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

RICHARD M. COHN

1. Introduction. In this note we prove an analogue for difference fields 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 of M.D.P. (corresponding to both the and 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. This study is contained in §4 below.

2. Definitions and statement of the theorem. We call a difference field periodic or aperiodic according to whether or not there exists an integer , fixed for , such that every element of is equal to its th transform. If is an aperiodic subfield of a difference field , and is any nonzero difference polynomial in the ring , there exist elements , ... , in which do not annihilate when substituted for , ... , respectively.

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 ( ) 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 $\mathbb{F}$ be an aperiodic difference field of characteristic 0. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements transformally algebraic over $\mathbb{F}$ and lying in a common extension of $\mathbb{F}$. Then there is an element $\beta$ in the difference field $\mathbb{F}\langle \alpha_1, \ldots, \alpha_n \rangle$ and an integer $t$ such that the $t$th transform of any element of $\mathbb{F}\langle \alpha_1, \ldots, \alpha_n \rangle$ is in $\mathbb{F}(\beta)$.\(^6\)

3. **First steps in the proof.** It is sufficient to consider the case $n=2$ and to show that there is an element $\beta$ in $\mathbb{F}\langle \alpha_1, \alpha_2 \rangle$ and an integer $t$ such that $\alpha_1^t$ and $\alpha_2^t$ are in $\mathbb{F}(\beta)$.

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

To $\mathbb{F}\langle \alpha_1, \alpha_2 \rangle$ we adjoin elements $\sigma_1, \sigma_2$ annulling no nonzero difference polynomial with coefficients in $\mathbb{F}\langle \alpha_1, \alpha_2 \rangle$. Let $\gamma = \sigma_1 \alpha_1 + \sigma_2 \alpha_2$. We introduce the new indeterminates $\lambda_1, \lambda_2, w$ and denote by $\Omega$ the reflexive prime difference ideal consisting of all polynomials in $\mathbb{F}\{\lambda_1, \lambda_2, w, y_1, y_2\}$ 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 $\Omega$ if and only if its coefficients, when it is considered as a polynomial in $\lambda_1, \lambda_2$ and their transforms, are polynomials of $\Sigma$. In particular $\Omega$ contains $\Sigma$, and therefore contains nonzero polynomials in $y_1$ alone and in $y_2$ alone, but $\Omega$ does not contain a nonzero polynomial in $\lambda_1$ and $\lambda_2$ alone. Since $\gamma$ is transformally algebraic over $\mathbb{F}(\sigma_1, \sigma_2)$, we see that $\Omega$ contains a nonzero polynomial in $\lambda_1, \lambda_2, w$. It follows that $\lambda_1$ and $\lambda_2$ constitute a set of parametric indeterminates for $\Omega$.

The work of §53 of M.D.P. and the definition of §47 of that paper show that $\Omega$ is quasi-linear in $y_1$ and $y_2$ when $\lambda_1$ and $\lambda_2$ are used as the parametric indeterminates. By Theorem XI of M.D.P. this implies that, for $i=1, 2$, $\Omega$ contains a polynomial $P_i$ in $\lambda_1, \lambda_2, w, y_i$ 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 $\Omega$. Since $\sigma_1, \sigma_2, \gamma, \alpha_1, \alpha_2$ constitute a

---

\(^6\) It is not always possible to find an element $\beta$ such that $\mathbb{F}(\beta) = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Let $\mathbb{F}$, for example, be the field obtained by adjoining to the field $R$ of rational numbers the elements $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ which annul no difference polynomial with coefficients in $R$. Let $\alpha_i$ be a solution of $y_i = \epsilon_i$, $i = 1, \ldots, n$, where $y_i$ denotes the transform of $y$. Then $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ is an $n$th order extension of $\mathbb{F}$. Each element of this extension evidently satisfies a first order equation with coefficients in $\mathbb{F}$, for its transform is in $\mathbb{F}$. Hence $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ cannot be obtained from $\mathbb{F}$ 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 \(\Omega\), it follows that there is an integer \(m\) such that \(\alpha_{1s}\) and \(\alpha_{2s}\) are algebraic over \(\mathfrak{F}(\sigma_1, \sigma_2, \gamma)\) when \(s \geq m\). Hence these \(\alpha_{1s}\) and \(\alpha_{2s}\) are algebraic over the algebraic field\(^9\) formed by adjoining a finite set, dependent on \(s\), of transforms of \(\sigma_1, \sigma_2, \) and \(\gamma\) to \(\mathfrak{F}\).

