解答例

STEP II 1991、第 9 問

純粋数学 ・ 行列群

> **STEP II 1991、問 9**
>
> 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/91-s2-q9

鍵となる考え方

すべては一つの事実に基づいている。すなわち、5 を法とする整数は体（field）をなす、ということである。0 でない剰余（residue）はどれも乗法逆元（multiplicative inverse）をもち、0 でない剰余どうしの積が 0 になることはない。これによって対角成分の扱いがうまくいき、閉性と逆元の存在はほとんど自動的に得られる。最後の小問では、$M^2 = I$ を解いて位数（order）が 1 または 2 の元を具体的に求め、そのうちの二つを掛けたものがその集合にとどまるかどうかを調べればよい。

解答

以下、計算はすべて 5 を法として行い、都合のよいときは 4 を -1 と書く。一般の元を

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

と表す。

G は群である

閉性（closure）。二つの元を掛けると

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

となる。これは成分が 5 を法とする上三角行列（upper triangular matrix）である。その対角成分 ad と cf は 0 でない。実際、5 は素数であるから、$5 \mid ad$ ならば $5 \mid a$ または $5 \mid d$ であるが、どちらも成り立たない。よって積は G に属する。

結合法則（associativity）は行列の積が結合的であることから成り立つ。

単位元（identity）。$I = M(1,0,1)$ は G に属し、任意の M に対して $IM = MI = M$ である。

逆元（inverse）。5 を法とする 0 でない剰余はすべて逆元をもつ（$1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$）。したがって、$M(a,b,c) \in G$ が与えられたとき

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

を作ることができ、$a^{-1}, c^{-1} \neq 0$ であるから N は G に属する。積の公式を用いると

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

となる。よってすべての元は G の中に逆元をもち、G は群（group）である。

G の位数

a の選び方は 4 通り、b は 5 通り、c は 4 通りであり、選び方が異なれば異なる行列が得られる。よって

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

である。

G は可換か？

可換（commutative）ではない。$A = M(1,1,1), B = M(2,0,1)$ とすると

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

であるから $AB \neq BA$ であり、G は可換ではない。

位数 1 または 2 の元

元 M の位数が 1 または 2 であるのは、$M^2 = I$ のときであり、かつそのときに限る。積の公式より

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

であるから、$a^2 = 1, c^2 = 1, b(a+c) = 0$ が必要である。

$1, 2, 3, 4$ の平方は 5 を法として $1, 4, 4, 1$ であるから、$a^2 = 1$ より $a = \pm 1$ であり、同様に $c = \pm 1$ である。

- $a = c$ のとき、$a + c = \pm 2 \neq 0$ である。$\mathbb{Z}_5$ には零因子（zero divisor）がないから、$b(a + c) = 0$ より $b = 0$ となる。これにより I と $-I$ が得られる。
- $c = -a$ のとき、$a + c = 0$ であるから b は何でもよい。これにより、$b = 0, 1, \ldots, 4$ に対する 10 個の行列 $M(1, b, -1)$ と $M(-1, b, 1)$ が得られる。

よって、位数 1 または 2 の元全体の集合 H の要素はちょうど 12 個である。

考えてみよう 自分自身が逆元であるような元の集合は、自動的に閉じているだろうか？

そうではない。この集合は I を含み、各元は自分自身の逆元であるから、単位元と逆元に関する公理は自動的に成り立つ。成り立たない可能性があるのは閉性だけであり、非可換な群では実際に成り立たないことが多い。$X^2 = Y^2 = I$ のとき $(XY)^2 = XYXY$ であるが、X と Y が可換でない限り、これが I になるとは限らない。

ここでも閉性は成り立たない。H の元 $X = M(1, 1, -1)$ と $Y = M(1, 0, -1)$ をとると

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

となる。これは $a = c = 1$ であるが $b = -1 \neq 0$ であるから、上の分類により H に属さない。（実際 $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$ であるから、この元の位数は 5 である。）したがって H は閉じておらず、G の部分群（subgroup）では**ない**。

ラグランジュ（Lagrange）の定理を知っていれば、もっと手早く示せる。部分群の位数は群の位数を割り切らなければならないが、$12 \nmid 80$ である。

検算

80 個の行列すべてをコンピュータで短時間に列挙すると、閉性、逆元の公式、および上の組に対する $AB \neq BA$ が確認できる。すべての元を 2 乗すると、予想どおりちょうど 12 個の $M^2 = I$ の解が見つかり、$XY = M(1, 4, 1)$ の位数は 5 である。手計算では、$M(-1, 3, 1)^2 = I$ を確かめてみるとよい。非対角成分は $3(-1 + 1) = 0$ となる。

よくある間違い

- 逆元が G に属することを示し忘れる。その対角成分 a^{-1}, c^{-1} が 0 でないことが必要である。
- $M^2 = I$ ならば M は対角行列であると思い込み、$b \neq 0$ である元 $M(1, b, -1)$ と

$M(-1, b, 1)$ を見落とす。

- H について単位元と逆元の公理だけを確認する。成り立たないのは閉性の公理である。

STEP のその先へ

G は有限体（finite field）$\mathbb{F}_5$ 上の可逆な 2×2 上三角行列全体のなす群であり、$\mathrm{GL}_2(\mathbb{F}_5)$ の**ボレル部分群**（Borel subgroup）である。$a = c = 1$ である行列全体は位数 5 の正規部分群（normal subgroup）をなし、G はこれと対角行列全体から半直積（semidirect product）として構成される。有限体上の行列のなす群は、群論（group theory）の入門講義において豊富な例の宝庫である。さらに学ぶには、Allenby, *Rings, Fields and Groups* を参照するとよい。

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。