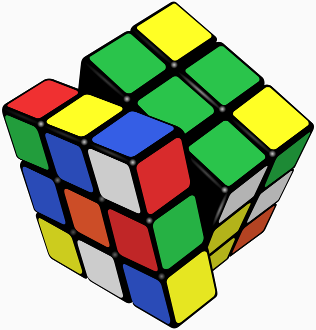
Rubik's cubes and permutation group theory

Lawrence Chen

October 7, 2022

Honours presentation



Contents

Some basic group theory
- What is a group?
- Order and generators
- Permutations
- Group actions

The Rubik's group

Analysing the Rubik's group

Concluding remarks
- References

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 $g, h, k \in G$.

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

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

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.

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.

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

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.

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

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.

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.

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 ∞).

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 ∞).

Example (Cyclic group)

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

Definition (order)

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

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 ∞).

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 ∞).

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 ∞).

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.

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 ∞).

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 ∞).

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 ∞).

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 ∞).

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 ∞).

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

Definition (order)

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

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^σ 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^σ not $\sigma(i)$ for *image*.

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

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

σ

It means

Permutations i

Definition (permutation)

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

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

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

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

It means

$$1^\sigma = 4,$$

Permutations i

Definition (permutation)

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

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

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

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

It means

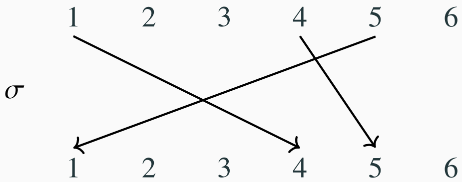
$$1^\sigma = 4,\ 4^\sigma = 5,$$

Definition (permutation)

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

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

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



It means

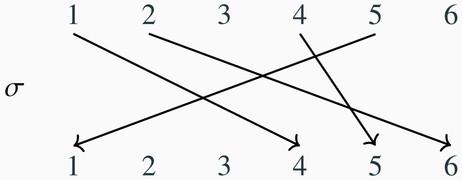
$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,$$

Definition (permutation)

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

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

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



It means

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

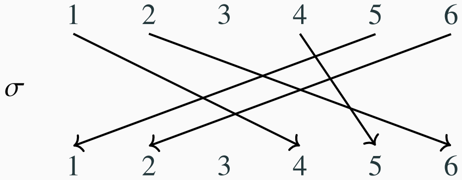
Permutations i

Definition (permutation)

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

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

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



It means

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

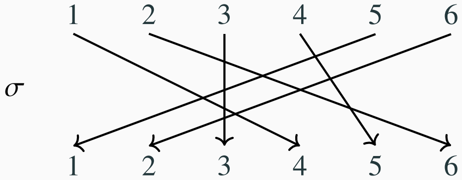
Permutations i

Definition (permutation)

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

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

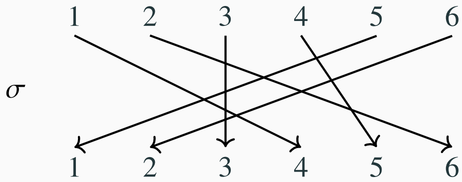
Cycle notation: $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:



It means

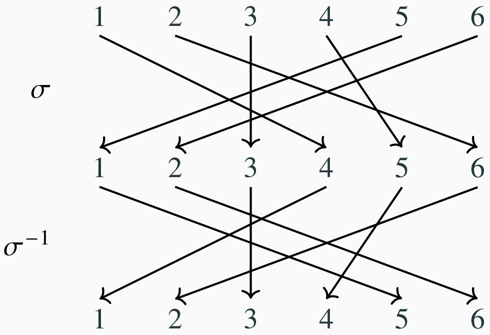
$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,\ 3^\sigma = 3.$$

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



Permutations ii

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

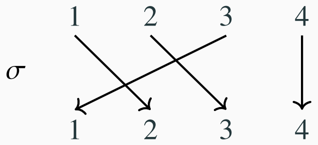


Inverse is $\sigma^{-1} = (1, 5, 4)(2, 6) \in \mathrm{Sym}(6)$.

