数理解析研究所講究録
第311巻 1977年 11-24

ガロア体上の原始既約多項式の係数について

早大 システム科学研究所
高橋磐郎，杉本英士

§0 まえがき

GF(p)（pは素数）上の次の原始既約多項式の構成には，勝手に多項式を手えてそれをチェックするとか，$x^{p^n-1}-1$の因数分解をするなど，多くの手間を必要とする．ここではFrobenius cycleの和から生成される環の分解を利用して原始既約多項式の係数を生成する簡単なアルゴリズムを提案する．$p=2$の場合には半単純環の中での直交化の一般的アルゴリズム（§A）をこの問題に適用することができるが，特殊な場合についての効率よい巡回的アルゴリズムを提案する（§2，3）．$p\neq 2$のときの具体的アルゴリズムはまだ完成していないが，同一の理論に基づくアルゴリズムの作成はそれ程むずかしくないだろう．

§1 基本定理

$GF(p)$ 上 $\bmod(x^{p^n-1}-1)$ の多項式環を R とし，

$$G=\{x, x^2, \cdots, x^{p^n-2}\} \tag{1}$$

とする．任意の $y\in G$ に対して $\{y, y^p, \cdots, y^{p^{m-1}}\}$ ($y^{p^m}=y$ で $l<m$ について $y^{p^l}\neq y$) を Frobenius cycle と呼び，1つの Frobenius cycle の中の元の総和

$$t(y)=y+y^p+y^{p^2}+\cdots+y^{p^{m-1}} \tag{2}$$

を y の trace と呼ぶ．もちろん $t(y)=t(y^{p^l})$ が成立つ．G の trace の全体を $\{t_0, t_1, \cdots, t_{k-1}\}$ とする．

定理1 2つの trace の積はつねに trace の（$GF(p)$ の元を係数とする）1次結合であらわされる．すなわち

$$t_i t_j=\sum_{\nu=0}^{k-1} c_{ij}^{\nu} t_\nu \quad (c_{ij}^{\nu}\in GF(p),\ 0\le i,j\le k-1) \tag{3}$$

したがって

$$T=\{x_0t_0+\cdots+x_{k-1}t_{k-1} : x_i\in GF(p),\ 0\le i\le k-1\} \tag{4}$$

は R の部分環である．さらに T は $GF(p)$ 上の多元環で，(3) を単積表とするものである．（証明略）

θ を $GF(p^n)$ の原始元とし，$f(x)$ を θ の $GF(p)$ 上の最小多項式つまり原始既約多項式とする．$f(x)$ を

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_0 \quad (a_i\in GF(p)) \tag{5}$$

とする．θ を含む Frobenius cycle の元 $\theta, \theta^p, \theta^{p^2}, \cdots, \theta^{p^{n-1}}$ はすべて $f(x)=0$ の根であるから，根と係数との関係から

$$a_1 = -\sum_{0\le i\le n-1} \theta^{p^i} \quad a_2 = \sum_{0\le i<j\le n-1} \theta^{p^i}\theta^{p^j} \quad a_3 = -\sum_{0\le i,j,k\le n-1} \theta^{p^i}\theta^{p^j}\theta^{p^k} \cdots \qquad (6)$$

が成立つ．又で形式的に

$$a_1(x) = -\sum_{0\le i\le n-1} x^{p^i}, \quad a_2(x) = \sum_{0\le i<j\le n-1} x^{p^i}x^{p^j}, \quad a_3(x) = -\sum_{0\le i,j,k\le n-1} x^{p^i}x^{p^j}x^{p^k}, \cdots \qquad (7)$$

と定義するとつぎが成立つ．

定理2 $a_1(x), \cdots, a_m(x)$ は trace $t_0, t_1, \cdots, t_{k-1}$ の（GF(p)の元を係数とする）1次結合であらわされる．

$$a_i(x) = \sum_{j=0}^{k-1} c_{ij} t_j, \quad c_{ij} \in GF(p), \quad \begin{matrix} 1\le i\le m \\ 0\le j\le k-1 \end{matrix} \qquad (8)$$

（又、$a_1(x), \cdots, a_m(x)$ は Tの元である．（証明略））

例1 $p=2$, $n=3$, $x^7=1$, $k=2$

$t_0 = x+x^2+x^4$, $t_1 = x^3+x^6+x^5$, $t_0^2 = t_0$, $t_1^2 = t_1$, $t_0t_1 = 0$

$a_1(x) = t_0$, $a_2(x) = t_1$, $a_3(x) = t_0+t_1$

例2 $p=2$, $n=4$, $x^{15}=1$, $k=4$

$t_0 = x+x^2+x^4+x^8$, $t_1 = x^7+x^{14}+x^{13}+x^{11}$, $t_2 = x^3+x^{16}+x^{12}+x^9$

$t_3 = x^5+x^{10}$ $\qquad t_i^2 = t_i$, $0\le i\le 3$

$t_0t_1 = t_0+t_1+t_2$, $t_0t_2 = t_0$, $t_1t_2 = t_1$, $t_0t_3 = t_1+t_2$

$t_1t_3 = t_2+t_0$, $t_2t_3 = t_0+t_1$

$a_1(x) = t_0$, $a_2(x) = t_2+t_3$, $a_3(x) = t_1$, $a_4(x) = t_0+t_1+t_2+t_3$

さてRの中に線形関係

$$(x^{p^n-1}-1)/(x^d-1)=0 \quad \text{for } \forall d \mid (p^n-1) \qquad (9)$$

を導入しよう. GF(p)上n次最小既約多項式全体は$(x^{p^n-1}-1)$の因数として表わされる. これらの全体の積つまりオーダーp^n-1の円周等分多項式を$p(x)$とすると, Rの中にmod $p(x)$を与えたものと(9)の線形関係とは同値であり, mod $p(x)$による環を$\bar{R}$とすると, (9)はRから$\bar{R}$への準同型を規定する. この準同型によるTの像を$\bar{T}$としよう.

例3 例2では(9)はつぎのようになる;

$$\left.\begin{aligned}(x^{15}-1)/(x-1) &= 1+x+x^2+\cdots+x^{14}=0\\ (x^{15}-1)/(x^3-1) &= 1+x^3+x^6+x^9+x^{12}=0\\ (x^{15}-1)/(x^5-1) &= 1+x^5+x^{10}=0\end{aligned}\right\} \qquad (10)$$

これらは $t_3=1$, $t_2=1$, $t_0+t_1=1$ となる. $x^{15}-1$ の既約因子分解は,

$$x^{15}-1=(x-1)(1+x+x^2)(1+x+x^2+x^3+x^4)(1+x+x^4)(1+x^3+x^4) \qquad (11)$$

となり, オーダー15の円周等分多項式は $p(x)=(1+x+x^4)\times(1+x^3+x^4)$ である. (10)なる関係はmod $p(x)$と同値で, Tの$\bar{T}$への準同型は, 表1のようになり

$$\bar{T}=\{0, t_0, t_1, t_0+t_1=1\}$$

である. //

表 1

T	$\overline{T}$	T	$\overline{T}$	T	$\overline{T}$
0	0	t_0+t_1	1	$t_0+t_1+t_2$	0
t_0	t_0	t_0+t_2	t_1	$t_0+t_1+t_3$	0
t_1	t_1	t_0+t_3	t_1	$t_0+t_2+t_3$	0
t_2	1	t_1+t_2	t_0	$t_1+t_2+t_3$	t_1
t_3	1	t_1+t_3	t_0	$t_0+t_1+t_2+t_3$	1
		t_2+t_3	0		

今後任意の $r \in R$ に対してこの準同型による像を $\overline{r}$ と書くことにする．これによると例 3 で $\overline{t_0}=t_0$, $\overline{t_1}=t_1$, $\overline{t_2}=1$, $\overline{t_3}=1$ などとなる．

