【問題】 G を位数 8 の非可換群とし，e をその単位元とする．以下を説明せよ．

(1) G は位数 8 の元を持たない．
(2) G は位数 4 の元を持つ．以下，位数 4 の元の一つを a とする．
(3) ある元 $b \in G$ が存在して，G は a, b で生成される．
(4) $bab^{-1} = a^3$.
(5) $b^2 = e$ または $b^2 = a^2$ が成り立つ．

(H22 年度九大数理学府)

【解答】 (1) 位数 8 の元を持つとすれば G は巡回群，従って可換群となり，G が非可換であるという仮定に反する．

(2) 仮に位数 4 の元がないとすると，各元の位数は 8 の約数だから，(1) より単位元以外の元の位数は 2 である．今，単位元以外の任意の $a, b \in G$ をとる．このとき $a^2 = b^2 = e$ および $(ab)^2 = abab = e$ となる．後者の両辺に左より a，右より b を掛けると

$$ba \;=\; a^2bab^2 \;=\; a(abab)b \;=\; aeb \;=\; ab$$

となり，a, b は可換，したがって G は可換群となるが，これは再び G が非可換であることに反する．故に G は位数 4 の元を持つ．

(3) a で生成される部分群を $H = \{e, a, a^2, a^3\}$ とする．H の位数は 4 だから，Lagrange の定理より左剰余類の数 $|G/H|$ は 2, 従って $G/H = \{H, bH\}$ $(b \notin H)$ となる $b \in G$ が存在する．これより

$$G = H \amalg bH = \{e, a, a^2, a^3\} \amalg \{b, ba, ba^2, ba^3\}$$

となり，G は a, b によって生成される事が分かる．

(4) $bab^{-1} = ba^i \in bH$ $(i = 0, 1, 2, 3)$ だとする．このとき $b^{-1} = a^{-1}b^{-1}ba^i = a^{i-1} \in H$ となり，$b \notin H$ という仮定に反する．故に $bab^{-1} = a^i$ $(i = 0, 1, 2, 3)$ と表される．

- $bab^{-1} = e$ だとすると $a = e$ となり $a \neq e$ に反する．
- $bab^{-1} = a$ だとすると $ba = ab$ となり G の非可換性に反する．
- $bab^{-1} = a^2$ だとすると

$$ba^2b^{-1} = bab^{-1}bab^{-1} = (bab^{-1})^2 = (a^2) = a^4 = e, \qquad a^2 = b^{-1}eb = e$$

となるが，a の位数が 4 である事に反する．

以上より $bab^{-1} = a^3$ となる．

(5) (4) の結果より H は G の正規部分群，従って G/H は位数 2 の群，特に $(bH)^2 = b^2H = eH$ となる．これは $b^2 = a^i \in H$ $(i = 0, 1, 2, 3)$ と表される事を意味する．仮に $b^2 = a$ だとすると (4) の結果より

$$b^2 = b^2 \cdot b \cdot b^{-1} = b \cdot b^2 \cdot b^{-1} = bab^{-1} = a^3, \qquad \therefore \quad b^2 \cdot b^2 = a \cdot a^3 = a^4 = e$$

再び $a = b^2$ である事から a の位数が 2 となってしまい，a の位数が 4 である事に反する．同様に $b^2 = a^3$ だとすると

$$b^2 = b \cdot b^2 \cdot b^{-1} = ba^3b^{-1} = (bab^{-1})^3 = a^9 = a$$

より $b^2 \cdot b^2 = a^3 \cdot a = e$ となるから $a^2 = a^6 = (b^2)^2 = e$，即ち a の位数が 2 となってしまい，再び a の位数が 4 である事に反する．　故に b^2 は e または a^2 である． □

〈雑感〉 与えられた条件より丹念に可能性を潰していき，予想された結果を導いていく様はホームズの推理の方法と似ている．公式を組み合わせて答えを作っていく積分の問題などとは根本的に異なっている．楽しいですね．

【問題】　整数係数の 3 次以下の多項式であって，定数項が 1 であるもの全体のなす集合 M で表す：

$$M = \{1 + ax + bx^2 + cx^3 \mid a, b, c \in \mathbb{Z}\}.$$

M に演算 $*$ を，各 $f, g \in M$ に対し

$$f * g = \left(\begin{array}{l} \text{多項式としての普通の積 } fg \text{ の} \\ \text{4 次以上の項を無視したもの} \end{array} \right) \in M$$

