代数学 I 第 5 回本レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

3 次対称群 $\mathfrak{S}_3$ の部分群を全て求めよ (答えのみで良い)．ただし，答えの見やすさのために，$\mathfrak{S}_3$ の 6 つの元にそれぞれ

$$e \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_1 \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma_2 \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\sigma_3 \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \sigma_4 \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_5 \coloneqq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

という名前を付け，『$\{e, \sigma_1\}$, $\{e, \sigma_1, \sigma_2\}$, $\ldots$』というような形で解答せよ．

問題 1 解答例． $\{e\}$, $\{e, \sigma_1\}$, $\{e, \sigma_2\}$, $\{e, \sigma_5\}$, $\{e, \sigma_3, \sigma_4\}$, $\mathfrak{S}_3$. □

問題 1 補足解説． まず $\mathfrak{S}_3$ の各元の逆元を計算すると以下のようになっている．

$$e^{-1} = e, \qquad \sigma_1^{-1} = \sigma_1, \qquad \sigma_2^{-1} = \sigma_2, \qquad \sigma_3^{-1} = \sigma_4, \qquad \sigma_4^{-1} = \sigma_3, \qquad \sigma_5^{-1} = \sigma_5.$$

部分群は空でない $\mathfrak{S}_3$ 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 (第 1,2 回講義資料命題 1.5)．部分群は必ず元の群 $\mathfrak{S}_3$ 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：
$$\{e, \sigma_1\},\ \{e, \sigma_2\},\ \{e, \sigma_5\}$$
- 元の個数が 3 個のもの：
$$\{e, \sigma_1, \sigma_2\},\ \{e, \sigma_1, \sigma_5\},\ \{e, \sigma_2, \sigma_5\},\ \{e, \sigma_3, \sigma_4\}$$
- 元の個数が 4 個のもの：
$$\{e, \sigma_1, \sigma_2, \sigma_5\},\ \{e, \sigma_1, \sigma_3, \sigma_4\},\ \{e, \sigma_2, \sigma_3, \sigma_4\},\ \{e, \sigma_3, \sigma_4, \sigma_5\}$$
- 元の個数が 5 個のもの：
$$\{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4\},\ \{e, \sigma_1, \sigma_3, \sigma_4, \sigma_5\},\ \{e, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$$
- 元の個数が 6 個のもの：
$$\mathfrak{S}_6$$

* *e-mail*： `hoya@shibaura-it.ac.jp`

ここで，$\mathfrak{S}_3$ の二項演算は以下のように定まっている．ただし，σ 行 σ' 列に $\sigma\sigma'$ を書くというルールで表を書いている (このような表を $\mathfrak{S}_3$ の**乗積表**と言う)．

	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_4	σ_5	σ_2	σ_3
σ_2	σ_2	σ_3	e	σ_1	σ_5	σ_4
σ_3	σ_3	σ_2	σ_5	σ_4	e	σ_1
σ_4	σ_4	σ_5	σ_1	e	σ_3	σ_2
σ_5	σ_5	σ_4	σ_3	σ_2	σ_1	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，$\{e, \sigma_1, \sigma_2\}$ は $\sigma_1\sigma_2 = \sigma_4 \notin \{e, \sigma_1, \sigma_2\}$ 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，乗積表は各行で見ると $\mathfrak{S}_3$ の元がちょうど 1 回ずつ出ており，各列で見ても $\mathfrak{S}_3$ 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．理由を考えてみよ．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 $\mathfrak{S}_3$ が非可換群であるということに対応している．

乗積表を計算するにあたっては，もちろん 2 行配列の表示を用いて頑張って計算しても良いが，互換を用いた表示が実は便利である．$\sigma_1 = (1\ 2), \sigma_2 = (2\ 3)$ なので，講義資料定理 4.7 より全ての元はこれらの何回かの合成として表される．具体的には，

$$\sigma_3 = \sigma_2\sigma_1 \qquad \sigma_4 = \sigma_1\sigma_2 \qquad \sigma_5 = \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$$

