数理解析研究所講究録
156巻 1972年 147-166

変換半群の生成元，基本関係式，元の長さ

青山学院大理工　　荒堀信子

§1. 変換半群とその生成元

$\Omega=\{1,2,\cdots,n\}$を有限集合とし，ΩからΩへの写像全体のつくる集合をΣ_nで表わす．Σ_nは写像の積の意味で単位元をもつ半群をなす．これを変換半群という．Σ_nの元でとくにbijection全体のつくる部分集合を$\mathfrak{S}_n$（n次対称群に同型）と書き，$\Sigma_n^*=\Sigma_n-\mathfrak{S}_n$とおく．容易にわかるように$\Sigma_n^*$は$\Sigma_n$の部分半群となる．

さてΣ_n中の特別な元σ_l^k，γ_j^iを次式で定義する．まずσ_l^kはΩ中の2文字k,l $(k\neq l)$の互換である．またγ_j^i $(i\neq j)$は，iをjに写し，i以外の元はそれ自身に写すような写像として定義する．すなわち式で書けば，

$$\sigma_l^k(x)=\begin{cases} k, & x=l \\ l, & x=k \\ x, & x\in\Omega-\{k,l\} \end{cases}$$

$$\gamma_j^i(x)=\begin{cases} j, & x=i \\ x, & x\in\Omega-\{i\} \end{cases}$$

となる．

すると次の定理が得られる．

<u>定理 1.</u>

(i) $\{\sigma_l^k, \gamma_j^i \mid k, l, i, j \in \Omega,\ k \neq l,\ i \neq j\}$ は半群 Σ_n を生成する．

(ii) $\{\gamma_j^i \mid i, j \in \Omega,\ i \neq j\}$ は半群 Σ_n^* を生成する．

本稿の主目的は，生成元系 $\{\sigma_l^k, \gamma_j^i\}$ に関して半群 Σ_n の基本関係を求めること，Σ_n^* の元 f をいくつかの γ_j^i の積として表わすときの因子の個数の最小値（すなわち，生成系 $\{\gamma_j^i\}$ に関する f の"長さ"）$l(f)$ を与える式を求めることである．

§2. Σ_n の $\mathfrak{S}_n$-両側分解

さて定理の前半 (i) は周知である．（例えば Clifford-Preston の本 [1] 参照）．(ii) の証明に関しては，後から基本関係を導びくときにも有用であるいくつかの補題から述べることにしよう．まず

<u>定義</u>　自然数 n の分割とは負でない整数の列

$$(\alpha_0, \alpha_1, \cdots, \alpha_n)$$

であって，$\alpha_0 + \alpha_1 + \cdots + \alpha_n = n$

かつ，$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$

を満たすものをいう．n の分割 $\Delta = (\alpha_0, \alpha_1, \cdots, \alpha_n)$

の全体のなす集合を $\mathcal{P}(n)$ と書くことにする．

各 $f \in \Sigma_n$ に対して，n の分割を次のように定める．

$$\alpha_i = \alpha_i(f) = \#\{x \in \Omega \mid |\{f^{-1}(x)\}| = i\}$$

ただし，$\#$，$|\cdots|$ はいづれも元の個数を意味する．

すると，$(\alpha_0, \alpha_1, \cdots, \alpha_n)$ は容易に n の分割になることがわかる．この分割を Δ_f と書き，f に属する分割と呼ぶ．

<u>補題 1.</u>　$f, g \in \Sigma_n$ に対して，

$$\mathfrak{S}_n f \mathfrak{S}_n = \mathfrak{S}_n g \mathfrak{S}_n \iff \Delta_f = \Delta_g$$

証明は省略する．

次に $\mathcal{P}(n) \ni \Delta = (\alpha_0, \alpha_1, \cdots, \alpha_n)$ に対して，次のように Σ_n の元 f_Δ を定義する．まず $\Lambda(\Delta) = \{i \mid 1 \leq i \leq n,\ \alpha_i > 0\}$ とし，$i \in \Lambda(\Delta)$ に対して Ω の部分集合 $J_{i,1}, J_{i,2}, \cdots, J_{i,\alpha_i}$ を次のように定める：

$$J_{i,p} = \left\{ \sum_{\substack{j \in \Lambda(\Delta) \\ j < i}} j\alpha_j + (p-1)i + \lambda \;\middle|\; \lambda = 1, 2, \cdots, i \right\} \qquad (p = 1, 2, \cdots, \alpha_i)$$

$J_{i,p}$ 中の最小の元を $a_{i,p}$ とする．また $J_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,\alpha_i}\}$ とおく．すると，Ω がこれらの $J_{i,p}$ $(i \in \Lambda(\Delta),\ 1 \leq p \leq \alpha_i)$ に分割されることは容易にわかる．そこで，写像 $f_\Delta : \Omega \to \Omega$ を，

$$f_\Delta(x) = a_{i,p} \qquad (x \in J_{i,p} \text{ のとき})$$

で定義する．f_Δ に属する分割は Δ に一致することは容易にわかる．

補題1により，直ちにΣ_nの$\mathfrak{S}_n$-両側類への分解を得る：

<u>補題 2.</u>
$$\Sigma_n = \bigcup_{\Delta \in \mathcal{P}(n)} \mathfrak{S}_n f_\Delta \mathfrak{S}_n \qquad (\text{disjoint union})$$

