MEMOIRS OF THE COLLEGE OF SCIENCE, UNIVERSITY OF KYOTO, SERIES A
Vol. XXVIII, Mathematics No. 2, 1953

On differential algebra of arbitrary characteristic

By

Kôtaro OKUGAWA

(Received October 1, 1953)

A number of results have been established for differential algebra,[1] and so it comes clear in the case of characteristic zero, but the case of nonzero characteristic was investigated only in a few papers. Among them, Kolchin (2) considered the basis theorem for systems of ordinary or partial differential polynomials over a differential ring, and Seidenberg (8) considered some basic theorems in the *ordinary* differential situation. In the following we shall generalize the results of Seidenberg in the *partial* differential situation. Our basis theorem is a generalization of the Kolchin's result if it is restricted to differential polynomials over a differential *field*. This restricted case seems useful in the application.

1. Differential polynomials. By a *differential ring* is meant a ring $\mathfrak{R}$ with a finite number m of given differentiations $\delta_1, \cdots, \delta_m$ which are mutually commutative. According as $m=1$ or >1, we shall say that $\mathfrak{R}$ is an *ordinary* or a *partial* differential ring. The differential ideal which is generated by a subset $\mathfrak{a}$ of $\mathfrak{R}$ will be denoted by $[\mathfrak{a}]$. The semiprime (or perfect) differential ideal generated by $\mathfrak{a}$ will be denoted by $\{\mathfrak{a}\}$. By a *differential field* is meant a differential ring which is a field; its characteristic p may be arbitrary.

Let $\mathfrak{F}$ be a differential field and $X_1, \cdots, X_n$ a finite number n of independent differential indeterminates over $\mathfrak{F}$. The differential ring of all differential polynomials over $\mathfrak{F}$ will be denoted by $\mathfrak{R}=\mathfrak{F}\{X_1, \cdots, X_n\}$. Dealing with differential polynomials, it is useful to introduce a linear order relation $\lesssim$ for differential polynomials (cf. Ritt (7) and Kolchin (2)). We define it below after some preliminary definitions.

1) A complete bibliography up to 1948 may be found in Ritt (7). To it may be added subsequent literatures: Herz (1), Okugawa (3-5) and Seidenberg (8); and Kolchin's works (especially, the one which is quoted in the footnote of p. 105).

Let $U=\delta_1^{h_1}\cdots\delta_m^{h_m}X_i$ and $V=\delta_1^{k_1}\cdots\delta_m^{k_m}X_j$ be two X-derivatives. U is called *lower* than V $(U<V)$ and V *higher* than U $(V>U)$ if and only if one of the following conditions are satisfied: 1) $i<j$, 2) $i=j$ and the total order $\sum_{i=1}^{m}h_i$ of U is less than the total order $\sum k_i$ of V, 3) $i=j$, total orders of U and V are equal and the first nonzero value of the differences $k_1-h_1, \cdots, k_m-h_m$ is positive.

Let A be a differential polynomial in $\mathfrak{R}$ and U an X-derivative. Then A can be written in the form

$$(1)\qquad A=A_0+A_1U+A_2U^2+\cdots+A_kU^k \quad (A_k\neq 0),$$

such that, for $p=0$, the A are polynomials over $\mathfrak{F}$ of X-derivatives other than U, and such that, for $p\neq 0$, the A are polynomials over $\mathfrak{F}$ of U^p and X-derivatives other than U and $0\leqq k\leqq p-1$. We shall say that U is contained in A *effectively*, provided $k>0$.

If some X-derivative is contained in a differential polynominal A effectively, the highest of such X-derivatives is called the *leader* of A. If A has the leader U with the expression (1) for A relative to U, then A_k is called the *initial* of A and the formal partial derivative $\partial A/\partial U=A_1+2A_2U+\cdots+kA_kU^{k-1}$ is called the *separant* of A. When no X-derivative is contained in A effectively, we say that A *lacks the leader.*

Definition. Let A and B be two differential polynomials. If both of A and B lack the leader, then $A\sim B$ (A is of the *same rank* as B). If A *lacks* the leader and B has the leader, then $A<B$ or $B>A$ (A is *lower* than B, or B is *higher* than A). If A and B have the leaders U and V respectively and if $U<V$, then $A<B$. If A and B have the same leader U and if $A=A_0+\cdots+A_hU^h$ and $B=B_0+\cdots+B_kU^k$ are the expressions as (1) relative to U, then $A<B$ or $A\sim B$ according as $h<k$ or $h=k$.[2]

The concepts of a differential polynomial being *reduced* with respect to another differential polynomial, a *chain*, the linear *order relation for chains*, the *characteristic set* and the reducedness of a differential polynomial with respect to a chain are defined as in Ritt and in Kolchin, using the order relation for differential polynomials defined above.

---

2) We shall have occasions to make use of an order relation with respect to an assigned one X_i of the indeterminates. In this case, we neglect the X-derivatives other than X_i-derivatives (or such X-derivatives are adjoined to the basic field $\mathfrak{F}$) and the order relation is defined in like manner concerning to X_i-derivatives only.

