

群論

陽明交大應數系營隊

在數學中，群論 (Group theory) 研究名為「群」的代數構。群論在許多的領域都有很重要的應用。像是，倍立方、化圓為方、三等分角，五次多項式 2 公式 i 無法解的原因都可以用群論來解釋。另外，像是標準粒子模型、量子力學 (李群)、晶體結構、密碼學等領域也有很多群論的應用。

1. 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: 我們來看一些例子：

- $\langle \mathbb{Z}, + \rangle$ 、 $\langle \mathbb{Q}, + \rangle$ 、 $\langle \mathbb{R}, + \rangle$
- $\langle \mathbb{Q}^+, \times \rangle$
- $\langle \mathbb{Z}_n, +_n \rangle$

Remark: 有時候我們會省略二元運算 $*$ ，以 G 表示一個群。

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)。

1.1. 群的性質

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 $a * a^{-1} = e$ 。

$$a * b = a * c$$

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

$$\Rightarrow e * b = e * c$$

■

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 $e_2 * a = a * e_2 = a \forall a \in G$ ，因為 $e \in G$ ，所以 $e_2 * e = e * e$ ，根據消去律 $e_2 = e$ 。

■

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

$$(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} \quad \text{結合律}$$

$$= aea^{-1}$$

$$= aa^{-1}$$

$$= e$$

根據反元素的定義， $(ab)^{-1} = b^{-1}a^{-1}$

■

2. 置換群

3. 空間對稱群

4. 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。

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 $gx \neq gy$

4.1. 不動點 (Fixed point)、穩定子群 (stabilizers subgroup)、軌道 (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**。

Theorem 4.2: 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 $x \sim z$ 。 ■

Definition 4.3: 讓 X 是一個 G -set, 每一個在 Theorem 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 。

Theorem 4.3: 讓 X 是一個 G -set, $x \in X$, 那麼 x 的軌道 $G_x = \{gx \mid g \in G\}$ 。

Theorem 4.4 (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 $|G| = |G_x| |Gx|$ 。

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

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

如果 $g \in \text{Stab}_G(x)$ ，那麼 $gx = x$ ，所以

$$f(hg) = hgx = hx = y$$

如果 $g \notin \text{Stab}_G(x)$ ，那麼 $gx \neq x$ ，所以

$$f(hg) = hgx \neq hx = y$$

所以 y 被打到那麼多次 $|\text{Stab}_G(x)|$ ，所以 $|G| = |G_x| |\text{Stab}_G(x)|$ 。 ■

4.2. 伯恩賽德引理 (Burnside's Lemma)

Theorem 4.5 (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

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

Proof: 我們考慮數組 (g, x) ，其中 $gx = x$ 。假設這樣的樹組有 N 個。對於每一個 $g \in G$ ，我們計算 (g, x) 的數量，這個數量是 $|X^g|$ 。所以

$$N = \sum_{g \in G} |X^g| \quad (1)$$

另一方面，對於每一個 $x \in X$ ，我們計算 (g, x) 的數量，這個數量是 $|\text{Stab}_G(x)|$ 。所以

$$N = \sum_{x \in X} |\text{Stab}_G(x)| \quad (2)$$

根據 **軌道穩定子定理** Thm 4.4， $|\text{Stab}_G(x)| |G_x| = |G|$ ，所以，

$$N = \sum_{x \in X} |\text{Stab}_G(x)| = \sum_{x \in X} \frac{|G|}{|G_x|} = |G| \sum_{x \in X} \frac{1}{|G_x|} \quad (3)$$

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

$$\sum_{x \in \mathcal{O}} \frac{1}{|G_x|} = \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = 1 \quad (4)$$

用 (3) 代入 (2)，我們得到

$$N = |G| \cdot (\text{軌道的數量}) = |G| \cdot r \quad (5)$$

因此，結合 (1) 和 (4)，我們得到

$$r \cdot |G| = \sum_{g \in G} |X^g| \quad (6)$$

■

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)

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：

$$|X^{\rho_0}| = 4^3$$

$$|X^{\rho_1}| = 4$$

$$|X^{\rho_2}| = 4$$

$$|X^{\tau_1}| = 4^2$$

$$|X^{\tau_2}| = 4^2$$

$$|X^{\tau_3}| = 4^2$$

根據伯恩斯德引理，我們有

$$6r = 4^3 + 4 + 4 + 4^2 + 4^2 + 4^2 r = 20$$

所以正三角形的相異著色方法有20種。

4.3. 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，根據博恩斯德引理，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。我們觀察一下 $g \in G$ ，我們知道 g 可以被寫成循環的形式，像是下面這樣：

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

所以 g 種共有 m_g 個循環。我們發現在這種情況下要在 g 下不動的著色方法必須滿足「每個循環內的顏色都一樣」，所以 $|X^g| = n^{m_g}$ 所以我們得到，

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

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 ($|X| = n^4$)，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 $|G| = 8$ ，然後我們計算不動點的個數：

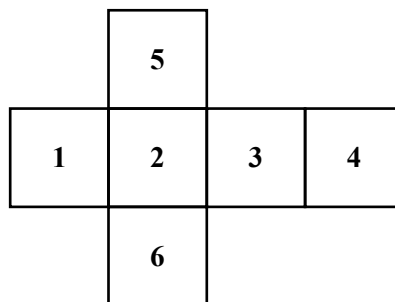
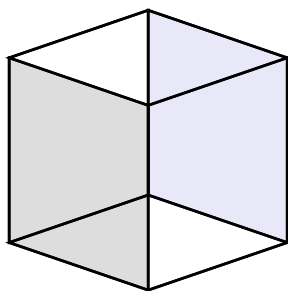
- 單位變換 $m_g = 4$
- 2個 $m_g = 1$ 的旋轉 ($90^\circ, 270^\circ$)，e.x. $g = (1, 2, 3, 4)$
- 1個 $m_g = 2$ 的旋轉 (180°)，e.x. $g = (1, 2)(3, 4)$
- 2個 $m_g = 3$ 的鏡射 (對角線的鏡射)，e.x. $g = (1)(3)(2, 4)$
- 2個 $m_g = 2$ 的鏡射 (中線的鏡射)，e.x. $g = (1, 3)(2, 4)$

所以我們有

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

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

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？



讓 D 是正六面體的對稱群，我們根據之前的討論，我們知道 $|D| = 24$ ，我們討論裡面的變換：

1. 單位變換: $(1)(2)(3)(4)(5)(6)$
2. 固定兩對面然會旋轉 $90^\circ, 270^\circ$ ，如: $(1, 2, 3, 4)(5)(6)$ ，共 6 個。
3. 固定兩對面然會旋轉 180° ，如: $(1, 3)(2, 4)(5)(6)$ ，共 3 個。
4. 固定兩對邊旋轉 180° ，如: $(1, 5)(3, 6)(2, 4)$ ，共 6 個。
5. 固定兩個對頂點旋轉 $120^\circ, 240^\circ$ ，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: 現在我們有一串項鍊，我們有 n 個不同的珠子，我們要把這些珠子串成一串項鍊，可以通過旋轉變換得到視為相同的項鍊。總共有多少種不同的項鍊？