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$a, b, c \in G$，

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

$\mathcal{G}_2$: 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: 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$a * a^{-1} = e$。

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

■

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

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

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$* : G \times A \to A$，滿足以下條件：
1. 對於所有$a \in A \quad ea = a$
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；

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

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

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

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$f : G \to G_x$，$f(g) = gx$。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$y = hx$。
如果$g \in \mathrm{Stab}_G(x)$，那$gx = x$，所以

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

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

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

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

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

$$N = \sum_{g \in G} |X^g| \tag{1}$$

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$|\mathrm{Stab}_G(x)|$。所以

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

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

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

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

$$\sum_{x \in \mathcal{O}} \frac{1}{|G_x|} = \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = 1 \tag{4}$$

用 **(3)** 代入 **(2)**，我們得到

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

因此， 結合 **(1)** 和 **(4)**，我們得到

$$r \cdot |G| = \sum_{g \in G} |X^g| \tag{6}$$

■

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**伯恩賽德引理**，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。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:

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

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，

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