抽象代數

群論

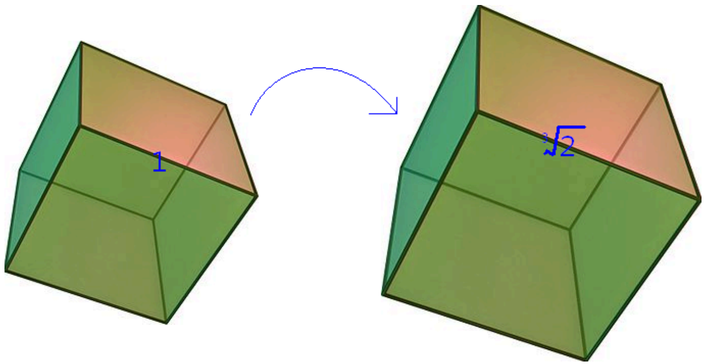
陽明交通大學應數系營隊

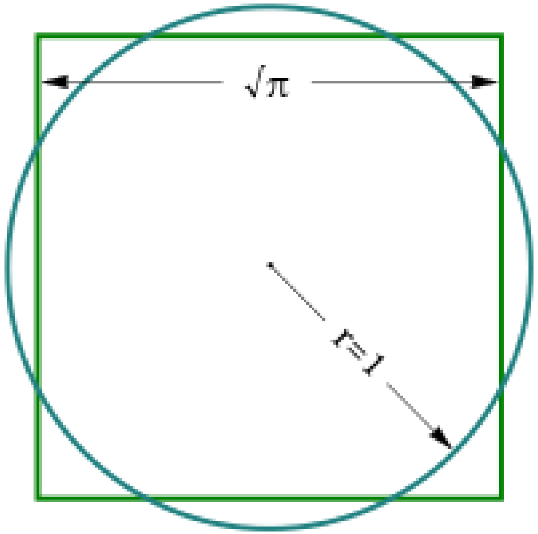
群論

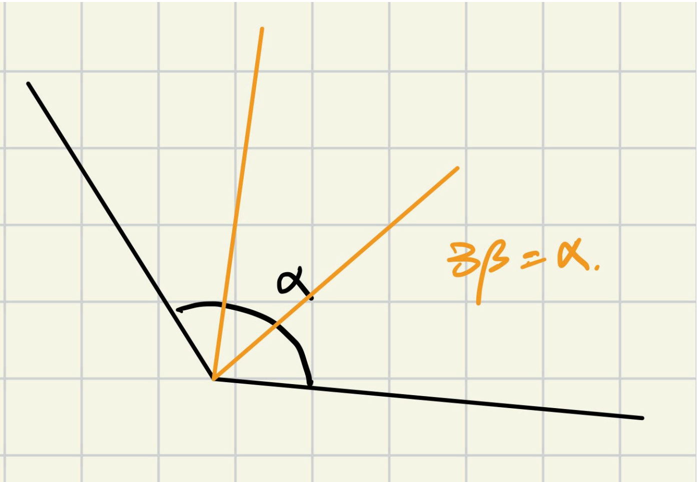
群(Group)是一個集合，並且配上一個良好的二元運算，而群論(Group Throry)是一們研究群這種結構的數學分支。群論在許多領域上有著廣泛的應用，以下介紹一些應用。

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

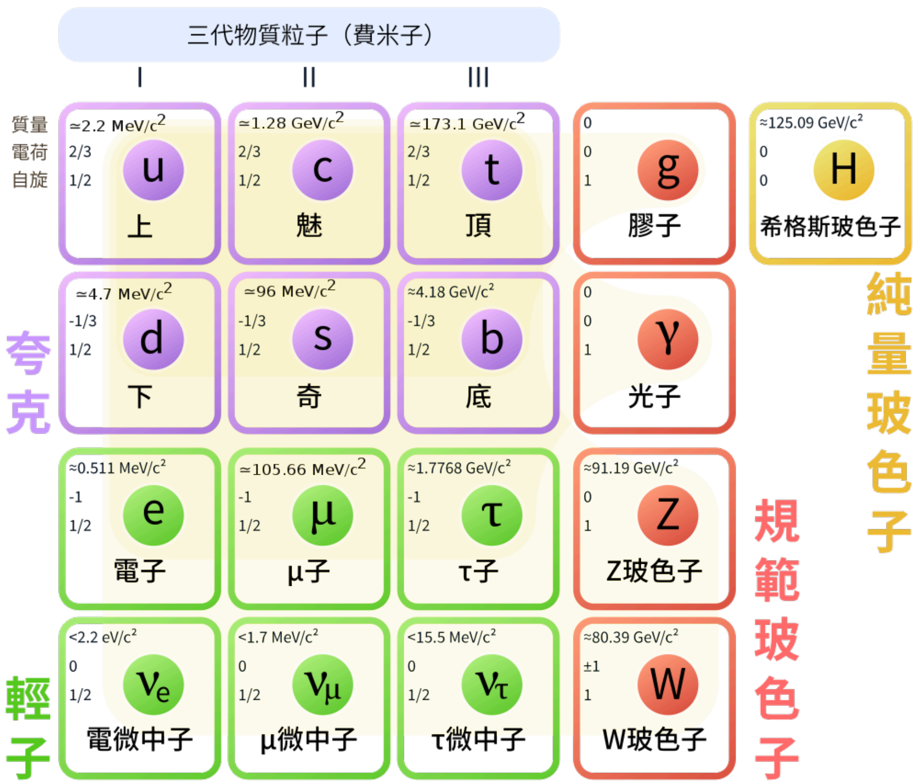
- 密碼學 (RSA 加密算法)
- 標準粒子模型中的對稱性

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 (RSA 加密算法)
- 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。
- $\langle \mathbb{Q}, + \rangle$,$\langle \mathbb{R}, + \rangle$ 是群。
- $C_3 = \{e, a, b\}$ 與下面的運算是一個群。

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3的模數群 $\mathbb{Z}_3 = \{0, 1, 2\}$ 與加法運算 $+$ 是一個群。