2. Allowable ideals. In this and the next sections, we consider the chain theorem and the decomposition theorem for semiprime differential ideals of $\mathfrak{R}=\mathfrak{F}\{X_1, \cdots, X_n\}$. These theorems do not hold true in general[3]. Seidenberg (8) has shown in the *ordinary* differential situation that these theorems hold true for "allowable" semiprime differential ideals. We prove that they hold true for allowable semiprime differential ideals also in the *partial* differential situation. The proof can be done by a modification of the proof of Kolchin (2). Therefore, we shall sketch only the line of our proof. *Our results are new only when* $m>1$ *and* $\mathfrak{F}$ *is an imperfect field.* Hence, for the sake of simplicity, *our description will mainly be intended to apply only to that case,* although it would be easy to reform them so as to cover all cases.

If $\mathfrak{F}$ is perfect, every semiprime differential ideal of $\mathfrak{R}$ wil be called *allowable.* To define allowable semiprime differential ideals for imperfect $\mathfrak{F}$, let $\mathfrak{R}_p$ be the ring of all polynomials over $\mathfrak{F}$ of p-th powers of all X-derivatives, and let $z_1, z_2, \cdots$ be a p-basis of $\mathfrak{F}/\mathfrak{F}^p$ which is fixed hencefore throughout this paper for convenience, and $w_1, w_2, \cdots$ all power products of $z_1, z_2, \cdots$ of exponents not exceeding $p-1$, so that $w_1, w_2, \cdots$ is a linear basis of $\mathfrak{F}/\mathfrak{F}^p$. Then, a semiprime differential ideal $\mathfrak{m}$ of $\mathfrak{R}$ is called *allowable* if $A=\sum_\iota A_\iota w_\iota \in \mathfrak{m}\cap\mathfrak{R}_p$ with $A_\iota \in \mathfrak{R}^p$ implies $A_\iota \in \mathfrak{m}$ for each ι. The definition does not depend on the choice of the p-basis z_ι.

In the case of imperfect $\mathfrak{F}$, a differentiation $\partial/\partial z_\iota$ in $\mathfrak{R}$ can be defined, for each ι, such that $\partial z_\iota/\partial z_\iota=1$, $\partial z_\varkappa/\partial z_\iota=0$ $(\varkappa\neq\iota)$ and $\partial U/\partial z_\iota=0$ for every X-derivative U. *A semiprime differential ideal* $\mathfrak{m}$ *of* $\mathfrak{R}$ *is allowable if and only if* $\mathfrak{m}\cap\mathfrak{R}_p$ *is closed under every differentiation* $\partial/\partial z_\iota$.

The notation of "allowable" is connected with the separability. Following Chevalley, a set $(x)=(x_1, \cdots, x_n)$ of quantities x_i over $\mathfrak{F}$ (elements of some differential extension field of $\mathfrak{F}$) is called *separable* over $\mathfrak{F}$ if and only if $\mathfrak{F}\langle x\rangle$ (the minimum differential extension field of $\mathfrak{F}$ containing $x_1, \cdots, x_n$) and $\mathfrak{F}^{1/p}$ are linearly disjoint over $\mathfrak{F}$. It is proved (Seidenberg (8)) that *a nonunit prime differential ideal* $\mathfrak{p}$ *of* $\mathfrak{R}$ *is allowable if and only if the generic point* (x) *of* $\mathfrak{p}$ *is separable over* $\mathfrak{F}$.

The intersection of any number of allowable semiprime dif-

3) Examples may be found in Seidenberg (8), pp. 185-186.

ferential ideals of $\mathfrak{R}$ is plainly an allowable semiprime differential ideal. Hence, if a subset α of $\mathfrak{R}$ is given, it determines the minimum allowable semiprime differential ideal containing α; this will be denoted by $\{\alpha\}_a$. Clearly $\{\alpha\} \subseteqq \{\alpha\}_a$ in general. If $\mathfrak{F}$ is perfect, then $\{\alpha\} = \{\alpha\}_a$ for every α. We define $\{\alpha\}^{(\lambda)}$ $(\lambda=0, 1, 2, \cdots)$ inductively by the rules; 1) $\{\alpha\}^{(0)} = \{\alpha\}$, and 2) $\{\alpha\}^{(\lambda+1)}$ is the semiprime differential ideal which is generated by $\{\alpha\}^{(\lambda)}$ and all (successive) derivatives for the differentiations $\partial/\partial z_t$ of elements of $\{\alpha\}^{(\lambda)} \cap \mathfrak{R}_p$. Then, we can easily prove that $\{\alpha\}^{(0)} \subseteqq \{\alpha\}^{(1)} \subseteqq \cdots \subseteqq \{\alpha\}^{(\lambda)} \subseteqq \cdots$ and that $\cup_{\lambda=0}^{\infty} \{\alpha\}^{(\lambda)} = \{\alpha\}_a$. If an allowable semiprime differential ideal $\mathfrak{m}$ has a finite subset $\boldsymbol{\alpha}$ such that $\mathfrak{m} = \{\alpha\}_a$, we shall say that $\mathfrak{m}$ has a finite basis $\boldsymbol{\alpha}$.[4]

