A Characterization of Linear Difference Equations Which are Solvable by Elementary Operations

CHARLES H. FRANKE (South Orange, New Jersey, U.S.A.)

1. Introduction and Summary

The purpose of this note is to clarify the concept of the solvability of linear homogeneous difference equations by elementary operations, particularly as it differs from the corresponding concept for differential equations.

In general the notation and terminology will be as in [1]. Some familiarity with [2, pp. 491–499] will be assumed. A brief introduction to the subject is given in the appendix to [7]. If L is a difference field then C_L is the subfield of L of constants. C_L^* is the algebraic closure of C_L. C_L^* does not have a difference field structure. Unless explicit exception is made, all other fields will be inversive difference fields characteristic zero. P_L is the subfield of L of periodic elements and P_L^t is the subfield of P_L of solutions to $y_t = y$. If N is a difference overfield of L then L_N is the algebraic closure in N of $L(C_N)$. Throughout, f is a linear homogeneous difference polynomial of effective order n with coefficients in k. *A solution field* for f is a difference overfield of k of the form $M = k\langle\alpha\rangle$ where $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(n)})$ is a fundamental system for f. α is called a *basis* for M. $G(N, L)$ is the transformal Galois group of N over L_N and $G_N = G(N, k)$. For a vector $v = (v^{(1)}, \ldots, v^{(n)})$, $W(v)$ and $W^{(s)}(v)$ are the $n \times n$ matrices $(v_j^{(i)})$ and $(v_{js}^{(i)})$ for $1 \leq i \leq n$, $0 \leq j < n$.

For a positive integer q, *L is a qLE of k*, if there is a chain $L^{(i)}$ of subfields of L, and a set $\zeta^{(i)}$ of elements of L, so that

$$k = L^{(0)} \subseteq L^{(1)} \subseteq \cdots \subseteq L^{(t)} = L, \; L^{(i+1)} = L^{(i)} \langle \zeta^{(i)} \rangle,$$

where either $\zeta^{(i)}$ is algebraic over $L^{(i)}$ or $\zeta^{(i)}$ satisfies an equation over $L^{(i)}$ of one of the forms $y_q = Ay$ or $y_q - y = A$. f is *solvable by elementary operations in M over k* if M is a solution field for f and M is contained in a qLE of k. (In Theorem 2 this concept is shown to be independent of the solution field M.) A group is *solvable* if it has a subnormal series whose factors are either finite or commutative.

With these definitions and the theorem of [4], Theorems 2.1 and 2.2 of [3] imply the following.

THEOREM 1. *f is solvable by elementary operations in M over k if and only if G_M is solvable.*

In the corresponding theory for differential equations [8], it is sufficient to consider

Received May 22, 1972

the case in which $C_M = C_k$ is algebraically closed. With this assumption, for differential or difference algebra if G_M is solvable then M is itself a $1LE$ of k. Further, some solution to f in M satisfies an equation of the form $y' = Ay$ $(y_1 = Ay)$, $A \in k$ and f is linearly reducible with a first order factor. [2, Th. 8; 6, Corollary to Th. 2.1; 8, Th. 1, p.35; Th. p. 38.]

In Section 2 it is shown that solvability by elementary operations does not depend on a particular fundamental system and that if f is solvable over k then f is solvable over any difference overfield of k. (These proofs are not trivial because of the possibility of incompatible extensions.)

If f is reducible at q to order r then there is an $F \in k^{(q)}\{y\}$ of order r, obtained in a canonical way, so that each solution to f is a solution to F [7, Introduction]. In Section 3 the relationship between solutions of f and of F is studied and it is shown that f is solvable over k if and only if F is solvable over $k^{(q)}$. f is reducible if there exists some q and some $r < n$ with f reducible at q to order r.

f *is linearly irreducible* if there does not exist a solution field M with f reducible with respect to M, and f is *irreducible* if f is not reducible. In Section 4 solution fields for linear homogeneous difference equations which are solvable by elementary operations, and which are linearly irreducible and irreducible are described in detail.

