Can. J. Math., Vol. XXII, No. 6, 1970, pp. 1224–1237

A DIFFERENCE-DIFFERENTIAL BASIS THEOREM

RICHARD M. COHN

Introduction. Our aim in this paper is to extend to difference-differential rings the beautiful theorem of Kolchin [**5**, Theorem 3] for the differential case. The necessity portion of Kolchin's result is not obtained.

What might well be called the Ritt basis theorem states that if a commutative ring R with identity is finitely generated over a subring R_0, then the ascending chain condition for radical ideals of R_0 implies the ascending chain condition for radical ideals of R. (This is indeed a basis theorem. If we define a basis for a radical ideal A to be a finite set B such that $A = \sqrt{(B)}$, then every radical ideal of a ring R has a basis if and only if the ascending chain condition for radical ideals holds in R.) It is the Ritt basis theorem rather than the Hilbert basis theorem which has appropriate generalizations in differential and difference algebra, where in fact it originated. For differential rings (even difference-differential rings) containing the rational numbers and for difference rings without restriction, this generalization has been known for about thirty years (see [**3**; **7**; **8**; **11**]) although the full results were not explicitly stated. They may be found in Theorem II and Corollary I to Theorem III below. The situation for differential rings not containing the rationals is much more subtle, and for such rings the basis theorem does not hold without restriction. Two different aspects of the problem were explored by Kolchin [**4**] and Seidenberg [**10**]. Then Kolchin [**5**] produced a definitive result which included the earlier theorems and much more.

Another feature of Kolchin's paper [**5**] was to generalize the basis theorem to certain subsets of the set of radical differential ideals. This generalization is very natural and does not complicate the proof of the basis theorem itself. It is also included in this paper and the necessary definitions are given in § 1.

In the first three sections of this paper we summarize the needed definitions and known results. Sections 4 and 5 contain the proof of the principal theorem. In the final section we discuss a criterion of Seidenberg related to the basis theorem. Some knowledge of differential algebra [**9**] or difference algebra [**1**], while not technically needed, is desirable for an intuitive understanding of this paper.

All rings discussed in this paper are commutative with identity, and all ring extensions are unitary.

1. Conservative systems. A set C of ideals in a ring R is called *conservative* if

Received March 31, 1970.

(a) If A_i, $i \in I$, are ideals of C, then $\bigcap_{i \in I} A_i \in C$. (In particular, taking I to be the empty set, we find $R \in C$.)

(b) If A_i, $i \in I$, are ideals of C linearly ordered by inclusion, then

$$\bigcup_{i \in I} A_i \in C.$$

A conservative set C is *divisible* if for $A \in C$, $x \in R$, $A{:}x \in C$. A divisible conservative set is *perfect* if its members are radical ideals. A set of ideals satisfying the ascending chain condition is called *Noetherian*.

If C is perfect and $A \in C$, then A is an intersection of prime ideals of C, and if C is also Noetherian, then A is the intersection of finitely many prime ideals of C. These facts give perfect sets their importance. In particular, the differential ideals called perfect by Raudenbush [**7**] and the difference ideals called perfect by Ritt and Raudenbush [**8**] form perfect sets according to the definition above, and the theorems showing that such ideals can be represented as the intersection of prime differential or prime difference ideals are special cases of the result just stated. The theory of conservative and of perfect sets (with some variations in terminology) is developed in [**2**; **5**; **6**].

Let C be a conservative set of ideals in R. Let $S \subseteq R$. We denote by $\{S; C\}$ the minimal ideal of C containing S, that is, the intersection of all ideals of C containing S. If S is finite, then S is called a *C-basis* for $\{S; C\}$. Evidently, C is Noetherian if and only if every ideal of C has a C-basis.

Let R_0 be a subring of R, and let C be a set of ideals of R. We denote by C/R_0 the set of ideals $A \cap R_0$, $A \in C$, of R_0. It is easy to see that the properties of being conservative, divisible, perfect, or Noetherian are inherited from C by C/R_0.

The following lemma [**5**, Lemma 2; **2**, Lemma 6] is fundamental in studying perfect sets of ideals.

LEMMA I. *Let R be a ring and C a perfect set of ideals in R. Let $S \subseteq R$, $T \subseteq R$. Let ST denote the set $\{st,\ s \in S,\ t \in T\}$. Then*

$$\{S; C\} \cap \{T; C\} = \{ST; C\}.$$

Kolchin [**5**, Lemmas 3 and 1] has proved the following results.

LEMMA II. *Let R be a ring and C a perfect set of ideals of R which is not Noetherian. Then there exist ideals maximal among those ideals of C which do not have a C-basis. Such ideals are prime.*

LEMMA III. *Let R be a ring, C a perfect set of ideals of R, $S \subseteq R$, and $a \in R$. If $a \in \{S; C\}$, then there exists a finite subset T of S such that $a \in \{T; C\}$.*

With the aid of these lemmas, Kolchin [**5**] established the following generalization of the Ritt basis theorem. The proof is a specialization of that of Theorem II below.

THEOREM I. *Let R be a ring and R_0 a subring of R such that R is finitely generated over R_0. Let C be a perfect set of ideals of R. If C/R_0 is Noetherian, then C is Noetherian.*

2. Difference-differential rings. Let R be a ring, $\Delta = (\delta_1, \ldots, \delta_m)$ derivations of R into R, and $\mathrm{T} = (\tau_1, \ldots, \tau_n)$ isomorphisms of R into R such that all pairs of members of $\Delta \cup \mathrm{T}$ commute. Then (R, Δ, T) is called a difference-differential ring. (If Δ is empty, then (R, Δ, T) is a difference ring, and if T is empty, a differential ring.) We denote by Θ the set of formal power products (including the identity) of δ_i and τ_j. Θ is called the set of difference-differential operators. If $\vartheta \in \Theta$, then the *order* of θ is the sum of the exponents of the δ_i and τ_j appearing in θ.