Let $\mathfrak{m}$ be a nontrivial allowable semiprime differential ideal. Then, $\mathfrak{m}$ contains certainly differential polynomials G having the leader with the initial not contained in $\mathfrak{m}$. In fact, let G_0 be a nonzero differential polynomial of $\mathfrak{m}$ of the least possible total degree in the X-derivatives. The total degree is necessarily positive. G_0 has clearly the leader for $p=0$. For $p \neq 0$, if G_0 lacked the leader, G_0 could be written as $G_0 = \sum G_t w_t$ with $G_t \in \mathfrak{m} \cap \mathfrak{R}^p$ and every $G_t^{1/p}$ would be contained in $\mathfrak{m}$, contradicting to the minimal property of G_0. Thus G_0 has the leader in all cases, and as its initial is of lesser total degree, the initial is not contained in $\mathfrak{m}$.

Consider the totality σ of all such differential polynomials G, and let $\boldsymbol{A} = (A_1, \cdots, A_r)$ be a characteristic set of σ, which will be called a modified characteristic set of $\mathfrak{m}$. Let the separant and the initial of A_t be S_t and I_t respectively $(t=1, \cdots, r)$. The I_t are not contained in $\mathfrak{m}$. We prove that so are the S_t. In fact, let us denote by U_t the leader of A_t and write $A_t = H_{t0} + \cdots + H_{tk} U_t^k$ $(H_{tk} = I_t$; k being dependent on $t)$ as in (1) of § 1. In the case $k=1$, $S_t = I_t$ is not contained in $\mathfrak{m}$. In the case $k>1$, S_t has the initial $kH_{tk} = kI_t$ which is not contained in $\mathfrak{m}$ and S_t is reduced with respect to $\boldsymbol{A}$, hence S_t cannot be contained in $\mathfrak{m}$.

Now, we consider, for each i $(1 \leqq i \leqq n)$ which is such that some of the X_i-derivatives are contained (in the usual sence) in $A_1, \cdots, A_r$, the set of X_i-derivatives which are not higher than the highest X_i-derivative contained in the A's, and the ring $\mathfrak{F}$ of polynomials over $\mathfrak{F}$ of all X-derivatives in these sets. We can prove

4) Cf. Theorem 1 of the next section.

that *there exists for every* $G \in \mathfrak{m}$ *a set of nonnegative integers* $s_1, \cdots, s_r, t_1, \cdots, t_r$ *such that we have the congruence*

$$S_1^{s_1} \cdots S_r^{s_r} I_1^{t_1} \cdots I_r^{t_r} G \equiv 0 \mod [\mathfrak{m} \cap \mathfrak{J}], \tag{1}$$

where $[\mathfrak{m} \cap \mathfrak{J}]$ *is the differential ideal generated by* $\mathfrak{m} \cap \mathfrak{J}$ *in* $\mathfrak{R}$.

Remark. It will be easily seen that, for $p=0$, the congruence holds true with respect to mod $[A_1, \cdots, A_r]$. The proof in the general case can be carried out by an easy modification of the proof of Kolchin (2).

LEMMA 1. *If* α *and* β *are two subsets of* $\mathfrak{R}$, *then* $\{\alpha\}_a \cap \{\beta\}_a = \{\alpha \cdot \beta\}_a$, *where* $\alpha \cdot \beta$ *denotes the set of all products of elements of* α *with those of* β.