2. Independence of Solvability on M and k

If L is a qLE of k containing M and N is a generic solution field for f then L and N are compatible, and their compositum is $L(C_N)$, a qLE of k. Therefore Theorem 2 is trivial when N is a generic solution field for f and one might expect an easy proof for the theorem. Such a proof has not been found.

LEMMA 1. *Assume $C_1 \subseteq C_2$ are ordinary algebraic fields and that G_i is a multiplicative group of matrices with entries in C_i. If G_1 is solvable, connected and dense in G_2 then G_2 is solvable.*

Proof. G_1 is connected as a subset of $n \times n$ affine space over C_2^* [3, Lemma 1]. Therefore, there is a matrix A in C_2^* so that AG_1A^{-1} consists of matrices in triangular form. Since G_1 is dense in G_2, AG_2A^{-1} consists of matrices in triangular form and G_2 is solvable.

LEMMA 2. *Assume that M is a solution field over k, N is a difference overfield of k compatible with M and $Q = M\langle N\rangle$. If G_M is solvable then $G^* = G\ (Q, N)$ is solvable. If M and N are linearly disjoint over k and G^* is solvable then G_M is solvable.*

Proof. Define I to be the set of difference isomorphisms of M into Q leaving k_M fixed. I is a connected algebraic matrix group containing G_M as a dense subgroup [5, Proposition 3.1.] The mapping of G^* which takes each automorphism to its restriction to M is an isomorphism of G^* into I. If G_M is solvable then I is solvable by Lemma 1 and G^* is solvable.

If M and N are linearly disjoint over k then each element of I extends uniquely to an element of G^*. Therefore the restriction mapping is onto I, and I and G^* are isomorphic. If G^* is solvable then I and hence G_M is solvable.

THEOREM 2. *If M and N are solution fields for f, and f is solvable by elementary operations in M then f is solvable by elementary operations in N.*

Proof. Since there are solution fields compatible with both N and M, it is sufficient to consider the case in which N and M are compatible. If $Q=M\langle N\rangle$ then $Q=M\ (C_N)=N\ (C_M)$. Since G_M is solvable $G_Q=G(M\ (C_N),\ k\,(C_N))$ is solvable. Since $k_N(C_M)$ and N are linearly disjoint over k_N and $G_Q=G(N\ (C_M),\ k_N(C_M))$, G_N is solvable.

While Theorem 3 may appear trivial at first glance on reflection it is not obviously true. For example, one might conjecture the existence of an equation f with the following property. Each qLE of k containing a solution field for f contains a fixed periodic element p algebraic over k and $k\langle p\rangle$ is not compatible with some extension L of k.

THEOREM 3. *If f is solvable by elementary operations over $k\subseteq L$ then f is solvable by elementary operations over L.*

Proof. If $L\langle\alpha\rangle$ is a generic solution field for f over L then $M=k\langle\alpha\rangle$ is a solution field for f which is linearly disjoint from L over k. By Theorem 2, G_M is solvable. If $Q=M\langle L\rangle$ then Q is a solution field for f over L and by Lemma 2 $G\,(Q,\ L)$ is solvable.

3. Reducible Equations

The following theorem, which is of some independent interest, permits one to limit the study of solvable equations to irreducible equations. Familiarity with the Introduction of [7] is assumed.

