H. Matsumura
Nagoya Math. J.
Vol. 87 (1982), 227-245

INTEGRABLE DERIVATIONS

HIDEYUKI MATSUMURA

Dedicated to Prof. Yoshikazu Nakai on his Sixtieth Birthday

Introduction

Let A be a commutative ring and D be a derivation of A into itself. If there exists a homomorphism $E: A \to A[[t]]$ such that

$$E(a) \equiv a + tD(a) \qquad \text{mod } t^2$$

then we say that D is integrable. Integrable derivations have many good properties. In fact, most of unpleasant phenomena of derivations in characteristic p disappear if we consider integrable derivations only.

In § 1 we state definitions and basic properties of differentiations, and we give some examples of non-integrable derivations.

§ 2 is devoted to theorems which are essentially due to Seidenberg ([18], [19], [20]). These theorems show that integrable derivations behave as they should, and provides us with necessary conditions for integrability.

Then in § 3 and § 4 we prove some sufficient conditions. In § 3 we consider smooth or formally smooth algebras, using André's homology theory. In § 4, by an elementary argument we prove a criterion of integrability, which shows that there are plenty of integrable derivations (in the case of an integral domain finitely generated over a perfect field).

§ 1. Definitions and examples

In this article all rings are assumed to be commutative with a unit element. Local rings are assumed to be noetherian.

Let A be a ring. The set of all derivations of A into itself is an A-module and is denoted by $\mathrm{Der}(A)$. If k is a subring of A, the submodule of $\mathrm{Der}(A)$ consisting of those derivations which vanish on k is denoted by $\mathrm{Der}_k(A)$.

Received December 26, 1980.

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

A differentiation $\underline{D}$ of A (in the sense of Hasse-Schmidt [7]) is an infinite sequence $\underline{D} = (D_0, D_1, D_2, \cdots)$ of additive endomorphisms $D_i : A \to A$ such that

(1.1) $$D_0 = \text{identity}\,, \qquad D_n(ab) = \sum_{i+j=n} D_i(a)D_j(b)\,.$$

It follows that D_1 is a derivation. D_i will be called the i-th component of $\underline{D}$. Let t be an indeterminate over A, and put

(1.2) $$E(a) = E_t(a) = \sum_{n=0}^{\infty} t^n D_n(a) \in A[[t]] \quad (a \in A)\,.$$

Then $E = E_t$ is a ring homomorphism from A into $A[[t]]$ such that $a \equiv E(a) \bmod t$. It can be uniquely extended to an endomorphism of $A[[t]]$ such that $E(t) = t$; namely, we define

(1.3) $$E\Big(\sum_{i=1}^{\infty} t^i a_i\Big) = \sum_{i=0}^{\infty} t^i E(a_i)\,.$$

Then, using

(1.4) $$E(a) \equiv a \bmod t \ \ (a \in A)\,, \qquad E(t) = t\,,$$

we can easily see that E is an automorphism of $A[[t]]$. Conversely, any automorphism of $A[[t]]$ satisfying (1.4) comes from a differentiation. We will denote the automorphism $E = E_t$ obtained from $\underline{D}$ by $\Lambda(\underline{D})$; thus Λ is a bijection from the set of differentiations of A to the set of automorphisms of $A[[t]]$ satisfying (1.4). This latter set is obviously a subgroup of Aut $(A[[t]])$, therefore by means of Λ we can make the set of differentiations a group, which we denote by HS(A) and call the Hasse-Schmidt group of A. If $\underline{D} = (1, D_1, \cdots)$ and $\underline{D}' = (1, D_1', \cdots)$ are differentiations of A, easy calculations show that

(1.5) $\underline{D}\,\underline{D}' = (1, D_1 + D_1', D_2 + D_1D_1' + D_2', \cdots, \sum_i D_iD_{n-i}', \cdots)$ and

(1.6) $\underline{D}^{-1} = (1, -D_1, D_1^2 - D_2, -D_1^3 + D_1D_2 + D_2D_1 - D_3, \cdots)\,.$

Moreover, from (1.1) we see that

(1.7) if $x \in A$, then $(1, xD_1, x^2D_2, \cdots, x^nD_n, \cdots)$ is a differentiation.

We say that a derivation $D \in \text{Der}\,(A)$ is *integrable* if there exists a differentiation $\underline{D} = (1, D_1, D_2, \cdots)$ of A with $D_1 = D$. Such $\underline{D}$ is called (by lack of better terminology) an *integral* of D; we also say that $\underline{D}$ lifts D. The formulas (1.5), (1.6), (1.7) show that the set of integrable derivations of A is an A-submodule of $\mathrm{Der}(A)$. We denote it by $\mathrm{Ider}(A)$. If A contains the rational number field $\mathbf{Q}$ it is easy to see that all derivations are integrable. The same holds when A is a field (of any characteristic), see Th. 6. But in general there are non-integrable derivations.

Remark 1. If t' is an element of $A[[t]]$ without constant term and $\underline{D}$ is a differentiation of A, we get a homomorphism $E_{t'}: A \to A[[t]]$ by $E_{t'}(a) = \sum_{n=0}^{\infty} t'^n D_n(a)$, and this can be uniquely extended to an automorphism of $A[[t]]$ as in (1.3). Applying Λ^{-1} to this, we get a new differentiation. For instance if $t' = xt$ then we get the differentiation of (1.7).

Remark 2. If E_t and E'_t correspond to $\underline{D}$ and $\underline{D}'$ respectively, and if we put $s = t^n$ for some $n > 1$, then $E_t \circ E'_s$ gives a differentiation of the form $(1, D_1, \cdots, D_{n-1}, D_n + D'_1, \cdots)$. From this it is clear that an integrable derivation can have many integrals.

Let k be a subring of A. A differentiation $\underline{D} = (1, D_1, D_2, \cdots)$ is called a differentiation of A over k if $D_i(a) = 0$ for all $i > 0$ and for all $a \in k$. The set of such differentiations is denoted by $\mathrm{HS}_k(A)$. A derivation D is said to be *integrable over* k if it has an integral belonging to $\mathrm{HS}_k(A)$. The set of derivations which are integrable over k will be denoted by $\mathrm{Ider}_k(A)$, which should not be confused with $\mathrm{Der}_k(A) \cap \mathrm{Ider}(A)$. For instance, if A is a ring of characteristic p and if $k = A^p$, then we have $\mathrm{Der}(A) = \mathrm{Der}_k(A)$, but in most cases $\mathrm{Ider}(A)$ is not equal to $\mathrm{Ider}_k(A)$, the latter being zero if A is reduced. In fact, if $\underline{D} = (1, D_1, D_2, \cdots) \in \mathrm{HS}(A)$ and if $q = p^r$ is a power of p, then we have

$$E_t(a^q) = E_t(a)^q = (a + tD_1(a) + \cdots)^q = a^q + t^q D_1(a)^q + \cdots,$$

therefore it holds that

$$D_i(a^q) = 0 \text{ if } i \not\equiv 0\,(q), \qquad D_q(a^q) = D_1(a)^q. \tag{1.8}$$

A differentiation $\underline{D}$ is said to be *iterative* if

$$D_i \circ D_j = \binom{i+j}{i} D_{i+j} \qquad \text{for all } i, j. \tag{1.9}$$

This is equivalent to saying that the following diagram

$$\begin{array}{ccc} A & \xrightarrow{E_t} & A[[t]] \\ {\scriptstyle E_{t+u}}\downarrow & & \downarrow{\scriptstyle E_u} \\ A[[t+u]] & \xrightarrow{i} & A[[t, u]] \end{array} \tag{1.10}$$

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

(where i is the inclusion map and $E_u(t) = t$) is commutative.