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**。

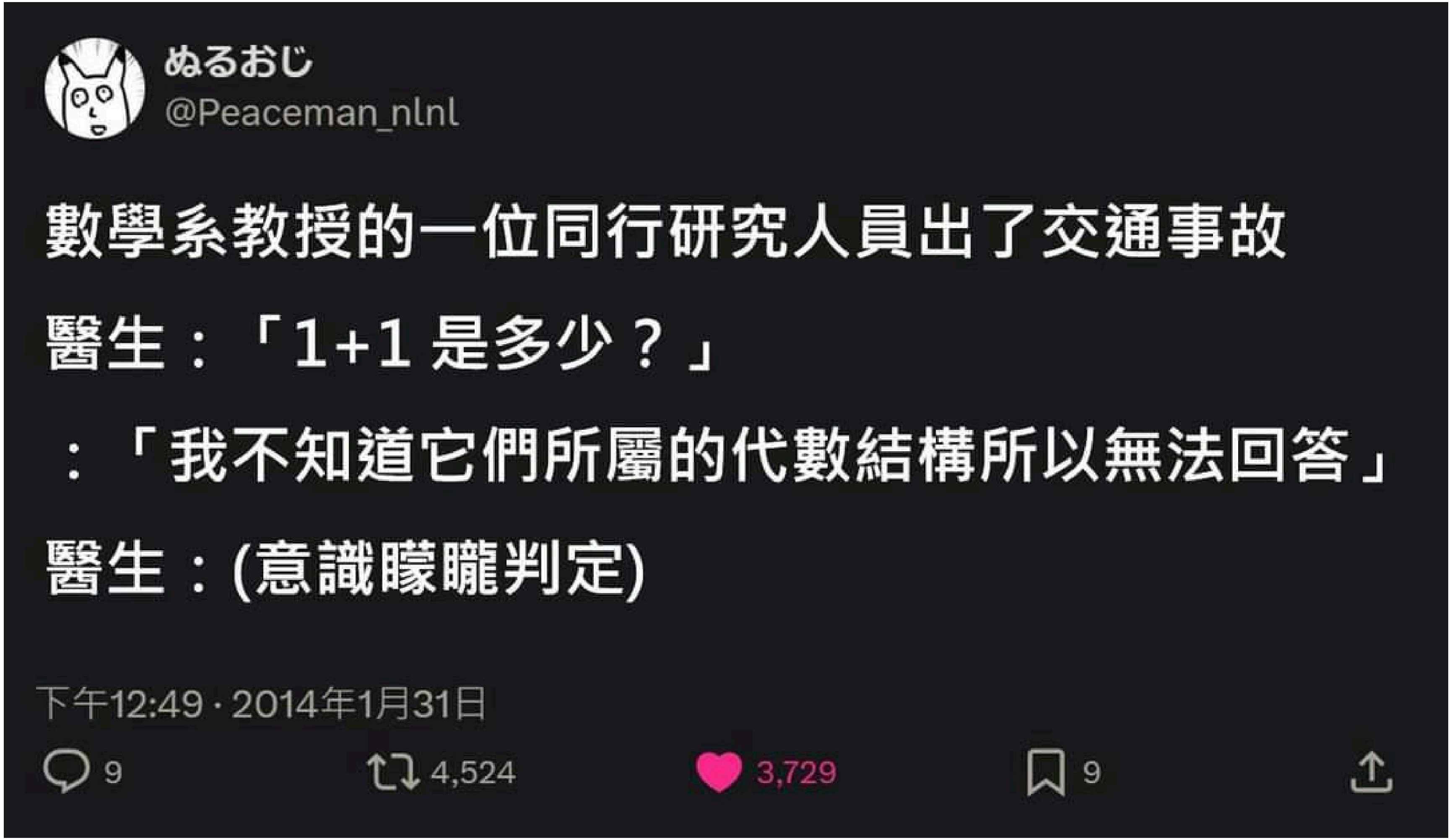
Definition 1.3：一個群G如果滿足交換率 i.e. 對於所有的$a, b \in G$，

$$a * b = b * a$$

，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。
- $C_3 = \{e, a, b\}$ 的 order 為 3。
- 可逆矩陣的集合與矩陣乘法是一個群，但不是交換群。


ぬるおじ
@Peaceman_nlnl
數學系教授的一位同行研究人員出了交通事故
醫生：「1+1 是多少？」
：「我不知道它們所屬的代數結構所以無法回答」
醫生：(意識矇矓判定)
下午12:49 · 2014年1月31日
9
4,524
3,729
9

群的基礎性質

Theorem 1.4: 如果G是一個群，那**消去率**成立，即對於所有的$a, b, c \in G$，

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

群的基礎性質

Theorem 1.4: 如果G是一個群，那**消去率**成立，即對於所有的$a, b, c \in G$，

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

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

$$a * b = a * c$$

$$\Rightarrow b = a$$

■

Theorem 1.4: 如果G是一個群，那**消去率**成立，即對於所有的$a, b, c \in G$，

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

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$a * a^{-1} = a^{-1} * a = e$。

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

■

Theorem 1.4: 如果G是一個群，那**消去率**成立，即對於所有的$a, b, c \in G$，

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

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$a * a^{-1} = a^{-1} * a = e$。

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

■

Theorem 1.4: 如果G是一個群，那**消去率**成立，即對於所有的$a, b, c \in G$，

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

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$a * a^{-1} = a^{-1} * a = e$。

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

■

Example

讓$x, y \in \mathbb{Z}$，假設$3 + x = 3 + y$，那麼$x = y$

Example

讓$x, y \in \mathbb{Z}$，假設$3 + x = 3 + y$，那麼$x = y$

讓A, B, C是$n \times n$的矩陣，如果$AB = AC$，那麼$B = C$？

Example

讓$x, y \in \mathbb{Z}$，假設$3 + x = 3 + y$，那麼$x = y$

讓A, B, C是$n \times n$的矩陣，如果$AB = AC$，那麼$\cancel{B = C}$？

Example

讓$x, y \in \mathbb{Z}$，假設$3 + x = 3 + y$，那麼$x = y$

讓A, B, C是$n \times n$的矩陣，如果$AB = AC$，那麼$\cancel{B = C}$?

讓A, B, C是$n \times n$的**可逆矩陣**，如果$BA = CA$，那麼$B = C$

群的基礎性質

Theorem 1.5: 群G的單位元素e唯一。

群的基礎性質

Theorem 1.5: 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 1.5: 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

$$e_2 * e = e$$

■

群的基礎性質

Theorem 1.5：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

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

■

Theorem 1.5: 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$e_2 = e$ ∎

Theorem 1.6: 讓G是一個群，$ab \in G$，那麼

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

我們有時候會省略運算符號，寫成ab代表$a * b$。

群的基礎性質

Theorem 1.6: 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，$(ab)^{-1} = b^{-1}a^{-1}$ ■

我們只證明了$(ab)^{-1}b^{-1}a^{-1} = e$，但是$b^{-1}a^{-1}(ab)^{-1} = e$也是成立的。

置换群

Permutation Group

置换

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

置換

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

$$\downarrow \sigma \text{ 排列}$$

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

置换

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

$$\downarrow \sigma \text{ 排列}$$

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

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

Figure 3: σ

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 4: 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 5: 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

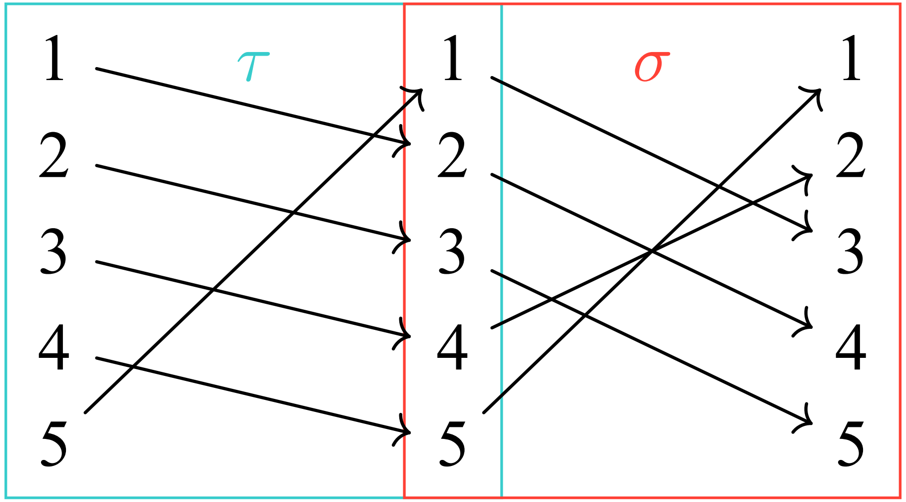
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

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

Eaxmple 置换

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

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



循環表示法(Cycle)

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

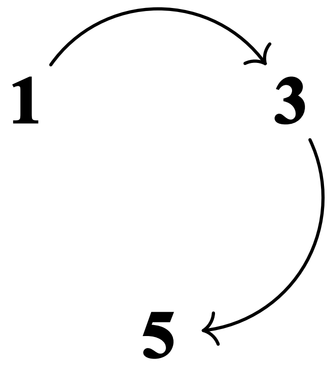
循環表示法(Cycle)

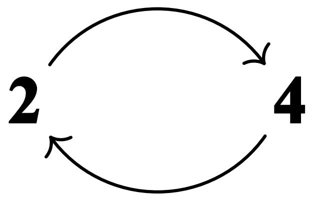
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

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

循環表示法(Cycle)

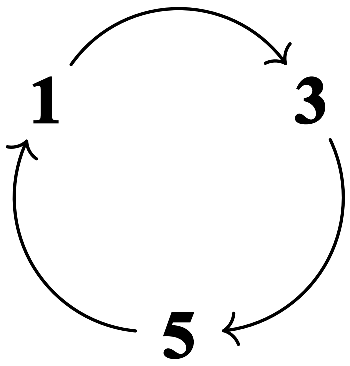
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