THEOREM 4. *If* rord $f=r$, *each solution to f is a solution to $g(y)=\sum_{j=0}^{r} B^{(j)}y_{tj}$, $B^{(r)}=1$, $B^{(j)}\in k$, α is a fundamental system for f with $\alpha^{(1)},\ldots,\alpha^{(r)}$ linearly independent over periodic elements, and $F\in k^{(t)}\{y\}$ is defined by $F\ (y)=\sum_{j=0}^{r} B^{(j)}y_j$ then the following hold.*

1. *$\alpha^{(1)},\ldots,\alpha^{(r)}$ is a fundamental system for F.*
2. *If $p=(p^{(1)},\ldots,p^{(t)})$ is a fundamental system for $y_t=y$ over $k\langle\alpha^{(1)},\ldots,\alpha^{(r)}\rangle$ then $\{p^{(i)}\alpha^{(j)}:1\leqslant i\leqslant t,\ 1\leqslant j\leqslant r\}$ is a fundamental system for g.*
3. *Any solution to g in a difference overfield of $k\langle\alpha\rangle$ is a linear combination of $\alpha^{(1)},\ldots,\alpha^{(r)}$ with coefficients periodic of order t. A solution to g is a solution to F. A solution to F in a difference overfield of k is a solution to g.*
4. *The following are equivalent.*

A. *f is solvable by elementary operations over k.*
B. *g is solvable by elementary operations over k.*
C. *F is solvable by elementary operations over $k^{(t)}$.*

Proof. 1. $M^{(t)}=(k\langle\alpha\rangle)^{(t)}$ is a difference overfield of $k^{(t)}$ containing the $\alpha^{(i)}$. $\alpha^{(1)},\dots,\alpha^{(r)}$ are linearly independent over $P^t_M=C_{M^{(t)}}$, and clearly satisfy F.

2. For any i and j, $g(p^{(i)}\alpha^{(j)})=p^{(i)}g(\alpha^{(j)})=0$. If the c_{ij} are constants with $\sum c_{ij}p^{(i)}\alpha^{(j)}=0$, then the linear independence of $\alpha^{(1)},\dots,\alpha^{(r)}$ over periodic elements gives $\sum c_{ij}p^{(i)}=0$. Then, the linear independence of the $p^{(i)}$ over constants gives $c_{ij}=0$. Therefore, the $p^{(i)}\alpha^{(j)}$ are rt solutions to g which are linearly independent over constants.

3. Assume that β is a solution to g in a difference overfield L of $k\langle\alpha\rangle$. If $p^{(1)},\dots,p^{(t)}$ is a fundamental system for $y_t=y$ over L then there are constants c_{ij} with $\beta=\sum(c_{ij}p^{(i)})\alpha^{(j)}$.

β is a solution to F since $\beta\in L^{(q)}\supseteq k^{(q)}$.

If γ is a solution to F then γ formally satisfies g. Therefore γ is a solution to g if γ is contained in a difference overfield of k.

4. $A\to B$. If $k\subseteq k\langle\alpha\rangle\subseteq L$ where L is a qLE of k choose a fundamental system p for y_t-y over L. Then $L\langle p\rangle$, a $qtLE$ of k, contains a solution field for g.

$B\to A$. Choose a generic solution field $M=k\langle\alpha\rangle$ for f and a generic solution field $N=M\langle p\rangle$ for y_t-y over M. Choose L^*, a qLE of k containing $N^*=k\langle p,\alpha^{(1)},\dots,\alpha^{(r)}\rangle$. Since N is a purely transcendental extension of N^*, L^* and N are compatible. Since $\alpha^{(s)}$ is a solution to g, $\alpha^{(s)}$ is a linear combination of the $p^{(i)}\alpha^{(j)}$, $j\leqslant r$, with constant coefficients. Therefore $L=L^*\langle N\rangle$ can be obtained from L^* by adjoining constants, and L is a qLE of k containing M.

$A\to C$. If N is a qLE of k containing $k\langle\alpha\rangle$ then $N^{(t)}$ is a difference overfield of $k^{(t)}$ containing $k^{(t)}\langle\alpha^{(1)},\dots,\alpha^{(r)}\rangle$. Therefore it is sufficient to prove the following lemma.

