H. Matsumura
Nagoya Math. J.
Vol. 68 (1977), 123-130

QUASI-COEFFICIENT RINGS OF A LOCAL RING

HIDEYUKI MATSUMURA

In this note we will make a few observations on the structure of fields and local rings. The main point is to show that a weaker version of Cohen structure theorem for complete local rings holds for any (not necessarily complete) local ring. The consideration of non-complete case makes the meaning of Cohen's theorem itself clearer. Moreover, quasi-coefficient fields (or rings) are handy when we consider derivations of a local ring.

1. All rings considered here are commutative rings with unit element. By a local ring $(A, \mathfrak{m})$ we mean a (not necessarily noetherian) ring A with unique maximal ideal $\mathfrak{m}$. The completion of $(A, \mathfrak{m})$ is $\varprojlim A/\mathfrak{m}^n$ and is denoted by A^*. We say that A is separated if $\bigcap_n \mathfrak{m}^n = (0)$, and that A is complete if $A = A^*$.

Let $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ be noetherian local rings and $\phi: A \to B$ be a local homomorphism. Then B is said to be *formally smooth* (resp. *formally unramified*, resp. *formally etale*) over A if, for every commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{u} & C/N \\ {\scriptstyle\phi}\uparrow & & \uparrow \\ A & \xrightarrow{v} & C \end{array}$$

where C is a ring, N is an ideal of C with $N^2 = (0)$ and $u(\mathfrak{m}^r) = (0)$ for sufficiently large r, there exists at least one (resp. at most one, resp. exactly one) homomorphism $B \to C$ which makes the diagram

$$\begin{array}{ccc} B & \longrightarrow & C/N \\ \uparrow & \searrow & \uparrow \\ A & \longrightarrow & C \end{array}$$

Received February 16, 1977.

commutative (cf. [3, § 19]).

If B is formally unramified over A, then $\mathrm{Der}_A(B, M) = 0$ for any B-module M such that $\bigcap_\nu \mathfrak{n}^\nu M = 0$. In particular, if we put $k = A/\mathfrak{m}$ and $K = B/\mathfrak{n}$, then $\mathrm{Der}_k(K) = 0$ (or what is the same, $\Omega_{K/k} = 0$). On the other hand, it is not difficult to show that if $\Omega_{K/k} = 0$ and $\mathfrak{n} = \mathfrak{m}B$ then B is formally unramified over A.

A necessary and sufficient condition for B to be formally smooth over A is that (1) B is flat over A and (2) $B/\mathfrak{m}B$ is formally smooth over $A/\mathfrak{m}$ [3, (19.7.1)]. If A and B are fields, then to say B is formally smooth over A is tantamount to saying that B is separable over A.

Let K be a field and k be a subfield. Then the following conditions are equivalent:

(a) K is formally etale over k;

(b) every derivation of k into a K-module M can be uniquely extended to a derivation of K into M;

(c) $\Omega_K = \Omega_k \otimes_k K$, where Ω_k denotes the module of differentials of k over the prime field;

(d) K is separable over k and $\Omega_{K/k} = 0$;

(e) $\mathrm{char}(k) = 0$ and K is algebraic over k; or $\mathrm{char}(k) = p > 0$ and a p-basis of k (over the prime field) is also a p-basis of K;

In the case of characteristic p, the above are also equivalent to

(f) $K = k \otimes_{k^p} K^p$.

THEOREM 1. *Let k be a field of characteristic p, and K be a separable extension of k; let $B = \{b_i\}_{i \in I}$ be a p-independent subset of K over k. Then B is algebraically independent over k.*

Proof. Assume the contrary and suppose $b_1, \cdots, b_n \in B$ are algebraically dependent over k. Take an algebraic relation

$$f(b_1, \cdots b_n) = 0\ , \qquad f \in k[X_1, \cdots, X_n]$$

of lowest possible degree. Put $\deg f = d$. We can write

$$f(X_1, \cdots, X_n) = \sum_{0 \leqslant \nu_1, \cdots \nu_n < p} g_{\nu_1, \cdots, \nu_n}(X_1^p, \cdots, X_n^p) X_1^{\nu_1} \cdots X_n^{\nu_n}\ ,$$

