PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 128, Number 2, Pages 353–360
S 0002-9939(99)05029-7
Article electronically published on July 6, 1999

A NOTE ON p-BASES OF RINGS

TOMOAKI ONO

(Communicated by Wolmer V. Vasconcelos)

Abstract. Let $R \supseteq R' \supseteq R^p$ be a tower of rings of characteristic $p > 0$. Suppose that R is a finitely presented R'-module. We give necessary and sufficient conditions for the existence of p-bases of R over R'. Next, let A be a polynomial ring $k[X_1, \ldots, X_n]$ where k is a perfect field of characteristic $p > 0$, and let B be a regular noetherian subring of A containing A^p such that $[Q(B) : Q(A^p)] = p$. Suppose that $Der_{A^p}(B)$ is a free B-module. Then, applying the above result to a tower $B \supseteq A^p \supseteq B^p$ of rings, we shall show that a polynomial of minimal degree in $B - A^p$ is a p-basis of B over A^p.

1. Preliminaries

Throughout this paper, let p be always a prime number, let R be a commutative ring with unity of characteristic p, and let R' be a subring of R containing $R^p = \{a^p \mid a \in R\}$. Then there is a canonical one-to-one correspondence between $Spec\, R$ and $Spec\, R'$ by Lemma 1 of [6]. So, for any given $\mathfrak{p} \in Spec\, R$, we denote by $\mathfrak{p}'$ the corresponding element in $Spec\, R'$, i.e., $\mathfrak{p}' = \mathfrak{p} \cap R'$.

A subset $\{x_1, ..., x_l\}$ of R is said to be a *p-basis* of R over R' if the monomials $x_1^{e_1} \cdots x_l^{e_l}$ $(0 \leq e_i \leq p-1)$ are linearly independent over R' and $R = R'[x_1, ..., x_l]$. If, for each $\mathfrak{p} \in Spec\, R$, there exists a p-basis of $R_{\mathfrak{p}}$ over $R'_{\mathfrak{p}'}$, we say that R *has locally p-bases over* R'. Moreover, if R is finitely generated and projective as an R'-module in addition to the previous condition, then the R'-algebra R is called *a Galois extension of* R' ([6]).

When R is a local ring, the existence of a p-basis of R over R' is studied for example in [1]. But it is not well-known whether there is a p-basis of R over R' or not, when R is not a local ring ([2]). If R has a p-basis over R', then for any $\mathfrak{p} \in SpecR$ the localization $R_{\mathfrak{p}}$ at $\mathfrak{p}$ also has a p-basis over $R'_{\mathfrak{p}'}$. The converse does not hold in general. In this paper, we study a condition for the existence of a p-basis of R over R', when R has locally p-bases over R' (Theorems 2.2 and 3.2). As an example we consider the existence of a p-basis of a regular ring which is contained in a polynomial ring over a perfect field (Theorem 4.1). A special basis of the module of derivations plays a central role in our study, and we use the results of [6] frequently.

Let $Der_{R'}(R)$ be the set of all derivations of R over R', let S be a multiplicatively closed subset of R, and let S' be $S \cap R'$. We denote by ϕ_S and τ_S the canonical

Received by the editors January 19, 1998 and, in revised form, April 1, 1998.
1991 *Mathematics Subject Classification.* Primary 13N05; Secondary 13B05.
Key words and phrases. p-basis, derivation, Galois extension.

maps $R \longrightarrow R_S$ and $Der_{R'}(R) \longrightarrow Der_{R'_{S'}}(R_S)$, respectively. In particular, when S is a multiplicatively closed subset $\{f^n\}_{n\geq 0}$ $(f \in R)$, resp. $R - \mathfrak{p}$, we denote by ϕ_f and τ_f, resp. $\phi_{\mathfrak{p}}$ and $\tau_{\mathfrak{p}}$ (or simply ϕ and τ), the previous canonical maps. Note that $\tau_S(D)(\phi_S(x)) = \phi_S(D(x))$ for any $x \in R$ and any $D \in Der_{R'}(R)$.

As is well-known, the following three facts hold:

(1) If R_S has a p-basis $\{x_1/s_1, ..., x_l/s_l\}$ over $R'_{S'}$, then $\{\phi_S(s_1^{p-1}x_1), ..., \phi_S(s_l^{p-1}x_l)\}$ is a p-basis of R_S over $R'_{S'}$, i.e., we can choose a p-basis of R_S over $R'_{S'}$ from the image $\phi(R)$.