(9) 式で $d=1$ とおくと $1+x+x^2+\cdots+x^{p^n-2}=0$ となるが，これは

$$1+\overline{t_0}+\overline{t_1}+\cdots+\overline{t_{p^n-1}}=0 \qquad (12)$$

となり，これから T は非零単位元 1 を p^n-1 本の素数であれば (9) から出る関係は (12) だけであよ．

定理 3 基本定理　T を $GF(p)$ に写す環準同型を ρ とし，

$$a_i=\rho(\overline{a_i(x)}) \qquad 1\le i\le m \qquad (13)$$

とすると，$a_1,\cdots,a_m$ は $GF(p)$ 上 m 次の原始既約多項式の係数 (→(5)) である．逆に任意の ($GF(p)$ 上 m 次) 原始既約多項式の係数は T から $GF(p)$ への適当な環準同型の $\overline{a_i(x)}$ の像として得られる．(証明略)

$\mathcal{T}$ から $GF(p)$ への準同型の核は $\mathcal{T}$ の極大イデアルである．逆に I を $\mathcal{T}$ の極大イデアルとすると，I を 0 に写す $\mathcal{T}$ から $GF(p)$ への剰余環は準同型を構成する．(→定理4)．よって原始既約多項式の係数を1組見出すことと $\mathcal{T}$ の極大イデアルを1つ見つけることとは同値である．

定理4 $\mathcal{T}$ は半単純環で

$$l = \varphi(p^n-1)/n \quad (\varphi \text{はオイラー関数}) \tag{14}$$

個の極小イデアル $M_0, \cdots, M_{l-1}$ の直和に一意的に分解される．つまり

$$\mathcal{T} = M_0 \oplus M_1 \oplus \cdots \oplus M_{l-1} \tag{15}$$

で各 M_i は $GF(p)$ に同型である．p^n-1 が素数のときは明らかに $l = k$　　(証明略)

そこで $\mathcal{T}$ の中に互に直交し和が1になる l 個のべき等元 $e_0, e_1, \cdots, e_{l-1}$;

$$\left.\begin{aligned} &e_i e_j = \delta_{ij} e_i \quad (\delta_{ij} \text{はクロネカーのデルタ}) \\ &e_0 + e_1 + \cdots + e_{l-1} = 1 \end{aligned}\right\} \quad 0 \le i, j \le l-1 \tag{16}$$

を得ることができれば，半単純環のよく知られた性質から [2]

$$M_i = \mathcal{T} e_i \,, \quad 0 \le i \le l-1 \tag{17}$$

が定理4における極小イデアルとなる．そして

$$\overline{M}_i = M_0 \oplus \cdots \oplus M_{i-1} \oplus M_{i+1} \oplus \cdots \oplus M_{l-1} \,, \quad 0 \le i \le l-1 \tag{18}$$

とすれば，$\overline{M}_i$ は $\mathcal{T}$ の極大イデアルで，$\overline{M}_0, \overline{M}_1, \cdots, \overline{M}_{l-1}$ 以外

に $\mathfrak{T}$ の極大イデアルはない.

このとき任意の $r \in \mathfrak{T}$ は

$$r = r_0 e_0 + r_1 e_1 + \cdots + r_{l-1} e_{l-1} \quad (r_i \in GF(p),\ 0 \le i \le l-1) \tag{19}$$

と一意に表わされて, 各 r_i は

$$re_i = r_i e_i \quad (r_i \in GF(p)) \tag{20}$$

によって定めることができる. そして $\overline{M}_i$ を 0 に写像する $\mathfrak{T}$ の $GF(p)$ への準同型を ρ_i とすると

$$\rho_i(r) = r_i \quad , 0 \le i \le l-1 \tag{21}$$

以上から原始既約多項式の係数を求めるアルゴリズムをまとめると;

(i) (8) によって $a_1(x), a_2(x), \cdots, a_m(x)$ を求める

(ii) (16) をみたすべき等元 e_i を1つ求める

(iii) $a_1(x)e_i = a_1 e_i,\ a_2(x)e_i = a_2 e_i, \cdots, a_m(x)e_i = a_m e_i$ (22)

とすると $a_1, a_2, \cdots, a_m$ が原始既約多項式 (5) の係数.

以上のことを $e_i = e_0, e_1, \cdots, e_{l-1}$ のおのおのについて行えばすべての原始既約多項式が作られる.

§2 巡回的アルゴリズム (p^m-1 が素数の場合)

以上によって結局は §1 (16) をみたす $e_0, e_1, \cdots, e_{l-1}$ を求めればよいことがわかった. $p=2$ の場合 §4 に示す直交化の方法を用いればこれは常に可能であるが, この §では p^m-1

が素数の場合をわめて簡単な巡回的アルゴリズムを提案しよう．また p^n-1 が素数なら $p=2$ で $k=l$ であることに注意しておこう．

まず t_i の中の x の指数の集合を N_i としておく．$j \in \{1, 2, \cdots, p^n-2\}$ について π_j を

$$x \longrightarrow x^j \pmod{x^{p^n-1}-1} \quad (G\text{上で}x\text{の指数を}j\text{倍する}) \tag{23}$$

なる変換とよう．これは $\{t_0, t_1, \cdots, t_{k-1}\}$ 上に置換をひき起す．よが

$$N_0 = \{1, p, p^2, \cdots, p^{n-1}\} \tag{24}$$

の元のとき π_j は恒等置換となる．N_0 は乗法群

$$N = \{1, 2, \cdots, p^n-2\} \bmod (p^n-1) \tag{25}$$

の部分群で，N を N_0 でコセット分割すれば各コセットは N_i となる．商群 $N/N_0 = \{N_0, N_1, \cdots, N_{k-1}\}$ は，N_1 が p^n-1 の原始根 ξ を含むとすると N_1 を生成元とする巡回群となる．このとき

$$N_0 = N_1^0,\ N_1 = N_1^1,\ N_2 = N_1^2,\ \cdots,\ N_{k-1} = N_1^{k-1} \tag{26}$$

のように番号をつけるとそれに対して $t_0, t_1, \cdots, t_{k-1}$ に1番号が定まる．つまり p^n-1 の原始根を1つ選ぶことにより trace に番号をつけることができる．

例4　$p=2$, $n=5$, $x^{31}=1$, $k=6$．31の原始根として3を選ぶとつぎのような順序が得られる．

$N_0 = \{1, 16, 8, 4, 2\}$ $t_0 = x + x^{16} + x^8 + x^4 + x^2$
$N_1 = \{3, 17, 24, 12, 6\}$ $t_1 = x^3 + x^{17} + x^{24} + x^{12} + x^6$
$N_2 = \{9, 20, 10, 5, 18\}$ $t_2 = x^9 + x^{20} + x^{10} + x^5 + x^{18}$
$N_3 = \{27, 29, 30, 15, 23\}$ $t_3 = x^{27} + x^{29} + x^{30} + x^{15} + x^{23}$
$N_4 = \{19, 25, 28, 14, 7\}$ $t_4 = x^{19} + x^{25} + x^{28} + x^{14} + x^7$
$N_5 = \{26, 13, 22, 11, 21\}$ $t_5 = x^{26} + x^{13} + x^{22} + x^{11} + x^{21}$

こうすると 乗積表も巡回的に得られる:

$t_0t_1 = t_0+t_2+t_5$ $t_0t_2 = t_1+t_2+t_4$ $t_0t_3 = t_2+t_5$
$t_1t_2 = t_1+t_3+t_0$ $t_1t_3 = t_2+t_3+t_5$ $t_1t_4 = t_3+t_0$
$t_2t_3 = t_2+t_4+t_1$ $t_2t_4 = t_3+t_4+t_0$ $t_2t_5 = t_4+t_1$
$t_3t_4 = t_3+t_5+t_2$ $t_3t_5 = t_4+t_5+t_1$
$t_4t_5 = t_4+t_0+t_3$ $t_4t_0 = t_5+t_0+t_2$
$t_5t_0 = t_5+t_1+t_4$ $t_5t_1 = t_0+t_1+t_3$ $t_i^2 = t_i$, $0 \leqslant i \leqslant 5$

$a_1(x)=t_0$, $a_2(x)=t_1+t_2$, $a_3(x)=t_4+t_5$, $a_4(x)=t_3$, $a_5(x)=1$

定理5 (予想) 上に定めた順に trace の番号 $t_0, t_1, \cdots t_{k-1}$ をつけるとする. $t_0t_1\cdots t_r = 0$ で r より小さい s については $t_0t_1\cdots t_s \neq 0$ であるなら,

$$e_i = t_i t_{i+1} \cdots t_{i+r-1} \quad (\text{添字は } \bmod k) \quad 0 \leq i \leq k-1 \qquad (27)$$

とおくと, $e_0, e_1, \cdots, e_{k-1}$ は 下 の表の直交べき等元で 和が 1 となる. つまり (16) をみたす.

