数理解析研究所講究録
608巻 1987年 139-151

$k[x]$ の k-form と additive group

富山大教育　浅沼照雄 (Teruo Asanuma)

k を体とするとき $k^{[n]}$ で n 変数多項式環を表わす。k-代数 A が $k^{[n]}$ の k-form であるとは有限次代数拡大 K/k が存在して $K\otimes A\cong K^{[n]}$ なることである。K/k が separable (resp. purely inseparable) にとれるとき separable (resp. purely inseparable) k-form という。$n=1,2$ のとき $k^{[n]}$ の sep. k-form は trivial すなわち $A\cong k^{[n]}$ ($n=1,2$) である。$n>2$ のときは不明。

さて k の標数を $p>0$ として K を含む normal field を K_1 とすると k と K_1 の中間体 K_2 が存在して K_1/K_2 : sep. ex. K_2/k : purely insep. ex. とできる。

$$K_1\otimes_{K_2}K_2\otimes_k A=K_1\otimes_K K\otimes_k A\cong K_1^{[n]}$$

であるから $K_2\otimes_k A$ は sep. K_2-form である。そこでとくに $n=1,2$ のときは nontrivial k-form A はすべて purely insep. となる。このノートでは purely insep. k-form A の structure を調べたい。とくに $n=1$ のときすなわち $k[x]:=k^{[1]}$ の k-form について述べる。

以下 k を標数 $p>0$ の体，$k^{[n]}=k[x_1,\dots,x_n]$ とする。$f_1,\dots,f_n\in k^{[n]}$ の Jacobian $\det(\partial f_i/\partial x_j)$ を $J(f_1,\dots,f_n)$ で表わす。

1. 定理．$J(f_1,\dots,f_n)\neq 0$ ならば任意の整数 $e\geq 0$ について

$$k[x_1^{p^e},\dots,x_n^{p^e}, f_1,\dots,f_n, J(f_1,\dots,f_n)^{-p^e}]\ni x_i$$

for all $i=1,\dots,n$.

証明のアウトライン．$k[x_1^{p^e},\dots,x_n^{p^e}]=R$ とおく。すると $k^{[n]}$ は free R-module．k を代数的閉体と仮定できる。いま $a=(a_1,\dots,a_n)\in k^n$ を $D(J(f_1,\dots,f_n))=k^n-V(J(f_1,\dots,f_n))$ とする。すなわち a は $J(f_1,\dots,f_n)$ の零点ではないとする。$y_i=x_i-a_i$ とおく。$f_i(x_1,\dots,x_n)=f_i(y_1+a_1,\dots,y_n+a_n)$ の $y_1,\dots,y_n$ についての1次の homogeneous form を $b_{i1}y_1+\dots+b_{in}y_n$ $(b_{ij}\in k)$ とすると $f_i(y_1+a_1,\dots,y_n+a_n)$ をテーラー展開することにより matrix (b_{ij}) は Jacobian matrix $(\partial f_i/\partial x_j)$ に $x_1=a_1,\dots,x_n=a_n$ を代入したものに等しい。$a\in D(J(f_1,\dots,f_n))$ であるから $(b_{ij})=(\partial f_i/\partial x_j)$ は invertible。ゆえ

$$k[y_1,\dots,y_n]/(y_1^{p^e},\dots,y_n^{p^e})=k[\bar{y}_1,\dots,\bar{y}_n]$$

とおくと $\bar{R}[\bar{f}_1,\dots,\bar{f}_n]=k[\bar{y}_1,\dots,\bar{y}_n]$ がなりたつ。ここで $^-$ は residual class modulo $(y_1^{p^e},\dots,y_n^{p^e})$ を表わす。ゆえに

$$R[f_1,\dots,f_n]+(y_1^{p^e},\dots,y_n^{p^e})=k[y_1,\dots,y_n].$$

いま $\mathfrak{m}_a$ を $y_1^{p^e},\dots,y_n^{p^e}$ で生成されたRの max. ideal とすると中山の補題より $R_{\mathfrak{m}_a}[f_1,\dots,f_n]=R_{\mathfrak{m}_a}[y_1,\dots,y_n]$。ゆえ

$$\bigcap_{a\in D} R_{\mathfrak{m}_a}[f_1,\dots,f_n]=\bigcap_{a\in D} R_{\mathfrak{m}_a}[y_1,\dots,y_n]$$

