J. Math. Soc. Japan
Vol. 34, No. 2, 1982

On Kunz's conjecture

By Tetsuzo KIMURA and Hiroshi NIITSUMA

(Received May 20, 1981)
(Revised Sept. 25, 1981)

The purpose of this paper is to give an affirmative answer for the following conjecture of Kunz*);

Let R be a regular local ring of characteristic $p>0$ and let R' be a regular subring of R such that R' contains R^p and such that R is a finite R'-module. Does R have a p-basis over R'?

First, we prove the conjecture for the case that R is a finite R^p-module. In this case, we have a technical lemma (see Lemma 4 in §2) which asserts that R has a p-basis over R' if and only if R' is regular and R' has a p-basis over R^p, where R and R' are the same as stated in the above conjecture. Therefore, to prove the conjecture in this case, it is sufficient to show that R' has a p-basis over R^p.

On the other hand, S. Yuan [**10**] defined the inseparable Galois extension as follows;

DEFINITION. Let A be a ring of characteristic p. An A-algebra C is called a Galois extension of A provided

(i) C is finitely generated projective as A-module,

(ii) $t^p \in A$ for all $t \in C$,

(iii) Given any prime ideal $\mathfrak{q}$ in C, then $C_{\mathfrak{q}}$ admits a p-basis over $A_{A\cap\mathfrak{q}}$.

With this definition, he proved the following;

*If $A \subset B \subset C$ is a tower of rings such that C is a Galois extension both over A and B, then B is a Galois extension over A (cf. Theorem 11 of [**10**]).*

However, the proof does not depend on the assumption that $C_{\mathfrak{q}}$ admits a p-basis over $B_{B\cap\mathfrak{q}}$. If R is a regular local ring such that R is a finite R^p-module and if R' is an intermediate regular local ring between R and R^p, then R is a Galois extension of R^p (cf. Corollary 3.2 of [**5**]) and R is a finite free R'-module (cf. Theorem 46 of [**6**]). Hence, Yuan's proof can be used to prove the assertion that R' has a p-basis over R^p. For convenience, we restate Yuan's proof with our notations in our proof (see §3).

The general case of the conjecture is reduced to the case that R is a finite

*) Professor H. Matsumura has kindly communicated to us that he had dropped the assumption $R' \supset R^p$ for the conjecture of Kunz described in §38 of [**6**] by mistake.

R^p-module by the completion and the immersion to a power series ring over an algebraically closed field (see § 3).

The authors would like to express their hearty thanks to Professor H. Matsumura for his encouragement and helpful suggestions.

§ 1. Notations and preliminaries.

In this paper, p is always a prime number and all rings are commutative with identity. A ring is called a local ring if it is noetherian and has only one maximal ideal. Let S be a ring of characteristic p and let S^p denote the subring $\{x^p \mid x \in S\}$. Let S' be a subring of S. A subset $\Gamma \subset S$ is said to be p-independent over S', if the monomials $b_1^{e_1} \cdots b_n^{e_n}$, where $b_1, \cdots, b_n$ are distinct elements of Γ and $0 \leqq e_i \leqq p-1$, are linearly independent over $S^p[S']$. Γ is called a p-basis of S over S' if it is p-independent over S' and $S^p[S', \Gamma]=S$.

From now on throughout this paper, R will denote (except in Lemma 1) a local domain of characteristic p, $\mathfrak{m}$ the maximal ideal of R, k the residue field of R and K the quotient field of R. We denote the Krull dimension of R by $\dim R$ and we put $\dim R=r$. We set $\mathfrak{m}^{(p)}=\{m^p \mid m \in \mathfrak{m}\}$. Since $\mathfrak{m} \cap R^p=\mathfrak{m}^{(p)}$, the natural map $R^p/\mathfrak{m}^{(p)} \to R/\mathfrak{m}=k$ is injective and its image is equal to $(R/\mathfrak{m})^p =k^p=\{\alpha^p \mid \alpha \in k\}$. In view of the above injection, the residue field $R^p/\mathfrak{m}^{(p)}$ of R^p can be identified with the subfield k^p of k. R' will denote an intermediate local ring between R and R^p, $\mathfrak{m}'$ the maximal ideal, k' the residue field and K' the quotient field. It is clear that R dominates R', that is, $\mathfrak{m} \cap R'=\mathfrak{m}'$. Since we may identify the residue field k' of R' with the corresponding subfield of k, we assume that $k^p \subset k' \subset k$. For any subset A of R, we denote by $\bar{A}$ the set of residue classes of the elements of A modulo $\mathfrak{m}$. When we say "$\bar{A}$ is a p-basis" we tacitly assume that A maps injectively to $\bar{A}$.

