代数学 I 中間試験解答例

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 4 点]

以下の元を括弧内で指定した形に直せ．解答は答えのみで良い．

(1) $\mathbb{Z}/15\mathbb{Z}$ の元 $[18]_{15} + [36]_{15} + [100]_{15}$.　【$[n]_{15}, 0 \leq n \leq 14$ の形】

(2) $(\mathbb{Z}/20\mathbb{Z})^{\times}$ の元 $[13]_{20}^{-1}$.　【$[n]_{20}, 0 \leq n \leq 19$ の形】

(3) $\mathfrak{S}_6$ の元 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$.
【$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix}$ の形】

(4) $\mathfrak{S}_7$ の元 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 6 & 5 & 3 \end{pmatrix}^{-1}$.　【$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \end{pmatrix}$ の形】

(5) D_6 の元 $\tau\sigma^2\sigma^5\tau^3\sigma^{-3}\tau$.　【$\sigma^m$，あるいは$\sigma^m\tau$ $(0 \leq m \leq 5)$ の形】

(6) D_5 の元 $(\sigma^4\tau\sigma)^{-1}$.　【$\sigma^m$，あるいは$\sigma^m\tau$ $(0 \leq m \leq 4)$ の形】

問題 1 解答例．

(1) $[4]_{15}$ □

(2) $[17]_{20}$ □

(3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 6 & 5 \end{pmatrix}$ □

(4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 1 & 6 & 5 & 4 \end{pmatrix}$ □

(5) $\sigma^2\tau$ □

(6) $\sigma^3\tau$ □

* *e-mail*：hoya@shibaura-it.ac.jp

問題 2 [各 8 点]

(1) $527x+408y=34$ を満たす整数の組 (x,y) を全て求めよ．ただし，計算過程も説明すること．

(2) D_3 とその部分群 $T:=\{e,\tau\}$ 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．

(2-1) D_3 における T による左剰余類 (D_3/T の元) を全て記述せよ．

(2-2) D_3 における T による右剰余類 ($T\backslash D_3$ の元) を全て記述せよ．

(2-3) D_3 の T に関する左完全代表系を 1 つ記述せよ．

(2-4) D_3 における T の指数 $[D_3:T]$ はいくらか．

(3) $\mathfrak{S}_4$ の元 $\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$ の位数を求めよ．ただし，計算過程も説明すること．

(4) G を巡回群でない位数 10 の群とする．元 $g\in G$ が $g^5\neq e$ (e は G の単位元) を満たすとき，g の位数を求めよ．ただし，計算過程も説明すること．

問題 2 解答例.

(1) まず，$\gcd(527,408)$ をユークリッド互除法で求める：

$$527=1\times 408+119 \qquad 408=3\times 119+51$$
$$119=2\times 51+17 \qquad 51=3\times 17+0$$

であるので，$\gcd(527,408)=17$．よって，$527x+408y=34(=2\times 17)$ を満たす整数の組 (x,y) は存在し，その 1 つは以下のように求められる．

$$\begin{aligned}34=2\times 17=2\times(119-2\times 51)&=2\times 119+(-4)\times 51\\&=2\times 119+(-4)\times(408-3\times 119)=(-4)\times 408+14\times 119\\&=(-4)\times 408+14\times(527-1\times 408)=14\times 527-18\times 408\end{aligned}$$

より，$(x,y)=(14,-18)$ が $527x+408y=34$ を満たす整数の組 (x,y) の 1 つである．これより，一般に，

$$\begin{aligned}527x+408y=34&\Leftrightarrow 527(x-14)+408(y+18)=0\\&\Leftrightarrow 31(x-14)+24(y+18)=0\ (\text{両辺を}\gcd(756,1064)=28\text{で割った})\\&\Leftrightarrow \text{ある}\ t\in\mathbb{Z}\ \text{を用いて,}\ (x-14,y+18)=(24t,-31t)\end{aligned}$$