(2) If R has a p-basis $\{x_1, ..., x_l\}$ over R', then the image $\{\phi_S(x_1), ..., \phi_S(x_l)\}$ in R_S is a p-basis of R_S over $R'_{S'}$.

(3) If R has a p-basis $\{x_1, ..., x_l\}$ over R', then there exists a unique set of derivations $D_{x_1}, ..., D_{x_l}$ of R over R' such that $D_{x_i}(x_j) = \delta_{ij}$ where δ_{ij} is Kronecker's delta. This set forms a basis for $Der_{R'}(R)$. We always denote by $D_{x_1}, ..., D_{x_l}$ such derivations which are associated with a p-basis $\{x_1, ..., x_l\}$ of R over R'.

Definition. Suppose R has locally p-bases over R'. Let $\{\mathfrak{m}\}$ be the set of all maximal ideals of R. We call $D \in Der_{R'}(R)$ the *preferable* derivation, if for each $\mathfrak{m}$ there is a p-basis $\{\phi_{\mathfrak{m}}(x)\}$ $(x \in R)$ of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$ such that $\phi_{\mathfrak{m}}(D(x))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{\mathfrak{m}'}\phi_{\mathfrak{m}}(x)^i$.

Lemma 1.1. *Suppose R has locally p-bases over R'. Let S be a multiplicatively closed subset of R disjoint from at least one prime ideal, and suppose R_S has a p-basis $\{\phi_S(x)\}$ over $R'_{S'}$. If $D \in Der_{R'}(R)$ is preferable, then $\phi_S(D(x))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{S'}\phi_S(x)^i$.*

Proof. Let $\{\mathfrak{p}\}$ be the set of all prime ideals of R disjoint from S. The set $\{\mathfrak{p}\}$ is non-empty by the assumption. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Since D is preferable, there exists a p-basis $\{\phi_{\mathfrak{m}}(y)\}$ $(y \in R)$ of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$ such that $\phi_{\mathfrak{m}}(D(y))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{\mathfrak{m}'}\phi_{\mathfrak{m}}(y)^i$. We use a symbol ϕ for the canonical map $R \longrightarrow R_{\mathfrak{p}}$. Then, by the above fact (2), $\{\phi(y)\}$ is a p-basis of $R_{\mathfrak{p}}$ over $R'_{\mathfrak{p}'}$, and $\phi(D(y))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{\mathfrak{p}'}\phi(y)^i$. Therefore we can take an element z of $R_{\mathfrak{p}}$ such that $\phi(D(y))^{p-1} = D_{\phi(y)}(z)$. Since $\{D_{\phi(y)}\}$ forms a basis for $Der_{R'_{\mathfrak{p}'}}(R_{\mathfrak{p}})$ and $D_{\phi(y)}(\phi(y)) = 1$, we have $\tau_{\mathfrak{p}}(D) = \tau_{\mathfrak{p}}(D)(\phi(y))D_{\phi(y)} = \phi(D(y))D_{\phi(y)}$.

Now, the fact (2) says that $\{\phi(x)\}$ is a p-basis of $R_{\mathfrak{p}}$ over $R'_{\mathfrak{p}'}$. Hence, there is a unique basis $\{D_{\phi(x)}\}$ of $Der_{R'_{\mathfrak{p}'}}(R_{\mathfrak{p}})$ such that $D_{\phi(x)}(\phi(x)) = 1$, and $D_{\phi(y)} = D_{\phi(y)}(\phi(x))D_{\phi(x)}$. From these facts, we get the following equations:

$$\begin{aligned}
\phi(D(x))^{p-1} &= \{\tau_{\mathfrak{p}}(D)(\phi(x))\}^{p-1} \\
&= \{\phi(D(y))D_{\phi(y)}(\phi(x))\}^{p-1} \\
&= D_{\phi(y)}(z)D_{\phi(y)}(\phi(x))^{p-1} \\
&= \{D_{\phi(y)}(\phi(x))D_{\phi(x)}(z)\}D_{\phi(y)}(\phi(x))^{p-1} \\
&= D_{\phi(y)}(\phi(x))^p D_{\phi(x)}(z).
\end{aligned}$$

