

biprefix code の 1 つの族について

東海大学短期大学部 中畑 登 (Noboru Nakahata)

この論文では biprefix code の 1 つの族を構成する。ただしこの族はかなり大きなもので、その一般的な構造は複雑である。そこでこの族の部分族として興味あると思われるものを中心に考察する。特に、この部分族に属する code の syntactic monoid を完全に決定する。

1 基本的な用語と命題

$A$  を  $n$  個の元からなる有限集合とし、これを alphabet と呼ぶ。  $A$  の各元を文字と呼び、文字の有限列を語という。文字を含む語というものを考え、これを空語として記号  $1$  で示す。語の全体を  $A^*$  で示す。  $u$  と  $v$  を任意の語とし、  $u = a_1 \cdots a_p$ ,  $v = b_1 \cdots b_q$  ( $a_i, b_j \in A$ ) とすると  $u$  と  $v$  の積を、  $uv = a_1 \cdots a_p b_1 \cdots b_q$  で定める。空語  $1$  をこの演算の単位元と考えて  $A^*$  は monoid の構造を持つ。この monoid を  $A$  上の free monoid と

いう。  $w = u \cdot v$  ( $u, v \in A^*$ ) と置くと、  $u$  と ( $v \in$ )  $w$  の左(右)因子という。  $A^*$  の任意の部分集合を言語という。 2つの言語  $L, L'$  に対してその積を  $L \cdot L' = \{l \cdot l' \mid l \in L, l' \in L'\}$  と定める。 もし  $L = L'$  のときは、  $L \cdot L = L^2$  等と中の形で表す。  $A^+ = A^* \setminus \{\epsilon\}$  とおく。

定義 1.1.  $M \subseteq A^*$  上の言語で  $\epsilon$  を含むとする。 もし  $M = M^2$  が成り立つとき、  $M \subseteq A^*$  の submonoid という。

定義 1.2.  $L \subseteq A^*$  上の言語とする。 空語  $\epsilon$  及び  $L$  の元の有限個の積全体を  $L^*$  で示す。  $L^*$  は明らかに  $A^*$  の submonoid である。 これを  $L$  から生成された submonoid という。

定義 1.3.  $M \subseteq A^*$  の submonoid とする。 集合  $(M \setminus \{\epsilon\}) \setminus (M \setminus \{\epsilon\})^2 \subseteq M$  の base という。 これを今  $C$  で表すとき、  $M = C^*$  が成り立つ。 もし  $M$  が、  $M = D^*$  と表されていれば、  $C \cap D$  に含まれていることが定義よりわかる。 そこで  $C \subseteq M$  の minimal generator という。

定義 1.4.  $C \subseteq A^*$  上の言語とする。  $C$  の任意の元  $x_1, \dots, x_p, y_1, \dots, y_q$  に対して、 もし  $x_1 \dots x_p = y_1 \dots y_q \Rightarrow p = q, x_i = y_i$  ( $i = 1, \dots, p$ ) が成立するとき、  $C \subseteq A^*$  上の code という。

定義 1.5.  $A^*$  の submonoid  $M$  が unitary とは、任意の語  $w$  に対して  
 $Mw \cap wM \cap M \neq \emptyset \Rightarrow w \in M$  が成立するときをいう。

命題 1.1.  $A^*$  の submonoid が unitary  $\Leftrightarrow M$  の base が code

定義 1.6.  $P \subseteq A$  上の言語とし、 $1 \notin P$  とする。もし、 $P \cap PA^+ = \emptyset$  ( $P \cap A^+P = \emptyset$ ) なら、 $P \subseteq A$  上の prefix code (suffix code) と  
いう。prefix code (suffix code) は定義 1.4 の意味で実際に code  
に存在する。

定義 1.7.  $A^*$  の submonoid  $M$  が右 unitary (左 unitary) とは、任意の  
 $w \in A^*$  に対して、 $Mw \cap M \neq \emptyset$  ( $wM \cap M \neq \emptyset$ )  $\Rightarrow w \in M$  を満たす  
ときをいう。もし  $M$  が右及び左 unitary のとき、 $M$  は biunitary と  
呼ぶ。

命題 1.2.  $A^*$  の submonoid  $M$  が右 unitary (左 unitary)  
 $\Leftrightarrow M$  の base が prefix code (suffix code)

biprefix code の例として次のものがある:

$\eta$  を  $A^*$  から群  $G$  の上への写像とする。又  $H \subseteq G$  の任意の部分  
群とする。このとき  $\eta^{-1}(H)$  は  $A^*$  の biunitary な submonoid に存在す

