

\mathfrak{m} -ADIC p -BASIS AND REGULAR LOCAL RING

MAMORU FURUYA AND HIROSHI NIITSUMA

(Communicated by Bernd Ulrich)

ABSTRACT. We introduce the concept of \mathfrak{m} -adic p -basis as an extension of the concept of p -basis. Let (S, \mathfrak{m}) be a regular local ring of prime characteristic p and R a ring such that $S \supset R \supset S^p$. Then we prove that R is a regular local ring if and only if there exists an \mathfrak{m} -adic p -basis of S/R and R is Noetherian.

1. INTRODUCTION

Some forty years ago, E. Kunz conjectured the following: If (S, \mathfrak{m}) is a regular local ring of prime characteristic p , and if R a ring with $S \supset R \supset S^p$ such that S is finite as an R -module, then the following are equivalent:

- (1) R is a regular local ring.
- (2) There exists a p -basis of S/R .

This was proved by T. Kimura and the second author ([KN2] or [K, 15.7]). Without the finiteness assumption, however, this result is not true anymore. In this paper we generalize this result to the non-finite situation by introducing a topological generalization of the concept of p -basis, which we call the \mathfrak{m} -adic p -basis (see Definition 2.1).

Then we prove the following main theorem:

Theorem 3.4. *Let (S, \mathfrak{m}) be a regular local ring of prime characteristic p , and R a ring such that $S \supset R \supset S^p$. Then the following conditions are equivalent:*

- (1) R is a regular local ring.
- (2) There exists an \mathfrak{m} -adic p -basis of S/R , and R is Noetherian.

This theorem covers the following situation: Let k be a field of characteristic p with $[k : k^p] = \infty$, and let $S = k[[X]]$. Then S is regular, but S/S^p does not have a p -basis (cf. [KN1, Example 3.8]). However S/R has an \mathfrak{m} -adic p -basis. That is, $C \cup \{X\}$ is an \mathfrak{m} -adic p -basis of S/S^p , where $\mathfrak{m} := (X)S$ and C is a p -basis of k/k^p .

If S is finite as an R -module, then any \mathfrak{m} -adic p -basis of S/R is a p -basis of S/R , and R is Noetherian (see Remark 3.5).

2. PRELIMINARIES

All rings in this paper are commutative rings with identity elements. We always denote by p a prime number.

Received by the editors January 29, 2003 and, in revised form, August 8, 2003.

2000 *Mathematics Subject Classification.* Primary 13H05, 13J10.

Key words and phrases. \mathfrak{m} -adic p -basis, regular local ring.

Let R be a ring and S an R -algebra with $\text{char}(S) = p$. Let \mathfrak{m} be an ideal of S .

Let S^p denote the subring $\{x^p; x \in S\}$ of S , $\mathfrak{m}^{(p)}$ the ideal $\{x^p; x \in \mathfrak{m}\}$ of S^p and RS^p the subring of S generated by the set $\{ax^p; a \in R, x \in S\}$. If (S, \mathfrak{m}) is a local ring and R is a ring such that $S \supset R \supset S^p$, then R is a local ring with the maximal ideal $\mathfrak{m} \cap R$. For any subset A of S , 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} .

As an extension of the concept of p -basis, we introduce the concept of \mathfrak{m} -adic p -basis as follows:

Definition 2.1. A subset B of S is called an \mathfrak{m} -adic p -basis of S/R if the following conditions are satisfied:

- (1) B is p -independent over RS^p .
- (2) S is the closure of the subring $T := RS^p[B]$ in S for the \mathfrak{m} -adic topology; that is, $S = \bar{T} = \bigcap_{r=0}^{\infty} (T + \mathfrak{m}^r)$.
- (3) $\mathfrak{m}^r \cap T = \mathfrak{m}_T^r$ for every $r \geq 1$, where $\mathfrak{m}_T := \mathfrak{m} \cap T$.

