ON THE BASIS THEOREM FOR DIFFERENTIAL SYSTEMS

BY

E. R. KOLCHIN

One of the principal points of departure in the study of polynomials and polynomial ideals is the Hilbert basis theorem, which states that every set $\mathfrak{m}$ of polynomials in a finite number of indeterminates contains a finite subset $f_1, \cdots, f_s$ such that

$$\mathfrak{m} \subseteq (f_1 \cdots f_s).$$

As originally proved by Hilbert, this theorem applied to polynomials whose coefficients were either elements of a field, or rational integers. In keeping with the modern tendency toward abstraction, however, one now finds the theorem proved for polynomials whose coefficients are elements of a commutative ring with unit element in which every set has a finite basis.

When one turns to differential polynomials and differential ideals one finds that the exact analogue of the Hilbert theorem is lacking(1). It is not true that every system of differential polynomials Σ contains a finite subset $F_1, \cdots, F_s$ such that

$$\Sigma \subseteq [F_1 \cdots F_s](2).$$

Instead one is forced to choose as a starting point a weakened analogue, the basis theorem of Ritt and Raudenbush. This theorem has been proved for differential polynomials in a finite number of unknowns (indeterminates) $y_1, \cdots, y_n$ with any differential field of characteristic zero as coefficient domain (3), and may be stated in either of the two following equivalent forms:

1. Every system Σ of differential polynomials has a finite subset $F_1, \cdots, F_s$ such that, for each differential polynomial $A \in \Sigma$ there is a positive integer t such that $A^t \in [F_1, \cdots, F_s]$.

2. Every system Σ of differential polynomials has a finite subset $F_1, \cdots, F_s$ such that Σ is contained in the perfect differential ideal generated by $F_1, \cdots, F_s$:

$$\Sigma \subseteq \{F_1 \cdots, F_s\}(4).$$

Presented to the Society, February 22, 1941; received by the editors July 3, 1941.

(1) See J. F. Ritt, *Differential Equations from the Algebraic Standpoint*, American Mathematical Society Colloquium Publications, vol. 14, New York, 1932, pp. 12–13.

(2) Square brackets [ ] are used for differential ideals. Parentheses ( ) denote, as usual, (algebraic) ideals.

(3) See H. W. Raudenbush, these Transactions, vol. 36 (1934), pp. 361–368.

(4) The perfect differential ideal generated by a set is denoted by the set enclosed in braces { }.

That these two statements are equivalent (when the coefficient domain is a differential field of characteristic zero) follows from the fact that the set of all differential polynomials some powers of which are in $[F_1, \cdots, F_s]$ is a perfect differential ideal(5).

It is the object of the present paper to generalize the basis theorem of Ritt and Raudenbush, as the Hilbert basis theorem has been generalized, to permit more general coefficient domains. There is nothing in the literature, for example, which allows treatment of differential polynomials with the set of rational integers, or a differential field of nonvanishing characteristic, as the domain of coefficients.

An easy counterexample shows at the outset that there is no hope of generalizing the first statement of the theorem. In $\mathfrak{I}\{y\}$, the set of all ordinary differential polynomials in y with rational integral coefficients, the system

$$y^p, y_1^p, y_2^p, \cdots$$

where p is any integer greater than 1, is such a counterexample(6). For, no matter what n is, no power of y_{n+1}^p is contained in $[y^p, y_1^p, \cdots, y_n^p]$. This is easy to see since y_{n+1} appears in $[y^p, y_1^p, \cdots, y_n^p]$ only in terms divisible by p or by some y_i^p $(i \leqq n)$.

On the other hand the second statement of the theorem above is susceptible of generalization, although not so wide a one as might be expected at first blush. A finite subset $b_1, \cdots, b_s$ of a subset ϕ of a differential ring $\mathfrak{R}$ is called a basis of ϕ if

$$\phi \subseteq \{b_1, \cdots, b_s\}.$$

If every subset of $\mathfrak{R}$ has a basis we say that the basis theorem holds in $\mathfrak{R}$. Our main theorem asserts that:

If $\mathfrak{R}$ is a commutative differential ring with unit element, in which the basis theorem holds, and if $\mathfrak{R}$ also satisfies a certain condition termed "regularity," then the basis theorem holds in any commutative differential ring $\mathfrak{R}'$ obtained from $\mathfrak{R}$ by a finite number of differential ring adjunctions. An example shows that the regularity condition is not superfluous.

The admittance of more general coefficient domains complicates the structure of perfect differential ideals and makes it desirable to represent, after Raudenbush, the perfect differential ideal $\{\phi\}$ generated by a set ϕ as the set-theoretic limit of a non-decreasing sequence of sets denoted by $\{\phi\}_n$. (See §1.) This permits the classification of some bases as 0-bases, 1-bases, 2-bases, and so on.

This naturally raises the question whether a set which has a basis has an

(5) Raudenbush, loc. cit., p. 363. Raudenbush neglects to state that the differential rings he considers must contain the rational number system.

