MANIFOLDS OF DIFFERENCE POLYNOMIALS

BY

RICHARD M. COHN

INTRODUCTION

1. It is the purpose of this paper to develop in some detail the structure of the manifolds determined by systems of difference polynomials. Our results will necessarily be confined to the case of polynomials in an abstract field, since a suitable existence theorem for analytic difference equations is not available. The ideal theory, developed by J. F. Ritt and H. W. Raudenbush(1) for abstract systems of difference polynomials, is therefore fundamental in our work.

2. In Part I of our paper we describe a theoretical method for elimination of unknowns in systems of algebraic difference equations. We employ this method to prove analogues for difference fields of fundamental theorems of algebra on field extensions. With the aid of these results we show in Theorem III that the number of arbitrary(2) unknowns in a prime difference ideal is constant for all possible choices of sets of arbitrary unknowns.

3. Part II is concerned with the manifold of a single algebraically irreducible difference polynomial in an abstract field. A factorization process for polynomials in analytic fields was developed by J. F. Ritt(3) in determinining the maximum number of irreducible manifolds, not held by polynomials of zero order, in the decomposition of the manifold of a first order difference polynomial. In Theorem IV we show that, when the Ritt factorization process is applied to a polynomial A in an abstract field, each of the polynomial sequences it produces actually determines a prime ideal held by A but not by any polynomial of lower order than A. Furthermore, all such prime ideals are obtained in this way. This constitutes a form of existence theorem for difference polynomials in abstract fields, and is fundamental in the further development of the theory.

The irreducible manifolds of A determined by the factorization process we call the general solution of A. We shall see that, if A is of first order, all solutions are included in the general solution. This result confirms, in a gen-

---

Presented to the Society, April 17, 1948; received by the editors May 17, 1947.

(1) J. F. Ritt and H. W. Raudenbush, Jr., *Ideal theory and algebraic difference equations*, Trans. Amer. Math. Soc. vol. 46 (1939) pp. 445–452. This paper will be designated below by R.

(2) We use this term in the same sense in which it is employed in the theory of algebraic differential equations. A formal definition is given in §13.

(3) J. F. Ritt, *Algebraic difference equations*, Bull. Amer. Math. Soc. vol. 40 (1934) pp. 303–308.

eral way, the heuristic statements of Boole(4) concerning first order difference polynomials. However, a simple example will be given to show that polynomials of higher order may have solutions not included in the general solution and therefore constituting essential singular manifolds similar to those familiar in the theory of algebraic differential equations. The structure of these manifolds awaits exploration.

Finally Part II presents certain detailed information concerning the basic sets of the general solution and provides a constructive method for determining whether or not a given polynomial holds the general solution. Examples are given illustrating the possible complexity of structure of the general solution.

4. In Part III we return to consideration of more general systems in abstract fields. Theorem IX is a general result on the nature of the basic sets of reflexive prime ideals. In combination with the results of Part I this theorem leads to a complete description of the dimensionality of such systems.

We return to the elimination problem and construct a form of resolvent system for prime difference ideals. The unknowns of the ideal are determined uniquely in terms of the solutions of the resolvent system. Peculiarly, the uniqueness does not imply that the unknowns of the ideal may be determined from the resolvent unknown by means of linear equations. Rather, we have, in general, a system of zero order equations, not necessarily of first degree, in combination with difference polynomials of higher order. Systems of this sort, having unique solutions, we term quasi-linear(5).

5. We take our notation and nomenclature from R and from the paper *Complete difference ideals*(6), with additions explained in the context. We follow the latter paper in distinguishing as reflexive those difference ideals which contain a polynomial A if they contain its transform, and dropping this requirement from the definition of difference ideal. We shall not employ a functional notation such as $y(x)$, $y(x+1)$ to denote an unknown and its transforms. Unknowns will be denoted by lower case letters and polynomials by upper case letters. Subscripts, when other meanings are not specifically assigned to them, indicate a transform of order equal to the subscript.

It will always be assumed that there is an underlying difference field which contains the coefficients of the polynomials under discussion. We consider only fields of characteristic zero.

We shall make constant use of the theory of systems of algebraic equations in the form presented by J. F. Ritt in chap. IV of his book *Differential equations from the algebraic standpoint*(7). In particular we require the theorem stated in §45 of that work with the obvious adaptations necessary for applica-

(4) Boole, *Calculus of finite differences*, 3d ed., 1880, chap. X, particularly article 21.

(5) This terminology was suggested by J. F. Ritt.

(6) J. F. Ritt, Amer. J. Math. vol. 63 (1941) p. 681.

(7) Amer. Math. Soc. Colloquium Publications, vol. 14. (Designated hereafter by A.D.E.)

tion to abstract fields(8). We conclude, from this theorem and its proof, that if $A_1, \cdots, A_n$ is an ascending set of algebraic polynomials which possesses a regular solution, but which is not the basic set of a prime ideal, an equation,

$$I_1^{\mu_1} I_2^{\mu_2} \cdots I_{k-1}^{\mu_{k-1}} [TA_k - G_1 G_2 \cdots G_r] = L_1 A_1 + L_2 A_2 + \cdots + L_{k-1} A_{k-1},$$

holds for some $k \leqq n$. The G_i are here polynomials reduced with respect to $A_1, \cdots, A_k$, T a polynomial of class lower than A_k, and reduced with respect to $A_1, \cdots, A_{k-1}$, the L_i polynomials of class not exceeding A_k, and the μ_i integers.

The reader should note that many common terms, such as "polynomial," "ascending set," "reduced," are required both in their algebraic sense, as they are employed in chap. IV of A.D.E., and in the sense of the theory of difference polynomials. Wherever necessary to avoid confusion we have used the adjective "algebraic" to distinguish the former of the two meanings. It should also be noted that a given field, polynomial, or system of polynomials is sometimes spoken of in terms of its purely algebraic properties, sometimes in terms of these properties and the transforming operation. We have not thought it desirable to employ separate symbols for the same entity in each of these connotations.

Part I. Extensions of difference fields

6. We shall say that an element t is *transformally algebraic*(9) over a difference field $\mathcal{J}$ if t annuls a nonzero difference polynomial with coefficients in $\mathcal{J}$. If t is not transformally algebraic we say it is *transformally transcendental.* We prove the following lemma:

Let an extension $\mathcal{K}$ of a field $\mathcal{J}$ be formed by adjoining to $\mathcal{J}$ a set of elements a_i each of which is transformally algebraic over $\mathcal{J}$. Let t be transformally algebraic over $\mathcal{K}$. Then t is transformally algebraic over $\mathcal{J}$.

There exists a nonzero polynomial B in an unknown z with coefficients in $\mathcal{K}$, which is annulled when z is replaced by t. The coefficients of B are rational combinations with coefficients in $\mathcal{J}$ of the transforms of a finite number of elements of the set a_i. We represent these elements by $b_1, b_2, \cdots, b_s$. If we replace each b_i in B by y_i we obtain a polynomial B' in z with coefficients which

(8) The solutions defined in this theorem become, in the abstract case, algebraic functions of $u_1, u_2, \cdots, u_q$, or what is the same thing, elements of an algebraic extension of $\mathcal{J}(u_1, \cdots, u_q)$, where $\mathcal{J}$ is the coefficient field. The necessity proof may be adopted without essential alteration. In the proof of sufficiency (§48 of A.D.E.) we do not, of course, form solutions for the particular values of the u_i. We merely observe that the polynomial $G_1 H_1$ of A.D.E. becomes, after substitution of the solutions, a zero element in an extension of $\mathcal{J}(u_1, \cdots, u_q)$. Then either G_1 or H_1 must be a zero element, and the proof continues as in A.D.E.

(9) We parallel here a terminology suggested by E. R. Kolchin for differential fields. The old term "algebraically transcendental" does not permit of distinction between difference and differential fields. See Kolchin, *Extensions of differential fields*, II, Ann. of Math. (2) vol. 45 (1944).

are rational combinations of the y_i and their transforms. Let B' be multiplied by the least common denominator of its coefficients. There results a polynomial C in unknowns $y_1, y_2, \cdots, y_s; z$, whose coefficients are in $\mathcal{J}$.

Let Λ be the prime reflexive difference ideal consisting of all difference polynomials in the unknowns $y_1, y_2, \cdots, y_s; z$, with coefficients in $\mathcal{J}$, which are annulled when each y_i is replaced by b_i, and z is replaced by t. Evidently the polynomial C is in Λ. Since the b_i are transformally algebraic over $\mathcal{J}$, Λ contains a nonzero polynomial in each y_i separately. Our lemma will follow immediately if we can show that Λ contains a nonzero polynomial in z alone.

7. For this purpose we shall select a sequence of finite systems of polynomials of Λ, to be called cycles of Λ, which we proceed to describe. In forming the cycles we shall deal at any one time with a finite number of the transforms y_{ij} of the y_i, and z_i of z. We shall treat these transforms as variables in the sense of algebra and adopt various conventions for ordering them as we proceed. We now describe the construction of the first cycle.

We shall be concerned only with y_{ij} at this stage, and we shall order them so that y_{ij} precedes y_{kl} if $i<k$, or if $i=k$ and $j<l$. We know that Λ contains nonzero polynomials in the y_{1j} only. The first polynomial $A_1^{(1)}$ of the first cycle is chosen to be a polynomial of lowest rank([10]) among all such polynomials.

Λ is held by a polynomial in the y_{2j} alone, and therefore reduced, in the algebraic sense, with respect to the first polynomial of the cycle. Of all polynomials in the y_{1j} and y_{2j}, effectively involving y_{20} or some transform of y_{20}, reduced with respect to the first polynomial of the cycle, and involving no transform of y_{10} higher than those occurring in the first polynomial of the cycle, we choose one which is algebraically lowest for the second polynomial $A_2^{(1)}$ of the cycle. We note that the initial of $A_2^{(1)}$ is lower than $A_2^{(1)}$, and reduced with respect to $A_1^{(1)}$, and so does not hold Λ. Observing now that Λ is held by a polynomial in y_3 alone, we select a lowest polynomial $A_3^{(1)}$ of Λ which is algebraically reduced with respect to the ascending set $A_1^{(1)}$, $A_2^{(1)}$, effectively involves transforms of y_3, but of no y_i with $i>3$, and does not involve any transform of y_1 or y_2 higher than those occurring in $A_1^{(1)}$, $A_2^{(1)}$. The initial of $A_3^{(1)}$ is not in Λ.

We see that we may continue this process and obtain the entire first cycle $A_1^{(1)}, A_2^{(1)}, \cdots, A_s^{(1)}$. These polynomials, considered algebraically, form an ascending set. They hold Λ, but their initials are not in Λ.

We shall now form some additional cycles involving y_{ij} only. During the formation of these cycles a new ordering is to be ascribed to the y_{ij} when they are considered as algebraic variables. Those y_{ij} which are effectively present, or whose transforms are effectively present, in the first cycle will retain the ordering they had in the formation of that cycle. The second cycle will introduce the next higher transform of each y_i, $i=1, 2, \cdots, s$, and these will

([10]) In the sense of A.D.E. for the ordering we have just assigned.

follow the already ordered unknowns, and have among themselves the order of their first subscripts. The third cycle will introduce the next higher transform of each y_i than occurred in the second cycle, and these will be ordered so as to follow the unknowns of the first two cycles and have among themselves the order of their first subscripts. Continuing, we may order the y_{ij} occurring in an arbitrarily large number of cycles. In the following section of this proof, we shall mean, by the rank or class of an algebraic polynomial, that rank or class determined by the ordering just described.

8. We specify that the mth polynomial, $A_m^{(k)}$, of the kth cycle must have the following properties:

(a) It must hold Λ.

(b) Its initial, in the sense of algebra, must not hold Λ.

(c) If $k \neq 1$, it must effectively involve the next higher transform of y_m than the highest present in $A_m^{(k-1)}$.

(d) It must involve no transform of any y_i, except the one specified in (c), which is not present, or some transform of which is not present, in preceding polynomials of the cycles (that is, in polynomials $A_p^{(r)}$ with $r<k$ or $r=k$ and $p<m$).

(e) It must be reduced algebraically with respect to all preceding polynomials of the cycles.

(f) Among all polynomials with properties (a) through (e) it must be one which is lowest in the algebraic sense.

The polynomials of the first cycle satisfy these conditions. We shall show that polynomials with properties (a) through (e) exist assuming that the polynomials of the first $k-1$ cycles and, if $m>1$, the first $m-1$ polynomials of the kth cycle have been obtained. Then we may select among the polynomials satisfying the other conditions one which is lowest, so that (f) is also satisfied. It will follow by induction that we may obtain polynomials $A_b^{(a)}$, $b=1, 2, \cdots, s$, for any a, and so obtain an arbitrarily large number of cycles.

We observe that the polynomials $A_1^{(1)}, A_2^{(1)}, \cdots, A_s^{(1)}; A_1^{(2)}, A_2^{(2)}, \cdots, A_s^{(2)}; \cdots; A_1^{(k)}, A_2^{(k)}, \cdots, A_{m-1}^{(k)}$ form an ascending algebraic set. We form the remainder R of the first transform of $A_m^{(k-1)}$ with respect to this set. We say that R satisfies conditions (a) through (e).

It is obvious that (a) and (e) are satisfied. We prove (b) and (c). Let v be the order of $A_m^{(1)}$ in y_m. Then y_{mw}, $w=v+k-1$, is the transform of y_m which must be effectively present in $A_m^{(k)}$ according to (c). Now R satisfies the equation:

$$R = \prod_{a,b} (I_b^{(a)})^{\mu_{a,b}} (A_m^{(k-1)})_1 + \sum_{a,b} K_b^{(a)} A_b^{(a)}, \tag{1}$$

where the $\mu_{a,b}$ are integers, the $K_b^{(a)}$ difference polynomials, and $I_b^{(a)}$ is the the algebraic initial of $A_b^{(a)}$. The indices ranges over all values occurring in polynomials which precede $A_m^{(k)}$ in the cycles; and in $(A_m^{(k-1)})_1$ the subscript 1

denotes transforming. Let n be the highest power of y_{mw} in $(A_m^{(k-1)})_1$. Then (1) shows that the coefficient of y_{mw}^n in R is I,

$$I = \prod_{a,b} (I_b^{(a)})^{\mu_{a,b}} (I_m^{(k-1)})_1 + \sum_{a,b} L_b^{(a)} A_b^{(a)}, \tag{2}$$

where the $L_b^{(a)}$ are difference polynomials, and the subscript 1 denotes transforming. I does not hold Λ since initials of already constructed polynomials in the cycles do not. Then I is a fortiori not zero and is the actual initial of R. Thus (b) and (c) are satisfied. (d) follows from equation (1) when it is remembered that the $K_b^{(a)}$ need involve no y_{ij} not present in the previously constructed polynomials of the cycles and $(A_m^{(k-1)})_1$. This completes the proof that an arbitrarily large number of cycles can be constructed.

9. There exists a nonzero polynomial in Λ, namely the C described in §6, which effectively involves z. Among all such polynomials let D be one which is lowest when considered as a difference polynomial in z, and whose initial is not in Λ.

Let t be an integer such that there occur in the first $t-1$ cycles constructed in §8 higher transforms of each y_i than the highest present in D. We shall retain only these cycles of §8, and construct higher cycles in which z appears effectively. We shall number these the tth, $(t+1)$th cycle, and so on, and shall continue to use the notation $A_m^{(k)}$ for the mth polynomial of the kth cycle in the new sense. Each cycle following the $(t-1)$th will contain $s+1$ polynomials.

The first s polynomials of the tth cycle are to be the s polynomials of the tth cycle of §8 without change. We shall now construct the remaining polynomial of this cycle. Let D be of order r in z. We introduce a new ordering of the unknowns. The y_{ij} present thus far in the cycles are to retain their original ordering among themselves. $z, z_1, \cdots, z_{r-1}$ are to precede all these y_{ij}, while z_r is to follow them.

