ALGEBRAIC RELATIONS AMONG SOLUTIONS OF LINEAR DIFFERENTIAL EQUATIONS: FANO'S THEOREM

By Michael F. Singer*

1. Introduction. In [3] Fano considered special cases of the following statement:

(1) Let $L(y) = 0$ be an n^{th} order homogeneous linear differential equation with coefficients that are rational functions with complex coefficients. Let $y_1, \ldots, y_n$ be linearly independent solutions of (1) $L(y) = 0$ and assume that there is a nonzero homogeneous polynomial P with complex coefficients such that $P(y_1, \ldots, y_n) = 0$. Then all solutions of $L(y) = 0$ can be expressed as algebraic combinations of solutions of linear differential equations of order less than n.

Fano showed that (1) is true for $n \leq 5$ and gave partial results for $n \geq 6$. This evidence led several people (e.g. [2] p. 45–46 and the present author) to suspect that (1) was true for all n. In this paper, we shall reprove this statement for $n \leq 5$, prove that it remains true for $n = 6$ and show that it is false for all $n \geq 7$. In fact we shall show that, for all $n \geq 7$, there is an n^{th} order homogeneous linear differential equation $L(y) = 0$ having the property that a set of linearly independent solutions satisfies $y_1^2 + \cdots + y_n^2 = 0$ although the solutions of $L(y) = 0$ cannot be expressed in terms of solutions of lower order linear differential equations.

Fano used a combination of group theoretic and geometric techniques to determine the possible algebraic relations that solutions of a linear differential equation of order ≤ 5 could satisfy. Using the determined form of these relations, Fano proceeded with a case-by-case study to determine the effects such relations would have on these equations. He was able to explicitly describe, in these cases, how the solutions could be expressed in terms

Manuscript received 29 August 1986.
*Research supported by NSF Grant DMS-84-20075.
American Journal of Mathematics 110 (1988), 115–144.

of solutions of lower order equations. For $n \geq 6$, Fano showed that if one assumes that the polynomial relation is of a specific form or that there are enough relations, then the linear differential equation could be solved in terms of linear equations of lower order. We take a different approach. We first formalize the notion of solving a linear differential equation in terms of linear differential equations of lower order. We then derive necessary and sufficient conditions (in terms of the lie algebra of the galois group) for the solutions of a homogeneous linear differential equation to be expressed in terms of linear differential equations of lower order. This allows us to characterize those equations that are *not* solvable in terms of linear equations of lower order. We can then show that for $n \leq 6$, the homogeneous linear differential equations of order n that are not solvable in terms of linear differential equations of lower order have the property that any set of linearly independent solutions satisfy no nonzero homogeneous polynomial equation. Our characterization also allows us to construct the counterexamples mentioned above. This method of proving the theorem does not yield the explicit results of Fano, but does show the extent to which his theorem generalizes. Yet Fano's results are too pretty to be swept under the rug in this manner. We therefore have included one of Fano's more explicit results with the hope of enticing the reader to delve further into Fano's paper.

The rest of the paper is organized as follows. Section 2 contains the formalization of the notion of solvability in terms of lower order linear differential equations and the characterization of homogeneous linear differential equations that can be solved in terms of lower order linear differential equations. Section 3 contains the proof of (1) for $n \leq 6$, and the counterexamples for $n \geq 7$. In Section 4, we prove the following result of Fano: If $L(y) = 0$ has solutions $(y_1, \ldots, y_n)$ that lie on an algebraic curve in $\mathbf{P}^{n-1}$, then either all solutions of $L(y) = 0$ are liouvillian or can be expressed in terms solutions of a second order homogeneous linear differential equation. We have included an appendix containing an elementary proof of the fact (crucial to our considerations) that if K is a Picard-Vessiot extension of k with connected galois group G, then K is the function field of a principal homogeneous space for G.

2. Solving homogeneous linear differential equations in terms of linear equations of lower order. The results of this section are based on the galois theory of linear differential equations (see [11] or [12]). Let k be a differential field of characteristic 0 with derivation denoted by $'$. Assume that the subfield of constants $C = \{c \in k \mid c' = 0\}$ is algebraically closed. If $L(y) = 0$ is a homogeneous linear differential equation with coefficients in k, we may form a differential extension K of k where K is generated (as a differential field) by a fundamental set of solutions of $L(y) = 0$ (i.e. n solutions linearly independent over C) and where the constant subfield of K is C. Such an extension is unique up to differential isomorphism and is called a Picard-Vessiot extension of k associated with $L(y) = 0$. The group of differential automorphisms of K that leave each element of k fixed is a linear algebraic group $G(K/k)$ defined over C. If $y_1, \ldots, y_n$ is a fundamental set of solutions and $\sigma \in G(K/k)$, then $\sigma(y_i) = \Sigma\, c_{ij} Y_j$ for $i = 1, \ldots, n$ and some $c_{ij} \in C$. Identifying each such σ with the matrix (c_{ij}) gives a faithful representation of G into $GL(n, C)$.

Definition. Let k and K be as above. $L(y) = 0$ is said to be solvable in terms of linear differential equations of lower order if there exists a tower of fields $k = K_0 \subset \cdots \subset K_r$ such that:

1) the Picard-Vessiot extension K of k associated with $L(y) = 0$ lies in K_r.

2) For each $i = 1, \ldots, r$, either

a) K_i is a finite algebraic extension of K_{i-1}, or

b) K_i is a Picard-Vessiot extension of K_{i-1} associated with an equation $L_i(y) = 0$ with coefficients in K_{i-1} and of order less than n.

LEMMA 1. *Let $L(y) = 0$ and k be as above and assume that $n \geq 3$. $L(y) = 0$ is solvable in terms of linear differential equations of smaller order if and only if the Picard-Vessiot extension of k associated with $L(y) = 0$ lies in a tower of fields $k = F_0 \subset \cdots \subset F_s$ where each F_i is algebraic over F_{i-1} or each F_i is generated over F_{i-1} by a solution of a (not necessarily homogeneous) linear differential equation of order less than n with coefficients in F_{i-1}.*

Proof. Necessity is obvious. To prove sufficiency, we shall show, by induction, that each F_i lies in a tower of the type described in the above definition. Assume that F_{i-1} lies in $k = K_0 \subset \cdots \subset K_{r-1}$. If F_i is algebraic over F_{i-1}, let $K_r = K_{r-1}(F_i)$. Otherwise, assume that F_i is generated, over F_{i-1}, by a solution of $L(y_i) = b_i$. Let K_r be the Picard-Vessiot extension of K_r associated with $L_i(y) = 0$. Using variation of parameters we see that any solution of $L_i(y) = b_i$ lies in a differential extension of K_r generated by certain integrals $\int b_j$ of elements b_j in K_r. Each of these integrals satisfies a second order homogeneous equation $y'' - (b_j'/b_j)y' = 0$

over K_r. Since $n > 2$, we can form a tower of the desired type by successively forming Picard-Vessiot extensions associated with these equations. This tower will then contain F_i.

Remark. Lemma 1 implies that if $n > 2$ and if $L(y) = 0$ can be solved in terms of liouvillian functions (i.e. the associated Picard-Vessiot extension lies in a tower of differential field where each field in the tower is generated over the preceeding field by an algebraic element, an integral or an exponential of an element in the preceeding field), then $L(y) = 0$ can be solved in terms of lower order linear equations. Therefore, this notion generalizes the notion of solvability in terms of liouvillian functions when $n > 2$. This is not necessarily true when $n = 2$, since one can show that $y'' - 2xy' - 2y = 0$ has liouvillian solutions $\exp(x^2)$ and $\int(\exp(x^2))$ while $\int(\exp(x^2))$ cannot lie in a field generated by successively adjoining solutions of first order homogeneous linear differential equations (i.e. exponentials). Since we shall be mainly interested in equations of order larger than 2, this point will not concern us here.

The following theorem is the main result of this section. Given a linear differential equation $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0y = 0$ we can use the substitution $z = y\exp(-1/n \int a_{n-1})$ to form a new equation whose coefficient of $z^{(n-1)}$ is zero. This new equation is solvable in terms of lower order linear equations if and only if the original equation is. It is known ([11], p. 41) that this implies, using the representation described above, that $G(K/k) \subset SL(n, C)$. Finally, we denote the lie algebra of the galois group of K over k by $g(K/k)$. In general, an algebraic group will be referred to using capital letters and its lie algebra will be referred to using lower case letters (e.g. $sl(n, C)$ is the lie algebra of $SL(n, C)$).

THEOREM 1. *Let k be a differential field of characteristic zero with algebraically closed field of constants C. Let $L(y) = 0$ be a homogeneous linear differential equation of order n, $n \geq 3$ with coefficients in k and let K be the associated Picard-Vessiot extension. Assume that $G(K/k) \subset SL(n, C)$. $L(y) = 0$ can be solved in terms of linear differential equations of lower order if and only if one of the following holds*:

a) *$g(K/k) \subset sl(n, C)$ leaves a nontrivial subspace of C^n invariant.*

b) *$g(k/k)$ is semisimple but not simple.*

c) *$g(K/k)$ is simple and there exists a nonzero lie algebra homomorphism $\rho : g(K/k) \to gl(m, C)$ for some $m < n$.*

Furthermore, if a) *holds then there exist homogeneous linear differ-*

ential polynomials L_{n-i} *and* L_i *of orders* $n - i$ *and* i $(i > 0)$ *with coefficients in the algebraic closure* k^* *of* k *in* K *such that* $L(y) = L_{n-i}(L_i(y))$. *If* b) *or* c) *holds, then there exist linear homogeneous differential polynomials* $L_i(y)$, $1 \leq i \leq m$ *(with* $m = 1$ *if* c) *holds), each having order less than* n *and coefficients in an algebraic extension* k_0 *of* k *such that* K *lies in an algebraic extension of* $M_1 \cdot \ldots \cdot M_m$, *where* M_i *is the Picard-Vessiot extension of* k_0 *associated with* $L_i(y) = 0$.