とが確かめられる。従ってその base は  $A$  上の biprefix code になる。これを我々は group code と呼ぶ。

## 2. biprefix code の構成

この節の目的は biprefix code の 1 つの族を構成することである。  $A = \{a_1, a_2, \dots, a_n\}$ ,  $n \geq 2$  とする。  $G$  は任意の群とし、  $g_0$  は  $G$  の 1 つの固定された元とする。又  $\Sigma = [\sigma_{ij}]$  は  $n \times n$  行列とし、各成分  $\sigma_{ij}$  は  $G$  から  $G$  への 1 対 1 の準同型写像とする。  $\Sigma$  を指示行列と呼ぶ。  $\sigma_{ij}$  の  $G$  の元  $g$  への作用は  $g\sigma_{ij}$  と書くことにする。さて、  $A^*$  の元  $w$  の各文字に  $G$  の元を次の方法で付けていく：

(1)  $g_0$  は各文字  $a_i$  に付ける。

(2)  $w = a_i \cdot a_j \cdots a_k \cdot a_l \cdots a_m$  とする。このとき  $g_0$  は  $w$  の最初の文字  $a_i$  に付ける。そして  $g_0\sigma_{ij}$  は  $a_j$  に付ける。もし  $g_0\sigma_{ij}$  が  $a_k$  に付いていたら、  $a_l$  には  $g_0\sigma_{kl}\sigma$  が付けられる。この様にして  $w$  のすべての文字に  $G$  の元が付けられる。

(3)  $G$  の単位元  $1$  は  $A^*$  の空語  $1$  に付く。

さて、  $A^*$  の各元  $w$ 、各  $i=1, \dots, n$  に対して  $\gamma_i(w) \in G$ 、  $w$  の中の文字  $a_i$  に付いてゐる  $G$  の元の積とする。もし  $a_i$  が  $w$  の中に現れなるときは  $\gamma_i(w) = 1$  とする。特に  $\gamma_i(1) = 1$  である。以上で  $A^*$

の各元  $w$  に対して 1 つの元  $(\gamma_1(w), \dots, \gamma_n(w)) \in \overbrace{G \times \dots \times G}^n = G^n$  が対応する。この写像を  $\gamma$  で表す。このとき次の命題が成り立つ。

命題 2.1. 任意の  $u, v \in A^*$  に対して、

$$\gamma(u \cdot v) = \gamma(u)(\gamma(v)\sigma)$$

が成り立つ。ここで  $\sigma$  は  $u$  と  $v$  に関係する  $G$  から  $G$  への 1 対 1 の準同型写像であり、 $\gamma(v)\sigma = (\gamma_1(v)\sigma, \dots, \gamma_n(v)\sigma)$  と定める。

よって  $M = \{w \in A^* \mid \gamma(w) = (1, \dots, 1)\}$  とおくと、次が導かれる。

命題 2.2.  $M$  は  $A^*$  の biunitary な submonoid である。

上で定義した  $M$  は、 $G^n$  の自明な部分群  $(1, \dots, 1)$  の  $\gamma$  による逆像であるが、もう少し一般化して次の性質を持つ部分群を考える： 任意の  $\sigma_{ij} \in \Sigma$  に対して、

$$(i). H\sigma_{ij} \subset H$$

$$(ii). g\sigma_{ij} \in H \Rightarrow g \in H$$

我々はこのような  $H$  を  $\Sigma$ -不変な部分群と呼ぶ。このとき  $M = \{w \in A^* \mid \gamma(w) \in H\}$  とおけば、やはり  $M$  は  $A^*$  の biunitary な submonoid になることがわかる。従ってその base は biprefix code になる。  $M$  の base を  $\Gamma(H)$ 、  $M$  自身を  $\Gamma^*(H)$  で表すことにする。任

意に与えられた  $\Sigma$ ,  $H$  に対して  $\Gamma^*(H)$  又は  $\Gamma(H)$  を考察すること  
 は非常に正すか1の様に見える。そこで次の特別な場合を  
 選ぶことにする:

(1).  $G$  とし  $\mathbb{Z}$  整数の加法群,  $g_0$  とし  $1$  を考える。

(2).  $\varepsilon \in \mathbb{Z}$  の自明な自己同型写像,  $\varepsilon'$  と自明でない唯一の  
 自己同型写像, 即ち  $k \cdot \varepsilon' = -k$ ,  $k \in \mathbb{Z}$ . 指示行列  $\Sigma = [\sigma_{ij}]$  とし

$$(i). \quad \sigma_{ii} = \varepsilon, \quad i=1, \dots, n$$

(iii).  $i \neq j$  に対して,  $\sigma_{ij} = \varepsilon$  又は  $\varepsilon'$  であり, もし  $\sigma_{ij} = \varepsilon$  なら  
 $\sigma_{ji} = \varepsilon'$  とする様に定める.  $\Pi = \{(i, j) \mid \sigma_{ij} = \varepsilon\}$  とおく。

(3).  $H$  とし  $\mathbb{Z}^n$  の任意の部分群を考える。明らかに  $H$  は  
 $\Sigma$ -不変である。

注意.  $\mathbb{Z}^n$  は abel 群だから, 加法の記号を採用する。  $\mathbb{Z}^n$  の零元  
 は単に  $0$  で示す。又  $\varepsilon, \varepsilon'$  をそれぞれ  $1, -1$  で表すことにす  
 る。