(6) y_j denotes the jth derivative of y.

m-basis for some m. This question is only partially answered below and still remains for investigation. If every set in a differential ring has an m-basis for some m dependent on the set then we say that the $*$-basis theorem holds in that ring. What we show is that *if the $*$-basis theorem holds in $\mathfrak{R}$ then the $*$-basis theorem holds in $\mathfrak{R}'$* ($\mathfrak{R}$, $\mathfrak{R}'$ as above). Thus we see that every set of differential polynomials in $\mathfrak{I}\{y_1, \cdots, y_n\}$ has an m-basis for some m. However, it is still unknown whether we may put a bound on m. An example shows that any such bound would depend on n.

For the sake of generality the proofs are given for partial differential rings. There is a proof for ordinary differential rings which is materially shorter and simpler, and which is not a specialization of the partial case. For its own interest we present in §11 an outline of this proof.

1. **Perfect differential ideals.** Throughout this paper $\mathfrak{R}$ will denote a commutative (partial) differential ring with r types of differentiation (or derivative operators) $\delta_1, \cdots, \delta_r$.

A differential ideal σ in $\mathfrak{R}$ is called *perfect* if σ contains an element of $\mathfrak{R}$ whenever it contains some power of that element: $a^t \in \sigma$ implies $a \in \sigma$.

Let ϕ be an arbitrary subset of $\mathfrak{R}$. There exists a perfect differential ideal in $\mathfrak{R}$ containing ϕ; for example, $\mathfrak{R}$ itself. The intersection of all perfect differential ideals containing ϕ is itself a perfect differential ideal containing ϕ, and is called the perfect differential ideal generated by ϕ; in symbols, $\{\phi\}$.

To exhibit the structure of $\{\phi\}$ we define by induction:

$\{\phi\}_0 = (\phi)$,

$\{\phi\}_n$ = set of all $a \in \mathfrak{R}$ such that $a^t \in [\{\phi\}_{n-1}]$ for some t, $n = 1, 2, \cdots$.

Each $\{\phi\}_n$ is an ideal. When $n > 0$, $\{\phi\}_n$ contains every element some power of which it contains. Moreover,

$$\{\{\phi\}_m\}_n = \{\phi\}_{m+n}$$

and

$$\phi \subseteq (\phi) = \{\phi\}_0 \subseteq \{\phi\}_1 \subseteq \{\phi\}_2 \subseteq \cdots \subseteq \{\phi\}.$$

The definitions imply that

$$\{\phi\} = \{\phi\}_0 + \{\phi\}_1 + \{\phi\}_2 + \cdots \text{ (7)}.$$

2. **Bases.** A finite subset $b_1, \cdots, b_s$ of $\phi \subseteq \mathfrak{R}$ is called a *basis* of ϕ if

$$\phi \subseteq \{b_1, \cdots, b_s\}.$$

The basis will be called an *m-basis* if

(7) If $\mathfrak{R}$ is a differential ring obtained by the differential ring adjunction of a finite number of unknowns to a differential field of characteristic 0 then $\{\phi\} = \{\phi\}_1$, as is well known. For general $\mathfrak{R}$ this is no longer true. For example, if $\mathfrak{R}$ is the totality of differential polynomials in y with rational integral coefficients, we see, because $y \in \{y^2\}$, that y_1, the derivative of y, is in $\{y^2\}$. Yet $y_1 \notin \{y^2\}_1$ because y_1 appears in $[\{y^2\}_0] = [y^2]$ only in terms which are divisible by y or by 2.

$$\phi \subseteq \{b_1, \cdots, b_s\}_m(^8).$$

One says that *the basis theorem holds in* $\mathfrak{R}$ if every subset of $\mathfrak{R}$ has a basis. If every subset of $\mathfrak{R}$ has an m-basis, with m depending on the subset, then we shall say that *the *-basis theorem holds in* $\mathfrak{R}$. If every subset has an m-basis, with a single m independent of the subset, we shall say that *the m-basis theorem holds in* $\mathfrak{R}$.

The basis theorem of Ritt and Raudenbush mentioned above is seen to be, in our terminology, a 1-basis theorem

3. **A useful result.** Let a be an arbitrary element of $\mathfrak{R}$, ϕ an arbitrary subset of $\mathfrak{R}$. Denote the set of all elements af $(f \in \phi)$ by $a \cdot \phi$.

We shall show that

$$a \cdot \{\phi\}_m \subseteq \{a \cdot \phi\}_m.$$

Indeed, since $\{\phi\}_0 = (\phi)$, the relation in question subsists when $m = 0$. Suppose it holds for $m = k$. Let $f \in \{\phi\}_k$. We show that

$$a^t \delta_1^{i_1} \cdots \delta_r^{i_r} f \in [a \cdot \{\phi\}_k] \subseteq [\{a \cdot \phi\}_k], \qquad t = i_1 + \cdots + i_r + 1.$$

Indeed, since this relation is obvious for $i_1 + \cdots + i_r = 0$ it follows in general from the fact that

$$a^{h+1}\delta_i g = a\delta_i(a^h g) - h a^h g \delta_i a \in [a^h g].$$

Thus, $a \cdot [\{\phi\}_k] \subseteq \{a \cdot \phi\}_{k+1}$. Hence, if $g \in \{\phi\}_{k+1}$, that is, if $g^t \in [\{\phi\}_k]$, then $ag^t \in \{a \cdot \phi\}_{k+1}$, $ag \in \{a \cdot \phi\}_{k+1}$, so that $a \cdot \{\phi\}_{k+1} \subseteq \{a \cdot \phi\}_{k+1}$, q.e.d.

