IDEAL THEORY AND ALGEBRAIC DIFFERENCE EQUATIONS*

BY

J. F. RITT AND H. W. RAUDENBUSH, JR.

Recent work of J. L. Doob, F. Herzog, W. C. Strodt and J. F. Ritt furnishes a theory of manifolds for systems of algebraic difference equations.† We present here a basis theorem for infinite systems of difference polynomials, and a restricted theory of ideals; there is obtained thus a counterpart, for difference equations, of Raudenbush's work on differential equations.‡

In the theory of algebraic polynomials, one derives an infinite system from a basis by forming linear combinations. A system of differential polynomials is obtained from a basis by differentiations, linear combinations and the extraction of roots. For difference polynomials, one performs "shufflings" in succession, each shuffling consisting in taking *transforms*, performing linear combinations and factoring forms into products of transforms.

We leave open the question as to how many shufflings are necessary in order to produce a system from its basis. Conceivably, an infinite number may be necessary in certain cases; we give an example, in §15, for which two shufflings are required.

We shall, in this paper, work with difference polynomials whose coefficients lie in an abstract field. If we have decided to relinquish the meromorphic coefficients used in R. D., it is because, with the present undeveloped state of the analytic theory of nonlinear difference equations, it appears tactical to proceed in an algebraic direction, hoping for analytical developments to follow. For example, the establishment of existence theorems which will permit the translation into analytic terms of the *Nullstellensatz* presented in §13, is a problem with a distinct challenge.

DIFFERENCE RINGS

1. Let $\mathfrak{R}$ denote a commutative ring§ possessing a unit element. Let us

* Presented to the Society, September 8, 1939; received by the editors May 24, 1939.

† For references, see *Semicentennial Addresses of the American Mathematical Society*, New York, 1938, pp. 54, 55. The present paper attaches particularly to Ritt and Doob, *Systems of algebraic difference equations*, American Journal of Mathematics, vol 55 (1933). That paper will be designated below by R. D.

‡ Actually, our considerations hold for equations involving a substitution of any type; for instance, for q-difference equations.

§ Defined as in van der Waerden, *Moderne Algebra*, chap. 3. Small italics will, until §9, usually represent elements of $\mathfrak{R}$.

suppose that, for every element a of $\mathfrak{R}$, $\mathfrak{R}$ contains a unique element a_1, called the *transform* of a, the correspondence between elements and their transforms being such that:

(α) the transform of unity is unity;

(β) for every a and b in $\mathfrak{R}$, $(a+b)_1=a_1+b_1$ and $(ab)_1=a_1b_1$.

We shall, under these circumstances, call $\mathfrak{R}$ a *difference* ring. If $\mathfrak{R}$, in addition to being a ring, is a field, we shall call $\mathfrak{R}$ a *difference field*.*

In everything which follows, we deal with a fixed difference ring $\mathfrak{R}$.

2. We denote $(a_1)_1$ by a_2 and, by induction, define a_n as $(a_{n-1})_1$ for every $n>1$. We shall call a_n the *transform of a of order n* or the *nth transform of a*. The element a will be described as its own transform of order 0 and will be denoted, at times, by a_0. We shall refer to the a_n, $n=0, 1, \cdots$, as *transforms* of a; *the* transform of a will continue to mean, as above, a_1.

IDEALS

3. An ideal π contained in $\mathfrak{R}$ will be called a *difference ideal* if, given any element a in $\mathfrak{R}$, the presence in π of either of a and a_1, where a_1 is the transform of a, implies the presence in π of the other. Thus, if a is in π, π contains every transform of a and also contains every element in $\mathfrak{R}$ of which a is a transform of some order.†

4. A difference ideal π will be called *perfect* if, whenever a is such that some product of positive integral powers of transforms of a is contained in π, a is also contained in π. That is, if

$$a_p^{i} a_q^{j} \cdots a_r^{k},$$

where $p, q, \cdots, r$ are distinct nonnegative integers and $i, j, \cdots, k$ are positive integers, is in π, a is in π.