A derivation D will be said to be *strongly integrable* if it has an iterative differentiation as integral.

If the ring A contains the rational number field $\mathbf{Q}$, then every derivation $D \in \mathrm{Der}(A)$ is strongly integrable, and there is a unique iterative differentiation which lifts D, namely $(1, D, (1/2!)D^2, \cdots, (1/n!)D^n, \cdots)$. When A is of characteristic p, a strongly integrable derivation D must satisfy $D^p = 0$. In fact, if $\underline{D} = (1, D_1, D_2, \cdots)$ is iterative, then by induction we have $D_1^i = i!\, D_i$ (all i), hence $D_1^p = 0$. The condition $D^p = 0$ is also sufficient for strong integrability when A is a field (cf. Th. 7). In the case of characteristic p the strongly integrable derivations do not form an A-module.

We shall say that differentiations $\underline{D} = (1, D_1, D_2, \cdots)$ and $\underline{D}' = (1, D'_1, D'_2, \cdots)$ *commute* if D_i and D'_j commute for every pair (i, j). If $\underline{D}$ and $\underline{D}'$ are iterative and commute with each other, then their product $\underline{D}\,\underline{D}'$ is again iterative, because $(E_u E'_u)(E_t E'_t) = E_u E_t E'_u E'_t = E_{t+u} E'_{t+u}$ (where all maps are viewed as automorphisms of $A[[t, u]]$ which leave t, u invariant).

Like derivations, differentiations can be uniquely extended to a localization. In fact, let A be a ring, S a multiplicative subset of A, $\underline{D} \in \mathrm{HS}(A)$ and $E_t : A \to A[[t]]$ the homomorphism corresponding to $\underline{D}$. Let $\psi : A \to A_S$ and $\psi' : A[[t]] \to A_S[[t]]$ be the natural maps. If $s \in S$ then the element $\psi'(E_t(s)) = \psi(s) + t\psi(D_1(s) + \cdots$ is invertible in $A_S[[t]]$, whence $\psi' \circ E_t$ factors through A_S, i.e. there exists a unique homomorphism $E' : A_S \to A_S[[t]]$ satisfying $\psi' \circ E_t = E'\psi \circ$.

Similarly, if I is an ideal of A and A^* is the I-adic completion of A, then a differentiation $\underline{D} = (1, D_1, D_2, \cdots)$ is uniquely extended to A^*. In fact, we have $D_n(I^\nu) \subseteq I^{\nu-n}$ for $\nu > n$, and so each D_n is uniformly continuous in the I-adic topology and can be uniquely extended to the completion A^*.

Example 1. Let k be a ring of characteristic p, and put $A = k[X]/(X^p)$. Put $x = X \bmod X^p$. Define $D \in \mathrm{Der}_k(A)$ by $Dx = 1$ (thus D is induced by d/dx of $k[X]$). If D were integrable we would have

$$0 = E_t(x^p) = E_t(x)^p = (x + t + \cdots)^p = t^p + \cdots,$$

which is a contradiction. Therefore D is not integrable. The derivation xD is integrable: in fact, $x \mapsto x(1+t) \in A[[t]]$ defines a k-algebra homomorphism. We have $\mathrm{Der}_k(A) = A \cdot D$ (a free module), $\mathrm{Ider}_k(A) = xA \cdot D \simeq$

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

xA (not free).

EXAMPLE 2. Let R be a discrete valuation ring of characteristic zero with maximal ideal pR, where p is a prime number. Put $k = R/pR$, $A = R[X, Y]/(pX - Y^p)$. Then the derivation $Y^{p-1}\partial/\partial X + \partial/\partial Y$ of $R[X, Y]$ induces a derivation D of A, which is not integrable. In fact, D induces a derivation $\bar{D}$ of $A/pA = k[X, Y]/(Y^p)$ such that $\bar{D}(y) = 1$, and as in the preceding example $\bar{D}$ is not integrable. If D were integrable then $\bar{D}$ would be so.

EXAMPLE 3. Let k be a field of characteristic p, and let $A = k[x, y] = k[X, Y]/(Y^p - X^p - X^{p+1})$. The polynomial $Y^p - X^p(1 + X)$ is irreducible (Eisenstein criterion), hence A is an integral domain. The partial derivation $\partial/\partial Y$ induces a derivation D of A over k. If D were integrable to $\underline{D} = (1, D_1, D_2, \cdots) \in \mathrm{HS}(A)$ with $D_1 = D$, then we should have

$$0 = D_p(y^p - x^p - x^{p+1}) = D(y)^p - D(x)^p - \sum_{i=0}^{p} D_i(x^p)D_{p-i}(x) = 1 - x^p D_p(x)\,.$$

Therefore $D_p(x) = 1/x^p$. But $1/x^p$ is not in A. Hence D is not integrable.

EXAMPLE 4. Let B be a ring and $A = B[[X]]$ be the formal power series ring over B. Let t be another indeterminate. Then the map $f(X) \mapsto f(X + t)$ defines an iterative differentiation of A. Similarly for $A[X]$.

§ 2. Seidenberg Theorems

Let A be a ring, I an ideal of A and $\underline{D} = (1, D_1, D_2, \cdots) \in \mathrm{HS}(A)$. The ideal I is said to be $\underline{D}$-invariant (or invariant under $\underline{D}$) if $D_i(I) \subseteq I$ for all i. When this is the case, the differentiation $\underline{D}$ induces a differentiation of A/I. Recall that an ideal of A is called a differential ideal if all derivations of A map the ideal into itself. We shall say that the ideal I is a HS-ideal (resp. HS_k-ideal) if it is invariant under all differentiations in $\mathrm{HS}(A)$ (resp. $\mathrm{HS}_k(A)$). If A contains $\mathbf{Q}$, then the differential ideals and the HS-ideals are the same (this can be seen using Remark 2 of § 1.)

THEOREM 1. *Let A be a ring, I an ideal of A and t an indeterminate over A; put $A^* = A[[t]]$ and $I^* = I[[t]]$. Let $\underline{D} \in \mathrm{HS}(A)$. Then I is $\underline{D}$-invariant if and only if the automorphism E_t of A^* associated to $\underline{D}$ maps I^* onto itself*: $E_t(I^*) = I^*$.

Proof. If $D_i(I) \subseteq I$ for all i, we have $E_t(I^*) \subseteq I^*$. It is easy to see that $(E_t)^{-1}(a) = \sum t^n D'_n(a)$ where D'_n is a polynomial in $D_1, \cdots, D_n$. Therefore we have $(E_t)^{-1}(I^*) \subseteq I^*$ also. Thus $E_t(I^*) = I^*$. The converse is obvious.