Lemma 2.2. Suppose that (S, \mathfrak{m}, L) is a local ring and R a ring such that $S \supset R \supset S^p$. Then the following assertions are true:

- (1) There are quasi coefficient fields k and k_R of S and R respectively such that $k \supset k_R \supset k^p$.
- (2) Let k and k_R be fields satisfying the conditions of (1), and let S^* and R^* be the \mathfrak{m} -adic and \mathfrak{m}_R -adic completions of S and R respectively, where $\mathfrak{m}_R := \mathfrak{m} \cap R$. Then there are unique coefficient fields K and K_R of S^* and R^* respectively such that $K \supset k$ and $K_R \supset k_R$ (cf. [M, Theorem 28.3]). If $S^* \supset R^* \supset (S^*)^p$, then the following assertions are true:
 - 1) $K \supset K_R \supset K^p$.
 - 2) Any p -basis of k/k_R is a p -basis of K/K_R , and any p -basis of k_R/k^p is a p -basis of K_R/K^p .

Proof. Put $L_R := R/\mathfrak{m}_R$. (1) Let $A = \{a_i; i \in I\}$ and $B = \{b_j; j \in J\}$ be subsets of S and R respectively such that $\bar{A} := \{\bar{a}_i; i \in I\}$ and $\bar{B} := \{\bar{b}_j; j \in J\}$ are p -bases of L/L_R and L_R/L^p respectively, where $\bar{a}_i := a_i + \mathfrak{m}, \bar{b}_j := b_j + \mathfrak{m}_R$. For the prime field h of S , we consider the subring $h[A, B]$. Since $h[A, B] \cap \mathfrak{m} = (0)$ in S , it follows that S contains the field of quotients $k := h(A, B)$ of $h[A, B]$ and k is a quasi coefficient field of S . Furthermore we see that $h(A^p, B) := k_R$ is a quasi coefficient field of R , where $A^p := \{a_i^p; i \in I\}$. Then we have $k \supset k_R \supset k^p$.

(2) Let K and K_R be the coefficient fields of S^* and R^* such that $K \supset k$ and $K_R \supset k_R$ respectively. Assume that $S^* \supset R^* \supset (S^*)^p$. Since K is integral over the subring $k_R[K^p]$, then $k_R[K^p] := K'$ is a field contained in R^* . Let $f : R^* \rightarrow L_R$ be the canonical mapping, and C a p -basis of k_R/k^p . Then $K' = K^p(C)$ and $f(K') = L^p(\bar{C})$, where $\bar{C} := \{f(c); c \in C\}$. Since \bar{C} is a p -basis of L_R/L^p , K' is a coefficient field of R^* . By the uniqueness of the coefficient field of R^* containing k_R , we see that $K' = K_R$, and hence $K \supset K_R \supset K^p$.

Assertion 2) of (2) is clear. □

Lemma 2.3. Let L be a field with $\text{char}(L) = p, K$ a field such that $L \supset K \supset L^p$ and C a p -basis of L/K . Put

$$S := L[[X_1, \dots, X_n]] \supset R := K[[X_1^p, \dots, X_r^p, X_{r+1}, \dots, X_n]]$$

for some r ($0 \leq r \leq n$). Then $C \cup \{X_1, \dots, X_r\}$ is an \mathbf{m} -adic p -basis of S/R , where $\mathbf{m} := (X_1, \dots, X_n)S$.

Proof. We have $R[X_1, \dots, X_r] = K[[X_1, \dots, X_n]]$. Put $T := R[C, X_1, \dots, X_r] = K[[X_1, \dots, X_n]][C]$ and $\mathbf{m}_T := \mathbf{m} \cap T$. Then $S \supset T \supset R \supset S^p$. By [M, Theorem 22.3], S is faithfully flat over T , and it follows from $\mathbf{m} = \mathbf{m}_T S$ that $\mathbf{m}^r \cap T = \mathbf{m}_T^r$ for every $r \geq 1$. A routine computation shows that $C \cup \{X_1, \dots, X_r\}$ is p -independent over R . Furthermore, since $S/\mathbf{m} = T/\mathbf{m}_T$ and $\mathbf{m} = \mathbf{m}_T S$, we have that S is the closure of T in S for the \mathbf{m} -adic topology. \square

3. MAIN RESULT

In this section, we use the following notation:

S is a regular local ring with $\text{char}(S) = p$,

\mathbf{m} is the maximal ideal of S ,

$L = S/\mathbf{m}$,

R is a ring such that $S \supset R \supset S^p$,

$\mathbf{n} = \mathbf{m} \cap R$,

For the proof of the main result, we need several lemmas.

