AN OUTLINE OF DIFFERENTIAL GALOIS THEORY

Michael F. Singer[1]
Department of Mathematics
Box 8205
North Carolina State University
Raleigh, N.C. 27695

In this paper, I will give an exposition of the differential galois theory of linear differential equations with the aim of trying to answer the following question:

> When can we effectively solve a linear differential equation in terms of some "simple" class of functions?

To make this question more concrete, let us look at some examples:

Example 0.1. The equation $y''' + (2/x)y'' - (1/4x^2)y' + (1/4x^3)y = 0$ has a solution space that is spanned by x, $\sqrt{x}$, $1/\sqrt{x}$. In general, one can ask: when does a linear differential equation with coefficients in $\mathbb{C}(x)$ have a solution space spanned by functions algebraic over $\mathbb{C}(x)$, ($\mathbb{C}$ is the complex numbers) ?

Example 0.2. The equation $y'' + (1/2x)y' - xy = 0$ has a solution

[1]Work on this paper was partially supported by NSF Grant DMS–8803109. The author would like to thank the Research Institute for Symbolic Computation (RISC–LINZ) for its hospitality and support during the preparation of this paper.

space spanned by $e^{\int\sqrt{x}}$ and $e^{-\int\sqrt{x}}$. Functions that are built up from $\mathbb{C}(x)$ using integration, exponentiation, algebraic functions and composition are called liouvillian functions. One can ask: when does a differential equation with coefficients in $\mathbb{C}(x)$ (or more generally, coefficients that are liouvillian functions) have a solution space that is spanned by liouvillian functions?

Example 0.3. The equation $y''' - 4xy' - 2y = 0$ has a solution space spanned by $y_1 = z_1^2$, $y_2 = z_1z_2$, $y_3 = z_2^2$, where z_1 and z_2 are linearly independent solutions of $y'' - xy = 0$. One can ask: when can the solutions of a linear differential equation be expressed in terms of solutions of second order linear differential equations? In, general when can the solutions of a linear differential equation be expressed in (possibly more complicated) terms of solutions of lower order linear differential equations? Note that in this example we have the relation $y_1y_3 - y_2^2 = 0$. In general, if linearly independent solutions of a linear differential equation satisfy some homogeneous polynomial equation, does this imply that all solutions of the linear differential equation can be expressed in terms of solutions of lower order linear differential equations?

We shall show that the questions raised in these examples can be answered using the galois theory of linear differential equations and in many cases one can even give algorithms to answer these questions. In section 1, we will describe the basics of this galois theory. In section 2, we will discuss the question of when a linear differential equation has liouvillian solutions. Section 3 is devoted to the question of when a linear differential equation can be solved in terms of second

order linear differential equations. Section 4 is devoted to explaining the deepest fact in the galois theory: the connection between rational functions on the galois group and solutions of linear differential equations. This connection is used in section 5 to describe when the solutions of a linear differential equation can be expressed in terms of solutions of linear differential equations of lower order. Finally, in section 6, I will discuss the ramifications of a linear differential equation having an algebraic relationship among its solutions. In all these sections I will not aim at stating the most general results or even giving complete proofs. My aim is always to give an overview of the subject together with a taste of the techniques used. All the results mentioned here appear in print in other sources. The reader familiar with these sources will readily see how heavily I have relied on them especially [KAP57] and [KOL73].

1. Differential Galois Theory.

In this section, I will give an exposition of the basic facts of the classical galois theory of homogeneous linear differential equations. This theory was founded in the 19th century by Picard and Vessiot and generalized and given modern mathematical rigor by Kolchin in the middle part of this century. This theory is enough for my purposes here, but there are now alternative approaches that I will not mention in detail. These are primarily due to Deligne [DEL70], Katz ([KATZ82], [KATZ87a], [KATZ87b], [KAPI87]) and Ramis ([RAM85a], [RAM85b]). Their approaches have also been successful used in [BEH88], [BEHE87] and [DUMI88] to compute galois groups.

In the ordinary galois theory of algebraic equations, questions of

solvability of equations are translated into questions about fields and finite groups. For differential equations, the proper setting is differential fields and algebraic groups. The exposition here closely follows that of Kaplansky [KAP57].

Definitions. Let k be a field. A map $D:k \to k$ is called a derivation if, for all $a,b \in k$, $D(a+b) = D(a) + D(b)$ and $D(ab) = D(a)b + a\,D(b)$. We shall usually denote a derivation by $'$, i.e. $a' = D(a)$. A field with a designated derivation is called a differential field. If k is a differential field, the set $\{ c \in k \mid c' = 0 \}$ is a subfield called the field of constants of k and denoted by Const(k).

A good example to keep in mind is the field $\mathbb{C}(x)$, where the derivation is d/dx. The field of constants is $\mathbb{C}$. In this paper all fields will be of characteristic zero. One could also define a differential field as a field with (possibly) several commuting derivations and the results that follow could be generalized to this case. We stick with one derivation to simplify the exposition. If $F \subset E$ are differential fields and S is a subset of E, we denote by $F\langle S\rangle$ the smallest differential subfield of E containing F and S. Note that $F\langle S\rangle$ is the field generated (over F) by the elements of S and their derivatives of all orders. In the galois theory of algebraic equations, one associates a splitting field with an algebraic equation. The following definition gives the analogous object in this setting.

Definition. Let k be a differential field and $L(y) = y^{(n)} + a_{n-1}\, y^{(n-1)} + \ldots + a_0\, y$ with $a_i \in k$. M is a Picard–Vessiot extension (or P–V extension) of k associated with $L(y) = 0$ if: (1) $M = k\langle y_1, \ldots, y_n\rangle$,

where $y_1, \ldots, y_n$ are solutions of $L(y) = 0$ linearly independent over Const(k), and (2) Const(M) = Const(k).

A set of linearly independent solutions $y_1, \ldots y_n$ of the n^{th} order equation $L(y) = 0$ is called a fundamental set of solutions. It is well known ([KAP57], p.21) that elements $y_1, \ldots, y_n$ are linearly independent over the constant subfield if and only if the wronskian determinant $Wr(y_1, \ldots, y_n) = \det(W) \neq 0$, where $W = (y_i^{(j)})$, $1 \le i \le n$, $0 \le j \le n-1$. One can show that in any differential field K, the set of solutions of $L(y) = 0$ forms a vector space over Const(k) of dimension at most n ([KAP57], p. 21). If $k = \mathbb{C}(x)$, then classical existence theorems guarantee that P–V extensions exist. In general if Const(k) is algebraically closed, one can show that for any L(y) as above, there exists a P–V extension associated with $L(y) = 0$ and that this extension is unique up to a differential k–isomorphism.

Definition. Let $k \subset K_1$ and $k \subset K_2$ be differential fields. A bijective field isomorphism $\sigma : K_1 \to K_2$ is a differential k–isomorphism if $(\sigma(a))' = \sigma(a')$ for all $a \in K_1$ and $\sigma(a) = a$ for all $a \in k$. If $K_1 = K_2 = K$, $G(K/k) = \{\sigma \mid \sigma$ is a differential k–automorphism of $K\}$ is called the galois group of K over k.

Let $k \subset K$ be differential fields with galois group $G = G(K/k)$. For $k \subset L \subset K$, define $L^{\check{}} = \{\sigma \in G \mid \sigma(a) = a\ \forall a \in L\}$. For $H \subset G$, define $H^{\check{}} = \{a \in K \mid \sigma(a) = a\ \forall \sigma \in H\}$. Note that $L^{\check{}}$ is a subgroup of G and $G^{\check{}}$ is a differential subfield of K. One can easily see that $((L^{\check{}})^{\check{}})^{\check{}} = L^{\check{}}$ and $((H^{\check{}})^{\check{}})^{\check{}} = H^{\check{}}$.

