代数学 I 中間試験解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

空でない集合 G に二項演算

$$\cdot\colon G\times G\to G,\quad (g_1,g_2)\mapsto g_1\cdot g_2$$

が与えられているとする．G がこの二項演算に関して群をなすための必要最低限の条件を述べよ．

問題 1 解答例. (以下に対応することが全て書かれていれば正解)

(I) 任意の $g_1,g_2,g_3\in G$ に対して，$(g_1\cdot g_2)\cdot g_3=g_1\cdot(g_2\cdot g_3)$ が成り立つ．
(II) ある $e\in G$ が存在して，任意の $g\in G$ に対し，$e\cdot g=g=g\cdot e$ が成り立つ．
(III) 任意の $g\in G$ に対して，ある $g'\in G$ が存在し，$g'\cdot g=e=g\cdot g'$ が成り立つ．

□

問題 2

(1) 加法群 $\mathbb{Z}/175\mathbb{Z}$ における部分群

$$H=\{[70m]_{175}\mid m\in\mathbb{Z}\}$$

の位数を求めよ．解答は答えのみで良い．

(2)

$$f\colon \mathbb{Z}/\boxed{ア}\mathbb{Z}\to\mathbb{Z}/\boxed{イ}\mathbb{Z},\ [a]_{\boxed{ア}}\mapsto\left[a^2\right]_{\boxed{イ}}$$

が well-defined な写像を与えるような $\boxed{ア}$, $\boxed{イ}$ の組み合わせとして正しいものを以下から全て選択せよ．

(1) $\boxed{ア}=2,\boxed{イ}=6$
(2) $\boxed{ア}=4,\boxed{イ}=8$
(3) $\boxed{ア}=3,\boxed{イ}=9$
(4) $\boxed{ア}=5,\boxed{イ}=5$
(5) $\boxed{ア}=6,\boxed{イ}=3$

(3) 乗法群 $(\mathbb{Z}/77\mathbb{Z})^\times$ における $[50]_{77}$ の逆元を求めよ．解答は答えのみで良い．

(4) 乗法群 $(\mathbb{Z}/15\mathbb{Z})^\times$ の位数を求めよ．解答は答えのみで良い．

問題 2 解答例.

(1) 5
(2) (2), (4), (5)
(3) $[57]_{77}$ ($[-20]_{77}$ 等の別の表示でも可)
(4) 8

* *e-mail* : hoya@shibaura-it.ac.jp

□

問題 2 補足解説.

(1) 第 3 回復習レポート課題問題 2 補足解説参照.

(2) 第 3 回復習レポート課題問題 1 補足解説参照.

(3) 第 3 回講義資料 p.10 例題参照.

(4) 第 3 回復習レポート課題問題 4 補足解説，第 3 回講義資料命題 2.9, 例 7 参照．なお,

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$$

となる．

□

問題 3

(1) $\mathfrak{S}_5$ の位数を答えよ．解答は答えのみで良い.

(2) $\mathfrak{S}_4$ において,

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

を満たす $\sigma \in \mathfrak{S}_4$ は

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \boxed{ア} & \boxed{イ} & \boxed{ウ} & \boxed{エ} \end{pmatrix}$$

である．$\boxed{ア}$〜$\boxed{エ}$に入る値を求めよ．解答は答えのみで良い.

(3) $\mathfrak{S}_4$ において,

$$s_1 = (1\ 2),\ s_2 = (2\ 3),\ s_3 = (3\ 4)$$

とする．このとき,

$$s_3 s_2 s_2 s_1 s_2 s_1 s_3 s_2 s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \boxed{ア} & \boxed{イ} & \boxed{ウ} & \boxed{エ} \end{pmatrix}$$

である．$\boxed{ア}$〜$\boxed{エ}$に入る値を求めよ．解答は答えのみで良い.

(4) $\mathfrak{S}_{10}$ において,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 5 & 7 & 1 & 6 & 2 & 3 & 4 & 9 & 8 \end{pmatrix}$$

を互いに素な巡回置換の合成で表せ．解答は答えのみで良い.

問題 3 解答例.

(1) $5! = 120$.

(2) $4, 3, 2, 1$

(3) $3, 4, 2, 1$

(4) $(1\ 10\ 8\ 4)(2\ 5\ 6)(3\ 7)$

□

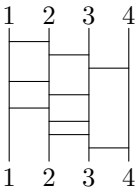
問題 3 補足解説.