となる．講義資料命題 4.4 より，

$$\sigma_1\sigma_1 = \sigma_2\sigma_2 = e$$

なので，これを用いれば，例えば

$$\begin{aligned}
&\sigma_2\sigma_3 = \sigma_2\sigma_2\sigma_1 = \sigma_1 \\
&\sigma_4\sigma_3 = \sigma_1\sigma_2\sigma_2\sigma_1 = \sigma_1\sigma_1 = e \\
&\sigma_4\sigma_4 = \sigma_1\sigma_2\sigma_1\sigma_2 = \sigma_2\sigma_1\sigma_2\sigma_2 = \sigma_2\sigma_1 = \sigma_3
\end{aligned}$$

というように簡単に計算ができる．

本問は $\mathfrak{S}_3$ 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，$\mathfrak{S}_3$ 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． $\square$

問題 2

以下の (1), (2) の主張をそれぞれ証明せよ．

(1) n を 2 以上の自然数とする．任意の巡回置換 $(i_1\ i_2\ \cdots\ i_k) \in \mathfrak{S}_n$ と $\sigma \in \mathfrak{S}_n$ に対し，

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$$

となる．

(2) $\mathfrak{S}_4$ において，

$$\sigma(1\ 2\ 3\ 4) = (1\ 2)(3\ 4)\sigma$$

を満たす $\sigma \in \mathfrak{S}_4$ は存在しない．(Hint : (1) で示した事実を用いて良い．)

問題 2 解答例．

(1) (1) の主張にある等式の両辺の元が写像 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ として一致していることを言えば良く，そのためには，各 $j = 1, \ldots, n$ に対し，

$$(\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1})(j) = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))(j) \qquad (*)$$

となることを示せば良い．

(i) $j \in \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)\}$ のとき： $j = \sigma(i_\ell)$ とすると，

$$((*) \text{の左辺}) = \sigma((i_1\ i_2\ \cdots\ i_k)(\sigma^{-1}(\sigma(i_\ell)))) = \sigma((i_1\ i_2\ \cdots\ i_k)(i_\ell)) = \sigma(i_{\ell+1}).$$

ただし，$\ell = k$ のとき $i_{\ell+1} = i_{k+1} \coloneqq i_1$．さらに，

$$((*) \text{の右辺}) = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))(\sigma(i_\ell)) = \sigma(i_{\ell+1}).$$

よって，$(*)$ は成立する．

(ii) $j \notin \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)\}$ のとき： 巡回置換の定義から，

$$((*) \text{の右辺}) = j$$

であり，さらに $\sigma^{-1}(j) \notin \{i_1, i_2, \ldots, i_k\}$ なので，

$$((*) \text{の左辺}) = \sigma((i_1\ i_2\ \cdots\ i_k)(\sigma^{-1}(j))) = \sigma(\sigma^{-1}(j)) = j.$$

よって，$(*)$ は成立する．

(i), (ii) より $(*)$ は示され，(1) は示された．

(2) 背理法で示す．

$$\sigma(1\ 2\ 3\ 4) = (1\ 2)(3\ 4)\sigma$$

を満たす $\sigma \in \mathfrak{S}_4$ が存在したと仮定して矛盾を導く．上式の両辺に右から σ^{-1} を合成すると，

$$\sigma(1\ 2\ 3\ 4)\sigma^{-1} = (1\ 2)(3\ 4).$$

さらに，(1) で示したことより，このとき

$$(\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)) = (1\ 2)(3\ 4).$$

これは $\mathfrak{S}_4$ 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 1 通りである (講義資料定理 4.7 (2)) ことに矛盾する．よって，(2) は示された． □