LEMMA 3. *If N is a qLE of k then $N^{(t)}$ is a qLE of $k^{(t)}$.*

Proof. If $\zeta_q=A\zeta$ then $\zeta_{qt}=AA_t\dots A_{q(t-1)}\zeta$. If $\zeta_q=\zeta+A$ then $\zeta_{qt}=\zeta+(A+A_t+\dots+A_{q(t-1)})$. Therefore a chain $k=L_1\subseteq L_2\subseteq\dots\subseteq L_s=N$ proving that N is a qLE of k corresponds to a chain $k^{(t)}=L_1^{(t)}\subseteq L_2^{(t)}\subseteq\dots\subseteq L_s^{(t)}=N^{(t)}$ proving that $N^{(t)}$ is a qLE of $k^{(t)}$.

$C\to B$. The proof will use two lemmas.

LEMMA 4. *Assume $L_1,\dots,L_s$ are solution fields over k which are compatible and $G_i=G_{L_i}$ is solvable. If N is a compositum of the L_i then G_N is solvable.*

Proof. Define $M_i=L_i(C_N)$ and $G_i^*=G_{M_i}$. By Lemma 2, G_i^* is solvable. G_N is naturally isomorphic to a subgroup of the direct product of the G_i^*, so G_N is solvable.

LEMMA 5. *If $M=k\langle\alpha\rangle$ and $L=k^{(t)}\langle\alpha\rangle$ is a solution field over $k^{(t)}$ with $G(L,k^{(t)})$ solvable then $G(M^{(t)},k^{(t)})$ is solvable.*

Proof. In view of Lemma 4 it is sufficient to show that if $M_j = k^{(t)}\langle\alpha_j\rangle$ and $G_j = G(M_j, k^{(t)})$ then M_j is a solution field over $k^{(t)}$ and G_j is solvable. If L is a solution field for $\sum B^{(i)} y_i$ over $k^{(t)}$ then M_j is a solution field for $\sum B_j^{(i)} y_i$ over $k^{(t)}$.

If τ is the transform of $k\langle\alpha\rangle$ then $\psi \to \tau^j \psi \tau^{-j}$ is an isomorphism between $G^{(j)}$ and $G^{(0)}$, so $G^{(j)}$ is solvable.

Proof $C \to B$. Choose a fundamental system $p = (1, p^{(2)}, \ldots, p^{(t)})$ for $y_t = y$ over k and set $k_* = k\langle p\rangle$. Then $M = k_*\langle\alpha^{(1)}, \ldots, \alpha^{(r)}\rangle$ is a solution field for g over k_*. Any qLE of k_* is a $qtLE$ of k, so it is sufficient to prove that $G(M, k_*)$ is solvable. Since F is solvable over $k^{(t)}$, F is solvable over $k_*^{(t)}$ by Theorem 3. If $L = k_*^{(t)}\langle\alpha^{(1)}, \ldots, \alpha^{(r)}\rangle$ then $G(L, k_*^{(t)})$ is solvable. Therefore $G(M^{(t)}, k_*^{(t)})$ is solvable by Lemma 5 and its subgroup $G(M, k_*)$ is solvable.

4. Characterization of Solvable Equations

The following example illustrates all the points of the main theorem.

EXAMPLE 1. Assume $k = C(x)$ where C is the complex numbers with the identity transform and x is transcendental over C with $x_1 = x + 1$. Define $f(y) = y_2 - y_1 - x^2(x-2)y$, A as the difference ideal in $k\{y\}$ generated by f, and $M = k\langle\alpha, \beta\rangle$ where (α, β) is a fundamental system for f. The unique difference polynomial, of the form $y^n - (F^{(n)} y_1 + G^{(n)} y)$, in A has, by induction, $F^{(n)}$ and $G^{(n)}$ polynomials in x with positive integral initial coefficients. Therefore $F^{(n)} \neq 0$ and f is not reducible [7, Introduction].