(1) 一般に n 次対称群 $\mathfrak{S}_n$ の位数は $n!$ である．第 4 回講義資料 p.3 上部参照.

(2) 与式の両辺に右から $\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}^{-1}$ を掛けて,

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

(3) 第 4 回復習レポート課題問題 2 補足解説, 第 5 回復習レポート課題問題 2 補足解説参照. 対応するあみだくじは以下の通りである.



(4) 第 4 回復習レポート課題問題 3 補足解説参照. □

問題 4

(1) D_7 において,

$$\sigma^{-100} = \sigma^{\boxed{ア}}$$

である. $\boxed{ア}$ に入る 0 以上 6 以下の整数を求めよ. 解答は答えのみで良い.

(2) D_6 において,

$$\sigma^5(\sigma\tau)^{-1}\tau^3\sigma^{-3}\tau\sigma^4 = \sigma^{\boxed{ア}}\tau^{\boxed{イ}}$$

である. $\boxed{ア}$, $\boxed{イ}$ に入る整数を求めよ. ただし, $\boxed{ア}$ は 0 以上 5 以下, $\boxed{イ}$ は 0 または 1 の値で解答せよ. 解答は答えのみで良い.

(3) D_8 の位数 2 の部分群の個数を求めよ. 解答は答えのみで良い.

問題 4 解答例.

(1) 5
(2) 5, 1
(3) 9

□

問題 4 補足解説.

(1) $\sigma^7 = e$ より, $e = (\sigma^7)^{-15} = \sigma^{-105}$. よって, $\sigma^5 = \sigma^{-100}$.
(2) 第 5 回復習レポート課題問題 3 補足解説参照.
(3) 第 5 回復習レポート課題問題 5 補足解説参照. なお, $e \neq g \in D_8$ で g^2 を満たすような g は

$$\sigma^4,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau,\ \sigma^4\tau,\ \sigma^5\tau,\ \sigma^6\tau,\ \sigma^7\tau$$

で全てである. □

問題 5

以下の問いに答えよ．ただし， 解答は「部分群となる」,「部分群とならない」のいずれかを答えるだけで良い.

(1) 乗法群 $\mathbb{C}^\times$ の以下の部分集合 H が $\mathbb{C}^\times$ の部分群となるかどうかを判定せよ ($i = \sqrt{-1}$).

$$H = \{1, i, -i\}.$$

(2) 乗法群 $(\mathbb{Z}/18\mathbb{Z})^\times$ の以下の部分集合 H が $(\mathbb{Z}/18\mathbb{Z})^\times$ の部分群となるかどうかを判定せよ.

$$H = \{[1]_{18}, [7]_{18}, [13]_{18}\}.$$

(3) $\mathfrak{S}_3$ の以下の部分集合 H が $\mathfrak{S}_3$ の部分群となるかどうかを判定せよ.

$$H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

(4) D_6 の以下の部分集合 H が D_6 の部分群となるかどうかを判定せよ.

$$H = \{e, \sigma^2, \sigma^4, \sigma^2\tau, \sigma^4\tau\}.$$

問題 5 解答例.

(1) 部分群とならない
(2) 部分群となる
(3) 部分群となる
(4) 部分群とならない

□

問題 5 補足解説. 群 G の部分集合 H が G の部分群であることの必要十分条件は,

H が空でなく，任意の $h, k \in H$ に対し，$h \cdot k \in H$ かつ $h^{-1} \in H$ となること

であった．このため，部分群であることを確かめるときはこの条件を確認すればよい．本問の部分群とならないものは何が満たされないかを述べておこう．

(1) $i \in H$ であるが，$i^2 = -1 \notin H$ である．よって，H は二項演算で閉じておらず，部分群でない．「任意の $h, k \in H$ に対し，$h \cdot k \in H$」という条件においては，h と k が異なっているという条件は入っていないので，$h = k$ の場合も考えないといけないということに注意しよう．ちなみに,

$$1^{-1} = 1, i^{-1} = -i, (-i)^{-1} = i$$

なので，H は逆元を取る操作では閉じている．

(4) $\sigma^4, \sigma^2\tau \in H$ であるが,

$$\sigma^4 \cdot \sigma^2\tau = \sigma^6\tau = \tau \notin H$$

である．よって，H は二項演算で閉じておらず，部分群でない．ちなみにこちらも逆元を取る操作では閉じている (各自確認してみてほしい). □

問題 6

一般線型群

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

を考える ($\det A$ は A の行列式を表す). 次の $GL_2(\mathbb{C})$ の部分集合 G_1, G_2, G_3 が，それぞれ $GL_2(\mathbb{C})$ の

(a) 部分群となる　　(b) 部分群とならない

のどちらになるかを選び，その理由を説明せよ.

