解答例

STEP III 1993、第 5 問

純粋数学 ・ 群と四元数

STEP III 1993、問 5

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/93-s3-q5

この問題は、*Beyond STEP* の第 6.7 節「**四元数群**」で詳しく解説されている：https://beyondstep.keithmcnulty.org/ja/ch06/quaternions.html

鍵となる考え方

この演算は一見すると恣意的に見えるが、最初の部分で求める四つの積がその構造を明らかにする。$(z,0)$ の形の組は通常の複素数と同じように掛け算され、第 2 成分は $j^2=-1$ を満たす新しい記号 j のように振る舞い、自分を通り過ぎるものを何でも複素共役（conjugate）に変える。これら四つの積が得られれば、S_1 の 8 個の元は $u\in\{1,i,-1,-i\}$ に対する $(u,0)$ と $(0,u)$ にすぎない。したがって、閉性、逆元、位数はわずか数行の一般的な議論から得られ、64 個の成分をもつ表を作る必要はない。

解答

結合法則と交換法則

$z=(z_1,z_2)$、$w=(w_1,w_2)$、$u=(u_1,u_2)$ とおく。以下では常に $(ab)^*=a^*b^*$、$(a\pm b)^*=a^*\pm b^*$、$a^{**}=a$ を用いる。まず

$$z\circ w=(z_1w_1-z_2w_2^*,\ z_1w_2+z_2w_1^*),$$

であるから、$(z\circ w)\circ u$ の二つの成分は

$$(z_1w_1-z_2w_2^*)u_1-(z_1w_2+z_2w_1^*)u_2^*=z_1w_1u_1-z_1w_2u_2^*-z_2w_1^*u_2^*-z_2w_2^*u_1,$$
$$(z_1w_1-z_2w_2^*)u_2+(z_1w_2+z_2w_1^*)u_1^*=z_1w_1u_2+z_1w_2u_1^*+z_2w_1^*u_1^*-z_2w_2^*u_2.$$

である。一方、$w \circ u = (w_1u_1 - w_2u_2^*,\ w_1u_2 + w_2u_1^*)$ であるから、$z \circ (w \circ u)$ の二つの成分は

$$z_1(w_1u_1 - w_2u_2^*) - z_2(w_1u_2 + w_2u_1^*)^* = z_1w_1u_1 - z_1w_2u_2^* - z_2w_1^*u_2^* - z_2w_2^*u_1,$$
$$z_1(w_1u_2 + w_2u_1^*) + z_2(w_1u_1 - w_2u_2^*)^* = z_1w_1u_2 + z_1w_2u_1^* + z_2w_1^*u_1^* - z_2w_2^*u_2.$$

である。右辺は項ごとに一致するので、$\circ$ は結合的（associative）である。

この演算は可換（commutative）ではない。たとえば

$$(0,1) \circ (i,0) = (0-0,\ 0+1\cdot i^*) = (0,-i), \qquad (i,0) \circ (0,1) = (0-0,\ i\cdot 1+0) = (0,i).$$

四つの積

定義に o を代入すると

$$(z,0) \circ (w,0) = (zw,\ 0), \qquad (z,0) \circ (0,w) = (0,\ zw),$$
$$(0,z) \circ (w,0) = (0,\ zw^*), \qquad (0,z) \circ (0,w) = (-zw^*,\ 0).$$

集合 S_1

$U = \{1, i, -1, -i\}$ とおく。このとき

$$S_1 = \{(u,0) : u \in U\} \cup \{(0,u) : u \in U\},$$

であり、A, C, E, G が第 1 の種類、B, D, F, H が第 2 の種類である。

閉性（closure）。集合 U は乗法、複素共役（$i^* = -i$）、符号の反転のいずれについても閉じている。四つの積により、S_1 の二つの元の積は、$z, w \in U$ として $(zw,0)$、$(0,zw)$、$(0,zw^*)$、$(-zw^*,0)$ のいずれかである。zw と $\pm zw^*$ はいずれも U に属するので、どの積も S_1 に属する。

単位元（identity）。任意の $(w_1,w_2) \in S$ に対して

$$(1,0) \circ (w_1,w_2) = (w_1,\ w_2), \qquad (w_1,w_2) \circ (1,0) = (w_1,\ w_2 \cdot 1^*) = (w_1,w_2),$$

であるから、$A = (1,0)$ は両側単位元であり、S_1 に属する。

逆元（inverse）と位数（order）。第 1 の種類の元については $(z,0) \circ (w,0) = (zw,0)$ であるから、これらは U の複素数とまったく同じように振る舞う。よって A は位数 1 で自分自身が逆元であり、$E = (-1,0)$ は位数 2 で自分自身が逆元であり、$C = (i,0)$ と $G = (-i,0)$ はいずれも位数 4 で互いに逆元である。