THEOREM 2. *Let A be a noetherian ring and $P \in \mathrm{Ass}(A)$. Then P is an* HS-*ideal, and consequently there are canonical maps*

$$\mathrm{HS}(A) \longrightarrow \mathrm{HS}(A/P), \qquad \mathrm{Ider}(A) \longrightarrow \mathrm{Ider}(A/P).$$

Proof. We give only a sketch of Seidenberg's proof in [19] pp. 23–24. If $(0) = q_1 \cap \cdots \cap q_r$ is an irredundant primary decomposition in A and if p_i is the associated prime ideal of q_i, then $(0) = q_1^* \cap \cdots \cap q_r^*$ is an irredundant primary decomposition in A^* and p_i^* is the associated prime ideal of q_i^*. Thus any automorphism E of A^* induces a permutation of $\mathrm{Ass}(A^*) = \{p_1^*, \cdots, p_r^*\}$. If E corresponds to a differentiation then from $E(p_i^*) = p_j^*$ it follows that $p_i \subseteq p_j$. Considering E^{-1} we get $p_i = p_j$, or what amounts to the same, $p_i^* = p_j^*$. By the preceding theorem this means that $p_1, \cdots, p_r$ are HS-ideals.

Remark 3. Example 1 shows that P is not necessarily a differential ideal.

THEOREM 3. *Let A be a noetherian integral domain and A' be its derived normal ring. Then any differentiation of A extends to A', and consequently there are canonical mappings*

$$\mathrm{HS}(A) \longrightarrow \mathrm{HS}(A'), \qquad \mathrm{Ider}(A) \longrightarrow \mathrm{Ider}(A').$$

Proof. Let K denote the quotient field of A, let $\underline{D} \in \mathrm{HS}(A)$ and let $E: A \to A[[t]]$ denote the corresponding homomorphism. We know that $\underline{D}$ and E can be extended uniquely to K; we denote the extensions by the same letters $\underline{D}$ and E. Then we have to show: $E(A') \subseteq A'[[t]]$.

It is well known that $A[[t]]$ is normal if A is a noetherian normal ring. In the present case the ring A' is not necessarily noetherian, but still it is a Krull ring (cf. Nagata, Local Rings, p. 118), therefore an intersection of discrete valuation rings: $A' = \bigcap_\alpha V_\alpha$. Then $A'[[t]] = \bigcap_\alpha V_\alpha[[t]]$, and each $V_\alpha[[t]]$ is normal. Therefore $A'[[t]]$ is also normal. Let $a' \in A'$, $a' = u/v$, $u \in A$, $v \in A$. Then $E(a') = E(u)/E(v)$ belongs to the quotient field of $A[[t]]$. Moreover, since a' is integral over A, $E(a')$ is integral over $A[[t]]$, hence a fortiori over $A'[[t]]$. Therefore $E(a') \in A'[[t]]$. Q.E.D.

Remark 4. If A' is finite over A then $A'[[t]]$ is finite over $A[[t]]$ and is equal to the derived normal ring of $A[[t]]$.

Remark 5. Example 3 of § 1, which is also due to Seidenberg, shows that a non-integrable derivation of A does not necessarily extend to A'.

COROLLARY. *Let A, A' be as in Th. 3 and $\mathfrak{c}$ be the conductor of A (i.e. $\mathfrak{c} = \{a \in A \mid aA' \subseteq A\}$). Then $\mathfrak{c}$ is an* HS-*ideal.*

Proof. Let $a \in \mathfrak{c}$, $x \in A'$, $\underline{D} = (1, D_1, D_2, \cdots) \in \mathrm{HS}(A)$. Then $ax \in A$ and so $D_n(ax) = D_n(a)x + D_{n-1}(a)D_1(x) + \cdots + aD_n(x) \in A$. We prove $D_n(a) \in \mathfrak{c}$ by induction on n. Suppose $D_i(a) \in \mathfrak{c}$ for $i < n$. Since $D_i(x) \in A'$ for all i, we have $D_n(a)x \in A$. As x is an arbitrary element of A' this means that $D_n(a) \in \mathfrak{c}$.

THEOREM 4. *Let A be an excellent ring, I be the largest ideal which defines* Sing (A) *and P be the generic point of an irreducible component of* Sing (A). *Then I and P are* HS-*ideals.*

Proof. Since P is an associated prime of I, if I is an HS-ideal then P is so by Th. 2. Thus it suffices to prove that I^* is invariant under any automorphism of $A^* = A[[t]]$. Now A^* is the t-adic completion of $A[t]$. Since $A[t]$ is excellent the canonical homomorphism $A[t] \to A^*$ is regular by a well-known theorem of Grothendieck (cf. [EGA IV–2] 7.8.3 (v) or [11] Th. 79). On the other hand it is obvious that the canonical map $A \to A[t]$ is regular (for any A). Therefore $A \to A^*$ is regular. It follows that I^* defines Sing (A^*). Since I is reduced (i.e. an intersection of prime ideals), so is I^*. Thus I^* is the largest ideal which defines Sing (A^*), and, as such, is invariant under any automorphism of A^*. Q.E.D.

Remark 6. Similarly, the largest ideal which defines the set $\{\mathfrak{p} \in \mathrm{Spec}(A) \mid A_\mathfrak{p}$ is not $Q\}$, where Q denotes the property normal, Cohen-Macaulay, Gorenstein (cf. [21]), or complete intersection (cf. [3]), is an HS-ideal.

Let k be a field and $A = k[x_1, \cdots, x_n]$ be a finitely generated k-algebra. Put $R = k[X_1, \cdots, X_n]$, and write $A = R/I$, where I is the kernel of the k-algebra homomorphism $R \to A$ which sends X_i to x_i. Let $f_1, \cdots, f_s$ be a system of generators of I. We write $\partial f/\partial x_i$ for $\partial f/\partial X_i \bmod I$. Consider the Jacobian matrix $(\partial f/\partial x) = (\partial f_i/\partial x_j)_{1 \leqslant i \leqslant s,\, 1 \leqslant j \leqslant n}$. Let ν be an integer, $0 \leqslant \nu < n$. The ideal of A generated by the $(n-\nu) \times (n-\nu)$ minors of $(\partial f/\partial x)$ will be called the ν-th Jacobian ideal of A and will be denoted by $J_\nu(A)$ or simply by J_ν. We put $J_n = J_{n+1} = \cdots = A$. Then we have $J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots$. Lipman [9] calls the first non-zero J_ν the Jacobian ideal of A. When k is a perfect field and A is an integral domain of dimension d, it is known that the matrix $(\partial f/\partial x)$ has rank $n-d$ ([AG] pp. 32–33). Therefore J_d is the Jacobian ideal of A in this case.