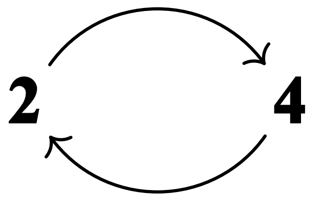




循環表示法(Cycle)

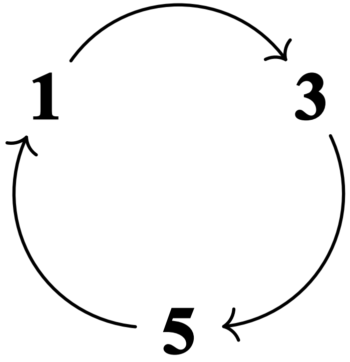
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

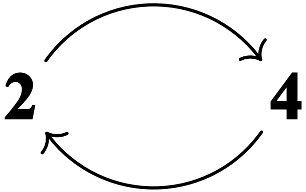




循環表示法(Cycle)

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





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

循環表示法(Cycle)

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

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

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = (3,4,5)(1)(2) = (3,4,5)$$

循環表示法(Cycle)

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

循環表示法(Cycle)

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

循環表示法(Cycle)

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

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

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。

我們驗證S_A確實是一個群。(單位元素、結合律、反元素)

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。

我們驗證S_A確實是一個群。(單位元素、結合律、反元素)

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。

我們驗證S_A確實是一個群。(單位元素、結合律、反元素)

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$5! = 120$。並且σ和τ的反元素

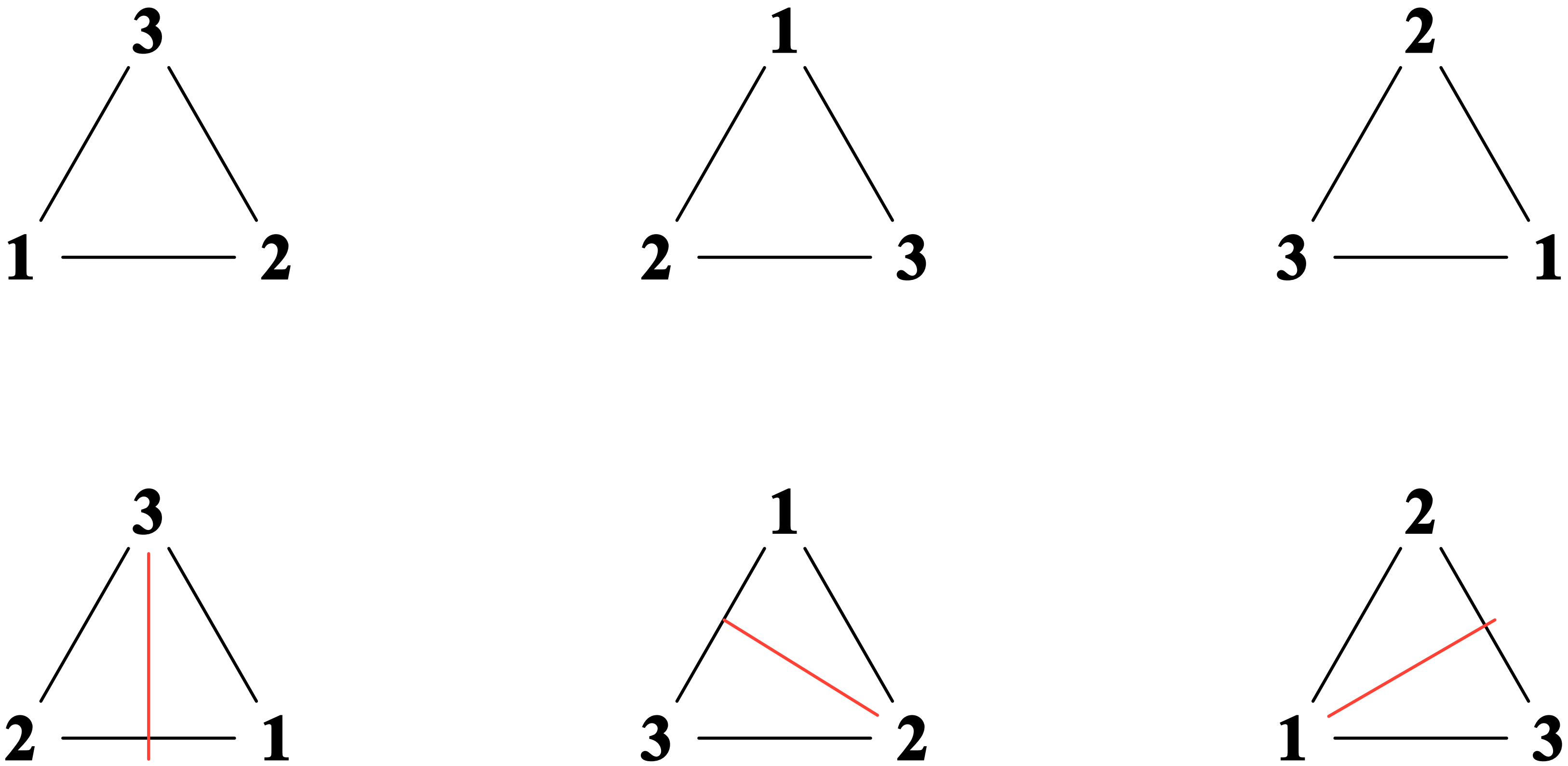
$$\sigma^{-1} = (5,3,1)(2,4)$$
$$\tau^{-1} = (5,4,3,2,1)$$

