代数学 I 期末試験解答例

担当：大矢 浩徳 (OYA Hironori)*

以下では，

- $\mathfrak{S}_n = \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \middle| \; i_1, i_2, \dots, i_n \text{は} 1, 2, \dots, n \text{の並べ替え} \right\}$ を n 次対称群，
- $D_n = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$ を n 次 2 面体群，ただし $\sigma^n = e, \tau^2 = e, \tau\sigma = \sigma^{-1}\tau$，

とする．

問題 1 [各 5 点]

以下の問に答えよ．解答は全て<u>答えのみ</u>で良い：

(1) 群準同型写像 $f\colon D_4 \to \mathfrak{S}_4$ であって，

$$\sigma \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

を満たすものが存在する．このとき，$\mathfrak{S}_4$ の元 $f(\tau\sigma^2\tau\sigma^3\tau)$ を $\begin{pmatrix} 1 & 2 & 3 & 4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}$ の形で具体的に求めよ．

(2) 群準同型写像 $f\colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_4$ であって，

$$([1]_2, [0]_2) \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad ([0]_2, [1]_2) \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

を満たすものが存在する．このとき，$\mathfrak{S}_4$ の元 $f(([1]_2, [1]_2))$ を $\begin{pmatrix} 1 & 2 & 3 & 4 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix}$ の形で具体的に求めよ．

(3) 群準同型写像 $f\colon \mathfrak{S}_3 \to GL_2(\mathbb{C})$ であって，

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$

を満たすものが存在する．このとき，$GL_2(\mathbb{C})$ の元 $f\left(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right)$ を具体的に求めよ．

(4) 42 で割ると 8 余り，65 で割ると 2 余る整数を 1 つ求めよ．

問題 1 解答例．

(1) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ □

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ □

(3) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ □

* *e-mail*：hoya@shibaura-it.ac.jp

(4) 4292 (mod 2730 で一致していれば良い) $\square$

問題 2 [各 6 点]

(1) $\mathfrak{S}_3$ とその部分群 $H := \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$ に関する以下の問に答えよ．ただし，解答は全て答えのみで良い：

(1-1) $\mathfrak{S}_3$ における H による左剰余類 ($\mathfrak{S}_3/H$ の元) を全て記述せよ．

(1-2) $\mathfrak{S}_3$ の H に関する左完全代表系を 1 つ記述せよ．

(1-3) $\mathfrak{S}_3$ における H の指数 $[\mathfrak{S}_3 : H]$ はいくらか．

(2) G を位数 27 の群とする．全射群準同型 $f\colon G \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ が存在するとき，$\operatorname{Ker} f$ の位数を求めよ．ただし，計算過程も説明すること．

(3) $\mathfrak{S}_5$ の各元 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ は 1 対 1 写像 $\sigma\colon \{1,2,3,4,5\} \to \{1,2,3,4,5\}, k \mapsto i_k =: \sigma(k)$ と考えられため，$X := \{\{i,j\} \mid i,j \in \{1,2,3,4,5\}\}$ としたとき，

$$\mathfrak{S}_5 \times X \to X, (\sigma, \{i,j\}) \mapsto \sigma.\{i,j\} := \{\sigma(i), \sigma(j)\}$$

は X 上の $\mathfrak{S}_5$ の作用を定める．ここで，$\{i,j\}$ は i,j の 2 元からなる集合の意味であり，特に $\{i,j\} = \{j,i\}$ であることに注意する．また，$\{i,j\} \in X$ は i,j の重複を許す．このとき，以下の問に答えよ．ただし，解答は全て答えのみで良い：

(3-1) $\mathfrak{S}_5$ の $\{2,3\} \in X$ における固定部分群 $(\mathfrak{S}_5)_{\{2,3\}}$ の位数を求めよ．

(3-2) $\mathfrak{S}_5$-軌道 $\mathfrak{S}_5.\{2,3\}$ に含まれる元の個数を求めよ．

(3-3) X における $\mathfrak{S}_5$-軌道の個数を求めよ．

問題 2 解答例.