(1) $G_1 = \{A \in GL_2(\mathbb{C}) \mid \det A \in \mathbb{Z}\}$.

(2) $G_2 = \left\{ A \in GL_2(\mathbb{C}) \middle| A \text{ は } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{を固有ベクトルに持つ} \right\}$.

(3) $G_3 = \{A \in GL_2(\mathbb{C}) \mid A$ は任意の $B \in GL_2(\mathbb{C})$ に対して，$AB = BA$ を満たす $\}$.

問題 6 解答例.

(1) (b) 部分群とならない

理由：$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ とすると，$\det A = 2 \times 1 - 0 \times 0 = 2 \in \mathbb{Z}$ より，$A \in G_1$ であるが,

$$A^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$$

なので,

$$\det(A^{-1}) = \frac{1}{2} \times 1 - 0 \times 0 = \frac{1}{2} \notin \mathbb{Z}$$

より，$A^{-1} \notin G_1$．よって，G_1 は逆元を取る操作で閉じていないから，G_1 は部分群とはならない. □

(2) (a) 部分群となる

理由：まず，単位行列 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ は

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

より，$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ を固有値 1 の固有ベクトルとして持つ．よって，$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G_2$ であるため，$G_2 \neq \varnothing$ である．次に，任意の $A, B \in G_2$ について，A, B がそれぞれ $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ を固有値 λ, μ の固有ベクトルとして持っていたとすると,

$$AB \begin{pmatrix} 1 \\ 1 \end{pmatrix} = A\left(\mu \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \mu\left(A \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \lambda\mu \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

よって，このとき AB は $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ を固有値 $\lambda\mu$ の固有ベクトルとして持つので，$AB \in G_2$．さらに，$A \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ の両辺に A^{-1} を左から掛けると,

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \lambda A^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

となるので，$\lambda \neq 0$ に注意して,

$$A^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\lambda} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

よって，このとき A^{-1} は $\begin{pmatrix}1\\1\end{pmatrix}$ を固有値 $1/\lambda$ の固有ベクトルとして持つので，$A^{-1} \in G_2$．以上より，G_2 は $GL_2(\mathbb{C})$ の部分群である． □

(3) (a) 部分群となる

理由： まず，単位行列 $I_2 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ は任意の $B \in GL_2(\mathbb{C})$ に対して，

$$I_2 B = B I_2$$

を満たすので，$I_2 \in G_3$ である．よって，$G_3 \neq \varnothing$ である．次に，任意の $A_1, A_2 \in G_3$ と任意の $B \in GL_2(\mathbb{C})$ に対して，

$$(A_1A_2)B = A_1(A_2B) = A_1(BA_2) = (A_1B)A_2 = (BA_1)A_2 = B(A_1A_2)$$

となるので，$A_1A_2 \in G_3$．さらに，$A_1B = BA_1$ の両辺に左右から A_1^{-1} を掛けることで，

$$BA_1^{-1} = A_1^{-1}B$$

となるから，このとき $A_1^{-1} \in G_3$ でもある．以上より，G_3 は $GL_2(\mathbb{C})$ の部分群である． □

問題 6 補足解説. 方針は問題 5 と同じである．群 G の部分集合 H が G の部分群であることの必要十分条件は，

> H が空でなく，任意の $h, k \in H$ に対し，$h \cdot k \in H$ かつ $h^{-1} \in H$ となること

であったので，部分群であることを確かめるときはこの条件を確認すればよい．ちなみに，$A, B \in GL_2(\mathbb{C})$ が $\det A, \det B \in \mathbb{Z}$ を満たすとき，

$$\det(AB) = \det A \cdot \det B \in \mathbb{Z}$$

も成り立つから，本問の G_1 は二項演算では閉じているが，逆元を取る操作では閉じていない部分集合である．また，本問の G_3 は以下のように一般化される．

> 一般の群 G に対し，
> $$Z(G) \coloneqq \{z \in G \mid zg = gz,\ \forall g \in G\}$$
> とし，$Z(G)$ を G の**中心 (center)** と呼ぶ[*1]．言葉で書くと，$Z(G)$ は「G の全ての元と可換な元を集めてきてできる集合」である．