次に各両側類$\mathfrak{S}_n f_\Delta \mathfrak{S}_n$のcardinalityを分割$\Delta=(\alpha_0,\alpha_1,\cdots,\alpha_n)$を用いて表わすことを考えよう．対称群$\mathfrak{S}_n$の直積である群を$G=\mathfrak{S}_n\times\mathfrak{S}_n$で表わす．$G$は$\mathfrak{S}_n f_\Delta \mathfrak{S}_n$に次のように左から作用している：$g=(\rho,\sigma)\in G$，$h\in\mathfrak{S}_n f_\Delta\mathfrak{S}_n$に対して，

$$g(h) = \rho^{-1} h \sigma .$$

明らかに，群Gは集合$\mathfrak{S}_n f_\Delta \mathfrak{S}_n$にtransitiveに作用している．よって点$f_\Delta$の$G$における固定化群（stabilizer）を$\Gamma_\Delta$とすると，

$$|\mathfrak{S}_n f_\Delta \mathfrak{S}_n| = [G:\Gamma_\Delta] = \frac{|G|}{|\Gamma_\Delta|} = \frac{(n!)^2}{|\Gamma_\Delta|} .$$

そこで，固定化群Γ_Δを求めよう．$G\ni(\rho^{-1},\sigma)$が$(\rho^{-1},\sigma)\in\Gamma_\Delta$となるための必要十分条件は，先程の記号$\Lambda(\Delta)$, $J_{i,p}$, $a_{i,p}$, J_iを用いて次のようになる：

<u>補題 3.</u> $G\ni(\rho^{-1},\sigma)$が$(\rho^{-1},\sigma)\in\Gamma_\Delta$であれば，

(i) 各$i\in\Lambda(\Delta)$に対して，$\rho(J_i)=J_i$となる．

したがって$\{1,2,\cdots,\alpha_i\}$の置換θ_iが

(i)′ $\rho^{-1}(a_{i,p}) = a_{i,\theta_i(p)} \qquad (p=1,2,\cdots,\alpha_i)$

により定まる．さて(i)を満たす$\rho\in\mathfrak{S}_n$に対して，$(\rho^{-1},\sigma)\in\Gamma_\Delta$となるための必要十分条件は

(ii) $\sigma(J_{i,p}) = J_{i,\theta_i(p)}$. $(i \in \Lambda(\Delta),\ 1 \le p \le \alpha_i)$

証明は直接な計算による.

補題3を用いて, $|\Gamma_\Delta|$ を求めよう. まず (i) を満たすような $\rho \in \mathfrak{S}_n$ のなす $\mathfrak{S}_n$ の部分群を L_Δ とすれば, 容易に

$$|L_\Delta| = \alpha_0!\,\alpha_1!\cdots\alpha_n!$$

となることがわかる. 次に L_Δ の元 ρ を一つ固定したとき, $(\rho^{-1},\sigma) \in \Gamma_\Delta$ となるような $\sigma \in \mathfrak{S}_n$ の部分集合を $R_{\Delta,\rho}$ とおく. (ii) より $|R_{\Delta,\rho}| = (1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}$ を得る. したがって $|R_{\Delta,\rho}|$ は $\rho \in L_\Delta$ のとり方によらない. これで

$$|\Gamma_\Delta| = \sum_{\rho\in L_\Delta} |R_{\Delta,\rho}| = |L_\Delta|\cdot|R_{\Delta,\rho}|$$
$$= \alpha_0!\,\alpha_1!\cdots\alpha_n!\,(1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}$$

を得て次の補題を得る.

<u>補題4.</u> n の分割 $\Delta = (\alpha_0, \alpha_1, \cdots, \alpha_n)$ に対して,

$$l_\Delta = \alpha_0!\,\alpha_1!\cdots\alpha_n!\ ,\qquad r_\Delta = (1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}$$

とおけば,

$$\text{(i)}\quad |\mathfrak{S}_n f_\Delta \mathfrak{S}_n| = \frac{n!}{l_\Delta}\frac{n!}{r_\Delta}$$

$$\text{(ii)}\quad n^n = \sum_{\Delta\in\mathcal{P}(n)} \frac{n!}{l_\Delta}\frac{n!}{r_\Delta}$$

§3. 定理1の証明.

n の分割 $\Delta = (\alpha_0, \alpha_1, \cdots, \alpha_n)$ に対する Σ_n の元 f_Δ は, $\alpha_1 = n$ ならば $\mathfrak{S}_n$ に属する. $\alpha_1 < n$ ならば $f_\Delta \in \Sigma_n^*$ である.