A difference ideal π will be called *prime* if, whenever ab is in π, at least one of a and b is in π; π will thus be a prime ideal in the sense in which that term is regularly used in algebra. *Every prime difference ideal is perfect.*

Henceforth, unless other indications are given, *ideal* will mean difference ideal.

---

* Let $b\neq 0$. By (α), $b_1(1/b)_1=1$. Hence $b_1\neq 0$ and $(a/b)_1=a_1/b_1$ for every a.

† Our insistence that π contain, together with a, all transforms of a "of negative orders" which may exist in $\mathfrak{R}$, is explained by the material of §4. Our definition of ideal appears to have sufficient generality for the purposes of the concrete applications; one will notice, for instance, that a difference form with meromorphic coefficients has the same manifold as its transform. (Cf. R. D.) The fact that many investigations on difference equations deal with half of the complex plane seems to make it undesirable to assume that, for every a in $\mathfrak{R}$, there is an element in $\mathfrak{R}$ of which a is a transform.

PERFECT IDEALS GENERATED BY A SET OF ELEMENTS

5. Let σ be any set of elements in $\mathfrak{R}$.* There exist perfect ideals in $\mathfrak{R}$, for instance $\mathfrak{R}$ itself, which contain σ. The intersection of all such perfect ideals is a perfect ideal which contains σ. We denote this intersection by $\{\sigma\}$ and call it the *perfect ideal generated by* σ.

We shall study the relationship of $\{\sigma\}$ to σ.

Let τ be any set of elements of $\mathfrak{R}$. Consider all elements of $\mathfrak{R}$ which are of the form

$$au + bv + \cdots + cw,$$

where $u, v, \cdots, w$ are transforms of any orders of elements of τ and $a, b, \cdots, c$ are in $\mathfrak{R}$. The totality of such elements will be denoted by $[\tau]$; $[\tau]$ may not be a difference ideal, but it will be an ideal in the sense of algebra and it will be closed with respect to "transforming."

Again, let a be any element in $\mathfrak{R}$ which is such that some product of positive powers of transforms of a is in τ. The totality of such elements a will be denoted by τ'.†

Returning to σ above, let $\sigma_1 = [\sigma]'$ and, continuing inductively, let $\sigma_n = [\sigma_{n-1}]'$ for every $n > 1$. The logical sum, or what is the same, the *limit*, of the sets σ_n is easily seen to be $\{\sigma\}$.

Because $[\sigma]$ and the $[\sigma_n]$ are closed with respect to "transforming," every σ_n is also so closed. Thus, for $n \geqq 1$, each element of $[\sigma_n]$ is a linear combination of elements of σ_n.

In what follows, a plus sign between two sets will indicate that the logical sum of the sets is to be taken.

6. We prove the following:

LEMMA I. *Let σ be any set of elements of $\mathfrak{R}$ and a and b any two elements of $\mathfrak{R}$. If d is contained in $(\sigma+a)_n$ and e in $(\sigma+b)_n$, $n \geqq 1$, then de is contained in $(\sigma+ab)_{n+1}$.*‡

First, let $n=1$. There exist a product $\bar{d}$ of positive powers of transforms of d, and an $\bar{e}$ similarly related to e, which have expressions

$$\bar{d} = gu + \cdots + hv + ka_i + \cdots + la_j,$$
$$\bar{e} = g'u' + \cdots + h'v' + k'b_p + \cdots + l'b_q,$$

* For the purposes of §§11, 12, it is desirable to allow a given element of $\mathfrak{R}$ to occur more than once in σ. Thus, the elements in σ are supposed to be provided with marks and a single element of $\mathfrak{R}$ may appear many times in σ, each time in association with a different mark. When we have to do with ideals, however, a given element will be assumed to appear only once.

† In $[\tau]$ and in τ' a given element will be understood to occur only once. The notation in the present paragraphs, as regards accents and subscripts, is of an episodic character.