Proof. If $\mathfrak{J}$ is perfect, this lemma is nothing but the well known fact that $\{\alpha\} \cap \{\beta\} = \{\alpha \cdot \beta\}$, hence we suppose $\mathfrak{J}$ imperfect. It suffices to prove the inclusion $\{\alpha \cdot \beta\}_a \supseteq \{\alpha\}_a \cap \{\beta\}_a$. To this object, we shall prove inductively the inclusions $\{\alpha \cdot \beta\}_a \supseteq \{\alpha\}^{(\lambda)} \cap \{\beta\}^{(\lambda)}$ ($\lambda = 0, 1, 2, \cdots$). By the same fact used above, $\{\alpha\}^{(0)} \cap \{\beta\}^{(0)} = \{\alpha \cdot \beta\} \subseteq \{\alpha \cdot \beta\}_a$. Now, assume $\{\alpha \cdot \beta\}_a \supseteq \{\alpha\}^{(\lambda)} \cap \{\beta\}^{(\lambda)}$ for a nonnegative integer λ, and let us deduce the inclusion $\{\alpha \cdot \beta\}_a \supseteq \{\alpha\}^{(\lambda+1)} \cap \{\beta\}^{(\lambda)}$. We denote by α' the set consisting of all elements of $\{\alpha\}^{(\lambda)}$ and all derivatives for the differentiations $\partial/\partial z_t$ of elements of $\{\alpha\}^{(\lambda)} \cap \mathfrak{R}_p$, and by β' the set of all elements of $\{\beta\}^{(\lambda)}$. Again by the fact used above, $\{\alpha\}^{(\lambda+1)} \cap \{\beta\}^{(\lambda)} = \{\alpha'\} \cap \{\beta'\} = \{\alpha' \cdot \beta'\}$. Hence, it is sufficient to prove the inclusion $\alpha' \cdot \beta' \subseteq \{\alpha \cdot \beta\}_a$. Let A' be any element of α'. If $A' \in \{\alpha\}^{(\lambda)}$, then $A'\beta' \subseteq \{\alpha\}^{(\lambda)} \cap \{\beta\}^{(\lambda)} \subseteq \{\alpha \cdot \beta\}_a$. On the other hand, suppose $A' \notin \{\alpha\}^{(\lambda)}$. Then, there is an element $A \in \{\alpha\}^{(\lambda)} \cap \mathfrak{R}_p$ such that A' is a derivative of A for the differentiations $\partial/\partial z_t$. For any element $B' \in \beta'$, we have $B'A \in \{\alpha\}^{(\lambda)} \cap \{\beta\}^{(\lambda)} \subseteq \{\alpha \cdot \beta\}_a$ and $B'^p \cdot A \in \{\alpha \cdot \beta\}_a \cap \mathfrak{R}_p$. Hence, $B'^p \cdot (\partial A/\partial z_t) = \partial(B'^p \cdot A)/\partial z_t \in \{\alpha \cdot \beta\}_a$, and $[B'(\partial A/\partial z_t)]^p \in \{\alpha \cdot \beta\}_a$. Therefore, $B'(\partial A/\partial z_t) \in \{\alpha \cdot \beta\}_a$. Repeating appropriately the differentiations $\partial/\partial z_t$, we get at $B'A' \in \{\alpha \cdot \beta\}_a$.

LEMMA 2. *Let* σ *be a subset of* $\mathfrak{R}$, *and* P *an element of* $\mathfrak{R}$. *If* $\{\sigma, P\}_a$ *has a finite basis, then there is a finite subset* α *of* σ *such that* $\{\sigma, P\}_a = \{\alpha, P\}_a$.

Proof. Let β be a finite basis of $\{\sigma, P\}_a$. Then, there is a nonnegative integer λ such that $\beta \subseteq \{\sigma, P\}^{(\lambda)}$. To begin with, suppose $\lambda = 0$. Then $\beta \subseteq (\sigma, P)^{(\mu)}$ for a sufficiently large integer μ[5].

5) If τ is a subset of $\mathfrak{R}$, we define $(\tau)^{(\lambda)}$ ($\lambda = 0, 1, 2, \cdots$) inductively by the rules that 1) $(\tau)^{(0)}$ is the set τ itself and 2) $(\tau)^{(\lambda+1)}$ is the radical indeal of $[(\tau)^{(\lambda)}]$. It is known that $\cup_{\lambda=0}^{\infty}(\tau)^{(\lambda)} = \{\tau\}$.

Suppose $\mu>0$. Then, there exists a nonnegative integer r such that the r-th power of every element of β is contained in $[(\sigma, P)^{(\mu-1)}]$. Hence, a finite subset γ of $(\sigma, P)^{(\mu-1)}$ can be chosen such that the r-th power of every element of β is a linear combination of γ-derivatives over $\mathfrak{R}$. Therefore, $\beta \subseteqq \{\gamma\} \subseteqq \{\sigma, P\}$, and $\{\sigma, P\}_a = \{\beta\}_a \subseteqq \{\gamma\}_a \subseteqq \{\sigma, P\}_a$. Thus $\{\sigma, P\}_a = \{\gamma\}_a$. Hence, we see that, if $\lambda = 0$, μ may be supposed zero and β may be supposed to be a subset of σ, P. If we denote by α the set of all those elements of β which are contained in σ, then $\beta \subseteqq (\alpha, P)^{(0)} \subseteqq (\sigma, P)^{(0)}$, and $\{\sigma, P\}_a = \{\beta\}_a \subseteqq \{\alpha, P\}_a \subseteqq \{\sigma, P\}_a$. Consequently $\{\sigma, P\}_a = \{\alpha, P\}_a$. Now suppose $\lambda>0$. If we prove the existence of a finite subset γ of $\{\sigma, P\}^{(\lambda-1)}$ which is a finite basis of $\{\sigma, P\}_a$, the proof of our lemma is completed. Let τ be the set consisting of $\{\sigma, P\}^{(\lambda-1)}$ and all derivatives for the differentiations $\partial/\partial z_t$ of elements of $\{\sigma, P\}^{(\lambda-1)} \cap \mathfrak{R}_p$. Since $\{\tau\} = \{\sigma, P\}^{(\lambda)}$, there is a nonnegative integer μ such that $\beta \subseteqq (\tau)^{(\mu)}$. Hence, we can prove as above the existence of a finite subset ε of τ such that $\{\varepsilon\}_a = \{\sigma, P\}_a$. The set ε consists of two parts ε_1 and ε_2, where ε_1 is a finite subset of $\{\sigma, P\}^{(\lambda-1)}$ and each element E' of ε_2 is a derivative for the differentiations $\partial/\partial z_t$ of an element $E \in \{\sigma, P\}^{(\lambda-1)} \cap \mathfrak{R}_p$. Let ε_3 be the finite set of all such E, and γ the union of ε_1 and ε_3. Then $\varepsilon \subseteqq \{\gamma\}_a \subseteqq \{\sigma, P\}_a$ and consequently $\{\gamma\}_a = \{\sigma, P\}_a$ with $\gamma \subseteqq \{\sigma, P\}^{(\lambda-1)}$.

