解答例

STEP III 1994、第 7 問

純粋数学 • 群の同型

> **STEP III 1994、問 7**
>
> 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/94-s3-q7

鍵となる考え方

2 つの群（group）が同型（isomorphic）になりうるのは、同型写像（isomorphism）が保つあらゆる構造的性質を両者が共有している場合に限られる。そのような性質のうち最も役に立つのは、元の位数（order）の一覧と、群が可換（commutative、アーベル的（abelian）ともいう）かどうかの 2 つである。位数を列挙するだけで、すでに S_3 と Z_6 は区別できる。2 つの群が同型であることを証明するには、具体的な全単射（bijection）を書き下し、それが演算を保つことを確かめればよい。最後の小問は可換性に帰着する。複素数からなる群はすべてアーベル群であるが、S_3 はそうではない。

解答

S_3 と Z_6 の元

3 つの対象に 1, 2, 3 と名前をつけ、巡回置換の記法（cycle notation）を用いる。合成は右から左に行う。つまり $\sigma\tau$ は「まず τ を行い、次に σ を行う」という意味である。6 つの置換（permutation）を以下に挙げる。

S_3 の元	e	(12)	(13)	(23)	(123)	(132)
位数	1	2	2	2	3	3

互換（transposition）は 2 つの対象を入れ替えるもので、2 回行うとすべてが元に戻るから、位数は 2 である。(123) のような 3-巡回置換は $1 \to 2 \to 3 \to 1$ と移すので、各対象を元の位置に戻すには 3 回適用する必要があり、位数は 3 である。

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ では単位元は 0 であり、a の位数は $na \equiv 0 \pmod 6$ を満たす最小

の $n \geq 1$、すなわち $6/\gcd(a,6)$ である。

Z_6 の元	0	1	2	3	4	5
位数	1	6	3	2	3	6

たとえば $4+4=8\equiv 2$、$4+4+4=12\equiv 0$ であるから、4 の位数は 3 である。

S_3 と Z_6 は同型か？

同型ではない。同型写像 θ は位数を保つ。実際、g の位数が n ならば $\theta(g)^k=\theta(g^k)$ であり、θ は単射（injective）であるから、これが単位元となるのは g^k が単位元であるときに限る。したがって、同型な群では各位数の元の個数が等しい。ところが Z_6 には位数 6 の元が 2 つあり、S_3 には 1 つもないので、両者は同型ではない。（位数 2 の元の個数も異なる。S_3 には 3 つあるが、Z_6 には 1 つしかない。）

もう 1 つの理由があり、これは最後にも再び用いる。加法は可換であるから、Z_6 はアーベル群である。一方、S_3 はアーベル群ではない。

$$(12)(13)=(132),\qquad (13)(12)=(123).$$

1 つ目の積については、(13) が $1\to 3$ と移し、次に (12) が 3 を固定するので、$1\to 3$ となる。同様に $3\to 2$、$2\to 1$ である。同型写像は可換な組を可換な組に移すから、非可換群がアーベル群と同型になることはありえない。

C_6 は Z_6 と同型である

$k=0,1,\dots,5$ に対して $\phi(k)=\alpha^k$ により $\phi: Z_6\to C_6$ を定める。

- **全単射であること。** $k=0,\dots,5$ に対する数 $\alpha^k=\mathrm{e}^{\mathrm{i}k\pi/3}$ の偏角は $0,\frac{\pi}{3},\dots,\frac{5\pi}{3}$ である。これらは $[0,2\pi)$ 内の相異なる角であるから、6 つの値は単位円上の相異なる点である。よって ϕ は単射であり、したがって要素数 6 の 2 つの集合の間の全単射である。
- **演算を保つこと。** $a,b\in Z_6$ とし、$r=(a+b) \bmod 6$ として $a+b=6q+r$ と書く。$\alpha^6=\mathrm{e}^{2\pi\mathrm{i}}=1$ であるから、

$$\phi(a)\,\phi(b)=\alpha^a\alpha^b=\alpha^{a+b}=(\alpha^6)^q\alpha^r=\alpha^r=\phi\big((a+b) \bmod 6\big).$$

このように ϕ は mod 6 の加法を複素数の乗法に移すので、同型写像である。よって $C_6\cong Z_6$ である。確認として、α と α^5（1 と 5 の像）の位数は 6、α^2 と α^4 の位数は 3、$\alpha^3=-1$ の位数は 2 であり、Z_6 の表と一致する。

S_3 と同型な $\mathbb{C}$ の部分群は存在するか？

考えてみよう 複素数からなる群がすべて共有している性質は何か？

それらはすべてアーベル群である。$(\mathbb{C}, +)$ の部分群（subgroup）H は、すべての複素数 z, w に対して $z + w = w + z$ であるからアーベル群である。0 でない複素数全体の乗法に関する部分群 H も、$zw = wz$ であるからアーベル群である。部分群は大きい群と同じ演算を用いるので、可換性を受け継ぐのである。

そこで、このような H に対して同型写像 $\theta : S_3 \to H$ が存在したと仮定する。これを上の非可換な組に適用する。H はアーベル群であるから、

$$\theta\big((12)(13)\big) = \theta(12)\,\theta(13) = \theta(13)\,\theta(12) = \theta\big((13)(12)\big),$$

となる（ここでは乗法的に書いた。加法の場合は積を和に置き換えればよい）。θ は単射であるから、これより $(12)(13) = (13)(12)$ が得られるが、これは誤りである。したがって、加法的であれ乗法的であれ、S_3 と同型な複素数の部分群は**存在しない**。

検算

- どちらの群でも位数は 6 を割り切る（ラグランジュの定理（Lagrange's theorem））。S_3 では $1, 2, 3$、Z_6 では $1, 2, 3, 6$ である。
- コンピュータで S_3、Z_6、C_6 のすべての位数を計算し直し、$(12)(13) \neq (13)(12)$ を確認し、さらに 36 通りすべての組 (a, b) について $\alpha^{(a+b) \bmod 6} = \alpha^a \alpha^b$ を誤差 10^{-12} 以内で数値的に確かめた。

よくある間違い

- 「どちらも元が 6 個あるから同型である」と述べてしまう。元の個数が等しいことは必要条件ではあるが、十分条件には程遠い。
- S_3 の位数 3 の元を (12) と (13) としてしまう。互換の位数は 2 であり、位数 3 をもつのは 3-巡回置換だけである。
- 最後の小問で、有限な乗法的部分群（1 の冪根（roots of unity）全体）の場合しか否定していない。可換性による議論を使えば、有限か無限か、加法的か乗法的かを問わず、すべての部分群を一度に扱える。

STEP のその先へ

この問題のテーマは不変量（invariant）、すなわち元の位数や可換性のように、同型な群が必ず共有する性質である。実は、位数 6 の群はすべて Z_6 か S_3 のいずれかと同型である。より一般に、0 でない複素数全体の乗法に関する有限部分群はすべて巡回群（cyclic group）であり、したがって 1 の冪根からなる群である。どちらの結果も、群論の最初の講義の早い段階で学ぶことになるだろう。これらについて読むには、Allenby の *Rings, Fields and Groups*（環・体・群）が親しみやすい。

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。