ON EXTENSIONS OF DIFFERENCE FIELDS AND THE RESOLVENTS OF PRIME DIFFERENCE IDEALS

RICHARD M. COHN[1]

1. **Introduction.** In this note we prove an analogue for difference fields[2] of the theorem that every finite algebraic extension of a field of characteristic 0 is a simple extension. We apply this analogue to the theory of the resolvent system of a reflexive prime difference ideal.

Our method is essentially that used in M.D.P. to obtain a weaker theorem; but we make a more careful study of the situation which exists before the indeterminates λ_i of M.D.P. (corresponding to both the σ_i and λ_i of this note) are specialized, in order to overcome the difficulty which arises because, even in polynomial rings over difference fields of characteristic 0, there exist prime difference ideals containing no linear polynomial of effective order zero and yet admitting no more than one solution in any extension of the coefficient field.[3] This study is contained in §4 below.

2. **Definitions and statement of the theorem.** We call a difference field $\mathfrak{F}$ *periodic* or *aperiodic* according to whether or not there exists an integer n, fixed for $\mathfrak{F}$, such that every element of $\mathfrak{F}$ is equal to its nth transform. If $\mathfrak{F}$ is an aperiodic subfield of a difference field $\mathfrak{G}$, and P is any nonzero difference polynomial in the ring[4] $\mathfrak{G}\{y_1, \cdots, y_n\}$, there exist elements $\mu_1, \cdots, \mu_n$ in $\mathfrak{F}$ which do not annul P when substituted for $y_1, \cdots, y_n$ respectively.[5]

Received by the editors June 5, 1951.

[1] This paper was written while the author held a University Research Grant from Rutgers University.

[2] For definitions and basic concepts see J. F. Ritt and H. W. Raudenbush, Jr., *Ideal theory and algebraic difference equations*, Trans. Amer. Math. Soc. vol. 46 (1939) pp. 445–452. Other results used in the present paper may be found in our Dissertation, *Manifolds of difference polynomials*, Trans. Amer. Math. Soc. vol. 64 (1948) pp. 133–172. This paper is henceforth referred to as M.D.P.

[3] These are the quasi-linear systems of M.D.P. For a further study of quasi-linearity and related phenomena see our paper *Extensions of difference fields*, Amer. J. Math.

[4] Brackets $\{ \}$ denote ring adjunction of the included elements and all their transforms so as to form a difference ring. It will be understood that the elements are indeterminates whenever this notation is used in this paper. Brackets $\langle \rangle$ denote field adjunction of the included elements and their transforms. The elements will not be indeterminates in all cases. Parentheses denote field adjunction of the included elements but not of their transforms, so that a field is obtained which need not be a difference field.

[5] See M.D.P., pp. 168–169. The statement of the result in M.D.P. is weaker than

We can now state our main result:

THEOREM I. *Let $\mathfrak{F}$ be an aperiodic difference field of characteristic* 0. *Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be elements transformally algebraic over $\mathfrak{F}$ and lying in a common extension of $\mathfrak{F}$. Then there is an element β in the difference field*[4] *$\mathfrak{F}\langle\alpha_1, \cdots, \alpha_n\rangle$ and an integer t such that the tth transform of any element of $\mathfrak{F}\langle\alpha_1, \cdots, \alpha_n\rangle$ is in $\mathfrak{F}\langle\beta\rangle$.*[6]

3. First steps in the proof.

It is sufficient to consider the case $n=2$ and to show that there is an element β in $\mathfrak{F}\langle\alpha_1, \alpha_2\rangle$ and an integer t such that[7] α_{1t} and α_{2t} are in $\mathfrak{F}\langle\beta\rangle$.

Let Σ be the reflexive prime difference ideal consisting of those polynomials of $\mathfrak{F}\{y_1, y_2\}$ which vanish when $y_1=\alpha_1$, $y_2=\alpha_2$.

To $\mathfrak{F}\langle\alpha_1, \alpha_2\rangle$ we adjoin elements σ_1, σ_2 annulling no nonzero difference polynomial with coefficients in $\mathfrak{F}\langle\alpha_1, \alpha_2\rangle$. Let $\gamma=\sigma_1\alpha_1+\sigma_2\alpha_2$. We introduce the new indeterminates λ_1, λ_2, w and denote by Ω the reflexive prime difference ideal consisting of all polynomials in $\mathfrak{F}\{\lambda_1, \lambda_2, w, y_1, y_2\}$ which vanish when $\lambda_1=\sigma_1$, $\lambda_2=\sigma_2$, $w=\gamma$, $y_1=\alpha_1$, $y_2=\alpha_2$.