§ 2. Purely inseparable extension of a local ring.

LEMMA 1. *Let R be a local ring of characteristic p and let R' be an intermediate local ring between R and R^p. Assume that R is a finite R'-module and R has a p-basis over R'. Then there exists a p-basis Γ of R over R' which is of the form $\Gamma=B \cup \{z_1, \cdots, z_s\}$, where B is a system of representatives of a p-basis of the residue field k of R over k', $\{z_1, \cdots, z_s\}$ is a subset of a minimal system of generators for $\mathfrak{m}$ and $s=\operatorname{rank}_k \mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2$.*

PROOF. Let Λ be a p-basis of R over R'. Then we can choose a subset B of Λ such that $\bar{B}$ is a p-basis of k over k', where $\bar{B}$ is the set of residue classes of the elements of B modulo $\mathfrak{m}$ (cf. Exercises of § 8, [**1**]). Then $R'[B]$ is a local ring with maximal ideal $\mathfrak{m}_B=\mathfrak{m}'R'[B]$ by Lemma 2.2 of [**5**]. Set $G =\Lambda-B$. Then G is a p-basis of R over $R'[B]$. Since $R=R'[B]+\mathfrak{m}$, we may assume that $G\subset\mathfrak{m}$. Therefore, we can choose a minimal system of generators for $\mathfrak{m}$ from $\mathfrak{m}'\cup G$. Let $\{z_1, \cdots, z_s, x_{s+1}, \cdots, x_r\}$, $z_i\in G$, $x_j\in\mathfrak{m}'$ $(i=1, \cdots, s, j=s+1, \cdots, r)$ be an arbitrary minimal system of generators for $\mathfrak{m}$ chosen from $\mathfrak{m}'\cup G$. Suppose that $\{z_1, \cdots, z_s\}\subsetneqq G$. Then there is an element $w_1\in G$ such that $w_1\neq z_i$ $(i=1, \cdots, s)$. Since $w_1\in\mathfrak{m}$, we have

$$w_1=\sum_{i=1}^{s}\alpha_i z_i+\sum_{j=s+1}^{r}\beta_j x_j \quad (\alpha_i, \beta_j\in R).$$

Since $G-\{z_1, \cdots, z_s\}$ is a p-basis of R over $R'[B, z_1, \cdots, z_s]$, we have that

$$\alpha_i=\sum_{(e_l)}\alpha_{i(e_l)}\Pi w_l^{e_l} \quad (\alpha_{i(e_l)}\in R'[B, z_1, \cdots, z_s],\ w_l\in G-\{z_1, \cdots, z_s\})$$

and

$$\beta_j=\sum_{(e_l)}\beta_{j(e_l)}\Pi w_l^{e_l} \quad (\beta_{j(e_l)}\in R'[B, z_1, \cdots, z_s],\ w_l\in G-\{z_1, \cdots, z_s\}).$$

From these three relations and p-independence of $G-\{z_1, \cdots, z_s\}$ over $R'[B, z_1, \cdots, z_s]$, we have an equality $1=\sum\alpha_{i(e_l)}z_i+\sum\beta_{j(e_l)}x_j$. This is a contradiction. That is, $G=\{z_1, \cdots, z_s\}$.

On the other hand, the sequence of k-module

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2 \longrightarrow \Omega_{R/R'}\otimes k \longrightarrow \Omega_{k/k'} \longrightarrow 0$$

is exact (cf. Rangsatz of [3] and Lemma 3 of [8]). Since R has a p-basis consisting of $s+|B|$ elements, $\Omega_{R/R'}$ is a free module of rank $s+|B|$ (cf. 38. A of [6]). Similarly, $\mathrm{rank}_k\Omega_{k/k'}=|B|$. Therefore we have

$$\begin{aligned}\mathrm{rank}_k\mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2&=\mathrm{rank}_k\Omega_{R/R'}\otimes k-\mathrm{rank}_k\Omega_{k/k'}\\&=s.\end{aligned}$$

