【問題】 3 次対称群 $\mathfrak{S}_3$ について
(i) 内部自己同型群 $\mathrm{Inn}(\mathfrak{S}_3)$ を決定せよ.
(ii) 自己同型群 $\mathrm{Aut}(\mathfrak{S}_3)$ を決定せよ.

(H13 東工大理学研究科 数学)

【解答】 (i) $\mathfrak{S}_3$ の中心を $Z(\mathfrak{S}_3)$ とすると，$\mathrm{Inn}(\mathfrak{S}_3) \simeq \mathfrak{S}_3/Z(\mathfrak{S}_3)$ となるから，中心が分かれば内部自己同型群が分かる．$\mathfrak{S}_3$ は $s_1 = (1,2)$, $s_2 = (2,3)$ ((i,j) は互換) で生成されるから，$\sigma \in \mathfrak{S}_3$ に対し $\sigma \in Z(\mathfrak{S}_3) \Leftrightarrow \sigma s_i \sigma^{-1} = s_i \ (i=1,2)$ である．

$$\sigma s_1 \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ \sigma(2) & \sigma(1) & \sigma(3) \end{pmatrix}$$

は $\sigma(3)$ のみ固定されるから，$\sigma s_1 \sigma^{-1} = s_1 \Leftrightarrow \sigma(3) = 3$．同様の計算より $\sigma s_2 \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ \sigma(1) & \sigma(3) & \sigma(2) \end{pmatrix}$ であり，$\sigma(1)$ のみ固定されるから，$\sigma s_2 \sigma^{-1} = s_2 \Leftrightarrow \sigma(1) = 1$ となる．以上から

$$\sigma \in Z(\mathfrak{S}_3) \quad \Leftrightarrow \quad \begin{array}{c} \sigma s_1 \sigma^{-1} = s_1 \\ \text{かつ} \quad \sigma s_2 \sigma^{-1} = s_2 \end{array} \quad \Leftrightarrow \quad \sigma(3) = 3 \text{ かつ } \sigma(1) = 1 \quad \Leftrightarrow \quad \sigma = e \text{ (恒等置換)}$$

即ち $Z(\mathfrak{S}_3) = \{e\}$ だから $\mathrm{Inn}(\mathfrak{S}_3) = \mathfrak{S}_3$ となる．

(ii) $\varphi \in \mathrm{Aut}(\mathfrak{S}_3)$ とする．φ は生成系 (s_1, s_2) の行き先 $(\varphi(s_1), \varphi(s_2))$ で決定される．$\mathfrak{S}_3$ の位数 2 の元の全体は $s_1, s_2, w_0 = (1,3)$ であり，元の位数は自己同型射に関し不変だから φ により (s_1, s_2) の行き先は

$$(s_1, s_2), \qquad (s_2, s_1), \qquad (w_0, s_2), \qquad (s_2, w_0), \qquad (s_1, w_0), \qquad (w_0, s_1)$$

の 6 通りである．以下，$g \in \mathfrak{S}_3$ による内部自己同型射を ι_g で表す．

(1) $(\varphi(s_1), \varphi(s_2)) = (s_1, s_2)$ ならば，$\varphi = id_{\mathfrak{S}_3}$ である．
(2) $(\varphi(s_1), \varphi(s_2)) = (s_2, s_1)$ のとき，$s_2 = w_0 s_1 w_0$, $s_1 = w_0 s_2 w_0$ より $\varphi = \iota_{w_0}$ である．
(3) $(\varphi(s_1), \varphi(s_2)) = (w_0, s_2)$ のとき，$w_0 = s_2 s_1 s_2$, $s_2^3 = s_2$ より $\varphi = \iota_{s_2}$ である．
(4) $(\varphi(s_1), \varphi(s_2)) = (s_2, w_0)$ のとき，$\varphi = \iota_{s_2} \cdot \iota_{w_0}$ である．
(5) $(\varphi(s_1), \varphi(s_2)) = (s_1, w_0)$ のとき，$s_1^3 = s_1$, $w_0 = s_1 s_2 s_1$ より $\varphi = \iota_{s_1}$ である．
(6) $(\varphi(s_1), \varphi(s_2)) = (w_0, s_1)$ のとき，$\varphi = \iota_{s_1} \cdot \iota_{w_0}$ である．