where $g_{\nu_1, \cdots, \nu_n}$ are polynomials with coefficients in k. Since $b_1, \cdots, b_n$ are p-independent over k, we must have

$$g_{\nu_1, \cdots, \nu_n}(b_1^p, \cdots, b_n^p) = 0$$

for all $\nu_1, \cdots, \nu_n$. By the choice of f this is possible only if

$$f(X_1, \cdots, X_n) = g_{0,\ldots,0}(X_1^p, \cdots, X_n^p) .$$

But then we would have

$$f(X_1, \cdots, X_n) = \phi(X_1, \cdots, X_n)^p \quad \text{with} \quad \phi \in k^{p^{-1}}[X_1, \cdots, X_n] .$$

Hence $\phi(b_1, \cdots, b_n) = 0$. By MacLane's criterion of separability, however, K and $k^{p^{-1}}$ are linearly disjoint over k; since the monomials of degree $< d$ in $b_1, \cdots, b_n$ are linearly independent over k, they are also linearly independent over $k^{p^{-1}}$. Therefore such a relation as $\phi(b_1, \cdots, b_n) = 0$ cannot exist, and we get a contradiction.

Remark 1. A p-basis of a separable extension K/k need not be a transcendence basis. For example, if k is a perfect field and x is an indeterminate over k, then the field $k(x, x^{p^{-1}}, x^{p^{-2}}, \cdots)$ is perfect, so that the empty set is a p-basis of this extension.

Remark 2. Recall that a *differential basis* $\{b_i\}_{i\in I}$ of a field extension K/k is a subset of K such that $\{db_i\}_{i\in I}$ is a linear basis of $\Omega_{K/k}$ over K. The notion of differential basis coincides with that of transcendence basis if $\operatorname{char}(k) = 0$, and with that of p-basis if $\operatorname{char}(k) = p$.

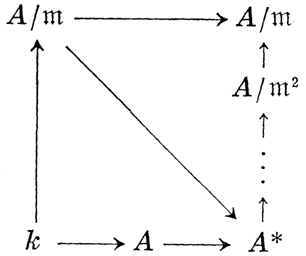
THEOREM 2. *Let K/k be a separable extension of fields. Then there is a subextension K' such that K'/k is purely transcendental and K/K' is formally etale.*

Proof. It suffices to take a differential basis B of K/k and put $K' = k(B)$.

2. DEFINITION. Let $(A, \mathfrak{m})$ be a local ring containing a field. A subfield k of A is called a *quasi-coefficient field* (q.c.f.) of A if the residue field $A/\mathfrak{m}$ is formally etale over k.

THEOREM 3. (i) *Let k be a q.c.f. of a local ring $(A, \mathfrak{m})$. Then there exists a unique coefficient field k' of the completion A^* of A such that $k \subset k'$.*
(ii) *If a local ring $(A, \mathfrak{m})$ includes a field k_0 and if $A/\mathfrak{m}$ is separable over k_0, then A has a q.c.f. k which includes k_0.*

Proof. (i) This is clear from the definitions and from the following diagram.



(ii) Let B be a differential basis of $A/\mathfrak{m}$ over k_0, and choose a pre-image x_λ for each element b_λ of B. If $f(X_1, \cdots, X_n)$ is a non-zero polynomial with coefficients in k_0 and if $b_1, \cdots, b_n$ are mutually distinct elements of B, then $f(b_1, \cdots, b_n) \neq 0$ by Theorem 1, hence $f(x_1, \cdots, x_n)$ is invertible in A. Therefore A includes the quotient field k of $k_0[\{x_\lambda\}]$, and k is obviously a q.c.f. of A.

Remark 3. In the notation of (i), every derivation D of A (into itself) over k is uniquely extended to a derivation of A^* over k'. Therefore we can identify $\mathrm{Der}_k(A)$ with an A-submodule of $\mathrm{Der}_{k'}(A^*)$.