LEMMA 2. *Let R be a regular local ring of characteristic p with* $\dim R=r$ *and let R' be an intermediate regular local ring between R and R^p. If there is a system of representatives C of a p-basis of k' over k^p such that $[K' : K^p(C)]=p^{r-s}$, where $s=\mathrm{rank}_k\mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2$, then R' has a p-basis over R^p.*

PROOF. By Lemma 2.4 and Lemma 2.5 of [5], $R^p[C]$ is a regular local ring with maximal ideal $\mathfrak{m}_c=\mathfrak{m}^{(p)}R^p[C]$. Put $s=\mathrm{rank}_k\mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2$. Then, there is a minimal system of generators $\{z_1, \cdots, z_s, x_{s+1}, \cdots, x_r\}$ for $\mathfrak{m}$, where $z_1, \cdots, z_s\in\mathfrak{m}$ and $x_{s+1}, \cdots, x_r\in\mathfrak{m}'$. Suppose that we could choose $y_1, \cdots, y_l$ $(l<r-s)$ in such a way that

(a) $y_i=x_{s+i}$ or $y_i=u_i x_{s+i}$ for $i=1, \cdots, l$, where u_i is a unit in R' (and therefore $\{y_1, \cdots, y_l\}$ is a subset of a minimal system of generators for $\mathfrak{m}$),

(b) $\{y_1, \cdots, y_l\}$ is p-independent over $K^p(C)$, and

(c) $R_l=R^p[C, y_1, \cdots, y_l]$ is a regular local ring with maximal ideal $\mathfrak{m}_l=\mathfrak{m}\cap R_l=\mathfrak{m}_c+(y_1, \cdots, y_l)R_l$.

Then we will prove that there exists an element $y_{l+1} \in R'$ which satisfies the following three properties;

(a) $\{y_1, \cdots, y_{l+1}\}$ is a subset of a minimal system of generators for $\mathfrak{m}$,

(b) $\{y_1, \cdots, y_{l+1}\}$ is p-independent over $K^p(C)$,

(c) $R_{l+1} = R^p[C, y_1, \cdots, y_{l+1}]$ is a regular local ring with maximal ideal $\mathfrak{m}_{l+1} = \mathfrak{m} \cap R_{l+1} = \mathfrak{m}_c + (y_1, \cdots, y_{l+1})R_{l+1}$.

Since $\bar{C}$ is a p-basis of k' over k^p, we have $R' = R^p[C] + \mathfrak{m}'$, $K' = K^p(C, \mathfrak{m}')$ and $[K' : K^p(C, y_1, \cdots, y_l)] = p^{r-s-l} \geqq p$. If $x_{s+l+1} \notin K^p(C, y_1, \cdots, y_l)$, we put $y_{l+1} = x_{s+l+1}$. Otherwise, we choose an element $m' \in \mathfrak{m}'$ such that $m' \notin K^p(C, y_1, \cdots, y_l)$. Let $u_{l+1} = 1 + m'$. Then u_{l+1} is a unit of R' and $u_{l+1} \notin K^p(C, y_1, \cdots, y_l)$. In this case, we set $y_{l+1} = u_{l+1} x_{s+l+1}$. In both cases, $y_{l+1} \in \mathfrak{m}'$ and $y_{l+1} \notin K^p(C, y_1, \cdots, y_l)$, that is, y_{l+1} is p-independent over $K^p(C, y_1, \cdots, y_l)$. We claim that $R_{l+1} = R^p[C, y_1, \cdots, y_{l+1}]$ is a regular local ring with maximal ideal $\mathfrak{m}_{l+1} = \mathfrak{m} \cap R_{l+1} = \mathfrak{m}_c + (y_1, \cdots, y_{l+1})R_{l+1}$. It is obvious that $\mathfrak{m}_{l+1} = \mathfrak{m}_c + (y_1, \cdots, y_{l+1})R_{l+1}$. To prove that $R_{l+1} = R_l[y_{l+1}]$ is regular, it is sufficient to show $y_{l+1}^p \notin \mathfrak{m}_l^2$ by 38.4 of [7]. Suppose that $y_{l+1}^p \in \mathfrak{m}_l^2$. Since $\mathfrak{m}_l = \mathfrak{m}_c + (y_1, \cdots, y_l)R_l$,

$$\mathfrak{m}_l^2 = (\mathfrak{m}^{(p)})^2 R^p[C] + \mathfrak{m}^{(p)}(y_1, \cdots, y_l)R_l + (y_1, \cdots, y_l)^2 R_l .$$

