詳細解答

STEP III 1989，第 3 題

純數學 • 矩陣群

STEP III 1989，第 3 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/89-s3-q3

關鍵思路

$\mathbf{M}$ 是轉角為 $2\pi/m$ 的旋轉（rotation），所以 $\mathbf{M}^m = \mathbf{I}$，而它各次冪之和是一個等比級數（geometric series）：把這個和乘以 $\mathbf{I}-\mathbf{M}$，各項便會逐一相消（telescope）。至於遞推關係（recurrence），只要寫出 $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$，規律便一目了然。之後的羣（group）全靠一條恆等式：把其中一個表達式代入另一個，結果只是把下標相加，所以這些元素的運算方式就像模（modulo）m 的整數一樣。

解答

M 的各次冪之和

$\mathbf{M}$ 是繞原點逆時針旋轉 $\theta = 2\pi/m$ 的矩陣。連續施行 k 次，就是旋轉 $k\theta$，所以

$$\mathbf{M}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}, \qquad \text{特別地} \qquad \mathbf{M}^m = \begin{pmatrix} \cos 2\pi & -\sin 2\pi \\ \sin 2\pi & \cos 2\pi \end{pmatrix} = \mathbf{I}.$$

（由於 $\mathbf{M}^{k+1} = \mathbf{M}\mathbf{M}^k$，$\mathbf{M}^k$ 的公式可用歸納法（induction）由複角公式（compound-angle formulae）推出。）

設 $\mathbf{S} = \mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1}$。這些矩陣全是 $\mathbf{M}$ 的冪，所以它們可交換（commute），而乘積中各項逐一相消：

$$(\mathbf{I}-\mathbf{M})\mathbf{S} = \mathbf{I} - \mathbf{M}^m = \mathbf{I} - \mathbf{I} = \mathbf{O}.$$

? **想一想** 我們可以直接「約去」因子 $\mathbf{I}-\mathbf{M}$ 嗎？

只有當 $\mathbf{I}-\mathbf{M}$ 可逆（invertible）時才可以：非零矩陣的乘積可以是 $\mathbf{O}$。這裏

$$\det(\mathbf{I}-\mathbf{M}) = (1-\cos\theta)^2 + \sin^2\theta = 2-2\cos\theta,$$

而由於 $m>1$，我們有 $0<\theta\le\pi$，所以 $\cos\theta\neq 1$，行列式（determinant）不等於零。在 $(\mathbf{I}-\mathbf{M})\mathbf{S}=\mathbf{O}$ 的左邊乘以 $(\mathbf{I}-\mathbf{M})^{-1}$，便得 $\mathbf{S}=\mathbf{O}$，這正是所求的結果。

$\mathbf{X}_k$ 的公式

算出最初幾項，

$$\mathbf{X}_1 = \mathbf{P}\mathbf{X}_0+\mathbf{Q},\quad \mathbf{X}_2 = \mathbf{P}^2\mathbf{X}_0+\mathbf{P}\mathbf{Q}+\mathbf{Q},\quad \mathbf{X}_3 = \mathbf{P}^3\mathbf{X}_0+(\mathbf{P}^2+\mathbf{P}+\mathbf{I})\mathbf{Q},$$

由此可猜想，對 $k\ge 0$，

$$\mathbf{X}_k = \mathbf{P}^k\mathbf{X}_0+\mathbf{S}_k\mathbf{Q},\qquad \text{其中}\quad \mathbf{S}_k = \mathbf{I}+\mathbf{P}+\cdots+\mathbf{P}^{k-1}\quad(\mathbf{S}_0=\mathbf{O}).$$

當 $k=0$ 時，這式子就是 $\mathbf{X}_0=\mathbf{X}_0$，顯然成立。假設它對某個 $k\ge 0$ 成立，則

$$\begin{aligned}\mathbf{X}_{k+1} &= \mathbf{P}\mathbf{X}_k+\mathbf{Q} = \mathbf{P}^{k+1}\mathbf{X}_0+(\mathbf{P}+\mathbf{P}^2+\cdots+\mathbf{P}^k)\mathbf{Q}+\mathbf{Q}\\ &= \mathbf{P}^{k+1}\mathbf{X}_0+\mathbf{S}_{k+1}\mathbf{Q},\end{aligned}$$

所以它對 $k+1$ 也成立，按歸納法，它對所有 $k\ge 0$ 都成立。要保持因子的次序：$\mathbf{P}$ 自始至終都是從左邊乘上去的，而 $\mathbf{P}$ 與 $\mathbf{Q}$ 不一定可交換。

羣

把 $\mathbf{X}_i$ 看成表達式 $\mathbf{P}^i\mathbf{X}_0+\mathbf{S}_i\mathbf{Q}$，即一條把任意矩陣 $\mathbf{X}_0$ 變成另一個矩陣的規則。以 $\mathbf{X}_j$ 代替 $\mathbf{X}_0$，得

$$\begin{aligned}\mathbf{X}_i * \mathbf{X}_j &= \mathbf{P}^i(\mathbf{P}^j\mathbf{X}_0+\mathbf{S}_j\mathbf{Q})+\mathbf{S}_i\mathbf{Q}\\ &= \mathbf{P}^{i+j}\mathbf{X}_0+(\mathbf{P}^i\mathbf{S}_j+\mathbf{S}_i)\mathbf{Q}.\end{aligned}$$

