PICARD-VESSIOT THEORY OF LINEAR HOMOGENEOUS DIFFERENCE EQUATIONS

BY
CHARLES H. FRANKE

1. **Introduction and acknowledgment.** In 1948 Professor E. Kolchin initiated the study of the Galois theory of differential fields with his papers on the Picard-Vessiot theory [3; 4]. In a recent paper Bialynicki-Birula developed a Galois theory, more general than is given here, but which will not handle the cases of interest in difference algebra([1]). The purpose of this paper is to develop a "Picard-Vessiot" theory for difference algebra.

It is a pleasure to acknowledge the advice received from Professor Richard Cohn of Rutgers University during the period in which this was written.

2. **Summary.** A solution field M/K is a field obtained from K by adjoining a fundamental system for a linear homogeneous difference polynomial. (All fields are inversive difference fields of characteristic zero.) If the field of constants of K is algebraically closed and equal to the field of constants of M, then M is a Picard-Vessiot extension (PVE) of K. The transformal Galois group G of a PVE is an algebraic matrix group over the field of constants of K. The Galois correspondence is one-to-one between relatively algebraically closed subfields of M and subgroups of G which are connected in the Zariski topology. A generalized Liouvillian extension (GLE) of K is a difference overfield of K which can be obtained from K by a chain of adjunctions of solutions to algebraic equations and equations of the form $y_1 = Ay$ or $y_1 = y + B$. A PVE is contained in a GLE if and only if the component of the identity of G is solvable. If $C(x)$ denotes the difference field of rational functions of x over the field of complex numbers with the transforming operation defined by $x_1 = x + 1$, then certain second order difference equations over $C(x)$ have the following property. Each solution is contained in a PVE of $C(x)$, but no solution is contained in a GLE of $C(x)$.

In [3] it is shown that if the corresponding definitions are made for differential equations then it is sufficient to restrict one's attention to the case of solution fields which are PVE. This is not the case in difference algebra since for some difference equations every fundamental system introduces new constants. For solution fields which are not PVE, a preliminary Galois theory and a theory of solvability analogous to the above are given. In order to apply either of these it is necessary to know that certain matrix groups are dense in varieties containing

Recejved by the editors July 18, 1962.

([1]) Amer. J. Math. **84** (1962), 89–109.

them. Examples are given to illustrate the difficulties involved. Certain nontrivial second order equations over $C(x)$ are shown to have the following property. No solution field is a PVE of $C(x)$ and no solution is contained in a GLE of $C(x)$.

The transcendence degree of a solution field over its constant field is an invariant of the equation. Compatible PVE are isomorphic, and a PVE is a specialization of any solution field compatible with it. Since any two solution fields over $C(x)$ are shown to be compatible, this is sufficient to establish the unicity of PVE (when they exist) over $C(x)$.

3. **Notation and terminology.** In general, the notation and terminology will be as in [1].

If L is a subfield of M then the transcedence degree of M over L is denoted by "t.d.(M, L)" and the algebraic closure of L in M by "$\bar{L}$". If $L = \bar{L}$ then L will be said to be "relatively closed." C_L is the field of constants of L, that is, the subset of L of elements satisfying $y_1 = y$. All fields will be inversive difference fields of characteristic zero. The ordinary difference field obtained from K by adjoining a solution of a linear difference equation is inversive. An "algebraic extension" will mean the inversive closure of a difference field extension by an algebraic element, and "$K\langle a\rangle$" will denote the inversive difference field generated by K and a. Since all fields are assumed to be inversive the concepts of order and effective order coincide.

The Casorati of a vector $b = (b^{(1)}, \cdots, b^{(n)})$ is defined as the determinant

$$\begin{vmatrix} b^{(1)} & \cdots & b^{(n)} \\ b_1^{(1)} & \cdots & b_1^{(n)} \\ \vdots & & \\ b_{n-1}^{(1)} & \cdots & b_{n-1}^{(n)} \end{vmatrix}$$

and denoted by "$C^*(b)$".

All topological statements will refer to the Zariski topology.

$C(x)$ will denote the rational functions of x over the field of complex numbers with the transforming operation defined by $x_1 = x + 1$.

4. **Galois theory.** M is a *solution field* over K for

$$f(y) = y_n + A^{(n-1)}y_{n-1} + \cdots + A^{(0)}y, \qquad A^{(0)} \neq 0, \qquad A^{(j)} \in K$$

if $M = K\langle b\rangle$ where $f(b^{(j)}) = 0$, and $C^*(b) \neq 0$. Any such vector b is a *basis* of M/K. If, in addition, C_K is algebraically closed and $C_M = C_K$ then M is a *Picard-Vessiot extension* (PVE) *of* K.

If $C^*(b) \neq 0$ then the elements $b^{(1)}, \cdots, b^{(n)}$ are linearly independent over the constant field of any difference field containing them [1, Chapter 8, Lemma 3]. The following proposition contains several results which will be needed in succeeding sections.

PROPOSITION 1. *Assume that M is a difference overfield of K and $R \subset C_M$.*

(1) *A subset of R linearly dependent over K is linearly dependent over C_K.*

(2) *A subset of R algebraically dependent over K is algebraically dependent over C_K.*

(3) *If N is a difference overfield of K with $C_N = C_K$ then N and $K(R)$ are linearly disjoint over K.*

(4) $C_{K(R)} = C_K(R)$.

Proof. Assume that (1) is false and w is a minimal linearly dependent set over K which is linearly independent over C_K. If $w^{(1)} = \sum k^{(j)} w^{(j)}$ for $k^{(j)} \in K$, then, transforming and subtracting shows that $k^{(j)} \in C_K$.

If w is an algebraically dependent set over K with $f(w) = 0$ and v is a vector space basis of K over C_K then f can be written $f(x) = \sum h^{(j)}(x) v^{(j)}$ for $h^{(j)} \in C_K[x]$. Since v is linearly independent over C_K, v is linearly independent over $C_{K(w)}$. Therefore $h^{(j)}(w) = 0$.

A vector space basis v of $K[R]/K$ can be chosen with $v^{(j)}$ a power product of elements of R, hence, constant. Then by (1), v is linearly independent over N. Therefore $K(R)$ and N are linearly disjoint over K [5, p. 50].

If (4) is false it is false for a finite set. By induction it is sufficient to consider the case where R consists of a single element d. If d is algebraic over K then each element of $K(d)$ can be written uniquely in the form $\sum a^{(i)} d^{(i)}$. Transforming and subtracting shows that $a^{(i)} \in C_M$. If d is transcendental over M then a new constant can be written uniquely as a quotient of relatively prime polynomials in d. Transforming shows that the coefficients are in C_M.

If M is a solution field for f over K with basis b and b' is any solution of f in a difference overfield N of M, then $b' = \sum c^{(j)} b^{(j)}$ for some $c^{(j)} \in C_N$ [1, Chapter 8, Theorem 13]. Therefore a homomorphism of $K\{b\}/K$ into a difference overfield N of M determines an $n \times n$ matrix c_{ij} in C_N by the equations $h(b^{(i)}) = \sum c_{ij} b^{(j)}$. The matrix so determined is unique as the $b^{(i)}$ are linearly independent over C_N. A homomorphism will be identified with its matrix. The following theorem and corollary show that the matrices corresponding to homomorphisms satisfy a set of algebraic equations over C_M, and, in the case of a PVE, form an algebraic matrix group.

THEOREM 1. *If M/K is a solution field with basis b then there is a set S_b in $C_M[x_{ij}]$ $(i,j = 1, \cdots, n)$ so that if N is a difference overfield of M then the following hold.*

(1) *A difference homomorphism of* $K\{b\}/K$ *to* N/K *determines a matrix in* C_N *satisfying* S_b.

(2) *A matrix in* C_N *satisfying* S_b *defines a difference homomorphism of* $K\{b\}/K$ *to* N/K.

(3) *If* $C_M = C_K$ *then a difference homomorphism of* $K\{b\}/K$ *to* N/K *determines a difference isomorphism if and only if its matrix is nonsingular.*

Proof. Define B to be the reflexive prime difference ideal in $K\{y\}$ with generic zero b. Define F from $K\{y\}$ to $M[x]$ by $F(y^{(i)}) = \sum x_{ij}b^{(j)}$, and J by $J = F(B)$. Each polynomial in J can be written as $H = \sum G^{(k)}v^{(k)}$ where $G^{(k)} \in C_M[x]$ and v is a vector space basis of M over C_M. Define S_b to be the set of all such G.

(1) If h is a difference homomorphism of $K\{b\}/K$ to N/K with matrix c_{ij} then the mappings $y^{(i)} \to b^{(i)} \to h(b^{(i)})$ and $y^{(i)} \to \sum x_{ij}b^{(j)} \to \sum c_{ij}b^{(j)}$ are identical. Therefore the latter sends B to zero, and each polynomial in J vanishes for $x_{ij} = c_{ij}$. Since the linear independence of v over C_M carries over to C_N, all the polynomials of S_b vanish at c_{ij}.

(2) If c_{ij} is a matrix in C_N satisfying S_b then the mapping

$$y^{(i)} \to \sum x_{ij}b^{(j)} \to \sum c_{ij}b^{(j)}$$

is a difference homomorphism of $K\{y\}/K$ whose kernel contains B. It therefore induces a homomorphism of $K\{b\}/K$ to N/K.

(3) The proof for the case $C_M = C_K$ can now be completed exactly as in [2, p. 35].

The proof of the following corollary follows easily from part (3).

COROLLARY. *If* M/K *is a PVE then the transformal Galois group is an algebraic matrix group* over C_K.

In the case of a PVE the Galois group corresponds to a variety T less its singular matrices. The singular matrices form a subvariety of lower dimension in the component of the identity of T, and cannot be dense in T. The following example shows that if $C_M \neq C_K$ then the variety T can be irreducible and have Zariski dense subsets of automorphisms, isomorphisms "into," and homomorphisms with nonzero kernel.

