

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 n 次の原始既約多項式の構成には、勝手に多項式を写してそれをチェックするとか、 $x^{p^n}-1$ の因数分解をやるなど、多くの手間を必要とする。ここでは Frobenius cycle の和から生成された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から成るが、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)。 $p \neq 2$ のときの具体的なアルゴリズムはまた完成してはいないが、同一の理論に基づくアルゴリズムの作成は容易に思われる。

§1 基本定理

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

$$G = \{x, x^2, \dots, x^{p^m-1}\} \quad (1)$$

とする. 任意の $y \in G$ に対して $\{y, y^p, \dots, y^{p^{m-1}}\}$ ($y^{p^m} = y$ 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

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

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 $\{t_0, t_1, \dots, t_{k-1}\}$ 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

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

いたから

$$T = \{x_0 t_0 + \dots + x_{k-1} t_{k-1} : x_i \in GF(p), 0 \leq i \leq k-1\} \quad (4)$$

は R の部分環である. さらに T は $GF(p)$ 上の多元環で,

(3) と乗積表とすることができる. (証明略)

$\theta \in GF(p^m)$ の原始元とし, $f(x) \in \theta$ 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

$$f(x) = x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_0 \quad (a_i \in GF(p)) \quad (5)$$

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

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

が成立 \rightarrow . $x = z$ 形式的に

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

を定義すると $x = z$ が成立する。

定理 2 $a_1(x), \dots, a_m(x)$ は trace t_0, t_1, \dots, t_{k-1} の
($\text{GF}(p)$ の元係数と T の) 1 次結合 T の元と見做す。

$$a_i(x) = \sum_{j=0}^{k-1} c_{ij} t_j, \quad c_{ij} \in \text{GF}(p), \quad 1 \leq i \leq m, \quad 0 \leq j \leq k-1 \quad (8)$$

(T 上, $\{ a_1(x), \dots, a_m(x) \}$ は T の元である。(証明略))

例 1 $p=2, n=3, x^7=1, k=2$

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

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

例 2 $p=2, n=4, x^{15}=1, k=4$

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

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

$$t_0 t_1 = t_0 + t_1 + t_2, \quad t_0 t_2 = t_0, \quad t_1 t_2 = t_1, \quad t_0 t_3 = t_1 + t_2$$

$$t_1 t_3 = t_2 + t_0, \quad t_2 t_3 = t_0 + t_1$$

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

$t \in R$ の中に線形関係

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

を導入しよう。GF(p) 上 n 次原始既約多項式全体は $(x^{p^m-1} - 1)$ の因数 t_i を表わかし、これら全体の積つまり σ - τ $p^m - 1$ の円周等分多項式 $p(x)$ とする、 R の中に $\text{mod } p(x)$ を与えたい τ の (9) の線形関係 t は同値であり、 $\text{mod } p(x)$ による環 \bar{R} とする、(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 τ の τ による;

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

これらは $t_3=1, t_2=1, t_0+t_1=1$ とする。 $x^{15}-1$ の既約因子分解は、

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

とる、 σ - τ 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) の関係は $\text{mod } p(x)$ と同値で、 T の \bar{T} への準同型は、表 1 の τ による

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

である。 //

表 1

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

今后任意の $r \in R$ に対し τ の準同型像 \bar{r} と書くことにする。これにより $\bar{t}_0 = t_0, \bar{t}_1 = t_1, \bar{t}_2 = 1, \bar{t}_3 = 1$ となる。

(9) 式で $d=1$ とおくと $1 + x + x^2 + \dots + x^{p^n-2} = 0$ となるから、これは

$$1 + \bar{t}_0 + \bar{t}_1 + \dots + \bar{t}_{p^n-1} = 0 \quad (12)$$

となり、これから \bar{T} は乘法単位元 1 を除く \mathbb{F}_p 上の p^n-1 乗数であるから (9) から出る関係は (12) のみである。

定理 3 基本定理 \bar{T} を $GF(p)$ に写す環準同型 ρ

とし、

$$a_i = \rho(\bar{a}_i(x)) \quad 1 \leq i \leq n \quad (13)$$

とすると、 a_1, \dots, a_n は $GF(p)$ 上の n 次原始既約多項式の係数 ($\rightarrow (5)$) である。逆に任意の ($GF(p)$ 上の n 次) 原始既約多項式の係数は \bar{T} から $GF(p)$ への適当な環準同型の $\bar{a}_i(x)$ の像 a_i として得られる。(証明略)

\bar{T} から $GF(p)$ への準同型の核は \bar{T} の極大イデアルである。逆に I を \bar{T} の極大イデアルとすると、 $I \neq 0$ に写す \bar{T} から $GF(p)$ への環同型を構成する。(→ 定理 4)。よって本環原始既約多項式の係数を 1 とし、 \bar{T} の極大イデアルを 1 つ見つけることは同値である。

定理 4 \bar{T} は半単純環である。

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

個々の極小イデアル M_0, \dots, M_{l-1} の直和に一意的に分解される。つまり

$$\bar{T} = M_0 \oplus M_1 \oplus \dots \oplus M_{l-1} \quad (15)$$

ここで各 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 $l = 1$ (証明略)

よって \bar{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, \dots, e_{l-1} ;

$$\left. \begin{aligned} e_i e_j &= \delta_{ij} e_i \quad (\delta_{ij} \text{ はクロネッカーのデルタ}) \\ e_0 + e_1 + \dots + e_{l-1} &= 1 \end{aligned} \right\} \quad (16)$$

を得る。これをたまには、半単純環のよく知られた性質から [2]

$$M_i = \bar{T} e_i, \quad 0 \leq i \leq l-1 \quad (17)$$

が定理 4 における極小イデアルとなる。よって

$$\bar{M}_i = M_0 \oplus \dots \oplus M_{i-1} \oplus M_{i+1} \oplus \dots \oplus M_{l-1}, \quad 0 \leq i \leq l-1 \quad (18)$$

とすれば、 \bar{M}_i は \bar{T} の極大イデアルで、 $\bar{M}_0, \bar{M}_1, \dots, \bar{M}_{l-1}$ は互

に \bar{T} の極大イデアルは l 個、

このうち任意の $r \in \bar{T}$ は

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

と一意に表わすため、各 r_i は

$$r e_i = r_i e_i \quad (r_i \in GF(p)) \quad (20)$$

によって r の値も r_i によって決まる。 χ_i を \bar{T} を 0 に写像する \bar{T}

の $GF(p)$ への準同型を f_i とすると

$$f_i(r) = r_i, \quad 0 \leq i \leq l-1 \quad (21)$$

以上から原始既約多項式の係数を決めるアルゴリズムを

と定める;

- (i) (8) によって $a_1(x), a_2(x), \dots, a_m(x)$ を求める
 (ii) (16) をみたすべき等元 e_i を 1 つ求める
 (iii) $a_1(x)e_i = a_1 e_i, a_2(x)e_i = a_2 e_i, \dots, a_m(x)e_i = a_m e_i$ (22)
 とすると a_1, a_2, \dots, a_m が原始既約多項式 (5) の係数

以上のことで $e_i = e_0, e_1, \dots, e_{l-1}$ のおの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 ($p^m - 1$ A-素数の場合)

以上によって結局は §1 (16) をみたす e_0, e_1, \dots, e_{l-1} を求めるのはよいことになった。 $p=2$ の場合 §A に示す直交化の方法を用いるの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 $p^m - 1$ が素数ならば $p = 2$ で $k = 1$ であることに注意しておこう。

まず t_k の中の x の指数の集合を N_k としておく。 $j \in \{1, 2, \dots, p^m - 2\}$ について π_j を

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

なる変換としよう。これは $\{t_0, t_1, \dots, t_{k-1}\}$ 上に置換をひま起す。よか

$$N_0 = \{1, p, p^2, \dots, p^{m-1}\} \quad (24)$$

の元のとま π_j は相等置換となる。 N_0 は乘法群

$$N = \{1, 2, \dots, p^m - 2\} \pmod{p^m - 1} \quad (25)$$

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_k となる。商群 $N/N_0 = \{N_0, N_1, \dots, N_{k-1}\}$ は、 N_1 が $p^m - 1$ の原始根 ε 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

$$N_0 = N_1^0, N_1 = N_1^1, N_2 = N_1^2, \dots, N_{k-1} = N_1^{k-1} \quad (26)$$

のように番号をつけるとそれに対えして t_0, t_1, \dots, t_{k-1} に番号が定まる。つまり $p^m - 1$ の原始根を1つ選ぶことにより trace に番号をつけることかできる。

例 4 $p = 2, m = 5, x^{31} = 1, k = 6$. 31の原始根として3を選ぶとつぎのよう順序を得られる。

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

このように乗積表は巡回的を得られる:

$$\begin{aligned}
 t_0 t_1 &= t_0 + t_2 + t_5 & t_0 t_2 &= t_1 + t_2 + t_4 & t_0 t_3 &= t_2 + t_5 \\
 t_1 t_2 &= t_1 + t_3 + t_0 & t_1 t_3 &= t_2 + t_3 + t_5 & t_1 t_4 &= t_3 + t_0 \\
 t_2 t_3 &= t_2 + t_4 + t_1 & t_2 t_4 &= t_3 + t_4 + t_0 & t_2 t_5 &= t_4 + t_1 \\
 t_3 t_4 &= t_3 + t_5 + t_2 & t_3 t_5 &= t_4 + t_5 + t_1 & & \\
 t_4 t_5 &= t_4 + t_0 + t_3 & t_4 t_0 &= t_5 + t_0 + t_2 & & \\
 t_5 t_0 &= t_5 + t_1 + t_4 & t_5 t_1 &= t_0 + t_1 + t_3 & & \\
 & & & & t_i^2 &= t_i, 0 \leq i \leq 5
 \end{aligned}$$

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

定理5 (予想) 上に定めた場合には trace の番号 t_0, t_1, \dots, t_{k-1} をつけるとする. $t_0 t_1 \dots t_{r-1} = 0$ であり、小さい i については $t_0 t_1 \dots t_{i-1} \neq 0$ であるとする.

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

とあくと、 e_0, e_1, \dots, e_{k-1} は \bar{F} の互いの直交ベキ等元で、 $e_i^2 = e_i$ 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) により、この原始既約多項式を求めた例を示す。左に (iii) のように直接 a_i を求める - なく t_i を仲介して。

例5 $p=2, n=5, x^{31}=1, k=6$

$$t_0 t_1 t_2 = 0 \quad (t_0 t_1 \neq 0)$$

$e_0 = t_0 t_1 (=t_0 + t_2 + t_5)$	$e_1 = t_1 t_2 (=t_1 + t_3 + t_0)$	$e_2 = t_2 t_3 (=t_2 + t_4 + t_1)$	$e_3 = t_3 t_4 (=t_3 + t_5 + t_2)$	$e_4 = t_4 t_5 (=t_4 + t_0 + t_3)$	$e_5 = t_5 t_0 (=t_5 + t_1 + t_4)$
------------------------------------	------------------------------------	------------------------------------	------------------------------------	------------------------------------	------------------------------------

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

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

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

例 6 $p=2, n=7, x^{127}=1, k=18$

原始根 α として $\varepsilon=3$ を選ぶ, t_0, t_1, \dots, t_{17} と番号をつける

$$t_0 t_1 \dots t_5 = 0 \quad (t_0 t_1 \dots t_\Delta \neq 0 \text{ for } \Delta < 5)$$

$$e_0 = t_0 t_1 t_2 t_3 t_4 t_5 (=t_0 + t_1 + t_3 + t_4 + t_5 + t_8 + t_{14} + t_{16} + t_{17})$$

e_1, e_2, \dots, e_{17} は e_0 から巡回的に決められる.

	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	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
								

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

上の表で e_0 の $t_0 \sim t_{17}$ に対応する行が決められる, これを元に e_1, e_2, \dots の $t_0 \sim t_{17}$ に対応する行が決められる. そのおのおのによって (28) 式を用いて $a_1 \sim a_7$ を決められる. なお $a_2(x)$ を決めるときは実際には $a_1(x), a_2(x), a_3(x)$ を決めるとは t_2 と t_{15} に対応する $a_6(x), a_5(x), a_4(x)$ を決める.

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

$\bar{N} (CN)$ を p^m-1 に素数数の集合とすると, \bar{N} は $\text{mod } (p^m-1)$ の中で乗法群を作る. $\forall i \in N_0 = \{1, 2, 2^2, \dots, 2^{m-1}\}$ は \bar{N} の部分群である. \therefore \bar{N}/N_0 が巡回群の場合を考える.

N_i を \bar{N}/N_0 の生成元とし, $N_0, N_1, N_2, \dots, N_{l-1}$ の番号とする

$$N_i = N_1^i, \quad 0 \leq i \leq l-1 \quad (29)$$

つまり, N_i の番号を N_i に与えてやる, $0 \leq i \leq l-1$.

$j \geq l$ について N_j の番号は任意である. \therefore このとき, 定理 5 は $l = l$ 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

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

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

$$t_0 t_1 = 0 \quad (\leftarrow \text{example 3}) \quad \text{so } e_0 = t_0, e_1 = t_1.$$

