解答例

# STEP III 1988、第 9 問

純粋数学 ・ 群の元の位数

> **STEP III 1988、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/88-s3-q9

## 鍵となる考え方

小問 (i) は形を変えた除法の原理（division algorithm）である。$N$ を $n$ の倍数と余りの和として表せば、$n$ の最小性から余りは 0 でなければならない。小問 (ii) がうまくいくのは、$g$ による共役（conjugation）が積を保つからであり、共役元の積では内側に現れる $g^{-1}g$ の組が打ち消し合う。小問 (iii) では $g$ による共役を繰り返し施す。$g^5 = e$ であるから、5 回施すと $h$ は自分自身に戻り、これによって $h$ の位数（order）が決まる。

## 解答

### 小問 (i)

除法の原理により、$q$ を整数、$0 \leq r < n$ として $N = qn + r$ と書ける（これは 0 や負の整数を含め、任意の整数 $N$ について成り立つ）。すると $g^n = e$ であるから

$$e = g^N = (g^n)^q g^r = e^q g^r = g^r.$$

もし $r$ が正であれば、$r$ は $g^r = e$ を満たす $n$ より小さい正の整数となり、$n = o(g)$ がそのような整数のうち**最小**のものであるという定義に矛盾する。よって $r = 0$ であり、$N = qn$ となるから、$n$ は $N$ を割り切る。

### 小問 (ii)

$m = 0$ **のとき**：両辺はともに $e$ に等しい。

$m \geq 1$ **のとき**：$m$ に関する帰納法（induction）を用いる。$m = 1$ の場合は明らかであ

る。$gh^m g^{-1} = (ghg^{-1})^m$ が成り立つと仮定すると

$$\begin{aligned}(ghg^{-1})^{m+1} &= (ghg^{-1})^m\,(ghg^{-1}) = (gh^m g^{-1})(ghg^{-1}) \\ &= gh^m(g^{-1}g)hg^{-1} = gh^{m+1}g^{-1},\end{aligned}$$

となり、帰納法が完結する（具体的に書き出すと、$(ghg^{-1})(ghg^{-1})\cdots(ghg^{-1})$ は次々と打ち消し合い、途中に現れる $g^{-1}g$ はすべて消える）。

$m \le -1$ **のとき：**まず、$ghg^{-1}$ の逆元は $gh^{-1}g^{-1}$ である。実際、

$$(ghg^{-1})(gh^{-1}g^{-1}) = gh(g^{-1}g)h^{-1}g^{-1} = ghh^{-1}g^{-1} = e.$$

次に、$k \ge 1$ として $m = -k$ と書く。$h$ の代わりに元 $h^{-1}$ に対して正の場合の結果を適用すると

$$gh^m g^{-1} = g(h^{-1})^k g^{-1} = (gh^{-1}g^{-1})^k = ((ghg^{-1})^{-1})^k = (ghg^{-1})^{-k} = (ghg^{-1})^m.$$

したがって、この等式はすべての整数 $m$ について成り立つ。

**小問 (iii)**

$ghg^{-1} = h^2$ を用い、さらに $m = 2$ として小問 (ii) を用いると

$$g^2hg^{-2} = g\,(ghg^{-1})\,g^{-1} = gh^2g^{-1} = (ghg^{-1})^2 = (h^2)^2 = h^4,$$

となり、示すべき式が得られる。

同じ操作はどの段階でも使える。すべての $k \ge 0$ について $g^khg^{-k} = h^{2^k}$ が成り立つことを示す。$k = 0$ のときは成り立つ。$k$ のとき成り立つとすると、$m = 2^k$ として小問 (ii) を用いれば

$$g^{k+1}hg^{-(k+1)} = g\,(g^khg^{-k})\,g^{-1} = gh^{2^k}g^{-1} = (ghg^{-1})^{2^k} = (h^2)^{2^k} = h^{2^{k+1}}.$$

$k = 5$ とし、$g^5 = e$（したがって $g^{-5} = e$ でもある）を用い、両辺に $h^{-1}$ を掛けると

$$h = g^5hg^{-5} = h^{32}, \qquad \text{よって} \qquad h^{31} = e$$

が得られる。

> **考えてみよう** $h^{31} = e$ であることはわかった。なぜこれから、$o(h)$ が単に 31 以下というだけでなく、ちょうど 31 であるといえるのだろうか。

小問 (i) により、$o(h)$ は 31 を割り切る。31 は素数（prime）であるから、$o(h)$ は 1 または 31 である。しかし $o(h) = 1$ は $h = e$ を意味し、これは条件により成り立たない。したがって

$$o(h) = 31.$$

このような群（group）は実際に存在するので、条件は矛盾しない。31 を法として、$\{0,1,\ldots,30\}$ の置換（permutation）$h(x)=x+1$ と $g(x)=2x$ を考える。すると $g^5(x)=32x=x$ であり、$ghg^{-1}(x)=2(\frac{x}{2}+1)=x+2=h^2(x)$ であり、さらに $h$ の位数は確かに 31 である。

## 検算

- 素数 31 が現れるのは理にかなっている。$g$ による共役は $h$ のべきに対して「指数を 2 倍する」という作用をし、5 回の倍化で元に戻らなければならないから、$o(h)$ を法として $2^5\equiv 1$ となる。言い換えれば、$o(h)$ は $2^5-1=31$ を割り切る。
- 31 を法とする置換 $g(x)=2x$ と $h(x)=x+1$ を用いたコンピュータによる検証で、$g^5=e$、$ghg^{-1}=h^2$、$k=0,\ldots,5$ に対する $g^khg^{-k}=h^{2^k}$、そして $o(h)=31$ が確認された。また、数百個のランダムな置換について、$-12\le m\le 12$ の範囲で (i) と (ii) も検証した。

## よくある間違い

- (ii) で $m\ge 1$ の場合だけを証明してしまう。問題文には**任意の整数**とあるので、$m=0$ と負の $m$ にはそれぞれ（短い）議論が必要である。
- $h^{31}=e$ から直ちに $o(h)=31$ と結論してしまう。そこからわかるのは $o(h)\mid 31$ だけであり、31 が素数であることと条件 $h\neq e$ も必要である。

## STEP のその先へ

写像 $x\mapsto gxg^{-1}$ は $G$ の**自己同型**（automorphism）（構造を保つ全単射（bijection））であり、小問 (ii) はそのことから導かれる帰結の一つである。小問 (iii) は**半直積**（semidirect product）の小さな例である。$g$ と $h$ で生成される群の位数は $5\times 31=155$ であり、その存在は 31 を法とする 2 の位数が 5 であることに依存している。この構成は、位数の小さな群を分類するうえで中心的な役割を果たす。位数、共役、ラグランジュ（Lagrange）の定理について学ぶには、Allenby の *Rings, Fields and Groups*（環・体・群）がよい出発点である。

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。