We denote by Θ' the subset of Θ consisting of formal power products of the δ_i only and by Θ^* the set of formal power products of the τ_j only. If $\theta \in \Theta$, then we have $\theta = \theta'\theta^*$, $\theta' \in \Theta'$, $\theta^* \in \Theta^*$. This representation is unique. If $a \in R$, $\theta \in \Theta^*$, then θa is called a *transform* of a. If $a \in R$, $\theta \in \Theta'$, and θ is not the empty product, then θa is called a *derivative* of a. The notation given here for the operators will be retained throughout the paper even where the notation for the ring itself is changed.

Remark 1. We shall generally use R to denote both the ring R and the difference-differential ring (R, Δ, T). At times we shall also regard R as a difference ring with isomorphisms T and the empty set of derivations. Note that Δ and T are ordered collections, not sets. This is essential in defining extensions and homomorphisms.

Let $(R', \Delta', \mathrm{T}')$ be another difference differential ring where $\Delta' = (\delta_1', \ldots, \delta_m')$ and $\mathrm{T}' = (\tau_1', \ldots, \tau_n')$ have the cardinality of Δ and T, respectively. A ring homomorphism ϕ from R to R' is called a difference-differential homomorphism if $\phi\delta_i = \delta_i'\phi$, $\phi\tau_j = \tau_j'\phi$, $1 \leqq i \leqq m$, $1 \leqq j \leqq n$. If R is a subring of R' and the injection map is a difference-differential homomorphism, then (R, Δ, T) is called a *difference-differential subring* of $(R', \Delta', \mathrm{T}')$ and we speak of the pair (R, Δ, T) and $(R', \Delta', \mathrm{T}')$ as forming a difference-differential ring extension which will frequently be denoted by R'/R. (By abuse of language we sometimes refer to $(R', \Delta', \mathrm{T}')$ itself as a difference-differential extension of (R, Δ, T).)

Let R'/R be a difference-differential ring extension, and let $S \subseteq R'$. We denote by $R\{S\}$ the smallest difference-differential subring of R' which contains R and S. If $R' = R\{T\}$, where T is finite, we say that R' is finitely generated in the difference-differential sense over R. If $R' = R\{y_1, \ldots, y_k\}$, and the set $Y = \{\theta y_i, \theta \in \Theta, 1 \leqq i \leqq k\}$ is algebraically independent over R, then R' is called a *polynomial difference-differential* ring over R (and R'/R a polynomial difference-differential extension) in the indeterminates $y_1, \ldots, y_k$. The elements of R' are then called difference-differential polynomials. It is evident that such extensions exist for every k and are unique to within isomorphism.

Every finitely generated difference-differential extension of R is obtained from a polynomial difference-differential extension through a difference-differential homomorphism which leaves R fixed.

A difference-differential ring will be said to be *ordinary* as a difference ring if $n = 1$. If $m = 0$, $n = 1$, it is an *ordinary difference ring*. A corresponding terminology is applied if $m = 1$, or $m = 1, n = 0$.

Let R' be a polynomial difference-differential ring over R. We use the notation of the preceding paragraph. If $u, v \in Y$ and there exists $\theta \in \Theta$ such that $v = \theta u$, then v will be called, with some abuse of language, a *multiple* of u (a *proper* multiple if θ is not the empty product). We introduce an ordering $<$ into Y as follows. Let $v \in Y$, $v = \theta'\theta^* y_i$, $\theta' \in \Theta'$, $\theta^* \in \Theta^*$, $1 \leqq i \leqq k$. We assign to v the $(m + n + 3)$-tuple $(a, b, c_1, \ldots, c_{m+n}, i)$, where a is the order of θ', b the order of θ^*, and the c_i are the exponents of the successive δ_i and τ_j in θ. Let the $(m + n + 3)$-tuples be ordered lexicographically, and order the elements of Y as their $(m + n + 3)$-tuples are ordered. Note the following properties of $<$.

(a) $<$ is a total ordering and a well-ordering.

(b) If $u, v \in Y$, $\theta \in \Theta$, and $u < v$, then $\theta u < \theta v$.

(c) If $u, v \in Y$, and v is a proper multiple of u, then $u < v$.

(d) If $u = \alpha'\alpha^* y_i$, $v = \beta'\beta^* y_j$, where α', $\beta' \in \Theta'$, α^*, $\beta^* \in \Theta^*$ and α' is of lower order than β', then $u < v$.

The following lemma is proved exactly as in [**9**, p. 147].

LEMMA IV. *With the notation of the preceding paragraph let $u_1 < u_2 < \ldots$ be elements of Y. Then there exist positive integers $i, j \neq i$, such that u_j is a multiple of u_i.*

If $P \in R' - R$, with R' (as above) a polynomial difference-differential ring over R, then the *leader* u of P is the highest member of Y in the ordering $<$ which is effectively present in P. The *initial* of P is the coefficient of the highest power of u in P when P is written as a polynomial in u with coefficients in $R[Y - u]$. The *separant* of P is the formal partial derivative $\partial P/\partial u$.