Thus $\phi(D(x))^{p-1}$ is contained in $\bigoplus_{i=0}^{p-2} R'_{\mathfrak{p}'}\phi(x)^i$. When we write $\phi_S(D(x))^{p-1}$ as $\sum_{i=0}^{p-1}(c_i/s_i)\phi_S(x)^i$ $(c_i \in R', s_i \in S')$, we can find for each $\mathfrak{p}$ an element t of $R' - \mathfrak{p}'$ such that $c_{p-1}t = 0$, i.e., $\phi(c_{p-1}) = 0$. This implies that $\phi_S(c_{p-1}) = 0$. Therefore $\phi_S(D(x))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{S'}\phi_S(x)^i$. $\square$

Lemma 1.2. *Suppose R is reduced and has locally p-bases over R'. Let $\{\mathfrak{q}\}$ be the set of all minimal prime ideals belonging to the zero ideal (0), and let $\{\phi_{\mathfrak{q}}(x)\}$ $(x \in R)$ be a p-basis of $R_{\mathfrak{q}}$ over $R_{\mathfrak{q}'}$. If $D \in Der_{R'}(R)$ satisfies that for each $\mathfrak{q}$*

$$\phi_{\mathfrak{q}}(D(x))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{\mathfrak{q}'}\phi_{\mathfrak{q}}(x)^i,$$

then D is preferable.

Proof. Let $\mathfrak{m}$ be a maximal ideal of R, and let $\{\phi_{\mathfrak{m}}(y)\}$ $(y \in R)$ be a p-basis of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$. By the same argument as in the proof of Lemma 1.1, we see that $\phi_{\mathfrak{q}}(D(y))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{\mathfrak{q}'}\phi_{\mathfrak{q}}(y)^i$ for each $\mathfrak{q}$ contained in $\mathfrak{m}$. Writing $\phi_{\mathfrak{m}}(D(y))^{p-1}$ as $\sum_{i=0}^{p-1}(c_i/s_i)\phi_{\mathfrak{m}}(y)^i$ $(c_i \in R', s_i \in R' - \mathfrak{m}')$, there exists an element t of $R' - \mathfrak{q}'$ such that $c_{p-1}t = 0$. This means that $c_{p-1} \in \bigcap_{\text{all}\mathfrak{q}\subseteq\mathfrak{m}} \mathfrak{q}'$. Since R is reduced, the localization $R'_{\mathfrak{m}'}$ of R' is also, i.e., the nilradical $(\bigcap_{\text{all}\mathfrak{q}\subseteq\mathfrak{m}} \mathfrak{q}')R'_{\mathfrak{m}'}$ is equal to (0). It follows that $c_{p-1}/s_{p-1} = 0$. Thus D is preferable. □

2. p-BASES WHICH CONSIST OF ONE ELEMENT

Lemma 2.1. *Let D be a derivation of R. Then, for any $a \in R$ we have*

$$(aD)^{p-1}(a) = -aD^{p-1}(a^{p-1}).$$

Proof. To prove this assertion, we make use of the proof of the Hochschild formula (see Theorem 25.5 of [4]). By induction, for $k \geq 1$ we get

$$(aD)^k = a^k D^k + \sum_{i=2}^{k-1} b_{k,i} D^i + (aD)^{k-1}(a)D,$$

where $b_{k,i} = f_{k,i}(a, D(a), D^2(a), ..., D^{k-i}(a))$ $(2 \leq i \leq p-1)$, more precisely the $f_{k,i}$ are polynomials with coefficients in $\mathbb{Z}/(p)$ not depending on R, on a or on D. Then according to the proof of Theorem 25.5 of [4], the polynomial $f_{p,i}$ is equal to 0 for any i. On the other hand, the following expansion is obtained:

$$\begin{aligned}(aD)^p = a^p D^p + a\{D(a^{p-1}) + b_{p-1,p-2}\}D^{p-1} + \sum_{i=3}^{p-2} a\{D(b_{p-1,i}) + b_{p-1,i-1}\}D^i \\ + a\{D(b_{p-1,2}) + (aD)^{p-2}(a)\}D^2 + (aD)^{p-1}(a)D.\end{aligned}$$

Hence, we get the following recurrence formula:

$$\begin{cases} D(a^{p-1}) + b_{p-1,p-2} = 0, \\ D(b_{p-1,i}) + b_{p-1,i-1} = 0 \qquad (3 \leq i \leq p-2), \\ D(b_{p-1,2}) + (aD)^{p-2}(a) = 0. \end{cases}$$

