SOLVABILITY OF LINEAR HOMOGENEOUS DIFFERENCE EQUATIONS BY ELEMENTARY OPERATIONS

CHARLES H. FRANKE

1. **Introduction and summary.** All notation and terminology will be as in [2]. In particular, all difference fields will be inversive difference fields of characteristic zero, and $K\langle\beta\rangle$ will denote the inversive difference field generated by K and β. C_L will denote the subfield of L consisting of all constants of L, and P_L will denote the subfield of L consisting of all periodic elements of L. If N is a difference overfield of L then Cl L denotes the algebraic closure of L in N and L_N denotes Cl$[L(C_N)]$. The Galois group of N over L is the set of difference automorphisms of N leaving L fixed. We assume throughout that f is a linear homogeneous difference equation of effective order n, and that M is a solution field for f over K with basis $\alpha=(\alpha^{(1)}, \cdots, \alpha^{(n)})$. A reference to "the matrix of an automorphism" refers to its matrix with respect to α.

If M is a Picard-Vessiot extension (PVE) of K, then M is contained in a generalized Liouvillian extension (GLE) of K if and only if the component of the identity of the Galois group of M over K is solvable [2, Theorem 8]. However, there are equations of the form $y_2=By$ for which the Galois group of M over K_M is commutative although M is not a GLE of K (Example 1, below). This indicates that it is not satisfactory from either the algebraic or analytic viewpoint to consider f to be "solvable by elementary operations" only if a solution field for f is contained in a GLE of K. In §2 a necessary and sufficient condition for the solvability of the Galois group in terms of more general overfields called qLE is given. This yields a definition of "solvability by elementary operations" which is acceptable at least from the algebraic viewpoint.

In §3 the application of the theory of §2 is illustrated.

In §4 an example is given correcting an error in an example of [2].

The author would like to thank Professor Richard Cohn of Rutgers University for his helpful comments on this paper. In particular Professor Cohn pointed out the error, and suggested the correction which appears in §4.

2. **Solvability of the Galois group.** The following example indicates that GLE are not sufficient for the study of the "solvability" of linear homogeneous difference equations.

Received by the editors November 24, 1964.

EXAMPLE 1. Assume that K contains an element j with $j_1 \neq j$ and $j_2 = j$, and an element B with the following property. If $B^k = PP_1$ or $B^k = P_1/P$ for $P \in K$ then $k = 0$. If α is any nonzero solution of $F(y) = y_2 - By$ then $M = K\langle\alpha\rangle$ is a solution field for F with basis $(\alpha, j\alpha)$. Further, [2, p. 511], t.d. $(M, K) = 2$, $C_M = C_K$ and the Galois group of M/K is commutative. We will show that M is not a GLE of K.

If M were a GLE of K then M would be a GLE of $N = K\langle\alpha\alpha_1\rangle$. Since M is just the rational functions in α and α_1 over K, N is algebraically closed in M. If the first nontrivial step in the chain showing that M is a GLE of N is $N \subset N\langle\beta\rangle$ then α is algebraic over $N\langle\beta\rangle$. If the minimal equation of α over $N\langle\beta\rangle$ is $\alpha^k + \cdots + P = 0$ then $P_2 = B^k P$. Therefore α^k/P is periodic and $\alpha^k \in N\langle\beta\rangle$. Since $N\langle\alpha^k\rangle \subset N\langle\beta\rangle$ there is an i with $N\langle\alpha^k\rangle = N\langle\beta^i\rangle$ [2, Propositions 5 and 6]. Since $\alpha\alpha_1 \in N\langle\alpha^k\rangle$, $N\langle\alpha^k\rangle = N(\alpha^k)$. Also $N\langle\beta^i\rangle = N(\beta^i)$. Therefore there are $P, Q, R, S \in N$ with