ここで $D=D(J(f_1,\dots,f_n))$。また

$$\bigcap_{a\in D} R_{\mathfrak{m}_a}=R[J(f_1,\dots,f_n)^{-p^e}]$$

であるから

$$R[f_1,\dots,f_n,J(f_1,\dots,f_n)^{-p^e}]=k[x_1,\dots,x_n,J(f_1,\dots,f_n)^{-p^e}]$$

である。 q.e.d.

$g_1,\dots,g_m\in k^{[n]}$ とする。$\{J(g_{\lambda_1},\dots,g_{\lambda_n})\mid 1\leq\lambda_i\leq m\}$ で生成された $k^{[n]}$ の ideal を $g_1,\dots,g_m$ についての Jacobian ideal といい $I(g_1,\dots,g_m)$ で表わす。

2.系. $k[x_1^{p^e},\dots,x_n^{p^e},g_1,\dots,g_m]=k[x_1,\dots,x_n]$ なるための必要十分条件は $I(g_1,\dots,g_m)=(1)$.

k-代数 B を次のようにおく。

$$B=k[x_1^{p^e},\dots,x_n^{p^e},f_1,\dots,f_n,J(f_1,\dots,f_n)^{-p^e}]\cap k^{p^{-e}}[x_1,\dots,x_n]$$

Bは明らかに $k[x_1^{p^e},\dots,x_n^{p^e}]$-代数である。このBが property P をみたすとは $g_1,\dots,g_m\in B$ が存在して $k^{p^{-e}}[x_1,\dots,x_n]$ における $g_1,\dots,g_m$ の Jacobian ideal が unit ideal なることをいう。

Aが$k^{[n]}$の purely insep k-form であるときあるeについて $k^{p^{-e}} \otimes A \cong k^{p^{-e}}[x_1, \dots, x_n]$ がなりたつ。このようなeの最小のものをAの height といい $ht\,A = e$ で表わす。

以下Aは$ht\,A = e$なる$k^{[n]}$の purely insep. k-form を表わすことにする。

3. 定理. Bが $ht\,B \leq e$ なる purely insep k-form なるための必要十分条件は property P をみたすことである。またAはつねに property P をみたすBに同型である。ゆえとくに $A \cong k[x_1^{p^e}, \dots, x_n^{p^e}, g_1, \dots, g_m]$ ここでg_iは上で定義したもの。

定理3よりAの structure は $g_1, \dots, g_m$ によってきまる。$n > 1$ のときこのようなg_iを一般的に与えるのは非常に困難である。

4. 系. $g_1, \dots, g_n \in k^{p^{-e}}[x_1, \dots, x_n]$ で $J(g_1, \dots, g_n) \in k^{p^{-e}} \setminus (0)$ とする。すると

$$A = k[x_1^{p^e}, \dots, x_n^{p^e}, g_1, \dots, g_n]$$

は $ht\,A \leq e$ なる purely insep. k-form でその differential A-module $\Omega_k(A)$ は free である。

問題. 系4の逆がなりたつか? すなわち $\Omega_k(A)$ が free なる $ht\,A = e$ の k-form A は上の $k[x_1^{p^e}, \dots, x_n^{p^e}, g_1, \dots, g_n]$ に同型になるか?

この問題について$n=1$の場合はのちにみるようになりたつ。また$n=2$, $p=2$, $\mathrm{ht}A=1$ の3条件を同時にみたすAについてはなりたつ。これ以外は不明.

