详细解答

STEP II 1991，第 9 题

纯数学 · 矩阵群

> **STEP II 1991，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/91-s2-q9

关键思路

一切都建基于一个事实：模 5 的整数构成一个域（field）。每个非零剩余（residue）都有乘法逆元（multiplicative inverse），而非零剩余之积永不为零。正因如此，对角线上的元素才会规规矩矩，封闭性和逆元几乎是不费工夫就得到的。至于最后一部分，可解 $M^2 = I$，把阶（order）为 1 或 2 的元素明确地找出来，然后检验其中两个相乘之后是否仍留在该集合之内。

解答

以下所有运算均以模 5 进行，并在方便时把 4 写成 -1。我们把一般的元素写成

$$M(a,b,c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \qquad a,c \in \{1,2,3,4\},\ b \in \{0,1,2,3,4\}.$$

G 是一个群

封闭性（closure）。把两个元素相乘，得

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}.$$

这是一个上三角矩阵（upper triangular matrix），各元素均为模 5 的数。它的对角线元素 ad 和 cf 都不是零：由于 5 是质数，若 $5 \mid ad$，则 $5 \mid a$ 或 $5 \mid d$，但两者皆不成立。所以这个积属于 G。

结合律（associativity）是已知的，因为矩阵乘法符合结合律。

单位元（identity）。$I = M(1,0,1)$ 属于 G，而且对每个 M 都有 $IM = MI = M$。

逆元（inverses）。每个模 5 的非零剩余都有逆元（$1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$）。所以，给定 $M(a,b,c) \in G$，我们可以构造

$$N = \begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix},$$

由于 $a^{-1}, c^{-1} \neq 0$，它属于 G。利用上面的乘积公式，

$$MN = \begin{pmatrix} aa^{-1} & -aa^{-1}bc^{-1} + bc^{-1} \\ 0 & cc^{-1} \end{pmatrix} = I, \qquad NM = \begin{pmatrix} a^{-1}a & a^{-1}b - a^{-1}bc^{-1}c \\ 0 & c^{-1}c \end{pmatrix} = I.$$

所以每个元素在 G 中都有逆元，因此 G 是一个群（group）。

G 的阶

a 有 4 个选择，b 有 5 个，c 有 4 个，而不同的选择给出不同的矩阵。所以

$$|G| = 4 \times 5 \times 4 = 80.$$

G 是否可交换?

不是。取 $A = M(1,1,1)$ 和 $B = M(2,0,1)$。则

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \qquad BA = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix},$$

所以 $AB \neq BA$，G 不是可交换（commutative）的。

阶为 1 或 2 的元素

元素 M 的阶为 1 或 2，当且仅当 $M^2 = I$。由乘积公式，

$$M(a,b,c)^2 = \begin{pmatrix} a^2 & b(a+c) \\ 0 & c^2 \end{pmatrix},$$

所以我们需要 $a^2 = 1$、$c^2 = 1$ 以及 $b(a+c) = 0$。

$1,2,3,4$ 在模 5 下的平方分别是 $1,4,4,1$，所以 $a^2 = 1$ 必然得出 $a = \pm 1$，同理 $c = \pm 1$。

- 若 $a = c$，则 $a + c = \pm 2 \neq 0$。由于 $\mathbb{Z}_5$ 没有零因子（zero divisor），$b(a+c) = 0$ 必然得出 $b = 0$。这给出 I 和 $-I$。
- 若 $c = -a$，则 $a + c = 0$，所以 b 可取任何值。这给出 10 个矩阵 $M(1,b,-1)$ 和 $M(-1,b,1)$，其中 $b = 0,1,\ldots,4$。

所以，由阶为 1 或 2 的元素组成的集合 H 恰好有 12 个成员。

想一想 由自逆元素组成的集合，是否必定封闭?

不是。这个集合包含 I，而且每个元素都是自己的逆元，所以单位元和逆元这两条公理自动成立。唯一可能不成立的是封闭性，而在非交换群中它通常都不成立：若 $X^2 = Y^2 = I$，则 $(XY)^2 = XYXY$，除非 X 与 Y 可交换，否则这未必能化简为 I。

在这里它确实不成立。取 $X = M(1,1,-1)$ 和 $Y = M(1,0,-1)$，两者都属于 H。则

$$XY = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

这个矩阵有 $a = c = 1$ 但 $b = -1 \neq 0$，所以按上面的分类，它不属于 H。（事实上 $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$，所以它的阶是 5。）因此 H 并不封闭，它不是 G 的子群（subgroup）。

如果你认识拉格朗日定理（Lagrange's theorem），还有一个更快捷的论证：子群的阶必须整除群的阶，而 $12 \nmid 80$。

验算

用电脑把全部 80 个矩阵简单枚举一遍，可确认封闭性、逆元公式，以及上述那对矩阵的 $AB \neq BA$。把每个元素平方，找到的正好是预测中 $M^2 = I$ 的 12 个解，而 $XY = M(1,4,1)$ 的阶是 5。用手算可验证 $M(-1,3,1)^2 = I$：非对角线元素是 $3(-1+1) = 0$。

常见错误

- 忘记证明逆元属于 G。它的对角线元素 a^{-1}、c^{-1} 必须不是零。
- 以为 $M^2 = I$ 必然令 M 是对角矩阵，因而漏掉 $b \neq 0$ 的元素 $M(1,b,-1)$ 和 $M(-1,b,1)$。
- 只为 H 检验单位元和逆元这两条公理。不成立的正是封闭性这条公理。

STEP 之外

G 是有限域（finite field）$\mathbb{F}_5$ 上所有可逆 2×2 上三角矩阵组成的群，是 $\mathrm{GL}_2(\mathbb{F}_5)$ 的一个博雷尔子群（*Borel subgroup*）。满足 $a = c = 1$ 的矩阵构成一个阶为 5 的正规子群（normal subgroup），而 G 是由它与对角矩阵以半直积（semidirect product）的方式构成的。有限域上的矩阵群，是群论入门课程中丰富的例子来源。想了解更多，可参阅 Allenby, *Rings, Fields and Groups*（环、域与群）。

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。