

# 変換半群の生成元, 基本関係式, 元の長さ

青山学院大理工 岩堀 信子

## §1. 変換半群とその生成元

$\Omega = \{1, 2, \dots, n\}$  を有限集合とし,  $\Omega$  から  $\Omega$  への写像全体のつくる集合を  $\Sigma_n$  で表わす.  $\Sigma_n$  は写像の積の意味で単位元をもつ半群となる. これを変換半群という.  $\Sigma_n$  の元ごとくに *bijection* 全体のつくる部分集合を  $\mathcal{G}_n$  ( $n$  次対称群と同型) と書き,  $\Sigma_n^* = \Sigma_n - \mathcal{G}_n$  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  $\Sigma_n$  中の特別な元  $\sigma_{kl}^k, \gamma_j^i$  を次式で定義する. まず  $\sigma_{kl}^k$  は  $\Omega$  中の 2 文字  $k, l$  ( $k \neq l$ ) の互換である. また  $\gamma_j^i$  ( $i \neq j$ ) は,  $i$  と  $j$  に写し,  $i$  以外の元はそれぞ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,

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

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

すると次の定理が得られる。

定理 1.

(i)  $\{\sigma_k, \gamma_j^i \mid k, l, i, j \in \Omega, k \neq l, i \neq j\}$  は半群  $\Sigma_n$  を生成する。

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

本稿の主目的は、生成元系  $\{\sigma_k, \gamma_j^i\}$  に関して半群  $\Sigma_n$  の基本関係式を求めること、 $\Sigma_n^*$  の元  $f$  をいくつかの  $\gamma_j^i$  の積として表わすときの因子の個数の最小値（すなわち、生成元系  $\{\gamma_j^i\}$  に関する  $f$  の“長さ”） $l(f)$  を与える式を求めるところである。

§2.  $\Sigma_n$  の  $\mathcal{G}_n$ -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、後から基本関係式導出する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。まづ

定義 自然数  $n$  の分割とは負でない整数の列

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

$$\text{であつて, } \alpha_0 + \alpha_1 + \dots + \alpha_n = n$$

$$\text{かつ, } \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n$$

と満たすものをいう。  $n$  の分割  $\Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$

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  $\mathcal{P}(n)$  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,  $\#, |\dots|$  はいつれも元の個数を意味する.

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

補題 1.  $f, g \in \Sigma_n$  に対し,

$$\mathcal{G}_n f \mathcal{G}_n = \mathcal{G}_n g \mathcal{G}_n \iff \Delta_f = \Delta_g$$

証明は省略する.

次に  $\mathcal{P}(n) \ni \Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  に対し, 次のように  $\Sigma_n$  の元  $f_\Delta$  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  $\Omega$  の部分集合  $J_{i,1}, J_{i,2}, \dots, J_{i,\alpha_i}$  を次のように定める:

$$J_{i,p} = \left\{ \sum_{\substack{j \in \Lambda(\Delta) \\ j < i}} j \alpha_j + (p-1)i + \lambda \mid \lambda = 1, 2, \dots, i \right\} \quad (p=1, 2, \dots, \alpha_i)$$

$J_{i,p}$  中の最も小さい元を  $a_{i,p}$  とする. また  $J_i = \{a_{i,1}, a_{i,2}, \dots, a_{i,\alpha_i}\}$  とおく. すると,  $\Omega$  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  $f_\Delta: \Omega \rightarrow \Omega$  と

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

を定義する.  $f_\Delta$  に属する分割は  $\Delta$  に一致することは容易にわかる.

