抽象代數

群論

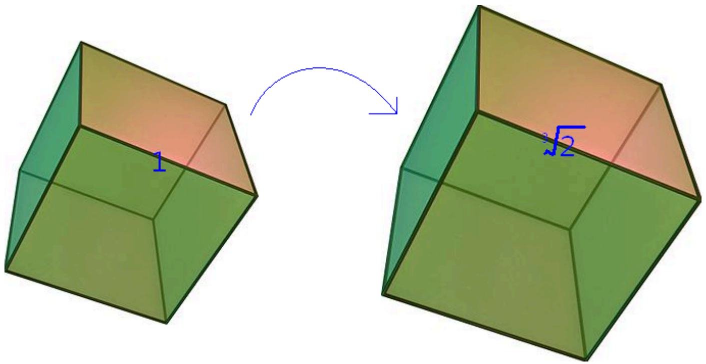
陽明交通大學應數系營隊

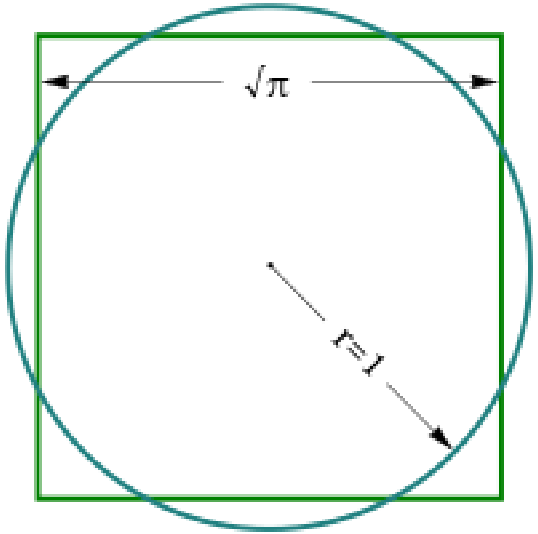
群論

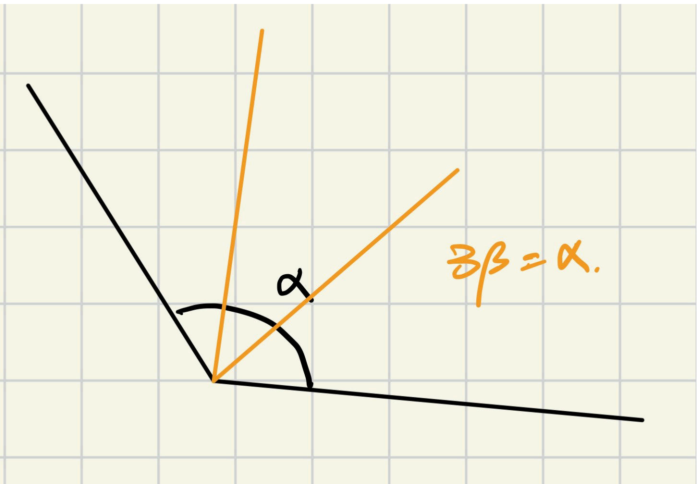
群(Group)是一個集合，並且配上一個良好的二元運算，而群論(Group Throry)是一們研究群這種結構的數學分支。群論在許多領域上有著廣泛的應用，以下介紹一些應用。