$$\alpha^k = (P\beta^i + Q)/(R\beta^i + S). \tag{1}$$

We assume first that β satisfies an equation of the form $y_1 = Dy$ over N. By eliminating α^k from (1) and its second transform, and equating the coefficients of the resulting polynomial in β to zero, one obtains the following equations. $PR_2B^k = P_2R$ and $QS_2B^k = Q_2S$. Since $\alpha^k \notin N$, $P = 0$ or $R = 0$, and $Q = 0$ or $S = 0$. In either case there is a $T \in N$ and an integer j with $\alpha^k = T\beta^j$. Therefore $(\alpha_1^k/\alpha^k) = (T_1D^j/T) \in N$ and α^k, $\alpha_1^k \in N$. This contradiction completes the proof in this case.

The second case, in which β satisfies an equation of the form $y_1 = y + D$ over N can be handled similarly.

If q is a positive integer then a *q-chain from K to N* is a sequence of fields

$$K = K_1 \subset K_2 \subset \cdots \subset K_t = N, \qquad K_{i+1} = K_i\langle\beta^{(i)}\rangle, \tag{2}$$

where $\beta^{(i)}$ is one of the following.

(a) Algebraic over K_i.

(b) A solution to an equation $y_q = y + B$ for some $B \in K_i$.

(c) A solution to an equation $y_q = Ay$ for some $A \in K_i$.

If there is a q-chain from K to N then *N is a qLE of K.*

If L is a difference field with algebraic field F and transform τ and j is a positive integer then $L^{(j)}$ will denote the difference field with algebraic field F and transform τ^j. In any discussion involving L and $L^{(j)}$ the notation A_1 will mean $\tau(A)$. We note that $L^{(j)}\langle\beta\rangle = L(\beta, \beta_j, \cdots)$ is contained in, but not always equal to, $(L\langle\beta\rangle)^{(j)}$. The relation between the concepts of qLE and GLE is given by the following.

PROPOSITION 2.1. *Assume that N is a difference overfield of K and q is a positive integer. N is a qLE of K if and only if $N^{(q)}$ is a GLE of $K^{(q)}$.*

PROOF. Assume that N is a qLE of K with q-chain (2). For each integer k, $\beta_k^{(1)}$ satisfies an equation of the same form as does $\beta^{(1)}$ over K_1, that is, an equation of one of the forms (a), (b) or (c). Therefore, the chain

$$K^{(q)} \subset K^{(q)}\langle\beta^{(1)}\rangle \subset K^{(q)}\langle\beta^{(1)}, \beta_1^{(1)}\rangle \subset \cdots$$
$$\subset K^{(q)}\langle\beta_1^{(1)}, \cdots, \beta_{q-1}^{(1)}\rangle = (K\langle\beta^{(1)}\rangle)^{(q)}$$

shows that $(K\langle\beta^{(1)}\rangle)^{(q)}$ is a GLE of $K^{(q)}$. Since $(K\langle\beta^{(1)}\rangle)^{(q)}$ is closed under the transform of N, the proof can be completed by induction on the length of the chain (2).

If $N^{(q)}$ is a GLE of $K^{(q)}$ with chain

$$K^{(q)} \subset K^{(q)}\langle\gamma\rangle \subset \cdots \subset N^{(q)}, \tag{3}$$

then $K\langle\gamma\rangle$ is a qLE of K. Since $K^{(q)}\langle\gamma\rangle \subset (K\langle\gamma\rangle)^{(q)}$, $N^{(q)}$ is a GLE of $(K\langle\gamma\rangle)^{(q)}$. Therefore, the proof can be completed by induction on the length of the chain (3).

The following theorem is a generalization of Theorem 7 of [2]. Its proof requires the following lemma for algebraic fields. F_t denotes the t-dimensional affine space over F.

