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 $\text{Der}_{A^p}(B)$ 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 $\text{Spec} R$ and $\text{Spec} R'$ by Lemma 1 of [6]. So, for any given $p \in \text{Spec} R$, we denote by $p'$ the corresponding element in $\text{Spec} R'$, i.e., $p' = p \cap R'$.

A subset $\{x_1, \ldots, x_t\}$ of $R$ is said to be a $p$-basis of $R$ over $R'$ if the monomials $x_1^{e_1} \cdots x_t^{e_t}$ $(0 \leq e_i \leq p - 1)$ are linearly independent over $R'$ and $R = R'[x_1, \ldots, x_t]$. If, for each $p \in \text{Spec} R$, there exists a $p$-basis of $R_p$ over $R'_p$, we say that $R$ has locally $p$-bases 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 $p \in \text{Spec} R$ the localization $R_p$ at $p$ also has a $p$-basis over $R'_p$. 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 $\text{Der}_R(R)$ 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 $\phi_S$ and $\tau_S$ the canonical
maps $R \to R_S$ and $\text{Der}_{R'}(R) \to \text{Der}_{R'}(R_S)$, respectively. In particular, when $S$ is a multiplicatively closed subset $\{f^n\}_{n \geq 0}$ (for $f \in R$), resp. $R - p$, we denote by $\phi_f$ and $\tau_f$, resp. $\phi_p$ and $\tau_p$ (or simply $\phi$ and $\tau$), the previous canonical maps. Note that $\tau_S(D)(\phi_S(x)) = \phi_S(D(x))$ for any $x \in R$ and any $D \in \text{Der}_{R'}(R)$.

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 $\{\phi_S(s_1^{-1}x_1), ..., \phi_S(s_l^{-1}x_l)\}$ 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 $\delta_{ij}$ is Kronecker’s delta. This set forms a basis for $\text{Der}_{R'}(R)$. 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 $\{m\}$ be the set of all maximal ideals of $R$. We call $D \in \text{Der}_{R'}(R)$ the preferable derivation, if for each $m$ there is a $p$-basis $\{\phi_m(x)\} \ (x \in R)$ of $R_m$ over $R'_m$, such that $\phi_m(D(y))p^{-1} \in \bigoplus_{i=0}^{m-2} R'_m \phi_m(x)^i$.

**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 $D \in \text{Der}_{R'}(R)$ is preferable, then $\phi_S(D(x))p^{-1} \in \bigoplus_{i=0}^{m-2} R'_S \phi_S(x)^i$.

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

Now, the fact (2) says that $\{\phi(x)\}$ is a p-basis of $R_p$ over $R'_p$. Hence, there is a unique basis $\{D_{\phi(x)}\}$ of $\text{Der}_{R'_p}(R_p)$ 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:

$$
\phi(D(x))p^{-1} = \{\tau_p(D)(\phi(x))\}p^{-1} = \{\phi(D(y))D_{\phi(y)}(\phi(x))\}p^{-1} = D_{\phi(y)}(z)D_{\phi(y)}(\phi(x))p^{-1} = \{D_{\phi(y)}(\phi(x))D_{\phi(y)}(z)\}D_{\phi(y)}(\phi(x))p^{-1} = D_{\phi(y)}(\phi(x))pD_{\phi(y)}(z).
$$

Thus $\phi(D(x))p^{-1}$ is contained in $\bigoplus_{i=0}^{p-2} R'_p \phi(x)^i$. 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 $p$ an element $t$ of $R' - p'$ such that $c_{p-1}t = 0$, i.e., $\phi(c_{p-1}) = 0$. This implies that $\phi_S(c_{p-1}) = 0$. Therefore $\phi_S(D(x))p^{-1} \in \bigoplus_{i=0}^{p-2} R'_S \phi_S(x)^i$. \qed
Lemma 1.2. Suppose $R$ is reduced and has locally $p$-bases over $R'$. Let $\{q\}$ be the set of all minimal prime ideals belonging to the zero ideal $(0)$, and let $\{\phi_q(x)\}$ $(x \in R)$ be a $p$-basis of $R_q$ over $R_q'$. If $D \in \text{Der}_{R'}(R)$ satisfies that for each $q$

$$\phi_q(D(x))^{p-1} \in \bigoplus_{i=0}^{p-2} R_q' \phi_q(x)^i,$$

then $D$ is preferable.