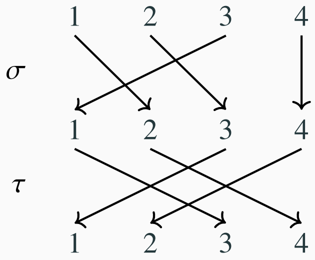
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$.

Permutations iii

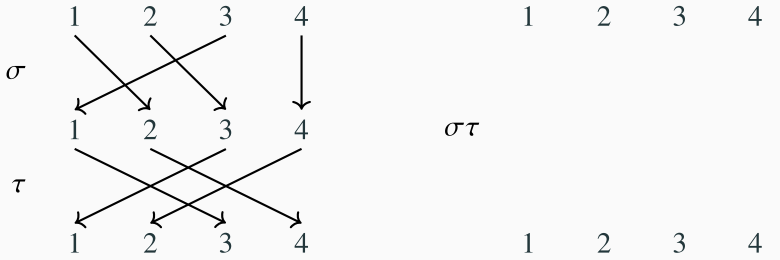
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3)$,



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



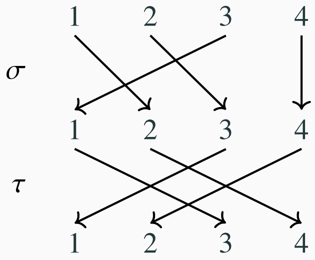
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,

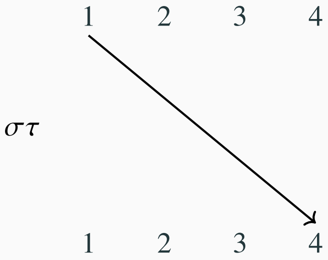


$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1,$$

Permutations iii

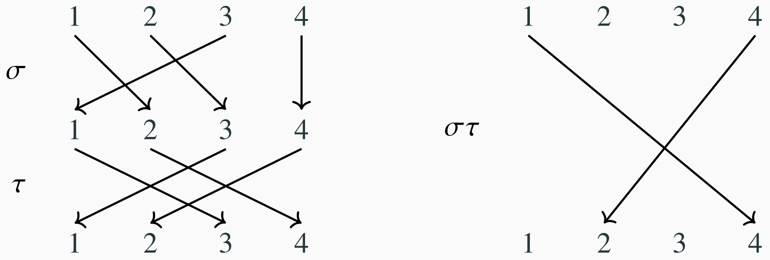
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,





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

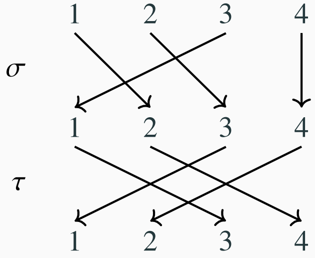
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^\sigma)^\tau$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,

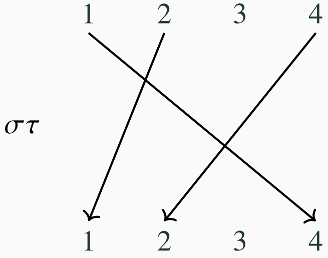


$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2$$

Permutations iii

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

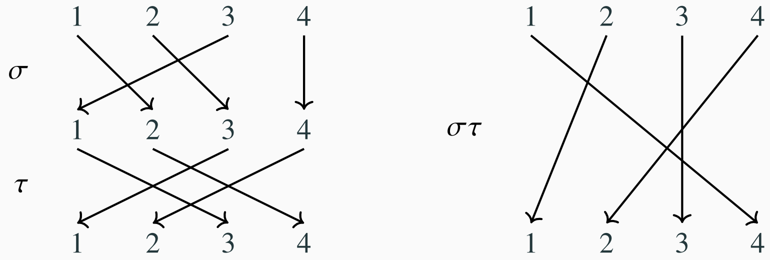




$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2)$$

Permutations iii

Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, 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

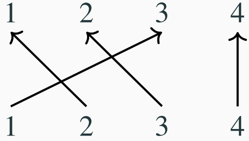
Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

Permutations iv

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

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

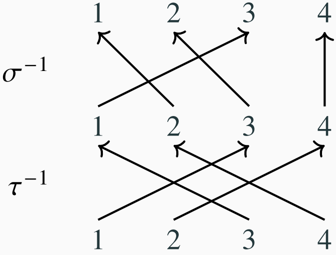
σ^{-1}



Permutations iv

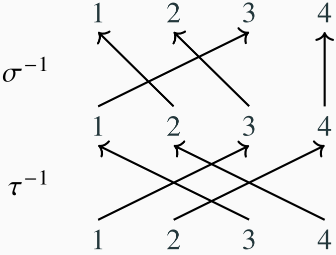
Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

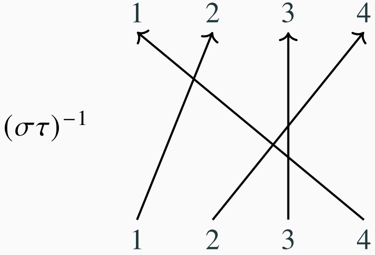
$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$,



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

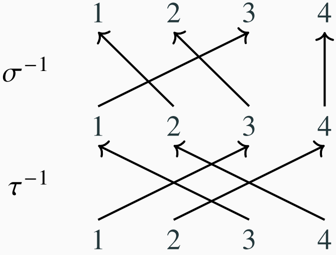
$\sigma^{-1} = (1, 3, 2)$, $\tau^{-1} = (1, 3)(2, 4)$, $(\sigma\tau)^{-1} = (1, 2, 4)$.

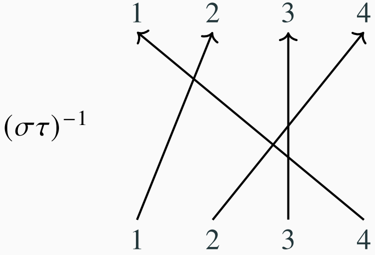




Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

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



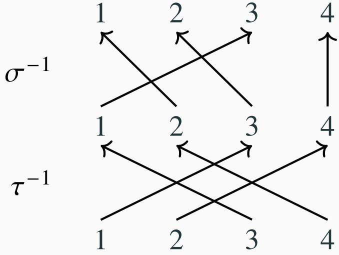


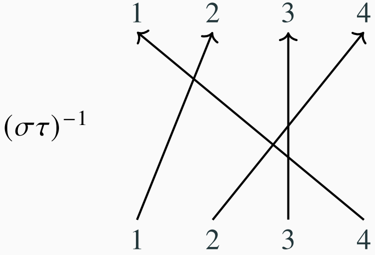
$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$

Permutations iv

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

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





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

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 $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$,

Permutations v

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

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

Permutations v

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

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

Group actions i

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 $k \in \mathbb{Z}$.

Group actions i

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 $\alpha \in [n]$, $g \in G$.

Group actions i

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 Ω, 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 (orbit)

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

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

Group actions ii

Definition (orbit)

If G acts on Ω, 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 Ω, 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

Group actions ii

Definition (orbit)

If G acts on Ω, 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 Ω, 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 Ω, 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 Ω, 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).

Definition (orbit)

If G acts on Ω, 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 Ω, 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 Ω, 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 Ω, 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 α is

Definition (orbit)

If G acts on Ω, 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 Ω, 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 α is $\{1\} = 1$ ($\alpha g = \alpha \implies g = 1$).

Definition (orbit, stabiliser)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

Example (Natural action)

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

Definition (orbit, stabiliser)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Group actions iii

Definition (orbit, stabiliser)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Definition (orbit, stabiliser)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

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 Ω, then for $\alpha \in G$, $|\alpha^G||G_\alpha| = |G|$.

The Rubik's group

Analysing the Rubik’s group

Concluding remarks

References i

- TODO