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

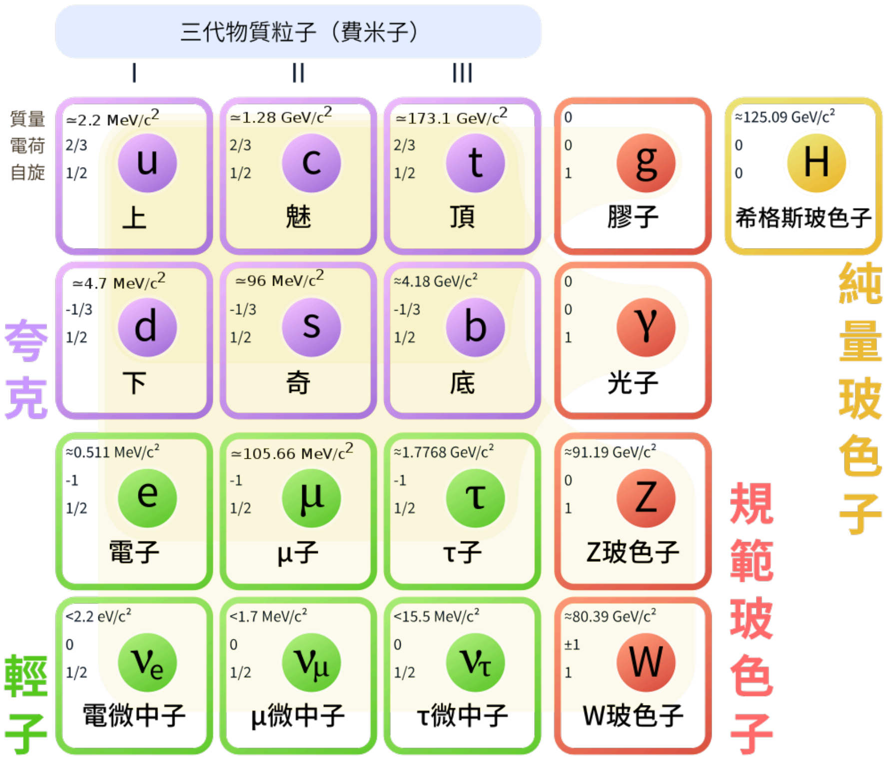
- 密碼學
- 「李群」在近代物理中有重要作用
- 標準粒子模型中的對稱性

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$a, b, c \in G$，

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

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

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

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

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

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$a * b = a * c$。

$$a * b = a * c$$

$$\Rightarrow b = a$$

■

群的基礎性質

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$a * a^{-1} = e$。

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

■

群的基礎性質

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$a * a^{-1} = e$。

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

■

群的基礎性質

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$a * a^{-1} = e$。

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

■

群的基礎性質

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

$$e_2 * a = a$$

■

群的基礎性質

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

$$e_2 * e = e$$

$\blacksquare$

群的基礎性質

Properties of Groups

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

$$\underbrace{e_2 * e}_{= e_2} = e$$

$\blacksquare$

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

$$\underbrace{e_2 * e}_{= e_2} = e$$

我們得到$e_2 = e$ ∎

群的基礎性質

Theorem 1.3：讓G是一個群，$ab \in G$，那麼

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

群的基礎性質

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

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

根據反元素的定義，$(ab)^{-1} = b^{-1}a^{-1}$ ∎

置换群

Permutation Group

置換

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

置換

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

$$\downarrow \sigma \text{ 排列}$$

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

置換

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

$$\downarrow \sigma \text{ 排列}$$

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

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

Figure 5: σ

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

置換

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

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

Figure 7: 一個置換 σ

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

Figure 8: 不是置換

置換的合成

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$a \in A$，

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

置換的合成

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。

Eaxmple 置换

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

Eaxmple 置换

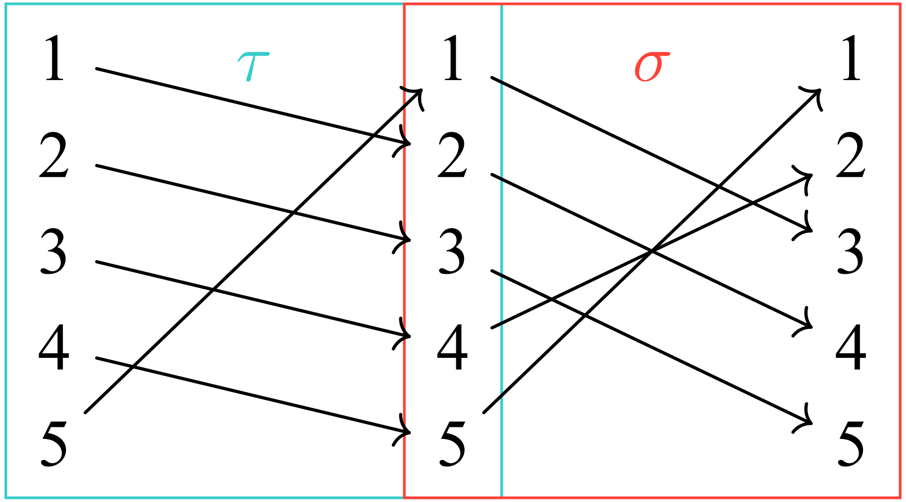
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

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

Eaxmple 置換

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

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



置換群

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。

置換群

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$n!$。

置換群

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$5! = 120$。

循環表示法(Cycle)

