详细解答

STEP III 样本试卷，第 9 题

纯数学 · 矩阵群

> **STEP III 样本试卷，第 9 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/spec-s3-q9

关键思路

一切都源自一个计算：把两个这种形状的一般矩阵相乘，看看结果是甚么。原来乘积仍是同一形状，各元素由一条简单的公式给出，而这条公式几乎不费吹灰之力就给了我们封闭性（closure）、单位元（identity）、逆元（inverse）、整数子群（subgroup）和可交换（commute）的条件。记

$$M(x,y,z)=\begin{pmatrix}1&0&0\\x&1&0\\y&z&1\end{pmatrix}.$$

解答

G 是一个群

乘积公式。以行乘列，得

$$M(a,b,c)\,M(x,y,z)=\begin{pmatrix}1&0&0\\a&1&0\\b&c&1\end{pmatrix}\begin{pmatrix}1&0&0\\x&1&0\\y&z&1\end{pmatrix}=\begin{pmatrix}1&0&0\\a+x&1&0\\b+cx+y&c+z&1\end{pmatrix},$$

即

$$M(a,b,c)\,M(x,y,z)=M(a+x,\ b+cx+y,\ c+z). \qquad (*)$$

封闭性。元素 $a+x$、$b+cx+y$ 和 $c+z$ 都是实数，所以乘积属于 G。

结合律（associativity）。题目容许我们假设矩阵乘法满足结合律。

单位元。单位矩阵是 $I = M(0,0,0)$，它属于 G，而且对每个矩阵 M 都有 $IM = MI = M$。

逆元。给定 $M(a,b,c)$，我们要找出 $M(x,y,z)$ 使乘积为 $M(0,0,0)$。由 $(*)$，我们需要 $a+x=0$、$c+z=0$ 和 $b+cx+y=0$，所以 $x=-a$、$z=-c$ 及 $y=-b-cx=ac-b$。由于矩阵乘法不满足交换律，另一个次序也要验证：

$$M(-a,\, ac-b,\, -c)\, M(a,b,c) = M(0,\ (ac-b)+(-c)a+b,\ 0) = M(0,0,0).$$

所以 $M(a,b,c)^{-1} = M(-a,\, ac-b,\, -c)$，它属于 G。

群（group）的四条公理全部成立，所以 G 在矩阵乘法下是一个群。

整数矩阵

设 H 为所有满足 $x,y,z \in \mathbb{Z}$ 的 $M(x,y,z)$ 所组成的集合。它是 G 的子集，并且包含 $I = M(0,0,0)$。若 a,b,c,x,y,z 都是整数，则 $a+x$、$b+cx+y$ 和 $c+z$ 也是整数，所以由 $(*)$ 可知 H 在乘法下封闭。逆元 $M(-a,\, ac-b,\, -c)$ 的元素也都是整数，所以 H 在取逆元下封闭。结合律则由 G 承袭而来。所以答案是**是**，H 是 G 的子群。

> ? **想一想** 为甚么单靠乘法下的封闭性并不足够?

对于无限子集，这是可以出错的：x,y,z 为非负整数的矩阵 $M(x,y,z)$ 在乘法下封闭，但 $M(1,0,0)$ 的逆元是 $M(-1,0,0)$，并不在该集合之内。在这里，逆元公式令我们始终留在整数之内，正是这一点使 H 成为子群。

与所有元素可交换的元素

取 $A = M(a,b,c)$ 和一般的 $B = M(x,y,z)$。由 $(*)$，按两个次序分别相乘，得

$$AB = M(a+x,\ b+cx+y,\ c+z), \qquad BA = M(x+a,\ y+za+b,\ z+c).$$

第一个和第三个元素必定相同，所以

$$AB = BA \iff cx = az.$$

（特别地，G 不是阿贝尔群（abelian group）：$M(1,0,0)$ 与 $M(0,0,1)$ 不可交换。）

要 A 与每一个 B 可交换，我们需要对所有实数 x 和 z 都有 $cx = az$。取 $x=1$、$z=0$ 得 $c=0$；取 $x=0$、$z=1$ 得 $a=0$。反过来，若 $a=c=0$，则对所有 x,z 都有 $cx = 0 = az$。所以与整个 G 可交换的元素恰好是

$$A = M(0,b,0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & 0 & 1 \end{pmatrix}, \qquad b \in \mathbb{R}.$$

有，这样的 A 存在：任何 $b \neq 0$ 都给出 $A \neq I$，例如 $A = M(0,1,0)$。由 $(*)$，对 G 中每一个 $B = M(x,y,z)$ 都有 $M(0,1,0)\, M(x,y,z) = M(x,\, 1+y,\, z) = M(x,y,z)\, M(0,1,0)$。

验算

- G 中每个矩阵都是下三角（lower triangular）矩阵，而且对角线上全是一，所以它的行列式（determinant）为 1，必定可逆：我们求得的逆矩阵必然存在，而且同样是这种形状。
- 数值验算：取 $A = M(2,3,5)$ 和 $B = M(1,0,0)$，由 $(*)$ 得 $AB = M(3,8,5)$，但 $BA = M(3,3,5)$，所以 A 与 B 不可交换，正如 $cx = 5 \neq 0 = az$ 所预测的一样。我们亦以分数作精确运算，用数千个随机矩阵验证了乘积公式、逆元公式和可交换的条件。

常见错误

- 只验证一边的逆元。在非阿贝尔的情况下，值得把两个乘积都确认一次（或者指出对方阵而言，单边逆元自动就是双边逆元）。
- 以“G 不是阿贝尔群，所以没有”来回答最后一部分。非阿贝尔群仍然可以有与所有元素可交换的非单位元元素，而这个群正是如此。
- 忘记逆命题：证明了 $a = c = 0$ 是必要条件之后，我们还须验证这样的 A 确实与每一个 B 可交换。

STEP 之外

这就是*海森堡群*（*Heisenberg group*），而与所有元素可交换的元素组成它的*中心*（*centre*）$Z(G)$，在这里就是矩阵 $M(0,b,0)$，相当于实数在加法下所成的群的一个复本。整数版本 H 是离散海森堡群，是群论和几何学中备受喜爱的例子；海森堡群本身则通过位置与动量的对易关系出现在量子力学之中。关于群、子群和中心，可参阅 Allenby 的 *Rings, Fields and Groups*。

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。