Since $f(\beta) = 0$, $\beta_1 \neq (2-x)\beta$. If $j = (\alpha_1 + (x-2)\alpha)/(\beta_1 + (x-2)\beta)$ then $j_2 = j$ but $j_1 \neq j$. (By direct computation $j = (\alpha_2 - P\alpha)/(\beta_2 - P\beta)$ where $P = (x-2)(x-1)(x+1)$ and $i_1 = (\alpha_2 - Q\alpha)/(\beta_2 - Q\beta)$ where $Q = (x-2)(x-1)x)$. If $j_1 = j$ then $(P - Q)(\alpha_2\beta - \alpha\beta_2) = 0$ and $(\alpha/\beta) \in P_M$ contradicts f not being reducible.) If $\zeta = \alpha - j\beta$, $\eta = \alpha - j_1\beta$ then $\zeta_2 = P\zeta$, $\eta_2 = Q\eta$ so $M = k\langle\zeta, \eta, j\rangle$ is a $2LE$ of k.

If $\sigma \in G_M$, $\sigma(\alpha) = a\alpha + b\beta$, $\sigma(\beta) = c\alpha + d\beta$ for $a, b, c, d \in C_M$ then the equation $\sigma(j) = j$ is $cj^2 + (d-a)j - b = 0$, or $[c(j + j_1) + d - a]j - [b + cjj_1] = 0$. Therefore each $\sigma \in G_M$ has a matrix of form

$$\begin{pmatrix} a & c \\ -cjj_1 & a - c(j + j_1) \end{pmatrix} \quad a, c \in C.$$

Since $C_{k\langle\zeta\rangle} = C$ and t.d. $(k\langle\zeta\rangle, k) = 2$, [2, Lemma 2, p. 511], t.d. $(M, k_M) \geqslant 2$. Therefore t.d. $(M, k_M) = \dim G_M = 2$, and G_M is the set of all non-singular matrices as above. Since (α, β) was an arbitrary fundamental system and G_M is not in reduced form, f is linearly irreducible. [6, Th 2.1] Further, $\sigma(\zeta) = (a - cj)\zeta$, $\sigma(n) = (a - cj_1)\eta$ and the mapping $\sigma \to a - cj$ is an isomorphism of G_M into the multiplicative subgroup of P_M.

By iteration f determines $g\in A$ where $g(y)=y_4-x(x+1)(2x+3)y_2+(x-2)(x-1)x^2(x+1)^2y$. Since f is not reducible g is uniquely determined. With the notation $G(y)\circ H(y)=G(H(y))$, g admits the factorizations

$$g(y)=[y_2-x^2(x+1)\,y]\circ[y_2-Py]$$
$$=x(x+1)\,[y_2-Py]\circ[(y_2/(x-2)\,(x-1))-xy],$$
$$g(y)=[y_2-x(x+1)^2\,y]\circ[y_2-Qy]$$
$$=x(x+1)\,[y_2-Qy]\circ[(y_2/(x-2)\,(x-1))-(x+1)\,y].$$

If f is linearly reducible or reducible then the solvability of f by elementary operations can be studied by replacing f by an equation of order lower than that of f. Therefore it is sufficient to describe solvable equations which are linearly irreducible and irreducible.

THEOREM 5. *Assume that f is solvable by elementary operations in M over k, that f is linearly irreducible, and that f is not reducible. Then there is a vector $p=(p^{(1)},\ldots,p^{(n)})$ with components in a difference overfield of M, so that if $k^*=k\langle p\rangle$, $M^*=M\langle p\rangle$, $K=k^*_{M^*}$ and $\zeta^{(i)}=\sum p_i^{(j)}\alpha^{(j)}$, $0\leqslant i<n$ then the following hold.*