以下に上の定理を利用して §1 の (i)(ii)(iii) によってすべての原始既約多項式を求めた例を示す. ただし (iii) のように直接 a_i を求めず一たん t_j を仲介した.

例5 $p=2$, $n=5$, $x^{31}=1$, $k=6$

$t_0t_1t_2=0$ ($t_0t_1\neq 0$)

$e_0=t_0t_1(=t_0+t_2+t_5)$
$e_1=t_1t_2(=t_1+t_3+t_0)$
$e_2=t_2t_3(=t_2+t_4+t_1)$
$e_3=t_3t_4(=t_3+t_5+t_2)$
$e_4=t_4t_5(=t_4+t_0+t_3)$
$e_5=t_5t_0(=t_5+t_1+t_4)$

	t_0	t_1	t_2	t_3	t_4	t_5	a_0	a_1	a_2	a_3	a_4	a_5
e_0	1	1	0	0	1	0	1	1	1	0	1	
e_1	0	1	1	0	0	1	0	0	1	0	1	
e_2	1	0	1	1	0	0	1	1	0	1	1	
e_3	0	1	0	1	1	0	0	1	1	1	1	
e_4	0	0	1	0	1	1	0	1	0	0	1	
e_5	1	0	0	1	0	1	1	0	1	1	1	

$a_1=t_0$
$a_2=t_1+t_2$
$a_3=t_4+t_5$
$a_4=t_3$
$a_5=1$

c_{ij}: $e_it_j=c_{ij}e_i$

例 6　$p=2$, $n=7$, $x^{127}=1$, $k=18$

原始根として $\xi=3$ を選び, $t_0, t_1, \cdots, t_{17}$ と番号づけする

$t_0t_1\cdots t_5=0$　($t_0t_1\cdots t_\Delta\neq 0$ for $\Delta<5$)

$e_0=t_0t_1t_2t_3t_4(=t_0+t_1+t_3+t_4+t_5+t_8+t_{14}+t_{16}+t_{17})$

$e_1, e_2, \cdots, e_{17}$ は e_0 から巡回的に求められる.

	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	a_1	a_2	a_3	a_4	a_5	a_6	a_7
e_0	1	1	1	1	1	0	1	0	0	0	0	1	0	0	0	1	1	0	1	1	1	0	0	0	1
e_1	0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	1	1	0	0	1	0	0	0	1
	•	•	•	•	•	•	•																		

$a_1(x)=t_0$, $a_2(x)=t_1+t_2+t_{15}$, $a_3(x)=t_4+t_7+t_8+t_{12}+t_{14}$
$a_6(x)=t_9$, $a_5(x)=t_6+t_{10}+t_{11}$, $a_4(x)=t_3+t_5+t_{13}+t_{16}+t_{17}$　$a_7(x)=1$　(28)

上の表で e_0 の t_0 ～ t_{17} に対する行が求まれば, これを右に1つずつずらせば $e_1, e_2, \cdots$ の t_0 ～ t_{17} に対する行が求まる. そのおのおのについて (28) 式を用いて a_1 ～ a_7 を求めればよい. なほ $a_i(x)$ を求める場合も実際には $a_1(x), a_2(x), a_3(x)$ だけでよく t_i を t_{i+q} にすれば $a_6(x), a_5(x), a_4(x)$ が求まる.

§3 巡回的アルゴリズム ($p=2$, $\bar{N}/N_0$ が巡回群)

$\bar{N}$ ($\subset N$) を p^n-1 に素な数の集合とすると, $\bar{N}$ は $\bmod(p^n-1)$ の中で乗法群を作る. そこで $N_0=\{1, 2, 2^2, \cdots, 2^{n-1}\}$ は $\bar{N}$ の部分群である. ここでは $\bar{N}/N_0$ が巡回群の場合を考える.

N_1 を $\bar{N}/N_0$ の生成元とし, $N_0, N_1, N_2, \cdots, N_{l-1}$ の番号を

$$N_i = N_1^i \quad , \quad 0 \le i \le l-1 \tag{29}$$

できめる. t_i の番号を N_i にならってつける, $0 \le i \le l-1$. $j \ge l$ について t_j の番号は任意でよい. このとき, 定理5は $k=l$ について成立する (予想).

以下に §2 と同様いくつかの例を示す.

例7

$p=2$, $n=4$, $x^{15}=1$, $k=4$, $l=2$

$\bar{N}$ {
$N_0=\{1,2,4,8\}$ $t_0=x+x^2+x^4+x^8$
$N_1=\{7,14,13,11\}$ $t_1=x^7+x^{14}+x^{13}+x^{11}$
$N_2=\{3,16,12,9\}$ $t_2=x^3+x^{16}+x^{12}+x^9$
$N_3=\{5,10\}$ $t_3=x^5+x^{10}$

$t_0t_1=0$ (←example 3) so $e_0=t_0$, $e_1=t_1$.

	t_0	t_1	a_1	a_2	a_3	a_4
e_0	1	0	1	0	0	1
e_1	0	1	0	0	1	1

$a_1(x)=t_0$, $a_2(x)=0$
$a_3(x)=t_1$, $a_4(x)=1$

例 8　　$p=2$, $n=6$, $x^{63}=1$, $k=12$, $l=6$

$t_0 = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$　　$t_6 = x^3 + x^6 + x^{12} + x^{24} + x^{48} + x^{33}$

$t_1 = x^5 + x^{10} + x^{20} + x^{40} + x^{17} + x^{34}$　　$t_7 = x^{15} + x^{30} + x^{60} + x^{57} + x^{51} + x^{39}$

$t_2 = x^{11} + x^{22} + x^{44} + x^{25} + x^{50} + x^{37}$　　$t_8 = x^7 + x^{14} + x^{28} + x^{56} + x^{49} + x^{35}$

$t_3 = x^{31} + x^{62} + x^{61} + x^{59} + x^{55} + x^{47}$　　$t_9 = x^9 + x^{18} + x^{36}$

$t_4 = x^{23} + x^{46} + x^{29} + x^{58} + x^{53} + x^{43}$　　$t_{10} = x^{27} + x^{54} + x^{45}$

$t_5 = x^{13} + x^{26} + x^{52} + x^{41} + x^{19} + x^{38}$　　$t_{10} = x^{21} + x^{42}$

$t_0 t_1 t_2 t_3 t_4 = 0$ ($t_0 t_1 \cdots t_s \neq 0$, $s<4$)　　$e_0 = t_0 t_1 t_2 t_3 (= t_1 + t_2 + t_6)$

	t_0	t_1	t_2	t_3	t_4	t_5	a_1	a_2	a_3	a_4	a_5	a_6
e_0	1	1	1	1	0	0	1	0	0	1	1	1
e_1	0	1	1	1	1	0	0	0	0	0	1	1
	.....											

$a_1(x)=t_0$, $a_2(x)=t_1+1$, $a_3(x)=t_2+t_5+1$, $a_4(x)=t_4+1$, $a_5(x)=t_3$

$a_6(x)=1$

where from (9)

$t_{11}=1$, $t_9+t_{10}=1$, $t_8=0$, $t_6+t_7=1$, $t_0+t_1+t_2+t_3+t_5=0$.