以上より $\mathfrak{S}_3$ の任意の自己同型射は内部自己同型射となるから $\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Inn}(\mathfrak{S}_3) \simeq \mathfrak{S}_3$ である． □

※※※ 対称群の自己同型群 ※※※ 上の問題から “n 次対称群の内部自己同型群，自己同型群は元の対称群に同型?” という疑問が生じる．$\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ は内部自己同型群，自己同型群は共に単位群だから $n=2$ のときは成立しないが，$n \geq 3$ ならどうだろうか?

(I) $\mathfrak{S}_n$ の内部自己同型群については次が知られている．

定理 1. $n \geq 3$ ならば 中心 $Z(\mathfrak{S}_n)$ は単位群となる．従って $\mathrm{Inn}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ となる．

【証明】 $n \geq 3$ のとき，解答と同様の計算により $\sigma \in Z(\mathfrak{S}_n)$ に対し

$$\sigma s_i \sigma^{-1} = \begin{pmatrix} \sigma(1) & \cdots & \sigma(i) & \sigma(i+1) & \cdots & \sigma(n) \\ \sigma(1) & \cdots & \sigma(i+1) & \sigma(i) & \cdots & \sigma(n) \end{pmatrix} = s_i \qquad \left(\begin{array}{c} s_i = (i, i+1) \text{ (= 隣接互換)}, \\ i = 1, \cdots, n-1 \end{array} \right)$$

が成立．s_i は $i, i+1$ 以外の元を固定しているので $\{\sigma(i), \sigma(i+1)\} = \{i, i+1\}$ となるから

$$\{\sigma(i)\} = \{\sigma(i-1), \sigma(i)\} \cap \{\sigma(i), \sigma(i+1)\} = \{i-1, i\} \cap \{i, i+1\} = \{i\} \qquad (i = 2, \cdots, n-1),$$

$$\begin{array}{c} \{\sigma(1)\} = \{\sigma(1), \sigma(2)\} - \{\sigma(2)\} = \{1,2\} - \{2\} = \{1\}, \\ \{\sigma(n)\} = \{\sigma(n-1), \sigma(n)\} - \{\sigma(n-1)\} = \{n-1, n\} - \{n-1\} = \{n\}. \end{array}$$

従って $\sigma = e$，即ち $Z(\mathfrak{S}_n)$ は単位群となる． □

(II) 一方，$\mathfrak{S}_n$ の自己同型群については次が知られている．

定理 2 (Hölder).
 (i) $n=2,6$ を除く全ての n に対し $\mathrm{Aut}(\mathfrak{S}_n)\simeq\mathfrak{S}_n$.
 (ii) $\mathrm{Aut}(\mathfrak{S}_6)=\langle\xi\rangle\ltimes\mathrm{Inn}(\mathfrak{S}_6)$ となる $\mathfrak{S}_6$ の位数 2 の自己同型射 ξ が存在する.

以下，この定理を証明する．$\mathfrak{S}_n$ の自己同型射を決定するには生成系 $\{s_1,\cdots,s_{n-1}\}$ ($s_i=(i,i+1)$ は隣接互換) の行き先を決定すればよい．$\mathfrak{S}_3$ の場合，位数 2 の元は互換しかないので位数だけ考えればよかったが，$n\geq 4$ のときは位数の情報だけで決定できない．対称群の場合，位数ではなく巡回置換の長さが有効である．

補題 1. $\varphi\in\mathrm{Aut}(\mathfrak{S}_n)$ が $\varphi\in\mathrm{Inn}(\mathfrak{S}_n)$ であるための必要十分条件は φ が任意の互換を互換に移す事である.

