详细解答

STEP II 1992，第 5 题

纯数学 · 矩阵群

> **STEP II 1992，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/92-s2-q5

关键思路

这里的一切都建基于条件 $wz - xy = 1$，它令 S 中矩阵（matrix）的逆矩阵（inverse）特别简单。处理阶为 3 的部分，最好的方法是留意到每个 2×2 矩阵都满足一条由其迹（trace）和行列式（determinant）构成的二次方程。对于 S 中的矩阵，我们可借此把 $\mathbf{A}^2$，继而把 $\mathbf{A}^3$，用 $\mathbf{A}$ 和 $\mathbf{I}$ 表示出来，于是条件 $\mathbf{A}^3 = \mathbf{I}$ 就变成关于迹 $w + z$ 的条件。

（试卷上把 $\mathbf{A}$ 右下角的元素印成 x；但最后一部分提到 z，可见原意显然是该位置为 z，以下一律采用此写法。）

解答

元素的阶

$g \in G$ 的阶（order）是使 $g^n = e$ 成立的最小正整数 n，其中 e 是 G 的单位元（identity）。若 g 的任何正整数次幂都不等于 e，则 g 的阶为无限。单位元是唯一阶为 1 的元素。

逆矩阵

设

$$\mathbf{A} = \begin{pmatrix} w & x \\ y & z \end{pmatrix}, \qquad wz - xy = 1.$$

2×2 逆矩阵的常用公式要除以行列式，而这里行列式为 1，所以

$$\mathbf{A}^{-1} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}.$$

乘开即可验证：$\mathbf{A}\mathbf{A}^{-1} = \begin{pmatrix} wz - xy & 0 \\ 0 & wz - xy \end{pmatrix} = \mathbf{I}$，同理 $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$。

S 是一个群

我们逐一检验群（group）的四条公理。

- 封闭性（*closure*）。若 $\mathbf{A}, \mathbf{B} \in S$，则 $\det(\mathbf{AB}) = \det\mathbf{A}\,\det\mathbf{B} = 1 \times 1 = 1$，所以 $\mathbf{AB} \in S$。
- 结合律（*associativity*）。矩阵乘法的结合律可视为已知。
- 单位元。$\det\mathbf{I} = 1$，所以 $\mathbf{I} \in S$，而且对每个 $\mathbf{A}$ 都有 $\mathbf{IA} = \mathbf{AI} = \mathbf{A}$。
- 逆元。上面求得的矩阵 $\mathbf{A}^{-1}$ 的行列式为 $wz - (-x)(-y) = wz - xy = 1$，所以它属于 S。

因此 S 在矩阵乘法下是一个群。

自逆元素与阶为 2 的元素

把 $\mathbf{A}^{-1}$ 与 $\mathbf{A}$ 逐个元素比较，可知 $\mathbf{A}^{-1} = \mathbf{A}$ 当且仅当

$$z = w, \qquad -x = x, \qquad -y = y,$$

即 $x = y = 0$ 且 $z = w$。这时行列式条件变成 $w^2 = 1$，所以 $w = \pm 1$。因此自逆（self-inverse）元素为

$$\mathbf{A} = \mathbf{I} \quad \text{和} \quad \mathbf{A} = -\mathbf{I}.$$

当 $\mathbf{A}^2 = \mathbf{I}$（等价于 $\mathbf{A}^{-1} = \mathbf{A}$）且 $\mathbf{A} \neq \mathbf{I}$ 时，元素的阶为 2。所以阶为 2 的元素只有 $-\mathbf{I}$。

阶为 3 的元素

记 $t = w + z$ 为 $\mathbf{A}$ 的迹。平方得

$$\mathbf{A}^2 = \begin{pmatrix} w^2 + xy & x(w+z) \\ y(w+z) & xy + z^2 \end{pmatrix}.$$

由于 $xy = wz - 1$，左上角的元素是 $w^2 + wz - 1 = tw - 1$，右下角的元素是 $tz - 1$。因此

$$\mathbf{A}^2 = t\mathbf{A} - \mathbf{I}. \tag{$*$}$$

想一想 $(*)$ 对计算 $\mathbf{A}^3$ 有甚么帮助?