Lemma 3.1. *Suppose that R is Noetherian. Then the following statements hold:*

(1) S is faithfully flat over R if and only if R is regular.

(2) Let S^* , R^* and $(S^p)^*$ be the \mathbf{m} -adic, \mathbf{n} -adic, and $\mathbf{m}^{(p)}$ -adic completions of S , R and S^p respectively. If R is regular, then $S^* \supset R^* \supset (S^p)^* = (S^*)^p$.

Proof. (1) The assertion follows from [M, Theorem 23.1 and Theorem 23.7].

(2) Suppose that S and R are regular. Since S is faithfully flat over R in virtue of (1), the \mathbf{n} -adic topology of R coincides with the topology induced by the \mathbf{m} -adic topology of S on the subspace $R \subset S$. Hence the \mathbf{m} -adic completion S^* contains the \mathbf{n} -adic completion R^* . The rest of assertion (2) is clear. \square

Lemma 3.2. *If R is regular, then $\mathbf{n} = \mathbf{m}^{(p)}R$ or $\mathbf{n} \not\subset \mathbf{m}^2$.*

Proof. By almost the same reasoning as that of the proof of [KN2, Lemma 5], we have the assertion. \square

Lemma 3.3. *Let R be regular, and let $\{\bar{a}_1, \dots, \bar{a}_r\}$ ($a_i \in \mathbf{m}, \bar{a}_i = a_i + (\mathbf{n}S + \mathbf{m}^2)$) and $\{\bar{b}_1, \dots, \bar{b}_s\}$ ($b_i \in \mathbf{n}, \bar{b}_i = b_i + \mathbf{m}^2$) be bases of the L -vector spaces*

$$\mathbf{m}/(\mathbf{n}S + \mathbf{m}^2) \quad \text{and} \quad (\mathbf{n}S + \mathbf{m}^2)/\mathbf{m}^2$$

respectively. Then $\dim S = \dim R = r + s$. Furthermore the maximal ideals of S and R are expressed respectively as follows: $\mathbf{m} = (a_1, \dots, a_r, b_1, \dots, b_s)S$ and $\mathbf{n} = (a'_1, \dots, a'_r, b_1, \dots, b_s)R$.

Proof. We have $\dim S = \dim_L \mathbf{m}/\mathbf{m}^2 = r + s$, and $\{a_1, \dots, a_r, b_1, \dots, b_s\}$ is a regular system of parameters of S . Furthermore we see that $\{\bar{b}_1, \dots, \bar{b}_s\}$ ($\bar{b}_i := b_i + \mathbf{n}^2 \in \mathbf{n}/\mathbf{n}^2$) is linearly independent over K ($:= R/\mathbf{n}$). Thus there exists a subset $\{y_1, \dots, y_r\}$ of \mathbf{n} such that $\{b_1, \dots, b_s, y_1, \dots, y_r\}$ is a regular system of parameters of R . Put $\mathbf{a} := (b_1, \dots, b_s)R$. Then we have that $\mathbf{a}S \cap R = \mathbf{a}$, since S/R is faithfully flat by Lemma 3.1. Put $S' := S/\mathbf{a}S, \mathbf{m}' := \mathbf{m}/\mathbf{a}S, R' := R/\mathbf{a}$ and $\mathbf{n}' := \mathbf{n}/\mathbf{a}$. Then (S', \mathbf{m}') and (R', \mathbf{n}') are regular local rings, with $S' \supset R' \supset (S')^p$, $\dim S' = \dim R' = r$, and each maximal ideal has the following form respectively: $\mathbf{m}' = (a'_1, \dots, a'_r)S'$ and $\mathbf{n}' = (y'_1, \dots, y'_r)R'$, where $a'_i := a_i + \mathbf{a}S$