COROLLARY. *Using the notation of Theorem* 1, $L(y) = 0$ cannot *be solved in terms of linear differential equations of lower order if and only if* $g(K/k)$ *is simple and has no nonzero representation of degree less than* n.

Proof of the Corollary. Any lie subalgebra of $sl(n,C)$ either leaves a nontrivial subspace of C^n invariant or is semisimple ([7], p. 102). Condition a) of Theorem 1 rules out the former and condition b) implies that $g(K/k)$ must be simple. Condition c) implies that $g(K/k)$ has no nonzero representation of degree less than n.

The proof of Theorem 1, depends on the following lemma. We shall use some facts about linear algebraic groups, for which the general references are [8] and [9]. If G is a connected linear algebraic group defined over an algebraically closed field C, we denote by $C[G]$ the coordinate ring of G and by $C(G)$ the function field of G. If k is a field containing C, we denote by $k(G)$ the field $C(G) \otimes_C k$. When necessary, we denote by G_C and G_k the C-valued and k-valued points of G. For any g in G_C, g acts on G_C by right multiplication $\rho_g(h) = hg$. This induces an automorphism ρ_g^* of $C[G]$ and therefore of $C(G)$ (similarly for $g \in G_k$, ρ_g^* is an automorphism of $k[G]$ and $k(G)$). If H is a normal subgroup of G defined over C (resp. over k) then the fixed field of $\{\rho_h^* \mid h \in H\}$ is $C(G/H)$ (resp. $k(G/H)$). Finally if k is a differential field of characteristic zero with algebraically closed field of constants and K is a Picard-Vessiot extension of K, we say that K is a $G(K/k)$—primitive extension of k ([12], p. 418) if there is an isomorphism $\phi : K \to k(G(K/k))$ such that, for any $\sigma \in G(K/k)$, and any $x \in K$, $\phi(\sigma(x)) = \rho_\sigma^*(\phi(x))$, i.e. the action of $G(K/k)$ on K is the same as the action of $G(K/k)_C$ on $k(G(K/k))$.

LEMMA 2. *Let* k *be a field of characteristic* 0 *with algebraically closed subfield of constants. Let* K *be a Picard-Vessiot extension of* k. *Assume that the galois group* $G(K/k)$ *of* K *is a connected simple algebraic group and let* V *be a finite dimensional* C*-space. For any irreducible faith-*

ful, representation $\Psi^* : g(K/k) \to gl(V)$, there exists a Picard-Vessiot extension M of k_0, a finite algebraic extension of k, associated with a linear differential equation $L^*(y) = 0$ such that:

a) $g(M/k_0) \simeq g(K/k)$

b) *If V^* is the C-space of solutions of $L^*(y) = 0$ in M, then the action of $G(M/k_0)$ on V^* induces a representation $\Gamma^* : g(M/k_0) \to gl(V^*)$ that is isomorphic to Ψ^*. In particular, the order of L^* equals the dimension of V^*.*

c) *K lies in an algebraic extension of M.*

Furthermore, if K is a $G(K/k)$-primitive extension of k, then we may choose k_0 to be k. In particular, this is the case if k is an algebraic extension of $C(x)$, $x' = 1$.

Proof. Since $G(K/k)$ is a connected simple algebraic group, its lie algebra $G(K/k)$ is simple. Therefore, there exists a simply connected algebraic group G with lie algebra isomorphic to $g(K/k)$ ([9], p. 260). Furthermore, $G(K/k)$ is isomorphic to G/H, where H is a normal algebraic subgroup of G. Since G and G/H have the same lie algebra, H must be finite. Since G is connected, H must be central and therefore abelian.

It is known ([12], p. 430 or see the Corollary to Theorem 5 in the appendix for an elementary proof of this fact) that there exists a finite normal algebraic extension k_0 of k such that:

i) $k_0 \otimes_k K$ is a Picard-Vessiot extension of k_0 with galois group isomorphic to $G(K/k)$

ii) $k_0 \otimes_k K$ is a $G(k_0 \otimes_k K/k_0)$-primitive extension of k_0.

Note that if K is already a $G(K/k)$-primitive extension then we may let $k_0 = k$. That this is always the case when k is an algebraic extension of $C(x)$, $x' = 1$, is explained in the appendix.

Therefore, we may write $k_0 \otimes_k K = k_0(G/H)$. There is a canonical embedding of $k_0(G/H)$ into $k_0(G)$ induced by the projection $\pi : G \to G/H$. Therefore we may identify $k_0 \otimes_k K \simeq k_0(G/H)$ with a subfield of $k_0(G)$. Since H is a finite normal subgroup of G, $k_0(G)$ is a finite algebraic extension of $k_0(G/H)$. This implies that the derivation on $k_0(G/H)$ extends uniquely to a derivation on $k_0(G)$, which we continue to write as $'$. Note that the field of constant remains unchanged since any constant of $k_0(G)$ is algebraic over C and therefore in C.

We now claim that for any $g \in G_C$ and any $z \in k_0(G)$, we have

$(\rho_g^*(z))' = \rho_g^*(z')$, that is, for each $g \in G_C$, ρ_g^* acts as a differential automorphism of $k_0(G)$. To see this, first note that C (and therefore $k_0(G/H)$) contains all roots of unity. Furthermore, $k_0(G)$ is an algebraic extension of $k_0(G/H)$ with abelian galois group H. Therefore $k_0(G) \simeq k_0(G/H)(z_1, \ldots, z_r)$ for some $z_i \in k_0(G)$ where for each i there is a non-zero integer n_i such that $z_i^{n_i} \in k_0(G/H)$. Since $(\rho_g^*(z))' = \rho_g^*(z)'$ for all $z \in k_0(G/H)$ and all $g \in G_C$, we have, for each i:

$$n_i \rho_g^*(z_i^{n_i-1})\rho_g^*(z_i') = \rho_g^*((z_i^{n_i})') = (\rho_g^*(z_i^{n_i}))' = n_i \rho_g^*(z_i)^{n_i-1}(\rho_g^*(z_i))'.$$

Therefore, $\rho_g^*(z_i') = (\rho_g^*(z_i))'$. This proves the claim.

We now claim that $k_0(G)$ contains a field M, satisfying conclusion b) of Lemma 2, such that $k_0(G)$ is an algebraic extension of M (which implies that c) is also satisfied). To verify this we proceed as follows. Since G_C is simply connected, any representation of its lie algebra induces a representation of the group itself. Let $\Psi : G_C \to GL(V)$ be the irreducible representation induced by Ψ^*. It is known ([4], p. 65), that $C[G_C] \subset k_0(G)$ contains a vector space V^* such that the representation $\Gamma : G_C \to GL(V^*)$ induced by the action ρ^* of G_C on $C[G_C]$ is isomorphic to Ψ. Γ induces a representation $\Gamma^* : g(K/k) \to gl(V^*)$ isomorphic to Ψ^* (note that the lie algebra of G_C is isomorphic to $g(K/k)$). Let $y_1, \ldots, y_m$ be a C-basis of V^* and let

$$L^*(y) = \frac{Wr(y, y_1, \ldots, y_m)}{Wr(y_1, \ldots, y_m)}$$

where Wr denotes the wronskian determinant. Let $M = k_0\langle y_1, \ldots, y_m\rangle$ (= the differential field generated by $y_1, \ldots, y_m$ over k_0). G_C leaves the coefficients of $L^*(y)$ fixed. Since G_C is dense in G_{k_0}, these coefficients lie in k_0. Therefore M is a Picard-Vessiot extension of k_0. Furthermore, if $g \in G_C$ leaves all the elements of M fixed, it must lie in the kernel of Γ and vice versa. Since this kernel is finite, the set of all $g \in G$ such that g leaves each element of M fixed is a finite normal subgroup N of G. Therefore M is isomorphic to $k_0(G/N)$ and $k_0(G)$ is a finite algebraic extension of M.

Finally, we show that $(G/N)_C$ is the galois group of M and so $g(M/k_0)$ is isomorphic to $g(K/k)$. Since N is a finite normal subgroup of G, it is abelian and therefore diagonalizable. In particular this implies that N is defined over C and so G/N is defined over C. The only elements of $k_0(G/$

N) left fixed by all of G/N are the elements of k_0. $(G/N)_C$ is dense in G/N and acts as a group of differential automorphisms of $k_0(G/N)$. Therefore $(G/N)_C$ is a subgroup of the galois group of M whose fixed field is k_0. The galois theory implies that $(G/N)_C$ must be the galois group.

Remarks.

1) In general, we do not know if k_0 may be replaced by k in the conclusion of Lemma 2.

2) The hypotheses that $G(K/k)$ is simple can be replaced by the assumption that $G(K/k)$ is connected and has a lie algebra with nilpotent radical. We only needed the original assumption to guarantee that there is a simply connected algebraic group with lie algebra $g(K/k)$ and the former assumption guarantees this as well ([9], p. 260).

Examples. The next two examples illustrate Lemma 2.