With this ordering let S be the remainder of D with respect to the algebraic ascending set consisting of the cycles available at this point. S can be obtained from an expression similar to the right-hand member of (1) with D replacing $(A_m^{(k-1)})_1$. If D is of degree p in z_r, we see that the coefficient J of z_r^p in S is given by an expression similar to the right-hand member of (2) with the initial of D (which is the same in either the sense of algebra or the theory of difference polynomials) replacing that of $(A_m^{(k-1)})_1$. It follows that J is not in Λ, and a fortiori is not zero. Thus J is the initial of S, and S is of the same rank as D when considered as a difference polynomial in z.

We now construct an arbitrarily large number of additional cycles of $s+1$ polynomials each. The mth polynomial, $A_m^{(k)}$, of the kth cycle must satisfy conditions (a) through (f) of §8, with the understanding that we are to write y_{s+1} for z. This understanding is also to be observed in the ordering to be assigned to the unknowns when considered as algebraic variables, and this ordering is then to be carried out precisely as described in §8. We may now

prove that an arbitrarily large number of additional cycles can be constructed by following word for word the proof of §8.

10. We consider the ascending set

$$A_1^{(1)}, A_2^{(1)}, \cdots, A_s^{(1)}; A_1^{(2)}, \cdots, A_b^{(a)}. \tag{3}$$

No polynomial P in the prime ideal Λ is reduced with respect to that ascending set (3) for which $A_b^{(a)}$ and P are of the same class when considered as algebraic polynomials with the ordering of the unknowns which arises when sufficient cycles have been constructed to contain higher transforms of each y_i and z than occur in P. For let P be reduced with respect to that ascending set. We write R_1 for P, R_2 for the initial of P in the algebraic sense, R_3 for the initial of R_2, and so on. Let T be the R_i of smallest subscript such that R_{i+1} does not hold Λ.

Suppose first that T is of greater order in z than the polynomial D of the preceding paragraph. Since the class of T, considered algebraically, exceeds that of D, T satisfies the conditions (a) through (e) at that stage in the formation of the cycles where the class of T equals the class of the transform whose presence is required by condition (c). Now the assumption about P shows that T is algebraically lower than the polynomial of the same class in the cycles. But this contradicts the fact that the polynomials of the cycles fulfill condition (f).

We next suppose that T is not of greater order than D in z, in which case it must be of lower degree in the highest transform of z which it contains, or of lower order than D in z. It then follows from the definition of D that T is either free of z or that its initial, when it is considered as a difference polynomial in z, holds Λ. In the latter case let T_1 represent the initial of T. If T_1 contains z we let T_2 be its initial when considered as a difference polynomial in z. Continuing, we eventually obtain a polynomial T' in Λ free of z. Let S_1 be the initial of T' considered as an algebraic polynomial, S_2 the initial of S_1 and so on. We let S be the S_i of least subscript such that S_{i+1} does not hold Λ. If T is free of z we let S be T. Now S satisfies conditions (a) through (e) at that stage in the formation of the cycles where the class of S equals the class of the transform whose presence is required by (c). Reasoning as above we again obtain a contradiction. This proves the statement concerning the ascending set (3) made at the head of this section.

11. We shall show that the ascending set (3) is the basic set of a prime system([11]). The product of the initials of the polynomials of (3) does not hold Λ. We consider a solution of Λ not annulling this product. This solution is a regular solution of (3) in the sense required by the theorem of §45 of

([11]) Following the convenient usage of Chapter IV of A.D.E. we employ this term to denote a prime ideal of algebraic polynomials in a finite number of unknowns, while the term "prime ideal," unless we specifically state otherwise, means prime difference ideal.

A.D.E. It is a consequence of that theorem, and of the existence of a regular solution, that if (3) is not the basic set of a prime system there is an equation

$$(4) \qquad (I_{A_1^{(1)}})^{\mu_{1,1}} \cdots (I_{A_b^{(a)}})^{\mu_{a,b}} [TA_b^{(a)} - G_1G_2 \cdots G_k] = \sum L_j^{(i)} A_j^{(i)},$$

where the $\mu_{i,j}$ are integers, the $L_j^{(i)}$ and T difference polynomials, and $I_{A_j^{(i)}}$ is the initial of $A_j^{(i)}$. The sum on the right-hand side extends over all polynomials $A_b^{(a)}$ preceding $A_j^{(i)}$ in (3), and each G_i is a polynomial of the class of $A_b^{(a)}$, which involves no unknowns not occurring in (3), and is reduced with respect to (3). Then no G_i can hold Λ, and consequently their product cannot. This contradicts equation (4), and it must follow that every set (3) is the basic set of a prime system.

We see that the unconditioned unknowns([12]) in any such prime system are the transforms of z of lower order than D in z and the transforms of each y_i which are of lower order than $A_i^{(1)}$ in y_i. Each new cycle, after the cycle containing D, introduces an additional transform of z. If we choose enough cycles we obtain the basic set of a prime system Ψ in which the transforms of z outnumber the unconditioned unknowns. Then Ψ is held by a nonzero polynomial V in the z_i alone. Then PV, where P is some product of powers of initials of the $A_j^{(i)}$, is a linear combination of the $A_j^{(i)}$ and therefore holds Λ. Then V holds Λ. This proves the lemma.

12. We shall say that an element t of an extension $\mathfrak{K}$ of a difference field $\mathfrak{J}$ *is transformally dependent on a set* M of elements of $\mathfrak{K}$ with respect to $\mathfrak{J}$ if t annuls a nonzero difference polynomial with coefficients in the field obtained by adjoining to $\mathfrak{J}$ the elements of M. In other words, t depends on M if it is transformally algebraic over $\mathfrak{J}(M)$. A set of elements M in an extension of $\mathfrak{J}$ will be said to depend on a set N in the same extension of $\mathfrak{J}$ if each element of M is transformally dependent on N with respect to $\mathfrak{J}$.

Two further definitions will be of use. Sets M and N in an extension of $\mathfrak{J}$ will be said to be *equivalent* if each depends transformally on the other relative to $\mathfrak{J}$. A set will be called *reducible* or *irreducible* according to whether it does or does not depend on any proper subset of itself.

With the aid of the lemma of §6, and the definitions just given, we may now transfer word for word the methods used by H. W. Raudenbush([13]) for differential fields to prove the following analogue of the theorem of Steinitz:

THEOREM I. *Every set contains an equivalent irreducible subset. In particular an extension* $\mathfrak{K}$ *of a difference field* $\mathfrak{J}$ *which is not a transformally algebraic ex-*

([12]) We again follow a convention of A.D.E. and reserve the term "unconditioned unknowns" for algebraic systems, and the term "arbitrary unknowns," which will be defined formally in §13, for systems of difference (or differential) equations. The formal definitions are identical, mutatis mutandis.

([13]) H. W. Raudenbush, *Differential fields and ideals of differential forms*, Ann. of Math. (2) vol. 34 (1933) p. 513.

tension of $\mathcal{J}$ may be obtained by the adjunction of an irreducible set followed by a transformally algebraic extension.

Again following Raudenbush we may prove the theorem[14]:

THEOREM II. *If an extension $\mathcal{K}$ of the field $\mathcal{J}$ is equivalent to two irreducible subsets, M and N, then M and N are of the same potency.*

Using Theorem II we see that we may define the *degree of transformal transcendency* of an extension $\mathcal{K}$ of a difference field $\mathcal{J}$ as the potency of an equivalent irreducible subset of $\mathcal{K}$.

13. **Invariance of the number of arbitrary unknowns.** We consider any perfect difference ideal Λ in the ring of polynomials in the unknowns $u_1, u_2, \cdots, u_q; y_1, y_2, \cdots, y_p$, whose transforms will be denoted by a second subscript. The u_i will be said to constitute a set of arbitrary unknowns of Λ if

(a) Λ is held by no nonzero difference polynomial in the u_i alone,

(b) for each k, $1 \leqq k \leqq p$, there exists a nonzero difference polynomial in y_k and $u_1, u_2, \cdots, u_q$ which holds Λ.

It may, of course, be possible to select several different sets of arbitrary unknowns for any one ideal. For prime ideals, however, we have the following theorem.

THEOREM III. *All sets of arbitrary unknowns of a reflexive prime difference ideal contain the same number of unknowns.*

Let Σ be a reflexive prime difference ideal in the unknowns $u_1, u_2, \cdots, u_q$; $y_1, y_2, \cdots, y_p$, the u_i constituting a set of arbitrary unknowns. Let $\mathcal{J}$ be the coefficient field of Σ.

It is shown in R that the quotient-field $\mathcal{K}$ of the remainder classes of Σ contains a general point solution of Σ[15]. Let $u_i = \alpha_i$, $i = 1, \cdots, q$; $y_i = \beta_i$, $i = 1, \cdots, p$ be the values of the unknowns in this general point solution. Then $\mathcal{K}$ is formed by adjoining the α_i and β_i to $\mathcal{J}$.

The α_i annul no difference polynomial with coefficients in $\mathcal{J}$, for otherwise Σ would contain a polynomial in the u_i alone. Thus the α_i constitute an irreducible set. Since Σ contains, for each j, a nonzero polynomial in y_j and the u_i only, it follows that each β_j is transformally dependent on the α_i. Finally, we note that each element of $\mathcal{K}$ is, in a trivial way, transformally algebraic over the field obtained by adjoining the α_i and β_i to $\mathcal{J}$, and therefore, by the

(14) We shall be concerned particularly with the case in which at least one of the sets mentioned in the theorem is known to be finite. A simpler proof is possible when this occurs. See van der Waerden, *Moderne Algebra*, vol. I, pp. 104–109 and 210–212, Frederick Ungar Publishing Co., New York.

(15) By the general point, or general point solution, of a reflexive prime ideal with coefficients in a field $\mathcal{J}$, we shall mean any solution, however obtained, lying in an extension of $\mathcal{J}$ and annulling no polynomial with coefficients in $\mathcal{J}$ which is not in the ideal.

lemma stated in §6, transformally algebraic over the field resulting when the α_i are adjoined to $\mathcal{J}$. It follows that the α_i constitute an equivalent irreducible subset of $\mathcal{K}$ relative to $\mathcal{J}$. The number q of the α_i is the degree of transformal transcendency of $\mathcal{K}$ relative to $\mathcal{J}$.

It follows that the number of unknowns in a set of arbitrary unknowns of Σ is a constant, namely the degree of transformal transcendency relative to $\mathcal{J}$ of the quotient-field of the remainder classes of Σ. Thus Theorem III is proved.

Part II. Polynomials in one unknown

14. Let $\mathcal{J}$ be an abstract difference field, and A a difference polynomial in the unknown y with coefficients in $\mathcal{J}$. It is assumed that A is algebraically irreducible in $\mathcal{J}$, and that it effectively involves y_0. Let n be the order of A in y, and r its degree in y_n. Let A_i denote the ith transform of A.

In order to study the separation of the manifold of A into irreducible manifolds we shall construct sets of elements which annul A and its transforms. We adjoin to $\mathcal{J}$ the transcendental elements α_i, $i=0, \cdots, n-1$, to form the field $\mathcal{J}_1$. $\mathcal{J}_1$ is not a difference field since the transforms of the α_i are not defined. The elements we shall construct will be algebraic over $\mathcal{J}_1$, and shall be referred to as the *algebraic solutions* of A. They do not necessarily correspond to any solutions of A in a difference field.

We start the formation of the algebraic solutions by letting $y_i=\alpha_i$, $i=0, \cdots, n-1$. Upon substituting these values into A we obtain a polynomial in y_n with coefficients in $\mathcal{J}_1$, and irreducible in that field. This polynomial will be annulled by an element in a suitable algebraic extension of $\mathcal{J}_1$. We select such an element as the value of y_n in the algebraic solution.

To continue the algebraic solution to higher transforms of y we must first show that no polynomial in $y_1, \cdots, y_n$ is annulled by the portion of the solution so far obtained. Let B be any such polynomial. We form the resultant R of A and B considered as polynomials in y_n. A and B can have no factors in common so that R cannot be identically zero. R is annulled by all common solutions of A and B. Since R does not involve y_n it certainly cannot vanish when the beginning of an algebraic solution, which has already been determined, is substituted into it. It follows that B also does not vanish. This proves the statement.

In particular, the initial of A_1 and its discriminant as a polynomial in y_{n+1} are not annulled by this solution, so that A_1 becomes, on substituting for $y_0, \cdots, y_n$ their values in the algebraic solution, a polynomial of degree r in y_{n+1}, which has no repeated factor. We continue the algebraic solution by letting y_{n+1} be an element in an algebraic extension of $\mathcal{J}_1$ which annuls this polynomial.

The process we have used may be continued to provide solutions for every A_i. To prove this we assume that solutions have been found in this way for

$A, \cdots, A_k$. We make the additional inductive hypothesis that the solutions so far obtained annul no polynomial in $y_k, \cdots, y_{n+k-1}$. Our inductive hypotheses are known to be satisfied for A itself.

We show first that A_k has no factor free of y_k. Suppose it has such a factor T, and let y_{l+k} be a transform of y which appears effectively in T. We consider the coefficients, S_i, of the powers of y in A. The S_i, as polynomials in y_l, have a resultant system which includes a nonvanishing polynomial D; for they have no common factor. D is a linear combination of the S_i. The kth transform of D is then a linear combination of the coefficients of y_k in A_k, and is free of y_{l+k}. It follows that these coefficients can have no factor involving y_{l+k}. This contradicts the fact that y_{1+k} appears in T, and proves our statement.

Let B be any polynomial in $y_{k+1}, \cdots, y_{n+k}$. Then B and A_k are relatively prime. The resultant R of B and A_k, considered as polynomials in y_{n+k}, is a nonzero polynomial in $y_k, \cdots, y_{n+k-1}$, which holds all common solutions of B and A_k. We know that R is not annulled by the solutions assumed in our inductive hypothesis. It follows immediately that B does not vanish for these solutions. This proves the latter part of the hypothesis. The initial of A_{k+1}, and its discriminant when it is considered as a polynomial in y_{n+k+1}, cannot be annulled by the solutions so far determined. It follows that by substituting any of these solutions into A_{k+1} we obtain a polynomial of degree r in y_{n+k+1} which has no repeated factors. We continue the algebraic solutions by letting y_{n+k+1} be an element in an algebraic extension of $\mathfrak{J}_1$ which annuls this polynomial. This completes the construction of the algebraic solutions.

Let C be a polynomial of order $s \geqq n$ which vanishes for all algebraic solutions of A. We substitute the values of y_i, $0 \leqq i < s$, in some algebraic solution, into C and $A_{s-n} \cdot C$ must become a multiple of A_{s-n} after the substitution, for otherwise we could find a value of y_s which, together with the previously determined values of $y_0, y_1, \cdots, y_{s-1}$, annuls A_{s-n} but does not annul C. We note that C must be of degree at least r in y_s if the coefficients of powers of y_s in C do not all vanish for every algebraic solution.

15. We now consider the system $A, A', A'', \cdots, A^{(k)}, \cdots$, where $A^{(k)}$ is obtained by taking the algebraic remainder with respect to $A, \cdots, A^{(k-1)}$ of A_k, using the ordering $y, y_1, \cdots, y_{n+k}$, of the unknowns. Evidently every $A^{(k)}$ and every transform of the $A^{(k)}$ will be annulled by the algebraic solutions.

