J. Math. Soc. Japan
Vol. 32, No. 2, 1980

Regular local ring of characteristic p and p-basis

By Tetsuzo KIMURA and Hiroshi NIITSUMA

(Received July 14, 1978)
(Revised March 2, 1979)

Let p be always a prime number, R a local ring of characteristic p and R' an intermediate local ring between R and R^p. A p-basis of R over R' means a subset Γ of R such that $R'[\Gamma]=R$ and such that for every finite subset $\{b_1, \cdots, b_s\}$ of Γ, $\{b_1^{n_1}\cdots b_s^{n_s} \mid 0 \leqq n_i < p\}$ is linearly independent over R'. The purpose of this paper is to prove the following two theorems:

THEOREM 3.1. *Let R be a regular local ring of characteristic p and let k be the residue field of R. If there is a system of representatives A of a p-basis of k over k^p such that R is a finite $R^p[A]$-module, then R has a p-basis over R^p. More precisely, a p-basis of R over R^p is obtained as the union of $\{z_1, \cdots, z_r\}$ and A where $r=\dim R$ and $\{z_1, \cdots, z_r\}$ is a special minimal system of generators for the maximal ideal of R.*

Conversely, if R is a reduced local ring of characteristic p and if R has a p-basis Γ over R^p, then R is a regular local ring and Γ is of the form $\Gamma= A\cup\{z_1+v_1, \cdots, z_r+v_r\}$, $v_i\in R^p[A]$ $(i=1, \cdots, r)$, where A is a system of representatives of a p-basis of the residue field k of R over k^p and $\{z_1, \cdots, z_r\}$ is a minimal system of generators for the maximal ideal of R.

THEOREM 3.4. *Let R be a locality[1)] over a field of characteristic p. Then R is regular if and only if R has a p-basis over R^p.*

To prove the first half of Theorem 3.1, we need two results due to M. Nagata. We record the results in §1 as Proposition 1.1 and Proposition 1.2. And we prove some variations of Proposition 1.1 as several lemmas in §2 for our proof. A key result is Lemma 2.6 which implies a sufficient condition for the existence of p-basis. The regularity of the second half of Theorem 3.1 follows immediately from Theorem 2.1 of [2]. For a regular locality over a field of characteristic p, we prove the existence of a p-basis by virtue of Lemma 2.6.

On the other hand, there is a regular local ring R which has no p-basis over R^p. For example, the formal power series ring $k[[x]]$, over a field k of

1) A locality over a field means a quotient ring of an affine domain over a field with respect to a prime ideal (cf. [5]).

characteristic $p>0$ such that $[k:k^p]=\infty$ has no p-basis over $k^p[[x^p]]$ (see Example 3.8 of § 3).

§ 1. Notations and preliminaries.

In this paper, all rings are commutative with identity. A ring is called a quasi-local ring if it has only one maximal ideal and a noetherian quasi-local ring is called a local ring.

First we record the results due to M. Nagata which will be needed later.

PROPOSITION 1.1 (38.4 of [5]). *Let $(R, \mathfrak{m})$ be a local integral domain and let a be an element of an integral extension of R. Assume that a is not in the field of quotients of R, that the characteristic p of R is different from zero and that $a^p \in R$. Then $R[a]$ is a local ring. Let $\mathfrak{m}'$ be the maximal ideal of $R[a]$. Then either*

$$\text{length}_{R/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2=\text{length}_{R[a]/\mathfrak{m}'}\mathfrak{m}'/\mathfrak{m}'^2$$

or

$$(\text{length}_{R/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2)+1=\text{length}_{R[a]/\mathfrak{m}'}\mathfrak{m}'/\mathfrak{m}'^2 .$$

The first equality holds if and only if either the irreducible polynomial X^p-a^p over R is irreducible modulo $\mathfrak{m}$ or there exists an element $b\in R$ such that $(a-b)^p \in \mathfrak{m}, \notin \mathfrak{m}^2$.