THEOREM 4. *Let $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ be local rings such that $A \subset B$, $\mathfrak{m} = A \cap \mathfrak{n}$. Suppose that A includes a field.*
(i) *If $B/\mathfrak{n}$ is separable over $A/\mathfrak{m}$, then every q.c.f. of A can be extended to a q.c.f. of B.*
(ii) *If A is of characteristic p and $B^p \subset A$, then there exists a q.c.f. of A which can be extended to a q.c.f. of B.*

Proof. (i) Immediate from (ii) of Theorem 3.
(ii) Put $K = A/\mathfrak{m}$ and $L = B/\mathfrak{n}$. Then $L^p \subset K \subset L$. Let $B = \{\beta_i\}_{i \in I}$ be a p-basis of L/K and $C = \{\gamma_j\}_{j \in J}$ be a p-basis of K/L^p. Then it is easy to see that $\{\gamma_j\} \cup \{\beta_i^p\}$ is a p-basis of K and $\{\beta_i\} \cup \{\gamma_j\}$ is a p-basis of L. Therefore, if $\{y_i\}$ (resp. $\{z_j\}$) is a set of representatives of $\{\beta_i\}$ in L (resp. of $\{\gamma_j\}$ in K), then $\boldsymbol{F}_p(\{y_i, \{z_j\})$ is a q.c.f. of L and $\boldsymbol{F}_p(\{z_j\}, \{y_i^p\})$ is a q.c.f. of K. (cf. Nagata [6]).

THEOREM 5. *Let A be a noetherian local integral domain of characteristic p, and let K be the quotient field of A. Suppose A is pseudo-geometric (i.e. Nagata ring in the terminology of* [4]). *Let A^* be the completion of A, $\mathfrak{p}$ be a minimal prime ideal of A^* and L be the quotient field of $A^*/\mathfrak{p}$. Let k be a q.c.f. of A and k' be the coefficient field of A^* including k. Then K is separable over k if and only if L is* *separable over* k'.

Proof. Since A is pseudo-geometric, L is separable over K [4, (31. F)]. Suppose K is separable over k. Then L is separable over k. Let d be a derivation of k' into L, and let d_0 denote the restriction of d to k. Then d_0 can be extended to a derivation $D: L \to L$. The restriction $D|k'$ must coincide with d, since k' is formally etale over k. Therefore D is an extension of d to L. This proves that L is separable over k'. The converse is easy, since a subextension of a separable extension is separable.

Remark 4. Chevalley [8] gave the following definitions. Let $\mathfrak{o}$ be a noetherian complete local ring which includes a field k, and $u_1, u_2, \cdots$ be a sequence of elements of $\mathfrak{o}$ which converges to 0 in $\mathfrak{o}$. If the conditions $\sum a_i u_i = 0$, $a_i \in k$, imply $a_i = 0$ for all i, then the elements u_i are said to be strongly linearly independent over k. The elements of a finite sequence are said to be strongly linearly independent over k when they are linearly independent. When char $(\mathfrak{o}) = p$, we will say that $\mathfrak{o}$ is strongly separable[1] over k if, for every finite or infinite sequence (u_i) of elements of $\mathfrak{o}$ which are strongly linearly independent over k, the elements u_i^p are strongly linearly independent over k. Suppose $\mathfrak{o}$ is an integral domain and let L denote its quotient field. Then clearly

$\mathfrak{o}$ is strongly separable over $k \Rightarrow L$ is separable over k. It is easy to see that the converse is also true if $[k : k^p] < \infty$, but in general the two conditions are not equivalent. Under the assumption that the residue field of $\mathfrak{o}$ is a finite algebraic extension of k, a noetherian complete local domain $\mathfrak{o}$ is strongly separable over k if and only if there exists a system of parameters $x_1, \cdots, x_n$ of $\mathfrak{o}$ such that L is separable over the quotient field $k((x_1, \cdots, x_n))$ of $k[[x_1, \cdots, x_n]]$ (Nagata [7]). It is desirable to study quasi-coefficient fields further in the direction of Theorem 5 taking these definitions and facts into consideration.

3. In the unequal characteristic case we must define quasi-coefficient ring. Let us recall that, when $(A, \mathfrak{m})$ is a complete local ring with char $(A/\mathfrak{m}) = p > 0$, a subring I of A is called a coefficient ring of A if (i) I is a noetherian complete local ring with maximal ideal pI (whence $pI = \mathfrak{m} \cap I$) and (ii) A and I have the same residue field, i.e. $A = I + \mathfrak{m}$.

1) In Chevalley's terminology $\mathfrak{o}$ is said to be separably generated over k.

