = \left\langle r, f \,\middle|\, r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



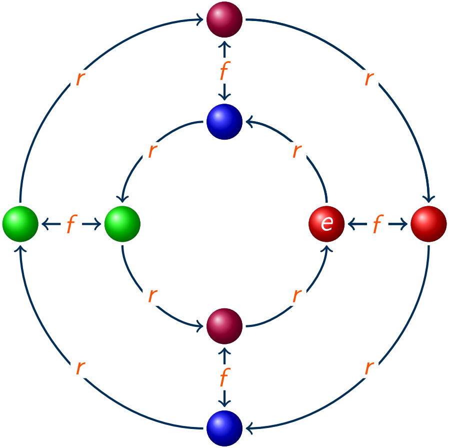

- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$

# $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



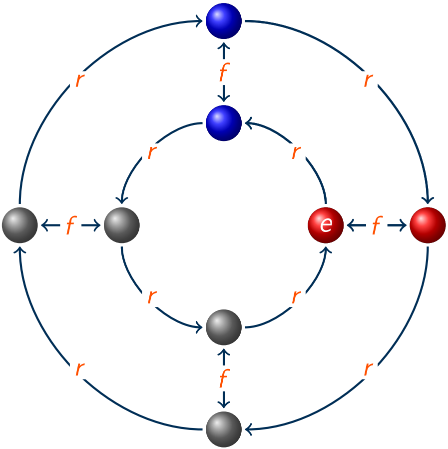

- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$

## $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



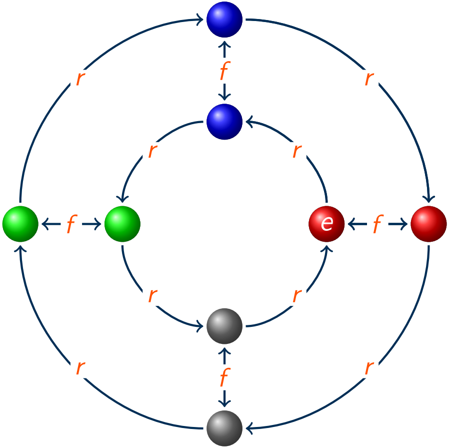

- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $r^2 \langle f \rangle = \{r^2 f, r^2\}$
- $r^3 \langle f \rangle = \{r^3 f, r^3\}$

## $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



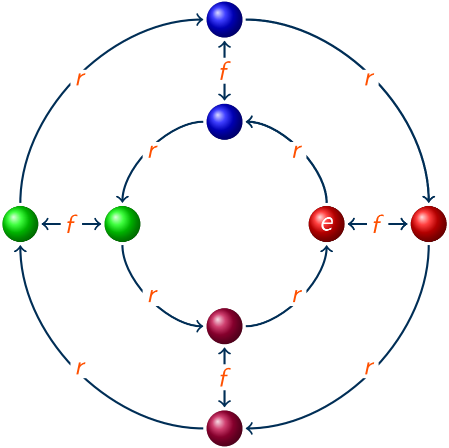

- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $r^2 \langle f \rangle = \{r^2 f, r^2\}$
- $r^3 \langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$

# $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



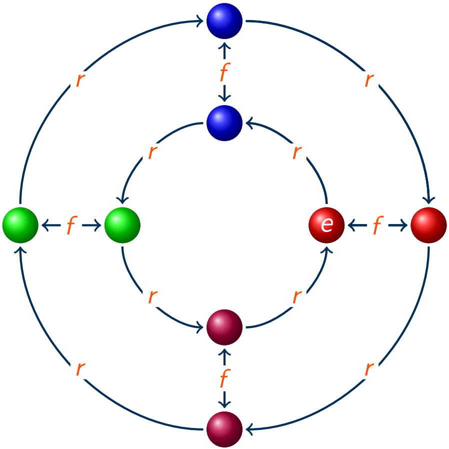

- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $r^2 \langle f \rangle = \left\{r^2 f, r^2\right\}$
- $r^3 \langle f \rangle = \left\{r^3 f, r^3\right\}$
- $\langle f \rangle r = \{fr, r\} = \left\{r^3 f, r\right\}$
- $\langle f \rangle r^2 = \left\{fr^2, r^2\right\} = \left\{r^2 f, r^2\right\}$

# $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



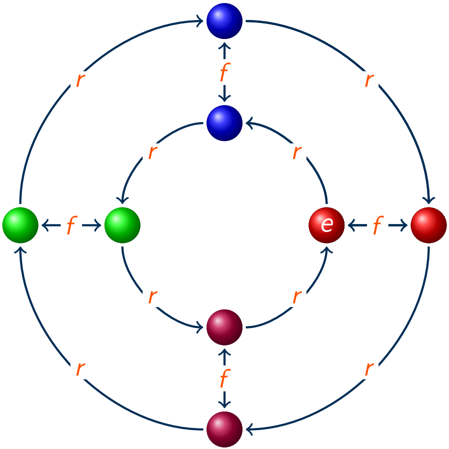

- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \left\{r^2f, r^2\right\}$
- $r^3\langle f \rangle = \left\{r^3f, r^3\right\}$
- $\langle f \rangle r = \{fr, r\} = \left\{r^3f, r\right\}$
- $\langle f \rangle r^2 = \left\{fr^2, r^2\right\} = \left\{r^2f, r^2\right\}$
- $\langle f \rangle r^3 = \left\{fr^3, r^3\right\} = \left\{rf, r^3\right\}$

# $D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$




- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $r^2 \langle f \rangle = \{r^2 f, r^2\}$
- $r^3 \langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$
- $\langle f \rangle r^2 = \{fr^2, r^2\} = \{r^2 f, r^2\}$
- $\langle f \rangle r^3 = \{fr^3, r^3\} = \{rf, r^3\}$
- $\exists g \in D_4 : g \langle f \rangle \neq \langle f \rangle g$

# $D_4 = \langle r, f \mid r^4 = f^2 = e, rf = fr^{-1} \rangle$




- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $r^2 \langle f \rangle = \{r^2 f, r^2\}$
- $r^3 \langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$
- $\langle f \rangle r^2 = \{fr^2, r^2\} = \{r^2 f, r^2\}$
- $\langle f \rangle r^3 = \{fr^3, r^3\} = \{rf, r^3\}$
- $\exists g \in D_4 : g \langle f \rangle \neq \langle f \rangle g$

$$D_4 = \langle f \rangle \cup r \langle f \rangle \cup r^2 \langle f \rangle \cup r^3 \langle f \rangle$$

# Definition of Cosets

**Definition (Coset)**

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

$$gH = \{gh|h \in H\}$$

is a **left coset of** $H$ and

$$Hg = \{hg|h \in H\}$$

is a **right coset of** $H$.