Definition. A differential subfield $k \subset L \subset K$ or a subgroup H of the galois group is closed if it equals its double check, i.e. $L^{\check{}\check{}} = L$ or $G^{\check{}\check{}} = G$.

One easily has the following fundamental aspect of galois theory:

Proposition 1.1. Any checked object is closed. Checking gives a one–to–one correspondence between closed subgroups and closed subfields.

To make this a useful fact one must answer the questions: Which subfields are closed? and Which subgroups are closed? To do this we restrict ourselves to P–V extensions K of a differential field k and assume that $C = \text{Const}(k)$ is algebraically closed (Proposition 1.1 is valid for any differential fields $k \subset K$). If K is the P–V extension of k associated with $L(y) = 0$, let $V = \{y \in K \mid L(y) = 0\}$. As noted before, this is a C–vector space of dimension n. If $\sigma \in G$ and $v \in V$, then $0 = \sigma(L(v)) = L(\sigma(v))$. Therefore, if $y_1, \ldots, y_n$ is a basis of V, then $\sigma(y_i) = \sum c_{ij} y_j$, for some c_{ij} in $\text{Const}(k)$. The identification of $\sigma \longmapsto (c_{ij})$ yields an isomorphism of G onto a subgroup of the group of invertible $n \times n$ matrices with constant coefficients, $GL(n,C)$. We shall now describe a topology where the closed (in the above sense) subgroups of G are precisely the subgroups of G that are topologically closed (see [ROS80], [SPR81], and [HUM81] for a fuller exposition of this material and the material on linear algebraic groups).

Definition. Let C be a field and m an integer. $X \subset C^m$ is Zariski closed if there is a subset S of $C[x_1, \ldots, x_m]$ such that $X = \{ \bar{c} \in C^m \mid f(\bar{c}) = 0 \ \forall f \in S \}$.

For example, if $m = 1$, the Zariski closed sets are the empty set, C, and finite sets. If $m = 2$, the Zariski closed sets are the empty set, C^2, finite sets, curves (zero sets of a single polynomial), and finite unions of these. The arbitrary intersection and finite union of Zariski closed sets are Zariski closed, so the Zariski closed sets define a topology, called the Zariski topology. This topology has some strange features. For example, if C is infinite, any two nonempty open sets intersect. The Hilbert Basis Theorem implies that this topology has the descending chain condition on closed sets (any chain $X_1 \supset X_2 \supset \ldots$ of closed sets eventually stabilizes). This implies that any closed set can be written as the disjoint union of a finite number of open and closed connected sets, called the connected components of the closed set. If we think of $GL(n,C)$ as a subset of C^{n^2}, we see that it is open in the Zariski topology; $GL(n,C) = \{ A \in C^{n^2} \mid \det(A) \neq 0 \}$. Sometimes it is convenient to identify $GL(n,C)$ with a Zariski closed subset of C^{n^2+1}. To do this we identify $A \in GL(n,C)$ with (A,a) where $a \cdot \det(A) = 1$. We make this identification in the following definition.

Definition. A linear algebraic group is a subgroup of $GL(n,C)$ that is closed in the Zariski topology.

For example, $GL(n,C)$, $SL(n,C) = \{ A \in GL(n,C) \mid \det(A) = 1 \}$, and $T(n,C) = \{A \in GL(n,C) \mid A = (a_{ij}) \text{ where } a_{ij} = 0 \text{ if } i > j \}$. If G is

a linear algebraic group then the maps $A \longmapsto A^{-1}$, $A \longmapsto AB$ and $A \longmapsto BA$ are continuous maps (for fixed B). This is because if X is a Zariski closed set and $F : X \longmapsto C^n$ is a map given componentwise by rational functions whose denominators are nowhere zero on X, then F is continuous in the Zariski topology. If G is a linear algebraic group, then one of the connected components of G contains the identity. This connected component is denoted by G^o. G^o is, in fact, a normal subgroup (of finite index) of G. To see this, note that $(G^o)^{-1}$ is again a connected component of G and contains the identity. Therefore, $(G^o)^{-1} = G^o$. Similarly, for $c \in G^o$, $c \cdot G^o = G^o$ and for $a \in G$, $a \cdot G^o \cdot a^{-1} = G^o$.

Proposition 1.2. If K is a P–V extension of k then $G = G(K/k) \subset GL(n,C)$ is Zariski closed. If H is a closed subgroup of G, then H is Zariski closed.

The second statement in Proposition 1.2 follows from the first since if H is closed then $H = G(K/H')$ and K is again a P–V extension of H'. Before proving Proposition 1.2 in a special case, we will consider two examples.

Example 1.2.1. Let $L(y) = y' - a\,y$ with $a \in k$. The P–V extension of k corresponding to L(y) is of the form $K = k\langle y\rangle = k(y)$, where $y' = a\,y$ (i.e. $y = \exp(\int a)$). If $\sigma \in G(K/k) = G$ then $\sigma(y'/y) = \sigma(a) = a = y'/y$. From this we can conclude that $(\sigma(y)/y)' = 0$. Therefore $\sigma(y) = c_\sigma \cdot y$ for some $c \in C - \{0\} = C^* = GL(1,C)$. The only Zariski closed subgroups of GL(1,C) are finite or all of GL(1,C). If G is finite, then it must be cyclic. This implies that $y^m \in k$ for some m. If G is not finite then $G = GL(1,C)$.

Example 1.2.2. Let $a \neq 0$ be in k and $L(y) = y'' - (a'/a)y'$. The P–V extension of k corresponding to L(y) = 0 is of the form $K = k\langle 1, y\rangle = k(y)$, where $y' = a$. For $\sigma \in G(K/k) = G$, $(\sigma(y) - y)' = 0$, so $\sigma(y) = y + c_\sigma$ for some $c_\sigma \in Const(k) = C$. Since $\sigma(1) = 1$, we can identify σ with the matrix $\begin{bmatrix} 1 & c \\ 0 & 1\sigma \end{bmatrix}$. The set of matrices of the form $\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}$ for $c \in C$ can be identified with the additive subgroup of C. Therefore, G is either the trivial subgroup or isomorphic to C.

We will prove Proposition 1.2 under the assumption that $k = \mathbb{C}(x)$, $x' = 1$, and that K is a P–V extension of k associated with a second order homogeneous linear differential equation, i.e. $K = \mathbb{C}(x)\langle y_1, y_2\rangle = \mathbb{C}(x, y_1, y_2, y_1', y_2')$. We shall show that $G = G(K/k) \subset GL(2,\mathbb{C})$ is the intersection of $GL(2,\mathbb{C})$ and the zero set of a collection of polynomials in four variables with coefficients in $\mathbb{C}$. After we make the identification $A \in GL(2,\mathbb{C}) \longleftrightarrow (A, (\det(A))^{-1}) \in \mathbb{C}^5$, we see that this implies that G is a linear algebraic group. We follow the exposition in ([KOV86]). Let Y_1, Y_2, Z_1, Z_2 be new variables and let ψ: $R = \mathbb{C}[x, Y_1, Y_2, Z_1, Z_2] \longrightarrow K = \mathbb{C}[x, y_1, y_2, y_1', y_2']$ be the obvious substitution homomorphism. Let P be the kernel of ψ. For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{C})$, A acts on R by leaving $\mathbb{C}[x]$ fixed and sending (Y_1, Y_2, Z_1, Z_2) to $(aY_1 + bY_2, cY_1 + dY_2, aZ_1 + bZ_2, cZ_1 + dZ_2)$. A will induce an automorphism of K if and only if A maps P to itself. We may write $P = (p_1, \ldots, p_s)$ where the p_i are linearly independent over $\mathbb{C}$. Let m be the maximum of the degrees of the p_i. A maps $V_m = \{p \in R \mid \deg p \leq m\}$ to itself. Extend $p_1, \ldots, p_s$ to a basis $p_1, \ldots, p_t$ of V_m. There exist polynomials $P_{ij}(a,b,c,d)$ such that the action of A on V_m is

given by $A \cdot p_i = \sum_j P_{ij}(a,b,c,d)p_j$. We then see that $A \in G$ if and only if $P_{ij}(a,b,c,d) = 0$ for $i = 1, \ldots, s$ and $j = s+1, \ldots, t$.