1. *$p^{(j)}$ is algebraic over C_M, $p^{(j)}\in P^n_{M^*}$, the least common multiple of the periods of the $p^{(j)}$ is n and there exist $B^{(i)}\in K$ with $\zeta^{(i)}_n=B^{(i)}\zeta^{(i)}$.*
2. *M^* is an nLE of k with a chain of $2n$ steps, n with equations $y_n=y$ adjoining the $p^{(j)}$ and n with equations $y_n=B^{(i)}y$ adjoining the $\zeta^{(i)}$.*
3. *G_M is isomorphic to a multiplicative subgroup of $P^n_{M^*}$ and G_M is commutative.*
4. *For $r=1,\ldots,n$ there exist $F^{(r)}\in K\{y\}$ of the form $F^{(r)}(y)=\sum_{i=0}^{n-1}b^{(i,r)}y_{ni}$, so that for any $iM^*=k\langle F^{(1)}(\alpha^{(i)}),\ldots,F^{(n)}(\alpha^{(i)})\rangle$* and *$(F^{(r)}(\alpha^{(i)}))_n=B^{(r)}F^{(r)}(\alpha^{(i)})$.*
5. *The unique difference polynomial $g(y)=\sum_{i=0}^{n}b^{(i)}y_{ni}$ in the ideal generated by $f(y)$ has $2n$ factorizations in the forms $g(y)=g^{(j)}(y)\circ(y_n-B^{(j)}y)$ and $g(y)=D^{(r)}(y_n-B^{(r)}y)\circ(F^{(r)}(y))$ for some $g^{(j)}\in K\{y\}$, $D^{(r)}\in K$.*

Proof. If α is any basis for M then there exist periodic elements $r^{(i)}$ so that if $\beta=\sum r^{(i)}\alpha^{(i)}$ then for each $\sigma\in G_M$ the unique extension σ' of σ to $M'=M\langle r\rangle$ with $\sigma'(r^{(i)})=r^{(i)}$ is such that there is a $\lambda\in P_M$, with $\sigma'(\beta)=\lambda\beta$[3, proof of Th 2.1]. Choose the smallest t so that for some basis α there is a $p=(p^{(1)},\ldots,p^{(t)})$ so that if $\zeta=\sum p^{(i)}\alpha^{(i)}$ then, with the notation as in the statement of the theorem, each $\sigma\in G_M$ extends to a $\sigma^*\in G_{M^*}$ for which there is a $q\in P_{M^*}$ with $\sigma^*(\zeta)=q\zeta$.

If $\sigma\in G_M$ and $\sigma(\alpha^{(j)})=\sum c_{ij}\alpha^{(i)}$ then

$$\sum_{i=1}^{t} qp_{(i)}\alpha^{(i)}=q\zeta=\sigma(\zeta)=\sum p^{(j)}\sigma(\alpha^{(j)})=\sum_{j=1}^{t}p^{(j)}\sum_{i=1}^{n}c_{ij}\alpha^{(i)}.$$

Therefore

$$qp^{(i)}=\sum_{j=1}^{t}c_{ij}p^{(j)}\quad\text{if}\quad i\leqslant t\quad\text{and}\quad\sum_{j=1}^{t}c_{ij}p^{(j)}=0\quad\text{if}\quad i>t.$$

If the $p^{(i)}$ were linearly dependent over C_M with $p^{(t)}=\sum_{i=1}^{t-1} c^{(i)} p^{(i)}$ then $\zeta=\sum_{i=1}^{t-1} p^{(i)}(\alpha^{(i)}+c^{(i)}\alpha^{(t)})$ would contradict the minimality of t. Therefore the $p^{(i)}$ are linearly independent over C_M and $c_{ij}=0$ for $j=1,\dots, t$, $i>t$. Therefore each $\sigma\in G_M$ maps the vector space generated by $\alpha^{(1)},\dots,\alpha^{(t)}$ onto itself. Since f is not linearly reducible with respect to M, $t=n$.