PROPOSITION 1.2 (31.8 of [5]). *A semi-local ring R which may not be Noetherian[2] is really Noetherian if and only if:* (1) *every finitely generated ideal of R is a closed subset of R, and* (2) *the maximal ideals of R have finite bases.*

From now on throughout this paper, R will denote a local ring of characteristic $p>0$, $\mathfrak{m}$ the maximal ideal of R and k the residue field of R. We denote the Krull dimension of R by $\dim R$ and we put $\dim R=r$. We set $R^p=\{a^p \mid a\in R\}$ and $\mathfrak{m}^{(p)}=\{m^p \mid m\in\mathfrak{m}\}$. Then R^p is a local ring of Krull dimension r with maximal ideal $\mathfrak{m}^{(p)}$. 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' denote an intermediate local ring between R and R^p, $\mathfrak{m}'$ the maximal ideal and k' the residue 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 subfield of k, we assume that $k^p\subset k'\subset k$. For any subset A of R, we denote by $R'[A]$ the intersection of all subrings of R which contain R' and A, and we denote by $\bar{A}$ the set of residue classes of the elements of

2) A quasi-semi-local ring R with the Jacobson radical $\mathfrak{m}$ is called a semi-local ring which may not be Noetherian if $\bigcap_{n=1}^{\infty}\mathfrak{m}^n=0$ (cf. [5]).

A modulo $\mathfrak{m}$. When we say "$\bar{A}$ is p-independent" we tacitly assume that A maps injectively to $\bar{A}$.

§ 2. Purely inseparable extension of a local ring.

In this section we assume that R is a local integral domain. Let K and K' be the quotient field of R and R' respectively.

LEMMA 2.1. *For any subset A of R, $R'[A]$ is a quasi-local ring with maximal ideal $\mathfrak{m}\cap R'[A]$.*

PROOF. Let $x\in R'[A]$ and $x\notin\mathfrak{m}$. So $\left(\frac{1}{x}\right)^p=\frac{1}{x^p}\in R^p\subset R'$ and $\frac{1}{x}=x^{p-1}\left(\frac{1}{x}\right)^p \in R'[A]$.

LEMMA 2.2. *Let A be a subset of R. If $\bar{A}$ is p-independent over k', then we have $\mathfrak{m}\cap R'[A]=\mathfrak{m}'R'[A]$.*

PROOF. Let ϕ be the canonical map $R'[A]\to R\to R/\mathfrak{m}=k$. Then clearly $\ker\phi=\mathfrak{m}\cap R'[A]$. On the other hand, an arbitrary element x of $R'[A]$ is written in the form

$$x=\sum\alpha_{(n_\iota)}\prod a_\iota^{n_\iota}\quad(\alpha_{(n_\iota)}\in R',\ a_\iota\in A,\ 0\leqq n_\iota\leqq p-1).$$

So if $\sum\bar{\alpha}_{(n_\iota)}\prod\bar{a}_\iota^{n_\iota}=0$, then $\bar{\alpha}_{(n_\iota)}=0$ for each (n_ι). Hence $\ker\phi\subset\mathfrak{m}'R'[A]$. The converse inclusion is clear. Therefore $\ker\phi=\mathfrak{m}'R'[A]$ and it follows that $\mathfrak{m}\cap R'[A]=\mathfrak{m}'R'[A]$.

LEMMA 2.3. *Let A be a subset of R. If A is p-independent over R' and $\bar{A}$ is p-independent over k', then $R'[A]$ is noetherian, that is, $R'[A]$ is a local ring.*

PROOF. Put $S=R'[A]$, $\mathfrak{n}=\mathfrak{m}\cap S$. We will check the conditions of Proposition 1.2. We have $\mathfrak{n}=\mathfrak{m}'S$ by Lemma 2.2, hence $\mathfrak{n}$ is finitely generated. Since $\bigcap_{n=1}^{\infty}\mathfrak{n}^n\subset\bigcap_{n=1}^{\infty}\mathfrak{m}^n=(0)$, S is separated for the $\mathfrak{n}$-adic topology. Let $I=\sum_{j=1}^{s}c_jS$ be a finitely generated ideal. Write

$$c_j=\sum_{(n_\iota)}\alpha_{j(n_\iota)}\prod a_\iota^{n_\iota}\qquad(\alpha_{j(n_\iota)}\in R',\ a_\iota\in A,\ 0\leqq n_\iota<p),$$