例 2.1.  $A = \{a, b\}$ ,  $\tau \in \mathbb{Z}^2$   $a = a_1, b = a_2$ , 指示行列  $\Sigma$  を

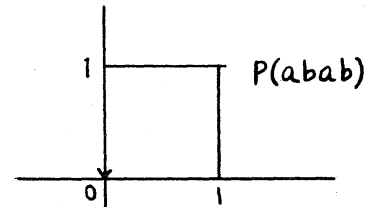
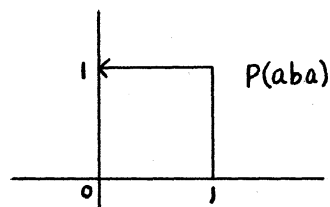
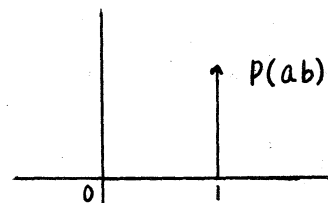
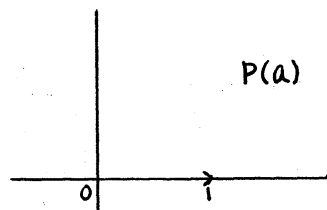
$$\Sigma = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \text{とし, } \Sigma\text{-不変な部分群を } H = \{0\} \text{ とする。}$$

$w$  の各文字に付けられる  $1$  又は  $-1$  を, その文字の下に書くこ

とにする。いくつかの語  $w$  に対して  $\gamma(w)$  を計算すると次の様になる。

1.  $w=a$  のとき  $w=\underset{1}{a}$  となり、 $\gamma(a)=(1,0)$
2.  $w=ab$  のとき  $w=\underset{1}{a}\underset{1}{b}$  となり、 $\gamma(ab)=(1,1)$
3.  $w=aba$  のとき  $w=\underset{1}{a}\underset{1}{b}\underset{-1}{a}$  となり、 $\gamma(aba)=(0,1)$
4.  $w=abab$  のとき  $w=\underset{1}{a}\underset{1}{b}\underset{-1}{a}\underset{-1}{b}$  となり、 $\gamma(abab)=(0,0)$

$A^*$  の各元  $w$  に対して、1つの道  $p(w)$  を  $n$ 次元の空間に対応させることができる。それは原点から出発して途中、点  $\gamma(u)$  を通り、終点  $\gamma(w)$  に終る道である。ただし  $u$  は  $w$  の各左因子である。  $n=2$  のとき、上の4つの語の道を次に示す:



語  $w$  が  $\Gamma^*(\{0\})$  に属することは、道  $p(w)$  が原点で終ることである。さて、仮定(1)(2)(3)のもとで  $\Gamma^*(H)$  の構造について考えて

いく。

定義 2.1.  $A$  上の言語  $L$  に対して、 $wA^* \cap L \neq \emptyset$  ( $A^*w \cap L \neq \emptyset$ ) が任意の  $w \in A^*$  に対して成り立つとき  $L$  を右 dense (左 dense) という。

命題 2.3.  $\Gamma^*(H)$  は右及び左 dense である。

証明  $\Gamma^*(H) \supset \Gamma^*(\{0\})$  より、 $\Gamma^*(\{0\})$  によって示せばよい。

$w = a_i \cdots a_j$  とする。又  $\Gamma^*(\{0\}) = \Gamma^*$  とおく。

Case 1:  $(i, j) \in \Pi, i \neq j$

まず  $w = a_i \cdots a_j$  より  $w \cdot w = a_i \cdots a_j a_i \cdots a_j$  より  $\gamma(w \cdot w) = \gamma(w) - \gamma(w) = 0$  とする。又  $w^2 \in wA^* \cap \Gamma^*, w^2 \in A^*w \cap \Gamma^*$ 。また  $w = a_i \cdots a_j$  より、 $u = w a_i a_j = a_i \cdots a_j a_i a_j$  及  $v = a_i a_j w = a_i a_j a_i \cdots a_j$  とする。従って  $\gamma(u^2) = 0$  及  $v^2 \in \Gamma^*$  とする。

Case 2:  $(j, i) \in \Pi, i \neq j$

このときも Case 1 と同様に考え、 $wA^* \cap \Gamma^* \neq \emptyset, A^*w \cap \Gamma^* \neq \emptyset$  と得る。

Case 3:  $i = j$

このときは  $k \neq i$  なる  $k$  を取り、語  $w a_k, a_k w$  は Case 1 又は Case 2 に適用すればよい。



定義 2.2.  $L \in A$  上の言語とする。  $L$  による  $A^*$  の syntactic congruence  $\equiv$  は次の様に定める:  $u, v \in A^*$  に対して、

$$u \equiv v \iff [\text{任意の } p, q \in A^* \text{ に対して, } puq \in L \iff pvq \in L]$$