1) Let $k = \mathbf{C}(x)$, $\mathbf{C} =$ the complex numbers and $x' = 1$. Let $G = SL(2, \mathbf{C})$. There exists a Picard-Vessiot extension $M = k\langle y_1, y_2\rangle$ of k corresponding to a second order equation $L^*(y) = 0$, whose galois group is G ([22]). Consider the $\mathbf{C}$-vector space spanned by y_1^2, y_1y_2, y_2^2. This space is left invariant by the action of G. Therefore,

$$L(y) = \frac{Wr(y, y_1^2, y_1y_2, y_2^2)}{Wr(y_1^2, y_1y_2, y_2^2)}$$

has coefficients in k. Let $K = k\langle y_1^2, y_1y_2, y_2^2\rangle$. This is a Picard-Vessiot extension of k corresponding to $L(y) = 0$. Note that $[M : F] = 2$ and that $G(K/k) = G/H$ where $H = \{\pm 1\}$. Note that $G(K/k) \simeq PSL(2, \mathbf{C})$ and that this latter group has no nontrivial representation of degree smaller than 3. Of course, $g(K/k) = g(M/k) \simeq sl(2, \mathbf{C})$. The action of $g(K/k)$ on the solution space V of $L(y) = 0$ corresponds to the irreducible representation of degree 3 of $sl(2, \mathbf{C})$ and the action of $g(M/k)$ on V^* corresponds to the irreducible representation of $sl(2, \mathbf{C})$ of degree 2. This example shows that the question of solvability in terms of lower order equations depends on the representations of the lie algebra of the galois group rather than on the representations of the galois group itself. This example might lead one to suspect that the M guaranteed by Lemma 2 can always be chosen to be an algebraic extension of K. The next example shows that this is not always the case.

2) Let $G = SPIN(7, \mathbf{C})$. The smallest faithful representation of G

occurs in $GL(8, \mathbf{C})$. The results of [22] again show that there is a Picard-Vessiot extension K of k corresponding to an eighth order equation $L(y) = 0$ such that the action of G on the solution space V of $L(y) = 0$ corresponds to this representation. On the other hand, $G/\{\pm 1\} \simeq SO(7, \mathbf{C})$ and this latter group obviously has an irreducible representation of degree seven.

Let $\Psi^* : so(7, \mathbf{C}) \to gl(7, \mathbf{C})$ correspond to this representation. Let $H = \{\pm 1\} \subset G$ and let $M =$ the fixed field of H in K. As in the proof of Lemma 2, one can show that M is the Picard-Vessiot extension of k corresponding to a seventh order equation $L^*(y) = 0$ and that $[K : M] = 2$.

Proof of Theorem 1. We start by proving sufficiency. Let G^0 be the connected component of the identity of $G(K/k)$ and let V be the solution space of $L(y) = 0$ in K. First assume that a) holds. Since $g(K/k)$ leaves a nonzero proper subspace W of V invariant, G^0 leaves W invariant ([8], p. 88). If $y_1, \ldots, y_i$ is a basis for W, the coefficients of

$$L_i(y) = \frac{Wr(y, y_1, \ldots, y_i)}{Wr(y_1, \ldots, y_i)}$$

are left fixed by the action of G^0 and therefore in k^*. If we formally divide $L_i(y)$ into $L(y)$ (in the noncommutative ring of linear differential operators over k^*) we may write $L(y) = L_{n-i}(L_i(y)) + R(y)$ where R is a linear operator of order less than i and L_{n-i} is a linear operator of order $n - i$. Since $R(y_j) = 0$ for $j = 1, \ldots, i$, we must have $R(y) \equiv 0$. To see that $L(y) = 0$ is solvable in terms of linear equations of lower order, note that K lies in the tower gotten by first forming the Picard-Vessiot extension K_1 of k^* corresponding to $L_i(y) = 0$, then the Picard-Vessiot extension K_2 of K_1 corresponding to $L_{n-i}(y) = 0$ and then forming the Picard-Vessiot extensions of K_2 corresponding to certain second order homogeneous linear differential equations whose solutions are the integrals needed to solve $L(y) = 0$ using variation of parameters.

Now assume that a) does not hold but that b) holds. Write $g(K/k) = g_1 \oplus \cdots \oplus g_m$ where each g_i is a simple ideal and $m \geq 2$. In this case $g(K/k)$ acts irreducibly on V and we can conclude that $V \simeq V_1 \otimes \cdots \otimes V_m$ where each V_i is an irreducible g_i module ([16], p. 109). In particular each g_i has an irreducible representation $\Psi_i^{*'} : g_i \to gl(V_i)$ of degree less than n. We can write $G^0 = G_i \cdot \ldots \cdot G_m$ where each G_i is a minimal normal simple algebraic subgroup of G ([8], p. 167). Let $H_i = G_1 \cdot \ldots$

$\cdot \hat{G}_i \cdot \ldots G_m$. H_i is a normal subgroup of G and G/H_i has lie algebra isomorphic to g_i. Let K_i be the fixed field of H_i. Since $g(K_i/k^*) \simeq g_i$ we can apply Lemma 2 to conclude that the exist algebraic extensions k_i of k and Picard-Vessiot extensions M_i of k_i corresponding to linear equations of order less than n such that each K_i lies in an algebraic extension of M_i. Therefore, $K^* = K_1 \cdot \ldots \cdot K_m$ lies in an algebraic extension of $M_1 \cdot \ldots \cdot M_m$. If $\sigma \in G(K/k)$ leaves all the elements of K^* fixed, then $\sigma \in H_i$ for $i = 1, \ldots, m$. Since the intersection of the H_i is finite, $G(K/K^*)$ is finite and so K is an algebraic extension of K^*. Therefore, K lies in an algebraic extension of $M_i \cdot \ldots \cdot M_m$. This shows that $L(y) = 0$ is solvable in terms of lower order equations. If case c) holds, then we can let $m = 1$ in the above argument and the conclusions follow.

We now deal with necessity. First note that for a lie algebra $g \subset sl(n)$, either g leaves a proper nonzero subspace invariant or g is semisimple ([7], p. 102). Cases a) or b) will automatically hold unless $g(K/k)$ is simple. Therefore, we can assume $g(K/k)$ is simple and by replacing k by its algebraic closure in K, we can assume that $G(K/k)$ is connected. Now assume that $L(y) = 0$ is solvable in terms of equations of lower order. This implies that there is a tower $k = K_0 \subset K_1 \subset \cdots \subset K_r$ such that either $G(K_i/K_{i-1})$ is finite or has a faithful representation of degree less than n. We proceed by induction on r. The galois theory implies that $G(K_1K/K_1) \simeq G(K/K \cap K_1)$ which is a normal subgroup of $G(K/k)$ (see Figure 1). Since this latter group is simple, we are confronted with two cases:

$$
\begin{tikzcd}
 & & K_r = F_{r-1} \arrow[d, dash] \\
 & & \vdots \arrow[d, dash] \\
 & K_1K \arrow[uur, dash] & K_2 = F_1 \\
K \arrow[ur, dash] & & K_1 = F_0 \arrow[u, dash] \arrow[ull, dash, start anchor=north west, end anchor=south east, phantom] \\
 & K \cap K_1 \arrow[ul, dash] \arrow[ur, dash] & \\
 & k \arrow[u, dash] &
\end{tikzcd}
$$

Figure 1

i) $G(K/K \cap K_1) = G(K/k)$, or
ii) $G(K/K \cap K_1)$ is finite.

In the first case, since K_1K is the Picard-Vessiot extension of $F_0 = K_1$ associated with $L(y) = 0$ and lies in a tower of smaller height, $g(K_1K/K_1) \simeq g(K/k)$ satisfies c) by induction. If ii) holds then $G(K \cap K_1/k) \simeq G(K/k)/G(K/K \cap K_1)$ so $g(K \cap K_1/k) \simeq g(K/k)$. We therefore have that $K \cap K_1 \subset K_1$ are Picard-Vessiot extensions of k, $g(K \cap K_1/k)$ is simple and $g(K_1/k)$ has a faithful representation of degree less than n. The galois theory implies that $G(K \cap K_1/k) \simeq G(K_1/k)/G(K_1/K \cap K_1)$. Therefore we have a surjective homomorphism $\pi : g(K_1/k) \to g(K \cap K_1/k)$. Since this latter lie algebra is simple, there exists a homomorphism $\lambda : g(K \cap K_1/k) \to g(K_1/k)$ such that $\pi \cdot \lambda$ is the identity on $g(K \cap K_1/k)$ ([9], p. 101). Composing λ with the representation of $g(K_1/k)$ gives a faithful representation of $g(K \cap K_1/k)$ of degree smaller than n. Therefore, c) is satisfied.

In light of Theorem 1, one could ask: Is there a procedure to decide if an n^{th} order homogeneous linear differential equation with coefficients in $Q(x)$, Q the rational numbers, can be solved in terms of linear differential equations of lower order. We have given a procedure when $n = 3$ ([20]) and have also given a procedure to decide if such an equation can be solved in terms of liouvillian functions ([19]). The general problem remains open.

3. Fano's Theorem.

THEOREM 2. *Let k be a differential field of characteristic zero with algebraically closed field of constants C. Let $L(y) = 0$ be a homogeneous linear differential equation of order n, $n \leq 6$, with coefficients in k and K the associated Picard-Vessiot extension of k. If $P(x_1, \ldots, x_n)$ is a homogeneous nonzero polynomial with coefficients in C and $P(y_1, \ldots, y_n) = 0$ for some fundamental set of solutions $y_1, \ldots, y_n$ of $L(y) = 0$ in K, then $L(y) = 0$ is solvable in terms of lower order linear differential equations.*

Proof. First note that for $n = 1$ or 2 this theorem is trivial since $P(y_1) = 0$ implies $y_1 = 0$ and $P(y_1, y_2) = 0$ implies $y_1 = cy_2$ for some $c \in C$, $c \neq 0$. Therefore we may assume that $n \geq 3$. Also note that if $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0y = 0$ has a fundamental set of solutions $y_1, \ldots, y_n$ such that $P(y_1, \ldots, y_n) = 0$ then, if $z_i = y_i \exp(-1/n \int a_{n-1})$, we have $P(z_1, \ldots, z_n) = 0$. Therefore we may also assume that $a_{n-1} = 0$ and that $G(K/k) \subset SL(n, C)$. We now prove the contrapositive of the Theorem 2.