and let T be the set of the elements a_ι which appear in the right hand side when j moves from 1 to s. Then T is a finite subset of A. Put $S_0=R'[T]$, $I_0=I\cap S_0$ and $\mathfrak{n}_0=\mathfrak{m}\cap S_0$. Then S_0 is a local ring and its maximal ideal $\mathfrak{n}_0$ is equal to $\mathfrak{m}'S_0$ by Lemma 2.2. Therefore we have $I=I_0S$, $\mathfrak{n}=\mathfrak{n}_0S$ and

$$I_0=\bigcap_{n=1}^{\infty}(I_0+\mathfrak{n}_0^n).$$

On the other hand we have $S=S_0[A-T]$, and $A-T$ is a p-basis of S over S_0. Therefore S is a free S_0-module, and so

$$I=I_0S=[\bigcap_{n=1}^{\infty}(I_0+\mathfrak{n}_0^n)]S$$

$$=\bigcap_{n=1}^{\infty}(I_0+\mathfrak{n}_0^n)S$$

$$=\bigcap_{n=1}^{\infty}(I+\mathfrak{n}^n).$$

Thus I is closed for the $\mathfrak{n}$-adic topology.

LEMMA 2.4. *Let A be a subset of R. If A is p-independent over R' and $\bar{A}$ is p-independent over k', then a minimal system of generators for $\mathfrak{m}'$ is also a minimal system of generators for the maximal ideal of $R'[A]$. In particular, if R' is regular, so is $R'[A]$.*

PROOF. Put $S=R'[A]$, $\mathfrak{n}=\mathfrak{m}\cap S$. Suppose that $\{x_1, \cdots, x_s\}$ is a minimal system of generators for $\mathfrak{m}'$. Since $\mathfrak{n}=\mathfrak{m}'S$ by Lemma 2.2, it is a system of generators for $\mathfrak{n}$. Suppose that $\{x_1, \cdots, x_s\}$ is not minimal. Then $\bar{x}_1, \cdots, \bar{x}_s$ are linearly dependent in the vector space $\mathfrak{n}/\mathfrak{n}^2$ over the field $S/\mathfrak{n}$, where $\bar{x}_i=$ the residue class of x_i modulo $\mathfrak{n}^2$. It follows that there exist $y\in\mathfrak{n}^2$ and $\{w_1, \cdots, w_s\}\subset S$ such that at least one of these elements $w_1, \cdots, w_s$ is a unit of S and $y=\sum_{i=1}^{s} w_ix_i$. Since w_i is of the form

$$w_i=\sum_{(n_\iota)}\beta_{i(n_\iota)}\Pi a_\iota^{n_\iota} \qquad (\beta_{i(n_\iota)}\in R',\ a_\iota\in A,\ 0\leqq n_\iota\leqq p-1),$$

we have

$$y=\sum_{(n_\iota)}\{\sum_{i=1}^{s}\beta_{i(n_\iota)}x_i\}\Pi a_\iota^{n_\iota}.$$

On the other hand, since $y\in\mathfrak{n}^2=\mathfrak{m}'^2S$, y is of the form

$$y=\sum\alpha_{(n_\iota)}\Pi a_\iota^{n_\iota} \qquad (\alpha_{(n_\iota)}\in\mathfrak{m}'^2,\ a_\iota\in A,\ 0\leqq n_\iota\leqq p-1).$$

By the p-independence of A over R', we get $\sum_{i=1}^{s}\beta_{i(n_\iota)}x_i=\alpha_{(n_\iota)}\in\mathfrak{m}'^2$ for any (n_ι), whence $\sum\bar{\beta}_{i(n_\iota)}\bar{x}_i=0$ in the space $\mathfrak{m}'/\mathfrak{m}'^2$ over k'. Since $\bar{x}_1, \cdots, \bar{x}_s$ are linearly independent in the space $\mathfrak{m}'/\mathfrak{m}'^2$ over k', it follows that $\bar{\beta}_{i(n_\iota)}=0$ in k', so $\beta_{i(n_\iota)}\in\mathfrak{m}'$ for all i. From this $w_i\in\mathfrak{n}$ for all i, which is a contradiction.