LEMMA 1. *Assume that A is a subfield of the field B and that M is a subset of A_t which is connected in the Zariski topology on A_t. Then M is connected in the Zariski topology on B_t.*

PROOF. If the lemma is false then there are sets of equations S_i, $i=1, 2$, $S_i \subset B[x] = B[x^{(1)}, \cdots, x^{(t)}]$ with the following properties. Each element of M annuls exactly one S_i; M does not annul S_i. If v is a vector space basis of B over A then each $f \in B[x]$ can be written uniquely in the form $f = \sum g^{(j)} v^{(j)}$ for $g^{(j)} \in A[x]$. If S_i' is the set of all such $g^{(j)}$ which appear when each $f \in S_i$ is so expressed, then an element $z \in M$ annuls S_i' if and only if it annuls S_i. This gives the contradiction that M is not connected in the Zariski topology on A_t.

THEOREM 2.1.[1] *If $K = K_M$, M is normal over K, and the Galois group G of M/K is solvable then M is contained in a qLE of K.*

PROOF. Choose an algebraic closure P of P_M. Denote the algebraic

[1] **Added in proof.** In [3] it is shown that if $K = K_M$ then M is a normal extension of K.

field of P by p. Since P is compatible with M we may define $M^* = M\langle P\rangle$ and $K^* = K\langle P\rangle$. Each automorphism $\sigma \in G$ extends to an automorphism σ^* of M^*/K^* [2, Proposition 9]. Define G^* to be the set of all such σ^*. The set of matrices corresponding to G is identical with the set of matrices corresponding to G^*, so G^* is connected in the Zariski topology on $p_{n\times n}$ by the preceding lemma. Therefore G^* is a solvable, connected, matrix group with entries in an algebraically closed field and G^* may be put in simultaneous triangular form. Therefore there is a nonsingular matrix $(b^{(i,j)})$ with the property that if $\beta^{(i)} = \sum b^{(i,j)}\alpha^{(j)}$ then for each $\sigma^* \in G^*$ there exist $\lambda^{(i,j)} \in P$ so that $\sigma(\beta^{(i)}) = \sum \lambda^{(i,j)}\beta^{(j)}$ where $\lambda^{(i,j)} = 0$ if $i < j$. Further, if q is a common period of the $b^{(i,j)}$ then q is a period of each $\lambda^{(i,j)}$.

If $K_1 = K\langle b^{(i,j)}\rangle$ then K_1 is a qLE of K; we will show that $M_1 = M\langle b^{(i,j)}\rangle$ is a qLE of K_1. Since $b^{(i,j)}$ is nonsingular, $K_1\langle\alpha\rangle = K_1\langle\beta\rangle$. Since K_1 is algebraic over K and K is algebraically closed in M, K_1 and M are linearly disjoint over K. If v is a vector space basis of K_1/K then each $z \in M_1$ can be written uniquely in the form $z = \sum a^{(i)}v^{(i)}$ for $a^{(i)} \in M$. Therefore each automorphism $\sigma \in G$ extends to an automorphism σ_1 defined by $\sigma_1(z) = \sum \sigma(a^{(i)})v^{(i)}$. If G_1 is the set of all such extensions then the fixed field of G_1 is K_1 and G_1 admits the same triangular matrix representation as does G^*.

We will show by induction on n that M_1 is a qLE of K_1. For each $\sigma_1 \in G_1$ there is a $\lambda^{(n,n)}$ with $\sigma_1(\beta^{(n)}) = \lambda^{(n,n)}\beta^{(n)}$. If $\beta^{(n)} = 0$ then the inductive assumption applies. If $\beta^{(n)} \neq 0$ then $\beta_q^{(n)}/\beta^{(n)}$ is in the fixed field of each σ_1 and $\beta^{(n)}$ satisfies an equation of the form $y_q = Dy$ over K_1. The proof may now be completed by a slight modification of the proof of Proposition 7 of [2].

We note that the proof of Theorem 2.1 can be carried over to differential algebra. Since, in this case, the $b^{(i,j)}$ are constants one obtains the following theorem for differential fields.