We consider $G(K/k)$ as acting on the projective space $\mathbf{P}(V)$ where V is the solution space of $L(y) = 0$ in K. If there exists a nonzero homogeneous polynomial P such that $P(y_1, \ldots, y_n) = 0$ for some fundamental set of solutions of $L(y) = 0$, then $G(K/k)$ leaves a proper algebraic subset of $\mathbf{P}(V)$ invariant. We shall show that if $L(y) = 0$ cannot be solved in terms of linear equations of lower order and $3 \leq n \leq 6$ then $G(K/k)$ acts transitively on $\mathbf{P}(V)$ and so no such P exists.

The Corollary to Theorem 1 states that $g(K/k)$ is a simple lie algebra that has no nontrivial representation of lower degree. Therefore we must examine those simple lie algebras g whose lowest dimensional nontrivial representation is of dimension n for $3 \leq n \leq 6$. We use the standard notation $A_n(n \geq 1)$, $B_n(n \geq 2)$, $C_n(n \geq 3)$, $D_n(n \geq 4)$, for the infinite families of simple lie algebras and refer to [7] for standard facts about their representations. We also use the fact that $SL(n, C)$ and $SP(n, C)$ act transitively on $\mathbf{P}(C^n)$ ([10], p. 360 and p. 374).

$n = 3$: $g = A_2$ and the representation of $A_2 = sl(3, C)$ is the canonical one as 3×3 matrices. The component G^0 of the identity in $G(K/k)$ must then be the group $SL(3, C)$.

$n = 4$: $g = A_3$ or B_2 ($\simeq C_2$). G^0 is either $SL(4, C)$ or $SP(4, C)$.

$n = 5$: $g = A_4$ and G^0 is $SL(4, C)$.

$n = 6$: $g = A_5$ or C_3. G^0 is either $SL(6, C)$ or $SP(6, C)$.

For $3 \leq n \leq 6$, any $L(y) = 0$ that is not solvable in terms of linear equations of lower order will have one of these groups as the connected component of the identity of its galois group. These groups leave no proper subvariety of $\mathbf{P}(C^n)$ invariant. Therefore, no fundamental set of solutions will satisfy a nonzero homogeneous polynomial equation.

We now show that, when $n \geq 7$ and $k = \mathbf{C}(x)$, $x' = 1$, Theorem 2 is false.

THEOREM 3. *For all $n \geq 7$, there exists a homogeneous linear differential equation $L_n(y) = 0$ of order n with coefficients in $\mathbf{C}(x)$ such that:*

i) *there is a fundamental set of solutions of $L_n(y) = 0$ satisfying $y_1^2 + \cdots + y_n^2 = 0$, and*

ii) *$L_n(y) = 0$ is not solvable in terms of lower order linear equations.*

Proof. Consider the special orthogonal group $SO(n, \mathbf{C})$. The results of [22] imply that for each n, there exists a linear differential equation $L_n^*(y) = 0$ with coefficients in $\mathbf{C}(x)$ whose galois group is $SO(n, \mathbf{C})$. Let $z_1, \ldots, z_n$ be a fundamental set of solutions of $L_n^*(y) = 0$ in K, the associated Picard-Vessiot extension of k. For $i = 1, \ldots, n$, let $y_i = a_0 z_i + a_1 z_i' + a_2 z_i''$ where a_0, a_1, and a_2 are elements of $\mathbf{C}(x)$ to be determined. $y_1^2 + \cdots + y_n^2 = Q(a_0, a_1, a_2)$ where Q is a homogeneous quadratic polynomial in the a_i whose coefficients are polynomials in $y_1, \ldots, y_n, y_1', \ldots, y_n', y_1'', \ldots, y_n''$. An easy calculation shows that these coefficients are left invariant under the action on $SO(n, \mathbf{C})$ and so lie in $\mathbf{C}(x)$. Since $Q(a_0, a_1, a_2)$ is a homogeneous polynomial of degree 2 in three variables, there exist a_0, a_1, a_2 in $\mathbf{C}(x)$, not all zero, such that $Q(a_0, a_1, a_2) = 0$ ([5], p. 22).

We now claim that $y_1, \ldots, y_n$ form a fundamental system of solutions of a linear differential equation $L_n^*(y) = 0$ of order n with coefficients in $\mathbf{C}(x)$. First of all, $y_1, \ldots, y_n$ are linearly independent over $\mathbf{C}$. To see this, assume that $c_1 y_1 + \cdots + c_n y_n = 0$ for some constants c_i. Then $a_0(c_1 z_1 + \cdots + c_n z_n) + a_1(c_1 z_1 + \cdots + c_n z_n)' + a_2(c_1 z_1 + \cdots + c_n z_n)'' = 0$. Therefore, $L_n(y) = 0$ and $a_2 y'' + a_1 y' + a_0 y = 0$ have a common solution. The space of all such common solutions is a proper subspace of the solution space of $L_n(y) = 0$ that is invariant under $SO(n, \mathbf{C})$ and therefore must be (0). This implies that $c_1 z_1 + \cdots + c_n z_n = 0$ so each $c_i = 0$. From the form of the y_i we see that the $\mathbf{C}$-space spanned by them is invariant under the action of $SO(n, \mathbf{C})$, so the coefficients of

$$L_n(y) = \frac{Wr(y, y_1, \ldots, y_n)}{Wr(y_1, \ldots, y_n)}$$

are left invariant under $SO(n, \mathbf{C})$ and so must lie in $\mathbf{C}(x)$. Clearly, $\mathbf{C}(x)\langle y_1, \ldots, y_n\rangle \subset K$. To see the opposite inclusion, differentiate the relations $y_i = a_0 z_i + a_1 z_i' + a_2 z_i''$ n times to get

$$\begin{bmatrix} y_1^{(n-1)} & \cdots & y_n^{(n-1)} \\ \vdots & & \vdots \\ y_1 & \cdots & y_n \end{bmatrix} = \begin{bmatrix} b_{n1} & \cdots & b_{nn} \\ \vdots & & \vdots \\ b_{11} & \cdots & b_{1n} \end{bmatrix} \begin{bmatrix} z_1^{(n-1)} & \cdots & z_n^{(n-1)} \\ \vdots & & \vdots \\ z_1 & \cdots & z_n \end{bmatrix}$$

for some b_{ij} in $\mathbf{C}(x)$. Since the matrices $[y_j^{(i)}]$ and $[z_j^{(i)}]$ are invertible, the matrix $[b_{ij}]$ is invertible. Therefore each $z_i \in \mathbf{C}(x)\langle y_1, \ldots, y_n\rangle$. This furthermore implies that the galois group of $L_n(y) = 0$ is $SO(n, \mathbf{C})$. For $n \geq 7$, $so(n, \mathbf{C})$ is a simple lie algebra with no nontrivial representations of dimension less than n. Therefore $L_n(y) = 0$ is not solvable in terms of linear equations of smaller order.

Note that for $n \leq 6$, $so(n, \mathbf{C})$ either is not simple or has a nontrivial representation of degree $<n$. Therefore the equations $L_n(y) = 0$ constructed in the above proof are solvable in terms of equations of lower order when $n \leq 6$.

4. Linear differential equations whose solutions lie on curves. In this section we discuss some of Fano's results relating to the title. Using these we characterize those homogeneous linear differential equations of order 3 having a fundamental set of solutions satisfying a nonzero homogeneous polynomial equation.

Let k be a differential field of characteristic 0 with algebraically closed constant subfield C and let $L(y) = 0$ be a homogeneous linear differential equation with coefficients in k. We say that $L(y) = 0$ has a fundamental set of solutions lying on an algebraic curve if there exists a fundamental set of solutions $\{y_1, \ldots, y_n\}$ such that the zero set of $I = \{P \mid P$ is a homogeneous polynomial with coefficients in C and $P(y_1, \ldots, y_n) = 0\}$ in $\mathbf{P}^{n-1}(C)$ is a curve (i.e. a one dimensional projective variety). I generates a prime ideal so the zero set $\mathcal{C}$ of I is irreducible. All of this is equivalent to saying that $\operatorname{Proj}(C[y_1, \ldots, y_n]) = \mathcal{C}$ has dimension 1. The main result (Theorem 4) is that if $L(y) = 0$ has a fundamental set of solutions lying on an algebraic curve then either all solutions of $L(y) = 0$ can be expressed in terms of liouvillian functions or can be expressed in terms of solutions of a second order homogeneous linear differential equation.

Before we prove the theorem, we need some facts about symmetric powers of linear differential operators. Given homogeneous linear differential equations $L_1(y) = 0$ and $L_2(y) = 0$ with coefficients in k, there exists ([20], p. 671) a unique linear differential equation $L_3(y) = 0$ with coefficients in k such that:

(i) If y_i is a solution of $L_i(y) = 0$ $(i = 1, 2)$ then $y_1 y_2$ is a solution of $L_3(y) = 0$.

(ii) $L_3(y)$ has leading coefficient 1 and has the smallest order of all homogeneous linear differential equations satisfying (i).

$L_3(y)$ is called the symmetric product of $L_1(y)$ and $L_2(y)$ and is denoted by $L_1 \circledS L_2(y)$. Given a homogeneous linear differential equation $L(y) = 0$, we can inductively define $L^{\circledS m}(y)$ by $L^{\circledS 1}(y) = L(y)$

and $L^{\circledS m}(y) = L^{\circledS m-1}(y) \circledS L(y)$. If $L(y)$ has order n, then $L^{\circledS m}(y)$ has order at most

$$\binom{m+n-1}{n-1}.$$

If $n = 2$, then $L^{\circledS m}(y)$ has order precisely $m + 1$ ([20], p. 673). Lemma 4 characterizes those homogeneous linear differential equations that are symmetric powers of second order equations as those equations having a fundamental set of solutions lying on the rational normal curve $\mathcal{R}_{n-1}$ of degree n in $\mathbf{P}^{n-1}$. Recall that the rational normal curve $\mathcal{R}_n$ in $\mathbf{P}^n$ is the image of $\mathbf{P}^1$ under the map $\varphi(s, t) = (s^n, s^{n-1}t, \ldots, t^n)$ ([6], p. 315). Finally, recall some facts about the representation theory of $SL(2, C)$. $SL(2, C)$ acts as a group of linear substitutions on the polynomial ring $C[X, Y]$. If H_n is the space of homogeneous polynomials of degree n, then H_n is an irreducible $SL(2, C)$ module and, up to isomorphism, these are the only irreducible $SL(2, C)$ modules. We denote the representation of $SL(2, C)$ in $SL(H_n) \simeq SL(n+1, C)$ by ρ_n. In the following Z_n will denote the center of $SL(n, C)$, that is the finite group of constant matrices in $SL(n, C)$.