EXAMPLE 1. If $M = K(c)$, where $c_1 = c$, then M is a solution field for $y_1 - y = 0$. If c is transcendental then the set of equations determined as in Theorem 1 is $\{0\}$. $h(c) = kc$ defines a difference homomorphism of $K[c]$ to M for each $k \in C_M$. If $k \neq 0$, $k \in C_K$ or $k = t/c^2$ for $t \neq 0$, $t \in C_K$, then h extends to a difference automorphism of M. If k is a polynomial of positive degree in c, h extends to an isomorphism of M into M. For $k = t/c$, where $t \in C_K$, h is a homomorphism of $K[c]$ with nonzero kernel.

If M/K is a solution field and b a basis of M/K then "S_b" will denote the set of polynomials in Theorem 1, and "T_b" its variety in the algebraic closure of C_M. If there is no danger of confusion they will be denoted by "S" and "T." The

following example shows that a matrix in T may not correspond to a difference homomorphism of $K\{b\}$.

EXAMPLE 2. Taking b as a solution to $y_1 + y = 0$ which is transcendental over K, the constant field of $K(b)$ contains $C_K(b^2)$. The set S is $\{0\}$ and T contains the algebraic closure of $C_K(b^2)$. Since no difference overfield of $K\langle b\rangle$ contains b in its constant field, Theorem 1 does not apply to the matrix (b). The algebraic isomorphism of $K\{b\}$ to $K\{b\}$ defined by $h(b) = b^2$, is not a difference homomorphism.

If M is a difference overfield of K then M is a *normal extension* of K if for each element x of $M - K$ there is an automorphism s of M/K with $s(x) \neq x$.

The existence of proper monadic algebraic extensions suggests the existence of solution fields which are not normal extensions. Whether or not $M/\bar{K}$ is always a normal extension is not known at present. The following theorem is a weaker result.

THEOREM 2. *If M/K is a solution field and K is relatively closed then T is irreducible and* $\dim T = t.d.\ (M/K)$.

Proof. Assume that M/K is a solution field for f with basis b. Define F, B, J and S as in Theorem 1 and $\bar{S}$ as the ideal generated by S in $C_M[x]$. If B' is the perfect ideal generated by B in $M\{y\}$, then B' is prime and consists of linear combinations of elements of B with coefficients in M [1, Chapter 8, Corollary to Theorem 5]. Define $J' = F(B')$ and S' as the set of $G \in C_M[x]$ which appear when each $H \in J'$ is written as $H = \sum G^{(k)} v^{(k)}$ for a vector space basis v of M/C_M.

F maps $M\{y\}$ onto $M[x]$ since the equations $F(y_k^{(i)}) = \sum x_{ij} b_k^{(j)}$ can be solved for the x_{ij}, showing that each x_{ij} is in the range of F.

If b' is a generic zero of B' then f vanishes at b' so there are constants k'_{ij} in a difference overfield N of M with $b'^{(i)} = \sum k'_{ij} b^{(j)}$. If $h \in M[x]$ and $h = F(g)$ then $h(x_{ij}) = F(g(y^{(i)})) = g(\sum x_{ij} b^{(j)})$ so $h(k'_{ij}) = g(b'^{(i)})$. Therefore $h(k'_{ij}) = 0$ if and only if $g \in B'$ and J' is a prime ideal in $M[x]$ with generic zero k'_{ij}. Since v is linearly independent over C_N, S' is a prime ideal in $C_M[x]$ with generic zero k'_{ij}.

If $P \in B'$ then $P = \sum P^{(j)} m^{(j)}$ for $P^{(j)} \in B$ and $m^{(j)} \in M$. Therefore any element in J' can be written $F(P) = \sum F(P^{(j)}) m^{(j)}$ for $F(P^{(j)}) \in J$. If $H \in S'$ there is an $L \in J'$ with $L = Hv^{(1)} + \sum H^{(j)} v^{(j)}$. Also

$$L = \sum L^{(j)} m^{(j)} = \sum G^{(i,j)} v^{(i)} m^{(j)} \text{ for } G^{(i,j)} \in S.$$

Therefore $L = \sum G^{(i,j)} d^{(i,j,k)} v^{(i,j,k)}$ for $d^{(i,j,k)} \in C_M$. By the unicity of expression in terms of a vector space basis $H = \sum d^{(i,j,k)} G^{(i,j)}$ where the sum is for all i, j, k with $v^{(i,j,k)} = v^{(1)}$. Therefore $H \in \bar{S}$. Since $\bar{S}$ is contained in S', $\bar{S} = S'$. Since S' is prime, T is irreducible.

Since M is compatible with a generic zero of B, $\operatorname{ord} B = \operatorname{ord} B'$ [1, Chapter 8, Theorem 9]. Therefore

$$\text{t.d.}(M,K) = \text{ord}\, B = \text{ord}\, B' = \text{t.d.}(M\langle b'\rangle, M)$$

$$= \text{t.d.}(M(k'_{ij}), M) = \text{t.d.}(C_M(k'_{ij}), C_M) = \dim S' = \dim T.$$

The Galois correspondence for relatively closed intermediate fields in a PVE is given by the following theorem. Primes will be used in the usual way to denote the Galois correspondence.

THEOREM 3. *Assume that M/K is a PVE with transformal Galois group G, L is an intermediate field and H is an algebraic subgroup of G.*

(1) *L' is an algebraic matrix group.*

(2) *H is Galois closed.*

(3) *If L is relatively closed, then M is normal over L and L is Galois closed.*

(4) *There is a one-to-one correspondence between relatively closed intermediate fields and connected algebraic subgroups.*

(5) *If H is connected and normal in G, then G/H is the full group of H' over K and H' is normal over $\bar{K}$.*

(6) *If L is relatively closed and normal over K, then L' is normal in G and G/L' is the full group of L over K.*

Proof. Since M/L is a PVE, the first assertion follows from Theorem 1.

Since H is Zariski closed by hypothesis, to show $H = H''$ it is sufficient to show that H is dense in H'', or that a polynomial vanishing on H vanishes on H''. If f vanishes on H but not on H'' define F by $F(y) = f(W_y W_b^{-1})$ where W_y and W_b are the Casorati matrices of y and b. If $s \in G$ and the matrix of s is S then $F(s(b)) = f(W_{s(b)} W_b^{-1}) = f(S W_b W_b^{-1}) = f(S)$. Therefore there are polynomials $F \in M\{y\}$ with $F(s(b)) = 0$ for all $s \in H$ but not for all $s \in H''$. Choose such a polynomial E of minimal length as a sum of monomials and with some coefficient 1. If for $t \in H$, "E_t" denotes the result of applying t to the coefficients of E, then $E_t(s(b)) = t(E((t^{-1}s)b)) = 0$ for $s \in H$. Since $E - E_t$ is shorter than E, it vanishes at $s(b)$ for all $s \in H''$. If $E - E_t$ were not identically zero there would be a $k \in M$ with $E - k(E - E_t)$ shorter than E. Since $E - k(E - E_t)$ is zero at $s(b)$ for all $s \in H$ but not all $s \in H''$, this contradicts the choice of E. Therefore $E - E_t$ is identically zero, and the coefficients of E are left fixed by each $t \in H$. Therefore they are in H' and are left fixed by H''. Therefore $E(t(b)) = t(E(b)) = 0$ for all $t \in H''$, contradicting the choice of E. This completes the proof of (2).

If H is connected and z is algebraic over H' with conjugates $z^{(1)}, \cdots, z^{(n)}$ then the equations $F(z) = z^{(i)}$ partition H into a finite number of closed, disjoint, hence open subsets. Since H is connected it is contained in one of them. Since H contains the identity, all of H leaves z fixed. Therefore $z \in H'$ and H' is relatively closed.

If L is relatively closed then M/L is a PVE whose variety T is irreducible by Theorem 2. By Theorem 1, $T = L' \cup R$ where R is the set of singular matrices

of T. Since T contains the identity, R is of lower dimension than T. Therefore L' is dense in T. If L' were not connected there would be closed sets E and F with L' contained in their union but not contained in either E or F. Since L' is dense in T and $E \cup F$ is closed, $T \subset E \cup F$. Since T is irreducible, T and therefore L' is contained in either E or F contradicting the choice of E and F. To show that M is normal over L and $L = L''$ it is sufficient to show that each element z of $M - L$ is not in L''. If this is not the case, since L' is connected, L'' is relatively closed and L' leaves $\overline{L\langle z\rangle}$ fixed. If T and $T^{(z)}$ are the varieties determined by L and $\overline{L\langle z\rangle}$ then $\dim T > \dim T^{(z)}$. As above $T = L' \cup R$. Since $L' \subset T^{(z)}$, T is contained in the union of two varieties of lower dimension than T. This contradiction completes the proof of (3) and (4).

Assume that H is normal in G and connected. If $x \in H'$, $s \in G$ and $t \in H$ then $s^{-1}ts \in H$ so $t(s(x)) = s(x)$ and $s(x) \in H'$. Since s^{-1} also maps H' into itself, s maps H' onto itself. Therefore the restriction mapping of G to the group D of H' over K is a homomorphism. Its kernel is H and its range is the subgroup of D of elements having extensions to elements of G. We wish to show that this is all of D. Assume that $s \in D$. Each z in H' can be written as P/Q for P and Q in $k\{b\}$. A difference isomorphism s' of M will map z to $s(z)$ if and only if it satisfies $s'(P) = s(z)s'(Q)$. Therefore s' maps z to $s(z)$ if and only if its matrix satisfies

$$P\left(\sum x_{ij}b^{(j)}\right) = s(z)Q\left(\sum x_{ij}b^{(j)}\right).$$

These equations for the x_{ij} can be combined with S to give a set of equations in $C_K[x]$ whose nonsingular solutions in difference overfields of M are difference isomorphisms extending s. Since H is relatively closed, there is an extension of s to a difference isomorphism of M [1, Chapter 9, Corollary to Theorem 1]. Therefore the set of equations has a nonsingular solution in C_N for some difference overfield N of M. Since C_K is algebraically closed there is a nonsingular solution in C_K, and s has an extension to an element s' of G. Finally, since M is normal over K and H' is stable under G, H' is normal over K.