# Definition of Cosets

**Definition (Coset)**

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

$$gH = \{gh | h \in H\}$$

is a **left coset of** $H$ and

$$Hg = \{hg | h \in H\}$$

is a **right coset of** $H$.

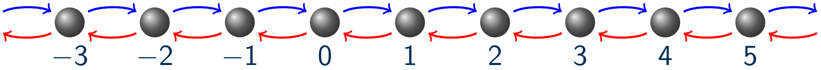
**Definition (Normal Subgroup)**

Given a group $G$ and subgroup $H$, if for all $g \in G$,

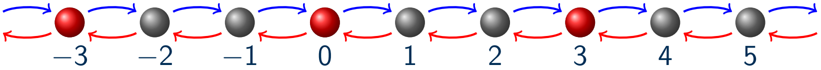
$$gH = Hg,$$

then we say that $H$ is a **normal subgroup** of $G$.

# $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$

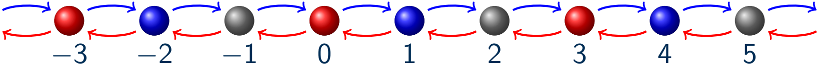


# $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



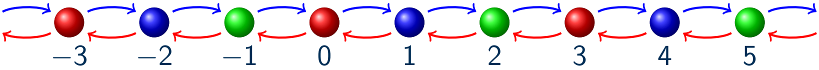

- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

# $\mathbb{Z} = \{0, \pm1, \pm2, \ldots\}$



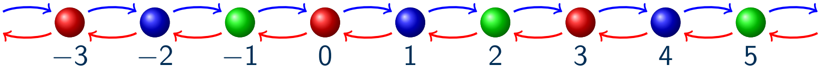

- $3\mathbb{Z} = \{0, \pm3, \pm6, \pm9, \ldots\}$
- $1 + 3\mathbb{Z} = \{1, -2, 4, -5, 7, \ldots\}$

# $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$




- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$
- $1 + 3\mathbb{Z} = \{1, -2, 4, -5, 7, \ldots\}$
- $2 + 3\mathbb{Z} = \{2, -1, 5, -4, 8, \ldots\}$

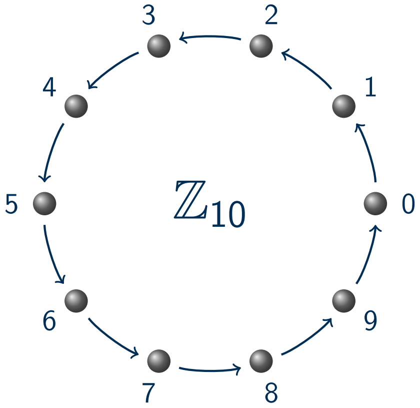
# $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



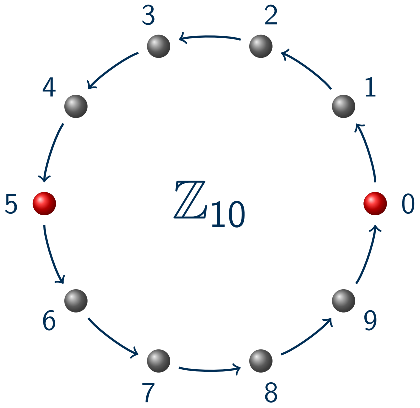

- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$
- $1 + 3\mathbb{Z} = \{1, -2, 4, -5, 7, \ldots\}$
- $2 + 3\mathbb{Z} = \{2, -1, 5, -4, 8, \ldots\}$

$$\mathbb{Z} = 3\mathbb{Z} \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z})$$

## $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

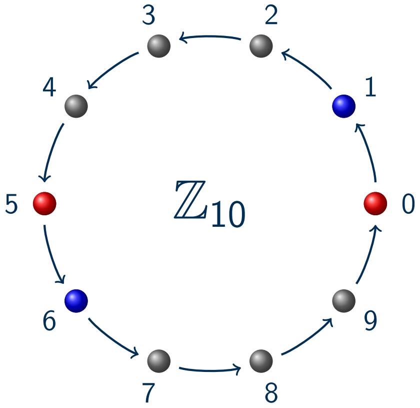


# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



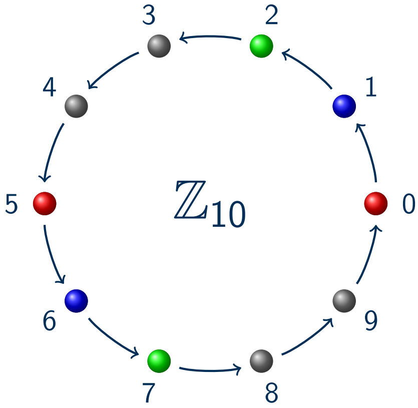

- $\langle 5 \rangle = \{0, 5\}$

# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



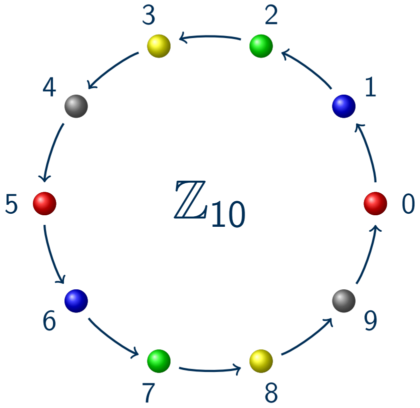

- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$

# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



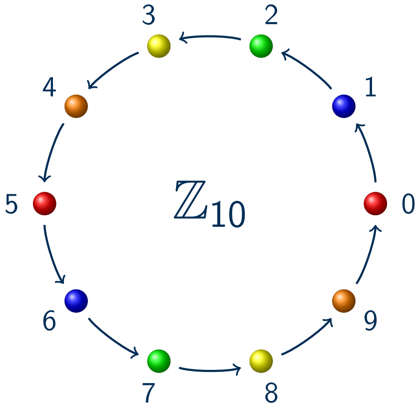

- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$

# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



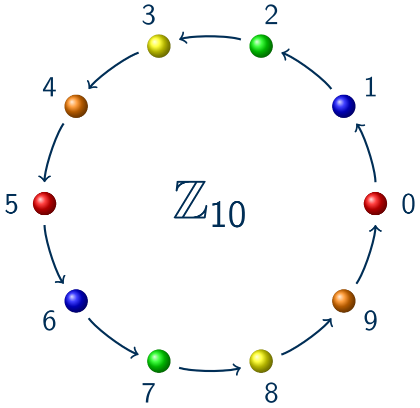

- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$
- $3 + \langle 5 \rangle = \{3, 8\}$

# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$




- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$
- $3 + \langle 5 \rangle = \{3, 8\}$
- $4 + \langle 5 \rangle = \{4, 9\}$

# $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$




- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$
- $3 + \langle 5 \rangle = \{3, 8\}$
- $4 + \langle 5 \rangle = \{4, 9\}$

$$\mathbb{Z}_{10} = (\langle 5 \rangle) \cup (1 + \langle 5 \rangle) \cup (2 + \langle 5 \rangle) \cup (3 + \langle 5 \rangle) \cup (4 + \langle 5 \rangle)$$

# Table of Contents

# Normal Subgroups

**Definition (Normal Subgroup)**

Given a group $G$ and subgroup $H$, if for all $g \in G$,

$$gH = Hg,$$

then we say that $H$ is a **normal subgroup** of $G$.

