

KÄHLER DIFFERENTIALS AND DIFFERENTIAL ALGEBRA IN ARBITRARY CHARACTERISTIC

BY
 JOSEPH JOHNSON

ABSTRACT. Let L and K be differential fields with L an extension of K . It is shown how the module of Kähler differentials $\Omega_{L/K}^1$ can be used to "linearize" properties of a differential field extension L/K . This is done without restriction on the characteristic p and yields a theory which for $p \neq 0$ is no harder than the case $p = 0$. As an application a new proof of the Ritt basis theorem is given.

Introduction. Let k be a field and A a finitely generated algebra over k . One can study the properties of A by taking a surjective homomorphism of k -algebras $\phi: k[y_1, \dots, y_n] \rightarrow A$ where y_1, \dots, y_n are indeterminates over k and then analyzing the kernel I of ϕ . This is for instance done in [1] for the case of A an integral domain. There one assumes that ϕ is chosen so that $\phi(y_1), \dots, \phi(y_p)$ is a transcendence basis for the quotient field of A over k . One then chooses nonzero F_j in $k[y_1, \dots, y_j] \cap I$ and d_j in \mathbb{N} for $p < j \leq n$ such that

- (1) d_j is the degree of F_j in y_j ,
- (2) $\text{Degree}_{y_i} F_j < d_i$ if $p < i < j$,
- (3) d_j is as small as possible.

One then observes that if S_j is defined by $F_j = S_j y_j^{d_j} + \text{terms of degree less than } d_j \text{ in } y_j$ and if $S = S_{p+1} \cdots S_n$, then $S \notin I$ and $k[y_1, \dots, y_n, 1/S]I$ is generated as an ideal of $k[y_1, \dots, y_n, 1/S]$ by F_{p+1}, \dots, F_n .

The subject of this paper is the study of a finitely generated differential algebra over a differential field. This matter has of course been considered before. However to prove anything beyond the most trivial statements one has customarily generalized the above-mentioned procedure, and this has led ultimately to a fairly complicated theory. Such theory is more complicated in nonzero characteristic than in characteristic zero. The purpose of this paper is to show that we may achieve our results in another way, and so that procedure is not followed here. Instead differential algebras are studied by reducing the number of derivation operators involved one at a time. To illustrate this method I have included a new proof of Seidenberg's version of the Ritt-Raudenbusch basis theorem.

The primary tool used in reducing the number of derivation operators is the theory of Kähler differentials, a method for "linearizing" much of the ring theory

Received by the editors June 14, 1972 and, in revised form, December 15, 1972.

AMS (MOS) subject classifications (1970). Primary 12H05.

Key words and phrases. Differential algebra, Kähler differentials, differential ring, differential module, Ritt basis theorem, nonzero characteristic.

Copyright © 1974, American Mathematical Society

involved. In [2] some uses for Kähler differentials in characteristic zero were shown. The subject matter of this paper is quite different. For a long time I did not know if Kähler differentials would be an effective tool for differential algebra in nonzero characteristic. The discovery that such methods give elegant (and slightly easier) proofs in characteristic $p > 0$ led to the writing of this paper. The fact which appears to be crucial in achieving this is the lemma of §2.

The conventions of §0 of [3] are followed in this paper.

1. Reduction of the number of derivation operators. The following theorem is the starting point for the treatment of differential algebras given here. Its proof and the meaning of "almost all choices" is given in [2, §3]. As in [2], $\Delta_{(m)} = \Delta - \{\delta_m\}$.

Theorem 1. *Let K be a differential field, k a differential subfield of K with infinitely many elements. Let M be a finitely generated differential vector space over K of differential dimension zero. Then for almost all choices of Δ , M is finitely generated as a $\Delta_{(m)}$ -differential vector space over K .*

The notational conventions of §3 of [2] will be used from here on.

2. Kähler differentials. The theory of Kähler differentials will be used to apply Theorem 1 to differential rings (see Theorem 2 of §3). The facts from that theory needed here are summarized in this section. Also a lemma is proved which is crucial to this paper.