LEMMA 3. *Let σ be a subset of $\mathfrak{R}$ and P, Q two elements of $\mathfrak{R}$. If both $\{\sigma, P\}_a$ and $\{\sigma, Q\}_a$ have finite bases, and if $P_1, \cdots, P_r$, $Q_1, \cdots, Q_s$ are elements of σ such that $\{\sigma, P\}_a = \{P_1, \cdots, P_r, P\}_a$ and $\{\sigma, Q\}_a = \{Q_1, \cdots, Q_s, Q\}_a$, then $\{\sigma, PQ\}_a = \{P_1, \cdots, P_r, Q_1, \cdots, Q_s, PQ\}_a$.*

Proof. We see immediately that $\{\sigma, PQ\}_a \subseteqq \{\sigma, P\}_a \cap \{\sigma, Q\}_a = \{P_1, \cdots, P_r, P\}_a \cap \{Q_1, \cdots, Q_s, Q\}_a = \{P_1Q_1, P_1Q_2, \cdots, P_rQ_s, P_1Q, \cdots, P_rQ, PQ_1, \cdots, PQ_s, PQ\}_a$ (by lemma 1) $\subseteqq \{P_0, \cdots, P_r, Q_1, \cdots, Q_s, PQ\}_a$.

3. The decomposision theorem. In this section, we prove the basis theorem, the chain theorem and the decomposition theorem for allowable semiprime differential ideals of $\mathfrak{R} = \mathfrak{F}\{X_1, \cdots, X_n\}$.

THEOREM 1 (Basis theorem). *Every allowable semiprime differential ideal of $\mathfrak{R}$ has a finite basis.*

Proof. We suppose the existence of allowable semiprime differential ideal without finite basis and deduce a contradiction. By Zorn's lemma, there is a maximal such ideal $\mathfrak{m}$. Let $\boldsymbol{A} = (A_1, \cdots, A_r)$ be a modified characteristic set of $\mathfrak{m}$, and S_i, I_i the separant and the initial of $A_i (i=1, \cdots, r)$, and $\mathfrak{F}$ as in § 2. Then, there

exists for every $G \in \mathfrak{m}$ a set of nonnegative integers s_i, t_i such that $S_1^{s_1} \cdots I_r^{t_r} G \equiv 0 \mod [\mathfrak{m} \cap \mathfrak{F}]$. Hence, we get the inclusion $S_1 \cdots S_r I_1 \cdots I_r \mathfrak{m} \subseteq \{\mathfrak{m} \cap \mathfrak{F}\}_a$. While, $\mathfrak{F}$ is the polynomial ring over $\mathfrak{f}$ of a finite number of X-derivatives. Therefore, the ideal $\mathfrak{m} \cap \mathfrak{F}$ in $\mathfrak{F}$ has a finite basis α in the usual sense, and we get at once the equality $\{\mathfrak{m} \cap \mathfrak{F}\}_a = \{\alpha\}_a$.

Now, by the maximality of $\mathfrak{m}$, both $\{\mathfrak{m}, S_i\}_a$ and $\{\mathfrak{m}, I_i\}_a$ have finite basis for each i. Hence, by Lemma 3 of § 2, $\{\mathfrak{m}, S_1 \cdots S_r I_1 \cdots I_r\}_a$ has also a finite basis. By Lemma 2 of § 2, we can choose a finite subset β of $\mathfrak{m}$ such that $\{\mathfrak{m}, S_1 \cdots I_r\}_a = \{S_1 \cdots I_r, \beta\}_a$. We see immediately the inclusions

$$\mathfrak{m}^2 \subseteq \mathfrak{m} \cdot \{\mathfrak{m}, S_1 \cdots I_r\}_a \subseteq \mathfrak{m} \cdot \{S_1 \cdots I_r, \beta\}_a \subseteq \{S_1 \cdots I_r \mathfrak{m}, \mathfrak{m}\beta\}_a \subseteq \{\alpha, \beta\}_a$$

and $\mathfrak{m} \subseteq \{\alpha, \beta\}_a$. Thus, $\mathfrak{m}$ has a finite basis α, β which contradicts to the assumption. q.e.d.

Now, we can easily deduce the following two theorems.