LEMMA 2.5. *Let A be a subset of R. If R' is regular and $\bar{A}$ is p-independent over k', then A is p-independent over K'.*

PROOF. We can choose a p-basis B of $K'(A)$ over K' such that $B\subset A$ (Exercises of § 8, [**1**]). Then clearly $K'(A)=K'(B)$ and $R'[A]$ is contained in the field of quotients of $R'[B]$. On the other hand, $R'[B]$ is regular by Lemma 2.4 and $R'[A]$ is integral over $R'[B]$. It follows that $R'[A]=R'[B]$.

Then we have $k'(\bar{A})=k'(\bar{B})$, whence $\bar{A}=\bar{B}$, so $A=B$. With this, Lemma 2.5 is proved.

LEMMA. 2.6. *Let R be a regular local ring with Krull dimension r, K the quotient field of R and let A be a subset of R such that $\bar{A}$ is a p-basis of k over k^p. Then we have $[K:K^p(A)]\geqq p^r$. More precisely, there exist $z_1, \cdots, z_r \in R$ which satisfy the following three properties;*

(a) *$\{z_1, \cdots, z_r\}$ is a minimal system of generators for the maximal ideal $\mathfrak{m}$ of R,*

(b) *$\{z_1, \cdots, z_r\}$ is p-independent over $K^p(A)$,*

(c) *$R_r=R^p[A, z_1, \cdots, z_r]$ is a regular local ring with maximal ideal $\mathfrak{m}_r=(z_1, \cdots, z_r)R_r$.*

In particular if $[K:K^p(A)]=p^r$, we have $R=R^p[A, z_1, \cdots, z_r]$, that is, $A\cup\{z_1, \cdots, z_r\}$ is a p-basis of R over R^p.

PROOF. We assume that $[K:K^p(A)]=p^s$ $(s\leqq r)$. Let $\{x_1, \cdots, x_r\}$ be a minimal system of generators for $\mathfrak{m}$ and let $\mathfrak{m}_A$ be the maximal ideal $\mathfrak{m}^{(p)}R^p[A]$ of $R^p[A]$. Suppose that we could choose $z_1, \cdots, z_t$ $(t<s)$ in such a way that

(a) $z_i=x_i$ or $z_i=u_ix_i$ for $i=1, 2, \cdots, t$, where u_i is a unit in R (and therefore $\{z_1, \cdots, z_t\}$ is a subset of a minimal system of generators for $\mathfrak{m}$),

(b) $\{z_1, \cdots, z_t\}$ is p-independent over $K^p(A)$, and

(c) $R_t=R^p[A, z_1, \cdots, z_t]$ is a regular local ring with maximal ideal $\mathfrak{m}_t=\mathfrak{m}\cap R_t=\mathfrak{m}_A+(z_1, \cdots, z_t)R_t$.

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

(a) $\{z_1, \cdots, z_{t+1}\}$ is a subset of a minimal system of generators for $\mathfrak{m}$,

(b) $\{z_1, \cdots, z_{t+1}\}$ is p-independent over $K^p(A)$,

(c) $R_{t+1}=R^p[A, z_1, \cdots, z_{t+1}]$ is a regular local ring with maximal ideal $\mathfrak{m}_{t+1}=\mathfrak{m}\cap R_{t+1}=\mathfrak{m}_A+(z_1, \cdots, z_{t+1})R_{t+1}$.

