詳細解答

STEP III 1993，第 5 題

純數學 • 群與四元數

> **STEP III 1993，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/93-s3-q5

本題在 *Beyond STEP* 第 6.7 節四元數章中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch06/quaternions.html

關鍵思路

這個運算看似隨意，但第一部分的四個乘積顯示了它的結構：形如 $(z,0)$ 的數對相乘時與普通複數（complex number）無異，而第二個位置則像一個滿足 $j^2=-1$ 的新符號 j，凡被它越過的數都會變成共軛（conjugate）。有了這四個乘積，S_1 的八個元素就只是 $(u,0)$ 和 $(0,u)$，其中 $u\in\{1,i,-1,-i\}$。因此，封閉性（closure）、逆元（inverse）和階（order）都可由幾行一般的論證得出，毋須列出有 64 項的運算表。

解答

結合律與交換律

記 $z=(z_1,z_2)$、$w=(w_1,w_2)$、$u=(u_1,u_2)$。以下會一直用到 $(ab)^*=a^*b^*$、$(a\pm b)^*=a^*\pm b^*$ 和 $a^{**}=a$。首先，

$$z\circ w=(z_1w_1-z_2w_2^*,\ z_1w_2+z_2w_1^*),$$

所以 $(z\circ w)\circ u$ 的兩個分量是

$$(z_1w_1-z_2w_2^*)u_1-(z_1w_2+z_2w_1^*)u_2^*=z_1w_1u_1-z_1w_2u_2^*-z_2w_1^*u_2^*-z_2w_2^*u_1,$$
$$(z_1w_1-z_2w_2^*)u_2+(z_1w_2+z_2w_1^*)u_1^*=z_1w_1u_2+z_1w_2u_1^*+z_2w_1^*u_1^*-z_2w_2^*u_2.$$

另一方面，$w \circ u = (w_1u_1 - w_2u_2^*,\ w_1u_2 + w_2u_1^*)$，所以 $z \circ (w \circ u)$ 的兩個分量是

$$z_1(w_1u_1 - w_2u_2^*) - z_2(w_1u_2 + w_2u_1^*)^* = z_1w_1u_1 - z_1w_2u_2^* - z_2w_1^*u_2^* - z_2w_2^*u_1,$$
$$z_1(w_1u_2 + w_2u_1^*) + z_2(w_1u_1 - w_2u_2^*)^* = z_1w_1u_2 + z_1w_2u_1^* + z_2w_1^*u_1^* - z_2w_2^*u_2.$$

兩組右式逐項相同，所以 $\circ$ 滿足結合律（associative）。

它並不滿足交換律（commutative）。例如，

$$(0,1) \circ (i,0) = (0-0,\ 0+1\cdot i^*) = (0,-i), \qquad (i,0) \circ (0,1) = (0-0,\ i\cdot 1+0) = (0,i).$$

四個乘積

把零代入定義，得

$$(z,0) \circ (w,0) = (zw,\ 0), \qquad (z,0) \circ (0,w) = (0,\ zw),$$
$$(0,z) \circ (w,0) = (0,\ zw^*), \qquad (0,z) \circ (0,w) = (-zw^*,\ 0).$$

集合 S_1

設 $U = \{1, i, -1, -i\}$。那麼

$$S_1 = \{(u,0) : u \in U\} \cup \{(0,u) : u \in U\},$$

其中 A, C, E, G 屬第一類，B, D, F, H 屬第二類。

封閉性。集合 U 在乘法、取複共軛（$i^* = -i$）和取負之下都是封閉的。根據四個乘積，S_1 中兩個元素的乘積是 $(zw,0)$、$(0,zw)$、$(0,zw^*)$ 或 $(-zw^*,0)$，其中 $z, w \in U$。zw 和 $\pm zw^*$ 都屬於 U，所以每個乘積都屬於 S_1。

單位元（identity）。對任意 $(w_1,w_2) \in S$，

$$(1,0) \circ (w_1,w_2) = (w_1,\ w_2), \qquad (w_1,w_2) \circ (1,0) = (w_1,\ w_2 \cdot 1^*) = (w_1,w_2),$$

所以 $A = (1,0)$ 是雙邊單位元，而且它屬於 S_1。

逆元與階。對第一類元素，$(z,0) \circ (w,0) = (zw,0)$，所以它們的表現與 U 中的複數完全一樣。因此 A 的階是 1，逆元是它本身；$E = (-1,0)$ 的階是 2，逆元是它本身；$C = (i,0)$ 和 $G = (-i,0)$ 的階都是 4，並且互為逆元。

想一想 第二類元素的平方是甚麼？

根據四個乘積中的最後一個，對 $u \in U$，

$$(0,u) \circ (0,u) = (-uu^*,\ 0) = (-|u|^2,\ 0) = (-1,0) = E.$$

所以 B, D, F, H 的平方都是 E。由於 E 的階是 2，這四個元素的階都是 4。至於逆元，$(0,u)\circ(0,w) = (-uw^*, 0)$ 等於 $(1,0)$，當且僅當 $w^* = -1/u = -u^*$（用到 $uu^* = 1$），即 $w = -u$。再檢查另一個次序，$(0,-u)\circ(0,u) = (uu^*, 0) = (1,0)$ 同樣成立。所以 $(0,u)$ 的逆元是 $(0,-u)$。

總結如下：

元素	A	B	C	D	E	F	G	H
逆元	A	F	G	H	E	B	C	D
階	1	4	4	4	2	4	4	4

羣（group）。至此四條公理都已齊備。S_1 在 $\circ$ 之下封閉。這個運算在整個 S 上滿足結合律，在 S_1 上自然也滿足。$A \in S_1$ 是單位元，而且每個元素在 S_1 中都有逆元。所以 S_1 在 $\circ$ 之下是一個羣，階為 8。它不是阿貝爾羣（abelian group）：$B\circ C = H$，但 $C\circ B = D$。

子羣與矩陣

利用以上的乘積，$B = (0,1)$ 的各次冪是

$$B^2 = E, \qquad B^3 = E\circ B = (-1,0)\circ(0,1) = (0,-1) = F, \qquad B^4 = E\circ E = A.$$

所以 $\{A, B, E, F\} = \{B^0, B^1, B^2, B^3\}$ 是由 B 生成的循環子羣（cyclic subgroup）。它是封閉的，因為 $B^m \circ B^n = B^{m+n}$，而指數可以模 4 化簡；它也包含 A，以及每個 B^k 的逆元 B^{4-k}。所以它是一個階為 4 的子羣。

設 $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$。那麼

$$M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad M^3 = -M, \qquad M^4 = I,$$

所以由 M 生成的羣是 $\{I, M, -I, -M\}$，同樣是階為 4 的循環羣。任何兩個同階的循環羣都是同構（isomorphic）的。這裏的映射

$$A \mapsto I, \quad B \mapsto M, \quad E \mapsto -I, \quad F \mapsto -M,$$

即 $B^k \mapsto M^k$，是一個雙射（bijection），並且滿足 $B^m \circ B^n = B^{m+n} \mapsto M^{m+n} = M^m M^n$。所以這兩個羣*確實*同構。

驗算

► 元素的階整除羣的階：1, 2, 4 這些階全都整除 8；對於子羣，2 和 4 都整除 4。

- 從複數的角度看：$(z,0)\circ(w,0) = (zw,0)$，所以 $C\circ C = (i^2,0) = E$，正好對應 $i^2=-1$。
- 用電腦作了簡短的核對：以 10 000 組隨機的複數對三元組驗證了結合律；建立了完整的 8×8 運算表，確認了封閉性、單位元、上述的逆元和階，以及 $B\circ C = H \neq D = C\circ B$；並確認了 $B^k \mapsto M^k$ 保持乘法。

常見錯誤

- 忘記取共軛：$(0,z)\circ(w,0)$ 是 $(0,zw^*)$，不是 $(0,zw)$。不可交換性正是由此而來。
- 只用一個數值例子來說明結合律成立。一個例子可以說明某條定律*不成立*，但要證明它成立，就必須作一般的展開。
- 因為一個羣由複數對組成、另一個由矩陣組成，就斷定兩者「不同構」。同構關乎乘法的結構，而不是元素本身是甚麼。

STEP 之外

這個運算就是哈密頓（Hamilton）的*四元數*（quaternion）乘法。數對 (z_1,z_2) 代表 $z_1+z_2 j$，其中 $j^2=-1$ 而 $jz = z^* j$。羣 S_1 就是*四元數羣*（quaternion group）$Q_8=\{\pm 1,\pm i,\pm j,\pm k\}$。它是每個子羣都是正規子羣（normal subgroup）的最小非阿貝爾羣，而它與另一個階為 8 的非阿貝爾羣（正方形的對稱羣）的分別，在於它只有一個階為 2 的元素。Allenby 的 *Rings, Fields and Groups*（環、域與羣）涵蓋了低階羣和四元數。

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。