詳細解答

STEP II 1992，第 5 題

純數學 • 矩陣群

> **STEP II 1992，第 5 題**
>
> 繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：
>
> step.maths.org/questions/92-s2-q5

關鍵思路

這裏的一切都建基於條件 $wz - xy = 1$，它令 S 中矩陣（matrix）的逆矩陣（inverse）特別簡單。處理階為 3 的部分，最好的方法是留意到每個 2×2 矩陣都滿足一條由其跡（trace）和行列式（determinant）構成的二次方程。對於 S 中的矩陣，我們可藉此把 $\mathbf{A}^2$，繼而把 $\mathbf{A}^3$，用 $\mathbf{A}$ 和 $\mathbf{I}$ 表示出來，於是條件 $\mathbf{A}^3 = \mathbf{I}$ 就變成關於跡 $w + z$ 的條件。

（試卷上把 $\mathbf{A}$ 右下角的元素印成 x；但最後一部分提到 z，可見原意顯然是該位置為 z，以下一律採用此寫法。）

解答

元素的階

$g \in G$ 的階（order）是使 $g^n = e$ 成立的最小正整數 n，其中 e 是 G 的單位元（identity）。若 g 的任何正整數次冪都不等於 e，則 g 的階為無限。單位元是唯一階為 1 的元素。

逆矩陣

設

$$\mathbf{A} = \begin{pmatrix} w & x \\ y & z \end{pmatrix}, \qquad wz - xy = 1.$$

2×2 逆矩陣的常用公式要除以行列式，而這裏行列式為 1，所以

$$\mathbf{A}^{-1} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}.$$

乘開即可驗證：$\mathbf{A}\mathbf{A}^{-1} = \begin{pmatrix} wz - xy & 0 \\ 0 & wz - xy \end{pmatrix} = \mathbf{I}$，同理 $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$。

S 是一個羣

我們逐一檢驗羣（group）的四條公理。

- 封閉性（*closure*）。若 $\mathbf{A}, \mathbf{B} \in S$，則 $\det(\mathbf{AB}) = \det\mathbf{A}\,\det\mathbf{B} = 1 \times 1 = 1$，所以 $\mathbf{AB} \in S$。
- 結合律（*associativity*）。矩陣乘法的結合律可視為已知。
- 單位元。$\det\mathbf{I} = 1$，所以 $\mathbf{I} \in S$，而且對每個 $\mathbf{A}$ 都有 $\mathbf{IA} = \mathbf{AI} = \mathbf{A}$。
- 逆元。上面求得的矩陣 $\mathbf{A}^{-1}$ 的行列式為 $wz - (-x)(-y) = wz - xy = 1$，所以它屬於 S。

因此 S 在矩陣乘法下是一個羣。

自逆元素與階為 2 的元素

把 $\mathbf{A}^{-1}$ 與 $\mathbf{A}$ 逐個元素比較，可知 $\mathbf{A}^{-1} = \mathbf{A}$ 當且僅當

$$z = w, \qquad -x = x, \qquad -y = y,$$

即 $x = y = 0$ 且 $z = w$。這時行列式條件變成 $w^2 = 1$，所以 $w = \pm 1$。因此自逆（self-inverse）元素為

$$\mathbf{A} = \mathbf{I} \quad \text{和} \quad \mathbf{A} = -\mathbf{I}.$$

當 $\mathbf{A}^2 = \mathbf{I}$（等價於 $\mathbf{A}^{-1} = \mathbf{A}$）且 $\mathbf{A} \neq \mathbf{I}$ 時，元素的階為 2。所以階為 2 的元素只有 $-\mathbf{I}$。

階為 3 的元素

記 $t = w + z$ 為 $\mathbf{A}$ 的跡。平方得

$$\mathbf{A}^2 = \begin{pmatrix} w^2 + xy & x(w+z) \\ y(w+z) & xy + z^2 \end{pmatrix}.$$

由於 $xy = wz - 1$，左上角的元素是 $w^2 + wz - 1 = tw - 1$，右下角的元素是 $tz - 1$。因此

$$\mathbf{A}^2 = t\mathbf{A} - \mathbf{I}. \tag{$*$}$$

? **想一想** $(*)$ 對計算 $\mathbf{A}^3$ 有甚麼幫助？

把 $(*)$ 乘以 $\mathbf{A}$，再用一次 $(*)$ 消去 $\mathbf{A}^2$：

$$\mathbf{A}^3 = t\mathbf{A}^2 - \mathbf{A} = t(t\mathbf{A} - \mathbf{I}) - \mathbf{A} = (t^2 - 1)\mathbf{A} - t\mathbf{I}.$$