Note that the above proof is not constructive. Given L(y), the proof does not show us how to construct the polynomials defining G. In fact, it is not known in general how to produce such a set and this is an important open problem in the galois theory. Many of the problems we discuss below could be easily shown to be decidable if we could effectively solve this problem. To show that the closed subgroups of G are precisely the Zariski closed subgroups, we need to show the following:

Proposition 1.3. Let K be a P–V extension of k with galois group G. Any Zariski closed subgroup of G is closed.

We shall follow ([KAP57], p.37) and only prove this proposition when K is associated with a linear differential equation of order 2, i.e. $K = k\langle y_1, y_2\rangle$. It is enough to show that if H is a subgroup of $G \subset GL(2,C)$, then H is Zariski–dense in $H^{\circ\circ}$. Assume not and we will argue to a contradiction. By assumption there is a polynomial f(a,b,c,d) with constant coefficients vanishing on H but not on $H^{\circ\circ}$. Let $\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} y_1 & y_2 \\ y_1' & y_2' \end{bmatrix}^{-1}$. For new differential variables, y and z, define the differential polynomial $F(y,z) = f(Ay+By', Az+Bz', Cy+Dy', Cz+Dz')$. For $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G, we set $y = \sigma(y_1)$ and $z = \sigma(y_2)$. We then have $F(\sigma(y_1), \sigma(y_2)) = f(a,b,c,d) = 0$ for all $\sigma \in H$ but not all $\sigma \in H^{\circ\circ}$. Among all differential

polynomials in y and z with coefficients in K, let E(y,z) have the smallest number of terms with this property. We can assume that some coefficient in E is 1. For $\tau \in H$, let E_τ be the polynomial gotten by applying τ to the coefficients of E. $E - E_\tau$ is shorter than E and vanishes for $y = \sigma(y_1)$ and $z = \sigma(y_2)$ for all $\sigma \in H$. Therefore it must vanish for $y = \sigma(y_1)$ and $z = \sigma(y_2)$ for all σ in $H^{\circ\circ}$. If $E - E_\tau$ is not identically zero, we can find an element $\gamma \in K$ such that $E - \gamma(E - E_\tau)$ is shorter than E and has the same property as E. This contradiction shows that the coefficients of E are left invariant by H. Therefore E has coefficients in H° and these coefficients must be left invariant by $H^{\circ\circ}$. For $\sigma \in H^{\circ\circ}$, $E(\sigma(y_1), \sigma(y_2)) = \sigma(E(\sigma^{-1}(\sigma(y_1)), \sigma^{-1}(\sigma(y_2)))) = \sigma(E(y_1,y_2)) = 0$. This contradicts the fact that $E(\sigma(y_1),\sigma(y_2)) \neq 0$ for some $\sigma \in H^{\circ\circ}$ and finishes the proof of Proposition 2.2.

We now turn to the problem of characterizing the closed subfields of K. It is a fact that the closed subfields of K are precisely the differential subfields F with $k \subset F \subset K$. The key step in showing this is the following proposition:

Proposition 1.4. Let K be a P–V extension of K and assume that C = Const(k) is algebraically closed. If $\alpha \in K - k$ then there is a $\sigma \in G(K/k)$ such that $\sigma(\alpha) \neq \alpha$.

We only give a rough sketch of the proof of this result. The proof proceeds in two steps. The first step is to show that for any differential fields $k \subset K$ and $\alpha \in K$–k, there is a differential field E containing K and k–isomorphism $\psi: K \longrightarrow E$ such that $\psi(\alpha) \neq \alpha$. The

proof of this fact relies on the fact that one can construct differential ideals not containing certain elements and requires a certain amount of differential ideal theory ([KAP57], p.13–17). The second step is to use this result when K is a P–V extension of k. In this case the isomorphism ψ is determined by its effect on $y_1, \ldots, y_n$, where $K = k\langle y_1, \ldots, y_n\rangle$. ψ is given by a matrix (d_{ij}) in GL(n,Const(E)). The fact that ψ is an isomorphism and $\psi(\alpha) \neq \alpha$ is equivalent to to (d_{ij}) satisfying a system of polynomials $f_1(d_{ij}) = 0, \ldots, f_s(d_{ij}) = 0, g(d_{ij}) \neq 0$. Since this system is consistent (it has the solution (d_{ij})), and Const(k) is algebraically closed, we can find c_{ij} in Const(k) satisfying this system. (c_{ij}) defines an element $\sigma \in GL(n,Const(k))$ with the desired properties.

Proposition 1.4 implies that any differential subfield E of K containing k is closed since K is a P–V extension of E. Combining Propositions 1.1, 1.2, 1.3 and 1.4 we have:

Theorem 1.5. Let $k \subset K$ be differential fields with K a P–V extension of k and Const(k) algebraically closed. Let $G = G(K/k) \subset GL(n,Const(k))$. Then G is a linear algebraic group and the correspondence described above is a bijective correspondence between Zariski closed subgroups of G and differential subfields E with $k \subset E \subset K$.

Just as in the galois theory of algebraic equations, one is able to identify those subfields corresponding to normal subgroups of the galois group.

Definition. Let $k \subset K$ be differential fields. We say that K is normal over k if for any $\alpha \in K-k$ there exists a $\sigma \in G(K/k)$ such that $\sigma(\alpha) \neq \alpha$.

Theorem 1.6. Let K be a P–V extension of k and assume Const(k) is algebraically closed. A Zariski closed subgroup H of $G = G(K/k)$ is normal in G if and only if $H^\sim$ is normal over k. In this case, $G(H^\sim/k)$ is isomorphic to G/H.

Assume that H is normal in G. Since K is normal over k, given any $\alpha \in H^\sim$ there is a $\sigma \in G$ such that $\sigma(\alpha) \neq \alpha$. Since H is normal in G, any $\sigma \in G$ leaves $H^\sim$ invariant and so induces an automorphism of $H^\sim$. Therefore $H^\sim$ is normal over k.

Now assume that $H^\sim$ is normal over k. One first shows that any k–automorphism ψ of $H^\sim$ can be extended to a k–isomorphism $\tilde{\psi}$ of K into a differential field E containing K. This done in way similar to that described in Proposition 1.4. As in Proposition 1.4, $\tilde{\psi}$ is determined by a matrix $(d_{ij}) \in GL(n,Const(E))$ and the fact that $\tilde{\psi}$ extends ψ and is an isomorphism is equivalent to a system of equations. Since this system is consistent we can find a solution $(c_{ij}) \in$ Const(k) that defines a k–automorphism that extends ψ. We now let H_1 be the normalizer of H in G. One can show that H_1 is Zariski closed. H_1 contains any automorphism of K that leaves $H^\sim$ invariant. Since $H^\sim$ is normal over k and all automorphisms of $H^\sim$ extend to K, $H_1^\sim = k$. Theorem 1.5 now implies that $H_1 = G$.

The final statement comes from the observation that restricting any $\sigma \in G$ to $H^\sim$ induces a homomorphism from G(K/k) to $G(H^\sim/k)$ whose kernel is H.

The usual galois theoretic arguments ([KAP57] p. 18–20) for algebraic extensions and algebraic equations can be generalized to show:

Theorem 1.7. Let K be a P–V extension of k and assume that Const(k) is algebraically closed. Let H be a Zariski closed subgroup of G = G(K/k). H has finite index in G if and only if $H^\sim$ is algebraic over k. In this case $|G:H| = [H^\sim:k]$.