Let I_m represent the coefficient of y_{n+m}^r in $A^{(m)}$. Let J_m represent the mth transform of the coefficient of y_n^r in A. We have already seen that no J_m is annulled by any algebraic solution. $I_0 = J_0$ is therefore not annulled by such solutions. Since

$$I_m = I_0^{\mu_0} I_1^{\mu_1} \cdots I_{m-1}^{\mu_{m-1}} J_m - S_0 A - S_1 A' - \cdots - S_{m-1} A^{(m-1)},$$

where the μ_i are integers and the S_i difference polynomials, we see inductively

that no I_m vanishes for any algebraic solution, and, in particular, that none is zero. Then I_m is the initial of $A^{(m)}$. Consideration of the successive transforms of the preceding equation shows that no transform of any I_m is annulled by the algebraic solutions.

It may be that every set $A, \cdots, A^{(k)}$, considered as an ascending set of algebraic polynomials in the field $\mathcal{J}$, is the basic set of a prime system. If this is not so, consider the shortest such set which is not. The existence of algebraic solutions assures that there will be a relation

$$(1)\ I_0^{\mu_0} I_1^{\mu_1} \cdots I_k^{\mu_k}(TA^{(k)} - G_1 \cdots G_p) - S_0 A - S_1 A^{(1)} - \cdots - S_{k-1} A^{(k-1)} = 0$$

where the μ_i are integers, and the S_i, G_i, and T polynomials. T and each G_i are reduced with respect to $A, A', \cdots, A^{(k-1)}$, and T is free of y_{n+k}.

The polynomials vanishing for algebraic solutions of $A, A', \cdots, A^{(k-1)}$ form a prime system ψ which is not held by T. Then some linear combination of T and polynomials of ψ is a polynomial L in $y_0, \cdots, y_{n-1}$ only. This is an application of the principle that the dimensionality of a prime algebraic ideal is greater than that of any of its proper extensions. No transform of L vanishes for any algebraic solution. Every polynomial of ψ has zero remainder with respect to $A, A', \cdots, A^{(k-1)}$ so that all its transforms vanish for all algebraic solutions. Then no transform of T is annulled by any algebraic solution. Similarly, no transform of an initial of any G_i is annulled by the algebraic solutions.

The degrees r_i of the G_i in y_{n+k} total r. Let the elements of an algebraic solution be substituted for $y_0, \cdots, y_{n+k-1}$ in $A^{(k)}$ and the G_i. Then $G_1 \cdots G_p$ becomes a multiple of $A^{(k)}$. Since no G_i is annulled by these substitutions, it follows that the polynomials resulting from the G_i have no repeated factors or factors in common. Thus any extension of the beginning of an algebraic solution to a solution of $A^{(k)}$ will annul precisely one G_i, and there will exist algebraic solutions annulling any G_i.

Every algebraic solution of $A, \cdots, A^{(k-1)}$ may thus be extended to an algebraic solution which annuls any G_i. Upon substituting the elements of such a solution into $A^{(k+1)}$ the latter becomes a polynomial of degree r in y_{n+k+1} which has no repeated factors. We use a second subscript to denote transforms of the G_i. Then the transform of equation (1) shows that the $G_{j1}, j=1, \cdots, p$, become polynomials of degree r_j which have no repeated or common factors. Thus some extension of the algebraic solution to a solution of $A^{(k+1)}$ can be found which annuls G_{m1}, for any given m, and, of course, annuls no other G_{j1}. In particular, there will be solutions annulling any G_i and its transform. In the remainder of this proof we shall be concerned only with solutions of this type.

We proceed in this manner to select algebraic solutions of A which annul sets of the form $A, \cdots, A^{(k-1)}; G_i, \cdots, G_{im}, \cdots$. By a process of taking remainders we construct from these sets systems of the type $A, \cdots, A^{(k-1)}$;

$G_i^{(0)}, \cdots, G_i^{(m)}, \cdots$ which have the property that, when interrupted at any point, the beginning of the sequence constitutes an ascending set of algebraic polynomials in the field $\mathfrak{J}$. Of course these systems are annulled by the appropriate algebraic solutions, while initials and transforms of initials of the polynomials of the systems are not. If we replace $y, y_1, \cdots, y_t, t=k+m+n$ in $G_i^{(m+1)}$ by elements of an algebraic solution annulling the corresponding system, $G_i^{(m+1)}$ becomes a polynomial of degree r_i in y_{t+1} which has no repeated factor.

It may be that all the ascending sets obtained as in the last paragraph are basic sets of prime systems. If not, new factorization equations similar to (1) may be obtained. These may be treated in the same manner. The number of factorizations obtainable is limited by the degree of A in y_n. We see that we obtain s sequences, $1 \leqq s \leqq r$, which we may represent by $B_{i0}, \cdots, B_{ik}, \cdots, i=1, \cdots, s$, which have the property that the finite sets obtained by discarding all polynomials beyond any given point in the sequence are all basic sets of prime systems. We shall refer to these sequences as the *basic sequences* of A. Each B_{i0} is of course A.

16. We let Λ_{kj} be the prime system of which $B_{k0}, \cdots, B_{kj}$ is a basic set and form the union, for fixed k, of the systems Λ_{kj}. We represent this union by Λ_k. Λ_k is evidently a prime algebraic ideal in the unknowns y_{ij}.

We shall see that each Λ_k is a reflexive prime difference ideal. The polynomials of Λ_k are exactly those which are annulled by the algebraic solutions of $B_{k0}, \cdots$. The initials and transforms of initials of the B_{kj} are therefore not in Λ_k. On the other hand, the transforms of the B_{kj} themselves are in Λ_k. If R is any polynomial in Λ_k, some product P of powers of the initials of the B_{kj} exists such that PR is a linear combination of the B_{kj}. Then the product of the transform of P by the transform of R is a linear combination of transforms of the B_{kj} and is therefore in Λ_k. Since the transform of P is not in the ideal Λ_k, the transform of R is in this ideal.

Let S_1, the transform of S, hold Λ_k. Then S is of order $n+h$, $h \geqq 0$. We shall show that S holds the prime system Ψ with basic set $B_{k0}, B_{k1}, \cdots, B_{kh}$, and is therefore in Λ_k. If not there exists a polynomial U in $y_0, \cdots, y_{n-1}$, such that

$$U = MS + \sum N_i D_i,$$

where the D_i are in Ψ, and therefore in Λ_k. Using the subscript 1 to denote transforming we have

$$U_1 = M_1 S_1 + \sum N_{i1} D_{i1}.$$

S_1 and the D_{i1} are in Λ_k. Then U_1 is in Λ_k and vanishes for all algebraic solutions which annul its basic sequence. This is impossible since U_1 involves only $y_1, \cdots, y_n$. Therefore S is in Λ_k.

These facts complete the proof that each Λ_k is a reflexive prime difference ideal. Evidently no Λ_k holds any other for each is annulled by algebraic solutions annulling no other.

17. Let Λ be any essential prime ideal in the decomposition of $\{A\}$ which is not held by a polynomial of order lower than A. Then Λ is held by the first polynomial $B_{k0}=A$ of the basic sequence of each Λ_k, but not by its initial. Let us suppose that Λ is held by the first m polynomials $B_{h0}, B_{h1}, \cdots, B_{hm}$ of some basic sequence of A, but not by the initial of any B_{hi}, $i \leqq m$. We shall show that Λ is held by the first $m+1$ polynomials $B_{h0}, B_{h1}, \cdots, B_{h,m+1}$ of some basic sequence but not their initials ([16]).

Let Ψ be the prime system with basic set $B_{h0}, \cdots, B_{hm}$. The polynomials of Ψ hold Λ for they have zero remainder with respect to this basic set. If D is any polynomial involving no transform of y higher than those in B_{hm} and if D is not in Ψ, then D does not hold Λ. For some linear combination of D and polynomials of Ψ is a polynomial in $y_0, \cdots, y_{m-1}$ only and cannot hold Λ.

Let k be such that B_{hk} but not $B_{h,k-1}$ is of the same degree as B_{hm} in their respective highest transforms of y (or let $k=0$ if B_{h0} and B_{hm} are of the same degree). Let C be the remainder with respect to $B_{h0}, \cdots, B_{hm}$ of the $(m+1-k)$th transform of B_{hk}. Then C holds Λ. Either C is the next polynomial of a basic sequence, or there is a factorization equation similar to (1) with C playing the role of $A^{(k)}$. Then at least one of the polynomials corresponding to the G_i of equation (1) holds Λ. In either case there is, perhaps after a change of notation, a basic set $B_{h0}, \cdots, B_{h,m+1}$ such that $B_{h,m+1}$ holds Λ. The initial of $B_{h,m+1}$ is reduced with respect to $B_{h0}, \cdots, B_{hm}$. It is therefore not in Ψ, and so, by the remark of the preceding paragraph, cannot hold Λ. Thus our statement is proved.

We see by induction that Λ is held by all polynomials of some basic sequence $B_{h0}, B_{h1}, \cdots$, but not by their initials. Then Λ must be held by Λ_h. Now Λ can contain no polynomial not in Λ_h. For if S is any polynomial not in Λ_h there is, as we have seen, a linear combination of S and polynomials of Λ_h which is of order $n-1$. But Λ is held by no polynomial of this order. It follows that the Λ_k are essential prime ideals in the decomposition of $\{A\}$ and are the only such ideals not held by a polynomial of order less than n; indeed, our last remark shows that there are not even ideals containing some Λ_i as a proper subideal and not held by a polynomial lower than A. This completes the proof of the following theorem.

THEOREM IV. *Let A be an algebraically irreducible difference polynomial in a difference field $\mathfrak{J}$, which is of order n and degree r in y_n and effectively involves y_0.*

([16]) There may be several ideals Λ_k whose basic sequences begin with $B_{h0}, \cdots, B_{hm}$, and therefore several possible values for the subscript h. As we proceed from m to $m+1$ the set of allowable values of the subscripts may diminish. We assume that the notation is then changed, if necessary, so as to assign to h a value permissible for $m+1$ (and therefore certainly for m).

There exist at least one and at most r essential prime ideals in the decomposition of $\{A\}$ *which are not held by any polynomial of order less than n. These ideals are the reflexive prime ideals determined by the basic sequences constructed above.*

We may speak of an algebraic solution of A which annuls all the polynomials of a basic sequence of A as an algebraic solution of that basic sequence. Let $\mathcal{G}$(17) represent the field obtained by adjoining to $\mathcal{J}$ an algebraic solution of the basic sequence of the prime ideal Λ_k as defined in Theorem IV. $\mathcal{G}$ consists of all rational combinations, with coefficients in $\mathcal{J}$, of the elements of the algebraic solution. The quotient field $\mathcal{K}$ of the remainder classes of Λ_k consists of all rational combinations, with coefficients in $\mathcal{J}$, of the remainder classes corresponding to $y_0, y_1, \cdots$. These remainder classes satisfy the same algebraic relations as the elements of an algebraic solution; for both annul all polynomials of Λ_k and no others. Than $\mathcal{G}$ must be algebraically isomorphic with $\mathcal{K}$. Then we can also introduce an isomorphic differencing operation into $\mathcal{G}$. The transform of the element corresponding to y_i in an algebraic solution will be the element corresponding to y_{i+1}. Thus $\mathcal{G}$ becomes a difference field and the algebraic solution of the basic sequence becomes a general point solution of Λ_k.

The field $\mathcal{G}$ is generated by transcendental adjunctions to $\mathcal{J}$ of elements corresponding to $y, y_1, \cdots, y_{n-1}$, followed by algebraic adjunctions. It follows that its degree of transcendence over $\mathcal{J}$, in the sense of algebra, is n.

18. **Polynomials in several unknowns.** Theorem IV may be extended to the case of a polynomial A in a dependent unknown y and arbitrary unknowns $u_1, u_2, \cdots, u_q$.

We first consider A as a polynomial in the field $\mathcal{J}(u_1, u_2, \cdots, u_q)$ and construct, by means of Theorem IV, the prime ideals Σ_i holding the essential irreducible manifolds of A. Those polynomials of Σ_i whose coefficients are integral in the u_i obviously constitute a reflexive prime difference ideal Λ_i in the ring $\mathcal{J}[u_i, \cdots, u_q, y]$. Each Λ_i is held by A, and no two Λ_i are identical.

Let Λ be any reflexive prime difference ideal of the ring $\mathcal{J}[u_1, \cdots, u_q; y]$ which is held by A. We denote by Σ the set of polynomials in y, with coefficients in $\mathcal{J}(u_1, \cdots, u_q)$, which, when multiplied by some suitable integral expression in the u_i become polynomials of Λ. Evidently Σ is a reflexive ideal. Furthermore it is a prime ideal. For let MN hold Σ. There exists a polynomial U in the u_i such that MNU thought of as a polynomial in the u_i and y holds Λ. Then either MU or NU holds Λ, and consequently either M or N must be in Σ. If Σ includes unity Λ is held by a polynomial in the u_i alone. Otherwise, as we have seen in the proof of Theorem IV, either Σ is identical with some Σ_i, and consequently Λ with some Λ_i, or Σ, and therefore Λ, are held by some polynomial of lower order than A in y.

(17) $\mathcal{G}$ is not a difference field.

For the basic sequence of each Λ_i we may use polynomials in Λ_i which are appropriate multiples of polynomials of a basic sequence of Σ_i. We may now state the following generalized form of Theorem IV.

THEOREM IV′. *Let A be an algebraically irreducible difference polynomial in the unknowns $u_1, u_2, \cdots, u_q; y$, with coefficients in a difference field $\mathcal{J}$, which is of order n in y and degree r in y_n, and effectively involves y_0. There exist at least one and at most r essential prime ideals in the decomposition of $\{A\}$ which are not held by any polynomial of order less than n in y. These ideals are the reflexive prime ideals corresponding to the basic sequences of A.*

To construct algebraic solutions of the polynomial A we adjoin q elements $v_1, v_2, \cdots, v_q$ to $\mathcal{J}$. The extension is to be a transformally transcendental one so that no algebraic relations exist among the transforms v_{ij} of the v_i. We denote the extended difference field by $\mathcal{J}(v_i)$. We shall henceforth frequently have occasion to make such transformally transcendental extensions of a field $\mathcal{J}$ where the number of adjunctions, q in this case, equals the number of arbitrary unknowns of some prime ideal. The symbol $\mathcal{J}(v_i)$ will be used to indicate adjunctions of this sort.

We form any algebraic solution $y_i=\alpha_i$, $i=0, 1, \cdots$, over $\mathcal{J}(v_i)$ of the polynomial B obtained from A by substituting v_i for u_i, $i=1, 2, \cdots, q$. Then $u_{ij}=v_{ij}$, $i=1, \cdots, q$, $j=0, 1, \cdots$, $y_k=\alpha_k$, $k=0, 1, \cdots$, shall constitute, by definition, an algebraic solution of A. We see that an algebraic solution of A will annul A and its transforms, but no polynomial of lower order than A in y, or free of y. Let C be a polynomial of order s in y which vanishes for all algebraic solutions. Then, on replacing the u_{ij} by v_{ij}, we obtain a polynomial C' which vanishes for all algebraic solutions of B. By the final remark of §14, and obvious considerations on the relations of algebraic solutions of C to those of C', we see that C must be of degree at least as great as A in their respective highest transforms of y, if the coefficients of powers of y_s in C do not all vanish for every algebraic solution of A.

We now select certain algebraic solutions which annul basic sequences of A. Among the reflexive prime ideals in $\mathcal{J}(v_i)$ determined by the essential irreducible manifolds of B, there are one or more ideals Φ_k not held by any polynomial of lower order than B. Each Φ_k can be obtained from Σ_k of Theorem IV′ by replacing the u_i in the polynomials of the latter with v_i, and each Σ_k gives rise in this way to some Φ_k. Then $u_{ij}=v_{ij}$, $y_i=\beta_i$ may be chosen as an algebraic solution of a basic sequence of Λ_k of Theorem IV′. It annuls the polynomials of Λ_k and no others. As in the case of polynomials in one unknown, we may set up an algebraic isomorphism between the quotient-field $\mathcal{G}$ of the remainder classes of Λ_k and the field resulting from the adjunction to $\mathcal{J}$ of an algebraic solution of a basic sequence. We may then define a transforming operation for the elements of the algebraic solution, which thus becomes a general point solution of Λ_k. We note that $\mathcal{G}$ is of algebraic degree of

transcendence n over $\mathcal{J}(v_i)$.