Let A be a commutative ring and B a commutative A -algebra. If M is any B -module, an A -derivation of B into M is any A -linear map D of B into M such that for b and b' in B we have $D(bb') = bD(b') + b'D(b)$. Write $\text{Der}_A(B, M)$ for the set of A derivations of B into M . There exists a B -module $\Omega_{B/A}$ and an A -derivation $d_{B/A}$ of B into $\Omega_{B/A}$ which is universal in the following sense:

If M is any B -module and if D is an A -derivation of B into M , then there exists a unique B -linear map p of $\Omega_{B/A}$ into M such that $p \circ d_{B/A} = D$.

The construction of $\Omega_{B/A}$ is given in §1 of [3] (or in [5]). Often d will be written for $d_{B/A}$. If E is a set of generators for B as an A -algebra, $d(E)$ generates the B -module $\Omega_{B/A}$. If f is a homomorphism of A into a ring A' and B' an A' algebra (hence also an A -algebra via f) and if g is an A -algebra homomorphism of B into B' , then there exists a unique B -module map $\Omega_{g/f}$ of $\Omega_{B/A}$ into $\Omega_{B'/A'}$ such that $\Omega_{g/f} \circ d_{B/A} = d_{B'/A'} \circ g$. When g is surjective, so is $\Omega_{g/f}$. We call $\Omega_{B/A}$ the module of Kähler differentials (of B over A).

The following lemma characterizes field extensions $K \supset L$ for which $\Omega_{K/L} = 0$.

Lemma. *Let K be a field, L a subfield of K and p the characteristic of K and L . Then $\Omega_{K/L} = 0$ is equivalent to*

- (1) $p = 0$ and K is an algebraic extension of L , or
- (2) $p > 0$ and $K = L \cdot K^p$.

For $p = 0$ this is well known. Assume $p > 0$. If $K = L \cdot K^p$, $d_{K/L}(K^p) = 0$ and generates $\Omega_{K/L}$, so $\Omega_{K/L} = 0$. Suppose now that $K \neq L \cdot K^p$. Let $x \in K - L \cdot K^p$ and let L' be a maximal subfield of K such that $x \notin L' \supset L \cdot K^p$. If $y \in K - L'(x)$, then $x \in L'(y)$ and $p = [L'(y): L'] > [L'(x): L'] = p$, a contradiction. Thus $K = L'(x)$. There exists a unique L' -derivation D of K into K such that $D(x) = 1$. Hence $\Omega_{K/L'} \neq 0$. Also since $\Omega_{K/L}$ maps onto $\Omega_{K/L'}$, $\Omega_{K/L} \neq 0$. This proves the lemma.

Finally I want to recall (§1 of [3]) that if A is a differential ring and B a differential algebra over A , then $\Omega_{B/A}$ has a unique structure of differential module for which $\delta(d(b)) = d(\delta(b))$ ($d = d_{B/A}$) for every $\delta \in \Delta$ and b in B . It is easy to see that if E generates B as a differential A -algebra, then $d(E)$ generates $\Omega_{B/A}$ as a differential B -module.

3. Applications to separable differential field extensions. If k is a differential field and K is a differential field extension of k , then the extension will be called *separable* if as a (nondifferential) field extension K is separable over k . The following theorem is the basis for the treatment of separable differential fields which is to be given here. As it involves no separability assumption it might be useful in studying the nonseparable case as well.

Theorem 2. *Let Δ and Δ' be finite sets and K a $\Delta \cup \Delta'$ -differential field extension of k . Suppose that as a Δ -differential field extension of k , K is finitely generated and that as a Δ' -differential vector space over K , $\Omega_{K/k}$ is finitely generated. Then K is finitely generated as a Δ' -differential field extension of k .*

Note we do not assume that Δ and Δ' are disjoint. For convenience the standard notations of differential algebra will be used with a subscript Δ or Δ' appropriately placed to indicate which set of derivation operators is being considered. For instance $k\langle y_1, \dots, y_n \rangle_\Delta$ will denote the smallest Δ -differential overfield of k containing y_1, \dots, y_n when these lie in a given Δ -differential overfield of k .