We define a ranking (that is, a pre-ordering) of the elements of R' as follows: Let $A, B \in R'$. Then A is of *lower rank* than B if one of the following holds: The leader of A is lower than the leader of B; A and B have the same leader u and A is of lower degree than B in u; $A \in R$, $B \in R' - R$.

A difference-differential field is a difference-differential ring which is a field. The terminology to be used for difference-differential fields is for the most part obvious. We need only note that if L/K is a difference-differential field extension and $S \subseteq L$, then $K\langle S\rangle$ denotes the smallest difference-differential subfield of L containing K and S. We say that S is a set of difference-differential generators of $K\langle S\rangle$ over K.

Let R be a difference-differential ring. The set I of difference-differential ideals of R (that is, of ideals of R closed under the operators Θ) is a conservative but not necessarily a divisible conservative set. Let D consist of those radical ideals A of I which satisfy:

(1) If for some $\tau \in \mathrm{T}$ and $a \in R$, $\tau a \in A$, then $a \in A$;

(2) If for some $\tau \in \mathrm{T}$ and $a \in R$, $a\tau a \in A$, then $a \in A$.

Then D is a perfect set of ideals [**2**, pp. 798–799] and indeed every perfect set contained in I is contained in D. Let $S \subseteq R$. We shall hereafter use the abbreviations $\{S\}$ for $\{S; D\}$ and $[S]$ for $\{S; I\}$. We call the ideals of D the perfect difference-differential ideals of R (perfect difference ideals or perfect differential ideals if Δ, or T respectively, is empty). These definitions accord with those of Ritt and Raudenbush mentioned above, and the abbreviated notation coincides with that conventionally used for perfect difference and differential ideals.

3. Transformal quasi-separability. Let L/K be a difference field extension. (That is, Δ is now the empty set or is disregarded.) A subset U of L is called *transformally independent* over K if $U^* = \{\theta u, \theta \in \Theta^*, u \in U\}$ consists of distinct elements (i.e., $\theta_1 u_1 = \theta_2 u_2$ implies $\theta_1 = \theta_2$ and $u_1 = u_2$) and these form an algebraically independent set over K. The properties of transformal independence have been established in [**1**, Chapter 5] for the case $n = 1$, and they carry over without essential change to the general case. The cardinality of a subset of L maximal among those transformally independent over K is an invariant of L/K called the *degree of transformal transcendence*.

Let U be a subset of L, V a subset of U maximal among those subsets of U transformally independent over K. If $U - V$ is finite we say that U is of *finite transformal codimension* over K. Exactly as with the usual codimension of field theory we establish that the cardinality of $U - V$ is independent of which maximal transformally independent set V is chosen.

A subset U of L is said to be *transformally separably independent* over K if U^* as defined above consists of distinct elements which constitute a separably independent set (that is, annul no separable polynomial) over K. We define L/K to be *transformally quasi-separable* if every subset of L transformally separably independent over K is of finite transformal codimension over K. If T is the empty set, this notion reduces to that of quasi-separability introduced by Kolchin [**5**] and essential to his basis theorem for differential rings. It is easy to see that if L/K is quasi-separable when regarded as a field extension, then it is transformally quasi-separable. The following examples show that these notions are not equivalent.

Example 1. Let F be an ordinary difference field of positive characteristic p. We write τ for τ_1. Let $F\langle x\rangle$ be an extension of F with x transformally independent over F. Let $K = F\langle x^p\rangle$. Then $F\langle x\rangle$ is not quasi-separable over K since the $\tau^i x$, $i = 0, 1, \ldots,$ form a separably independent set of infinite codimension. Of course, this set is not transformally separably independent and so does not violate the definition of transformal quasi-separability. To show that

$F\langle x\rangle$ is in fact transformally quasi-separable over K, note that if it were not, there would exist an infinite ascending chain of difference fields between K and $F\langle x\rangle$. Using [**1**, Chapter 5, Theorem XVIII], it is easy to see that no such chain exists. Indeed, every finitely generated extension of an ordinary difference field is transformally quasi-separable.

Example 2. Let F be a field of positive characteristic p. Let $c_1, c_2, \ldots$ be algebraically independent over F. Let

$$K = F(c_1^p, c_2^p, \ldots) \qquad \text{and} \qquad L = F(c_1, c_2, \ldots).$$

Then L/K is not quasi-separable. Let τ be the identity automorphism of L. Then L/K may be regarded as a difference field extension. It is transformally quasi-separable since there are no transformally separably independent sets.

Let R be a difference ring, R_0 a difference subring of R. Let P be a prime and perfect difference ideal of R. (A prime difference ideal need not be perfect since it may fail to satisfy (1) of § 2.) Let K be the quotient field of $R_0/(R_0 \cap P)$ and L the quotient field of R/P. In an obvious canonical way, we may regard L/K as a difference field extension. In [**5**] Kolchin defined (independently, of course, of the difference field structure) P to be quasi-separable over R_0 if L/K is quasi-separable. We shall say that P is *transformally quasi-separable* over R_0 if L/K is transformally quasi-separable. Similarly, P is separable over R_0 if L/K is separable.