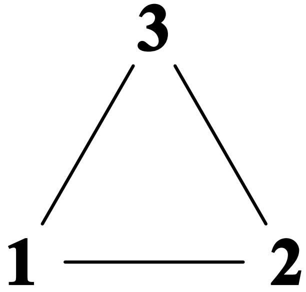
對稱群

Symmetry Group

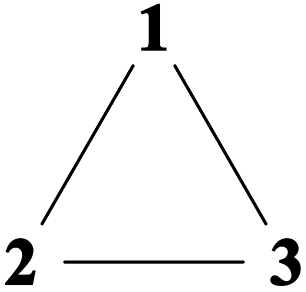
對稱群

我們接下來考慮一個正三角形，他有那些對稱性？

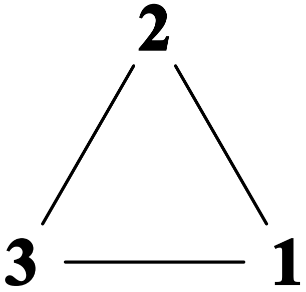

3
1
2
1
2
3
2
3
1
3
2
1
1
3
2
2
1
3



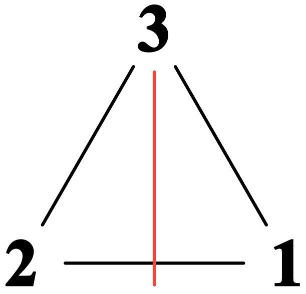
$(1)(2)(3)$



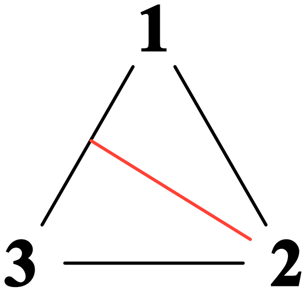
$(1,2,3)$



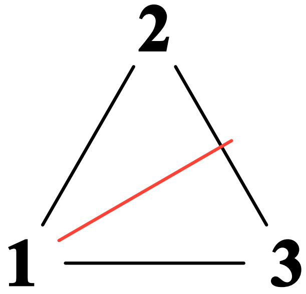
$(3,2,1)$



$(1,2)$



$(1,3)$

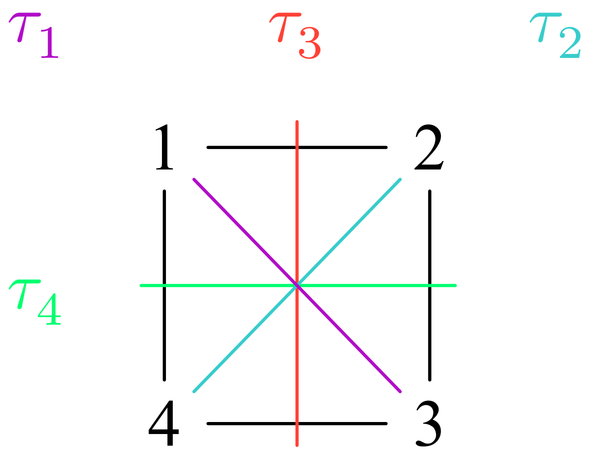


$(2,3)$

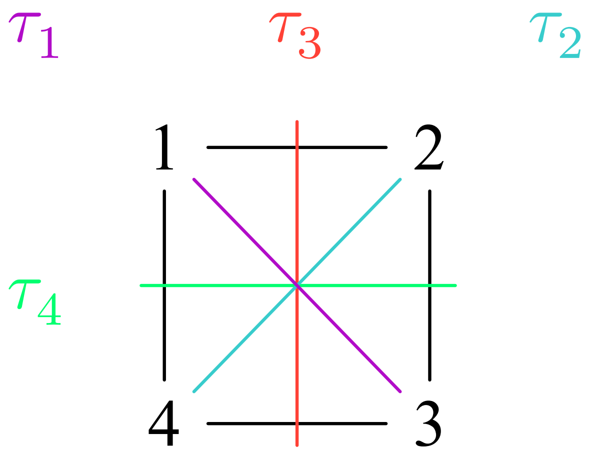
把上面正三角形的對稱性的置換收集起來，我們得到一個群，稱為正三角形的**對稱群**D_3。

那D_3的 order 是多少？只有6個嗎？

D_4



$$
\begin{aligned}
e &= (1)(2)(3)(4) \\
\rho_1 &= (1,2,3,4) \\
\rho_2 &= (1,3)(2,4) \\
\rho_3 &= (1,4,3,2) \\
\tau_1 &= (1)(2,4)(3) \\
\tau_2 &= (1,3)(2)(4) \\
\tau_3 &= (1,2)(4,3) \\
\tau_4 &= (1,4)(2,3)
\end{aligned}
$$



$$
\begin{aligned}
e &= (1)(2)(3)(4) \\
\rho_1 &= (1,2,3,4) \\
\rho_2 &= (1,3)(2,4) \\
\rho_3 &= (1,4,3,2) \\
\tau_1 &= (1)(2,4)(3) \\
\tau_2 &= (1,3)(2)(4) \\
\tau_3 &= (1,2)(4,3) \\
\tau_4 &= (1,4)(2,3)
\end{aligned}
$$

那D_4的 order 是多少？
只有8個嗎？

如何計算對稱群

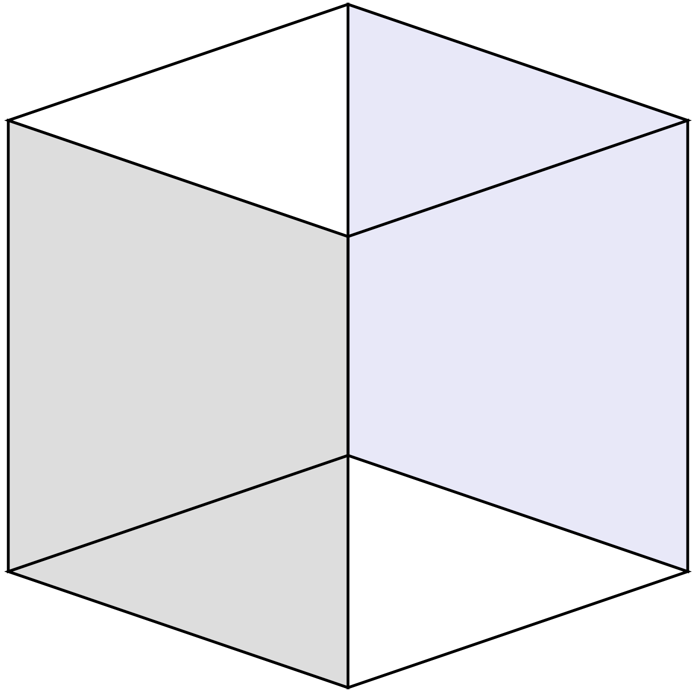
1. 先找到圖形的不動點
2. 畫一條通過不動點的直線。
3. 假設有m個對稱稱使得這條線不動，而條線在對稱性下會被打到n個不同的位子。
4. 那麼這個對稱群的 order 就是$n \times m$。

下一節會證明這個方法是正確的。

如何計算對稱群

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。



群作用

Group Action

群作用

Definition 4.1：一個群$\langle G, *\rangle$對一個集合A的**作用**是一個映射 $\varphi : G \times A \to A$，滿足以下條件：

1. 對於所有 $a \in A \quad \varphi(e, a) = a$
2. 對於所有 $a \in A$ 和 $g, h \in G$，$\varphi(g * h, a) = \varphi(g, \varphi(h, a))$

在這個情況下，我們稱A是一個G**-set**。

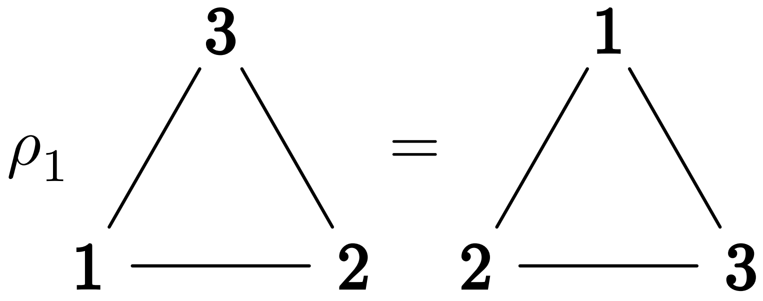
為了簡化，我們有時候會省略運算符號，寫成ga代表$\varphi(g, a)$。所以上述的條件可以寫成

$$ea = a$$
$$(gh)a = g(ha)$$

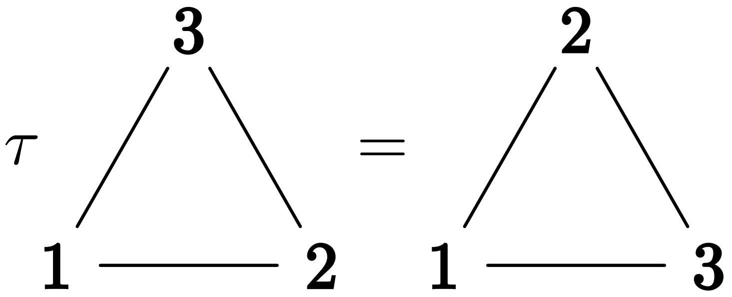
像是在上一章節中，我們考慮了對稱群D_3對正三角形的作用。

Example

$$\rho_1 = (1, 2, 3) \in D_3$$



$$\tau = (1)(2, 3) \in D_3$$



Theorem 4.2：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$gx \neq gy$

軌道 Orbits

Theorem 4.3：讓X是一個G-**set**，我們定義一個在X上的關係$\sim$，對於所有的$x, y \in X$，$x \sim y$當且僅當存在$g \in G$，使得$gx = y$。這個關係是一個等價關係。

軌道 Orbits

Theorem 4.3：讓X是一個G-**set**，我們定義一個在X上的關係$\sim$，對於所有的$x, y \in X$，$x \sim y$當且僅當存在$g \in G$，使得$gx = y$。這個關係是一個等價關係。