【証明】 対称群の置換の型は共役に関する不変量だから，φ が内部自己同型射ならば互換を互換に移す事は明らか.

逆に φ が任意の互換を互換に移すとする．このとき命題

$$\mathrm{P}:\quad \iota_{g_t}^{-1}\cdots\iota_{g_2}^{-1}\varphi \text{ が } (1,2),(1,3),\cdots,(1,t) \text{ を固定するような } g_2,\cdots,g_t\in\mathfrak{S}_n \text{ が存在する」}$$

を $t\geq 2$ に関する帰納法により証明する.

$t=2$ のとき，仮定より $\varphi(1,2)=(i,j)$ と表される．$(1,i)(2,j)(1,2)(2,j)(1,i)=(i,j)$ より $g_2=(1,i)(2,j)$ とすれば $\varphi(1,2)=\iota_{g_2}(1,2)$，$\iota_{g_2}^{-1}\varphi(1,2)=(1,2)$ となる.

$t>2$ とする．帰納法の仮定より $\iota_{g_{t-1}}^{-1}\cdots\iota_{g_2}^{-1}\varphi(1,\ell)=(1,\ell)$ $(\ell=2,\cdots,t-1)$ となる $g_2,\cdots,g_{t-1}\in\mathfrak{S}_n$ が存在する．$\psi=\iota_{g_{t-1}}^{-1}\cdots\iota_{g_2}^{-1}\varphi$ と置く．仮定より $\psi(1,t)=(\ell,k)$ と表される．$\psi(1,2)=(1,2)$ だから $\{\ell,k\}\neq\{1,2\}$．また $\{1,2\}\cap\{\ell,k\}=\varnothing$ だとすると $(1,2)(1.t)$ は

$$((1,2)(1,t))^3=(2,t)(1,t)(2,t)(2,t)(1,2)(1,t)=(1,2)(2,t)(1,2)(1,t)=(1,t)^2=e$$

より位数 3 だが，$\psi((1,2)(1,t))=(1,2)(\ell,k)$ は位数 2 だから矛盾．従って $\psi(1,t)$ は $(1,k)$ または $(2,k)=(1,2)(1,k)(1,2)$ という形になる．$k<t$ だとすると

$$\psi(1,t)=(1,k)=\psi(1,k),\qquad \text{または}\qquad \psi(1,t)=(2,k)=\psi((1,2)(1,k)(1,2))$$

となり矛盾．従って $t\leq k$ となる．ここで $\psi(1,t)=(1,k)$ のときは $g_t=(t,k)$，$\psi(1,t)=(2,k)$ のとき $g_t=(t,k)(1,2)$ と置けば

$$\psi(1,t)=\iota_{g_t}(1,t),\qquad \iota_{g_t}(1,i)=(1,i)\quad(i=2,\cdots,t-1)$$

だから $\iota_{g_t}^{-1}\psi=\iota_{g_t}^{-1}\iota_{g_{t-1}}^{-1}\cdots\iota_{g_2}^{-1}\varphi$ は $(1,2),\cdots,(1,t)$ を固定する.

以上より命題 P が成立し，ここで $t=n$ とすれば $\iota_{g_n}^{-1}\cdots\iota_{g_2}^{-1}\varphi$ が $(1,2),\cdots,(1,n)$ を固定するような $g_2,\cdots,g_n\in\mathrm{S}_n$ が存在する．$(i,i+1)=(1,i+1)(1,i)(1,i+1)$ より $(1,2),\cdots,(1,n)$ は $\mathfrak{S}_n$ を生成するから $\varphi=\iota_{g_2}\cdots\iota_{g_n}$ となる． □

【定理 2 (i) の証明】 (Segal) (1) $\mathfrak{S}_n$ の元 σ を互いに素な巡回置換の積

$$\sigma=\sigma_1\sigma_2\cdots\sigma_\ell\qquad(\mathrm{length}(\sigma_i)=2\ (1\leq i\leq t),\quad 3\leq\mathrm{length}(\sigma_i)\ (t+1\leq i\leq\ell))$$

で表すとき，$3\leq\mathrm{length}(\sigma_i)$ だとすると $\sigma_i^2\neq e$ だから $\mathrm{ord}\ \sigma=2\ \Leftrightarrow\ t=\ell$ となる.