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

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

次に各両側類  $\mathfrak{S}_n f_{\Delta} \mathfrak{S}_n$  の cardinality を分割  $\Delta = (\alpha_1, \alpha_2, \dots, \alpha_n)$  を用いて表わすことと考へよう. 対称群  $\mathfrak{S}_n$  の直積である群  $G = \mathfrak{S}_n \times \mathfrak{S}_n$  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  $f_{\Delta}$  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  $\Gamma_{\Delta}$  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:

補題 3.  $G \ni (\rho^{-1}, \sigma)$  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  $\{1, 2, \dots, \alpha_i\}$  の置換  $\theta_i$  が

(i)'  $\rho^{-1}(a_{i,p}) = a_{i, \theta_i(p)}$  ( $p=1, 2, \dots, \alpha_i$ )

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

$$(i) \quad \sigma(J_{i,p}) = J_{i, \sigma(p)}. \quad (i \in \Lambda(\Delta), 1 \leq p \leq \alpha_i)$$

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  $f \in \mathfrak{S}_n$  のなす  $\mathfrak{S}_n$  の部分群を  $L_\Delta$  とすれば, 容易に

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

となることかわかる. 次に  $L_\Delta$  の元  $f$  を一つ固定したとき,  $(f^{-1}\sigma) \in \Gamma_\Delta$  となるような  $\sigma \in \mathfrak{S}_n$  の部分集合を  $R_{\Delta, f}$  とおく.

(ii) より  $|R_{\Delta, f}| = (1!)^{\alpha_0} (2!)^{\alpha_1} \cdots (n!)^{\alpha_n}$  を得る. (これによって  $|R_{\Delta, f}|$  は  $f \in L_\Delta$  のとり方によらない. したがって

$$\begin{aligned} |\Gamma_\Delta| &= \sum_{f \in L_\Delta} |R_{\Delta, f}| = |L_\Delta| \cdot |R_{\Delta, f}| \\ &= \alpha_0! \alpha_1! \cdots \alpha_n! (1!)^{\alpha_0} (2!)^{\alpha_1} \cdots (n!)^{\alpha_n} \end{aligned}$$

を得て次の補題を得る.

補題4.  $n$  の分割  $\Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  に対して,

$$l_\Delta = \alpha_0! \alpha_1! \cdots \alpha_n! \quad , \quad \gamma_\Delta = (1!)^{\alpha_0} (2!)^{\alpha_1} \cdots (n!)^{\alpha_n}$$

とすれば,

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

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

### §3. 定理1の証明.

$n$  の分割  $\Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  に対する  $\Sigma_n$  の元  $f_\Delta$  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,  $f_\Delta$  は次のように  $\gamma_j^i$  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

$$\gamma_{a_i p}^a \quad (a \in J_{ip} - \{a_{ip}\})$$

の積と  $z_{ip}$  とおく。すると,  $z_{i1}, \dots, z_{i\alpha_i}$  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

わら,

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

これと補題2より,  $\mathcal{G}_n$  と  $\{\gamma_j^i\}$  とが  $\Sigma_n$  を生成することになった。次に  $\{\gamma_j^i\}$  が  $\Sigma_n^*$  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  $\Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  とすると,  $\alpha_1 < n$  である。また  $f \in \mathcal{G}_n f_\Delta \mathcal{G}_n$  である。(補題1) 以下,  $\{\gamma_j^i\}$  の生成する  $\Sigma_n^*$  の部分半群を  $\mathcal{M}$  とおく。  $f_\Delta \in \mathcal{M}$  であるから,  $\mathcal{M} = \Sigma_n^*$  を示すためには,

$$\mathcal{G}_n \mathcal{M} \subset \mathcal{M}, \quad \mathcal{M} \mathcal{G}_n \subset \mathcal{M}$$

をいえばよい。これは次の補題から直ちに得られる。

補題5.  $\gamma_j^i \sigma_l^k = \gamma_k^l \gamma_l^i \gamma_i^j \gamma_j^k \quad (\#\{i, j, k, l\} = 4)$

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

$$\sigma \gamma_j^i \sigma^{-1} = \gamma_{\sigma(j)}^{\sigma(i)} \quad (\sigma \in \mathcal{G}_n).$$

◎注意:  $\Sigma_n$  は  $\mathcal{G}_n$  の適当な生成元2個と  $\gamma_2^1$  の3個で生成される。また  $\Sigma_n^*$  は  $\frac{1}{2}n(n-1)$  個の  $\gamma_j^i$  で生成されたと証明

これ、それ以下の個数では生成されないことも証明出来る。

#### § 4. $\{\gamma_j^i, \sigma_l^k\}$ に関する $\Sigma_n$ の基本関係式

よび次の等式 (1) ~ (15) が  $\Sigma_n$  で成り立つことは、直接計算でわかる。

$$(1) \quad \sigma_l^k = \sigma_k^l$$

$$(2) \quad \sigma_l^k \sigma_l^k = e$$

( $e$  は恒等置換)

$$(3) \quad \sigma_j^l \sigma_l^k = \sigma_j^k \sigma_l^j$$

( $\#\{k, l, j\} = 3$ )

$$(4) \quad \sigma_j^i \sigma_l^k = \sigma_l^k \sigma_j^i$$

( $\#\{k, l, i, j\} = 4$ )

$$(5) \quad \sigma_l^k \gamma_j^i \sigma_l^k = \gamma_j^i$$

( $\#\{k, l, i, j\} = 4$ )

$$(6) \quad \sigma_k^i \gamma_j^i \sigma_k^i = \gamma_j^k$$

( $\#\{k, i, j\} = 3$ )

$$(7) \quad \sigma_j^k \gamma_j^i \sigma_j^k = \gamma_k^i$$

( $\#\{k, i, j\} = 3$ )

$$(8) \quad \sigma_j^i \gamma_j^i \sigma_j^i = \gamma_i^j$$

( $\#\{i, j\} = 2$ )

$$(9) \quad \gamma_j^i \gamma_l^k = \gamma_l^k \gamma_j^i$$

( $\#\{k, l, i, j\} = 4$ )

$$(10) \quad \gamma_j^i \gamma_j^k = \gamma_j^k \gamma_j^i = \gamma_j^i \gamma_i^k$$

( $\#\{k, i, j\} = 3$ )

$$(11) \quad \gamma_j^i \gamma_k^j = \gamma_k^i \sigma_j^i$$

( $\#\{k, i, j\} = 3$ )

$$(12) \quad \gamma_j^i \gamma_k^i = \gamma_k^i$$

( $\#\{k, i, j\} = 3$ )

$$(13) \quad \gamma_j^i \gamma_j^i = \gamma_j^i$$

$$(14) \quad \gamma_i^j \gamma_j^i = \gamma_i^j$$

$$(15) \quad \gamma_j^i \sigma_j^i = \gamma_j^i$$

定理 2.  $n$  を自然数とし,  $\mathcal{G}$  を単位元  $1$  をもつ半群で,  
 元  $c_j^i, \sigma_l^k$  ( $1 \leq i, j, k, l \leq n, i \neq j, k \neq l$ ) から  
 生成され,  $c_j^i, \sigma_l^k$  は  $\gamma_j^i \leftrightarrow c_j^i, \sigma_l^k \leftrightarrow \sigma_l^k$  なる  
 対応かえり (1) ~ (15) を満たすものとする. すると,  
 $|\mathcal{G}| \leq n^n$  であり, 準同型  $\theta: \Sigma_n \rightarrow \mathcal{G}$  が存在  
 して, 各  $i, j, k, l$  に対して

$$\theta(\gamma_j^i) = c_j^i, \quad \theta(\sigma_l^k) = \sigma_l^k \quad \text{となる.}$$

証明は次のような段階に分かれる. まず,  $\{\sigma_l^k \mid 1 \leq k, l \leq n, k \neq l\}$  の生成する  $\mathcal{G}$  の部分半群  $S$  は,  $\sigma_l^k \sigma_l^k = 1$  により,  
 $\mathcal{G}$  の部分群となり,  $S$  の単位元は  $\mathcal{G}$  の単位元  $1$  と一致する.  
 $\{\sigma_l^k\}$  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

$$\pi: \mathcal{G}_n \rightarrow S$$

が存在して, 各  $k, l$  に対して  $\pi(\sigma_l^k) = \sigma_l^k$  となる.  
 いま,  $\mathcal{G}_n$  の元と  $\mathcal{G}$  の元の“積”を次のように  $\mathcal{G}$  の元として  
 定義する:

$$\sigma \cdot t = \pi(\sigma)t \quad (\sigma \in \mathcal{G}_n, t \in \mathcal{G})$$

$$t \cdot \sigma = t\pi(\sigma) \quad (\sigma \in \mathcal{G}_n, t \in \mathcal{G})$$

すると, “結合律”

$$(\sigma_1 t)\sigma_2 = \sigma_1(t\sigma_2) \quad (\sigma_1, \sigma_2 \in \mathcal{G}, t \in \mathcal{G})$$

の成立は明らかである. さて  $\mathcal{G}$  において,



補題 6  $\sigma c_j^i \sigma^{-1} = c_{\sigma(j)}^{\sigma(i)}$ . ( $\sigma \in \mathcal{G}_n$ )

証明:  $\sigma$  と  $\mathcal{G}_n$  の生成元  $\sigma_k^l$  ととって示せばよい.  
しかしそれは (5) ~ (8) である.

補題 7. (Reduction Rule in 7).  $p \geq 2$  とし,

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

$$(i) \{i_\nu, j_\nu\} \cap \{i_1, i_2, \dots, i_{\nu-1}\} = \emptyset \quad (2 \leq \nu \leq p-1)$$

$$(ii) \{i_p, j_p\} \cap \{i_1, i_2, \dots, i_{p-1}\} \neq \emptyset \quad \text{を満すならば,}$$

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

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. (i), (5) ~ (15) とこの二つを用いる.

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

定義  $J = \{j_1, \dots, j_r\}$ ,  $r = |J|$  とし,

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

この (10) により, 右辺の積は  $j_1, \dots, j_r$  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.

補題 8. (Normalization)  $f = c_{j_p}^{i_p} \cdots c_{j_1}^{i_1} \in \mathcal{F}$  か

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

を満す可ならば,  $\{i_1, \dots, i_p\}$  の空でない部分集合  $K_1, \dots, K_m$

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

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

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

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

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  $\Delta$  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.

$c_\Delta \in \mathcal{F}$  と

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

と定義する. 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

補題 9  $\mathcal{F} = \bigcup_{\Delta \in \mathcal{P}(n)} S c_\Delta S$

証明:  $f \in \mathcal{F}$  はいくつかの  $c_j^i$  といくつかの  $\sigma_{i_2}^{k_2}$  の積の形に書ける. 一方補題 6 により  $\sigma c_{i_2}^{p_2} = c_{i_2}^{p_2'} \sigma$  ( $p_2' = \sigma(p_2)$ ,  $i_2' = \sigma(i_2)$ ,  $\sigma \in \mathcal{G}_n$ ) となるから,  $\sigma_{i_2}^{k_2} \cdots \sigma_{i_1}^{k_1} c_j^i$  の形は,  $c_j^i \sigma_{i_2}^{k_2'} \cdots \sigma_{i_1}^{k_1'}$  の形に書き直せる. よって,  $f$  は

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

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

中の元  $k_1, \dots, k_m$  が存在して

$$c_{jk}^{i_k} \cdots c_{ji}^{i_1} = c_{k_1}^{K_1} \cdots c_{k_m}^{K_m},$$

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

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

となる。すると、 $n$  の分割  $\Delta$  と  $\mathfrak{S}_n$  中の置換  $f$  が存在して、

$$c_{jk}^{i_k} \cdots c_{ji}^{i_1} = f c_\Delta f^{-1}$$

となることが容易にわかる。よって、 $f = f c_\Delta f^{-1} \in \mathfrak{S}_n c_\Delta \mathfrak{S}_n = S c_\Delta S$ 。次に  $\{i_p, j_p\} \cap \{i_1, \dots, i_{p-1}\} \neq \emptyset$  なる番号  $p$ ,  $2 \leq p \leq k$  が存在する場合は考えよう。そのような  $p$  のうち最小なものを選び、これを  $p$  とすると、 $\{i_\nu, j_\nu\} \cap \{i_1, \dots, i_{\nu-1}\} = \emptyset$  ( $\nu=2, \dots, p-1$ ) となる。よって補題 7 (Reduction Rule) により、

$$c_{jk}^{i_k} \cdots c_{ji}^{i_1} = c_{jk}^{i_k} \cdots c_{j_{p+1}}^{i_{p+1}} \theta c_{j_{p-1}}^{i_{p-1}} \cdots c_{ji}^{i_1}$$

と書ける。ただし、 $\theta=1$  または  $\theta = d_{j_p}^{i_p}$  である。すると、 $f$  は長個より少ない  $c_j^{i_j}$  の積と  $S$  の元の積の形：

$$(*) \quad f = c_{m_t}^{i_t} \cdots c_{m_1}^{i_1} d', \quad d' \in S$$

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。これを

$$f = c_{j_t}^{i_t} \cdots c_{j_1}^{i_1} d'', \quad d'' \in S$$

とすれば、 $\{i_\nu, j_\nu\} \cap \{i_1, \dots, i_{\nu-1}\} = \emptyset$  が  $\nu=2, \dots, t$  に対しても成り立つ。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  $\Delta \in \mathcal{Y}_p(n)$  に對して、

補題 10.  $\Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  に対し, §2 と同様に  $\Lambda(\Delta), J_{ip}, a_{ip}, J_i (i \in \Lambda(\Delta))$  と考へる.  $f(J_i) = J_i$  (各  $i \in \Lambda(\Delta)$  に対し) を満たすような  $f \in \mathfrak{S}_n$  のなす  $\mathfrak{S}_n$  の部分群を  $L_\Delta$  とする. すると  $L_\Delta$  の各元  $f$  に対し  $f c_\Delta \sigma = c_\Delta$  を満たす  $\sigma \in \mathfrak{S}_n$  が存在する.

証明:  $L_\Delta$  の生成系中の  $f$  について,  $\sigma$  の存在を証明すればよい. ( $f_1 c_\Delta \sigma_1 = c_\Delta, f_2 c_\Delta \sigma_2 = c_\Delta$  から  $f_2 f_1 c_\Delta \sigma_1 \sigma_2 = c_\Delta$  が導かれるからである) よって  $f$  が  $J_i$  中の 2 元  $a_{ip}$  と  $a_{iq}$  の互換である場合とすれば十分である.  $J_{ip} = \{x_1, \dots, x_i\}$   $x_1 = a_{ip}$ ,  $J_{iq} = \{y_1, \dots, y_i\}$ ,  $y_1 = a_{iq}$  とする. このとき  $\sigma = \sigma_{y_1}^{x_1} \sigma_{y_2}^{x_2} \dots \sigma_{y_i}^{x_i}$  とおくと  $f c_\Delta \sigma = c_\Delta$  が成り立つことが基本関係を用いて示せる.

補題 11.  $\mathcal{N}_p(n) \ni \Delta = (\alpha_0, \alpha_1, \dots, \alpha_n)$  に対し

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

証明: 補題 10 の部分群  $L_\Delta$  の各元  $f$  に対し,

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

とおく.  $R_{\Delta, f} \neq \emptyset$  である.  $R_{\Delta, f}$  の元  $\sigma_1$  を一つ固定すると,  $\sigma \in \mathfrak{S}_n$  に対し

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

であるから

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

とおくと,  $Q_\Delta$  は  $\mathfrak{S}_n$  の部分群で,  $R_{\Delta, \rho} = Q_\Delta \sigma$  となる.