4. The reduction theorem. Let R be a difference-differential ring and $R' = R\{y_1, \ldots, y_k\}$ a polynomial difference-differential ring over R. Let $A \in R' - R$, $B \in R'$, and let A be of degree d in its leader u. We say that B is *reduced* with respect to A if B is free of transforms of derivatives of u and of degree less than d in each transform of u. Let $F = \{F_i, i \in I\}$ be a set of elements of $R' - R$. We say that F is an *autoreduced* set if for each $i, j \in I$ with $i \neq j$, F_j is reduced with respect to F_i. It follows easily from Lemma IV that all autoreduced sets are finite. Let $H \in R'$, and let F be autoreduced. We say that H is reduced with respect to F if H is reduced with respect to each F_i, $i \in I$. (If F is empty, every member of R' is reduced with respect to F.)

REDUCTION THEOREM. *Let R be a difference-differential ring,*

$$R' = R\{y_1, \ldots, y_k\}$$

a polynomial difference-differential ring over R. Let $F = \{F_1, \ldots, F_r\}$ be an autoreduced set in R'. Let $G \in R'$. Then there exists a polynomial H in R' reduced with respect to F, a product J of powers of transforms of separants and initials of the F_i, and a polynomial L in $[F_1, \ldots, F_r]$ such that

(1) $H = JG - L$.

https://doi.org/10.4153/CJM-1970-141-3 Published online by Cambridge University Press

We may choose (1) *such that neither J nor L effectively involves a member of Y higher than the leader of G. If R is a difference ring, J may be taken to be a product of transforms of initials of the F_i.*

Proof. If F is empty, we may let $H = G, J = 1, L = 0$. Let F not be empty. Let u_j denote the leader, I_j the initial, S_j the separant, and d_j the degree in u_j of F_j, $1 \leqq j \leqq r$. If a polynomial A of R' is not reduced with respect to F, then it involves one or more multiples of leaders of the F_j to degrees which violate the definition of reduction. The highest such multiple is called the F-leader of A. We assume that there are polynomials for which no relation of the form of (1) exists and obtain a contradiction. Clearly no S_j is 0, since otherwise (1) follows trivially.

All polynomials for which no relation of the form of (1) holds must have F-leaders. Among such polynomials let A be one which has lowest F-leader v and among these is of lowest degree d in v. For some (not necessarily unique) j, $1 \leqq j \leqq r$, v is a multiple of u_j, say $v = \theta u_j$, $\theta \in \Theta$. Let E denote the initial of θF_j. If $\theta \in \Theta^*$, then $E = \theta I_j$, θF_j is of degree d_j in θu_j, and $d \geqq d_j$. If $\theta \notin \Theta^*$, then E is a transform of S_j and θF_j is linear in θu_j.

By the division algorithm there exists a non-negative integer a and a polynomial $M \in R'$ such that $A_1 = E^a A - M(\theta F_j)$ is of degree less than d_j in v, and is free of v if $\theta \notin \Theta^*$. Neither M nor θF_j effectively involves a member of Y higher than the leader of A. Now A_1 can involve effectively only those members of Y which are present either in θF_j or in A. Furthermore, those present in A but not in θF_j appear to the same degree in A and in A_1. Let $u \in Y$, $u > v$, be effectively present to degree e in A_1. Then u is not present in θF_j, and so A is of degree at least e in u. Since v is the F-leader of A, it must be that if u is a multiple of some u_j, then $u = \theta^* u_i$, $\theta^* \in \Theta^*$, and $e < d_i$. Hence, u is not the F-leader of A_1. Then A_1 either has no F-leader, has F-leader lower than v, or has F-leader v and is of degree less than that of A in its F-leader. In all cases there exists a relation $J_1 A_1 - L_1 = A_2$ of the form of (1). Combining this with the relation above between A and A_1 we obtain the contradiction that A satisfies a relation of the form of (1). To prove the last statement of the theorem, note that if R' is a difference ring, the argument above can be carried out without reference to separants.

5. The basis theorems. The first result below, Theorem II, applies to rings which are difference rings only. It is needed for the proof of Theorem III for difference-differential rings.

Remark 2. It is a reasonable conjecture that Theorem II is a special case of Theorem III: This is so for ordinary difference rings since, as we have observed (Example 1), the condition of transformal quasi-separability required in Theorem III is satisfied by any finitely generated extension of an ordinary difference field.

Remark 3. Theorem II is not really new. For ordinary difference rings it is, except for the generalization to arbitrary perfect sets of difference ideals, a theorem of Ritt and Raudenbush [**8**, Theorem]. The general case is obtained by applying to the work of Strodt [**11**] the ideal-theoretic considerations of [**8**].

THEOREM II. *Let R be a difference ring and R_0 a difference subring of R such that R is finitely generated in the difference ring sense over R_0. Let C be a perfect set of ideals of R whose members are difference ideals. (Then they are necessarily perfect difference ideals.) If C/R_0 is Noetherian, then C is Noetherian.*

Proof. R is the homomorphic image of a polynomial difference ring $R_0\{y_1, \ldots, y_k\}$. Let C' be the set of ideals which are the complete pre-images in $R_0\{y_1, \ldots, y_k\}$ of the ideals of C. Using [**2**, § 4 (Lemma XII, and the final paragraph)], it is easy to see that if C satisfies the hypotheses of Theorem II, then so does C', and that it is sufficient to prove C' Noetherian. Hence, we shall suppose henceforth that $R = R_0\{y_1, \ldots, y_k\}$.