Then we have

$$y_{l+1}^p = \sum \alpha_{(n_\iota)}^p \prod c_\iota^{n_\iota} + \sum \beta_{(n_\iota)(e_j)}^p \prod c_\iota^{n_\iota} \prod y_j^{e_j} + \sum \gamma_{(n_\iota)(f_j)}^p \prod c_\iota^{n_\iota} \prod y_j^{f_j}$$

where $c_\iota \in C$, $\alpha_{(n_\iota)} \in \mathfrak{m}^2$, $\beta_{(n_\iota)(e_j)} \in \mathfrak{m}$, $\gamma_{(n_\iota)(f_j)} \in R$, $\sum e_j \geqq 1$ and $\sum f_j \geqq 2$. Regarding the p-th powers of c_ι and y_j as elements of R^p, we have

$$y_{l+1}^p = \sum \eta_{(m_\iota)}^p \prod c_\iota^{m_\iota} + \sum \xi_{(m_\iota)(g_j)}^p \prod c_\iota^{m_\iota} \prod y_j^{g_j} + \sum \zeta_{(m_\iota)(h_j)}^p \prod c_\iota^{m_\iota} \prod y_j^{h_j}$$

where $c_\iota \in C$, $\eta_{(m_\iota)} \in \mathfrak{m}^2$, $\xi_{(m_\iota)(g_j)} \in \mathfrak{m}$, $\zeta_{(m_\iota)(h_j)} \in R$ and $0 \leqq m_\iota, g_j, h_j \leqq p-1$. Since $\sum e_j \geqq 1$ and $\sum f_j \geqq 2$, we have $\xi_{(0)(0)} \in \mathfrak{m}^2$ and $\zeta_{(0)(0)} \in \sum_{i=1}^{l} y_i R$. Because of p-independence of $\{C, y_1, \cdots, y_l\}$ over K^p, it follows that

$$y_{l+1} = \eta_{(0)} + \xi_{(0)(0)} + \zeta_{(0)(0)} .$$

Set $\zeta_{(0)(0)} = \sum_{i=1}^{l} d_i y_i$, where $d_i \in R$. Then we have $y_{l+1} - \sum_{i=1}^{l} d_i y_i \in \mathfrak{m}^2$. This is a contradiction because $\{y_1, \cdots, y_{l+1}\}$ is a subset of a minimal system of generators for $\mathfrak{m}$.

Thus we have proved that there exist $y_1, \cdots, y_{r-s} \in R'$ which satisfy the following three properties;

(a) $\{y_1, \cdots, y_{r-s}\}$ is a part of a minimal system of generators for $\mathfrak{m}$,

(b) $\{y_1, \cdots, y_{r-s}\}$ is p-independent over $K^p(C)$ (that is, the field of quotients of $R_{r-s} = R^p[C, y_1, \cdots, y_{r-s}]$ is K'),

(c) $R_{r-s} = R^p[C, y_1, \cdots, y_{r-s}]$ is a regular local ring with maximal ideal

$\mathfrak{m}_{r-s}=\mathfrak{m}_c+(y_1, \cdots, y_{r-s})R_{r-s}$.

Since R_{r-s} is normal and R' is integral over R_{r-s}, we have $R'=R_{r-s}$. It follows that $\{C, y_1, \cdots, y_{r-s}\}$ is a p-basis of R' over R^p.

LEMMA 3. *Let R be a local ring of characteristic p such that R is a finite R^p-module and let R' be an intermediate local ring between R and R^p. Then, R' is a finite R^p-module and hence R' is a finite R'^p-module.*

PROOF. Since R^p is a noetherian ring and R a finite R^p-module, the submodule R' of R is a finite R^p-module.