The exact sequence (cf. [11] Th. 58)

$$I/I^2 \longrightarrow \Omega_{R/k} \otimes_R A = AdX_1 \oplus \cdots \oplus AdX_n \longrightarrow \Omega_{A/k} \longrightarrow 0$$

shows that J_ν is the ν-th Fitting invariant of $\Omega_{A/k}$ (cf. [15]). Therefore the ideals J_ν are invariants of the k-algebra A, independent of the representation $A = R/I$ and of the choice of the generators $f_1, \cdots, f_s$ of I. We will state the invariance more precisely in the following lemma.

LEMMA 1. *The ideals J_ν are left fixed by all automorphisms of the k-algebra A.*

Proof. Let σ be an automorphism of the k-algebra A, and M be an A-module. The A-module structure on M is defined by a k-algebra homomorphism $\psi: A \to \mathrm{End}_k(M)$. We define a new A-module structure on M by $\psi \circ \sigma$, and denote the new A-module by M_σ. Thus, ax in $M_\sigma = a^\sigma x$ in M $(a \in A, x \in M)$. If $D: A \to M$ is a k-derivation, then $D \circ \sigma$ is a k-derivation of A into M_σ. Call it D^σ.

$$\begin{aligned} D^\sigma(ab) = D(a^\sigma b^\sigma) &= a^\sigma D(b^\sigma) + b^\sigma D(a^\sigma) \qquad \text{in } M \\ &= aD^\sigma(b) + bD^\sigma(a) \qquad \text{in } M_\sigma\,. \end{aligned}$$

Let $\Omega_{A/k} = \sum_1^n Adx_i$. $\sum a_i dx_i = 0$ means that $\sum a_i D(x_i) = 0$ holds for every A-module M and for every derivation $D: A \to M$. Then $\sum a_i D^\sigma(x_i) = 0$ in M_σ, i.e. $\sum a_i^\sigma D(x_i^\sigma) = 0$ in M. Therefore we have $\sum a_i^\sigma\, dx_i^\sigma = 0$. Thus, by putting

$$(\textstyle\sum a_i\, dx_i)^\sigma = \sum a_i^\sigma\, dx_i^\sigma$$

we can define an automorphism of the k-module $\Omega_{A/k}$ such that

$$(a\omega)^\sigma = a^\sigma \omega^\sigma \qquad (a \in A, \omega \in \Omega_{A/k})\,.$$

If $dx_1, \cdots, dx_n$ generate $\Omega_{A/k}$, then $dx_1^\sigma, \cdots, dx_n^\sigma$ also generate $\Omega_{A/k}$. Moreover, the σ-image of a relation matrix of $dx_1, \cdots, dx_n$ is a relation matrix of $dx_1^\sigma, \cdots, dx_n^\sigma$. By the independence of Fitting ideals on the choice of generators of the A-module, our lemma is now obvious.

Let B be a k-algebra. The module $\Omega_{B/k}$ represents the functor $M \to \mathrm{Der}_k(B, M)$ on the category of all B-modules. If the restriction of this functor to the category of finite B-modules is representable, i.e. if there exist a finite B-module M_0 and a k-derivation $d_0 : B \to M_0$ with the universal mapping property for the k-derivations of B into finite B-modules, then M_0 is called the universal finite module of differentials of B over k and is denoted by $D_k(B)$, cf. [17] or [22]. The following lemmas can be easily proved from the definition.

LEMMA 2. *Let B be a noetherian k-algebra such that $D_k(B)$ exists. Then $D_k(B^*)$ also exists (where $B^* = B[[t]]$), and we have*

$$D_k(B^*) = (D_k(B) \otimes_B B^*) \oplus B^* dt .$$

LEMMA 3. *Let R be a noetherian k-algebra, I an ideal of R and $B = R/I$. Suppose $D_k(R)$ exists. Then $D_k(B)$ also exists, and we have an exact sequence*

$$I/I^2 \longrightarrow D_k(R) \otimes_R B \longrightarrow D_k(B) \longrightarrow 0 .$$

(cf. [22].)

Returning to the situation $R = k[X_1, \cdots, X_n]$, $I = (f_1, \cdots, f_s)$ and $A = R/I$, we have

$$A^* = R^*/I^* , \qquad I^* = \sum_1^n f_i R^*$$

and the sequence

$$I^*/I^{*2} \longrightarrow D_k(R^*) \otimes_{R^*} A^* \longrightarrow D_k(A^*) \longrightarrow 0$$

is exact. Moreover, $D_k(R^*) \otimes_{R^*} A^* = (D_k(R) \otimes_R A^*) \oplus A^* dt$ is a free A^*-module with basis $dX_1, \cdots, dX_n, dt$. Therefore $J_\nu A^*$ is the $(\nu + 1)$st Fitting invariant of $D_k(A^*)$, and proof of Lemma 1 can be applied, mutatis mutandis, to show that $J_\nu A^*$ is invariant under all k-algebra automorphisms of A^*. This proves the following theorem.

THEOREM 5. *Let k be a field and A be a k-algebra of finite type. Then the ideals J_ν are* HS_k*-ideals.*

EXAMPLE 5. Let k be a field of characteristic $p \geqslant 0$ and let $A = k[x, y] = k[X, Y]/(Y^2 - X^3)$. The derived normal ring A' is $k[u]$ where $u = y/x$, and we have $x = u^2$, $y = u^3$. The conductor is $xA' = (x, y)A$, which is also the largest ideal that defines $\mathrm{Sing}\,(A)$. Put $D_0 = d/du \in \mathrm{Der}_k\,(A')$.

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

The derivation uD_0 induces an integrable derivation D_1 of A because $E_t : A' \to A'[[t]]$ defined by $E_t(u) = u(1 + t)$ maps $x = u^2$ and $y = u^3$ into $A[[t]]$. Similarly u^2D_0 induces an integrable derivation D_2 of A. Let $D \in \mathrm{Ider}_k(A)$. Then $D \in \mathrm{Ider}_k(A') = A'D_0$. If $p \neq 2$ then $D_0(x) = 2u \notin A$ and so $D_0 \notin \mathrm{Der}_k(A)$. If $p = 2$ then for any element f in $k[u]$ we have $(u + t + ft^2)^3 = u^3 + 3u^2t + 3(u + u^2f)t^2 + \cdots$, and $u + u^2f \notin A$. Thus $D_0 \notin \mathrm{Ider}_k(A)$ in all cases. Therefore we have $\mathrm{Ider}_k(A) = AD_1 + AD_2$. When $p \neq 2, 3$ it is easy to see that $\mathrm{Der}_k(A) = AD_1 + AD_2 = \mathrm{Ider}_k(A)$.

If $p = 2$ then the Jacobian ideal of A is x^2A. The partial derivation $\partial/\partial Y$ of $k[X, Y]$ induces a derivation D_3 on A, and $D_0 = xD_3$. We have $\mathrm{Der}_k(A) = AD_3$, $\mathrm{Ider}_k(A) = AD_1 + AD_2 = AyD_3 + Ax^2D_3$. The derivation D_0 maps x^2A and $(x, y)A$ into themselves, but it is not integrable as we have already seen.

If $p = 3$ the partial derivation $\partial/\partial X$ induces a derivation D_4 on A. We have $\mathrm{Der}_k(A) = AD_4$, $\mathrm{Ider}_k(A) = AxD_4 + AyD_4$.