LEMMA 3. *Let $G \subset SL(n, C)$ be a group leaving the variety defined by*

$$y_i y_{i+2} - y_{i+1}^2 = 0 \qquad i = 1, \ldots, n-2 \tag{2}$$

invariant. Then $G \subset \rho_{n-1}(SL(2, C)) \cdot Z_n$.

Proof. Equations (2) define the rational normal curve $\mathcal{R}_{n-1}$ in $\mathbf{P}^{n-1}$. Let $\varphi: \mathbf{P}^1 \to \mathbf{P}^{n-1}$ be the regular birational map $\varphi(s, t) = (s^{n-1}, s^{n-2}t, \ldots, t^{n-1})$ mapping $\mathbf{P}'$ to $\mathcal{R}_{n-1}$. The automorphism group of $\mathbf{P}^1$ is $SL(2, C)/\{\pm 1\}$ and G acts as automorphisms of $\mathcal{R}_{n-1}$. Therefore, for any $\sigma \in G$, there exists a $\tau \in SL(2, C)$ such that $\sigma(s^{n-1}, s^{n-2}t, \ldots, t^{n-1}) = \zeta(s, t) \cdot \varphi(\tau(s, t)) = \zeta(s, t) \cdot \rho_{n-1}(s^{n-1}, s^{n-2}t, \ldots, t^{n-1})$ for all $(s, t) \in C^2 - \{(0, 0)\}$, where for each (s, t), $\zeta(s, t)$ is a constant matrix. Since ζ is a rational map from $\mathbf{P}^1$ to Z_n and $\mathbf{P}^1$ is connected, $\zeta(s, t)$ is constant on $\mathbf{P}^1$. Therefore, $\sigma = \rho_{n-1}(\tau) \cdot \zeta$ for some τ in $SL(2, C)$ and $\zeta \in Z_n$.

LEMMA 4. *Let k and $L(y)$ be as above. $L(y) = L_2^{\circledS n-1}(y)$ for some second order homogeneous linear differential polynomial $L_2(y)$ with* *coefficients in k if and only if there exists a fundamental set of solutions $\{y_1, \ldots, y_n\}$ of $L(y) = 0$ such that equations* (2) *hold.*

Proof. If $L(y) = L_2^{\circledS n-1}(y)$, let $\{u, v\}$ be a fundamental set of solutions of $L_2(y) = 0$. Then $y_i = u^{n-i}v^{i-1}$, $i = 1, \ldots, n$ is a basis for the solution space of $L(y) = 0$ and equations (2) hold. Now assume that (2) hold for some fundamental set $\{y_1, \ldots, y_n\}$ of solutions of $L(y) = 0$ and let K be the Picard-Vessiot extension of k corresponding to $L(y) = 0$. Let $u = y_1^{1/(n-1)}$ and $v = y_2/u^{n-2}$. Equations (2) imply that $y_i = u^{n-i}v^{i-1}$ for $i = 1, \ldots, n$. If K^* is a universal differential field extension of K and σ : $K\langle u, v\rangle \to K^*$ then $\sigma(u^{n-1}) = \zeta(au + bv)^{n-1}$ and $\sigma(v^{n-1}) = \zeta(cu + dv)^{n-1}$ for some a, b, c, d in the constant subfield C^* of K^* with $ad - bc = 1$ and some ζ with $\zeta^n = 1$. This follows from Lemma 3. Therefore any such σ acts linearly on the C^*-span of u and v. So σ leaves the coefficients of

$$L_2(y) = \frac{Wr(y, u, v)}{Wr(u, v)}$$

invariant. $L_2(y)$ therefore has coefficients in k and $L(y) = L_2^{\circledS n-1}(y)$.

THEOREM 4. *Let k be a differential field of characteristic zero with algebraically closed field of constants C and let $L(y) = 0$ be a homogeneous linear differential equation with coefficients in k. If $L(y) = 0$ has a fundamental set of solutions lying on an irreducible algebraic curve $\mathcal{C}$, then one of the following holds:*

a) *There exists a $v \in k$ such that if y is a solution of $L(y) = 0$, then $ye^{\int v}$ is algebraic over k.*

b) *There exist a second order homogeneous linear differential equation $L_2(y) = 0$ with coefficients in k such that $L(y) = L_2^{\circledS n-1}(y)$.*

c) *There exist v_1 and v_2 that are the two roots of a quadratic polynomial over k, and nonnegative integers $N > n$ and $i_1 < \cdots < i_n \leq N$ such that $\{w_1^{i_1}w_2^{N-i_1}, \ldots, w_1^{i_n}w_2^{N-i_n}\}$ forms a fundamental set of solutions of $L(y) = 0$, where $w_1 = \exp(\int v_1)$ and $w_2 = \exp(\int v_2)$.*

Before we give the proof, we will make some comments and give some examples.

First note that we can make a further deduction from conclusion c). $\{w_1, w_2\}$ is a fundamental set of solutions of the second order homogeneous linear differential equation

$$L_2(y) = y'' - \left(2a + \frac{b'}{2b}\right)y' - \left(3a^2 + b^2 + a' + \frac{ab'}{2b}\right)y = 0$$

where $a = (v_1 + v_2)/2$ and $b = [(v_1 + v_2)^2 - 4v_1v_2]/4$ are in k. Therefore $L_2^{\circledS N}(y) = L_{N-n}(L(y))$ for some homogeneous linear differential polynomial $L_{N-n}(y)$ with coefficients in k.

Secondly, conclusions b) and c) of the theorem are sufficient conditions as well. To see this assume that b) holds and let $\{v_1, v_2\}$ be a fundamental set of solutions of $L_2(y) = 0$. $\{y_1 = w_1^{n-1}, \ldots, y_n = w_2^{n-1}\}$ forms a fundamental set of solutions of $L(y) = 0$ and satisfies (2). Therefore, $L(y) = 0$ has a fundamental set of solutions lying on a rational normal curve. If c) holds, then $y_1 = v_1^N, \ldots, y_{N+1} = v_2^N$ lies on a rational normal curve $\mathcal{R}_N$ in $\mathbf{P}^N$. $\{y_{i_1}, \ldots, y_{i_n}\}$ form a fundamental set of solutions of $L(y) = 0$ that lie on a projection of $\mathcal{R}_N$.

Finally, conclusion a) is, in general, not sufficient. For example, let $k = C\langle t_1, \ldots, t_n\rangle$ where $t_1, \ldots, t_n$ are differentially algebraically independent. $\{t_1, \ldots, t_n\}$ form a fundamental set of solutions of some homogeneous linear differential equation $L(y) = 0$ with coefficients in k. If $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions of $L(y) = 0$, then $\{t_1, \ldots, t_n\} \subset C(y_1, \ldots, y_n)$ so $\text{tr.deg.}_C C(y_1, \ldots, y_n) = n$. Therefore, $y_1, \ldots, y_n$ could not lie on a curve defined over C. On the other hand, if $k = C(x)$, $x' = 1$, (or more generally, if $\text{tr.deg.}_C k = 1$) then a) is a sufficient condition. To see this, let $\{y_1, \ldots, y_n\}$ be a fundamental set of solutions of $L(y) = 0$ and assume that each y_i is algebraic over k. We then have that the $\text{tr.deg.}_C C(y_2/y_1, \ldots, y_n/y_1) \leq 1$. This transcendence degree cannot equal 0, otherwise each $y_i/y_1 \in C$ contradicting the fact that the y_i are linearly independent over C. This implies that $(y_2/y_1, \ldots, y_n/y_1)$ is the generic point of an affine curve, so $(y_1, \ldots, y_n)$ lies on an algebraic curve.

We shall now give examples to show that each of a), b) and c) can occur. Let $k = \mathbf{C}(x)$, $x' = 1$.

a) Let y_1, y_2, and y_3 be the three solutions of

$$y^3 - xy^2 + \frac{1}{x}y - x^6 = 0.$$

This equation is irreducible over $\mathbf{C}(x)$. Furthermore,

$$(y_1 + y_2 + y_3)^5 = (y_1y_2 + y_2y_3 + y_1y_3)(y_1y_2y_3) \tag{3}$$

since $x^5 = (1/x)x^6$. Therefore, (y_1, y_2, y_3) lies on the curve defined by (3). One can check that this is a nonsingular curve of degree $d = 5$ and so has genus $(d - 1)(d - 2)/2 = 6$. y_1, y_2, y_3 are linearly independent over $\mathbf{C}$. To see this assume that $ay_1 + by_2 + cy_3 = 0$ for some $a, b, c \in \mathbf{C}$, not all zero. The galois group of $\mathbf{C}(x)(y_1, y_2, y_3)$ over $\mathbf{C}(x)$ contains a 3-cycle, so $ay_2 + by_3 + cy_1 = ay_3 + by_1 + cy_2 = 0$. Since

$$-\begin{vmatrix} y_1 & y_2 & y_3 \\ y_2 & y_3 & y_1 \\ y_3 & y_1 & y_2 \end{vmatrix} = y_1^3 + y_2^3 + y_3^3 - 3y_1y_2y_3 = x^3 - 1 \neq 0$$

we get a contradiction. The $\mathbf{C}$-space spanned by y_1, y_2, y_3 is left invariant by the galois group so $\{y_1, y_2, y_3\}$ is a fundamental set of solutions for the third order linear differential equation

$$L(y) = \frac{Wr(y, y_1, y_2, y_3)}{Wr(y_1, y_2, y_3)}.$$

In this example $v = 0$.