定義より  $\equiv$  は  $A^*$  の同値関係となり、さらに  $A^*$  の congruence となる。つまり  $u \equiv u', v \equiv v' \Rightarrow u \cdot u' \equiv v \cdot v'$  が成り立つ。以後  $\Gamma^*(H)$  による  $A^*$  の syntactic congruence について考える。このとき次の 2 つの場合が生じる:

(A).  $\mathbb{Z}^n/H$  の任意の元  $t$  に対して、 $t = -t$  が成立する場合、つまり  $\mathbb{Z}^n/H$  が位数が 2 のベキの基本 abel 群のとき。

(B). そうでないとき、つまり  $t \neq -t$  となる  $t \in \mathbb{Z}^n/H$  があるとき。

最初に (B) をあつかう。  $\bar{\gamma}(w) \in \gamma(w)$  の  $H$  立法とした剰余類とする。仮定 (B) のもとで、 $\equiv$  は次の様に特徴づけられる。

定理 2.4.  $w = a_i u a_j$ 、 $w' = a_k u' a_s$  とする。このとき

$$w \equiv w' \iff \begin{cases} \text{(i)} & \bar{\gamma}(w) = \bar{\gamma}(w') \\ \text{(ii)} & a_i = a_k \\ \text{(iii)} & a_j = a_s \\ \text{(iv)} & \gamma = s \end{cases}$$

証明. (i), (ii), (iii), (iv) が成立すると仮定する.  $p, g \in A^*$  に対して  $pwg \in \Gamma^*(H)$  のとき,  $pw'g \in \Gamma^*(H)$  を示す. 従って

$$\bar{0} = \bar{\gamma}(pwg) = \bar{\gamma}(pa_i u a_j g) = \bar{\gamma}(p) + x \{ \bar{\gamma}(a_i u a_j) + y \bar{\gamma}(g) \} \quad (1)$$

ここで,  $x$  は  $1$  または  $-1$  で  $p$  と  $a_i$ , あるいは  $p$  の最後の文字と  $a_i$  に付けられた値にだけ関係する. 又  $y$  についても  $g$  と  $a_j$ , あるいは  $g$  の最初の文字と  $a_j$  に付けられた値にだけ関係する. (i) - (iii) より (1) 式は,

$$\bar{0} = \bar{\gamma}(p) + x \{ \bar{\gamma}(a_i u' a_j) + y \bar{\gamma}(g) \} \quad (2)$$

となる. さらば (iv) より (2) の右辺は, まさに  $\bar{\gamma}(pw'g)$  である. 従って  $pw'g \in \Gamma^*(H)$  となる.

逆に  $w \equiv w'$  とする. (i) を示すため, 最初から  $a_i = a_k$  と仮定してよい. 存在する, もし  $a_i \neq a_k$  で仮りに  $(i, k) \in \Pi$  であらば,  $T_i$  とする. 従って  $\bar{\gamma}(a_i w) = \bar{\gamma}(a_i) + \bar{\gamma}(w)$ ,  $\bar{\gamma}(a_i w') = \bar{\gamma}(a_i) + \bar{\gamma}(w')$  となる. 又  $w \equiv w'$  より  $a_i w \equiv a_i w'$  である. 今ここで, もし  $\bar{\gamma}(a_i w) = \bar{\gamma}(a_i w')$  ならば,  $\bar{\gamma}(w) = \bar{\gamma}(w')$  がわかる. 同じ理由で  $a_j = a_l$  とする.

Case 1:  $(i, j) \in \Pi, i \neq j$

$$(a) \quad w = a_i u a_j \quad \text{又は} \quad w' = a_i u' a_j \quad (\text{前者を仮定する})$$

$$\text{このとき} \quad \bar{\gamma}(ww) = \bar{\gamma}(w) - \bar{\gamma}(w) = \bar{0} \quad \text{となるから} \quad w \cdot w \in \Gamma^*(H).$$

$$w \equiv w' \text{ より } ww' \in \Gamma^*(H) \text{ となる. 従って } \bar{0} = \bar{\gamma}(ww') = \bar{\gamma}(w) - \bar{\gamma}(w')$$

$$\text{より } \bar{\gamma}(w) = \bar{\gamma}(w') \text{ を得る.}$$

$$(b) \quad w = a_i u a_j \quad \text{及} \quad w' = a_i u' a_j$$

このとき、 $w a_i a_j = a_i u_{-i} a_j a_i a_j \equiv w' a_i a_j = a_i u'_{-i} a_j a_i a_j$  である。