If L is normal over K and relatively closed in M then, as above, every automorphism s of L over K extends to an $s' \in G$. Since L is stable under s', if $t \in L'$ and $x \in L$ then $t(s'(x)) = s'(x)$, so $s'^{-1}ts' \in L'$. Therefore each such $s' \in N$, where N is the normalizer of L'. Since L is normal over K, $N' \cap L = K$. Since $L' \subset N$, $N' \subset L$ so $N' = K$. The normalizer of an algebraic matrix group is an algebraic matrix group [2, p. 29], so $N = G$. Therefore L' is normal in G. G/L' is the full group of L over K by (5).

In general the full transformal Galois group is not naturally isomorphic to a matrix group. The matrix of the composite of g and h is the matrix of g times the matrix obtained by applying g to the entries of the matrix of h. However, by adjoining the field C_M to K, and considering M as a solution field over $K(C_M)$, one obtains a group D which is naturally isomorphic to a group of matrices

contained in an algebraic variety T. Theorem 1 implies that T consists only of isomorphisms and singular matrices. The Galois correspondence given in Theorem 4 below for D and fields between $K(C_M)$ and M depends in part on whether a subgroup of D is dense in a variety containing it. Examples where this is not the case are not known.

THEOREM 4. *Assume that M/K is a solution field with basis b and H is any group of automorphisms of M/K which is naturally isomorphic to the set of matrices in T_b corresponding to H.*

(1) *Algebraic subgroups of H are Galois closed in H.*

(2) *Connected subgroups of H correspond to relatively closed intermediate fields.*

(3) *Assume that L is a relatively closed intermediate field, L' is the subset of H leaving L fixed, and T_b^L is the variety obtained by considering M as a solution field over L with basis b. If L' is dense in T_b^L then L is Galois closed with respect to H and L' is connected.*

Proof. The first two assertions can be proved as in Theorem 3. If L is relatively closed then T_b^L is irreducible. L' is dense in an irreducible variety so L' is connected. Assume that z is not in L but L' leaves z fixed. Since L' is connected, L' leaves $\overline{L\langle z\rangle}$ fixed. However, by Theorem 2 the variety of $\overline{L\langle z\rangle}$ is of lower dimension than T_b^L and cannot contain a dense subset of T_b^L. This contradiction shows that $L = L''$.

A crucial step in the study of the solvability of differential equations is the theorem that a solvable connected matrix group over an algebraically closed field is triangularable. To imitate the approach used in differential algebra, it is necessary to obtain a group of automorphisms whose matrix entries, with respect to some basis, are in an algebraically closed field, and whose fixed field has simple structure over K. If M/K is a solution field with basis b then the subsets of T_b and D consisting of nonsingular matrices with entries in C_K are automorphism groups. The following propositions and examples investigate these groups.

PROPOSITION 2. *If M/K is a solution field with basis b and Γ is a subfield of C_M then there is a set $S_b' \subset \Gamma[x_{ij}]$ so that the following hold.*

(1) *A solution to S_b' is a solution to S_b.*

(2) *A solution to S_b in Γ is a solution to S_b'.*

(3) *If Γ is algebraically closed and contained in K, then the variety of S_b' over Γ is an algebraic matrix group of automorphisms of M/K plus singular matrices.*

Proof. Write the polynomials F of S_b as $F = \sum f^{(k)} v^{(k)}$ where v is a vector basis of C_M over Γ and $f^{(k)} \in \Gamma[x_{ij}]$. Take S_b' as the set of all such $f^{(k)}$. The first two statements are now clear and the third can be proved using [2, Lemma 5.3].

Theorem 4 applies to any group $G_b^{(1)}$ obtained by deleting the singular

matrices from a variety $T_b^{(1)}$ determined as in Proposition 2 by a basis b and a subfield Γ. In all applications Γ will be the constants of the original ground field. That is, even if M is being considered as a solution field over $K(C_M)$, $G_b^{(1)}$ will be the group of automorphisms of $M/K(C_M)$ with matrix entries with respect to b in C_K. To be useful in the study of solvability it is necessary for each element in the fixed field of such a group to be algebraic over $K(C_M)$.

PROPOSITION 3. *Assume that M/K is a solution field with basis b, Γ is an algebraically closed field of constants of K, $G_b^{(1)}$ is the group determined as in Proposition 2, $C_b^{(1)}$ the component of the identity of $G_b^{(1)}$ and C_b the irreducible subvariety of T_b determined by $\bar{K}$. The following are equivalent and imply that $\bar{K}$ is Galois closed with respect to $C_b^{(1)}$.*

(a) *$C_b^{(1)}$ is dense in C_b.*

(b) $\dim C_b = \dim C_b^{(1)}$.

(c) *There is a basis for the ideal of C_b in $C[x]$.*

Proof. If $C_b^{(1)}$ is dense in C_b then $\bar{K}$ is Galois closed with respect to $C_b^{(1)}$ by Theorem 4. (Special case of (3) with $\bar{K} = L$, $C_b^{(1)} = L$ and $C_b = T_b^L$.)

a $\rightarrow$ b. The ideal of $C_b^{(1)}$ generates a prime ideal over C_M whose variety V has dimension $\dim C_b^{(1)}$. If $\dim C_b^{(1)} < \dim C_b$ there is a polynomial in $C_M[x]$ which vanishes on V but not on C_b. Therefore there is a closed set containing $C_b^{(1)}$ but not containing C_b. This contradicts (a).

b $\rightarrow$ c. If f is in the ideal of C_b write $f = \sum h^{(k)} v^{(k)}$ where $h^{(k)} \in \Gamma[x]$ and v is a vector space basis of C_M/Γ. If A is the set of all such $h^{(k)}$ then a solution to A is in C_b. Since the variety of A over $\bar{C}_M$ contains $C_b^{(1)}$ it has dimension $\dim C_b$. Since C_b is irreducible, C_b is the variety of A.

c $\rightarrow$ a. If S_b is the set of polynomials determined as in Theorem 1 by considering M as a solution field over $\bar{K}$ then C_b is the variety of S_b. If $S_b^{(1)}$ is the set of polynomials determined as in Proposition 2 by $M/\bar{K}$, b and Γ then $C_b^{(1)}$ is the variety of $S_b^{(1)}$. $S_b^{(1)}$ consists of all $h^{(k)} \in \Gamma[x]$ which appear when each $f \in S_b$ is written $f = \sum h^{(k)} v^{(k)}$ for a vector space basis of C_M/Γ. If R is a basis for S_b in $\Gamma[x]$ then each f in S_b can be written $f = \sum g^{(t)} R^{(t)}$ for $g^{(t)} \in C_M[x]$. To express f in the form $\sum h^{(k)} v^{(k)}$ it is sufficient to express the $g^{(t)}$ in that form. Therefore R is also a basis for $S_b^{(1)}$ and a polynomial vanishing on $C_b^{(1)}$ vanishes on C_b.

A solution field M/K is a *generalized Picard-Vessiot extension* (GPVE) if there is a basis b and an algebraically closed subfield Γ of C_K with $C_b^{(1)}$ dense in C_b. A solution field M/K for an equation f of order n will be called a *generic solution field for f* provided t.d. $(M, K) = n^2$.

PROPOSITION 4. *Every linear homogeneous difference equation has a generic solution field M/K. Therefore if C_K contains an algebraically closed subfield every linear homogeneous difference equation over K has a solution field which is a GPVE.*

Proof. If b is a basis for some solution field, choose n^2 algebraically independent constants c_{ij}, and set $d^{(i)} = \sum c_{ij} b^{(j)}$. Then $d^{(i)}$ is a solution to f, and $C^*(d) = \det c_{ij} C^*(b) \neq 0$. To determine the equations S_d it is sufficient by the proof of Theorem 1, to take all polynomials F in $K\{y\}$ with $F(d) = 0$, and write the equations $F(\sum x_{1j} d^{(j)}, \cdots, \sum x_{nj} d^{(j)}) = 0$ in terms of a basis of M over C_M. However, since the c_{ij} are algebraically independent over $K\langle b\rangle$ the equation

$$F(d) = F(\sum c_{1j} b^{(j)}, \cdots, \sum c_{nj} b^{(j)}) = 0$$

is an identity for constants c_{ij}. Therefore

$$F\left(\sum_k \left(\sum_j x_{1j} c_{jk}\right) b^{(k)}, \cdots, \sum_k \left(\sum_j x_{nj} c_{jk}\right) b^{(k)}\right) = 0$$

for all x_{ij}. Therefore S_d is $\{0\}$ and T_d is the full set of $n \times n$ matrices.

The following example shows that if b and d are two different bases for the same solution field then $C_b^{(1)}$ may be dense while $C_d^{(1)}$ is not.

EXAMPLE 3. If C_K is algebraically closed, z and z_1 are algebraically independent over K, and $z_2 = z$ then $K\langle z\rangle$ is a solution field over K for $y_2 - y = 0$. Among the bases are $b = (1, z)$ and $d = (z, z + zz_1)$. By the dimension theorem a generic zero of C_b and of $C_b^{(1)}$ is

$$\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix}$$

where x and y are algebraically independent over C_M.