本問の G_3 は $Z(GL_2(\mathbb{C}))$ である．このとき，以下が成立する．証明は (3) の解答例と本質的に同じである．

命題

任意の群 G において，中心 $Z(G)$ は G の部分群である．

証明. まず単位元の定義より $eg = g = ge,\ \forall g \in G$ なので，$e \in Z(G)$．特に $Z(G) \neq \varnothing$．さらに $z_1, z_2 \in Z(G)$ と任意の $g \in G$ に対し，

$$\begin{aligned}(z_1z_2)g &= z_1(z_2g) = z_1(gz_2) = (z_1g)z_2 = (gz_1)z_2 = g(z_1z_2),\\ z_1^{-1}g &= z_1^{-1}gz_1z_1^{-1} = z_1^{-1}z_1gz_1^{-1} = gz_1^{-1}.\end{aligned}$$

となるので，$z_1z_2, z_1^{-1} \in Z(G)$．よって，二項演算と逆元を取る操作について閉じているので，$Z(S)$ は G の部分群である． □

[*1] $Z(G)$ の Z はドイツ語の Zentrum(中心) に由来.

なお，$G_3 = Z(GL_2(\mathbb{C}))$ は以下のように具体的にも求められる．このような具体形を求めてから G_3 が部分群であることを証明したという解答ももちろん OK である．

命題

$\mathbb{K} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ のとき，

$$Z(GL_2(\mathbb{K})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in \mathbb{K}^\times \right\}.$$

証明. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $b \neq 0$ 又は $c \neq 0$ のとき，

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 2a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

となるので，$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$．よって，$Z(GL_2(\mathbb{K}))$ の元は $b = c = 0$ を満たす対角行列．

次に，$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $a \neq d$ のとき，

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix} \neq \begin{pmatrix} a & a \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

となるので，$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$．よって，$Z(GL_2(\mathbb{K}))$ の元は $a = d$ を満たす対角行列，つまり単位行列の定数倍の形をしているもののみ．逆に，単位行列の定数倍が任意の $GL_2(\mathbb{K})$ の元と可換であることは容易にわかるので，結局 $Z(GL_2(\mathbb{K})) = \{aI_2 \mid a \in \mathbb{K}^\times\}$ である． □

なお，同様の方法で，以下もわかる．

命題

$\mathbb{K} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ のとき，

$$Z(GL_n(\mathbb{K})) = \left\{ aI_n \;\middle|\; a \in \mathbb{K}^\times \right\}.$$

ただし，I_n は n 次単位行列．

一般に群の中心を求める簡単な方法はなく，上のように各群に対して “頑張って” 求める必要がある． □

Extra 問題

(1) 集合 $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ に以下の二項演算を考えたものが群となるかどうかを判定し，その理由を説明せよ．

$$\circ\colon \mathbb{R}^\times \times \mathbb{R}^\times \to \mathbb{R}^\times,\ (r_1, r_2) \mapsto r_1 \circ r_2 := 2r_1 r_2.$$

(2) D_3 の部分群を全て求めよ．解答は答えのみで良い．

(3) $\mathfrak{S}_4$ において，

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

を満たす $\sigma \in \mathfrak{S}_4$ は存在しないことを証明せよ．

(4) 7 以上の任意の素数 p に対し，$3^{p-2} + 5^{p-2} + 7 \times 15^{p-2}$ を p で割った余りは 1 であることを証明せよ．(Hint: フェルマーの小定理を使える形を目指す．)

Extra 問題解答例.

(1) 群となる.

理由：与えられた二項演算が群の二項演算として満たすべき性質を満たしていることを順にチェックすれば良い.

(I) [結合法則]　任意の $r_1, r_2, r_3 \in \mathbb{R}^\times$ に対し,

$$(r_1 \circ r_2) \circ r_3 = (2r_1r_2) \circ r_3 = 2(2r_1r_2)r_3 = 4r_1r_2r_3$$
$$r_1 \circ (r_2 \circ r_3) = r_1 \circ (2r_2r_3) = 2r_1(2r_2r_3) = 4r_1r_2r_3$$

より，$(r_1 \circ r_2) \circ r_3 = r_1 \circ (r_2 \circ r_3)$ は満たされる.