THEOREM 2.1′. *If M is generated from K by adjoining a fundamental system for a linear homogeneous differential equation, $K = K_M$, M is normal over K, and the Galois group of M/K is solvable then M is contained in a GLE of K.*

The converse of Theorem 2.1 is a special case of the following generalization of Theorem 9 of [2]. The Galois groups referred to in Theorem 2.2 are not associated with solution fields. Therefore, they are not matrix groups.

THEOREM 2.2. *Assume that N is a qLE of K and that L is an intermediate field. The Galois group G of L over K_L is solvable.*

PROOF. Since G is isomorphic to a subgroup of the Galois group of $L^{(q)}$ over $\mathrm{Cl}[K(C_L)]^{(q)}$ it is sufficient to consider the case where N is a GLE of K. The proof is then the same as that of Theorem 9 of [2], except that there L is assumed to be a solution field over K and matrix groups are used. The proof may be modified by interpreting the notation in the following way.

For "$G(M, K)$" read "the Galois group of M/K."

For "$C(M, K)$" read "the Galois group of $M/\mathrm{Cl}\ K$."

For "$H<G$" read "H is isomorphic to a subgroup of G."

3. **Application to second order equations.** In this section we assume that K is $C(x)$, the rational functions over the complex numbers C with $x_1=x+1$, $f(y)=y_2-(A/D)y_1-(B/F)y$ where A, B, D, F, $\in C[x]$ and $(A, D)=1=(B, F)$. Further, we assume that D and F are monic and (α, β) is a basis for M over K. Lower case letters denote degrees of corresponding polynomials.

Theorem 3.1 is an illustration of the application of the theory. The theory is not complete since it is not known at present if there exists a solution field L for f with L normal over K_L.[2]

LEMMA 2. *If some solution to f is contained in a qLE of K then every solution field for f is contained in a qLE of K.*

PROOF. Assume that α is contained in a qLE of K. If $W=\alpha\beta_1-\alpha_1\beta$ then $W_1=-(B/F)W$. Over $K\langle\alpha, W\rangle\beta$ satisfies $y_1-y=(W/\alpha\alpha_1)$. Therefore M is contained in a qLE of K. If L is any solution field for f over K then L and M are compatible and there is a set of constants S with $L(S)=M(S)$ [2, Theorem 5].

THEOREM 3.1. *Assume that some solution field L for f is normal over K_L. If one of the following holds then no solution to f is contained in a qLE of K.*

(a) $D=F=1$, $a>2b$.

(b) $A=B=1$, $d>f$.

(c) *The leading coefficients of A and B are real and of the same sign,* $f>b$, *and* $a>f+2b+4d$.

PROOF. The computational details will be given for (a) only; (b) and (c) can be proved similarly.

We will show first that α/β is not periodic. For each integer t, f determines a unique equation $y_t=\Lambda^{(t)}y_1+M^{(t)}y$. If $(\alpha/\beta)_t=\alpha/\beta$ then $\Lambda^{(t)}(\alpha_1\beta-\alpha\beta_1)=0$ so $\Lambda^{(t)}=0$. However, from the recursion relation

[2] **Added in proof.** In view of the previously noted result of [3], this comment is no longer true, and the proof of Theorem 3.1 could be shortened slightly.

$$\Lambda^{(2)} = A, \quad \Lambda^{(3)} = AA_1 + B_1, \quad \Lambda^{(t+1)} = A\Lambda_1^{(t)} + B_1\Lambda_2^{(t-1)}$$

we find $\lambda^{(t+1)} = at$ and $\Lambda^{(t)} \neq 0$.

If a solution to f is contained in a qLE of K then we may assume that M is contained in a qLE of K and that M is normal over K_M. As in the proof of Theorem 2.1 there is a 2×2 matrix $b^{(i,j)}$ so that the following holds. If $M^* = M\langle b^{(i,j)}\rangle$ and $K^* = K\langle b^{(i,j)}\rangle$ then there is a group G of difference automorphisms of M^* over K^* with fixed field K^*. Further, if $\sigma \in G$ then there is a periodic element i with

$$\sigma(b^{(2,1)}\alpha + b^{(2,2)}\beta) = i(b^{(2,1)}\alpha + b^{(2,2)}\beta). \tag{1}$$

We will now define an element γ by cases.