and $y'_i := y_i + \mathbf{a}$. Furthermore we have $r = \dim_L \mathbf{m}'/(\mathbf{m}')^2 = \dim_L \mathbf{m}/(\mathbf{m}^2 + \mathbf{a}S)$ and $\dim_L \mathbf{m}'/(\mathbf{n}'S' + (\mathbf{m}')^2) = \dim_L \mathbf{m}/(\mathbf{n}S + \mathbf{m}^2) = r$, so that $\dim_L \mathbf{m}'/(\mathbf{m}')^2 = \dim_L \mathbf{m}'/(\mathbf{n}'S' + (\mathbf{m}')^2)$. On the other hand, since

$$\dim_L \mathbf{m}'/(\mathbf{m}')^2 = \dim_L(\mathbf{n}'S' + (\mathbf{m}')^2)/(\mathbf{m}')^2 + \dim_L \mathbf{m}'/(\mathbf{n}'S' + (\mathbf{m}')^2),$$

we have

$$\dim_L \mathbf{n}'S' + (\mathbf{m}')^2/(\mathbf{m}')^2 = 0,$$

and thus we get $\mathbf{n}'S' + (\mathbf{m}')^2 = (\mathbf{m}')^2$. By Lemma 3.2, we see that $\mathbf{n}' = \mathbf{m}'^{(p)}R'$. This implies that $\mathbf{n} = (a_1^p, \dots, a_r^p, b_1, \dots, b_s)R$. □

The main result of this paper is the following theorem:

Theorem 3.4. *Let (S, \mathbf{m}) be a regular local ring with $\text{char}(R) = p$ and R a ring such that $S \supset R \supset S^p$. Then the following conditions are equivalent:*

- (1) *R is a regular local ring.*
- (2) *There exists an \mathbf{m} -adic p -basis of S/R , and R is Noetherian.*

Proof. (1) \Rightarrow (2). With the same notation as for Lemma 3.3, we have $\dim S = \dim R = r + s$, $\mathbf{m} = (a_1, \dots, a_r, b_1, \dots, b_s)S$ and $\mathbf{n} = (a_1^p, \dots, a_r^p, b_1, \dots, b_s)R$. Let S^* and R^* be the \mathbf{m} -adic and \mathbf{n} -adic completions of S and R respectively. Then we have $S^* \supset R^* \supset (S^*)^p$ by Lemma 3.1. Hence there are coefficient fields K and K_R of S^* and R^* respectively such that $K \supset K_R \supset K^p$ and K/K_R has a p -basis C with $C \subset S$, by Lemma 2.2. Thus the complete local rings S^* and R^* have the forms $S^* = K[[a_1, \dots, a_r, b_1, \dots, b_s]]$ and $R^* = K_R[[a_1^p, \dots, a_r^p, b_1, \dots, b_s]]$, whence $A := C \cup \{a_1, \dots, a_r\}$ is an \mathbf{m}^* -adic p -basis of S^*/R^* by Lemma 2.3, where $\mathbf{m}^* := \mathbf{m}S^*$. Then $S \supset A$, and A is also p -independent over R . Put $T := R[A]$ and $\mathbf{m}_T = \mathbf{m} \cap T$. Then (T, \mathbf{m}_T) is a Noetherian local ring (cf. [KN1, Lemma 2.3]). Furthermore, $\mathbf{m}_T = (a_1, \dots, a_r, b_1, \dots, b_s)T$, and so (T, \mathbf{m}_T) is regular. It follows that S is faithfully flat over T by Lemma 3.1. Therefore $\mathbf{m}^r \cap T = \mathbf{m}_T^r$ for every $r \geq 1$. Since $T/\mathbf{m}_T = S/\mathbf{m}$ and $\mathbf{m} = \mathbf{m}_T S$, we have $S = \overline{T}$, where \overline{T} is the closure of T in S for the \mathbf{m} -adic topology. Consequently, A is an \mathbf{m} -adic p -basis of S/R .

