解答例

STEP III 1989、第 3 問

純粋数学 ・ 行列群

> **STEP III 1989、問 3**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/89-s3-q3

鍵となる考え方

$\mathbf{M}$ は角 $2\pi/m$ の回転（rotation）であるから $\mathbf{M}^m = \mathbf{I}$ であり、その累乗の和は等比級数（geometric series）になる。これに $\mathbf{I} - \mathbf{M}$ を掛ければ、項がすべて打ち消し合う（telescoping）。漸化式（recurrence）については、$\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$ を書き出せば規則性は明らかである。群（group）はただ一つの恒等式から得られる。すなわち、これらの式の一つを別の式に代入すると添字がちょうど足し合わされるので、元は m を法とする整数（integers modulo）のように振る舞うのである。

解答

$\mathbf{M}$ の累乗の和

$\mathbf{M}$ は原点を中心とする角 $\theta = 2\pi/m$ の反時計回りの回転を表す行列である。これを k 回施すと角 $k\theta$ だけ回転するので、

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

（$\mathbf{M}^{k+1} = \mathbf{M}\mathbf{M}^k$ であるから、$\mathbf{M}^k$ の式は加法定理（compound-angle formulae）を用いた数学的帰納法（induction）により示される。）

$\mathbf{S} = \mathbf{I} + \mathbf{M} + \cdots + \mathbf{M}^{m-1}$ とおく。これらの行列はすべて $\mathbf{M}$ の累乗であるから互いに可換（commute）であり、積は次のように打ち消し合う：

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

考えてみよう 因子 $\mathbf{I}-\mathbf{M}$ を単純に「約分」してよいだろうか？

それが許されるのは $\mathbf{I}-\mathbf{M}$ が正則（invertible）である場合に限る。零行列でない行列どうしの積が $\mathbf{O}$ になることもあるからである。ここでは

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

であり、$m>1$ より $0<\theta\leq\pi$ であるから $\cos\theta\neq 1$ となり、行列式（determinant）は 0 でない。$(\mathbf{I}-\mathbf{M})\mathbf{S}=\mathbf{O}$ の左から $(\mathbf{I}-\mathbf{M})^{-1}$ を掛けると $\mathbf{S}=\mathbf{O}$ が得られ、これが求める結果である。

$\mathbf{X}_k$ の一般式

最初の数項を計算すると

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

となり、$k\geq 0$ に対して

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

であることが予想される。$k=0$ のとき、これは $\mathbf{X}_0=\mathbf{X}_0$ となり成り立つ。ある $k\geq 0$ で成り立つと仮定すると、

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

となるので $k+1$ でも成り立ち、数学的帰納法によりすべての $k\geq 0$ で成り立つ。因子の順序に注意せよ。$\mathbf{P}$ は常に左から掛かっており、$\mathbf{P}$ と $\mathbf{Q}$ は可換とは限らない。

群

$\mathbf{X}_i$ を、任意の行列 $\mathbf{X}_0$ を別の行列に移す規則、すなわち式 $\mathbf{P}^i\mathbf{X}_0+\mathbf{S}_i\mathbf{Q}$ とみなす。$\mathbf{X}_0$ に $\mathbf{X}_j$ を代入すると

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

を得る。ここで $\mathbf{P}^i\mathbf{S}_j = \mathbf{P}^i+\cdots+\mathbf{P}^{i+j-1}$ であり、これに $\mathbf{S}_i=\mathbf{I}+\cdots+\mathbf{P}^{i-1}$ を加えるとちょうど $\mathbf{S}_{i+j}$ になる。よって、任意の $\mathbf{P}$ に対して

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

が成り立つ。（これは驚くことではない。漸化式を j ステップ進め、さらに i ステップ進めることは、$i+j$ ステップ進めることと同じだからである。）

ここで $\mathbf{P}=\mathbf{M}$ とする。前半の結果より $\mathbf{M}^m=\mathbf{I}$ かつ $\mathbf{S}_m=\mathbf{O}$ であるから、

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

すなわち $\mathbf{X}_m$ はすべての行列を変えない式である。すると任意の k に対して $\mathbf{X}_{k+m}=\mathbf{X}_k*\mathbf{X}_m=\mathbf{X}_k$ となるので、式の列は周期 m で繰り返し、