となるので，求める整数の組は，$(x,y)=(14+24t,-18-31t),t\in\mathbb{Z}$． □

(2)

(2-1) $T=\{e,\tau\},\sigma T=\{\sigma,\sigma\tau\},\sigma^2T=\{\sigma^2,\sigma^2\tau\}$ □

(2-2) $T=\{e,\tau\},T\sigma=\{\sigma,\tau\sigma\}=\{\sigma,\sigma^2\tau\},T\sigma^2=\{\sigma^2,\tau\sigma^2\}=\{\sigma^2,\sigma\tau\}$ □

(2-3) $\{e,\sigma,\sigma^2\}$ □

(2-4) $[D_3:T]=3$ □

(3)

$$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^1\neq\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^2=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\neq\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

$$\begin{aligned}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^3&=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^2\\&=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}\neq\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\end{aligned}$$

$$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^4=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}^3=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

となるので，$\mathrm{ord}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}=4$ である． □

(4) Lagrange の定理より，$\mathrm{ord}(g)$ は $|G|=10$ の約数である．よって，$\mathrm{ord}(g)$ は $1,2,5,10$ のいずれかである．ここで，$\mathrm{ord}(g)=1$ または 5 とすると，$g^5=e$ となるので仮定に反する．また，$\mathrm{ord}(g)=10$ とすると，位数の定義より $|\langle g\rangle|=10$ となるが，$|G|=10$ より，このとき $G=\langle g\rangle$ となる．これは，G が巡回群でないという仮定に反する．

以上より，$\mathrm{ord}(g)=2$ である． □

問題 3 [各 8 点]

行列群

$$GL_2(\mathbb{C}) := \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{C}, ad-bc\neq 0\right\}$$

を考える．次の部分集合 G_1，G_2，G_3 が，それぞれ $GL_2(\mathbb{C})$ の

(a) 正規部分群となる　(b) 部分群となるが正規部分群ではない　(c) 部分群とならない

のどれになるかを選び，その理由を説明せよ．

(1) $G_1=\left\{\begin{pmatrix}e^{\frac{2m\pi i}{n}}&0\\0&e^{\frac{2m\pi i}{n}}\end{pmatrix}\middle|\, m\in\mathbb{Z}\right\}$.　(2) $G_2=\left\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\middle|\, a,b,d\in\mathbb{C}, ad\neq 0\right\}$.

(3) $G_3=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{C}, ad\neq 0, bc=0\right\}$.

問題 3 解答例.

(1) (a) 正規部分群となる．

理由：G_1 は定義より明らかに空ではない．さらに，各 $m,m'\in\mathbb{Z}$ に対し，

$$\begin{pmatrix}e^{\frac{2m\pi i}{n}}&0\\0&e^{\frac{2m\pi i}{n}}\end{pmatrix}\begin{pmatrix}e^{\frac{2m'\pi i}{n}}&0\\0&e^{\frac{2m'\pi i}{n}}\end{pmatrix}=\begin{pmatrix}e^{\frac{2(m+m')\pi i}{n}}&0\\0&e^{\frac{2(m+m')\pi i}{n}}\end{pmatrix}\in G_1$$

$$\begin{pmatrix}e^{\frac{2m\pi i}{n}}&0\\0&e^{\frac{2m\pi i}{n}}\end{pmatrix}^{-1}=\begin{pmatrix}e^{-\frac{2m\pi i}{n}}&0\\0&e^{-\frac{2m\pi i}{n}}\end{pmatrix}=\begin{pmatrix}e^{\frac{2(-m)\pi i}{n}}&0\\0&e^{\frac{2(-m)\pi i}{n}}\end{pmatrix}\in G_1$$