19. **The effective order of difference polynomials.** We shall now generalize our considerations still further so as to include polynomials in $u_1, \cdots, u_q; y$, which are free of y_0 and not necessarily transforms of polynomials involving y_0. We do not obtain an extension of Theorem IV to this case, but we shall prove results which are needed in Part III.

Let A be a polynomial in the unknown y and unknowns u_i, with coefficients in a difference field $\mathcal{J}$. Let the order of A in y be $n+k$, and let y_k, but no transform of y of order less than k, appear effectively in A. We shall define *the effective order of A in y* as n, the difference between the orders of the highest and lowest transforms of y effectively present. We denote by A^+ the polynomial obtained from A by the substitution $z=y_k$. We shall show that by means of this equation we can obtain a solution of A^+ from any solution of A and, conversely, a solution of A from any solution of A^+.

The first half of our statement is obvious. To prove the second it suffices to show that the equation $w_1-c=0$ can always be solved for w when c is any element of a difference field. This is equivalent to stating that the perfect ideal $\{w_1-c\}$ does not contain unity. Suppose on the contrary that unity is in this ideal. Then there exists a finite number of transforms of w_1-c from which unity can be obtained in a finite number of steps by the processes of linear combination and shuffling. Throughout all steps of this process we take the transforms of the polynomials involved. Then we still obtain unity by a process involving only the first and higher transforms of w. We may therefore substitute v_i for w_{i+1}, $i=0, 1, 2, \cdots$, throughout. Then unity will have been obtained by means of linear combinations and shufflings from $v-c$. But this is impossible since $v=c$ annuls the ideal $\{v-c\}$. This proves our statement concerning $\{w_1-c\}$ and shows that the equation $w_1-c=0$ may always be solved.

By solution of successive equations of the form $w_1-c=0$ we may solve $y_k-z=0$ and therefore obtain a solution of A from a solution of A^+. Obviously, in any given extension of $\mathcal{J}$ there can exist at most one solution of A so obtained from any one solution of A^+. We now assume that A is algebraically irreducible. Let B hold A, and let the substitution $z=y_k$ carry B_k into B_k^+. Then B_k^+ holds A^+ so that B_k^+ must be of effective order at least n([18]). Then B must be of effective order at least as great as that of A.

Among the reflexive prime ideals in the resolution of $\{A\}$ there must, from what we have just seen, be one or more not held by polynomials of effective order less than n. Let Λ be one such ideal. On substituting $z=y_k$ into those polynomials of Λ free of $y, \cdots, y_{k-1}$ we obtain an ideal Λ^+ held

([18]) This is an immediate consequence of results obtained in the course of proving Theorems IV and IV′. For if B_k^+ holds A^+ it must vanish for some algebraic solution of A^+, and we have seen that no algebraic solution of A^+ can annul a polynomial in fewer than n successive transforms of z.

by A^+ but by no polynomial of order less than n. It is easy to see that Λ^+ is a prime reflexive ideal of order n so that it must be held by one of the ideals Λ_h^+ obtained from A^+ by the procedure of Theorem IV′. Then Λ^+ and Λ_h^+ must be identical. Two distinct ideals Λ_1, Λ_2 of A give rise to distinct ideals Λ_1^+, Λ_2^+. For let S be in Λ_1 and not in Λ_2. Then S_k is not in Λ_2 and S_k^+ is in Λ_1^+ but not in Λ_2^+.

Conversely, let Λ^+ be a reflexive prime ideal of order n obtained from A^+ as in Theorem IV′. Let Σ be the system of polynomials resulting from Λ^+ by the substitution of $y_k = z$, and let $\Lambda = \{\Sigma\}$. Then Λ is prime. For let BC hold Λ. Then $B_k^+ C_k^+$ (19) holds Λ^+. Then either B_k^+ or C_k^+ holds Λ^+ and either B or C is in Λ. Λ contains no polynomial of effective order less than n. For if it contained such a polynomial C, C_k^+ would be a polynomial of Λ^+ of effective order less than n. Λ is an essential ideal in the decomposition of $\{A\}$. For otherwise it contains a proper subideal Λ', which is an essential ideal in $\{A\}$. The intersection of Λ' and Σ must be a proper subset Σ' of Σ. Σ' is an ideal which becomes, on replacing z by y_k, a subideal Λ'^+ of Λ^+. But the manifold of Λ'^+ must be identical with that of Λ^+, since otherwise $\{\Lambda'^+\}$, which contains A^+, would hold but be distinct from Λ^+. It is now easy to see that Λ and Λ' have identical manifolds. Then, since they are both perfect, they are identical, which contradicts the definition of Λ'. Finally, we consider two distinct ideals, Λ_1^+, Λ_2^+, if such exist, obtained from A^+ by the procedure of Theorem IV′. The ideals Λ_1 and Λ_2 obtained as above from Λ_1^+ and Λ_2^+ are distinct. For Λ_1^+ can be obtained from Λ_1 and Λ_2^+ from Λ_2 by the method of the preceding paragraph. Then if Λ_1 and Λ_2 are identical so are Λ_1^+ and Λ_2^+. Λ_1 cannot hold Λ_2; for then Λ_1^+ would hold Λ_2^+ which is impossible by Theorem IV′.

20. Consider any reflexive prime ideal Λ in the unknowns $u_1, \cdots, u_q; y$, the u_i arbitrary. We may define the order and effective order of Λ in y as respectively the lowest of the orders and the effective orders in y of polynomials of Λ. The preceding section shows that, if A is of effective order n, there is a one-to-one correspondence between reflexive prime ideals of effective order n in the decomposition of $\{A\}$ and reflexive prime ideals of order n in the decomposition of $\{A^+\}$ (20).

We shall now show that the effective order of a prime ideal Λ, as above, is

(19) Throughout this discussion symbols with a superscript $+$ will be used to represent the result obtained by the substitution $z = y_k$. BC can be obtained from polynomials of Σ by shufflings and linear combinations. Taking the kth transforms of all polynomials involved in this process, and substituting $z = y_k$, we prove our result above.

(20) It should be noted that the basic sets of the ideals obtained from $\{A\}$ need not begin with A nor with a polynomial whose transform is A. In the footnote to §45, for example, we shall consider the prime ideal Σ with basic set $y^2 - k$, $y_1 - k$, where k is an element such that $k_1 = k^2$. Let $A = y_1 - k$. Then $A^+ = z - k$ determines a single prime ideal of order zero. Then there is but one ideal of effective order zero held by $y_1 - k$. Evidently it must be Σ. $y^2 - k$ is the first polynomial of its basic set, and also of the ascending set $y^2 - k$, $y_1 + k$ which is also the basic set of a prime ideal.

equal to the effective order of the first polynomial in its basic set. Then it will follow that the order and effective order of Λ are determined by the order and effective order of this polynomial. Let A, of order $n+k$ and effective order n, be the first polynomial in the basic set of Λ. We make the usual substitution $z=y_k$ carrying A into A^+. Those polynomials of Λ free of $y, \cdots, y_{k-1}$ become, after this substitution, a prime reflexive ideal Λ^+. A^+ is the first polynomial in a basic set of Λ^+, and is of order and effective order n. Theorem IV′ shows that Λ^+ is of effective order n. Then the effective order of Λ must be n. For if Λ contained a polynomial C of effective order $s<n$, C_k^+ would be a polynomial of Λ^+ of effective order s. Our statement is proved.

We shall now study the quotient field of the remainder classes of Λ. We introduce the field $\mathcal{J}(v_i)$ as in §15. We say that the quotient field of the remainder classes of Λ is isomorphic to an extension $\mathcal{G}$ of $\mathcal{J}(v_i)$ which is of algebraic degree of transcendence over $\mathcal{J}(v_i)$ equal to the order $n+k$ of Λ. Furthermore, $\mathcal{G}$ contains a subfield $\mathcal{H}$ of degree of transcendence over $\mathcal{J}(v_i)$ equal to the effective order n of Λ and containing elements corresponding to all but a finite number of transforms of y. No subfield of $\mathcal{G}$, or of any extension of $\mathcal{J}(v_i)$ containing a general point of Λ, of lower degree of transcendence has this property.

The proof is by induction on the difference between the order and effective order of Λ. When this difference is zero, the existence of $\mathcal{G}$ follows from the remarks made after Theorem IV′, and $\mathcal{H}$ may be taken to be $\mathcal{G}$ itself. No subfield of degree of transcendence over $\mathcal{J}(v_i)$ less than the degree of transcendence n of $\mathcal{H}$ contains elements corresponding to all but a finite number of transforms of y. For then there would be an algebraic equation among fewer than n elements corresponding to successive transforms of y. Substituting u_{ij} for v_{ij} and transforms of y for the corresponding elements of $\mathcal{G}$, and multiplying by a polynomial in the u_{ij} to remove denominators, one would obtain a difference equation of effective order less than n in y which is annulled by a general point of Λ. This contradicts the fact that Λ is of effective order n.

We now assume the truth of our statements when the order and effective order differ by less than k and proceed to prove them for order $n+k$ and effective order n. We substitute w for y_1 in all polynomials of Λ free of y_0. The resulting polynomials form a reflexive prime ideal Λ' of order $n+k-1$ and effective order n. An extension $\mathcal{G}'$ of $\mathcal{J}(v_i)$ contains a general point of Λ', has degree of transcendence $n+k-1$ over $\mathcal{J}(v_i)$ and contains a subfield $\mathcal{H}'$ of order of transcendence n over $\mathcal{J}(v_i)$ and containing elements corresponding to all but a finite number of transforms of w.

Let α be the element corresponding to w in $\mathcal{G}'$, and consider the equation $y_1=\alpha$. We have seen that this equation has a solution β in an extension $\mathcal{G}$ of $\mathcal{G}'$. It is easy to see that β annuls all polynomials of Λ, for its transform, α, annuls their transforms when substituted for y_1. It annuls no polynomial not in Λ since α cannot annul the transform of such a polynomial. Then β is a

general point of Λ.

$\mathcal{G}$ may be constructed by identifying certain elements of the quotient-field of the remainder classes of $\{y_1-\alpha\}$ (21) with elements of $\mathcal{G}'$. The other elements are all rational combinations of the remainder class β corresponding to y, and its transforms. But these transforms are simply transforms of α and are already included in $\mathcal{G}'$. Thus $\mathcal{G}$ results from $\mathcal{G}'$ by the adjunction in the sense of algebra of a single element β. Since $\mathcal{G}'$ is of degree of transcendence $n+k-1$ over $\mathcal{F}(v_i)$, $\mathcal{G}$ is of degree of transcendence $n+k-1$ or $n+k$. But the former is impossible since it would imply that Λ is held by a polynomial of order $n+k-1$. Thus $\mathcal{G}$ is of degree of transcendence $n+k$ over $\mathcal{F}(v_i)$ and no field of lower degree of transcendence contains a general point of Λ. For the subfield $\mathcal{H}$ of $\mathcal{G}$, we may use the subfield of $\mathcal{G}'$ which contains all but a finite number of the elements corresponding to transforms of y. $\mathcal{H}$ is of order of transcendence n over $\mathcal{F}(v_i)$. No subfield of $\mathcal{G}$, or of any extension of $\mathcal{F}(v_i)$ containing a general point of Λ, which is of degree of transcendence less than n over $\mathcal{F}(v_i)$, contains elements corresponding to all but a finite number of transforms of y; for, as in the case of $k=0$, the existence of such a subfield would imply that Λ is held by a polynomial of effective order in y less than n.

We may summarize our results as follows: *Let Λ be a reflexive prime difference ideal in y and arbitrary unknowns u_i. The order $n+k$ and effective order n of Λ in y are equal respectively to the order and effective order in y of the first polynomial in its basic set. A general point of Λ lies in a field $\mathcal{G}$ obtained from $\mathcal{F}(v_i)$ by $n+k$ transcendental adjunctions followed by algebraic adjunctions, and not in any field obtained by fewer transcendental adjunctions. $\mathcal{G}$ has a subfield $\mathcal{H}$ containing all but a finite number of the transforms of y and of degree of transcendence n over $\mathcal{F}(v_i)$. No field of lower degree of transcendence has this property.*

21. **Singular solutions.** We have seen that an algebraically irreducible difference polynomial A in the unknown y has one or more essential manifolds not held by polynomials of lower effective order than A. Such a manifold we call an (essential) *ordinary manifold* of A, while all other essential manifolds will be known as *essential singular manifolds* of A. The totality of solutions of the ordinary manifolds constitutes the *general solution* of A.

Let A, for example, be the polynomial yy_2+y_1. Then $yA_1-A=y_1(yy_3-1)$. Evidently yy_3-1 vanishes for all solutions of A except $y=0$, which constitutes a singular manifold. We shall see that first order difference polynomials have no singular manifolds. We prove, in fact, the following theorem.

THEOREM V. *An algebraically irreducible difference polynomial in one unknown and of effective order one has no essential singular manifolds.*

22. Let A be an algebraically irreducible difference polynomial in the unknown y and of effective order one. Let $\mathcal{F}$ be the coefficient field of A.

(21) We require the fact that $\{y_1-\alpha\}$ is a prime ideal. This follows, by the correspondence of §19, from the fact that $\{z-\alpha\}$ is prime. It may also easily be proved directly.

Let Σ be a reflexive prime ideal of effective order zero which A holds. We shall show that the solutions of Σ are contained in some ordinary manifold of A.

We may assume that Σ and A are of order zero and one respectively. For, if not, we can make them so by a transformation of the form $w=y_i$.

Let $y=u$ be a general point of Σ. Upon making the substitution $y=z+u$, A becomes a polynomial A^+ in z and z_1 which vanishes when we put both z and z_1 equal to zero, but not when we put z or z_1 alone equal to zero. It follows that A^+ can be annulled formally by substituting for z_1 a series z_1' in positive rational powers of z which is not identically zero.

The exponents occurring in z_1' have a common denominator k. The coefficients of the expansion lie in a field obtained from $\mathcal{J}(u)$ by a finite number of algebraic adjunctions. Now Theorem IV shows that, given a finite algebraic extension $\mathcal{G}'$ of a difference field $\mathcal{G}$, there exists an extension $\mathcal{G}''$ of $\mathcal{G}'$ to which the transforming operation of $\mathcal{G}$ may be extended so that $\mathcal{G}''$ is a difference field containing $\mathcal{G}$. For $\mathcal{G}'$ may be obtained from $\mathcal{G}$, by adjoining a root of a single irreducible algebraic polynomial B. If we adjoin to $\mathcal{G}$ a general point of one of the prime ideals Λ_k obtained from B as in Theorem IV, we obtain the difference field $\mathcal{G}''$. Then there exists a difference field $\mathcal{J}_1$ which is an extension of $\mathcal{J}(u)$ and contains all the coefficients of the series z_1'.

23. We now construct a formal series from z_1' by the following procedure. First we replace each coefficient by its transform in $\mathcal{J}_1$. Next we replace z by z_1 throughout the series. We call the resulting power series z_2''. There exists a formal power series in positive rational powers of z whose kth power is z_1'. We replace $z_1^{1/k}$ by this series. z_2'' then becomes a formal power series z_2' in positive rational powers of z with coefficients in a difference field $\mathcal{J}_2$ and exponents with common denominator k^2. $\mathcal{J}_2$ is an extension of $\mathcal{J}_1$.