THEOREM 2 (Chain theorem). *Every ascending chain of semi-prime differential ideals of* $\mathfrak{R}$ *contains only a finite number of distinct terms.*

THEOREM 3 (Decomposition theorem). *Every allowable semi-prime differential ideal* $\mathfrak{m}$ *of* $\mathfrak{R}$ *is an intersection of a finite number of allowable prime differential ideals* $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ *of* $\mathfrak{R}$. *If these prime ideals* $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ *are chosen irredundantly, they are uniquely determined by* $\mathfrak{m}$ *up to their order.*

4. Differential dimension. To introduce the theory of dimension, Seidenberg (8) called a quantity x "differentially algebraic" over an ordinary differential field $\mathfrak{f}$ if and only if $\mathfrak{f}\langle x \rangle$ is a finite extension of $\mathfrak{f}$. This definition is appropriate only for ordinary differential field. For partial differential field, it does not cover the notion of being differentially algebraic which has been used in the case of characteristic zero. We shall adopt the following definition.

Definition. A quantity x is called *differentially algebraic* over a differential field $\mathfrak{f}$ if and only if x annihilates a nonzero differential polynomial $G(X)$ over $\mathfrak{f}$. A quantity x is called *differentially S-algebraic* over $\mathfrak{f}$ if and only if x annihilates a differential polynomial $G(X)$ over $\mathfrak{f}$ containing some X-derivative effectively.[6]

6) For the ordinary differential case, our "differentially S-algebraic" implies Seidenberg's "differentially algebraic."

PROPOSITION. *Let x be separable* (in the sense of § 2) *over $\mathfrak{F}$. Then, x is differentially S-algebraic over $\mathfrak{F}$ if and only if it is differentially algebraic over $\mathfrak{F}$.*

Proof. Suppose x differentially algebraic over $\mathfrak{F}$. Then, the set of all differentials polynomials$G(X)$ over $\mathfrak{F}$ with $G(x)=0$ forms a nontrivial allowable prime differential ideal $\mathfrak{p}$. Hence, $\mathfrak{p}$ contains a differential polynomial $G_0(X)$ containing some X-derivative effectively. q.e.d.

We cannot establish in general the theory of dimension with respect to "differentially algebraic", but we can do it with respect to " differentially S-algebraic ", and the notion of dimension in this sense is useful for us. If we agree to call a quantity u *dependent* on a set of quantities $u_1, \cdots, u_n$ when u is differentially S-algebraic over $\mathfrak{F}\langle u_1, \cdots, u_n\rangle$, then it is sufficient for our purpose to prove the following properties:

i) Each u_i is dependent on $u_1, \cdots, u_n$.

ii) If w is dependent on $u_1, \cdots, u_n, v$ and not on $u_1, \cdots, u_n$, then v is dependent on $u_1, \cdots, u_n, w$.

iii) If w is dependent on $v_1, \cdots, v_r$ and if each v_i is dependent on $u_1, \cdots, u_n$, then w is dependent on $u_1, \cdots, u_n$.

Property (i) is trivial. Properties (ii) and (iii) can be proved by modifying the method of Raudenbush (6).

Thus, the concept of *differential dimension* can be established. Now, let $x_1, \cdots, x_n$ be a finite set of quantities which is separable (in the sense of § 2) over a differential field $\mathfrak{F}$. If $\mathfrak{p}$ is the set of all differential polynomials $G(X)$ in $\mathfrak{R}=\mathfrak{F}\{X_1, \cdots, X_n\}$ with $G(X)=0$, then $\mathfrak{p}$ is a nonunit allowable prime differential ideal of $\mathfrak{R}$. Suppose it nonzero ideal. Let $\boldsymbol{A}=(A_1, \cdots, A_t)$ be a modified characteristic set of $\mathfrak{p}$, and U_i the leader of A_i $(i=1, \cdots, t)$. Each U_i is a derivative of some one of the X's; let the number of such X's be s, and $X_{k_1}, \cdots, X_{k_r}$ be the other X's $(r+s=n)$. If we denote by $X^{(\tau)}$ all those X-derivatives which are not U_i-derivatives for any i, then we can conclude that the corresponding x-derivatives $x^{(\tau)}$ are algebraically independent over $\mathfrak{F}$. In fact, assume that $x^{(\tau)}$ are algebraically dependent over $\mathfrak{F}$ and let $G_0(X^{(\tau)})$ be a nonzero polynomial of $X^{(\tau)}$ over $\mathfrak{F}$ which is contained in $\mathfrak{p}$ and whose number of terms is as small as possible, and furthermore whose total degree is as low as possible. Then, G_0 must have the leader and its initial cannot be contained in $\mathfrak{p}$. This contradicts to the definition of $\boldsymbol{A}$.