現在 $\mathbf{P}^i\mathbf{S}_j = \mathbf{P}^i+\cdots+\mathbf{P}^{i+j-1}$，再加上 $\mathbf{S}_i=\mathbf{I}+\cdots+\mathbf{P}^{i-1}$，剛好就是 $\mathbf{S}_{i+j}$。所以，對任意 $\mathbf{P}$，

$$\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}.$$

（這並不令人意外：先按遞推關係走 j 步，再多走 i 步，就是走了 $i+j$ 步。）

現在取 $\mathbf{P}=\mathbf{M}$。由第一部分，$\mathbf{M}^m=\mathbf{I}$ 且 $\mathbf{S}_m=\mathbf{O}$，所以

$$\mathbf{X}_m = \mathbf{X}_0,$$

也就是說，$\mathbf{X}_m$ 是令每個矩陣保持不變的表達式。於是對任意 k，$\mathbf{X}_{k+m}=\mathbf{X}_k*\mathbf{X}_m=\mathbf{X}_k$，所以這列表達式以週期 m 重複出現，而

$$G=\{\mathbf{X}_1,\mathbf{X}_2,\mathbf{X}_3,\ldots\}=\{\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_m\}$$

是一個有限集。我們逐一檢驗羣公理。

- 封閉性（*closure*）。$\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}$，而 $i+j \geq 1$，所以它屬於 G。
- 結合律（*associativity*）。$(\mathbf{X}_i * \mathbf{X}_j) * \mathbf{X}_k$ 與 $\mathbf{X}_i * (\mathbf{X}_j * \mathbf{X}_k)$ 都等於 $\mathbf{X}_{i+j+k}$。（更一般地說，代入就是函數的複合，而函數的複合必定滿足結合律。）
- 單位元（*identity*）。$\mathbf{X}_m * \mathbf{X}_j = \mathbf{X}_{m+j} = \mathbf{X}_j$ 且 $\mathbf{X}_j * \mathbf{X}_m = \mathbf{X}_j$，所以 $\mathbf{X}_m$ 是單位元。
- 逆元（*inverses*）。對 $1 \leq i < m$，$\mathbf{X}_i * \mathbf{X}_{m-i} = \mathbf{X}_{m-i} * \mathbf{X}_i = \mathbf{X}_m$，而 $\mathbf{X}_m$ 的逆元就是它自己。每個逆元都屬於 G。

所以 G 在運算 $*$ 下是一個有限羣。

事實上，它剛好有 m 個元素：$\mathbf{X}_1, \ldots, \mathbf{X}_m$ 是互不相同的表達式，因為它們的係數 $\mathbf{M}^1, \ldots, \mathbf{M}^m$ 是轉角各不相同的旋轉，轉角都在 $(0, 2\pi]$ 之內。由於每個元素都是 $\mathbf{X}_1$ 的「冪」，G 就是階（order）為 m 的循環羣（cyclic group）。

驗算

- 當 $m = 2$ 時，$\mathbf{M} = -\mathbf{I}$，和為 $\mathbf{I} + (-\mathbf{I}) = \mathbf{O}$。當 $m = 4$ 時，$\mathbf{M}$ 是四分之一圈的旋轉，而 $\mathbf{I} + \mathbf{M} + \mathbf{M}^2 + \mathbf{M}^3 = \mathbf{I} + \mathbf{M} - \mathbf{I} - \mathbf{M} = \mathbf{O}$。
- 以數值計算，對由 2 至 39 的每個 m，各次冪之和都是 $\mathbf{O}$（在捨入誤差之內）；對隨機選取的 $\mathbf{P}$、$\mathbf{Q}$、$\mathbf{X}_0$，$\mathbf{X}_k$ 的公式與遞推關係吻合；而當 $\mathbf{P} = \mathbf{M}$，$\mathbf{Q}$ 和 $\mathbf{X}_0$ 隨機選取時，按遞推關係走 m 步後剛好回到 $\mathbf{X}_0$。

常見錯誤

- 沒有檢查 $\mathbf{I} - \mathbf{M}$ 是否可逆便把它約去。
- 寫成 $\mathbf{Q}\mathbf{S}_k$ 或 $\mathbf{X}_0\mathbf{P}^k$：矩陣乘法不可交換，而遞推關係中 $\mathbf{P}$ 是放在左邊的。
- 把 $\mathbf{X}_0$ 當作單位元：按題目所列，$\mathbf{X}_0$ 並不在 G 之內；單位元是 $\mathbf{X}_m$，它之所以等於 $\mathbf{X}_0$，全因 $\mathbf{S}_m = \mathbf{O}$。

STEP 之外

每個 $\mathbf{X}_i$ 都是一個仿射映射（*affine map*）$\mathbf{X} \mapsto \mathbf{A}\mathbf{X} + \mathbf{B}$，而 $\mathbf{A}$ 可逆的仿射映射在複合運算下構成一個羣；這裏我們找到的是一個階為 m 的循環子羣（cyclic subgroup），它由單獨一個映射生成，而這個映射的 m 次冪是單位元。$\mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1} = \mathbf{O}$ 這個事實，正是「m 次單位根（roots of unity）之和為零」的矩陣版本；而背後的一般想法，即

一個羣以變換的方式作用於一個集合，是大學第一門羣論（group theory）課程的核心。Allenby 的 *Rings, Fields and Groups* 對此有詳細闡述。

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。