Proof. Let $m$ be a maximal ideal of $R$, and let $\{\phi_m(y)\}$ $(y \in R)$ be a $p$-basis of $R_m$ over $R_m'$. By the same argument as in the proof of Lemma 1.1, we see that $\phi_q(D(y))^{p-1} \in \bigoplus_{i=0}^{p-2} R_q' \phi_q(y)^i$ for each $q$ contained in $m$. Writing $\phi_m(D(y))^{p-1}$ as $\sum_{i=0}^{p-1}(c_i/s_i)\phi_m(y)^i$ ($c_i \in R'$, $s_i \in R' - m'$), there exists an element $t$ of $R' - q'$ such that $c_{p-1}t = 0$. This means that $c_{p-1} \in \bigcap_{i \in A} q_i$. Since $R$ is reduced, the localization $R_{m'}$ of $R'$ is also, i.e., the nilradical $\bigcap_{i \in A} q_i R_{m'}$ 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

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

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:

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

Hence, we get the following recurrence formula:

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

It follows that

$$(aD)^{p-2}(a) = -D(b_{p-1,2}) = -D(-D(b_{p-1,3})) = \ldots = (-1)^{p-3}D^{p-3}(-D(a^{p-1})) = (-1)^{p-2}D^{p-2}(a^{p-1}).$$

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

\[\square\]
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 $\text{Der}_{R'}(R)$ has a basis $D$ such that $D^p = 0$.
3. $R$ has locally $p$-bases over $R'$ and $\text{Der}_{R'}(R)$ has a basis which consists of one preferable derivation.

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

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

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

By virtue of Lemma 2.1, we have

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

Hence, the following equation is obtained:

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

Now, $\phi(D(x))$ is a unit in $R_m$, because $\tau_m(D)$ forms a basis for $\text{Der}_{R'_m}(R_m)$. From this $D^p = 0$ implies $D_{\phi(x)}^{p-1}(\phi(D(x))^{p-1}) = 0$. Thus $D$ is preferable.

(3) $\Rightarrow$ (1). Let $\{p\}$ be the set of all prime ideals of $R$, and for each $p$ let $\{\phi(x)\}$ ($x \in R$) be a $p$-basis of $R_p$ over $R'_p$, where $\phi$ is the canonical map $R \longrightarrow R_p$. Let $D$ be a preferable derivation which is a basis of $\text{Der}_{R'}(R)$. Since $R$ is a finitely presented $R'$-module, $\tau_m(D)$ forms a basis for $\text{Der}_{R'_m}(R_m)$ as in the proof of (2) $\Rightarrow$ (3), so $D(x) \notin p$. We claim that $\text{Ker} D = R'$. 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 $\text{Der}_{R'_m}(R_f)$ such that $\text{Ker} D_{(f)} = R'_f$ and $D_{(f)}(\phi_f(x)) = 1$. Moreover, $\tau_{f,p}(D_{(f)}) = (\tau_{f,p}(D_{(f)}))^{p} = (\phi_{(f)}(p))^{p} = 0$ for any prime ideal $p$ which does not contain $f$, where $\tau_{f,p}$ is the canonical map $\text{Der}_{R'_m}(R_f) \longrightarrow \text{Der}_{R'_p}(R_p)$. By Theorem 27.3 (i) of [4], $\{\phi_f(x)\}$ is a $p$-basis of $R_f$ over $R'_f$.

Now, since $\text{Spec} R'$ is quasi-compact, we can take a finite subset $\{f_1, \ldots, f_m\}$ of $\{f\}_{p \in \text{Spec} R}$ and a finite subset $\{g_1, \ldots, g_m\}$ of $R'$ 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 $\phi_{f_j}(D(x_j))^{p-1} = \bigoplus_{i=0}^{p-2} R'_f \phi_{f_j}(x_j)^i$ for each $j$. Hence, we can write $\phi_{f_j}(D(x_j))^{p-1}$ as $\sum_{i=0}^{p-2} (i+1)c_{ij}x_j^i$, where $c_{ij}$ $(0 \leq i \leq p-1, 1 \leq j \leq m)$ are elements of $R'$ and $n_{ij}$ $(1 \leq j \leq m)$ are non-negative integers. There exists a positive integer $e$ such that $p^e \geq n_{ij} + 1$ and $f_j^{p^e-n_{ij}} \{f_j^{n_{ij}}D(x_j)^{p-1} - \sum_{i=0}^{p-2}(i+1)c_{ij}x_j^i\} = 0$.
for all $j$. Here, put $z = \sum_{j=1}^{m} g_j^p (z^p - n_j^{-1} c_{ij} x_j^{i+1})$. Then we have

$$D(z) = \sum_{j=1}^{m} g_j^p \left( \sum_{i=0}^{p-2} (i+1) f_j^p x_j^i \right) D(x_j)$$

$$= \sum_{j=1}^{m} g_j^p (f_j^p - 1) D(x_j)$$

$$= \sum_{j=1}^{m} f_j^p g_j^p = 1.$$

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 $\text{Der}_{R'}(R)$, 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. $\text{Der}_{R'}(R)$ has a basis $D$ such that $D^p = 0$.
3. $\text{Der}_{R'}(R)$ 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 $\text{Der}_{R'}(R)$. Then the following holds:

1. $R$ is a Galois extension of $\text{Ker} D$.
2. $\text{Ker} D$ is a Galois extension of $R'$.
3. $RD = \text{Der}_{R'}(R)$.