(2) k 個の互いに素な互換の積で表される $\mathfrak{S}_n$ の元の全体を T_k と置く．置換の型は共役に関し不変だから T_k は単一の共役類となる．$\varphi\in\mathrm{Aut}(\mathfrak{S}_n)$ について $\varphi(\sigma)\in T_k$ となる $\sigma\in T_\ell$ が存在したとする．T_ℓ の元は互いに共役であり，任意の $\sigma'\in T_\ell$ に対し $\tau\sigma\tau^{-1}=\sigma'$ となる $\tau\in\mathfrak{S}_n$ が存在する．このとき

$$\varphi(\sigma')=\varphi(\tau\sigma\tau^{-1})=\varphi(\tau)\varphi(\sigma)\varphi(\tau)^{-1}$$

より $\varphi(\sigma')$ は $\varphi(\sigma)$ と共役となり，従って $\varphi(\sigma')\in T_k$ となる．故に $\varphi(T_\ell)\cap T_k\neq\varnothing$ ならば $\varphi(T_\ell)\subset T_k$ が成立する．φ^{-1} に対し同様の議論を行えば，$\varphi(T_\ell)\cap T_k\neq\varnothing$ ならば φ により T_ℓ から T_k への全単射が誘導され，特に $|T_\ell|=|T_k|$ が成立する.

(3) $|T_k|$ を考える．$1,2,\cdots,n$ から 2 元からなる互いに素な k 個の部分集合の選び方は

$$\frac{1}{k!}{}_nC_2\times{}_{n-2}C_2\times\cdots\times{}_{n-2(k-1)}C_2=\frac{n(n-1)\cdot(n-2)(n-3)\cdots(n-2k+2)(n-2k+1)}{k!2^k}$$

となる．仮に $\varphi(T_1)\cap T_k\neq\varnothing$ ならば $\frac{n(n-1)\cdot(n-2)(n-3)\cdots(n-2k+2)(n-2k+1)}{k!2^k}=\frac{n(n-1)}{2}$ 従って

$$(n-2)(n-3)\cdots(n-2k+2)(n-2k+1)=k!2^{k-1}\tag{1}$$

が成立．右辺が正だから $n \geq 2k$ となり，このとき

$$(1) \text{ の左辺 } \geq (2k-2)(2k-3)\cdots(2k-2k+2)(2k-2k+1) = (2k-2)!$$

となる．この式の最右辺について $k \geq 4$ のとき $(2k-2)! > k!2^{k-1}$ が成立する．(実際，$k=4$ のときは $6! > 4! \cdot 8$ より成立し，$k > 4$ のとき $k-1$ までの成立を仮定すると $(2k-2)(2k-3) - 2k = 4(k-\frac{3}{2})^2 - 3 > 0$ より

$$(2k-2)! = (2k-2)(2k-3)(2(k-1)-2)! > (2k-2)(2k-3)(k-1)!2^{k-2} > 2k\cdot(k-1)!2^{k-2} = k!2^{k-1}.$$

これより $k \geq 4$ となる k について (1) を満たす n は存在せず，従って $\varphi(T_1) \cap T_k = \varnothing$ である．

$k=2$ のとき，(1) は $(n-2)(n-3) = 2!2^1 = 4$ となるが，左辺は必ずとなるから (1) を満たす整数 n はない．

$k=3$ のとき，

$$\begin{aligned}(1) \text{ の左辺} - 3!2^{3-1} &= (n-2)(n-3)(n-4)(n-5) - 24 \\ &= n^4 - 14n^3 + 71n^2 - 154n + 96 = (n-1)(n-6)(n^2-7n+16)\end{aligned}$$