An easy consequence of our result is that

$$\{\phi\}_m \cdot \{\psi\}_n \subseteq \{\phi \cdot \psi\}_{m+n}.$$

4. **Maximal subsets**(9). Let $\mathfrak{M}$ be a collection of subsets of $\mathfrak{R}$ such that every transfinite sequence ϕ_ξ of subsets of $\mathfrak{R}$ in $\mathfrak{M}$ which satisfies the condition

$$\phi_\xi \subset \phi_\eta, \qquad \text{if } \xi < \eta,$$

also satisfies the condition

$$\Sigma \phi_\xi \in \mathfrak{M}.$$

We shall prove that $\mathfrak{M}$ *contains a maximal subset of* $\mathfrak{R}$, that is, a $\phi \in \mathfrak{M}$ such that $\psi \in \mathfrak{M}$ implies $\phi \not\subset \psi$.

Indeed, let ϕ_ξ be a well-ordering of $\mathfrak{M}$. Define by transfinite induction:

$\psi_1 = \phi_1$,

$\psi_\eta =$ the first ϕ_ξ such that $\psi_\nu \subset \phi_\xi$ for all $\nu < \eta$.

By the construction, no ϕ_η properly contains every ψ_η. The resulting transfinite sequence ψ_η must have a last element. For otherwise $\Sigma \psi_\eta$ would be a ϕ_ξ properly containing every ψ_η. This last element is a maximal subset.

(8) Thus, if $m \leqq n$, every m-basis is an n-basis.

(9) In this section $\mathfrak{R}$ may be an abstract set.

5. **Systems of differential polynomials of bounded order.** We suppose henceforth that $\mathfrak{R}$ contains a unit element 1.

Let $y_1, \cdots, y_n$ be unknowns, and let Φ be a set of (partial) differential polynomials, or forms, in $\mathfrak{R}\{y_1, \cdots, y_n\}$ [10] of bounded orders. We shall show that *if the basis (or *-basis) theorem holds in* $\mathfrak{R}$ *then* Φ *has a basis (or m-basis, for some finite m).*

Proof. Because the differential polynomials in Φ are of bounded orders, only a finite number of partial derivatives of the y_i are effectively present in the forms of Φ. Let q be the least integer such that there exists a set Φ, involving only q derivatives of the y_i which has no basis (or m-basis). By the hypothesis on $\mathfrak{R}$, $q>0$. We work toward a contradiction.

If Φ_ξ is a transfinite sequence of sets of differential polynomials in $\mathfrak{R}\{y_1, \cdots, y_n\}$ involving only q derivatives of the y_i such that

$$\Phi_\xi \subset \Phi_\eta, \qquad \text{if } \xi < \eta,$$

no Φ_ξ having a basis (or m-basis), then $\Sigma\Phi_\xi$ involves only q derivatives of the y_i and has no basis (or m-basis). For if $\Sigma\Phi_\xi$ had a basis (or m-basis) there would be a single Φ_ξ which would contain every differential polynomial of the basis, and that Φ_ξ itself would have a basis (or m-basis). Therefore, by §4, there is a maximal set of forms involving only q derivatives of the y_i which has no basis (or m-basis).

Let Φ be such a maximal set. Denote the q partial derivatives of the y_i present in Φ by $\alpha_1, \cdots, \alpha_q$.

It is clear that Φ is an ideal in $\mathfrak{R}[\alpha_1, \cdots, \alpha_q]$, for otherwise the ideal generated by Φ in $\mathfrak{R}[\alpha_1, \cdots, \alpha_q]$ would properly contain Φ, would involve only q derivatives, and would have no basis (or m-basis).

Let Φ' be the set of differential polynomials in Φ which are free of α_q.

If every element of Φ, written as a polynomial in α_q, had each coefficient in Φ', we would have $\Phi \subseteq (\Phi')$, so that Φ would have a basis (or m-basis), because Φ' does. Hence Φ contains a form in which α_q is effectively present and which, when written as a polynomial in α_q, has its leading coefficient not in Φ.

Of all such differential polynomials let

$$B = I\alpha_q^s + \cdots, \qquad I \notin \Phi,$$

be one of minimum degree s in α_q. Then, for each $G \in \Phi$, we have, for suitable t,

$$I^t G \equiv G' (B),$$

where $G' \in \Phi$ has its degree in α_q less than s [11]. By the minimal nature of

[10] $\mathfrak{R}\{y_1, \cdots, y_n\}$ means the ring obtained by the differential ring adjunction of $y_1, \cdots, y_n$ to $\mathfrak{R}$.

