詳細解答

STEP III 1995，第 7 題

純數學 • 群與同構

> **STEP III 1995，第 7 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/95-s3-q7

關鍵思路

結合律（associativity）已經給定，所以對每個集合只需檢查三件事：封閉性（closure）、單位元（identity），以及每個元素都有逆元（inverse）。只要其中一項不成立，該集合就不是羣（group），而且舉出一個明確的反例便已足夠。至於同構（isomorphism），則要找出任何同構都必須保持的結構特徵：元素的個數，以及各元素的階（order）。

解答

以下所說的「乘法」，視乎情況而定，分別指複數的普通乘法、模（modulo）n 乘法，或矩陣乘法。

第 (i) 部分

設 $S = \{z \in \mathbb{C} : |z| = 1\}$。

- 封閉性：若 $|z| = |w| = 1$，則 $|zw| = |z||w| = 1$。
- 單位元：$1 \in S$，且 $1z = z1 = z$。
- 逆元：若 $|z| = 1$，則 $z \neq 0$，而 $z^{-1} = \bar{z}$（因為 $z\bar{z} = |z|^2 = 1$），其模（modulus）同樣是 1。

所以 S 是一個羣（而且是無限羣）。

第 (ii) 部分

在模 4 乘法之下，集合 $\{0,1,2,3\}$ 是封閉的，並有單位元 1，但 0 沒有逆元，因為對任何 b 都有 $0\times b\equiv 0\not\equiv 1$。所以它不是羣。（即使把 0 拿走也無補於事：2 仍然沒有逆元，因為 $2b$ 必為偶數；事實上 $2\times 2\equiv 0$，所以 $\{1,2,3\}$ 連封閉性也不具備。）

第 (iii) 部分

利用複角公式（compound-angle formulae），

$$\mathrm{M}(\alpha)\mathrm{M}(\beta)=\begin{pmatrix} c_\alpha c_\beta - s_\alpha s_\beta & -(s_\alpha c_\beta + c_\alpha s_\beta) \\ s_\alpha c_\beta + c_\alpha s_\beta & c_\alpha c_\beta - s_\alpha s_\beta \end{pmatrix} = \mathrm{M}(\alpha+\beta),$$

其中 $c_\alpha=\cos\alpha$，$s_\alpha=\sin\alpha$，如此類推。由於 cos 和 sin 的週期為 2π，故 $\mathrm{M}(\alpha+\beta)=\mathrm{M}(\gamma)$，其中 γ 是把 $\alpha+\beta$ 約化至 $[0,2\pi)$ 內所得的角。因此：

- *封閉性*：集合中兩個矩陣的積仍在集合之內。
- *單位元*：$\mathrm{M}(0)=I$。
- *逆元*：當 $0<\theta<2\pi$ 時，$\mathrm{M}(\theta)\mathrm{M}(2\pi-\theta)=\mathrm{M}(2\pi)=I$；而 $\mathrm{M}(0)$ 的逆元就是它自己。

所以這個集合是一個羣。

第 (iv) 部分

模 8 之下，

$$3^2=9\equiv 1,\qquad 5^2=25\equiv 1,\qquad 7^2=49\equiv 1,$$
$$3\times 5=15\equiv 7,\qquad 3\times 7=21\equiv 5,\qquad 5\times 7=35\equiv 3.$$

連同涉及 1 的平凡乘積，這就給出了整個乘法表（乘法滿足交換律（commutative）），而每個乘積都在 $\{1,3,5,7\}$ 之內，所以集合是封閉的。單位元是 1，而每個元素的逆元都是它自己。所以這是一個羣，階為 4，其中除 1 以外每個元素的階都是 2。

第 (v) 部分

單位矩陣 I 的元素都是整數，而且集合是封閉的（整數的積與和仍是整數），但逆元這一項不成立。零矩陣根本沒有逆矩陣。即使是可逆矩陣也可能出問題：$A=\begin{pmatrix}2&0\\0&1\end{pmatrix}$ 在實矩陣中的逆矩陣是 $\begin{pmatrix}\frac{1}{2}&0\\0&1\end{pmatrix}$，而逆矩陣是唯一的，所以 A 沒有元素全為整數的逆矩陣。所以這個集合不是羣。

想一想 單單指出零矩陣真的足夠嗎？還是需要就所有矩陣說明一下？

只要有一個元素沒有逆元，就足以證明該集合不是羣。第二個例子則說明，問題並不止於奇異矩陣（singular matrix）。一個整數矩陣有整數逆矩陣，當且僅當它的行列式（determinant）是 ± 1，因為 $\det A \det A^{-1} = 1$，而兩個行列式都是整數。若只考慮這些矩陣，便確實得到一個羣。