Since $\bar{A}$ is a p-basis of k over k^p, we have $R=R^p[A]+\mathfrak{m}$, $K=K^p(A, \mathfrak{m})$ and

$$[K:K^p(A, z_1, \cdots, z_t)]=p^{s-t}\geqq p\,.$$

If $x_{t+1}\notin K^p(A, z_1, \cdots, z_t)$, we put $z_{t+1}=x_{t+1}$. Otherwise, we choose an element m of $\mathfrak{m}$ such that $m\notin K^p(A, z_1, \cdots, z_t)$. Let $u_{t+1}=1+m$. Then u_{t+1} is a unit of R and $u\notin K^p(A, z_1, \cdots, z_t)$. In this case, we set $z_{t+1}=u_{t+1}x_{t+1}$. In both cases, $z_{t+1}\in\mathfrak{m}$ and $z_{t+1}\notin K^p(A, z_1, \cdots, z_t)$, that is, z_{t+1} is p-independent over $K^p(A, z_1, \cdots, z_t)$. We claim that $R_{t+1}=R^p[A, z_1, \cdots, z_{t+1}]$ is a regular local ring with maximal ideal

$$\mathfrak{m}_{t+1}=\mathfrak{m}\cap R_{t+1}=\mathfrak{m}_A+(z_1, \cdots, z_{t+1})R_{t+1}\,.$$

It is obvious that $\mathfrak{m}_{t+1}=\mathfrak{m}_A+(z_1, \cdots, z_{t+1})R_{t+1}$. To prove that $R_{t+1}=R_t[z_{t+1}]$ is regular, it is sufficient to show $z_{t+1}^p\notin\mathfrak{m}_t^2$ by Proposition 1.1. Suppose that

$z_{t+1}^p \in \mathfrak{m}_t^2$. Since $\mathfrak{m}_t = \mathfrak{m}_A + (z_1, \cdots, z_t)R_t$,

$$\mathfrak{m}_t^2 = (\mathfrak{m}^{(p)})^2 R^p[A] + \mathfrak{m}^{(p)}(z_1, \cdots, z_t)R_t + (z_1, \cdots, z_t)^2 R_t .$$

Then we have

$$z_{t+1}^p = \sum \alpha_{(n_\iota)}^p \Pi a_\iota^{n_\iota} + \sum \beta_{(n_\iota)(e_j)}^p \Pi a_\iota^{n_\iota} \Pi z_j^{e_j} + \sum \gamma_{(n_\iota)(f_j)}^p \Pi a_\iota^{n_\iota} \Pi z_j^{f_j}$$

where $a_\iota \in A$, $\alpha_{(n_\iota)} \in \mathfrak{m}^2$, $\beta_{(n_\iota)(e_j)} \in \mathfrak{m}$, $\gamma_{(n_\iota)(f_j)} \in R$, $\sum e_j \geqq 1$ and $\sum f_j \geqq 2$. Regarding the p-th power of a_ι and z_j as the elements of R^p, we have

$$z_{t+1}^p = \sum \eta_{(m_\iota)}^p \Pi a_\iota^{m_\iota} + \sum \xi_{(m_\iota)(g_j)}^p \Pi a_\iota^{m_\iota} \Pi z_j^{g_j} + \sum \zeta_{(m_\iota)(h_j)}^p \Pi a_\iota^{m_\iota} \Pi z_j^{h_j}$$

where $a_\iota \in A$, $\eta_{(m_\iota)} \in \mathfrak{m}^2$, $\xi_{(m_\iota)(g_j)} \in \mathfrak{m}$, $\zeta_{(m_\iota)(h_j)} \in R$ 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 $\zeta_{(0)(0)} \in \sum_{i=1}^t z_i R + \mathfrak{m}^2$. Because of p-independence of $\{A, z_1, \cdots, z_t\}$ over K^p, it follows that

$$z_{t+1} = \eta_{(0)} + \xi_{(0)(0)} + \zeta_{(0)(0)} .$$

Set $\zeta_{(0)(0)} = \sum_{i=1}^t d_i z_i + m$, where $d_i \in R$ and $m \in \mathfrak{m}^2$. Then we have $z_{t+1} - \sum_{i=1}^t d_i z_i \in \mathfrak{m}^2$. By the choice of z_{t+1}, $\{z_1, \cdots, z_{t+1}\}$ is a subset of a minimal system of generators for $\mathfrak{m}$ and hence $\{\bar{z}_1, \cdots, \bar{z}_{t+1}\}$ is linearly independent in the space $\mathfrak{m}/\mathfrak{m}^2$ over k. Therefore the relation $\bar{z}_{t+1} - \sum_{i=1}^t \bar{d}_i \bar{z}_i = 0$ implies $\bar{1} = 0$ in k, which is a contradiction.

