详细解答

STEP III 1989，第 3 题

纯数学 · 矩阵群

STEP III 1989，第 3 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/89-s3-q3

关键思路

$\mathbf{M}$ 是转角为 $2\pi/m$ 的旋转（rotation），所以 $\mathbf{M}^m = \mathbf{I}$，而它各次幂之和是一个等比级数（geometric series）：把这个和乘以 $\mathbf{I}-\mathbf{M}$，各项便会逐一相消（telescope）。至于递推关系（recurrence），只要写出 $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$，规律便一目了然。之后的群（group）全靠一条恒等式：把其中一个表达式代入另一个，结果只是把下标相加，所以这些元素的运算方式就像模（modulo）m 的整数一样。

解答

$\mathbf{M}$ 的各次幂之和

$\mathbf{M}$ 是绕原点逆时针旋转 $\theta = 2\pi/m$ 的矩阵。连续施行 k 次，就是旋转 $k\theta$，所以

$$\mathbf{M}^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}, \qquad \text{特别地} \qquad \mathbf{M}^m = \begin{pmatrix} \cos 2\pi & -\sin 2\pi \\ \sin 2\pi & \cos 2\pi \end{pmatrix} = \mathbf{I}.$$

（由于 $\mathbf{M}^{k+1} = \mathbf{M}\mathbf{M}^k$，$\mathbf{M}^k$ 的公式可用归纳法（induction）由复角公式（compound-angle formulae）推出。）

设 $\mathbf{S} = \mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1}$。这些矩阵全是 $\mathbf{M}$ 的幂，所以它们可交换（commute），而乘积中各项逐一相消：

$$(\mathbf{I}-\mathbf{M})\mathbf{S} = \mathbf{I} - \mathbf{M}^m = \mathbf{I} - \mathbf{I} = \mathbf{O}.$$

? **想一想** 我们可以直接“约去”因子 $\mathbf{I}-\mathbf{M}$ 吗？

只有当 $\mathbf{I}-\mathbf{M}$ 可逆（invertible）时才可以：非零矩阵的乘积可以是 $\mathbf{O}$。这里

$$\det(\mathbf{I}-\mathbf{M}) = (1-\cos\theta)^2 + \sin^2\theta = 2-2\cos\theta,$$

而由于 $m>1$，我们有 $0<\theta\le\pi$，所以 $\cos\theta\neq 1$，行列式（determinant）不等于零。在 $(\mathbf{I}-\mathbf{M})\mathbf{S}=\mathbf{O}$ 的左边乘以 $(\mathbf{I}-\mathbf{M})^{-1}$，便得 $\mathbf{S}=\mathbf{O}$，这正是所求的结果。

$\mathbf{X}_k$ 的公式

算出最初几项，

$$\mathbf{X}_1 = \mathbf{P}\mathbf{X}_0+\mathbf{Q},\quad \mathbf{X}_2 = \mathbf{P}^2\mathbf{X}_0+\mathbf{P}\mathbf{Q}+\mathbf{Q},\quad \mathbf{X}_3 = \mathbf{P}^3\mathbf{X}_0+(\mathbf{P}^2+\mathbf{P}+\mathbf{I})\mathbf{Q},$$

由此可猜想，对 $k\ge 0$，

$$\mathbf{X}_k = \mathbf{P}^k\mathbf{X}_0+\mathbf{S}_k\mathbf{Q},\qquad \text{其中}\quad \mathbf{S}_k = \mathbf{I}+\mathbf{P}+\cdots+\mathbf{P}^{k-1}\quad(\mathbf{S}_0=\mathbf{O}).$$

当 $k=0$ 时，这式子就是 $\mathbf{X}_0=\mathbf{X}_0$，显然成立。假设它对某个 $k\ge 0$ 成立，则

$$\begin{aligned}\mathbf{X}_{k+1} &= \mathbf{P}\mathbf{X}_k+\mathbf{Q} = \mathbf{P}^{k+1}\mathbf{X}_0+(\mathbf{P}+\mathbf{P}^2+\cdots+\mathbf{P}^k)\mathbf{Q}+\mathbf{Q}\\ &= \mathbf{P}^{k+1}\mathbf{X}_0+\mathbf{S}_{k+1}\mathbf{Q},\end{aligned}$$

所以它对 $k+1$ 也成立，按归纳法，它对所有 $k\ge 0$ 都成立。要保持因子的次序：$\mathbf{P}$ 自始至终都是从左边乘上去的，而 $\mathbf{P}$ 与 $\mathbf{Q}$ 不一定可交换。

群

把 $\mathbf{X}_i$ 看成表达式 $\mathbf{P}^i\mathbf{X}_0+\mathbf{S}_i\mathbf{Q}$，即一条把任意矩阵 $\mathbf{X}_0$ 变成另一个矩阵的规则。以 $\mathbf{X}_j$ 代替 $\mathbf{X}_0$，得

$$\begin{aligned}\mathbf{X}_i * \mathbf{X}_j &= \mathbf{P}^i(\mathbf{P}^j\mathbf{X}_0+\mathbf{S}_j\mathbf{Q})+\mathbf{S}_i\mathbf{Q}\\ &= \mathbf{P}^{i+j}\mathbf{X}_0+(\mathbf{P}^i\mathbf{S}_j+\mathbf{S}_i)\mathbf{Q}.\end{aligned}$$