[11] Here we use for the first time the fact that $\mathfrak{R}$ contains a unit element.

the degree of B it follows that $G' \in (\Phi')$. But Φ' has a basis (or m_1-basis) $D_1, \cdots, D_u$. Hence $IG \in \{B, D_1, \cdots, D_u\}$ (or $IG \in \{B, D_1, \cdots, D_u\}_{m_1}$).

Now, by the maximality of Φ, (I, Φ) has a basis (or m_2-basis) which we may write as $I, D_{u+1}, \cdots, D_v$, where each $D_i \in \Phi$. Hence, referring to §3,

$$G^2 \in G \cdot (I, \Phi) \subseteq G \cdot \{I, D_{u+1}, \cdots, D_v\}$$
$$\subseteq \{IG, D_{u+1}, \cdots, D_v\} \subseteq \{\{B, D_1, \cdots, D_u\}, D_{u+1}, \cdots, D_v\},$$
$$G \in \{B, D_1, \cdots, D_v\},$$
$$\Phi \subseteq \{B, D_1, \cdots, D_v\}$$

(or, similarly, $\Phi \subseteq \{B, D_1, \cdots, D_v\}_{m_1+m_2}$). This contradiction completes the proof.

6. **Regular differential rings.** A differential ring $\mathfrak{R}$ will be called *regular* if every prime differential ideal $\pi \subseteq \mathfrak{R}$ which contains a prime rational integer p is such that the congruence

$$a \equiv x^p \ (\pi)$$

has a solution $x \in \mathfrak{R}$ for every $a \in \mathfrak{R}$ (that is, if every element has a pth root modulo π).

If $\mathfrak{R}$ is of characteristic $p > 0$ then every ideal contains p and no ideal other than $\mathfrak{R}$ itself contains a prime number different from p.

Examples of regular differential rings are:

1. every differential ring which contains the rational number system;
2. every differential ring with unit element of characteristic $q > 0$ in which each element has a qth root;
3. every perfect ("vollständig") differential field;
4. the differential ring of rational integers.

7. **The basis theorem.** The theorem we shall prove is the following:

Let $\mathfrak{R}$ be a regular commutative differential ring with unit element. Let $\mathfrak{R}'$ be a commutative differential ring obtained from $\mathfrak{R}$ by the differential ring adjunction of a finite number of elements: $\mathfrak{R}' = \mathfrak{R}\{\eta_1, \cdots, \eta_n\}$ [12]. *If the basis (or *-basis) theorem holds in $\mathfrak{R}$ then the basis (or *-basis) theorem holds in $\mathfrak{R}'$.*

It is necessary to prove the theorem only for the case in which the η_i are all unknowns, $\eta_i = y_i$; for if the basis theorem holds in $\mathfrak{R}\{y_1, \cdots, y_n\}$ then it is easy to see that it will continue to hold when any or all of the y_i are replaced by elements among which an algebraic differential relation subsists.

8. **The proof begun.** Assume that there exists in $\mathfrak{R}' = \mathfrak{R}\{y_1, \cdots, y_n\}$ a system which does not have a basis (or m-basis for any m).

If Σ_ξ is a transfinite sequence of such systems with $\Sigma_\xi \subset \Sigma_\eta$ whenever $\xi < \eta$ then the logical sum of the Σ_ξ is again such a system. For if the logical

[12] The η_i may be hypertranscendental over $\mathfrak{R}$ (for example, they may be unknowns) or may satisfy some algebraic differential relation with coefficients in $\mathfrak{R}$.

sum had a basis (or m-basis) then there would be a single Σ_ξ which would contain every form of the basis, and that Σ_ξ itself would have a basis (or m-basis).

By §4 it follows that there is a maximal system which has no basis (or m-basis). We let Σ be such a maximal system and seek a contradiction.

Σ is a differential ideal, for $[\Sigma]$, like Σ, has no basis (or m-basis) and therefore can not properly contain Σ. Moreover, Σ is prime. To prove this, assume to the contrary that $AB \in \Sigma$, $A \notin \Sigma$, $B \notin \Sigma$. Then (Σ, A) and (Σ, B) properly contain Σ and must have bases (or m_1- and m_2-bases, respectively), say $A, C_1, \cdots, C_u$ and $B, C_{u+1}, \cdots, C_v$, respectively, where the C_i are in Σ. Thus

$$\Sigma^2 \subseteq (\Sigma, A)(\Sigma, B) \subseteq \{A, C_1, \cdots, C_u\}\{B, C_{u+1}, \cdots, C_v\} \subseteq \{AB, C_1, \cdots, C_v\},$$

so that $\Sigma \subseteq \{AB, C_1, \cdots, C_v\}$, and Σ has a basis (or, similarly, an (m_1+m_2)-basis).

9. **The proof continued.** The object of this section is to show that Σ contains a prime rational integer p([13]). To accomplish this we introduce a set of differential polynomials analogous to the "basic sets" used by Ritt.