By direct computation and the dimension theorem a generic zero of C_d is

$$\begin{pmatrix} x & y \\ x + y - w & w \end{pmatrix}$$

where x and y are algebraically independent over C_M and

$$w = y + (x + y)^2 + y^2 z z_1 + y(x + y)(z + z_1).$$

Therefore a generic zero of $C_d^{(1)}$ is

$$\begin{pmatrix} x & 0 \\ x - x^2 & x^2 \end{pmatrix}$$

which shows that $C_d^{(1)}$ is not dense in C_d.

5. **Unicity of compatible Picard-Vessiot extensions.** If L and M are compatible difference overfields then there are fields of the form $L\langle M'\rangle$ where M' is isomor-

phic to M. If K is algebraically closed in L then L is compatible with any difference overfield of K [1, Chapter 7, Corollary to Lemma 1].

The following theorem indicates the relation between the various solution fields for a given equation.

THEOREM 5. *If $L = K\langle a\rangle$ and $M = K\langle b\rangle$ are solution fields over K for f then t.d. $(L, K(C_L)) =$ t.d. $(M, K(C_M))$. If L and M are compatible the following hold.*

(1) *There is an isomorph M' of M and a set of constants R with $L(R) = M'(R)$.*

(2) *If L is a PVE, then there is a specialization $b \to b^*$ with $L = K\langle b^*\rangle$.*

(3) *If L and M are PVE of K, then L and M are transformally isomorphic over K.*

Proof. Choose a generic solution field $N = K\langle d\rangle$. K is algebraically closed in N so N and L are compatible. Choose $N\langle L'\rangle$ with $L' = K\langle a'\rangle$ isomorphic to L and set $D = C_{N\langle L'\rangle}$. Since there are $f_{ij}, g_{ij} \in D$ with $d^{(i)} = \sum f_{ij} a'^{(j)}$ and $a'^{(i)} = \sum g_{ij} d^{(j)}$, $N(D) = N\langle L'\rangle = L'(D)$.

Since $K(D)$ is linearly disjoint from N over $K(C_N)$ and L' over $K(C'_L)$, t.d. $(N, K(C_N))$ = t.d. $(N(D), K(D))$ = t.d. $(L'(D), K(D))$ = t.d. $(L', K(C'_L))$ = t.d. $(L, K(C_L))$. Therefore t.d. $(L, K(C_L))$ = t.d. $(M, K(C_M))$.

If L and M are compatible then there is a field $L\langle M'\rangle$ with $M' = K\langle b'\rangle$ isomorphic to M. If $R = C_{L\langle M'\rangle}$ then $L(R) = L\langle M'\rangle = M'\langle R\rangle$ as above. If L is a PVE of K and $b'^{(i)} = \sum c_{ij} a^{(j)}$ with $c_{ij} \in R$ then there is a specialization $k \to k^*$ of the generators of R into C_K not annulling $\det c_{ij}$. Since L and $K(R)$ are linearly disjoint over K, $(a, k) \to (a, k^*)$ is a specialization of $L(R)$ into L. Since $M'(R) = L(R)$, it restricts to a specialization of M' into L. Since $\det c^*_{ij} \neq 0$, the specialization is onto L. If M is also a PVE then t.d.(M, K) = t.d.(L, K) and the specialization is generic.

If $K = C(x)$ then K is algebraically closed in any solution field M. (If $Z \in M$ is an algebraic function then l.d.$(K\langle Z\rangle, K) = 1$. Therefore there is a j with $Z_j \in K(Z, \cdots, Z_{j-1})$ and the branch points of Z_j are among those of $Z, \cdots, Z_{j-1}$. Then Z_j has no branch points and Z is rational.) Therefore any two solution fields over K are compatible and Theorem 5 applies to equations over $C(x)$.

If K is the inversive closure of the rational functions of x over C where $x_1 = x^3$ then a and b, defined by $a^2 = b^2 = x$, $a_1 = xa$, and $b_1 = -xb$, are solutions to $y_2 = xy$. If d is a solution with t.d.$(K\langle d\rangle, K) = 2$ then $K\langle a, d\rangle$ and $K\langle b, d\rangle$ are solution fields for $y_2 = xy$ which are not compatible.

Example 7 shows that even if K is algebraically closed in solution fields L and M which are minimal in the sense that their only specializations are generic, L and M need not be transformally isomorphic over K.

6. **Solvability of difference equations in generalized Liouvillian extensions.** In order to study the solvability of linear homogeneous difference equations three

types of extensions will be used for constructing solution fields. They are solution fields for equations of the form $y_1 = Ay$ or $y_1 - y = B$, and algebraic extensions.

Equations of the form $y_1 - y = B$ have especially simple solution fields.

PROPOSITION 5. *If B is in K, $B \neq 0$, and a is a solution to $y_1 - y = B$ then $M = K(a)$ is a solution field over K with basis $b = (a, 1)$. If there is no solution to $y_1 - y = B$ in K then a is transcendental, $K(a)$ has no new constants, and there are no intermediate difference fields different from K and $K(a)$. If there is a solution $f \in K$ then $K(a)$ is an extension of K by a constant, which may be either transcendental or algebraic over K. If a is transcendental then T_b is the set of all matrices*

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

for c in the algebraic closure of C_M. If $C_M = C_K$ then the full Galois group of M/K is isomorphic to the additive group of C_K.

Proof. $C^*(a, 1) = -B \neq 0$ so $K\langle a \rangle$ is a solution field over K for $y_2 - ((B + B_1)/B)y_1 + (B_1/B)y$.

If there is no solution to $y_1 - y = B$ in K, then a is transcendental as an algebraic relation $a^n + Aa^{n-1} + \cdots + E = 0$ transforms to

$$(a + B)^n + A_1(a + B)^{n-1} + \cdots + E_1 = 0.$$

Equating coefficients, $A = A_1 + nB$, and $-(A/n)$ satisfies $y_1 - y = B$, a contradiction.

If for $C \neq 0$ the rational function of a,

$$P/Q = (Ca^n + Aa^{n-1} + \cdots + D)/(a^m + Ea^{m-1} + \cdots + F)$$

is constant, then $PQ_1 = QP_1$ so

$$P((a+B)^m + E_1(a+B)^{m-1} + \cdots + F_1) = Q(C_1(a+B)^n + A_1(a+B)^{n-1} + \cdots + D_1).$$

Therefore $C_1a^{n+m} = Ca^{n+m}$ and $C_1 = C$. Equating coefficients of a^{n+m-1} gives $mBC + E_1C + A = C_1E + A_1 + nBC_1$. Then, since $C_1 = C$, $(A/C) - E$ satisfies $y_1 - y = (m - n)B$ and $m = n$. If there were constants not in K, then there would be a rational function F of a whose numerator had minimal positive degree. By the above, F is of the form

$$F(a) = (Ca^n + f(a))/(a^n + g(a)) = C + (f(a) - Cg(a))/(a^n + g(a)).$$

Since C is constant, $f(a) - Cg(a) = 0$, and $F(a) = C$, a contradiction.

Now suppose L is an intermediate difference field, $L \neq K$. L is not algebraic over K as $K(a)$ is just the ordinary rational functions over K. Therefore a is algebraic over L. Then, as in the first step of the proof, there is an element E in L

satisfying $y_1 - y = B$. Then $a - E$ is constant and in C_K, so $a \in L$ and $L = K(a)$.

If there is a solution $f \in K$ to $y_1 - y = B$, then $a - f$ is constant and $K(a) = K(a - f)$ is an extension of K by a constant.

To obtain the matrices with respect to $(a, 1)$, clearly $1 \to 1$. If $a \to xa + y$ then the equation $a_1 - a = B$ gives $x = 1$. Therefore, the eligible matrices are at most all the matrices

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}.$$

By the dimension theorem, if a is transcendental, the matrices are all of the above. The last assertion is obvious.

It is not always possible to solve equations of the form $y_1 = Ay$ in a PVE. The following example shows that the existence of a PVE depends essentially on the ground field and not on A.

EXAMPLE 4. If C_K is algebraically closed and there is no solution to $y_1 = A^n y$ in K then Proposition 6 (below) shows that adjoining a solution b to $y_1 = -Ay$ preserves the constants of K. If a is a solution to $y_1 = Ay$ over $K\langle b\rangle$ then a^2/b^2 is constant. It cannot be specialized to a constant in C_K as a/b is not constant and C_K is algebraically closed.

PROPOSITION 6. *If a is a nonzero solution to $y_1 - Ay = 0$ over K and there is no nonzero solution in K to $y_1 - A^n y = 0$ for positive integral n, then a is transcendental and $K(a)$ has no new constants. If L is an intermediate difference field then $L = K(a^n)$ for some integer n. If there is such a solution in K then $K(a)$ is obtained from K by an extension by a constant, which may be either transcendental or algebraic, followed by an algebraic extension. If a is transcendental the variety T_a is the full set of all constants. If $C_{K(a)} = C_K$ then the full Galois group of $K(a)/K$ is a multiplicative subgroup of C_K.*

Proof. If there is no nonzero solution to $y_1 = A^n y$ in K then a is transcendental as an algebraic equation $a^n + \cdots + E = 0$ transforms to $A^n a^n + \cdots + E_1 = 0$. Then $E_1 = A^n E$, and $E = 0$ contradicts the minimality of n.

If $P/Q = (Ca^n + \cdots + B)/(a^m + \cdots + F)$ is constant with $C \neq 0$, then by by inverting if necessary we can assume $m \geqq n$. Since $P_1 Q = PQ_1$,

$$Q(C_1 A^n a^n + \cdots + B_1) = P(A^m a^m + \cdots + F_1).$$

Equating coefficients of a^{n+m} gives $C_1 A^n = CA^m$. Therefore $C_1 = A^{m-n}C$, and $C \neq 0$ gives $m = n$, $C_1 = C$. The proof that there are no new constants can now be completed as in Proposition 5.

If L is an intermediate difference field and $L \neq K$, then a is algebraic over L. As above there is a nonzero solution E in L to $y_1 = A^n y$, for some positive integer n.