§ 3. Integrability and smoothness

The theorems of the preceding section give various necessary conditions for a derivation to be integrable. In this section we will consider sufficient conditions of integrability.

Let k be a ring and A a k-algebra. To give a derivation $D \in \mathrm{Der}_k(A)$ is to give a k-algebra homomorphism $\phi_1: A \to A[t]/(t^2)$ such that $\phi_1(a) \equiv a \bmod t$. Saying that D is integrable (over k) is equivalent to saying that ϕ_1 can be lifted to a k-algebra homomorphism $E : A \to A[[t]]$, and since $A[[t]] = \varprojlim A[t]/(t^n)$ it suffices to find, step by step, k-algebra homomorphisms $\phi_n : A \to A[t]/(t^{n+1})$ such that $\phi_{n-1}(a) = \phi_n(a) \bmod t^n$. Such lifting is always possible if A is a smooth k-algebra in the sense of [11] (i.e. formally smooth with respect to the discrete topology in the sense of EGA, or 0-smooth in the sense of André [1].)

THEOREM 6. *Let k be a field and K be a separable extension field of k. Then K is a smooth k-algebra. Consequently, every derivation of K over k is integrable over k.*

Proof. The smoothness is well known, cf. [5], [11]. Actually, one can say more: Let B be a differential basis of K over k. Then $k(B)$ is a purely transcendental extension of k, and K is formally etale over $k(B)$. (Cf. [10, Th. 2].)

COROLLARY. *Let K be a field. Then any derivation of K is integrable.*

Proof. Put $k =$ the prime field in K in the theorem.

LEMMA 4. *Let A be a ring of characteristic p, and D be a derivation of A with $D^p = 0$. Put $A_0 = \{a \in A \mid Da = 0\}$. If $x \in A$ satisfies $Dx = 1$, then A is a free A_0-module with $1, x, x^2, \cdots, x^{p-1}$ as a basis.*

Proof. Put $A_i = \{a \in A \mid D^{i+1}a = 0\}$ for $0 \leqslant i < p$. By the assumption $D^p = 0$ we have $A_{p-1} = A$. We will prove

$$A_i = A_0 + A_0 x + \cdots + A_0 x^i$$

by induction on i. For $i = 0$ there is nothing to prove. Let $D^{i+1}a = 0$. Then $D^i a \in A_0$, and if we put $b = a - (i!)^{-1} x^i D^i a$, *then* $D^i b = 0$, i.e. $b \in A_{i-1} = A_0 + A_0 x + \cdots + A_0 x^{i-1}$. Thus $a \in A_0 + A_0 x + \cdots + A_0 x^i$, as wanted. The linear independence of $1, x, \cdots, x^{p-1}$ over A_0 is obvious.

THEOREM 7. *Let K be a separable extension field of a field k of characteristic p. Let $D \in \mathrm{Der}_k(K)$. Then D is strongly integrable over k iff $D^p = 0$.*

Proof. We have already seen the necessity. To prove the sufficiency, we may assume $D \neq 0$, $D^p = 0$. Take $y \in K$ with $Dy \neq 0$. Then there exists a positive integer $i < p$ such that $D^i y \neq 0$, $D^{i+1} y = 0$. Put $x = D^{i-1}y/D^i y$. Then $Dx = 1$. Therefore, putting $K_0 = \{a \in K \mid Da = 0\}$ we have $K = K_0(x)$ and $[K : K_0] = p$ by Lemma 4. The separability of K/k implies that K^p and k are linearly disjoint over k^p. Suppose $x^p \in K_0^p k$. Then we can write $x^p = \sum_{i=1}^r y_i^p c_i$, where $y_i \in K_0$, $c_i \in k$ and $y_1^p, \cdots, y_r^p$ are linearly independent over k^p. Then $y_1, \cdots, y_r$ are linearly independent over k, and since $x \notin K_0$ and $k \subset K_0$ we see that $x, y_1, \cdots, y_r$ are also linearly independent over k. Therefore $x^p, y_1^p, \cdots, y_r^p$ must be linearly independent over k^p, hence over k by the linear disjointness. But this contradicts our assumption $x^p = \sum y_i^p c_i$. Therefore $x^p \notin K_0^p k$, and so there exists a p-basis B_0 of K_0/k containing x^p as a member. Put

$$B = (B_0 - \{x^p\}) \cup \{x\}.$$

Then, putting $y = x^p$ and $I = (X^p - y)K_0[X]$, we have $K = K_0[X]/I$. The exact sequence

$$I/I^2 \longrightarrow \Omega_{K_0[X]/k} \otimes K = (\Omega_{K_0/k} \otimes K) \oplus K dX \longrightarrow \Omega_{K/k} \longrightarrow 0$$

shows

$$\Omega_{K/k} \simeq ((\Omega_{K_0/k} \otimes_{K_0} K)/Kdy) \oplus Kdx .$$

This means that B is a p-basis of K/k. Put $k' = k(B_0 - \{x^p\})$. Then x is transendental over k' (cf. [10, Th. 1]), hence we can define a homomorphism of k'-algebras

$$E_t : k'(x) \longrightarrow k'(x)[[t]]$$

by $E_t(x) = x + t$. Since K is formally etale over $k'(x) = k(B)$, it follows from the diagram

$$\begin{array}{ccccccccc} k'(x) & \multicolumn{7}{c}{\longrightarrow} & K \\ \downarrow & & & & & & & & \downarrow{\scriptstyle id} \\ k'(x)[[t]] & \to & K[[t]] & \to \cdots \to & K[[t]]/(t^2) & \to & K[[t]]/(t) & = & K \end{array}$$

that E_t can be uniquely extended to a homomorphism of k'-algebras

$$E_t : K \longrightarrow K[[t]] .$$

Consider the diagram

$$\begin{array}{ccc} K & \xrightarrow{E_t} & K[[t]] \\ {\scriptstyle E_{t+u}}\downarrow & & \downarrow{\scriptstyle E_u} \\ K[[t+u]] & \xrightarrow{i} & K[[t, u]] . \end{array}$$

We have $E_u E_t(a) \equiv a \equiv E_{t+u}(a) \bmod (t, u)$ for all $a \in K$ and $E_u \circ E_t = i \circ E_{t+u}$ on $k'(x)$. Hence the diagram commutes by the formal etaleness of $K/k'(x)$. Therefore E_t determines an iterative differentiation $\underline{D} = (1, D_1, D_2, \cdots)$ of K over k' such that $D_1(x) = 1 = D(x)$, $D_i(x) = 0$ $(i > 1)$. Since $D_1(\alpha) = 0 = D(\alpha)$ for $\alpha \in K^p k' = K_0$, we have $D_1 = D$. Q.E.D.