DEFINITION. Let $(A, \mathfrak{m})$ be a (not necessarily complete) local ring with $\operatorname{char}(A/\mathfrak{m}) = p > 0$. A subring I of A is called a quasi-coefficient ring of A if

(i′) I is a noetherian local ring with maximal ideal pI, and

(ii′) the residue field $A/\mathfrak{m}$ of A is formally etale over I/pI.

In both cases, all ideals of I have the form $p^m I$ $(m \geqslant 0)$. Therefore, if $\operatorname{char}(A) = 0$ (i.e. the unique homomorphism $\boldsymbol{Z} \to A$ is injective) then $p^m I \neq 0$ for all $m \geqslant 0$ and I is a discrete valuation ring. If $\operatorname{char}(A) = p^n$, $n > 0$, then we have $p^{n-1} I \neq 0$, $p^n I = 0$ and I is artinian.

Remark 5. In the case $\operatorname{char}(A) = p^n$, there exists a complete discrete valuation ring W with maximal ideal pW such that $I \cong W/p^n W$, and such W is uniquely determined. In fact, for each field k of characteristic p there exists a complete discrete valuation ring W of characteristic zero such that $W/pW \cong k$, and such W is necessarily flat over $\boldsymbol{Z}_{p\boldsymbol{Z}}$, hence is unique up to isomorphism [3, (19.7.2)]. Moreover, W is formally smooth over $\boldsymbol{Z}_{p\boldsymbol{Z}}$ by [3, (19.7.1)], hence for any complete local ring $(B, \mathfrak{m}_B)$ with residue field k there exists at least one homomorphism $W \to B$ which lifts the isomorphism $W/pW \cong B/\mathfrak{m}_B$. The ring I considered above with maximal ideal pI such that $p^{n-1} I \neq 0$, $p^n I = 0$, is artinian, hence complete, and if we take I for B then the homomorphism $W \to I$ is surjective with kernel $p^n W$.

THEOREM 6. *Let $(A, \mathfrak{m})$ be a noetherian local ring and A^* be its completion. Let I be a quasi-coefficient ring of A. Then there exists a unique coefficient ring J of A^* including I, and J is formally unramified over I. If A is flat over I, then A^* is flat over J and J is formally etale over I.*

Proof. Since A is separated, we may view A and I as subrings of A^*. By [3, (19.7.2)] there exists a complete noetherian local ring J' and a flat local homomorphism $I \to J'$ such that $J'/pJ' \cong A/\mathfrak{m}$ over I/pI. Since $\operatorname{rad}(J') = pJ' = \operatorname{rad}(I)J'$ and since J'/pJ' is formally etale over I/pI, it is easy to see that J' is formally etale over I. Therefore there is a unique homomorphism $\phi: J' \to A^*$ which makes the following diagram commutative:

$$\begin{array}{ccc} J' & \longrightarrow & A/\mathfrak{m} \\ \uparrow & \searrow^{\phi} & \uparrow \\ I & \longrightarrow & A^* \end{array}$$

Put $J = \phi(J')$. Then J is a coefficient ring of A^*. Since J' is formally unramified over I, so is J. If A is flat over I then A^* is also flat over I, hence we have

$$pJ' \otimes_{J'} A^* = (pI \otimes_I J') \otimes_{J'} A^* = pI \otimes_I A^* = pA^* .$$

Therefore (by [1, Ch. 3, § 5, no. 2, Theorem 1 (iii)], [4, (20.C)]) the map ϕ makes A^* a flat J'-module, and consequently ϕ is injective (since it is local). Thus $J' \cong J$.

It remains to prove the uniqueness of J. If J'' is a coefficient ring of A^* including I, then we can use the same argument to prove the existence of a homomorphism $\psi : J' \to J''$ such that

$$\begin{array}{ccc} J' & \longrightarrow & A/\mathfrak{m} = J''/pJ'' \\ \uparrow & \searrow^{\psi} & \uparrow \\ I & \longrightarrow & J'' \end{array}$$

commutes. Let $i : J'' \to A^*$ denote the inclusion map. Then $\phi = i \circ \psi$ by the uniqueness of ϕ, hence $J'' = J$. QED.