しかもこのとき，f_Δ は次のように γ_j^i の積として表わされる．すなわち既述の記号を用いて，互いに可換な元

$$\gamma_{a_{ip}}^{a} \qquad (a \in J_{ip} - \{a_{ip}\})$$

の積を Z_{ip} とおく．すると，$Z_{i1}, \cdots, Z_{i\alpha_i}$ も互いに可換である．その積を Z_i とすると Z_i も又互いに可換である．すなわち，

$$f_\Delta = \prod_{\substack{i \in \Lambda(\Delta) \\ i \geq 2}} \prod_{p=1}^{\alpha_i} \prod_{a \in J_{ip} - \{a_{ip}\}} \gamma_{a_{ip}}^{a} .$$

これと補題2より，$\mathfrak{S}_n$ と $\{\gamma_j^i\}$ とが Σ_n を生成することがわかった．次に $\{\gamma_j^i\}$ が Σ_n^* を生成することを示そう．

与えられた $f \in \Sigma_n^*$ に属する分割を $\Delta = (\alpha_0, \alpha_1, \cdots, \alpha_n)$ とすると，$\alpha_1 < n$ である．また $f \in \mathfrak{S}_n f_\Delta \mathfrak{S}_n$ である．(補題1.) いま，$\{\gamma_j^i\}$ の生成する Σ_n^* の部分半群を $\mathfrak{M}$ とおく．$f_\Delta \in \mathfrak{M}$ であるから，$\mathfrak{M} = \Sigma_n^*$ を示すためには，

$$\mathfrak{S}_n \mathfrak{M} \subset \mathfrak{M}, \quad \mathfrak{M} \mathfrak{S}_n \subset \mathfrak{M}$$

をいえばよい．これは次の補題から直ちに得られる．

<u>補題 5.</u>

$$\gamma_j^i \sigma_\ell^k = \gamma_k^i \gamma_\ell^k \gamma_i^\ell \gamma_j^i \qquad (\#\{i,j,k,\ell\} = 4)$$

$$\gamma_j^i \sigma_j^k = \gamma_j^i \gamma_k^j \gamma_i^k \qquad (\#\{i,j,k\} = 3)$$

$$\sigma \gamma_j^i \sigma^{-1} = \gamma_{\sigma(j)}^{\sigma(i)} \qquad (\sigma \in \mathfrak{S}_n) .$$

◎注意：Σ_n は $\mathfrak{S}_n$ の適当な生成元2個と γ_2^1 の3個で生成される．また Σ_n^* は $\frac{1}{2}n(n-1)$ 個の γ_j^i で生成されることも証明

され，それ以下の個数では生成されないことも証明出来る．

§4. $\{\gamma^i_j, \sigma^k_l\}$ に関する Σ_n の基本関係式

まず次の等式 (1)〜(15) が Σ_n で成り立つことは，直接計算でわかる．

(1) $\sigma^k_l = \sigma^l_k$

(2) $\sigma^k_l \sigma^k_l = e$ （e は恒等置換）

(3) $\sigma^l_j \sigma^k_l = \sigma^k_j \sigma^j_l$ （$\#\{k, l, j\} = 3$）

(4) $\sigma^i_j \sigma^k_l = \sigma^k_l \sigma^i_j$ （$\#\{k, l, i, j\} = 4$）

(5) $\sigma^k_l \gamma^i_j \sigma^k_l = \gamma^i_j$ （$\#\{k, l, i, j\} = 4$）

(6) $\sigma^i_k \gamma^i_j \sigma^i_k = \gamma^k_j$ （$\#\{k, i, j\} = 3$）

(7) $\sigma^k_j \gamma^i_j \sigma^k_j = \gamma^i_k$ （$\#\{k, i, j\} = 3$）

(8) $\sigma^i_j \gamma^i_j \sigma^i_j = \gamma^j_i$ （$\#\{i, j\} = 2$）

(9) $\gamma^i_j \gamma^k_l = \gamma^k_l \gamma^i_j$ （$\#\{k, l, i, j\} = 4$）

(10) $\gamma^i_j \gamma^k_j = \gamma^k_j \gamma^i_j = \gamma^i_j \gamma^k_i$ （$\#\{k, i, j\} = 3$）

(11) $\gamma^i_j \gamma^j_k = \gamma^i_k \sigma^i_j$ （$\#\{k, i, j\} = 3$）

(12) $\gamma^i_j \gamma^i_k = \gamma^i_k$ （$\#\{k, i, j\} = 3$）

(13) $\gamma^i_j \gamma^i_j = \gamma^i_j$

(14) $\gamma^j_i \gamma^i_j = \gamma^j_i$

(15) $\gamma^i_j \sigma^i_j = \gamma^i_j$

<u>定理 2.</u> n を自然数とし，$\mathcal{T}$ を単位元 1 をもつ半群で，元 c^i_j，s^k_l $(1 \leq i, j, k, l \leq n,\ i \neq j,\ k \neq l)$ から生成され，c^i_j，s^k_l は $\gamma^i_j \leftrightarrow c^i_j$，$\sigma^k_l \leftrightarrow s^k_l$ なるおきかえで (1) ～ (15) を満たすものとする．すると，$|\mathcal{T}| \leq n^n$ であり，準同型 $\theta : \Sigma_n \longrightarrow \mathcal{T}$ が存在して，各 i, j, k, l に対して

$$\theta(\gamma^i_j) = c^i_j, \quad \theta(\sigma^k_l) = s^k_l \qquad \text{となる．}$$