Resuming our general discussion at the beginning of this section, we put $A_n = A[t]/(t^{n+1})$ and consider the extension of k-algebras

$$0 \longrightarrow N \longrightarrow A_n \xrightarrow{\pi} A_{n-1} \longrightarrow 0 , \tag{3.1}$$

where $N = At^n$ is an ideal of square zero in A_n and $N \simeq A$ as A-module. The pull-back of (3.1) by $\phi_{n-1} : A \to A_{n-1}$ is the extension

$$0 \longrightarrow A \longrightarrow B \longrightarrow A \longrightarrow 0 \tag{3.2}$$

where B is the fibre product of A and A_n over A_{n-1}:

$$B = \{(\alpha, a) \in A_n \times A \,|\, \pi(\alpha) = \phi_{n-1}(a)\} . \tag{3.3}$$

The extension (3.2) is trivial if and only if ϕ_{n-1} is liftable to $A \to A_n$. Thus the obstruction to lifting ϕ_{n-1} is the cohomology class represented by (3.2) in the group $H^1(k, A, A)$ of M. André. (Cf. [1] Chap. XVI. It coincides with the group $\text{Exalcom}_k(A, A)$ of EGA.) Therefore we have

THEOREM 8. *Let k be a ring and A be a k-algebra. If*

$$H^1(k, A, A) = 0\,,$$

then every derivation D of A over k is integrable over k.

Remark 7. As a matter of fact the extensions (3.1), (3.2) are Hochschild extensions, and so the obstruction class lies in the subgroup $H_k^2(A, A)^s$ of $\text{Exalcom}_k(A, A)$, cf. [5] p. 65. But we will not discuss this group here.

We will apply Th. 8 to regular local rings of characteristic p. Let (A, m, K) be a regular local ring, and k be a field of characteristic p contained in A. If the residue field K is separable over k then A is formally smooth (with respect to the m-adic topology) over k, but not conversely.

Formal smoothness is equivalent to $H^1(k, A, K) = 0$, and then $H^1(k, A, M) = 0$ for all A-modules M which satisfy $m^\nu M = 0$ for some ν. Smoothness is equivalent to $H^1(k, A, M) = 0$ for all A-modules M. ([1] p. 223 Prop. 17, p. 222 Def. 14.) Also the following lemma is known.

LEMMA 5. *Let (A, m, K) be a noetherian local ring containing a field k. Assume that A is formally smooth* (*with respect to the maximal ideal*) *over k. Then*:

i) *for any prime ideal P of A the local ring A_P is formally smooth over k,*

ii) *$H_i(k, A, M) = 0$ for all A-modules M and for all $i > 0$,*

iii) *$H_0(k, A, A) = \Omega_{A/k}$ is A-flat,*

iv) *$H^i(k, A, M) = \text{Ext}_A^i(H_0(k, A, A), M)$ for all A-modules M and for all $i \geqslant 0$.*

Proof. i) Formal smoothness over k is equivalent to geometric regularity over k([5] (22.5.8), [11] p. 279 Th. 93). If k' is a finite extension field of k, then $A_P \otimes_k k'$ is a localization of $A \otimes_k k'$. Therefore it is regular.

ii) follows from i) and [1] p. 331 Th. 30.

iii) and iv): By [1] p. 41 Lemma 19, $H_i(k, A, A) = 0$ $(i > 0)$ implies

$$H_i(k, A, M) = \text{Tor}_i^A(H_0(k, A, A), M), \quad H^i(k, A, M) = \text{Ext}_A^i(H_0(k, A, A), M)$$

for all $i \geqslant 0$. The first equation and ii) imply that $H_0(k, A, A)$ is A-flat.

THEOREM 9. *Let k be a field and A be a noetherian local ring containing k. Assume that A is formally smooth over k and that $\Omega_{A/k}$ is a finite A-module. Then A is smooth over k. Consequently, we have*

$$\mathrm{Der}_k(A) = \mathrm{Ider}_k(A).$$

Proof. The module of differentials $\Omega_{A/k}$ is finite by assumption and flat by Lemma 5. Hence it is free, and so $H^1(k, A, M) = \mathrm{Ext}^1_A(\Omega_{A/k}, M) = 0$ for every A-module M. Therefore A is smooth over k.

Remark 8. The finiteness of $\Omega_{A/k}$ holds in each of the following cases:

1) A is a localization of a finitely generated k-algebra;

2) $\mathrm{char}(k) = p$ and A is finite over $k[A^p]$.

The second case includes in particular $k[[X_1, \cdots, X_n]]$ with $[k : k^p]$ finite.

THEOREM 10. *If A is a complete local ring formally smooth over a subfield k, then $H^1(k, A, M) = 0$ for all finite A-module M. Consequently, we have*

$$\mathrm{Der}_k(A) = \mathrm{Ider}_k(A).$$

Proof. Consider an extension of k-algebras

$$0 \longrightarrow N \longrightarrow B \xrightarrow{\alpha} A \longrightarrow 0 \tag{3.4}$$

where N is a finite A-module. Let m denote the maximal ideal of A. The extension $0 \to N/mN \to B/mN \xrightarrow{\alpha_1} A \to 0$ splits because N/mN is an A/m-module. Therefore there exists a k-algebra homomorphism $\phi_1 : A \to B/mN$ such that $\alpha_1 \circ \phi_1 =$ identity. Using formal smoothness we can lift ϕ_1 to $\phi_2, \phi_3, \cdots$, where $\phi_i : A \to B/m^iN$, successively, because the kernel of the natural map $B/m^{i+1}N \to B/m^iN$ is an A/m-module. Since N is a finite A-module, it is m-adically complete and separated. It follows easily that B is canonically isomorphic to $\varprojlim B/m^iN$. Therefore we obtain a k-algebra homomorphism $\phi : A \to B$ by $\phi = \varprojlim \phi_i$. Since $\alpha = \alpha_1 \circ p_1$ (where p_1 is the natural map $B \to B/mN$) and $p_1 \circ \phi = \phi_1$, we get $\alpha \circ \phi = \alpha_1 \circ p_1 \circ \phi = \alpha_1 \circ \phi_1 =$ identity. Therefore every extension of A by N splits, or equivalently, $H^1(k, A, N) = 0$. Q.E.D.

The author does not know whether $H^1(k, A, A)$ is zero for every formally smooth local k-algebra A, nor whether $H^1(k, A, A) = 0$ for a local

k-algebra A (essentially of finite type, say) implies that A is regular. Of course the equality $\mathrm{Der}_k(A) = \mathrm{Ider}_k(A)$ may happen even if $H^1(k, A, A) \neq 0$. But anyway normality of a local ring is not enough to guarantee the integrability of all derivations, as we see in the following example.

EXAMPLE 6. Let k be a field of characteristic 2 and consider

$$A = k[x, y, z]_{(x,y,z)}\,, \qquad xy = z^2\,.$$

This is a local ring of dimension 2, and since it is a complete intersection and has an isolated singular point, it is normal. The derivations $\partial/\partial Z$ and $X\partial/\partial X + Y\partial/\partial Y$ of $k[X, Y, Z]$ induce derivations D_1, D_2 of A. Suppose D_1 is integrable. Then there exist power series

$$E_t(x) = x + t^2\xi_2 + \cdots,\ E_t(y) = y + t^2\eta_2 + \cdots,\ E_t(z) = z + t + t^2\zeta_2 + \cdots$$

($\xi_i, \eta_i, \zeta_i \in A$) such that

$$(x + t^2\xi_2 + \cdots)(y + t^2\eta_2 + \cdots) = (z + t + t^2\zeta_2 + \cdots)^2\,.$$

Then $x\eta_2 + y\xi_2 = 1$, hence $1 \in m_A$, contradiction. Therefore D_1 is not integrable. One can show that $xD_1, yD_1, zD_1 + D_2 \in \mathrm{Ider}_k(A)$. The A-module $\mathrm{Der}_k(A)$ is a free module generated by D_1, D_2.