(したがって,  $|R_{\Delta, \rho}| = |Q_\Delta|$ . 次に

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

を示そう.  $A^*(\Delta) = \{ i \in A(\Delta) \mid i \geq 2 \}$  とおき,  $\mathfrak{S}_n$  の部分群

$$R_\Delta = \{ \theta \in \mathfrak{S}_n \mid \theta(J_{i,p}) = J_{i,p} \ (i \in A^*(\Delta), 1 \leq p \leq \alpha_i) \}$$

を考える.  $|R_\Delta| = (1!)^{\alpha_1} (2!)^{\alpha_2} \cdots (n!)^{\alpha_n}$  であるから,

$Q_\Delta \supset R_\Delta$  と言えはよい. これには  $R_\Delta$  の生成元である  $J_{i,p}$  中の 2 元の互換  $\theta$  が  $Q_\Delta$  に属すること, すなわち,  $c_\Delta \theta = c_\Delta$  と言えはよい. 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

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

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

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

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

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  $|\tilde{\Sigma}| \leq n^n$ .  
 次に単位元 1 を有し, 元  $\tilde{c}_j^i, \tilde{\sigma}_\ell^k$  から生成され,  $\tilde{\gamma}_j^i$  と  
 $\tilde{c}_j^i, \tilde{\sigma}_\ell^k$  と  $\tilde{\delta}_\ell^k$  と考えらるべき (1) ~ (15) を基本関係にも  
 つ universal な半群  $\tilde{\Sigma}$  とする. すると準同型  $\varphi$ :  
 $\tilde{\Sigma} \rightarrow \Sigma_n$  が存在して,  $\varphi(1) = 1, \varphi(\tilde{c}_j^i) = \gamma_j^i,$   
 $\varphi(\tilde{\delta}_\ell^k) = \sigma_\ell^k$  ( $1 \leq i, j, k, \ell \leq n$ ) となる. よって  $\varphi(\tilde{\Sigma})$   
 $= \Sigma_n$  であるが, 上に証明した定理 2 の前半により,  $|\tilde{\Sigma}|$   
 $\leq n^n = |\Sigma_n|$  となる. (したがって  $\varphi$  は 1:1 となり,  
 $\tilde{\Sigma} \cong \Sigma_n$  である. 故に定理 2 の後半が証明された.

#### § 4. $\Sigma_n$ の元の $\mathcal{G}_n$ - $\gamma$ -length.

定義  $\Sigma_n$  の元  $f$  は

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

の形で表わされる. このよりの表示全体の中で  $k$  の値の最  
 小値を  $f$  の  $\mathcal{G}_n$ - $\gamma$ -length と呼び, これを  $l^*(f)$  と書く.

定理 3.  $f \in \Sigma_n$  に対して,

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

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

さて、 $l$  に対する帰納法により、こゝで

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

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.

系  $f, g \in \Sigma_n$ ,  $f = \gamma_j^i g$  のとき,

$$l^*(f) = \begin{cases} l^*(g) + 1, & (\{i, j\} \subset g(\Omega) \text{ の時}) \\ l^*(g), & (\{i, j\} \notin g(\Omega) \text{ の時}) \end{cases}$$

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  $\Sigma_n$  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. $\Sigma_n^*$ の元の $\gamma$ -length

定義  $\Sigma_n^*$  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  $l$  の値の最小値を  $f$  の  $\gamma$ -length と呼び、これを  $l(f)$  と書く。

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

$\mathcal{D}(f)$  の頂点  $\cdots \Omega = \{1, 2, \dots, n\}$  の元。

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

有向線分がある  $\iff f(i) = j$ .

(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



が  $\mathcal{D}(f)$  である.

さて,  $f \in \Sigma_n^*$  に対して  $\mathcal{D}(f)$  中の loop となつてい  
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  $\Omega$  の部分集合  $C$  であつて,

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  $\mathcal{S}_C$  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  $\{5, 6\}$  は純回路ではない.



定義.  $f \in \Sigma_n^*$  に対して,  $\mathcal{D}(f)$  中の純回路全体のなる集合を

$\mathcal{P}_f$  と表わす.

定理 4.  $f \in \Sigma_n^*$  に対して,

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

証明: いくつかの  $\gamma_j^i$  のなる長さ  $s$  の系列  $c = (\gamma_{j_1}^{i_1}, \dots, \gamma_{j_s}^{i_s})$  ( $\gamma_j^i$  の中には等しいものがあるもよい) 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. これは  $\Omega$  の元よりなる長さ  $s+1$  の系列

$$x_0, x_1, \dots, x_s$$

であって,

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

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

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

で定義する.  $\gamma_j^i$  の定義により,  $v \in J$  に対して,

$$v \in H_x(c) \iff x_{v-1} = i_v, x_v = j_v$$

となることに注意しておく.

補題 12.  $f \in \Sigma_n^*$ ,  $c = (\gamma_{j_1}^{i_1}, \dots, \gamma_{j_s}^{i_s})$

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

とする. また  $x, y$  は  $\Omega$  の元で  $x \neq y$  とする. もし  $x \in \text{合}$

よいうな純回路  $C$  が  $\mathcal{D}(f)$  中に存在すれば

$$H_x(C) \cap H_y(C) = \emptyset.$$

証明: 省略. 定義に戻って考えれば容易.

補題 13.  $f, c$  は補題 12 と同様とする.

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

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

証明: 省略. これは定義から容易に出来る.

補題 14.  $f, c$  は補題 12 と同様とする.

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

したがって, とくに

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

証明:  $J = \{1, 2, \dots, s\}$  とし,  $H = \bigcup_{x \in \Omega} H_x(c)$  とおく.

$\mathcal{D}(f)$  中のすべての純回路を並べ,  $\mathcal{P}_f = \{C_1, \dots, C_k\}$ ,

$k = |\mathcal{P}_f|$  とする.  $C_f = C_1 \cup \dots \cup C_k$ ,  $M_f = \Omega -$

$(C_f \cup F_f)$  とおく. 純回路の定義より,  $C_\mu \cap C_\nu = \emptyset$  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:  $H = H_1 \cup H_2$ ,  $H_1 \cap H_2 = \emptyset$ . 更に補

題 12, 13 12より

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

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

$$\begin{aligned} \delta \geq |H| &= |H_1| + |H_2| \\ &\geq k + \sum_{i=1}^k |C_i| + |M_f| \\ &= n + k - |F_f| = n + |P_f| - |F_f|. \end{aligned}$$

補題 15  $f \in \Sigma_n^*$  に対し,

$$N(f) = n + |P_f| - |F_f|$$

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

$$l(f) \leq N(f).$$

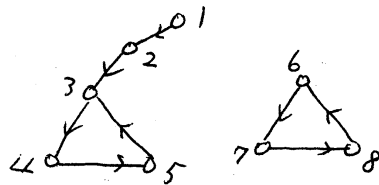
証明:  $n$  に関する帰納法による. ( $n=2$  のときは明らか).

しかし長くなるので省略する.

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

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

$D(f)$  :



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

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

expression がある。

①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  $f = \gamma_{jk}^{i_k} \cdots \gamma_{ji}^{i_1}$  に対して, "必ず"  $j_k = i_{k-1}, j_{k-1} = i_{k-2}, \dots, j_2 = i_1$  となることが証明出来るか? この証明は長くなるが有用である。

### 参考文献

- [1] Clifford - Preston : The Algebraic Theory of Semi-group. vol. I. A.M.S.
- [2] Steinberg : Appendix of Finite Reflection Group of "Lectures on Chevalley Groups" Yale Univ.