ON THE BASIS THEOREM FOR INFINITE SYSTEMS OF DIFFERENTIAL POLYNOMIALS*

E. R. KOLCHIN

Introduction. Let $\mathcal{J}$ be a differential field of characteristic zero.† We consider an infinite system Σ of differential polynomials in the letters $y_1, \cdots, y_n$, the coefficients of the differential polynomials being in $\mathcal{J}$.‡

A finite set Φ of forms in Σ is called a *basis* of Σ if, for every form G in Σ, there is a positive integer p, dependent on G, such that G^p is in the differential ideal of Φ. If a single p will serve for every G in Σ, then we shall call the basis *strong*.

It has been shown that every system has a basis.§ Raudenbush has shown further,‖ that there exist systems, not every basis of which is strong. It is now natural to ask whether or not every system of forms contains at least one strong basis.

We answer this question in the negative by showing that even a perfect differential ideal of forms may have no strong basis. The perfect differential ideal with which we work is the one generated by the form uv in the two unknowns u, v.

We employ several ideas used by Raudenbush in the second of his above mentioned papers.

1. **The assumption.** Consider a form¶ G every term of which is divisible by some u_iv_j.** Let Σ be the set of all such forms G. Then Σ is a differential ideal, and is perfect. For, if a form has a term free of, say, every u_i, then every power of the form will have such a term.

* Presented to the Society, February 25, 1939.

† For the definition of differential field, and other terms, see H. W. Raudenbush, *Ideal theory and differential equations*, Transactions of this Society, vol. 36 (1934), pp. 361–368.

‡ Throughout the rest of this paper we shall use, as is customary, the term *form* for *differential polynomial*.

§ For differential fields of meromorphic functions this was essentially shown by J. F. Ritt in his book *Differential Equations from the Algebraic Standpoint*, American Mathematical Society Colloquium Publications, vol. 14, New York, 1932. See especially §§ 7, 77. Following the work of Ritt, Raudenbush treated the case of the general differential field of characteristic zero by purely algebraic methods. See Raudenbush, loc. cit.

‖ *On the analog for differential equations of the Hilbert-Netto theorem*, this Bulletin, vol. 42 (1936), pp. 371–373.

¶ For $\mathcal{J}$ we can use any differential field of characteristic zero.

** Subscripts denote derivatives.

It is easy to see that Σ is the perfect differential ideal generated by uv.

If Σ has a strong basis, then it has one consisting purely of forms u_iv_j.

Let

$$(1) \qquad u_iv_j, \qquad i + j \leqq s,$$

be a strong basis for Σ, and let p be the associated positive integer. We work toward a contradiction.

We denote by α a positive integer to be fixed later.

Consider the set of all forms

$$(2) \qquad u_{i_1}v_{j_1} \cdots u_{i_p}v_{j_p}, \qquad i_1 + j_1 + \cdots + i_p + j_p = \alpha.$$

Every such form has an expression $\sum_{g=1}^{r} c_g(\sum_{h=1}^{p} a_{gh}u_{i_h}v_{j_h})^p$, where r is some positive integer, and the c_g and the a_{gh} are rational numbers.* Therefore, by our assumption on the nature of the basis (1) and the integer p, every form (2) is in the differential ideal generated by the forms (1).

Hence each form (2) is a linear combination, with coefficients in F, of forms

$$(3) \qquad \begin{gathered} (u_iv_j)_k u_{i_1}v_{j_1} \cdots u_{i_{p-1}}v_{j_{p-1}}, \\ i + j \leqq s, \; i + j + k + i_1 + j_1 + \cdots + i_{p-1} + j_{p-1} = \alpha. \end{gathered}$$

Since the forms (2) are all linearly independent over $\mathcal{J}$, it follows that the number of distinct forms (2) cannot exceed the number of distinct forms (3).

We denote the number of distinct forms (2) by $R_{p,\alpha}$, and the number of distinct forms (3) by $Q_{p,\alpha}$. We thus have $R_{p,\alpha} \leqq Q_{p,\alpha}$.

In the next section we force the contradiction that $R_{p,\alpha} > Q_{p,\alpha}$ for α sufficiently large.