と定義する．

(1)　M はこの演算 $*$ に関し Abel 群をなすことを示し，$1 + ax + bx^2 + cx^3 \in M$ の逆元を求めよ．

(2)　この Abel 群 M は有限生成自由 Abel 群であることを示し，その ($\mathbb{Z}$ 加群としての) 基底を一つ求めよ．

(3)　M の三つの元

$$f_1 = 1 + 2x + x^2 + 2x^3, \quad f_2 = 1 + 6x^2 + 6x^3, \quad f_3 = 1 + 2x - 5x^2 - 16x^3$$

により生成される M の部分群を N とする．このとき，剰余群 M/N の Abel 群としての構造を求めよ．

(H16 年度九大数理学府)

【解答】　(1)　$f_i = 1 + a_i x + b_i x^2 + c_i x^3$　$(i = 1, 2, 3)$ に対し

$$\begin{aligned}
(f_1 * f_2) * f_3 =& \{1 + (a_1 + a_2)x + (b_1 + a_2 a_1 + b_2)x^2 + (a_1 b_2 + a_2 b_1 + c_1 + c_2)x^3\}(1 + a_3 x + b_3 x^2 + c_3 x^3) \\
=& \{1 + (a_1 + a_2 + a_3)x + (a_1 a_2 + a_2 a_3 + a_3 a_1 + b_1 + b_2 + b_3)x^2 \\
& + (a_1 a_2 a_3 + a_1(b_2 + b_3) + a_2(b_3 + b_1) + a_3(b_1 + b_2) + c_1 + c_2 + c_3\}x^3 \\
f_1 * (f_2 * f_3) =& (1 + a_1 x + b_1 x^2 + c_1 x^3)\{1 + (a_2 + a_3)x + (b_2 + a_3 a_2 + b_3)x^2 + (a_2 b_3 + a_3 b_2 + c_2 + c_3)x^3\} \\
=& 1 + (a_1 + a_2 + a_3)x + (a_1 a_2 + a_2 b a_3 + a_3 a_1 + b_1 + b_2 + b_3)x^2 \\
& + \{a_1 a_2 b a_3 + a_1(b_2 + b_3) + a_2(b_3 + b_1) + a_3(b_1 + b_2) + c_1 + c_2 + c_3\}x^3
\end{aligned}$$

より $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$，即ち結合律が成立する．また

$$\begin{aligned}
f_1 * f_2 =& \{1 + (a_1 + a_2)x + (b_1 + a_2 a_1 + b_2)x^2 + (a_1 b_2 + a_2 b_1 + c_1 + c_2)x^3\} \\
f_2 * f_1 =& \{1 + (a_2 + a_1)x + (b_2 + a_1 a_2 + b_1)x^2 + (a_2 b_1 + a_1 b_2 + c_2 + c_1)x^3\}
\end{aligned}$$

より $f_1 * f_2 = f_2 * f_1$，即ち交換律が成立する．　$f * 1 = 1 * f = f$ より 1 が零元であり，$f = 1 + ax + bx^2 + cx^3$ に対し $g = 1 - ax - (b - a^2)x^2 - (a^3 - 2ab + c)x^3$ とすれば $f * g = 1$ となる．

(2)　$f \in M$ の n 倍を nf と記す．$e_1 = 1 + x$, $e_2 = 1 + x^2$, $e_3 = 1 + x^3$ のとき，任意の $n \in \mathbb{Z}$ に対して

$$ne_1 = 1 + nx + \frac{n(n-1)}{2}x^2 + \frac{n(n-1)(n-2)}{6}x^3, \qquad ne_2 = 1 + nx^2, \qquad ne_3 = 1 + nx^3$$

である．

・　$n_1, n_2, n_3 \in \mathbb{Z}$ について $n_1 e_1 * n_2 e_2 * n_3 e_3 = 1$ だとすると

$$n_2 e_2 * n_3 e_3 = -n_1 e_1 = 1 - n_1 x + \frac{n_1(n_1+1)}{2}x^2 - \frac{n_1(n_1+1)(n_1+2)}{6}x^3$$

が成立．左辺は $1 + bx^2 + cx^3$ という形になるから $n_1 = 0$ となる．更に $1 + n_2 x^2 = n_2 e_2 = -n_3 e_3 = 1 - n_3 x^3$ より $n_2 = n_3 = 0$ となる．従って e_1, e_2, e_3 は $\mathbb{Z}$ 上 1 次独立である．