(II) [単位元の存在]　任意の $r \in \mathbb{R}^\times$ に対し,

$$\frac{1}{2} \circ r = 2 \cdot \frac{1}{2} \cdot r = r$$
$$r \circ \frac{1}{2} = 2 \cdot r \cdot \frac{1}{2} = r$$

より，$e = 1/2 \in \mathbb{R}^\times$ が単位元の定義条件を満たす.

(III) [逆元の存在]　任意の $r \in \mathbb{R}^\times$ に対し,

$$\frac{1}{4r} \circ r = 2 \cdot \frac{1}{4r} \cdot r = \frac{1}{2} = e$$
$$r \circ \frac{1}{4r} = 2 \cdot r \cdot \frac{1}{4r} = \frac{1}{2} = e$$

より，r の逆元として $1/4r \in \mathbb{R}^\times$ が取れる.

以上より，$(\mathbb{R}^\times, \circ)$ は群となる. □

(2) $\{e\}, \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, \{e, \sigma, \sigma^2\}, D_3$. □

(3) 任意の $\sigma \in \mathfrak{S}_4$ に対して,

$$\sigma \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \\ \sigma(2) & \sigma(3) & \sigma(4) & \sigma(1) \end{pmatrix} = (\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4))$$

となるので，$\sigma \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \sigma^{-1}$ は長さ 4 の巡回置換である．一方，$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ を互いに素な巡回置換の合成で書くと,

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

となる．$\mathfrak{S}_4$ の元を互いに素な巡回置換の合成として書く方法は合成の順序の違いを除いて一意的なので，$(1\ 3)(2\ 4)$ が長さ 4 の巡回置換として書けるということはない．よって,

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

を満たす $\sigma \in \mathfrak{S}_4$ は存在しない. □

(4) 7 以上の任意の素数 p に対し，$[3^{p-2} + 5^{p-2} + 7 \times 15^{p-2}]_p = [1]_p$ であることを示せばよい．いま，p は 7 以上の素数なので，$\gcd(p, 15) = 1$ である，よって，$[15]_p$ は $\mathbb{Z}/p\mathbb{Z}$ において $\times$ に関する逆元 $[15]_p^{-1}$ を持つ．よって,

$$\begin{aligned} [3^{p-2} + 5^{p-2} + 7 \times 15^{p-2}]_p = [1]_p &\Leftrightarrow [15]_p[3^{p-2} + 5^{p-2} + 7 \times 15^{p-2}]_p = [15]_p[1]_p \\ &\Leftrightarrow [5 \cdot 3^{p-1} + 3 \cdot 5^{p-1} + 7 \times 15^{p-1}]_p = [15]_p \end{aligned}$$

となるので，$[5 \cdot 3^{p-1} + 3 \cdot 5^{p-1} + 7 \times 15^{p-1}]_p = [15]_p$ を示せばよい.

フェルマーの小定理より,

$$[3^{p-1}]_p = [5^{p-1}]_p = [15^{p-1}]_p = [1]_p$$

なので，

$$[5\cdot 3^{p-1}+3\cdot 5^{p-1}+7\times 15^{p-1}]_p=[5]_p[3^{p-1}]_p+[3]_p[5^{p-1}]_p+[7]_p[15^{p-1}]_p=[5]_p[1]_p+[3]_p[1]_p+[7]_p[1]_p=[15]_p$$

よって，示すべきことは示された． □

Extra 問題補足解説.

(1) 少し自然でない群構造についての出題である．同じ集合上であってもそれを群にするような二項演算は様々なものが考えられるということを体感してもらいたい．

(2) まず D_3 の各元の逆元を計算すると以下のようになっている．

$$e^{-1}=e,\qquad \sigma^{-1}=\sigma^2,\qquad (\sigma^2)^{-1}=\sigma,\qquad \tau^{-1}=\tau,\qquad (\sigma\tau)^{-1}=\sigma\tau,\qquad (\sigma^2\tau)^{-1}=\sigma^2\tau.$$