Suppose that the theorem is false. By Lemma II, there exists a prime ideal $P \in C$ such that P has no C-basis, and every ideal of C properly containing P has a C-basis. Let $P_0 = P \cap R_0$, $C_0 = C/R_0$. Then P_0 has a C_0-basis T. Let S denote the set of polynomials of P which have no coefficient in P_0. Of course, the members of S are in $R - R_0$. We proceed to construct inductively an autoreduced set F of members of S. If S is the empty set, let F be the empty set. (It can easily be proved that this case cannot, in fact, occur.) Suppose that S is not empty. Let F_1 be a polynomial of lowest rank among those in S. Suppose that $F_1, \ldots, F_i$, $i \geqq 1$, have been found and constitute an autoreduced set. If no polynomial of S is reduced with respect to $F_1, \ldots, F_i$, the set is complete. If S contains polynomials reduced with respect to $F_1, \ldots, F_i$, let F_{i+1} be one of lowest rank. Then $F_1, \ldots, F_{i+1}$ is autoreduced. In a finite number, say r, of steps, the process must terminate. Clearly, no polynomial of S is reduced with respect to F. Let $A \in P$ be reduced with respect to F. If A' is the sum of those terms of A with coefficients not in P_0, then $A' \in P$, and A' is reduced with respect to F. Hence $A' = 0$. Therefore, all coefficients of terms of A are in P_0.

Let I_j, $1 \leqq j \leqq r$, denote the initial of F_j. No I_j is in P. For suppose that for some j, $I_j \in P$. Since I_j is reduced with respect to F, it has some coefficient in P_0. Then F_j has some coefficient in P_0, contradicting $F_j \in S$.

Let $J = I_1 \ldots I_r$. Since P is prime, $J \notin P$. By the maximality of P, the ideal $\{P, J; C\}$ has a C-basis U. Using Lemma III we see that we may choose $U = J, V_1, \ldots, V_t$, where the V_i are in P. Let $G \in P$. It follows from the final statement in the reduction theorem that there exists some product K of powers of transforms of J and a polynomial $L \in [F_1, \ldots, F_r]$ such that $R = KG - L$ is reduced with respect to F. Since $R \in P$, every coefficient of R is in P_0. Then $R \in \{T; C\}$. Hence, $KG \in \{T, F_1, \ldots, F_r; C\}$, and so $JG \in \{T, F_1, \ldots, F_r; C\}$. Let JP denote the set $\{JG, G \in P\}$. Then $JP \subseteq \{T, F_1, \ldots, F_r; C\}$.

Using Lemma I we find

$$P = P \cap \{P, J; C\} \subseteq \{JP, V_1, \ldots, V_t; C\} \subseteq \{T, F_1, \ldots, F_r, V_1, \ldots, V_t; C\} \subseteq P.$$

Hence, P has a finite basis, contradicting its definition.

THEOREM III. *Let R be a difference-differential ring and R_0 a difference subring of R such that R is finitely generated in the difference-differential sense over R_0. Let C be a perfect set of ideals of R whose members are difference-differential ideals. Let every prime ideal of C be transformally quasi-separable over R_0. If C/R_0 is Noetherian, then C is Noetherian.*

Proof. As in the proof of Theorem II we may assume that R is a polynomial difference-differential ring, $R = R_0\{y_1, \ldots, y_k\}$.

Suppose that the theorem is false. We define P and P_0 as in the proof of Theorem II. Let S be the set of polynomials of P which are not in R_0 and have separant not in P. (S may be empty.) We construct inductively an autoreduced set F in S. If S is empty, let F be empty. If S is not empty, let F_1 be a polynomial of lowest rank in S. Suppose that $F_1, \ldots, F_i$ have been found. If S contains no polynomial reduced with respect to $F_1, \ldots, F_i$, the set is complete. If S contains polynomials reduced with respect to $F_1, \ldots, F_i$, let F_{i+1} be one of lowest rank. Let $F_1, \ldots, F_r$ be the autoreduced set obtained by this procedure. No polynomial of S is reduced with respect to F.

Let u_j denote the leader, S_j the separant, and I_j the initial of F_j. We claim that $I_j \notin P, j = 1, \ldots, r$. Let t denote the degree of F_j in u_j and put $F_j = I_j u_j^t + A$. If $I_j \in P$, then $A \in P$. Since A is reduced with respect to F, the separant of A is in P. Then $\partial A/\partial u_j \in P$, since either it is this separant, or A does not involve u_j. If I_j were in P, we would find

$$S_j = t u_j^{t-1} I_j + \partial A/\partial u_j \in P,$$

a contradiction. Let $J = I_1 \ldots I_r S_1 \ldots S_r$. Then $J \notin P$.

If U is any subset of Y, then U^* will denote the set of transforms of the members of U. (Note that $U \subset U^*$.) Evidently, $R_0[U^*]$ is a difference ring under the contractions to it of the members of T. For each j, $1 \leqq j \leqq r$, we write $u_j = \alpha_j \beta_j y_{i(j)}, \alpha_j \in \theta', \beta_j \in \Theta^*, 1 \leqq i(j) \leqq k$. Let V consist of those θy_i, $\theta \in \Theta'$, $1 \leqq i \leqq k$, which are not derivatives of any $\alpha_j y_{i(j)}$. Every member of P reduced with respect to F is in $R_0[V^*]$. We are going to partition V^*.

Let X consist of those members of V which have no derivative in V. Then X is finite. For if not, there exists an infinite sequence $x_1 < x_2 < \ldots$ of elements of X. By Lemma IV there exist integers $i, j > i$, such that x_j is a multiple of x_i. This contradicts the fact that no derivative of x_i is in V.