LEMMA 4. *Let R be a regular local ring of characteristic p such that R is a finite R^p-module. Let R' be an intermediate local ring between R and R^p. Then the following conditions are equivalent:*

(i) *R has a p-basis over R'.*

(ii) *R' is regular and $[K: K']=p^{l+s}$, where $[k : k']=p^l$ and $s=\mathrm{rank}_k\mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2$.*

(iii) *R' is regular and R' has a p-basis over R^p.*

PROOF. (i) $\Rightarrow$ (ii). By Theorem 51 of [**6**], R' is regular. $[K: K']=p^{l+s}$ follows from Lemma 1. (ii) $\Rightarrow$ (iii). We have only to show that R' has a p-basis over R^p. Let B be a subset of R such that $\bar{B}$ is a p-basis of k over k' and let C be a subset of R' such that $\bar{C}$ is a p-basis of k' over k^p. Since $|B|=l$, we have $[K: K'(B)]=p^s$. On the other hand, it holds that $[K: K^p]=p^{|B\cup C|+r}$ by Theorem 3.1 of [**5**]. Then we have $[K' : K^p(C)]=p^{r-s}$. Thus R' has a p-basis over R^p by Lemma 2. (iii) $\Rightarrow$ (i). R' is a finite R'^p-module by Lemma 3. We have already proved (i) $\Rightarrow$ (iii). Replacing R^p, R' and R by R'^p, R^p and R' respectively, it follows from the implication (i) $\Rightarrow$ (iii) that R^p has a p-basis over R'^p. Then obviously R has a p-basis over R'. This completes the proof.

§ 3. Proof of the conjecture.

THEOREM. *Let R be a regular local ring of characteristic $p>0$ and let R' be a regular subring of R such that R contains R^p and such that R is a finite R'-module. Then R has a p-basis over R'.*

PROOF FOR THE CASE WHERE R IS A FINITE R^p-MODULE. In this case, it is sufficient to show that R' has a p-basis over R^p by Lemma 4. The assertion that R' has a p-basis over R^p follows from the same argument that S. Yuan used in the proof of Theorem 11 of [**10**]. We restate it below for convenience.

For simplicity of notations, we put $\tilde{R}'=R'/\mathfrak{m}^{(p)}R'$ and $\tilde{R}=R/\mathfrak{m}^{(p)}R$. In view of Theorem 46 of [**6**], R is a finite free R'-module, so that $\tilde{R}$ is a finite free $\tilde{R}'$-module. Let $b_1, \cdots, b_n$ be a basis for the free $\tilde{R}'$-module. Let ∂ be a k^p-derivation on $\tilde{R}$. For any $x\in\tilde{R}'$, ∂x may be expressed in the form $(\partial_1 x)b_1+\cdots$

$+(\partial_n x)b_n$ with $\partial_i x \in \tilde{R}'$. It is easily seen that the map $x \mapsto \partial_i x$ is a k^p-derivation on $\tilde{R}'$ for each i. Now, since R has a p-basis over R^p (cf. Corollary 3.2 of [**5**]), R is a Galois extension over R^p. Then we have $\mathrm{Hom}_{R^p}(R, R)=R[D]$ by Theorem 9 of [**10**], where $D=\mathrm{Der}_{R^p}(R)$. Hence, we have $\mathrm{Hom}_{k^p}(\tilde{R}, \tilde{R})=\tilde{R}[\tilde{D}]$, where $\tilde{D}=D/\mathfrak{m}^{(p)}D$. So no nontrivial ideal in $\tilde{R}$ is stable under $\tilde{D}$. Let I be a nonzero proper ideal in $\tilde{R}'$. Then there is a k^p-derivation ∂ on $\tilde{R}$ such that $\partial(I\tilde{R})$ is not contained in $I\tilde{R}$. This means $\partial_i I$ cannot be contained in I for some i. Thus $\tilde{R}'$ is a differentiably simple ring. And so by Corollary 2.8 of [**9**], $\tilde{R}'$ has a p-basis over k^p. Let A be a set of representatives in R' of a p-basis of $\tilde{R}'$ over k^p. Then $R'=R^p[A]$ by the lemma of Nakayama. Since R' is a free R^p-module, every minimal basis of R' is linearly independent over R^p. Hence A is a p-basis of R' over R^p (cf. [**2**], Chap. II, § 3, Corollaire 1 of Proposition 5). This completes the proof.

PROOF FOR THE GENERAL CASE. We first prove the following lemma.