2. Liouvillian Solutions of Homogeneous Linear Differential Equations.

Recall that the notion of "solvability in terms of radicals" for algebraic equations can be formalized in terms of towers of fields and that necessary and sufficient conditions can be given in terms of the galois group. An analogous situation holds for linear differential equations and "solvability in terms of exponentials, integrals and algebraics". We start with the

Definition. Let $k \subset K$ be differential fields. K is a liouvillian extension of k if there exists a tower $k = K_0 \subset K_1 \subset \ldots \subset K_n = K$ such that for each i, $K_i = K_{i-1}(t_i)$ where either

(i) t_i is algebraic over K_{i-1}, or

(ii) $t_i'/t_i \in K_{i-1}$ (i.e. $t_i = e^{\int u_i}$ for some $u_i \in K_{i-1}$), or

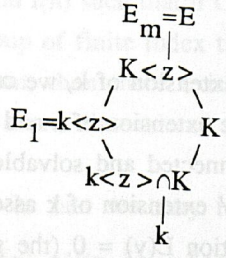
(iii) $t_i' \in K_{i-1}$ (i.e. $t_i = \int u_i$ for some $u_i \in K_{i-1}$).

For example $y = e^{\int \sqrt{x}}$ lies in a liouvillian extension of $\mathbb{C}(x)$

since $y \in \mathbb{C}(x,\sqrt{x},e^{\int\sqrt{x}})$. The galois theoretic criterion for solvability in terms of these functions is

Theorem 2.1. K be a P–V extension of k with galois group G = G(K/k) and assume that Const(k) is algebraically closed. K is contained in a liouvillian extension of k if and only if the connected component G^0 of the identity is a solvable group.

We start by assuming that K is contained in a liouvillian extension E of k with Const(E) = Const(k) (in general one can show that if K is contained in a liouvillian extension of k, then it is contained in one with the same constants ([KOL73] p. 408). Let E be defined by the tower $k = E_0 \subset \ldots \subset E_m = E$. We proceed by induction on m. Let $E_1 = k\langle z\rangle$.



$K\langle z\rangle$ is a P–V extension of $k\langle z\rangle$, so by the induction hypothesis $G(K\langle z\rangle/k\langle z\rangle)$ has a solvable component of the identity. Restricting any $\sigma \in G(K\langle z\rangle/k\langle z\rangle)$ to K gives a k–automorphism of K. This gives an isomorphism of $G(K\langle z\rangle/k\langle z\rangle)$ onto the subgroup $H = (k\langle z\rangle \cap K)^\sim$ of G(K/k). We now consider the three possibilities for z. If z is algebraic over k, then Theorem 1.7 implies that $|G:H| < \infty$. In this case $|G^0:H^0| < \infty$, so $G^0 = H^0$, since G^0 is connected. Therefore G^0 is solvable. If $z' \in k$ or $z'/z \in k$, then examples 1.2.1 and 1.2.2 show that $G(k\langle z\rangle/k)$ is abelian. Theorem 1.6 (applied to the P–V extension $k\langle z\rangle$ of k) then implies that $k\langle z\rangle \cap K$ is a normal extension of k with

abelian galois group. Therefore H is normal in G and G/H is abelian. We now get the desired conclusion from the following group theoretic fact: If G is a linear algebraic group and H is a Zariski closed subgroup such that H is normal in G, G/H is abelian and H^o is solvable, then G^o is solvable. We refer to ([KAP57] p.29) for a proof of this fact.

Now let us assume that the connected component G^o of G is solvable. The proof that K lies in a liouvillian extension of k relies heavily on the following group theoretic result (the reader is referred to ([KAP57 p. 30) or ([ROS80]) for a proof of this result):

Lie – Kolchin Theorem. Let C be an algebraically closed field and G $\subset$ GL(n,C) a solvable linear algebraic group that is connected in the Zariski topology. Then there exists an A $\in$ GL(n,C) such that AGA^{-1} $\subset$ T(n,C), i.e. the elements of G can be put in simultaneous triangular form

To show that K lies in a liouvillian extension of k, we can first replace k by $(G^o)^{\sim}$. This is a finite algebraic extension of k and allows us to assume that the galois group G is connected and solvable. We now specialize to the case where K is a P–V extension of k associated with a second order linear differential equation L(y) = 0 (the general case follows in a similar fashion). G acts on the solution space V of L(y) = 0 and, by the Lie – Kolchin Theorem, we may assume that V has a basis y_1, y_2 such that for all $\sigma \in G$ there exists a $c_\sigma \in G$ such that $\sigma(y_1) = c_\sigma(y_1)$. This implies that y_1'/y_1 is left fixed G and so lies in K. Therefore $k(y_1)$ is a liuovillian extension of k. Let $W = y_1'y_2 - y_2'y_1$. For $\sigma \in G$, $\sigma(W) = (\det \sigma)\cdot W$. Therefore W'/W is left fixed by G and so lies in k. $(y_1/y_2)' = W/y_1^2$ so $k(y_1, W, y_2/y_1)$ is a

liouvillian extension of k that contains K.

Theorem 2.1 gives necessary and sufficient conditions for all solutions of a linear differential equation to be liouvillian, but it does not tell us how one can effectively decide this question. We will use Theorem 2.1 to show that if a linear differential equation has a liouvillian solution then it has one of a very special form. We will then describe an algorithm to find such a solution. We first need a more effective version of the Lie – Kolchin Theorem. Note that the Lie – Kolchin Theorem implies that if G is a connected solvable linear algebraic group in GL(n,C), then G has an invariant one dimensional subspace in C^n.

Proposition 2.2. Let C be an algebraically closed field. There is a function I(n) such that if G is a subgroup of GL(n,C) and H is a normal subgroup of finite index that leaves a one dimensional subspace of C^n invariant, then there exists a subgroup $\tilde{H}$ of G of index $\leq$ I(n) that leaves a one dimensional subspace of C^n invariant.

In fact we may take I(n) to be defined by I(0) = 1, I(n) = $\max\{J(n), n!I(n-1)\}$ where $J(n) = (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$. This proposition and the bounds depend heavily on Jordan's Theorem: any finite subgroup of GL(n,C) contains an abelian normal subgroup of index at most J(n). A proof of Proposition 2.2 can be found in [SING81].

Proposition 2.3. Let k be a differential field, L(y) = 0 a linear differential equation of order n with coefficients in k and assume Const(k) are algebraically closed. If L(y) = 0 has a nonzero solution in

a liouvillian extension of k, then $L(y) = 0$ has a nonzero solution z such that z'/z is algebraic over k of degree $\leq I(n)$.

To prove this proposition, we first note that we can assume that if $L(y) = 0$ has a nonzero solution in a liouvillian extension of k, then it has such a solution in the P–V extension K of k associated with $L(y) = 0$ (this is a technical point whose proof is contained in [SING81]). Let $W = \{w \in K \mid L(w) = 0$ and w lies in a liouvillian extension of $k\}$. W is a nontrivial vector space over Const(k) that is left invariant by the G(K/k). Let $w_1, \ldots, w_m$ be a basis of W and let $L_m(y) = Wr(y, w_1, \ldots, w_m)/Wr(w_1, \ldots, w_m)$. The coefficients of $L_m(y)$ are left fixed by G(K/k) since applying $\sigma \in G(K/k)$ to these wronskians just multiplies each of them by the determinant of the linear map induced by σ on W. Therefore $L_m(y)$ has coefficients in k and has all of its solutions lying in some liouvillian extension of k. Since any solution of $L_m(y) = 0$ is a solution of $L(y) = 0$, we will prove the result for $L_m(y) = 0$.