Since a^n is also a solution to $y_1 = A^n y, a^n = CE$ for some C in C_K and $K(a^n) \subset L$. Then $L = K(a^m)$ for some positive integer m.∎

If there is an $f \in K$ with $f_1 = A^n f$ then $K(a)$ may be obtained from K by the chain $K \subset K(a^n/f) = K(a^n) \subset K(a)$. The first step is an extension by a constant and the last algebraic.

The final assertion is obvious.

The following definition is motivated by Propositions 5 and 6. N/K is a *Liouvillian extension* (LE) if there is a chain

$$K \subset K_1 \subset K_2 \cdots \subset K_t = N, \qquad K_{j+1} = K_j\langle a^{(j)}\rangle \tag{1}$$

where $a^{(j)}$ is one of the following.

(a) A solution to an equation $y_1 - y = B$, where $B \in K_j$ and there is no solution in K_j to $y_1 - y = B$.

(b) A solution to an equation $y_1 = Ay$ where $A \in K_j$ and there is no nonzero solution in K_j to any equation $y_1 = A^n y$, n a positive integer.

(c) Algebraic over K_j.

More generally N is a *generalized Liouvillian* extension (GLE) of K if there is a chain (1) with $a^{(j)}$ one of the following.

(a) A solution to $y_1 - y = B$, $B \in K_j$.

(b) A solution to $y_1 = Ay$, $A \in K_j$.

(c) Algebraic over K_j.

Theorem 6 is an immediate consequence of the definition of LE.

THEOREM 6. *If M/K is a solution field with C_K algebraically closed, and M is contained in a LE N/K then M is a PVE of K.*

Proof. It is sufficient to show that $C_N = C_K$. By the preceding propositions it is sufficient to show that an algebraic step in the chain (1) does not introduce new constants. The first such constant introduced would be algebraic over C_K. Since C_K is algebraically closed this is impossible.

Detection of the solvability of an equation from the solvability of a matrix group is based on the following proposition.

PROPOSITION 7. *If $M = K\langle a^{(1)}, \cdots, a^{(n)}\rangle$ and S is a set of isomorphisms of M with the property that for $h \in S$ there are constants $C_{ij} \in M$, with*

$$h(a^{(j)}) = C_{jj}a^{(j)} + \cdots + C_{jn}a^{(n)},$$

then M is a GLE of the fixed field L of S.

If each $C_{jj} = 1$ then M can be obtained from L by solving equations of the type $y_1 - y = B$.

If $C_{ij} = \delta_{ij}C_{ij}$ then M can be obtained from L by solving equations of the type $y_1 = Ay$.

Proof. The proof will be made by induction on the number of nonzero $a^{(j)}$.

Since $h(a^{(n)}) = C_{nn}a^{(n)}$ for each h, $a_1^{(n)}/a^{(n)} \in L$ and $a^{(n)}$ may be adjoined to L by solving $y_1 - (a_1^{(n)}/a^{(n)})y = 0$. Set $b^{(j)} = (a^{(j)}/a^{(n)})$, $c^{(j)} = b_1^{(j)} - b^{(j)}$ and $\bar{C}_{jk} = C_{jk}/C_{nn}$.

$$h(b^{(j)}) = \bar{C}_{jj}b^{(j)} + \cdots + \bar{C}_{j,n-1}b^{(n-1)} + \bar{C}_{nn}$$

$$h(c^{(j)}) = \bar{C}_{jj}c^{(j)} + \cdots + \bar{C}_{j,n-1}c^{(n-1)}$$

The $c^{(j)}$ may be adjoined by the inductive assumption, and then the $b^{(j)}$ by solving $y_1 - y = c^{(j)}$.

If $C_{ij} = \delta_{ij}C_{ij}$ then for each h, $h(a^{(j)}) = C_{jj}a^{(j)}$ so $(a_1^{(j)}/a^{(j)}) \in L$.

The proof for the case $C_{jj} = 1$ will be made by induction. Since $h(a^{(n)}) = a^{(n)}$, $a^{(n)}$ is already in L. In the above $\bar{C}_{jj} = 1$ so the $c^{(j)}$ can be adjoined by the inductive assumption, and the $b^{(j)}$ as above.

THEOREM 7. *Assume that M/K is a solution field and H is a connected group of automorphisms of M/K with matrix entries with respect to some basis b in an algebraically closed subfield of C_M. (It need not be isomorphic to the set of matrices corresponding to H.)*

(a) *If H is solvable M/H' is a GLE.*

(b) *If H is reducible to diagonal form, M/H' can be obtained by solving equations of the type $y_1 = Ay$.*

(c) *If H is reducible to special triangular form, M/H' can be obtained by solving equations of the type $y_1 - y = B$.*

Proof. By the previous proposition it is sufficient to apply the theorem that a solvable connected matrix group over an algebraically closed field admits triangular form.

COROLLARY. *If M/K or $M/K(C_M)$ is a GPVE with $C_b^{(1)}$ dense and solvable then M/K is a GLE.*

For PVE the situation is as in differential algebra.

THEOREM 8. *If M/K is a PVE then M/K is a GLE if and only if the component of the identity of the Galois group is solvable.*

Proof. If the component of the identity is solvable then M is a GLE of its fixed field by Theorem 7. Therefore by Theorem 3 M is a GLE of $\bar{K}$ and hence of K [1, Chapter 5, Theorem 18]. The converse is a special case of Theorem 9 below.

The group of M/K will be denoted by "$G(M, K)$" and its component of the identity by "$C(M, K)$." If G and H are groups of automorphisms having matrix representations with respect to a vector b then "$H < G$" will mean that each matrix of an automorphism in H is the matrix of an automorphism in G. (It is not necessary that H and G be isomorphic to their matrices.)

The following proposition will be used to extend the theory to solution fields contained in GLE.

PROPOSITION 8. *Assume that M/K is a solution field for f, $M_1 = M\langle R\rangle$ and $K_1 = K\langle R\rangle$.*

(1) *If K_1 and M are linearly disjoint over K then $G(M,K) < G(M_1,K_1)$.*

(2) *If $C_M = C_K$ and R consists of constants then $G(M,K) < G(M_1,K_1)$.*

(3) *If R is an algebraically independent set over M and $K\langle R\rangle = K(R)$ then $G(M,K) < G(M_1,K_1)$.*

(4) *If R consists of elements algebraic over K then $G(M,\bar{K}) < G(M_1,\bar{K}\langle R\rangle)$.*

Proof. An automorphism s of M/K extends uniquely to an s' of M_1/K_1 [1, Chapter 8, Lemma 1]. The mapping of s to s' is the identity on matrices so $G(M,K) < G(M_1,K_1)$.

If R consists of constants, Proposition 1 (3) applies.

If R is an algebraically independent set over M then $K(R)$ and M are linearly disjoint over K [5, Chapter 3, Proposition 3].

If R consists of elements algebraic over K then $\bar{K}\langle R\rangle$ and M are linearly disjoint over $\bar{K}$ [5, Chapter 3, Theorem 2].

THEOREM 9. *If M/K is a solution field contained in a GLE N/K then $C(M,K(C_M))$ is solvable.*

Proof. By Proposition 8 (2) $C(M,K(C_M)) < C(M(C_N),K(C_N))$. Therefore it is sufficient to consider the case $C_N = C_K$. If the chain from K to N is $K \subset K\langle a\rangle \subset \cdots \subset N$ then by induction on the length of the chain $C(M\langle a\rangle/K\langle a\rangle)$ is solvable. If a is transcendental over M then, since a satisfies $a_1 = a + B$ or $a_1 = Aa$ over K, $K\langle a\rangle = K(a)$. By Proposition 8 (3) $G(M,K) < G(M\langle a\rangle,K\langle a\rangle)$ and $C(M,K)$ is solvable. If a is algebraic over K then by Proposition 8 (4) $C(M,K) < G(M,\bar{K}) < G(M\langle a\rangle,\bar{K}\langle a\rangle) < G(M\langle a\rangle,K\langle a\rangle)$ so $C(M,K)$ is solvable.

If a is transcendental over K but algebraic over M there are two cases. If a satisfies $y_1 - y = B$ over K then $a \in M$, $K(a)$ is stable under $G(M,K)$ and $G(K(a),K)$ is commutative (Proposition 5). Therefore $G(M,K(a))$ is normal in $G(M,K)$ with commutative factor group and $C(M,K)$ is solvable [2, Lemma 4.9].

If a satisfies $y_1 = Ay$ over K then a^n is in M for some positive integer n, $K(a^n)$ is stable under $G(M,K)$ and $G(K(a^n), K)$ is commutative (Proposition 6). $C(M,K(a^n)) < G(M, K\langle a^n\rangle) < G(M\langle a\rangle, K\langle a\rangle)$ (by Proposition 8 (4)) so $C(M,K(a^n))$ is solvable. Since $G(M,K(a^n))$ is normal in $G(M,K)$ with commutative factor group $C(M,K)$ is solvable [2, Lemma 4.9].

COROLLARY. *If M/K is a solution field contained in a GLE N/K and $M/K(C_M)$ is a GPVE then M/K is a GLE.*

The following theorem is useful in the study of the solvability of particular difference equations in GLE (e.g. Theorem 13 below).

THEOREM 10. *Assume that K is a difference field and L and M are solution fields for f over K. If L is contained in a GLE N of K and M is compatible with N then M is contained in a GLE of K.*

Proof. Since M and N are compatible there is a field $M\langle N'\rangle$ with N' isomorphic to N. Then $M\langle N'\rangle = N'\langle C_{M\langle N'\rangle}\rangle$ is a GLE of K containing M.

COROLLARY 1. *If N is a generic solution field for f and some solution field for f is contained in a GLE of K then N is contained in a GLE of K.*

Proof. K is algebraically closed in N.