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

は有限集合である。群の公理（group axioms）を確かめよう。

- **演算について閉じていること**（*closure*）。$\mathbf{X}_i*\mathbf{X}_j=\mathbf{X}_{i+j}$ であり、$i+j\geq 1$ であるから、これは G に属する。
- **結合法則**（*associativity*）。$(\mathbf{X}_i*\mathbf{X}_j)*\mathbf{X}_k$ と $\mathbf{X}_i*(\mathbf{X}_j*\mathbf{X}_k)$ はどちらも $\mathbf{X}_{i+j+k}$ に等しい。（より一般に、代入とは関数の合成（composition）であり、合成は常に結合法則を満たす。）
- **単位元**（*identity*）。$\mathbf{X}_m*\mathbf{X}_j=\mathbf{X}_{m+j}=\mathbf{X}_j$ かつ $\mathbf{X}_j*\mathbf{X}_m=\mathbf{X}_j$ であるから、$\mathbf{X}_m$ が単位元である。
- **逆元**（*inverses*）。$1\leq i<m$ に対して $\mathbf{X}_i*\mathbf{X}_{m-i}=\mathbf{X}_{m-i}*\mathbf{X}_i=\mathbf{X}_m$ であり、$\mathbf{X}_m$ は自分自身の逆元である。いずれの逆元も G に属する。

したがって、G は $*$ に関して有限群である。

実際、G の元はちょうど m 個である。$\mathbf{X}_1,\ldots,\mathbf{X}_m$ の係数 $\mathbf{M}^1,\ldots,\mathbf{M}^m$ は $(0,2\pi]$ 内の相異なる角の回転であるから、これらは相異なる式だからである。すべての元が $\mathbf{X}_1$ の「累乗」であるから、G は位数（order）m の巡回群（cyclic group）である。

検算

- $m=2$ のとき $\mathbf{M}=-\mathbf{I}$ であり、和は $\mathbf{I}+(-\mathbf{I})=\mathbf{O}$ となる。$m=4$ のとき $\mathbf{M}$ は 4 分の 1 回転であり、$\mathbf{I}+\mathbf{M}+\mathbf{M}^2+\mathbf{M}^3=\mathbf{I}+\mathbf{M}-\mathbf{I}-\mathbf{M}=\mathbf{O}$ となる。
- 数値計算により、2 から 39 までのすべての m について累乗の和が（丸め誤差の範囲で）$\mathbf{O}$ になること、ランダムな $\mathbf{P},\mathbf{Q},\mathbf{X}_0$ に対して $\mathbf{X}_k$ の式が漸化式と一致すること、そして $\mathbf{P}=\mathbf{M}$ とし $\mathbf{Q}$ と $\mathbf{X}_0$ をランダムにとったとき、漸化式を m ステップ進めるとちょうど $\mathbf{X}_0$ に戻ることを確かめた。

よくある間違い

- $\mathbf{I}-\mathbf{M}$ が正則であることを確かめずに約分してしまう。
- $\mathbf{QS}_k$ や $\mathbf{X}_0\mathbf{P}^k$ と書いてしまう。行列は一般に可換ではなく、漸化式では $\mathbf{P}$ が左に掛かっている。
- $\mathbf{X}_0$ を単位元としてしまう。列挙した G に $\mathbf{X}_0$ は含まれていない。単位元は $\mathbf{X}_m$ であり、それが $\mathbf{X}_0$ に等しいのは $\mathbf{S}_m=\mathbf{O}$ だからにすぎない。

STEP のその先へ

各 $\mathbf{X}_i$ はアフィン写像（affine map）$\mathbf{X}\mapsto\mathbf{AX}+\mathbf{B}$ であり、$\mathbf{A}$ が正則であるアフィン写像全体は合成に関して群をなす。ここで見つけたのは、m 乗が恒等写像になるただ一つの写像によって生成される位数 m の巡回部分群（subgroup）である。$\mathbf{I}+\mathbf{M}+\cdots+\mathbf{M}^{m-1}=\mathbf{O}$ という事実は、1 の m 乗根の和が 0 になることの行列版である。そして一般的な考え方、すなわち群が変換によって集合に作用するという群作用（group action）の考え方は、群論の最初の講義の中心的な主題である。Allenby の *Rings, Fields and Groups*（環・体・群）でこの考え方が展開されている。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。