Let s be the maximum of the orders of elements of X. Let W consist of the elements of V of order at most s, and let $Z = V - W$. (If X is empty, let W be empty.) Note that each $\alpha_i y_{i(j)}$ is in W. If $w \in W^*, z \in Z^*$, then $w < z$. Every member of Z^* has some first derivative in Z^*. Every member of

https://doi.org/10.4153/CJM-1970-141-3 Published online by Cambridge University Press

$P \cap R_0[Z^*]$ is reduced with respect to F. $V^* = W^* \cup Z^*$ is the desired partition.

Let $A \in R - R_0$ with leader u. Let $v \in Y$ appear effectively in A. Then $d(A, v)$ is defined to be the difference between the first entries in the $(m + n + 3)$-tuples assigned as in § 2 to u and to v. Let $A \in P$ be reduced with respect to F, and let $z \in Z^*$. It will be shown that $\partial A/\partial z \in P$. For suppose that $\partial A/\partial z \notin P$. We may assume that A and z have been chosen so that $d(A, z)$ is minimal. We may also assume that if $z' \in Z^*$, $\partial A/\partial z' \notin P$, then $z' \leqq z$. Let $z_1, \ldots, z_t$ be the members of Z^* and $w_1, \ldots, w_m$ the members of W^* appearing effectively in A. We may choose the subscripts so that $z_1 < z_2 < \ldots < z_t$. Of course $w_i < z_1$, $1 \leqq i \leqq m$. Since z_t is the leader of A, $\partial A/\partial z_t \in P$. It follows that $z = z_s$ for some s, $1 \leqq s \leqq t - 1$. We have $\partial A/\partial z_i \in P$, $s + 1 \leqq i \leqq t$.

There exists $\delta \in \Delta$ such that $\delta z \in Z^*$. Let

$$A_1 = \delta A - \sum_{s+1}^{t} (\partial A/\partial z_i)\delta z_i$$
$$= A' + \sum_{1}^{s} (\partial A/\partial z_i)\delta z_i + \sum_{1}^{m} (\partial A/\partial w_i)\delta w_i,$$

where A' involves effectively only certain w_i and z_j. Evidently, $A_1 \in P$. It may be that A_1 is not reduced with respect to F. This can result only from the presence in A_1 of certain δw_i or of certain δz_j, $j < s$. Using the reduction theorem, we see that there exists a product K of powers of transforms of initials and separants of F and a polynomial L in $[F_1, \ldots, F_r]$ such that $A_2 = KA_1 - L$ is reduced with respect to F. Furthermore, K and L may be chosen so that they involve only members of Y lower than δz_s.

If δz_s is either not effectively present in A_2 or is its leader, then $\partial A_2/\partial(\delta z_s) \in P$. In the remaining case the leader of A_2 is some z_i, $s < i \leqq t$, and $d(A_2, \delta z_s) < d(A, z_s)$. It follows from the minimality of $d(A, z_s)$ that in this case also $\partial A_2/\partial(\delta z_s) \in P$. Since $\partial A_2/\partial(\delta z_s) = K\partial A_1/\partial(\delta z_s)$, and $K \notin P$, it remains only to prove that $\partial A_1/\partial(\delta z_s) \notin P$ in order to obtain a contradiction. If δz_s is not one of the z_i, then $\partial A_1/\partial(\delta z_s) = \partial A/\partial z_s \notin P$. Suppose that $\delta z_s = z_j$. Then

$$\partial A_1/\partial(\delta z_s) = \partial A/\partial z_s + \delta(\partial A/\partial z_j) - \sum_{s+1}^{t} (\partial^2 A/\partial z_i \partial z_j)\delta z_i,$$

where the sum is over i. Since $j > s$, $\delta(\partial A/\partial z_j) \in P$. Also $\partial A/\partial z_i \in P$ and $d(\partial A/\partial z_i, z_j) < d(A, z)$, so that $\partial^2 A/\partial z_i \partial z_j \in P$, $s + 1 \leqq i \leqq t$. Hence in this case also, $\partial A_1/\partial(\delta z_s) \notin P$.

It follows in particular from the above that if $A \in P \cap R_0[Z^*]$, $z \in Z^*$, then $\partial A/\partial z \in P$. Let ϕ be the canonical homomorphism of R onto R/P. Then one sees easily that ϕZ is transformally separably independent over the quotient field L of ϕR_0. By the hypothesis of transformal quasi-separability, ϕZ is of finite transformal codimension over L. It follows exactly as in [**5**, p. 12], with transformal independence replacing algebraic independence, that there is a finite subset T of V such that $P \cap R_0[V^*]$ is contained in the perfect difference ideal generated in $R_0[V^*]$ by $P \cap R_0[T^*]$. Now $R_0[T^*]$ is finitely generated as a difference ring over R_0. By Theorem II there exists a finite set B which is a $C/R_0[T^*]$-basis for $P \cap R_0[T^*]$. Then $P \cap R_0[V^*] \subseteq \{B; C\}$. Every polynomial of P reduced with respect to F is therefore in $\{B; C\}$. Since P is properly contained in $\{P, J; C\}$, there is a C-basis for $\{P, J; C\}$, and by Lemma III we may take this basis to be $A_1, \ldots, A_g, J$ with the $A_i \in P$. The proof may be completed as for Theorem II.

A differential (or difference-differential) ring is called a *Ritt algebra* if it contains the rational numbers.

COROLLARY I. *Let R_0 be a difference-differential ring which is a Ritt algebra. Let the set of perfect difference-differential ideals of R_0 be Noetherian. If R is a difference-differential ring finitely generated in the difference-differential sense over R_0, and C is the set of perfect difference-differential ideals of R, then C is Noetherian.*

Proof. C is a perfect set. Every prime ideal of R is separable over R_0 and therefore certainly transformally quasi-separable.

Remark 4. One can give a direct proof of Corollary I similar to the proof of Theorem II and shorter than the proof of Theorem III.

Kolchin defines a differential field K to be *differentially quasi-perfect* if every differential extension field of K is quasi-separable over K. Of course, every field of characteristic 0 and every perfect field of positive characteristic is differentially quasi-perfect. Let K be of positive characteristic p. Let C be the subfield of K consisting of differential constants; that is,

$$c \in C \quad \text{if } \delta_i c = 0, \qquad i = 1, \ldots, m.$$

Kolchin has shown [**5**, p. 7–07] that K is differentially quasi-perfect if and only if $C{:}K^p$ is finite.

COROLLARY II. *Let K be a difference-differential field which is differentially quasi-perfect when regarded as a differential field. Let R be a difference-differential ring finitely generated over K, and let C be the set of perfect difference-differential ideals of R. Then C is Noetherian.*

Proof. C is a perfect set. By the result of Kolchin mentioned above, every prime difference-differential ideal of R is quasi-separable, and therefore certainly transformally quasi-separable.

If K is a differential field only, then C is Noetherian if and only if K is quasi-perfect [**5**, Theorem 2, Corollary 2]. Theorem II and the examples of § 3 show that this condition is not necessary (though clearly sufficient) for K a difference-differential field. The question remains open whether it is necessary that every difference-differential extension of K be transformally quasi-separable.

6. Separability criteria. Throughout this section F denotes a field of positive characteristic p. Let $\{z_i, i \in I\}$ be a p-basis for F/F^p. There exist uniquely determined derivations d_i, $i \in I$, such that

$$d_i z_i = 1, \quad d_i z_j = 0, \qquad i, j \in I, i \neq j.$$

Let $R = F[\{x_j, j \in J\}]$ be a polynomial ring (in possibly infinitely many indeterminates) over F and let P be a prime ideal of R. We extend the d_i to R by defining $d_i x_j = 0$, $i \in I, j \in J$. Seidenberg [**10**] showed that P is separable if and only if given $A \in P \cap F[\{x_j^p, j \in J\}]$, every $d_i A \in P$. Since separable ideals are certainly quasi-separable, this criterion can be applied to differential polynomial rings to select a Noetherian set of perfect differential ideals; and this is carried out in [**10**].

Let λ be the map of R into R defined as follows: Let $A \in R$. If

$$A \in F[\{x_j^p, j \in J\}],$$

then $\lambda A = A$. Otherwise $\lambda A = 1$. We may restate Seidenberg's criterion in terms of links [**2**, § 5] as follows: A radical ideal Q of R will be called *allowable* if it admits the links $\{\lambda; d_i\}$, that is, if

(2) $\lambda A \in Q$ implies $d_i A \in Q$, $i \in I$.

Seidenberg's criterion stated above thus becomes: a prime ideal is separable if and only if it is allowable. Seidenberg also showed that the set C of allowable radical ideals is perfect. (There is a more general result in [**5**, p. 7–08, Example 3].) Hence, every allowable radical ideal is the intersection of separable prime ideals. Using the mechanism of [**2**] we may prove these results very rapidly. In fact [**2**, Lemma XIV], C is perfect if every ideal Q of C satisfies

(2′) Let $A, B \in R$. $B\lambda A \in Q$ implies $Bd_i A \in Q$, $i \in I$.

We need merely show that (2′) follows from (2). Suppose that Q satisfies (2) and $B\lambda A \in Q$. If $\lambda A = 1$, then $B \in Q$ and so $Bd_i A \in Q$, $i \in I$. Suppose that $\lambda A = A$. Then $BA \in Q$, and so $B^p A \in Q$. Since $\lambda(B^p A) = B^p A$ in this case, it follows from (2) that every $d_i(B^p A) \in Q$. But $d_i(B^p A) = B^p d_i A$. Since Q is radical, each $Bd_i A \in Q$.

There is an easy generalization of Seidenberg's criterion. A set D of (not necessarily commuting) derivations of F into F will be called *adequate* if given $x \in F - F^p$ there exists $d \in D$ such that $dx \neq 0$. It is easily seen (for example, using [**10**, Theorem 4]) that $\{d_i, i \in I\}$ is adequate. Let R and λ be as above. We extend D to R by defining $dx_j = 0$, $d \in D, j \in J$. A radical ideal Q of R is *D-allowable* if it admits all the links $\{\lambda; d\}$, $d \in D$, that is, if

(2*) $\lambda A \in Q$ implies $dA \in Q$, $d \in D$.

LEMMA V. *The D-allowable radical ideals of R form a perfect set C. If D is adequate, then a prime ideal of R is separable if and only if it is D-allowable,* *and C consists precisely of the ideals of R which are intersections of separable prime ideals.*

Proof. To prove the first statement we proceed exactly as in the special case of allowable ideals using (2*) instead of (2). It remains only to prove that if D is adequate, then a prime ideal is separable if and only if it is D-allowable, since the last part of the lemma then follows at once from a property of perfect sets stated in § 1.

Let U denote the set of power products of the x_i. Let D be adequate and let P be a D-allowable prime ideal of R. We must show that if $A \in P$,

$$A = \sum_{i=1}^{n} a_i u_i^p,$$

where the u_i are elements of U and the a_i are in F and not all 0, then there exist b_i, $1 \leqq i \leqq n$, in F and not all 0 such that $B = \sum_{i=1}^n b_i u_i \in P$. Suppose that this is false and that A is chosen with n minimal such that no such B exists. Without loss of generality we may assume that $a_1 = 1$. There exists j, $2 \leqq j \leqq n$, such that $a_j \notin F^p$. There is some $d \in D$ such that $da_2 \neq 0$. Then $dA = \sum_{i=2}^n (da_i)u_i^p \in P$, and not all coefficients of dA are 0. By the minimality of n, there exist c_i, $2 \leqq i \leqq n$, in F and not all 0 such that $\sum_{i=2}^n c_i u_i \in P$. This is a contradiction.

Now let P denote a separable prime ideal of R and let $A = \sum_{i=1}^n a_i u_i^p \in P$, where the a_i are in F. We shall see that if d is *any* derivation of F into F, then $dA \in P$. (We extend d to R by letting $dx_j = 0, j \in J$.) We again suppose that this is false and choose A with n minimal such that $dA \notin P$. Then no a_i is 0. By the separability of P there exist b_i, $1 \leqq i \leqq n$, in F and not all 0 such that $B = \sum_{i=1}^n b_i u_i \in P$. We may suppose that $b_1 \neq 0$. Then

$$C = b_1^p A - a_1 B^p \in P \cap F[\{x_j^p, j \in J\}].$$

Either C is "shorter" than A or $C = 0$. Hence, $dC \in P$. Computing dC we find the contradiction $dA \in P$.

THEOREM IV. *Let K be a difference-differential field of positive characteristic p. Let $R = K\{y_1, \ldots, y_k\}$ be a polynomial difference-differential ring over K and D an adequate set of derivations of K into K. Let C be the set of D-allowable perfect difference-differential ideals of R. Then C is a perfect set and is Noetherian.*

Proof. C is the intersection of two perfect sets: the set of perfect difference-differential ideals and the set of D-allowable ideals. It follows easily from the definition that C is perfect. By Lemma V, every prime ideal of C is separable and therefore transformally quasi-separable. It follows from Theorem III that C is Noetherian.

The following result is the extension to difference-differential ideals of a theorem of Seidenberg [**10**, Theorem 5].

COROLLARY III. *Let K and R be as in Theorem* IV. *Let C be the set of difference-*

differential ideals of R which are intersections of separable prime and perfect difference-differential ideals of R. Then C is perfect and Noetherian.

Proof. Let D be the set of derivations $\{d_i, i \in I\}$ defined at the beginning of this section. As has been stated, D is adequate. By Theorem IV the set C' of D-allowable perfect difference-differential ideals of R is perfect and Noetherian. Lemma V shows that C and C' contain the same prime ideals. Since C' is perfect, it consists precisely of the intersections of its prime ideals. Then $C = C'$ by definition of C.

COROLLARY IV. *Let K and R be as in Theorem* IV. *If* Δ *is adequate, the set of perfect difference-differential ideals of R is Noetherian and every prime and perfect difference-differential ideal of R is separable.*

Proof. Every perfect difference-differential ideal of R is Δ-allowable.

Remark 5. Let K be a differential field. If Δ is not adequate, there is a prime differential ideal in the polynomial differential ring $K\{y\}$ which is not separable. For there exists $a \in K - K^p$ such that $\delta_i a = 0$, $1 \leqq i \leqq m$. Then $\{y^p - a\}$ is a prime but not separable differential ideal. With slight modification to allow for extensions which are not finitely generated, Corollary IV and the result just stated are equivalent to the following theorem stated by Kolchin in [**5**]. *Let C be the subfield of differential constants of K. Then K is differentially separable* (*that is, every differential extension of K is separable*) *if and only if* $C = K^p$. Corollary IV could easily have been proved using this theorem.

REFERENCES

1. R. M. Cohn, *Difference algebra* (Interscience, New York, 1965).

2. ——— *Systems of ideals*, Can. J. Math. *21* (1969), 783–807.

3. F. Herzog, *Systems of algebraic mixed difference equations*, Trans. Amer. Math. Soc. *37* (1935), 286–300.

4. E. R. Kolchin, *On the basis theorem for differential fields*, Trans. Amer. Math. Soc. *52* (1942), 115–129.

5. ——— *Le théorème de la base finie pour les polynômes différentiels*, Séminaire P. Dubreil, M.-L. Dubreil–Jacotin et C. Pisot, 14e Année: 1960/61, Algèbre et théorie des nombres, Fasc. 1 (Secrétariat mathématique, Paris, 1963).

6. ——— *Notes on differential algebra*, unpublished.

7. H. W. Raudenbush, *Ideal theory and algebraic differential equations*, Trans. Amer. Math. Soc. *36* (1934), 361–368.

8. H. W. Raudenbush and J. F. Ritt, *Ideal theory and algebraic difference equations*, Trans Amer. Math. Soc. *46* (1939), 445–452.

9. J. F. Ritt, *Differential algebra*, Amer. Math. Soc. Colloq. Publ., Vol. 33 (Amer. Math. Soc., Providence, R. I., 1950).

10. A. Seidenberg, *Some basic theorems in differential algebra* (*characteristic p, arbitrary*), Trans. Amer. Math. Soc. *73* (1952), 174–190.

11. W. C. Strodt, *Systems of algebraic partial difference equations*, unpublished master's essay, Columbia University, New York, 1937.

Rutgers University,
New Brunswick, New Jersey