We assume that the partial derivatives of the y_i are completely ordered by a system of marks in such a way that every partial derivative of the y_i is lower than (precedes) every other derivative of the y_i of higher order, and if α and β are two derivatives of the y_i with α lower than β then $\delta_i\alpha$ is lower than $\delta_i\beta$, $i=1, \cdots, r$. Such an ordering can always be effected([14]).

Let $\sigma = \Sigma \cap \mathfrak{R}$. Clearly σ is a prime differential ideal in $\mathfrak{R}$. Since the basis (or $*$-basis) theorem holds in $\mathfrak{R}$, σ has a basis (or m-basis). Hence $\Sigma \neq (\sigma)$ so that Σ must contain forms none of whose coefficients is in σ.

Of all the forms in Σ none of whose coefficients is in σ, consider those with lowest possible leader α_1 (the leader of a form is the highest derivative of the y_i effectively present in the form). Of all those forms let A_1 be one whose degree in α_1 is as low as possible.

Of all the forms in Σ none of whose coefficients is in σ, which do not contain a proper derivative (that is, a derivative of positive order) of α_1, and which are of lower degree in α_1 than A_1, consider those with lowest possible leader α_2. Of all those let A_2 be one whose degree in α_2 is a minimum.

Continuing, at the jth step, consider, of the forms in Σ none of whose coefficients is in σ, which do not contain a proper derivative of α_i $(i=1, \cdots, j-1)$ and which are of lower degree in α_i than A_i $(i=1, \cdots, j-1)$, those forms which have the lowest leader α_j. Of all those forms let A_j be one whose degree in α_j is a minimum.

Since no α_i is a derivative of any preceding α_i, there can be only a finite

([13]) If $\mathfrak{R}$ contained all the rational numbers this would suffice, for then Σ would contain $1 = (1/p) \cdot p$, and would have 1 as a basis.

([14]) Ritt, loc. cit., pp. 141–143.

number of the α_i([15]), so that the process for defining the forms A_i must stop. Let A_s be the last A_i.

It is easy to see that if G is a form in Σ which contains no proper derivative of any α_i and whose degree in each α_i is lower than that of the corresponding A_i, then $G\in(\sigma)$.

Let I_i and S_i be the initial and separant of A_i. The coefficients of I_i are coefficients of A_i and therefore are not in σ. I_i contains no proper derivative of any α_j and is of lower degree in α_j than A_j $(j=1, \cdots, s)$. Hence $I_i\notin\Sigma$.

We shall show that at least one S_i is in Σ.

Let no S_i be in Σ. For an arbitrary form $G\in\Sigma$ there exist integers g_i, h_i such that

$$I_1^{g_1}S_1^{h_1}\cdots I_s^{g_s}S_s^{h_s}G\equiv G'[A_1, \cdots, A_s],$$

where $G'\in\Sigma$ contains no proper derivative of any α_i and is of lower degree in α_i than A_i. Thus, by the above, $G'\in(\sigma)$, so that

$$\begin{aligned} I_1^{g_1}S_1^{h_1}\cdots I_s^{g_s}S_s^{h_s}G &\equiv 0[A_1, \cdots, A_s, \sigma],\\ I_1S_1\cdots I_sS_sG &\in \{A_1, \cdots, A_s, \sigma\}_1,\\ I_1S_1\cdots I_sS_s\cdot\Sigma &\subseteq \{A_1, \cdots, A_s, \sigma\}_1. \end{aligned}$$

Now, Σ is prime and contains no I_i or S_i, so that $I_1S_1\cdots I_sS_s\notin\Sigma$. Hence, by the maximality of Σ, the system

$$\Sigma,\ I_1S_1\cdots I_sS_s$$

has a basis (or m_1-basis) which we may write as

$$I_1S_1\cdots I_sS_s,\ B_1, \cdots, B_t.$$

Denoting by $B_{t+1}, \cdots, B_u$ a basis (or m_2-basis) of σ, we have

$$\begin{aligned} \Sigma^2 &\subseteq \Sigma(\Sigma, I_1S_1\cdots I_sS_s)\subseteq\Sigma\{I_1S_1\cdots I_sS_s, B_1, \cdots, B_t\}\\ &\subseteq \{I_1S_1\cdots I_sS_s\cdot\Sigma, B_1, \cdots, B_t\}\subseteq\{A_1, \cdots, A_s, \sigma, B_1, \cdots, B_t\}\\ &\subseteq \{A_1, \cdots, A_s, B_1, \cdots, B_u\},\\ \Sigma &\subseteq \{A_1, \cdots, A_s, B_1, \cdots, B_u\} \end{aligned}$$

(or, similarly, $\Sigma\subseteq\{A_1, \cdots, A_s, B_1, \cdots, B_u\}_{m_1+m_2+1}$). This contradicts the fact that Σ has no basis (or m-basis) and proves that $S_i\in\Sigma$ for at least one i.

Let S_j be the first S_i contained in Σ. S_j contains no proper derivative of any α_i and is of lower degree in α_i than A_i $(i=1, \cdots, s)$. Hence $S_j\in(\sigma)$. It follows that $n_jI_j\in\Sigma$, where n_j is the degree of A_j in α_j, so that $n_j\in\Sigma$, and one of the prime factors p of n_j must be in Σ. This completes the proof of the result at the beginning of this section.