さて $n=1$ のときすなわち $k[x]:=k^{[1]}$ の purely insep k-form A の structure を考えてみる。このときは $f\in k[x]$ について $J(f)=\partial f/\partial x=f'$, つまり $J(f)$ は x による微分であるから定理3より

$$A=k[x^{p^e}, f, (f')^{-p^e}]\cap k^{p^{-e}}[x]$$

としおいてこのAが property P をみたすとしてよい。つまり $A\ni g_1,\cdots,g_m$ が存在して $I(g_1,\cdots,g_m)=(1)=k^{p^{-e}}[x]$.
明らかに $I(g_1,\cdots,g_m)$ は $g_1',\cdots,g_m'$ で生成された ideal であるから $g.c.d.(g_1',\cdots,g_m')=1$ となる。再び定理3より
$A=k[x^{p^e}, g_1,\cdots,g_m]$ と表わせるが とくに $m=2$ とできる。
つまり Aは algebraic space curve の座標環である。まとめて

5.系. $k[x]$ の k-form は $k[x^{p^e}, g_1, g_2]$ と表わされる。ここに g_1, g_2 は $k[x^{p^e}, f, (f')^{-p^e}]\cap k^{p^{-e}}[x]$ の元で互いに素なるものである。逆にこのような環 $k[x^{p^e}, g_1, g_2]$ は k-form である。

この系5によってAの structure は g_1, g_2 による。まず $g_2=0$ のときを考てみる。このときは $g'\in k^{p^{-e}}\setminus(0)$ ゆえ

$$g_1 = a_0 + cx + a_1x^p + \cdots + a_n x^{np} \quad (a_i \in k^{p^{-e}},\ c \in k^{p^{-e}} \setminus (0))$$

と表わされる。cx をあらたに x とおくことによってはじめから $c = 1$ としてよい。つまり

$$A = k[x^{p^e}, a_0 + x + a_1x^p + \cdots + a_n x^{np}] \quad (a_i \in k^{p^{-e}})$$

となる。このような form を p-polynomial type という。

6. 系. $k[x]$ の k-form についてその differential module が free ならば p-polynomial type である。

7. 系 $k[x]$ の k-form が U.F.D ならば p-polynomial type である。

8. 系 (Kambayashi - Miyanishi - Takeuchi) $k[x]$ の k-form が U.F.D かつ rational prime ideal $\mathfrak{p}$ (i.e. $A/\mathfrak{p} = k$ なる k-form A の prime ideal $\mathfrak{p}$) が存在すれば trivial である。

A に代数群の structure が入っているとする。つまり A はホップ代数とすると $\Omega_k(A)$ は free. ゆえ系6より p-polynomial type である。このことから

9. 系. (Russell) A がホップ代数の structure をもてば $A \cong k[x^{p^e}, x + a_1x^p + \cdots + a_s x^{p^s}]$ $(a_i \in k^{p^{-e}})$.

次に $\Omega_k(A)$ がかならずしも free でない場合を考える。まず A の quotient field $Q(A)$ が rational field のときは

10. 系. $Q(A) \cong k(x)$ とすると

$$A \cong k[x^{p^e}, x^{p^e-1}(1+ax), x(1+ax)^{p^e-1}] \quad (a \in k^{p^{-e}})$$

さらに $\Omega_k(A)$ が free かつ $A \not\cong k[x]$ とすると $p=2$ で

$$A \cong k[x^2, x+ax^2] \quad (a \in k^{\frac{1}{2}} \setminus k)$$

系10において $x^{p^e}, x^{p^e-1}(1+ax), x(1+ax)^{p^e-1}$ をパラメータとする space curve はのちに述べるように set theoritic complete intersection である。しかし $p=2$ かつ $e=1$ 以外のときは一般的に ideal theoritic complete intersection とはならない。

$Q(A)$ がかならずしも rational field でないときを考える。$e \geq 2$ のときはきわめて複雑になるので $e=1$ のときのみを以下であつかう。ゆえこれからは $ht\, A \leq 1$ とする。ゆえ $A = k[x^p, f, (f')^{-p}] \cap k^{p^{-1}}[x] = k[x^p, g_1, \dots, g_m] = k[x^p, g_1, g_2]$ で g_1, g_2 は互いに素となっている。g_1, g_2 を f から求めてみよう。