(1)

(1-1) $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$ $\square$

(1-2) $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$ $\square$

(1-3) $[\mathfrak{S}_3 : H] = 3$ $\square$

(2) 準同型定理より，$G/\ker f \simeq \operatorname{Im} f$ であるが，f は全射なので，$\operatorname{Im} f = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. よって，

$$|G/\ker f| = |\operatorname{Im} f| = |\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}| = 9.$$

これと Lagrange の定理より，

$$|\operatorname{Ker} f| = \frac{|G|}{|G/\ker f|} = \frac{27}{9} = 3.$$

(3)

(3-1) $|(\mathfrak{S}_5)_{\{2,3\}}| = 12$ $\square$

(3-2) $|\mathfrak{S}_5.\{2,3\}| = 10$ $\square$

(3-3) 2 個 $\square$

$\square$

問題 3 [計 22 点]

n 次 2 面体群 D_n に関する以下の問に答えよ．ただし，解答は全て答えのみで良い：

(1) $k, \ell \in \{0, 1 \ldots, n-1\}$ とする．このとき，以下の D_n の元 (a)，(b)，(c)，(d) を再び σ^m，あるいは $\sigma^m \tau$ $(m \in \mathbb{Z})$ の形[*1]で表せ．

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

(2) D_4 の共役類を具体的な元を用いてすべて記述せよ．

(3) D_5 の部分群を全て求めよ．また，その中で正規部分群であるものを挙げよ．

(4) D_6 の中心 $Z(D_6)$ を具体的な元を用いて記述せよ．

問題 3 解答例.

(1)

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

□

(2) $\{e\}$，$\{\sigma, \sigma^3\}$，$\{\sigma^2\}$，$\{\tau, \sigma^2\tau\}$，$\{\sigma\tau, \sigma^3\tau\}$ □

(3) $\{e\}$，$\{e, \tau\}$，$\{e, \sigma\tau\}$，$\{e, \sigma^2\tau\}$，$\{e, \sigma^3\tau\}$，$\{e, \sigma^4\tau\}$，$\{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$，$D_5$

正規部分群であるもの：$\{e\}$，$\{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$，$D_5$

(4) $\{e, \sigma^3\}$ □

問題 4 [計 30 点]

G を位数 18 の群とする．

$$X := \{\{g_1, g_2, g_3\} \subset G \mid g_1, g_2, g_3 \text{は相異なる } G \text{ の } 3 \text{ 元}\}$$

としたとき，

$$G \times X \to X, (g, \{g_1, g_2, g_3\}) \mapsto \{gg_1, gg_2, gg_3\}$$

は X 上の G の作用を定める (このことは証明しなくて良い)．このとき，以下の問に答えよ：

(1) X の元の個数を求めよ．解答は答えのみで良い．

(2) 任意の $\{g_1, g_2, g_3\} \in X$ に対し，その固定部分群 $G_{\{g_1,g_2,g_3\}}$ の位数は 3 以下であることを証明せよ．

(3) X 上の G の作用は元の個数が 6 である G-軌道を少なくとも 1 つ持つことを証明せよ．

(4) G は位数 3 の部分群を少なくとも 1 つ持つことを証明せよ．

(5) 9 次 2 面体群 D_9 の位数 3 の部分群を具体的に挙げよ．解答は答えのみで良い．

問題 4 解答例.