Example: $\langle r^2 \rangle \subset D_8$

- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $r^k \langle r^2 \rangle = \{r^{2+k}, r^{4+k}, r^{6+k}, r^k\} = \langle r^2 \rangle r^k$
- $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $\langle r^2 \rangle f = \{r^2 f, r^4 f, r^6 f, f\} = \{fr^6, fr^4, fr^2, f\}$
- $D_8 = \langle r^2 \rangle \cup r \langle r^2 \rangle \cup f \langle r^2 \rangle \cup rf \langle r^2 \rangle$

# Normal Subgroups

**Definition (Normal Subgroup)**

Given a group $G$ and subgroup $H$, if for all $g \in G$,

$$gH = Hg,$$

then we say that $H$ is a **normal subgroup** of $G$.

Example: $\langle r \rangle \subset D_8$

- $\langle r \rangle = \{r, r^2, r^3, r^4, r^5, r^6, r^7, e\}$
- $f \langle r \rangle = \{fr, fr^2, fr^3, fr^4, fr^5, fr^6, fr^7, f\}$
- $D_8 = \langle r \rangle \cup f \langle r \rangle$

# Normal Subgroups

## Definition (Normal Subgroup)

Given a group $G$ and subgroup $H$, if for all $g \in G$,

$$gH = Hg,$$

then we say that $H$ is a **normal subgroup** of $G$.

Example: $\langle 2 \rangle \subset \mathbb{Z}_8$

- $\langle 2 \rangle = \{2, 4, 6, 0\}$
- $1 + \langle 2 \rangle = \{3, 5, 7, 1\} = \langle 2 \rangle + 1$
- $\mathbb{Z}_8 = \langle 2 \rangle \cup (1 + \langle 2 \rangle)$

# Normal Subgroups

**Definition (Normal Subgroup)**

Given a group $G$ and subgroup $H$, if for all $g \in G$,

$$gH = Hg,$$

then we say that $H$ is a **normal subgroup** of $G$.

Non-Example: $\langle f \rangle \subset D_8$

- $\langle f \rangle = \{f, e\}$
- $r \langle f \rangle = \{rf, r\}$
- $\langle f \rangle r = \{fr, r\} = \{r^7 f, r\} \neq r \langle f \rangle$

# Results on Normal Subgroups

**Theorem**

*If $G$ is an abelian group, then all subgroups are normal.*

# Results on Normal Subgroups

**Theorem**

*If $G$ is an abelian group, then all subgroups are normal.*

**Theorem**

*If $G$ is a finite group and a subgroup $H$ has index 2, then $H$ is normal.*

# Coset Properties

## Theorem

*Given a group $G$, subgroup $H \subseteq G$, and elements $a, b \in G$:*

1. $|H| = |aH|$,
2. $|aH| = |bH|$,
3. $aH = bH$ *or* $aH \cap bH = \emptyset$, *and*
4. $aH = bH$ *if and only if* $b^{-1}a \in H$.

## Theorem

*From the previous theorem, given a group $G$ and subgroup $H \subseteq G$, the cosets of $H$ partition $G$, e.g. for some set of $g_i \in G$*

$$\bigcup_i g_i H = G$$

*and* $g_i H \cap g_j H = \emptyset$ *when* $i \neq j$.

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$

□

# Index 2 Implies Normal Proof

Proof.

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$

□

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$
- $gH \cap H = \emptyset$ and $G = gH \cup H$

□

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$
- $gH \cap H = \emptyset$ and $G = gH \cup H$
- $gH = G \setminus H$

□

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$
- $gH \cap H = \emptyset$ and $G = gH \cup H$
- $gH = G \setminus H$
- $Hg \cap H = \emptyset$ and $G = Hg \cup H$

□

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$
- $gH \cap H = \emptyset$ and $G = gH \cup H$
- $gH = G \setminus H$
- $Hg \cap H = \emptyset$ and $G = Hg \cup H$
- $Hg = G \setminus H$

□

# Index 2 Implies Normal Proof

**Proof.**

- $G$ a group, $H$ a subgroup, and $[G : H] = 2$
- $g \in G$ and $g \notin H$
- $gH \cap H = \emptyset$ and $G = gH \cup H$
- $gH = G \setminus H$
- $Hg \cap H = \emptyset$ and $G = Hg \cup H$
- $Hg = G \setminus H$
- $\therefore gH = Hg$

□

# Results on Normal Subgroups

**Theorem**

*If $G$ is an abelian group, then all subgroups are normal.*

**Theorem**

*If $G$ is a finite group and a subgroup $H$ has index 2, then $H$ is normal.*

**Theorem**

*Let $G$ be a group with subgroup $N$, then $N$ is normal if and only if for all $g \in G$, $gNg^{-1} = N$.*

# $gNg^{-1} = N$ Proof

**Part 1.**

- $G$ a group, $N$ normal

□

# $gNg^{-1} = N$ Proof

**Part 1.**

- $G$ a group, $N$ normal
- $gN = Ng, \forall g \in G\, \forall n_1 \in N\, \exists n_2 \in N : gn_1 = n_2 g$ (e.g. $fr = r^{-1}f$ in $D_n$)

□

# $gNg^{-1} = N$ Proof

## Part 1.

- $G$ a group, $N$ normal
- $gN = Ng$, $\forall g \in G\, \forall n_1 \in N\, \exists n_2 \in N : gn_1 = n_2 g$ (e.g. $fr = r^{-1}f$ in $D_n$)
- $gNg^{-1} = \{gng^{-1} | n \in N\}$

□

# $gNg^{-1} = N$ Proof

**Part 1.**

- $G$ a group, $N$ normal
- $gN = Ng$, $\forall g \in G\, \forall n_1 \in N\, \exists n_2 \in N : gn_1 = n_2 g$ (e.g. $fr = r^{-1}f$ in $D_n$)
- $gNg^{-1} = \left\{gng^{-1} \middle| n \in N\right\}$
- $gn_1g^{-1} = n_2gg^{-1} = n_2 \in N$, so $gNg^{-1} \subseteq N$