? **考えてみよう** 第 2 の種類の元を 2 乗すると何になるか？

四つの積の最後のものにより、$u \in U$ に対して

$$(0,u)\circ(0,u) = (-uu^*,\,0) = (-|u|^2,\,0) = (-1,0) = E.$$

したがって B, D, F, H はいずれも 2 乗すると E になる。E の位数は 2 であるから、これらの位数はいずれも 4 である。逆元については、$(0,u)\circ(0,w) = (-uw^*,0)$ が $(1,0)$ に等しくなるのは、（$uu^* = 1$ を用いると）$w^* = -1/u = -u^*$、すなわち $w = -u$ のときに限る。逆の順序も確かめると、$(0,-u)\circ(0,u) = (uu^*,0) = (1,0)$ もやはり成り立つ。よって $(0,u)$ の逆元は $(0,-u)$ である。

まとめると次のようになる。

元	A	B	C	D	E	F	G	H
逆元	A	F	G	H	E	B	C	D
位数	1	4	4	4	2	4	4	4

群（group）。これで四つの公理がすべてそろった。S_1 は $\circ$ について閉じている。演算は S 全体で結合的であり、とくに S_1 上でも結合的である。$A \in S_1$ は単位元であり、すべての元が S_1 の中に逆元をもつ。したがって S_1 は $\circ$ について位数 8 の群である。これは非可換（non-abelian）である。実際、$B\circ C = H$ であるが $C\circ B = D$ である。

部分群と行列

上の積を用いると、$B = (0,1)$ の累乗は

$$B^2 = E, \qquad B^3 = E\circ B = (-1,0)\circ(0,1) = (0,-1) = F, \qquad B^4 = E\circ E = A.$$

である。よって $\{A,B,E,F\} = \{B^0, B^1, B^2, B^3\}$ は B が生成する巡回部分群（cyclic subgroup）である。$B^m \circ B^n = B^{m+n}$ であり指数は mod 4 で簡約できるので、この集合は閉じており、また A と各 B^k の逆元 B^{4-k} を含む。したがってこれは位数 4 の部分群である。

$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ とおく。このとき

$$M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad M^3 = -M, \qquad M^4 = I,$$

であるから、M が生成する群は $\{I, M, -I, -M\}$ であり、これも位数 4 の巡回群である。位数の等しい二つの巡回群は同型（isomorphic）である。ここでは写像

$$A \mapsto I, \quad B \mapsto M, \quad E \mapsto -I, \quad F \mapsto -M,$$

すなわち $B^k \mapsto M^k$ は全単射（bijection）であり、$B^m \circ B^n = B^{m+n} \mapsto M^{m+n} = M^m M^n$ を満たす。よって二つの群は確かに**同型である**。

検算

- 元の位数は群の位数を割り切る：位数 $1, 2, 4$ はすべて 8 を割り切り、部分群については 2 と 4 が 4 を割り切る。
- 複素数としての見方：$(z,0)\circ(w,0)=(zw,0)$ であるから、$C\circ C=(i^2,0)=E$ となり、$i^2=-1$ とまったく同じである。
- 簡単なコンピュータによる検証で、複素数の組の無作為な三つ組 10 000 個について結合法則を確認し、8×8 の完全な表を作って閉性、単位元、上の逆元と位数、および $B\circ C=H\neq D=C\circ B$ を確認し、さらに $B^k\mapsto M^k$ が乗法を保つことを確認した。

よくある間違い

- 共役を忘れること：$(0,z)\circ(w,0)$ は $(0,zw^*)$ であって、$(0,zw)$ ではない。非可換性はここから生じる。
- 数値例を一つ示しただけで結合法則を示したとすること。例はある法則が**成り立たない**ことを示すことはできるが、成り立つことの証明には一般的な展開が必要である。
- 一方の群が複素数の組から、もう一方が行列からできているという理由で「同型でない」と結論すること。同型とは乗法の構造に関することであって、元が何であるかには関係しない。

STEP のその先へ

この演算はハミルトン（Hamilton）による**四元数**（quaternions）の乗法である。組 (z_1,z_2) は z_1+z_2j を表し、ここで $j^2=-1$、$jz=z^*j$ である。群 S_1 は**四元数群**（quaternion group）$Q_8=\{\pm1,\pm i,\pm j,\pm k\}$ である。これはすべての部分群が正規部分群（normal subgroup）であるような最小の非可換群であり、位数 8 のもう一つの非可換群（正方形の対称性の群）とは、位数 2 の元を一つしかもたない点で異なる。Allenby の *Rings, Fields and Groups*（環・体・群）では、小さい位数の群と四元数が扱われている。

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。