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

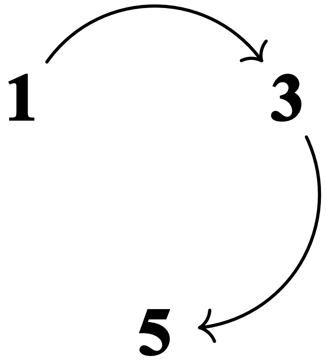
循環表示法(Cycle)

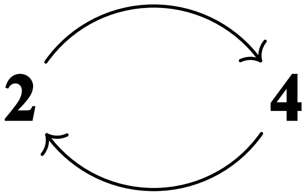
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$\mathbf{1} \rightarrow \mathbf{3} \qquad\qquad \mathbf{2} \rightarrow \mathbf{4}$$

循環表示法(Cycle)

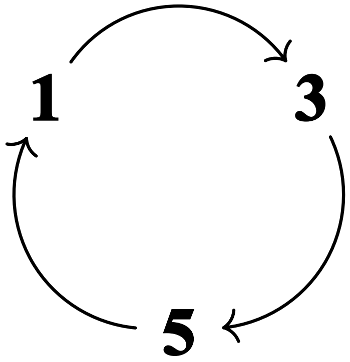
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

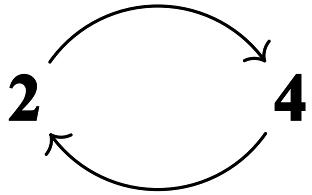




循環表示法(Cycle)

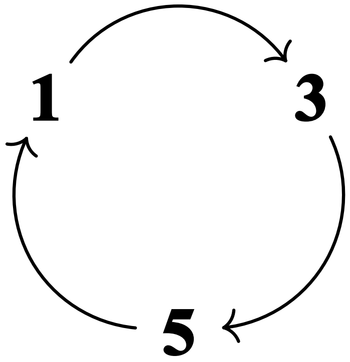
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

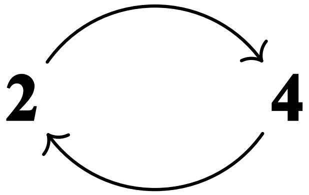




循環表示法(Cycle)

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





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

空間對稱群

Symmetry Group

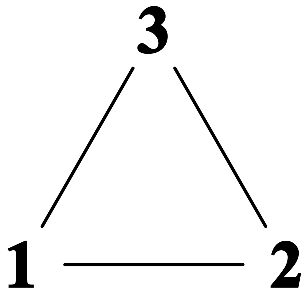
對稱群

我們接下來考慮一種特殊的置換群。

對稱群

對稱群

我們接下來考慮一種特殊的置換群。

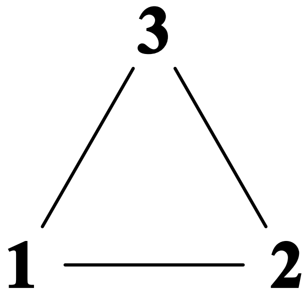


正三角形

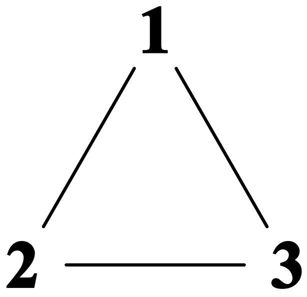
對稱群

對稱群

我們接下來考慮一種特殊的置換群。



正三角形

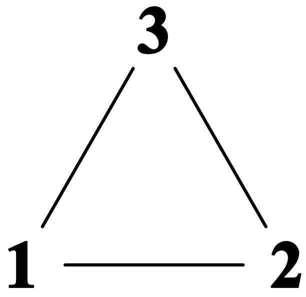


順時針旋轉 120 度

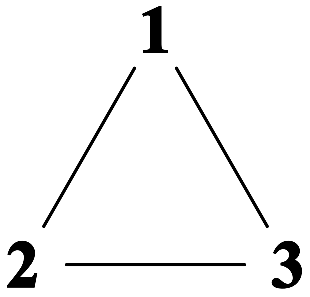
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

對稱群

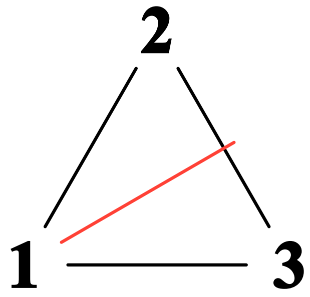
我們接下來考慮一種特殊的置換群。



正三角形



順時針旋轉 120 度



沿某一軸鏡射

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

對稱群