Theorem 2 will first be proved for characteristic $p \neq 0$. Choose y_1, \dots, y_n in K so that dy_1, \dots, dy_n generate $\Omega_{K/k}$ as a Δ' -differential vector space over K and so that $K = k\langle y_1, \dots, y_n \rangle_\Delta$. Let L be the subfield $k \cdot K^p$ of K and let $K_1 = L\langle y_1, \dots, y_n \rangle_\Delta$. Now the $d_{K/k}y$ have zero image under the (surjective) map of $\Omega_{K/k}$ to Ω_{K/K_1} , so $\Omega_{K/K_1} = 0$. As $K_1 \supset K^p$, by the lemma of §2, $K = K_1$. Since the elements δy_i for $\delta \in \Delta$ and $i = 1, \dots, n$ comprise a finite subset of $K = K_1$, they belong to a subfield $H = k(c_1, \dots, c_h)\langle y_1, \dots, y_n \rangle_\Delta$ for appropriately chosen elements c_1, \dots, c_h of K^p . Clearly H as a Δ' -differential field extension of k is

finitely generated. Since y_1, \dots, y_n are in H , it will suffice to show that H is a Δ -differential subfield of K . This is immediate because if $\delta \in \Delta$, $\theta \in \Theta_{\Delta}$ and $i = 1, \dots, n$ we have $\delta(\theta y_i) = \theta(\delta y_i) \in H$. This completes the proof of Theorem 2 for $p \neq 0$.

Suppose now that $p = 0$. Choose y_1, \dots, y_n as before and let

$$K_1 = k\langle y_1, \dots, y_n \rangle_{\Delta}.$$

Then $\Omega_{K/K_1} = 0$, so K is an algebraic extension of K_1 . Let c_1, \dots, c_h be the δy_i for $\delta \in \Delta$, $i = 1, \dots, n$, and let $H = K_1\langle c_1, \dots, c_h \rangle_{\Delta}$. Given any c_j , let $F(X)$ be a polynomial with coefficients in K_1 such that $F(c_j) = 0$ and $F'(c_j) \neq 0$ where $F' = dF/dX$. Then if $\delta \in \Delta$, $F^{\delta}(c_j) + F'(c_j)\delta c_j = \delta(F(c_j)) = 0$ where F^{δ} is the result of applying δ to the coefficients of F . Now $\delta(K_1) \subset H$ since if $\theta \in \Theta_{\Delta}$, $\delta(\theta y_i) = \theta(\delta y_i) \in \theta(H) \subset H$. Hence $\delta c_j = -F^{\delta}(c_j)/F'(c_j)$ is in H . It follows that if z is any of $y_1, \dots, y_n, c_1, \dots, c_h$, then $\delta(\theta z) \in H$ for every $\theta \in \Theta_{\Delta}$ and H is a Δ -differential subfield of K . As H contains k and y_1, \dots, y_n we have $H = K$ proving Theorem 2.

In using Theorem 2 for studying separable differential field extensions the following theorem of Seidenberg [4] plays a crucial role. For a proof one may consult [4] or [6].

Theorem 3 (Seidenberg). *Let K be a separable differential field extension of k and suppose that $\text{Card } \Delta > 0$. Then if B is a subset of K differentially algebraically independent over k , K is a separable extension of $k\langle B \rangle$.*

Proposition. *Let $m > 0$ and let K be a differential field extension of k which is separable over k . Write $d = d_{K/k}$, and let $y_1, \dots, y_n \in K$. Then dy_1, \dots, dy_n are differentially linearly independent over K if and only if y_1, \dots, y_n are differentially algebraically independent over k .*