□

# $gNg^{-1} = N$ Proof

**Part 1.**

- $G$ a group, $N$ normal
- $gN = Ng$, $\forall g \in G \, \forall n_1 \in N \, \exists n_2 \in N : gn_1 = n_2 g$ (e.g. $fr = r^{-1}f$ in $D_n$)
- $gNg^{-1} = \{gng^{-1} | n \in N\}$
- $gn_1g^{-1} = n_2gg^{-1} = n_2 \in N$, so $gNg^{-1} \subseteq N$
- But, the previous steps are reversible, $n_2 = n_2gg^{-1} = gn_1g^{-1}$, so $N \subseteq gNg^{-1}$

□

# $gNg^{-1} = N$ Proof

## Part 1.

- $G$ a group, $N$ normal
- $gN = Ng$, $\forall g \in G\, \forall n_1 \in N\, \exists n_2 \in N : gn_1 = n_2 g$ (e.g. $fr = r^{-1}f$ in $D_n$)
- $gNg^{-1} = \left\{gng^{-1} \middle| n \in N\right\}$
- $gn_1g^{-1} = n_2gg^{-1} = n_2 \in N$, so $gNg^{-1} \subseteq N$
- But, the previous steps are reversible, $n_2 = n_2gg^{-1} = gn_1g^{-1}$, so $N \subseteq gNg^{-1}$
- $\therefore gNg^{-1} = N$

$\square$

# $gNg^{-1} = N$ Proof Continued

**Part 2.**

- $G$ a group, $\forall g \in G: \; gNg^{-1} = N$

□

# $gNg^{-1} = N$ Proof Continued

**Part 2.**

- $G$ a group, $\forall g \in G: \ gNg^{-1} = N$
- $\forall g \in G \, \forall n_1 \in N \, \exists n_2 \in N : gn_1g^{-1} = n_2$

□

# $gNg^{-1} = N$ Proof Continued

**Part 2.**

- $G$ a group, $\forall g \in G: \; gNg^{-1} = N$
- $\forall g \in G \, \forall n_1 \in N \, \exists n_2 \in N : gn_1g^{-1} = n_2$
- $gn_1 = n_2g$

□

# $gNg^{-1} = N$ Proof Continued

**Part 2.**

- $G$ a group, $\forall g \in G: \; gNg^{-1} = N$
- $\forall g \in G \, \forall n_1 \in N \, \exists n_2 \in N : gn_1g^{-1} = n_2$
- $gn_1 = n_2g$
- $\therefore gN = Ng$ and $N$ is normal

$\square$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$f \left\langle r^2 \right\rangle f = \left\{ fr^2 f, fef \right\}$$

# Example and Non-Example in $D_4$

**Example $\langle r^2 \rangle$**

$$\begin{aligned} f\left\langle r^2\right\rangle f &= \left\{fr^2f, fef\right\} \\ &= \left\{ffr^2, e\right\} = \left\{r^2, e\right\} \end{aligned}$$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$
\begin{aligned}
f \left\langle r^2 \right\rangle f &= \left\{ fr^2 f, fef \right\} \\
&= \left\{ ffr^2, e \right\} = \left\{ r^2, e \right\} \\
&= \left\langle r^2 \right\rangle
\end{aligned}
$$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$
\begin{aligned}
f \left\langle r^2 \right\rangle f &= \left\{ fr^2 f, fef \right\} \\
&= \left\{ ffr^2, e \right\} = \left\{ r^2, e \right\} \\
&= \left\langle r^2 \right\rangle
\end{aligned}
$$

## Non-Example $\langle f \rangle$

$$
r \langle f \rangle r^3 = \left\{ rfr^3, rer^3 \right\}
$$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$
\begin{aligned}
f \left\langle r^2 \right\rangle f &= \left\{ fr^2 f, fef \right\} \\
&= \left\{ ffr^2, e \right\} = \left\{ r^2, e \right\} \\
&= \left\langle r^2 \right\rangle
\end{aligned}
$$

## Non-Example $\langle f \rangle$

$$
\begin{aligned}
r \langle f \rangle r^3 &= \left\{ rfr^3, rer^3 \right\} \\
&= \{ rrf, e \} = \left\{ r^2 f, e \right\}
\end{aligned}
$$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$\begin{aligned} f\left\langle r^2\right\rangle f &= \left\{fr^2f, fef\right\} \\ &= \left\{ffr^2, e\right\} = \left\{r^2, e\right\} \\ &= \left\langle r^2\right\rangle \end{aligned}$$

## Non-Example $\langle f \rangle$

$$\begin{aligned} r\langle f\rangle r^3 &= \left\{rfr^3, rer^3\right\} \\ &= \{rrf, e\} = \left\{r^2f, e\right\} \\ &\neq \langle f\rangle \end{aligned}$$

# Example and Non-Example in $D_4$

## Example $\langle r^2 \rangle$

$$\begin{aligned} f\left\langle r^2\right\rangle f &= \left\{fr^2f, fef\right\} \\ &= \left\{ffr^2, e\right\} = \left\{r^2, e\right\} \\ &= \left\langle r^2\right\rangle \end{aligned}$$

## Non-Example $\langle f \rangle$

$$\begin{aligned} r\langle f\rangle r^3 &= \left\{rfr^3, rer^3\right\} \\ &= \{rrf, e\} = \left\{r^2f, e\right\} \\ &\neq \langle f\rangle \end{aligned}$$

(But, $\left\{r^2f, e\right\}$, is another subgroup of order 2.)

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism* $\phi : G \to \overline{G}$, *the kernel of* $\phi$ *is a normal subgroup.*

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\, \phi$ and $g \in G$

□

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\,\phi$ and $g \in G$
- $\phi(kk') = \phi(k)\phi(k') = e_{\overline{G}}e_{\overline{G}} = e_{\overline{G}}$

□

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\, \phi$ and $g \in G$
- $\phi(kk') = \phi(k)\phi(k') = e_{\overline{G}}e_{\overline{G}} = e_{\overline{G}}$
- $\phi(k^{-1}) = \phi(k)^{-1} = e_{\overline{G}}$

□

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\,\phi$ and $g \in G$
- $\phi(kk') = \phi(k)\phi(k') = e_{\overline{G}}e_{\overline{G}} = e_{\overline{G}}$
- $\phi(k^{-1}) = \phi(k)^{-1} = e_{\overline{G}}$
- $\therefore$ $ker\,\phi$ is a subgroup

□

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\, \phi$ and $g \in G$
- $\phi(kk') = \phi(k)\phi(k') = e_{\overline{G}} e_{\overline{G}} = e_{\overline{G}}$
- $\phi(k^{-1}) = \phi(k)^{-1} = e_{\overline{G}}$
- $\therefore ker\, \phi$ is a subgroup
- $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)e_{\overline{G}}\phi(g)^{-1} = e_{\overline{G}}$