・　$f = 1 + ax + bx^2 + cx^3 \in M$ に対し

$$\begin{aligned}
& ae_1 * \left\{b - \frac{a(a-1)}{2}\right\} e_2 * \left\{c - ab + \frac{a(a^2-1)}{3}\right\} e_3 \\
=& \left\{1 + ax + \frac{a(a-1)}{2}x^2 + \frac{a(a-1)(a-2)}{6}x^3\right\} * \left\{1 + \left(b - \frac{a(a-1)}{2}\right)x^2 + \left(c - ab + \frac{a(a^2-1)}{3}\right)x^3\right\} \\
=& 1 + ax + \frac{a(a-1)}{2}x^2 + \frac{a(a-1)(a-2)}{6}x^3 \\
& + \left(b - \frac{a(a-1)}{2}\right)x^2 + \left(ab - \frac{a^2(a-1)}{2}\right)x^3 + \left(c - ab + \frac{a(a^2-1)}{3}\right)x^3 = 1 + ax + bx^2 + cx^3
\end{aligned}$$

より $f = ae_1 * (b - \frac{a(a-1)}{2})e_2 * (c - ab + \frac{a(a^2-1)}{3})e_3$ となり，e_1, e_2, e_3 は M を生成する．

従って e_1, e_2, e_3 は M の $\mathbb{Z}$ 上の基底となり，M は有限生成 Abel 群である．

(3) (2) の計算より

$$f_1 = 2e_1 * 0e_2 * 2e_3, \qquad f_2 = 0e_1 * 6e_2 * 6e_3, \qquad f_3 = 2e_1 * (-6)e_2 * (-4)e_3$$

となる．ここで $A = \begin{bmatrix} 2 & 0 & 2 \\ 0 & 6 & -6 \\ 2 & 6 & -4 \end{bmatrix}$，$P = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$，$Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ とすれば $P, Q \in GL_3(\mathbb{Z})$，かつ $Q^{-1}AP = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ となる．前者より

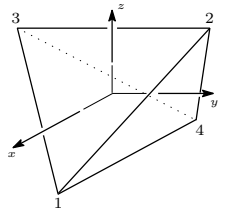
$$(\widetilde{e_1}, \widetilde{e_2}, \widetilde{e_3}) = (e_1 * e_3, e_2 * e_3, e_3), \qquad (\widetilde{f_1}, \widetilde{f_2}, \widetilde{f_3}) = (f_1, f_2, (-1)f_1 * f_2 * f_3)$$

と置けば $(\widetilde{e_1}, \widetilde{e_2}, \widetilde{e_3})$ は再び M の $\mathbb{Z}$ 上の基底，$(\widetilde{f_1}, \widetilde{f_2}, \widetilde{f_3})$ は N の生成系であり，後者より $(\widetilde{f_1}, \widetilde{f_2}, \widetilde{f_3}) = (2\widetilde{e_1}, 6\widetilde{e_2}, 0\widetilde{e_3})$ となる．従って

$$M/N \simeq (\mathbb{Z}\widetilde{f_1} * \mathbb{Z}\widetilde{f_2} * \mathbb{Z}\widetilde{f_3})/(2\mathbb{Z}\widetilde{e_1} * 6\mathbb{Z}\widetilde{e_2} * 0\widetilde{e_2}) \simeq \mathbb{Z}^3/(2\mathbb{Z} \oplus 6\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$$

中国式剰余定理より $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ だから $M/N \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}$ となる． □

【問題】 3 次元空間 $\mathbb{R}^3$ 内の原点を重心に持つ正四面体 T を下図のように取り，その各頂点に下のように番号を付ける．T を T の上に移す $\mathbb{R}^3$ の向きを保つ線型変換全体のなす群 G を考える．



(1) $G_4 := \{g \in G \mid g(4) = 4\}$ は $\mathbb{Z}/3\mathbb{Z}$ に同型であることを示せ．

(2) $\mathbb{R}^3$ の恒等変換を e と書く．

$$K := \{g \in G \mid g(i) \neq i \ (1 \leq i \leq 4)\} \cup \{e\}$$

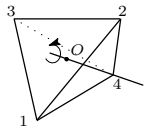
は G の正規部分群であることを示せ．

(3) 商群 G/K を決定し，G を求めよ．

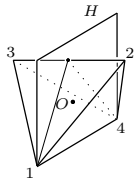
(H15 年度九大数理学府)