Therefore, $\mathfrak{F}(x^{(\tau)})$ is purely transcendental over $\mathfrak{F}$, and so is $\mathfrak{F}\langle x_{k_1}, \cdots, x_{k_r}\rangle$. If u_i is the x-derivative corresponding to U_i, then $\mathfrak{F}\langle x_1, \cdots, x_n\rangle = \mathfrak{F}(x^{(\tau)})(u_1, \cdots, u_t)$ and $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is separable algebraic over $\mathfrak{F}(x^{(\tau)})$. $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is differentially algebraic over $\mathfrak{F}\langle x_{k_1}, \cdots, x_{k_r}\rangle$ and we see that r is the differential dimension of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$. As $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is separable over $\mathfrak{F}$ and $\mathfrak{F}\langle x_{k_1}, \cdots, x_{k_r}\rangle$ is purely transcendental over $\mathfrak{F}$, $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is also separable over $\mathfrak{F}\langle x_{k_1}, \cdots, x_{k_r}\rangle$. Thus we have proved:

THEOREM 4. *Let $x_1, \cdots, x_n$ be a finite set of quantities which is separable over a differential field $\mathfrak{F}$ and r the differential dimension of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$. Then, the x_i can be renumbered such that $\mathfrak{F}\langle x_1, \cdots, x_r\rangle$ is purely transcendental over $\mathfrak{F}$ and that $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is separable and differentially algebraic over $\mathfrak{F}\langle x_1, \cdots, x_r\rangle$.*

It is now not difficult to prove:

THEOREM 5. *Let $\mathfrak{p}$ be a nonunit allowable prime differential ideal of $\mathfrak{R}=\mathfrak{F}\{X_1, \cdots, X_n\}$. If the differential dimension r of $\mathfrak{p}$ (i.e. of the generic point of $\mathfrak{p}$ over $\mathfrak{F}$) is positive, and if G is a given differential polynomial nōt contained in $\mathfrak{p}$, then there exists an allowable prime differential ideal of $\mathfrak{R}$ of differential dimension $r-1$ which contains $\mathfrak{p}$ and does not contain G.* (Cf. Seidenberg)

5. The theorem of the primitive element. In this section, we prove the theorem of the primitive element which generalizes the corresponding theorem of Seidenberg (8).

THEOREM 6. *If a differential field $\mathfrak{F}$ has no finite linear basis over the subfield $\mathfrak{F}_0$ of constants, and if u and v are differentially S-algebraic over $\mathfrak{F}$, then there exists an element w in $F\langle u, v\rangle = \mathfrak{F}\langle w\rangle$.*

The theorem can be proved by the two lemmi below, following the lines of Seidenberg's proof.

LEMMA 1.* *Let $\xi_1, \cdots, \xi_s$ be a finite number s of elements of a differential field $\mathfrak{F}$ with m given differentiations $\partial_1, \cdots, \partial_m$. In order that $\xi_1, \cdots, \xi_s$ shall be linearly dependent over the subfield $\mathfrak{F}_0$ of constants, it is necessary and sufficient that the matrix $(\partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i)$ of the ξ-derivatives of total orders $< s$ has a rank $< s$.*

Proof. For $s=1$, the lemma is trivial. Suppose $s>1$ and assume that our lemma is true for $s-1$. We prove only the sufficiency of the condition for s. There exists a nontrivial linear relation

*) It is found in correcting the press that this lemma is already used by Kolchin [Proc. Amer. Math. Soc., vol. 3 (1952)].

$\sum_{i=1}^{s} c_i \partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i = 0$ $(\sum k < s)$ with $c_i \in \mathfrak{F}$. We can suppose that $\xi_1, \cdots, \xi_{s-1}$ are linearly independent over $\mathfrak{F}$ and consequently that $c_s = 1$. For $\sum k < s-1$, we get $0 = \partial_j(\sum_{i=1}^{s} c_i \partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i) = \sum_{i=1}^{s-1} \partial_i c_i \cdot \partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i$ $(j=1, \cdots, m)$. By the induction assumption, we see that $\partial_j c_1 = \cdots = \partial_j c_{s-1} = 0$ $(j=1, \cdots, m)$.

LEMMA 2. *When a nonzero differential polynomial $G(X_1, \cdots, X_n)$ over a differential field $\mathfrak{F}$ is arbitrarily given, we can choose elements $x_1, \cdots, x_n$ of $\mathfrak{F}$ such that $G(X) \neq 0$ if and only if $\mathfrak{F}$ has no finite linear basis over the subfield $\mathfrak{F}_0$ of constants.*

Proof. Suppose that $\mathfrak{F}$ has a finite linear basis $\xi_1, \cdots, \xi_s$ (linearly independent) over $\mathfrak{F}_0$. Let X be a differential indeterminate over $\mathfrak{F}$, and consider the matrix $(\partial_1^{k_1} \cdots \partial_m^{k_m} \xi_1, \cdots, \partial_1^{k_1} \cdots \partial_m^{k_m} \xi_s, \partial_1^{k_1} \cdots \partial_m^{k_m} X)$ $(\sum k < s+1)$. By lemma 1, every minor determinant of degree $s+1$ vanishes if we substitute for X any element of $\mathfrak{F}$. But, since the matrix $(\partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i)$ $(\sum k < s)$ has the rank s, there exists among minor determinants of degree $s+1$ of the former matrix a nonzero differential polynomial of X.