(2) \Rightarrow (1). Let A be an \mathbf{m} -adic p -basis of S/R . Put $T := R[A]$ and $\mathbf{m}_T := \mathbf{m} \cap T$. Then $S \supset T \supset S^p$, and $T/\mathbf{m}_T = L$. Thus there exists a subset C of A such that $\overline{C} := \{\bar{c}; c \in C\}$ ($\bar{c} := c + \mathbf{m}$) is a p -basis of L/K , where $K := R/\mathbf{n}$. Put $A_1 := A - C$ and $P := R[C]$. Then $T = P[A_1]$. Since the L -vector space $\mathbf{m}_T/\mathbf{m}_T^2$ is a subspace of \mathbf{m}/\mathbf{m}^2 , we have $\dim_L \mathbf{m}_T/\mathbf{m}_T^2 \leq \dim_L \mathbf{m}/\mathbf{m}^2 = \dim S < \infty$. The module of differentials $\Omega_{T/P}$ is the free T -module with the free basis $\{da; a \in A_1\}$, where d is the associated derivation of $\Omega_{T/P}$. On the other hand, we have the following exact sequence:

$$0 \rightarrow \mathbf{m}_T/(\mathbf{m}_T^2 + \mathbf{m}_P T) \rightarrow \Omega_{T/P}/\mathbf{m}_T \Omega_{T/P} \rightarrow \Omega_{L/L} \rightarrow 0,$$

where $\mathbf{m}_P := \mathbf{m} \cap P$ (cf. [K, 6.7]). Therefore we get

$$|A_1| = \dim_L \Omega_{T/P}/\mathbf{m}_T \Omega_{T/P} = \dim_L \mathbf{m}_T/(\mathbf{m}_T^2 + \mathbf{m}_P T) \leq \dim_L \mathbf{m}_T/\mathbf{m}_T^2 < \infty,$$

whence A_1 is a finite set. Since the ring P is Noetherian (cf. [KN2, Lemma 2.3]), T is also Noetherian and hence

$$\dim T \leq \dim_L \mathbf{m}_T/\mathbf{m}_T^2 \leq \dim_L \mathbf{m}/\mathbf{m}^2 = \dim S = \dim T,$$

so we have $\dim T = \dim_L \mathbf{m}_T/\mathbf{m}_T^2$. It follows that T is a regular local ring. By Lemma 3.1, then S is flat over T , and so S is flat over R . Consequently, R is regular by the same lemma. □

Remarks 3.5. Let (S, \mathfrak{m}) be a Noetherian local ring with $\text{char}(S) = p$, and R a ring such that $S \supset R \supset S^p$. Assume that S is finitely generated as an R -module. Then it is known that R is Noetherian (see [M, Theorem 3.7]). Furthermore, a subset B of S is an \mathfrak{m} -adic p -basis of S/R if and only if B is a p -basis. For, let B be an \mathfrak{m} -adic p -basis of S/R . Then $T := R[B]$ is an R -submodule of the R -module S , and (R, \mathfrak{n}) ($\mathfrak{n} := \mathfrak{m} \cap R$) is a Zariski ring. Since $\mathfrak{m}^s \subset \mathfrak{n}S$ for some $s \geq 1$, the \mathfrak{m} -adic topology of S coincides with the \mathfrak{n} -adic topology of the R -module S . Thus T is closed in S for the \mathfrak{m} -adic topology, and so we have $S = T$. Therefore B is a p -basis of S/R .

ACKNOWLEDGEMENT

The authors sincerely thank the referee for helpful suggestions which improved the paper.

REFERENCES

[K] E. Kunz, *Kähler Differentials*, Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 1986. MR 88e:14025
 [KN1] T. Kimura and N. Niitsuma, Regular local ring of prime characteristic p and p -basis, *J. Math. Soc. Japan*, **32** (1980), 363-371. MR 81j:13022
 [KN2] T. Kimura and N. Niitsuma, On Kunz's conjecture, *J. Math. Soc. Japan*, **34** (1982), 371-378. MR 83h:13030
 [M] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, Cambridge, UK, 1986. MR 88h:13001

DEPARTMENT OF MATHEMATICS, MEIJO UNIVERSITY, SHIOGAMAGUCHI, TENPAKU, NAGOYA, 468-8502, JAPAN

E-mail address: furuya@ccmfs.meijo-u.ac.jp

FACULTY OF SCIENCE, SCIENCE UNIVERSITY OF TOKYO, 1-3, KAGURAZAKA, SHINJUKU-KU, TOKYO, 162-8601, JAPAN

E-mail address: niitsuma@rs.kagu.tus.ac.jp