代数学 I 期末テスト問題 3、4 解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 3

n 次 2 面体群を

$$D_n = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$$

と書く．ここで、$\sigma^n = e$、$\tau^2 = e$、$\sigma\tau = \tau\sigma^{-1}$ である．以下の問に答えよ．

(1) n を 3 以上の整数、$k, \ell \in \{0, 1 \dots, n-1\}$ とする．このとき、以下の D_n の元 (a)、(b)、(c)、(d) を再び $\sigma^{m'}$、あるいは $\sigma^{m'}\tau$ $(m' \in \mathbb{Z})$ の形で表せ (答えのみでよい)．

(a) $\sigma^k(\sigma^\ell)(\sigma^k)^{-1}$ (b) $(\sigma^k\tau)(\sigma^\ell)(\sigma^k\tau)^{-1}$ (c) $\sigma^k(\sigma^\ell\tau)(\sigma^k)^{-1}$ (d) $(\sigma^k\tau)(\sigma^\ell\tau)(\sigma^k\tau)^{-1}$.

(2) D_3 の共役類を具体的な元を用いてすべて記述せよ (答えのみでよい)．

(3) n を 3 以上の整数、$k, \ell \in \{0, 1 \dots, n-1\}$ とする．このとき、以下の D_n の元 (a)、(b)、(c)、(d) を再び $\sigma^{m'}$、あるいは $\sigma^{m'}\tau$ $(m' \in \mathbb{Z})$ の形で表せ (答えのみでよい)．

(a) $[\sigma^k, \sigma^\ell]$ (b) $[\sigma^k\tau, \sigma^\ell]$ (c) $[\sigma^k, \sigma^\ell\tau]$ (d) $[\sigma^k\tau, \sigma^\ell\tau]$.

ここで、任意の 2 元 $g, h \in D_n$ に対し、$[g, h] := ghg^{-1}h^{-1}$ である．

(4) D_4 の交換子群 $\mathrm{D}(D_4)$ を具体的な元を用いて記述せよ (答えのみでよい)．また、D_4 が可解か非可解かを理由を付けて述べよ．

問題 3 解答例.

(1)

(a) σ^ℓ (b) $\sigma^{-\ell}$ (c) $\sigma^{\ell+2k}\tau$ (d) $\sigma^{2k-\ell}\tau$

□

(2) $\{e\}$、$\{\sigma, \sigma^2\}$、$\{\tau, \sigma\tau, \sigma^2\tau\}$. □

(3)

(a) e (b) $\sigma^{-2\ell}$ (c) σ^{2k} (d) $\sigma^{2(k-\ell)}$

□

(4) $\mathrm{D}(D_4) = \{e, \sigma^2\}$. さらに、$\mathrm{D}(D_4)$ は可換群なので、$\mathrm{D}(\mathrm{D}(D_4)) = \{e\}$. よって、$D_4$ は可解である． □

問題 3(1) 補足解説. $\sigma\tau = \tau\sigma^{-1}$ の両辺に左から σ^{-1}、右から σ をかけて $\tau\sigma = \sigma^{-1}\tau$ も成立するので、これらを繰り返し用いると、任意の $k \in \mathbb{Z}$ に対して、

$$\tau\sigma^k = \sigma^{-k}\tau$$

が成立する．これを用いて計算を行う． □

問題 3(2) 補足解説. まず、共役類の定義を思い出す．

* Department of Mathematical Sciences, Shibaura Institute of Technology, 307 Fukasaku, Minuma-ku, Saitama-shi, Saitama, 337-8570, JAPAN *e-mail* : hoya@shibaura-it.ac.jp

定義. G を群とする. 各 $g \in G$ に対し、g **を含む共役類** $K(g)$ は、

$$K(g) := \{hgh^{-1} \mid h \in G\}$$

と定義される. これは同値関係

$$g_1 \sim g_2 \;\Leftrightarrow\; \text{ある } h \in G \text{ が存在して、} g_1 = hg_2h^{-1}$$

に関する同値類であることに注意する. なお $g_1 \sim g_2$ のとき、g_1 **と** g_2 **は共役である**という.

最初に単位元 e を含む共役類を考えると、任意の $h \in D_3$ に対し、$heh^{-1} = e$ なので、$K(e) = \{e\}$ である. なおこれは任意の群 G で正しい.