Conversely, suppose that $\mathfrak{F}$ has no finite linear basis over $\mathfrak{F}$. It suffices to prove that, if a nonzero differential polynomial $G(X)$ over $\mathfrak{F}$ of a single indeterminate X is given, we can choose an element $x \in \mathfrak{F}$ such that $G(x) \neq 0$. Let s be the total order of $G(X)$, and take $\xi_0, \xi_1, \cdots, \xi_s \in \mathfrak{F}$ linearly independent over $\mathfrak{F}_0$. We can prove the existence of $c_0, c_1, \cdots, c_s \in \mathfrak{F}_0$ such that $x = \sum_{i=0}^{s} c_i \xi_i$ has the desired property. Assume inductively that there are such constants c_i for every differential polynomial of X over $\mathfrak{F}$ of total order $\leqq s$ and of total degree less than that of G. (For the differential polynomial of total degree zero, the existence of such constants is trivial.)

Suppose that G contains some X-derivative effectively. If $G(x) = G(\sum_i c_i \xi_i) = 0$ were satisfied by every choice of $c_i \in \mathfrak{F}_0$, its formal partial derivatives with respect to c_i would be all zero[7], and we should get

$$\sum_{k_1 + \cdots + k_m \leqq s} \partial G(x) / \partial(\partial_1^{k_1} \cdots \partial_m^{k_m} x) \cdot \partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i = 0 \quad (i = 0, 1, \cdots, s).$$

As the matrix $(\partial_1^{k_1} \cdots \partial_m^{k_m} \xi_i)$ $(\sum k < s+1)$ has the rank $s+1$, $\partial G(x) / \partial(\partial_1^{k_1} \cdots \partial_m^{k_m} x)$ would vanish for all $c_i \in \mathfrak{F}_0$. Thus a con-

7) Notice that $\mathfrak{F}_0$ must have infinitely many elements even when $p \neq 0$: If we take $\eta \in \mathfrak{F}$ such that $\eta \notin \mathfrak{F}_0$, then $\eta^p \in \mathfrak{F}_0$ is nonalgebraic over the prime field.

tradiction to the induction assumption would take place.

Suppose, next, that G is of the form $G=\sum_t w_t G_t^r$ (G_t: differential polynomial of X over $\mathfrak{F}$). As there is a nonzero $G_t(X)$ and G_t is of lesser total degree than G, we choose $c_i \in \mathfrak{F}$ such that $G_t(x) \neq 0$ and consequently $G(x) \neq 0$.

Proof of Theorem 6. Let Λ be a differential indeterminate over $\mathfrak{F}\langle u, v\rangle$. Since u and v are differentially S-algebraic over $\mathfrak{F}\langle\Lambda\rangle$, so is $u+\Lambda v$ over $\mathfrak{F}<\Lambda>$. Hence, there are differential polynomial $P(X;\Lambda)$ over $\mathfrak{F}$ which contain some X-derivative effectively and for which $P(u+\Lambda v;\Lambda)=0$. Let $P(X;\Lambda)$ be such a differential polynomial which is as low as possible in X, and $\delta_1^{k_1}\cdots\delta_m^{k_m}X$ its leader and S its separant. Differentiating $P(u+\Lambda v;\Lambda)=0$ formally in $\delta_1^{k_1}\cdots\delta_m^{k_m}\Lambda$, we get

$$S(u+\Lambda v;\Lambda)\cdot v+Q(u+\Lambda v;\Lambda)=0$$

$$(Q(X;\Lambda)=\partial P(X;\Lambda)/\partial(\delta_1^{k_1}\cdots\delta_m^{k_m}\Lambda)).$$

Since $S(u+\Lambda v;\Lambda)\neq 0$, we see that $v \in \mathfrak{F}\langle\Lambda, u+\Lambda v\rangle$. By the proof of Lemma 2, we see that $\lambda \in \mathfrak{F}$ can be chosen such that $S(u+\lambda v;\lambda)\neq 0$. Therefore, $v \in \mathfrak{F}\langle\lambda, u+\lambda v\rangle=\mathfrak{F}\langle u+\lambda v\rangle$, and $w=u+\lambda v$ has the desired property.

BIBLIOGRAPHY

1. Herz, J.-C., Sur les systemes de polynomes differentiels, Comptes rendus des seances de l'Acad. des Sci., vol. 235 (1952), pp. 1085–1087.

2. Kolchin, E. R., On the basis theorem for differential systems, Trans. of the Amer. Math. Soc., vol. 52 (1942), pp. 115–127.

3. Okugawa, K., On the ring with derivations, Mathematica Japonicae, vol. 1 (1949), pp. 152–163.

4. Okugawa, K., Basis theorem for D-polynomials, Mathematica Japonicae, vol. 2 (1950), pp. 35–39.

5. Okugawa, K., Extensions of the ground field in the theory of algebraic differential equations, Mem. of the College of Sci., Univ. of Kyoto, Ser. A, vol. 27, math. (1953), pp. 257–265.

6. Raudenbush, H. W., Hypertranscendental adjunctions to partial differential fields, Bull. of the Amer. Math. Soc., vol. 40 (1934), pp. 714–720.

7. Ritt, J. F., Differential algebra, Amer. Math. Soc. Coloq. Publ., vol. 33, New York, 1950.

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