従って (a) より  $\bar{\gamma}(w a_i a_j) = \bar{\gamma}(w' a_i a_j)$  となり、又  $\bar{\gamma}(w a_i a_j) = \bar{\gamma}(w) + \bar{\gamma}(a_i a_j)$  及  $u$   $\bar{\gamma}(w' a_i a_j) = \bar{\gamma}(w') + \bar{\gamma}(a_i a_j)$  より  $\bar{\gamma}(w) = \bar{\gamma}(w')$  と得る。

Case 2:  $(j, i) \in \Pi, i \neq j$

(a)  $w = a_i u_{-i} a_j$  又は  $w' = a_i u'_{-i} a_j$

このとき Case 1 (a) と同様に求める結果を得る。この場合  $i = j$  でも正しい。

(b)  $w = a_i u_{-i} a_j$  及  $u$   $w' = a_i u'_{-i} a_j$

このとき  $w a_i a_j \equiv w' a_i a_j$  となり (a) を使って主張を得る。

Case 3:  $i = j$

(a)  $w = a_i u_{-i} a_j$  又は  $w' = a_i u'_{-i} a_j$

このとき  $w, w'$  は Case 2 (a) を使って  $\bar{\gamma}(w) = \bar{\gamma}(w')$  と得る。

(b)  $w = a_i u_{-i} a_j$  及  $u$   $w' = a_i u'_{-i} a_j$

このとき、 $k \neq i$  なる番号を取り、語  $w a_k, w' a_k$  に Case 1 又は Case 2 を適用して  $\bar{\gamma}(w) = \bar{\gamma}(w')$  と得る。

以上で (ii) が示された。次に (iii) を示す。 $a_i \neq a_k$  と仮定して矛盾を出す。さて任意の  $z \in A^+$  に対して  $\bar{\gamma}(z)$  は  $\pm \bar{\gamma}(a_p)$ ,  $p=1, \dots, n$  の適当な和として書かれる。我々は今 (B) を仮定し、さらに  $\bar{\gamma}$  は上への写像となることもわかるから、少なくとも1つの  $a_m$  に対して  $2\bar{\gamma}(a_m) \neq \bar{0}$  が成り立つ。 $i \neq k$  より  $(i, k) \in \Pi$  としてよい。 $w = a_i u_{-i} a_j, w' = a_k u'_{-k} a_r$  である。さらに  $2\bar{\gamma}(a_i u_{-i} a_j) \neq \bar{0}$  とし

てよい。もしそうではないならば  $w a_m$  を考えればよい。さて  $(i, k) \in \Pi$  で  $i \neq k$  と仮定し、 $a_k a_i u a_j \equiv a_k a_k u' a_l$  である。従って、 $\bar{\gamma}(a_k a_i u a_j) = \bar{\gamma}(a_k) - \bar{\gamma}(a_i u a_j) = \bar{\gamma}(a_k a_k u' a_l) = \bar{\gamma}(a_k) + \bar{\gamma}(a_k u' a_l)$ 。  $\bar{\gamma}(a_i u a_j) = \bar{\gamma}(a_k u' a_l)$  より  $2\bar{\gamma}(a_i u a_j) = 0$  を得て矛盾となる。

以上で (iii) が示された。次に (iii) を示す。今までのことから、

$$w = a_i u a_j, w' = a_i u' a_l, w \equiv w', \bar{\gamma}(w) = \bar{\gamma}(w') \text{ となる。}$$

前と同様に  $2\bar{\gamma}(a_i u a_j) \neq 0$  とする。もしそうではないときは、

$$a_m w \text{ を考えればよい。さて } j \neq l \text{ と仮定し、} (j, l) \in \Pi \text{ とする。}$$

$$\text{Case 1: } a_i u a_j \equiv a_i u' a_l$$

$$\text{このとき } a_i u a_j a_j \equiv a_i u' a_l a_j \text{ となる。ある } z \in A^* \text{ とし、}$$

$$a_i u a_j a_j z \in \Gamma^*(H), a_i u' a_l a_j z \in \Gamma^*(H) \text{ とできる。これから}$$

$$\bar{0} = \bar{\gamma}(a_i u a_j) + \bar{\gamma}(a_j z), \bar{0} = \bar{\gamma}(a_i u' a_l) - \bar{\gamma}(a_j z) \text{ を得る。}$$

$$\bar{\gamma}(a_i u a_j) = \bar{\gamma}(a_i u' a_l) \text{ より } 2\bar{\gamma}(a_i u a_j) = \bar{0} \text{ となる、これは矛盾。}$$

$$\text{Case 2: } a_i u a_j \equiv a_i u' a_l$$

$$\text{このとき、} a_i u a_j a_j \equiv a_i u' a_l a_j \text{ となるから上と同様に考}$$

えて矛盾を得る。

$$\text{Case 3: } a_i u a_j \equiv a_i u' a_l \text{ 又は } a_i u a_j \equiv a_i u' a_l$$