証明は次のような段階に分かれる．まづ，$\{s^k_l \mid 1 \leq k, l \leq n,\ k \neq l\}$ の生成する $\mathcal{T}$ の部分半群 S は，$s^k_l s^k_l = 1$ により，$\mathcal{T}$ の部分群となり，S の単位元は $\mathcal{T}$ の単位元 1 と一致する．$\{s^k_l\}$ が (1) ～ (4) を満たすから，対称群の理論においてよく知られているように（例えば [2] を参照）群準同型

$$\pi : \mathfrak{S}_n \longrightarrow S$$

が存在して，各 k, l に対して $\pi(\sigma^k_l) = s^k_l$ となる．いま，$\mathfrak{S}_n$ の元と $\mathcal{T}$ の元の"積"を次のように $\mathcal{T}$ の元として定義する：

$$\sigma \cdot t = \pi(\sigma) t \qquad (\sigma \in \mathfrak{S}_n,\ t \in \mathcal{T})$$

$$t \cdot \sigma = t \cdot \pi(\sigma) \qquad (\sigma \in \mathfrak{S}_n,\ t \in \mathcal{T})$$

すると，"結合律"

$$(\sigma_1 t)\sigma_2 = \sigma_1 (t \sigma_2) \qquad (\sigma_1, \sigma_2 \in \mathfrak{S}_n,\ t \in \mathcal{T})$$

の成立は明らかである．さて $\mathcal{T}$ において，

<u>補題 6</u>　　$\sigma c_j^i \sigma^{-1} = c_{\sigma(j)}^{\sigma(i)}$.　　$(\sigma \in \mathfrak{S}_n)$

証明：σ として $\mathfrak{S}_n$ の生成元 σ_ℓ^k をとって示せばよい．しかしそれが (5) ～ (8) である．

<u>補題 7.</u> (Reduction Rule in $\mathfrak{F}$)．$p \geq 2$ とし，

$$f = c_{j_p}^{i_p} c_{j_{p-1}}^{i_{p-1}} \cdots c_{j_1}^{i_1} \in \mathfrak{F} \quad \text{が}$$

(i) $\{i_\nu, j_\nu\} \cap \{i_1, i_2, \cdots, i_{\nu-1}\} = \phi \qquad (2 \leq \nu \leq p-1)$

(ii) $\{i_p, j_p\} \cap \{i_1, i_2, \cdots, i_{p-1}\} \neq \phi$ を満たせば，

$$f = \begin{cases} c_{j_{p-1}}^{i_{p-1}} \cdots c_{j_1}^{i_1}, & i_p \in \{i_1, i_2, \cdots, i_{p-1}\} \\ \delta_{j_p}^{i_p} c_{j_{p-1}}^{i_{p-1}} \cdots c_{j_1}^{i_1}, & i_p \notin \{i_1, i_2, \cdots, i_{p-1}\} \end{cases}$$

証明：$p=2$ のときは成り立つ．p による帰納法で証明する．$p>3$ のときは $p-1$ のときに帰着するが長くなるので省略する．(1)，(5) ～ (15) をこゝで用いる．

一般に，$\Omega = \{1, 2, \cdots, n\}$ の部分集合を $J (\neq \phi)$ とし，$\Omega - J$ 中の元 j に対して，$\mathfrak{F}$ の元 c_j^J を次で定義する：

<u>定義</u>　$J = \{j_1, \cdots, j_r\}$，$r = |J|$ として，

$$c_j^J = c_j^{j_1} \cdots\cdots c_j^{j_r}.$$

こゝで (10) により，右辺の積は $j_1, \cdots, j_r$ の並べ方によらないことに注意する．すると次が成り立つ．

<u>補題 8.</u> (Normalization)　$f = c_{j_p}^{i_p} \cdots c_{j_1}^{i_1} \in \mathfrak{F}$ が

$$\{i_\nu, j_\nu\} \cap \{i_1, \cdots, i_{\nu-1}\} = \phi, \quad (\nu = 2, \cdots, p)$$

を満たすならば，$\{i_1, \cdots, i_p\}$ の空でない部分集合 $K_1, \cdots, K_m$

と，$\{j_1, \cdots, j_p\}$ の元 $k_1, \cdots, k_m$ が存在して

$$f = c_{k_1}^{K_1} \cdots\cdots c_{k_m}^{K_m} \qquad \text{となる．}$$

ただし，$K_1 \cup \cdots\cdots \cup K_m = \{i_1, \cdots, i_p\}$

$$(K_\mu \cup \{k_\mu\}) \cap (K_\nu \cup \{k_\nu\}) = \phi, \quad (1 \leq \mu, \nu \leq m)$$

証明：これも長くなるので省略するが，p に関する帰納法による．

さて，n の分割 Δ に対して，§2 の $\Lambda(\Delta)$, $J_{i,p}$, $a_{i,p}$, J_i を考え，また $\Lambda^*(\Delta) = \{i \in \Lambda(\Delta) \mid i \geq 2\}$ とおく．

$c_\Delta \in \mathfrak{F}$ を

$$c_\Delta = \prod_{i \in \Lambda^*(\Delta)} \prod_{p=1}^{\alpha_i} c_{a_{i,p}}^{J_{i,p}^*}$$

で定義する．ただし，$J_{i,p}^* = J_{i,p} - \{a_{i,p}\}$ である．（(9)により $c_{a_{i,p}}^{J_{i,p}^*}$ は互いに交換可能であることに注意．）すると

<u>補題 9</u>　$\mathfrak{F} = \bigcup_{\Delta \in \mathcal{P}(n)} S c_\Delta S$

証明：$f \in \mathfrak{F}$ はいくつかの c_j^i といくつかの σ_ℓ^k の積の形に書ける．一方補題 6 により $\sigma c_q^p = c_{q'}^{p'} \sigma$ $(p' = \sigma(p),\ q' = \sigma(q),\ \sigma \in \mathfrak{S}_n)$ となるから，$s_{\ell_t}^{k_t} \cdots s_{\ell_1}^{k_1} c_j^i$ の形は，$c_{j'}^{i'} s_{\ell_t}^{k_t} \cdots s_{\ell_1}^{k_1}$ の形に書き直せる．よって，f は

$$f = c_{j_k}^{i_k} \cdots\cdots c_{j_1}^{i_1} s, \qquad s \in S$$

の形に書き直せる．もし $\{i_\nu, j_\nu\} \cap \{i_1, \cdots, i_{\nu-1}\} = \phi$ が $\nu = 2, \cdots, k$ に対して成立すれば，補題 8 (normalization) により $\{i_1, \cdots, i_k\}$ の空でない部分集合 $K_1, \cdots, K_m$ と，$\{j_1, \cdots, j_k\}$

中の元 $k_1, \cdots, k_m$ が存在して

$$c_{j_k}^{i_k} \cdots c_{j_1}^{i_1} = c_{k_1}^{K_1} \cdots c_{k_m}^{K_m},$$

$$K_1 \cup \cdots \cup K_m = \{i_1, \cdots, i_k\},$$

$$(K_\mu \cup \{k_\mu\}) \cap (K_\nu \cup \{k_\nu\}) = \phi, \quad (1 \leq \mu, \nu \leq m)$$

となる．すると，n の分割 Δ と $\mathfrak{S}_n$ 中の置換 ρ が存在して，

$$c_{j_k}^{i_k} \cdots c_{j_1}^{i_1} = \rho c_\Delta \rho^{-1}$$

となることが容易にわかる．よって，$f = \rho c_\Delta \rho^{-1} \sigma \in \mathfrak{S}_n c_\Delta \mathfrak{S}_n = S c_\Delta S$．次に $\{i_p, j_p\} \cap \{i_1, \cdots, i_{p-1}\} \neq \phi$ なる番号 p, $2 \leq p \leq k$ が存在する場合を考えよう．そのような p のうちで最小なものを改めて p とすると，$\{i_\nu, j_\nu\} \cap \{i_1, \cdots, i_{\nu-1}\} = \phi \quad (\nu = 2, \cdots, p-1)$ となる．よって補題7（Reduction Rule）により，

$$c_{j_k}^{i_k} \cdots\cdots c_{j_1}^{i_1} = c_{j_k}^{i_k} \cdots c_{j_{p+1}}^{i_{p+1}} \theta \, c_{j_{p-1}}^{i_{p-1}} \cdots c_{j_1}^{i_1}$$

と書ける．ただし，$\theta = 1$ または $\theta = s_{j_p}^{i_p}$ である．すると，f は k 個より少ない c_j^i の積と S の元の積の形：

$$(*) \qquad f = c_{m_t}^{l_t} \cdots c_{m_1}^{l_1} s', \qquad s' \in S$$

に書ける．この操作をくり返せば，結局 $(*)$ の形の表示で，t が最小値に達するように出来る．それを

$$f = c_{j_g}^{i_g} \cdots c_{j_1}^{i_1} s'', \qquad s'' \in S$$

とすれば，$\{i_\nu, j_\nu\} \cap \{i_1, \cdots, i_{\nu-1}\} = \phi$ が $\nu = 2, \cdots, g$ に対して成り立つ．すると上述のように $f \in \mathfrak{S}_n c_\Delta \mathfrak{S}_n = S c_\Delta S$ となる．ある $\Delta \in \mathcal{P}(n)$ に対して，

<u>補題 10.</u> $\Delta=(\alpha_0,\alpha_1,\cdots,\alpha_n)$ に対して，§2 と同様に $\Lambda(\Delta)$, J_{ip}, a_{ip}, J_i $(i\in\Lambda(\Delta))$ を考える．$\rho(J_i)=J_i$ (各 $i\in\Lambda(\Delta)$ に対して) を満たすような $\rho\in\mathfrak{S}_n$ のなす $\mathfrak{S}_n$ の部分群を L_Δ とする．すると L_Δ の各元 ρ に対して $\rho c_\Delta\sigma=c_\Delta$ を満たす $\sigma\in\mathfrak{S}_n$ が存在する．

証明： L_Δ の生成系中の ρ について，σ の存在を証明すればよい．($\rho_1 c_\Delta\sigma_1=c_\Delta$, $\rho_2 c_\Delta\sigma_2=c_\Delta$ から $\rho_2\rho_1 c_\Delta\sigma_1\sigma_2=c_\Delta$ が導かれるからである.) よって ρ が J_i 中の 2 元 a_{ip} と a_{iq} の互換である場合をすれば十分である．$J_{ip}=\{x_1,\cdots,x_i\}$ $x_1=a_{ip}$, $J_{iq}=\{y_1,\cdots,y_i\}$, $y_1=a_{iq}$ とする．このとき $\sigma=\sigma_{y_1}^{x_1}\sigma_{y_2}^{x_2}\cdots\sigma_{y_i}^{x_i}$ とおくと $\rho c_\Delta\sigma=c_\Delta$ が成り立つことが基本関係を用いて示せる．

<u>補題 11.</u> $\mathcal{P}(n)\ni\Delta=(\alpha_0,\alpha_1,\cdots,\alpha_n)$ に対して

$$|S c_\Delta S|\le\frac{n!}{\alpha_0!\,\alpha_1!\cdots\alpha_n!}\,\frac{n!}{(1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}}.$$

証明： 補題 10 の部分群 L_Δ の各元 ρ に対して，

$$R_{\Delta,\rho}=\{\sigma\in\mathfrak{S}_n\mid\rho c_\Delta\sigma=c_\Delta\}$$

とおく．$R_{\Delta,\rho}\neq\phi$ である．$R_{\Delta,\rho}$ の元 σ_1 を一つ固定すると，$\sigma\in\mathfrak{S}_n$ に対して

$$\rho c_\Delta\sigma=\rho c_\Delta\sigma_1\iff c_\Delta=c_\Delta\sigma\sigma_1^{-1}$$

であるから

$$Q_\Delta = \{ \theta \in \mathfrak{S}_n \mid c_\Delta \theta = c_\Delta \}$$

とおくと，Q_Δ は $\mathfrak{S}_n$ の部分群で，$R_{\Delta,\rho} = Q_\Delta \sigma_1$ となる．したがって，$|R_{\Delta,\rho}| = |Q_\Delta|$．次に

$$(**) \qquad |Q_\Delta| \geq (1!)^{\alpha_1}(2!)^{\alpha_2}\cdots\cdots(n!)^{\alpha_n}$$

を示そう．$\Lambda^*(\Delta) = \{ i \in \Lambda(\Delta) \mid i \geq 2 \}$ とおき，$\mathfrak{S}_n$ の部分群 $R_\Delta = \{ \theta \in \mathfrak{S}_n \mid \theta(J_{i,p}) = J_{i,p} \ (i \in \Lambda^*(\Delta),\ 1 \leq p \leq \alpha_i) \}$ を考える．$|R_\Delta| = (1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}$ であるから，$Q_\Delta \supset R_\Delta$ を言えばよい．それには R_Δ の生成元である $J_{i,p}$ 中の 2元の互換 θ が Q_Δ に属すること，すなわち，$c_\Delta \theta = c_\Delta$ を言えばよい．これも基本関係から導かれ，よって $(**)$ を得る．次に $\mathfrak{S}_n \times \mathfrak{S}_n$ の部分群

$$T_\Delta = \{ (\rho^{-1}, \sigma) \mid \rho c_\Delta \sigma = c_\Delta \}$$

を考えよう．$|S c_\Delta S| = |\mathfrak{S}_n c_\Delta \mathfrak{S}_n| = [\mathfrak{S}_n \times \mathfrak{S}_n : T_\Delta]$ である．一方

$$T_\Delta \supseteq \bigcup_{\rho \in L_\Delta} R_{\Delta,\rho}$$

よって，$|T_\Delta| \geq \sum_{\rho \in L_\Delta} |R_{\Delta,\rho}| = |L_\Delta| \cdot |Q_\Delta|$．

前に計算したように，$|L_\Delta| = \alpha_0!\,\alpha_1!\cdots\alpha_n!$ であるから，

$$|T_\Delta| \geq \alpha_0!\,\alpha_1!\cdots\alpha_n!\,(1!)^{\alpha_1}(2!)^{\alpha_2}\cdots\cdots(n!)^{\alpha_n}.$$

これから，

$$|S c_\Delta S| \leq \frac{n!}{\alpha_0!\,\alpha_1!\cdots\alpha_n!} \cdot \frac{n!}{(1!)^{\alpha_1}(2!)^{\alpha_2}\cdots(n!)^{\alpha_n}}$$

定理2の証明：　補題9, 11 および補題4から $|\mathcal{T}| \leq n^n$.
次に単位元1を有し，元 $\tilde{c}_j^i$, $\tilde{\sigma}_\ell^k$ から生成され，γ_j^i を $\tilde{c}_j^i$, σ_ℓ^k を $\tilde{\sigma}_\ell^k$ と考えたとき (1)〜(15) を基本関係にもつ universal な半群を $\tilde{\mathcal{T}}$ とする．すると準同型 φ: $\tilde{\mathcal{T}} \to \Sigma_n$ が存在して，$\varphi(1)=1$, $\varphi(\tilde{c}_j^i)=\gamma_j^i$, $\varphi(\tilde{\sigma}_\ell^k)=\sigma_\ell^k$ $(1 \leq i, j, k, \ell \leq n)$ となる．よって $\varphi(\tilde{\mathcal{T}}) = \Sigma_n$ であるが，上に証明した定理2の前半により，$|\tilde{\mathcal{T}}| \leq n^n = |\Sigma_n|$ となる．したがって φ は 1:1 となり，$\tilde{\mathcal{T}} \cong \Sigma_n$ である．故に定理2の後半が証明された．

§4. Σ_n の元の $\mathfrak{S}_n$-γ-length.

<u>定義</u>　Σ_n の元 f は

$$f = \gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1} \sigma \quad , \quad \sigma \in \mathfrak{S}_n$$

の形で表わされる．このような表示全体の中で k の値の最小値を f の $\mathfrak{S}_n$-γ-length と呼び，これを $\ell^*(f)$ と書く．

<u>定理3.</u>　$f \in \Sigma_n$ に対して，

$$\ell^*(f) = n - |f(\Omega)| .$$

証明：　$\ell^*(f)=k$ とし，最小値 k を与える f の表示をとり，これを　$f = \gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1} \sigma$, $\sigma \in \mathfrak{S}_n$ とする．
このとき，補題7 (Reduction Rule) により，$\{i_\nu, j_\nu\} \cap \{i_1, \cdots, i_{\nu-1}\} = \phi$ が $\nu = 2, \cdots, k$ に対して成り立つ．

さて，kに対する帰納法によりこゝで

$$f(\Omega) = \Omega - \{i_1, \cdots, i_k\},$$

の成立がわかり，$|f(\Omega)| = n-k$．故に $l^*(f) = n - |f(\Omega)|$．

これの系として次のことがわかる．

<u>系</u>　$f, g \in \Sigma_n$，　$f = \gamma_j^i g$　のとき，

$$l^*(f) = \begin{cases} l^*(g)+1, & (\{i,j\} \subset g(\Omega)\text{の時}) \\ l^*(g), & (\{i,j\} \not\subset g(\Omega)\text{の時}) \end{cases}$$

実は，上の定理3，系をあらかじめ独立に証明しておくことにより Σ_n における Reduction Rule の成立が導かれる．これが Reduction Rule を発見する動機であった．

§5.　Σ_n^* の元の γ-length

<u>定義</u>　Σ_n^* の元 f は

$$f = \gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1}$$

の形で表わされる．このような表示全体の中で k の値の最小値を f の γ-length と呼び，これを $l(f)$ と書く．

$l(f)$ の値を，f から自然に定まる一つの"有向グラフ" $\mathfrak{D}(f)$ を用いて表わす式を述べよう．$\mathfrak{D}(f)$ の定義は次の通りである：

$\mathfrak{D}(f)$ の頂点 $\cdots$ $\Omega = \{1, 2, \cdots, n\}$ の元．

$\mathfrak{D}(f)$ の2頂点 i, j に対して $\mathfrak{D}(f)$ における i から j へ行く

有向線分がある $\Longleftrightarrow$ $f(i)=j$.

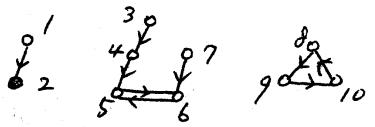
したがって，$f(i)=i$ のときは頂点 i は loop となる．

以下 有向グラフ $\mathcal{D}(f)$ の図示において，頂点 $i\in\Omega$ は

$$\begin{cases} f(i)=i & \text{のとき } \bullet^{i} \text{ で} \\ f(i)\neq i & \text{のとき } \circ^{i} \text{ で} \end{cases}$$

表わすことにする．

例．　$f=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 2 & 4 & 5 & 6 & 5 & 6 & 9 & 10 & 8 \end{pmatrix}$ とすると



から $\mathcal{D}(f)$ である．

さて，$f\in\Sigma_n^*$ に対して $\mathcal{D}(f)$ 中の loop となっている頂点の全体を F_f とする．すなわち，

$$F_f=\{x\in\Omega \mid f(x)=x\}.$$

次に，$\mathcal{D}(f)$ 中の純回路なるものを次で定義する．すなわち Ω の部分集合 C であって，

1) $|C|>1$

2) $f(C)\subset C$

3) $f(\Omega-C)\subset\Omega-C$

4) f の C 上の制限 $f|_C$ は C の置換全体のなす群 $\mathfrak{S}_C$ の中で C 上に transitive な部分群を生成する．

例．　上の例では $F_f=\{2\}$，純回路は $C=\{8,9,10\}$ だけで $\{5,6\}$ は純回路ではない．

<u>定義</u>. $f \in \Sigma_n^*$ に対して，$\mathcal{D}(f)$ 中の純回路全体のなす集合を

$\mathcal{P}_f$ で表わす.