Proof: 自反性、對稱性、傳遞性 ∎

軌道 Orbits

Theorem 4.3: 讓X是一個G**-set**，我們定義一個在X上的關係$\sim$，對於所有的$x, y \in X$，$x \sim y$當且僅當存在$g \in G$，使得$gx = y$。這個關係是一個等價關係。

Proof: 自反性、對稱性、傳遞性

自反性：對於所有的$x \in X$，$x \sim x$，因為$ex = x$。

∎

軌道 Orbits

Theorem 4.3: 讓X是一個G-**set**，我們定義一個在X上的關係$\sim$，對於所有的$x, y \in X$，$x \sim y$當且僅當存在$g \in G$，使得$gx = y$。這個關係是一個等價關係。

Proof: 自反性、對稱性、傳遞性

自反性：對於所有的$x \in X$，$x \sim x$，因為$ex = x$。

對稱性：如果$x \sim y$，那麼存在$g \in G$，使得$gx = y$，所以$g^{-1}y = x$，所以$y \sim x$。

■

軌道 Orbits

Theorem 4.3: 讓X是一個G**-set**，我們定義一個在X上的關係$\sim$，對於所有的$x, y \in X$，$x \sim y$當且僅當存在$g \in G$，使得$gx = y$。這個關係是一個等價關係。

Proof: 自反性、對稱性、傳遞性

自反性：對於所有的$x \in X$，$x \sim x$，因為$ex = x$。

對稱性：如果$x \sim y$，那麼存在$g \in G$，使得$gx = y$，所以$g^{-1}y = x$，所以$y \sim x$。

傳遞性：如果$x \sim y$且$y \sim z$，那麼存在$g, h \in G$，使得$gx = y$且$hy = z$，所以$hgx = z$，所以$x \sim z$。 ■

軌道 Orbits

Definition 4.4：讓X是一個G-**set**，每一個在 Therorem 4.2 下的等價類稱為一個**軌道**。如果$x \in X$，包含x的分割是x的軌道，記作G_x。

Remark：讓 X 是一個 G-**set**，$x \in X$，那麼 x 的軌道 $G_x = \{gx \mid g \in G\}$。

Fixed point, Stabilizers subgroup

Definition 4.5: 讓X是一個G-**set**，讓$x \in X$，$g \in G$。我們定義；

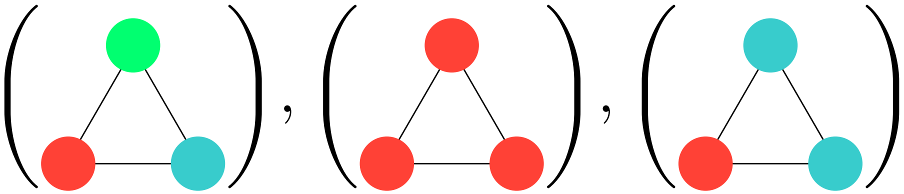
$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$$
$$X^g = \{x \in X \mid gx = x\}$$

$\mathrm{Stab}_G(x)$稱為x的**穩定子群**，X^g稱為g的**不動點**。

Example

讓$G = D_3$，X是用3種顏色為三角形的頂點上色所有可能所成的集合。

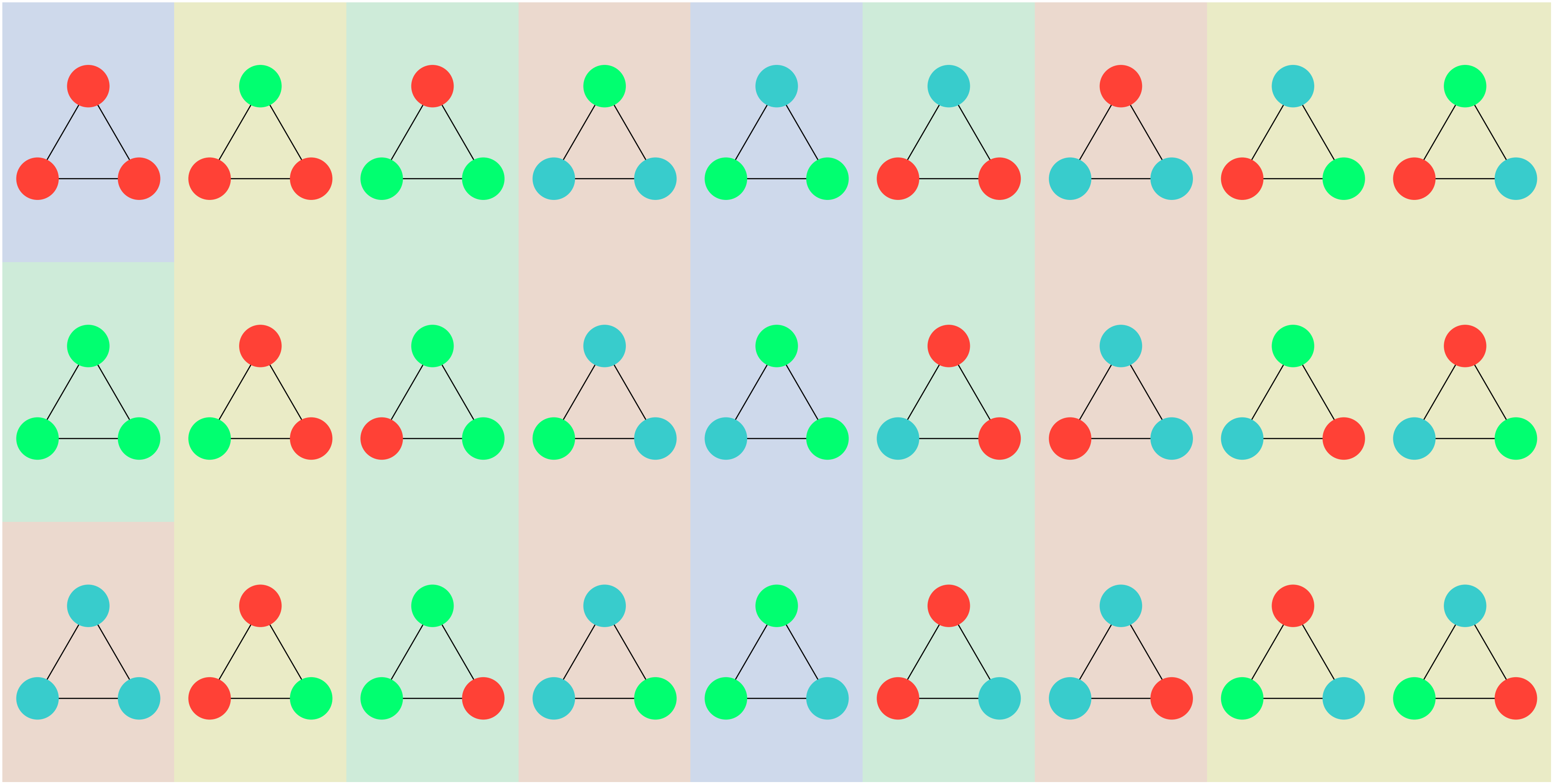
e.g.