LEMMA 5. *Let R be a regular local ring of characteristic p and let R' be an intermediate local ring between R and R^p such that R is a finite R'-module. If R' is regular, then $\mathfrak{m}'=\mathfrak{m}^{(p)}R'$ or $\mathfrak{m}' \not\subset \mathfrak{m}^2$.*

PROOF. First we assume that R is a finite R^p-module. If R' is regular, then R has a p-basis over R' by the above proof. By Lemma 1, there exists a p-basis of R over R' which is of the form $\Gamma=B\cup\{z_1, \cdots, z_s\}$, where B is a system of representatives of a p-basis of residue field k of R over k', $\{z_1, \cdots, z_s\}$ is a subset of a minimal system of generators for $\mathfrak{m}$ and $s=\mathrm{rank}_k \mathfrak{m}/\mathfrak{m}'R+\mathfrak{m}^2$. If $s<r$, there is a minimal system of generators for $\mathfrak{m}$, $\{z_1, \cdots, z_s, x_{s+1}, \cdots, x_r\}$, where $x_j \in \mathfrak{m}'$ $(j=s+1, \cdots, r)$. Then $\mathfrak{m}' \not\subset \mathfrak{m}^2$. If $s=r$, $\log_p[K' : K^p]=\log_p[k' : k^p]$, because we have $\log_p[K : K^p]=|C|+|B|+r$ by Theorem 3.1 of [**5**], where C is a system of representatives of a p-basis of k' over k^p. By Lemma 2.4 and Lemma 2.5 of [**5**], $R^p[C]$ is regular. Then, $R^p[C]=R'$. Therefore we have $\mathfrak{m}'=\mathfrak{m}^{(p)}R'$ by Lemma 2.2 of [**5**].

In the general case, let B be a subset of R such that $\bar{B}$ is a p-basis of k over k'. Since $R'[B]$ is regular by Lemma 2.4 and Lemma 2.5 of [**5**], we may assume that $k=k'$. Since the completion $\hat{R}$ is faithfully flat over R and $\hat{R}'$ is faithfully flat over R', in order to prove that $\mathfrak{m}'=\mathfrak{m}^{(p)}R'$ or $\mathfrak{m}' \not\subset \mathfrak{m}^2$, we may assume that R and R' are complete. That is, we assume that $R=k[[Z_1, \cdots, Z_r]]$ and $R'=k[[Y_1, \cdots, Y_r]]$ where $\{Z_1, \cdots, Z_r\}$ and $\{Y_1, \cdots, Y_r\}$ are variables over k respectively and $Z_i^p \in R'$ for $i=1, \cdots, r$. Let $\bar{k}$ be the algebraic closure of k. Then we have

$$\bar{k}[[Z_1, \cdots, Z_r]]/(Z_1, \cdots, Z_r)^\nu=\bar{k}\otimes_k(k[[Z_1, \cdots, Z_r]]/(Z_1, \cdots, Z_r)^\nu).$$

It follows from Local criteria of flatness that $\bar{k}[[Z_1, \cdots, Z_r]]$ is faithfully flat over $k[[Z_1, \cdots, Z_r]]$. Therefore, we may assume that $R=\bar{k}[[Z_1, \cdots, Z_r]]$ and $R'=\bar{k}[[Y_1, \cdots, Y_r]]$. In this case, we have that $\mathfrak{m}'=\mathfrak{m}^{(p)}R$ or $\mathfrak{m}' \not\subset \mathfrak{m}^2$ by the finite case.

PROOF OF THE THEOREM. We prove the theorem by induction on $\dim R=r$. When $r=0$ the assertion is trivial. Assume $r>0$. We have either $\mathfrak{m}'=\mathfrak{m}^{(p)}R'$ or $\mathfrak{m}'\not\subset\mathfrak{m}^2$ by the preceding lemma.