Therefore, we may assume that the P–V extension K of k associated with $L(y) = 0$ lies in a liouvillian extension of k. Theorem 2.1 implies that the connected component G^0 of G(K/k) is solvable and the Lie – Kolchin Theorem implies that G^0 leaves a one dimensional subspace invariant. Proposition 2.2 implies that G has a subgroup $\tilde{H}$ of index $\leq I(m) \leq I(n)$ such that $\tilde{H}$ has a one dimensional invariant subspace. Let z be a solution of $L(y) = 0$ such that for all $\sigma \in \tilde{H}$ there is a $c_\sigma \in$ Const(k) such that $\sigma(z) = c_\sigma z$. We then have $\sigma(z'/z) = z'/z$ for all $\sigma \in \tilde{H}$ so $z \in (\tilde{H})^\sim$. Therefore $[k(z):k] \leq [(\tilde{H})^\sim:k] = |G:(\tilde{H})^\sim| \leq I(n)$.

Proposition 2.3 tells us that if we want to decide if an nth order linear differential equation $L(y) = 0$ has a nonzero liouvillian solution over k, we need to decide if there is an element u, algebraic over k of degree $\leq I(n)$, such that $L(e^{\int u}) = 0$. I will describe an algorithm that searches for the minimal polynomial of such a u when $k = C(x)$, where C is a computable algebraically closed field (a computable field is one in which the field operations are recursive and over which one can factor polynomials). This algorithm depends on the following two propositions.

Proposition 2.4. Let $L_1(y) = 0$ and $L_2(y) = 0$ be two homogeneous linear differential equations with coefficients in C(x). One can effectively construct homogeneous linear differential equations $L_3(y) = 0$, $L_4(y) = 0$ and $L_5(y) = 0$ such that

(a) the solution space of $L_3(y) = 0$ contains $\{y_1 \cdot y_2 \mid L_i(y_i) = 0$ for $i = 1,2\}$,

(b) the solution space of $L_4(y) = 0$ contains $\{y_1 + y_2 \mid L_i(y_i) = 0$ for $i = 1,2\}$, and

(c) the solution space of $L_5(y) = 0$ contains $\{y' \mid L_1(y) = 0\}$.

I will only justify part (a) of this proposition. Assume that the orders of $L_1(y)$ and $L_2(y)$ are n and m respectively. Let U and V be new differential variables. Formally differentiate UV $n \cdot m$ times. Whenever $U^{(i)}$ occurs for $i \geq n$, we use the relation $L_1(U) = 0$ and its derivatives to replace $U^{(i)}$ with a C(x)–linear combination of the $U^{(j)}$, $0 \leq j \leq n-1$. We proceed similarly for $V^{(i)}$ for $i \geq m$ using $L_2(V) = 0$. In

this way the $(UV)^{(s)}$ $0\le s\le m\cdot n$ yield $m\cdot n+1$ linear forms in the $U^{(i)}V^{(j)}$, $0\le i\le n-1$, $0\le i\le m-1$, that is $m\cdot n+1$ linear forms in $m\cdot n$ indeterminates. Therefore we can find $a_i \in C(x)$, not all zero, such that

$$L_3(UV) = \sum_{s=0}^{m\cdot n} a_s(UV)^{(s)} = 0.$$

Proposition 2.5. Let $L(y) = 0$ be a homogeneous linear differential equation with coefficients in $C(x)$. One can find an integer N such that if z is a solution of $L(y) = 0$ and $z'/z \in C(x)$, then the degrees of the numerator and denominator of z are less than N.

The proof of this proposition depends on the following classical fact ([SCH95] vol.I, section 94–95 and vol. 2 section 177 or [TOU87]). Given $L(y)$ there exist finite sets $S_1 \subset C$ and $S_2 \subset C[x]$, which depend on L and can be effectively determined such that if $L(y) = 0$ has a solution of the form $y = Ax^{\rho}e^{p(x)}\phi(x)$ where $\rho, A \in C$, $p(x) \in C[x]$, and $\phi(x)$ of the form $\phi(x) = c_o + c_1x^{-1} + \dots$, $c_i \in C$, $c_o \neq 0$, the $\rho \in S_1$ and $p(x) \in S_2$. Now assume that $L(z) = 0$ and $z'/z = R(x) \in C(x)$. Let a be a pole of $R(x)$. If a is a nonsingular point of $L(y) = 0$ (i.e. a is not the zero of a denominator of a coefficient of $L(y)$), then $R(x)$ can have at most a pole of order 1 at a with residue a positive integer. Therefore,

$$R(x) = p(x) + c_{s+1,1}/(x-a_{s+1}) + \dots + c_{m,1}/(x-a_m) + \sum_{i=1}^{s}\sum_{j=1}^{n_i} c_{i,j}/(x-a_i)^j,$$

where $a_1, \dots a_s$ are the finite singular points of L, $a_{s+1}, \dots, a_m$ are (unknown) nonsingular points and $c_{s+1,1}, \dots, c_{m,1}$ are positive integers. Let a_j be a singular point. Expanding z at a_j we have

$z = (x-a_j)^{c_{j,1}}\exp(-c_{j,2}/(x-a_j) - \dots - c_{j,n_j}/(n_j-1)(x-a_j)^{n_j-1})\phi(x)$, where ϕ is a formal power series at a_j and $\phi(a_j)\neq 0$. Via the transform $x \longmapsto 1/(x-a_j)$ we can use the above mentioned fact to determine n_j and $c_{j,1}$ up to some finite set of possibilities. Expanding z at infinity, we get $z = x^{\rho}\exp(\int p(x))\phi_\infty(x)$ where $\phi_\infty(x)$ has a power series expansion at infinity, $\phi_\infty(\infty)\neq 0$, and $\rho = c_{1,1} + \dots + c_{s,1} + \dots + c_{m,1}$. Again using the above fact, we can determine $p(x)$ up to a finite number of possibilities and, since the set $\{c_{1,1}, \dots, c_{m,1}\}$ is determined up to a finite number of possibilities and $c_{s,1}, \dots, c_{m,1}$ are positive integers, we can bound m. These bounds allow us to find a suitable N. A more detailed analysis of this procedure is given in [GRI88], where better bounds are also given.

We now show how to effectively answer the question: Given $L(y) = 0$ in $C(x)$, does $L(y) = 0$ have a solution z such that z'/z is algebraic over $C(x)$ of degree $\le I(n)$. We start by fixing an integer $N \le I(n)$. We want to test if there exist $a_i \in C(x)$ and u satisfying $P(u) = u^N + a_{N-1}u^{N-1} + \dots + a_o = 0$ such that $z = e^{\int u}$ is a solution of $L(z) = 0$. We may assume that such a P is irreducible. In this case, if some u with $P(u) = 0$ satisfies $L(e^{\int u}) = 0$, then for all u with $P(u) = 0$, we have $L(e^{\int u}) = 0$. Let us consider the possibilities for a_{N-1}. If $u_1, \dots, u_N$ are the roots of $P(u) = 0$ then $a_{N-1} = -(u_1 + \dots + u_N) = -(y_1'/y_1 + \dots + y_N'/y_N) = -(\Pi y_i)'/\Pi y_i$ where $y_i = \exp(\int u_i)$ is a solution of $L(y) = 0$. Proposition 2.4 allows us to construct a linear differential equation $\tilde{L}(y)$ such that $\tilde{L}(w) = 0$ for any $w = \prod_{i=1}^{N} y_i$, where the y_i are solutions of

$L(y) = 0$. Proposition 2.5 allows us to bound the degrees of the numerators and denominators of solutions of $w'/w \in C(x)$ with $\tilde{L}(w) = 0$. This gives us a bound on the degrees of the numerators and denominators of the possible a_{N-1}. One can bound these degrees for the other a_i in a similar (but more complicated) way ([SING81], p.671). We therefore write $P(u) = P(u, c_1, \ldots, c_M)$ where the c_j are undetermined coefficients appearing in the a_i. We then need to decide if there exist $\tilde{c}_j \in C$ such that if u is a solution of $P(u, \tilde{c}_1, \ldots, \tilde{c}_M) = 0$, then $L(e^{\int u}) = 0$. Using $P(u, \tilde{c}_1, \ldots, \tilde{c}_M) = 0$, we can replace all derivatives of u in $L(e^{\int u}) = 0$ by expressions that are polynomials in u (of degree $\leq N-1$) with coefficients involving the $\tilde{c}_j$. Dividing by $e^{\int u}$ and equating coefficients of powers of u equal to 0, yields a system of polynomials that determine the $\tilde{c}_j$ (with coefficients in C(x)). This is equivalent to a system of polynomials with coefficients in C and we can use elimination theory to decide if this system has a solution.