4. The principal step. For any non-negative integer \(k\) and a sufficiently great integer \(l\), every \(\alpha_{1i}, i \geq k\), is algebraic over \(\mathfrak{F}(\alpha_{1k}, \ldots, \alpha_{1,k+i})\) and every \(\alpha_{2i}, i \geq k\), is algebraic over \(\mathfrak{F}(\alpha_{2k}, \ldots, \alpha_{2,k+i})\). This is so by the conclusion of §20 of M.D.P. since \(\alpha_1\) and \(\alpha_2\) 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 \(\sigma_1, \sigma_2, \) and \(\gamma\) such that \(\alpha_{1k}, \ldots, \alpha_{1,k+t}; \alpha_{2k}, \ldots, \alpha_{2,k+t}\) are algebraic over the algebraic field \(\mathfrak{F}(T)\). Then every \(\alpha_{1i}\) and \(\alpha_{2i}, i \geq k\), 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 \(\sigma_1, \sigma_2, \) or \(\gamma\) occurring in \(T\). Then \(\alpha_{1t}\) and \(\alpha_{2t}\) are algebraic over \(\mathfrak{F}(T)\), while \(\sigma_{1t}\) and \(\sigma_{2t}\) are transcendental over \(\mathfrak{F}(T)\) since they are even transcendental over the field \(\mathfrak{F}(\alpha_{10}, \ldots, \alpha_{1,t-1}; \alpha_{20}, \ldots, \alpha_{2,t-1}; \sigma_{10}, \ldots, \sigma_{1,t-1}; \sigma_{20}, \ldots, \sigma_{2,t-1})\) which contains \(\mathfrak{F}(T)\).

It follows that \(\alpha_{1t}\) and \(\alpha_{2t}\) are rational combinations of \(\sigma_{1t}, \sigma_{2t}, \) and \(\gamma_t\) with coefficients in \(\mathfrak{F}(T)\). Hence \(\alpha_{1t}\) and \(\alpha_{2t}\) are in the difference field \(\mathfrak{F}(\sigma_t, \sigma, \gamma)\).

5. Completion of the proof. Let \(\alpha_{it} = M_i/N, i = 1, 2,\) where the \(M_i\) and \(N\) are difference polynomials in \(\sigma_1, \sigma_2, \) and \(\gamma\) with coefficients in \(\mathfrak{F}\). In the relation \(N\alpha_{it} = M_i\) we replace \(\gamma\) by \(\sigma_1\alpha_1 + \sigma_2\alpha_2\). There results a relation \(\overline{N}\alpha_{it} = \overline{M}_i\), where \(\overline{N}\) and \(\overline{M}_i\) are difference polynomials in \(\sigma_1, \sigma_2, \alpha_1, \alpha_2\). Any product of powers of \(\sigma_1, \sigma_2\) and their transforms must have equal coefficients on both sides of this equation. Hence this relation continues to hold if we replace \(\sigma_1\) by any element \(\mu_1\) of \(\mathfrak{F}\) and \(\sigma_2\) by any element \(\mu_2\) of \(\mathfrak{F}\). Then the relation \(N\alpha_{it} = M_i\) remains valid if we replace \(\sigma_1\) and \(\sigma_2\) by \(\mu_1\) and \(\mu_2\) respectively and replace \(\gamma\) 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 \(\sigma_1, \sigma_2\) with coefficients in \(\mathfrak{F}(\alpha_1, \alpha_2)\), we see from the result stated in §2 that we may choose \(\mu_1\) and \(\mu_2\) so that \(\overline{N}\) does not vanish when the \(\sigma_i\) are replaced by the \(\mu_i\). With this choice of \(\mu_1\) and \(\mu_2\), \(N\) cannot vanish when the \(\sigma_i\) 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 $\mu_i$ and $\gamma$ is replaced by $\beta$. We see that $\alpha_{2t}$ and $\alpha_{2t}$ are in $\mathfrak{F}(\beta)$. This proves Theorem I. For later use we note that we may choose the $\mu_i$ from any aperiodic subfield of $\mathfrak{F}$.

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

**Theorem II.** Let $\mathfrak{F}$ be aperiodic, or let $q = 0$. There is a linear combination $L = \sum_{i=1}^{p} \lambda_i y_i$ of the $y_i$, the $\lambda_i$ being polynomials$^{10}$ in the $u_i$ 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 $\Pi$ contains difference polynomials $Ny_i - M_i, i=1, \ldots, p$, where $N$ and the $M_i$ are polynomials in $w$ and the $u_i$ only, and $N$ is not in $\Pi$.