We recall the famous Zariski-Lipman conjecture: Let A be the local ring of a point of a variety over a field k of characteristic zero. *If* $\mathrm{Der}_k(A)$ *is free then* A *is regular.* Lipman [8] proved that A is normal. The conjecture has been proved only in the case of a hypersurface by Scheja-Storch [17]. The above example shows that the conjecture does not hold in characteristic p. But if we modify the conjecture as follows, then it may be true:

CONJECTURE. If k is perfect, if $\mathrm{Der}_k(A) = \mathrm{Ider}_k(A)$ and if this module is A-free, then A is regular.

§ 4. Finitely generated k-algebras

Let k be a perfect field and let

$$A = k[x_1, \cdots, x_n] = k[X_1, \cdots, X_n]/P\,, \qquad P = (f_1, \cdots, f_s)$$

be an integral domain of dimension $n - r$. Let J be the Jacobian ideal of A, i.e. the ideal generated by the $r \times r$ minors of the Jacobian matrix $(\partial f/\partial x)$. (Cf. § 2.) We have seen that $D \in \mathrm{Ider}_k(A)$ implies $D(J) \subset J$. The converse is false, but we have the following theorem.

THEOREM 11. *If* $D \in \mathrm{Der}_k(A)$ *and* $D(A) \subset J$, *then* $D \in \mathrm{Ider}_k(A)$.

COROLLARY 1. *If* Δ *is a non-zero* $r \times r$ *minor of* $(\partial f/\partial x)$, *then*

$$\Delta\, \mathrm{Der}_k(A) \subset \mathrm{Ider}_k(A)\,.$$

Consequently, we have

$$\mathrm{rank}\ \mathrm{Der}_k(A) = \mathrm{rank}\ \mathrm{Ider}_k(A)\,,$$

where rank M for an A-module M means the maximal number of linearly independent elements in M.

Proof of Th. 11. Put $D(x_i) = \xi_{1i}\ (\in J)$, $\xi_1 = (\xi_{11}, \cdots, \xi_{1n})$. Then we have

$$f_\alpha(x + t\xi_1) \equiv 0 \bmod t^2\,, \qquad 1 \leqslant \alpha \leqslant s\,.$$

By induction, suppose that, for some $\nu > 1$, we have found $\xi_{\mu j} \in J$ $(1 \leqslant \mu < \nu$, $1 \leqslant j \leqslant n)$ such that

$$f_\alpha\Big(x + \sum_{\mu=1}^{\nu-1} t^\mu \xi_\mu\Big) \equiv 0 \bmod t^\nu\,, \qquad 1 \leqslant \alpha \leqslant s\,.$$

Then we can write

$$f_\alpha\Big(x + \sum_{1}^{\nu-1} t^\mu \xi_\mu\Big) \equiv t^\nu F_\alpha(x) \bmod t^{\nu+1}\,, \qquad 1 \leqslant \alpha \leqslant s\,.$$

Then the $F_\alpha(x)$'s are linear combinations, with coefficients in A, of monomials of the form $\xi_{\mu_1 j_1}\xi_{\mu_2 j_2}\cdots\xi_{\mu_q j_q}$, $\mu_1 + \mu_2 + \cdots + \mu_q = \nu$. Since $\mu_i < \nu$ we have $q \geqslant 2$. Therefore $F_\alpha(x) \in J^2$. If $\xi_{\nu 1}, \xi_{\nu 2}, \cdots, \xi_{\nu n}$ are elements of A we have

$$f_\alpha\Big(x + \sum_{1}^{\nu} t^\mu \xi_\mu\Big) \equiv t^\nu\Big[F_\alpha(x) + \sum_{j=1}^{n} (\partial f_\alpha/\partial x_j)\xi_{\nu j}\Big] \bmod t^{\nu+1}\,, \quad 1 \leqslant \alpha \leqslant s\,.$$

Therefore, if we can find $\xi_{\nu j} \in J$ $(1 \leqslant j \leqslant n)$ which satisfy

$$F_\alpha(x) + \sum_{j} (\partial f_\alpha/\partial x_j)\xi_{\nu j} = 0 \quad (1 \leqslant \alpha \leqslant s) \tag{4.1}$$

then we can continue the induction and we are done.

Let $\Delta_1, \cdots, \Delta_a$ be the non-zero $r \times r$ minors of the Jacobian matrix $(\partial f/\partial x)$. We may suppose that the first r rows of the matrix $(\partial f/\partial x)$ are linearly independent. Put $k[X_1, \cdots, X_n] = R$. The local ring R_P is regular of dimension r, and the map $\psi : R_P \to K^n$ (K = quotient field of A) defined by

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

$$\psi(f) = (\partial f/\partial x_1, \cdots, \partial f/\partial x_n)$$

maps P^2R_P to zero. Therefore $f_1, \cdots, f_r$ are linearly independent modulo P^2R_P, hence we have $PR_P = (f_1, \cdots, f_r)R_P$. Since $F_\alpha(x) \in J^2$ for all α, we can write

$$(4.2) \qquad F_i(x) = \sum_\lambda \Delta_\lambda h_{\lambda i}(x), \qquad h_{\lambda i} \in J \ (1 \leqslant i \leqslant r).$$

Let $f_{r+q} = \sum_{i=1}^r a_{qi} f_i$, $a_{qi}(X) \in R_P$. Then we have

$$(4.3) \qquad \partial f_{r+q}/\partial x_j = \sum a_{qi}(x) \partial f_i/\partial x_j .$$

Moreover, we have $F_{r+q}(x) = \sum_i a_{qi}(x) F_i(x)$ because $f_i(x + \sum_1^{\nu-1} t^\mu \xi_\mu) \equiv t^\nu F_i(x)$ mod $t^{\nu+1}$. Thus, putting

$$(4.4) \qquad h_{\lambda, r+q}(x) = \sum_1^r a_{qi}(x) h_{\lambda i}(x)$$

we see that (4.2) holds for $i = 1, \cdots, s$.