$f' = \varphi_1^{\lambda_1} \dots \varphi_n^{\lambda_n}$ を $k^{p^{-1}}[x]$ での既約分解とする。任意の $G \in k^{p^{-1}}[x]$ が $G \in A$ なるための必要十分条件は

$$G \varphi_1^{\nu_1 p} \dots \varphi_n^{\nu_n p} = \alpha_0 + \alpha_1 f + \dots + \alpha_{p-1} f^{p-1} \quad (\alpha_i \in k[x^p]) \dots (*)$$

と表わせることである。もし $\varphi_i^p \mid \alpha_j \ (j=1, \dots, p-1)$ ならば $\alpha_j / \varphi_i^p \in k[x^p]$ であるから最初から φ_i^p は $\alpha_1, \dots, \alpha_{p-1}$ の公約元

でないと仮定してよい。$\bar{k}$をkの代数閉包として$a_i \in \bar{k}$をφ_iの1つの根とする。そこで

$$t_i = [\,k(a_i^p) : k(a_i^p, f(a_i))\,]$$

とおくと　$f(a_i) \in k^{p^{-1}}(a_i)$ より $f(a_i)^p \in k(a_i)$ ゆえ $t_i \leq p$.
そこで $t_i = p$ とする。すると $\nu_i = 0$。なぜならば $\nu_i > 0$ とすると (*) の両辺に a_iを代入して

$$0 = \alpha_0(a_i) + \alpha_1(a_i) f(a_i) + \cdots + \alpha_{p-1}(a_i) f(a_i)^{p-1}$$

ゆえ $\alpha_j(a_i) = 0$ $(j = 1, \cdots, p-1)$ となるがこれは φ_i^p は $\alpha_1, \cdots, \alpha_{p-1}$ の公約元ではないという仮定に矛盾する。ゆえ $\nu_i = 0$。そこで (*) の両辺を xで微分して

$$G' \varphi_1^{\nu_1 p} \cdots \varphi_n^{\nu_n p} = (\alpha_1 + 2\alpha_2 f + \cdots + (p-1)\alpha_{p-1} f^{p-2}) f'.$$

ゆえに $\varphi_i^p \mid G' \varphi_1^{\nu_1 p} \cdots \varphi_n^{\nu_n p}$。ところで $\nu_i = 0$ かつ $\varphi_i \nmid \varphi_j$ $(i \neq j)$ より $\varphi_i^p \mid G'$ でなければならない。とくに $\varphi_i^p \mid g_j'$ (for all $j = 1, \cdots, m$) これは g.c.d.$(g_1', \cdots, g_m')$ に矛盾する。つまり t_iは 1 である。
ゆえ $h_i(x^p) \in k[x^p]$ が存在して $h_i(a_i^p) = f(a_i)$ とおける。剰余定理より $h(x^p) \in k[x^p]$ をうまくとって $h(x^p) \equiv f(x) \pmod{\varphi_i}$ とできる。fを$f - h$ とおきかえることによって初めから $\varphi_i \mid f$ と仮定してよい。つまり $f = \varphi_0 \varphi_1^{\sigma_1} \cdots \varphi_n^{\sigma_n}$ と表わせる。
ここで φ_0は φ_i $(i = 1, \cdots, n)$ と互いに素な $k^{p^{-1}}[x]$ の元である。
そこで $f' = \varphi_1^{\lambda_1} \cdots \varphi_n^{\lambda_n}$ の λ_iが p 以上ならばあきらかに $\sigma_i \geq p$。また $A = k[x^p, f, \varphi_1^{-p}, \ldots, \varphi_n^{-p}] \cap k^{p^{-1}}[x]$