It follows that

$$\begin{aligned}(aD)^{p-2}(a) &= -D(b_{p-1,2}) \\ &= -D(-D(b_{p-1,3})) \\ &\cdots\cdots \\ &= (-1)^{p-3}D^{p-3}(-D(a^{p-1})) \\ &= (-1)^{p-2}D^{p-2}(a^{p-1}).\end{aligned}$$

Consequently, we have $(aD)^{p-1}(a) = -aD^{p-1}(a^{p-1})$. □

Theorem 2.2. *Suppose R is finitely presented as an R'-module. Then the following conditions are equivalent:*

(1) *R has a p-basis over R' which consists of one element.*

(2) *R has locally p-bases over R' and $Der_{R'}(R)$ has a basis D such that $D^p = 0$.*

(3) *R has locally p-bases over R' and $Der_{R'}(R)$ has a basis which consists of one preferable derivation.*

Proof. (1) $\Rightarrow$ (2). This assertion is obvious.

(2) $\Rightarrow$ (3). Let $\mathfrak{m}$ be a maximal ideal of R. Since R is a finitely presented R'-module, the module $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$ is canonically isomorphic to $Der_{R'}(R) \otimes_R R_{\mathfrak{m}}$. This implies that $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$ is a free $R_{\mathfrak{m}}$-module with rank 1. So any p-basis of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$ consists of one element. Let $\phi(x)$ $(x \in R)$ be a p-basis of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$, where ϕ expresses the canonical map $R \longrightarrow R_{\mathfrak{m}}$. For the canonical map $\tau_{\mathfrak{m}}$, note that $\tau_{\mathfrak{m}}(D^p) = \tau_{\mathfrak{m}}(D)^p$. Since $D_{\phi(x)}$ forms a basis for $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$, we have

$$\tau_{\mathfrak{m}}(D) = \phi(D(x))D_{\phi(x)} \quad \text{and} \quad \tau_{\mathfrak{m}}(D^p) = \phi(D^p(x))D_{\phi(x)}.$$

By virtue of Lemma 2.1, we have

$$\phi(D^p(x)) = \{\phi(D(x))D_{\phi(x)}\}^{p-1}(\phi(D(x))) = -\phi(D(x))D^{p-1}_{\phi(x)}(\phi(D(x))^{p-1}).$$

Hence, the following equation is obtained:

$$\tau_{\mathfrak{m}}(D^p) = -\phi(D(x))D^{p-1}_{\phi(x)}(\phi(D(x))^{p-1})D_{\phi(x)}.$$

Now, $\phi(D(x))$ is a unit in $R_{\mathfrak{m}}$, because $\tau_{\mathfrak{m}}(D)$ forms a basis for $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$. From this $D^p = 0$ implies $D^{p-1}_{\phi(x)}(\phi(D(x))^{p-1}) = 0$. Thus D is preferable.

(3) $\Rightarrow$ (1). Let $\{\mathfrak{p}\}$ be the set of all prime ideals of R, and for each $\mathfrak{p}$ let $\{\phi(x)\}$ $(x \in R)$ be a p-basis of $R_{\mathfrak{p}}$ over $R'_{\mathfrak{p}'}$, where ϕ is the canonical map $R \longrightarrow R_{\mathfrak{p}}$. Let D be a preferable derivation which is a basis of $Der_{R'}(R)$. Since R is a finitely presented R'-module, $\tau_{\mathfrak{p}}(D)$ forms a basis for $Der_{R'_{\mathfrak{p}'}}(R_{\mathfrak{p}})$ as in the proof of (2) $\Rightarrow$ (3), so $D(x) \notin \mathfrak{p}$. We claim that $Ker\, D = R'$. Indeed, R is a Galois extension of R', and the claim follows from Theorem 9 (2) of [6]. Put $f = D(x)^p$ and $D_{(f)} = \{D(x)^{p-1}/f\}\tau_f(D)$. Then $D_{(f)}$ is an element of $Der_{R'_f}(R_f)$ such that $Ker\, D_{(f)} = R'_f$ and $D_{(f)}(\phi_f(x)) = 1$. Moreover, $D^p_{(f)} = 0$, because $\tau_{f,\mathfrak{p}}(D^p_{(f)}) = (\tau_{f,\mathfrak{p}}(D_{(f)}))^p = (D_{\phi(x)})^p = 0$ for any prime ideal $\mathfrak{p}$ which does not contain f, where $\tau_{f,\mathfrak{p}}$ is the canonical map $Der_{R'_f}(R_f) \longrightarrow Der_{R'_{\mathfrak{p}'}}(R_{\mathfrak{p}})$. By Theorem 27.3 (i) of [4], $\{\phi_f(x)\}$ is a p-basis of R_f over R'_f.