Now fix an index λ and consider the simultaneous equations

$$(4.5) \qquad \Delta_\lambda h_{\lambda i}(x) + \sum_{j=1}^n (\partial f_\alpha/\partial x_j)\xi_j^{(\lambda)} = 0, \qquad 1 \leqslant i \leqslant s .$$

Let $\Gamma = \{i_1, \cdots, i_r\}$ denote the set of indices of the rows of $(\partial f/\partial x)$ which appear in Δ_λ. These rows are linearly independent, and by (4.3) and (4.4) we have

$$\operatorname{rank}\begin{pmatrix} \partial f_1/\partial x_1 \cdots \partial f_1/\partial x_n & h_{\lambda 1} \\ \vdots \qquad\qquad \vdots & \\ \partial f_s/\partial x_1 \cdots \partial f_s/\partial x_n & h_{\lambda s} \end{pmatrix} = \operatorname{rank}(\partial f/\partial x) = r .$$

Therefore, to solve (4.4) we have only to solve them for $i \in \Gamma$. We put $\xi_j^{(\lambda)} = 0$ if the j-th column of $(\partial f/\partial x)$ does not appear in Δ_λ, and we find the other $\xi_j^{(\lambda)}$ by Cramer's rule. Since $h_{\lambda i}(x) \in J$ we have $\xi_j^{(\lambda)} \in J$. Then $\xi_{\lambda j} := \sum_\lambda \xi_j^{(\lambda)}$ satisfy (4.1). Q.E.D.

COROLLARY 2. *Let k, A, J be as above and let S be a multiplicative subset of A. Put $B = S^{-1}A$. Then $S^{-1}J = JB$ is the first non-zero Fitting ideal of $\Omega_{B/k}$, and if $D \in \mathrm{Der}_k(B)$ maps B into JB then $D \in \mathrm{Ider}_k(B)$.*

Proof. There exists $a \in S$ such that $aD(A) \in J$. Then $aD \in \mathrm{Ider}_k(A)$, hence $D \in \mathrm{Ider}_k(B)$.

COROLLARY 3. *Theorem 11 remains true if we replace the polynomial*

https://doi.org/10.1017/S002776300002002X Published online by Cambridge University Press

ring $k[X_1, \cdots, X_n]$ *by the formal power series ring* $k[[X_1, \cdots, X_n]]$.

Proof. The above proof of Th. 11 applies to this case as well.

Under the assumptions of Th. 11 we have rank $\mathrm{Ider}_k(A) = \mathrm{rank}\,\mathrm{Der}_k(A) = n - r = \dim A$. More generally, if (A, m) is a noetherian local ring and k is a quasi-coefficient field of A (i.e. k is a subfield of A such that A/m is formally etale over k), then for each $P \in \mathrm{Ass}(\hat{A})$ we have rank $\mathrm{Ider}_k(A) \leqslant \dim \hat{A}/P$ (Mollinelli [12]), whereas rank $\mathrm{Der}_k(A)$ can be bigger than $\dim A$. In the case when k is imperfect Cor. 1 is false in general, as the following example shows.

EXAMPLE 7. Let k be an imperfect field of characteristic $p > 2$, and let $a, b \in k$ be such that $[k^p(a, b) : k^p] = p^2$. Put $A = k[x, y] = k[X, Y]/(X^{2p} + aX^p + bY^p)$. The partial derivations of $k[X, Y]$ induce derivations D_x, D_y of A over k, and we have $\mathrm{Der}_k(A) = AD_x + AD_y$. Suppose $uD_x + vD_y$ is integrable, where $u = f(x, y)$ and $v = g(x, y)$. Considering the coefficient of t^p in the relation $(x + tu + \cdots)^{2p} + a(x + tu + \cdots)^p + b(y + tv + \cdots)^p = 0$ we get

$$(*) \qquad 2x^p u^p + au^p + bv^p = 0\,.$$

Therefore $2X^p f(X, Y)^p + af(X, Y)^p + bg(X, Y)^p = (X^{2p} + aX^p + bY^p)H(X, Y)$ for some $H(X, Y) \in k[X, Y]$. Applying derivations D_a, D_b of k such that $D_a(a) = 1$, $D_a(b) = 0$, $D_b(a) = 0$, $D_b(b) = 1$ to the last relation and substituting x, y for X, Y we get

$$u^p = x^p w\,, \quad v^p = y^p w\,, \quad w = H(x, y)\,.$$

Substituting them into $(*)$ we have $w = 0$. Hence $u = v = 0$. Thus $\mathrm{Ider}_k(A) = 0$.

REFERENCES

[1] André, M., Homologie des algèbres commutatives, Springer, 1974.

[2] ——, Méthodes simpliciale en Algèbre Homologique et Algèbre Commutative, Springer Lecture Notes in Math., **32** (1967).

[3] Avramov, L. L., Flat morphisms of complete intersections, Soviet Math. Dokl., **16** (1975), 1413–1417.

[4] Brown, W. C., On the imbedding of derivations of finite rank into derivations of infinite rank, Osaka J. Math., **15** (1978), 381–389.

[5] Grothendieck, A., Éléments de Géométrie Algébrique, IV-1, Publ. I.H.E.S., no. 20, 1964.

[6] ——, ibid., IV-2, Publ. I.H.E.S., no. 24, 1965.

[7] Hasse, H. and Schmidt, F. K., Noch eine Begründung der Theorie der höheren

Differentialquotienten in einem algebraischen Funktionenkorper einer Unbestimmten, J. reine u. angew. Math., **117** (1937).
[8] Lipman, J., Free derivation modules on algebraic varieties, Amer. J. Math., **87** (1965), 874–898.
[9] ——, On the Jacobian ideal of the module of differentials, Proc. Amer. Math. Soc., **21** (1969), 422–426.
[10] Matsumura, H., Quasi-coefficient rings of a local ring, Nagoya Math. J., **68** (1977), 123–130.
[11] ——, Commutative Algebra, 2nd Ed. Benjamin, 1980.
[12] Molinelli, S., Sul modulo delle derivazioni integrabili in caratteristica positiva, Ann. Mat. Pura Appl., **121** (1979), 25–38.
[13] Nakai, Y., High order derivations I, Osaka J. Math., **7** (1970), 1–27.
[14] ——, On locally finite iterative higher derivations, ibid., **15** (1978), 655–662.
[15] Northcott, D. G., Finite Free Resolutions, Camb. Tracts in Math., **71**, Camb. Univ. Press, 1976.
[16] Restuccia, G., Sul rango del modulo delle derivazioni di un anello in caratteristica diseguale, Rend. Sem. Mat. Univ. Politecn. Torino, **36** (1977–78), 449–462.
[17] Scheja-Storch, Differentielle Eigenschaften der Lokalisierungen analytischer Algebren, Math. Ann., **197** (1972), 137–170.
[18] Seidenberg, A., Derivations and integral closure, Pacific J. Math., **16** (1966), 167–173.
[19] ——, Differential ideals in rings of finitely generated type, Amer. J. Math., **89** (1967), 22–42.
[20] ——, Differential ideals in complete local rings, ibid., **95** (1973), 52–58.
[21] Watanabe, K., Ishikawa, T., Tachibana, S. and Otsuka, K., On tensor products of Gorenstein rings, J. Math. Kyoto Univ., **9** (1969), 413–423.
[22] Yamauchi, N., On an algebra over a field with universal finite module of differentials, Nagoya Math. J., **83** (1981), 107–121.
[AG] Hartshorne, R., Algebraic Geometry, Springer, 1977.

Department of Mathematics
Nagoya University