となるので，G_1 は $GL_2(\mathbb{C})$ の部分群である．次に任意の $g\in GL_2(\mathbb{C})$，$m\in\mathbb{Z}$ に対し，

$$g\begin{pmatrix}e^{\frac{2m\pi i}{n}}&0\\0&e^{\frac{2m\pi i}{n}}\end{pmatrix}g^{-1}=e^{\frac{2m\pi i}{n}}\cdot\left(g\begin{pmatrix}1&0\\0&1\end{pmatrix}g^{-1}\right)=e^{\frac{2m\pi i}{n}}\cdot(gg^{-1})=\begin{pmatrix}e^{\frac{2m\pi i}{n}}&0\\0&e^{\frac{2m\pi i}{n}}\end{pmatrix}\in G_1$$

である．よって，G_1 は $GL_2(\mathbb{C})$ の正規部分群となる． □

(2) (b) 部分群となるが正規部分群ではない．

理由：$\begin{pmatrix}1&0\\0&1\end{pmatrix}\in G_2$ より，G_2 は空ではない．任意の $g,h\in G_2$ に対し，$g=\begin{pmatrix}a&b\\0&d\end{pmatrix}$，$h=\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}$ とすると，

$$gh=\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}=\begin{pmatrix}aa'&ab'+bd'\\0&dd'\end{pmatrix}$$

であり，$(aa')(dd')=(ad)(a'd')\neq 0$ なので，$gh\in G_2$．さらに，$g^{-1}=\dfrac{1}{ad}\begin{pmatrix}d&-b\\0&a\end{pmatrix}$ より，$g^{-1}\in G_2$．以上より，G_2 は $GL_2(\mathbb{C})$ の部分群である．

一方，例えば $\begin{pmatrix}1&1\\0&1\end{pmatrix}\in G_2$ に対し，

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}=\begin{pmatrix}0&1\\-1&2\end{pmatrix}\notin G_2$$

となる．よって，G_2 は正規部分群とならない． □

(3) (c) 部分群とならない．

理由：部分群であるためには任意の $g,h \in G_3$ の元に対して，$gh \in G_3$ である必要がある．しかし，例えば $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in G_3$ に対し，

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

となり，これは $1 \cdot 1 \neq 0$ より，G_3 の元でないため． □

問題 4 [計 20 点]

$\mathfrak{S}_3$ に関する以下の問に答えよ．

(1) $\mathfrak{S}_3$ の部分群を具体的に全て挙げよ．ただし，解答は答えのみで良い．

(2) (1) で挙げたもののうち，正規部分群であるものを全て述べ，それぞれについて正規部分群である理由を説明せよ．(※ (1) で数え落としがあっても (2) は独立に採点します.)

問題 4 解答例.

(1) $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\},$
$\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$, $\mathfrak{S}_3$. □

(2) 正規部分群は，$\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$, $\mathfrak{S}_3$ の 3 つ．

- $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$ が正規部分群であること：
  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ は単位元なので，任意の $\sigma \in \mathfrak{S}_3$ に対し，
  $$\sigma \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \sigma^{-1} = \sigma\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}.$$
  よって，$\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$ は $\mathfrak{S}_3$ の正規部分群である．
- $\mathfrak{S}_3$ が正規部分群であること：
  任意の $\sigma, \sigma' \in \mathfrak{S}_3$ に対し，$\sigma\sigma'\sigma^{-1} \in \mathfrak{S}_3$ であるので，$\mathfrak{S}_3$ 自身は $\mathfrak{S}_3$ の正規部分群である．
- $\mathfrak{A} := \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$ が正規部分群であること：
  $\mathfrak{S}_3$ における $\mathfrak{A}$ の指数 $[\mathfrak{S}_3 : \mathfrak{A}]$ は Lagrange の定理より，
  $$[\mathfrak{S}_3 : \mathfrak{A}] = \frac{|\mathfrak{S}_3|}{|\mathfrak{A}|} = \frac{6}{3} = 2$$
  である．これより，$\sigma_0 \notin \mathfrak{A}$ なる $\mathfrak{S}_3$ の元を任意にとると，$\mathfrak{S}_3$ の $\mathfrak{A}$ による左・右剰余類への分解は
  $$\mathfrak{S}_3 = \mathfrak{A} \cup \sigma_0\mathfrak{A} = \mathfrak{A} \cup \mathfrak{A}\sigma_0$$
  となる．ここで，$\mathfrak{A} \cap \sigma_0\mathfrak{A} = \mathfrak{A} \cap \mathfrak{A}\sigma_0 = \emptyset$ であるので，$\sigma_0\mathfrak{A} = \mathfrak{S}_3 \setminus \mathfrak{A} = \mathfrak{A}\sigma_0$ である．($\mathfrak{S}_3 \setminus \mathfrak{A}$ は商空間ではなく $\mathfrak{A}$ の $\mathfrak{S}_3$ における補集合の意味.)
  よって，各 $\sigma \in \mathfrak{S}_3$ に対して，
  $$\begin{cases} \sigma \in \mathfrak{A} \text{ のとき}, \sigma\mathfrak{A} = \mathfrak{A} = \mathfrak{A}\sigma \\ \sigma \notin \mathfrak{A} \text{ のとき}, \sigma\mathfrak{A} = \mathfrak{S}_3 \setminus \mathfrak{A} = \mathfrak{A}\sigma \end{cases}$$