把 $(*)$ 乘以 $\mathbf{A}$，再用一次 $(*)$ 消去 $\mathbf{A}^2$：

$$\mathbf{A}^3 = t\mathbf{A}^2 - \mathbf{A} = t(t\mathbf{A} - \mathbf{I}) - \mathbf{A} = (t^2 - 1)\mathbf{A} - t\mathbf{I}.$$

所以 $\mathbf{A}$ 的任何次幂都是 $\mathbf{A}$ 和 $\mathbf{I}$ 的组合，我们可以比较系数。

若 $w+z+1=0$：则 $t=-1$，所以 $t^2-1=0$，从而 $\mathbf{A}^3=\mathbf{I}$。另外 $\mathbf{A}\neq\mathbf{I}$，因为 $\mathbf{I}$ 的迹是 $2\neq-1$。$\mathbf{A}$ 的阶整除 3 而又不是 1，所以是 3。

反过来，假设 $\mathbf{A}$ 的阶为 3。则 $\mathbf{A}^3=\mathbf{I}$ 且 $\mathbf{A}\neq\mathbf{I}$，所以

$$(t^2-1)\mathbf{A}=(1+t)\mathbf{I}.$$

- 若 $t^2\neq1$，则 $\mathbf{A}=\dfrac{1+t}{t^2-1}\mathbf{I}=\dfrac{1}{t-1}\mathbf{I}$，是单位矩阵的倍数 $\lambda\mathbf{I}$。它的行列式为 $\lambda^2=1$，所以 $\lambda=\pm1$。但 $\mathbf{A}=\mathbf{I}$ 已被排除，而 $\mathbf{A}=-\mathbf{I}$ 的阶是 2，不是 3。所以这个情况不可能出现。
- 若 $t=1$，等式变成 $\mathbf{0}=2\mathbf{I}$，这并不成立。

余下唯一的可能是 $t=-1$，即 $w+z+1=0$。这就证明了“当且仅当”（if and only if）。

一个例子。取 $w=0$ 和 $z=-1$，并选 $x=-1$、$y=1$，使得 $wz-xy=0+1=1$：

$$\mathbf{A}=\begin{pmatrix}0&-1\\1&-1\end{pmatrix},\qquad \mathbf{A}^2=\begin{pmatrix}-1&1\\-1&0\end{pmatrix},\qquad \mathbf{A}^3=\mathbf{I}.$$

验算

- 把上面的例子乘开，直接看出 $\mathbf{A}^3=\mathbf{I}$。
- 旋转 120° 的矩阵 $\begin{pmatrix}-\frac{1}{2}&-\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix}$ 的行列式为 1，迹为 -1，而它的阶当然是 3。
- 我们用电脑对 S 中 20 000 个随机有理数矩阵验证了 $\mathbf{A}^2=t\mathbf{A}-\mathbf{I}$。我们亦搜索了 S 中所有元素均为 $\frac{1}{2}$ 的倍数且介乎 -4 与 4 之间的矩阵：阶为 3 的恰好就是迹为 -1 的那 48 个，而 $-\mathbf{I}$ 是唯一阶为 2 的矩阵。

常见错误

- 把 $\mathbf{I}$ 算作阶为 2 的元素。它是自逆的，但它的阶是 1。
- 只证明了阶为 3 这个结果的其中一个方向。逆命题（converse）需要排除 $t^2\neq1$ 和 $t=1$ 这两个情况。
- 验证群公理时，忘记检查逆矩阵本身的行列式也是 1。

STEP 之外

群 S 就是特殊线性群（special linear group）SL_2，是数学中最重要的群之一。恒等式 $\mathbf{A}^2 - (\operatorname{tr}\mathbf{A})\mathbf{A} + (\det\mathbf{A})\mathbf{I} = \mathbf{0}$ 是凯莱–哈密顿定理（Cayley–Hamilton theorem）的 2×2 情形：每个方阵都满足它自己的特征方程（characteristic equation）。它亦显示出单凭迹就能告诉我们多少关于 SL_2 中元素的信息：上面的论证可以推广，证明阶为有限数 n 的元素，其迹必为 $2\cos(2\pi k/n)$，其中 k 为某个整数。想进一步了解矩阵群，可参阅 Allenby 的 *Rings, Fields and Groups*（环、域与群）；至于凯莱–哈密顿定理和特征值（eigenvalue），可参阅 Strang 的 *Introduction to Linear Algebra*（线性代数导论）。

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。