‡ The parentheses are ordinary symbols of aggregation. Thus, $(\sigma+a)_1 = [\sigma+a]'$.

where $u, \cdots, v$ and $u', \cdots, v'$ are transforms of elements of σ and the subscripted a and b are transforms of a and b. Thus $\bar{d}\bar{e}$ has an expression in which some terms are in $[\sigma]$ and in which the others are of the type fa_rb_s. For any r and s, the product of a_rb_s by a suitable transform of itself is a multiple* of a transform of ab. Thus every a_rb_s is in $[ab]'$ and, a fortiori, in $(\sigma+ab)_1$. Then $\bar{d}\bar{e}$ is in $[(\sigma+ab)_1]$. Some product of powers of transforms of de is a multiple of $\bar{d}\bar{e}$. Thus de is in $(\sigma+ab)_2$.

Now, let $n=2$. Let $\bar{d}$, described as above, be in $[(\sigma+a)_1]$. By §5, $\bar{d}$ is a linear combination of elements of $(\sigma+a)_1$. We use an $\bar{e}$, described as above, which is linear in elements of $(\sigma+b)_1$. Then $\bar{d}\bar{e}$ has an expression in which each term is of the type guv with u in $(\sigma+a)_1$ and v in $(\sigma+b)_1$. Now uv, by the case of $n=1$, is in $(\sigma+ab)_2$. Hence $\bar{d}\bar{e}$ is in $[(\sigma+ab)_2]$. This puts de in $(\sigma+ab)_3$.

The proof continues by induction.

LEMMA II. *Let σ be any set of elements of $\mathfrak{R}$ and a and b any two elements of $\mathfrak{R}$. Then $\{\sigma+ab\}$ is the intersection of $\{\sigma+a\}$ and $\{\sigma+b\}$.*

We have only to show that, c being any element in the intersection, c is contained in $\{\sigma+ab\}$. Let n be such that c is contained in $(\sigma+a)_n$ and in $(\sigma+b)_n$. Then c^2 is in $(\sigma+ab)_{n+1}$. Thus c is also in $(\sigma+ab)_{n+1}$.

BASES

7. Let σ be a system of elements in $\mathfrak{R}$. A finite subset ϕ of σ will be called a *basis* of σ if $\{\phi\}$ contains σ.

A finite system of elements is a basis for itself. If every infinite system of elements in $\mathfrak{R}$ has a basis, we shall call $\mathfrak{R}$ a *difference ring with a basis theorem.*

DECOMPOSITION OF PERFECT DIFFERENCE IDEALS

8. Let $\mathfrak{R}$ have a basis theorem. We prove the theorem:

THEOREM. *Every perfect ideal in $\mathfrak{R}$ is the intersection of a finite set of prime ideals.*

Let π be a perfect ideal for which our statement is false. Then π is not prime. Let ab be in π while neither a nor b is. Then π is the intersection of $\{\pi+a\}$ and $\{\pi+b\}$ (Lemma II). At least one of the two latter ideals does not have the property of being the intersection of a finite set of prime ideals. Of the two ideals, let π_1 designate one which lacks the property. We give π_1 the treatment accorded to π and continue, forming a sequence of perfect ideals

$$\pi, \pi_1, \cdots, \pi_n, \cdots, \tag{1}$$

* The meaning is obvious.

each a proper part of its successor. Let σ be the logical sum of the ideals in (1) and let ϕ be a basis of σ. There is some π_n which contains ϕ. That π_n will contain σ. This contradiction proves the theorem.

It is easy now to see that every perfect ideal in $\mathfrak{R}$ has a *unique* representation as the intersection of a finite number of prime ideals *none of which contains any other*.

Ideals of difference polynomials

9. Let n be any positive integer. We consider n symbols $y_1(x), \cdots, y_n(x)$. If j is any nonnegative integer, we shall call the symbol $y_i(x+j)$ the *jth transform* of $y_i(x)$.