COROLLARY 2. *If $K = C(x)$ and a solution field for f is contained in a GLE of K then every solution field for f is contained in a GLE of K.*

Proof. K is algebraically closed in any solution field.

7. **Application to second order equations.** Throughout this section L will be the difference polynomial $y_2 - Ay_1 - By$ over a difference field K with C_K algebraically closed, and α will be a solution to L with t.d. $(K\langle\alpha\rangle, K) = 2$. The following theorem may be used to show that PVE suffice for the study of the solution fields of a particular difference equation.

THEOREM 11. *If the only nonzero solutions to $y_1 = B^n y$ in $K\langle\alpha\rangle$ are $n = 0$, $y \in C_K$ then any solution b of L is contained in a PVE M of K. If b is contained in a GLE of K then M is a GLE of K.*

Proof. Assume that b is contained in a GLE N of K and choose a solution α of L with t.d. $(N\langle\alpha\rangle, N) = 2$. If $W = C^*(\alpha, b)$ then $W_1 = -BW$ so $N(W)$ is a GLE of K. Over $N(W)$ α/b satisfies $y_1 - y = W/bb_1$ so $N\langle\alpha\rangle$ is a GLE of K. To complete the proof it is sufficient to define a PVE M/K with $b \in M$ and $M \subset N\langle\alpha\rangle$.

By Proposition 6, $K\langle\alpha, W\rangle$ has constant field C_K and t.d. $(K\langle\alpha, W\rangle, K) = 3$. If b is algebraic over $K\langle\alpha, W\rangle$ then $K\langle\alpha, b\rangle$ is a PVE of K. If b is transcendental over $K\langle\alpha, W\rangle$ then t.d. $(K\langle b\rangle, K) = 2$ and $K\langle b, W\rangle$ has constant field C_K. Since α/b satisfies $y_1 - y = W/bb_1$ over $K\langle b, W\rangle$, either $K\langle b, \alpha\rangle$ is a PVE or there is an element d of $K\langle b, W\rangle$ with $d = \alpha + cb$ for some constant c. $C^*(b, d) = C^*(b, \alpha) \neq 0$, and $K\langle b, d\rangle = K\langle b, W\rangle$ is a PVE of K for L.

The following lemma will be used to prove the existence of PVE for certain equations over $C(x)$.

LEMMA. *If $K = C(x)$ and there is a solution in $K\langle\alpha\rangle$ not in K to $y_1 = Dy$ for some $D \in K$ then there exist E, $F \in C[x]$, $G \in K$ and a positive integer n with $(E\alpha_1 + F\alpha)_n = G(E\alpha_1 + F\alpha) \neq 0$.*

Proof. If $z_1 = Dz$ then z may be written as s/t for s and t relatively prime in $K[\alpha, \alpha_1]$. Since $s_1 t = Dst_1$, there is a $T \in K$ with $s_1 = Ts$, $Tt = Dt_1$. Therefore there is a solution in $K[\alpha, \alpha_1] - K$ to an equation of the form $y_1 = Dy$.

Since transforming preserves total degree in α and α_1, such a solution can be taken homogeneous of positive degree in $K[\alpha, \alpha_1]$. Then

$$(A^{(0)}\alpha_1^n + \cdots + A^{(n)}\alpha^n)_1 = D(A^{(0)}\alpha_1^n + \cdots + A^{(n)}\alpha^n)$$

or

$$A_1^{(0)}\alpha_2^n + \cdots + A_1^{(n)}\alpha_1^n = D(A^{(0)}\alpha_1^n + \cdots + A^{(n)}\alpha^n).$$

If $b = \alpha_1/\alpha$ then $b_1 = (Ab + B)/b$ and $\alpha_2/\alpha = bb_1$. Dividing by α^n gives

$$b^n(A_1^{(0)}b_1^n + \cdots + A_1^{(n)}) = D(A^{(0)}b^n + \cdots + A^{(n)}).$$

Define f in $K[t]$ by $f(t) = A^{(0)}t^n + \cdots + A^{(n)}$, and denote $A_1^{(0)}t^n + \cdots + A_1^{(n)}$ by $f_1(t)$.

Choose an extension of the transform to the algebraic closure $\bar{K}$ of K and define $t_1 = t$. Factor f in $\bar{K}[t]$ to $f(t) = H(t - s^{(1)}) \cdots (t - s^{(m)})$. Then $f_1(t) = (f(t))_1 = H_1(t - s_1^{(1)}) \cdots (t - s_1^{(m)})$ and since $b^n f_1(b_1) = Df(b)$,

$$b^n H_1\left(\frac{Ab + B}{b} - s_1^{(1)}\right) \cdots \left(\frac{Ab + B}{b} - s_1^{(m)}\right) = DH(b - s^{(1)}) \cdots (b - s^{(m)}).$$

Assume that some $s^{(j)}$ is not in K. Then there is an i with $s_1^{(i)} = (As^{(i)} + B)/s^{(j)}$. $s^{(i)}$ is not rational as $B \neq 0$ and for some k, $s_1^{(k)} = (As^{(i)} + B)/s^{(i)}$, $s^{(k)} = ((AA_1 + B_1)s^{(j)} + A_1 B)/(As^{(j)} + B)$. Continuing in this way one obtains a chain $s^{(j)}, s^{(i)}, s^{(k)}, \cdots$ in which each term is not rational and so that each term has a transform which can be expressed rationally in terms of any preceding term. Such a chain must have a repetition so some $s_p^{(q)}$, $p > 0$, can be expressed rationally in terms of $s^{(q)}$. Since $s^{(q)}$ is not rational, $s^{(q)}$ and $s_p^{(q)}$ have different branch points. This contradiction shows that each $s^{(j)}$ is rational.

Replacing $s^{(j)}$ by $E^{(j)}/F^{(j)}$ and b by α_1/α one obtains

$$\alpha_1^{n-m}(F^{(1)}\alpha_1 + E^{(1)}\alpha)_1 \cdots (F^{(m)}\alpha_1 + E^{(m)}\alpha)_1 = G^{(0)}\alpha^{n-m}(F^{(1)}\alpha_1 + E^{(1)}\alpha) \cdots (F^{(m)}\alpha_1 + E^{(m)}\alpha).$$

This can be rewritten as

$$(F^{(1)}\alpha_1 + E^{(1)}\alpha)_1 \cdots (F^{(n)}\alpha_1 + E^{(n)}\alpha)_1 = G^{(0)}(F^{(1)}\alpha_1 + E^{(1)}\alpha) \cdots (F^{(n)}\alpha_1 + E^{(n)}\alpha).$$

Any $(F^{(j)}\alpha_1 + E^{(j)}\alpha)_1$ divides the right side of the equation in $K[\alpha, \alpha_1]$ so there is a chain $F^{(1)}\alpha_1 + E^{(1)}\alpha$, $F^{(i)}\alpha_1 + E^{(i)}\alpha, \cdots$ in which any two different elements

satisfy a relation of the form $(E^{(i)}\alpha_1 + F^{(i)}\alpha)_k = G(E^{(j)}\alpha_1 + F^{(j)}\alpha)$ and no term is zero. An eventual repetition in this chain gives a relation of the desired form.

THEOREM 12. *If $K = C(x)$ and B is monic and of degree one in $C[x]$ then every solution to $L(y) = y_2 - y_1 - By$ is contained in a PVE of K. No solution of L is contained in a GLE of K.*

Proof. Assume that M is a PVE of K for L contained in a GLE of K. By Theorem 9 the group G of M/K has a solvable component of the identity H. Therefore H is triangularable and some solution a of L is such that a_1/a is left fixed by H. Therefore a_1/a is an algebraic function b. Since $b_1 = 1 + (B/b)$, b and b_1 have the same branch points. Therefore b is a rational function. If $b = P/Q$ for P, $Q \in C[x]$ then $PP_1 = PQ_1 + BQQ_1$. However, if $dP > dQ$ then PP_1 has greater degree than $PQ_1 + BQQ_1$. If $dQ \geqq dP$ then

$$d(BQQ_1) > d(PP_1 - PQ_1).$$

Therefore no such relation is possible and no PVE of K for L is contained in a GLE of K.

To complete the proof it is sufficient by Theorem 11 and Proposition 9 to show that if $Z_1 = B^nZ$ for $Z \neq 0$ and Z in $K\langle\alpha\rangle$ then $n = 0$ and $Z \in C_K$. If $Z \in K$ then $n = 0$ and $Z \in C_K$. If Z is not in K then the lemma applies and there are polynomials E, F not both zero and a rational function G with $(E\alpha_1 + F\alpha)_j = G(E\alpha_1 + F\alpha)$ for some $j > 0$. To complete the proof it is sufficient to show that no such relation can exist.

If either E or F is zero the relation has the form $\alpha_j = H\alpha$ for some H in K. This is clearly impossible for $j = 1$. To show that it is impossible for $j > 1$ we will show that for each such j there exist unique polynomials R and S with positive leading coefficients so that $\alpha_j = R\alpha_1 + S\alpha$. The unicity is immediate since t.d. $(K\langle\alpha\rangle, K) = 2$ and the existence will be proved by induction. For $j = 2$, $\alpha_2 = \alpha_1 + B\alpha$. If $\alpha_k = R\alpha_1 + S\alpha$ where R and S have positive leading coefficients then

$$\alpha_{k+1} = (R_1 + S_1)\alpha_1 + R_1B\alpha$$

so α_{k+1} is of the same form.

If neither E nor F is zero we may assume that either E or F is monic. We may also assume that j is even. If $E^{(j)}\alpha_1 + F^{(j)}\alpha = (E\alpha_1 + F\alpha)_j$ then

$$E^{(0)} = E \qquad E^{(2j+2)} = (1 + B_1)E_2^{(2j)} + F_2^{(2j)},$$

$$F^{(0)} = F \qquad F^{(2j+2)} = B(E_2^{(2j)} + F_2^{(2j)}).$$

Since a relation as above gives $E^{(2j)} = GE$ and $F^{(2j)} = GF$ the following must hold.