となる．これより，任意の $\sigma \in \mathfrak{S}_3$ に対して $\sigma\mathfrak{A} = \mathfrak{A}\sigma$ となるので，$\mathfrak{A}$ は $\mathfrak{S}_3$ の正規部分群である．

$\square$

問題 4(1) 補足解説. 一般に群 G は $\{e\}$，G という 2 つの自明な部分群を持つことに注意する．(これらも立派な部分群である.) さらに，これらの自明な部分群は問題 4(2) の解答例と同じ方法で正規部分群であることが示される．

次に，$\mathfrak{S}_3$ の自明でない部分群を全て求めることを考える．$\mathfrak{S}_3$ は位数 6 の部分群であるので，Lagrange の定理より，その部分群の位数は 6 の約数となる．よって，自明でない $\mathfrak{S}_3$ の部分群の位数は 2 または 3 のいずれかである．さらに 2 と 3 は素数なので，再び Lagrange の定理から，$\mathfrak{S}_3$ の自明でない部分群は全て巡回群であることがわかる．これより，$\mathfrak{S}_3$ の自明でない部分群は $\mathfrak{S}_3$ の各元 σ の生成する部分群

$$\langle\sigma\rangle = \{\sigma^m \mid m \in \mathbb{Z}\} = \{e, \sigma, \ldots, \sigma^{\mathrm{ord}(\sigma)-1}\}$$

として全て求められる．$\square$

問題 4(2) 補足解説. $\mathfrak{A} := \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right\}$ が正規部分群であることを示すためには，任意の $\sigma \in \mathfrak{S}_3$，$\sigma' \in \mathfrak{A}$ に対して，

$$\sigma\sigma'\sigma^{-1} \in \mathfrak{A}$$

となることを直接計算で確かめても良い．(しかし計算量は多くなる.) 解答例は第 7 回レポート課題解答の問題 1(2) 補足解説内で示した，以下の命題の証明を本問の設定に焼き直したものである．

命題.

群 G の指数 2 の部分群 H は正規部分群となる．

なお，ここで現れた $\mathfrak{A}$ は *3* **次交代群** (alternating group of degree 3) と呼ばれる群である．一般の n 次交代群は $\mathfrak{S}_n$ の中で，符号 sgn が 1 の元を集めてできる位数 $n!/2$ の $\mathfrak{S}_n$ の部分群 $\mathfrak{A}_n$ として定義される．(符号の定義については第 3 回レポート課題解答の 2 ページ目を参照のこと．) $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$ であり，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の正規部分群である．

なお，解答に挙げたもの以外が正規部分群でないことは解答では求めていないが確認しておくと良い勉強になる．1 つだけやってみると，$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \in \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\right\}$ に対し，

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \notin \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\right\}$$

より，$\left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\right\}$ は正規部分群ではない．$\square$