及び $n^2 - 7n + 16 > 0$ より，$n=1, n=6$ のとき (1) が成立．$n=1$ のときはそもそも互換はないので，$n=6$ のとき $|T_1| = |T_3|$ となり，$n \neq 6$ ならば $\varphi(T_1) \cap T_3 = \varnothing$ となる．

以上の事から $n \neq 6$ ならば，$\varphi(T_1) = T_1$ となり，補題 1 より $\varphi \in \mathrm{Inn}(\mathfrak{S}_n)$ となる． □

【定理 2 (ii) の証明】 $n=6$ の場合について考える．補題 1 より $\xi \in \mathrm{Aut}(\mathfrak{S}_6)$ が内部自己同型射でなければ，上の証明より $\xi(T_1) = T_3$ となる．この事に注意して ξ，特に $\mathfrak{S}_6$ の生成系 $s_1, \cdots, s_5$ の ξ の像を次のように定める：

$$\begin{gathered}\xi(s_1) = \sigma_1 := (1,3)(2,4)(5,6), \quad \xi(s_2) = \sigma_2 := (1,6)(2,5)(3,4), \quad \xi(s_3) = \sigma_3 := (1,4)(2,3)(5,6), \\ \xi(s_4) = \sigma_4 := (1,6)(2,4)(3,5), \quad \xi(s_5) = \sigma_5 := (1,2)(3,4)(5,6)\end{gathered}$$

$\sigma_1, \cdots, \sigma_5$ について

$$\begin{gathered}\sigma_1\sigma_3 = \sigma_3\sigma_1 = (1,2)(3,4), \qquad \sigma_1\sigma_4 = \sigma_4\sigma_1 = (1,5)(3,6), \qquad \sigma_1\sigma_5 = \sigma_5\sigma_1 = (1,4)(2,3) \\ \sigma_2\sigma_4 = \sigma_4\sigma_2 = (2,3)(4,5), \qquad \sigma_2\sigma_5 = \sigma_5\sigma_2 = (1,5)(2,6), \qquad \sigma_3\sigma_5 = \sigma_5\sigma_3 = (1,3)(2,4)\end{gathered}$$

$$\begin{gathered}\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 = (1,2)(3,5)(4,6), \qquad \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3 = (6,3)(5,4)(2,1) \\ \sigma_3\sigma_4\sigma_3 = \sigma_4\sigma_3\sigma_4 = (4,5)(3,1)(2,6), \qquad \sigma_4\sigma_5\sigma_4 = \sigma_5\sigma_4\sigma_5 = (6,4)(5,2)(3,1)\end{gathered}$$

となる事が確かめられ，従って $\{\sigma_1, \cdots, \sigma_5\}$ は $\mathfrak{S}_6$ の生成系 $\mathfrak{S}_6$ の $\{s_1, \cdots, s_5\}$ が満たす基本関係式と同一の関係式

$$\sigma_i^2 = e \quad (1 \leq i \leq), \qquad (\sigma_i\sigma_{i+1})^3 = e \quad (1 \leq i \leq 4), \qquad (\sigma_i\sigma_j)^2 = 2 \quad (|i-j| > 1)$$

と満たすから，ξ は $\mathfrak{S}_6$ の自己準同型射となる．更に

$$\begin{gathered}s_1 = \sigma_2\sigma_1\sigma_3\sigma_5\sigma_2, \qquad s_2 = \sigma_2\sigma_1\sigma_3\sigma_5\sigma_2\sigma_4\sigma_1\sigma_3\sigma_5\sigma_4\sigma_2\sigma_1\sigma_3\sigma_5\sigma_2, \\ s_3 = \sigma_1\sigma_2\sigma_1\sigma_3\sigma_5\sigma_2\sigma_1, \qquad s_4 = \sigma_4\sigma_2\sigma_1\sigma_3\sigma_5\sigma_2\sigma_4\sigma_1\sigma_3\sigma_5\sigma_4\sigma_2\sigma_1\sigma_3\sigma_5\sigma_2\sigma_4, \qquad s_5 = \sigma_1\sigma_3\sigma_5\end{gathered}$$