(1) $dE^{(2j)} - dE = dF^{(2j)} - dF$.

(2) $e^{(2j)} = e$ if and only if $f^{(2j)} = f$.

(Lower case letters denote leading coefficients.) In each of the possible cases a contradiction to (1) or (2) will be obtained.

Case I. $dF > dE + 1$. Assume $e = 1$. A contradiction to (1) can be obtained by proving by induction that

$$dE^{(2j)} = dF + (j-1) \qquad e^{(2j)} = jf$$

$$dF^{(2j)} = dF + j \qquad f^{(2j)} = f.$$

Case II. $dF = dE + 1$. Assume $f = 1$.

A. If e is not a negative integer, a contradiction to (2) is obtained by proving the following:

(a) $$dE^{(2j)} = dE + j \qquad e^{(2j)} = e + j,$$

(b) $$dF^{(2j)} = dF + j \qquad f^{(2j)} = 1.$$

B. If $e = -k$ for a positive integer k then (b) holds, (a) holds for $j \neq k$ and $dE^{(2k)} < dE + k$. The proof can be made in three steps, by induction for $j < k$, the special case $j = k$ with subcases $k \neq 1$, $k = 1$, and by induction for $j > k$. This contradicts (2) for $j \neq k$ and (1) for $j = k$.

Case III. $dF = dE$. Assume $e = 1$.

A. If f is not a negative integer, a contradiction to (2) follows from

(a) $$dE^{(2j)} = dE + j \qquad e^{(2j)} = 1,$$

(b) $$dF^{(2j)} = dF + d \qquad f^{(2j)} = f + j.$$

B. If $f = -k$ for a positive integer k then (a) holds, (b) holds for $j \neq k$ and $dF^{(2k)} < dF + k$. This can be proved and the proof completed as in Case II part B.

Case IV. $dF < dE$. Assume $e = 1$. A contradiction to (1) follows from the following relations:

$$dE^{(2j)} = dE + j \qquad e^{(2j)} = 1,$$

$$dF^{(2j)} = dE + j \qquad f^{(2j)} = j.$$

The following example shows that neither part of Theorem 12 can be generalized without some restriction on the polynomial B.

EXAMPLE 5. If D is any rational function then the equation

$$y_2 - y_1 - (D_1 D - D)y = 0$$

is satisfied by a solution a to $y_1 = Dy$. Any solution field $K\langle a, b\rangle$ is a GLE of K as $W = C(a, b)$ can be adjoined to $K\langle a\rangle$ by solving $y_1 = (D - D_1 D)y$ and b/a can be adjoined to $K\langle a, W\rangle$ by solving $y_1 - y = W/aa_1$.

Taking $D = x$ the equation $y_2 - y_1 - x^2 y = 0$ is therefore solvable in a GLE. If b is solution with $C(a, b) \neq 0$ and $Z = (b_1 - xb)/a$ then $Z \neq 0$ and $Z_1 = -Z$. Therefore is a Z^2 constant not in C_K, and no PVE of K contains a.

If b is a solution with t.d.$(K\langle b\rangle, K) = 2$ then a linear polynomial as described in the lemma is $b_1 - xb$, since $(b_1 - xb)_1 = -x(b_1 - xb)$.

By trivial modifications of the proof of Theorem 12 one may show that equations of various types do not have solution fields which are PVE contained in GLE of $C(x)$. The difficulty is in showing that PVE suffice for the study of the solution fields of such equations.

The following lemmas will be used to prove that equations exist which do not have solution fields M/K with $M/K(C_M)$ a GPVE.

LEMMA 1. *If M/K is a solution field for $y_2 - By$, then the group of $M/\overline{K(C_M)}$ is commutative. A matrix representation of the group consists of matrices of the form*

$$\begin{pmatrix} x & -ye \\ y & x - yf \end{pmatrix}$$

where e and f are fixed constants not both in C_K, and x and y are in C_M.

Proof. If (a, b) is a basis set $j = a/b$. Then $j_2 = j$ so $e = jj_1$ and $f = j + j_1$ are constants. Since $C^*(a, b) \neq 0$, $j_1 \neq j$. Since j is algebraic over $C_K(e,f)$ and C_K is algebraically closed $C_K(e,f) \neq C_K$.

An automorphism with matrix

$$\begin{pmatrix} E & F \\ G & H \end{pmatrix}$$

leaving $\overline{K(C_M)}$ fixed, leaves j fixed and satisfies

$$(Ea + Fb)b = (Ga + Hb)a.$$

Since $ab = jb^2$ and $a^2 = j^2b^2$, $(E - H)j + F - Gj^2 = 0$. Since $j^2 = jf - e$, $(E - H - Gf)j + (F + Ge) = 0$. Since 1 and j are linearly independent over C_M, $H = E - Gf$ and $F = -Ge$.

LEMMA 2. *Assume that B has the following properties.*

(1) *If $B^n = PP_1$ for P in K then $n = 0$.*

(2) *If $B^n = P_1/P$ for P in K then $n = 0$.*

If a is a nonzero solution to $L(y) = y_2 - By$, then $K\langle a\rangle$ has constant field C_K and t.d.$(K\langle a\rangle, K) = 2$.

Proof. If a were algebraic over K with minimal equation $a^n + \cdots + P = 0$ then $B^n a^n + \cdots + P_2 = 0$ and $P_2 = B^n P$ contradicts (1), since

$$P_2/P = (P_1/P)(P_2/P_1).$$

If t.d.$(K\langle a\rangle, K) = 1$ and c is a constant in $K\langle a\rangle$ but not in C_K then a is

algebraic over $K(c)$. Therefore there is a P in $K(c)$ with $P_2 = B^t P$. P can be written in the form

$$c^n + \cdots + Qc^j/Rc^m + \cdots + Sc^i$$

where $SQ \neq 0$.

Transforming twice gives $Q_2 S = B^t Q S_2$ and Q/S contradicts (1). Therefore $K\langle a\rangle$ has constant field C_K. If the minimal equation of a over $K(a_1)$ is $a^n + Qa^{n-1} + \cdots + P = 0$ then $P_2 = B^n P$. Since a^n also satisfies $y_2 = B^n y$, a^n/P is periodic and therefore in C_K. Since the equation $Qa^{n-1} + \cdots + (P + a^n) = 0$ has coefficients in $K(a_1)$, $n = 1$ and $a \in K(a_1)$. Similarly if the equation of a_1 over $K(a)$ is $a_1^n + \cdots + P = 0$ then $P_2 = B_1^n P$, $(a_1^n/P) \in C_K$, and $a_1 \in K(a)$. Therefore a can be written in the form $a = (Pa_1 + Q)/(Ra_1 + S)$ where $Q = 1$ or $S = 1$. If $Q = 1$, transforming twice and comparing ratios of coefficients gives $P = B_1 P_2$ and $S = BS_2$. Therefore $P = S = 0$ and $aa_1 = T$. Then $B = T_1/T$ contradicting (2). If $S = 1$, proceeding as above gives $R = 0$ and $Q = 0$. Therefore $a_1 = Ta$ and $B = TT_1$ contradicting (1). Therefore t.d.$(K\langle a\rangle, K) = 2$.

Since transforming preserves total degree in a and a_1, a constant in $K\langle a\rangle$ not in K can be taken as a quotient of homogeneous polynominals in $K[a, a_1]$. If F is such a quotient then, by inverting if necessary, F can be written in the form

$$(Sa_1^n + \cdots + Pa^n)/(Ra_1^m + \cdots + Qa^m)$$

with $R \neq 0$ or $Q \neq 0$. Since F_1 is

$$(P_1 a_1^n + \cdots + S_1 B^n a^n)/(Q_1 a_1^m + \cdots + R_1 B^m a^m)$$

$RQ \neq 0$ and $P = 0$ if and only if $S = 0$. Therefore F can be written as

$$F = a^i a_1^i (Sa_1^n + \cdots + Pa^n)/(Ra_1^m + \cdots + Qa^m)$$

with $PQRS \neq 0$.

$$F_1 = B^i a^i a_1^i (P_1 a_1^n + \cdots + S_1 B^n a^n)/(Q_1 a_1^m + \cdots + R_1 B^m a^m).$$

Therefore $B^i RP_1 = SQ_1$ and $B^{n+i} QS_1 = B^m PR_1$ and $B^m = B^n (QS_1/PR_1)(SQ_1/RP_1)$. Therefore $B^{m-n} = (QS/PR)(Q_1 S_1/P_1 R_1)$ and $m = n$ by (1). Further $B^i = SQ_1/RP_1$ and $B^i = PR_1/QS_1$ so $B^{2i} = (SP/RQ)(RQ/SP)_1$ and $i = 0$ by (2).

Therefore a constant must be of the form

$$F = (Sa_1^n + \cdots + Pa^n)/(a_1^n + \cdots + Qa^n)$$

for $SPQ \neq 0$. Transforming twice gives $SB_1^n = S_2 B_1^n$ so S is constant. Long division shows that $F - S = 0$, and each constant in $K\langle a\rangle$ is in C_K.

EXAMPLE 6. The following examples indicate that hypotheses (1) and (2) of Lemma 2 are necessary. The equation $y_2 = PP_1 y$ has a solution defined by

$a_1 = Pa$ with t.d.$(K\langle a\rangle, K) = 1$. If b is a solution with t.d.$(K\langle b\rangle, K) = 2$ then $(Pb + b_1)^2/Pbb_1$ is a constant not in C_K.

The equation $y_2 = (P_1/P)y$ has a solution defined by $a_1 = P/a$ with t.d.$(K\langle a\rangle, K) = 1$. If b is a solution with t.d.$(K\langle b\rangle, K) = 2$ then bb_1/P is a constant not in C_K.