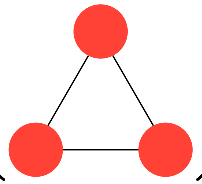
$\in X$

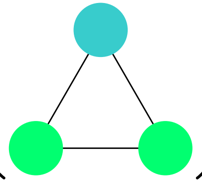
$$|X| = 3 \times 3 \times 3$$

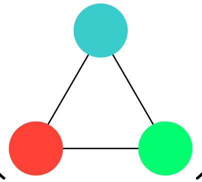
Example: 軌道

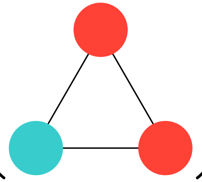


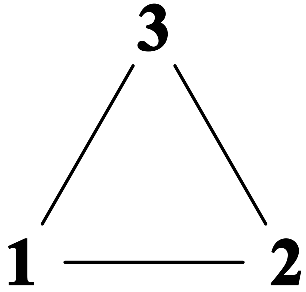
Example: Stabilizer

$\mathrm{Stab}_G\Big($  $\Big) = D_3$

$\mathrm{Stab}_G\Big($  $\Big) = \{e, (1,2)\}$

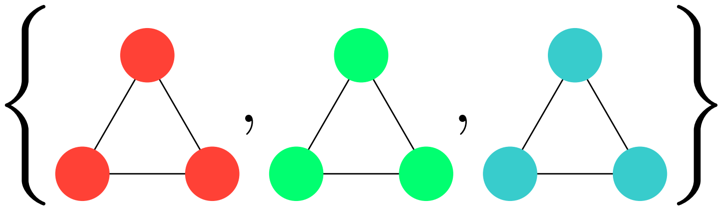
$\mathrm{Stab}_G\Big($  $\Big) = \{e\}$

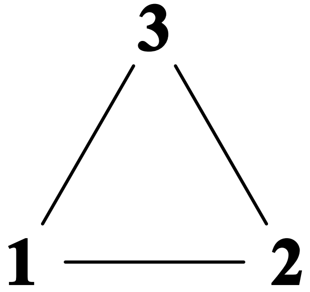
$\mathrm{Stab}_G\Big($  $\Big) = \{e, (2,3)\}$



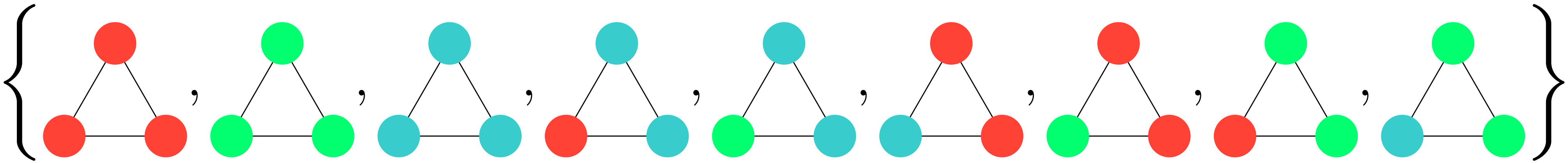
Example: Fixed Point

$g = e \, , X^g = X$

$g = (1,2,3) \, , X^g =$ 

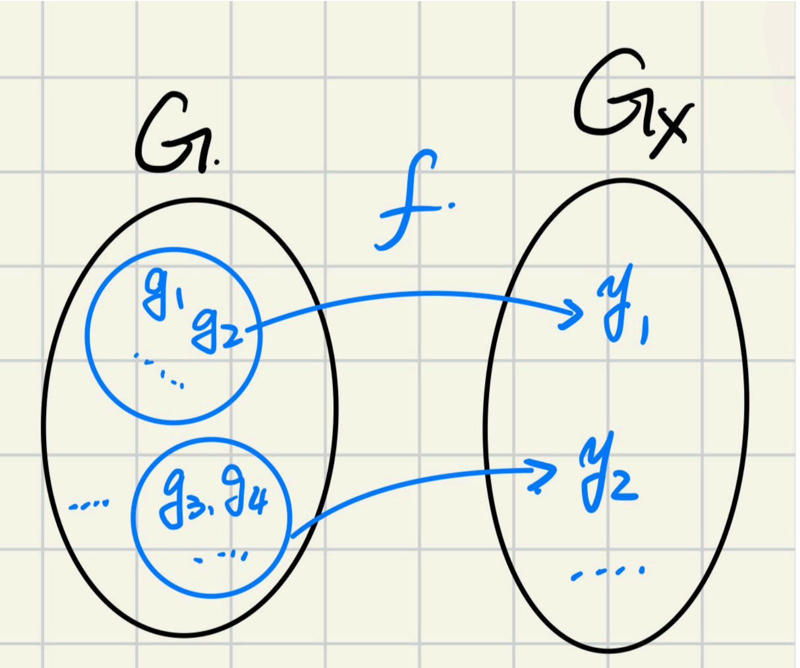


$g = (2,3) \, , X^g =$



軌道-穩定子定理

Theorem 4.6 (軌道-穩定子定理 (Orbit-Stabilizer Theorem))：讓G是一個有限群，讓 X 是一個 G**-set**，$x \in X$，那麼 $|G| = |G_x||\mathrm{Stab}_G(x)|$。



Proof

定義$f : G \to G_x$，$f(g) = gx$。我們證明每一個在G_x裡的元素都被打到$|\mathrm{Stab}_G(x)|$這麼多次。

給定一個$y \in G_x$，那麼存在$h \in G$使得$y = hx$。

Proof

定義$f: G \to G_x$，$f(g) = gx$。我們證明每一個在G_x裡的元素都被打到$|\mathrm{Stab}_G(x)|$這麼多次。

給定一個$y \in G_x$，那麼存在$h \in G$使得$y = hx$。

我們先證明這個引理: $f(g) = y \iff h^{-1}g \in \mathrm{Stab}_G(x)$。

Proof

定義$f : G \to G_x$，$f(g) = gx$。我們證明每一個在G_x裡的元素都被打到$|\mathrm{Stab}_G(x)|$這麼多次。

給定一個$y \in G_x$，那麼存在$h \in G$使得$y = hx$。

我們先證明這個引理: $f(g) = y \iff h^{-1}g \in \mathrm{Stab}_G(x)$。

$\Rightarrow$：如果$f(g) = y$，那麼$gx = hx$，所以$h^{-1}gx = x$，所以$h^{-1}g \in \mathrm{Stab}_G(x)$。

Proof

定義$f : G \to G_x$，$f(g) = gx$。我們證明每一個在G_x裡的元素都被打到$|\mathrm{Stab}_G(x)|$這麼多次。

給定一個$y \in G_x$，那麼存在$h \in G$使得$y = hx$。

我們先證明這個引理: $f(g) = y \iff h^{-1}g \in \mathrm{Stab}_G(x)$。

$\Rightarrow$：如果$f(g) = y$，那麼$gx = hx$，所以$h^{-1}gx = x$，所以$h^{-1}g \in \mathrm{Stab}_G(x)$。

$\Leftarrow$：如果$h^{-1}g \in \mathrm{Stab}_G(x)$，那麼$h^{-1}gx = x$，所以$gx = hx$，所以$f(g) = y$。

接著我們來討論有多少 $g \in G$ 使得 $h^{-1}g \in \mathrm{Stab}_G(x)$。

接著我們來討論有多少 $g \in G$ 使得 $h^{-1}g \in \mathrm{Stab}_G(x)$。

$$\begin{aligned} h^{-1}g \in \mathrm{Stab}_G(x) &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x)\ s.t.\ h^{-1}g = \tilde{g} \\ &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x)\ s.t.\ g = h\tilde{g} \\ &\iff g \in \{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\} \end{aligned}$$

接著我們來討論有多少 $g \in G$ 使得 $h^{-1}g \in \mathrm{Stab}_G(x)$。

$$\begin{aligned} h^{-1}g \in \mathrm{Stab}_G(x) &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x) \ s.t.\ h^{-1}g = \tilde{g} \\ &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x) \ s.t.\ g = h\tilde{g} \\ &\iff g \in \{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\} \end{aligned}$$

所以，$f(g) = y \iff g \in \{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\}$，並且，對於所有$\tilde{g} \in \mathrm{Stab}_{G(x)}$，

$f(h\tilde{g}) = h\tilde{g}x = hx = y$。

因此，每個$y \in G_x$ 都 $|\mathrm{Stab}_G(x)|$ 個 $g \in G$ 使得 $f(g) = y$。所以，$|G| = |G_x||\mathrm{Stab}_G(x)|$。

接著我們來討論有多少 $g \in G$ 使得 $h^{-1}g \in \mathrm{Stab}_G(x)$。

$$\begin{aligned} h^{-1}g \in \mathrm{Stab}_G(x) &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x) \ s.t. \ h^{-1}g = \tilde{g} \\ &\iff \exists \tilde{g} \in \mathrm{Stab}_G(x) \ s.t. \ g = h\tilde{g} \\ &\iff g \in \{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\} \end{aligned}$$