现在 $\mathbf{P}^i\mathbf{S}_j = \mathbf{P}^i+\cdots+\mathbf{P}^{i+j-1}$，再加上 $\mathbf{S}_i=\mathbf{I}+\cdots+\mathbf{P}^{i-1}$，刚好就是 $\mathbf{S}_{i+j}$。所以，对任意 $\mathbf{P}$，

$$\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}.$$

（这并不令人意外：先按递推关系走 j 步，再多走 i 步，就是走了 $i+j$ 步。）

现在取 $\mathbf{P}=\mathbf{M}$。由第一部分，$\mathbf{M}^m=\mathbf{I}$ 且 $\mathbf{S}_m=\mathbf{O}$，所以

$$\mathbf{X}_m = \mathbf{X}_0,$$

也就是说，$\mathbf{X}_m$ 是令每个矩阵保持不变的表达式。于是对任意 k，$\mathbf{X}_{k+m}=\mathbf{X}_k*\mathbf{X}_m=\mathbf{X}_k$，所以这列表达式以周期 m 重复出现，而

$$G = \{\mathbf{X}_1,\mathbf{X}_2,\mathbf{X}_3,\ldots\} = \{\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_m\}$$

是一个有限集。我们逐一检验群公理。

- 封闭性（*closure*）。$\mathbf{X}_i * \mathbf{X}_j = \mathbf{X}_{i+j}$，而 $i+j \geq 1$，所以它属于 G。
- 结合律（*associativity*）。$(\mathbf{X}_i * \mathbf{X}_j) * \mathbf{X}_k$ 与 $\mathbf{X}_i * (\mathbf{X}_j * \mathbf{X}_k)$ 都等于 $\mathbf{X}_{i+j+k}$。（更一般地说，代入就是函数的复合，而函数的复合必定满足结合律。）
- 单位元（*identity*）。$\mathbf{X}_m * \mathbf{X}_j = \mathbf{X}_{m+j} = \mathbf{X}_j$ 且 $\mathbf{X}_j * \mathbf{X}_m = \mathbf{X}_j$，所以 $\mathbf{X}_m$ 是单位元。
- 逆元（*inverses*）。对 $1 \leq i < m$，$\mathbf{X}_i * \mathbf{X}_{m-i} = \mathbf{X}_{m-i} * \mathbf{X}_i = \mathbf{X}_m$，而 $\mathbf{X}_m$ 的逆元就是它自己。每个逆元都属于 G。

所以 G 在运算 $*$ 下是一个有限群。

事实上，它刚好有 m 个元素：$\mathbf{X}_1, \ldots, \mathbf{X}_m$ 是互不相同的表达式，因为它们的系数 $\mathbf{M}^1, \ldots, \mathbf{M}^m$ 是转角各不相同的旋转，转角都在 $(0, 2\pi]$ 之内。由于每个元素都是 $\mathbf{X}_1$ 的“幂”，G 就是阶（order）为 m 的循环群（cyclic group）。

验算

- 当 $m = 2$ 时，$\mathbf{M} = -\mathbf{I}$，和为 $\mathbf{I} + (-\mathbf{I}) = \mathbf{O}$。当 $m = 4$ 时，$\mathbf{M}$ 是四分之一圈的旋转，而 $\mathbf{I} + \mathbf{M} + \mathbf{M}^2 + \mathbf{M}^3 = \mathbf{I} + \mathbf{M} - \mathbf{I} - \mathbf{M} = \mathbf{O}$。
- 以数值计算，对由 2 至 39 的每个 m，各次幂之和都是 $\mathbf{O}$（在舍入误差之内）；对随机选取的 $\mathbf{P}$、$\mathbf{Q}$、$\mathbf{X}_0$，$\mathbf{X}_k$ 的公式与递推关系吻合；而当 $\mathbf{P} = \mathbf{M}$，$\mathbf{Q}$ 和 $\mathbf{X}_0$ 随机选取时，按递推关系走 m 步后刚好回到 $\mathbf{X}_0$。

常见错误

- 没有检查 $\mathbf{I} - \mathbf{M}$ 是否可逆便把它约去。
- 写成 $\mathbf{Q}\mathbf{S}_k$ 或 $\mathbf{X}_0\mathbf{P}^k$：矩阵乘法不可交换，而递推关系中 $\mathbf{P}$ 是放在左边的。
- 把 $\mathbf{X}_0$ 当作单位元：按题目所列，$\mathbf{X}_0$ 并不在 G 之内；单位元是 $\mathbf{X}_m$，它之所以等于 $\mathbf{X}_0$，全因 $\mathbf{S}_m = \mathbf{O}$。

STEP 之外

每个 $\mathbf{X}_i$ 都是一个仿射映射（*affine map*）$\mathbf{X} \mapsto \mathbf{A}\mathbf{X} + \mathbf{B}$，而 $\mathbf{A}$ 可逆的仿射映射在复合运算下构成一个群；这里我们找到的是一个阶为 m 的循环子群（cyclic subgroup），它由单独一个映射生成，而这个映射的 m 次幂是单位元。$\mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1} = \mathbf{O}$ 这个事实，正是“m 次单位根（roots of unity）之和为零”的矩阵版本；而背后的一般想法，即

一个群以变换的方式作用于一个集合，是大学第一门群论（group theory）课程的核心。Allenby 的 *Rings, Fields and Groups* 对此有详细阐述。

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。