COROLLARY. *Let $(A, \mathfrak{m})$ and I be as in the theorem, and let $\{y_\lambda\}$ be a system of generators of $\mathfrak{m}$. If $D \in \mathrm{Der}_I(A)$ and $D(y_\lambda) = 0$ for all λ, then $D = 0$.*

Proof. Extend D to A^* by continuity. Then $D = 0$ on J, hence on A^*.

Quasi-coefficient rings exist in any local ring of unequal characteristic. In fact, our next theorem gives a little stronger existence statement.

THEOREM 7. *Let $(A, \mathfrak{m})$ be a local ring, and $(C, \mathfrak{p})$ be a noetherian local ring such that $C \subset A$, $\mathfrak{p} = \mathfrak{m} \cap C$. Suppose $A/\mathfrak{m}$ is separable over $C/\mathfrak{p}$. Then there is a noetherian local ring $(B, \mathfrak{n})$ such that $C \subset B \subset A$,*

$\mathfrak{n} = \mathfrak{p}B = \mathfrak{m} \cap C$ and such that $A/\mathfrak{m}$ is formally etale over $B/\mathfrak{n}$. If A is flat over C, then A is also flat over B.

Proof. Let $\{\bar{x}_i\}_{i \in I}$ be a differential basis of $A/\mathfrak{m}$ over $C/\mathfrak{p}$, and let $x_i \in A$ be a pre-image of $\bar{x}_i$ for each $i \in I$. Let $\{X_i\}_{i \in I}$ be independent variables and put $R = C[\{X_i\}]$, $B' = R_{\mathfrak{p}R}$. Then B' is noetherian. In fact, it is a local ring with finitely generated maximal ideal, and $\bigcap_\nu \mathfrak{p}^\nu B' = (0)$ because $(\cap \mathfrak{p}^\nu B') \cap R = \cap \mathfrak{p}^\nu R = (0)$. Moreover, if $\mathfrak{a} = (f_1, \cdots, f_r)$ is a finitely generated ideal of B' then $B'/\mathfrak{a}$ is also a localization of a polynomial ring over a noetherian local ring, hence $B'/\mathfrak{a}$ is also separated. In other words, every finitely generated ideal of B' is closed. It follows that B' is noetherian [5, (31.8)].

Consider the C-homomorphism $R \to A$ which maps X_i to x_i. Since $\{\bar{x}_i\}_{i \in I}$ is algebraically independent over $C/\mathfrak{p}$, the homomorphism $R \to A$ factors as $R \to B' \to A$. Denote the image of B' in A by B. Then B is a noetherian local ring with maximal ideal $\mathfrak{p}B$. Since $\mathfrak{p} \subset \mathfrak{m}$ we have $\mathfrak{p}B = \mathfrak{m} \cap B$. The last assertion of the theorem is proved as in Theorem 6.

If $(A, \mathfrak{m})$ is a local ring with $\mathrm{char}(A/\mathfrak{m}) = p > 0$, then we can find a local subring C with maximal ideal pC satisfying the condition of Theorem 7. It suffices to take $C = \boldsymbol{Z}_{p\boldsymbol{Z}}$ when $\mathrm{char}(A) = 0$, and $C = \boldsymbol{Z}/p^n$ when $\mathrm{char}(A) = p^n$. Then the local ring B of the theorem is a quasi-coefficient ring of A.

REFERENCES

[1] N. Bourbaki, Algèbre Commutative, Ch. 3,4. Hermann, Paris, 1961.
[2] I. S. Cohen, On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc. **59** (1946), 54–106.
[3] A. Grothendieck and J. Dieudonné, Éléments de Géométrie Algébrique, Ch. IV, Première Partie, Publ. IHES, No. 20, 1964.
[4] H. Matsumura, Commutative Algebra, Benjamin, New York 1970.
[5] M. Nagata, Local Rings, Interscience, New York 1962.
[6] ——, Note on coefficient fields of complete local rings. Mem. Coll. Sci., Univ. Kyoto **32** (1959), 91–92.
[7] ——, Note on complete local integrity domains. Mem. Coll. Sci., Univ. Kyoto **28** (1954), 271–278.
[8] C. Chevalley, Some properties of ideals in rings of power series. Trans. Amer. Math. Soc. **55** (1944), 68–84.

Department of Mathematics
Nagoya University