□

# Kernels are Normal Subgroups

**Theorem**

*Given a homomorphism $\phi : G \to \overline{G}$, the kernel of $\phi$ is a normal subgroup.*

**Proof.**

- $k, k' \in ker\, \phi$ and $g \in G$
- $\phi(kk') = \phi(k)\phi(k') = e_{\overline{G}} e_{\overline{G}} = e_{\overline{G}}$
- $\phi(k^{-1}) = \phi(k)^{-1} = e_{\overline{G}}$
- $\therefore$ $ker\, \phi$ is a subgroup
- $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)e_{\overline{G}}\phi(g)^{-1} = e_{\overline{G}}$
- $\therefore g(ker\, \phi)g^{-1} = ker\, \phi$ and $ker\, \phi$ is normal

□

# Table of Contents

# Quotients and Normal Subgroups

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then*

$$G/N = \{gN|g \in G\}$$

*is a group with arithmetic defined by $(gN)(hN) = (ghN)$.*

# Coset Properties

**Theorem**

*Given a group $G$, subgroup $H \subseteq G$, and elements $a, b \in G$:*

1. $|H| = |aH|$,
2. $|aH| = |bH|$,
3. $aH = bH$ *or* $aH \cap bH = \emptyset$, *and*
4. $aH = bH$ *if and only if* $b^{-1}a \in H$.

# Quotients and Normal Subgroups Proof

**Part 1: Closure and Associativity.**

- $g, h \in G$ and $n_1, n_2 \in N$ and $N$ is normal

□

# Quotients and Normal Subgroups Proof

**Part 1: Closure and Associativity.**

- $g, h \in G$ and $n_1, n_2 \in N$ and $N$ is normal
- $gn_1 \in gN$ and $hn_2 \in hN$

□

# Quotients and Normal Subgroups Proof

**Part 1: Closure and Associativity.**

- $g, h \in G$ and $n_1, n_2 \in N$ and $N$ is normal
- $gn_1 \in gN$ and $hn_2 \in hN$
- $gn_1hn_2 = ghn_3n_2 \in ghN$ for some $n_3 \in N$

□

# Quotients and Normal Subgroups Proof

**Part 1: Closure and Associativity.**

- $g, h \in G$ and $n_1, n_2 \in N$ and $N$ is normal
- $gn_1 \in gN$ and $hn_2 \in hN$
- $gn_1hn_2 = ghn_3n_2 \in ghN$ for some $n_3 \in N$
- $\therefore$ We get closure

□

# Quotients and Normal Subgroups Proof

**Part 1: Closure and Associativity.**

- $g, h \in G$ and $n_1, n_2 \in N$ and $N$ is normal
- $gn_1 \in gN$ and $hn_2 \in hN$
- $gn_1hn_2 = ghn_3n_2 \in ghN$ for some $n_3 \in N$
- $\therefore$ We get closure
- Associativity is "inhereted" from $G$

□

# Quotients and Normal Subgroups Proof

**Part 2: Well Defined.**

- $g, h, g', h' \in G$ with $gN = g'N$ and $hN = h'N$

□

# Quotients and Normal Subgroups Proof

**Part 2: Well Defined.**

- $g, h, g', h' \in G$ with $gN = g'N$ and $hN = h'N$
- $g^{-1}g' = n_1 \in N$ and $h^{-1}h' = n_2 \in N$

□

# Quotients and Normal Subgroups Proof

**Part 2: Well Defined.**

- $g, h, g', h' \in G$ with $gN = g'N$ and $hN = h'N$
- $g^{-1}g' = n_1 \in N$ and $h^{-1}h' = n_2 \in N$
- $(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h' = h^{-1}n_1h' = h^{-1}h'n_3 = n_2n_3 \in N$

$\square$

# Quotients and Normal Subgroups Proof

**Part 2: Well Defined.**

- $g, h, g', h' \in G$ with $gN = g'N$ and $hN = h'N$
- $g^{-1}g' = n_1 \in N$ and $h^{-1}h' = n_2 \in N$
- $(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h' = h^{-1}n_1h' = h^{-1}h'n_3 = n_2n_3 \in N$
- $ghN = g'h'N$

□

# Quotients and Normal Subgroups Proof

**Part 2: Well Defined.**

- $g, h, g', h' \in G$ with $gN = g'N$ and $hN = h'N$
- $g^{-1}g' = n_1 \in N$ and $h^{-1}h' = n_2 \in N$
- $(gh)^{-1}(g'h') = h^{-1}g^{-1}g'h' = h^{-1}n_1h' = h^{-1}h'n_3 = n_2n_3 \in N$
- $ghN = g'h'N$
- $\therefore (gN)(hN) = ghN$ is well defined

□

# Quotients and Normal Subgroups Proof

**Part 3: Identity and Inverses.**

- $g \in G$

□

# Quotients and Normal Subgroups Proof

**Part 3: Identity and Inverses.**

- $g \in G$
- $(gN)(eN) = geN = gN$

□

# Quotients and Normal Subgroups Proof

**Part 3: Identity and Inverses.**

- $g \in G$
- $(gN)(eN) = geN = gN$
- $(gN)(g^{-1}N) = gg^{-1}N = eN = N$

□

# Quotients and Normal Subgroups Proof

**Part 3: Identity and Inverses.**

- $g \in G$
- $(gN)(eN) = geN = gN$
- $(gN)(g^{-1}N) = gg^{-1}N = eN = N$
- $\therefore$ There exists an identity and inverses

□

# Quotients and Normal Subgroups Proof

**Part 3: Identity and Inverses.**

- $g \in G$
- $(gN)(eN) = geN = gN$
- $(gN)(g^{-1}N) = gg^{-1}N = eN = N$
- $\therefore$ There exists an identity and inverses
- $\therefore G/N$ is a group

□

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r \langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr \langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $r^2$ | $rf$ | $rfr$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $fr^2$ | $frf$ | $frfr$ |

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $r^2$ | $rf$ | $rfr$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $fr^2$ | $frf$ | $frfr$ |

Rewrite each element in the table so that it is in the form $r^k$ or $fr^k$, then identify which coset it's in.

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $e$ | $fr$ | $f$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $fr^2$ | $frf$ | $frfr$ |

Rewrite each element in the table so that it is in the form $r^k$ or $fr^k$, then identify which coset it's in.

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $e$ | $fr$ | $f$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $f$ | $r$ | $e$ |

Rewrite each element in the table so that it is in the form $r^k$ or $fr^k$, then identify which coset it's in.