Assume that $p^{(1)},\dots,p^{(s)}$ is a maximal subset of the $p^{(i)}$ linearly independent over C_{M^*}. If $p^{(s+i)}=\sum_{j=1}^{s} d_{ij}p^{(j)}$, $d_{ij}\in C_{M^*}$ one obtains $\zeta=\sum_{i=1}^{s} p^{(i)}\beta^{(i)}$ where $\beta^{(i)}=\alpha^{(i)}+\sum_{j=1}^{n-s} d_{ji}\alpha^{(j+s)}$. As above, $s<n$ yields the contradiction that f is linearly reducible with respect to $k\langle\beta^{(1)},\dots,\beta^{(s)},\alpha^{(s+1)},\dots,\alpha^{(n)}\rangle$. Therefore $s=n$ and p is linearly independent with respect to C_{M^*}.

Since $\sum_{j=1}^{n} c_{ij}p^{(j)}=qp^{(i)}$, the n vectors $p_a=(p_a^{(1)},\dots,p_a^{(n)})$, $0\leqslant a<n$, are eigenvectors (c_{ij}) with eigenvalues q_a. Since $\det W(p)\neq 0$ the row rank of $W(p)$ is n and the p_a are linearly independent over C_{M^*}. Therefore $q,\dots,q_{n-1}$ are all of the eigenvalues of (c_{ij}). Then the characteristic equation, $F(t)$ of the $n\times n$ matrix (c_{ij}) has the form $[(t-q)\dots(t-q_{j-1})]^m$ where j is the period of q. Therefore j divides n for each q and $\sigma^*(\zeta_n/\zeta)=\zeta_n/\zeta$ for each $\sigma\in G_M$. As in the proof of Lemma 2, G_M is dense in G_{M^*} and $\zeta_n/\zeta\in K$. Further

$$\sigma^*(\zeta^{(i)})=\sum p_i^{(j)}\sigma(\alpha^{(j)})=\sum p_i^{(j)}c_{sj}\alpha^{(s)}=\sum_s\big(\sum_j c_{sj}p_i^{(j)}\big)\alpha^{(s)}=\sum_s q_ip_i^{(s)}\alpha^{(s)}=q_i\zeta^{(i)}.$$

As above $\zeta_n^{(i)}/\zeta^{(i)}\in K$. This completes the proof of 1 and 2 is now obvious.

The mapping of G_M into $P_{M^*}^n$ defined by $\sigma\to q$ is the isomorphism of 3.

Since $\det W(p)\neq 0$ the equations $\zeta^{(i)}=\sum p_i^{(j)}\alpha^{(j)}$ can be solved in the form $\alpha^{(j)}=\sum Q^{(i,j)}\zeta^{(i)}$ where $Q^{(i,j)}\in p_{M^*}^n$ and $(Q^{(i,j)})$ is non-singular. To prove that $Q^{(i,j)}\neq 0$ it is sufficient to show that any $n-1\times n-1$ submatrix of $W(p)$ is non-singular. If a column of such a submatrix W' is $(p^{(j)},\dots,p_{t-1}^{(j)},p_{t+1}^{(j)},\dots,p_{n-1}^{(j)})$ and $s=n-t-1$ then the s'th transform of W' has columns of the form $(p_s^{(j)},\dots,p_{n-2}^{(j)},p^{(j)},\dots,p_{s-1}^{(j)})$. W' is non-singular since any $n-1$ of the $p^{(j)}$ are linearly independent over C_{M^*}.

Choose $B^{(i)}\in K$ with $\zeta_n^{(i)}=B^{(i)}\zeta^{(i)}$. Then $\alpha_{nt}^{(j)}=\sum B^{(t,i)}Q^{(i,j)}\zeta^{(i)}$ where $B^{(t,i)}=B^{(i)}\dots B_{n(t-1)}^{(i)}$. Define $D^{(s,t)}=\delta(s,t)\zeta^{(s)}$. Then $W^{(n)}(\alpha)=W^{(n)}(\zeta)Q=BDQ$. Therefore $\zeta^{(1)}\dots\zeta^{(q)}\det Q\det B=\det W^{(n)}(\alpha)$. Since f is not reducible, $W^{(n)}(\alpha)$ is non-singular [7, Prop. 2.2], and B is non-singular. Define $F^{(r)}(y)=\det(B')/\det B$ where B' is like B except that the r'th column of B' is $(y,y_n,\dots,y_{n(n-1)})$. Then $F^{(r)}(\alpha^{(j)})=Q^{(r,j)}\zeta^{(r)}$, $F^{(r)}\in K\{y\}$, and $F^{(r)}(\alpha^{(j)})$ satisfies $y_n=B^{(r)}y$. Further $M^*=K\langle\zeta\rangle=K\langle F^{(1)}(\alpha^{(j)}),\dots,F^{(n)}(\alpha^{(j)})\rangle$ for any j. This completes the proof of 4.