**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 $\text{Der}_{R'}(R)$. Theorem 12 of [6] says that $R$ is a Galois extension of $\text{Ker} D$ and $RD = \text{Der}_{R'}(R)$. Therefore $\text{Ker} D$ 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 $\text{Der}_{R'}(R)$ 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) ⇒ (2). This immediately follows from fact (3) in §1.
(2) ⇒ (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_i\} for $R$ 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 $\{D_i|_{R_1}\}_{i=2,...,l}$ forms a basis for $Der_{R_1}(R)$. First of all, we claim that $D_i|_{R_1} \in Der_{R_1}(R_1)$ 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 $\{D_1, \ldots, D_l\}$ is a basis of $Der_{R_1}(R)$. Thus $D_i|_{R_1} \neq 0$. Let $m$ be a maximal ideal of $R$ and let $n$ be the maximal ideal $m \cap R_1$ of $R_1$. Since $R_1$ is a Galois extension of $R'$ by Lemma 3.1, there is a subset $\{y_2, \ldots, y_l\}$ of $R_{ln}$ which is a $p$-basis of $R_{ln}$ over $R'_{ln}$. Obviously, $\{\phi_m(x_1), y_2, \ldots, y_l\}$ is a $p$-basis of $R_m$ over $R'_{m}$. Let $D_{\phi_m(x_1)}, D_{y_2}, \ldots, D_{y_l}$ be the derivations of $R_m$ over $R'_{m}$ associated with this $p$-basis (see fact (3) in §1). Denote by $D_j'$ the derivation $D_{y_j}|_{R_1n}$ of $R_1$ over $R'_{m}$. Then $\tau_n(D_i|_{R_1})$ is written as $\sum_{i=2}^l a_{ij} D_j'$ for each $i \geq 2$ where $a_{ij} \in R_{1n}$, because $\{D_j'\}_{j=2,...,l}$ forms a basis for $Der_{R'_{ln}}(R_{ln})$. Since $R$ is finitely presented as an $R'$-module, the module $Der_{R'_{m}}(R_m)$ is isomorphic to $Der_{R'}(R) \otimes_R R_m$. Hence, $\{\tau_n(D_1), \ldots, \tau_n(D_l)\}$ forms a basis for $Der_{R'_{m}}(R_m)$, so the derivation $D_{y_j}$ is expressed as $\sum_{i=1}^l b_{ji} \tau_n(D_i)$ for each $j \geq 2$ where $b_{ji} \in R_m$. For each $j \geq 2$ we have

$$D_j' = \sum_{i=1}^l b_{ji} \tau_n(D_i)|_{R_1n} = \sum_{i=2}^l b_{ji} \tau_n(D_i|_{R_1}).$$

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., $b_{ji} \in R_{1n}$. Thus, for any maximal ideal $n$ of $R_1$, $\{\tau_n(D_i|_{R_1})\}_{i=2,...,l}$ is a basis of $Der_{R'_{m}}(R_{ln})$. This implies that $\{D_i|_{R_1}\}_{i=2,...,l}$ forms a basis for $Der_{R_1}(R_1)$.

Set $R_h = Ker D_1 \cap \cdots \cap Ker D_h$ for $h = 2, \ldots, l$. 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, $\{x_1, \ldots, x_l\}$ is a $p$-basis of $R$ over $R'$.

\[\square\]

**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 $\{D_1, \ldots, D_l\}$ such that $D_i^p = 0$ and $[D_i, D_j] = 0$ for any $i, j = 1, 2, \ldots, l$.

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

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 $k[X_1, \ldots, X_n]$, 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 $A^p$, and $B$ is also by Theorem 11 (1) of [6].

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

\[
\text{Der}_{A^p}(A) = \text{Der}_B(A) \oplus A \text{Der}_{A^p}(B). 
\]

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

\[
\frac{\partial}{\partial X_i} = D_i + a_i \tilde{D} \quad \text{for } i = 1, \ldots, n.
\]

Hence, for each $i$ we have

\[
\frac{\partial F}{\partial X_i} = a_i \tilde{D}(F).
\]

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

\[(\dagger) \quad \text{deg} \tilde{D}(F) \leq \text{deg} \frac{\partial F}{\partial X_j} < \text{deg} F.\]

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

\[(\ddagger) \quad \tilde{D}(F) = \tilde{D}|_B(F) = D(F) \in B - \{0\}.
\]

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

\[(\ast) \quad D(F) \in A^p - \{0\}.
\]

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 $\text{Der}_{Q(A^p)}(Q(B))$, 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 $\text{Der}_{A^p}(B) \rightarrow \text{Der}_{Q(A^p)}(Q(B))$. 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 $\sum_{i=0}^{p-1} a_pF^i$ ($a_i \in A$), $(\ast)$ 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] $\text{Der}_{A^p}(B)$ is finitely generated and projective as a $B$-module. By virtue of Quillen’s result of [5], $\text{Der}_{A^p}(B)$ 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**


**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