A note on p-basis of a polynomial ring defined over a non perfect field

Shigenori Terashima*

1 Introduction

In this paper, letting p be a prime number, we consider rings defined over a prime field $\mathbb{F}_p$. We shall study the existence of a p-basis of a ring A over B, where B is an intermediate ring of A and A^p. Here A^p denotes the image of A by the Frobenius map. The sequence $A \supsetneq B \supsetneq A^p$ is said to be a Frobenius Sandwitch.

If A has a p-basis over B and B has a p-basis over A^p, then we say that the Frobenius Sandwitch has a p-basis.

When A is a regular local ring and B is also a regular local ring, the existence of a p-basis of the Frobenius Sandwitch was proved by T.Kimura and H.Niitsuma[3], which had been conjectured by E.Kunz.

When A is a polynomial ring $k[x_1, x_2]$ over k, k is a perfect field and B is the middle ring of the Frobenius Sandwitch which is written as $k[y_1, y_2]$, the existence was also proved by T.Kimura and H.Niitsuma[5].

Here, we shall prove the existence of a p-basis of the Frobenius Sandwitch $A \supsetneq B \supsetneq A^p$ in the case where $A = k[x_1, x_2], B = k'[y_1, y_2]$ and $A^p = k^p[x_1^p, x_2^p]$, k being a field, k' being an interemediate field between k and k^p, and x_1 and x_2 being algebraically independent over k. Namely, we obtain the following result:

Main Theorem

Let k be a field of characteristic $p > 0$. Let $A = k[x_1, x_2], A' = k'[x_1, x_2], B = k'[y_1, y_2]$ and $A^p = k^p[x_1^p, x_2^p]$ which are the polynomial rings over k in two variables such that $A \supsetneq B \supsetneq A^p$. Assume that $y_1, y_2 \in k'[x_1, x_2]$, $x_1^p, x_2^p \in k'^p[y_1, y_2]$ and $[\Phi(A') : \Phi(B)] = p$. Then, there exists a p-basis of the Frobenius Sandwitch.

Here, $\Phi(A)$ denotes the field of fractions of an integral domain A.
Note that the above result is a generalization of the following Theorem[5].

Theorem[5]

Let k be a perfect field of characteristic $p > 0$. Let $A = k[x_1, x_2], B = k[y_1, y_2]$ and $A^p = k[x_1^p, x_2^p]$ which are the polynomial rings over k in two variables such that $A \supsetneq B \supsetneq A^p$. Assume that $[\Phi(A) : \Phi(B)] = p$. Then, there exists a p-basis of the Frobenius Sandwitch.

* Associate Professor, Tokyo Polytechnic University.
Received Oct. 3, 2006

2 Preliminaries

We use the notion of the Galois extension of rings introduced by S.Yuan[6].

Definition 2.1
Let D be a ring of characteristic p. When a D-algebra C satisfies the following conditions, C is said to be a Galois extension of D.

(1) C is finitely generated and projective as a D-module,

(2) $t^p \in D$ for all $t \in C$,

(3) for any prime ideal P in C, C_P admits a p-basis over D_Q, where $Q = P \cap D$.

Theorem 2.2 (Yuan[6])
Let C be a Galois extension of A. Then the following three conditions hold.

(1) $Der_A(C)$ is finitely generated as a C-module.

(2) $A = \{t \in C | dt = 0, {}^\forall d \in Der_A(C)\}$.

(3) $Hom_A(C, C) = C[Der_A(C)]$.

Here, $\mathrm{Der}_A(C)$ is the set of derivations of C over A, and $C[\mathrm{Der}_A(C)]$ is the ring generated by $Der_A(C)$ over C.

Theorem 2.3 (Yuan[6])
Let $C \supset D \supset E$ be a tower of rings such that C is a Galois extension over E and also over D. Then

(1) D is a Galois extension over E.

(2) $d \in Der_E(D)$ is uniquely extended to $\tilde{d} \in Der_E(C)$.

(3) Let $G_E(D)$ be the set of the extensions by (2) from the members of $Der_E(D)$. Then

$$Der_E(C) = C \cdot G_E(D) \oplus Der_D(C).$$

We also use the following theorem[1, p.116].

Theorem 2.4
Let P be an A-module, and n a non-negative integer. Then the following conditions are equivalent.

(1) P is a projective module of rank n.

(2) P is finitely generated as an A-module and for any maximal ideal $\mathfrak{m}$ of A, $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of rank n.

(3) P is finitely generated as an A-module and for any prime ideal $\mathfrak{p}$ of A, $P_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank n.

(4) For any maximal ideal $\mathfrak{m}$ of A, there exists $f \in A \setminus \mathfrak{m}$ such that P_f is a free A_f-module of rank n.

Note the following theorem[2, p257].

Theorem 2.5
Let A be a ring of characteristic p and x an element of A. Suppose $D \in Der(A)$ satisfies $Dx = 1$ and $D^p = 0$; $A_0 = \{a \in A | Da = 0\}$. Then A is a free module over A_0 with basis $1, x, x^2, \ldots, x^{p-1}$.

3 Lemmas and propositions

Our proof of Main Theorem depends on the following result.

Lemma 3.1
Let $A \supsetneq B \supsetneq A^p$ be an inclusion sequence of integral domains of characteristic $p > 0$, P a prime ideal of A and $Q = P \cap B$. Then, when A_P has a p-basis, the cardinal number of the p-basis is independent of the choice of P.

Proof: Let $\Gamma \subset A_P$ be a p-basis of A_P over B_Q. Localizing both sides of $A_P = B_Q[\Gamma]$ by $\{1/s \mid s \in P - \{0\}\}$, we have $\Phi(A) = \Phi(B)[\Gamma]$. For any finite subset of Γ denoted by $\{x_1, \ldots, x_n\}$, assume

$$\sum_{0 \le e_1, \ldots, e_n \le p-1} \frac{b_{e_1 \cdots e_n}}{t_{e_1 \cdots e_n}} x_1^{e_1} \cdots x_n^{e_n} = 0 \quad \left(\frac{b_{e_1 \cdots e_n}}{t_{e_1 \cdots e_n}} \in Q(B) \right).$$

Putting

$$t = \prod_{0 \le e_1, \ldots, e_n \le p-1} t_{e_1 \cdots e_n},$$

multiply the above expression by t. Then we get

$$\sum_{0 \le e_1, \ldots, e_n \le p-1} b'_{e_1 \cdots e_n} x_1^{e_1} \cdots x_n^{e_n} = 0 \quad (b'_{e_1 \cdots e_n} \in B \subset B_Q).$$

Since $\{x_1, \ldots, x_n\}$ are p-independent over B_Q, the coefficients $b'_{e_1 \cdots e_n}$ vanish.
Here, $b'_{e_1 \cdots e_n} = (b_{e_1 \cdots e_n}/t_{e_1 \cdots e_n}) \cdot t$, where $t \neq 0$. So all of $b_{e_1 \cdots e_n}/t_{e_1 \cdots e_n}$ are also vanish. Thus, Γ is p-independent also over $\Phi(B)$. Therefore, Γ is a p-basis of $\Phi(A)$ over $\Phi(B)$, too. We conclude that the cardinal number of the p-basis is independent of the choice of P.

Proposition 3.2
Let A', B, B' be the same as in Main Theorem. Then

(1) $Der_B(A')$ is a free A'-module of rank 1,

(2) $Der_{B'}(B)$ is a free B- module of rank 1.

Proof: Let P be an arbitrary prime ideal of A' and $Q = P \cap B$. Then, A'_P and B_Q are regular local rings, since the polynomial rings over a field are regular rings by [2, p190]. Clearly, A'_P is finitely generated as a B_Q-module. Applying the theorem[3](Kunz's conjecture), we see that A'_P has a p-basis over B_Q. The assumption $[\Phi(A') : \Phi(B)] = p$ implies the p-basis of $\Phi(A')$ over

$\Phi(B)$ consists of a single member. By Lemma 3.1, the p-basis of A'_P also consists of a single member. By Proposition5.6[7, p76],

$$\{x_\lambda\}_{\lambda\in\Lambda} \text{ is a } p\text{-basis of } A \text{ over } B \Leftrightarrow \{dx_\lambda\}_{\lambda\in\Lambda} \text{ is a basis of } \Omega_B(A).$$

So $\Omega_{B_Q}(A'_P)$ is a free A'_P-module of rank 1. On the other hand, by Proposition3.3[8, p57], we get

$$\Omega_{B_Q}(A'_P) = (\Omega_B(A'))_P = \Omega_B(A') \otimes_{A'} A'_P.$$

By Corollary[2, p64], letting M and N be A-modules, we have

$$\mathrm{Hom}_A(M,N) \otimes_A A_P = \mathrm{Hom}_{A_P}(M_P, N_P).$$

Accordingly,

$$\begin{aligned}
(\mathrm{Der}_B(A'))_P &= \mathrm{Der}_B(A') \otimes_{A'} A'_P \\
&= \mathrm{Hom}_{A'}(\Omega_B(A'), A') \otimes_{A'} A'_P \\
&= \mathrm{Hom}_{A'_P}((\Omega_B(A'))_P, A'_P) \\
&= \mathrm{Hom}_{A'_P}(\Omega_{B_Q}(A'_P), A'_P) \\
&= \mathrm{Der}_{B_Q}(A'_P).
\end{aligned}$$