所以 $\mathbf{A}$ 的任何次冪都是 $\mathbf{A}$ 和 $\mathbf{I}$ 的組合，我們可以比較係數。

若 $w + z + 1 = 0$：則 $t = -1$，所以 $t^2 - 1 = 0$，從而 $\mathbf{A}^3 = \mathbf{I}$。另外 $\mathbf{A} \neq \mathbf{I}$，因為 $\mathbf{I}$ 的跡是 $2 \neq -1$。$\mathbf{A}$ 的階整除 3 而又不是 1，所以是 3。

反過來，假設 $\mathbf{A}$ 的階爲 3。則 $\mathbf{A}^3 = \mathbf{I}$ 且 $\mathbf{A} \neq \mathbf{I}$，所以

$$(t^2 - 1)\mathbf{A} = (1 + t)\mathbf{I}.$$

- 若 $t^2 \neq 1$，則 $\mathbf{A} = \dfrac{1+t}{t^2-1}\mathbf{I} = \dfrac{1}{t-1}\mathbf{I}$，是單位矩陣的倍數 $\lambda\mathbf{I}$。它的行列式為 $\lambda^2 = 1$，所以 $\lambda = \pm 1$。但 $\mathbf{A} = \mathbf{I}$ 已被排除，而 $\mathbf{A} = -\mathbf{I}$ 的階是 2，不是 3。所以這個情況不可能出現。
- 若 $t = 1$，等式變成 $\mathbf{0} = 2\mathbf{I}$，這並不成立。

餘下唯一的可能是 $t = -1$，即 $w + z + 1 = 0$。這就證明了「當且僅當」(if and only if)。

一個例子。取 $w = 0$ 和 $z = -1$，並選 $x = -1$、$y = 1$，使得 $wz - xy = 0 + 1 = 1$：

$$\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \mathbf{A}^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{A}^3 = \mathbf{I}.$$

驗算

- 把上面的例子乘開，直接看出 $\mathbf{A}^3 = \mathbf{I}$。
- 旋轉 120° 的矩陣 $\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ 的行列式為 1，跡為 -1，而它的階當然是 3。
- 我們用電腦對 S 中 20 000 個隨機有理數矩陣驗證了 $\mathbf{A}^2 = t\mathbf{A} - \mathbf{I}$。我們亦搜尋了 S 中所有元素均為 $\frac{1}{2}$ 的倍數且介乎 -4 與 4 之間的矩陣：階為 3 的恰好就是跡為 -1 的那 48 個，而 $-\mathbf{I}$ 是唯一階為 2 的矩陣。

常見錯誤

- 把 $\mathbf{I}$ 算作階為 2 的元素。它是自逆的，但它的階是 1。
- 只證明了階為 3 這個結果的其中一個方向。逆命題（converse）需要排除 $t^2 \neq 1$ 和 $t = 1$ 這兩個情況。
- 驗證羣公理時，忘記檢查逆矩陣本身的行列式也是 1。

STEP 之外

羣 S 就是特殊線性羣（special linear group）SL_2，是數學中最重要的羣之一。恆等式 $\mathbf{A}^2 - (\operatorname{tr}\mathbf{A})\mathbf{A} + (\det\mathbf{A})\mathbf{I} = \mathbf{0}$ 是凱萊–哈密頓定理（Cayley–Hamilton theorem）的 2×2 情形：每個方陣都滿足它自己的特徵方程（characteristic equation）。它亦顯示出單憑跡就能告訴我們多少關於 SL_2 中元素的資訊：上面的論證可以推廣，證明階為有限數 n 的元素，其跡必為 $2\cos(2\pi k/n)$，其中 k 為某個整數。想進一步了解矩陣羣，可參閱 Allenby 的 *Rings, Fields and Groups*（環、域與羣）；至於凱萊–哈密頓定理和特徵值（eigenvalue），可參閱 Strang 的 *Introduction to Linear Algebra*（線性代數導論）。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。