The above procedure can be generalized to show the following [SIN88b]:

Proposition 2.6. Let F be either an algebraic extension of a purely transcendental liouvillian extension of C(x) or an elementary extension of C(x) (where C is as above). If $L(y) = 0$ is a linear differential equation with coefficients in F then one can find in a finite number of steps, a vector space basis for the space of solutions $L(y) = 0$ that are liouvillian over F.

An elementary extension of a field k is a liouvillian extension of k where condition (iii) of the definition of liouvillian extension is

replaced by: (iii)* $t' = u_i'/u_i$ where $u_i \in K_{i-1}$ (i.e. $t_i = \log u_i$).

The problem of finding liouvillian solutions (or even algebraic solutions) of linear differential equations has a long history. In the 1870's, H.A. Schwarz determined which hypergeometric equations have only algebraic (over $\mathbb{C}(x)$) solutions. Klein, in 1877, showed that if a second order linear differential equation had only algebraic solutions then it could be transformed, via a change of variables, to an equation on Schwarz's list. Baldassari and Dwork made this method effective ([BADW79], see their paper for references to Schwarz, Klein and their contemporaries). For $n \geq 2$, Painleve and his student Boulanger gave a procedure, [BOU98], to decide if an nth order linear differential equation has only algebraic solutions. This procedure was rediscovered in [SING80]. A procedure to decide when a second order linear differential equation with coefficients in $\mathbb{C}(x)$ has liouvillian solutions is given in [KOV86]. A procedure to find a basis for the space of liouvillian solutions of $L(y) = 0$ when L(y) has coefficients in an algebraic extension of $\mathbb{C}(x)$ is given in [SING81] (but many of the ideas already occur in [MAR98] which was not known to me when [SING81] was written). The problem of deciding if an inhomogeneous equation $L(y) = b$ has liouvillian solutions is discussed in [DAV84], [DAV85], and [DASI86].

3. Solving Homogeneous Linear Differential Equations in Terms of Second Order Linear Differential Equations.

Liouvillian extensions are defined by adjoining solutions of algebraic equations or of the first order equations $y'+ay=0$ or $y'=a$. Any first order linear differential equation $y'+ay=b$ can be solved in terms of these latter two equations. Therefore we can think of "solving

in terms of liouvillian functions" as "solving in terms of first order linear differential equations." The next natural question is: when can one solve homogeneous linear differential equations in terms of second order linear differential equations. Intuitively this means that the solutions lie in a tower of field where each field is gotten from the previous one by adjoining a solution of a second order linear differential equation or an algebraic equation (where we think of first order equations as degenerate second order equations). The motivates the following

Definition. Let $F \subset E$ be differential fields. We say E is a second order solvable extension of F (an SOS extension of F) if there is a tower of fields $F = F_0 \subset \ldots \subset F_n = E$ such that either

(i) $F_i = F_{i-1}(t_i)$ where t_i is algebraic over F_i, or

(ii) $F_i = F_{i-1}(t_i)$ where $t_i' \in F_{i-1}$, or

(iii) $F_i = F_{i-1}(t_i)$ where $t_i'/t_i \in F_{i-1}$, or

(iv) $F_i = F_{i-1}(u_i,v_i)$ where u_i,v_i are linearly independent solutions of an equation of the form $y''+a_iy = 0$ with $a_i \in F_{i-1}$.

To give a group theoretic characterization of those P–V extensions that lie in an SOS extension, we need the following

Definition. Let C be a field. We say that a linear algebraic group G is second order solvable (an SOS group) if there is a tower of subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_0 = \{e\}$ such that G_i is a normal linear

algebraic subgroup of G_{i+1} and G_{i+1}/G_i is isomorphic to one of the following:

(i) a finite group,

(ii) the additive group $C \cong \{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in C \}$,

(iii) the multiplicative group $C^* \cong GL(1,C)$,

(iv) $SL(2,C)$,

(v) $PSL(2,C) \cong SL(2,C)/\{\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\}$.

Note that if we define a linear algebraic group G to be liouvillian if there is a tower as above where each quotient is isomorphic to (i), (ii), or (iii), one can show that the liouvillian groups are precisely the groups where G^0 is solvable.

Theorem 3.1. Let K be a P–V extension of k where C = Const(k) is algebraically closed. K lies in an SOS extension of k if and only if G(K/k) is an SOS group.

A complete proof of this is given in [SING85]. If K lies in an SOS extension of k, one shows that G(K/k) is an SOS group by induction on the length of the tower defining the SOS extension containing K. This is very similar to showing that G(K/k) has solvable component of the identity if K lies in a liouvillian extension of k and is omitted. If G(K/k) is an SOS group, one shows that K lies in an SOS extension of k by induction on the length of the tower of groups. The key step here is to show that if G(K/k) is isomorphic to a finite group, C, C^*, SL(2,C), or PSL(2,C), then K lies in an SOS extension of k. Before we outline the proof of this fact, we give the following

Definitions. (1) A map $\rho : C^n \longrightarrow C^m$ is a polynomial map if $\rho(\bar{c}) = (\rho_1(\bar{c}), \ldots, \rho_m(\bar{c}))$, where $\rho_1, \ldots, \rho_m$ are polynomials in n variables.

(2) For $G \subset GL(n,C) \subset C^{n^2+1}$ and m an integer, we say a homomorphism $\rho : G \longrightarrow GL(m,C) \subset C^{m^2+1}$ is a polynomial representation if ρ is a polynomial map from C^{n^2+1} to C^{m^2+1}.

(3) A polynomial representation $\rho: G \longrightarrow GL(n,C)$ is irreducible if the only $\rho(G)$ invariant subspaces of C^{n^2} are (0) and C^{n^2}.

(4) Two polynomial representations $\rho_1: G \longrightarrow GL(m,C)$ and $\rho_2: G \longrightarrow GL(m,C)$ are isomorphic if there is a linear isomorphism $\varphi: C^m \longrightarrow C^m$ such that $(\varphi^{-1} \circ \rho_1(g) \circ \varphi)(v) = \rho_2(g)(v)$ for all $v \in C^m$ and $g \in G$.

We will need the following fact that will be proved in the next section.

Proposition 3.2. Let K be a P–V extension of k, an algebraically closed field with constants C and $G = G(K/k)$.

(a)If $\rho: G \longrightarrow GL(m,C)$ is an irreducible polynomial representation of G then there exists a homogeneous linear differential equation $L(y) = y^{(m)} + a_{m-1}y^{(m-1)} + \ldots + a_0 y = 0$ with the $a_i \in k$ and a fundamental set of solutions $\{y_1, \ldots, y_m\}$ of $L(y) = 0$ in K such that the action of G on the C–span of $\{y_1, \ldots, y_m\}$ is isomorphic to ρ.

(b)If $G = C$, the additive group, then $K = k(y)$ for some $y \in K$ with $y' \in K$.