b) Let $L_2(y) = y'' - xy$ and $L(y) = L_2^{\circledS 2}(y) = y''' - 4xy' - 2y$. Clearly, if $\{y_1, y_2\}$ is a fundamental set of solutions of $L_2(y) = 0$, then $\{y_1^2, y_1y_2, y_2^2\}$ is a fundamental set of solutions of $L(y) = 0$ with $(y_1y_2)^2 - y_1^2y_2^2 = 0$.

c) Let $v_1 = x^{1/2}$ and $v_2 = x^{-1/2}$. We then have that $w_1 = e^{\int x^{1/2}}$ and $w_2 = e^{\int -x^{1/2}}$. These satisfy a second order linear differential equation $L_2(y) = 0$ whose Picard-Vessiot extension is $K = \mathbf{C}(x)(x^{1/2}, y_1, y_2)$. The galois group of K over $\mathbf{C}(x, x^{1/2})$ is

$$\left\{ \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \middle| \, a \neq 0 \right\}$$

and the galois group of $\mathbf{C}(x, x^{1/2})$ over $\mathbf{C}(x)$ is the two element cyclic group. Using this one sees that $G(K/\mathbf{C}(x))$ leaves the space spanned by $z_1 = y_1^6$, $z_2 = y_1^5y_2$, $z_3 = y_1^3y_2^3$, $z_4 = y_1y_2^5$, $z_5 = y_2^6$ invariant. Therefore, $\{z_1, \ldots, z_5\}$ is a fundamental set of solutions of a fifth order homogeneous linear differential equation $L(y) = 0$. This fundamental set lies on a curve in $\mathbf{P}^4$

parameterized by $(s^6, s^5t, s^3t^3, st^5, t^6)$. This is a curve of degree 6 and so is not a rational normal curve. Therefore, $L(y)$ is not the symmetric power of a second order homogeneous linear differential equation.

Proof of Theorem 4. Let $\{y_1, \ldots, y_n\}$ be a fundamental set of solutions of $L(y) = 0$ that lie on the curve $\mathcal{C}$ in $\mathbf{P}^{n-1}$ and let K be the Picard-Vessiot extension of k corresponding to $L(y) = 0$. The galois group $G(K/k)$ acts on the C-span of $\{y_1, \ldots, y_n\}$ and therefore give a faithful representation ρ of $G(K/k)$ into $GL(n, C)$.

We shall first show how to reduce the problem to the case where $\rho(G(K/k)) \subset SL(n, C)$. If $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0y$, then letting $z_i = \exp(-1/n \int a_{n-1})y_i$, we see that $\{z_1, \ldots, z_n\}$ form a fundamental set of solutions of a new homogeneous linear differential equation $L^*(y) = y^{(n)} + b_{n-2}y^{(n-2)} + \cdots + b_0y$ with the $b_i \in k$. Furthermore if P is a homogeneous polynomial with coefficients in C, then $P(y_1, \ldots, y_n) = 0$ if and only if $P(z_1, \ldots, z_n) = 0$. Therefore, $(z_1, \ldots, z_n)$ lies on $\mathcal{C}$. If either a), b), or c) hold for $L^*(y)$ then the corresponding conclusion will hold for $L(y)$. Therefore, we shall assume that $\rho(G(K/k)) \subset SL(n, C)$.

We first deal with the case of genus$(\mathcal{C}) \geq 1$. If V is the C-span of $\{y_1, \ldots, y_n\}$, then $G(K/k)$ acts on $\mathbf{P}(V)$, giving a representation φ of $G(K/k)$ into $PGL(V)$ with finite kernel. We shall show that the image of φ is finite as well. $\varphi(G(K/k))$ acts as a group of automorphisms of $\mathcal{C}$. Since $\mathcal{C}$ spans $\mathbf{P}(V)$, this action is faithful. If genus$(\mathcal{C}) \geq 2$, the automorphism group of $\mathcal{C}$ is finite ([6], p. 348) so the image of φ is finite. If genus$(\mathcal{C}) = 1$, the automorphism group of $\mathcal{C}$ is a projective variety ([6], p. 321). The image of $G(K/k)$ in this group is closed and affine so it must be finite ([8], p. 45). Therefore, if genus$(\mathcal{C}) \geq 1$, $G(K/k)$ is finite, so all solutions of $L(y) = 0$ are algebraic.

If genus$(\mathcal{C}) = 0$, then the degree of $\mathcal{C} \geq n - 1$ ([6], p. 315). If the degree of $\mathcal{C} = n - 1$ then, after making a linear change of coordinates, we may assume that $\mathcal{C}$ is the rational normal curve $\mathcal{R}_{n-1}$. Lemma 4 allows us to conclude that b) holds.

Now assume that genus$(\mathcal{C}) = 0$ and $\mathcal{C}$ has degree $N > n - 1$. There exists a regular birational map $\eta : \mathbf{P}^1 \to \mathcal{C}$ given by $\eta(s, t) = (\eta_1(s, t), \ldots, \eta_n(s, t))$ where the η_i are homogeneous polynomials of degree N. η allows us to identify $\varphi(G(K/k))$ with a subgroup of $SL(2, C)/\{\pm 1\}$, the automorphism group of $\mathbf{P}^1$. Therefore there is a subgroup G of $SL(2, C)$ such that $G/\{\pm 1\} \simeq \varphi(G(K/k))$. As in the proof of Lemma 3, for any $\sigma \in G(K/k)$ there is a $\tau \in SL(2, C)$ and $\zeta \in C$, $\zeta^n = 1$, such that

$$\eta(\tau(s, t)) = \rho_N(\tau)(\eta(s, t)) = \zeta \cdot \sigma(\eta(s, t)) \tag{4}$$

for all $(s, t) \in \mathbf{P}^1$. This further implies that the space spanned by $\eta_1, \ldots, \eta_n$ in H_N, the space of homogeneous polynomials of degree N in s and t, is left invariant by G under the representation ρ_N of $SL(2, C)$ on H_N.

We claim that the only unipotent element of G is the identity. To see this, one easily checks that for $a \neq 0$,

$$\rho_N\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right)$$

has a unique nontrivial invariant subspace and that this subspace has dimension 1. Therefore

$$\rho_N\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right)$$

cannot leave a proper n dimensional subspace ($n > 1$) invariant. We can conclude that G consists of semisimple elements ([8], p. 99). The only such subgroups of $SL(2, C)$ are finite or have connected component of the identity, G^0, conjugate to the diagonal group

$$D = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \,\middle|\, a \neq 0\right\}.$$

If G is finite, then $G(K/k)$ is finite and so all solutions of $L(y) = 0$ are algebraic over k. We may therefore assume that G^0 is conjugate to D. In this case $[G : G^0] = 1$ or 2, since every element of G permutes the two one dimensional eigenspaces of D.

We identify V with a subspace of H_N. H_N is the sum of one dimensional $\rho_N(D)$ invariant subspaces V_i, where V_i is spanned by $s^i t^{N-i}$ and

$$\rho_N\left(\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\right)(s^i t^{N-i}) = a^{2i-N} s^i t^{N-i}. \tag{5}$$

Therefore, there is a basis of V of the form $z_1 = s^{i_1} t^{N-i_1}, \ldots, z_n =$

$s^{i_n}t^{N-i_n}$, $i_1 < \cdots < i_n$. Notice that for all s and t, the point $(z_1, \ldots, z_n)$ satisfies

$$z_1^{i_n-i_1}z_n^{i_k-i_1} = z_k^{i_n-i_1}z_1^{i_k-i_1} \qquad k = 2, \ldots, n-1 \tag{6}$$

These equations define a curve $\mathcal{C}^*$ and the automorphism of V taking y_i to z_i takes $\mathcal{C}$ to $\mathcal{C}^*$. Therefore we may assume that $L(y) = 0$ has a fundamental set of solutions $z_1, \ldots, z_n$ such that equations (6) hold.

Let w_1 and w_2 be elements of an algebraic extension of K such that

$$\begin{aligned} w_1^{i_1}w_2^{N-i_1} &= z_1 \\ w_1^{i_n}w_2^{N-i_n} &= z_n \end{aligned} \tag{7}$$

that is,

$$\begin{aligned} w_1^{N(i_1-i_n)} &= z_1^{N-i_n}z_n^{i_1-N} \\ w_2^{N(i_n-i_1)} &= z_1^{i_n}z_n^{-i_1} \end{aligned} \tag{8}$$

Equations (6) and (7) imply that $z_k = \zeta_k w_1^{i_k}w_2^{N-i_k}$, for some root of unity ζ_k and $k = 1, \ldots, n$. Therefore, $L(y) = 0$ has a fundamental set of solutions of the form $\{w_1^{i_1}w_2^{N-i_1}, \ldots, w_1^{i_n}w_2^{N-i_n}\}$. We now deal with the two cases $[G : G^0] = 1$ and $[G : G^0] = 2$.

If $G = G^0 = D$, then for any $\sigma \in G(K/k)$ (4) and (8) imply that

$$\begin{aligned} \sigma(w_1^{N(i_1-i_n)}) &= d_1 w_1^{N(i_1-i_n)} \\ \sigma(w_2^{N(i_n-i_1)}) &= d_2 w_2^{N(i_n-i_1)} \end{aligned} \tag{9}$$

for some $d_1, d_2 \in C$. Therefore, $w_1'/w_1 = v_1$ and $w_2'/w_2 = v_2$ are left fixed by $G(K/k)$ and so lie in k. $\{w_1, w_2\}$ is a fundamental set of solutions of a second order homogeneous linear differential equation with coefficients in k and satisfy c).