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f \langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r \langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr \langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $e$ | $fr$ | $f$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $f$ | $r$ | $e$ |

Abelian group with all elements of order 2.

# Quotient Group Example: $N = \langle r^2 \rangle \subset D_8$

From before we have:

1. $N = \langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
2. $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
3. $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
4. $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$

Thus we get

$$D_8 = N \cup fN \cup rN \cup frN$$

Composition Table for $D_8/N$:

(Below an element $g$ represents the coset $gN$)

| $\circ$ | $e$ | $r$ | $f$ | $fr$ |
|---|---|---|---|---|
| $e$ | $e$ | $r$ | $f$ | $fr$ |
| $r$ | $r$ | $e$ | $fr$ | $f$ |
| $f$ | $f$ | $fr$ | $e$ | $r$ |
| $fr$ | $fr$ | $f$ | $r$ | $e$ |

Abelian group with all elements of order 2.

$$D_8/N \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$

## $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) =$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) =$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$

## $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) =$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) = (1, 2k + 1) \equiv (1, 1)$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) = (1, 2k + 1) \equiv (1, 1)$
- $\phi(fr^{-2k-1}) =$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) = (1, 2k + 1) \equiv (1, 1)$
- $\phi(fr^{-2k-1}) = (1, -2k - 1) \equiv (1, 1)$

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) = (1, 2k + 1) \equiv (1, 1)$
- $\phi(fr^{-2k-1}) = (1, -2k - 1) \equiv (1, 1)$
- $\phi(f^l r^k) = (l, k) \equiv (0, 0)$ implies $l$ and $k$ are both even

# $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k} f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1} f) = (1, 2k + 1) \equiv (1, 1)$
- $\phi(fr^{-2k-1}) = (1, -2k - 1) \equiv (1, 1)$
- $\phi(f^l r^k) = (l, k) \equiv (0, 0)$ implies $l$ and $k$ are both even
- $ker\, \phi = \langle r^2 \rangle$

## $\phi : D_8 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$

- $\phi : D_8 \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\phi(r) = (0, 1)$
- $\phi(f) = (1, 0)$
- $\phi(r^{2k}f) = (1, 2k) \equiv (1, 0)$
- $\phi(fr^{-2k}) = (1, -2k) \equiv (1, 0)$
- $\phi(r^{2k+1}f) = (1, 2k + 1) \equiv (1, 1)$
- $\phi(fr^{-2k-1}) = (1, -2k - 1) \equiv (1, 1)$
- $\phi(f^l r^k) = (l, k) \equiv (0, 0)$ implies $l$ and $k$ are both even
- $ker\, \phi = \langle r^2 \rangle$
- We will show, eventually, that this is why $D_8/\langle r^2 \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

# Normal Subgroups are Kernels

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then $N$ is the kernel of a homomorphism.*

# Normal Subgroups are Kernels

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then $N$ is the kernel of a homomorphism.*

**Proof.**

1. Define $\phi(g) = gN$ in $G/N$

□

# Normal Subgroups are Kernels

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then $N$ is the kernel of a homomorphism.*

**Proof.**

1. Define $\phi(g) = gN$ in $G/N$
2. $\forall n \in N : \phi(n) = nN = eN$, so $N \subseteq \ker \phi$

□

# Normal Subgroups are Kernels

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then $N$ is the kernel of a homomorphism.*

**Proof.**

1. Define $\phi(g) = gN$ in $G/N$
2. $\forall n \in N : \phi(n) = nN = eN$, so $N \subseteq ker\,\phi$
3. $\forall k \in ker\,\phi : \phi(k) = kN = eN$, thus $k = ek \in N$ and $ker\,\phi \subseteq N$

□

# Normal Subgroups are Kernels

**Theorem**

*If $G$ is a group and $N$ is a normal subgroup, then $N$ is the kernel of a homomorphism.*

**Proof.**

1. Define $\phi(g) = gN$ in $G/N$
2. $\forall n \in N : \phi(n) = nN = eN$, so $N \subseteq ker\,\phi$
3. $\forall k \in ker\,\phi : \phi(k) = kN = eN$, thus $k = ek \in N$ and $ker\,\phi \subseteq N$
4. $\therefore N = ker\,\phi$

□

# Table of Contents

# First Isomorphism Theorem

**Theorem**

*If $\phi : G \to \overline{G}$ is a surjective homomorphism with kernel $K = \ker \phi$, then $G/K \cong \overline{G}$.*

# Examples

**$\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$**

Define $\phi(f^l r^k) = (l, k) \pmod 2$, then from before $ker\,\phi = \langle r^2 \rangle$ and $D_8/ker\,\phi \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. This agrees with the conclusion of the **First Isomorphism Theorem**.

# Examples

**$\phi : D_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$**

Define $\phi(f^l r^k) = (l, k) \pmod 2$, then from before $ker\,\phi = \langle r^2 \rangle$ and $D_8 / ker\,\phi \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. This agrees with the conclusion of the **First Isomorphism Theorem**.

**$\phi : \mathbb{Z} \to \mathbb{Z}_n$**

If we define $\phi(z) = z \pmod n$, then the kernel will be $ker\,\phi = n\mathbb{Z}$ since those are precisely the numbers equal to zero modulo $n$. The **First Isomorphism Theorem** tells us then that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

# Null Space

**$T : \mathbb{Z}^2 \to \mathbb{Z}^2$**

- $T(\vec{v}) = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 3y \\ 2x + 6y \end{pmatrix}$

# Null Space

$T : \mathbb{Z}^2 \to \mathbb{Z}^2$

- $T(\vec{v}) = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 3y \\ 2x + 6y \end{pmatrix}$
- $T = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix}$

# Null Space

**$T : \mathbb{Z}^2 \to \mathbb{Z}^2$**

- $T(\vec{v}) = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 3y \\ 2x + 6y \end{pmatrix}$
- $T = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix}$
- $ker\ T = Null\ T = \left\langle \begin{pmatrix} -3 \\ 1 \end{pmatrix} \right\rangle$

# Null Space

$T : \mathbb{Z}^2 \to \mathbb{Z}^2$

- $T(\vec{v}) = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+3y \\ 2x+6y \end{pmatrix}$
- $T = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix}$
- $ker\ T = Null\ T = \left\langle \begin{pmatrix} -3 \\ 1 \end{pmatrix} \right\rangle$
- $Col\ T = \left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\rangle \cong \mathbb{Z}^2/ker\ T = \left\{ \begin{pmatrix} z \\ 0 \end{pmatrix} + ker\ T \middle| z \in \mathbb{Z} \right\}$

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$

□

# First Isomorphism Theorem Proof

Proof.