次に $\sigma \in D_3$ の共役類を考えると、(1) の (a)、(b) での計算より、

$$\begin{aligned} K(\sigma) &= \{\sigma^k\sigma(\sigma^k)^{-1}, (\sigma^k\tau)\sigma(\sigma^k\tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\sigma, \sigma^{-1}\} = \{\sigma, \sigma^2\}. \end{aligned}$$

ここで、共役類は共役という同値関係に関する同値類なので、$\sigma^2 \in K(\sigma)$ であることから、$K(\sigma) = K(\sigma^2)$ となることに注意する.

$K(e)$、$K(\sigma)$ のいずれにも含まれない元として、τ をとる. このとき、(1) の (c)、(d) での計算より、

$$\begin{aligned} K(\tau) &= \{\sigma^k\tau(\sigma^k)^{-1}, (\sigma^k\tau)\tau(\sigma^k\tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\tau, \sigma^2\tau, \sigma^4\tau\} = \{\tau, \sigma\tau, \sigma^2\tau\}. \end{aligned}$$

ここで、$\sigma^3 = e$ を用いた. 以上より、$D_3 = K(e) \cup K(\sigma) \cup K(\tau)$ となるので、D_3 の共役類は $K(e)$、$K(\sigma)$、$K(\tau)$ で全てである.

全く同様の計算により、一般の 3 以上の整数 n に対して、D_n の共役類への分解は

$$\begin{cases} n \text{ が奇数のとき、} D_n = \{e\} \cup \{\sigma, \sigma^{n-1}\} \cup \cdots \{\sigma^{\frac{n-1}{2}}, \sigma^{\frac{n+1}{2}}\} \cup \{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\} \\ n \text{ が偶数のとき、} D_n = \{e\} \cup \{\sigma, \sigma^{n-1}\} \cup \cdots \{\sigma^{\frac{n}{2}-1}, \sigma^{\frac{n}{2}+1}\} \cup \{\sigma^{\frac{n}{2}}\} \cup \{\tau, \sigma^2\tau, \ldots, \sigma^{n-2}\tau\} \cup \{\sigma\tau, \sigma^3\tau, \ldots, \sigma^{n-1}\tau\} \end{cases}$$

となる. □

問題 3(3) 補足解説. 問題 3(1) 補足解説に述べた式を用いて、(1) と同様の計算を定義に基づいて行えばよい.
□

問題 3(4) 補足解説. $\mathrm{D}(D_4)$ は定義より $\{[g, h] \mid g, h \in D_4\}$ で生成される. (3) より、これは σ^2 で生成される群 $\{\sigma^{2m} \mid m \in \mathbb{Z}\}$ に等しいが、D_4 においては $\sigma^4 = e$ より、$\mathrm{D}(D_4) = \{e, \sigma^2\}$ となる. これは D_4 の中心でもある.

また一般の 3 以上の整数 n に対して、

$$\begin{cases} n \text{ が奇数のとき、} \mathrm{D}(D_n) = \{e, \sigma, \sigma^2, \cdots, \sigma^{n-1}\} \\ n \text{ が偶数のとき、} \mathrm{D}(D_n) = \{e, \sigma^2, \sigma^4, \cdots, \sigma^{n-2}\} \end{cases}$$

となる. さらにこれらは共に可換群なので、$\mathrm{D}(\mathrm{D}(D_n)) = \{e\}$ となり D_n は可解群となることがわかる. □

問題 4

以下の事実を証明せよ.

(1) $\mathbb{Z}/15\mathbb{Z}$ と $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ は同型である.

(2) $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ は同型でない.

(3) 2 次一般線型群 $GL_2(\mathbb{R})$ の元 $\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}$ は位数が無限である.

問題 4 解答例.

(1) 写像 $f\colon \mathbb{Z}\to\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}, n\mapsto(n+3\mathbb{Z}, n+5\mathbb{Z})$ を考えると、これは加法群の群準同型である. また、

$$\begin{aligned}\operatorname{Ker} f &= \{n\in\mathbb{Z}\mid n+3\mathbb{Z}=3\mathbb{Z}, n+5\mathbb{Z}=5\mathbb{Z}\}\\ &= \{n\in\mathbb{Z}\mid n\in3\mathbb{Z}, n\in5\mathbb{Z}\}\\ &= \{n\in\mathbb{Z}\mid n\text{ は }3\text{ の倍数かつ }5\text{ の倍数 }\}\\ &= \{n\in\mathbb{Z}\mid n\text{ は }15\text{ の倍数 }\}=15\mathbb{Z}.\end{aligned}$$

