詳細解答

STEP II 1991，第 9 題

純數學 • 矩陣群

> **STEP II 1991，第 9 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/91-s2-q9

關鍵思路

一切都建基於一個事實：模 5 的整數構成一個域（field）。每個非零剩餘（residue）都有乘法逆元（multiplicative inverse），而非零剩餘之積永不為零。正因如此，對角線上的元素才會規規矩矩，封閉性和逆元幾乎是不費工夫就得到的。至於最後一部分，可解 $M^2 = I$，把階（order）為 1 或 2 的元素明確地找出來，然後檢驗其中兩個相乘之後是否仍留在該集合之內。

解答

以下所有運算均以模 5 進行，並在方便時把 4 寫成 -1。我們把一般的元素寫成

$$M(a,b,c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \qquad a,c \in \{1,2,3,4\},\ b \in \{0,1,2,3,4\}.$$

G 是一個羣

封閉性（closure）。把兩個元素相乘，得

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}.$$

這是一個上三角矩陣（upper triangular matrix），各元素均為模 5 的數。它的對角線元素 ad 和 cf 都不是零：由於 5 是質數，若 $5 \mid ad$，則 $5 \mid a$ 或 $5 \mid d$，但兩者皆不成立。所以這個積屬於 G。

結合律（associativity）是已知的，因為矩陣乘法符合結合律。

單位元（identity）。$I = M(1,0,1)$ 屬於 G，而且對每個 M 都有 $IM = MI = M$。

逆元（inverses）。每個模 5 的非零剩餘都有逆元（$1^{-1}=1$，$2^{-1}=3$，$3^{-1}=2$，$4^{-1}=4$）。所以，給定 $M(a,b,c)\in G$，我們可以構造

$$N=\begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix},$$

由於 $a^{-1},c^{-1}\neq 0$，它屬於 G。利用上面的乘積公式，

$$MN=\begin{pmatrix} aa^{-1} & -aa^{-1}bc^{-1}+bc^{-1} \\ 0 & cc^{-1} \end{pmatrix}=I, \qquad NM=\begin{pmatrix} a^{-1}a & a^{-1}b-a^{-1}bc^{-1}c \\ 0 & c^{-1}c \end{pmatrix}=I.$$

所以每個元素在 G 中都有逆元，因此 G 是一個羣（group）。

G 的階

a 有 4 個選擇，b 有 5 個，c 有 4 個，而不同的選擇給出不同的矩陣。所以

$$|G|=4\times 5\times 4=80.$$

G 是否可交換？

不是。取 $A=M(1,1,1)$ 和 $B=M(2,0,1)$。則

$$AB=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}2&0\\0&1\end{pmatrix}=\begin{pmatrix}2&1\\0&1\end{pmatrix}, \qquad BA=\begin{pmatrix}2&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}2&2\\0&1\end{pmatrix},$$

所以 $AB\neq BA$，G 不是可交換（commutative）的。

階為 1 或 2 的元素

元素 M 的階為 1 或 2，當且僅當 $M^2=I$。由乘積公式，

$$M(a,b,c)^2=\begin{pmatrix} a^2 & b(a+c) \\ 0 & c^2 \end{pmatrix},$$

所以我們需要 $a^2=1$、$c^2=1$ 以及 $b(a+c)=0$。

$1,2,3,4$ 在模 5 下的平方分別是 $1,4,4,1$，所以 $a^2=1$ 必然得出 $a=\pm 1$，同理 $c=\pm 1$。

- 若 $a=c$，則 $a+c=\pm 2\neq 0$。由於 $\mathbb{Z}_5$ 沒有零因子（zero divisor），$b(a+c)=0$ 必然得出 $b=0$。這給出 I 和 $-I$。
- 若 $c=-a$，則 $a+c=0$，所以 b 可取任何值。這給出 10 個矩陣 $M(1,b,-1)$ 和 $M(-1,b,1)$，其中 $b=0,1,\ldots,4$。

所以，由階為 1 或 2 的元素組成的集合 H 恰好有 12 個成員。

想一想 由自逆元素組成的集合，是否必定封閉？

不是。這個集合包含 I，而且每個元素都是自己的逆元，所以單位元和逆元這兩條公理自動成立。唯一可能不成立的是封閉性，而在非交換羣中它通常都不成立：若 $X^2 = Y^2 = I$，則 $(XY)^2 = XYXY$，除非 X 與 Y 可交換，否則這未必能化簡為 I。

在這裏它確實不成立。取 $X = M(1,1,-1)$ 和 $Y = M(1,0,-1)$，兩者都屬於 H。則

$$XY = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

這個矩陣有 $a = c = 1$ 但 $b = -1 \neq 0$，所以按上面的分類，它不屬於 H。（事實上 $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$，所以它的階是 5。）因此 H 並不封閉，它不是 G 的子羣（subgroup）。

如果你認識拉格朗日定理（Lagrange's theorem），還有一個更快捷的論證：子羣的階必須整除羣的階，而 $12 \nmid 80$。

驗算

用電腦把全部 80 個矩陣簡單枚舉一遍，可確認封閉性、逆元公式，以及上述那對矩陣的 $AB \neq BA$。把每個元素平方，找到的正好是預測中 $M^2 = I$ 的 12 個解，而 $XY = M(1,4,1)$ 的階是 5。用手算可驗證 $M(-1,3,1)^2 = I$：非對角線元素是 $3(-1+1) = 0$。

常見錯誤

- 忘記證明逆元屬於 G。它的對角線元素 a^{-1}、c^{-1} 必須不是零。
- 以為 $M^2 = I$ 必然令 M 是對角矩陣，因而漏掉 $b \neq 0$ 的元素 $M(1,b,-1)$ 和 $M(-1,b,1)$。
- 只為 H 檢驗單位元和逆元這兩條公理。不成立的正是封閉性這條公理。

STEP 之外

G 是有限域（finite field）$\mathbb{F}_5$ 上所有可逆 2×2 上三角矩陣組成的羣，是 $\mathrm{GL}_2(\mathbb{F}_5)$ 的一個博雷爾子羣（*Borel subgroup*）。滿足 $a = c = 1$ 的矩陣構成一個階為 5 的正規子羣（normal subgroup），而 G 是由它與對角矩陣以半直積（semidirect product）的方式構成的。有限域上的矩陣羣，是羣論入門課程中豐富的例子來源。想了解更多，可參閱 Allenby, *Rings, Fields and Groups*（環、域與羣）。

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。