前者のときは、 $a_i u a_j a_l \equiv a_i u' a_l a_l$  となり、今までの方法で矛盾を得る。後者は同様。

従って (iii) が示された。最後に (iv) を示す。もし主張が  $zw \equiv zw'$

にっつて正しければ、 $w$ と $w'$ にっつても正しい。そこで再び  
 $2\bar{\gamma}(a_i u a_j) \neq \bar{0}$ と仮定する。 $a_i u a_j \equiv a_i u' a_j$ より $a_i u a_j a_j \equiv$   
 $a_i u' a_j a_j$ である。従って、もし $\gamma \neq s$ なら今までの方法から  
 $2\bar{\gamma}(a_i u a_j) = \bar{0}$ となってしまう。

以上で定理が示された。

注意  $w \equiv 1$ なら $w = 1$ である。なぜなら、もし $w = a_i z$ ,  $z \in A^*$ なら $a_i z a_j \equiv a_j$  ( $j \neq i$ )となり定理の(ii)に反する。

仮定(A)のもとで次を得る。

定理2.5. 任意の $w, w' \in A^*$ に対して、

$$w \equiv w' \iff \bar{\gamma}(w) = \bar{\gamma}(w')$$

証明. 仮定(A)のもとでは、任意の $u \in A^*$ に対して $\bar{\gamma}(u) = -\bar{\gamma}(u)$   
 である。つまり $\bar{\gamma}$ は $A^*$ から $\mathbb{Z}^n/H$ の上への準同型写像である。  
 このことから求める主張が導かれる。

### 3. $\Gamma^*(H)$ の syntactic monoid の構造

この節では $\Gamma^*(H)$ の syntactic monoid にっつて考える。次の定  
 理は定理2.5の結果である。

定理3.1.  $M = \text{Syn}(\Gamma^*(H))$ と置く。仮定(A)のもとで、 $M \cong \mathbb{Z}^n/H$ 。

次に仮定(B)のもとで考えよう。次の概念が半群論から必要になる。

定義3.1.  $M$  を任意の monoid とする。次の3つの  $M$  上の同値関係をそれぞれ、 $\mathcal{R}$ 、 $\mathcal{L}$ 、 $\mathcal{H}$  で表わす:

$$m \mathcal{R} n \iff mM = nM$$

$$m \mathcal{L} n \iff Mm = Mn$$

$$m \mathcal{H} n \iff mM = nM \text{ 及び } Mm = Mn$$

これらの関係は半群論において基本的な役割をする。

定理3.2.  $\eta$  を  $A^*$  から  $M = \text{Syn}(\Gamma^*(H))$  への自然な写像とする。

即ち、 $w \in A^*$  に対して  $\eta(w)$  は  $w$  を含む類である。このとき、

$$\eta(w) \mathcal{R} \eta(w') \iff w \text{ と } w' \text{ が同じ文字から始まる。}$$

証明は定理2.4を用いて示されるが、省略する。又関係についても次が成り立つ:

定理3.3.  $\eta(w) \mathcal{L} \eta(w') \iff w \text{ と } w' \text{ が同じ文字で終る。}$

上の2つの定理より次がわかる:

定理 3.4.  $\eta(w) \sim \eta(w') \iff w$  と  $w'$  が同じ文字で始まり同じ文字で終る。

次に、 $M$  の各  $\mathcal{R}$ -class ( $\mathcal{R}$ -equivalent 分類) の構造を決定する。 $A_0 = \{1\}$ ,  $A_i = \{a_i\} \cup \{a_i w a_i \mid w \in A^*\}$ ,  $A_{ij} = \{a_i u a_j \mid u \in A^*\}$  とおく。 $\exists i, j = 1, \dots, n, i \neq j$ 。さらに  $\eta(A_0) = H_0$ ,  $\eta(A_i) = H_i$ ,  $\eta(A_{ij}) = H_{ij}$  とおく。定理 3.4 より、 $H_0, H_i, H_{ij}$  は  $M$  の  $\mathcal{R}$ -class を作ることはわかる。又、各  $\mathcal{R}$ -class は乗法で閉じていることがわかる。従って半群論の一般論から、それらは群となる。

定義 3.2.  $S$  を任意の半群とする。 $S$  の部分集合  $J \neq \emptyset$  が、 $S \cdot J \cdot S \subset J$  を満足するとき、 $J$  は  $S$  の ideal という。 $S$  自身は  $S$  の 1 つの ideal である。もし、 $S$  が  $S$  以外に ideal を持たないとき、 $S$  は単純と呼ばれる。

さて、 $S = \text{Syn}(\Gamma^*(H)) \setminus \{1\}$  とおく。このとき  $S$  が単純になることが確かめられる。又一般論より、 $S$  の各  $\mathcal{R}$ -class は互いに同型な群になることがわかる。そこで 1 つの  $\mathcal{R}$ -class、例えば  $H_1$  について考えればよい。

定理 3.5.  $F$  は  $\mathbb{Z}^n/H$  と同型な群、 $\varphi$  は  $F$  の自己同型写像で、 $x \in F$

に対して、 $xg = x^{-1}$  なるものとする。このとき、 $F$  の  $\langle g \rangle$  による半直積が  $H_1$  と同型になる： $H_1 \cong \langle g \rangle * F$ .