第 (vi) 部分

模 5 之下，2 的各次冪是

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 3, \quad 2^4 = 16 \equiv 1.$$

所以 $\{1,2,3,4\} = \{2^0, 2^1, 2^2, 2^3\}$，而 $2^a 2^b = 2^{a+b}$，其中指數按模 4 計算。因此集合是封閉的，1 是單位元，而 2^a 的逆元是 2^{4-a}。它是一個羣：階為 4 的循環羣（cyclic group），由 2（或由 3）生成。

同構

是羣的有 (i)、(iii)、(iv) 和 (vi)，共可組成六對。

(i) 與 (iii) 同構。每個單位複數都可以唯一地寫成 $\mathrm{e}^{\mathrm{i}\theta}$，其中 $0 \leq \theta < 2\pi$。定義 $\phi(\mathrm{e}^{\mathrm{i}\theta}) = \mathrm{M}(\theta)$。這是一個雙射（bijection），因為 $[0, 2\pi)$ 內不同的 θ 給出不同的矩陣（第一列 $(\cos\theta, \sin\theta)$ 已決定了 θ）。它也保持乘法：$\mathrm{e}^{\mathrm{i}\alpha}\mathrm{e}^{\mathrm{i}\beta} = \mathrm{e}^{\mathrm{i}(\alpha+\beta)}$ 及 $\mathrm{M}(\alpha)\mathrm{M}(\beta) = \mathrm{M}(\alpha+\beta)$，而在兩個羣中，角都是按模 2π 約化的。從幾何角度看，兩個羣都是平面繞原點的旋轉。

(i) 或 (iii) 與 (iv) 或 (vi)：不同構。同構是雙射，所以兩個羣的元素個數必須相同。羣 (i) 和 (iii) 是無限的，而 (iv) 和 (vi) 各有四個元素。這樣就排除了四對。

想一想 (iv) 和 (vi) 都有四個元素，而且都滿足交換律。有甚麼可以把它們區分開來？

(iv) 與 (vi)：不同構。同構 ϕ 保持每個元素的階：$\phi(g)^n = \phi(g^n)$，而它等於單位元當且僅當 g^n 是單位元，因為 ϕ 是單射（injective），並把單位元映到單位元。在 (vi) 中，元素 2 的階是 4。在 (iv) 中，每個元素 g 都滿足 $g^2 = 1$，所以沒有元素的階是 4。因此不存在同構。

總括而言，唯一同構的一對是 (i) 和 (iii)。

驗算

我們用電腦對 (iv) 和 (vi) 的乘法表逐一窮舉，確認了封閉性、單位元和逆元三項性質。電腦亦發現，模 4 之下 0 和 2 沒有逆元，而元素的階在 (iv) 中是 $1,2,2,2$，在 (vi) 中是 $1,4,4,2$（依次對應 $1,2,3,4$）。它還在 10^4 個隨機角上驗證了 $\mathrm{M}(\alpha)\mathrm{M}(\beta) = \mathrm{M}(\alpha+\beta)$ 以及與 $\mathrm{e}^{i\theta}$ 的對應關係。(iv) 可以很快用手算驗證：任何奇數的平方在模 8 之下都是 1，因為 $(2k+1)^2 = 4k(k+1)+1$，而 $k(k+1)$ 是偶數。

常見錯誤

- 說 (iv) 和 (vi) 同構，「因為兩者都有四個元素」。元素個數相等是必要條件，但並非充分條件。
- 在 (v) 中只檢查 $\det A \neq 0$。逆矩陣的元素也必須全為整數。
- 把 (ii) 誤讀成模 4 加法。在加法之下，它會是一個階為 4 的循環羣，與 (vi) 同構，但題目指明的是乘法。

STEP 之外

在同構意義下，階為 4 的羣恰好只有兩個：循環羣 C_4，即 (vi)；以及克萊因四元羣（Klein four-group）$C_2 \times C_2$，即 (iv)。按元素的階把小階數的羣分類，是大學羣論課程最先處理的課題之一。(i) 和 (iii) 的圓羣（circle group）是李羣（Lie group）最簡單的例子；李羣是指同時也是光滑曲線或曲面的羣。(v) 中行列式為 ± 1 的整數矩陣構成羣 $\mathrm{GL}_2(\mathbb{Z})$，它在數論中十分重要。想進一步了解，Allenby 的 *Rings, Fields and Groups* 是一本很好的讀物。

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。