We obtain z_3'' from z_2' by replacing each coefficient of the series by its transform and then replacing z by z_1. We now form z_3' from z_3'' by replacing z_1^{1/k^2} by an appropriate expansion in powers of z. This expansion must be so chosen that its kth power is the series substituted for $z_1^{1/k}$ in the preceding step.

We continue in this way to construct series z_i', $i=1, 2, \cdots$, in powers of z, and z_i'', $i=2, 3, \cdots$, in powers of z_1. The coefficients of z_i' lie in a difference field $\mathcal{J}_i$. At each step we require a power series in z which when raised formally to the power k^r, for some integer r, is the series z_1'. We must choose this series so that its kth power is the corresponding series used in the preceding step.

24. Let $y_i'=z_i'+u_i$, $i=1, 2, \cdots$, $y_0'=u+z$; and let $y_i''=z_i''+u_i$, $i=2, 3, \cdots$, $y_1''=u_1+z_1$. Let C be any difference polynomial with coefficients in $\mathcal{J}$. The result of substituting y_i' for y_i in C and its transform C_1 are formal power series C' and C_1'. Let C_1' result from C_1 by the substitution of y_i'' for y_i, $i=1, 2, \cdots$. Evidently C_1'' results from C' by replacing z by z_1 and each coefficient of the expansion by its transform in a field $\mathcal{J}_i$ which contains it.

C_1' may now be obtained from C_1'' by replacing z_1^s, $s=1/k^r$ where r is a sufficiently large integer, by the power series in z substituted for z_1^s during the construction of the z_i' and z_i''. We see that if C' vanishes identically so does C_1'. The converse is also true. For if C' is not identically zero neither is C_1''. Then C_1' begins with a nonzero term obtained from the first term of C_1'', which cannot be cancelled by any other term.

25. It follows that the set of polynomials which are formally annulled when each y_i is replaced by y_i' forms a reflexive difference ideal Λ.

It is obvious that Λ is prime, and that A holds Λ. A polynomial D of zero order cannot hold Λ. For it may be written as a product of linear factors in an algebraic extension of $\mathfrak{J}$, none of which is annulled by the substitution $y_0=y_0'=u+Z$. It follows that Λ is one of the prime reflexive ideals obtained from the basic sequences of A.

Every polynomial of Λ must be annulled by the y_i'. Now on substituting the y_i' into a polynomial C a term of zero degree in z is obtained which is equal to the result of substituting u_i for y_i in C. Since this term vanishes for every polynomial of Λ, Λ is annulled by the substitution $y=u$. Then Λ holds Σ. This proves the theorem.

26. **Constructive methods.** The procedure of Theorem IV enables us to construct all polynomials, of order not exceeding a given integer k, of the basic sequences of an algebraically irreducible difference polynomial A in an unknown y, and of equal order and effective order. Reference to the proof of Theorem IV will, in fact, show that in order to determine successively the polynomials of the basic sequences the operations which must be carried out are: first, formation of the remainder of a polynomial with respect to an ascending set; second, determination of the polynomials G_i whenever a factorization (1) is possible. The first of these steps can obviously be carried out by an actual construction. The second can be carried out, if the coefficient field is analytic, by the methods of §§50 and 55 of A.D.E. In the general case the treatment of §50 of A.D.E. must be replaced by the more general method to be found in van der Waerden's *Moderne Algebra*, vol. 1, p. 130.

We have no means of deciding, in general, at what point in the construction of the basic sequences all factorizations have occurred. We cannot, therefore, complete with present techniques the problem of determining constructively the ordinary manifolds of a given difference polynomial. We may nevertheless solve the following problem:

Given an algebraically irreducible difference polynomial A in the unknown y and of equal order and effective order, it is desired to determine whether a given polynomial B is annulled by the general solution of A.

We know from the proof of Theorem IV that B will be annulled by an ordinary manifold of A if, and only if, it has zero remainder with respect to that portion of the corresponding basic sequence consisting of polynomials of order not greater than that of B. We may determine all ascending sets

$B_{i0}, \cdots, B_{ik}$ which are beginnings of basic sequences of A, such that the order of B_{ik} is that of B. Then for B to be annulled by the general solution of A it is necessary and sufficient that it have zero remainder with respect to each such ascending set.

27. **Nature of the basic sets.** We have studied the resolution of a polynomial A with the aid of its basic sequences. It is desirable to relate these sequences to the basic sets of the ideals connected with A. For this purpose we prove the following theorems:

28. THEOREM VI. *Let A be an algebraically irreducible difference polynomial in the unknowns $u_1, u_2, \cdots, u_q; y$. Then a basic set of the ideal $[A]$ is A.*

Let A be of order n and degree r in y_n. Any polynomial in $[A]$ must vanish for all algebraic solutions. It will be sufficient to prove that a polynomial reduced with respect to A (as a difference polynomial) cannot vanish for all algebraic solutions. This is obviously true of polynomials of order n or less. We shall assume it to be true of polynomials of order less than $n+k$ and prove that it holds for polynomials of that order. Let R be any such polynomial. From the inductive hypothesis we see that there are algebraic solutions which do not annul the initial of R. But since R must be of degree less than r in y_{n+k} the concluding remark of §14 shows that there is an algebraic solution for which R does not vanish. This proves the theorem. We have actually proved the following slightly stronger result:

A is the basic set of the polynomials, powers of which are linear combinations of it and its transforms. Indeed, all polynomials of this ideal are annulled by every algebraic solution, and so cannot be reduced with respect to A.

29. THEOREM VII. *Let A be an algebraically irreducible polynomial in the unknowns $u_1, u_2, \cdots, u_q; y$. Let $B_0, B_1, B_2, \cdots$ be a basic sequence of A determining a prime ideal Λ. Denote by $C_1, \cdots, C_k$ the set consisting of those B_i, $i>0$, which are of lower degree than B_{i-1} in their respective highest transforms. Then $C_0=A, C_1, \cdots, C_k$ is a basic set of Λ.*

Evidently the C_i constitute an ascending set whose members and their transforms vanish for all algebraic solutions of $B_0, B_1, \cdots$. Let R be reduced with respect to $C_0, C_1, \cdots, C_k$. Then R is also reduced in the algebraic sense with respect to $B_0, B_1, \cdots, B_t$, where B_t is of the same order as R. Consequently R is not in the prime system of which $B_0, \cdots, B_t$ is a basic set. It follows that R is not in Λ. Then $C_0, \cdots, C_k$ constitute a basic set of Λ, for no polynomial reduced with respect to this set holds Λ.

30. **Examples of difference manifolds.** We shall conclude this section of our paper by giving some examples of difference polynomials with complicated manifolds having lengthy basic sets. Such examples are necessary to show that the theory developed above is nontrivial.

31. We prove the following theorem.

THEOREM VIII. *Let F be a difference polynomial of zero order and degree $n>1$ which is algebraically irreducible in the field $\mathcal{J}$. Let each element of $\mathcal{J}$ be equal to its transform. Let k be the largest integer such that $\omega_1, \omega_2, \cdots, \omega_n$ constitutes some enumeration of the roots of F, and there exist automorphisms of $\mathcal{J}(\omega_1, \cdots, \omega_n)$ such that $\mathcal{J}$ is fixed and*

$$\omega_1 \to \omega_2,\ \omega_2 \to \omega_3,\ \cdots,\ \omega_{k-1} \to \omega_k,\ \omega_k \to \omega_{k+1},$$

$$\omega_1 \to \omega_2,\ \omega_2 \to \omega_3,\ \cdots,\ \omega_{k-1} \to \omega_k,\ \omega_k \to \omega_m,$$

and $\omega_{k+1} \neq \omega_m$. Then:

(1) *There are n prime ideals in the decomposition of $\{F\}$.*

(2) *The basic set of each of these ideals contains a polynomial of first order and a polynomial linear in its highest transform.*

(3) *At least two of the ideals have polynomials of order k in their basic sets.*

(4) *None of the ideals has a polynomial of order exceeding k in its basic set.*

Any automorphism of the field $\mathcal{J}(\omega_i, \cdots, \omega_n)$ which leaves $\mathcal{J}$ fixed may be considered to define a transforming operation. The ω_i, with their transforms defined by any such transforming operation, constitute a solution of F. Conversely any solution of F defines an automorphism of a subfield of $\mathcal{J}(\omega_1, \omega_2, \cdots, \omega_n)$. We extend this to an automorphism of $\mathcal{J}(\omega_1, \omega_2, \cdots, \omega_n)$ by the specification that such ω_i as are not included in the subfield are to transform into themselves.

We observe that every solution of F is equal to one of its transforms of order n or less, and consequently to its transform of order $n!$. It follows that any irreducible manifold in the manifold of F has a basic set which terminates in a linear polynomial. Otherwise $y_{n!}-y$, which must hold the manifold, would be reduced with respect to its basic set. There must be n prime ideals in the decomposition of $\{F\}$ since the degrees in their highest transforms of the last polynomials in the basic sets must total n.

It is evident that F_1-F is divisible by y_1-y so that, in forming the basic sequences of F, a factorization (1) will occur after a single transform has been taken. It follows that every irreducible manifold of F has a first order polynomial in its basic set. One such manifold is, of course, held by y_1-y, and includes those solutions for which the transforming operation is the identical automorphism. This completes the proof of statements (1) and (2).

32. The first k polynomials of some basic sequence of F will be annulled by a solution for which $y_i=\omega_{i+1}$, $i=0, 1, \cdots, k-1$. Let $B_0, \cdots, B_{k-1}, \cdots$ be the polynomials of this sequence. Any other basic sequence annulled by an algebraic solution with this beginning must also begin with $B_0, \cdots, B_{k-1}$. Let C be the transform of B_{k-1}. Then C must be annulled by both the solutions $y_i=\omega_{i+1}$, $i=0, \cdots, k$, and $y_i=\omega_{i+1}$, $i=0, \cdots, k-1$, $y_k=\omega_m$. Then C must be of greater than first degree in y_k. Consequently B_{k-1} is not linear in y_{k-1}, and there must be a factorization (1) involving polynomials of order at

least k.

33. Conversely, let us assume that a polynomial of order k or greater, in a basic sequence of F, is nonlinear in its highest transform. We could then obtain a beginning of an algebraic solution $\omega_{i_1}, \omega_{i_2}, \cdots, \omega_{i_r}, r>k$, which could be extended in two or more ways to algebraic solutions of a basic sequence. Each of these algebraic solutions would then become, when transforms are properly defined, a solution defining an automorphism of $\mathcal{J}(\omega_1, \cdots, \omega_n)$. Then there would be two such automorphisms and in each we would have $\omega_{i_1}\rightarrow\omega_{i_2}, \omega_{i_2}\rightarrow\omega_{i_3}, \cdots, \omega_{i_{r-1}}\rightarrow\omega_{i_r}, r>k$, contrary to the hypothesis of our theorem. We conclude that all polynomials of order k or greater in the basic sequences must be linear in their highest transforms. Then the basic sets of the irreducible manifolds of F will not contain polynomials of order exceeding k. We have shown that at least two such basic sets contain polynomials of order at least k. This proves the theorem.

34. Consider, as an example, the polynomial y^4-2y^2-1 whose roots are $\pm(1\pm 2^{1/2})^{1/2}$. We shall work in the field R of rational numbers. On subtracting this polynomial from its transform we obtained the factors y_1-y, y_1+y and $y_1^2+y^2-2$. The former correspond to the identical automorphism and the automorphism $+(1+2^{1/2})^{1/2}\rightarrow-(1+2^{1/2})^{1/2}$. We shall show that the latter factor is not reducible without further transforming. From the original equation we see that $y^2-2=1/y^2$ and substituting this we obtain $y_1^2=-1/y^2$, $y_1=\pm i/y$, $y_1y=\pm i$. Thus if y_1 were in the field $R((1+2^{1/2})^{1/2})$ this field would contain i. Evidently it contains only real numbers. It follows that we must use the next transform to obtain a factorization of $y_1^2+y^2-2$. Subtracting this polynomial from its transform we find the factors y_2-y, y_2+y. These correspond to the automorphisms:

$$(1+2^{1/2})^{1/2}\rightarrow(1-2^{1/2})^{1/2}\rightarrow(1+2^{1/2})^{1/2},$$
$$(1+2^{1/2})^{1/2}\rightarrow(1-2^{1/2})^{1/2}\rightarrow-(1+2^{1/2})^{1/2}.$$

The various basic sets are obtained by following the arrows in the diagram.

$$\begin{array}{ccccc} & & y_1-y & & y_2-y \\ y^4-2y^2-1 & \rightarrow & y_1^2+y^2-2 & \begin{array}{c}\nearrow\\ \searrow\end{array} & \\ & & y_1+y & & y_2+y \end{array}$$

35. It is desirable to obtain examples of this sort for genuine difference equations of order greater than zero. To do this we let P be the homogeneous difference polynomial of order 1 obtained by substituting y_1/y for y in F and multiplying by y^n.

In any of the difference fields $\mathcal{J}(\omega_1, \cdots, \omega_n)$, P separates into linear factors and the solutions annulling these factors are isomorphic to algebraic solutions of the form $y_1=\omega_i y$, $y_2=\omega_j y_1, \cdots$. All these solutions may be

considered as solutions of P over the field $\mathcal{J}$.

Conversely, if y is any solution of P as a polynomial in $\mathcal{J}$, $y_1/y=\omega_i$ for some i, so that the solution will define some ω_i and its transforms and be identical with a solution in one of the fields $\mathcal{J}(\omega_1, \cdots, \omega_n)$. Evidently the algebraic solution must be of the form $y_1=\omega_i y$, $y_2=\omega_j y_1=\omega_j\omega_i y$ and $\omega_i, \omega_j, \cdots$ must constitute a succession of transforms of ω_i. The algebraic solutions of P are therefore merely the algebraic solutions of F multiplied by the appropriate transform of y.

We may now apply the reasoning of Theorem VIII to derive analogous statements concerning P(22). The polynomial y_1-y is replaced by $y_2/y_1-y_1/y$ or $y_2y-y_1^2$ which is annulled by all solutions for which the transforming operation in $\mathcal{J}(\omega_1, \cdots, \omega_n)$ is the identical automorphism.

$y_{(n+1)!}/y_{n!}-y_1/y$ or $y_{(n+1)!}y-y_{n!}y_1$ vanishes for all solutions and plays the same role as $y_{n!}-y$ in Theorem VIII. The details of the proof may be left to the reader.

36. As a final example we shall consider the polynomial $Q=1+yP+y_1^p$, where p is any odd prime and the coefficient field is the field R of rational numbers. $Q_1-Q=y_2^p-y^p$ is divisible by y_2-y so that a factorization occurs at this point. We shall show that the factors of second order are not all linear.

Let ω be a pth root of unity, $\omega\neq 1$. We may define a transforming operation in $R(\omega)$ by the automorphism $\omega\rightarrow\omega^i$, for any $i=1, 2, \cdots, p-1$. In any of the difference fields $R(\omega)$, $y_2^p-y^p$ separates into linear factors from which we can determine algebraic solutions, isomorphic to solutions, of Q in this field. Such solutions have the form y, $y_1=(-1-y^p)^{1/p}$, $y_2=\omega y$, $y_3=\omega^i y_1 =\omega^i(-1-y^p)^{1/p}, \cdots$.

Now when Q is considered as a polynomial in R its basic sequences, except the one including y_2-y, must also have the algebraic solutions $y_1=(-1-y^p)^{1/p}$, $y_2=\omega y$, for some pth root ω of unity. For given ω there can exist but one beginning Q, S of a basic sequence which is annulled by this algebraic solution. For the same ω this solution, together with $y_3=\omega^i y_1 =\omega^i(-1-y^p)^{1/p}$, for each i from 1 to $p-1$, is an algebraic solution of the beginning of a basic sequence of Q as a polynomial in some difference field obtained from $R(\omega)$. From each such algebraic solution we obtain a solution of Q in an extension of R, and no two such solutions are isomorphic. Since they annul no polynomial of zero order, each of these solutions must be a general point of a prime ideal determined by a basic sequence of Q. Evidently each annuls Q, S, and to each must correspond a distinct algebraic solution of a continuation of Q, S, to a set of three polynomials. There are then at least $p-1$ such extensions, so that S is of degree $p-1$. Evidently S and y_2-y are the only polynomials obtained at the first factorization.