Thus we have proved that there exist $z_1, \cdots, z_s \in R$ which satisfy the following three properties;

(a) $\{z_1, \cdots, z_s\}$ is a part of a minimal system of generators for $\mathfrak{m}$,

(b) $\{z_1, \cdots, z_s\}$ is p-independent over $K^p(A)$ (that is, the field of quotients of $R_s = R^p[A, z_1, \cdots, z_s]$ is K),

(c) R_s is a regular local ring with maximal ideal $\mathfrak{m}_s = \mathfrak{m}_A + (z_1, \cdots, z_s)R_s$.

Since R_s is normal and R is integral over R_s, we have $R = R_s$. Then we have $\mathfrak{m} = \mathfrak{m}_s$, hence $\mathfrak{m} = \mathfrak{m}_A + (z_1, \cdots, z_s)R$. Since $\mathfrak{m}_A \subset \mathfrak{m}^2$, we have $\mathfrak{m} = (z_1, \cdots, z_s)R$ by Nakayama's lemma. Therefore $s = r$. Consequently we have $[K : K^p(A)] \geqq p^r$.

§ 3. Main theorem.

We are now ready to prove the main theorem.

THEOREM 3.1. *Let R be a regular local ring of characteristic p and let k be the residue field of R. If there is a system of representatives A of a p-basis of k over k^p such that R is a finite $R^p[A]$-module, then R has a p-basis over R^p. More precisely, a p-basis of R over R^p is obtained as the union of $\{z_1, \cdots, z_r\}$ and A where $r = \dim R$ and $\{z_1, \cdots, z_r\}$ is a special minimal system of generators for the maximal ideal of R.*

Conversely, if R is a reduced local ring of characteristic p and if R has a p-basis Γ over R^p, then R is a regular local ring and Γ is of the form $\Gamma = A \cup \{z_1+v_1, \cdots, z_r+v_r\}$, $v_i \in R^p[A]$ $(i=1, \cdots, r)$, where A is a system of representatives of a p-basis of the residue field k of R over k^p and $\{z_1, \cdots, z_r\}$ is a minimal system of generators for the maximal ideal of R.

PROOF. Let R be a regular local ring with Krull dimension r, K the quotient field of R and let A be a subset of R such that $\bar{A}$ is a p-basis of k over k^p and such that R is a finite $R^p[A]$-module. To prove the first half of Theorem 3.1, it is sufficient to prove that $[K: K^p(A)] \leqq p^r$ by Lemma 2.6.

Suppose that $[K: K^p(A)] > p^r$. Let $\hat{R}$ and $\hat{R}_r$ be the $\mathfrak{m}$-adic and $\mathfrak{m}_r$-adic completion of R and R_r respectively. By Cohen's structure theorem for complete local rings, we have $\hat{R} = k[[X_1, \cdots, X_r]]$ where $X_1, \cdots, X_r$ are indeterminates. Furthermore, we have $\hat{R}_r = k[[X_1, \cdots, X_r]]$ where $X_1, \cdots, X_r$ are indeterminates. In fact, R_r is regular, $\mathfrak{m}$ and $\mathfrak{m}_r$ have the same minimal system of generators by Lemma 2.6 and $R_r/\mathfrak{m}_r = k$. Therefore $\hat{R} = \hat{R}_r$. On the other hand, since $[K: K^p(A, z_1, \cdots, z_r)] \geqq p$, there is an element $y \in R$ such that $y \notin K^p(A, z_1, \cdots, z_r)$. Since R is a finite $R^p[A]$-module, R is a finite R_r-module. Hence $\hat{R}_r \subsetneqq \widehat{R_r[y]} \subseteqq \hat{R}$. This is a contradiction.