より $\{s_1, \cdots, s_5\} \subset \xi(\mathfrak{S}_6)$，$\xi(\mathfrak{S}_6) = \mathfrak{S}_6$ となるから ξ は同型射である．

次に ξ^2 について考える．$\sigma_5 = s_1s_3s_5$ であることに注意すれば $\xi^2(s_5) = \xi(\sigma_5) = \xi(s_1s_3s_5) = \sigma_1\sigma_3\sigma_5 = s_5$ となる．次に s_1 について，$\sigma_1 = (s_1s_2s_1)(s_2s_3s_2)s_5$ より

$$\xi^2(s_1) = \xi(\sigma_1) = (\sigma_1\sigma_2\sigma_1)(\sigma_2\sigma_3\sigma_2)\sigma_5 = (\sigma_2\sigma_1)\sigma_3\sigma_2\sigma_5 = \sigma_2\sigma_1\sigma_3\sigma_5\sigma_2 = s_1.$$

s_3 について，$\sigma_3 = (s_1s_2s_3s_2s_1)s_2s_5$ より

$$\xi^2(s_3) = \xi(\sigma_3) = \sigma_1\sigma_2\sigma_3(\sigma_2\sigma_1\sigma_2)\sigma_5 = \sigma_1\sigma_2\sigma_3(\sigma_1\sigma_2\sigma_1)\sigma_5 = \sigma_1(\sigma_2(\sigma_3\sigma_1\sigma_5)\sigma_2)\sigma_1 = s_3.$$

s_2 について，$\sigma_2 = (s_1s_2s_3s_4s_5s_4s_3s_2s_1)(s_2s_3s_4s_3s_2)s_3$，及び $\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1 = (4,5)(3,2)(6,1)$，$\sigma_2\sigma_3\sigma_4\sigma_3\sigma_2 = (3,2)(4,6)(5,1)$ より

$$\begin{aligned}\xi^2(s_2) = \xi(\sigma_2) &= (\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1)(\sigma_2\sigma_3\sigma_4\sigma_3\sigma_2)\sigma_3 \\ &= (4,5)(3,2)(6,1)\cdot(3,2)(4,6)(5,1)\cdot(1,4)(2,3)(5,6) = (2,3) = s_2.\end{aligned}$$

s_4 について，$\sigma_4 = (s_1s_2s_3s_4s_5s_4s_3s_2s_1)(s_2s_3s_2)(s_3s_4s_3)$ より

$$\begin{aligned}\xi^2(s_4) = \xi(\sigma_4) &= (\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1)(\sigma_2\sigma_3\sigma_2)(\sigma_3\sigma_4\sigma_3) \\ &= (4,5)(3,2)(6,1)\cdot(6,3)(5,4)(2,1)\cdot(4,5)(3,1)(2,6) = (4,5) = s_4.\end{aligned}$$

従って ξ は位数 2 の自己同型射となる．

$\varphi(T_1) = T_3$ となる $\varphi \in \mathrm{Aut}(\mathfrak{S}_6)$ について $\xi^{-1}\varphi(T_1) = T_1$ だから $\varphi \in \xi\mathrm{Inn}(\mathfrak{S}_6)$． 明らかに $\langle\xi\rangle \cap \mathrm{Inn}(\mathfrak{S}_6) = \{e\}$ であり，$\mathrm{Inn}(\mathfrak{S}_6) \lhd \mathrm{Aut}(\mathfrak{S}_6)$ だから $\mathrm{Aut}(\mathfrak{S}_6) = \langle\xi\rangle \ltimes \mathrm{Inn}(\mathfrak{S}_6)$ となる． $\square$

果たして，この互換の積はどうのようにして得られたのだろうか？ そのうち調べる事にする． $\square$