The existence of g follows from the $n+1$ equations $y_{nt}=\sum_{i=0}^{n-1}A^{(i,t)}y_i$, $A^{(i,t)}\in k$, $t=0,\dots,n$ which are determined by f. g is unique since f is not reducible. If $r^{(1)},\dots,r^{(n)}$ are periodic elements of period n which are linearly independent over constants then $(r^{(1)}\zeta^{(i)},\dots,r^{(n)}\zeta^{(i)})$ is a fundamental system for $y_n=B^{(i)}y$. Since $g(r^{(i)}\zeta^{(j)})=0$, g admits a factorization $g(y)=g^{(i)}(y)\circ(y_n-B^{(i)}y)$. If $b^{(r)}$ is the leading coefficient of $F^{(r)}$ and $h(y)=[F^{(r)}(y_n)-B^{(r)}F^{(r)}(y)]$ then the unicity of g gives $h=g$ and $g(y)=1/b_n^{(r)}(y_n-B^{(r)}y)\circ F^{(r)}(y)$.

Remark 1. If $f(y)=y_2+Ay_1+By$ is solvable by elementary operations and is linearly irreducible and not reducible then by 5 the uniquely determined equation $g(y)=y_4+Cy_2+Dy$ can be factored in $(y_2+Ey)\circ(y_2+Fy)$. In this case the existence of such a factorization is also clearly sufficient for the solvability of f.

Remark 2. In Example 2.3 of [6] an example is given of a difference field K and an equation f so that there exist solution fields L and M for f with L a $1LE$ of K and M a proper subset of L. It does not appear that M is itself a qLE of K. There is no apparent test to determine if M is itself a qLE or even a $1LE$ of K.

Remark. 3. In Example 1 of [3] an example is given where a solution field M is a $2LE$ but not a $1LE$ of K. It does not appear that M is contained in a $1LE$ of K, but again there is no obvious approach to a proof of this conjecture.

REFERENCES

[1] COHN, R. M., *Difference Algebra* (Interscience Publ., New York, N.Y. 1965).

[2] FRANKE, C. H., *Picard-Vessiot Theory of Linear Homogeneous Difference Equations*, Trans. Amer. Math. Soc. *108*, 491–515 (1963).

[3] FRANKE, C. H., *Solvability of Linear Homogeneous Difference Equations by Elementary Operations*, Proc. Amer. Math. Soc. *17*, 240–246 (1966).

[4] FRANKE, C. H., *A Note on the Galois Theory of Linear Homogeneous Difference Equations*, Proc. Amer. Math. Soc. *18*, 548–551 (1967).

[5] FRANKE, C. H., *The Galois Correspondence for Linear Homogeneous Difference Equations*, Proc. Amer. Math. Soc. *21*, 397–401 (1969).

[6] FRANKE, C. H., *Linearly Reducible Linear Difference Operators*, Aequationes Math. *6*, 188–194 (1971).

[7] FRANKE, C. H., *Reducible Linear Difference Operators* Aequationes Math. *9*, 136–144 (1973).

[8] KOLCHIN, E. R., *Algebraic Matric Groups and the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations*, Ann. of Math. (2) *49*, 1–42 (1948).

Seton Hall University