であるから $A = k[x^p, f\varphi_i^{-p}, \varphi_1^{-p}, \ldots, \varphi_n^{-p}] \cap k^{p^{-1}}[x]$。ゆえ f を $f\varphi_i^{-p}$ でおきかえることができる。これを繰り返して最初から $1 \le \lambda_i < p$ と仮定してよい。ゆえ $1 < \sigma_i < p$ である。ここで任意の整数 σ に対して $0 \le \bar{\sigma} < p$, $\bar{\sigma} \equiv \sigma \pmod{p}$ とおく。さらに $f^{\bar{i}} = \varphi_0^{i}\varphi_1^{\overline{i\sigma_1}}\cdots\varphi_n^{\overline{i\sigma_n}}$ とおくと明らかに

$$A \supset k[x^p, f, f^{\bar{2}}, \ldots, f^{\overline{p-1}}]$$

がなりたつ。この右辺は $1, f, f^{\bar{2}}, \ldots, f^{\overline{p-1}}$ を basis とする free $k[x^p]$-module である。ゆえ任意の $G \in k^{p^{-1}}[x]$ が $G \in A$ なるための条件は (*) のときと同様に

$$G\varphi_1^{\nu_1 p}\cdots\varphi_n^{\nu_n p} = \alpha_0 + \alpha_1 f + \alpha_2 f^{\bar{2}} + \cdots + \alpha_{p-1} f^{\overline{p-1}} \quad (\alpha_i \in k^p[x^p]) \quad (**)$$

ここで $\varphi_i^p \nmid \mathrm{g.c.d.}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$ と表わせることである。整数 j に対して $0 < j^* < p$ で j の modulo p における逆元を表わすことにすると $\overline{j i^* i} = \bar{j}$。ゆえ $0 \le j \le p-1$ に対して $\mu_j = \overline{j i^*}$ とおくと $\{\mu_0, \ldots, \mu_{p-1}\} = \{0, 1, \ldots, p-1\}$。仮定より $\varphi_i^p | \alpha_0, \ldots, \varphi_i^p | \alpha_{\mu_{j-1}}$, $\varphi_i^p \nmid \alpha_{\mu_j}$ とできる。ゆえ (**) において $\alpha_t f^{\bar{t}}$ は $t = \mu_j$ 以外は φ^{j+1} でわれて $t = \mu_j$ のときは φ^{j+1} でわれない。これは $\nu_i = 0$ であることを示している。すなわち $A = k[x^p, f, f^{\bar{2}}, \ldots, f^{\overline{p-1}}]$. さらに

$$\mathrm{g.c.d.}(f', f^{\bar{2}\prime}, \ldots, f^{\overline{p-1}\prime}) = \sum_{i=1}^{p-1} \sigma_i \varphi_0\cdots\varphi_{i-1}\varphi_i'\varphi_{i+1}\cdots\varphi_{p-1}$$
$$= a \in k^{p^{-1}} \setminus (0) \quad (\sigma_0 = 1)$$

でなければならない。ここで $f_1 = \varphi_0$, $f_2 = \prod_{\sigma_i = 2} \varphi_i, \ldots,$

$f_{p-1} = \prod_{\sigma_i = p-1} \varphi_i$ とおくと f_i は $k^{p-1}[x]$ で square free で $f = f_1 \cdots f_{p-1}^{p-1}$ かつ $\sum_{i=1}^{p-1} i f_1 f_2 \cdots f_{i-1} f_i' f_{i+1} \cdots f_{p-1} = a \in k^{p-1} \setminus (0)$ がなりたつ。以上より次の定理を得る。

11.定理. $f, \overline{f^2}, \cdots, \overline{f^{p-1}}$ を上のものとする。このとき $k[x^p, f, \overline{f^2}, \cdots, \overline{f^{p-1}}]$ は height が 1 以下の k-form である。逆に height が 1 の $k[x]$ の k-form はこの環に同型になる。さらに $k[x^p, f, \overline{f^2}, \cdots, \overline{f^{p-1}}] = k[x^p, f, \overline{f^2} + \cdots + \overline{f^{p-1}}]$ がなりたつ。