Let $\mathfrak{F}$ be a given difference field. By a *difference polynomial* we shall mean a polynomial in a certain (eo ipso finite) number of the $y_i(x+j)$, with coefficients in $\mathfrak{F}$. As a rule, we shall substitute the briefer term *form* for "difference polynomial." By the *transform* of a form A, we mean the form obtained when x is replaced by $(x+1)$ in the $y_i(x+j)$ appearing in A, and when the coefficients in A are replaced by their transforms. Transforms of higher order are defined similarly. Because the transform of unity is unity, these definitions are consistent with the definition given above of the jth transform of $y_i(x)$.

The totality of forms with coefficients in $\mathfrak{F}$ is a difference ring, which we shall call the *ring of forms in the unknowns* $y_1, \cdots, y_n$. Any form of this ring will be called a *form in* $y_1, \cdots, y_n$.

10. We prove the theorem:

Theorem. *For any difference field $\mathfrak{F}$, the ring of difference polynomials in the unknowns $y_1, \cdots, y_n$ is a difference ring with a basis theorem.*

We assume the theorem to be false and work towards a contradiction. We shall use methods and results of R. D. The items of that paper which will be employed here acquire validity, with no essential change, for an abstract field $\mathfrak{F}$.

11. We prove the following lemma:

Lemma III. *Let Σ be a system of forms in $y_1, \cdots, y_n$ which has no basis. Let $F_1, \cdots, F_s$ be such that, by multiplying each form in Σ by some product of nonnegative powers of transforms of $F_1, \cdots, F_s$, a system Λ is obtained which has a basis. Then at least one of the systems $\Sigma+F_i$, $i=1, \cdots, s$, has no basis.*

Suppose that every $\Sigma+F_i$ has a basis. Then, for each i, there is a finite subset Φ_i of $\Sigma+F_i$ such that $\{\Phi_i\}$ contains $\Sigma+F_i$. As Φ_i may evidently be replaced by any finite subset of $\Sigma+F_i$ which contains Φ_i, we may (and shall) suppose Φ_i, for every i, to be of the type

$$F_i, A_1, \cdots, A_q, \tag{2}$$

with the set

$$A_1, \cdots, A_q \tag{3}$$

independent of i. Enlarging (3) if necessary, we assume that the subset of Λ obtained from (3) by the above described multiplications is a basis of Λ. Thus, the perfect ideal generated by the set (3) contains Λ.

Let L be any form in Σ. Then L is contained, for every i, in the perfect ideal generated by the set (2). Certainly, L is contained in the perfect ideal generated by

$$L, A_1, \cdots, A_q.$$

By Lemma II of §6, L is contained in the perfect ideal generated by

$$F_1F_2 \cdots F_sL, A_1, \cdots, A_q. \tag{4}$$

Some KL, with K a product of powers of transforms of the F_i, belongs to Λ. Now an appropriate product of powers of transforms of $F_1F_2 \cdots F_sL$ is a multiple of KL. Since Λ is contained in the perfect ideal generated by (3), $F_1 \cdots F_sL$ is also so contained. Inspecting (4), we see that L is contained in the perfect ideal generated by (3). Then (3) is a basis of Σ. This contradiction proves the lemma.

12. From among all systems of forms in $y_1, \cdots, y_n$ which have no basis, we select one, Σ, whose basic sets are not higher than those of any other system which has no basis. Let

$$A_1, \cdots, A_r \tag{5}$$

be a basic set of Σ. Then A_1 must be of class greater than 0, else Σ would be contained in $\{A_1\}$. Let I_i be the initial of A_i, $i=1, \cdots, r$.

For every form of Σ not in (5), let a remainder with respect to (5) be found. Let Λ be the system composed of the forms in (5) and of the products of the forms of Σ not in (5) by the power products of transforms of the I_i used in forming the remainders. Let Ω be the system composed of (5) and of the remainders of the forms of Σ not in (5).