Proposition 3.2 says that any irreducible polynomial representation of G(K/k) already occurs in K. This result can be proven without the assumption that k is algebraically closed, but we will only need this weaker form. The importance of this fact cannot be overestimated and I will return to it several times in the next sections. I will now show that if G(K/k) is isomorphic to one of the five types of groups mentioned above, then K lies in an SOS extension of k. I deal with each case separately.

(i) G(K/k) is finite. For any $\alpha \in K$, let $f_\alpha(x) = \Pi(x - \sigma(\alpha))$ where this latter product is over all $\sigma \in G(K/k)$. $f_\alpha(x)$ has coefficients in k and $f_\alpha(\alpha) = 0$ so α is algebraic over k. Therefore K is an algebraic extension of k and so is an SOS extension of k.

(ii) $G(K/k) \cong C$. If we replace k by its algebraic closure $\tilde{k}$, then $G(K \cdot \tilde{k}/\tilde{k}) = G(K/k)$, since G(K/k) is connected. It is enough to show that $K \cdot \tilde{k}$ is contained in a SOS extension of $\tilde{k}$, since this will imply that K is contained in an SOS extension of K. We therefore can assume that k is algebraically closed. Applying Proposition 3.2(b), we have that $K = k(y)$ with $y' \in k$. This clearly implies that K is an SOS extension of k.

(iii) $G(K/k) \cong C^*$. We again can assume that k is algebraically closed. Applying Proposition 3.2 to the representation of G(K/k) as GL(1,C), we see that there is a first order homogeneous linear differential equation with coefficients in k and solution y in K such that for each $\sigma \in G(K/k)$, $\sigma(y) = c_\sigma y$ for some $c_\sigma \in C$. This implies $y'/y \in k$ and so $k\langle y \rangle$ is an SOS extension of k. $k\langle y \rangle \subset K$ and one sees that $(k\langle y \rangle)^*$ is the trivial subgroup. Therefore the galois theory implies that $k\langle y \rangle = K$..

(iv) $G(K/k) \cong SL(2,C)$. Again, we may assume that k is algebraically closed. One shows as above that there is a second order

homogeneous linear differential equation with coefficients in k and solutions y_1, y_2 such that $K = k\langle y_1, y_2\rangle$. This means that K is an SOS extension of k.

(v) $G(K/k) \cong PSL(2,C)$. The idea of the construction in this last case is the following. PSL(2,C) does not have a representation as 2×2 matrices but there is a finite map $\rho: SL(2,C) \longrightarrow PSL(2,C)$ and of course SL(2,C) has a 2×2 matrix representation. This allows us to construct an algebraic extension of K that is generated by solutions of a second order linear differential equation. We again assume that k is algebraically closed. Note that SL(2,C) acts on the space of polynomials in two variables x,y via substitution $x \longrightarrow ax+by$, $y \longrightarrow cx+dy$. This action leaves each space V_n of homogeneous polynomials of degree n invariant. The representation of SL(2,C) on V_3 with respect to the basis x^2, xy, y^2 is given by

$$\varphi\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 & 2ab & b^2 \\ ab & ad+bc & bd \\ b^2 & 2cd & d^2 \end{bmatrix}.$$

This induces an isomorphism ρ of PSL(2,C) into SL(3,C). Applying Proposition 3.2 to this ρ, we see that there exists a third order homogeneous linear differential equation $L(y) = 0$ with coefficients in k and solutions y_1, y_2, y_3 in K such that the action of G(K/k) on the C–span of $\{y_1, y_2, y_3\}$ is given by ρ. As before, the galois theory implies that $K = k\langle y_1, y_2, y_3\rangle$. I will now show that $k\langle y_1, y_2, y_3\rangle$ lies in a P–V extension of an algebraic extension of k corresponding to a second order homogeneous linear differential equation. Let a,b, and c be indeterminates and consider the expressions $z_i = ay_i + by_i' + cy_i''$ for i = 1,2,3. The expression $z_1z_3 - z_2^2$ is a polynomial in a,b,c whose

coefficients are left invariant by G(K/k). Therefore we can select a,b,c in an algebraic extension k_o of k such that $z_1z_3 - z_2^2 = 0$. Let $w_1 = \pm\sqrt{z_1}$ and $w_2 = \pm\sqrt{z_2}$ and select the signs so that $z_2 = w_1w_2$. One can show that any k_o–isomorphism σ of $k_o(w_1,w_2)$ into any differential field F sends w_1 to aw_1+bw_2 and w_2 to cw_1+dw_2 where $\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \pm 1$ and $a,b,c,d \in Const(F)$. This implies that $L_2(y) = Wr(y,y_1,y_2)/Wr(y_1,y_2)$ is a second order linear differential equation whose coefficients are left fixed by any such isomorphism. A generalization of the galois theory shows that $L_2(y)$ has coefficients in k_o. I will now show that K lies in $k_0\langle w_1,w_2\rangle$. Since $z_i = ay_i + by_i' + cy_i''$, the action of the galois group $G(k_o\langle y_1, y_2, y_3\rangle/k_o)$ on the span of $\{z_1, z_2, z_3\}$ is the same as the action on the span of $\{y_1, y_2, y_3\}$. Therefore, $(k_o\langle z_1, z_2, z_3\rangle)^{\sim}$ is this group and $K \subset k_o\langle y_1, y_2, y_3\rangle = k_o\langle z_1, z_2, z_3\rangle \subset k_o\langle w_1, w_2\rangle$.

We now specialize these results to solving third order homogeneous linear differential equations in terms of second order linear differential equations. We first need some sharper group theoretic statements.

Proposition 3.3. Let C be an algebraically closed field and G an SOS linear algebraic subgroup of SL(3,C). Then either

(i) G is finite, or

(ii) G^o leaves a one dimensional subspace of C^3 invariant, or

(iii) G leaves a two dimensional subspace of C^3 invariant, or

(iv) G^o leaves no nontrivial subspaces invariant and G^o is conjugate to $\rho(SL(2,C))$, ρ as above.

This is proven in [SING85], as is the following application.

Proposition 3.4. Let k be a differential field with algebraically closed field of constants. Let $L(y) = y''' - p\,y' - q\,y = 0$ be a linear differential equation with $p,q \in k$ and let K be the associated P–V extension. K lies in an SOS extension of k if and only if one of the following holds:

(i) all solutions of $L(y) = 0$ are algebraic over k, or

(ii) $L(y) = L_2(L_1(y))$, where $L_2(y) = y'' + a\,y' + b\,y$ and $L_1(y) = y' + c\,y$, where a,b,and c are algebraic over k, or

(iii) $L(y) = L_1(L_2(y))$ with $L_1(y)$, $L_2(y)$ as in (ii) with a,b, and c in k, or

(iv) there exist a_o, a_1, a_2, b, c algebraic over k such that for some fundamental set of solutions {u,v} of $L_2(y) = y'' + b\,y' + c\,y = 0$, $\{y_1,y_2,y_3\}$ forms a fundamental set of solutions for $L(y) = 0$, where

$$y_1 = a_o(u^2) + a_1(u^2)' + a_2(u^2)''$$
$$y_2 = a_o(uv) + a_1(uv)' + a_2(uv)''$$
$$y_3 = a_o(v^2) + a_1(v^2)' + a_2(v^2)''.$$

This result follows from Theorem 3.1 and Proposition 3.3.

Conclusions (i) and (iv) follow from (i) and (iv) of Proposition 3.3 for the reasons given in the discussion following Theorem 3.1. Conclusions (ii) and (iii) follow from (ii) and (iii) of Proposition 3.3 using the following result

Proposition 3.5. Let K be a P–V extension of k corresponding to an n^{th} order homogeneous linear differential equation $L(y) = 0$ and assume that Const(k) is algebraically closed. Let V be the solution space of $L(y) = 0$ in K. If G(K/k) leaves an m dimensional subspace of V invariant, then $L(y) = L_{n-m}(L_m(y))$ where $L_{n-m}(y)$ and $L_m(y)$ have coefficients in k and are of order m–n and m.