いま上の $\overline{f^2} + \cdots + \overline{f^{p-1}}$ を g とおいて $\varphi(X) = x^p$, $\varphi(Y) = f$, $\varphi(Z) = g$ で定義された natural map $\varphi : k[X, Y, Z] \to k[x^p, f, g]$ を考える。この kernel を $\mathfrak{P}$ とすると

$$\mathfrak{P} = \sqrt{(Y^p + f^p(X),\ Z^p + g^p(X))}$$

である。ここで $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ について $f^p(X) = a_0^p + a_1^p X + \cdots + a_n^p X^n$ とする。$g^p(X)$ も同様。前にも述べたように $p \neq 2$ のとき $\mathfrak{P}$ はかならずしも ideal theoritic に complete intersection にならない。ゆえ定理11をいいかえて

12.定理. A が $ht A \leq 1$ なる $k[x]$ の k-form なるための必要十分条件は $A \cong k[X, Y, Z]/\mathfrak{P}$。ここで $\mathfrak{P}$ は上のように定義されたものである。

定理11,12 によって $ht A = 1$ なる k-form A の structure は上の $f_1, \cdots, f_{p-1}$ を与えることによってきまる。

まず $p=2$ のときを考える。このときは定理11よりただちに

$$A = k[X, Y]/(Y^p + a_0^p + X + a_1^p X^p + \cdots + a_n^p X^{np}) \quad (a_i \in k^{p^{-1}}).$$

ゆえ $\Omega_k(A)$ はつねに free.

$p=3$ のとき。　$A = k[x^p, f_1 f_2^2, f_1^2 f_2]$ で

$$f_1' f_2 + 2 f_1 f_2' = f_1' f_2 - f_1 f_2' = a \in k^{p^{-1}} \setminus (0)$$ となる。まず

$$f_1 = \alpha_0 + \alpha_1 x + \alpha_2 x^2, \quad f_2 = \beta_0 + \beta_1 x + \beta_2 x^2$$

ここで $\alpha_i, \beta_i \in k^{p^{-1}}[x^p]$, と表わせる。

$$k^{p^{-1}}[x^p] + k^{p^{-1}}[x^p] f_1 f_2^2 + k^{p^{-1}}[x^p] f_1^2 f_2 = k^{p^{-1}}[x^p] + k^{p^{-1}}[x^p]x + k^{p^{-1}}[x^p]x^2$$

ゆえこの両辺を x で微分して

$$k^{p^{-1}}[x^p] f_2 + k^{p^{-1}}[x^p] f_1 = k^{p^{-1}}[x^p] + k^{p^{-1}}[x^p] x.$$

ゆえ $\alpha_2 = \beta_2 = 0$, $\alpha_1 \beta_0 - \alpha_0 \beta_1 \in k^{p^{-1}} \setminus (0)$ となる。一方このような α_i, β_i に対して $((\alpha_0 + \alpha_1 x)(\beta_0 + \beta_1 x)^2)' = \alpha_1 \beta_0 - \alpha_0 \beta_1$ がなりたつから

$$A = k[x^p, (\alpha_0 + \alpha_1 x)(\beta_0 + \beta_1 x)^2, (\alpha_0 + \alpha_1 x)^2 (\beta_0 + \beta_1 x)]$$

である。

$p \geq 5$ のとき。　このときは $p=2, 3$ にくらべて複雑になるが $f_1, \cdots, f_{p-1}$ を具体的に求めることができる。以下それについて述べる。まず $(f_1 f_2^2 \cdots f_{p-1}^{p-1})' = f_2 f_3^2 \cdots f_{p-1}^{p-2}$ であるから

$$f_2 f_3^2 \cdots f_{p-1}^{p-2} = \alpha_0 + \alpha_1 x + \cdots + \alpha_{p-2} x^{p-2}, \quad (\alpha_i \in k^{p^{-1}}[x^p])$$

をみたさなくてはならない。このような $f_2, \cdots, f_{p-1}$ に対して f_1 を与えればよい。まず

$$\Phi = \alpha_0 x + \frac{1}{2}\alpha_1 x^2 + \cdots + \frac{1}{p-1}\alpha_{p-1} x^{p-1}$$