<u>定理 4.</u> $f \in \Sigma_n^*$ に対して，

$$l(f) = n + |\mathcal{P}_f| - |F_f| .$$

証明： いくつかの γ_j^i のなす長さ s の系列 $c = (\gamma_{j_1}^{i_1}, \cdots, \gamma_{j_s}^{i_s})$ ($\gamma_{j_\nu}^{i_\nu}$ の中には等しいものがあってもよい.) と，$x \in \Omega$ に対して，x の c-系列なるものを次のように定義する. それは Ω の元よりなる長さ $s+1$ の系列

$$x_0, x_1, \cdots\cdots, x_s$$

であって，

$$x_0 = x, \quad x_1 = \gamma_{j_1}^{i_1}(x_0), \quad x_2 = \gamma_{j_2}^{i_2}(x_1), \cdots, x_s = \gamma_{j_s}^{i_s}(x_{s-1})$$

で定義されたものである. このとき，$J = \{1, 2, \cdots, s\}$ の部分集合 $H_x(c)$ を

$$H_x(c) = \{\nu \in J \mid x_{\nu-1} \neq x_\nu\}$$

で定義する. γ_j^i の定義により，$\nu \in J$ に対して，

$$\nu \in H_x(c) \iff x_{\nu-1} = i_\nu, \quad x_\nu = j_\nu$$

となることに注意しておく.

<u>補題 12.</u> $f \in \Sigma_n^*$, $c = (\gamma_{j_1}^{i_1}, \cdots, \gamma_{j_s}^{i_s})$

$$f = \gamma_{j_s}^{i_s} \cdots\cdots \gamma_{j_1}^{i_1}$$

とする. また x, y は Ω の元で $x \neq y$ とする. もし x を含

ような純回路 C が $\mathfrak{D}(f)$ 中に存在すれば

$$H_x(c) \cap H_y(c) = \phi .$$

証明： 省略．定義に戻って考えれば容易．

<u>補題 13.</u> f, c を補題 12 と同様とする．

(i) $x \in \Omega - F_f$ ならば $|H_x(c)| \geq 1$,

(ii) $C \in \mathfrak{P}_f$ ならば，ある $x \in C$ に対して $|H_x(c)| \geq 2$.

証明： 省略．これも定義から容易に出来る．

<u>補題 14.</u> f, c を補題 12 と同様とする．

$$s \geq n - |F_f| + |\mathfrak{P}_f|$$

したがって，とくに

$$l(f) \geq n - |F_f| + |\mathfrak{P}_f| \quad \text{を得る．}$$

証明： $J = \{1, 2, \cdots, s\}$ とし，$H = \bigcup_{x \in \Omega} H_x(c)$ とおく．$\mathfrak{D}(f)$ 中のすべての純回路を並べて，$\mathfrak{P}_f = \{C_1, \cdots, C_k\}$, $k = |\mathfrak{P}_f|$ とする．$C_f = C_1 \cup \cdots \cup C_k$, $M_f = \Omega - (C_f \cup F_f)$ とおく．純回路の定義より，$C_\mu \cap C_\nu = \phi$ である．補題 12 より，H は

$$H_1 = \bigcup_{i=1}^{k} \bigcup_{x \in C_i} H_x(c)$$

と

$$H_2 = \left\{ \bigcup_{y \in M_f} H_y(c) \right\} \cup \left\{ \bigcup_{z \in F_f} H_z(c) \right\}$$

とに分かれる： $H = H_1 \cup H_2$, $H_1 \cap H_2 = \phi$．更に補

題 12, 13 により

$$|H_1| = \sum_{i=1}^{k} \sum_{x \in C_i} |H_x(c)|$$
$$\geq \sum_{i=1}^{k} (|C_i| + 1) = k + \sum_{i=1}^{k} |C_i|$$

が成り立つ. $|H_2| \geq |M_f|$ は容易にわかる. よって,

$$s \geq |H| = |H_1| + |H_2|$$
$$\geq k + \sum_{i=1}^{k} |C_i| + |M_f|$$
$$= n + k - |F_f| = n + |\mathcal{P}_f| - |F_f|.$$

<u>補題 15</u>　$f \in \Sigma_n^*$ に対して,

$$N(f) = n + |\mathcal{P}_f| - |F_f|$$

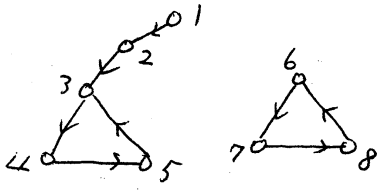
とおくと, f は $N(f)$ 個の γ_j^i の積で書ける. したがって, $\ell(f) \leq N(f)$.

証明: n に関する帰納法による. ($n=2$ のときは明らか). しかし長くなるので省略する.

補題 14, 15 より $\ell(f) = N(f)$ となって定理 4 の証明は完了した.

例. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 3 & 7 & 8 & 6 \end{pmatrix}$

$\mathcal{D}(f)$:



$$\ell(f) = 8 + 1 - 0 = 9.$$

$f = \gamma_2^1 \gamma_3^2 \gamma_4^3 \gamma_5^4 \gamma_6^5 \gamma_7^6 \gamma_8^7 \gamma_5^8 \gamma_2^5$ は一つの minimal

expression である.

◎注意: $f \in \Sigma_n^*$ が $|f(\Omega)| = n-1$ であるときには, f の任意の minimal expression $f = \gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1}$ に対して, 必らず $j_k = i_{k-1}$, $j_{k-1} = i_{k-2}$, $\cdots$, $j_2 = i_1$ となることが証明出来るが その証明は長くなるので省略する.

参考文献

[1] Clifford - Preston : The Algebraic Theory of Semigroup. vol. I. A.M.S.

[2] Steinberg : Appendix of Finite Reflection Group of "Lectures on Chevalley Groups" Yale Univ.