First, suppose that $\mathfrak{m}'=\mathfrak{m}^{(p)}R'$. Let B be a subset of R such that $\bar{B}$ is a p-basis of k over k'. Since $R'[B]$ is regular by Lemma 2.4 and Lemma 2.5 of [**5**], we may assume that $k=k'$. Let $\{z_1, \cdots, z_r\}$ be a regular system of parameters of R and let $\hat{R}$ and $\hat{R}'$ be the $\mathfrak{m}$-adic and $\mathfrak{m}'$-adic completion of R and R' respectively. Since R is finite over R', we have $\hat{R}=R\otimes_{R'}\hat{R}'$. Hence we have $\hat{R}=k[[Z_1, \cdots, Z_r]]$ and $\hat{R}'=k[[Z_1^p, \cdots, Z_r^p]]$, where $Z_1, \cdots, Z_r$ are indeterminates. Therefore, $z_1, \cdots, z_r$ are p-independent over R'. If $R'[z_1, \cdots, z_r]$ is regular, we have $R=R'[z_1, \cdots, z_r]$, because $[K:K']=p^r$. In fact, the maximal ideal of $R'[z_1, \cdots, z_r]$ is generated by r elements $z_1, \cdots, z_r$ and the Krull dimension of $R'[z_1, \cdots, z_r]$ is r, hence $R'[z_1, \cdots, z_r]$ is regular.

Next, suppose that $\mathfrak{m}'\not\subset\mathfrak{m}^2$. We assume that it holds for the case of Krull dimension $r-1$. Since $\mathfrak{m}'\not\subset\mathfrak{m}^2$, we may choose an element y_1 of $\mathfrak{m}'$ such that $y_1\notin\mathfrak{m}^2$. Then R/y_1R and R'/y_1R' are regular local rings of Krull dimension $r-1$. Since R is faithfully flat over R', $y_1R\cap R'=y_1R'$ and so $R/y_1R\supset R'/y_1R'$. Therefore by the induction hypothesis R/y_1R has a p-basis, say $\bar{P}$, over R'/y_1R'. If P is a set of representatives of $\bar{P}$ in R, then the same argument as at the end of the proof for the finite case shows that P is a p-basis of R over R'.

COROLLARY 1. *Let R be a regular local ring of characteristic p such that R is a finite R^p-module and let R' be an intermediate local ring between R and R^p. Then R' is regular if and only if R' is generated over R^p by a subset of a p-basis of R over R^p.*

PROOF. If R' is regular, there exists a p-basis of R over R' by Theorem. Then by Lemma 4, there exists a p-basis of R' over R^p. The union of these two p-basis is a p-basis of R over R^p. Thus R' is generated over R^p by a subset of a p-basis of R over R^p.

Conversely, if R' is generated over R^p by a subset of a p-basis of R over R^p, then R has a p-basis over R'. Therefore, R' is regular by Theorem 51 of [**6**].

Similarly, we have

COROLLARY 2. *Let k be a field of characteristic p, let $R=k[[X_1, \cdots, X_n]]$ and let R' be an intermediate local ring between R and $k[[X_1^p, \cdots, X_n^p]]$. Then R' is regular if and only if, after a suitable change of variables in R, R' is of the form $R'=k[[X_1, \cdots, X_s, X_{s+1}^p, \cdots, X_n^p]]$.*

References

[1] N. Bourbaki, Algèbre, Chap. 5, Hermann, Paris, 1959.
[2] N. Bourbaki, Algèbre commutative, Chap. 1, 2, Hermann, Paris, 1961.
[3] E. Kunz, Die Primidealteiler der differenten in allgemeinen Ringen, J. Reine Angew. Math., **204** (1960), 165-182.
[4] E. Kunz, On noetherian rings of characteristic p, Amer. J. Math., **98** (1976), 999-1013.
[5] T. Kimura and H. Niitsuma, Regular local ring of characteristic p and p-basis, J. Math. Soc. Japan, **32** (1980), 363-371.
[6] H. Matsumura, Commutative Algbra (Second Edition), Benjamin, New York, 1980.
[7] M. Nagata, Local Rings, Interscience Tracts in Pure and Applied Math., No. 13, 1962.
[8] S. Suzuki, Some results on Hausdorff $\mathfrak{m}$-adic modules and $\mathfrak{m}$-adic differentials, J. Math. Kyoto Univ., **2-2** (1963), 157-182.
[9] S. Yuan, Differentiably simple rings of prime characteristic, Duke Math. J, **31** (1964), 623-630.
[10] S. Yuan, Inseparable Galois theory of exponent one, Trans. Amer. Math. Soc., **149** (1970), 163-170.

Tetsuzo KIMURA
Nippon Kogyo Daigaku
Miyashiro-machi, Saitama 345
Japan

Hiroshi NIITSUMA
Nippon Kogyo Daigaku
Miyashiro-machi, Saitama 345
Japan