To see why this is true, let $y_1, \ldots, y_m$ be a basis of the invariant subspace. The linear differential equation $L_m(y) = Wr(y, y_1, \ldots, y_m)/Wr(y_1, \ldots, y_m)$ has coefficients that are fixed by G(K/k) and so must lie in k. If we formally divide L(y) by $L_m(y)$ (thinking of these as differential operators in k[D]), we have $L = L_{n-m}(L_m(y)) + R(y)$, where the order of R(y) is less than m. Since $L(y_i) = L_m(y_i) = 0$, we have $R(y_i) = 0$ for $i = 1, \ldots, m$. This implies that $R(y) \equiv 0$.

Proposition 3.4 is the heart of a decision procedure given in [SING84]. This procedure allows one to decide if a given third order homogeneous linear differential equation with coefficients in $\mathbb{Q}(x)$ can be solved in terms of second order linear differential equations. A related open problem is to give a decision procedure to decide if a third order homogeneous linear differential equation can be solved in terms of a restricted class of second order linear differential equations such as

the equations defining the Bessel functions.

4. Picard–Vessiot Extensions and Rational Functions on the Galois Group.

In this section I will show how solutions of homogeneous linear differential equations can be though of as functions on the galois group of the associated P–V extension. This point of view is very fruitful and will be used to justify Proposition 3.2 above. I first need some more definitions and facts concerning Zariski closed sets.

Let C be an field and $V \subset C^n$ be a Zariski closed set. Denote by I(V) the set $\{f \in C[x_1, \ldots, x_n] \mid f(\bar{a}) = 0 \text{ for all } \bar{a} \in V\}$. I(V) is an ideal in the ring $C[x_1, \ldots, x_n]$.

Definitions. a) V is irreducible if $V \subset X_1 \cup X_2$ with X_1 and X_2 Zariski closed, implies that $V \subset X_1$ of $V \subset X_2$.

b) $C[x_1, \ldots, x_n]/I(V)$ is called the coordinate ring of V and is denoted by C[V].

c) If V is irreducible, the quotient field of C[V] is called the function field of V and is denoted by C(V).

Note that V is irreducible if and only if I(V) is a prime ideal if and only if C[V] is an integral domain. If V is a linear algebraic group, then V is irreducible if and only if V is connected. We give two examples of the above concepts.

Example 4.1.1. Consider the linear algebraic group $GL(1,C) = C^* = \{(a,b) \in C^2 \mid ab = 1\}$. $I(GL(1,C)) = (x_1x_2 - 1)$ so $C[GL(1,C)] = C[x_1,x_2]/(x_1x_2-1) = C[x_1,x_1^{-1}]$. $C(GL(1,C)) = C(x_1)$.

Example 4.1.2. Consider the linear group $C = \{ \begin{bmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{bmatrix} \mid x_{11} = x_{22} = 1, x_{21} = 0, \text{ and } x_{12} \text{ is arbitrary}\}$. $I(C) = (x_{11} - 1, x_{22} - 1, x_{21})$, so $C[C] = C[x_{12}]$ and $C(C) = C(x_{12})$.

Definition. If V is an irreducible Zariski closed set, the dimension of V is defined to be the transcendence degree of C(V) over C and is denoted by Dim(V).

For example, $Dim(GL(n,C)) = n^2$, $Dim(SL(n,C)) = n^2-1$, and $Dim(T(n,C)) = n(n+1)/2$.

Let V be a Zariski closed set. The set of polynomial maps from V to C^1 forms a ring that can be seen to be isomorphic to C[V]. If $F: V \longrightarrow W \subset C^m$ is a polynomial map, then F induces a ring homomorphism $F^*: C[W] \longrightarrow C[V]$ given by $F^*(f) = f \circ F$. Conversely any such ring homomorphism is induced by a polynomial map. If $F: V \longrightarrow W$ is a polynomial map with F(V) Zariski dense in W, then F^* is injective. If in addition V and W are irreducible F^* induces a map from C(W) to C(V). For example, if G is a linear algebraic group and $g \in G$, we can define the polynomial map $\rho_g: G \longrightarrow G$ by $\rho_g(h) = hg$. $\rho_g^*: C[W] \longrightarrow C[V]$ is an isomorphism. One can similarly define λ_g by $\lambda_g(h) = hg$.

It will be necessary in the following to consider points in a Zariski closed set whose coordinates lie in different fields. If $C \subset k$ are fields, we say that a subset $V \subset k^n$ is C–closed if it is the zeros of a

collection of polynomials with coefficients in C. Given a Zariski closed subset V of C^n, then we can use the equations defining V to define a Zariski closed subset V_k of k^n. We shall let V_C denote the points in V_k, all of whose coordinates are in C. If C is algebraically closed and V is a Zariski closed subset of C^n, then V_C is Zariski dense in V_k. As an example, let K be a P–V extension of k and assume C = Const(k) is algebraically closed. Assume further that k is algebraically closed. This implies that G(K/k) is connected since the fixed field of $G(K/k)^0$ is a finite extension of k and so must equal k. The galois group G(K/k) is a linear algebraic group defined over C, but these equations also define a linear algebraic group G over k. G_C then gives those elements of G corresponding to the galois group. Given $g \in G_C$, g acts (via the galois action) as an automorphism of K and also acts (via ρ_g^*) as an automorphism of k(G). The following theorem relates these two actions:

Theorem 4.1. Let k be an algebraically closed differential field with constants C and K a P–V extension of k with galois group G = G(K/k). There exists a k–isomorphism $\psi: K \longrightarrow k(G)$ such that for any $\sigma \in G_C$ and $z \in K$, $\sigma(z) = \rho_\sigma^*(\psi(z))$.

The condition that k be algebraically closed can be removed but this leads to several complications. First of all G(K/k) need not be connected and we must define k(G) in a different manner. Secondly, K is not necessarily isomorphic to k(G), but is isomorphic to the function field of a principal homogeneous space for G (this result was originally

proved by Kolchin and Lang, see [KOLA58], [BIA62], or [SING88a]). In his book [KOL73], Kolchin develops a theory of differential galois cohomology that gives the machinery to understand the correspondence between P–V extension (or more generally, strongly normal extensions) and principal homogeneous spaces of the galois group. We will only prove the above result (following [SING88a]) since it will be sufficient for our purposes. We first need the following result.

Proposition 4.2. (a) Let $k \subset K$ be differential fields with the same fields 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 $y = d\Pi x_i^{n_i}$.

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

To prove a), we first show that if $z_1, \ldots, z_m$ are nonzero elements of K such that $z'/z \in k$ and $z_i/z_j \notin k$ for $i \neq j$, then $\sum z_i \neq 0$. Assume this is not true and let N be the smallest integer for which there are such elements with $\sum_{i=1}^{N} z_i = 0$. We then have $\sum_{i=1}^{N} z_i' = 0$, so $\sum_{i=2}^{N} (z_i'/z_i - z_1'/z_1)z_i = 0$. By minimality, this would imply that $z_i'/z_i - z_1'/z_1 = 0$ for $i = 2, \ldots, N$, and therefore that $(z_i/z_1)' = 0$. This contradicts the fact that $z_i/z_1 \notin k$.

Now let $y \in K$ satisfy $y'/y \in k$. We may choose a k–basis $\{u_i\}$

of $k[x_1, \ldots, x_n]$ such that each u_i is a monomial in $x_1, \ldots, x_n$. If we write $y = (\Sigma a_i u_i)/(\Sigma b_j u_i)$ with $a_i, b_j \in k$, then $\Sigma a_i y u_i - \Sigma b_j u_j = 0$. