有限体上のある多項式環の自己同型写像について

岩根博之

On the Polynomial Ring over GF(Ⅲ)

Hirosi Iwane

Abstract

Let F_p be finite filed. p is ch(F). p is prime. $F_p[x_1, x_2, \quad ,x_n]$ is the polynomial ring n-variables over F_p. Let A be $F_p[x_1, x_2, \quad, x_n]/(x_1-1)^p \quad (x_n-1)^p$. A is the ring that has zero divizor. We stydy that hormophism on A is one to one.

1. Introduction

F_pを有限体とし元の個数をp（素数）とする．環$F_p[X_1, \quad ,X_n]$を$(X_1-1)^p \quad (X_n-1)^p$で剰余した環を考える．$e_1=X_1-1, e_2=X_2-1, \quad ,e_n=X_n-1$とおき$A=F_p[X_1 X_2 \quad X_n]/e_1^p \quad e_n^p$とする　Aの中では$e_i^p=0$が成り立つ，Aの minimalideal をE_nとおく．

定理 A

E_nは$e_1^{p-1}e_2^{p-1} \quad e_n^{p-1}$で生成される．

すると次の定理がかんたんに証明できる．

定理 B

Aの中の零イデアルでないイデアルはE_nを必ず含む

環Aから環Aへの自己準同型写像をφとおく．φが1対1の写像になるためには次の定理が成り立てばよい．

定理 C

Aの自己準同型写像φが1対1になるためには$\varphi(E_n)\neq 0$が必要十分条件になる．

定理Cを具体的に$P=3$の場合に行列をつかって書き表した時に定理Cではどんな形になるかをしらべた．$P=3$の時は環Aはコード理論のなかにもよくでてくる環である

2. 定理 A, 定理 B, 定理 C の証明

F_pは有限体で標数pでpは奇素数とする　$F_p[X_1, \quad ,X_n]$をF_p上のn変数の多項式環とする　$e_1=X_1-1, e_2=X_2-1, \quad ,e_n=X_n-1$とおく．

$A=F_p[X_1,\quad,X_n]/e_1^p e_2^p \quad e_n^p$ とおく　$e_i^p=x^p-1$ になる　A のなかの最小イデアルを E_n とおく

定理 A　　E_n は $e_1^{p-1}e_2^{p-1}\quad e_n^{p-1}$ で生成される

証明

$e_1^{p-1}\quad e_n^{p-1}$ で生成されるイデアルを I とおく　I は明らかに零イデアルではなく A でもないのでイテアルをつくる A のなかの零イデアルでなく A でもない任意のイデアルを J とおく　環 A のイデアルは A か主イデアル環になることから J を生成する非正則元 f が 1 コある　非正則元 f は $e_i^j(0<j<p)$ のものしかない　J は e_i^j の形のもので生成される　I の元は $K\quad e_1^{p1}e_2^{p2}\quad e_i^{pi}\quad e_n^{p-1}$ の形になり $L\quad e_i^j$ となるから，$I\subseteq J$ になる J は任意にとれるから I は最小イデアルになる

E_n は最小イデアルだから次の定理 B は明らかになる

定理 B　　A の中の零イデアルでないイデアルは E_n を必ず含む

環 A から環 A への自己準同型写像を φ とおく

定理 C　　A の自己準同型写像 φ が 1 対 1 になるためには $\varphi(E_n)\neq 0$ が必要十分条件になる

証明

φ が 1 対 1 とすると $\ker\varphi=0$ になる　ところで $\ker\varphi$ はイデアルになる．$\ker\varphi\neq 0$ ならば定理 B より $\ker\varphi\supseteq E_n\varphi(E_n)\neq 0$ なら $\ker\varphi$ は零イデアルになり φ は 1 対 1　φ が 1 対 1 なら $\varphi(E_n)\neq 0$ はあきらか

3．$\varphi(E_n)$ について

φ が準同型写像であること使って $\varphi(E_n)$ を計算する　$\varphi(E_n)$ は一般にはつぎのようにかける　ただし K は $(p-1)$ 次以下の多項式

$$\varphi(K\quad e_1^{p-1}\quad e_n^{p-1})$$

φ が準同型であることから $\varphi(K\cdot e_1^{p-1}\quad e_n^{p-1})=K(\varphi(e_1)\quad \varphi(e_n))^{p-1}$ になる　$\varphi(e_i)$ の像を決めれば φ がきまる．$\varphi(e_i)$ を e_1 で剰余しあまりを e_2 で剰余する e_n まで続けることと $\varphi(e_i^p)=0$ になることから $\varphi(e_i)$ は次のようにかける

$$\varphi(e_i)=A_1^i e_1+A_2^i e_2+\quad +A_n^i e_n$$

$(\varphi(e_1)\quad \varphi(e_n))^{p-1}$ を計算する

$$((A_1^1 e_1+\quad +A_n^1 e_n)(A_1^2 e_1+\quad +A_n^2 e_n)\quad (A_1^n e_1+\quad +A_n^n e_n))^{p-1}$$

$$=\Big(\sum_{j1\to j2\ \ \to jn/n} C_{j1j2\ \ jn}\, e_1^{j1}e_2^{j2}\quad e_n^{jn}\Big)^{p-1}$$

ここで $C_{j1j2\ \ jn}$ は A_j^i 達でつくれる多項式になっている　そこで $E^J=e_1^{j1}e_2^{j2}\quad e_n^{jn}$ とおく　ただし $J=(j_1\quad j_n)$ で $\Sigma_i j_i=n$ になる

$$\sum_{s1\to\ \ \to spI\ \ 1/p-1}\frac{(p-1)!}{s_1!\quad s_{p-1}!}(c_{j1\ \ jn})^{s1}\quad (c_{k1\ \ kn})^{spI\ 1}E^{J1s1}\quad E^{JpI\ 1spI\ 1}$$

と書き表せる　行列をつかって書くことにする

$$L=(J_1\ J_2\quad J_l)=\begin{pmatrix} j_1 \\ j_2 \\ \\ j_n \end{pmatrix}$$

とおいてやる　l は展開したときの項の数になる

Eの指数をならべ，最後に$p-1$をつけたしたベクトルを$\alpha=(x_1,\ \ ,x_n,\ p-1)$とおき すなわち各$e_i$の指数が$x_i$になるようにしておく　$\beta=(s_1\ \ s_l)$とおいてやる　そこで行列Lを次のようにおきなおす　n+1行を1でうめる

$$L=\begin{pmatrix} J_1 & J_2 & & J_l & 1 \\ 1 & & & 1 & \end{pmatrix}$$

つぎの関係式がなりたつ.

$$L^t\beta={}^t\alpha$$

Lは$l\times n+1$の行列で$n+1\times n+1$の小行列式は1行からn行までの和が一定であることから0になる　$J=(0,\ \ ,0,n,0,\ \ ,0)$のものが含まれることからrank $L=n$になる.

$L^t\beta={}^t\alpha$を連立方程式とみて解${}^t\beta$が存在するためにはrank$(L\ {}^t\alpha)=n$になるはずであり.

$\begin{pmatrix} & L & \\ 1 & & 1\end{pmatrix}$の縦ベクトル$n$本の一次結合で$\begin{pmatrix} x_1 \\ \\ x_n \\ p-1\end{pmatrix}$がかけることになる

$j_1=(n,0,\ \ ,0,1)$ $j_2=(0,n,0,\ \ ,0,1)$　$j_n=(0,\ \ ,0,n,1)$とLの中からn本一次独立なものを選ぶ

$$y_1{}^t j_1+y_2{}^t j_2+\ \ y_n{}^t j_n={}^t(x_1,x_2,\ \ x_n,p-1)$$

成分ごとにみると$y_i n=x_i$と$y_1+y_2+\ \ +y_n=p-1$で$y_i=x_i/n$になる$0\leqq x_i\leqq p-1$だから$x_i\neq p-1$だと$y_1+y_2+\ \ +y_n=x_1+x_2+\ \ x_n/n\neq p-1$になるから$x_i=p-1$である.

$e_1^{p-1}e_2^{p-1}\ \ e_n^{p-1}$の項しかでてこない

4．$p=3$の場合

$$(A_1^1e_1+A_2^1e_2+\ \ +A_n^1e_n)(A_1^2e_1+A_2^2e_2+\ \ +A_n^2e_n)\ \ (A_1^ne_1+A_2^ne_2+\ \ +A_n^ne_n)$$

$$=\sum_{s1+s2+\ \ +sl=2}\frac{2!}{s_1!s_2!\ \ s_l!}(C_{k1})^{s1}\ \ (C_{kl})^{sl}E^{j1s1}E^{j2s2}\ \ E^{jlsl}$$ C_{ki}のk_iはベクトルである.

$s_1+s_2+\ \ +s_t=2$，$s_i>0$から次の2つのcaseがおこりk_iの形も決定できる

case 1　$s_i=2$で他は0　$k_i=(1111\ \ 1)$になる

case 2　$s_i=s_j=1$他は0　$k_i=(111\ \ 1)$，$k_j=(111\ \ 1)$と$k_i=(1120111\ \ 1)$，$k_j=(110211\ \ 1)$2がでてくる場合の2通りになる　そこで展開式書き直す

$$(A_1^1e_1+A_2^1e_2+\ \ +A_n^1e_n)(A_1^2e_1+A_2^2e_2+\ \ +A_n^2e_n)\ \ (A_1^ne_1+A_2^ne_2+\ \ +A_n^ne_n)$$

$$=\sum C_{j1j2\ \ jn}e^{j1}\ \ e^{jn}$$

case 1の時

$$C_{11\ \ 1}=\sum_{\sigma\in Sn}A_1^{\sigma(1)}A_2^{\sigma(2)}\ \ A_n^{\sigma(n)}$$ S_nはn次の置換の集合

case 2の時

$(2,0,1,\ \ ,1)$ $(0,2,1\ \ 1)$の場合を考えてみる

$$C_{2\,0,1\ \ 1}=\sum_{\sigma\in Sn}A_1^{\sigma(1)}A_1{}^{\sigma(2)}A_3^{\sigma(3)}\ \ A_n^{\sigma(n)}$$

$$C_{0\,2,1\ \ 1}=\sum_{\sigma\in Sn}A_2^{\sigma(1)}A_2^{\sigma(2)}A_3^{\sigma(3)}\ \ A_n^{\sigma(n)}$$

一般に$j_{s1}=j_{s2}=\ \ j_{st}=2$，$j_{r1}=j_{r2}=\ \ j_{rt}=0$ならば

$C_{j1j2\ \ jn}\sum_{\sigma\in Sn} A_{j1}^{\sigma(1)} A_{j1}^{\sigma(2)} A_{j2}^{\sigma(3)} A_{j2}^{\sigma(4)}\ \ A_{jn}^{\sigma(n)}$ になる

そこで行列 A を $A=\begin{pmatrix} A_1^1 & & A_n^1 \\ A_2^1 & & A_n^2 \\ & & \\ A_1^n & & A_n^n \end{pmatrix}$ とおく

$D(A)=\sum_{\sigma\subset Sn} A_1^{\sigma(1)}\ \ A_n^{\sigma(n)}$（$A$ の行列式から－を除いたもの）$A_{(i\ j)(k\ l)}$ で A の j 列を i 列に l 列を k 列に置き換えた行列を表す

case 1 は $D(A)$ になる　case 2 は $D(A_{(s1\ j1)\ \ (sn\ jn)})$ になる
展開式は$D(A)e_1e_2\ \ e_n+\sum_{all\ pairs(i\ j)} D(A_{(i\ j)(k\ l)})e_1\ \ e_i^2\ \ e_n$と表せる　そこで$p=3$ だから２乗を計算する

$$\begin{aligned}&(D(A)e_1e_2\ \ e_n+\sum_{all\ pairs(i\ j)} D(A_{(i\ j)})e_1\ \ \mathrm{e}_i^2\ \ e_n)^2\\ &\quad=\{D(A)^2+\sum_{all\ pairs(i\ j)} D(A_{(i\ j)}D(A_{(j\ i)}\}e_1^2e_2^2\ \ e_n^2\end{aligned}$$

各A_i^j は $a_i^j+F_i^j(e_1\ e_2\ \ e_n)$ $a_i^j\in F$, F_i^j は $e_1\ e_2\ \ e_n$ の多項式の形になる
$D(A)=D(A)+\{e_1\ e_2\ \ e_n$ の多項式$\}$ また $D(A_i^j)D(A_j^i)$ についても同様　たたし行列 A を a_i^j 定数項だけを成分とする行列にとして展開式を書き直す　$A_{i\ j}$ は j 行を i 行に置き換えたものとする

$(D^2(A)+\sum_{all(i\ j)\ (k\ l)} D(A_{(i\ j)\ (k\ l)}D_{(j\ i)\ (l\ k)}+(e_1\ \ e_n$ の多項式$))e_1^2\ \ e_n^2$ となる　そこでつぎの補題が成り立つ

Lemma

φ か一対一となるのは$(D(A)^2+\sum_{all(i\ j)\ (k\ l)} D(A_{(i\ j)\ (l\ l)})\ D(A_{(j\ i)\ (l\ l)}))\neq 0$

$D(A_{(i\ j)\ (l\ l)})\ D(A_{(j\ i)\ (l\ k)})$ を考える.
そこで行列 $A=\{a_1\ \ a_n\}$ と行列 $B=\{b_1\ \ b_n\}$ とおく　ただし $\{a_1\ \ a_n\}$ $\{b_1\ \ b_n\}$ は縦ベクトルとする

$a_i\ b_j=\begin{pmatrix} a_1^i\ b_1^j \\ \\ \mathrm{a}_n^i\ \mathrm{b}_n^j \end{pmatrix}$ とおく
次の式か成り立つ

$$D(A)D(B)=\sum_{\sigma\in Sn}(a_1b_{\sigma(1)}\,a_2b_{\sigma(2)}\ \ a_nb_{\sigma(n)})\ {*}{*}{*}{*}{*}{*}\ (0)$$

証明

$$\begin{aligned}右辺&=\sum_{\sigma\in Sn}\sum_{\gamma\in Sn} a_{\gamma(1)}^1\ b_{\gamma(1)}^{\sigma(1)}\ a_{\gamma(2)}^2\ b_{\gamma(2)}^{\sigma(2)}\ \ a_{\gamma(n)}^n\ b_{\gamma(n)}^{\sigma(n)}\\ &=\sum_{\gamma\subset Sn}(\sum_{\sigma\subset Sn} a_{\gamma(1)}^1\ \mathrm{b}_{\gamma(1)}^{\sigma(1)}\ a_{\gamma(2)}^2\ b_{\gamma(2)}^{\sigma(2)}\ \ a_{\gamma(n)}^n\ b_{\gamma(n)}^{\sigma(n)})\end{aligned}$$

$$= \sum_{\gamma \in Sn} a^1_{\gamma(1)} \quad a^n_{\gamma(n)} \sum_{\sigma \in Sn} b^{\sigma(1)}_{\gamma(1)} \quad b^{\sigma(n)}_{\gamma(n)})$$
$$= \sum_{\gamma \in Sn} a^1_{\gamma(1)} \quad a^n_{\gamma(n)} D(B)$$
$$= D(A)D(B)$$

$$D(A_{(ij)\ (kl)})\ D(A_{(ji)\ (lk)}) \quad ****** \quad (1)$$

(1)を(0)をつかって展開する

$$D(A_{(ij)\ (kl)})\ D(A_{(ji)\ (lk)}) = \sum_{\gamma \in Sn} D(A_{(ij)\ (kl)})\ D(A_{(j\gamma(i))\ (l\gamma(k))})$$

(ij) $(k\ l)$ を置換の元として σ とおく

$$\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$A=(A_1\ A_2\ \ A_n)$ A_i は縦ベクトルを固定しておく．

$\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ $(\forall \sigma \in S_n)$ の j 番目と l 番目の上下を入れ換える操作を U_{jl} とおく

条件 α　上の列下の列に重複する数字が少なくとも1個ある

$\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ $(\forall \sigma \in S_n)$ 上の段が (1) の左の index 下の段が (1) 右の index を示すためには $U_{(ij)\ (kl)}$ で条件 α を満たすように i , j , k , l 存在することである

(0) で展開したとき index は $\gamma \in S_n$ と $U_{i\ \ k}$ が存在して $U_{i\ \ k}$ $\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}'$

と書ける．γ は上下同時に作用する

展開式では下の列に S_n がはたらくので同じものがでてくる．互換としては $(\,i\ \ i\,)$ のものが対応する

$U\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ で条件 α を満たしたものとそれの（上下一致）の置換のものがでてくる

$\begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ で条件 α を満たすような置き換えの個数を数える．その数を N とおく．

σ をサイクルに分ける．$\sum_{i=1}^{n} is_i = n$ 長さ i のものが s_i 個

C^{σ}(k) を置換 σ で重複が k 個で長さ k 以下のサイクルをふくまない個数とする
重複する文字が k 個あれば互換を考えることで 2^k 個でてくる

$$\mathrm{N} = \sum_{k=1}^{n-1} C^{\sigma}(k)2^k$$

Lemma

$$\sum_{k=1}^{n-1} C^{\sigma}(k)x^k = (1+2x)^{s_2}(1+3x+3x^2)^{s_3} \quad (1+\sum_{i}^{n-1}\binom{n}{i}x^i)^{s_n} - 1$$

証明

$n=2, s_2=1$ の時（1 1）と（2 2）の2個だけで $1+2x$ になる

$s_2=0$ の時0になる

$G_n^- = (1+2x)^{s_2} \quad (1+\sum \binom{n}{i} x^i)^{s_n}$ π はある置換で s_i はサイクルの分解とおく