By the considerations of R. D., Ω has a basis. Such a basis is a basis of $\{\Omega\}$. Now $[\Lambda]$ is identical with $[\Omega]$, so that $\{\Lambda\}$ is identical with $\{\Omega\}$. Thus $\{\Lambda\}$ has a basis. It is easy now to see that $\{\Lambda\}$ has a basis composed of forms of Λ. Such a basis is a basis of Λ.

The lemma of §11 informs us now that some $\Sigma+I_i$ has no basis. As in R. D., this is impossible. The theorem is proved.

HILBERT-NETTO THEOREM

13. Following the procedure of Raudenbush for differential equations, one can prove that if Φ is a finite system of difference polynomials with coefficients in a difference field $\mathfrak{F}$ and if G is a form which is not in $\{\Phi\}$, then there exists an extension $\mathfrak{F}'$, of $\mathfrak{F}$, containing a solution of Φ which is not a solution of G.*

DERIVATION OF AN INFINITE SYSTEM FROM A BASIS

14. Let Σ be an infinite system of forms in $y_1, \cdots, y_n$ and Φ a basis of Σ. Given any form A in Σ, there is some Φ_i (notation as in §5) which contains A. It is natural to ask whether there is some Φ_i which contains Σ, and, indeed, whether Φ_1 contains Σ.

We shall present a system Σ which has no basis Φ for which Φ_1 holds Σ. Whether there is a system with no basis for which Φ_2 contains Σ, we do not know.

15. Our example will deal with forms in a single unknown y. We use the field of constants, each constant being its own transform. The jth transform of y will be denoted by y_j. The system Σ will consist of the sequence of forms $A_0, A_1, \cdots$, where

$$A_j = (y_0 + y_1 + \cdots + y_{2^j-1})(y_{2^j} + \cdots + y_{2^{j+1}-1}).$$

Let m be any nonnegative integer. Let Φ consist of $A_0, \cdots, A_m$. We shall show that A_{m+1} is not contained in Φ_1.

Consider any A_j with $j \leqq m$. Each term in A_j is of the type $y_a y_b$ with

$$0 < b - a \leqq 2^{m+1} - 1. \tag{6}$$

Hence, if G is any form in $[\Phi]$, each term in G has, among its letters, two letters y_a and y_b where a and b satisfy (6). We shall show that if K is a product of powers of transforms of A_{m+1}, K contains a term each of whose letters y_j has its subscript j divisible by 2^{m+1}. This will prove that A_{m+1} is not contained in Φ_1.

Let B_i represent the ith transform of A_{m+1}, $i=0, 1, \cdots$. Let B_j^r, with $r>0$, be one of the powers of which K is a product. Let

$$j = p2^{m+1} + q,$$

with p and q nonnegative integers and $q<2^{m+1}$. We have

$$B_j = (y_j + \cdots + y_{2^{m+1}+j-1})(y_{2^{m+1}+j} + \cdots + y_{2^{m+2}+j-1}). \tag{7}$$

* These Transactions, vol. 36 (1934), p. 368. The term *extension* is self-explanatory.

If $q=0$, the first parenthesis in (7) contains $y_{p2^{m+1}}$ and the second contains $y_{(p+1)2^{m+1}}$. If $q>0$, the first parenthesis contains $y_{(p+1)2^{m+1}}$ and the second $y_{(p+2)2^{m+1}}$. In any case, B_j contains one and only one term $y_a y_b$ in which a and b are both divisible by 2^{m+1}. Furthermore, $B_j{}^r$ contains a term which is a power of $y_a y_b$, and that term of $B_j{}^r$ is the only one in which every subscript is divisible by 2^{m+1}. Our statement with respect to K follows.

We observe that A_0 is a basis of Σ and that, if Ψ represents A_0, Ψ_1 contains y_0 so that $[\Psi_1]$ and Ψ_2 contain Σ.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.,
QUEENS COLLEGE,
FLUSHING, N. Y.