If $[G : G^0] = 2$, we may assume that G is generated by D and

$$\tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

so any element of G is of the form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix}.$$

$$\rho_N\left(\begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix}\right)$$

maps V_i to V_{N-i}. Since this element leaves $V = V_{i_1} \oplus \cdots \oplus V_{i_n}$ invariant, we must have $i_1 = N - i_n$. Therefore,

$$\rho_N\left(\begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix}\right)(z_1) = c_1 z_n$$

(10)

$$\rho_N\left(\begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix}\right)(z_n) = c_2 z_1$$

for some $c_1, c_2 \in C$. This implies that for any $\sigma \in G(K/k)$, either (9) holds or we have

$$\sigma(w_1^{N(i_1 - i_n)}) = d_1 z_n^{N-i_n} z_1^{i_1 - N}$$

(11)

$$\sigma(w_2^{N(i_n - i_1)}) = d_2 z_n^{i_n} z_1^{-i_1}$$

(9), (11) and $i_1 = N - i_n$ imply that

(12) $$\frac{w_1'}{w_1} + \frac{w_2'}{w_2} \quad \text{and} \quad \frac{w_1'}{w_1} \cdot \frac{w_2'}{w_2}$$

are left fixed by all elements of $G(K/k)$. Therefore, $w_1'/w_1 = v_1$ and $w_2'/w_2 = v_2$ are conjugate roots of some quadratic equation over k, and $\{w_1, w_2\}$ satisfies c).

The following is an immediate consequence of Theorem 4.

COROLLARY. *Let k be as above and let $L(y) = 0$ be a third order homogeneous linear equation with coefficients in k. If there exists a non-*

zero homogeneous polynomial P with constant coefficients and a fundamental set of solutions $\{y_1, y_2, y_3\}$ of $L(y) = 0$ such that $P(y_1, y_2, y_3) = 0$, then either all solutions of $L(y) = 0$ are liouvillian over k or $L(y)$ is the second symmetric power of a second order homogeneous linear differential equation with coefficients in k.

Theorem 4 and this corollary appear in ([3], p. 495 and p. 579–580), although Fano only states them when $k = \mathbf{C}(x)$ and omits many details. His statement of conclusion c) of Theorem 4 (op. cit., bottom of p. 580) is particularly vague. A similar result appears in ([17], p. 226] with a proof based on the theory of differential invariants. Fano also considers the situation when a fundamental set of solutions of $L(y) = 0$ lies on an algebraic surface or on a 3-fold, as well as classifying those n^{th} order homogeneous linear differential equations ($n \leq 5$) having a fundamental set of solutions satisfying some homogeneous polynomial equation.

Appendix. We shall explain the connection between Picard-Vessiot extensions with galois group G and principal homogeneous G-spaces. This connection is well known and has been described in the more general situation of strongly normal extensions and principal homogeneous spaces for arbitrary algebraic groups by Kolchin and Lang [13], Biaynicki-Birula [1], and Kolchin [12]. The two former presentations rely heavily on criteria of Weil for a variety to be birationally equivalent to either an algebraic group or a principal homogeneous space. The latter makes the connection in a more natural way but at the expense of having to develop the theory of algebraic groups and homogeneous spaces in a way that is far from the standard approaches. Our aim here is to rely only on the most elementary aspects of the galois theory of linear differential equations (as presented in [11]) and the standard presentation of the theory of linear algebraic groups (e.g. [8]) to give an elementary exposition of the relationship between Picard-Vessiot extensions and principal homogeneous spaces. Part of our proof has already appeared in [21]. We will need the following special case of a theorem of Rosenlicht [15]:

LEMMA 5. *Let $k \subset K$ be differential fields of characteristic 0 with the same field of constants and assume that $K = k(x_1, \ldots, x_n)$ where $x_i'/x_i \in k$ for $i = 1, \ldots, n$. If $y \in K$ and $y'/y \in k$, then there exists a $d \in k$ and integers n_i such that $y = d \prod x_i^{n_i}$.*

Proof. We first show that if $z_1, \ldots, z_m$ are nonzero elements of K with $z_i'/z_i \in k$ and $z_i/z_k \notin k$ for $i \neq j$, then $\Sigma z_i \neq 0$. Assume that this is not true and let N be the smallest integer for which there are such elements with $z_1 + \cdots + z_N = 0$. We then have $z_1' + \cdots + z_N' = 0$ so

$$\sum_{i=2}^{N} \left(\frac{z_i'}{z_i} - \frac{z_1'}{z_1}\right) z_i = 0.$$

Therefore, we have a smaller counterexample unless

$$\frac{z_i'}{z_i} - \frac{z_1'}{z_1} = 0,$$

for $i = 2, \ldots, N$. This would imply

$$\left(\frac{z_i}{z_1}\right)' = 0 \quad \text{or} \quad \frac{z_i}{z_1} \in k,$$

a contradiction.

Now let $y \in K$ satisfy $y'/y \in k$. We may choose a k-basis $\{u_i\}$ of $k[x_1, \ldots, x_n]$ over k in such a way that each u_i is a monomial in $x_1, \ldots, x_n$. We may then write

$$y = \frac{\sum a_i u_i}{\sum b_j u_j}$$

with $a_i, b_j \in k$, so $\sum a_i y u_i - \sum b_j u_j = 0$. Note that for $i \neq j$, $a_i y u_i / a_j y u_j = a_i u_i / a_j u_j \notin k$ since the u_i are linearly independent over k. Similarly, $b_i u_i / b_j u_j \notin k$. Therefore, for some i and j, we must have $a_i y u_i / b_j u_j \in k$ so $y = d \prod x_i^{n_i}$.

COROLLARY. *Let $k \subset K$ be differential fields of characteristic zero with the same field of constants. Let $E = \{y \in K \mid y'/y \in k\}$ and $k^\times$ be the nonzero elements of k. If k is finitely generated (as a field) over k, then $E/k^\times$ is a finitely generated abelian group.*

Proof. $k(E)$ is a subfield of K and so it is finitely generated over k. We may therefore write $k(E) = k(x_1, \ldots, x_n)$ for some $x_i \in E$. Lemma 5 implies that $E/k^\times$ is generated by $x_1, \ldots, x_n$.

Let C be an algebraically closed field of characteristic zero and let G

be a connected C-group, that is a group defined over C. If k is a field containing C, then $k[G] \simeq C[G] \otimes_C k$. G_C (resp. G_k) will denote the C-points (resp. k-points) of G. When no subscript is used we are referring to points in some large algebraically closed field U containing all fields under discussion. Let X be an affine variety defined over k. We say that X is a principal homogeneous G-space over k if there is a morphism, defined over k, $\varphi : X \times G \to X$, where $\varphi(x, g)$ is denoted by $x \cdot g$, such that:

a) $(x \cdot g) \cdot h = x \cdot (gh)$ for all $x \in X$ and $g, h \in G$
b) $x \cdot e = x$ for all $x \in X$
c) for all $x, y \in X$ there is a unique $g \in \gamma$ such that $x \cdot g = y$.

For example G itself is a principal homogeneous G-space over any k with $C \subset k$, where G acts on G by right multiplication. Note that φ induces a k-algebra homomorphism $\varphi^* : k[X] \to K[X] \otimes_k K[G]$ and that for any $g \in G_k$ we have an isomorphism $g^* : k[X] \to k[X]$ given by $g^*(f)(x) = f(x \cdot g)$. In this way G_k acts as a group of k-automorphisms of $k(X)$ such that the fixed field of G_k is k. Let K_1, K_2 be two fields containing k and k_1 a field with $C \subset k_1 \subset k$ (we shall only be concerned with the cases of $k_1 = C$ or $k_1 = k$). If G_{k_1} acts as a group of k-automorphisms of K_1 and K_2 we say that K_1 and K_2 are G_{k_1}-isomorphic if there is a k-isomorphism $\psi^* : K_1 \to K_2$ such that $g \cdot \psi^*(f) = \psi^*(g \cdot f)$ for all $f \in K_1$ and all $g \in G_{k_1}$. If X_1 and X_2 are two principal homogeneous G-spaces defined over k, we say that X_1 and X_2 are G_{k_1}-isomorphic if there is an isomorphism $\psi : X_1 \to X_2$, defined over k, such that $(\psi(x)) \cdot g = \psi(x \cdot g)$ for all $x \in X_1$ and $g \in G_{k_1}$. One can easily show that two principal homogeneous G-spaces are G_k-isomorphic if and only if $k(X_1)$ and $k(X_2)$ are G_k-isomorphic. If X is a principal homogeneous G-space over k and D is a derivation of $k(X)$, we say that D is a G_C-derivation if $D(g^*(f)) = g^*(D(f))$ for all $f \in k(X)$ and $g \in G_C$. The following is a special case of Theorem 9 in ([12], p. 430).

THEOREM 5. *Let k be a differential field of characteristic zero with algebraically closed field of constant C and let G be a connected C-group.*

a) *If K is a Picard-Vessiot extension of k with galois group G_C, then there exists a principal homogeneous G-space X, defined over k, such that K is G_C-isomorphic to $k(X)$. Furthermore, X is unique up to G_k-isomorphism.*

b) *Let X be a principal homogeneous G-space defined over k such that the derivation of k extends to a G_C-derivation of $k(X)$ without introducing any new constants. Then $k(X)$ is a Picard-Vessiot extension of k*

with galois group G_C where the galois action of G_C on $k(X)$ is that induced by the action of G_C on X.