Applying duality of free modules to $\mathrm{Der}_{B_Q}(A'_P)$ and $\Omega_{B_Q}(A'_P)$, we have $\mathrm{Der}_{B_Q}(A'_P) \cong \Omega_{B_Q}(A'_P)$. Thus, $(\mathrm{Der}_B(A'))_P$ is a free A'_P-module of rank 1. Then, by 2.4, $\mathrm{Der}_B(A')$ is a projective A'-module of rank 1. By Serre's conjecture which was proved(see [9]), $\mathrm{Der}_B(A')$ turns out to be an A'-module of rank 1. Therefore, $\mathrm{Der}_B(A')$ is an A'-module of rank 1. Thus we complete the proof of (1). As for (2), the same argument can be applied, since $[\Phi(B) : \Phi(B')] = p$.

Proposition 3.3
Let A', B, B' be the same as in Main Theorem and F a polynomial in A' such that $F \notin B' = k'[x_1^p, x_2^p]$. If there exists $G \in B'$ such that $\partial F/\partial x_1 = \alpha_1 G$ and $\partial F/\partial x_2 = \alpha_2 G$ $(\alpha_1, \alpha_2 \in A')$, then we have $F = \alpha G + H$ $(\alpha \in A',\ H \in B')$.

Proof: $F \notin B' = k'[x_1^p, x_2^p]$ implies that one of the following assertion holds.

(1) F has a term $ax_1^\nu x_2^m$ where ν is not a multiple of p,

(2) F has a term $ax_1^m x_2^\nu$ where ν is not a multiple of p.

Without loss of generality, we assume (1). Then, $\partial F/\partial x_1 = \alpha_1 G \neq 0$ and we shall show that

$$F = \alpha_3 G + \beta \quad (\alpha_3 \in A',\ \beta \in B'[x_2] = k'[x_1^p, x_2]). \qquad \cdots(*)$$

Since $G \in B' = k'[x_1^p, x_2^p]$, it follows that

$$\begin{aligned}
\frac{\partial}{\partial x_1}(\alpha_3 G + \beta) &= \frac{\partial}{\partial x_1}(\alpha_3 G) + \frac{\partial}{\partial x_1}(\beta) \\
&= \frac{\partial}{\partial x_1}(\alpha_3 G) \\
&= G\frac{\partial}{\partial x_1}(\alpha_3) + \alpha_3 \frac{\partial}{\partial x_1}(G) \\
&= G\frac{\partial}{\partial x_1}(\alpha_3).
\end{aligned}$$

Thus, we can prove $(*)$ if we find $\alpha_3 \in A'$ such that $\partial\alpha_3/\partial x_1 = \alpha_1$.
Actually, for

$$\alpha_1 = \beta_n x_1^n + \beta_{n-1}x_1^{n-1} + \cdots + \beta_0 \quad (\beta_i \in B'[x_2]),$$

we can take

$$\alpha_3 = \frac{\beta_n}{n+1}x_1^{n+1} + \frac{\beta_{n-1}}{n}x_1^n + \cdots + \beta_0 x_1.$$

Note that $\alpha_1 G$ doesn't have a term $ax_1^\nu x_2^m$ where $\nu+1$ is not a multiple of p, since $\alpha_1 G$ is the result of partial differentiation with respect to x_1. So the right hand side above makes sense. By partial differentiation of $(*)$ with respect to x_2, we get

$$\begin{aligned}\frac{\partial F}{\partial x_2} &= \frac{\partial}{\partial x_2}(\alpha_3 G) + \frac{\partial}{\partial x_2}(\beta)\\ &= G\frac{\partial}{\partial x_2}(\alpha_3) + \alpha_3\frac{\partial}{\partial x_2}(G) + \frac{\partial}{\partial x_2}(\beta)\\ &= G\frac{\partial}{\partial x_2}(\alpha_3) + \frac{\partial}{\partial x_2}(\beta).\end{aligned}$$