If P is a polynomial free of w, then P is in Ω if and only if its coefficients, when it is considered as a polynomial in λ_1, λ_2 and their transforms, are polynomials of Σ. In particular Ω contains Σ, and therefore contains nonzero polynomials in y_1 alone and in y_2 alone, but Ω does not contain a nonzero polynomial in λ_1 and λ_2 alone. Since γ is transformally algebraic over $\mathfrak{F}\langle\sigma_1, \sigma_2\rangle$, we see that Ω contains a nonzero polynomial in λ_1, λ_2, and w. It follows that λ_1 and λ_2 constitute a set of parametric indeterminates[8] for Ω.

The work of §53 of M.D.P. and the definition of §47 of that paper show that Ω is quasi-linear in y_1 and y_2 when λ_1 and λ_2 are used as the parametric indeterminates. By Theorem XI of M.D.P. this implies that, for $i=1, 2$, Ω contains a polynomial P_i in λ_1, λ_2, w, y_i which is of zero effective order in y_i and whose coefficients, when it is regarded as a polynomial in y_i, are not all in Ω. Since σ_1, σ_2, γ, α_1, α_2 constitute a

the statement above, but it is easy to see that the proof applies directly to the present situation.

[6] It is not always possible to find an element β such that $\mathfrak{F}\langle\beta\rangle=\mathfrak{F}\langle\alpha_1, \cdots, \alpha_n\rangle$. Let $\mathfrak{F}$, for example, be the field obtained by adjoining to the field R of rational numbers the elements $c_1, c_2, \cdots, c_n$ which annul no difference polynomial with coefficients in R. Let α_i be a solution of $y_1=c_i$, $i=1, \cdots, n$, where y_1 denotes the transform of y. Then $\mathfrak{F}\langle\alpha_1, \cdots, \alpha_n\rangle$ is an nth order extension of $\mathfrak{F}$. Each element of this extension evidently satisfies a first order equation with coefficients in $\mathfrak{F}$, for its transform is in $\mathfrak{F}$. Hence $\mathfrak{F}\langle\alpha_1, \cdots, \alpha_n\rangle$ cannot be obtained from $\mathfrak{F}$ by fewer than n adjunctions.

[7] A second subscript, or a single subscript attached to a symbol that is also used without subscripts, denotes the transform of order equal to that subscript.

generic zero[8] of Ω, it follows that there is an integer m such that α_{1s} and α_{2s} are algebraic over $\mathfrak{F}\langle\sigma_1, \sigma_2, \gamma\rangle$ when $s \geqq m$. Hence these α_{1s} and α_{2s} are algebraic over the algebraic field[9] formed by adjoining a finite set, dependent on s, of transforms of σ_1, σ_2, and γ to $\mathfrak{F}$.

4. **The principal step.** For any non-negative integer k and a sufficiently great integer l, every α_{1i}, $i \geqq k$, is algebraic over $\mathfrak{F}\langle\alpha_{1k}, \cdots, \alpha_{1,k+l}\rangle$ and every α_{2i}, $i \geqq k$, is algebraic over $\mathfrak{F}\langle\alpha_{2k}, \cdots, \alpha_{2,k+l}\rangle$. This is so by the conclusion of §20 of M.D.P. since α_1 and α_2 are transformally algebraic over $\mathfrak{F}$. We choose k to exceed s of the preceding paragraph. Hence there is a finite set T of transforms of σ_1, σ_2, and γ such that $\alpha_{1k}, \cdots, \alpha_{1,k+l}$; $\alpha_{2k}, \cdots, \alpha_{2,k+l}$ are algebraic over the algebraic field $\mathfrak{F}(T)$. Then every α_{1i} and α_{2i}, $i \geqq k$, is algebraic over $\mathfrak{F}(T)$.

Let t be an integer which is not less than k and which exceeds the order of any transform of σ_1, σ_2, or γ occurring in T. Then α_{1t}, α_{2t} are algebraic over $\mathfrak{F}(T)$, while σ_{1t}, σ_{2t} are transcendental over $\mathfrak{F}(T)$ since they are even transcendental over the field $\mathfrak{F}(\alpha_{10}, \cdots, \alpha_{1,t-1}; \alpha_{20}, \cdots, \alpha_{2,t-1}; \sigma_{10}, \cdots, \sigma_{1,t-1}; \sigma_{20}, \cdots, \sigma_{2,t-1})$ which contains $\mathfrak{F}(T)$.