【解答】 $g \in G$ を頂点の集合 $\{1,2,3,4\}$ に制限したものを σ_g とする．これを 4 次対称群 $\mathfrak{S}_4$ の元と考え，この対応により G から $\mathfrak{S}_4$ への群の準同型 σ を定義する．原点を始点，頂点 i を終点とするベクトルを $\boldsymbol{v}_i$ とする．このとき $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$ は $\mathbb{R}^3$ の基底であり，σ_g が $\mathfrak{S}_4$ の単位元だとすると，g は基底 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$ を不変にするから，g は恒等変換，即ち σ は単射である．

(1) σ_g を $\{1,2,3,4\}$ の置換と考えれば $g \in G_4 \Leftrightarrow \sigma_g(4) = 4$ でありさらに 3 頂点 $1,2,3$ について順序 $1 \to 2 \to 3 \to 1$ を変えない．そのような置換は e (単位置換)，および $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ の 3 種類から成る．$\sigma = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ とすれば $\sigma^2 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$, $\sigma^3 = e$ であるから，$1 + 3\mathbb{Z} \mapsto \sigma$ という対応で $\mathbb{Z}/3\mathbb{Z} \simeq G_4$ となる事が分かる



(2) $k \in K$ $(k \neq e)$, $g \in G$ とする．任意の $1 \leq i \leq 4$ に対し $j = g^{-1}(i)$ とすれば $kg^{-1}(i) = k(j) \neq j = g^{-1}(i)$ より $gkg^{-1}(i) \neq i$ となり，従って $gkg^{-1} \in K$，即ち K は G の正規部分群となる．



(3) (a) (2 個以上の頂点を固定する場合) $g \in G$ について $\sigma_g(i) = i, \sigma_g(j) = j$ $(1 \leq i < j \leq 4)$ だとする．このとき $\boldsymbol{v}_i$, $\boldsymbol{v}_j$ を含む平面 H の各点は g によって固定される．一方，$\{k,\ell\} = \{1,2,3,4\} \setminus \{i,j\}$ とするとき，k,ℓ を通る直線は平面 H に直交している (左図の例参照)．仮に $\sigma_g(k) = \ell$ $(\sigma_g(\ell) = k)$ ならば，σ_g は H に直交するベクトルを -1 倍する．これは g が $\mathbb{R}^3$ の向きを保存するという仮定に反する．従って σ_g は各頂点を固定し，故に g は恒等変換となる．即ち，2 個以上の頂点を固定する $g \in G$ は恒等変換しかない．

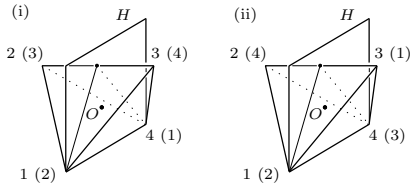
(b) (唯 1 つの頂点を固定する場合) (1) と同様に考えれば，ただ 1 個の頂点を固定する変換，に対応する $\mathfrak{S}_4$ の元は次の 8 個である事が分かる．

$$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$$

(c) (固定される頂点がない場合) 頂点 1 を頂点 2 に移す変換 g について考える．

(i) $g(2) = 3$ だとする．$g(3) = 1$ ならば頂点 4 は固定されるので $g(3) = 4$, $g(4) = 1$ となる (図 (i) 参照)．

(ii) $g(2) = 4$ だとすると $g(4) = 1$ ならば頂点 3 は固定されるので $g(4) = 3$, $g(3) = 1$ となる (図 (ii) 参照)．



※ カッコ内は変換前の頂点を表す

(i) (ii) の場合共に g は $\overrightarrow{32}$ を $\overrightarrow{23}$ に移し，従って g は向きを保存しない．故に $g(2)=1$ であり，更に $g(3)=4$, $g(4)=3$ となる．上と同様に考えれば，頂点を固定しない変換に対応する $\mathfrak{S}_4$ の元は次の 3 個である事が分かる．

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\qquad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\qquad \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

ここに恒等置換を合わせたものが K となる．

以上の考察より G は 8+4=12 個の変換から成る群，K は 4 個の元から成る部分群だから，その商群 G/K の位数は $12\div 4=3$ となる．故に G/K は 3 次の巡回群 $\mathbb{Z}/3\mathbb{Z}$ と同型． □