We can compute the third polynomials in the basic sequences beginning

(22) Of course k becomes $k+1$ in (3) and (4) of Theorem VIII and polynomials of second order replace polynomials of the first order in (2).

with Q, S. For we have always $(y_3/y_1)^p=(y_2/y)^p=1$ so that y_3/y_1 and y_2/y are both roots of unity, and for some k we must have $y_3/y_1=(y_2/y)^k$. Then $\prod(y_3y^k-y_2^ky_1)$ holds the manifolds determined by Q, S. Evidently each irreducible manifold arising from Q, S is held by some polynomial $y_3y^k-y_2^ky_1$, and has therefore a polynomial linear in y_3 following S in its basic sequence. We conclude that there must be $p-1$ such manifolds. The basic set of Q must then be([23]).

$$
\begin{array}{lll}
 & & y_3y - y_2y_1 \\
 & y_2^{p-1} + yy_2^{p-2} + \cdots + y^{p-1} \nearrow & \rightarrow y_3y^2 - y_2^2y_1 \\
Q \nearrow & & \searrow \\
 & & \text{— — — — — — —} \\
 & & \text{— — — — — — —} \\
\searrow & y_2 - y & \text{— — — — — — —} \\
 & & \searrow y_3y^{p-2} - y_2^{p-2}y_1 \\
 & & \searrow y_3y^{p-1} + y_1(yy_2^{p-2} + y^2y_2^{p-3} + \cdots + y^{p-1})
\end{array}
$$

All polynomials of the form $1+y^p+y_1^p+\cdots+y_n^p$ may be treated similarly.

Part III. Dimensionality and the resolvent

37. We shall consider systems of polynomials in unknowns $u_1, \cdots, u_q$; $y_1, \cdots, y_p$, where the u_i constitute a set of arbitrary unknowns. Transforms of the u_i and y_i will be denoted by a second subscript.

For the basic sets of such systems we shall also employ a double subscript notation, denoting by A_{i0} the polynomial introducing y_i and by $A_{i1}, \cdots, A_{i,j_i}$ the other polynomials of the same class and successively higher orders. We shall refer to the A_{i0} as the *leaders* of the basic set. The following theorem holds:

38. Theorem IX. *In order that the ascending set $A_{10}, \cdots, A_{i-1,j}$ $A_{i0}, \cdots, A_{pk}$, where the subscript i has any fixed value from 1 to p, be the basic set of a reflexive prime ideal with coefficients in the field $\mathcal{J}$ it is necessary and sufficient that:*

(1) *$A_{10}, \cdots, A_{i-1,j}$ be the basic set of a reflexive prime ideal Σ in the unknowns $u_1, \cdots, u_q$; $y_1, \cdots, y_{i-1}$ with coefficients in $\mathcal{J}$.*

(2) *When the general point of Σ is substituted for $u_1, \cdots, u_q$; $y_1, \cdots, y_{i-1}$ in $A_{i0}, \cdots, A_{pk}$ the latter become the basic set of a reflexive prime ideal in the unknowns $y_i, \cdots, y_p$ with coefficients in the remainder class field of Σ.*

We shall first prove necessity. Let Λ be a reflexive prime ideal with coefficients in a difference field $\mathcal{J}$ and with basic set $A_{10}, \cdots, A_{i-1,j}$; $A_{i0}, \cdots, A_{pk}$. We denote by Σ the ideal consisting of those polynomials of Λ which involve only the u_j and $y_1, \cdots, y_{i-1}$. Evidently Σ is a reflexive prime ideal and has

([23]) Since $y_3y^{p-1}-y_2^{p-1}y_1$ is not reduced with respect to S, it is replaced in the basic set by its remainder with respect to Q, S.

$A_{10}, \cdots, A_{i-1,j}$ for its basic set.

Let $\mathfrak{J}'$ be the quotient field of the remainder classes of Σ. We denote by B' the result of substituting the general point of Σ for the u_i and $y_1, \cdots, y_{i-1}$ in any polynomial B.

The initials of $A_{i0}, \cdots, A_{pk}$ are not annulled by this substitution. Consequently the polynomials of $A'_{i0}, \cdots, A'_{pk}$ constitute an ascending set with coefficients in $\mathfrak{J}'$. We represent by Φ the reflexive difference ideal consisting of all polynomials in $y_i, \cdots, y_p$, with coefficients in $\mathfrak{J}'$, which are annulled by all regular solutions of this ascending set. We shall show that Φ is a prime difference ideal.

We let $U'V'$ hold Φ and prove that either U' or V' holds Φ. We may assume that U' and V' can actually be obtained from polynomials U and V with coefficients in $\mathfrak{J}$ by the appropriate substitution. This situation may, if necessary, be brought about by multiplying the given polynomials by suitable elements of $\mathfrak{J}'$ without affecting their inclusion in Φ.

There exists a polynomial P', which is a product of powers of initials and transforms of initials of $A'_{i0}, \cdots, A'_{pk}$, and which is such that $P'U'V' - L' = 0$, where L' is a linear combination of $A'_{i0}, \cdots, A'_{pk}$ and their transforms with coefficients which are polynomials with coefficients in $\mathfrak{J}'$. In this equation we substitute the u_j and $y_1, \cdots, y_{i-1}$ for the general point of Σ([24]). We obtain $PUV - L = T$, where T is a rational expression in the $u_i, y_1, \cdots, y_p$ and their transforms whose numerator does, but whose denominator does not, hold Σ, L is a linear combination of $A_{i0}, \cdots, A_{pk}$ and their transforms with rational coefficients whose denominators do not hold Σ, and P is a product of powers of initials and transforms of initials of $A_{i0}, \cdots, A_{pk}$. It readily follows that either U or V, say U, holds Λ.

Any regular solution of $A'_{i0}, \cdots, A'_{pk}$, in conjunction with the general point of Σ, is a solution of Λ and therefore annuls U. It follows that a regular solution of $A'_{i0}, \cdots, A'_{pk}$ annuls U'. Then U' is in Φ and the latter must be a reflexive prime difference ideal. $A'_{i0}, \cdots, A'_{pk}$ is the basic set of Φ. For let B' be reduced with respect to $A'_{i0}, \cdots, A'_{pk}$. We assume as before that B' is derived from a polynomial B by a substitution of the general point of Σ for the u_{ij} and $y_1, y_2, \cdots, y_{i-1}$. Let C be the remainder of B with respect to $A_{10}, \cdots, A_{i-1,j}$. We see that if $C=0$, $B'=0$. Otherwise C is reduced with respect to $A_{10}, \cdots, A_{pk}$. The general point of Λ cannot then annul C. Then it does not annul B. It follows that B' cannot hold Φ. This proves that $A'_{i0}, \cdots, A'_{pk}$ is a basic set of Φ.

([24]) This substitution is, of course, not unique, and we may even replace a given element of the general point in different ways in the same equation. T depends, of course, on the particular substitution used, but it is evident that it will always have the properties stated in the text. We note, for use in the next paragraph, that the polynomial C corresponding as above to a polynomial C' with coefficients in $\mathfrak{J}'$ may always be chosen so as to involve only the same power products of transforms of $y_{i+1}, \cdots, y_p$ as occur in C'.

The necessity of conditions (1) and (2) has now been completely verified.

39. We now consider an ascending set $A_{10}, \cdots, A_{pk}$ satisfying the given conditions. We shall prove that it is the basic set of a reflexive prime ideal. Let Λ be the ideal consisting of all polynomials which vanish for the solutions of $A_{10}, \cdots, A_{i-1,j}; A_{i0}, \cdots, A_{pk}$ which are obtained by letting the arbitrary unknowns and $y_1, \cdots, y_{i-1}$ be elements of the general point of Σ used in condition (2) and $y_i, \cdots, y_p$ be elements of a general point of Φ. Then Λ is reflexive. We shall show that it is also prime.

Let UV hold Λ. We substitute for the arbitrary unknowns and $y_1, \cdots, y_{i-1}$ of U and V a general point of Σ obtaining U' and V'. If either U' or V' is zero, U or V holds Λ. We assume this is not the case. Then $U'V'$ is annulled by the general point of Φ and is consequently in Φ. Since Φ is prime, either U' or V', say U', holds Φ. Then U is in Λ. This proves the statement of the preceding paragraph.

Let R be reduced with respect to $A_{10}, \cdots, A_{i-1,j}; A_{i0}, \cdots, A_{pk}$. Then R', the polynomial which results from substituting into R a general point of Σ, is not zero and is reduced with respect to $A_{i0}, \cdots, A_{pk}$. Since Φ is prime reflexive, R' does not hold Φ. It follows that R does not hold Λ and that $A_{10}, \cdots, A_{i-1,j}; A_{i0}, \cdots, A_{pk}$ is a basic set of Λ. This demonstrates the sufficiency of conditions (1) and (2) and completes the proof of Theorem IX.

40. As a simple example of the ideals we are discussing, consider the pair of polynomials y_1^2-x, $y_2^2-(x+k)$ where k is any positive integer, in the field $R(x)$ of rational functions of x, with the transform of x defined to be $x+1$.

y_1^2-x has a general solution consisting of one irreducible manifold. For if a factorization equation (1) of Part II could be obtained, there would exist an integer n such that $(x+n)^{1/2}$ could be expressed rationally in terms of $x^{1/2}, (x+1)^{1/2}, \cdots, (x+n-1)^{1/2}$. Any such rational expression returns to its original value as one traces a small circle about the point $-n$ in the plane of the complex variable x, whereas $(x+n)^{1/2}$ changes sign. It follows that the expressions cannot be equal, so that no factorization occurs.

The same proof indicates that $y_2^2-(x+k)$ will remain irreducible in the field obtained by adjoining to R the first $k-1$ transforms of y_1. However, if we subtract from $y_2^2-(x+k)$ the kth transform of y_1^2-x we get $y_2^2-y_{1k}^2 = (y_2-y_{1k})(y_2+y_{1k})$. Evidently the system has two irreducible manifolds, one with basic set

$$y_1^2 - x, \qquad y_2 - y_{1k},$$

and the other with basic set

$$y_1^2 - x, \qquad y_2 + y_{1k}.$$

These basic sets obviously satisfy the conditions of Theorem IX.

The number of transforms required before factorization occurs is the

integer k which can be made arbitrarily large. We see that this number is not limited by the degree or order of the polynomials. For this reason our methods will not suffice in general even for the construction of the beginnings of basic sets of prime ideals involving several dependent unknowns.

41. **Order and effective order of a prime ideal.** We began the description of the dimensionality of a reflexive prime difference ideal in §1, where we proved that the number of arbitrary unknowns is a constant for the ideal. We shall now complete this description by defining the order and effective order of a reflexive prime ideal in any number of unknowns.

Let Λ, then, be a reflexive prime ideal in the unknowns $u_1, \cdots, u_q$; $y_1, \cdots, y_p$, the u_i arbitrary, with coefficients in a difference field $\mathcal{J}$. Let $\mathcal{G}$ be the quotient field of the remainder classes of Λ. Then $\mathcal{G}$ contains a general point of Λ. We shall show that $\mathcal{G}$ is isomorphic to a field which is, in the algebraic sense, of finite degree of transcendence s over a difference field $\mathcal{J}(v_i)$ obtained by adjoining successively to $\mathcal{J}$ transformally transcendental elements v_i, $i=1, 2, \cdots, q$. *Then s is the order of* Λ. Let r be the smallest integer such that there exists a subfield $\mathcal{K}$ of $\mathcal{G}$, isomorphic to a field of degree of transcendence r over $\mathcal{J}(v_i)$, and containing all but a finite number of the elements of $\mathcal{G}$ which are remainder classes of the y_{ij}. *Then r is the effective order of* Λ.

It is evident that s and r, if they exist, are independent of the ordering of the y_{ij} and, for $p=1$, coincide with the order and effective order as defined in Part II. Their values may vary with the choice of the set of arbitrary unknowns.

42. Before proceeding to the proof of the existence of s and r, and the determination of their values, we must construct, by means of Theorem IX, a set of ideals $\Sigma_1, \cdots, \Sigma_p$. Let $i=2$ in the statement of Theorem IX. Then the ideal Σ of that theorem is the ideal we shall now call Σ_1. It will consist of all polynomials of Λ which are free of $y_2, \cdots, y_p$. To the corresponding ideal Φ we again apply Theorem IX with $i=2$, and define Σ' and Φ'. Σ' is the prime ideal consisting of all polynomials of Φ in y_2 only, while Φ' is the ideal in $y_3, \cdots, y_p$ defined by the procedure of Theorem IX. Σ' is the ideal we shall designate as Σ_2. From Φ', by a further application of the same procedure, we obtain Σ_3 and Φ''. Eventually we get all the Σ_i.

We now construct a general point of Λ. Let $u_i=v_i$, $i=1, 2, \cdots, q$; and let y_1 be given its value in a general point of Σ_1 with $u_i=v_i$. Adjoining this solution to $\mathcal{J}$ we obtain the field $\mathcal{J}_1(v_i)$. $\Sigma_2, \cdots, \Sigma_p$ may be constructed using this general point for Σ_1. To this field we adjoin a value of y_2 which is a general point of Σ_2, forming $\mathcal{J}_2(v_i)$. We continue this procedure adjoining successively the general points of each Σ_i, $i=3, 4, \cdots, p$, as values of $y_3, \cdots, y_p$, and forming successively the fields $\mathcal{J}_3(v_i)$, $\mathcal{J}_4(v_i)$, $\cdots$, $\mathcal{J}_p(v_i)$. The resulting solution is a general point of Λ, for we observe, by successive applications of Theorem IX, that Λ consists of all polynomials annulled by the indicated

solution of the Σ_i. The field $\mathcal{J}_p(v_i)$ contains a general point of Λ. But every element of $\mathcal{J}_p(v_i)$ is either in $\mathcal{J}$ or is a rational combination, with coefficients in $\mathcal{J}$, of elements of the general point. Then $\mathcal{J}_p(v_i)$ is isomorphic with $\mathcal{G}$, the quotient field of the remainder classes of Λ. Evidently $\mathcal{J}_p(v_i)$ is of degree of transcendence over $\mathcal{J}(v_i)$ equal to the sum of the orders of the Σ_i. But this quantity is s. Since the order of each Σ_i is equal to the order of the first polynomial in its basic set, s equals the sum of the orders of the leaders of a basic set of Λ in the unknown of highest class which they respectively involve.

43. The existence of a finite r follows from that of s, since r cannot exceed s.

To determine r we make the substitution $z_i = y_{i,t_i}$, $i = 1, 2, \cdots, p$, the t_i positive integers to be specified later. Those polynomials of Λ which can sustain this substitution become the polynomials of a reflexive prime ideal Λ^+ in the z_i. Λ^+ is of the same effective order as Λ. Let $y_{ij} = \alpha_{ij}$ be the values of the general point solution of Λ constructed in the previous paragraph. Then $z_{ij} = \alpha_{ik}$, $k = j + t_i$, will be the general point of Λ^+. We see that for large t_i this general point will lie in a field isomorphic to a subfield of the subfield $\mathcal{K}$ used to define the effective order of Λ. In that case Λ will be of equal order and effective order.

