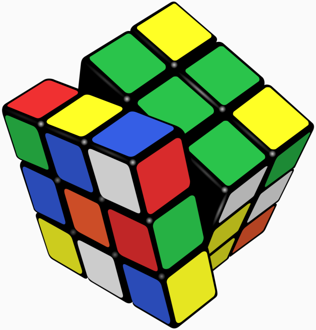
# Rubik's cubes and permutation group theory

**Lawrence Chen**

October 6, 2022

**Honours presentation**



# Contents

# Some basic group theory

# What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G, \ (g, h) \mapsto gh$,

# What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g,h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

# What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g,h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

## What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

# What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses

# What is a group? i

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

**Example (Cyclic group)**

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

**Example (Cyclic group)**

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity $1 = a^0$, inverses

**Definition (group)**

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

**Example (Integers under addition)**

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

**Example (Cyclic group)**

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity $1 = a^0$, inverses $a^{-k}$ for $a^k \in C_n$, associative.

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

## Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is

# Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is

## Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is

# Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$.

# Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$. (If $|X| = 1$, $G$ is **cyclic**.)

# Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$. (If $|X| = 1$, $G$ is **cyclic**.)

**Example (Cyclic group)**

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$:

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$. (If $|X| = 1$, $G$ is **cyclic**.)

**Example (Cyclic group)**

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$.

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$. (If $|X| = 1$, $G$ is **cyclic**.)

**Example (Cyclic group)**

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$. If $b = a^2$, $c = a^3$ then $C_6 = \langle b, c \rangle$ since

# Order and generators i

**Definition (order)**

**Order** of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise $\infty$).

**Example (Cyclic group)**

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of $a$ is 4, order of $a^2$ is 2, order of $a^3$ is 4.

**Definition (generator)**

Set $X$ **generates** $G$ if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$. (If $|X| = 1$, $G$ is **cyclic**.)

**Example (Cyclic group)**

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$. If $b = a^2$, $c = a^3$ then $C_6 = \langle b, c \rangle$ since $a = cb^{-1}$ so $a^k = cb^{-1} \cdots cb^{-1} = c^k b^{-k}$.

# Permutations i

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

# Permutations i

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

$$\sigma$$

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

It means

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:

$$
\begin{tikzcd}
& 1 \arrow[drrr] & 2 & 3 & 4 & 5 & 6 \\
\sigma & & & & & & \\
& 1 & 2 & 3 & 4 & 5 & 6
\end{tikzcd}
$$

It means

$$1^\sigma = 4,$$

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:

$$\begin{tikzcd} & 1 \arrow[drrr] & 2 & 3 & 4 \arrow[dr] & 5 & 6 \\ \sigma & & & & & & \\ & 1 & 2 & 3 & 4 & 5 & 6 \end{tikzcd}$$

It means

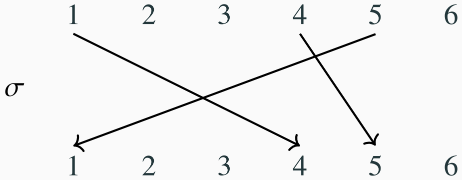
$$1^\sigma = 4,\ 4^\sigma = 5,$$

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$ is:




It means

$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,$$

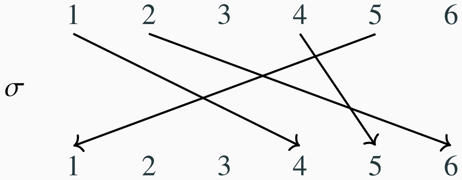
# Permutations i

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:




It means

$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,$$

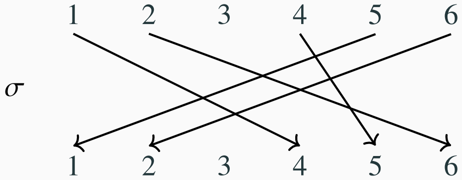
# Permutations i

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:




It means

$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,$$

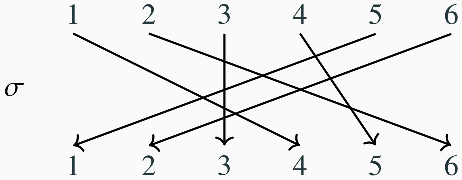
# Permutations i

**Definition (permutation)**

**Permutation** of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Write $1 = ()$ for identity. Write $i^\sigma$ not $\sigma(i)$ for *image*.

*Cycle notation:* $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$ is:

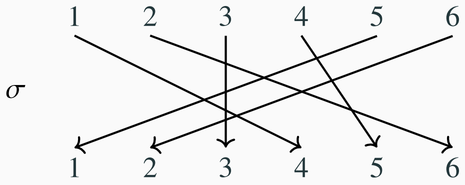



It means

$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,\ 3^\sigma = 3.$$

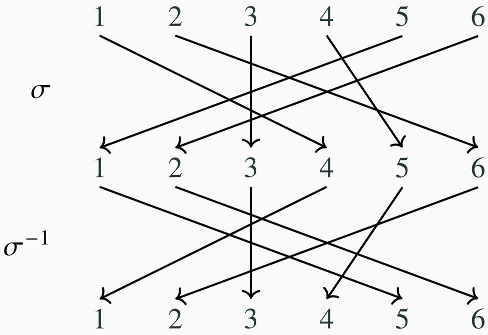
# Permutations ii

*Inverses:* For $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$:



## Permutations ii

*Inverses:* For $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$:



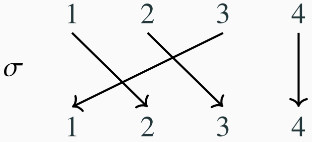

Inverse is $\sigma^{-1} = (1, 5, 4)(2, 6) \in \mathrm{Sym}(6)$.

# Permutations iii

*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$.

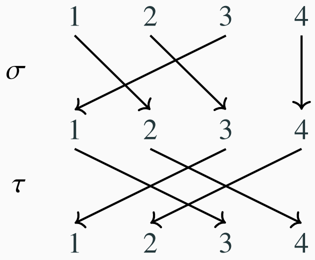
## Permutations iii

*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first $\sigma$, then $\tau$”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3)$,

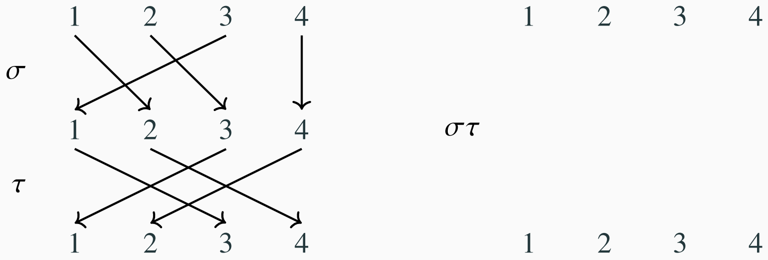


# Permutations iii

*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,



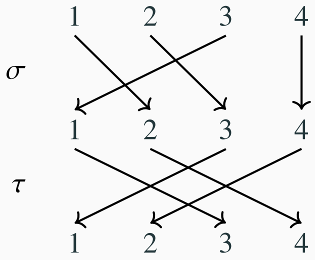
*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,

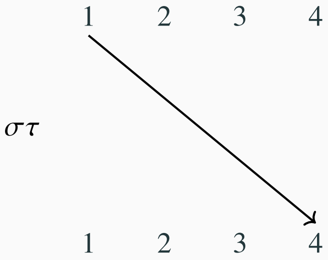



$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,$$

# Permutations iii

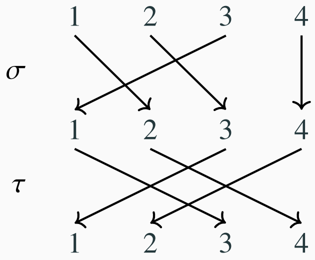
*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,

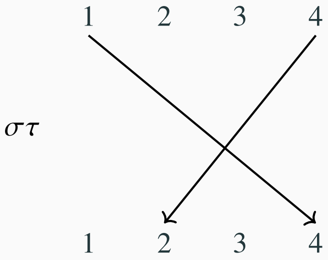



$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4,$$

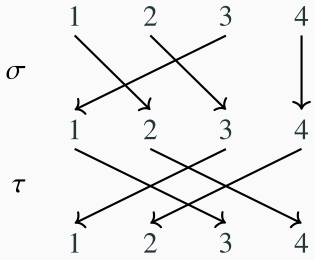
*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,

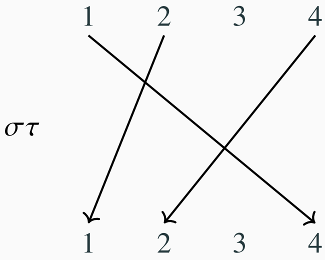



$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2$$

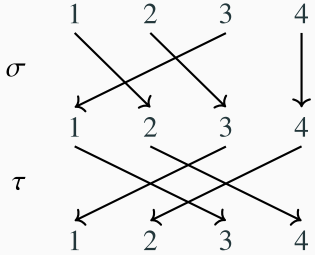
*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first $\sigma$, then $\tau$”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,

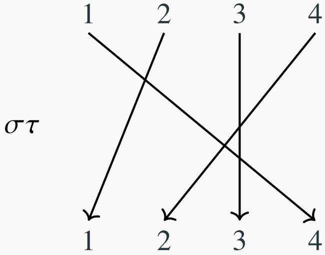



$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4, 2)$$

*Product/composition:* for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first $\sigma$, then $\tau$", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,




$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2) \in \mathrm{Sym}(4).$$

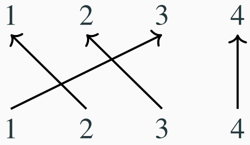
# Permutations iv

*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1, 3, 2)$,

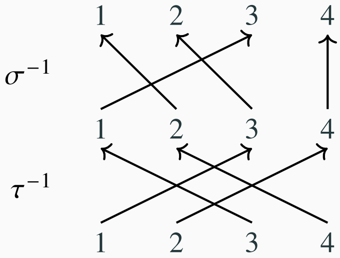
$\sigma^{-1}$



# Permutations iv

*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1, 3, 2)$, $\tau^{-1} = (1, 3)(2, 4)$,

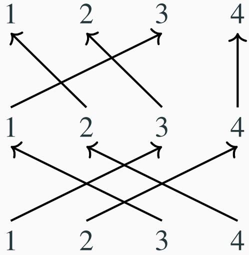


*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

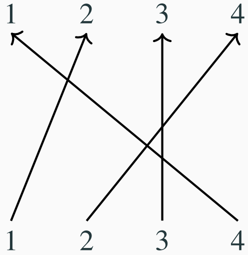
$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.

$\sigma^{-1}$

$\tau^{-1}$



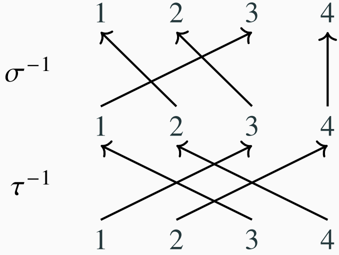

$(\sigma\tau)^{-1}$

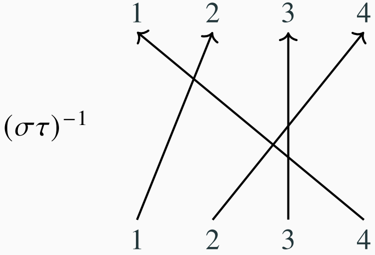


# Permutations iv

*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.

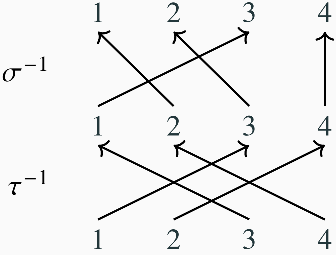


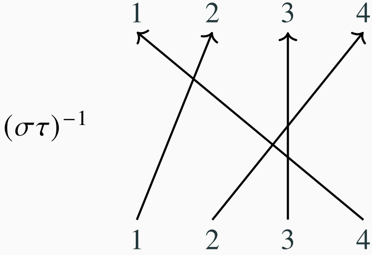




$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$

*Inverse of product:* Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.