	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

$$a_1(x) = t_0, \quad a_2(x) = 0$$

$$a_3(x) = t_1, \quad a_4(x) = 1$$

例 8

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

$$\begin{aligned}
 t_0 &= x + x^2 + x^4 + x^8 + x^{16} + x^{32} & t_6 &= x^3 + x^6 + x^{12} + x^{24} + x^{48} + x^{33} \\
 t_1 &= x^5 + x^{10} + x^{20} + x^{40} + x^{17} + x^{34} & t_7 &= x^{15} + x^{30} + x^{60} + x^{57} + x^{51} + x^{39} \\
 t_2 &= x^{11} + x^{22} + x^{44} + x^{25} + x^{50} + x^{37} & t_8 &= x^7 + x^{14} + x^{28} + x^{56} + x^{49} + x^{35} \\
 t_3 &= x^{31} + x^{62} + x^{61} + x^{59} + x^{55} + x^{47} & t_9 &= x^9 + x^{18} + x^{36} \\
 t_4 &= x^{23} + x^{46} + x^{29} + x^{58} + x^{53} + x^{43} & t_{10} &= x^{27} + x^{54} + x^{45} \\
 t_5 &= x^{13} + x^{26} + x^{52} + x^{41} + x^{19} + x^{38} & t_{10} &= x^{21} + x^{42}
 \end{aligned}$$

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

	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, \dots, t_{k-1} (必ずしも1次独立である) とする。

$p=2$ ならばこれはすべてべき等である。

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

手順2 $e_i t_1, e_i(1+t_1)$ のうち $\neq 0$ である i を1つ選ぶ。
 たゞ $i=0$ から選ぶ。 $e_0 t_1, e_0(1+t_1)$ はべき等として互に直交し、 e_0 と e_1 の和は e_0 となるから、改めて

$$e_0 t_1 \rightarrow e_0, e_0(1+t_1) \rightarrow e_1, e_1 \rightarrow e_2$$

とすると、これは直交べき等として全体の和が1となる。

手順3 $e_i t_2, e_i(1+t_2)$ のうち $\neq 0$ である i を1つ選ぶ。
 たゞ $i=1$ から選ぶ。 e_1 と $e_1 t_2, e_1(1+t_2)$ の2つに分割して改めて

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

とすると、これは直交べき等として全体の和が1となる。

以上の手順を繰り返して

$e_i t_{k-1}, e_i(1+t_{k-1})$ のうち $\neq 0$ である i から存在しなくなるまでの、 e_0, e_1, \dots, e_{k-1} から原始べき等

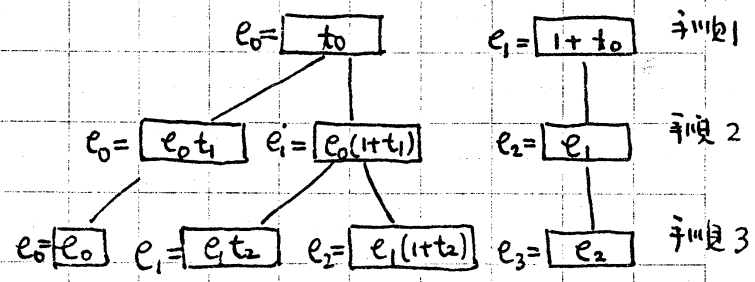


図1

元となり、 $R e_i$ から直交イデアルとなるのである。

例 10 $p=2, m=5, x^3=1, k=l=6$ の場合に上のアルゴリズムを適用すると以下の図²のようになる。ただし図²では変化しないべき等元を重複して書くことはしてある。

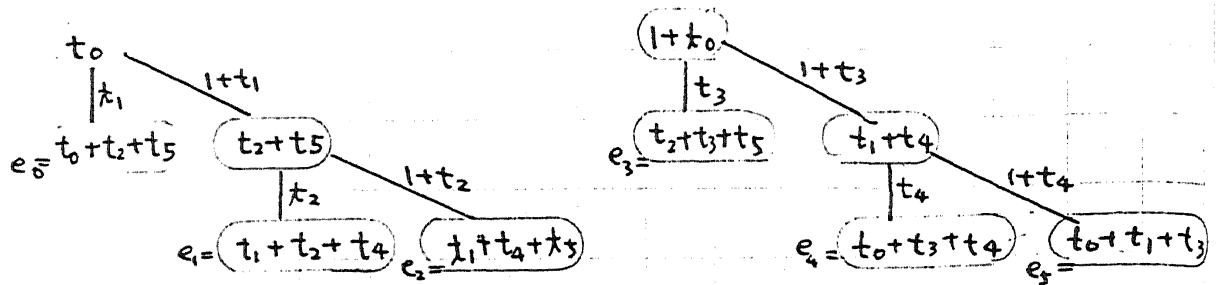


図 2

ここで得られた e_0, e_1, \dots, e_5 は例 5 で与えられた t の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] J. F. Blake & R. C. Mullin "The Mathematical Theory
of Coding" Academic Press (1975)

この研究に当って群馬大学 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。