Let ideals Σ_i^+ be constructed from Λ^+ as the Σ_i were constructed from Λ. Σ_1^+ consists of all polynomials of Λ^+ in z_1 and the u_i only. Then Σ_1^+ can be obtained from Σ_1 by making the transformation $z_1 = y_{1,t_1}$ wherever possible in the polynomials of Σ_1. $z_{1j} = \alpha_{1,j+t_1}$ will be a general point of Σ_1^+. Σ_2^+ consists of those polynomials of Λ in y_1, y_2 and the u_i only, in which the substitutions $z_1 = y_{1,t_1}$, $z_2 = y_{2,t_2}$ and then the substitution $\alpha_{1,j+t_1} = z_{1,j}$ have been made. In general Σ_k^+ consists of those polynomials of Λ in which the substitutions

$$(1) \qquad z_i = y_{i,\ t_i}, \quad i = 1, 2, \cdots, k, \quad \alpha_{i,j+t_i} = z_{ij}, \quad i = 1, 2, \cdots, k-1,$$

can be and have been made. The order of Λ^+ is the sum of the orders of the Σ_k^+.

44. Let s_1 be the difference between the order and effective order of A_{10}. We choose a transform of A_{20} which is free of y_{1i}, $i < s_1$. Let s_2 be the difference between its order and effective order in y_2. We choose a transform of A_{30} free of y_{1i}, $i < s_1$, and y_{2j}, $j < s_2$, and let s_3 be the difference between its order and effective order in y_3. Similarly we define $s_4, s_5, \cdots, s_p$. Then the transformation $w_i = y_{i,s_i}$ carries a transform of each A_{i0} into a polynomial A'_{i0} whose order and effective order are equal. We now let $t_i = t + s_i$, where t is chosen sufficiently large so that Λ^+ is of equal order and effective order for the resulting t_i. The transformation $z_i = y_{i,t_i} = w_{it}$ carries the tth transform of each A'_{k0} into a polynomial A^+_{k0} of equal order and effective order in z_k.

To compute the effective order of Λ we need merely find the order of Λ^+, and this is the sum of the orders of the Σ_i^+. Now each Σ_i^+ is held by a polynomial A^+_{i0} whose order in z_i is the effective order of A_{i0} in y_i. Let us suppose

that there is a $k \leqq p$ such that Σ_k^+ is held by a polynomial B^+ of order less than the order of A_{k0}^+. If in B^+ we replace z_k by y_{k,t_k} we obtain a polynomial B of Σ_k of effective order less than that of A_{k0} in y_k. But the first polynomial of the basic set of Σ_k is of effective order equal to that of A_{k0} in y_k. Then Σ_k is of this effective order. Thus B^+ cannot exist. We see that every Σ_i^+ is of order equal to the effective order of A_{i0} in y_i. The effective order r of Λ is the sum of these orders and is therefore the sum of the effective orders of the A_{i0} in the y_i.

These results enable us to describe the dimensionality of any reflexive prime difference ideal first by means of the number of arbitrary unknowns, a constant for the ideal as proved in Theorem III, and second by means of its order and effective order which have been defined above. For the order and effective order the following theorem holds:

THEOREM X. *The order and effective order of a reflexive prime ideal are equal to the sum of the orders and the sum of the effective orders respectively of the leaders of a basic set of the ideal in the unknowns which each leader respectively introduces.*

45. **Quasi-linear systems.** A nontrivial reflexive prime ideal Σ of difference polynomials in the unknowns $y_1, \cdots, y_p$ with coefficients in the field $\mathcal{J}$ shall be said to be quasi-linear if, in every extension of $\mathcal{J}$, there exists at most one set of values of $y_1, \cdots, y_p$ which annuls the polynomials of Σ.

A quasi-linear system may not be held by linear zero-order polynomials in its unknowns. For example, let us adjoin to the field R of complex numbers, with the transform of each number defined to be equal to the number itself, an element k satisfying the equation $y_1 - y^2 = 0$. This may be accomplished in an abstract field by adjoining the general point of $\{y_1 - y^2\}$ whose existence is assured by Theorem IV, or analytically by adjoining the function e^u, where $u = 2^z$.

Considering the abstract case, we know that the difference field $R(k)$ is isomorphic, so far as the algebraic operations are concerned, with the field obtained by adjoining to R an algebraic solution of $y_1 - y^2$. Let $y = \alpha$, where α is transcendental over R, be the first element of an algebraic solution. We solve successively for $y_1, y_2, \cdots$ from the equation $y_1 - y^2 = 0$ and its transforms. On account of the linearity of these equations every y_i lies in the field $R(\alpha)$, where the adjunction is now made in the sense of algebra. Then $R(k)$ is isomorphic in the sense of algebra to this field, and k corresponds to α under this isomorphism. Since $R(\alpha)$ does not contain an element whose cube is α, $R(k)$ does not contain an element whose cube is k. We consider the equation $y^3 - k = 0$, which is algebraically irreducible in $R(k)$.

Taking the transform of this equation and using the relation $k_1 = k^2$ we obtain $y_1^3 - y^6 = 0$. $y_1^3 - y^6$ has the irreducible factor $y_1 - y^2$, so that $y^3 - k$, $y_1 - y^2$ is the basic set of a prime ideal Σ. We shall show that Σ is quasi-

linear[25].

Theorem IV shows that Σ has solutions. Let $y=\alpha$ be a solution of Σ in any extension R' of $R(k)$. Evidently $\alpha_1=\alpha^2$. The only other solutions of $y^3-k=0$ in R' or any extension of R' are $\beta=\omega\alpha$, $\gamma=\omega^2\alpha$, where ω is a complex cube root of unity. But $\beta_1=\omega\alpha_1=\omega\alpha^2\neq\beta^2$, $\gamma_1=\omega^2\alpha_1=\omega^2\alpha^2\neq\gamma^2$. Then β and γ do not annul y_1-y^2, and so do not annul Σ. Thus $y=\alpha$ is the only solution of Σ in any extension of R'.

46. We shall prove the following theorem.

THEOREM XI. *Let Σ be a quasi-linear ideal in the unknowns $y_1, \cdots, y_n$ with coefficients in a field $\mathcal{J}$. Let $A_{10}, A_{11}, \cdots, A_{1j}; A_{20}, A_{21}, \cdots, A_{2k}; \cdots; A_{n0}, A_{n1}, \cdots, A_{np}$ be a basic set of Σ, where each A_{i0} introduces y_i. Then each A_{i0} is of effective order zero in y_i.*

Assume that some A_{i0} is not of zero effective order in y_i. We adjoin to $\mathcal{J}$ the general point of Σ forming a field $\mathcal{G}$. Let $\mathcal{J}_1$ be the field consisting of those elements of $\mathcal{G}$ which are algebraic over $\mathcal{J}$.

The set of all polynomials with coefficients in $\mathcal{J}_1$ which vanish for the general point we have just considered forms a prime ideal Σ_1. Obviously, a polynomial with coefficients in $\mathcal{J}$ is in Σ_1 if and only if it is in Σ. Σ_1 is quasi-linear, for its solutions are solutions of Σ. Some leader of the basic set of Σ_1 is not of effective order zero. Otherwise Σ_1 would have by Theorem X a general point solution in which all but a finite number of the y_{ij} are algebraic over $\mathcal{J}_1$ and therefore over $\mathcal{J}$. This general point solution would also be a general point of Σ. For, otherwise, it would annul a polynomial with coefficients in $\mathcal{J}$ which is not in Σ. But, by a previous remark, no such polynomial is in Σ_1. Our assumption about the A_{i0} shows that Σ cannot have a general point of this character.

We may assume that Σ_1 is of equal order and effective order. For, if it is not, it may be replaced in all that follows by an ideal with this property obtained from it by a substitution of the form $z_i=y_{i,l_i}$.

Let $C_{10}, C_{11}, \cdots, C_{1r}; C_{20}, \cdots, C_{ns}$ be a basic set of Σ_1. We construct the prime algebraic ideals Φ_k consisting of all polynomials of Σ_1 of order not exceeding k in each y_i. We order the y_{ij} in Φ_k so that y_{ij} precedes y_{mn} if $i<m$ or if $i=m$ and $j<n$. For each k we choose a basic set of Φ_k. It is evident that, if k is sufficiently large, the polynomials of class t in the basic set of Σ_1 can be formed from the polynomials introducing the y_{tj} in a basic set of Φ_k, by the procedure used in Theorem VII for extracting a basic set from a basic se-

(25) We might have considered the simpler basic set y^2-k, y_1-k in the field obtained by adjoining k to the rational numbers only. This system is also easily seen to be quasi-linear. However, y^2-k becomes reducible if inverse transforms of k are adjoined to the coefficient field, and one might be led to think that the absence of inverse transforms is an essential feature of the phenomenon. Our example in the text shows it is not, since this example evidently remains valid when inverse transforms of k are adjoined.

quence. In particular we may thus obtain the basic set $C_{10}, \cdots, C_{1r}$; $C_{20}, \cdots, C_{ns}$ of Σ_1.

Let us consider an extension $\mathfrak{K}$ of the coefficient field $\mathfrak{J}_1$ such that Σ_1 has a general point in an extension of $\mathfrak{K}$, and with the following property: for any k the set Ψ_k of polynomials in $\mathfrak{K}$, of order not exceeding k in each y_i, which are annulled by every general point of Φ_k in an extension of $\mathfrak{K}$ constitutes a prime system having the same basic set as Φ_k. A general point of the prime difference ideal Σ_1 furnishes a general point of every Φ_k and therefore annuls every Ψ_k.

We shall need the following observation: We may choose for a basic set of Ψ_k a basic set of Φ_k. Let P be a product of powers of initials of the polynomials of this basic set. Then the transform of P is not annulled by a general point of Σ_1 and so is not in Ψ_{k+1}.

Let Ψ be the union of the Ψ_k. Ψ is a difference ideal. For suppose S is in Ψ. Then S has zero remainder with respect to the basic set of some Ψ_k. Taking the transform of the equation which expresses this fact we see that the product of the transform S_1 of S by a polynomial not in Ψ_{k+1} is a linear combination of polynomials of Ψ_{k+1}. Then S_1 is in Ψ_{k+1} and therefore in Ψ.

Ψ is annulled by the general point of Σ_1 in an extension of $\mathfrak{K}$. We shall see that Ψ is a prime reflexive ideal. It is prime in consequence of the fact that the Ψ_k are prime. To prove that Ψ is reflexive let S be a polynomial which does not hold Ψ. We shall assume that its transform S_1 holds Ψ and obtain a contradiction.

Since S is in no Ψ_k there is a polynomial T which is a linear combination of S and the polynomials of some Ψ_k and is of lower order than C_{i0} in y_i for every i from 1 to n. T_1, the transform of T, must hold Ψ and is therefore annulled by every general point of Φ_m for some m.

We may assume that m is sufficiently large so that the set $C_{10}, \cdots, C_{ns}$ may be extracted from a basic set of Ψ_m. Let $D_{10}, \cdots, D_{20}, \cdots, D_{nt}$ be a basic set of Ψ_m, where D_{ij} introduces a transform of y_i. Evidently $D_{i0} = C_{i0}$ and the unconditioned unknowns of Ψ_m are those y_{ij} with j less than the order of D_{i0} in y_i.

Let y_{1p} be the highest transform of y_1 appearing in D_{10}. Then T_1 involves no transform of y_1 of order exceeding p. T_1 is free of y_{10}, which appears effectively in D_{10}. It follows that the resultant R of T_1 and D_{10} with respect to y_{1p} is a nonzero polynomial. The ascending set formed by selecting the polynomials of the form D_{1j} from the basic set of Ψ_m has a regular solution not annulling R or the coefficients of the power products of the y_{ij}, $i > 1$, in $D_{20}, \cdots, D_{nt}$. Then this solution does not annul T_1.

Let the transforms of y_1 be replaced in T_1 and $D_{20}, \cdots, D_{nt}$ by the values of this regular solution giving a nonzero polynomial T_1', and an ascending set $D_{20}', \cdots, D_{nt}'$ which is the basic set of a prime system.

T_1' is free of y_{20}, which appears in D_{20}', and it involves no y_{2k} higher than

those present in D'_{20}. Replacing D'_{20}, if necessary, by an irreducible factor we may repeat the preceding construction and obtain a regular solution of the ascending set formed by the polynomials D'_{2j} which does not annul T'_1 or the coefficients of power products of the y_{ij}, $i>2$, in $D'_{30}, \cdots, D'_{nt}$.

We continue this process for each D_{i0}. The resulting values of the y_i form a regular solution of $D_{10}, \cdots, D_{nt}$, and therefore a solution of Ψ_m, which does not annul T_1. This contradicts our assumption, so that Ψ must be a reflexive ideal. Since the Ψ_i have the same relation to Ψ that the Φ_i have to Σ_1 we see that $C_{10}, \cdots, C_{ns}$ is a basic set of Ψ.

We shall now show that $\mathcal{G}$ is an extension of $\mathcal{J}_1$ satisfying the condition imposed on $\mathcal{H}$ in the preceding paragraph. This will follow if we can show that an algebraically irreducible resolvent R_k of Φ_k remains algebraically irreducible in $\mathcal{G}$([26]). We shall show, indeed, that every polynomial irreducible in $\mathcal{J}_1$ is irreducible in $\mathcal{G}$. Consider a polynomial S. Choose its initial for some ordering of the unknowns, then the initial of its initial, and so on, till an element of the coefficient field results. Without loss of generality we may assume that this element is $+1$ and place a similar restriction on the factors of S in any field. Then the factorization is unique. If S is a polynomial in one unknown it separates into linear factors in some algebraic extension of $\mathcal{J}_1$. Then all possible factors of S satisfying our restriction on the initials are products of these linear factors and have coefficients algebraic over $\mathcal{J}_1$. Now every element of $\mathcal{G}$ which is algebraic over $\mathcal{J}_1$ is in $\mathcal{J}_1$. Consequently any factor of S with coefficients in $\mathcal{G}$ has coefficients in $\mathcal{J}_1$, and if S is irreducible in $\mathcal{J}_1$ it must be irreducible in $\mathcal{G}$. If S is a polynomial in several unknowns its factors may be found by modifying appropriate factors of a related polynomial in one unknown, with coefficients in the same field([27]). It follows again that S has identical factorizations in $\mathcal{J}_1$ and $\mathcal{G}$, so that an irreducible S remains irreducible in $\mathcal{G}$. Our statement concerning $\mathcal{G}$ is proved, and we see that $C_{10}, \cdots, C_{ns}$ is the basic set of a reflexive prime ideal Ψ with coefficients in $\mathcal{G}$, which is annulled by a general point of Σ_1.

Now Σ_1 has a general point which lies in $\mathcal{G}$ and is a solution of Ψ. It must be the only solution of Ψ, for otherwise Σ_1 would not be quasi-linear. It

---

([26]) For then R_k, and the linear equations determining the unknowns of Φ_k in terms of the resolvent unknown w, form the basic set of a prime system T_k in $\mathcal{G}$. Let Ψ'_k be the set of polynomials in T_k free of w. A general point of Φ_k, together with the corresponding value of w, furnishes a regular solution of the basic set of T_k and consequently annuls all polynomials of Ψ'_k. Conversely, suppose a polynomial B with coefficients in $\mathcal{G}$ is annulled by every general point of Φ_k in any extension of $\mathcal{G}$. Then B vanishes for a general point of T_k, constructed from a general point of Φ_k, and is therefore in Ψ'_k. Then Ψ'_k is precisely the ideal Ψ_k we defined above. Both Ψ_k and Φ_k are of the same degree, namely that of R_k. Then the basic set of Φ_k is a basic set of Ψ_k. For, if not, the product of the degrees of the polynomials of a basic set of Ψ_k will be lower than the corresponding product for Φ_k. But these products are the degrees of the ideals and must therefore be equal. Thus our statement is proved.