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$
- $\overline{\phi}(gK) = \phi(g)$

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$
- $\overline{\phi}(gK) = \phi(g)$
- $\overline{\phi}(g_1K) = \overline{\phi}(g_2K)$ implies $\phi(g_1) = \phi(g_2)$

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$
- $\overline{\phi}(gK) = \phi(g)$
- $\overline{\phi}(g_1K) = \overline{\phi}(g_2K)$ implies $\phi(g_1) = \phi(g_2)$
- $e_{\overline{G}} = \phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1)$

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\, \phi$
- $\overline{\phi}(gK) = \phi(g)$
- $\overline{\phi}(g_1 K) = \overline{\phi}(g_2 K)$ implies $\phi(g_1) = \phi(g_2)$
- $e_{\overline{G}} = \phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1)$
- $g_2^{-1}g_1 \in K$ and $g_1 K = g_2 K$

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$
- $\overline{\phi}(gK) = \phi(g)$
- $\overline{\phi}(g_1K) = \overline{\phi}(g_2K)$ implies $\phi(g_1) = \phi(g_2)$
- $e_{\overline{G}} = \phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1)$
- $g_2^{-1}g_1 \in K$ and $g_1K = g_2K$
- $\therefore\ \overline{\phi}$ is injective and thus an isomorphism

□

# First Isomorphism Theorem Proof

**Proof.**

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$
- $\overline{\phi}(gK) = \phi(g)$
- $\overline{\phi}(g_1K) = \overline{\phi}(g_2K)$ implies $\phi(g_1) = \phi(g_2)$
- $e_{\overline{G}} = \phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1)$
- $g_2^{-1}g_1 \in K$ and $g_1K = g_2K$
- $\therefore \overline{\phi}$ is injective and thus an isomorphism
- Why didn't we have to show $\overline{\phi}$ is surjective?

□

# Table of Contents

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$
- $a \equiv b \pmod{n}$ if and only if $n|(a-b)$

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$
- $a \equiv b \pmod{n}$ if and only if $n|(a-b)$
- Theorem: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$
- $a \equiv b \pmod{n}$ if and only if $n|(a-b)$
- Theorem: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
    1. $a \pm c \equiv b \pm d \pmod{n}$

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$
- $a \equiv b \pmod{n}$ if and only if $n|(a-b)$
- Theorem: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
  1. $a \pm c \equiv b \pm d \pmod{n}$
  2. $ac \equiv bd \pmod{n}$

# Modular Equivalence and Arithmetic

- $n > 0$ an element of $\mathbb{Z}$
- $a \equiv b \pmod{n}$ if and only if $n|(a-b)$
- Theorem: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
  1. $a \pm c \equiv b \pm d \pmod{n}$
  2. $ac \equiv bd \pmod{n}$
- $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} | a \in \mathbb{Z}\}$

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$
- $a(x) \equiv b(x) \pmod{n(x)}$ if and only if $n(x) | (a(x) - b(x))$

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$
- $a(x) \equiv b(x) \pmod{n(x)}$ if and only if $n(x) | (a(x) - b(x))$
- Theorem: If $a(x) \equiv b(x) \pmod{n(x)}$ and $c(x) \equiv d(x) \pmod{n(x)}$, then

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$
- $a(x) \equiv b(x) \pmod{n(x)}$ if and only if $n(x) | (a(x) - b(x))$
- Theorem: If $a(x) \equiv b(x) \pmod{n(x)}$ and $c(x) \equiv d(x) \pmod{n(x)}$, then
  1. $a(x) \pm c(x) \equiv b(x) \pm d(x) \pmod{n(x)}$

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$
- $a(x) \equiv b(x) \pmod{n(x)}$ if and only if $n(x)|(a(x) - b(x))$
- Theorem: If $a(x) \equiv b(x) \pmod{n(x)}$ and $c(x) \equiv d(x) \pmod{n(x)}$, then
  1. $a(x) \pm c(x) \equiv b(x) \pm d(x) \pmod{n(x)}$
  2. $a(x)c(x) \equiv b(x)d(x) \pmod{n(x)}$

# Polynomial Equivalence and Arithmetic

- $n(x) \neq 0$ an element of $F[x]$
- $a(x) \equiv b(x) \pmod{n(x)}$ if and only if $n(x) | (a(x) - b(x))$
- Theorem: If $a(x) \equiv b(x) \pmod{n(x)}$ and $c(x) \equiv d(x) \pmod{n(x)}$, then
  1. $a(x) \pm c(x) \equiv b(x) \pm d(x) \pmod{n(x)}$
  2. $a(x)c(x) \equiv b(x)d(x) \pmod{n(x)}$
- $F[x] / \langle n(x) \rangle = \{a(x) + \langle n(x) \rangle | a(x) \in F[x]\}$

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$
- $a \equiv b \pmod{I}$ if and only if $a - b \in I$

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$
- $a \equiv b \pmod{I}$ if and only if $a - b \in I$
- Theorem: If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$
- $a \equiv b \pmod{I}$ if and only if $a - b \in I$
- Theorem: If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then
  1. $a \pm c \equiv b \pm d \pmod{I}$

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$
- $a \equiv b \pmod{I}$ if and only if $a - b \in I$
- Theorem: If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then
  1. $a \pm c \equiv b \pm d \pmod{I}$
  2. $ac \equiv bd \pmod{I}$

# Ideals and Quotient Rings

- $I$ an (two-sided) ideal in $R$
- $a \equiv b \pmod{I}$ if and only if $a - b \in I$
- Theorem: If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then
  1. $a \pm c \equiv b \pm d \pmod{I}$
  2. $ac \equiv bd \pmod{I}$
- Quotient Ring $R/I = \{r + I | r \in R\}$

# First Isomorphism Theorem for Rings

- $\phi : R \to S$ a surjective homomorphism

# First Isomorphism Theorem for Rings

- $\phi : R \to S$ a surjective homomorphism
- $K = ker\,\phi$ is an ideal

# First Isomorphism Theorem for Rings

- $\phi : R \to S$ a surjective homomorphism
- $K = ker\, \phi$ is an ideal
- $R/K$ is a ring

# First Isomorphism Theorem for Rings

- $\phi : R \to S$ a surjective homomorphism
- $K = ker\,\phi$ is an ideal
- $R/K$ is a ring
- $R/K \cong S$

# First Isomorphism Theorem for Rings

- $\phi : R \to S$ a surjective homomorphism
- $K = ker\,\phi$ is an ideal
- $R/K$ is a ring
- $R/K \cong S$
- $I$ is an ideal of $R$ if and only if it is the kernel of a homomorphism

# Normal Subgroups and Quotient Groups

- $N$ a normal subgroup in $(G, \cdot)$

# Normal Subgroups and Quotient Groups

- $N$ a normal subgroup in $(G, \cdot)$
- $a \equiv b \pmod{N}$ if and only if $b^{-1}a \in N$