問題 2 補足解説．

(1) より一般に $\sigma, \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n$ に対して，

$$\sigma \circ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

となる．ここで，右辺の 1 行目は必ずしも $1, \ldots, n$ の順には並んでいないが，上下の対応だけを見て，$\sigma(k)$ を $\sigma(i_k)$ に送る写像を表していると考える．証明は本問と同様の方針でできるので試してみてほしい．

(2)：発展的な補足 $\sigma_0 \in \mathfrak{S}_n$ がどの 2 つも互いに素な巡回置換の合成として，

$$\sigma_0 = (i_{1,1}\ i_{1,2}\ \cdots\ i_{1,\ell_1})(i_{2,1}\ i_{2,2}\ \cdots\ i_{2,\ell_2})\cdots(i_{t,1}\ i_{t,2}\ \cdots\ i_{t,\ell_t}),\ \ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$$

と書かれるとき，(1) で示したことを用いると，任意の $\sigma \in \mathfrak{S}_n$ に対し，

$$\begin{aligned} \sigma\sigma_0\sigma^{-1} &= \sigma(i_{1,1}\ i_{1,2}\ \cdots\ i_{1,\ell_1})\sigma^{-1}\sigma(i_{2,1}\ i_{2,2}\ \cdots\ i_{2,\ell_2})\sigma^{-1}\cdots\sigma(i_{t,1}\ i_{t,2}\ \cdots\ i_{t,\ell_t})\sigma^{-1} \\ &= (\sigma(i_{1,1})\ \sigma(i_{1,2})\ \cdots\ \sigma(i_{1,\ell_1}))(\sigma(i_{2,1})\ \sigma(i_{2,2})\ \cdots\ \sigma(i_{2,\ell_2}))\cdots(\sigma(i_{t,1})\ \sigma(i_{t,2})\ \cdots\ \sigma(i_{t,\ell_t})) \end{aligned}$$

となることがわかる．ここで，σ は全単射写像 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ なので，最後の式もどの 2 つも互いに素な巡回置換の合成となっている．これより，σ_0 と $\sigma\sigma_0\sigma^{-1}$ をどの 2 つも互いに素な巡回置換の合成として書いたときには，そこに現れる巡回置換の長さおよびその数は一致するということがわかる．この巡回置換の長さを並べた $(\ell_1, \ell_2, \ldots, \ell_t)$ を σ_0 の**サイクルタイプ**と呼ぶ．ここで，後の便利さのために，上の表示においては，σ_0 で動かされない数字 k があった時にも (k) という自明な (=単位元に等しい) 巡回置換が合成されていると考えて，常に $\ell_1 + \ell_2 + \cdots + \ell_t = n$ となるようにすることにする．例えば，$\mathfrak{S}_3$ においては，

$$e = (1)(2)(3) \qquad (1\ 2) = (1\ 2)(3) \qquad (2\ 3) = (2\ 3)(1) \qquad (3\ 1) = (3\ 1)(2)$$

というようにする．こうすると，$\mathfrak{S}_3$ の元

$$e,\ (1\ 2),\ (2\ 3),\ (3\ 1),\ (1\ 2\ 3),\ (1\ 3\ 2)$$

のサイクルタイプはこの順に，

$$(1,1,1),\ (2,1),\ (2,1),\ (2,1),\ (3),\ (3)$$

である．上で見たように，一般に σ_0 と $\sigma\sigma_0\sigma^{-1}$ のサイクルタイプは等しい．本問では，$\sigma(1\ 2\ 3\ 4)\sigma^{-1}$ のサイクルタイプが $(1\ 2\ 3\ 4)$ のサイクルタイプと等しく (4) で，$(1\ 2)(3\ 4)$ のサイクルタイプが $(2,2)$ であったことから，これらが一致することは無いということになる．この「サイクルタイプによる元の分類」の考え方は講義の終盤で学ぶ**共役類**という考え方と対応しており，例えば "表現論"[*1] と呼ばれる分野等で非常に重要なものとなる． □

[*1] 表現論に興味のある方は私 (大矢) の専門分野となるので是非お話しましょう．