Comparing the right hand side above with that of the assumption $\partial F/\partial x_2 = \alpha_2 G$, we have

$$\frac{\partial\beta}{\partial x_2} = \alpha_4 G \quad (\alpha_4 \in A').$$

Clearly, α_4 doesn't have any term $ax_1^\nu x_2^m$ or $ax_1^m x_2^\nu$ where $\nu+1$ is not a multiple of p, since $\beta \in B'[x_2] = k'[x_1^p, x_2]$. By the same way as above, by integrating with respect to x_1, we can show that

$$\beta = G\delta + H \quad (\delta \in A',\ H \in B'). \quad \cdots(**)$$

Note that H must be an element of B', since $\beta \in B'[x_2]$. Actually,

$$\begin{aligned}\frac{\partial}{\partial x_2}(G\delta + H) &= G\frac{\partial}{\partial x_2}(\delta) + \delta\frac{\partial}{\partial x_2}(G) + \frac{\partial}{\partial x_2}(H)\\ &= G\frac{\partial}{\partial x_2}(\delta).\end{aligned}$$

Then, we can prove $(**)$ if we find $\delta \in A'$ such that $\partial\delta/\partial x_2 = \alpha_4$. We do have the δ by the same argument as above, since α_4 doesn't have a term $ax_1^m x_2^\nu$ where ν is not a multiple of p. Putting $\alpha = \alpha_3 + \delta$, we get

$$F = \alpha G + H \quad (\alpha \in A',\ H \in B').$$

4 Proof of Main Theorem

First, we prove that B has a p-basis over B'. Let Q be an arbitrary prime ideal and $q = Q \cap B'$. As we mentioned in the proof of Lemma 3.3, both of B_Q and B'_q are regular local rings and B_Q is finitely generated as a B'_q-module. By Kunz's conjecture[3], B_Q has a p-basis over B'_q (1). By definition of p-basis, B_Q is a finitely generated free B'_q-module. By Lemma 3.1, the rank of B_Q as a B'_q-module is unique regardless of the choice of Q. Thus, by Theorem 2.4, B is a finitely

generated projective B'-module (2). By (1) and (2), B is a Galois extention of B'. Similarly, A' is a Galois extention of B. So A' is a Galois extention of B'. Hence, by Theorem 2.3, we get

$$\mathrm{Der}_{B'}(A') = A' \cdot G_{B'}(B) \oplus \mathrm{Der}_B(A').$$

Moreover, by Proposition 3.2, we have

$$\begin{aligned} \mathrm{Der}_{B'}(B) &= Bd_1 \quad \text{where } d_1 \in \mathrm{Der}_{B'}(B), \\ \mathrm{Der}_B(A') &= A'd_2 \quad \text{where } d_2 \in \mathrm{Der}_B(A'). \end{aligned}$$

Let $\tilde{d_1}$ be the extention of d_1 (see 2.3(2)). For simplicity, $\tilde{d_1}$ is written as d_1. Thus we have

$$\mathrm{Der}_{B'}(A') = A'd_1 \oplus A'd_2 \quad (d_1 \in \mathrm{Der}_{B'}(B),\ d_2 \in \mathrm{Der}_B(A')).$$

It follows that

$$\begin{aligned} \frac{\partial}{\partial x_1} &= \alpha_1 d_1 + \beta_1 d_2 \text{ for some } \alpha_1, \beta_1 \in A', \\ \frac{\partial}{\partial x_2} &= \alpha_2 d_1 + \beta_2 d_2 \text{ for some } \alpha_2, \beta_2 \in A'. \end{aligned}$$

Since $d_2 \in \mathrm{Der}_B(A')$, if $B \ni F$, then

$$\begin{aligned} \frac{\partial F}{\partial x_1} &= \alpha_1 d_1 F \quad \text{for some } \alpha_1 \in A', \\ \frac{\partial F}{\partial x_2} &= \alpha_2 d_1 F \quad \text{for some } \alpha_2 \in A'. \end{aligned}$$

We take $F \in B \setminus B'$ such that the degree of F with respect to x_1 and x_2 is the smallest one in $B \setminus B'$. If d_1 doesn't decrease the degree of F, by the equations above, both $\partial/\partial x_1$ and $\partial/\partial x_2$ don't also decrease the degree of F. Then, F must be a constant. This is a contradiction. Thus, we have $d_1 F \in B'$ because of the choice of F.
By Proposition 3.3, we have

$$F = \alpha d_1 F + H \ (\alpha \in A',\ H \in B').$$

Since B is integrally closed in $\Phi(B)$, it follows that $\alpha \in B$. We shall show that $d_1 F \in k' - \{0\}$ in the following two steps.
Step1. If $d_1 F = 0$, then $F = \alpha d_1 F + H = H \in B'$, which contradicts $F \notin B'$.
Since $\alpha \in B \subset A' = B'[x_1, x_2]$, it follows that

$$\alpha = \sum_{0 \le e_1, e_2 \le p-1} \alpha'_{e_1 e_2} x_1^{e_1} x_2^{e_2} \quad (\alpha'_{e_1 e_2} \in B').$$