If $K = C(x)$ then hypothesis (2) of Lemma 3 is satisfied by any rational function B of nonzero degree. If B has a zero or pole c with $c + n$ neither a zero nor pole for $n \neq 0$ then B will satisfy (1).

PROPOSITION 9. *If B is as in Lemma 2 and M/K is a solution field for L then $M/\overline{K(C_M)}$ is not a GPVE.*

Proof. If (a, b) is any basis then by Lemma 2 K and $K\langle a\rangle$ have the same constant field. By Proposition 1, $K\langle a\rangle$ and $K(C_M)$ are linearly disjoint over K. Therefore t.d. $(K\langle a, C_M\rangle, K\langle C_M\rangle) =$ t.d. $(K\langle a\rangle, K) = 2$. Therefore by Lemma 1, t.d.$(M, \overline{K(C_M)}) = 2$, and the group of $M/\overline{K(C_M)}$ is the full set of matrices of Lemma 1. The subgroups of matrices with entries in C_K is the set of scalar matrices which is not dense.

EXAMPLE 7. Assume that B is as in Lemma 2 and α is any solution to L. Choose g and h transcendental over $K\langle\alpha\rangle$ and set $g_1 = -g$, $h_1 = 1/h$, $M = K\langle\alpha, g\rangle$ and $N = K\langle\alpha, h\rangle$. M and N are solution fields for L with bases $(\alpha, g\alpha)$ and $(\alpha, h\alpha)$. M and N are minimal solution fields in the sense that their only specializations are generic. If M and N were transformally isomorphic over K there would be $A, B, C, D \in C_N$ so that $\alpha \to A\alpha + B\alpha h$, $g\alpha \to C\alpha + D\alpha h$, and therefore $g \to (A + Bh)/(C + Dh)$. By direct computation from $g_1 = -g$ one obtains the contradiction $h = -1$.

The following theorem establishes a second class of equations solvable in PVE but not in GLE. In addition the concept of GPVE is shown to be nonvacuous.

THEOREM 13. *Assume that $K = C(x)$, $L(y) = y_2 - Ay_1 - ey$ where A is a polynomial of positive degree and e a complex number, and M is a solution field for L.*

(1) *No solution of L is contained in a GLE of K.*
(2) *M is a GPVE of $\overline{M(K(C_M))}$.*
(3) *If e is not a root of unity then M is generic and a PVE.*
(4) *If e is a root of unity but $e \neq -1$ then M is not a PVE.*

Proof. If a solution of L is contained in a GLE of K then a generic solution field $N = K\langle\alpha, \beta\rangle$ is contained in a GLE and the group D of $N/\overline{K(C_N)}$ is solvable. A contradiction will be obtained by showing that D is the full group of 2×2 matrices if e is not a root of unity and the full unimodular group if e is a root of unity. The complete proof will use the following three lemmas whose proofs are below.

(1) If $z \in K\langle \alpha \rangle$ and $z_1 = cz$ for $c \in C$ then $c = 1$ and $z \in C$.

(2) If $z \in K\langle \alpha \rangle - K$ and $h \in K$ then $z_1 \neq hz$.

(3) If $z \in K\langle \alpha, W \rangle$ where $W = C^*(\alpha, \beta)$ then $z_1 - z \neq W/\alpha\alpha_1$.

Assume that e is not a root of unity. By (1), $K\langle \alpha, W \rangle$ has constant field C. Since β/α satisfies $y_1 - y = W/\alpha\alpha_1$ over $K\langle \alpha, W \rangle$ by (3) $N = K\langle \alpha, \beta \rangle$ is a PVE. Since t.d.$(N, K) = 4$, D is the full group of 2×2 matrices. If M is any solution field for L then t.d.$(M, K(C_M)) = 4$ so M is a generic solution field and a PVE.

If $e^n = 1$ then $C_{K\langle \alpha \rangle} = C$ by (1). Since $W_1 = -eW$, W is periodic. By (3) $C_N = C_{K\langle \alpha, W \rangle}$. Therefore $\overline{K(C_N)} = K(W)$, and D is the full unimodular group. If $M = K\langle a, b \rangle$ is any solution field and $W' = C^*(a,b)$ then t.d.$(\overline{M, K(C_M)}) = 3$ and $W' \in \overline{K(C_M)}$. Therefore the group G of $M/\overline{K(C_M)}$ is a three-dimensional unimodular group, and consequently the full unimodular group. The full unimodular group over C is dense in G and $M/\overline{K(C_M)}$ is a GPVE.

If $e^n = 1$ but $e \neq -1$ then W' is periodic but not constant so M is not a PVE of K.

Proof of lemmas.

(1) If $z \in K$ then z can be written uniquely as a quotient of relatively prime polynomials with the numerator monic. z_1 is of the same form so $c = 1$ and $z \in C$. For $z \notin K$, (1) is a special case of (2).

(2) By the lemma preceding Theorem 12 there are $E, F \in C[x]$, $G \in C(x)$ and $j > 0$ with $(E\alpha_1 + F\alpha)_j = G(E\alpha_1 + F\alpha) \neq 0$. If $EF = 0$ then there is a relation of the form $\alpha_j = G\alpha$ for some $j > 0$. This is clearly impossible for $j = 1$. For $j > 1$ we will show by induction that if $\alpha_k = R\alpha_1 + S\alpha$ is the (necessarily unique) representation of α_k with $R, S \in K$ then $R, S \in C[x]$ and $dR > dS$. $\alpha_2 = A\alpha_1 + e\alpha$ and, if $\alpha_k = R\alpha_1 + S\alpha$ then $\alpha_{k+1} = (AR_1 + S_1)\alpha_1 + eR_1\alpha$.

If $EF \neq 0$ then E and F can be taken with $(E,F) = 1$. If $(E\alpha_1 + F\alpha)_k = E^{(k)}\alpha_1 + F^{(k)}\alpha$ then $E^{(k+1)} = AE_1^{(k)} + F_1^{(k)}$ and $F^{(k+1)} = eE_1^{(k)}$. If $(E^{(k)}, F^{(k)}) = 1$ then $(E_1^{(k)}, F_1^{(k)}) = 1$ so $(E^{(k+1)}, F^{(k+1)}) = 1$. Therefore $(E^{(j)}, F^{(j)}) = 1$ and since $E^{(j)}/F^{(j)} = E/F$, $dE = dE^{(j)}$. By the relations above $E^{(k+1)} = AE_1^{(k)} + eE_2^{(k-1)}$. Since $dE^{(k)} \geqq 0$, there is an n with $dE^{(n)} + dA > dE^{(n-1)}$. By induction $dE^{(n+k)} = dE^{(n)} + kdA$. Therefore there is an m with $dE^{(k)} > dE$ for $k > m$. However, $(E\alpha_1 + F\alpha)_{kj} = (GG_1 \cdots G_{k-1})(E\alpha_1 + F\alpha)$ and $dE^{(kj)} = dE$ for all k. This contradiction proves (2).

(3) If $z_1 - z = W/\alpha\alpha_1$ and $z = P/Q$ where $(P, Q) = 1$, $P, Q \in K(W)[\alpha, \alpha_1]$ then $(\alpha\alpha_1/QQ_1)(P_1Q - Q_1P) = W$. If $\alpha \mid Q$ set $Q = \alpha S$, $R = P$. If $\alpha \nmid Q$ set $R = \alpha P$, $S = Q$. Since $(\alpha SR_1 - \alpha_1 RS_1)/SS_1 = W$ and $(S, R) = 1$, $S \mid \alpha_1 S_1$ and $S_1 \mid \alpha S$. If $wS = \alpha_1 S_1$ and $vS_1 = \alpha S$ then $wv = \alpha\alpha_1$ and there are four possibilities each of which will be shown to lead to a contradiction.

(a) $w \in K(W)$. $wS = \alpha_1 S_1$ is not possible since a monomial of S of degree n transforms to a sum of monomials of degree n.

(b) $v \in K(W)$. $vS_1 = \alpha S$ is impossible as in (a).

(c) $w/\alpha \in K(W)$. Then there is a solution, $S\alpha$ in $K(W)[\alpha, \alpha_1] - K(W)$ to an equation $y_1 = ky$ for $k \in K(W)$. A common denominator shows that there is such a solution, z in $K[\alpha, \alpha_1, W] - K[W]$. If $z = \sum g^{(i)} W^i$ with $g^{(i)} \in K[\alpha, \alpha_1]$ then $g_1^{(i)}(-e)^i W^i = kg^{(i)} W^i$ and there is a solution $g \in K[\alpha, \alpha_1]$ to $y_1 = hy$ for some $h \in K(W)$. Since $h = g_1/g$, $h \in K$. Therefore by (2) $g \in C$. This contradicts $z \notin K[W]$.

(d) $w/\alpha_1 \in K(W)$. Then $S_1/S \in K(W)$ so as in (c) $S \in K(W)$. Setting $\alpha = \alpha_1 = 0$ in $(\alpha S R_1 - \alpha_1 RS)/SS_1 = W$ gives the contradiction $W = 0$.

BIBLIOGRAPHY

1. R. Cohn, *Difference algebra*, Interscience Tracts in Pure and Applied Mathematics, New York (in preparation).

2. I. Kaplansky, *An introduction to differential algebra*, Actualités. Sci. Ind. No. 1251 = Publ. Inst. Math. Univ. Nancago No. 5, Hermann, Paris, 1957.

3. E. Kolchin, *Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Bull. Amer. Math. Soc. **54** (1948), 927–932.

4. ———, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) **49** (1948), 1–42.

5. S. Lang. *Introduction to algebraic geometry*, Interscience Tracts in Pure and Applied Mathematics, New York, 1958.

BELL TELEPHONE LABORATORIES,
WHIPPANY, NEW JERSEY