It follows that α_{1t} and α_{2t} are rational combinations of σ_{1t}, σ_{2t}, and γ_t with coefficients in $\mathfrak{F}(T)$. Hence α_{1t} and α_{2t} are in the difference field $\mathfrak{F}\langle\sigma_1, \sigma_2, \gamma\rangle$.

5. **Completion of the proof.** Let $\alpha_{it} = M_i/N$, $i = 1, 2$, where the M_i and N are difference polynomials in σ_1, σ_2, and γ with coefficients in $\mathfrak{F}$. In the relation $N\alpha_{1t} = M_1$ we replace γ by $\sigma_1\alpha_1 + \sigma_2\alpha_2$. There results a relation $\overline{N}\alpha_{1t} = \overline{M}_1$, where $\overline{N}$ and $\overline{M}_1$ are difference polynomials in σ_1, σ_2, α_1, α_2. Any product of powers of σ_1, σ_2 and their transforms must have equal coefficients on both sides of this equation. Hence this relation continues to hold if we replace σ_1 by any element μ_1 of $\mathfrak{F}$ and σ_2 by any element μ_2 of $\mathfrak{F}$. Then the relation $N\alpha_{1t} = M_1$ remains valid if we replace σ_1 and σ_2 by μ_1 and μ_2 respectively and replace γ by $\beta = \mu_1\alpha_1 + \mu_2\alpha_2$. Similarly the relation $N\alpha_{2t} = M_2$ remains valid after these replacements.

Considering $\overline{N}$ as a polynomial in σ_1, σ_2 with coefficients in $\mathfrak{F}\langle\alpha_1, \alpha_2\rangle$, we see from the result stated in §2 that we may choose μ_1 and μ_2 so that $\overline{N}$ does not vanish when the σ_i are replaced by the μ_i. With this choice of μ_1 and μ_2, N cannot vanish when the σ_i are

[8] These are called arbitrary unknowns in M.D.P. The changed terminology conforms with that of J. F. Ritt, *Differential algebra*, Amer. Math. Soc. Colloquium Publications, vol. 33. For the same reason we also use the terms "generic zero," "characteristic set," in place of "general point" and "basic set" respectively of M.D.P.

[9] That is to say, a field in the usual sense, not a difference field.

replaced by the μ_i and γ is replaced by β. We see that α_{1t} and α_{2t} are in $\mathfrak{F}\langle\beta\rangle$. This proves Theorem I. For later use we note that we may choose the μ_i from any aperiodic subfield of $\mathfrak{F}$.

6. Resolvent systems. We consider a reflexive prime difference ideal Σ in $\mathfrak{F}\{u_1, \cdots, u_q; y_1, \cdots, y_p\}$, the u_i forming a set of parametric indeterminates. If Σ has no parametric indeterminates, we let $q=0$.

THEOREM II. *Let $\mathfrak{F}$ be aperiodic, or let $q\neq 0$. There is a linear combination $L=\sum_{i=1}^{p}\lambda_i y_i$ of the y_i, the λ_i being polynomials*[10] *in the u_j with coefficients in $\mathfrak{F}$, which is such that:*

(1) *$\Pi=\{\Sigma, w-L\}$, where w is a new indeterminate, is a reflexive prime difference ideal. There is an integer t such that Π contains difference polynomials $Ny_{it}-M_i$, $i=1, \cdots, p$, where N and the M_i are polynomials in w and the u_j only, and N is not in Π.*

(2) *The u_j constitute a set of parametric indeterminates for Π.*

(3) *The solutions of Σ and the corresponding values computed for w from the equation $w=L$ constitute the totality of solutions of Π.*

(4) *If the indeterminates of Π are given the ordering $u_1, \cdots, u_q$; w; $y_1, \cdots, y_p$, then the first polynomial of a characteristic set*[8] *of Π is of effective order in w equal to the effective order of Σ, the remaining leaders of the characteristic set of Π, which introduce the y_i, $i=1, \cdots, p$, are of zero effective order in the indeterminates they introduce, and the sum of the orders of the leaders of the characteristic set of Π in the indeterminates they introduce is the order of Σ.*

(5) *If Σ is of equal order and effective order, the first polynomial of a characteristic set of Π with the ordering of the indeterminates given in (4) above is of this order and this effective order, and the remaining leaders of the characteristic set are of zero order in the indeterminates they introduce.*