Denote the matrix of σ with respect to (α, β) by C. If $b^{(2,1)} = 0$ set $\gamma = \beta$. Then $b^{(2,2)} \neq 0$, so $\sigma(\beta) = i\beta$ and $C^{(2,1)}\alpha + (C^{(2,2)} - i)\beta = 0$. Since α/β is not periodic, i is constant. If for each $\sigma \in G$, $C^{(2,1)} = 0$, set $\gamma = \beta$. If $b^{(2,1)} \neq 0$ and some $C^{(2,1)} \neq 0$ then (1) may be written as $\sigma(\alpha + j\beta) = i(\alpha + j\beta)$. Define $\gamma = \alpha + j\beta$. Proceeding as above we obtain

$$C^{(2,1)}j^2 + (C^{(2,2)} - C^{(1,1)})j - C^{(1,2)} = 0$$

and

$$i^2 - (C^{(1,1)} + C^{(2,2)})i + C^{(2,2)}C^{(1,1)} - C^{(2,1)}C^{(1,2)} = 0.$$

Since i and j satisfy quadratics with constant coefficients they satisfy $y_2 = y$. We note that in any case $\delta = \gamma_2/\gamma$ is left fixed by G.

From f we obtain

$$Ay_4 = (AA_1A_2 + AB_2 + A_2B_1)y_2 - (A_2BB_1)y \tag{2}$$

by transforming twice and eliminating odd order terms. Since γ satisfies (2), δ satisfies

$$A\delta\delta_2 = (AA_1A_2 + AB_2 + A_2B_1)\delta - A_2BB_1. \tag{3}$$

Since G leaves δ fixed there is a set of constants U with δ algebraic over $C(x, U)$. Since δ_2 can be expressed rationally in terms of δ, δ has no branch points and is rational in x. Writing $\delta = P/Q$ where P and Q are relatively prime in x, (3) becomes

$$APP_2 = (AA_1A_2 + AB_2 + A_2B_1)PQ_2 - A_2BB_1QQ_2.$$

There are three possibilities.

1. $a + 2p = 3a + p + q$.
2. $a + 2p = a + 2b + 2q \geqq 3a + p + q$.
3. $3a + p + q = a + 2b + 2q$.

Since $P \mid A_2BB_1Q_2$ and $Q_2 \mid AP$, $p \leqq a+2b+q$ and $q \leqq a+p$. The former contradicts 1, the latter 3, and 2 is inconsistent.

4. **Nonisomorphic solution fields.** Example 7 of [2] is incorrect in that the fields $K\langle \alpha, g\rangle$ and $K\langle \alpha, h\rangle$ defined there are actually isomorphic. The example may be corrected by defining h by $h_1^4 = -(h^4+1)$, $h_2 = h$. The field $K\langle h\rangle$ contains a subfield, $K(h, h_1^2)$, of genus one, while $K\langle g\rangle$ is of genus zero. $K\langle \alpha, g\rangle$ and $K\langle \alpha, h\rangle$ are not transformally isomorphic since a difference isomorphism between them would induce an isomorphism of $K\langle g\rangle$ and $K\langle h\rangle$.

It is interesting to note that $K\langle h\rangle$ contains a subfield isomorphic to $K\langle g\rangle$, namely the subfield generated by $h^4+(1/2)$.

References

1. R. Cohn, *Difference algebra*, Interscience, New York, 1965.

2. C. Franke, *Picard-Vissiot theory of homogeneous linear difference equations*, Trans. Amer. Math. Soc. **108** (1963), 491–515.

3. ———, *A note on the Picard-Vessiot theory of homogeneous linear difference equations* (in preparation).

Bell Telephone Laboratories, Inc., Whippany, New Jersey