Now, since $Spec\, R^p$ is quasi-compact, we can take a finite subset $\{f_1, \ldots, f_m\}$ of $\{f\}_{\mathfrak{p} \in Spec\, R}$ and a finite subset $\{g_1, \ldots, g_m\}$ of R^p such that $\sum_{j=1}^m f_j g_j = 1$. Denote by x_j the element x associated with each f_j. Since D is preferable, by Lemma 1.1 we have $\phi_{f_j}(D(x_j))^{p-1} \in \bigoplus_{i=0}^{p-2} R'_{f_j}\phi_{f_j}(x_j)^i$ for each j. Hence, we can write $\phi_{f_j}(D(x_j))^{p-1}$ as $\{\sum_{i=0}^{p-2}(i+1)c_{ij}x_j^i\}/f_j^{n_j}$, where c_{ij} $(0 \le i \le p-1,\ 1 \le j \le m)$ are elements of R' and n_j $(1 \le j \le m)$ are non-negative integers. There exists a positive integer e such that $p^e \ge n_j + 1$ and $f_j^{p^e - n_j - 1}\{f_j^{n_j} D(x_j)^{p-1} - \sum_{i=0}^{p-2}(i+1)c_{ij}x_j^i\} = 0$

for all j. Here, put $z = \sum_{j=1}^{m} g_j^{p^e} (\sum_{i=0}^{p-2} f_j^{p^e-n_j-1} c_{ij} x_j^{i+1})$. Then we have

$$\begin{aligned} D(z) &= \sum_{j=1}^{m} g_j^{p^e} \{\sum_{i=0}^{p-2} (i+1) f_j^{p^e-n_j-1} c_{ij} x_j^i\} D(x_j) \\ &= \sum_{j=1}^{m} g_j^{p^e} (f_j^{p^e-1} D(x_j)^{p-1}) D(x_j) \\ &= \sum_{j=1}^{m} f_j^{p^e} g_j^{p^e} = 1. \end{aligned}$$

Now, we shall show that $\{z\}$ is a p-basis of R over R'. According to Theorem 27.3 (i) of [4], nothing remains but to show $D^p = 0$. Since D forms a basis for $Der_{R'}(R)$, the derivation D^p is equal to aD ($a \in R$). Clearly, $a = aD(z) = D^p(z) = 0$. Thus $D^p = 0$. Therefore R has the p-basis $\{z\}$ over R'. □

Corollary 2.3. *Suppose that R and R' are regular noetherian rings, and suppose that R is finitely generated as an R'-module. Then the following conditions are equivalent:*

(1) *R has a p-basis over R' which consists of one element.*
(2) *$Der_{R'}(R)$ has a basis D such that $D^p = 0$.*
(3) *$Der_{R'}(R)$ has a basis which consists of one preferable derivation.*

Proof. By the Theorem of [1] (cf. [3], Theorem 15.7), R has locally p-bases over R'. Therefore this is an immediate consequence of Theorem 2.2. □

3. p-BASES WHICH CONSIST OF l ELEMENTS

Lemma 3.1. *Suppose that R is a Galois extension of R'. Let D be a derivation of R over R', and suppose that $D^p = 0$ and the R-module RD is a direct summand of $Der_{R'}(R)$. Then the following holds:*

(1) *R is a Galois extension of $Ker\, D$,*
(2) *$Ker\, D$ is a Galois extension of R',*
(3) *$RD = Der_{Ker\, D}(R)$.*