2. The $u_i$ constitute a set of parametric indeterminates for $\Pi$.

3. The solutions of $\Sigma$ and the corresponding values computed for $w$ from the equation $w = L$ constitute the totality of solutions of $\Pi$.

4. If the indeterminates of $\Pi$ are given the ordering $u_1, \ldots, u_q; w; y_1, \ldots, y_p$, then the first polynomial of a characteristic set$^8$ of $\Pi$ is of effective order in $w$ equal to the effective order of $\Sigma$, the remaining leaders of the characteristic set of $\Pi$, which introduce the $y_i, i = 1, \ldots, p$, are of zero effective order in the indeterminates they introduce, and the sum of the orders of the leaders of the characteristic set of $\Pi$ in the indeterminates they introduce is the order of $\Sigma$.

5. If $\Sigma$ is of equal order and effective order, the first polynomial of a characteristic set of $\Pi$ 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 $\Pi$ which are free of the $y_i$ constitute a reflexive prime difference ideal $\Lambda$. A characteristic set of $\Lambda$, with the $u_i$ used as the parametric indeterminates, will be called a resolvent system for $\Sigma$. We obtain a solution of the resolvent system from any solution of $\Sigma$ by using the equation $w = L$. From any solution of the resolvent system not annulling a certain polynomial $G$ which is not in $\Lambda$, we may obtain a solution of $\Sigma$ 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 $\lambda_i$ are in $\mathfrak{F}$.

11 In order to verify this we make the substitutions $y_i' = y_i, i = 1, \ldots, p$, the
To prove Theorem II we consider a generic zero \( u_j = \sigma_j, j = 1, \ldots, q \); \( y_i = \alpha_i, i = 1, \ldots, p \), of \( \Sigma \). Then the \( \alpha_i \) are transformally algebraic over the aperiodic difference field \( \mathcal{G} = \mathfrak{F}(\sigma_1, \ldots, \sigma_q) \). By Theorem I there exist elements \( \mu_i, i = 1, \ldots, p \), in \( \mathcal{G} \) such that \( \mathcal{G}(\mu_1 \alpha_1 + \cdots + \mu_p \alpha_p) \) contains some transform of each \( \alpha_i \).

If \( \mathfrak{F} \) is aperiodic, we may choose \( \mu_i \) in \( \mathfrak{F} \) by the final remark of \( \S 5 \). If \( \mathfrak{F} \) is periodic, \( q \neq 0 \) and there exist \( \mu_i \) which are quotients of difference polynomials in the \( \sigma_j \). We may, in fact, select quotients with denominator 1, for an extension \( \mathcal{G}(\gamma) \) of \( \mathcal{G} \) is identical with \( \mathcal{G}(\lambda \gamma) \) where \( \lambda \) is any element of \( \mathcal{G} \).

We consider \( \mu_i \) which are polynomials in the \( \sigma_j \) or, if \( q = 0 \), are elements of \( \mathfrak{F} \). To obtain the \( \lambda_i \) of Theorem II we replace the \( \sigma_j \), \( j = 1, \ldots, q \), in each polynomial \( \mu_i \) by the corresponding \( u_j \). Then \( \Pi \) is the ideal with generic zero \( u_j = \sigma_j, j = 1, \ldots, q, w = \sum_{i=1}^p \mu_i \alpha_i, y_i = \alpha_i, i = 1, \ldots, p \). For on the one hand this is evidently a solution of \( \Pi \). 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 \( u_j = \sigma_j, j = 1, \ldots, q; y_i = \alpha_i, i = 1, \ldots, p \). Hence \( \overline{R} \) is in \( \Sigma \). 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 \( \Pi \). (3) is evident. The field formed by adjoining to \( \mathfrak{F} \) the \( \sigma_j, j = 1, \ldots, q \), and \( \sum_{i=1}^p \mu_i \alpha_i \) contains all but a finite number of transforms of the \( \alpha_i \). The statements in (4) concerning effective orders follow from this. We obtain the same field by adjoining a generic zero of \( \Pi \) to \( \mathfrak{F} \) as we obtain by adjoining a generic zero of \( \Sigma \). This proves the statement in (4) concerning orders. If \( \Sigma \) is of the same order as effective order, then \( \Pi \) is also. (5) follows from this remark and (4).

Rutgers University