部分群は空でない D_3 の部分集合で，二項演算と逆元をとる操作で閉じているものであった．部分群は必ずもとの群 D_3 の単位元 e を含むことにも注意すると，e を含み，逆元を取る操作で閉じている以下の部分集合のうち，二項演算でも閉じているものを見つければ良いことになる．

- 元の個数が 1 個のもの：
$$\{e\}$$
- 元の個数が 2 個のもの：
$$\{e,\tau\},\ \{e,\sigma\tau\},\ \{e,\sigma^2\tau\}$$
- 元の個数が 3 個のもの：
$$\{e,\sigma,\sigma^2\},\ \{e,\tau,\sigma\tau\},\ \{e,\tau,\sigma^2\tau\},\ \{e,\sigma\tau,\sigma^2\tau\}$$
- 元の個数が 4 個のもの：
$$\{e,\sigma,\sigma^2,\tau\},\ \{e,\sigma,\sigma^2,\sigma\tau\},\ \{e,\sigma,\sigma^2,\sigma^2\tau\},\ \{e,\tau,\sigma\tau,\sigma^2\tau\}$$
- 元の個数が 5 個のもの：
$$\{e,\sigma,\sigma^2,\tau,\sigma\tau\},\ \{e,\sigma,\sigma^2,\tau,\sigma^2\tau\},\ \{e,\sigma,\sigma^2,\sigma\tau,\sigma^2\tau\}$$
- 元の個数が 6 個のもの：
$$D_3$$

ここで，D_3 の二項演算は以下のように定まっている．ただし，g 行 g' 列に gg' を書くというルールで表を書いている (このような表を D_3 の**乗積表**と言う)．

	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

この表を見ながら，上記の集合のうち二項演算で閉じているものを選んでくれば良い．例えば，$\{e,\sigma,\tau\}$ は $\sigma\tau\notin\{e,\sigma,\tau\}$ となるので二項演算では閉じていないとわかる．このような観察を繰り返す．なお，$\{e\}$ や D_3 も部分群であることに注意しよう (自明な部分群と呼ばれた)．

なお，乗積表は各行で見ると D_3 の元がちょうど 1 回ずつ出ており，各列で見ても D_3 の元がちょうど 1 回ずつ出ているということに注意しよう．実はこの性質は任意の群 G の乗積表で成り立つ．理由を考えてみてほしい．また，乗積表を “転置” しても元の表と同じにはならないということが D_3 が非可換群であるということに対応している．

本問は D_3 における計算を沢山行ってもらい，計算に慣れていただこうということでこのタイミングで出題をした (さらに部分集合が部分群となるのがどれくらい特別なことかということを感じて頂きたかった)．しかし，実際にはこの先の講義で群論をもう少し学ぶと，この問題は実はずっと簡単に解けるようになる！用語を用いながら概略を説明すると以下のようになる (定義のない用語は今後の講義で解説を行う)．

まず,「部分群の位数はもとの群の位数の約数になるしかない」という事実を学ぶ (**ラグランジュの定理**)．これにより，自明でない部分群の位数は 2 か 3 であることがわかり，元の個数が 4 つや 5 つの部分集合は初めから考えなくてよいということになる．さらに，位数が 2 や 3 の群は巡回群と呼ばれるものしかないということも学ぶ．そうすると結局自明でない部分群は，D_3 の各元によって生成されるものだけであるということがわかる．そうすると，解答例の 6 つのものだけであることが直ちにわかる．

(3) 第 5 回復習レポート課題問題 1 補足解説参照．本問も互いに素な巡回置換の合成による対称群の元の表示の応用例である．

(4) フェルマーの小定理の応用問題である．$[1/2]_p$ や $[1/3]_p$ というような記号を使いたくなるかもしれないが，このような元は $\mathbb{Z}/p\mathbb{Z}$ には存在しないので注意しよう．必ず $[2]_p^{-1}, [3]_p^{-1}$ 等という形で書かないといけない．ちなみに，$p = 2$ のとき，$3^{p-2} + 5^{p-2} + 7 \times 15^{p-2} = 1 + 1 + 7 = 9$，$p = 3$ のとき，$3^{p-2} + 5^{p-2} + 7 \times 15^{p-2} = 3 + 5 + 105 = 113$，$p = 5$ のとき，$3^{p-2} + 5^{p-2} + 7 \times 15^{p-2} = 23777$ なので，(4) の主張が成り立たない素数は $p = 3, 5$ のみである． □