([27]) See van der Waerden, *Moderne Algebra*, 1st ed., vol. 1, p. 129.

follows that the basic set of Ψ consists of linear zero-order polynomials. This contradicts the fact that $C_{10}, \cdots, C_{ns}$ is a basic set of Ψ, and some C_{i0} is not of zero order. Thus Theorem XI is established[28].

47. Let Σ be a nontrivial prime ideal in the field $\mathcal{J}$ with unknowns $u_1, \cdots, u_q; v_1, \cdots, v_r; y_1, \cdots, y_s$, where the u_i form a set of arbitrary unknowns. We shall say that Σ is *quasi-linear in the unknowns* $y_1, \cdots, y_s$ if, for any values of $u_1, \cdots, u_q; v_1, \cdots, v_r$, not annulling some polynomial G in these unknowns which does not hold Σ, there exists at most one set of values of the y_i in any extension of $\mathcal{J}$, which annuls Σ.

We represent by Λ the reflexive prime ideal consisting of those polynomials of Σ which are free of the y_i. G is not annulled by the general point of Λ.

Using the ordering $u_1, \cdots, u_q; v_1, \cdots, v_r; y_1, \cdots, y_s$ we construct a basic set, $A_{10}, \cdots, A_{rk}; B_{10}, \cdots, B_{sl}$, of Σ. Here the A_{i0} introduce the v_i, and the B_{i0} introduce the y_i. We adjoin to $\mathcal{J}$ a general point of Λ, or transformally transcendental elements $\omega_1, \omega_2, \cdots, \omega_q$, if no v_i exist. Let $\mathcal{G}$ be the resulting field, and let each B_{ij} become B'_{ij} when the u_i and v_i it contains are replaced by appropriate elements of the general point of Λ, or by ω_i. $B'_{10}, \cdots, B'_{sl}$ becomes the basic set of a reflexive prime ideal Φ in $\mathcal{G}$. Evidently Φ is quasi-linear, so that its basic set consists of linear polynomials of effective order zero. Since no initial of a B_{i0} is annulled by a general point of Λ, or by the ω_i, each B_{i0} must be of zero effective order in y_i.

48. **The resolvent of a prime ideal.** We shall require the following lemma. Let $\mathcal{J}$ be any difference field which contains an element c not equal to any of its transforms. Let G be a polynomial not identically zero, in unknowns $y_1, \cdots, y_n$. There exist elements $a_1, \cdots, a_n$ of $\mathcal{J}$ (dependent on G) which do not annul G when substituted for the y_i.

Evidently it will be sufficient to consider only polynomials G in one unknown. We shall show that, if any polynomial G, in the unknown y, is annulled by all elements of $\mathcal{J}$, then a linear homogeneous polynomial is annulled by all elements of $\mathcal{J}$.

49. We write $G = G_0 + G_1 + \cdots + G_r$, where each G_i is homogeneous and of total degree i in the transforms of y. Substituting ky for y, where k is any rational number, we obtain

$$G(ky) = G_0 + kG_1 + \cdots + k^iG_i + \cdots + k^rG_r. \tag{2}$$

$G(ky)$ vanishes for all y in $\mathcal{J}$ and all rational values of k. It follows that each G_i must vanish for all y in $\mathcal{J}$. Some G_i, say G_e, is not identically zero. G_e is a

[28] The hypothesis of Theorem XI is so stated as to exclude the possibility that Σ has arbitrary unknowns. It is not necessary, however, to include this condition in the hypothesis. If it is omitted the proof may be carried out with only verbal changes, and the contradiction will be obtained if either Σ has arbitrary unknowns, or some A_{i0} is not of effective order zero.

homogeneous polynomial annulled by all y in $\mathcal{J}$.

50. Let H be a homogeneous polynomial of lowest possible total degree which is annulled by all y in $\mathcal{J}$. We substitute $y+z$ for y in H and obtain

$$
\begin{aligned}
H(y+z) = H &+ z\frac{\partial H}{\partial y} + z_1\frac{\partial H}{\partial y_1} + \cdots + z_r\frac{\partial H}{\partial y_r} \\
&+ \frac{1}{2}\left(z^2\frac{\partial^2 H}{\partial y^2} + 2zz_1\frac{\partial^2 H}{\partial y\partial y_1} + \cdots + z_r^2\frac{\partial^2 H}{\partial y_r^2}\right) + \cdots \\
&+ \frac{1}{k!}\left(z^k\frac{\partial^k H}{\partial y^k} + \cdots + z_r^k\frac{\partial^k H}{\partial y_r^k}\right).
\end{aligned}
\tag{3}
$$

Here the derivative symbols are used in their obvious formal sense, and k is the degree and r the order of H.

Evidently $H(y+z)$ vanishes for all y and z in $\mathcal{J}$. Some polynomial $\partial H/\partial y_i$ is not identically zero. It does not vanish for all y in $\mathcal{J}$ since it is homogeneous and of lower degree than H. We choose y in $\mathcal{J}$ so that it does not annul all $\partial H/\partial y_i$ and substitute this value of y in (3). The right-hand member of (3) becomes a difference polynomial in z which is annulled by all z in $\mathcal{J}$ and which contains terms of first degree in z and its transforms.

Our proof above shows that the terms of first degree taken by themselves must constitute a polynomial which is annulled by all z in $\mathcal{J}$. This proves our statement that, if any polynomial has this property, then there is a homogeneous linear polynomial with the property.

51. It is well known that the solutions of a linear homogeneous difference equation of order n are linear combinations with constant coefficients of n independent solutions, where by "constant" is meant an element, not necessarily in $\mathcal{J}$, which is equal to its first transform. To complete the proof of the lemma we shall show that, for arbitrary n, $\mathcal{J}$ contains more than n elements linearly independent with respect to constants. Then not all elements of $\mathcal{J}$ can annul any linear homogeneous difference polynomial.

We may choose $1/c$, $1/(c+1)$, $1/(c+2)$, $\cdots$, $1/(c+n)$ as a set of $n+1$ linearly independent elements. Suppose there exists a relation $a_0/c+a_1/(c+1) + \cdots +a_n/(c+n)=0$, with the a_i constants which are not all zero. On multiplying the left-hand member by $c(c+1)\cdots(c+n)$ we obtain a polynomial in c whose coefficients are linear homogeneous expressions in the a_i with integral coefficients. This polynomial must, for appropriate constant a_i, either be annulled by c or be identically zero. The former alternative is impossible since it would result in c being equal to one of its transforms. The latter requires that the a_i satisfy a system of linear homogeneous equations with integral coefficients. If such a system has nonzero solutions, it has nonzero solutions which are rational. For such solutions the function, $a_0/x+a_1/(x+1)+\cdots+a_n/(x+n)$, of the complex variable x, would be

identically zero; but this is impossible since this function has a pole at the point $x=-j$, where a_j is one of the a_i which is not equal to zero. We conclude that the elements $1/c$, $1/(c+1)$, $\cdots$, $1/(c+n)$ are linearly independent with respect to constant coefficients. This establishes the lemma.

52. We are now prepared to construct a form of resolvent for prime ideals of difference polynomials. The resolvent unknown will be a linear combination of the unknowns of the ideal. These unknowns may, in general, be determined from the resolvent unknown by solving a quasi-linear system.

53. Let Σ be a nontrivial prime ideal in the unknowns $u_1, \cdots, u_q$; $y_1, \cdots, y_p$ with the u_i arbitrary unknowns. We assume that either the coefficient field $\mathcal{J}$ contains an element c which is not equal to any of its transforms, or that u_i exist.

We shall show that there exist polynomials $\mu_1, \cdots, \mu_p$ in the u_i alone with coefficients in $\mathcal{J}$ (if there are no u_i the μ_i are elements of $\mathcal{J}$) and a nonzero polynomial G, free of the y_i, such that

(a) There exist no two solutions of Σ in any extension of $\mathcal{J}$ with the same u_i,

$$u_1, \cdots, u_q; \qquad y_1', \cdots, y_p',$$
$$u_1, \cdots, u_q; \qquad y_1'', \cdots, y_p''$$

for which G does not vanish and in which, for some i, y_i' is not identical with y_i'', or

(b) Such pairs of solutions exist and for each pair, $\mu_1(y_1'-y_1'')+\cdots+\mu_p(y_p'-y_p'')$ is not zero.

We proceed, precisely as in §25 of A.D.E., to introduce new unknowns z_i, λ_i, $i=1, 2, \cdots, p$, and construct the perfect ideal Ω in the u_i, y_i, z_i and λ_i which is obtained by the processes of shuffling and linear combination from

(a) the polynomials of Σ,

(b) the polynomials obtained by replacing each y_i by z_i, $i=1, 2, \cdots, p$, in the polynomials of Σ, and

(c) the polynomial $\lambda_1(y_1-z_1)+\lambda_2(y_2-z_2)+\cdots+\lambda_p(y_p-z_p)$.

Let Λ be any reflexive prime ideal in the decomposition of Ω. Suppose that some y_i-z_i, say y_1-z_1, does not hold Λ. We shall prove that Λ is held by a nonzero polynomial in the u_i and λ_i alone.

Let $\mathcal{G}$ be the quotient-field of the remainder classes of Λ. Let $\mathcal{K}$ be the subfield of $\mathcal{G}$ formed by adjoining to $\mathcal{J}$ the elements of $\mathcal{G}$ which are the remainder classes of the u_i and $\lambda_2, \cdots, \lambda_p$. It will suffice to show that the remainder class T of λ_1 is transformally algebraic over $\mathcal{K}$.

Conditions (a) and (b) above, and the definition of the u_i, show that the remainder classes of the y_i and z_i are transformally algebraic over $\mathcal{K}$. Let $\mathcal{K}$ be the field which results when these elements are adjoined to $\mathcal{K}$. Then it follows from Theorem I that we shall have our result if we prove that T is transformally algebraic over $\mathcal{K}$.

We shall show, indeed, that T is an element of $\mathcal{K}$. For the remainder class of y_1-z_1 is not zero by our assumption concerning Λ. It then follows from (c) that T is a rational combination of the remainder classes of the y_i, z_i, and $\lambda_2, \cdots, \lambda_p$. Thus the existence of the required nonzero difference polynomial is established.

54. We may again proceed as in §25 of A.D.E., using the lemma established above, or the method of §26 of A.D.E. if there are arbitrary unknowns, to replace the λ_i by μ_i. In this way the proof of our statements may be completed.

55. We let $Q=\mu_1y_1+\mu_2y_2+\cdots+\mu_py_p$.

We introduce an unknown w and adjoin to Σ the polynomial $w-Q$. We denote by Π the ideal $\{w-Q, \Sigma\}$. We shall prove that Π is a reflexive prime ideal.

Those polynomials in Π which are free of w are in Σ. Let BC hold Π. Substituting Q for w in B and C we obtain B' and C' respectively. $B'C'$ holds Σ. Then either B' or C', say B', holds Σ. Then B holds Π. The reflexivity of Π follows from its definition as a perfect ideal.

56. Π is held by a polynomial in w and the u_i alone. To see this we adjoin to $\mathcal{J}$ the general point of Π forming a field $\mathcal{G}$. It is sufficient to adjoin those elements which correspond to the u_i and y_i only, since w is given by a rational combination of such elements. The elements of $\mathcal{G}$ corresponding to the u_i and y_i annul all polynomials of Σ and no other polynomial in the y_i and u_i alone. It follows that they are isomorphic to the general point of Σ, so that $\mathcal{G}$ is isomorphic to the field obtained by adjoining to $\mathcal{J}$ the general point of Σ. Therefore $\mathcal{G}$ may be constructed by adjoining to $\mathcal{J}$ transcendentals corresponding to the u_{ij} to form $\mathcal{J}(v_i)$, and then making a finite number r of transcendental adjunctions followed by algebraic adjunctions to $\mathcal{J}(v_i)$. Consequently any $r+1$ members of $\mathcal{G}$ satisfy an algebraic equation with coefficients in $\mathcal{J}(v_i)$. In particular the elements corresponding to w and its first r transforms satisfy such an equation. Replacing elements of $\mathcal{J}(v_i)$ by corresponding rational expressions in the u_{ij}, and multiplying the resulting equation by a suitable polynomial in the u_{ij}, we obtain a nonzero difference polynomial in w and the u_i of order not exceeding r in w, which is annulled by the general point of Π, and consequently holds Π. Since the field obtained by adjoining to $\mathcal{J}$ a general point of Π is isomorphic to that obtained by adjoining a general point of Σ, Π and Σ are of equal order and equal effective order.

57. The method of constructing Π shows that it is a quasi-linear system in the y_i. We list the unknowns of Π in the order $u_1, \cdots, u_q; w; y_1, \cdots, y_p$. The u_i constitute a set of arbitrary unknowns. We choose a basic set for Π, $A, A_1, \cdots, A_k; A_{10}, \cdots, A_{ps}$, where A introduces w, and each A_{i0} introduces y_i. Evidently each A_{i0} is of zero effective order in y_i. It follows that the effective order of A is equal to that of Σ. When, in particular, Σ is of equal order and effective order, A is also, its order equals that of Σ, and each A_{i0}

is of zero order.

Combining the results we have proved above we obtain:

THEOREM XII. *Let Σ be a reflexive prime ideal in the unknowns $u_1, \cdots, u_q$; $y_1, \cdots, y_p$ with coefficients in a difference field $\mathcal{J}$. Let there exist u_i, or let $\mathcal{J}$ contain an element c which is not equal to any of its transforms. There exists a linear combination w of the y_i, with coefficients which are polynomials in the u_i or elements of $\mathcal{J}$ if there are no u_i, such that:*

1. *There exists a reflexive prime ideal Π in the u_i, w, and the y_i, which is quasi-linear in the y_i.*
2. *The solutions of Σ and the corresponding w constitute the totality of solutions of Π.*
3. *The u_i constitute a set of arbitrary unknowns for Π.*
4. *If the unknowns of Π are given the ordering $u_1, u_2, \cdots, u_q; w; y_1, y_2, \cdots, y_p$, then the first polynomial of a basic set of Π is of effective order in w equal to the effective order of the ideal Σ, the remaining leaders of the basic set of Π, introducing the y_i, are of zero effective order in the unknowns they introduce, and the sum of the orders of the leaders of the basic set of Π in the unknowns they introduce is the order of the ideal Σ.*
5. *If Σ is of equal order and effective order, the first polynomial in a basic set of Π with the ordering of the unknowns given in* (4) *above is of this order and this effective order, and the remaining leaders of the basic set are of zero order in the unknowns they introduce.*

58. As an example consider the prime ideal Σ in the field R of rational functions of x with rational coefficients, with basic set: $y_1 - y^2$, $z^2 - y$, $z_1 - y$.

The example discussed in footnote 25 indicates that the conditions of Theorem IX are satisfied, so that we are dealing with the basic set of a reflexive prime ideal. The equation $z_1 = y$ indicates that z is uniquely determined by y in any extension of R.

For the resolvent we first choose $w = y$. Evidently y and z are uniquely determined by w. Furthermore, $z^2 - y$, $z_1 - y$ will remain the basic set of a prime ideal in the field obtained by adjoining solutions for y and w to R, when y is replaced by its value in this solution. Consequently, the basic set of Π will be

$$w_1 - w^2, \qquad y - w, \qquad z^2 - w, \qquad z_1 - w.$$

These relations are quasi-linear but not linear. On the other hand, let us choose as resolvent $w = z$. Then $w^2 = w_1 = y$. We have for the basic set of Π: $w_1 - w^2$, $y - w^2$, $z - w$. Here y and z are determined by linear equations in w.

Whether there exists for every prime ideal Σ some resolvent in terms of which the y_i may be determined by actually linear equations is an interesting problem which remains unsolved.

COLUMBIA UNIVERSITY
NEW YORK, N. Y.