Proof.

a) Write $K = k\langle y_1, \ldots, y_n\rangle = k(y_1, \ldots, y_n, \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$. Let $E = \{y \in K \mid y'/y \in k\}$. The above corollary implies that there exist $x_1, \ldots, x_n \in E$ that generate $E/k^\times$. Let $R = k[y_1, \ldots, y_n, \ldots, y_1^{(n-1)}, \ldots, y^{(n-1)}, x_1, \ldots, x_m, x_1^{-1} \cdots x_m^{-1}]$. R is a finitely generated integral k-algebra, so $R = k[X]$ for some variety X defined over k. Furthermore, $G(K/k)$ acts as a group of k-algebra isomorphisms of R (note that for any $\sigma \in G(K/k)$, $\sigma x_i = c_\sigma x_i$ for some $c_\sigma \in C$). Since $G(K/k) = G_C$, there exists a k-morphism $\varphi : X \times G \to X$ (denoted by $\psi(x, g) = x \cdot g$) such that $(x \cdot g) \cdot h = x \cdot (gh)$ and $x \cdot e = e$ for all $x \in X$ and $g, h \in G$.

We now need to show that for any $x, y \in X$, there is a unique $g \in G$ such that $x \cdot g = y$. If we can show that the Zariski closure (with respect to our large algebraically closed field U) of the orbit of any element x in X is all of X, then, since orbits of minimal dimension are closed, we will have shown the existence part of this statement. Since G is connected, the galois theory allows us to conclude that k is algebraically closed in K. Therefore, the variety X is irreducible in the (U-) Zariski topology. We shall show that the k-Zariski closure $cl_k(x \cdot G) = X$. The Zariski closure of $x \cdot G$ will be an irreducible component of $cl_k(x \cdot G)$. Since X is irreducible, we can then conclude that the Zariski closure of $x \cdot G = X$. To show that $cl_k(x \cdot G) = X$, we must show that the only G_k-invariant ideals of R are (0) and R. Let $I \neq (0)$ be a G invariant ideal of R. Since any f in R satisfies a homogeneous linear differential equation over k, the G_C orbit of f lies in a finite dimensional G_C-invariant subspace of R. Let $v_1, \ldots, v_r \in I$ be a basis of such a subspace. For any $\sigma \in G(K/k)$ and $w = Wr(v_1, \ldots, v_r)$, we have $\sigma(w) = c_\sigma w$ for some $c_\sigma \in C$. This implies that $w'/w \in k$ and $w \in E$. Therefore, w and $1/w$ are in R. We also have that $w \in I$, as can be seen by expanding $Wr(v_1, \ldots, v_r)$ by minors. Therefore $1 \in I$.

We shall now show uniqueness of the element g such that $x \cdot g = h$. To do this it is enough to show that for any $z \in X$ and $h \in G$, if $z \cdot h = z$ then $h = e$. Let $z = (z_{11}, z_{12}, \ldots, z_{nn}, \ldots)$ and let Z be the $n \times n$ matrix (z_{ij}). The action of G on z induces an action of G on Z, given by matrix multiplication. For $h \in G$ there is an $n \times n$ matrix H such that the first n^2 entries of $z \cdot h$ are gotten from the entries of $Z \cdot H$. Therefore, $Z = Z \cdot H$. Since $1/Wr(y_1, \ldots, y_n) \in R$, $\det Z \neq 0$. Therefore, H is the identity matrix. Since H determines the action of h on X, we have $h = e$. This completes the proof that X is a principal homogeneous G-space. If X^* is another principal homogeneous G-space satisfying a), then $k(X)$ and $k(X^*)$ are G_C isomorphic. Since G_C is dense in G_k, these two fields are G_k isomorphic. Therefore X and X^* are G_k isomorphic.

b) Let $k[X] = k[y_1, \ldots, y_n]$. We first show that each $y \in k[X]$ lies in a finite dimensional G_C-invariant C-space. For $y \in k[X]$, let $\varphi^*(y) = \Sigma\, u_i v_i$ where $u_i \in k[X]$ an $v_i \in k[G]$. Since $k[G] \simeq k \otimes_C C[G]$, we may assume that the $v_i \in C[G]$. Therefore, for any $x \in X$ and $g \in G_C$, we have $g^*(f)(x) = \Sigma\, u_i(x)v_i(g)$. Since $v_i(g) \in C$, we have that, for all $g \in G_C$, $g^*(f)$ lies in the C-span of the u_i. Therefore the space spanned by $\{g^*(f)\,|g \in G_C\}$ is finite dimensional and G_C-invariant.

We may therefore assume that $\{y_i, \ldots, y_n\}$ are linearly independent over C and span a G_C-invariant C-subspace V of $k[X]$. This implies that we have a representation of G_C into $GL(V)$ and, since X is a principal homogeneous space, this representation is faithful. Furthermore, each element of G_C leaves the coefficients of

$$L(y) = \frac{Wr(y, y_1, \ldots, y_n)}{Wr(y_1, \ldots, y_n)}$$

fixed. Since G_C is dense in G and the only G_k-invariant functions on V are the k, $L(y)$ has coefficients in k. Clearly K is a Picard-Vessiot extension of k corresponding to $L(y) = 0$ and $G_C \subset G(K/k)$. Since the fixed field of G_C is k, we have that $G_C = G(K/k)$.

In the above proof, we used the corollary of Lemma 5 to produce a finitely generated ring R, which turned out to be the coordinate ring of the principal homogeneous space. We could have avoided this corollary completely by letting R be the ring of all elements in K that satisfy homogeneous linear differential equations over k. The same proof shows that this ring has no G-invariant ideals other than R and (0). A result of Magid ([14]. Theorem 4.5) allows us to conclude that R is the coordinate ring of a G-homogeneous space. We then can show, as above, that this homogeneous space is principal.

For the next corollary, recall that a Picard-Vessiot extension K of k is said to be a $G(K/k)$ primitive extension of k if there is an isomorphism φ : $K \to k(G(K/k))$ such that, for any $\sigma \in G(K/k)$, and any $x \in K$, $\varphi(\sigma(x)) = \varphi_\sigma^*(\varphi(x))$, where ρ_σ is the action of σ on $G(K/k)$ by right multiplication. In light of Theorem 4, this is equivalent to saying that the principal homogeneous G-space associated to K as in part a) is just G itself with the action of G on G given by right multiplication.

COROLLARY. *Let k be a differential field of characteristic zero with algebraically closed fields of constants and let K be a Picard-Vessiot extension of k with connected galois group $G(K/k)$. There exists a finite algebraic extension k_0 of k such that:*

i) *$k_0 \otimes_k K$ is a Picard-Vessiot extension of k_0 with galois group isomorphic to $G(K/k)$.*

ii) *$k_0 \otimes_k K$ is a $G(k_0 \otimes_k K/k_0)$-primitive extension of k_0.*

Furthermore, if k has transcendence degree one over its field of constants, then we may choose $k_0 = k$.

Proof. Theorem 4a) implies that K is the function field of a principal homogeneous G-space X over k. X will have a point x rational over some finite algebraic extension k_0 of k. Therefore, X is k_0-isomorphic (via the map $g \to xg$) to the principal homogeneous G-space G. Since $G(K/k)$ is connected and the galois group of $k_0 \otimes_k K$ is isomorphic to a subgroup of $G(K/k)$ of finite index, we have that $G(k_0 \otimes_k K/k_0) \simeq G(K/k)$. This proves i) and ii).

If the transcendence degree of k over its field of constants is 1, then for any connected group G, $H^1(G, k) = 0$ ([18], II.10 and III.10–14). This implies that all principal homogeneous G-spaces are G-isomorphic over k to G and so K is already the function field of the homogeneous G-space G.

NORTH CAROLINA STATE UNIVERSITY

REFERENCES

[1] A. Bialynicki-Birula, On Galois theory of fields with operators, *American Journal of Math.*, **84** (1962), 89–109.

[2] D. V. Chudnovsky and G. V. Chudnovsky, The wronskian formalism for linear differential equations and Pade approximation, *Adv. in Math.*, **53** (1984), 28–54.

[3] G. Fano, Ueber Lineare homogene Differentialgleichungen mit algebraischen Rela-

tionen Zwischen den Fundamentalloesungen, *Math. Ann.*, **53** (1900), 493-590.

[4] J. Fogarty, *Invariant Theory*, W. A. Benjamin, New York, 1969.

[5] M. J. Greenberg, *Lectures on Forms in Many Variables*, W. A. Benjamin, New York, 1969.

[6] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[7] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1976.

[8] ______, *Linear Algebraic Groups*, Springer-Verlag, New York, 1981.

[9] G. Hochschild, *Basic Theory of Algebraic Groups and Lie Algebras*, Springer-Verlag, New York, 1981.

[10] N. Jacobson, *Basic Algebra I*, W. H. Freeman, San Francisco, 1974.

[11] I. Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris, 1957.

[12] E. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[13] ______ and S. Lang, Algebraic Groups and the Galois Theory of Differential Fields, *American Journal of Math.*, **80** (1958), 103-110.

[14] A. Magid, Equivariant completions of rings with reductive group actions, manuscript.

[15] M. Rosenlicht, Differential extension fields of exponential type, *Pac. J. of Math.*, **12** (1975), 289-230.

[16] H. Samelson, *Notes on Lie Algebras*, Van Nostrand Reinhold, New York, 1969.

[17] L. Schlesinger, *Handbuch der Theorie der Linearen Differentialgleichungen*, Zweiter Band, Johnson Reprint Corporation, New York, 1968.

[18] J.-P. Serre, *Cohomologie Galoisienne*, Springer-Verlag, New York, 1964.

[19] M. F. Singer, Liouvillian solutions of n^{th} order linear differential equations, *American Journal of Math.*, **103** (1981), 661-682.

[20] ______, Solving homogeneous linear differential equations in terms of second Order Linear Differential Equations, *American Journal of Math.*, **107** (1985), 663-696.

[21] ______, Algebraic relations among solutions of linear differential equations, *Trans. Am. Math. Soc.*, **295** (1986), 753-763.

[22] C. Tretkoff and M. Tretkoff, Solution of the inverse problem of differential Galois theory in the classical case, *American Journal of Math.*, **101** (1979), 1327-1332.