([15]) Ritt, loc. cit., pp. 135–136.

10. **The proof concluded.** Let F be any nonzero differential polynomial, γ any partial derivative of the y_i. F can be written in one and only one way as a polynomial

$$H_0 + H_1\gamma + \cdots + H_h\gamma^h, \qquad H_h \not\equiv 0,$$

in γ of degree $h<p$, where γ does not appear in the H_i except raised to powers divisible by p. We shall call h the p-degree of F in γ. The highest derivative of the y_i in which F has a positive p-degree (if such a derivative exists) shall be called the p-leader of F. If γ is the p-leader of F and if h is the p-degree of F in γ, we shall call the coefficient of γ^h the p-initial of F, and $\partial F/\partial\gamma$ the p-separant of F.

We shall need the fact that Σ contains a form, none of whose coefficients is in σ, whose p-degree in some derivative of the y_i is positive and whose p-initial is not in Σ. To prove this assume the contrary and let G be a form of Σ, none of whose coefficients is in σ, of least possible (total) degree. Every term of G involves only powers divisible by p, else the p-degree of G in some derivative of the y_i would be positive and the p-initial of G would be a form in Σ, none of whose coefficients is in σ, of lower degree than G. Moreover, by the regularity of $\mathfrak{R}$, the coefficient of each term of G may be replaced modulo σ by the pth power of an element of $\mathfrak{R}$([16]). Since $p\in\sigma$ it follows that $G\equiv H^p\ (\sigma)$, where H is the form obtained from G by replacing each term by its pth root modulo σ. H is of lower degree than G and is in Σ. This contradicts the definition of G and proves the required fact.

Of all the forms of Σ, none of whose coefficients is in σ, which involve derivatives of the y_i to a power not divisible by p and whose p-initials are not in Σ, consider those with lowest p-leader β_1. Of all those forms let B_1 be one whose p-degree in β_1 is as low as possible.

Of all the forms in Σ, none of whose coefficients is in σ, which involve derivatives of the y_i to a power not a multiple of p, whose p-initials are not in Σ, which do not contain a proper derivative of β_1 except raised to a power divisible by p, and which have a p-degree in β_1 less than that of B_1, consider those with lowest possible p-leader β_2. Of all those let B_2 be one whose p-degree in β_2 is a minimum.

Continuing, at the jth step, of all the forms in Σ, none of whose coefficients is in σ, which contain derivatives of the y_i to powers not divisible by p, whose p-initials are not in Σ, which do not contain a proper derivative of β_i except to a power divisible by p $(i=1, \cdots, j-1)$ and which have a p-degree in β_i less than that of B_i $(i=1, \cdots, j-1)$, consider those with lowest p-leader β_j. Of all those forms let B_j be one whose p-degree in β_j is as low as possible.

As with the A_i of §9, the process of defining the B_i must stop after a finite number of steps. Let B_s be the last B_i([17]). Let J_i and T_i be the p-initial and p-separant, respectively, of B_i.

([16]) Up to this point we have not used the regularity. Henceforth it will be important.

([17]) The s here is not necessarily the same as that of §9.

If G is a form of Σ, none of whose coefficients is in σ, which contains no proper derivative of any β_i except raised to powers divisible by p and whose p-degree in each β_i is less than that of the corresponding B_i, then either G contains no derivative of the y_i that is raised to a power not divisible by p, or the p-initial of G is in Σ.

From this it can be shown that the T_i are not contained in Σ. We already know that the I_i are not in Σ.

Let α represent the highest derivative of the y_i effectively present in $B_1, \cdots, B_s$([18]). Let Σ_α denote the totality of forms in Σ which contain no derivative of the y_i which is higher than α. The forms of Σ_α are of bounded order.

We shall show that for each differential polynomial $G \in \Sigma$ there exist non-negative integers e_i, f_i such that

$$J_1^{e_1} T_1^{f_1} \cdots J_s^{e_s} T_s^{f_s} G \equiv 0 [\Sigma_\alpha].$$

Assume that this is not so. If G is a form in Σ for which such a congruence fails to hold it is easy to see that there is a relation

$$J_1^{g_1} T_1^{h_1} \cdots J_s^{g_s} T_s^{h_s} G \equiv G' [B_1, \cdots, B_s],$$

where G' is a form in Σ for which such a congruence fails to hold, which contains no proper derivative of any β_i except to a power divisible by p, and which has, in each β_i, a p-degree lower than that of the corresponding B_i. Of all forms in Σ which fail to satisfy a congruence as above, which contain no proper derivative of any β_i except to a power divisible p, and which have, in each β_i, a p-degree lower than that of the corresponding B_i, consider those with the least number of terms. Of all those forms let G be one with a minimum (total) degree. Since $\sigma \subseteq \Sigma_\alpha$, no coefficient of G is in σ. Hence, either G contains only powers divisible by p or the p-initial of G is in Σ. Suppose G contains only powers divisible by p. By the regularity of $\mathfrak{R}$, each coefficient of G may be replaced modulo σ by the pth power of an element of $\mathfrak{R}$. Hence $G \equiv H^p$ (σ), where $H \in \Sigma$, having the same number of terms as G and being of lower degree than G, satisfies a congruence as above. But this is impossible as then G would satisfy such a congruence. Thus G has a p-leader γ and the p-initial of G is in Σ:

$$G = K_0 + \cdots + K_g \gamma^g, \qquad K_g \in \Sigma.$$

Since K_g is of lower degree than G, K_g satisfies a congruence of the type in question. But $K_0 + \cdots + K_{g-1} \gamma^{g-1}$, which is in Σ and has fewer terms than G, must also satisfy such a congruence. This is impossible, however, for it implies that G itself satisfies the same kind of congruence.

Thus we have shown that

([18]) α may be higher than β_s as the p-degree of each B_i in α may be 0.

$$J_1T_1 \cdots J_sT_s \cdot \Sigma \subseteq \{\Sigma_\alpha\}_1.$$

Now, by the result of §5, Σ_α has a basis (or m_1-basis), say $D_1, \cdots, D_t$. Also, by the maximality of Σ, the system

$$\Sigma,\ J_1T_1 \cdots J_sT_s$$

has a basis (or m_2-basis) which we may write as

$$J_1T_1 \cdots J_sT_s,\ D_{t+1}, \cdots, D_u \qquad D_i \in \Sigma.$$

Hence, by §3,

$$\begin{aligned}\Sigma^2 &\subseteq \Sigma(\Sigma, J_1T_1 \cdots J_sT_s) \subseteq \Sigma\{J_1T_1 \cdots J_sT_s, D_{t+1}, \cdots, D_u\} \\ &\subseteq \{J_1T_1 \cdots J_sT_s \cdot \Sigma, D_{t+1}, \cdots, D_u\} \subseteq \{D_1, \cdots, D_u\}, \\ \Sigma &\subseteq \{D_1, \cdots, D_u\}\end{aligned}$$

(or, similarly, $\Sigma \subseteq \{D_1, \cdots, D_u\}_{m_1+m_2+1}$). This contradiction completes the proof of the theorem stated in §7.

11. **Shorter proof in the ordinary case.** We sketch in this section a shorter proof of the theorem under the assumption that we are dealing with *ordinary* differential rings, that is, differential rings with one type of differentiation.

Denote the jth derivative of any letter u by u_j.

Of the above proof we take over §§1–6.

We first show that, when the basis (or *-basis) theorem holds in $\mathfrak{R}$ and $\mathfrak{R}$ is regular, the basis (or *-basis) theorem holds in $\mathfrak{R}\{y\}$. Assuming the contrary we obtain, as in §8, a maximal system $\Sigma \subset \mathfrak{R}\{y\}$ which has no basis (or m-basis). Σ is a prime differential ideal. If F were a form in Σ whose separant S was not in Σ, $S \cdot \Sigma$ would have a basis (or m_1-basis), $B_1, \cdots, B_s$, for which we could write, for each $G \in \Sigma$, $S^qG \equiv G'[F]$, with G' of order no higher than that of F, so that we would have $S \cdot \Sigma \subseteq \{\Sigma'\}$, where Σ' is the set of forms of Σ whose orders are less than or equal to the order of F. Also, by the maximality of Σ, the system Σ, S would have a basis (or m_2-basis), say $S, B_{s+1}, \cdots, B_t$. Thus we would have

$$\begin{aligned}\Sigma^2 &\subseteq \Sigma(\Sigma, S) \subseteq \Sigma\{S, B_{s+1}, \cdots, B_t\} \\ &\subseteq \{S \cdot \Sigma, B_{s+1}, \cdots, B_t\} \subseteq \{B_1, \cdots, B_t\}, \\ \Sigma &\subseteq \{B_1, \cdots, B_t\}\end{aligned}$$

(or, similarly, $\Sigma \subseteq \{B_1, \cdots, B_t\}_{m_1+m_2}$). This cannot be, so that every form in Σ must have its separant in Σ.

Of all forms in Σ none of whose coefficients is in Σ let A be one whose (total) degree is a minimum. Since S, the separant of A, is of lower degree than A, all the coefficients of S must be in Σ. These coefficients are coefficients of A multiplied by the exponents to which y_q appears in A. (Here q is the order of A.) Since Σ is prime and the coefficients of A are not in Σ,

these exponents must be in Σ. These exponents have a common prime factor $p \in \Sigma$, and we see that y_q appears in A only to powers divisible by p. It is now easy to see that every derivative of y appears in A only to powers divisible by p; for suppose y_j is the y_i of highest subscript which appears in A to a power not a multiple of p. Then the $(q-j+1)$st derivative of A would be, terms divisible by p neglected, a form in Σ whose separant is not in Σ, an impossibility.

Now, by the regularity of $\mathfrak{R}$, we may replace modulo Σ each coefficient of A by the pth power of an element of $\mathfrak{R}$. Hence $A \equiv B^p(\Sigma)$, where $B \in \Sigma$ has no coefficient in Σ and is of lower degree than A. This completes the proof for $\mathfrak{R}\{y\}$.