Proof. For any $a,\ b \in R$, we have

$$[aD,\ bD] = \{aD(b) - bD(a)\}D,$$

and by the Hochschild formula

$$(aD)^p = a^p D^p + (aD)^{p-1}(a)D = (aD)^{p-1}(a)D.$$

Thus $[aD,\ bD]$ and $(aD)^p$ are contained in RD. It follows that RD is a p-Lie subalgebra of $Der_{R'}(R)$. Theorem 12 of [6] says that R is a Galois extension of $Ker\, D$ and $RD = Der_{Ker\, D}(R)$. Therefore $Ker\, D$ is a Galois extension of R' by Theorem 11 of [6]. □

Theorem 3.2. *Let l be an integer greater than 1. Suppose R is finitely presented as an R'-module. Then the following conditions are equivalent:*

(1) *R has a p-basis over R' which consists of l elements.*
(2) *R has locally p-bases over R' and $Der_{R'}(R)$ has a basis $\{D_1, \ldots, D_l\}$ such that $D_i^p = 0$ and $[D_i,\ D_j] = 0$ for any $i,\ j = 1, 2, \ldots, l$.*

Proof. (1) $\Rightarrow$ (2). This immediately follows from fact (3) in §1.

(2) $\Rightarrow$ (1). Let R_1 be the kernel of the derivation D_1 which is an R'-algebra. Then, by Lemma 3.1 R is a Galois extension of R_1 and $RD_1 = Der_{R_1}(R)$. Hence, there exists a p-basis $\{x_1\}$ of R over R_1 by Theorem 2.2.

Now, in order to find the other elements which constitute a p-basis of R over R', we need to show that $\{D_i|_{R_1}\}_{i=2,\dots,l}$ forms a basis for $Der_{R'}(R_1)$. First of all, we claim that $D_i|_{R_1} \in Der_{R'}(R_1)$ and $D_i|_{R_1} \neq 0$ for any $i \geq 2$. The first assertion follows from $[D_1, D_i] = 0$. To show the second assertion, assume $R_1 \subseteq Ker\, D_i$. Then $D_i \in Der_{R_1}(R) = RD_1$. This contradicts the fact that $\{D_1, \dots, D_l\}$ is a basis of $Der_{R'}(R)$. Thus $D_i|_{R_1} \neq 0$. Let $\mathfrak{m}$ be a maximal ideal of R and let $\mathfrak{n}$ be the maximal ideal $\mathfrak{m} \cap R_1$ of R_1. Since R_1 is a Galois extension of R' by Lemma 3.1, there is a subset $\{y_2, \dots, y_l\}$ of $R_{1\mathfrak{n}}$ which is a p-basis of $R_{1\mathfrak{n}}$ over $R'_{\mathfrak{m}'}$. Obviously, $\{\phi_{\mathfrak{m}}(x_1), y_2, \dots, y_l\}$ is a p-basis of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$. Let $D_{\phi_{\mathfrak{m}}(x_1)}, D_{y_2}, \dots, D_{y_l}$ be the derivations of $R_{\mathfrak{m}}$ over $R'_{\mathfrak{m}'}$ associated with this p-basis (see fact (3) in §1). Denote by D'_j the derivation $D_{y_j}|_{R_{1\mathfrak{n}}}$ of $R_{1\mathfrak{n}}$ over $R'_{\mathfrak{m}'}$. Then $\tau_{\mathfrak{n}}(D_i|_{R_1})$ is written as $\sum_{j=2}^{l} a_{ij} D'_j$ for each $i \geq 2$ where $a_{ij} \in R_{1\mathfrak{n}}$, because $\{D'_j\}_{j=2,\dots,l}$ forms a basis for $Der_{R'_{\mathfrak{m}'}}(R_{1\mathfrak{n}})$. Since R is finitely presented as an R'-module, the module $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$ is isomorphic to $Der_{R'}(R) \otimes_R R_{\mathfrak{m}}$. Hence, $\{\tau_{\mathfrak{m}}(D_1), \dots, \tau_{\mathfrak{m}}(D_l)\}$ forms a basis for $Der_{R'_{\mathfrak{m}'}}(R_{\mathfrak{m}})$, so the derivation D_{y_j} is expressed as $\sum_{i=1}^{l} b_{ji} \tau_{\mathfrak{m}}(D_i)$ for each $j \geq 2$ where $b_{ji} \in R_{\mathfrak{m}}$. For each $j \geq 2$ we have

$$D'_j = \sum_{i=1}^{l} b_{ji} \tau_{\mathfrak{m}}(D_i)|_{R_{1\mathfrak{n}}} = \sum_{i=2}^{l} b_{ji} \tau_{\mathfrak{n}}(D_i|_{R_1}).$$