とおく。$\Phi' = f_2 f_3^2 \cdots f_{p-1}^{p-2}$ に注意する。f_i は square free であるから $f_i = \varphi_{i1} \cdots \varphi_{i\lambda_i}$ と $k^{p^{-1}}[x]$ で既約分解できる。a_{ij} を φ_{ij} の1つの根とすると $k^{p^{-1}}(a_{ij})/k^{p^{-1}}$ は sep. なぜならば insep. とするとどのような f_1 をえらんでも $\sum i f_1 \cdots f_{i-1} f_i' f_{i+1} \cdots f_{p-1}$ は unit にならない。ゆえに $k^{p^{-1}}(a_{ij}^p) = k^{p^{-1}}(a_{ij})$，すなわち $h_{ij} \in k^{p^{-1}}[x^p]$ が存在して $\Phi \equiv h_{ij} \pmod{\varphi_{ij}}$、剰余定理より $h \in k^{p^{-1}}[x^p]$ をうまくえらんで $\Phi \equiv h \pmod{\varphi_{ij}}$ $(i = 1, \cdots, p-1,\ j = 1, \cdots, \lambda_i)$ とできる。すなわち $f_2 f_3 \cdots f_{p-1} \mid \Phi - h$ がなりたつ。そこで $(\Phi - h)' = \Phi' = f_2 f_3^2 \cdots f_{p-1}^{p-2}$ に注意すれば $f_2^2 f_3^3 \cdots f_{p-1}^{p-1} \mid \Phi - h$ であるから $f_1 = (\Phi - h) f_2^{-2} f_3^{-2} \cdots f_{p-1}^{-p+1} a$ $(a \in k^{p^{-1}} \setminus \{0\})$ とおけば f_1 が求めるものである。逆に任意の $f_1, \cdots, f_{p-1}$ はすべてこの方法で求めることができる。

$P = 5$ のときこのようにして一つの例をつくってみる。まず $\pi \in k^{p^{-1}} \setminus k$ とする。そこで

$$f_2 = x + a,\quad f_3 = x + \pi,\quad f_4 = x \qquad (a \in k^{p^{-1}})$$

なる場合を考えてみよう。

$$f_2 f_3^2 f_4^3 = (x+a)(x+\pi)^2 x^3$$
$$= x^6 + (2\pi + a)x^5 + (\pi^2 + 2\pi a)x^4 + a\pi^2 x^3$$

f_1が存在するためには $p-1=4$ 次の係数が 0 でなければならないから $a=2\pi$。これ以外の a の値では f_1 が存在しない。
ゆえ

$$f_2 f_3^2 f_4^3 = x^6 - \pi x^5 + 2\pi^3 x^3$$

そこで

$$\Phi = 3x^7 - \pi x^6 + 3\pi^3 x^4$$

となる。 $\Phi(-2\pi)=0$, $\Phi(-\pi) = -\pi^7$, $\Phi(0)=0$。 $h \in k^{p^{-1}}[x^5]$ は $h \equiv 0 \pmod{f_2}$, $h \equiv -\pi^7 \pmod{f_3}$, $h \equiv 0 \pmod{f_4}$ なるように選ぶ。たとえば $h = \pi^{-3}x^5(x+2\pi)^5$ はこれをみたす。ゆえ $f_1 = (\Phi - h)/f_2^2 f_3^3 f_4^4$ とすればよい。
これを具体的に求めると $f_1 = -\pi^{-3}(x-2\pi)$ である。
ゆえ

$$\begin{aligned} k[x^5,\ & \pi^{-3}(x-2\pi)(x+2\pi)^2(x+\pi)^3 x^4, \\ & \pi^{-1}(x-2\pi)^2(x+2\pi)^4(x+\pi)x^3, \\ & \pi^{-4}(x-2\pi)^3(x+2\pi)(x+\pi)^4 x^2, \\ & \pi^{-2}(x-2\pi)^4(x+2\pi)(x+\pi)^2 x\ ] \end{aligned}$$

は k-form である。

文献

T. Asanuma, *Purely inseparable forms of polynomial rings*, preprint.