(1) $|X| = {}_{18}\mathrm{C}_3 = \dfrac{18 \cdot 17 \cdot 16}{3 \cdot 2 \cdot 1} = 816.$ □

(2) $G_{\{g_1,g_2,g_3\}} = \{g \in G \mid \{gg_1, gg_2, gg_3\} = \{g_1, g_2, g_3\}\}$ であるので，各 $g \in G_{\{g_1,g_2,g_3\}}$ に対してある $i \in \{1, 2, 3\}$ が定まり，$gg_1 = g_i$，つまり $g = g_i g_1^{-1}$．よって，

$$G_{\{g_1,g_2,g_3\}} \subset \{g_i g_1^{-1} \mid i = 1, 2, 3\}.$$

これより，$|G_{\{g_1,g_2,g_3\}}| \leq 3.$ □

(3) 各 $\{g_1, g_2, g_3\} \in X$ に対し，

$$|G.\{g_1, g_2, g_3\}| = \frac{|G|}{|G_{\{g_1,g_2,g_3\}}|}$$

[*1] m を $0 \leq m \leq n-1$ に取る必要は無い．

が成立する．(2) より，$|G_{\{g_1,g_2,g_3\}}| \leq 3$ であり，Lagrange の定理よりこの値は $|G| = 18$ の約数であることから，$|G_{\{g_1,g_2,g_3\}}|$ は $1, 2, 3$ のいずれか．よって，$|G.\{g_1, g_2, g_3\}|$ は，$18, 9, 6$ のいずれか．

ここで元の個数が 6 の軌道が存在しないとすると，X を軌道分解したときに元の個数が 18 または 9 の軌道で軌道分解されるので，特に X の元の個数は 9 の倍数となる．しかし，(1) より X の元の個数は 816 で 9 の倍数ではない．これらより，元の個数が 6 である G-軌道が少なくとも 1 つ存在することがわかる．

(4) (3) より元の個数が 6 である G-軌道がとれるので，この軌道に含まれる元を $\{g_1, g_2, g_3\}$ とすると，

$$|G_{\{g_1,g_2,g_3\}}| = \frac{|G|}{|G.\{g_1, g_2, g_3\}|} = \frac{18}{6} = 3.$$

よって，この $G_{\{g_1,g_2,g_3\}}$ が位数 3 の G の部分群の例としてとれる．

(5) $\{e, \sigma^3, \sigma^6\}$ □

問題 5 [各 8 点]

(1) 5 で割ると 4 余り，13 で割ると 10 余り，24 で割ると 2 余る整数を 1 つ求めよ．

(2) $\mathbb{Z}/12\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ は同型でないことを証明せよ．

(3) 加法群 $\mathbb{Q}$ と乗法群 $\mathbb{Q}_{>0}$ は同型でないことを証明せよ．

(4) p を素数とする．このとき，位数 p^k(k は 1 以上の整数) の群 G の中心 $Z(G)$ は $Z(G) \neq \{e\}$ となることを証明せよ．

問題 5 解答例.

(1) 5 と 13 は互いに素なので，中国剰余定理より，5 で割ると 4 余り，13 で割ると 10 余る整数が mod 65 でただ 1 つ存在する．まずこれを求める．

$$13 = 2 \times 5 + 3 \qquad 5 = 1 \times 3 + 2 \qquad 3 = 1 \times 2 + 1$$

より，

$$\begin{aligned} 1 &= 3 - 1 \times 2 = 3 - 1 \times (5 - 1 \times 3) \\ &= 2 \times 3 + (-1) \times 5 = 2 \times (13 - 2 \times 5) + (-1) \times 5 = (-5) \times 5 + 2 \times 13. \end{aligned}$$

いま，

$$10 \times ((-5) \times 5) + 4 \times (2 \times 13) = -146 \equiv 49 \mod 65$$

であるので，5 で割ると 4 余り，13 で割ると 10 余る整数は mod 65 で 49 である数，つまり，65 で割って 49 余る整数である．

これより，65 で割って 49 余り，24 で割ると 2 余る整数を 1 つ求めればよいことがわかる．いま，

$$65 = 2 \times 24 + 17 \qquad 24 = 1 \times 17 + 7 \qquad 17 = 2 \times 7 + 3 \qquad 7 = 2 \times 3 + 1$$