$n-1$ まで成り立つとする

$s_n=1$ ならば $s_i=0$ で $1+\binom{n}{1}x+\binom{n}{2}x^2 \quad +\binom{n}{n-1}x^{n-1}$ n個をとらないとり方

$s_n=0$, $s_1 \neq 0$ の時1個はずすと $n-1$ になる仮定から成り立つ

$s_n=0$, $s_1=0$ の時 $\min\{j \mid s_j \neq 0\}=k$ として $\pi^* = (s_k-1, \quad , sn-k)$ を考えれば $G_n^- = (1+\binom{k}{1}x+ \quad +\binom{k}{k+1}x^{k-1})\ G_{n-k}^{-*}$ がなりたちすべての n でなりたつ　右辺は $((1+x)^i-x^i)^{s_i}$ の形になる

上の式で $x=2$ としてやると $N=\sum_k C(k)2^k=\prod_{i=1}^{i=n}((1+2)^i-2)^{s_i}$ になる　mod 3で考えると次の式が成り立つ

$$N=\sum_{k=2}^{n-1} C^\sigma(k)2^k \equiv (-1)^{s_2+ \quad +(n-1)s_n}-1 \pmod 3$$

次の命題が成り立つ

定理

$(1, \sigma(1)) \quad (n, \sigma(n))$ の index を持つものは F_3 の係数では σ が奇置換ならは1で σ が偶置換ならば0になる

そこで上の結果使って計算する

定理

$$\sum_{all(i\ j)\ (k\ l)} D(A_{(i\ j)\ \ (k\ l)})\ D(A_{(j\ i)\ \ (l\ k)}) = 2D^+(A)D^-(A)$$

ただし $D^+(A)$ は偶置換の和 $D^-(A)$ は奇置換の和

証明

左辺の展開には奇置換しかでてこないから奇置換の集合を B_n とおき $C_n=S_n-B_n$ とする

左辺 $=\sum_{\sigma\in C_n} D(A_1\ A_{\sigma(1)}\ A_2\ A_{\sigma(2)} \quad A_n\ A_{\sigma(n)})$

$=\sum_{\sigma\in C_n}\sum_{\gamma\in S_n} a^1_{\gamma(1)}\ a^{\sigma(1)}_{\gamma(1)}\ a^2_{\gamma(2)}\ a^{\sigma(2)}_{\gamma(2)}\ a^n_{\gamma(n)}\ a^{\sigma(n)}_{\gamma(n)}$

$=\sum_{\sigma\in C_n}\sum_{\gamma\in S_n} a^1_{\gamma(1)}\ a^2_{\gamma(2)} \quad a^n_{\gamma(n)}\ a^{\sigma(1)}_{\gamma(1)} \quad a^{\sigma(n)}_{\gamma(n)}$

$=\sum_{\sigma\in C_n}\sum_{\gamma\in S_n} a^1_{\gamma(1)}\ a^2_{\gamma(2)}\ a^n_{\gamma(n)}\ a^1_{\gamma\sigma^{-1}(1)} \quad a^n_{\gamma\sigma^{-1}(n)}$

$=\sum_{\gamma\in B_n}\sum_{\sigma\in C_n} a^1_{\gamma(1)}\ a^2_{\gamma(2)}\ a^n_{\gamma(n)}\ a^1_{\gamma\sigma^{-1}(1)} \quad a^n_{\gamma\sigma^{-1}(n)} + \sum_{\gamma\in C_n}\sum_{\sigma\in C_n} a^1_{\gamma(1)} \quad a^n_{\gamma(n)}\ a^{\sigma(1)}_{\gamma(1)} \quad a^{\sigma(n)}_{\gamma(n)}$

$=D^+(A)\ D^-(A)+D^-(A)\ D^+(A)$

$=2D^+(A)\ D^-(A)$

簡単な計算で mod 3では $(\det(A))^2=D(A)^2+2D^+(A)D^-(A)$ がなりたつ　そこでつぎの事が成り立つ

命題

$$D^2(A)+\sum_{(i\ j)\ (k\ l)} D(A_{(i\ j)\ (k\ l)})\ D(A_{(j\ i)\ (l\ k)})=D^2(A)+2D^{+}(A)\ D^{-}(A)=(\det(A))^2$$

命題

φが１対１のためには$\varphi(e_i)=A_1^i e_1+A_2^i e_2 \quad A_n^i e_n$の定数項のつくる行列（$A_i^k$）の行列式が０でない

参考文献

１）成田政雄　イデアル論入門，共立全書（1973）

２）ヴェラプレス　符号理論入門，ワィリージャパン（1984）