Assume first that dy_1, \dots, dy_n are differentially linearly independent over K , and let us show that then y_1, \dots, y_n are differentially algebraically independent over k . Suppose to the contrary that there exists a nontrivial relation $F(y_1, \dots, y_n) = 0$ where F is a differential polynomial in the y . Choose such an F of least degree. Then there must exist a derivative u of one of the y_j such that $\partial F / \partial u \neq 0$. Indeed for characteristic $p > 0$ if every partial derivative $\partial F / \partial u = 0$, we may write $F = \sum a_M M^p$ where M runs over a finite set of monomials in $\Theta_{y_1} \cup \dots \cup \Theta_{y_n}$. By taking the p th root of $F(y)$ it follows that the $M(y)$ are dependent over $k^{1/p}$ and hence also over k because of the separability condition. By writing a nontrivial dependence relation $0 = \sum b_M M(y) = G(y)$ where the b are in k we obtain a nonzero differential polynomial G in the y with coefficients from k with $G(y) = 0$ and $\text{degree } G < \text{degree } F$, a contradiction. In characteristic zero an easier argument shows that some $\partial F / \partial u \neq 0$. Thus

$\sum (\partial F / \partial \theta y_j) d(\theta y_j) = 0$ where the sum is over $\Theta \times \{1, \dots, n\}$ is a nontrivial linear dependence relation on the dy contradicting our initial hypothesis.

Conversely assume that y_1, \dots, y_n are differentially algebraically independent over k . Because $m > 0$, K is a separable extension of $k\langle y_1, \dots, y_n \rangle$ by Theorem 3. Hence there exist elements $D_{\theta i}$ of $\text{Der}_k(K, K)$ for $\theta \in \Theta$ and $i = 1, \dots, n$ such that

$$\begin{aligned} D_{\theta i}(\theta' y_j) &= 1 && \text{if } \theta = \theta', i = j, \\ &= 0 && \text{otherwise} \end{aligned}$$

[5, (20.6.3)]. Let $p_{\theta i}$ be the K -linear map of $\Omega_{K/k}$ into K such that $p_{\theta i} \circ d_{K/k} = D_{\theta i}$. A relation $\sum a_{\theta i} \theta dy_i = 0$ with the a in K must be trivial since by applying $p_{\theta i}$ to both sides one obtains $a_{\theta i} = 0$. Hence the dy are differentially linearly independent.

The following is immediate.

Corollary 1. *Let K be a separable differential field extension of k . Then $\text{diff tr deg}_k K = \text{diff dim}_K \Omega_{K/k}$.*

Corollary 2. *Let K be a separable and finitely generated differential field extension of k and suppose that k is infinite. If $\text{diff tr deg}_k K = 0$, then for almost all choices of Δ , K is finitely generated as a $\Delta_{(m)}$ -differential field extension of k .*

Indeed by Corollary 1 and by Theorem 1, $\Omega_{K/k}$ is finitely generated as a $\Delta_{(m)}$ -differential vector space over K for almost all choices of Δ . If we apply Theorem 2 with $\Delta' = \Delta_{(m)}$, Corollary 2 follows immediately.

4. A new proof of the Ritt basis theorem.

Theorem 4. *Let k be a differential field, A a finitely generated differential algebra over k , I a k -separable differential ideal of A . Then I is finitely generated, i.e., there is a finite subset U of I such that I is the smallest k -separable differential ideal which contains U .*

This form of the Ritt basis theorem is due to Seidenberg. Recall that a k -separable ideal of A is an ideal I such that

- (1) $\sqrt{I} = I$,
- (2) $I = A$, or k and $(A/I)^p$ are linearly disjoint over k^p , where p is the characteristic exponent of k .

Use will be made of the following lemma whose proof will be left to the reader. In it if S is any multiplicative set of A and I an ideal of A , $I:S$ denotes the ideal of elements a in A such that Sa intersects I . Note that this is *not* the traditional meaning of $I:S$.

Lemma. (i) *The family of k -separable differential ideals of A is closed under intersection and ascending union. If S is a multiplicatively closed subset of A and if*

I is a k -separable differential ideal of A , then $I:S$ is a k -separable differential ideal of A .

(ii) *If I is a k -separable differential ideal, then I is the intersection of all prime k -separable differential ideals of A which contain I .*

(iii) *If U is a subset of A , let $\{U\}_k$ denote the smallest k -separable differential ideal containing U . Then $\{UV\}_k = \{U\}_k \cap \{V\}_k$.*

The usual arguments show that Theorem 4 is equivalent to the assertion that there does not exist an infinite strictly ascending chain of k -separable differential ideals in A . Assume that the theorem is false for a particular A . By Zorn's lemma if the family of nonfinitely generated k -separable differential ideals is not empty it has a maximal element I . We may write I as an ascending union $I = \bigcup_{p \in P} I_p$ where the I_p are k -separable differential ideals of A none of which is equal to I . Now I must be prime. Indeed let $a, b \in A - I$. Then $\{I_p, a\}_k = \{I, a\}_k$ and $\{I_p, b\}_k = \{I, b\}_k$ for some p in P . Then $ab \notin I$ since otherwise we could by taking p larger assume ab in I_p and we would then have

$$I = \{I, ab\}_k = \{I, a\}_k \cap \{I, b\}_k = \{I_p, a\}_k \cap \{I_p, b\}_k = \{I_p, ab\}_k = I_p$$

which is a contradiction. Hence I is prime as asserted. The next theorem, whose proof follows, will now be used. In it S^∞ is the multiplicative set generated by the element S .

Theorem 5. *Let A be a finitely generated differential algebra over a differential integral domain R and I a prime differential ideal of A such that $I \cap R = (0)$ and such that $\text{qf}(A/I)$ is a separable extension of $\text{qf } R$. Then there is a finitely generated differential ideal $J \subset I$ and S in $A - I$ such that $I = J : S^\infty$.*

Let J and S be as given by Theorem 5. Then there exists a p in P such that $J \subset I_p$ and so then $I = I_p : S^\infty$. On the other hand since $S \notin I$, by the maximality of I , $\{I_p, S\}_k = \{I, S\}_k$ if we redefine p appropriately. Then $I_p = (I_p : S) \cap \{I_p, S\}_k = (I : S) \cap \{I, S\}_k = I$ which is a contradiction.

Let us now prove Theorem 5, first under the assumption that R is infinite. The conclusion of Theorem 5 means that there exists an S in $A - I$ such that $A[1/S]I$ is a finitely generated differential ideal of $A[1/S]$. Let $\bar{x} = x + I$ if x is in A . We may first reduce to the case $\text{diff tr deg}_R A/I = 0$ if we replace R by $R\{y_1, \dots, y_d\}$ where the y are in A and chosen so that $\bar{y}_1, \dots, \bar{y}_d$ is a separating differential transcendence basis for A/I over R . This we can do without loss of generality since neither hypothesis nor conclusion are thereby changed.

The case $m = 0$, which may be done using the method sketched in the introduction or in analogy to the case $m > 0$, is elementary. It will therefore be shown how the theorem follows by induction on m leaving aside the case $m = 0$. It will be shown that if A is replaced by $A[1/S]$ for an appropriate S not in I and I by $A[1/S]I$, then there exists a finitely generated differential ideal $J \subset I$ such

that A/J is finitely generated as a $\Delta_{(m)}$ -differential algebra over R , for an appropriate choice of Δ .

This will be sufficient because one can then apply the case $m - 1$ to obtain that I/J is finitely generated as a $\Delta_{(m)}$ -differential ideal of A/J and hence a fortiori as a Δ -differential ideal of A/J . Then from the exact sequence $0 \rightarrow J \rightarrow I \rightarrow I/J \rightarrow 0$ of differential modules over A one can conclude I is a finitely generated differential ideal of A .

Let K be the quotient field of A/I . By Corollary 2 of §3, for an appropriate choice of Δ , K is finitely generated as a $\Delta_{(m)}$ -differential field extension of the quotient field of R . Let y_1, \dots, y_n be a set of generators for A as a Δ -differential algebra over R . Choose z_1, \dots, z_p in A so that $\bar{z}_1, \dots, \bar{z}_p$ generate the quotient field of A/I as a $\Delta_{(m)}$ -differential field extension of the field of quotients of R . We may assume that the y occur among the z . There exist elements of I of the form $G_i = S\delta_m z_i - F_i$ where S and the F_i are in $R\{z\}_{(m)}$, and $S \notin I$. Replace A by $A[1/S]$ and I by $A[1/S]I$. It will be shown that A/J is finitely generated as a $\Delta_{(m)}$ -differential algebra where $J = [G_1, \dots, G_p]$. Indeed if x is in A , let $\hat{x} = x + J$. Let B be the $\Delta_{(m)}$ -differential subalgebra of A/J generated by $\hat{z}_1, \dots, \hat{z}_p$ and $1/\hat{S}$. Since $\hat{y}_1, \dots, \hat{y}_n$ are in B , once we show $\delta_m(B) \subset B$ it will follow that $B = A/J$ since then clearly B is a Δ -differential R -subalgebra of A/J which contains the \hat{y} . Now as an algebra over R , B is generated by the $\theta\hat{z}$ for θ in $\Theta_{(m)}$. Apply θ to the relation $\delta_m \hat{z}_i = \hat{F}_i/\hat{S}$ and it follows that $\delta_m(\theta\hat{z}_i)$ is in B whenever θ is in $\Theta_{(m)}$. Hence $B = A/J$ is generated as a $\Delta_{(m)}$ -differential algebra by $\hat{z}_1, \dots, \hat{z}_p$ and $1/\hat{S}$. This proves the theorem when R is infinite.

Assume R is finite and let x be an indeterminate constant. Let $A' = A[x]$ and $R' = R[x]$. Theorem 5 applies to the prime differential ideal $I' = A'I$ of A' and so there is a finitely generated differential ideal J' of A' and S' in $A' - I'$ such that $I' = J': S'^\infty$. Without losing anything we may at any point replace J' by the differential ideal of A' generated by J' and a finite subset of I' . Thus by adding to J' the coefficients of a finite generating set of J' we may assume $J' = A'J$ where J is a finitely generated differential of A . Let S be the lowest degree coefficient of S' not in I and let d be its degree. Enlarge J to contain the S'_e for $e < d$, where for any element T' of A' , T'_e is the coefficient of x^e in T' . If $a \in I$, then $S'^N a \in J'$ for some N and $(S'^N)_{Nd} \equiv S^N \pmod{J}$, so $S^N a \in J$. Thus $I = J: S^\infty$. This proves Theorem 5.

It should be noticed that in proving Theorem 5 the following result was established.

Theorem 5'. *Let A be a finitely generated differential algebra over a differential integral domain R such that R contains infinitely many elements. Let I be a prime differential ideal of A such that $I \cap R = 0$ and such that $\text{qf}(A/I)$ is a separable extension of $\text{qf } R$. Then for almost all choices of Δ there exists a finitely generated differential ideal $J \subset I$ and S in $A - I$ such that if $A' = A[1/S]$, then $A'/A'J$ is finitely generated as a $\Delta_{(m)}$ -differential algebra over R .*

BIBLIOGRAPHY

1. Solomon Lefschetz, *Algebraic geometry*, Princeton Univ. Press, Princeton, N.J., 1953, Chap 3, §3. MR 15, 150.
2. Joseph Johnson, *A notion of Krull dimension for differential rings*, Comment. Math. Helv. 44 (1969), 207–216. MR 39 #4127.
3. ———, *Kähler differentials and differential algebra*, Ann. of Math. (2) 89 (1969), 92–98. MR 39 #187.
4. Abraham Seidenberg, *Some basic theorems in partial differential algebra*, Mem. Coll. Sci. Univ. Kyoto Ser. A Math. 31 (1958), 1–8. MR 20 #4099.
5. A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. No. 20 (1964), 259 pp. MR 30 #3885.
6. E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903