Conversely, let R be a reduced local ring of characteristic p. We assume that R has a p-basis Γ over R^p. Then the regularity of R follows from Theorem 2.1 of [2]. Since $R = R^p[\Gamma]$, $R/\mathfrak{m} = k = k^p(\bar{\Gamma})$ where $\bar{\Gamma}$ is the set of the residue classes of the elements of Γ modulo $\mathfrak{m}$. Therefore we may select a subset A of Γ such that $\bar{A}$ is a p-basis of k over k^p. Then $B = \Gamma - A$ is a p-basis of R over $R^p[A]$. Furthermore, we may assume that $B \subset \mathfrak{m}$, because $R = R^p[A] + \mathfrak{m}$. Since $R = R^p[A][B]$, we have $\mathfrak{m} = \mathfrak{m}_A + BR$ where $\mathfrak{m}_A$ is the maximal ideal $\mathfrak{m}^{(p)} R^p[A]$ of $R^p[A]$. Hence $\mathfrak{m} = \mathfrak{m}^2 + BR$ and $\mathfrak{m} = BR$ by Nakayama's lemma. Then we choose $\{z_1, \cdots, z_r\}$ a minimal system of generators for $\mathfrak{m}$ from B. For a moment, suppose that $\{z_1, \cdots, z_r\} \subsetneqq B$. Then there is an element $b \in B$ such that $b \neq z_i$ $(i=1, \cdots, r)$. Since $b \in \mathfrak{m}$ we have

$$b = \sum_{i=1}^{r} \gamma_i z_i \qquad (\gamma_i \in R).$$

On the other hand,

$$\gamma_i = \sum_{(e_\lambda)} \alpha_{i(e_\lambda)} \Pi b_\lambda^{e_\lambda}$$

$(\alpha_{i(e_\lambda)} \in R^p[A, z_1, \cdots, z_r]$, $b_\lambda \in B - \{z_1, \cdots, z_r\}$, $0 \leqq e_\lambda \leqq p-1)$. From these relations and p-independence of $B - \{z_1, \cdots, z_r\}$ over $K^p(A, z_1, \cdots, z_r)$, we have an equality $1 = \sum \beta_i z_i$ $(\beta_i \in R)$. This is a contradiction. That is, $\{z_1, \cdots, z_r\} = B$. This completes the proof.

COROLLARY 3.2. *If R is a regular local ring of characteristic p and if R is a finite R^p-module, then R has a p-basis over R^p.*

REMARK 3.3. Let R be a regular local ring of characteristic p and $\mathfrak{p}$ be a prime ideal of R. If R has a p-basis Γ over R^p, then Γ is clearly a p-basis of $R_{\mathfrak{p}}$ over $(R_{\mathfrak{p}})^p$.

THEOREM 3.4. *Let R be a locality over a field of characteristic p. Then R is regular if and only if R has a p-basis over R^p.*

PROOF. Let R be a regular locality over a field L of characteristic p. Then, it is sufficient to prove that there is a subset A of R, a system of representatives of a p-basis of the residue field k of R over k^p such that $[K:K^p(A)]=p^r$ by Lemma 2.6, where K is the quotient field of R and $r=\dim R$.

Let $S=L[x_1, \cdots, x_n]$, $\mathfrak{p}$ a prime ideal of S, $R=S_{\mathfrak{p}}$ and let $k=L(\bar{x}_1, \cdots, \bar{x}_n)$ be the residue field of R. We choose a p-basis $\bar{A}$ of k over k^p such as stated in the following lemma.

LEMMA 3.5 (Lemma 3 of [3]). *Let $k=L(\bar{x}_1, \cdots, \bar{x}_n)$ be a finitely generated over a field L, $\mathrm{tr.deg.}_L k=s$ and let $\Pi=\{y_\lambda\}_{\lambda\in\Lambda}$ be a p-basis of L over L^p. Then we can choose a p-basis of k over k^p as the union of a suitable subset $\{w_1, \cdots, w_{t+s}\}$ of k and $\Pi-\{y_1, \cdots, y_t\}$ where $\{y_1, \cdots, y_t\}$ is a suitable subset of Π $(t\leqq n)$.*