These show that the matrix $[b_{ji}]_{2 \leq i,j \leq l}$ is equal to the inverse matrix of $[a_{ij}]_{2 \leq i,j \leq l}$, i.e., $b_{ji} \in R_{1\mathfrak{n}}$. Thus, for any maximal ideal $\mathfrak{n}$ of R_1, $\{\tau_{\mathfrak{n}}(D_i|_{R_1})\}_{i=2,\dots,l}$ is a basis of $Der_{R'_{\mathfrak{m}'}}(R_{1\mathfrak{n}})$. This implies that $\{D_i|_{R_1}\}_{i=2,\dots,l}$ forms a basis for $Der_{R'}(R_1)$.

Set $R_h = Ker\, D_1 \cap \cdots \cap Ker\, D_h$ for $h = 2, \dots, l$. Repeating the previous argument in the situation that $R_{h-1} \supseteq R_h \supseteq R'$, we can show that there exists a p-basis $\{x_h\}$ of R_{h-1} over R_h inductively. Then Theorem 9 (2) of [6] says that $R_l = R'$. In conclusion, $\{x_1, \dots, x_l\}$ is a p-basis of R over R'. □

Corollary 3.3. *Let l be an integer greater than 1. Suppose that R and R' are regular noetherian rings, and suppose that R is finitely generated as an R'-module. Then the following are equivalent:*

(1) *R has a p-basis over R' which consists of l elements.*

(2) *$Der_{R'}(R)$ has a basis $\{D_1, \dots, D_l\}$ such that $D_i^p = 0$ and $[D_i, D_j] = 0$ for any $i, j = 1, 2, \dots, l$.*

Proof. By virtue of the Theorem of [1], R has locally p-bases over R'. Clearly, the assertion holds by Theorem 3.2. □

4. p-bases of polynomial rings

In this section, when R is an integral domain, $Q(R)$ denotes the field of fractions of R. The next theorem is an analogy of the result of [2].

Theorem 4.1. *Let k be a perfect field of characteristic $p > 0$. Let A be a polynomial ring $k[X_1, \dots, X_n]$, and let B be a regular noetherian subring of A containing A^p such that $[Q(B) : Q(A^p)] = p$. Suppose that $Der_{A^p}(B)$ is a free B-module. If F*

is a polynomial of minimal degree (in $X_1, \ldots, X_n$) in $B - A^p$ which has no terms of elements in A^p, then $\{F\}$ is a p-basis of B over A^p.

Proof. Since A is finitely generated as an A^p-module and B is noetherian, A is finitely presented as a B-module. By the Theorem of [1], A is a Galois extension of B. Clearly A is a Galois extension of A^p, and B is also by Theorem 11 (1) of [6].

Set $H = \{D \in Der_{A^p}(A) \mid D(B) \subseteq B\}$. Then, by Theorem 11 (2) of [6], there is a B-module homomorphism $\Phi : Der_{A^p}(B) \longrightarrow H$ which, followed by the restriction map $H \longrightarrow Der_{A^p}(B)$ given by $D \longrightarrow D|_B$, is the identity map on $Der_{A^p}(B)$. We write $\widetilde{Der_{A^p}(B)}$ for the image of $Der_{A^p}(B)$ in H. Theorem 11 (3) of [6] says that

$$(*) \qquad Der_{A^p}(A) = Der_B(A) \oplus A\widetilde{Der_{A^p}(B)}.$$

We see that $rank_B\, Der_{A^p}(B) = 1$, because $[Q(B) : Q(A^p)] = p$. Let D be a basis for $Der_{A^p}(B)$, and put $\widetilde{D} = \Phi(D)$. Obviously $\widetilde{D}|_B = D$, so $\widetilde{D}$ generates $\widetilde{Der_{A^p}(B)}$. From $(*)$, there are a derivation $D_i \in Der_B(A)$ and an element $a_i \in A$ such that

$$\frac{\partial}{\partial X_i} = D_i + a_i\widetilde{D} \qquad \text{for } i = 1, \ldots, n.$$

Hence, for each i we have

$$\frac{\partial F}{\partial X_i} = a_i\widetilde{D}(F).$$

Now, $F \notin A^p$ implies $a_j \neq 0$ for some j. It follows that

$$(\dagger) \qquad deg\, \widetilde{D}(F) \leq deg\, \frac{\partial F}{\partial X_j} < deg\, F.$$