# Normal Subgroups and Quotient Groups

- $N$ a normal subgroup in $(G, \cdot)$
- $a \equiv b \pmod{N}$ if and only if $b^{-1}a \in N$
- Theorem: If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then

# Normal Subgroups and Quotient Groups

- $N$ a normal subgroup in $(G, \cdot)$
- $a \equiv b \pmod{N}$ if and only if $b^{-1}a \in N$
- Theorem: If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then
  1. $ac \equiv bd \pmod{N}$

# Normal Subgroups and Quotient Groups

- $N$ a normal subgroup in $(G, \cdot)$
- $a \equiv b \pmod{N}$ if and only if $b^{-1}a \in N$
- Theorem: If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then
  1. $ac \equiv bd \pmod{N}$
- Quotient Group $G/N = \{gN | g \in G\}$

# First Isomorphism Theorem for Groups

- $\phi : G \to \overline{G}$ a surjective homomorphism

# First Isomorphism Theorem for Groups

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$ is a normal subgroup

# First Isomorphism Theorem for Groups

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\,\phi$ is a normal subgroup
- $G/K$ is a group

# First Isomorphism Theorem for Groups

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\, \phi$ is a normal subgroup
- $G/K$ is a group
- $G/K \cong \overline{G}$

# First Isomorphism Theorem for Groups

- $\phi : G \to \overline{G}$ a surjective homomorphism
- $K = ker\, \phi$ is a normal subgroup
- $G/K$ is a group
- $G/K \cong \overline{G}$
- $N$ is a normal subgroup of $G$ if and only if it is the kernel of a homomorphism

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation $(T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w}))$

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation $(T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w}))$
- $K = ker\ T = Null\ T$ is a subspace of $V$

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation $(T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w}))$
- $K = ker\ T = Null\ T$ is a subspace of $V$
- $\vec{v} \equiv \vec{w} \pmod{K}$ if and only if $\vec{v} - \vec{w} \in K$

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation ($T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w})$)
- $K = ker\ T = Null\ T$ is a subspace of $V$
- $\vec{v} \equiv \vec{w} \pmod{K}$ if and only if $\vec{v} - \vec{w} \in K$
- Theorem: If $\vec{a} \equiv \vec{b} \pmod{K}$ and $\vec{c} \equiv \vec{d} \pmod{K}$, then

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation ($T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w})$)
- $K = ker\ T = Null\ T$ is a subspace of $V$
- $\vec{v} \equiv \vec{w} \pmod{K}$ if and only if $\vec{v} - \vec{w} \in K$
- Theorem: If $\vec{a} \equiv \vec{b} \pmod{K}$ and $\vec{c} \equiv \vec{d} \pmod{K}$, then
  1. $x\vec{a} + y\vec{c} \equiv x\vec{b} + y\vec{d} \pmod{K}$

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation $(T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w}))$
- $K = ker\ T = Null\ T$ is a subspace of $V$
- $\vec{v} \equiv \vec{w} \pmod{K}$ if and only if $\vec{v} - \vec{w} \in K$
- Theorem: If $\vec{a} \equiv \vec{b} \pmod{K}$ and $\vec{c} \equiv \vec{d} \pmod{K}$, then
  1. $x\vec{a} + y\vec{c} \equiv x\vec{b} + y\vec{d} \pmod{K}$
- Quotient Space $V/K = \{\vec{v} + K | \vec{v} \in V\} \cong Col\ T \subseteq \overline{V}$

# Vector Spaces and Linear Transformations

- $V$ and $\overline{V}$ vector spaces
- $T : V \to \overline{V}$ a linear transformation $(T(a\vec{v} + b\vec{w}) = aT(\vec{v}) + bT(\vec{w}))$
- $K = ker\ T = Null\ T$ is a subspace of $V$
- $\vec{v} \equiv \vec{w} \pmod{K}$ if and only if $\vec{v} - \vec{w} \in K$
- Theorem: If $\vec{a} \equiv \vec{b} \pmod{K}$ and $\vec{c} \equiv \vec{d} \pmod{K}$, then
  1. $x\vec{a} + y\vec{c} \equiv x\vec{b} + y\vec{d} \pmod{K}$
- Quotient Space $V/K = \{\vec{v} + K | \vec{v} \in V\} \cong Col\ T \subseteq \overline{V}$
- Every null space/kernel is a subspace and any subspace can be a null space/kernel

# Quotient Structures

- $S$ an algebraic structure with some set of operations $\{*_s\}$

# Quotient Structures

- $S$ an algebraic structure with some set of operations $\{*_s\}$
- Equivalence Relation $a \sim b$ defined on $S$

# Quotient Structures

- $S$ an algebraic structure with some set of operations $\{*_s\}$
- Equivalence Relation $a \sim b$ defined on $S$
- If the relation respects the operations on $S$, i.e. $a \sim b$ and $c \sim d$ implies $a *_s c \sim b *_s d$, then

# Quotient Structures

- $S$ an algebraic structure with some set of operations $\{*_s\}$
- Equivalence Relation $a \sim b$ defined on $S$
- If the relation respects the operations on $S$, i.e. $a \sim b$ and $c \sim d$ implies $a *_s c \sim b *_s d$, then
- Quotient Structure $S/\sim$, the set of equivalence classes, has the same sort of structure as $S$

# First Isomorphism Theorem

- $S$ and $\overline{S}$ algebraic structures with some set of operations

# First Isomorphism Theorem

- $S$ and $\overline{S}$ algebraic structures with some set of operations
- $\phi : S \to \overline{S}$ a function respecting the operations in $S$ and $\overline{S}$

# First Isomorphism Theorem

- $S$ and $\overline{S}$ algebraic structures with some set of operations
- $\phi : S \to \overline{S}$ a function respecting the operations in $S$ and $\overline{S}$
- $K = ker\,\phi$ is a substructure of $S$

# First Isomorphism Theorem

- $S$ and $\overline{S}$ algebraic structures with some set of operations
- $\phi : S \to \overline{S}$ a function respecting the operations in $S$ and $\overline{S}$
- $K = ker\, \phi$ is a substructure of $S$
- $S/K \cong \phi(S) \subseteq \overline{S}$

# First Isomorphism Theorem

- $S$ and $\overline{S}$ algebraic structures with some set of operations
- $\phi : S \to \overline{S}$ a function respecting the operations in $S$ and $\overline{S}$
- $K = ker\,\phi$ is a substructure of $S$
- $S/K \cong \phi(S) \subseteq \overline{S}$
- There is a class of substructures of $S$ that are all possible kernels

# Quotients and Homomorphisms

Dr. Chuck Rocca