§A　$p=2$ の場合の直交化アルゴリズム（[1] 52頁の要約）

R の生成元を $t_0, t_1, \cdots, t_{k-1}$（必ずしも1次従属でない）とする。$p=2$ だからこれらはすべてべき等元である。

手順1　$e_0 = t_0$, $e_1 = 1+t_0$ とすると $e_0 e_1 = 0$, $e_0 + e_1 = 1$

手順2　$e_i t_1$, $e_i(1+t_1)$ のどちらも 0 でないような i を1つ選ぶ。たとえば $i=0$ がそうなら、$e_0 t_1$, $e_0(1+t_1)$ はべき等元で互に直交し、しかもそれぞれ他の e_i と直交する。（のみならずその和は e_0 となるから、改めて

$$e_0 t_1 \to e_0,\quad e_0(1+t_1) \to e_1,\quad e_1 \to e_2$$

とおくと、これらは直交べき等元で全体の和が1となる。

手順3　$e_i t_2$, $e_i(1+t_2)$ のどちらも 0 でないような i を1つ選ぶ。たとえば $i=1$ がそうなら、e_1 を $e_1 t_2$, $e_1(1+t_2)$ の2つに分割して改めて

$$e_0 \to e_0,\quad e_1 t_2 \to e_1,\quad e_1(1+t_2) \to e_2,\quad e_2 \to e_3$$

とおくと、これらは直交べき等元で全体の和が1となる。

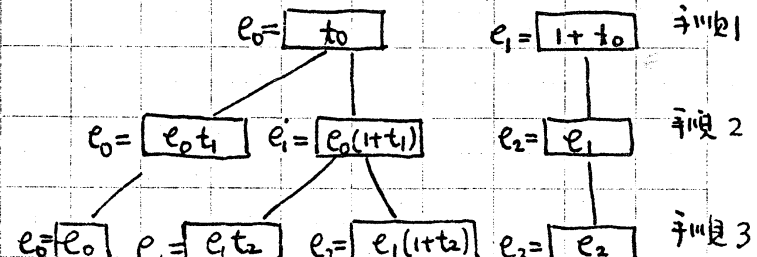

図1

以上の手順をつづけて $e_i t_{l-1}$, $e_i(1+t_{l-1})$ のどちらも 0 でない i が存在しなくなるまでの、$e_0, e_1, \cdots, e_{l-1}$ が原始的べき等元つまり、Re_i が極小イデアルとなるものである。

例[9]　$p=2$, $n=5$, $x^{31}=1$, $k=l=6$ の場合に上のアルゴリズムを適用するとつぎの図[12]のようになる。ただし図[12]では変化しないべき等元を重複して書くことはしていない。

24

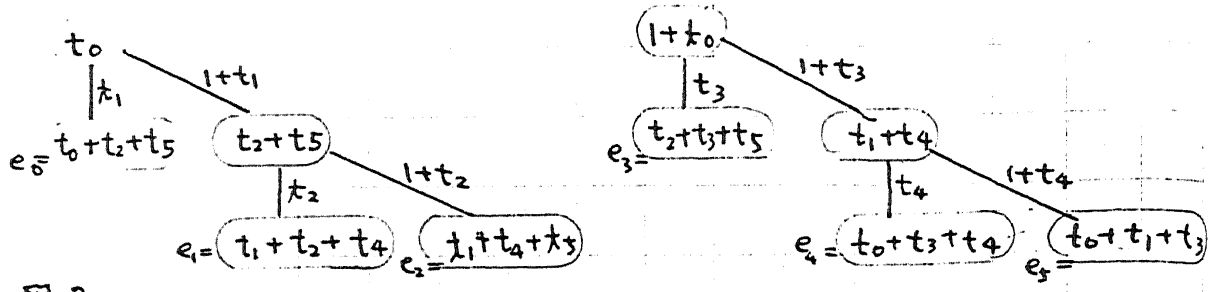

図2

ここで得られた $e_0, e_1, \cdots, e_5$ は例5で求めたものと順序を除いて完全に一致している.

参考文献

[1] J. H. van Lint "Coding Theory" Springer-Verlag Lecture Notes in Math. 201 (1971)

[2] I. F. Blake & R. C. Mullin "The Mathematical Theory of Coding" Academic Press (1975)

この研究に当って群馬高専須田健二氏, 東京理科大学の神保雅一氏から有益な助言をいただいたのでここに感謝いたします.