Let A be a system of representatives of $\bar{A}$ and let $\Pi'=\Pi-\{y_1, \cdots, y_t\}$. We assert that $[K:K^p(A)]=p^r$. Let L' be a field of definition for S[3] and let $L''=L'(y_1, \cdots, y_t)$. Then L'' is also a field of definition for S. Let $\{\beta_1, \cdots, \beta_l\}$ be a p-basis of L'' over L^p. Since $L=L''(\Pi')$, we can choose a p-basis A' of L over L'' such that $A'\subseteqq\Pi'$. Then $A'\cup\{\beta_1, \cdots, \beta_l\}$ is a p-basis of L over L^p. Thus, we have $[L:L^p(A')]=p^l$ and

$$[K:K^p(A')]=p^{l+\mathrm{tr.deg.}_L K}$$

by Lemma 1 of [6]. Since $[L:L^p(A')]=p^l$ and $[L:L^p(\Pi')]=p^t$, we have $[L^p(\Pi'):L^p(A')]=p^{l-t}$. Because A is p-independent over K^p by Lemma 2.5,

$$\begin{aligned}[K^p(A):K^p(A')]&=[K^p(A):K^p(\Pi')][K^p(\Pi'):K^p(A')]\\&=p^{t+s}\cdot p^{l-t}\\&=p^{l+s}.\end{aligned}$$

On the other hand, $\mathrm{tr.deg.}_L K=s+r$. So, we have

$$[K:K^p(A')]=p^{l+s+\dim R}$$

and

$$[K:K^p(A)]=p^r.$$

3) A field of definition for S means a field L' such that $\mathfrak{P}$ is generated by elements in $L'[X_1, \cdots, X_n]$, $L'\supset L^p$ and such that $[L':L^p]<\infty$ where $\mathfrak{P}$ is a prime ideal of $L[X_1, \cdots, X_n]$ satisfied $S=L[X_1, \cdots, X_n]/\mathfrak{P}$ (cf. [3] and [6]).

Finally we note that our proof is valid for the case where the ground field L is perfect.

COLLORARY 3.6. *Let R be a locality over a field of characteristic $p>0$. Then the following three conditions are equivalent to each other.*

(a) *R is a regular local ring,*

(b) *R has a p-basis over R^p,*

(c) *the differential module $\Omega_{R^p}(R)$ of R over R^p is a free R-module.*

PROOF. (a) and (c) are equivalent by Theorem 1 of [**2**].

COROLLARY 3.7. *If L is a field of characteristic p such that $[L:L^p]<\infty$, then any regular locality R over L is a finite free R^p-module.*

EXAMPLE 3.8. Let k be a field of characteristic p such that $[k:k^p]=\infty$ and put $R=k[[x]]$. Then R has no p-basis over R^p.

PROOF. Suppose that R has a p-basis over R^p. Then, there is a p-basis of the form $A\cup\{f\}$ where A is a p-basis of $R/(x)$ over $(R/(x))^p$ and f is a generator for xR, by virtue of Theorem 3.1. Since R is a complete local ring, there is a coefficient field k' of R which contains A by 31.9 of [**5**]. Then we have $fR=xR$ and $R=k'[[f]]$. Therefore, replacing k by k' and x by f, we may assume that $A\subset k$ without loss of generality. Thus we have $R=R^p[A, x]$ and $R=k^p[[x]][k]$. On the other hand, $k^p[[x]][k]\neq R$ (E3.1 of [**5**]). This is a contradiction.

ACKNOWLEDGEMENTS.

The authors would like to acknowledge the many helpful suggestions with Professor H. Matsumura. Especially Example 3.8 owes to him. And the authors owe a great deal to Professor Y. Kawahara, only a small part of which was the suggestion of this problem.

References

[1] N. Bourbaki, Algèbre, Chap. 5, Hermann, Paris, 1959.

[2] E. Kunz, Characterization of regular local ring of characteristic p, Amer. J. Math., **91** (1969), 772-784.

[3] E. Kunz, Differentialformen inseparabler algebraischer funktionenkörper, Math. Zeitschr., **76** (1961), 56-74.

[4] H. Matsumura, Commutative Algebra, Benjamin, New York, 1970.

[5] M. Nagata, Local rings, Interscience Tracts in Pure and Applied Math., no. 13, 1962.

[6] Y. Nakai, Note on differential theoretic characterization of regular local rings, J. Math. Soc. Japan, **20** (1968), 268-274.

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

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