解答例

STEP III 1990、第 3 問

純粋数学 ・ 群の公理と共役

> **STEP III 1990、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/90-s3-q3

鍵となる考え方

3 つの小問はいずれも群の公理（group axioms）だけから導かれ、どの小問でも、ある元を別の元を用いて書き直すことが有効な一手となる。位数（order）2 の元は自分自身の逆元（inverse）であり、これにより (i) は 1 行の計算に帰着する。(ii) と (iii) で用いる道具は**共役**（*conjugation*）である。写像 $x \mapsto c^{-1}xc$ は積を保つので、べきをべきに移す。

以下では $x * y$ を xy と書き、単位元（identity）を e と書く。

解答

小問 (i)

元 x の位数が 2 であるのは、$x \neq e$ かつ $x^2 = e$ のとき、そしてそのときに限る。2 つ目の条件は $x^{-1} = x$ ということである。よって

$$a^{-1} = a, \qquad b^{-1} = b, \qquad (ab)^{-1} = ab.$$

群の任意の元について $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。実際、$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$ である。したがって

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

となり、a と b は可換（commute）である。

小問 (ii)

まず、dc は cd の共役元（conjugate）であることに注意する。

$$c^{-1}(cd)\,c = (c^{-1}c)\,dc = dc.$$

考えてみよう $dc = c^{-1}(cd)c$ と書くことが、なぜ位数を調べるのに役立つのか。

共役はべきと交換できるからである。任意の x と任意の正の整数 n に対して

$$(c^{-1}xc)^n = (c^{-1}xc)(c^{-1}xc)\cdots(c^{-1}xc) = c^{-1}x^nc,$$

が成り立つ。途中で隣り合う $c\,c^{-1}$ がすべて打ち消し合うからである。$x = cd$ とおくと $(dc)^n = c^{-1}(cd)^nc$ を得る。ここで

$$(dc)^n = e \iff c^{-1}(cd)^nc = e \iff (cd)^n = cec^{-1} = e,$$

であり、2つ目の同値では左から c、右から c^{-1} を掛けている（逆向きには c^{-1} と c を掛ける）。よって、$(cd)^n = e$ を満たす正の整数 n は、$(dc)^n = e$ を満たす正の整数 n とちょうど一致する。位数はそのような n の最小値であるから、cd と dc の位数は等しい。そのような n が存在しない場合は、両者とも位数が無限大となるので、この場合にも主張は成り立つ。

小問 (iii)

$c^{-1}bc = b^r$ が与えられている。正の整数 s に対して、(ii) の打ち消し合いの議論により

$$c^{-1}b^sc = (c^{-1}bc)^s = (b^r)^s = b^{sr}.$$

を得る。$s = 0$ のときも同じ式が成り立つ（両辺とも e である）。s が負のときは、$t > 0$ として $s = -t$ と書く。すると $(c^{-1}b^tc)(c^{-1}b^{-t}c) = e$ であるから、$c^{-1}b^sc = (c^{-1}b^tc)^{-1}$ となる。よって

$$c^{-1}b^sc = (b^{tr})^{-1} = b^{-tr} = b^{sr}.$$

以上より、すべての整数 s に対して $c^{-1}b^sc = b^{sr}$ が成り立つ。

2つ目の結果は、$n \geq 1$ に関する数学的帰納法（induction）で、すべての整数 s について同時に示す。$n = 1$ の場合はいま証明したことそのものである。すべての整数 s に対して $c^{-n}b^sc^n = b^{sr^n}$ が成り立つと仮定する。このとき

$$\begin{aligned} c^{-(n+1)}\,b^s\,c^{n+1} &= c^{-1}(c^{-n}b^sc^n)c \\ &= c^{-1}\,b^{sr^n}\,c \\ &= b^{(sr^n)r} = b^{sr^{n+1}}, \end{aligned}$$

となる。ただし最後の行では、1つ目の結果を s の代わりに整数 sr^n に対して用いた。これで帰納法が完成し、すべての正の整数 n に対して $c^{-n}b^sc^n = b^{sr^n}$ が成り立つ。

考えてみよう なぜわざわざ1つ目の結果を負の s についても証明したのか。

r が負の場合（たとえば二面体群（dihedral group）における $c^{-1}bc = b^{-1}$）、s が正であっても sr^n は負になりうる。そして帰納法のステップでは、1つ目の結果を s の代わりに sr^n に対して用いている。すべての整数 s について証明しておくことで、r の符号によらず帰納法が機能するのである。

検算

小さな群で確かめてみよう。正方形の対称性のなす群において、2本の対角線に関する鏡映とその積（半回転）はいずれも位数2であり、(i) の予想どおり、2つの鏡映は確かに可換である。S_3 において $c = (12)$、$d = (13)$ とすると、cd と dc は2つの3-巡回置換であり、どちらも位数は3である。(iii) については、二面体群において鏡映 c と回転 b は $c^{-1}bc = b^{-1}$ を満たすので $r = -1$ であり、公式は $c^{-n}b^sc^n = b^{(-1)^ns}$ を与える。これは正しい。鏡映による共役を2回行うと何も変わらないからである。さらに、3つの主張すべてを計算機でも確認した。S_4（(i) については S_5 も）のすべての該当する元について網羅的に調べ、また13を法とする写像 $x \mapsto ux + v$ のなす群でも確かめた。

よくある間違い

- $(ab)^{-1} = a^{-1}b^{-1}$ と書いてしまうこと。順序は逆になる。そしてこの逆転こそが (i) を成り立たせている。
- (ii) で $(cd)^n = e \Rightarrow (dc)^n = e$ だけを証明すること。両方向が必要であり（あるいは対称性を用いて c と d の役割を入れ替えてもよい）、位数が無限大の場合にも言及すべきである。
- (iii) で、2つ目の結果について帰納法を用いず、点を3つ並べて書くだけの「証明」をすること。

STEP のその先へ

写像 $x \mapsto c^{-1}xc$ は群の**自己同型**（*automorphism*）である。すなわち、G から自分自身への全単射（bijection）で演算を保つものであり、したがって位数を保ち、べきをべ

きに移す。小問 (iii) は**半直積**（*semidirect products*）における鍵となる関係式である。$c^{-1}bc = b^r$ を満たす b と c で生成される群には、二面体群（$r = -1$）や、素数を法とする写像 $x \mapsto ux + v$ のなす群が含まれる。Allenby の *Rings, Fields and Groups*（『環・体・群』）では、共役とこれらの例が丁寧に展開されている。

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。