$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$
$$\tau^{-1}\sigma^{-1} = (1,3)(2,4)(1,3,2) = (1,2,4) = (\sigma\tau)^{-1}.$$

## Permutations v

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$?

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$,

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so $\sigma^6 = () = 1$; order of $\sigma$ is 6.

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so $\sigma^6 = () = 1$; order of $\sigma$ is 6.

*Fact:* order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so $\sigma^6 = () = 1$; order of $\sigma$ is 6.

*Fact:* order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

**Definition (subgroup)**

Subset $H$ of group $G$ is **subgroup** if it is group under same operation; write $H \leq G$. (Need to check: nonempty, closure, inverses.)

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? Answer: $n!$

**Example (Order of permutation)**

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so $\sigma^6 = () = 1$; order of $\sigma$ is 6.

*Fact:* order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

**Definition (subgroup)**

Subset $H$ of group $G$ is **subgroup** if it is group under same operation; write $H \leq G$. (Need to check: nonempty, closure, inverses.)

**Definition (permutation group)**

A **permutation group** of *degree* $n$ is a subgroup of $\mathrm{Sym}(n)$.

**Definition (group action)**

If $G$ is group and $\Omega \neq \emptyset$ is set, a $G$**-action** is a map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$.

*Idea:* $\alpha \in \Omega$ is *state*, apply *move* $g \in G$ to get state $\alpha^g \in \Omega$, in way that respects group operation.

**Definition (group action)**

If $G$ is group and $\Omega \neq \emptyset$ is set, a $G$**-action** is a map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$.

*Idea:* $\alpha \in \Omega$ is *state*, apply *move* $g \in G$ to get state $\alpha^g \in \Omega$, in way that respects group operation.

**Example (adding time)**

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

**Definition (group action)**

If $G$ is group and $\Omega \neq \emptyset$ is set, a $G$**-action** is a map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$.

*Idea:* $\alpha \in \Omega$ is *state*, apply *move* $g \in G$ to get state $\alpha^g \in \Omega$, in way that respects group operation.

**Example (adding time)**

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5+9]_{12}{:}00 = 2{:}00$.

**Definition (group action)**

If $G$ is group and $\Omega \neq \emptyset$ is set, a $G$**-action** is a map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$.

*Idea:* $\alpha \in \Omega$ is *state*, apply *move* $g \in G$ to get state $\alpha^g \in \Omega$, in way that respects group operation.

**Example (adding time)**

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5 + 9]_{12}{:}00 = 2{:}00$.

**Example (natural action)**

$G \leq \mathrm{Sym}(n)$ acts on $\Omega = [n]$ by $\alpha^g = \alpha g$ (image) for $\alpha \in [n]$, $g \in G$.

**Definition (group action)**

If $G$ is group and $\Omega \neq \emptyset$ is set, a $G$**-action** is a map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$.

*Idea:* $\alpha \in \Omega$ is *state*, apply *move* $g \in G$ to get state $\alpha^g \in \Omega$, in way that respects group operation.

**Example (adding time)**

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5 + 9]_{12}{:}00 = 2{:}00$.

**Example (natural action)**

$G \leq \mathrm{Sym}(n)$ acts on $\Omega = [n]$ by $\alpha^g = \alpha^g$ (image) for $\alpha \in [n]$, $g \in G$.

**Example (right regular action)**

Group $G$ acts on $\Omega = G$ (itself) via $\alpha^g = \alpha g$ for $\alpha, g \in G$.

# Group actions ii

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

# Group actions ii

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).

$\mathbb{Z}$-stabiliser of 11:00 is

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

# Group actions ii

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

**Example (right regular action)**

$G$ acts on $\Omega = G$ via $\alpha^g = \alpha g$ for $\alpha, g \in G$. Orbit of $\alpha \in G$ is

# Group actions ii

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

**Example (right regular action)**

$G$ acts on $\Omega = G$ via $\alpha^g = \alpha g$ for $\alpha, g \in G$. Orbit of $\alpha \in G$ is $\Omega = G$ ($\alpha^{\alpha^{-1}\beta} = \beta \in G$); stabiliser of $\alpha$ is

## Group actions ii

**Definition (orbit)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$.

*Idea:* states $\alpha^g \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $g \in G$.

**Definition (stabiliser)**

If $G$ acts on $\Omega$, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

*Idea:* moves $g \in G$ that fix given $\alpha \in \Omega$.

**Example (Adding time)**

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

**Example (right regular action)**

$G$ acts on $\Omega = G$ via $\alpha^g = \alpha g$ for $\alpha, g \in G$. Orbit of $\alpha \in G$ is $\Omega = G$ ($\alpha^{\alpha^{-1}\beta} = \beta \in G$); stabiliser of $\alpha$ is $\{1\} = 1$ ($\alpha g = \alpha \implies g = 1$).

# Group actions iii

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is

# Group actions iii

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally. Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1.$ Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally. Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

Note: $|1^G||G_1| = 3 \cdot 1 = 3$

# Group actions iii

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

Note: $|1^G||G_1| = 3 \cdot 1 = 3 = |G|$,

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally. Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

Note: $|1^G||G_1| = 3 \cdot 1 = 3 = |G|$, $|3^G||G_3| = 1 \cdot 3 = 3 = |G|$.

**Definition (orbit, stabiliser)**

If $G$ acts on $\Omega$, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^g : g \in G\}$ and **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

**Example (Natural action)**

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally. Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

Note: $|1^G||G_1| = 3 \cdot 1 = 3 = |G|$, $|3^G||G_3| = 1 \cdot 3 = 3 = |G|$.

**Theorem (orbit-stabiliser)**

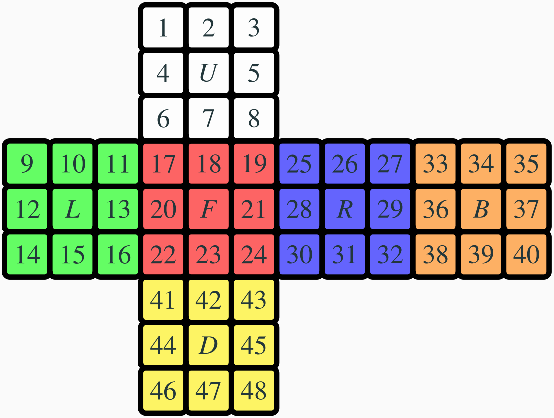
*If $G$ acts on $\Omega$, then for $\alpha \in G$, $|\alpha^G||G_\alpha| = |G|$.*

# The Rubik’s group

# Representing the cube i

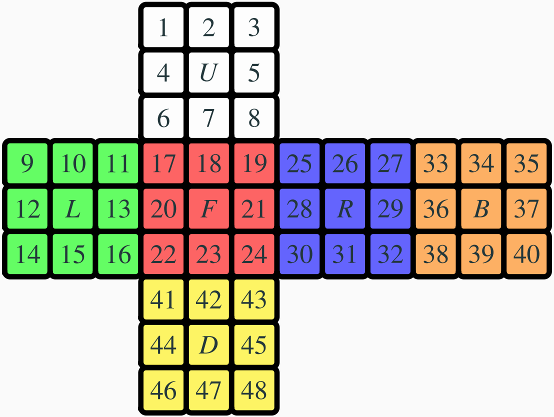
A Rubik's cube has 6 large faces (each with $3 \times 3$ smaller faces).

Label all smaller faces except centre on each side, using [48]:



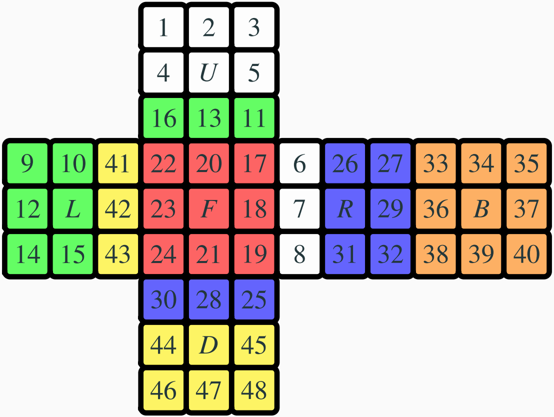

6 *elementary moves* (**generators**): $U, L, F, R, B, D$ (rotate clockwise).

Consider move $F$ which rotates front face clockwise:



# Representing the cube ii

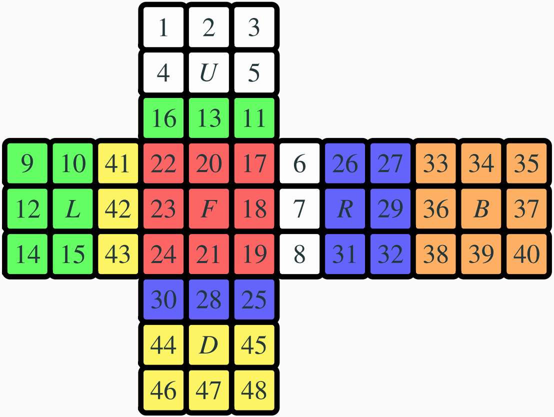
Consider move $F$ which rotates front face clockwise:




Under $F$: $17 \mapsto 19 \mapsto 24 \mapsto 22 \mapsto 17$, $18 \mapsto 21 \mapsto 23 \mapsto 20 \mapsto 18$, $6 \mapsto 25 \mapsto 43 \mapsto 16 \mapsto 6$, $7 \mapsto 28 \mapsto 42 \mapsto 13 \mapsto 7$, $8 \mapsto 30 \mapsto 41 \mapsto 11 \mapsto 8$, else fixed. So

# Representing the cube ii

Consider move $F$ which rotates front face clockwise:




Under $F$: $17 \mapsto 19 \mapsto 24 \mapsto 22 \mapsto 17$, $18 \mapsto 21 \mapsto 23 \mapsto 20 \mapsto 18$, $6 \mapsto 25 \mapsto 43 \mapsto 16 \mapsto 6$, $7 \mapsto 28 \mapsto 42 \mapsto 13 \mapsto 7$, $8 \mapsto 30 \mapsto 41 \mapsto 11 \mapsto 8$, else fixed. So

$$F = (17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11) \in \mathrm{Sym}(48).$$

Generators as permutations of labels [48]:

- $U = (1, 3, 8, 6)(2, 5, 7, 4)(9, 33, 25, 17)(10, 34, 26, 18)(11, 35, 27, 19)$
- $L = (9, 11, 16, 14)(10, 13, 15, 12)(1, 17, 41, 40)(4, 20, 44, 37)(6, 22, 46, 35)$
- $F = (17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11)$
- $R = (25, 27, 32, 30)(26, 29, 31, 28)(3, 38, 43, 19)(5, 36, 45, 21)(8, 33, 48, 24)$
- $B = (33, 35, 40, 38)(34, 37, 39, 36)(3, 9, 46, 32)(2, 12, 47, 29)(1, 14, 48, 27)$
- $D = (41, 43, 48, 46)(42, 45, 47, 44)(14, 22, 30, 38)(15, 23, 31, 39)(16, 24, 32, 40)$

*Empty move* is $1 = ()$. In cubing community, *inverse elementary moves* usually denoted $U', L', F', R', B', D'$ (instead of $U^{-1}$, etc.); powers usually denoted $U2, R2$ etc. (instead of $U^2, R^2$).

*Valid move* is sequence of elementary moves (product of generators). E.g. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, $RUR^{-1}URU^2R^{-1}U^2$.

# Moves vs states for Rubik's cube ii

Moves don't generally commute: $RU \neq UR$ since

$$19^{RU} = (19^R)^U = 3^U = 8 \quad \text{but} \quad 19^{UR} = (19^U)^R = 11^R = 11.$$

Let $\mathcal{S}$ be valid **states**; can represent state $x \in \mathcal{S}$ as element of $\mathrm{Sym}(48)$ giving permutation of labels from solved state $1 = ()$.

Let $\mathcal{G}$ be valid **moves**; can represent move $\sigma \in \mathcal{G}$ as element of $\mathrm{Sym}(48)$ giving corresponding permutation of labels.

- State $x \in \mathcal{S}$ corresponds to move $x \in \mathcal{G}$ required to get solved state $1 = ()$ into state $x$.
- Move $\sigma \in \mathcal{G}$ corresponds to state $\sigma \in \mathcal{S}$ reached by applying move $\sigma$ to solved state $1 = ()$.

So moves $\leftrightarrow$ states for Rubik's cube; as sets, $\mathcal{S} = \mathcal{G}$.

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move $1 = () \in \mathcal{G}$, inverse moves exist; associative.

**Definition (Rubik's group)**
$\mathcal{G} \leq \mathrm{Sym}(48)$ is permutation group of degree 48, called the **Rubik's group**; it acts naturally on $[48]$. Note: $G = \langle U, L, F, R, B, D \rangle$.

For move $\sigma \in \mathcal{G}$ and state $x \in \mathcal{S}$, applying $\sigma$ to $x$ gives state $x^{\sigma} = x\sigma \in \mathcal{S}$. This is regular action of $\mathcal{G}$. (Consider states $x \in \mathcal{G}$.)

Clearly $\mathcal{G}$ finite (states $\leftrightarrow$ moves; also $|\mathcal{G}| \leq 48!$). But what is $|\mathcal{G}|$?

TODO: orbits, stabilisers (corner pieces/edge pieces), GAP code?

# Orders of moves i

TODO

Order of generators: all 4

Order of commutator $RUR^{-1}U^{-1}$ is 6 (write out, get Wes video)

Order of $URU^{-1}L^{-1}UR^{-1}U^{-1}L$ is 3 (write out, get Wes video) – last layer corner permutation (3 states)

Order of $RUR^{-1}URU^2R^{-1}U^2$ is 3 (write out, get Wes video) – last layer edge permutation (3 states)

Order of $RU$ is 105, order of Clayton's move $UL'$ is 63

What is element of order 5? $(RU)^{21}$ since $((RU)^{21})^5 = (RU)^{105} = 1$.

**Theorem (Jake Vandenberg's conjecture)**
*There is no Rubik's cube move that cycles through all states.*

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^\sigma = x\sigma \in \mathcal{G}$.

Equivalent question: for starting state, WLOG $1 = ()$, is there $\sigma \in \mathcal{G}$ with $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$? In group theory language:

**Theorem (Jake Vandenberg's conjecture)**
*The Rubik's group $\mathcal{G}$ is not cyclic. (I.e. no $\sigma \in \mathcal{G}$ with $\mathcal{G} = \langle \sigma \rangle$.)*

**Proof.**
If $\mathcal{G}$ is cyclic, then $\mathcal{G}$ is abelian. But $\mathcal{G}$ is not abelian: $RU \neq UR$. $\square$

**Theorem (Jake Vandenberg's theorem)**
*There is no Rubik's cube move that when repeated, if starting from the solved state, never returns to the solved state.*

A $k$-fold repetition of move $\sigma \in G$, applied to solved state $1 = ()$, gives $1^{\sigma^k} = 1\sigma^k = \sigma^k$. Returning to solved state: $\sigma^k = 1$ (for $k > 0$).

Equivalent question: does any $\sigma \in G$ have infinite order?

**Proposition**
*If $G$ is finite group and $g \in G$, then $g^{|G|} = 1$.*

**Corollary (Jake Vandenberg's theorem)**
*There is no $\sigma \in \mathcal{G}$ with infinite order (since $\mathcal{G}$ is finite).*

# Analysing the Rubik’s group

# Bases and stabiliser chains i

TODO

# How many valid states are there? i

TODO

# Can this restickering be solved? i

TODO

# Generating random Rubik's cube states i

TODO

# Solving a Rubik's cube... i

TODO

# Concluding remarks

# References i

- TODO