より，

$$\begin{aligned} 1 &= 7 - 2 \times 3 = 7 - 2 \times (17 - 2 \times 7) = 5 \times 7 + (-2) \times 17 \\ &= 5 \times (24 - 1 \times 17) + (-2) \times 17 = 5 \times 24 + (-7) \times 17 \\ &= 5 \times 24 + (-7) \times (65 - 2 \times 24) = 19 \times 24 + (-7) \times 65. \end{aligned}$$

これより求める値の 1 つは，

$$49 \times (19 \times 24) + 2 \times ((-7) \times 65) = 21434. \text{ (答えは mod 1560 で一致していれば良い)}$$

□

(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ の任意の元 $([m_1]_2, [m_2]_6)$ は

$$\underbrace{([m_1]_2, [m_2]_6) + \cdots + ([m_1]_2, [m_2]_6)}_{6\text{ 個}} = ([6m_1]_2, [6m_2]_6) = ([0]_2, [0]_6)$$

を満たす．特に，$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ の元の位数は全て 6 以下である．一方，$\mathbb{Z}/12\mathbb{Z}$ は位数 12 の元 $[1]_{12}$ を持つ．これより，$\mathbb{Z}/12\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ は同型でない． □

注意．本問において，『写像 $f\colon \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, [m]_{12} \mapsto ([m]_2, [m]_6)$ が同型写像とならないことを示す』という方針は不適である．なぜなら，2 つの群が同型でないことを示すためには，「同型写像の候補の 1 つに過ぎない f が実際には同型とならない」ということだけでなく，「どう頑張っても同型写像が作れない」ということを示す必要があるためである．

(3) 背理法で証明する．$f\colon \mathbb{Q} \to \mathbb{Q}_{>0}$ が群同型写像であるとする．f は特に全射であることから，$f(a) = 2$ となる $a \in \mathbb{Q}$ が存在する．このとき，$a/2 \in \mathbb{Q}$ であり，さらに f は群準同型写像であることから，

$$2 = f(a) = f(a/2 + a/2) = f(a/2)^2$$

となる．いま，$f(a/2) \in \mathbb{Q}_{>0}$ であるが，正の有理数であって 2 乗すると 2 となるものは存在しないため，これは矛盾である．よって，$\mathbb{Q}$ と $\mathbb{Q}_{>0}$ は同型でない． □

注意．(2) の注意と同様に，『$\exp\colon \mathbb{R} \to \mathbb{R}_{>0}, x \mapsto e^x$ は群同型写像だが，$\exp(1) = e \notin \mathbb{Q}_{>0}$ より，$\exp(\mathbb{Q}) \not\subset \mathbb{Q}_{>0}$ であるため』というような解答は不適である．1 つ候補を勝手に持ってきて，それではダメだというのではなく，「どう頑張っても同型写像が作れない」ということを示すことが大事である．

(4) G の共役類への分割を，

$$K(e) \cup K(g_1) \cup K(g_2) \cup \cdots \cup K(g_m)$$

とする．(ただし，$K(g)$ は $g \in G$ の共役類を意味し，$i \neq j$ のとき，$K(g_i) \neq K(g_j) (\neq K(e))$ となるとする.)

背理法で証明する．もし，$Z(G) = \{e\}$ となるとすると，全ての $\ell = 1, \ldots, m$ に対し，$K(g_\ell) \neq \{g_\ell\}$ より，$|K(g_\ell)| > 1$ である．一方，共役類は共役作用に関する G-軌道なので，$|K(g_\ell)|$ は $|G| = p^k$ の約数である．これらより，各 $\ell = 1, \ldots, m$ に対し，$|K(g_\ell)|$ は p の倍数となる．よって，

$$p^k = |G| = |K(e)| + |K(g_1)| + \cdots + |K(g_m)| \equiv |K(e)| = 1 \mod p$$

となり，これは矛盾である．以上より，$Z(G) \neq \{e\}$． □