详细解答

STEP III 1995，第 7 题

纯数学 · 群与同构

> **STEP III 1995，第 7 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/95-s3-q7

关键思路

结合律（associativity）已经给定，所以对每个集合只需检查三件事：封闭性（closure）、单位元（identity），以及每个元素都有逆元（inverse）。只要其中一项不成立，该集合就不是群（group），而且举出一个明确的反例便已足够。至于同构（isomorphism），则要找出任何同构都必须保持的结构特征：元素的个数，以及各元素的阶（order）。

解答

以下所说的“乘法”，视乎情况而定，分别指复数的普通乘法、模（modulo）n 乘法，或矩阵乘法。

第 (i) 部分

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

- 封闭性：若 $|z| = |w| = 1$，则 $|zw| = |z||w| = 1$。
- 单位元：$1 \in S$，且 $1z = z1 = z$。
- 逆元：若 $|z| = 1$，则 $z \neq 0$，而 $z^{-1} = \bar{z}$（因为 $z\bar{z} = |z|^2 = 1$），其模（modulus）同样是 1。

所以 S 是一个群（而且是无限群）。

第 (ii) 部分

在模 4 乘法之下，集合 $\{0,1,2,3\}$ 是封闭的，并有单位元 1，但 0 没有逆元，因为对任何 b 都有 $0\times b\equiv 0\not\equiv 1$。所以它不是群。（即使把 0 拿走也无补于事：2 仍然没有逆元，因为 $2b$ 必为偶数；事实上 $2\times 2\equiv 0$，所以 $\{1,2,3\}$ 连封闭性也不具备。）

第 (iii) 部分

利用复角公式（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 $c_\alpha=\cos\alpha, s_\alpha=\sin\alpha$，如此类推。由于 cos 和 sin 的周期为 2π，故 $\mathrm{M}(\alpha+\beta)=\mathrm{M}(\gamma)$，其中 γ 是把 $\alpha+\beta$ 约化至 $[0,2\pi)$ 内所得的角。因此：

- 封闭性：集合中两个矩阵的积仍在集合之内。
- 单位元：$\mathrm{M}(0)=I$。
- 逆元：当 $0<\theta<2\pi$ 时，$\mathrm{M}(\theta)\mathrm{M}(2\pi-\theta)=\mathrm{M}(2\pi)=I$；而 $\mathrm{M}(0)$ 的逆元就是它自己。

所以这个集合是一个群。

第 (iv) 部分

模 8 之下，

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

连同涉及 1 的平凡乘积，这就给出了整个乘法表（乘法满足交换律（commutative）），而每个乘积都在 $\{1,3,5,7\}$ 之内，所以集合是封闭的。单位元是 1，而每个元素的逆元都是它自己。所以这是一个群，阶为 4，其中除 1 以外每个元素的阶都是 2。

第 (v) 部分

单位矩阵 I 的元素都是整数，而且集合是封闭的（整数的积与和仍是整数），但逆元这一项不成立。零矩阵根本没有逆矩阵。即使是可逆矩阵也可能出问题：$A=\begin{pmatrix}2&0\\0&1\end{pmatrix}$ 在实矩阵中的逆矩阵是 $\begin{pmatrix}\frac{1}{2}&0\\0&1\end{pmatrix}$，而逆矩阵是唯一的，所以 A 没有元素全为整数的逆矩阵。所以这个集合不是群。

想一想 单单指出零矩阵真的足够吗？还是需要就所有矩阵说明一下？

只要有一个元素没有逆元，就足以证明该集合不是群。第二个例子则说明，问题并不止于奇异矩阵（singular matrix）。一个整数矩阵有整数逆矩阵，当且仅当它的行列式（determinant）是 ± 1，因为 $\det A \det A^{-1} = 1$，而两个行列式都是整数。若只考虑这些矩阵，便确实得到一个群。

第 (vi) 部分

模 5 之下，2 的各次幂是

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

所以 $\{1,2,3,4\} = \{2^0, 2^1, 2^2, 2^3\}$，而 $2^a 2^b = 2^{a+b}$，其中指数按模 4 计算。因此集合是封闭的，1 是单位元，而 2^a 的逆元是 2^{4-a}。它是一个群：阶为 4 的循环群（cyclic group），由 2（或由 3）生成。

同构

是群的有 (i)、(iii)、(iv) 和 (vi)，共可组成六对。

(i) 与 (iii) 同构。每个单位复数都可以唯一地写成 $\mathrm{e}^{\mathrm{i}\theta}$，其中 $0 \le \theta < 2\pi$。定义 $\phi(\mathrm{e}^{\mathrm{i}\theta}) = \mathrm{M}(\theta)$。这是一个双射（bijection），因为 $[0, 2\pi)$ 内不同的 θ 给出不同的矩阵（第一列 $(\cos\theta, \sin\theta)$ 已决定了 θ）。它也保持乘法：$\mathrm{e}^{\mathrm{i}\alpha}\mathrm{e}^{\mathrm{i}\beta} = \mathrm{e}^{\mathrm{i}(\alpha+\beta)}$ 及 $\mathrm{M}(\alpha)\mathrm{M}(\beta) = \mathrm{M}(\alpha+\beta)$，而在两个群中，角都是按模 2π 约化的。从几何角度看，两个群都是平面绕原点的旋转。

(i) 或 (iii) 与 (iv) 或 (vi)：不同构。同构是双射，所以两个群的元素个数必须相同。群 (i) 和 (iii) 是无限的，而 (iv) 和 (vi) 各有四个元素。这样就排除了四对。

想一想 (iv) 和 (vi) 都有四个元素，而且都满足交换律。有甚么可以把它们区分开来？

(iv) 与 (vi)：不同构。同构 ϕ 保持每个元素的阶：$\phi(g)^n = \phi(g^n)$，而它等于单位元当且仅当 g^n 是单位元，因为 ϕ 是单射（injective），并把单位元映到单位元。在 (vi) 中，元素 2 的阶是 4。在 (iv) 中，每个元素 g 都满足 $g^2 = 1$，所以没有元素的阶是 4。因此不存在同构。

总括而言，唯一同构的一对是 (i) 和 (iii)。

验算

我们用电脑对 (iv) 和 (vi) 的乘法表逐一穷举，确认了封闭性、单位元和逆元三项性质。电脑亦发现，模 4 之下 0 和 2 没有逆元，而元素的阶在 (iv) 中是 $1,2,2,2$，在 (vi) 中是 $1,4,4,2$（依次对应 $1,2,3,4$）。它还在 10^4 个随机角上验证了 $\mathrm{M}(\alpha)\mathrm{M}(\beta)=\mathrm{M}(\alpha+\beta)$ 以及与 $\mathrm{e}^{i\theta}$ 的对应关系。(iv) 可以很快用手算验证：任何奇数的平方在模 8 之下都是 1，因为 $(2k+1)^2=4k(k+1)+1$，而 $k(k+1)$ 是偶数。

常见错误

- 说 (iv) 和 (vi) 同构，“因为两者都有四个元素”。元素个数相等是必要条件，但并非充分条件。
- 在 (v) 中只检查 $\det A\neq 0$。逆矩阵的元素也必须全为整数。
- 把 (ii) 误读成模 4 加法。在加法之下，它会是一个阶为 4 的循环群，与 (vi) 同构，但题目指明的是乘法。

STEP 之外

在同构意义下，阶为 4 的群恰好只有两个：循环群 C_4，即 (vi)；以及克莱因四元群（Klein four-group）$C_2\times C_2$，即 (iv)。按元素的阶把小阶数的群分类，是大学群论课程最先处理的课题之一。(i) 和 (iii) 的圆群（circle group）是李群（Lie group）最简单的例子；李群是指同时也是光滑曲线或曲面的群。(v) 中行列式为 ±1 的整数矩阵构成群 $\mathrm{GL}_2(\mathbb{Z})$，它在数论中十分重要。想进一步了解，Allenby 的 *Rings, Fields and Groups* 是一本很好的读物。

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。