補題 任意の  $w \in A^+$  に対して  $\bar{\gamma}(w) = \bar{\gamma}(w')$  又  $1 \neq \bar{\gamma}(w')$  及  $u''$   
 $w' = a_1 \cdots a_l$  とする  $w' \in A^*$  がある。

証明  $w = a_k \cdots a_l$  とおく。又  $u = a_1 a_k a_1 a_k w a_l a_1 a_l a_1$  とおく。ここで、もし  $k=1$  ( $l=1$ ) なら  $u$  の最初の(最後の)4つの文字は現われないのである。このとき  $\bar{\gamma}(w) = \pm \bar{\gamma}(u)$  がわかる。もし  $u$  の最後の文字に値1が付いていなければ  $u$  が求める語である。そうでないときは文字  $a_j, j \neq 1$  を取り、語  $w' = a_1 a_j a_1 a_j a_j a_1 a_j a_1 u$  を考えると、この語  $w'$  が求めるものになる。

定理3.5の証明  $\mathbb{Z}^n/H$  は巡回群の直和である：

$$\mathbb{Z}^n/H = \langle g_1 \rangle \oplus \cdots \oplus \langle g_n \rangle, \quad 1 \leq n.$$

補題より、必要ならば  $g_i \neq -g_i = 1$  として、初めから  $g_i = \bar{\gamma}(w_i)$ ,  
 $w_i = a_1 u_i a_1$  としてよい。  $\eta(w_i) = h_i$  及  $u'' \eta(w) = g$  とおく。ただし  
 $w = a_1 a_s a_1$  ( $s \neq 1$ )。このとき  $g^2$  は中乗元になることがわかる。  
つまり  $H_i$  の単位元である。  $g^2 = e$  とおく。次に各  $i$  に対して  
 $g h_i g^{-1} h_i = e$  とする。実際、  $u = a_1 a_s a_1 w_i a_1 a_s a_1 w_i$  とおくと定理  
2.4の下すべての条件が、  $u$  と  $w^2$  に対して成り立つ。従って、  $u$   
 $\equiv w^2$  とする。これは  $\eta(u) = \eta(w) \eta(w_i) \eta(w) \eta(w_i) = \eta(w^2) = e$  を意味



する。つまり  $g^{-1}h_i g h_i = e$  又は  $g^{-1}h_i g = h_i$  とする。

次に、 $F \ni h_1, \dots, h_r$  から生成された群とする。  $F$  が、巡回群  $\langle h_1 \rangle, \dots, \langle h_r \rangle$  の直積に等しいことを示す。そのために、 $h_1^{m_1} \dots h_r^{m_r} = e$  と仮定する。これは  $A^*$  の中で考えたと  $w_1^{m_1} \dots w_r^{m_r} \equiv w^2$  と意味し、従って  $\bar{\gamma}(w_1^{m_1} \dots w_r^{m_r}) = m_1 g_1 + \dots + m_r g_r = \bar{\gamma}(w^2) = \bar{0}$  とする。従って  $m_i g_i = \bar{0}$  となり、さらに  $w_i^{m_i} \equiv w^2$  と得る。これは  $\eta(w_i^{m_i}) = h_i^{m_i} = \eta(w^2) = e$  と意味する。即ち、 $F$  は  $\langle h_1 \rangle, \dots, \langle h_r \rangle$  の直積である。最後に、 $H_1$  は  $F$  と  $\langle g \rangle$  により生成されていることを示す。  $z \in A_1$  の任意の元とする。このとき、語  $u$  を次の様に定める：

$$u = z, \quad (z = a_1 \dots a_1 \text{ のとき}) \quad (1)$$

$$u = wz, \quad (z = a_1 \dots a_1 \text{ のとき}) \quad (2)$$

$\bar{\gamma}(u) = m_1 g_1 + \dots + m_r g_r$  と表示する。このとき、 $u$  と、 $v = w_1^{m_1} \dots w_r^{m_r}$  は合同になる。従って  $\eta(u) = \eta(v) = h_1^{m_1} \dots h_r^{m_r}$  とする。これは、(1) 又は (2) に従って  $\eta(z) = h_1^{m_1} \dots h_r^{m_r}$  又は  $\eta(w)\eta(z) = h_1^{m_1} \dots h_r^{m_r}$  と意味する。  $\eta(w) = g = g^{-1}$  より、 $H_1$  の任意の元  $\eta(z)$  は、群  $\langle g, F \rangle$  に属する。従って  $H_1 = \langle g, F \rangle = \langle g \rangle * F$  とする。

群  $H_1$  ( $S$  のすべての  $\mathcal{N}$ -class と同型になり、その) を code  $\Gamma(H)$  の群と呼ぶ。これについての詳しいことは  $\square$  又は  $\square$  を参照。