On the other hand, since $F \in B - A^p$ and $Ker\, D = A^p$ (see [6], Theorem 9 (2)), we obtain

$$(\ddagger) \qquad \widetilde{D}(F) = \widetilde{D}|_B(F) = D(F) \in B - \{0\}.$$

Since the degree of F is minimal in $B - A^p$, the above $(\dagger)$ and $(\ddagger)$ yield that

$$(\star) \qquad D(F) \in A^p - \{0\}.$$

Let t ($t \in B$) be a p-basis of $Q(B)$ over $Q(A^p)$, and let D_t be a derivation of $Q(B)$ over $Q(A^p)$ such that $D_t(t) = 1$. Then, since D_t is a basis of $Der_{Q(A^p)}(Q(B))$, the derivation D is equal to $D(t)D_t$, where D is regarded as the derivation of $Q(B)$ over $Q(A^p)$ by the canonical inclusion map $Der_{A^p}(B) \longrightarrow Der_{Q(A^p)}(Q(B))$. So we have

$$D(t)^{p-1} = \frac{1}{D(F)} D(t)^p D_t(F) \in \bigoplus_{i=0}^{p-2} Q(A^p)t^i.$$

Hence, D is preferable by Lemma 1.2. According to the proof of Theorem 2.2, there exists a p-basis $\{F'\}$ of B over A^p such that $D(F') = 1$. We may assume that F' has no terms of elements in A^p. Writing F as $\sum_{i=0}^{p-1} a_i^p F'^i$ ($a_i \in A$), $(\star)$ implies that $a_2 = a_3 = \cdots = a_{p-1} = 0$. Considering the assumptions for the degree and the terms of F, we have $a_0 = 0$ and $a_1 \in k - \{0\}$. Consequently, $\{F\}$ is a p-basis of B over A^p. □

Remark. The following assertions immediately follow from the proof of Theorem 4.1.

(1) F is unique up to multiplication by elements of $k - \{0\}$.

(2) Any p-basis of B over A^p can be uniquely expressed as $cF + a^p$ ($c \in k - \{0\}$, $a \in A$).

Corollary 4.2 (Kimura-Niitsuma)**.** *Let k and A be as in Theorem 4.1. Let B be a polynomial ring $k[Y_1, \ldots, Y_n]$ which is a subring of A containing A^p such that $[Q(B) : Q(A^p)] = p$ (resp. $[Q(A) : Q(B)] = p$). Then B has a p-basis over A^p (resp. A has a p-basis over B).*

Proof. Suppose $[Q(B) : Q(A^p)] = p$. Recall that B is a Galois extension of A^p (see the proof of Theorem 4.1). By Theorem 9 of [6] $Der_{A^p}(B)$ is afinitely generated and projective as a B-module. By virtue of Quillen's result of [5], $Der_{A^p}(B)$ is free. Therefore the assertion holds by Theorem 4.1.

Next, suppose $[Q(A) : Q(B)] = p$. Then by a similar argument we can show that there is a p-basis $\{F^p\}$ ($F \in A$) of A^p over B^p. Obviously, $\{F\}$ is a p-basis of A over B. □

Remark. In 1990, the above result was first announced by T. Kimura and H. Niitsuma.

References

[1] T. Kimura and H. Niitsuma, *On Kunz's conjecture*, J. Math. Soc. Japan **34** (1982), 371–378. MR **83h:**13030

[2] ———, *A note on p-basis of polynomial ring in two variable*, SUT J. Math. **25** (1989), 33–38. MR **91a:**13002

[3] E. Kunz, *Kähler Differentials*, Vieweg Advanced Lectures in Math., 1986. MR **88e:**14025

[4] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986. MR **88h:**13001

[5] D. Quillen, *Projective modules over polynomial rings*, Invent. Math. **36** (1976), 167–171. MR **55:**337

[6] S. Yuan, *Inseparable Galois theory of exponent one*, Trans. Amer. Math. Soc. **149** (1970), 163–170. MR **41:**1717

Tokyo Metropolitan College of Aeronautical Engineering 8-52-1, Minami-senju, Arakawa-ku, Tokyo 116-0003, Japan

E-mail address: tono@kouku-k.ac.jp