よって、準同型定理より $\mathbb{Z}/15\mathbb{Z}\simeq\operatorname{Im} f\subset\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ であるが、$\mathbb{Z}/15\mathbb{Z}$ と $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ はともに位数 15 なので、$\operatorname{Im} f=\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ である. よって、$\mathbb{Z}/15\mathbb{Z}\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ である. □

(2) $n\in\mathbb{Z}$ に対し、$n+2\mathbb{Z}\in\mathbb{Z}/2\mathbb{Z}$ を $\overline{n}$ と表記することにすると、

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}=\{(\overline{0},\overline{0}),(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{1})\}$$

である. ここで、

$$\begin{aligned}(\overline{1},\overline{0})+(\overline{1},\overline{0})&=(\overline{2},\overline{0})=(\overline{0},\overline{0})\\ (\overline{0},\overline{1})+(\overline{0},\overline{1})&=(\overline{0},\overline{2})=(\overline{0},\overline{0})\\ (\overline{1},\overline{1})+(\overline{1},\overline{1})&=(\overline{2},\overline{2})=(\overline{0},\overline{0})\end{aligned}$$

より、

$$\operatorname{ord}(\overline{0},\overline{0})=1 \qquad \operatorname{ord}(\overline{1},\overline{0})=\operatorname{ord}(\overline{0},\overline{1})=\operatorname{ord}(\overline{1},\overline{1})=2.$$

一方、$\mathbb{Z}/4\mathbb{Z}$ は位数 4 の元 $1+4\mathbb{Z}$ を持つ巡回群である. よって、$\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ とは同型ではない. □

(3) 背理法で証明する. $g=\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}$ とし、g の位数が $n(<\infty)$ であるとすると、$g^n=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ より、$\det(g^n)=1$ である. さらに行列式 $\det\colon GL_2(\mathbb{R})\to\mathbb{R}^\times$ は群準同型なので、このとき

$$1=\det(g^n)=(\det g)^n=(1\times1-(-2)\times(-2))^n=(-3)^n.$$

群の元の位数は定義より 1 以上の整数であるが、この等式を満たす 1 以上の整数 n は存在しないので矛盾. よって、$\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}$ の位数は無限である. □

問題 4(1) 補足解説. この証明の議論が “うまくいくこと” の本質的な部分は、

$$\{n\in\mathbb{Z}\mid n\text{ は }3\text{ の倍数かつ }5\text{ の倍数 }\}=\{n\in\mathbb{Z}\mid n\text{ は }15\text{ の倍数 }\}$$

の部分である. より一般に、2 以上の整数 m_1、m_2 に対し、

$$\{n\in\mathbb{Z}\mid n\text{ は }m_1\text{の倍数かつ }m_2\text{の倍数 }\}=\{n\in\mathbb{Z}\mid n\text{ は }m_1m_2\text{の倍数 }\}$$

が成立するための必要十分条件は m_1 と m_2 が互いに素であることである．よって、m_1、m_2 が互いに素のときこの等式が成立し、あとは (1) の解答と全く同じ議論により、

$$\mathbb{Z}/m_1m_2\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

となる．特に、n の素因数分解を $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$ (各 p_i は素数であり、$i \neq j$ のとき、$p_i \neq p_j$) と書くと、上の同型を繰り返し用いて、

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{k_\ell}\mathbb{Z}$$

となる．これは**中国剰余定理** (Chinese remainder theorem) と呼ばれる定理の特別な場合である．

ちなみに、有限群の分類で位数 15 の群は $\mathbb{Z}/15\mathbb{Z}$ に全て同型であることが知られている．(参考書の例 1.9.5 参照.) □

問題 4(3) 補足解説. 解答例の議論より、一般に行列群 $GL_n(\mathbb{R})$ に含まれる位数が有限の元の行列式は何乗かすると 1 になるような値 (つまり、$e^{\frac{2k\pi}{m}}$、$m, k \in \mathbb{Z}_{>0}$ の形) であることがわかる．

なお具体的に計算すると、各 $\ell \in \mathbb{Z}$ に対し、

$$\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}^\ell = \frac{1}{2}\begin{pmatrix} (-1)^\ell + 3^\ell & (-1)^\ell - 3^\ell \\ (-1)^\ell - 3^\ell & (-1)^\ell + 3^\ell \end{pmatrix}$$

となる． □