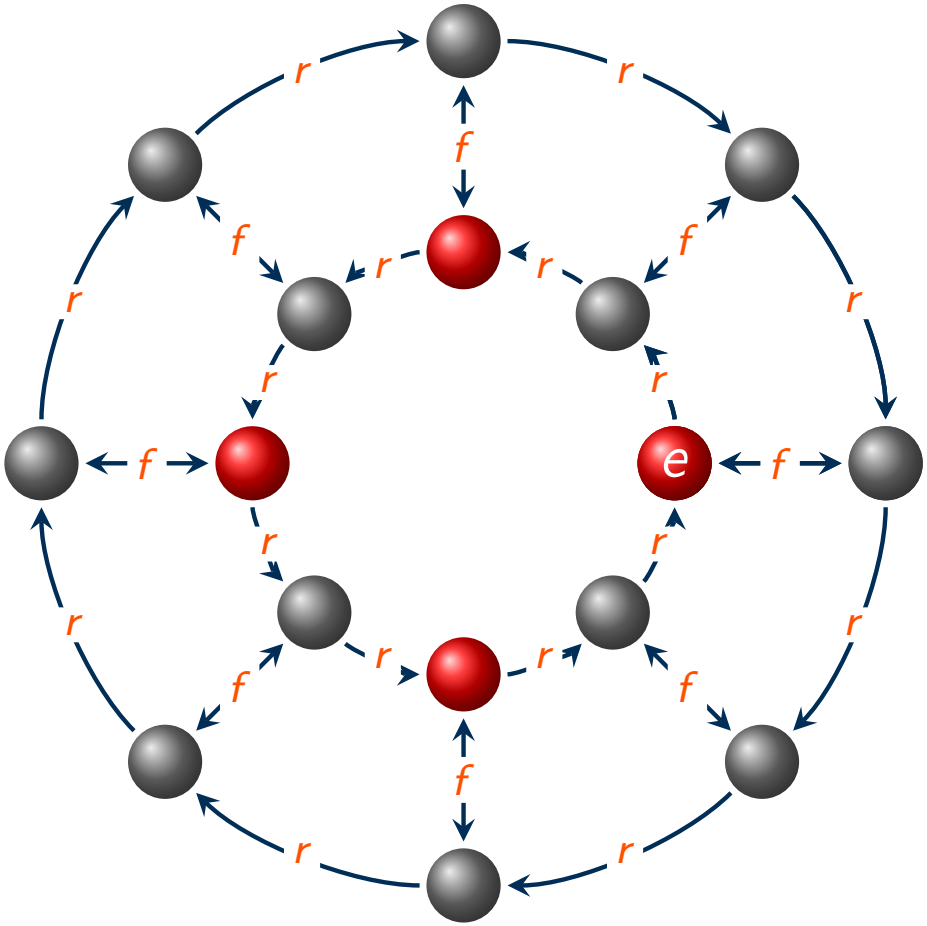
Cosets and Lagrange

Dr. Chuck Rocca

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

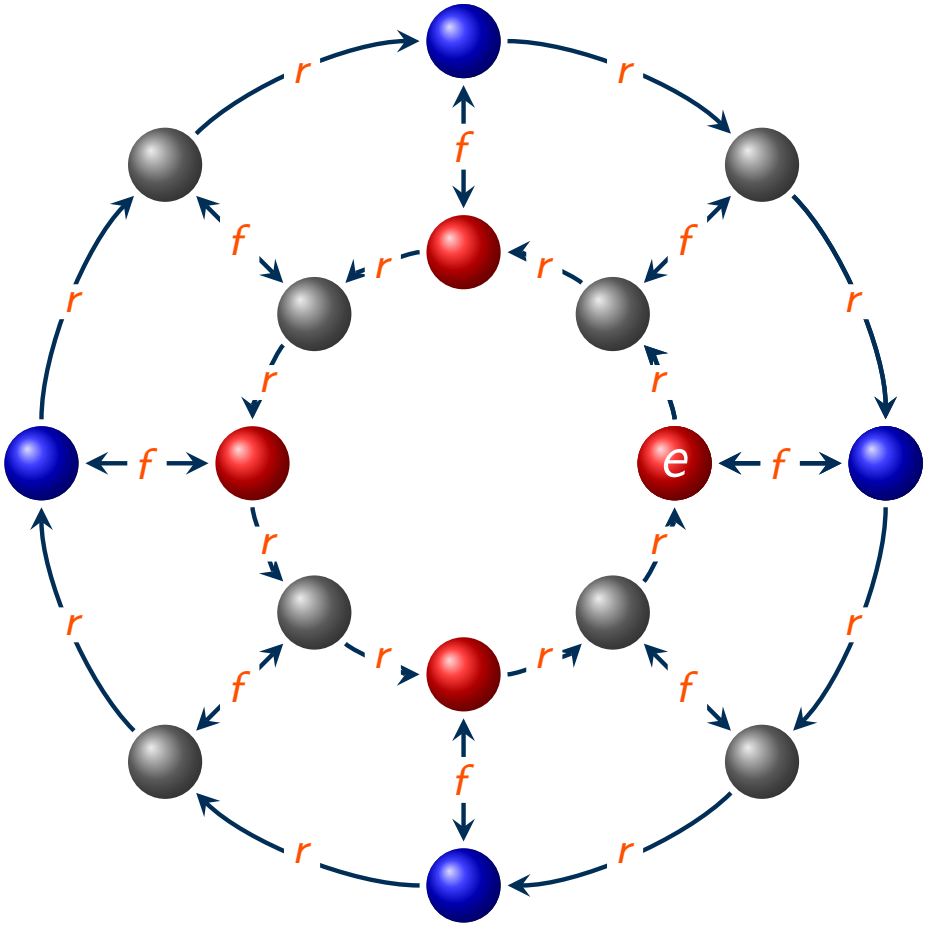
Table of Contents

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



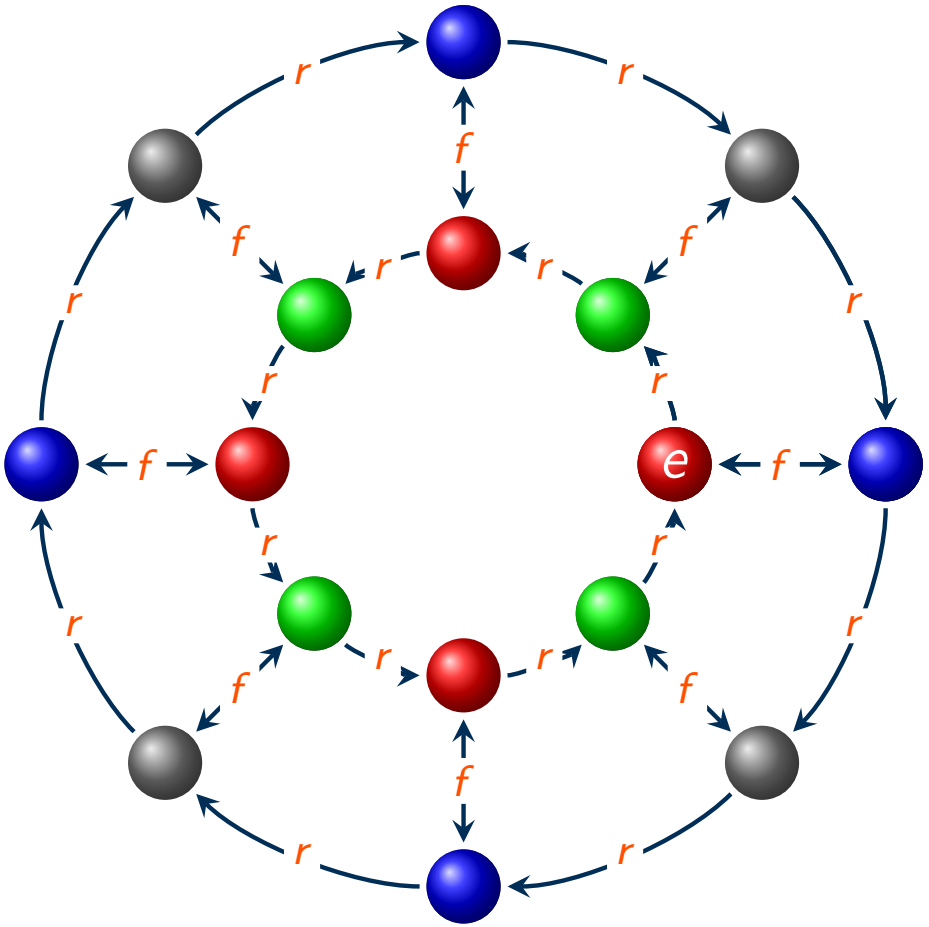
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$

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



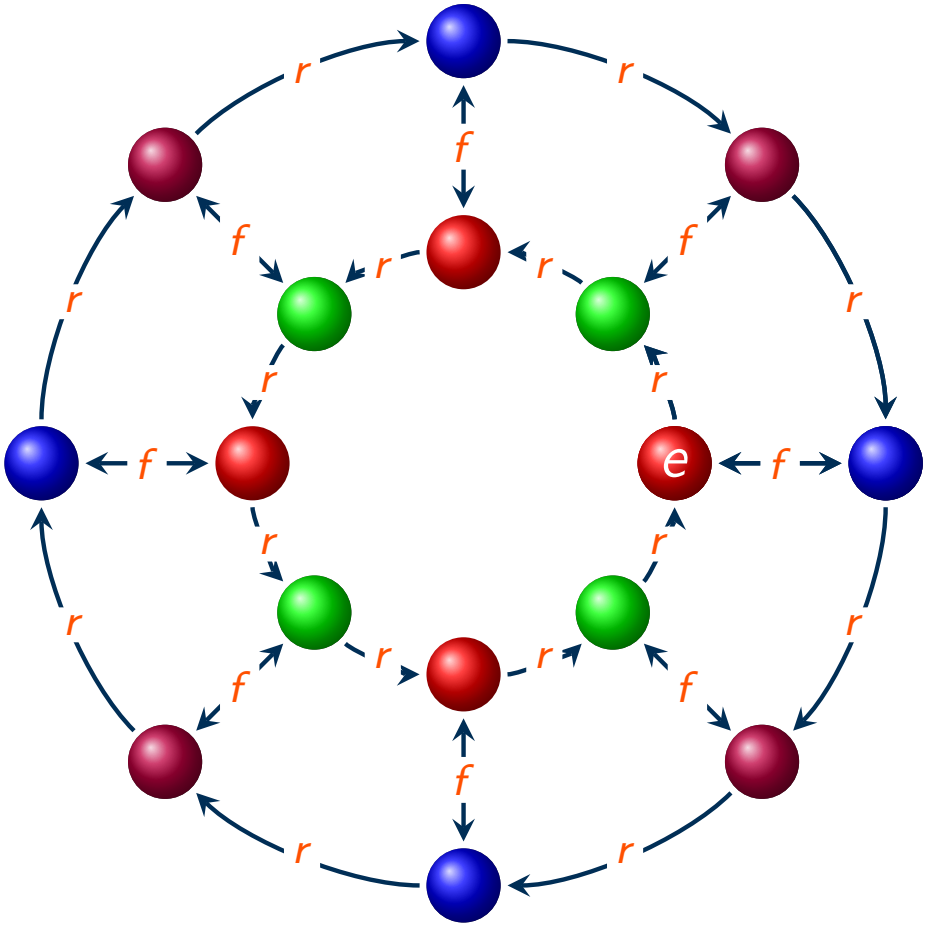
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$

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



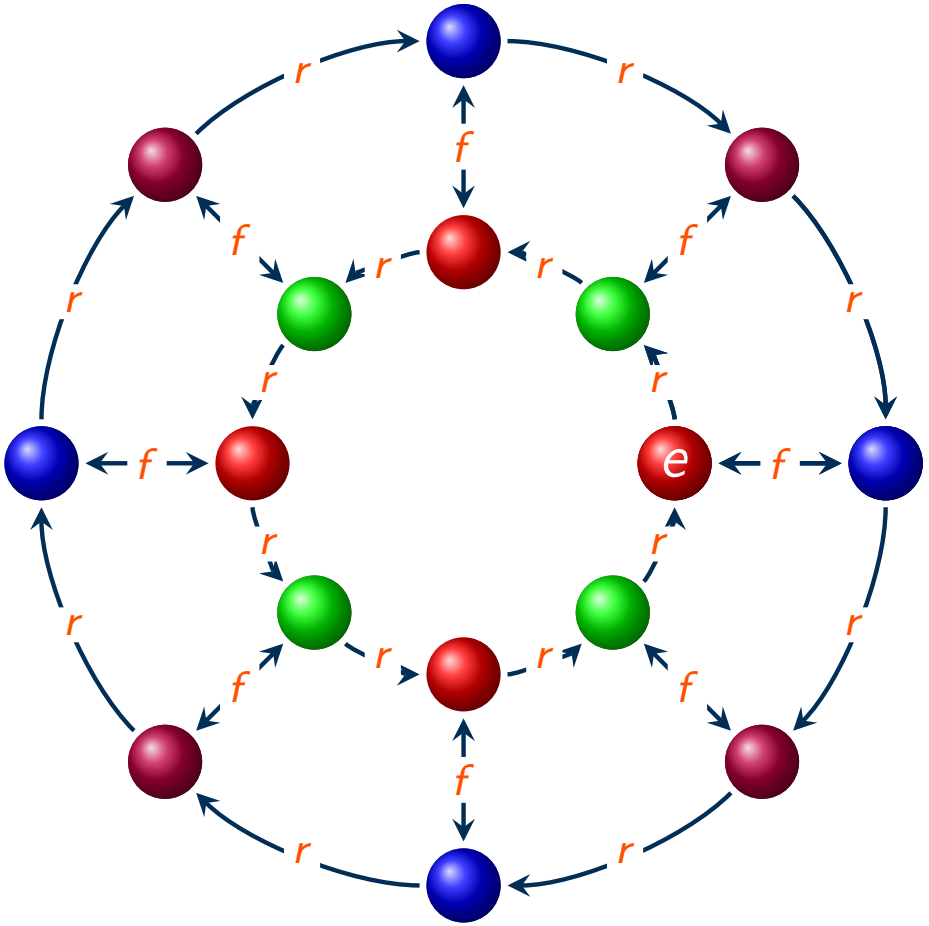
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$

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



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

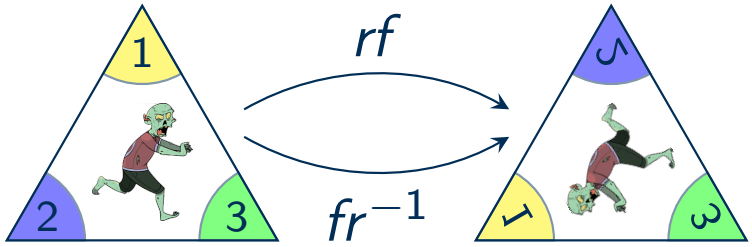
$D_8 = \langle r, f | r^8 = f^2 = e, rf = fr^{-1} \rangle$



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

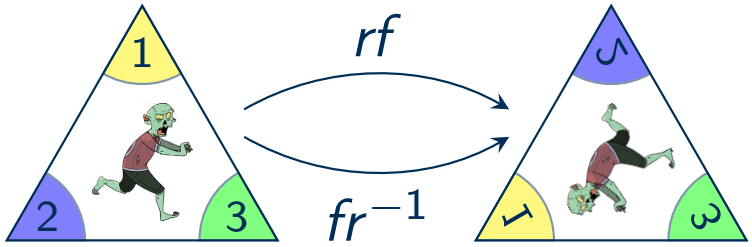
Calculating in D_n

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



Calculating in D_n

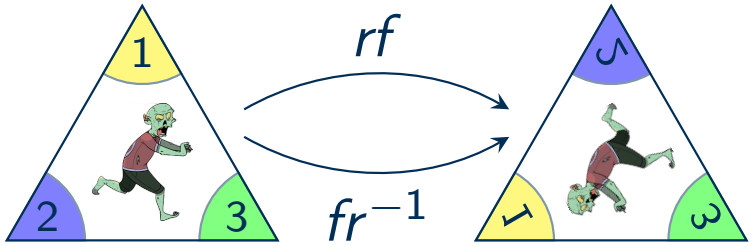
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



$$r^3 f$$

Calculating in D_n

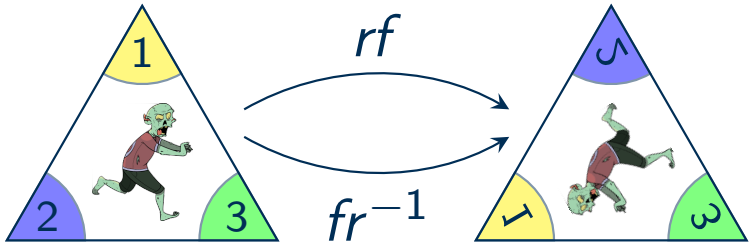
$$D_n = \left\langle r, f \middle| r^n = f^2 = e, rf = fr^{-1} \right\rangle$$



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

Calculating in D_n

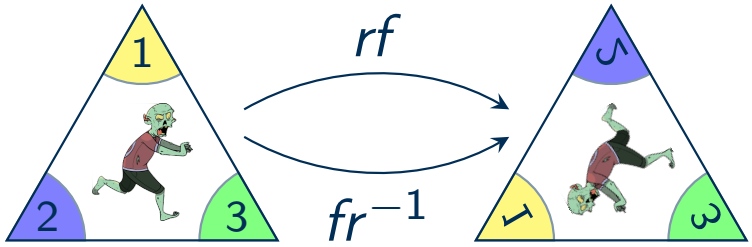
$$D_n = \left\langle r, f \middle| r^n = f^2 = e, rf = fr^{-1} \right\rangle$$



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

Calculating in D_n

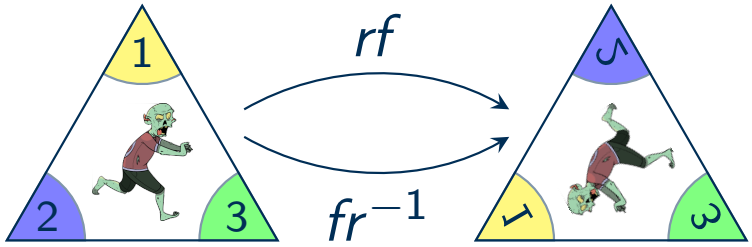
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



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

Calculating in D_n

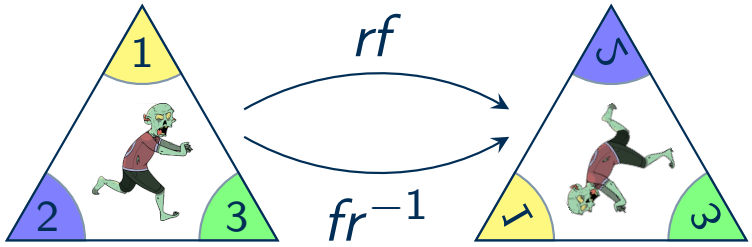
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



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

Calculating in D_n

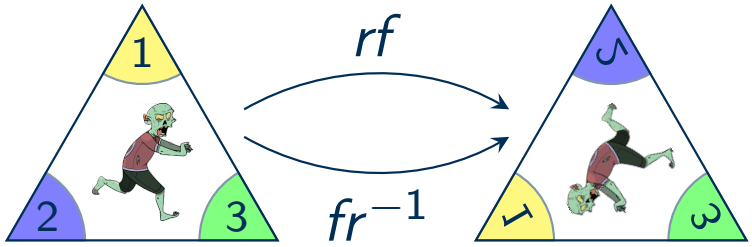
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



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

Calculating in D_n

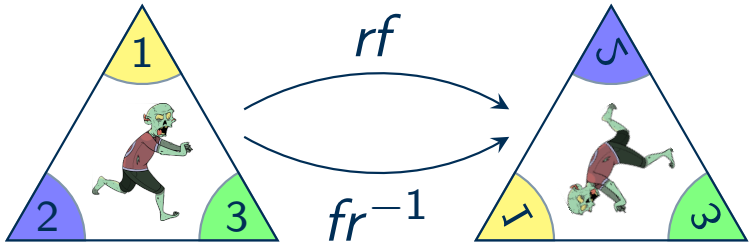
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



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

Calculating in D_n

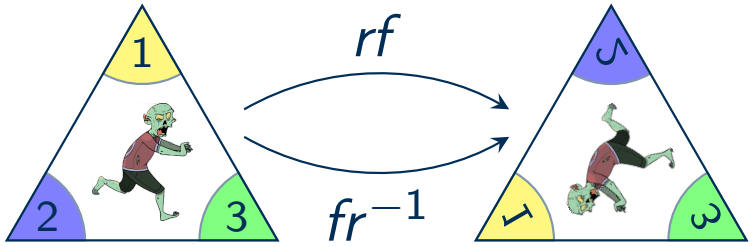
$$D_n = \langle r, f \,|\, r^n = f^2 = e, rf = fr^{-1} \rangle$$



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

Calculating in D_n

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

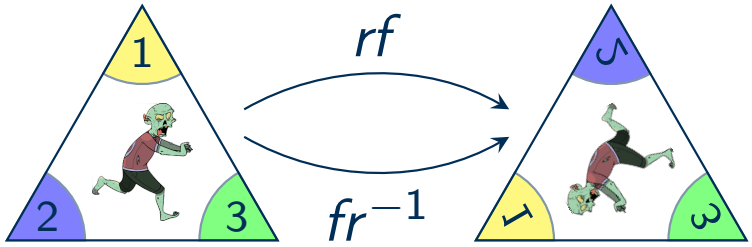


$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \\ &= fr^{n-3} \end{aligned}$$

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

Calculating in D_n

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

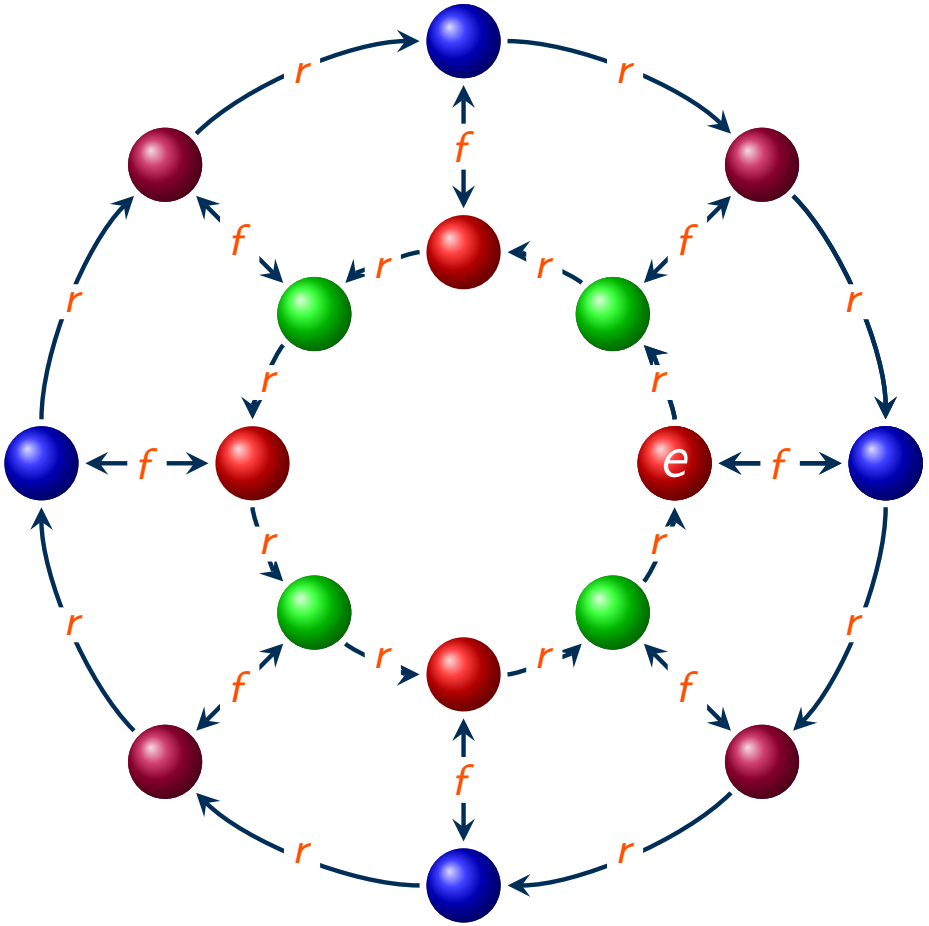


$$\begin{aligned} r^3 f &= r^2(rf) \\ &= r^2(fr^{-1}) \\ &= r(rf)r^{n-1} \\ &= r(fr^{-1})r^{n-1} \\ &= (rf)r^{n-2} \\ &= (fr^{-1})r^{n-2} \\ &= fr^{n-3} \end{aligned}$$

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

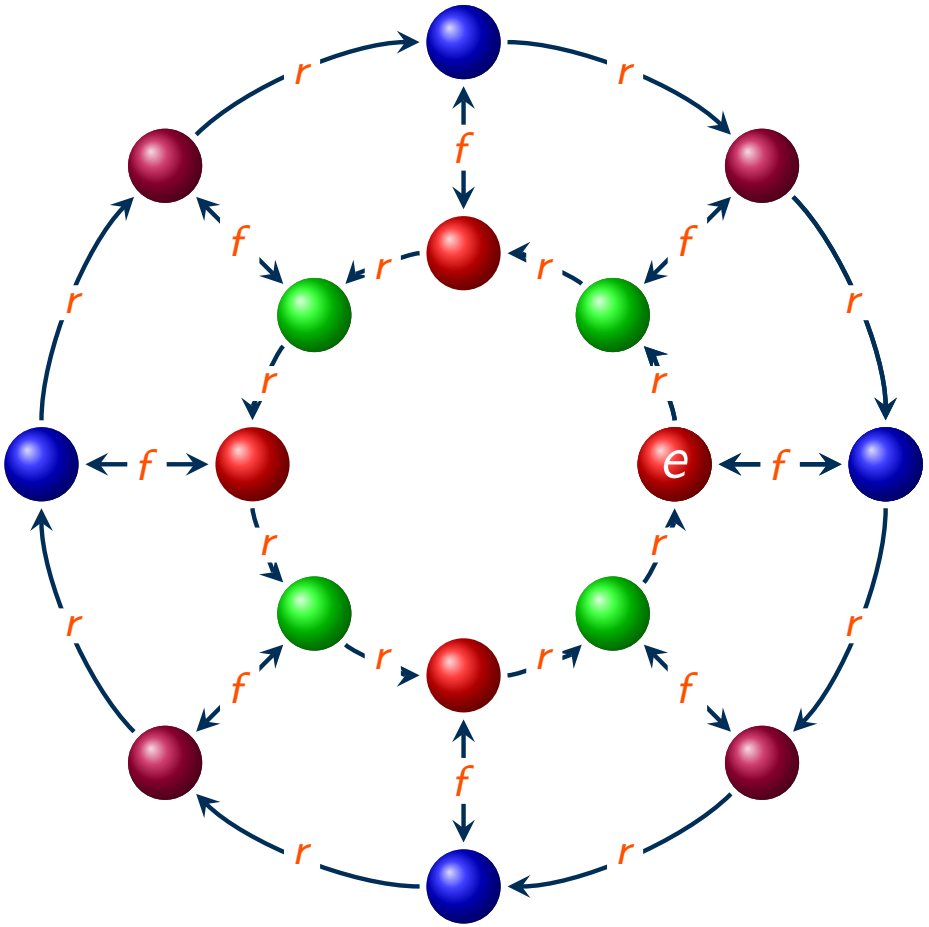
$$fr^k = r^{-k} f = r^{n-k} f$$

$D_8 = \langle r, f \mid r^8 = f^2 = e, rf = fr^{-1} \rangle$



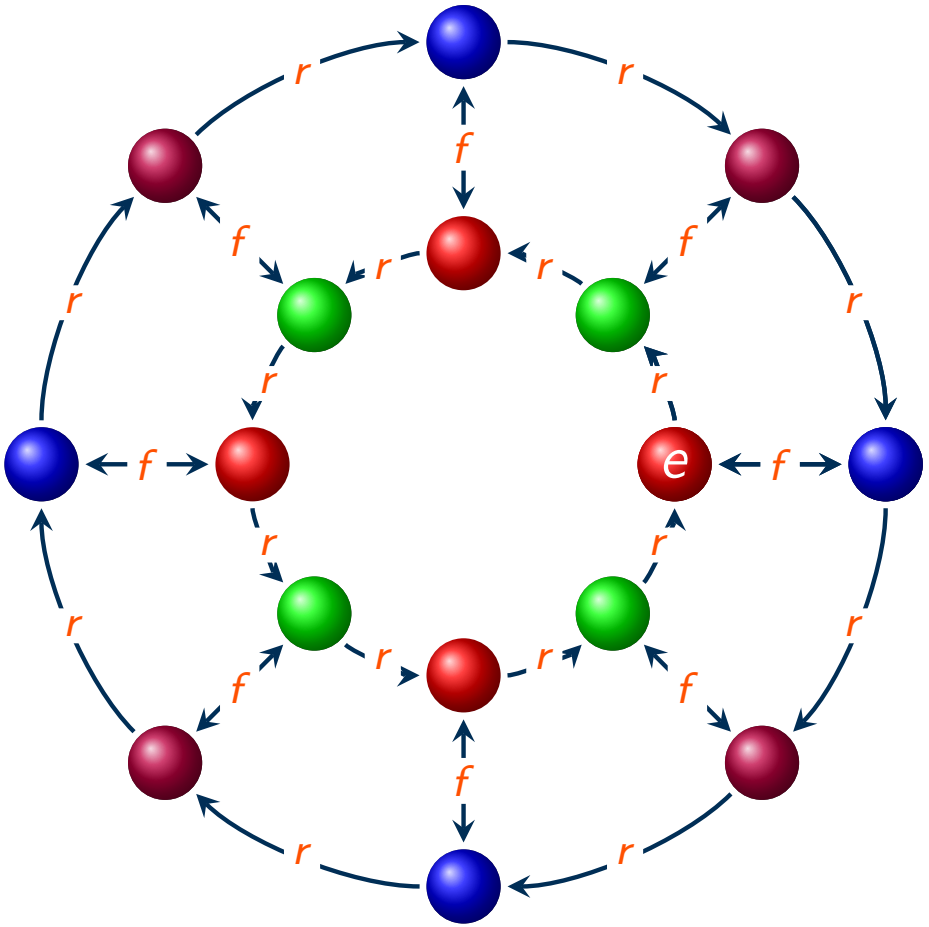
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{r^2 f, r^4 f, r^6 f, f\}$

$D_8 = \langle r, f \mid r^8 = f^2 = e, rf = fr^{-1} \rangle$



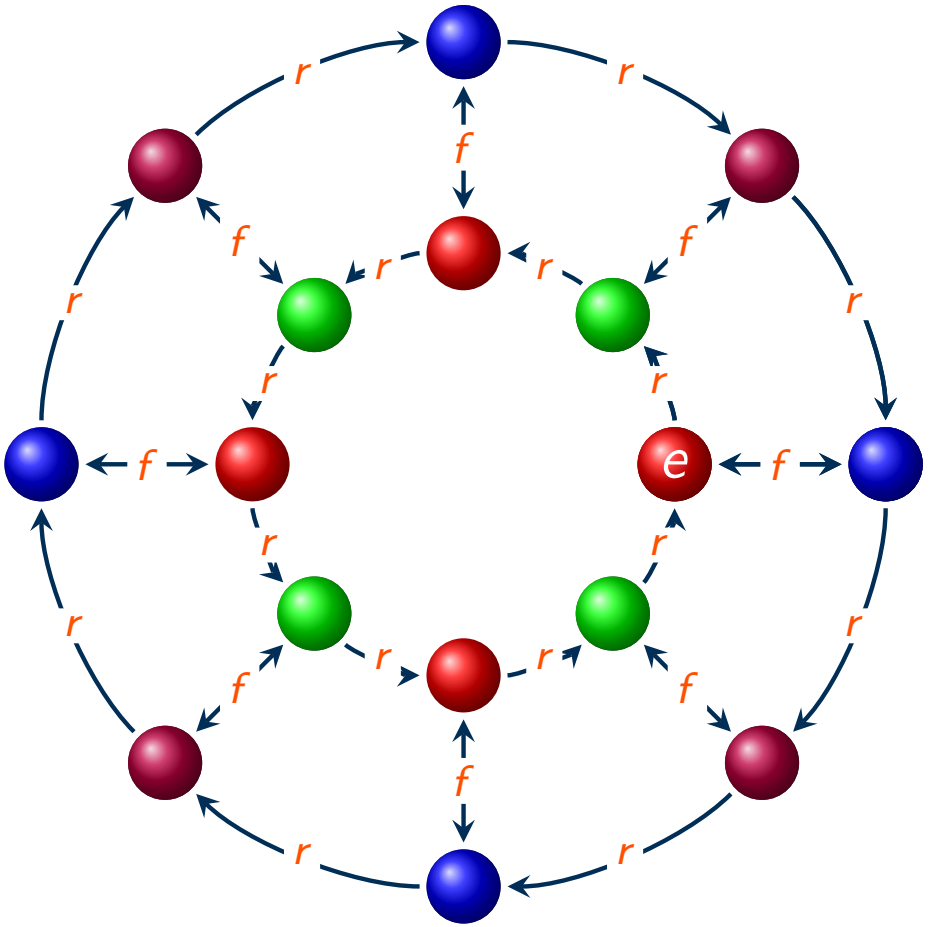
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$

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



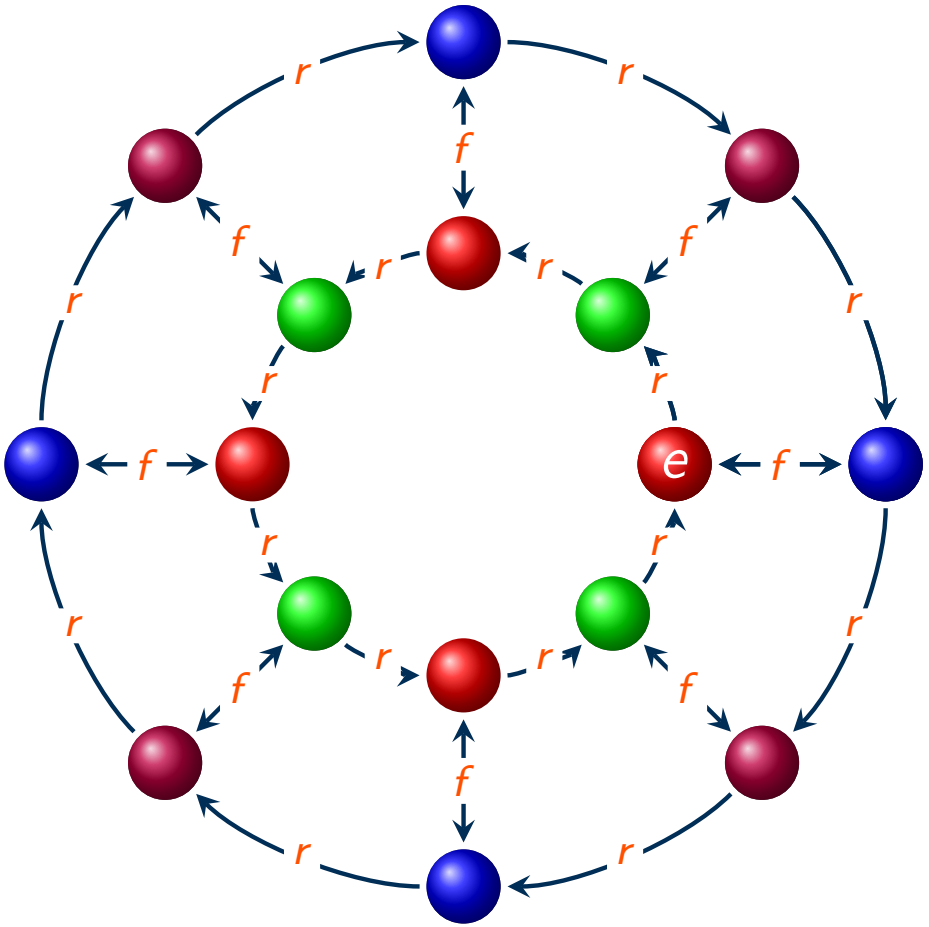
- $\langle r^2 \rangle = \{r^2, r^4, r^6, e\}$
- $f\langle r^2 \rangle = \{fr^2, fr^4, fr^6, f\}$
- $r\langle r^2 \rangle = \{r^3, r^5, r^7, r\}$
- $fr\langle r^2 \rangle = \{fr^3, fr^5, fr^7, fr\}$
- $\langle r^2 \rangle f = \{fr^6, fr^4, fr^2, f\}$
- $\langle r^2 \rangle r = \{r^3, r^5, r^7, r\}$

$D_8 = \langle r, f \mid r^8 = f^2 = e, rf = fr^{-1} \rangle$



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

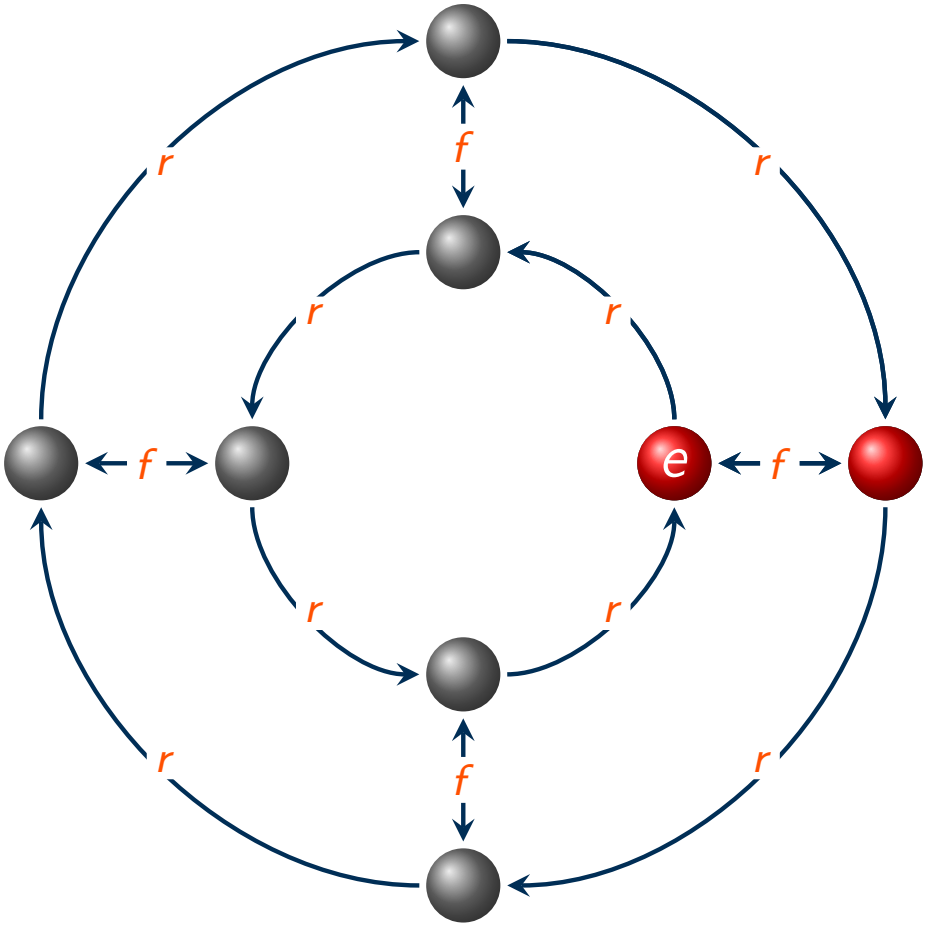
$D_8 = \left\langle r, f \middle| r^8 = f^2 = e, rf = fr^{-1} \right\rangle$



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

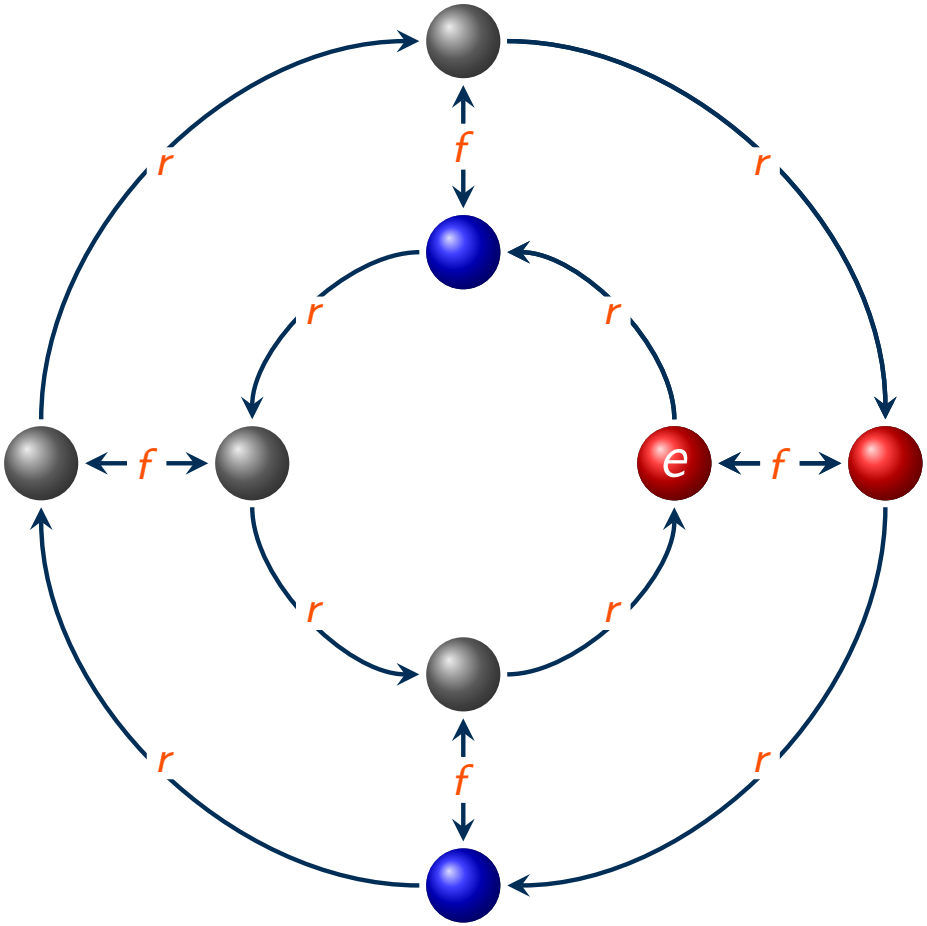
$$D_8 = \left\langle r^2 \right\rangle \cup f\left\langle r^2 \right\rangle \cup r\left\langle r^2 \right\rangle \cup fr\left\langle r^2 \right\rangle$$

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



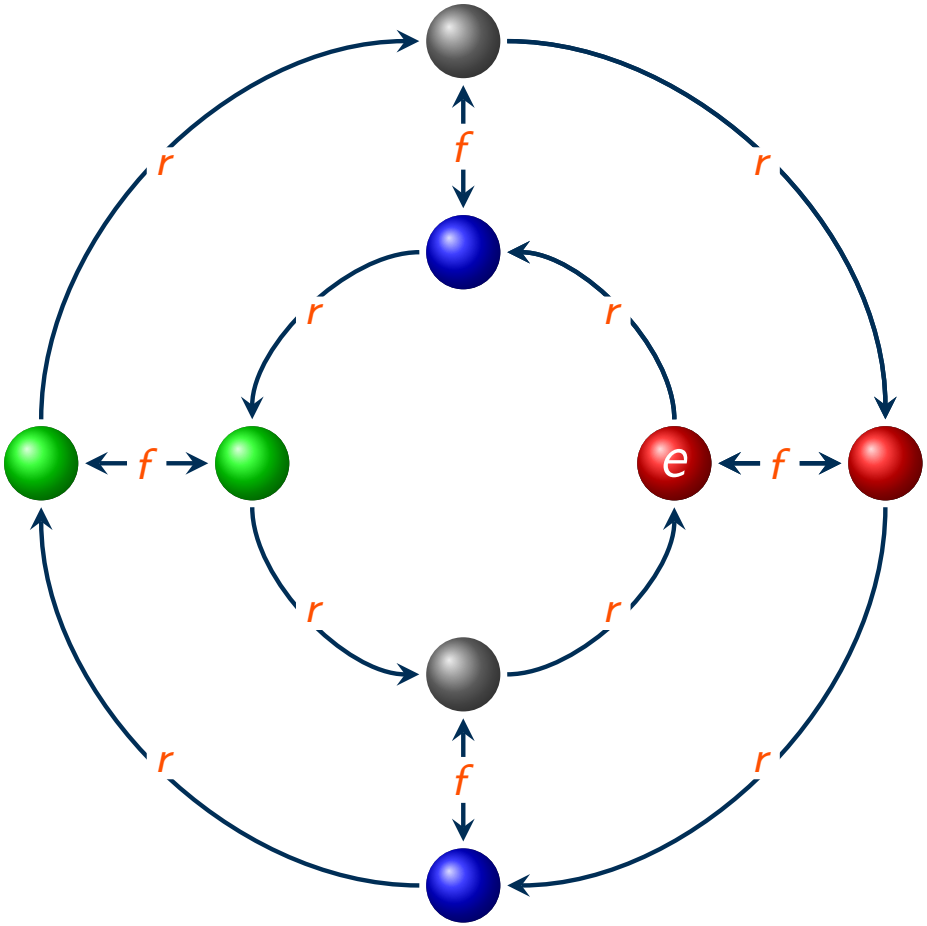
- $\langle f \rangle = \{f, e\}$

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



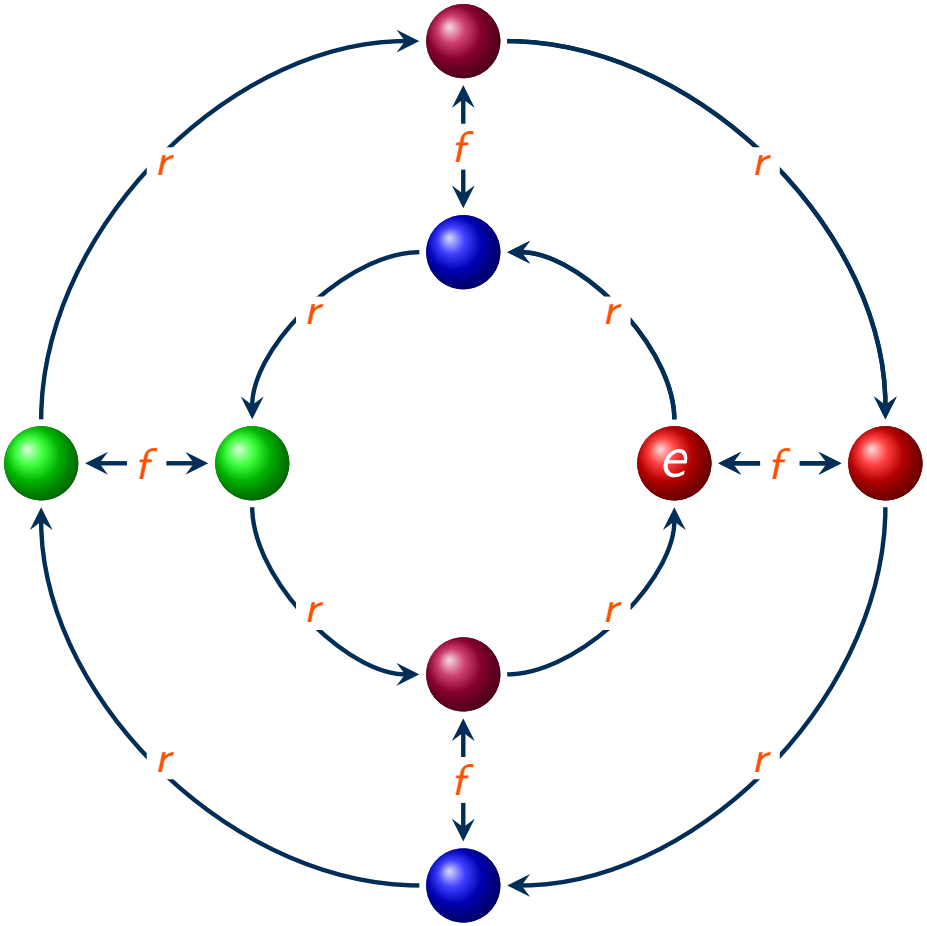
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$

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



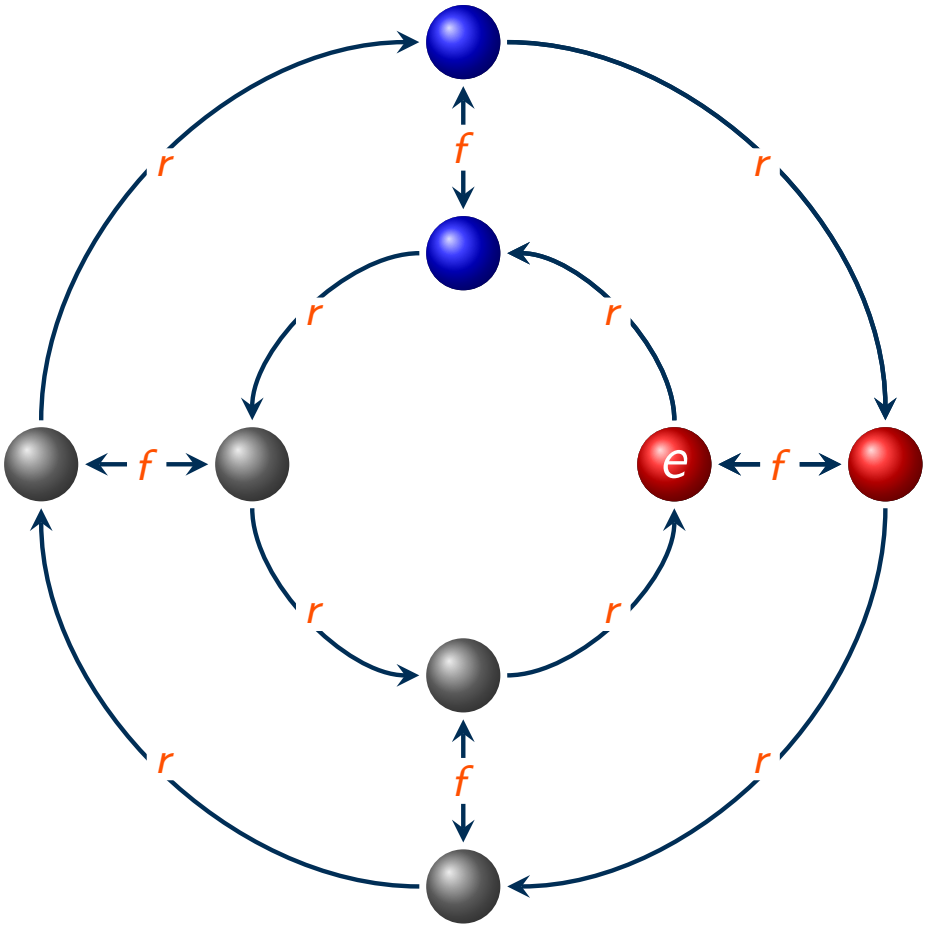
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$

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



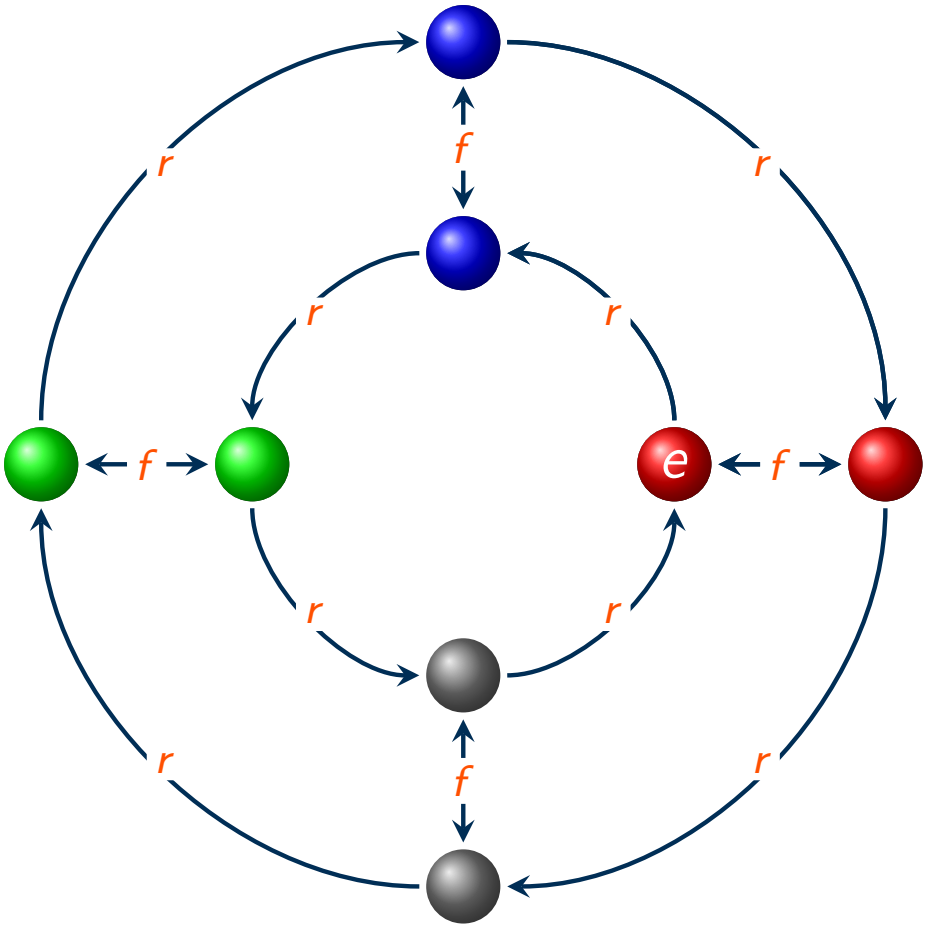
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$
- $r^3\langle f \rangle = \{r^3 f, r^3\}$

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



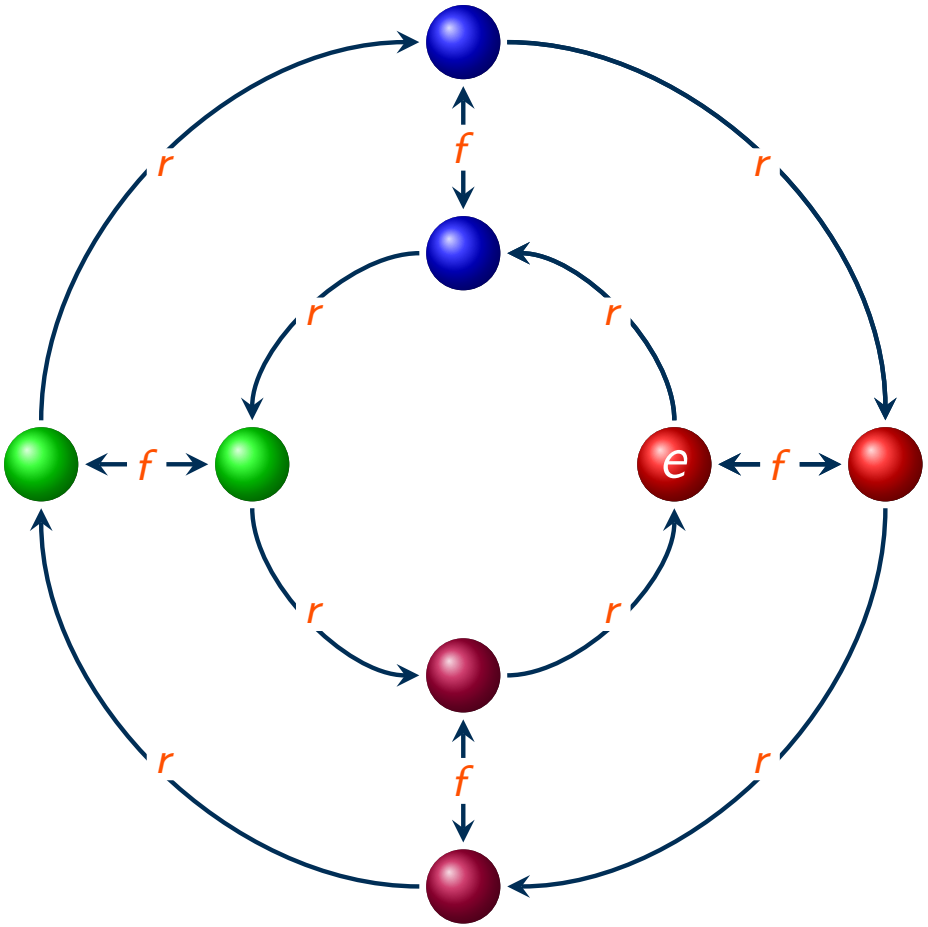
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$
- $r^3\langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$

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



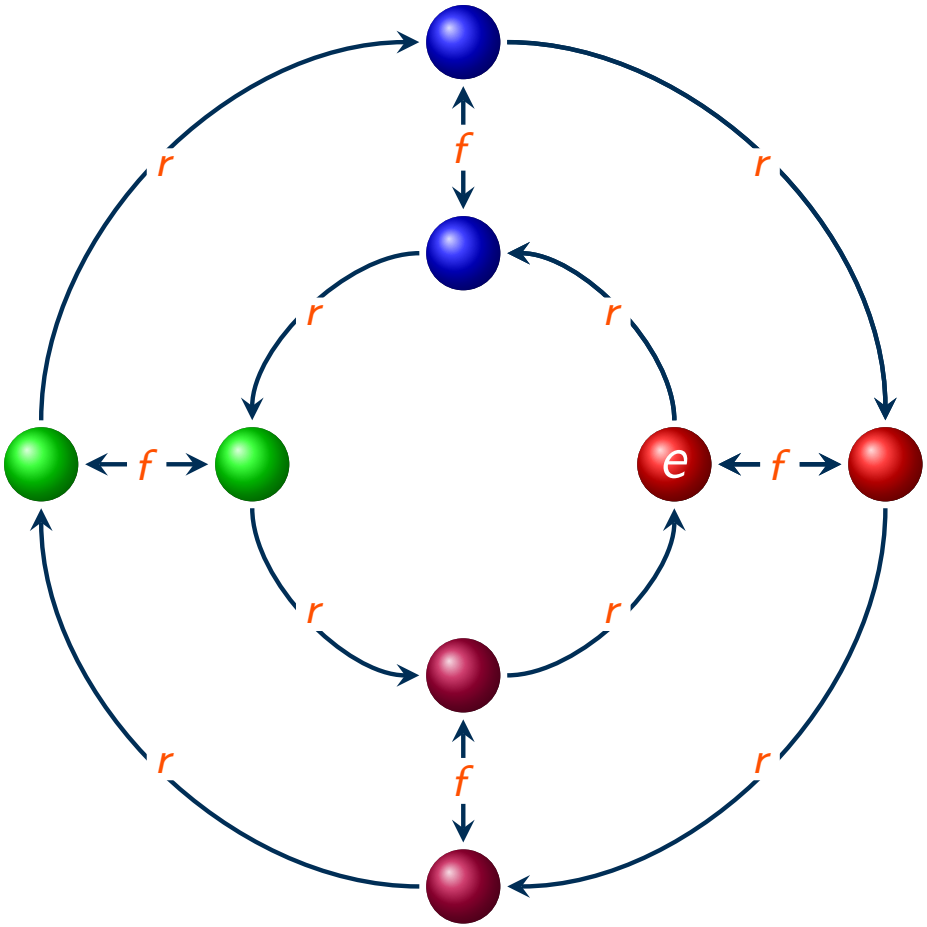
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$
- $r^3\langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$
- $\langle f \rangle r^2 = \{fr^2, r^2\} = \{r^2 f, r^2\}$

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



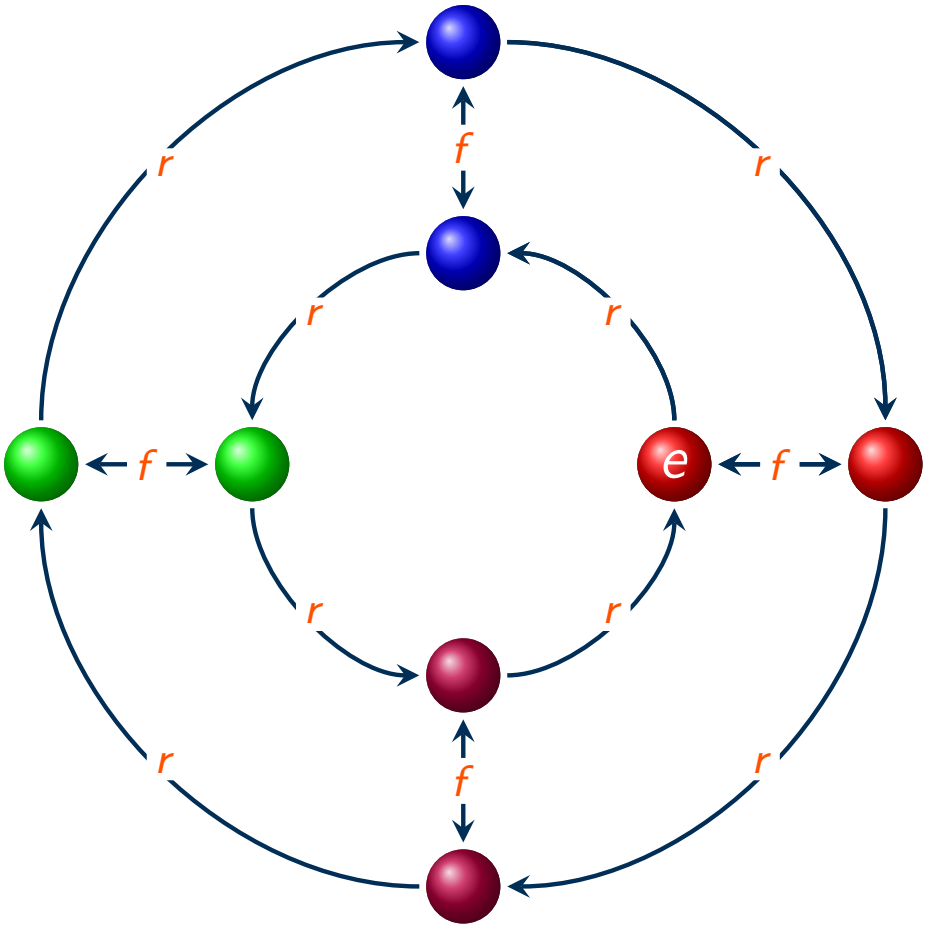
- $\langle f \rangle = \{f, e\}$
- $r\langle f \rangle = \{rf, r\}$
- $r^2\langle f \rangle = \{r^2 f, r^2\}$
- $r^3\langle f \rangle = \{r^3 f, r^3\}$
- $\langle f \rangle r = \{fr, r\} = \{r^3 f, r\}$
- $\langle f \rangle r^2 = \{fr^2, r^2\} = \{r^2 f, r^2\}$
- $\langle f \rangle r^3 = \{fr^3, r^3\}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

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



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

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



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

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

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.

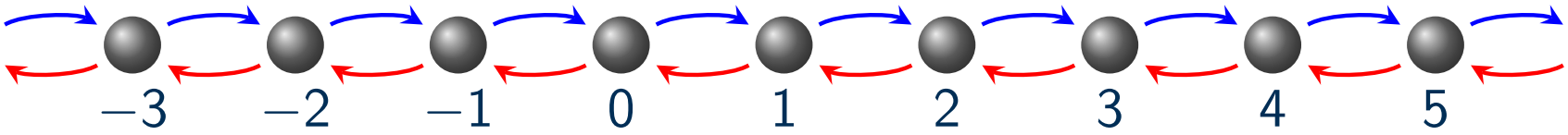
Definition (Normal Subgroup)

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

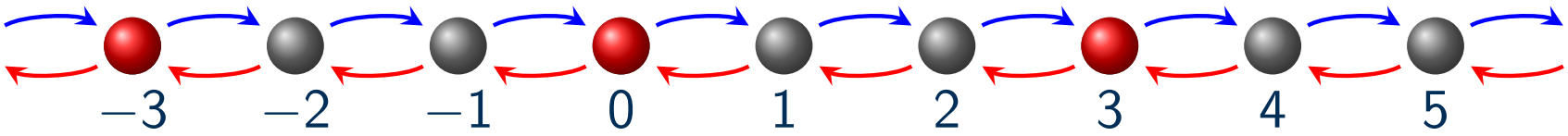
$$gH = Hg,$$

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

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

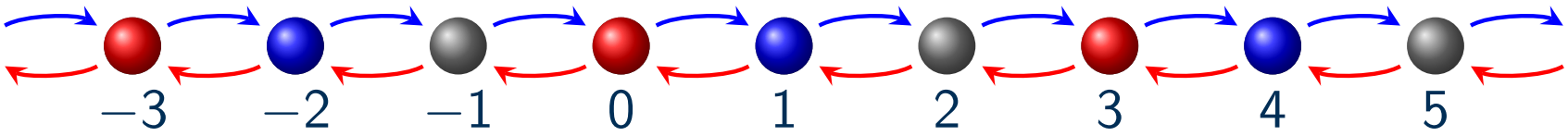


$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



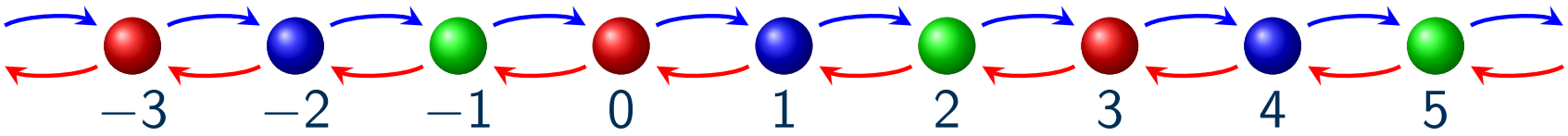
- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

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



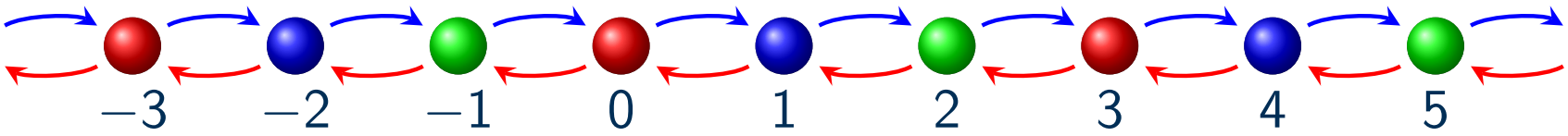
- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$
- $1 + 3\mathbb{Z} = \{1, -2, 4, -5, 7, \ldots\}$

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



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

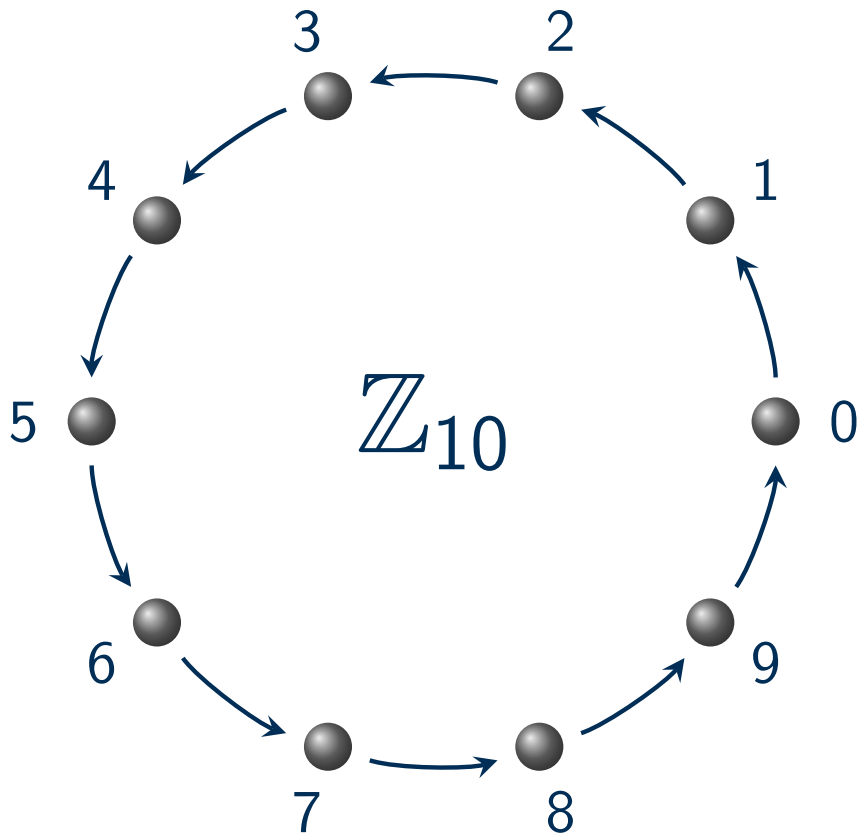
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



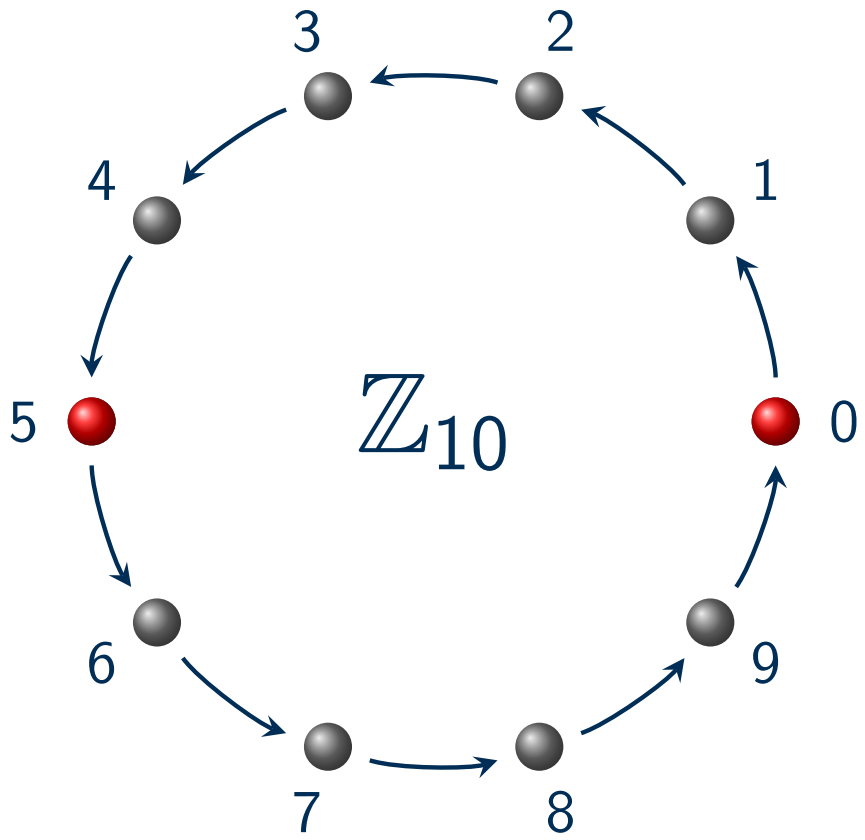
- $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$
- $1 + 3\mathbb{Z} = \{1, -2, 4, -5, 7, \ldots\}$
- $2 + 3\mathbb{Z} = \{2, -1, 5, -4, 8, \ldots\}$

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

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

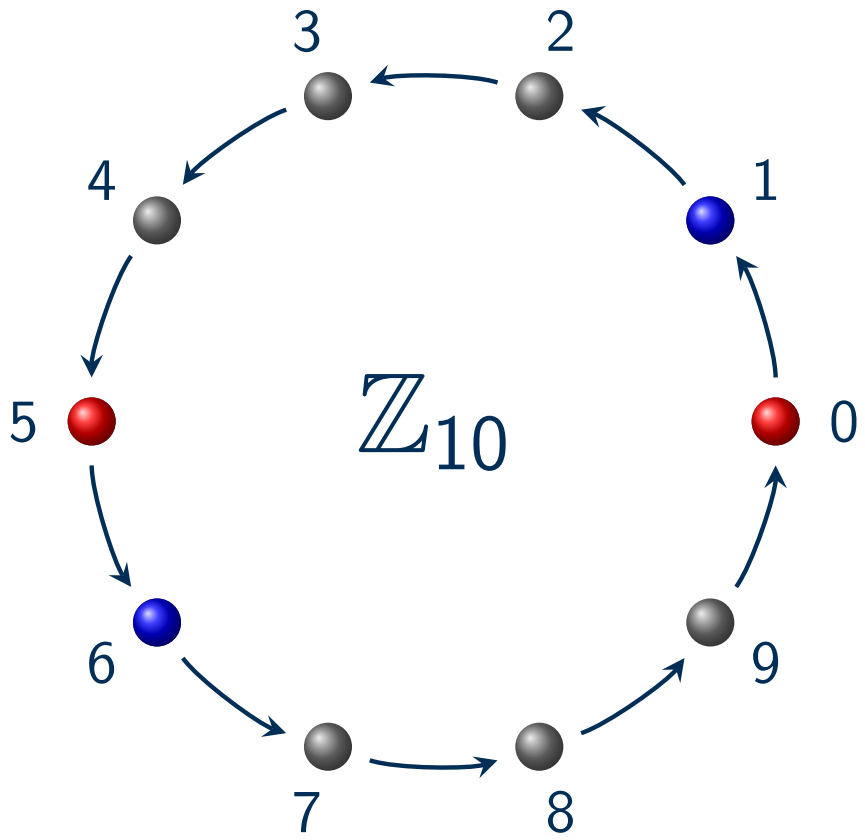


$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



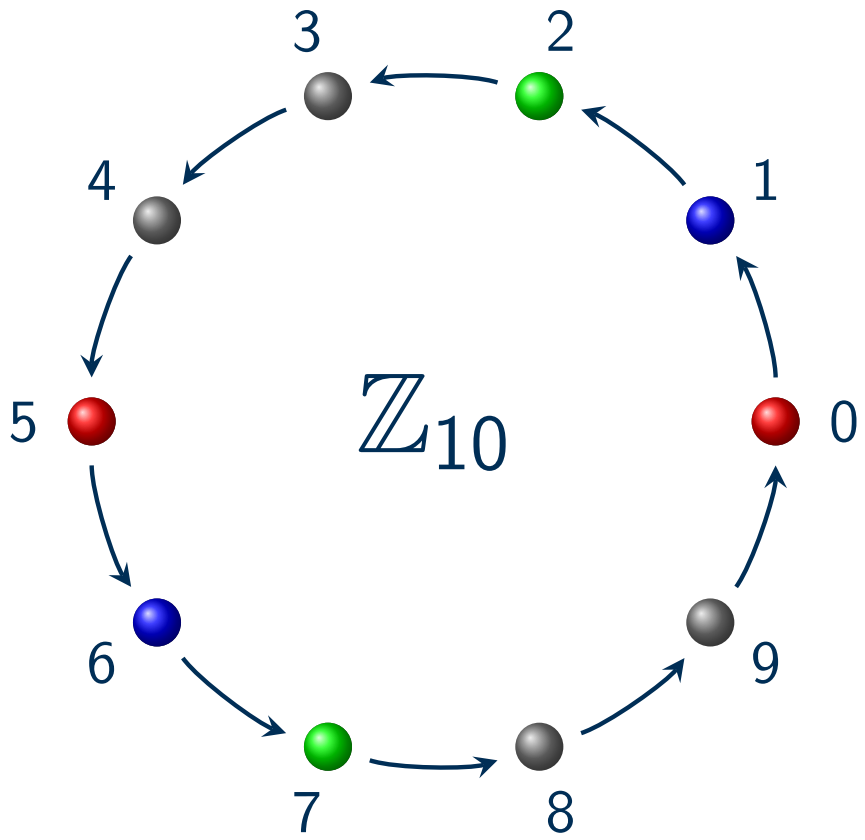
- $\langle 5 \rangle = \{0, 5\}$

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



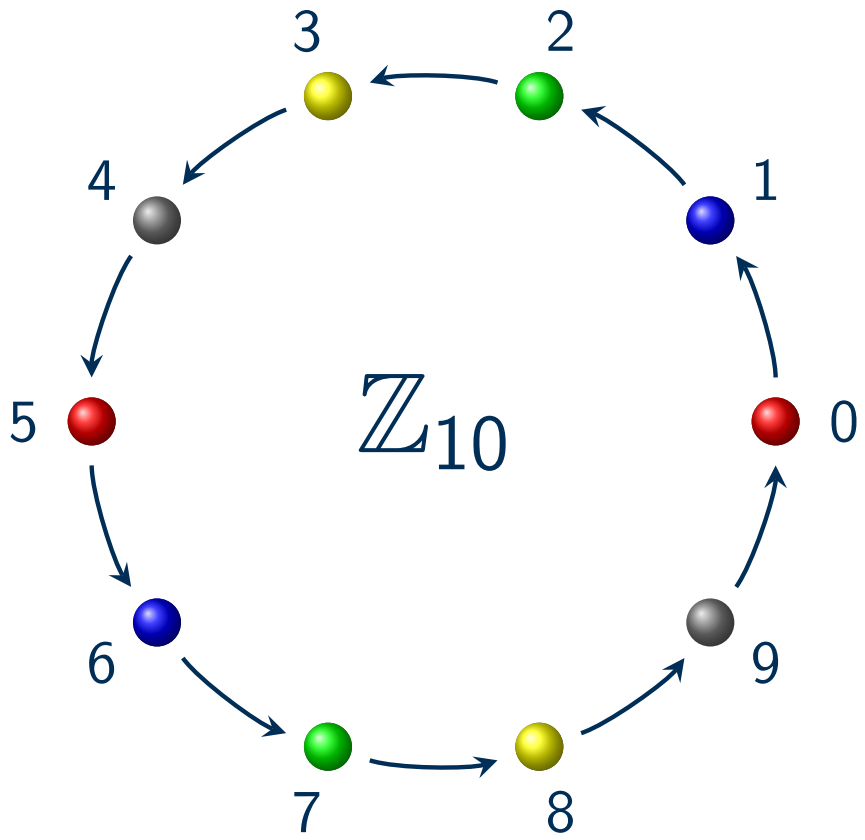
- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$

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



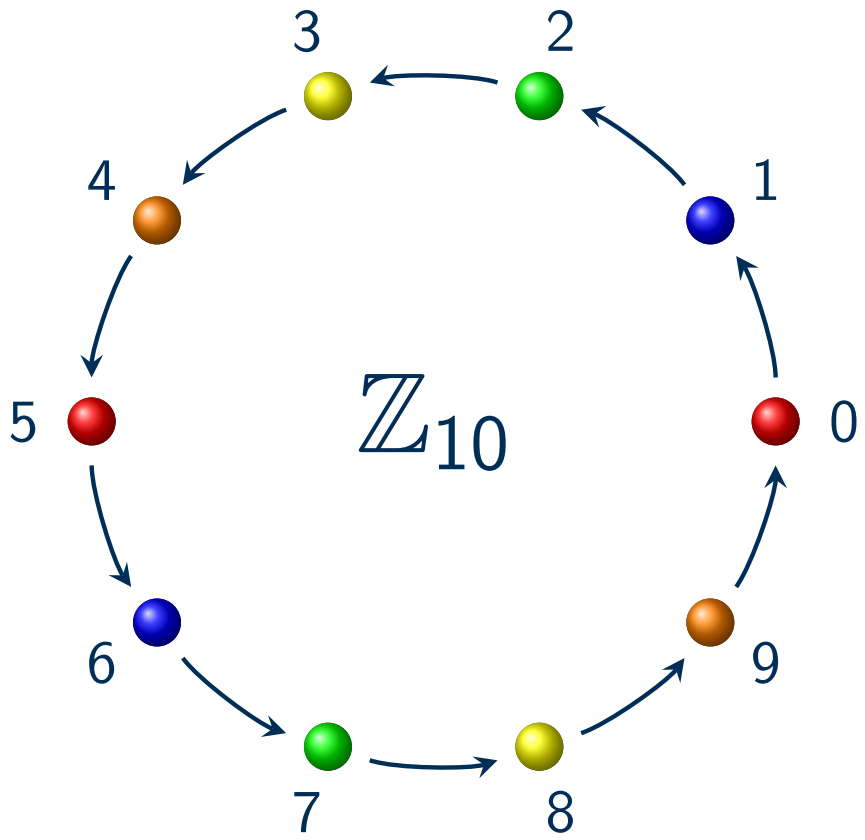
- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$

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



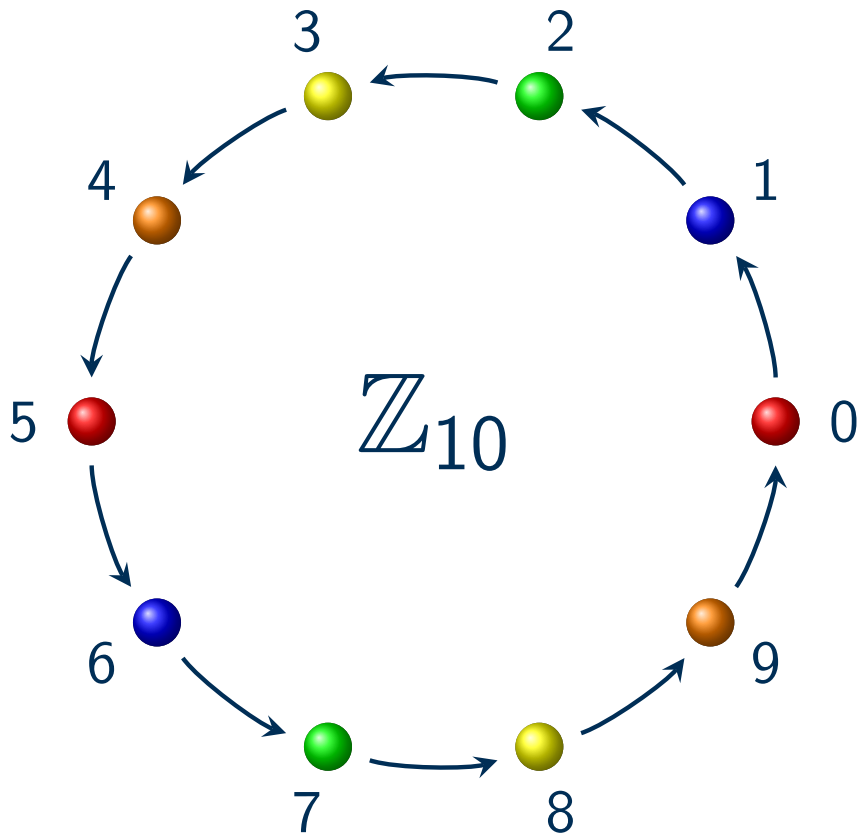
- $\langle 5 \rangle = \{0, 5\}$
- $1 + \langle 5 \rangle = \{1, 6\}$
- $2 + \langle 5 \rangle = \{2, 7\}$
- $3 + \langle 5 \rangle = \{3, 8\}$

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



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

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



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

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

Table of Contents

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* $b^{-1}a \in H$.

Properties' Proofs

Proof.

□

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.

□

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$. Then we can write $a = bh_b h_a^{-1}$ and $b = ah_a h_b^{-1}$.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$. Then we can write $a = bh_b h_a^{-1}$ and $b = ah_a h_b^{-1}$. Therefore, for all $h \in H$,

$$ah = (bh_b h_a^{-1})h = b(h_b h_a^{-1} h) \in bH$$

and $aH \subseteq bH$.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$. Then we can write $a = bh_b h_a^{-1}$ and $b = ah_a h_b^{-1}$. Therefore, for all $h \in H$,

$$ah = (bh_b h_a^{-1})h = b(h_b h_a^{-1} h) \in bH$$

and $aH \subseteq bH$. Similarly, $bH \subseteq aH$ and $aH = bH$ if they are not disjoint.

Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$. Then we can write $a = bh_b h_a^{-1}$ and $b = ah_a h_b^{-1}$. Therefore, for all $h \in H$,

$$ah = (bh_b h_a^{-1})h = b(h_b h_a^{-1} h) \in bH$$

   and $aH \subseteq bH$. Similarly, $bH \subseteq aH$ and $aH = bH$ if they are not disjoint.
4. Note, $aH = bH$ implies $\forall h \in H \, \exists h' \in H$ with $ah = bh'$; so $b^{-1}a = h'h^{-1} \in H$.

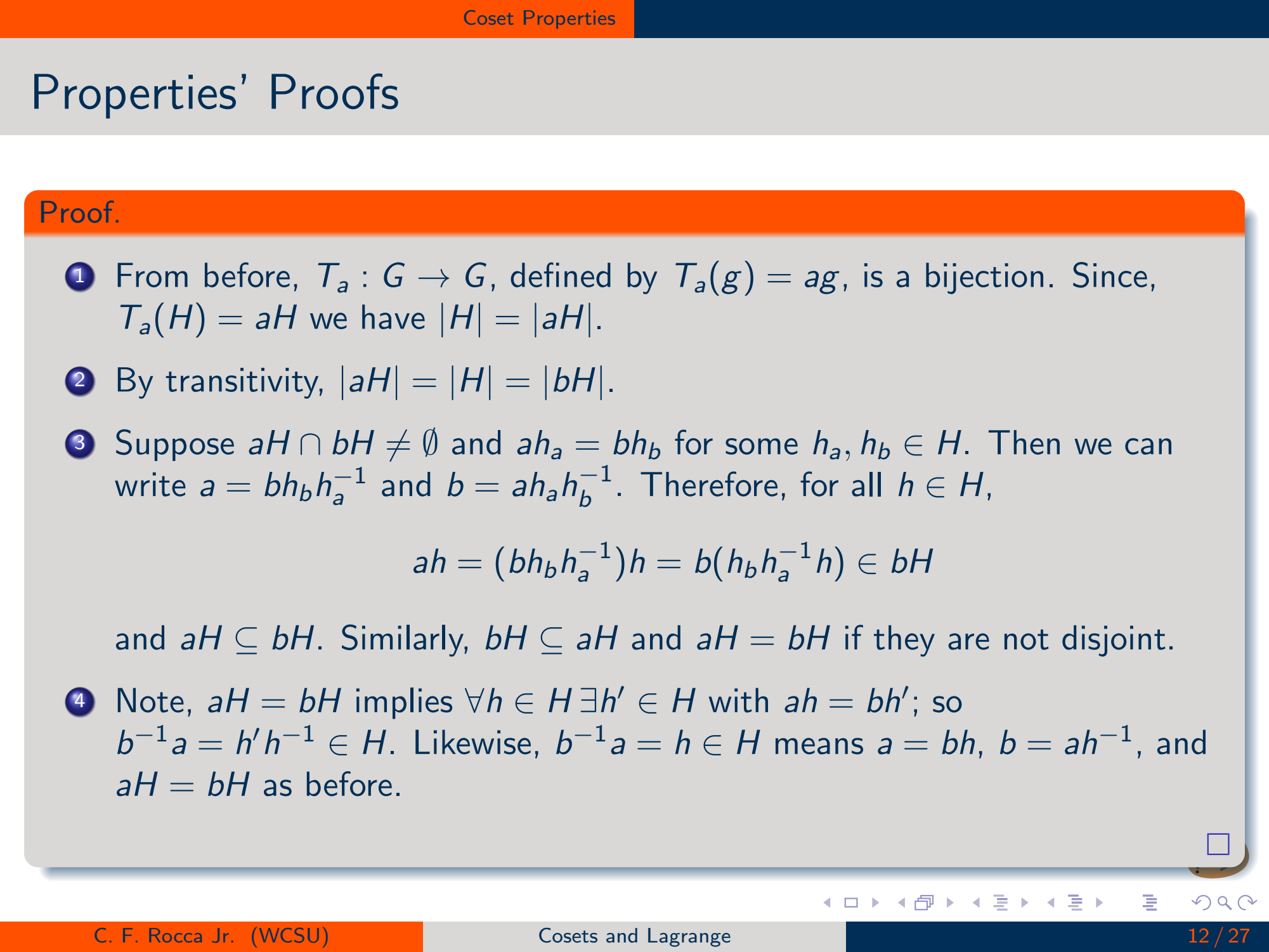
Properties' Proofs

Proof.

1. From before, $T_a : G \to G$, defined by $T_a(g) = ag$, is a bijection. Since, $T_a(H) = aH$ we have $|H| = |aH|$.
2. By transitivity, $|aH| = |H| = |bH|$.
3. Suppose $aH \cap bH \neq \emptyset$ and $ah_a = bh_b$ for some $h_a, h_b \in H$. Then we can write $a = bh_b h_a^{-1}$ and $b = ah_a h_b^{-1}$. Therefore, for all $h \in H$,

$$ah = (bh_b h_a^{-1})h = b(h_b h_a^{-1} h) \in bH$$

   and $aH \subseteq bH$. Similarly, $bH \subseteq aH$ and $aH = bH$ if they are not disjoint.
4. Note, $aH = bH$ implies $\forall h \in H \, \exists h' \in H$ with $ah = bh'$; so $b^{-1}a = h'h^{-1} \in H$. Likewise, $b^{-1}a = h \in H$ means $a = bh$, $b = ah^{-1}$, and $aH = bH$ as before.



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* $b^{-1}a \in H$.

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 $i \neq j$.

Equivalence Classes and Partitions

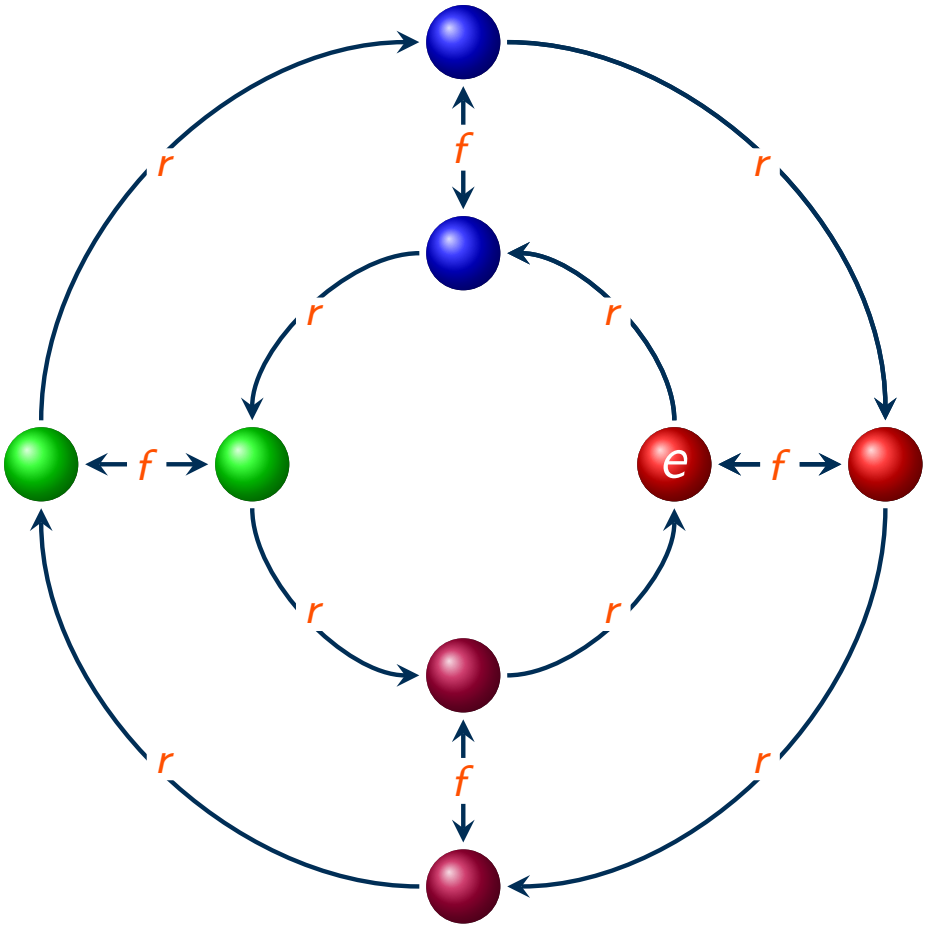
Definition

Given a group G, subgroup $H \subseteq G$, and elements $a, b \in G$ we say

$$a \equiv b \pmod{H}$$

if and only if $b^{-1}a \in H$ (i.e. $aH = bH$).
(We could show that this is an equivalence relation using the properties of cosets.)

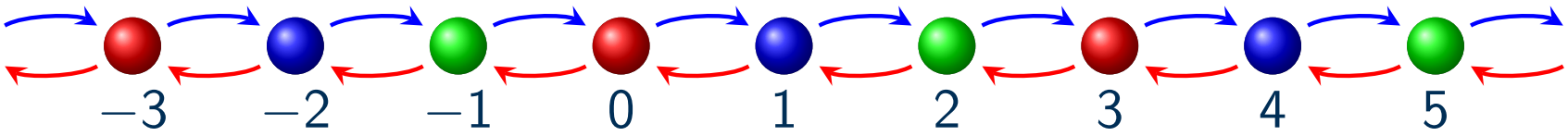
$D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



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

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

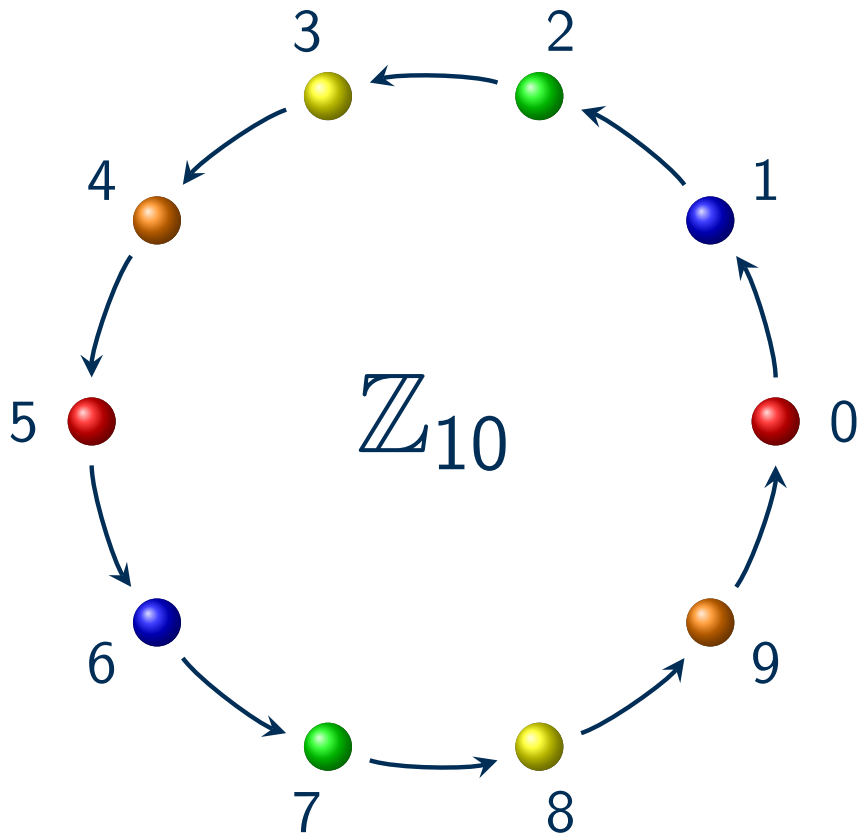
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



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

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

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



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

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

Table of Contents

Lagrange's Theorem

Theorem (Lagrange's Theorem)

Given a finite group G and subgroup $H \subseteq G$, the order of H divides the order of G, $|H| \big| |G|$.

Proof of Lagrange's Theorem

Proof.

□

Proof of Lagrange's Theorem

Proof.

From previous theorems we have that for some set of $g_i \in G$, we can write

$$G = \bigcup_i g_i H$$

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

□

Proof of Lagrange's Theorem

Proof.

From previous theorems we have that for some set of $g_i \in G$, we can write

$$G = \bigcup_i g_i H$$

with $g_i H \cap g_j H = \emptyset$ when $i \neq j$. Then

$$|G| = \left| \bigcup_i g_i H \right|$$

□

Proof of Lagrange's Theorem

Proof.

From previous theorems we have that for some set of $g_i \in G$, we can write

$$G = \bigcup_i g_i H$$

with $g_i H \cap g_j H = \emptyset$ when $i \neq j$. Then

$$|G| = \left| \bigcup_i g_i H \right| = \sum_i |g_i H|$$

□

Proof of Lagrange's Theorem

Proof.

From previous theorems we have that for some set of $g_i \in G$, we can write

$$G = \bigcup_i g_i H$$

with $g_i H \cap g_j H = \emptyset$ when $i \neq j$. Then

$$|G| = \left| \bigcup_i g_i H \right| = \sum_i |g_i H| = \sum_i |H| .$$

□

Proof of Lagrange's Theorem

Proof.

From previous theorems we have that for some set of $g_i \in G$, we can write

$$G = \bigcup_i g_i H$$

with $g_i H \cap g_j H = \emptyset$ when $i \neq j$. Then

$$|G| = \left| \bigcup_i g_i H \right| = \sum_i |g_i H| = \sum_i |H| .$$

Therefore, $|G| = n|H|$ for some integer n. □

Lagrange's Theorem

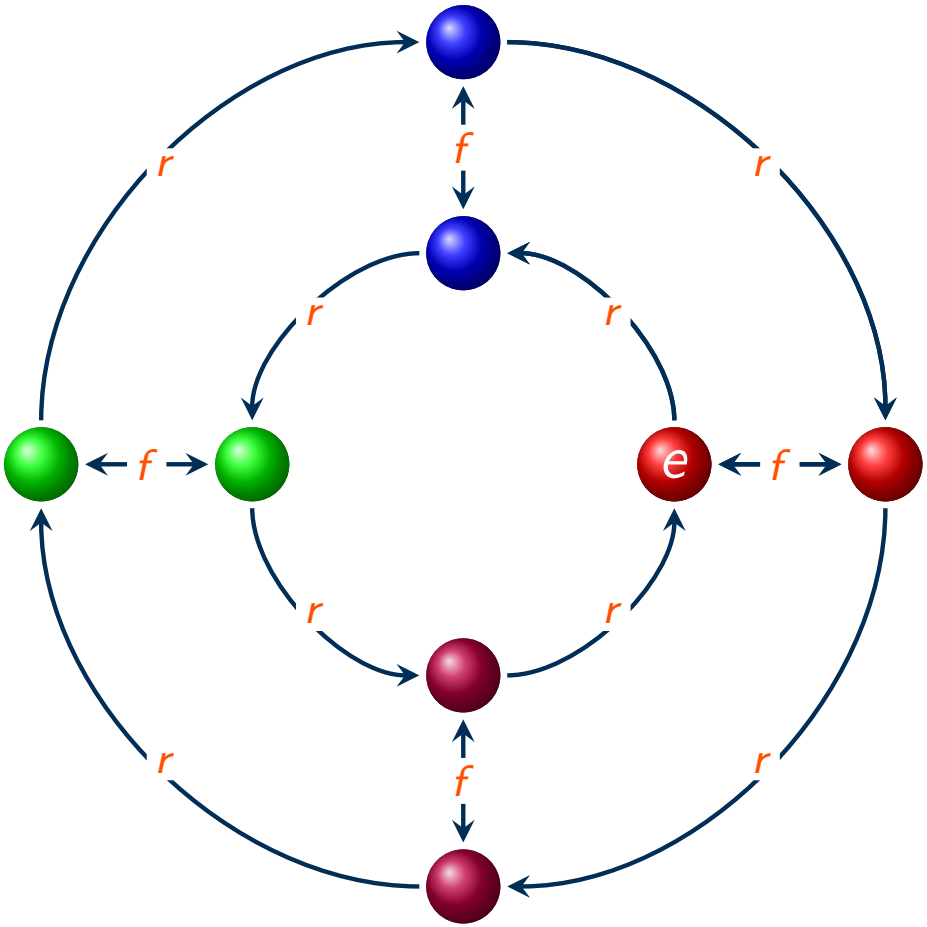
Theorem (Lagrange's Theorem)

Given a finite group G and subgroup $H \subseteq G$, the order of H divides the order of G, $|H| \mid |G|$.

Definition (Index of a Subgroup)

The number of distinct left cosets of $H \subseteq G$ is called the **index of H in G** and denoted $[G : H]$. If $|G|$ is finite then $|G| = [G : H]|H|$.

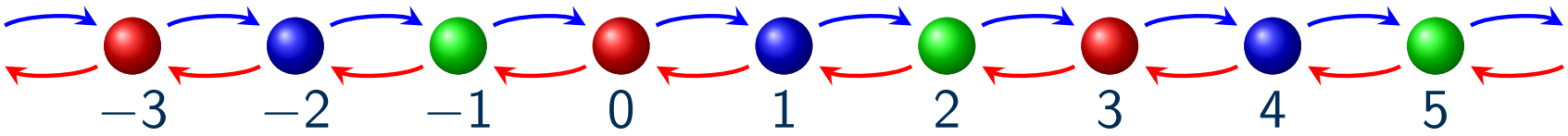
$D_4 = \left\langle r, f \middle| r^4 = f^2 = e, rf = fr^{-1} \right\rangle$



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

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

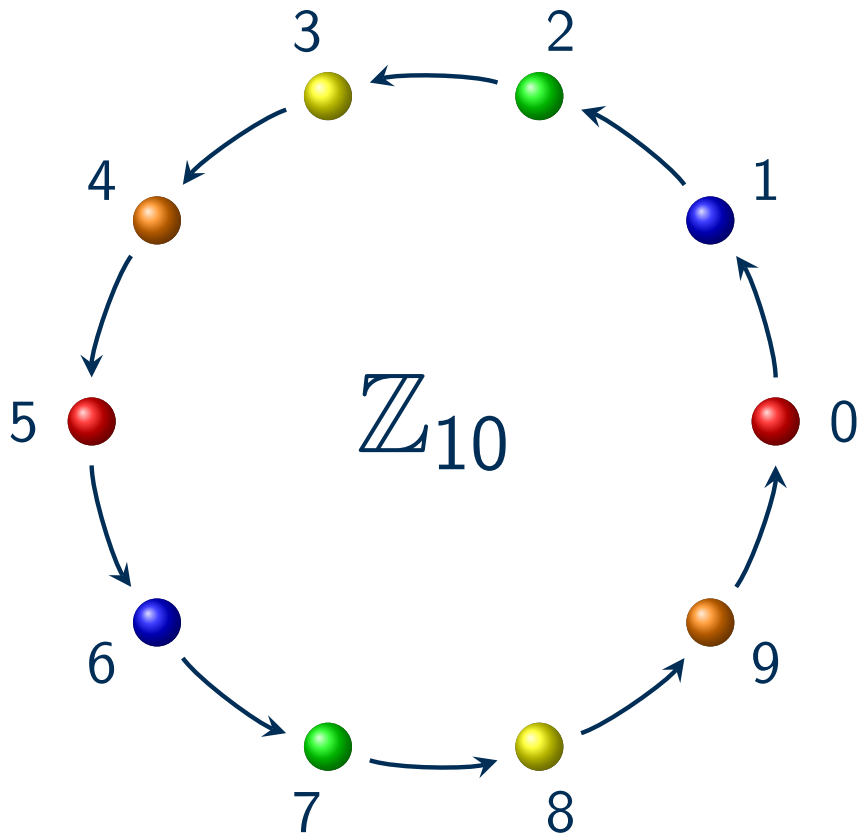
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$



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

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

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



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

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

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Proof.

The order of a is the least l such that $a^l = e$.

.

□

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Proof.

The order of a is the least l such that $a^l = e$. This will also be the order of the cyclic subgroup $\langle a \rangle = \{a, a^2, \ldots, a^{l-1}, e\}$ and so divides $k = |G|$ by Lagrange's Theorem.

□

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Proof.

The order of a is the least l such that $a^l = e$. This will also be the order of the cyclic subgroup $\langle a \rangle = \{a, a^2, \ldots, a^{l-1}, e\}$ and so divides $k = |G|$ by Lagrange's Theorem. Now we may write $k = ql$ for some unique q and therefore

$$a^k = a^{ql} = (a^l)^q = e.$$

□

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Theorem

Given a finite group G,if the order of G is prime, $|G| = p$, then G isomorphic to $\mathbb{Z}_p$.

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Theorem

Given a finite group G,if the order of G is prime, $|G| = p$, then G isomorphic to $\mathbb{Z}_p$.

Proof.

The only divisors of $p = |G|$ are 1 and p.

□

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

Theorem

Given a finite group G,if the order of G is prime, $|G| = p$, then G isomorphic to $\mathbb{Z}_p$.

Proof.

The only divisors of $p = |G|$ are 1 and p. Therefore, every non-identity element $a \in G$ has order p and $G = \langle a \rangle$. □

Corollaries to Lagrange

Corollary

Given a finite group G with $k = |G|$, and $a \in G$:

1. $|a|$ *divides* $k = |G|$
2. $a^k = e \in G$

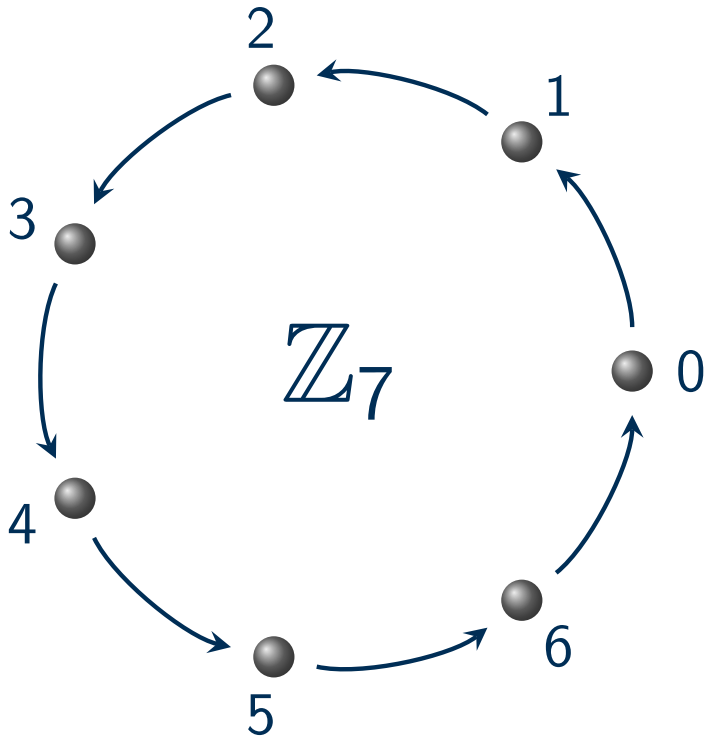
Theorem

Given a finite group G,if the order of G is prime, $|G| = p$, then G isomorphic to $\mathbb{Z}_p$.

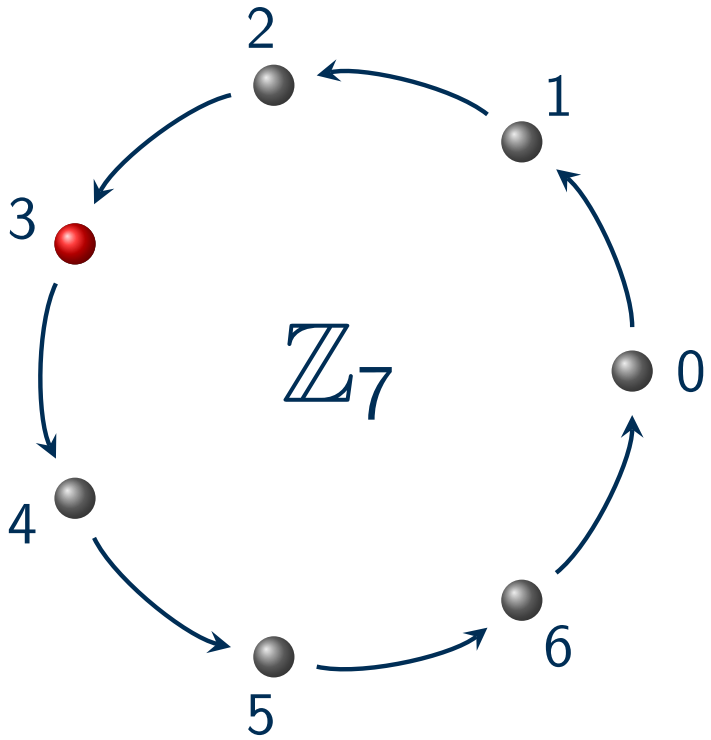
Proof.

The only divisors of $p = |G|$ are 1 and p. Therefore, every non-identity element $a \in G$ has order p and $G = \langle a \rangle$. Hence, we have $G = \langle a \rangle \cong \mathbb{Z}_p$. □

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$$

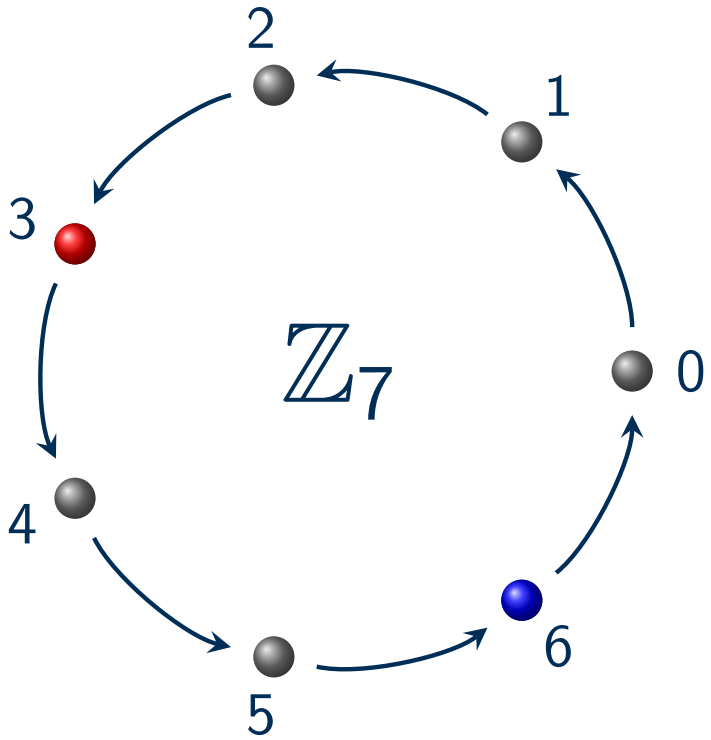


$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



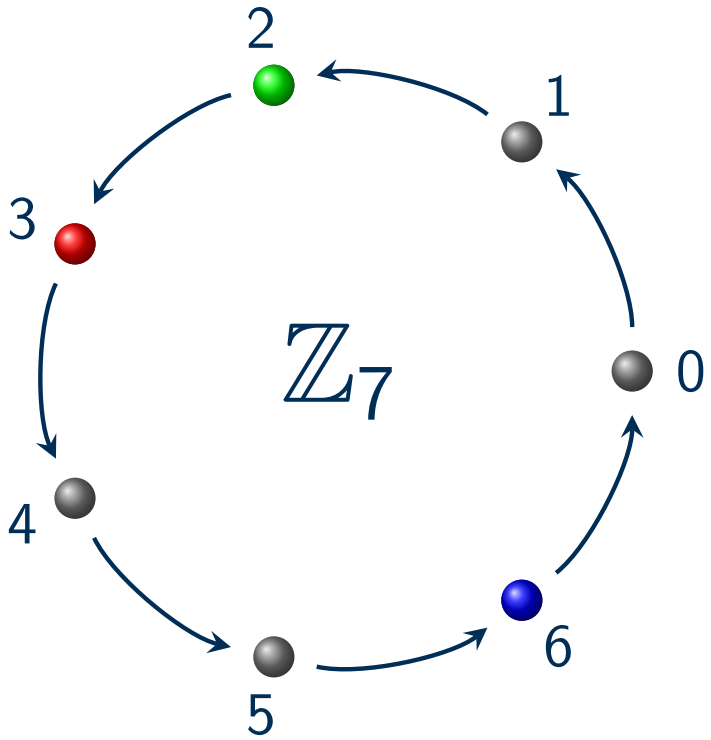
1. $1 \cdot 3 \equiv 3 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



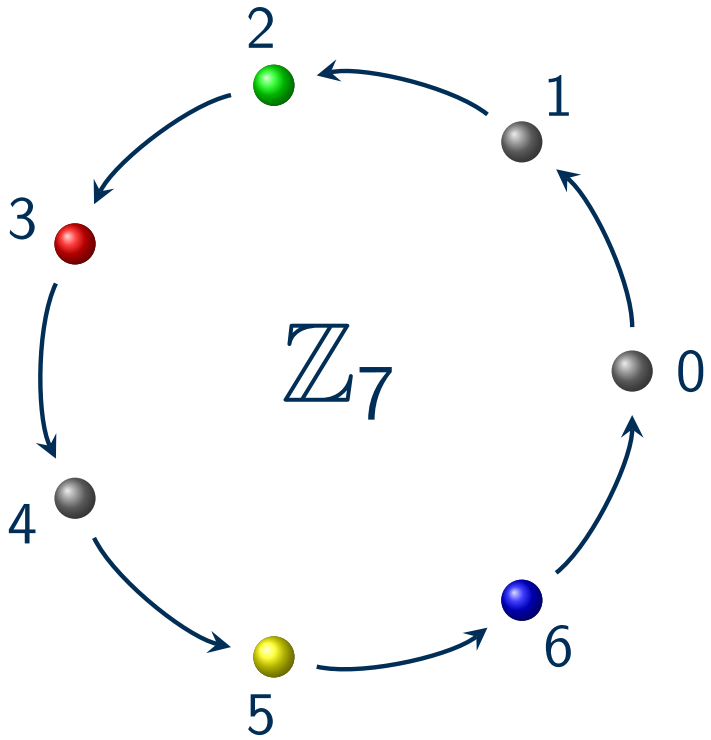
1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



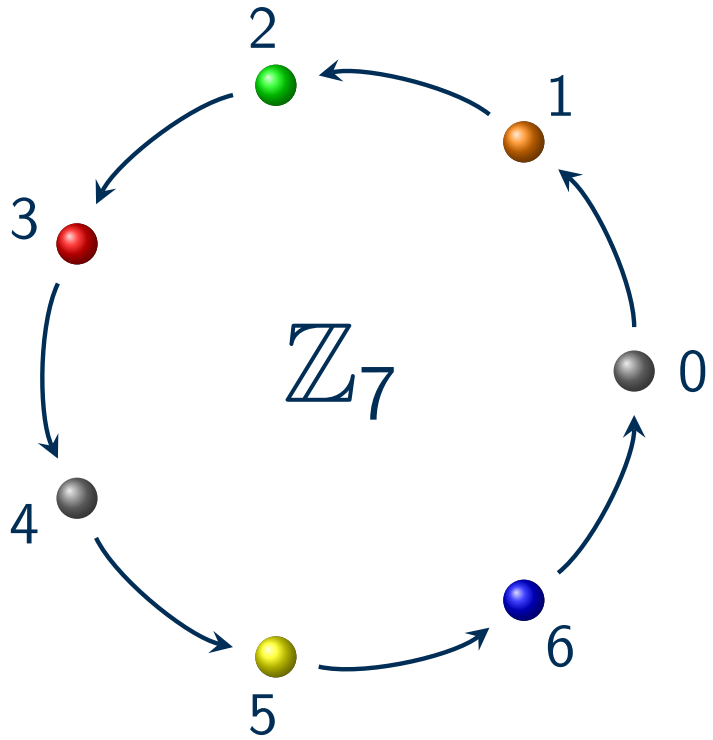
1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$
3. $3 \cdot 3 \equiv 2 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



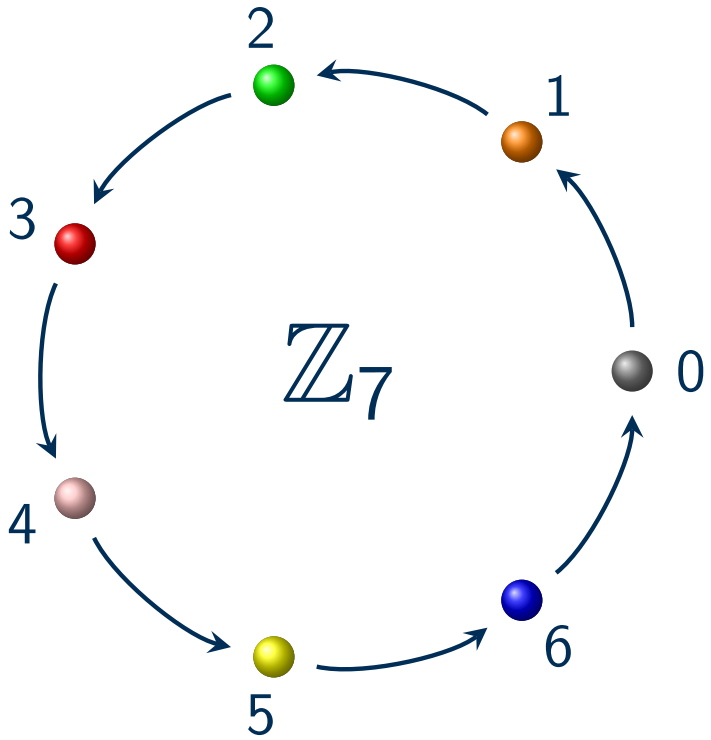
1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$
3. $3 \cdot 3 \equiv 2 \pmod 7$
4. $4 \cdot 3 \equiv 5 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



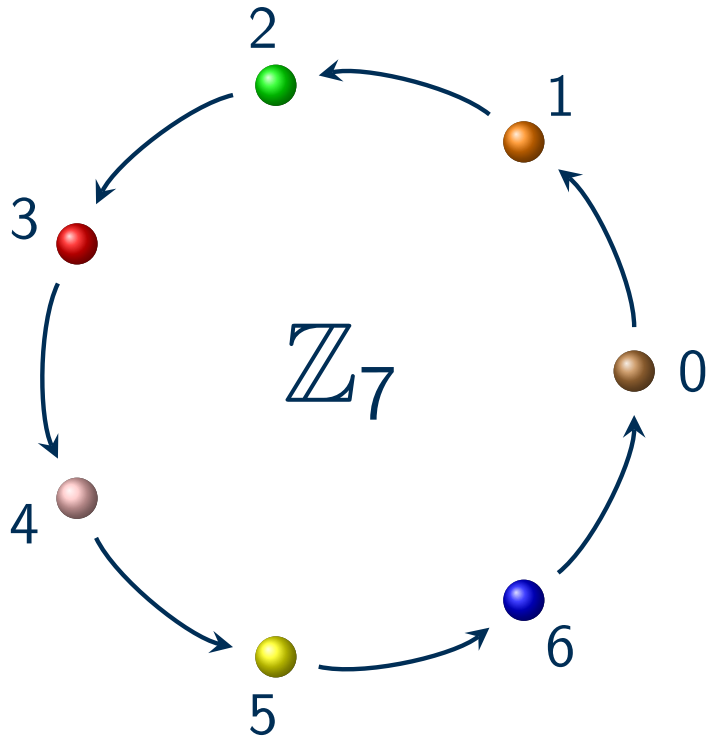
1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$
3. $3 \cdot 3 \equiv 2 \pmod 7$
4. $4 \cdot 3 \equiv 5 \pmod 7$
5. $5 \cdot 3 \equiv 1 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$
3. $3 \cdot 3 \equiv 2 \pmod 7$
4. $4 \cdot 3 \equiv 5 \pmod 7$
5. $5 \cdot 3 \equiv 1 \pmod 7$
6. $6 \cdot 3 \equiv 4 \pmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$



1. $1 \cdot 3 \equiv 3 \pmod 7$
2. $2 \cdot 3 \equiv 6 \pmod 7$
3. $3 \cdot 3 \equiv 2 \pmod 7$
4. $4 \cdot 3 \equiv 5 \pmod 7$
5. $5 \cdot 3 \equiv 1 \pmod 7$
6. $6 \cdot 3 \equiv 4 \pmod 7$
7. $7 \cdot 3 \equiv 0 \pmod 7$

Cosets and Lagrange

Dr. Chuck Rocca

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES