

抽象代數

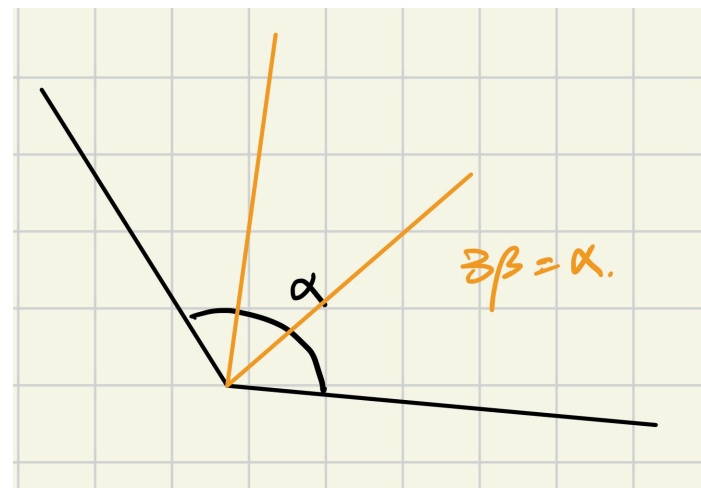
群論

陽明交通大學應數系營隊

群(Group)是一個集合，並且配上一個良好的二元運算，而群論(Group Theory)是一門研究群這種結構的數學分支。群論在許多領域上有著廣泛的應用，以下介紹一些應用。

群論的應用

倍立方、化圓為方、三等分角等，尺規作圖問題。



群論的應用

我們都知道一元二次方程 $ax^2 + bx + c = 0$ 的解為

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

但是對於一元五次方程 $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ ，可以用群論證明，我們無法用根式解析解來表示。

群論的應用

除了數學上的應用外，在其他領域也有著廣泛的應用，例如

- 密碼學
- 「李群」在近代物理中有重要作用
- 標準粒子模型中的對稱性

群論的應用

除了數學上的應用外，在其他領域也有著廣泛的應用，例如

- 密碼學
- 「李群」在近代物理中有重要作用
- 標準粒子模型中的對稱性

粒子物理標準模型



群

Group

Definition 1.1: $\langle G, * \rangle$ 是一個集合 G 與一個二元運算 $* : G \times G \mapsto G$ ，滿足以下條件：

\mathcal{G}_1 : 對於所有的 $a, b, c \in G$ ，

$$(a * b) * c = a * (b * c) \quad \text{結合律}$$

\mathcal{G}_2 : 存在一個元素 $e \in G$ ，使得對於所有的 $a \in G$ ，

$$a * e = e * a = a \quad \text{單位元素}$$

\mathcal{G}_3 : 對於每一個 $a \in G$ ，存在一個元素 $a^{-1} \in G$ ，使得

$$a * a^{-1} = a^{-1} * a = e \quad \text{反元素}$$

Example:

- 整數集合 \mathbb{Z} 與加法運算 $+$ 構成一個群。 $\langle \mathbb{Z}, + \rangle$
單位元素為 0 ，反元素為 $-a$ 。
- 整數集合 \mathbb{Z} 與乘法運算 $*$ 不是一個群。
乘法在整數裡沒有反元素。
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ 與加法運算 $+_4$ 構成一個群。
其中 $+_4$ 定義為 $a +_4 b = (a + b) \bmod 4$ 。

Definition 1.2: 讓 G 是一個群，定義 $|G|$ 是 G 的元素個數，稱為 G 的 **order**。

Definition 1.3: 一個群 G 如果滿足交換率 i.e. 對於所有的 $a, b \in G$ ，

$$a * b = b * a$$

，則稱 G 是一個**交換群**(Abelian groups)。

Definition 1.2: 讓 G 是一個群，定義 $|G|$ 是 G 的元素個數，稱為 G 的 **order**。

Definition 1.3: 一個群 G 如果滿足交換率 i.e. 對於所有的 $a, b \in G$ ，

$$a * b = b * a$$

，則稱 G 是一個**交換群**(Abelian groups)。

Example:

- 整數集合 \mathbb{Z} 與加法運算 $+$ 是一個交換群。
- \mathbb{Z}_4 的 order 為 4。
- 可逆矩陣的集合與矩陣乘法是一個群，但不是交換群。

Theorem 1.1: 如果 G 是一個群，那消去率成立，即對於所有的 $a, b, c \in G$ ，

$$a * b = a * c \Rightarrow b = c$$

$$b * a = b * c \Rightarrow b = c$$

Theorem 1.1: 如果 G 是一個群，那**消去率**成立，即對於所有的 $a, b, c \in G$ ，

$$a * b = a * c \Rightarrow b = c$$

$$b * a = b * c \Rightarrow b = c$$

Proof: 讓 G 是一個群， $a, b, c \in G$ 。假設 $a * b = a * c$ 。

$$a * b = a * c$$

$$\Rightarrow b = c$$



Theorem 1.1: 如果 G 是一個群，那消去率成立，即對於所有的 $a, b, c \in G$ ，

$$a * b = a * c \Rightarrow b = c$$

$$b * a = b * c \Rightarrow b = c$$

Proof: 讓 G 是一個群， $a, b, c \in G$ 。假設 $a * b = a * c$ 。因為 $a \in G$ ，所以 a 的反元素 a^{-1} 存在，且 $a * a^{-1} = e$ 。

$$a * b = a * c$$

$$\Rightarrow a^{-1} * a * b = a^{-1} * a * c$$

$$\Rightarrow b = c$$



Theorem 1.1: 如果 G 是一個群，那消去率成立，即對於所有的 $a, b, c \in G$ ，

$$a * b = a * c \Rightarrow b = c$$

$$b * a = b * c \Rightarrow b = c$$

Proof: 讓 G 是一個群， $a, b, c \in G$ 。假設 $a * b = a * c$ 。因為 $a \in G$ ，所以 a 的反元素 a^{-1} 存在，且 $a * a^{-1} = e$ 。

$$a * b = a * c$$

$$\Rightarrow a^{-1} * a * b = a^{-1} * a * c$$

$$\Rightarrow b = c$$



Theorem 1.1: 如果 G 是一個群，那消去率成立，即對於所有的 $a, b, c \in G$ ，

$$a * b = a * c \Rightarrow b = c$$

$$b * a = b * c \Rightarrow b = c$$

Proof: 讓 G 是一個群， $a, b, c \in G$ 。假設 $a * b = a * c$ 。因為 $a \in G$ ，所以 a 的反元素 a^{-1} 存在，且 $a * a^{-1} = e$ 。

$$\begin{aligned} a * b &= a * c \\ \Rightarrow a^{-1} * a * b &= a^{-1} * a * c \\ \Rightarrow e * b &= e * a \\ \Rightarrow b &= a \end{aligned}$$

■

Theorem 1.2: 群 G 的單位元素 e 唯一。

Theorem 1.2: 群 G 的單位元素 e 唯一。

Proof: 假設存在第二個單位元素 e_2 ，滿足對於所有 $a \in G$

$$e_2 * a = a * e_2 = a$$

因為 $e \in G$ ，所以

$$e_2 * a = a$$



Theorem 1.2: 群 G 的單位元素 e 唯一。

Proof: 假設存在第二個單位元素 e_2 ，滿足對於所有 $a \in G$

$$e_2 * a = a * e_2 = a$$

因為 $e \in G$ ，所以

$$e_2 * e = e$$

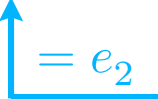


Theorem 1.2: 群 G 的單位元素 e 唯一。

Proof: 假設存在第二個單位元素 e_2 ，滿足對於所有 $a \in G$

$$e_2 * a = a * e_2 = a$$

因為 $e \in G$ ，所以

$$e_2 * e = e$$


$= e_2$



Theorem 1.2: 群 G 的單位元素 e 唯一。

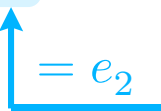
Proof: 假設存在第二個單位元素 e_2 ，滿足對於所有 $a \in G$

$$e_2 * a = a * e_2 = a$$

因為 $e \in G$ ，所以

$$e_2 * e = e$$

我們得到 $e_2 = e$


$$= e_2$$



Theorem 1.3: 讓 G 是一個群， $ab \in G$ ，那麼

$$(ab)^{-1} = b^{-1}a^{-1}$$

Theorem 1.3: 讓 G 是一個群， $ab \in G$ ，那麼

$$(ab)^{-1} = b^{-1}a^{-1}$$

Proof: 我們直接相乘

$$\begin{aligned}(ab)b^{-1}a^{-1} &= a(bb^{-1})a^{-1} \\ &= aea^{-1} \\ &= aa^{-1} \\ &= e\end{aligned}$$

根據反元素的定義， $(ab)^{-1} = b^{-1}a^{-1}$



置換群

Permutation Group

$$A = \{1, 2, 3, 4, 5\}$$

$$A = \{1, 2, 3, 4, 5\}$$

$\downarrow \sigma$ 排列

$$A = \{3, 1, 5, 2, 4\}$$

$$A = \{1, 2, 3, 4, 5\}$$

$\downarrow \sigma$ 排列

$$A = \{3, 1, 5, 2, 4\}$$

$$1 \rightarrow 3$$

$$2 \rightarrow 4$$

$$3 \rightarrow 5$$

$$4 \rightarrow 2$$

$$5 \rightarrow 1$$

$$1 \rightarrow 2$$

$$2 \rightarrow 3$$

$$3 \rightarrow 2$$

$$4 \rightarrow 5$$

$$5 \rightarrow 1$$

Figure 5: σ

Definition 2.1: 一個 A 的置換是一個一一對應的函數 $\varphi : A \rightarrow A$ 。(one-one and onto)

$$\begin{aligned} 1 &\rightarrow 3 \\ 2 &\rightarrow 4 \\ 3 &\rightarrow 5 \\ 4 &\rightarrow 2 \\ 5 &\rightarrow 1 \end{aligned}$$

Figure 7: 一個置換 σ

$$\begin{aligned} 1 &\rightarrow 2 \\ 2 &\rightarrow 3 \\ 3 &\rightarrow 2 \\ 4 &\rightarrow 5 \\ 5 &\rightarrow 1 \end{aligned}$$

Figure 8: 不是置換

Definition: 讓 σ 和 τ 是兩個置換，定義 σ 和 τ 的**合成**是一個新的置換 $\sigma \circ \tau$ ，使得對於所有的 $a \in A$ ，

$$(\sigma \circ \tau)(a) = \sigma(\tau(a))$$

Definition: 讓 σ 和 τ 是兩個置換，定義 σ 和 τ 的**合成**是一個新的置換 $\sigma \circ \tau$ ，使得對於所有的 $a \in A$ ，

$$(\sigma \circ \tau)(a) = \sigma(\tau(a))$$

$$(\sigma \circ \tau)(x) = \sigma(\tau(x))$$

$$A \xrightarrow{\tau} A \xrightarrow{\sigma} A$$

因為 σ 和 τ 都是一一對應的函數，所以 $\sigma \circ \tau$ 也是一一對應的函數。
所以 $\sigma \circ \tau$ 是一個置換。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

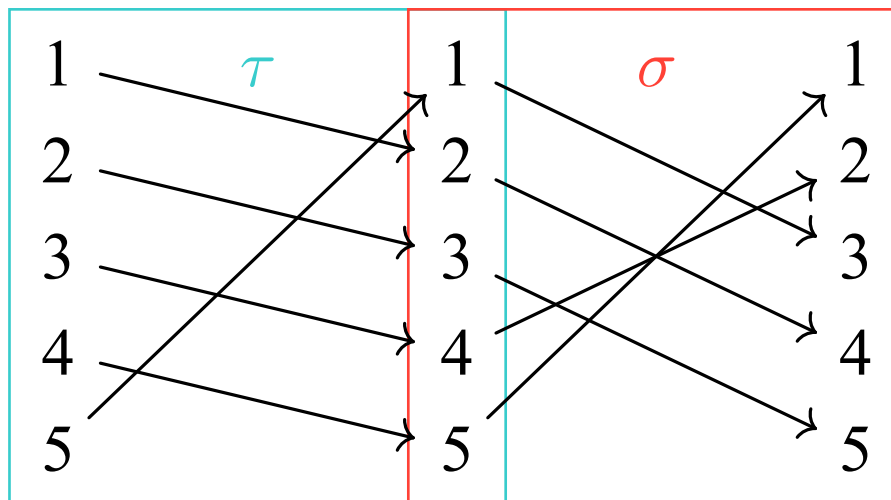
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$



Definition 2.2: 一個集合 A 的所有置換構成一個群，稱為 A 的置換群，記為 S_A 。

Definition 2.2: 一個集合 A 的所有置換構成一個群，稱為 A 的置換群，記為 S_A 。

Remark: n 個元素的集合的置換群計為 S_n 的 order 為 $n!$ 。

Definition 2.2: 一個集合 A 的所有置換構成一個群，稱為 A 的置換群，記為 S_A 。

Remark: n 個元素的集合的置換群計為 S_n 的 order 為 $n!$ 。

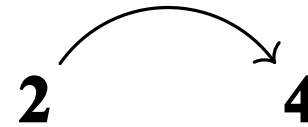
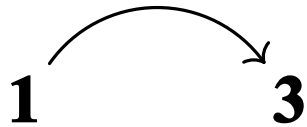
Example:

上述的例子中， τ 和 σ 是 S_5 的元素。

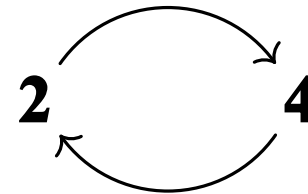
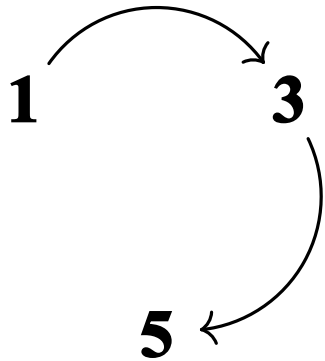
S_5 的 order 為 $5! = 120$ 。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

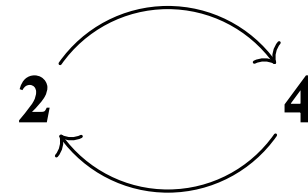
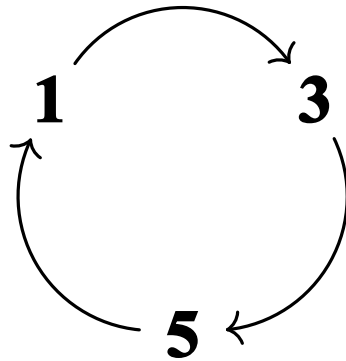
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$



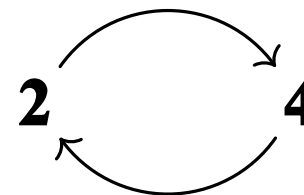
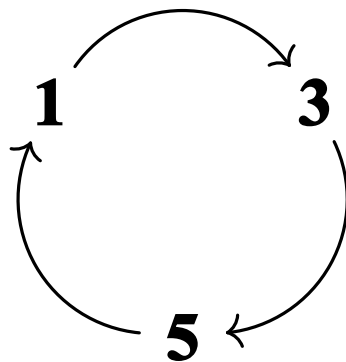
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$



$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$



$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$



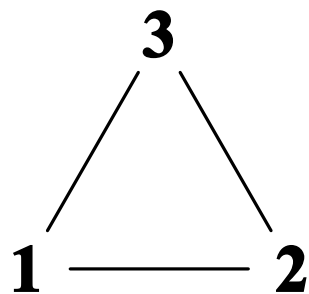
$$\sigma = (1, 3, 5)(2, 4)$$

空間對稱群

Symmetry Group

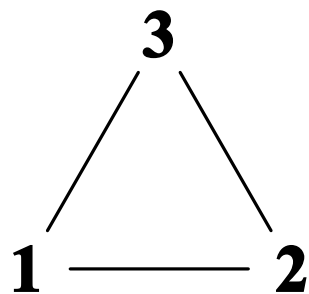
我們接下來考慮一種特殊的置換群。

我們接下來考慮一種特殊的置換群。

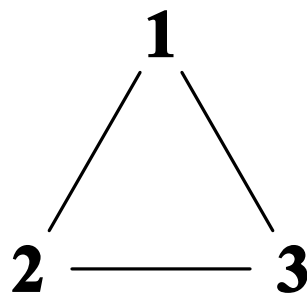


正三角形

我們接下來考慮一種特殊的置換群。



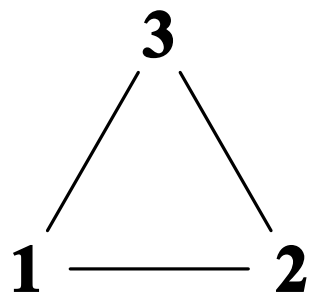
正三角形



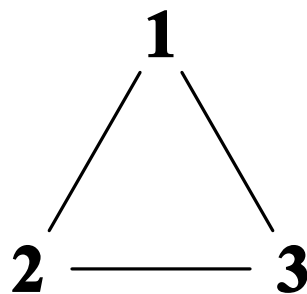
順時針旋轉 120 度

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

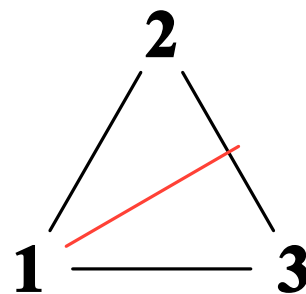
我們接下來考慮一種特殊的置換群。



正三角形



順時針旋轉 120 度

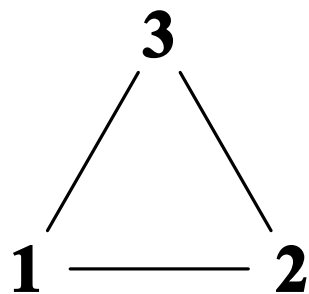


沿某一軸鏡射

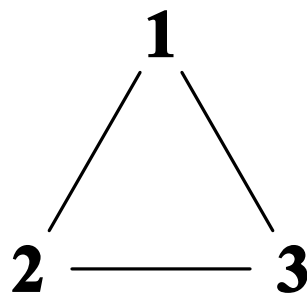
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2, 3)$$

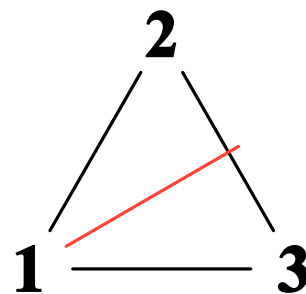
我們接下來考慮一種特殊的置換群。



正三角形



順時針旋轉 120 度



沿某一軸鏡射

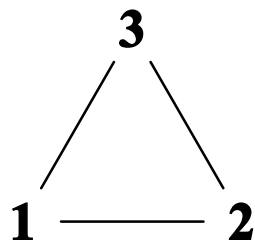
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2, 3)$$

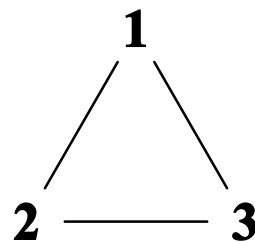
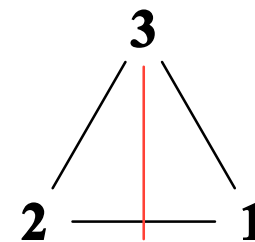
我們稱這些置換為對稱置換。

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2, 3)$$



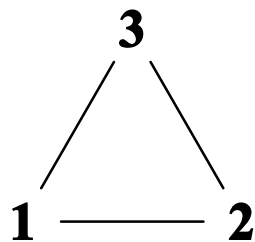
正三角形

 ρ_1  $\tau_1 \circ \rho_1$

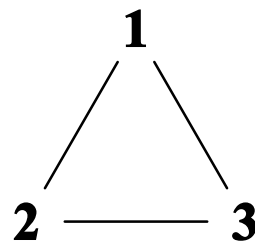
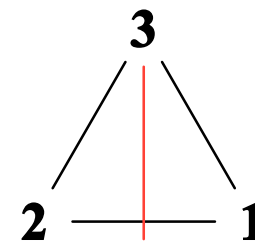
$$\tau_1 \circ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2, 3)$$



正三角形

 ρ_1  $\tau_1 \circ \rho_1$

$$\tau_1 \circ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2)$$

對稱置換的合成還是一個對稱置換。

我們把三角形的所有對稱的置換枚舉出來：

$$e = \rho_0 = (1)(2)(3) \quad \text{不動}$$

$$\rho_1 = (1, 2, 3) \quad \text{旋轉 120 度}$$

$$\rho_2 = (1, 3, 2) \quad \text{旋轉 240 度}$$

$$\tau_1 = (1)(2, 3) \quad \text{鏡射}$$

$$\tau_2 = (1, 3, 2) \quad \text{鏡射}$$

$$\tau_3 = (1, 2)(3) \quad \text{鏡射}$$

我們把三角形的所有對稱的置換枚舉出來：

$$e = \rho_0 = (1)(2)(3) \quad \text{不動}$$

$$\rho_1 = (1, 2, 3) \quad \text{旋轉 120 度}$$

$$\rho_2 = (1, 3, 2) \quad \text{旋轉 240 度}$$

$$\tau_1 = (1)(2, 3) \quad \text{鏡射}$$

$$\tau_2 = (1, 3, 2) \quad \text{鏡射}$$

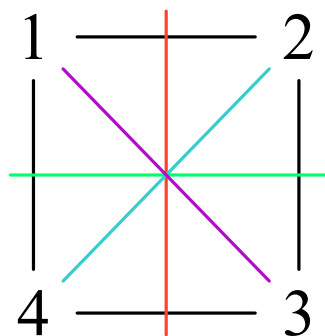
$$\tau_3 = (1, 2)(3) \quad \text{鏡射}$$

把上述的對稱置換構成的群稱為 D_3 ，稱為正三角形的空間對稱群。

$$D_3 = \{e, \rho_1, \rho_2, \tau_1, \tau_2, \tau_3\}$$

\circ	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
e	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	e	τ_3	τ_1	τ_2
ρ_2	ρ_2	e	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_3	τ_2	e	ρ_2	ρ_1
τ_2	τ_2	τ_1	τ_3	ρ_2	e	ρ_1
τ_3	τ_3	τ_2	τ_1	ρ_1	ρ_2	e

$$D_4 = \{e, \rho_1, \rho_2, \rho_3, \tau_1, \tau_2, \tau_3, \tau_4\}$$

 τ_1 τ_3 τ_2 τ_4 

$$e = (1)(2)(3)(4)$$

$$\rho_1 = (1, 2, 3, 4)$$

$$\rho_2 = (1, 3)(2, 4)$$

$$\rho_3 = (1, 4, 3, 2)$$

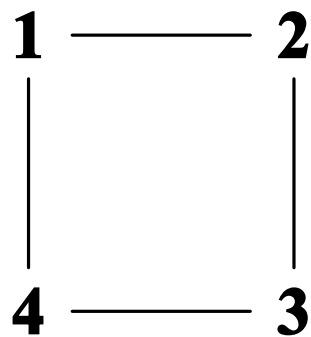
$$\tau_1 = (1)(2, 4)(3)$$

$$\tau_2 = (1, 3)(2)(4)$$

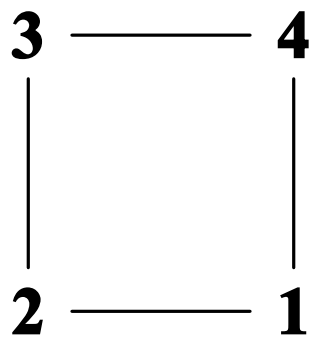
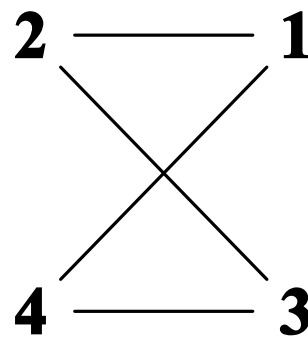
$$\tau_3 = (1, 2)(4, 3)$$

$$\tau_4 = (1, 4)(2, 3)$$

值得注意的是 $\sigma = (1, 2)(4, 3)$ 他是一個置換，但不是一個對稱置換，因為他不能把正方形打回自身。



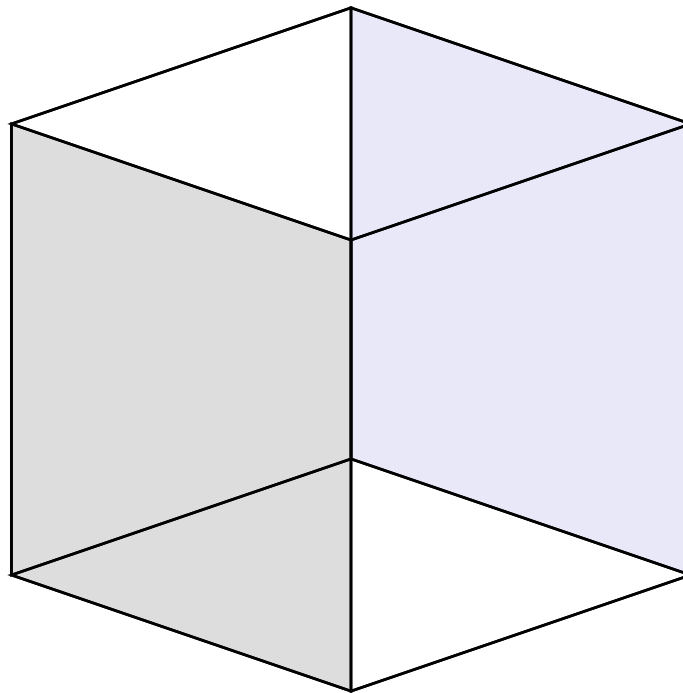
正方形

 ρ_2  σ 不是一個對稱置換

如何計算空間對稱群

正 n 邊形的對稱群的 order 是多少？

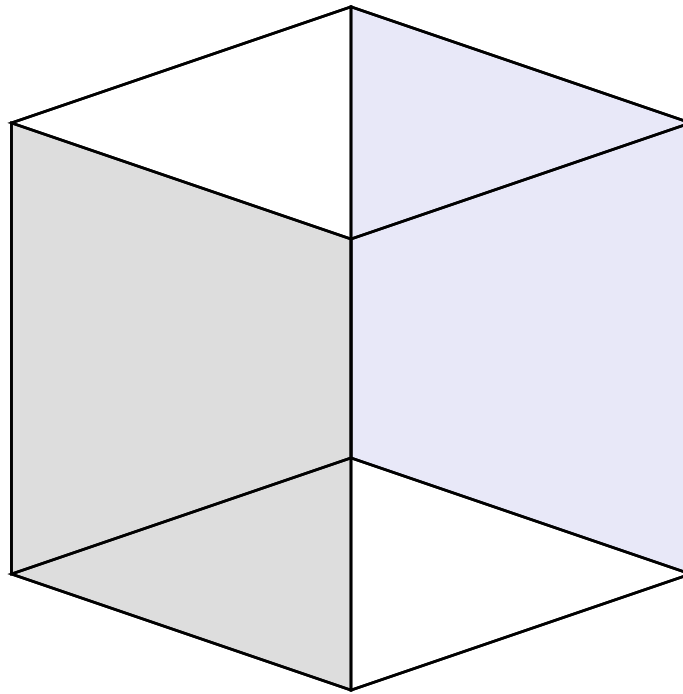
立方體的有多少不同的旋轉。



如何計算空間對稱群

正 n 邊形的對稱群的 order 是 $2n$ 。

立方體的有24個不同的旋轉。



作用群

Group Action

Definition 4.1: 一個群 G 對一個集合 A 的作用是一個映射 $*: G \times A \rightarrow A$ ，滿足以下條件：

1. 對於所有 $a \in A$ $ea = a$
2. 對於所有 $a \in A$ 和 $g, h \in G$ ， $(gh)a = g(ha)$

在這個情況下，我們稱 A 是一個 **G -set**。

像是在上一章節中，我們考慮了對稱群 D_3 對正三角形的作用。

Theorem 4.1: 讓 X 是一個 G -set。如果 $gx_1 = gx_2$ ，那 $x_1 = x_2$

Proof: 假設 $gx_1 = gx_2$ ，那麼 $g^{-1}gx_1 = g^{-1}gx_2$ ，所以 $ex_1 = ex_2$ ，所以 $x_1 = x_2$ 。 ■

Remark: 如果 $x \neq y$ ，那 $gx \neq gy$

Fixed point, Stabilizers subgroup, Orbits

Definition 4.2: 讓 X 是一個 G -set，讓 $x \in X$ ， $g \in G$ 。我們定義：

$$\text{Stab}_G(x) = \{g \in G \mid gx = x\}$$

$$X^g = \{x \in X \mid gx = x\}$$

$\text{Stab}_G(x)$ 稱為 x 的穩定子群， X^g 稱為 g 的不動點。