The polynomials of Π which are free of the y_i constitute a reflexive prime difference ideal Λ. A characteristic set of Λ, with the u_j used as the parametric indeterminates, will be called a *resolvent system* for Σ. We obtain a solution of the resolvent system from any solution of Σ by using the equation $w=L$. From any solution of the resolvent system not annulling a certain polynomial G which is not in Λ, we may obtain a solution of Σ by the operations of taking transforms, taking inverse transforms, and forming rational combinations. For G we may use the product of N and the initials of the polynomials of the resolvent system.[11]

[10] If $q=0$ this is to mean that the λ_i are in $\mathfrak{F}$.

[11] In order to verify this we make the substitutions $y_i' = y_{it}$, $i=1, \cdots, p$, the

To prove Theorem II we consider a generic zero $u_j=\sigma_j$, $j=1, \cdots, q$; $y_i=\alpha_i$, $i=1, \cdots, p$, of Σ. Then the α_i are transformally algebraic over the aperiodic difference field $\mathfrak{G}=\mathfrak{F}\langle\sigma_1, \cdots, \sigma_q\rangle$. By Theorem I there exist elements μ_i, $i=1, \cdots, p$, in $\mathfrak{G}$ such that $\mathfrak{G}\langle\mu_1\alpha_1+ \cdots +\mu_p\alpha_p\rangle$ contains some transform of each α_i.

If $\mathfrak{F}$ is aperiodic, we may choose μ_i in $\mathfrak{F}$ by the final remark of §5. If $\mathfrak{F}$ is periodic, $q\neq 0$ and there exist μ_i which are quotients of difference polynomials in the σ_j. We may, in fact, select quotients with denominator 1, for an extension $\mathfrak{G}\langle\gamma\rangle$ of $\mathfrak{G}$ is identical with $\mathfrak{G}\langle\lambda\gamma\rangle$ where λ is any element of $\mathfrak{G}$.

We consider μ_i which are polynomials in the σ_j or, if $q=0$, are elements of $\mathfrak{F}$. To obtain the λ_i of Theorem II we replace the σ_j, $j=1, \cdots, q$, in each polynomial μ_i by the corresponding u_j. Then Π is the ideal with generic zero $u_j=\sigma_j$, $j=1, \cdots, q$, $w=\sum_{i=1}^{p} \mu_i\alpha_i$, $y_i=\alpha_i$, $i=1, \cdots, p$. For on the one hand this is evidently a solution of Π. On the other hand let R be a polynomial which vanishes for these values of the u_j, w, and y_i. If we replace each transform of w occurring in R by the corresponding transform of L, we obtain a polynomial $\overline{R}$ free of w which has the solution $u_j=\sigma_j$, $j=1, \cdots, q$; $y_i=\alpha_i$, $i=1, \cdots, p$. Hence $\overline{R}$ is in Σ. But if the replacements of transforms of w by transforms of L are made step by step, it is easy to see that $R-\overline{R}$ is a linear combination of $w-L$ and its transforms. Hence R is in $\Pi=\{\Sigma, w-L\}$.

Statements (1) and (2) of Theorem II follow from the properties of the generic zero of Π. (3) is evident. The field formed by adjoining to $\mathfrak{F}$ the σ_j, $j=1, \cdots, q$, and $\sum_{i=1}^{p} \mu_i\alpha_i$ contains all but a finite number of transforms of the α_i. The statements in (4) concerning effective orders follow from this. We obtain the same field by adjoining a generic zero of Π to $\mathfrak{F}$ as we obtain by adjoining a generic zero of Σ. This proves the statement in (4) concerning orders. If Σ is of the same order as effective order, then Π is also. (5) follows from this remark and (4).

RUTGERS UNIVERSITY

value of w, however, remaining unchanged. These substitutions carry Σ and Π into the reflexive prime difference ideals Σ' and Π' respectively. Π' is held by the polynomials $Ny_i^{f}-M_i$. Hence it is easy to see that every solution of the resolvent system not annulling the product of its initials with N can be extended to a solution of Π' and therefore gives rise to a solution of Σ'. Since it is always possible to adjoin inverse transforms of its elements to a difference field, a solution of Σ' can be extended to a solution of Σ.

These considerations are made necessary by the fact that the leaders of the characteristic set of Π which introduce the y_i may be nonlinear in the y_i.