Proceeding by induction, suppose the theorem has been proved for $\mathfrak{R}\{y_1, \cdots, y_{n-1}\}$ [19]. As above, we find, for a maximal system $\Sigma \subset \mathfrak{R}\{y_1, \cdots, y_n\}$, that the separant of each form of Σ must itself be in Σ. This must be true no matter how we order the unknowns. Letting A be a form in Σ, with no coefficients in Σ, of minimum degree, we see from the above that each y_{ij} appears in A only to powers divisible by a prime rational integer $p \in \Sigma$. As in the case of one unknown this leads to a contradiction and completes the proof.

12. **Examples.** From the point of view of analogy with the Hilbert basis theorem, it might be imagined that the regularity condition imposed in the basis theorem above is unnecessary. The following example shows that this is not so.

EXAMPLE 1. Let $\mathfrak{R}$ be the ordinary differential field of characteristic $p>0$ obtained from the field of rational integers modulo p by the differential field adjunction of the set of "indeterminate constants" $c_0, c_1, c_2, \cdots$, that is, each c_i is a letter whose derivative is taken to be 0, and $\mathfrak{R} = \mathfrak{I}_p\langle c_0, c_1, c_2, \cdots \rangle$. Let y be an unknown and consider, in $\mathfrak{R}\{y\}$, the system Φ:

$$y^p + c_0,\ y_1^p + c_1,\ \cdots,\ y_k^p + c_k,\ \cdots.$$

We shall show that Φ *has no basis.*

Indeed, if Φ had a basis we should have, for some k,

$$y_k^p + c_k \in \{y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}\}.$$

Now, $(y_i^p + c_i)_1 = p y_i^{p-1} y_{i+1} + c_{i1} = 0$, so that

$$[y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}] = (y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}).$$

But clearly $AB \in (y^p + c_0, \cdots, y_{k-1}^p + c_{k-1})$ implies that A or $B \in (y^p + c_0, \cdots, y_{k-1}^p + c_{k-1})$. Hence $(y^p + c_0, \cdots, y_{k-1}^p + c_{k-1})$ is a prime differential ideal, so that

$$\{y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}\} = (y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}).$$

[19] The y_i are unknowns. The jth derivative of y_i is denoted by y_{ij}.

But it is easy to verify that

$$y_k^p + c_k \notin (y^p + c_0, \cdots, y_{k-1}^p + c_{k-1}).$$

Let $\mathfrak{Z}$ be the ordinary differential ring of rational integers. Let $n = 2^{m-1}$, where m is any positive integer. The following example shows that the m-basis theorem does not hold in $\mathfrak{Z}\{y_1, \cdots, y_n\}$.

EXAMPLE 2. Let Φ be the system in $\mathfrak{Z}\{y_1, \cdots, y_n\}$ consisting of the forms

$$y_1^2 \cdots y_n^2,\ y_{11}^2 \cdots y_{n1}^2, \cdots, y_{1k}^2 \cdots y_{nk}^2, \cdots.$$

Φ has no m-basis.

To prove this assume the contrary. Then, for some k,

$$\begin{aligned} y_{1k}^2 \cdots y_{n'k}^2 &\in \{y_1^2 \cdots y_{n'}^2, \cdots, y_{1,k-1}^2 \cdots y_{n',k-1}^2\}_m \\ &\subseteq \{2, y_1 \cdots y_{n'}, \cdots, y_{1,k-1} \cdots y_{n',k-1}\}_{m-1}, \\ y_{1k} \cdots y_{n'k} &\in \{2, y_1 \cdots y_{n'}, \cdots, y_{1,k-1} \cdots y_{n',k-1}\}_{m-1}. \end{aligned}$$

Letting $y_1 = y_2 = z_1$, $y_3 = y_4 = z_2$, $\cdots$, $y_{n-1} = y_n = z_{n'}$, where $n' = n/2 = 2^{m-2}$, we see, in the differential ring $\mathfrak{R}\{z_1, \cdots, z_{n'}\}$, that

$$\begin{aligned} z_{1k}^2 \cdots z_{n'k}^2 &\in \{2, z_1^2 \cdots z_{n'}^2, \cdots, z_{1,k-1}^2 \cdots z_{n',k-1}^2\}_{m-1} \\ &\subseteq \{2, z_1 \cdots z_{n'}, \cdots, z_{1,k-1} \cdots z_{n',k-1}\}_{m-2}, \\ z_{1k} \cdots z_{n'k} &\in \{2, z_1 \cdots z_{n'}, \cdots, z_{1,k-1} \cdots z_{n',k-1}\}_{m-2}. \end{aligned}$$

Continuing, at each step we reduce the number of unknowns by one half until we arrive, in $\mathfrak{R}\{u_1\}$, at the relation

$$u_{1k} \in \{2, u_1, \cdots, u_{1,k-1}\}_0 = (2, u_1, \cdots, u_{1,k-1}).$$

This contradiction completes the proof.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.