## 4. いくつかの code の例とその群

この節では簡単な code の例を4つ与える。code  $\Gamma(H)$  は  $\mathbb{Z}^n$  の部分群  $H$  によつて定まる。 $\mathbb{Z}^n$  は有限生成な自由 abel 群だから  $H$  が自明でなければ、 $H$  は基  $u_1, \dots, u_k$  を持つ。そこで code  $\Gamma(H)$  とこの基と同一視して、行列

$$\begin{bmatrix} u_1 \\ \vdots \\ u_k \end{bmatrix}$$

で表すことにする。前の様に  $A = \{a, b\}$ 、 $a = a_1$ 、 $b = a_2$ 、

$$\Sigma = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

とする。又、 $C_m$ 、 $D_m$  とそれぞれ位数  $m$  の巡回群、2面体群とする。

例 4.1.  $H = \mathbb{Z}(2, 0) + \mathbb{Z}(0, 1)$  のとき

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \{b\} \cup \{a^i b^j \mid i \geq 0\}$$

図 4.1.

$H$  の点から出発し、初めて  $H$  の点に終る道  $p(w)$  に対して、 $w$  が code  $\Gamma(H)$  の元となる。この code の群は、定理 3.1 より  $C_2$  である。

例 4.2.  $H = \mathbb{Z}(2, 0) + \mathbb{Z}(1, 1)$  このとき

$$\begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} = \{a^2, ab, ba, b^2\} \quad \text{図 4.2.}$$

この code の群も  $C_2$  である。

例 4.3.  $H = \mathbb{Z}(3, 0) + \mathbb{Z}(0, 1)$  このとき

$$\begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} = \{b\} \cup \{ab^h a \mid h \geq 1\} \cup a^2 \cdot \{b^k a \mid k \geq 1\} \cdot a \quad \text{図 4.3.}$$

$\mathbb{Z}^2/H \cong C_3$  であるから、定理 3.5 よりこの code の群は  $D_6$  となる。

例 4.4  $H = \mathbb{Z}(3, 0) + \mathbb{Z}(1, 1)$  このとき

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix} = \{a^3, a^2ba, a^2b^2, ab, ba^2, (ba)^2, bab^2, b^2a, b^3\} \quad \text{図 4.4.}$$

$\mathbb{Z}^2/H \cong C_3$  より、code の群は  $D_6$  である。

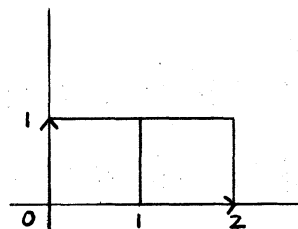


図 4.1

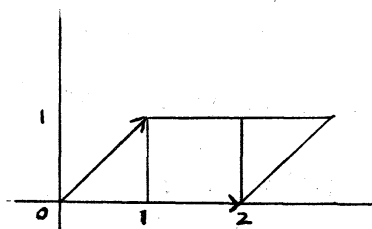


図 4.2

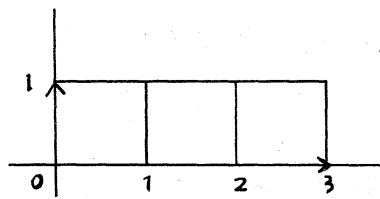


図4.3

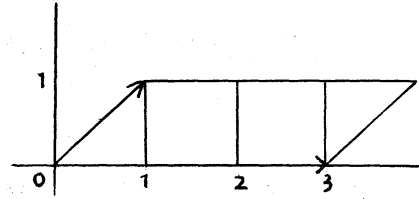


図4.4

命題4.1.  $\mathbb{Z}^n/H$  が位数  $d$  の有限群とする。このとき、各  $a_i \in A$  に対して、 $a_i^{d_i} \in \Gamma(H)$  とする  $d$  の約数  $d_i$  が一意に定まる。

証明. 仮定より  $n$  個のベクトル  $u_1, \dots, u_n$  があり  $H$  を生成する。そのとき、行列  $D = [{}^t u_1, \dots, {}^t u_n]$  は正則で、 $d$  は行列  $D$  の行列式の絶対値に等しい。さらに各  $i=1, \dots, n$  に対して、 $x_1 u_1 + \dots + x_n u_n = (0, \dots, d, \dots, 0)$  とする整数  $x_1, \dots, x_n$  が存在する。  $\gamma(a_i^d) = (0, \dots, d, \dots, 0) \in H$  より  $a_i^d \in \Gamma^*(H)$  となり、 $\Gamma(H)$  は code だから、求める  $d_i$  が存在する。

### 参考文献

- ①. Lallement, G. 1979. "Semigroups and Combinatorial Applications"
- ②. Berstel, J., Perrin, D. 1985. "Theory of Codes." Academic Press, London, New York.