Step2. Suppose that $d_1 F \notin k'$. Since $F = \alpha d_1 F + H$ where $\alpha \in A'$and $H \in B'$), $\alpha - \alpha'_{(00)}$ is an element of B, its degree is lower than that of F. Thus $\alpha - \alpha'_{(00)} \in B'$. Then, $\alpha \in B'$. Since $\alpha'_{(00)} \in B'$, it follows that $\alpha \in B'$. Then $F = \alpha d_1 F + H \in B'$, which contradicts $F \notin B'$.
Accordingly,

$$d_1 F \in k' - \{0\}.$$

If $F \in \Phi(B')$, then $F = f/g$, where $f, g \in B'$ and $d_1F = d_1(f/g) = (gd_1f - fd_1g)/g^2 = 0$. This contradicts $d_1F \in k' - 0$. Thus $F \notin \Phi(B')$. Therefore,

$$[\Phi(B')(F) : \Phi(B')] > 1.$$

Since $\Phi(B')(F)$ is purely inseparable over $\Phi(B')$ and $[\Phi(B) : \Phi(B')] = p$, it follows that

$$\Phi(B) = \Phi(B')(F) = \Phi(B')[F].$$

Hence, any $x \in B$ is written as

$$x = \beta_{p-1}F^{p-1} + \beta_{p-2}F^{p-2} + \cdots + \beta_1F + \beta_0 \quad (\beta_i \in \Phi(B')).$$

Since $d_1F \in k' \subset \Phi(B')$, we get

$$\begin{aligned} d_1x &= d_1(\beta_{p-1}F^{p-1}) + d_1(\beta_{p-2}F^{p-2}) + \cdots + d_1(\beta_1F) + d_1(\beta_0) \\ &= \beta_{p-1}(p-1)F^{p-2}d_1F + \beta_{p-2}(p-2)F^{p-3}d_1F + \cdots + \beta_1d_1F + 0 \\ &= \beta'_{p-2}F^{p-2} + \beta'_{p-3}F^{p-3} + \cdots + \beta'_0 \quad (\beta'_i \in \Phi(B')) \end{aligned}$$

Repeating such operations, we get $d_1^p = 0$. Since d_1F is a unit of B', we have

$$d_1\left(\frac{F}{d_1F}\right) = 1.$$

Applying Theorem 2.5, $\{F/d_1F\}$ is a p-basis of B over Ker d_1. On the other hand, since $\mathrm{Der}_{B'}(B) = Bd_1$ and B is a Galois extention of B', we get

$$\text{Ker } d_1 = \mathrm{Ker}(\mathrm{Der}_{B'}(B)) = B',$$

applying Theorem 2.2. Hence, $\{F/d_1F\}$ is a p-basis of B over B'.
Let $C = k'^p[y_1, y_2]$, $D = k'^p[x_1^p, x_2^p]$ and $E = k'^p[y_1^p, y_2^p]$. Applying the same argument to the inclusion sequence $C \supset D \supset E$, we can prove that D has a p-basis over E. Using the inverse of Frobenius map, A' has a p-basis over B. Noting that k has a p-basis over k' and k' has a p-basis over k^p, we complete the proof of Main Theorem.

References

[1] Bourbaki, Sugaku Genron, Kakan Daisu1, Tokyo Toshyo, in Japanese, 1971.

[2] Hideyuki Matsumura, Kakan Kanron, Kyoritsu Syuppan, 1980.

[3] T. Kimura and H. Niitsuma, On Kunz's conjecture, J. Math. Soc. Japan, 34 (1982), 371-378.

[4] R. Ganong, Plane Frobenius sandwiches, Proc. Amer. Math. Soc., 84(1982), 474-478.

[5] T. Kimura and H. Niitsuma, A note on p-basis of polynomial ring in two variables, SUT J. Math., 25 (1989), 33-38.

[6] S. Yuan, Inseparable Galois theory of exponent one, Trans. Amer. Math. Soc, 149(1970), 163-170.

[7] E. Kunz, Kähler Differentials, Vieweg Advanced Lectures in Math., 1986

[8] Shigeru Iitaka, Heimen Kyokusen no Kika, Kyouritsu Shyuppan, 2001.

[9] T. Y. Lam, Serre's conjecture, Lecture Notes in Mathematics Vol.635 Springer-Verlag, 1978.