2. **The contradiction.** We consider those expressions (2) for which $i_1+j_1=\nu$, $(0 \leqq \nu \leqq \alpha)$. The coefficient of $u_{i_1}v_{j_1}$ in (2) is then

$$(4) \qquad u_{i_2}v_{j_2} \cdots u_{i_p}v_{j_p}, \qquad i_2 + j_2 + \cdots + i_p + j_p = \alpha - \nu.$$

The number of distinct forms (4) is $R_{p-1,\alpha-\nu}$, and therefore the number of distinct symbols† (4) is not less than $R_{p-1,\alpha-\nu}$. Since the number of expressions $u_{i_1}v_{j_1}$ with $i_1+j_1=\nu$ is $\nu+1$, the total number of sym-

* We can solve the equations $(w_1+\lambda w_2)^t = \sum_{i=0}^{t} C_{t,i}\lambda^i w_1^{t-i}w_2^i$, $(\lambda = 1, \cdots, t+1)$, for $w_1w_2^{t-1}$, obtaining $w_1w_2^{t-1} = \sum_{\lambda=1}^{t+1} d_\lambda(w_1+\lambda w_2)^t$. Using this special case, we can show by induction that $w_1 \cdots w_p = \sum_{g=1}^{r} c_g(\sum_{h=1}^{p} a_{gh}w_h)^p$. Setting $w_h = u_{i_h}v_{j_h}$, we obtain the desired representation of the forms (2).

† Two distinct symbols (4) may represent the same form.

bols (2) is not less than $\sum_{\nu=0}^{\alpha}(\nu+1)R_{p-1,\alpha-\nu}$. But not more than $(p!)^2$ distinct symbols (2) can represent the same form. Hence

$$R_{p,\alpha} \geqq (p!)^{-2}\sum_{\nu=0}^{\alpha}(\nu+1)R_{p-1,\alpha-\nu}. \tag{5}$$

We now show that there exist positive numbers b_p, $(p=1, 2, \cdots)$, independent of α, such that

$$R_{p,\alpha} \geqq b_p(\alpha+1)^{2p-1}. \tag{6}$$

Obviously $R_{1,\alpha}=\alpha+1$, so that (6) holds for $p=1$. Suppose (6) holds for $p=m-1$. Then, by (5), using $[x]$ to denote the greatest integer not exceeding x, we have

$$\begin{aligned} R_{m,\alpha} &\geqq (m!)^{-2}\sum_{\nu=0}^{\alpha}(\nu+1)b_{m-1}(\alpha-\nu+1)^{2m-3} \\ &\geqq (m!)^{-2}b_{m-1}\sum_{\nu=[\alpha/4]}^{[3\alpha/4]}(\nu+1)(\alpha-\nu+1)^{2m-3} \\ &\geqq (m!)^{-2}b_{m-1}\sum_{\nu=[\alpha/4]}^{[3\alpha/4]}([\alpha/4]+1)(\alpha/4+1)^{2m-3} \\ &\geqq (m!)^{-2}b_{m-1}(2[\alpha/4]+1)([\alpha/4]+1)(\alpha/4+1)^{2m-3} \\ &\geqq b_m(\alpha+1)^{2m-1}, \end{aligned}$$

where $b_m=(m!)^{-2}4^{-2m}b_{m-1}$. Thus (6) holds for all p.

We now consider those expressions (3) for which $i+j+k=\mu$, $(0\leqq\mu\leqq\alpha)$. The number of distinct expressions $(u_iv_j)_k$ with $i+j+k=\mu$ and with $i+j\leqq s$ does not exceed $(s+1)^2$. The coefficient of $(u_iv_j)_k$ in (3) is $u_{i_1}v_{j_1}\cdots u_{i_{p-1}}v_{j_{p-1}}$, $(i_1+j_1+\cdots+i_{p-1}+j_{p-1}=\alpha-\mu)$. Since the number of distinct forms of this kind is $R_{p-1,\alpha-\mu}$, we have for the total number of distinct forms (3):

$$Q_{p,\alpha} \leqq \sum_{\mu=0}^{\alpha}(s+1)^2R_{p-1,\alpha-\mu}. \tag{7}$$

We shall show that, for $p=1, 2, \cdots$,

$$R_{p,\alpha} \leqq (\alpha+1)^{2p-1}. \tag{8}$$

For since $R_{1,\alpha}=\alpha+1$, (8) holds for $p=1$. Suppose (8) holds for $p=m-1$. Looking at (2), it is easy to see that

$$R_{m,\alpha} \leqq \sum_{\nu=0}^{\alpha}(\nu+1)R_{m-1,\alpha-\nu}.$$

Therefore

$$R_{m,\alpha} \leqq \sum_{\nu=0}^{\alpha} (\nu + 1)(\alpha - \nu + 1)^{2m-3}$$

$$\leqq \sum_{\nu=0}^{\alpha} (\alpha + 1)(\alpha + 1)^{2m-3} = (\alpha + 1)^{2m-1}.$$

Thus (8) holds for all p.

Using (8) in (7), we find

$$Q_{p,\alpha} \leqq (s + 1)^2 \sum_{\mu=0}^{\alpha} (\alpha - \mu + 1)^{2p-3},$$

so that

$$Q_{p,\alpha} \leqq (s + 1)^2(\alpha + 1)^{2p-2}.$$

Comparing this with (6), we see that, for α sufficiently large, $R_{p,\alpha} > Q_{p,\alpha}$.

COLUMBIA UNIVERSITY