详细解答

STEP III 1993，第 5 题

纯数学 · 群与四元数

STEP III 1993，第 5 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

step.maths.org/questions/93-s3-q5

本题在 *Beyond STEP* 第 6.7 节四元数群中有完整的引导式讲解：https://beyondstep.keithmcnulty.org/zh-hans/ch06/quaternions.html

关键思路

这个运算看似随意，但第一部分的四个乘积显示了它的结构：形如 $(z,0)$ 的数对相乘时与普通复数（complex number）无异，而第二个位置则像一个满足 $j^2=-1$ 的新符号 j，凡被它越过的数都会变成共轭（conjugate）。有了这四个乘积，S_1 的八个元素就只是 $(u,0)$ 和 $(0,u)$，其中 $u\in\{1,i,-1,-i\}$。因此，封闭性（closure）、逆元（inverse）和阶（order）都可由几行一般的论证得出，毋须列出有 64 项的运算表。

解答

结合律与交换律

记 $z=(z_1,z_2)$、$w=(w_1,w_2)$、$u=(u_1,u_2)$。以下会一直用到 $(ab)^*=a^*b^*$、$(a\pm b)^*=a^*\pm b^*$ 和 $a^{**}=a$。首先，

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

所以 $(z\circ w)\circ u$ 的两个分量是

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

另一方面，$w \circ u = (w_1u_1 - w_2u_2^*,\ w_1u_2 + w_2u_1^*)$，所以 $z \circ (w \circ u)$ 的两个分量是

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

两组右式逐项相同，所以 $\circ$ 满足结合律（associative）。

它并不满足交换律（commutative）。例如，

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

四个乘积

把零代入定义，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

设 $U = \{1, i, -1, -i\}$。那么

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

其中 A, C, E, G 属第一类，B, D, F, H 属第二类。

封闭性。集合 U 在乘法、取复共轭（$i^* = -i$）和取负之下都是封闭的。根据四个乘积，S_1 中两个元素的乘积是 $(zw,0)$、$(0,zw)$、$(0,zw^*)$ 或 $(-zw^*,0)$，其中 $z, w \in U$。zw 和 $\pm zw^*$ 都属于 U，所以每个乘积都属于 S_1。

单位元（identity）。对任意 $(w_1,w_2) \in S$，

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

所以 $A = (1,0)$ 是双边单位元，而且它属于 S_1。

逆元与阶。对第一类元素，$(z,0) \circ (w,0) = (zw,0)$，所以它们的表现与 U 中的复数完全一样。因此 A 的阶是 1，逆元是它本身；$E = (-1,0)$ 的阶是 2，逆元是它本身；$C = (i,0)$ 和 $G = (-i,0)$ 的阶都是 4，并且互为逆元。

想一想 第二类元素的平方是甚么？

根据四个乘积中的最后一个，对 $u \in U$，

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

所以 B, D, F, H 的平方都是 E。由于 E 的阶是 2，这四个元素的阶都是 4。至于逆元，$(0,u)\circ(0,w)=(-uw^*,0)$ 等于 $(1,0)$，当且仅当 $w^*=-1/u=-u^*$（用到 $uu^*=1$），即 $w=-u$。再检查另一个次序，$(0,-u)\circ(0,u)=(uu^*,0)=(1,0)$ 同样成立。所以 $(0,u)$ 的逆元是 $(0,-u)$。

总结如下：

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

群（group）。至此四条公理都已齐备。S_1 在 $\circ$ 之下封闭。这个运算在整个 S 上满足结合律，在 S_1 上自然也满足。$A\in S_1$ 是单位元，而且每个元素在 S_1 中都有逆元。所以 S_1 在 $\circ$ 之下是一个群，阶为 8。它不是阿贝尔群（abelian group）：$B\circ C=H$，但 $C\circ B=D$。

子群与矩阵

利用以上的乘积，$B=(0,1)$ 的各次幂是

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

所以 $\{A,B,E,F\}=\{B^0,B^1,B^2,B^3\}$ 是由 B 生成的循环子群（cyclic subgroup）。它是封闭的，因为 $B^m\circ B^n=B^{m+n}$，而指数可以模 4 化简；它也包含 A，以及每个 B^k 的逆元 B^{4-k}。所以它是一个阶为 4 的子群。

设 $M=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$。那么

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

所以由 M 生成的群是 $\{I,M,-I,-M\}$，同样是阶为 4 的循环群。任何两个同阶的循环群都是同构（isomorphic）的。这里的映射

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

即 $B^k\mapsto M^k$，是一个双射（bijection），并且满足 $B^m\circ B^n=B^{m+n}\mapsto M^{m+n}=M^mM^n$。所以这两个群确实同构。

验算

▶ 元素的阶整除群的阶：1, 2, 4 这些阶全都整除 8；对于子群，2 和 4 都整除 4。

- 从复数的角度看：$(z,0)\circ(w,0)=(zw,0)$，所以 $C\circ C=(i^2,0)=E$，正好对应 $i^2=-1$。
- 用电脑作了简短的核对：以 10 000 组随机的复数对三元组验证了结合律；建立了完整的 8×8 运算表，确认了封闭性、单位元、上述的逆元和阶，以及 $B\circ C=H\neq D=C\circ B$；并确认了 $B^k\mapsto M^k$ 保持乘法。

常见错误

- 忘记取共轭：$(0,z)\circ(w,0)$ 是 $(0,zw^*)$，不是 $(0,zw)$。不可交换性正是由此而来。
- 只用一个数值例子来说明结合律成立。一个例子可以说明某条定律*不成立*，但要证明它成立，就必须作一般的展开。
- 因为一个群由复数对组成、另一个由矩阵组成，就断定两者“不同构”。同构关乎乘法的结构，而不是元素本身是甚么。

STEP 之外

这个运算就是哈密顿（Hamilton）的*四元数*（quaternion）乘法。数对 (z_1,z_2) 代表 z_1+z_2j，其中 $j^2=-1$ 而 $jz=z^*j$。群 S_1 就是*四元数群*（quaternion group）$Q_8=\{\pm 1,\pm i,\pm j,\pm k\}$。它是每个子群都是正规子群（normal subgroup）的最小非阿贝尔群，而它与另一个阶为 8 的非阿贝尔群（正方形的对称群）的分别，在于它只有一个阶为 2 的元素。Allenby 的 *Rings, Fields and Groups*（环、域与群）涵盖了低阶群和四元数。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。