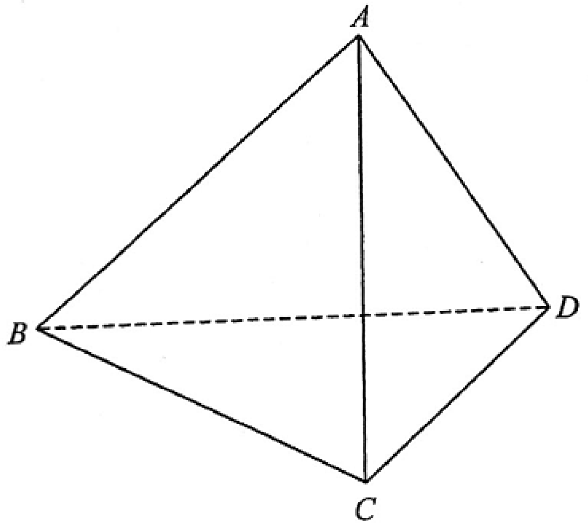
所以，$f(g) = y \iff g \in \{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\}$，並且，對於所有$\tilde{g} \in \mathrm{Stab}_{G(x)}$，

$f(h\tilde{g}) = h\tilde{g}x = hx = y$。

因此，每個$y \in G_x$ 都 $|\mathrm{Stab}_G(x)|$ 個 $g \in G$ 使得 $f(g) = y$。所以，$|G| = |G_x||\mathrm{Stab}_G(x)|$。

Exercise

1. 為什麼$\{h\tilde{g} \mid \tilde{g} \in \mathrm{Stab}_G(x)\}$ 的基數(cardinality)和 $\mathrm{Stab}_G(x)$ 的基數相等？
2. 判斷下列圖形的對稱群的 order:



伯恩賽德引理 (Burnside's Lemma)

Lemma 4.7 (伯恩賽德引理): 讓G是一個有限群，讓X是一個G**-set**。讓r是X的軌道數，那麼

$$r \cdot |G| = \sum_{g \in G} |X^g|$$

伯恩賽德引理 (Burnside's Lemma)

Lemma 4.7 (**伯恩賽德引理**): 讓G是一個有限群，讓X是一個G-**set**。讓r是X的軌道數，那麼

$$r \cdot |G| = \sum_{g \in G} |X^g|$$

我們通過雙重計數來證明這個引理。考慮所有滿足$gx = x$的序組(g, x)，我們用兩種方式計數這些序組，這樣就會有一個很自然的等式。

Proof

我們考慮序組(g,x)，其中$gx = x$。假設這樣的序組有N個。 給定 一個$g \in G$，我們計算(g,x)的數量，這個數量是$|X^g|$。所以

$$N = \sum_{g \in G} |X^g|$$

Proof

我們考慮序組(g, x)，其中$gx = x$。假設這樣的序組有N個。 給定 一個$g \in G$，我們計算(g, x)的數量，這個數量是$|X^g|$。所以

$$N = \sum_{g \in G} |X^g|$$

另一方面，給定一個$x \in X$，我們計算(g, x)的數量，這個數量是$|\mathrm{Stab}_G(x)|$。所以

$$N = \sum_{x \in X} |\mathrm{Stab}_G(x)|$$

根據 **軌道穩定子定理** Thm ，$|\mathrm{Stab}_G(x)||G_x| = |G|$，所以，

$$N = \sum_{x\in X} |\mathrm{Stab}_G(x)| = \sum_{x\in X} \frac{|G|}{|G_x|} = |G| \sum_{x\in X} \frac{1}{|G_x|}$$

對於在相同軌道的元素，$|G_x|$是相同的。讓$\mathcal{O}$是一個軌道，我們有

$$\sum_{x\in\mathcal{O}} \frac{1}{|G_x|} = \sum_{x\in\mathcal{O}} \frac{1}{|\mathcal{O}|} = 1$$

因此，

$$\sum_{x\in X} \frac{1}{|G_x|} = (\text{軌道的數量})$$

$$N = |G| \cdot (\text{軌道的數量}) = |G| \cdot r$$

$$r \cdot |G| = \sum_{g \in G} |X^g|$$

Example

用4個顏色對一個正三角形的三個邊進行著色，有幾種不同的著色方法？(兩種著色方式被認為是相同的，如果他們可以通過旋轉、鏡射相互變換)

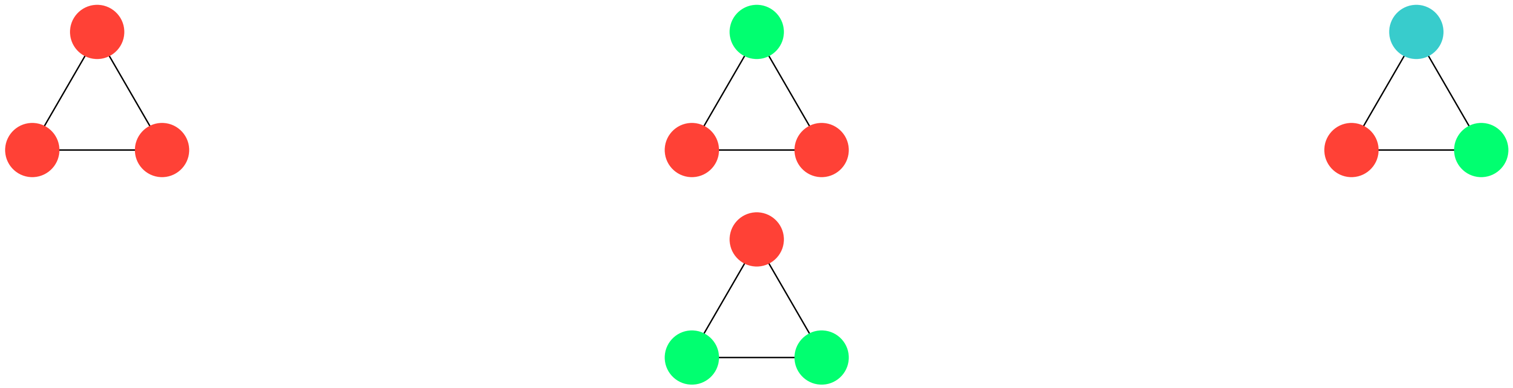
Example

用4個顏色對一個正三角形的三個邊進行著色，有幾種不同的著色方法？(兩種著色方式被認為是相同的，如果他們可以通過旋轉、鏡射相互變換)

Method1: 分別討論有$1, 2, 3$個顏色時的著色方法數量。

$$C_1^4 \times 1 + C_2^4 \times 2 + C_3^4 \times 1 = 20$$

e.g.



Method2: Burnside's lemma

我們讓$G = D_3$是三角型的對稱群，X是所有著色的結果($|X| = 4^3$)，所以我們要求X在G下有幾個軌道。根據前的討論，我們知道$|G| = 6$，然後我們計算不動點的個數：

$$|X^{\rho_0}| = 4^3 \qquad |X^{\tau_1}| = 4^2$$
$$|X^{\rho_1}| = 4 \qquad |X^{\tau_2}| = 4^2$$
$$|X^{\rho_2}| = 4 \qquad |X^{\tau_3}| = 4^2$$

根據**伯恩賽德引理**，我們有

$$\begin{aligned} 6r &= 4^3 + 4 + 4 + 4^2 + 4^2 + 4^2 = 120 \\ r &= 20 \end{aligned}$$

Method2: Burnside's lemma

所以正三角形的相異著色方法有20種。

著色多項式

我們考慮我們有n個顏色，幫一個有對稱性的圖形上色，我們假設在對稱性下有r種上色方式。 讓X是所有上色方法的集合，讓G是該圖形的對稱群，根據博恩賽德引理，我們有

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

其中X^g是在g下的不動點的集合。

著色多項式

我們考慮我們有n個顏色，幫一個有對稱性的圖形上色，我們假設在對稱性下有r種上色方式。 讓X是所有上色方法的集合，讓G是該圖形的對稱群，根據博恩賽德引理，我們有

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

其中X^g是在g下的不動點的集合。

$$g = \underbrace{(1, 2, 3)(5, 4)...(\#, \#)}_{m_g}$$

「每個循環內的顏色都一樣」$|X^g| = n^{m_g}$

著色多項式

我們考慮我們有n個顏色，幫一個有對稱性的圖形上色，我們假設在對稱性下有r種上色方式。 讓X是所有上色方法的集合，讓G是該圖形的對稱群，根據博恩賽德引理，我們有

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

其中X^g是在g下的不動點的集合。

$$g = \underbrace{(1,2,3)(5,4)...(\#,\#)}_{m_g}$$

「每個循環內的顏色都一樣」 $|X^g| = n^{m_g}$

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{1}{|G|}\sum_{g\in G}n^{m_g}$$

Example

我們考慮有n個顏色，對一個正四邊形的頂點上色，我們要求在對稱性下有幾種不同的著色方法。

Example

我們考慮有n個顏色，對一個正四邊形的頂點上色，我們要求在對稱性下有幾種不同的著色方法。

我們讓$G = D_4$是正四邊形的對稱群，X是所有著色的結果$(|X| = n^4)$，我們知道$|G| = 8$

Example

我們考慮有n個顏色，對一個正四邊形的頂點上色，我們要求在對稱性下有幾種不同的著色方法。

我們讓$G = D_4$是正四邊形的對稱群，X是所有著色的結果($|X| = n^4$)，我們知道$|G| = 8$

- 1個 4 cycle 的單位變換，$e = (1)(2)(3)(4)$
- 2個 1 cycle 的旋轉(90°, 270°)，e.x. $g = (1, 2, 3, 4)$
- 1個 2 cycle 的旋轉(180°)，e.x. $g = (1, 2)(3, 4)$
- 2個 3 cycle 的鏡射(對角線的鏡射)，e.x. $g = (1)(3)(2, 4)$
- 2個 2 cycle 的鏡射(中線的鏡射)，e.x. $g = (1, 3)(2, 4)$

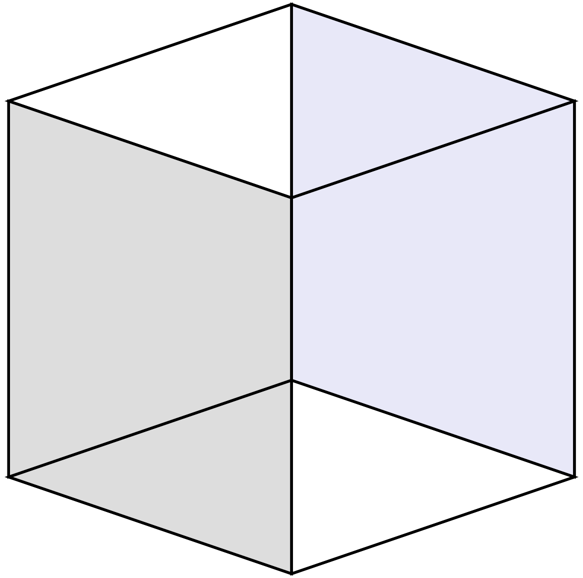
所以我們有

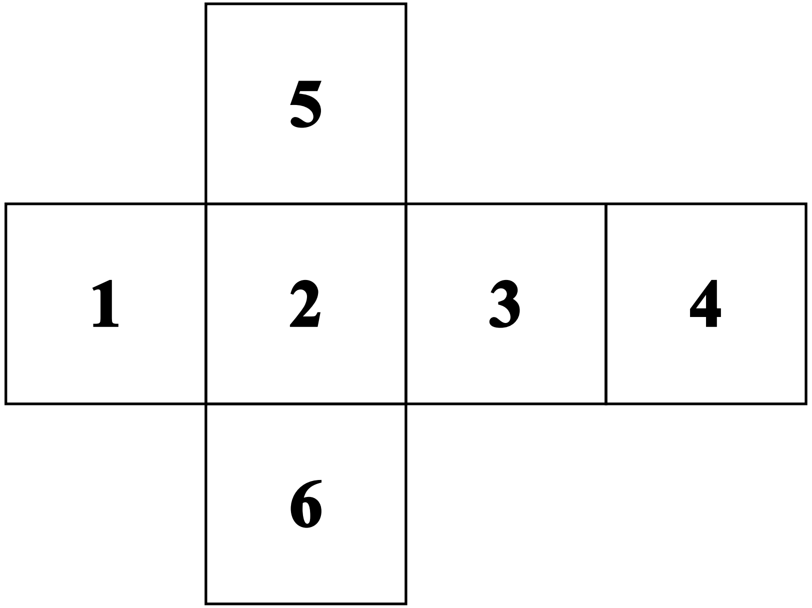
$$r = \frac{1}{8}(n^4 + 2n + n^2 + 2n^3 + 2n^2)$$

$$r = \frac{1}{8}(n^4 + 2n^3 + 3n^2 + 2n)$$

Example

我們現在有n個顏色，幫一個正六面體上色，可以通過旋轉變換得到視為相同的著色方式。總共有多少種不同的著色方式？





我們讓$G = D$是正六面體的對稱群，X是所有著色的結果($|X| = n^6$)，我們知道 $|G| = 24$

我們讓$G = D$是正六面體的對稱群，X是所有著色的結果($|X| = n^6$)，我們知道$|G| = 24$

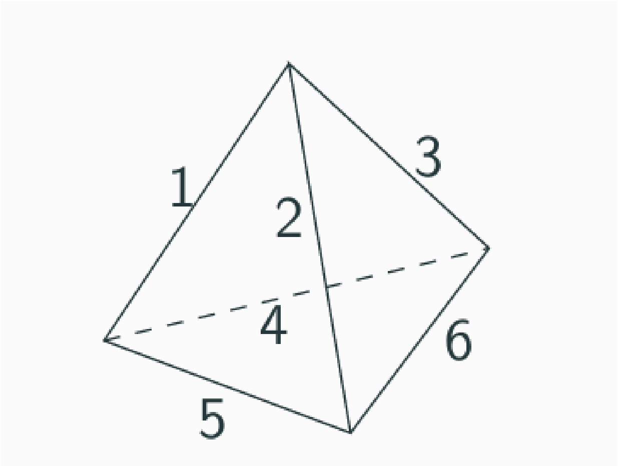
1. 單位變換:$(1)(2)(3)(4)(5)(6)$
2. 過對面中點轉軸旋轉$90°, 270°$，如:$(1,2,3,4)(5)(6)$，共 6 個。
3. 過對面中點轉軸旋轉$180°$，如:$(1,3)(2,4)(5)(6)$，共 3 個。
4. 過對邊中點轉軸旋轉$180°$，如:$(1,5)(3,6)(2,4)$，共 6 個。
5. 過對頂點轉軸旋轉$120°, 240°$，如:$(1,5,4)(2,3,6)$，共 8 個

所以我們有

$$r = \frac{1}{24}(n^6 + 6n^3 + 3n^4 + 6n^3 + 8n^2)$$
$$r = \frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2)$$

Example

在旋轉的對稱姓下，用n個顏色對一個正四面體的邊上色，總共有多少種不同的著色方式？



我們讓G是正四面體的對稱群，我們通過軌道-穩定子定理，我們可以得到$|G| = 12$

我們討論裡面的對置換：

- 單位變換:$(1)(2)(3)(4)(5)(6)$
- 8個以一面中點的垂線為轉軸的旋轉:$(1,2,3)(4,5,6)$
- 3個以過兩對邊中點的轉軸旋轉:$(1)(6)(2,4)(5,3)$

所以我們有

$$r = \frac{1}{12}(n^6 + 8n^2 + 3n^4)$$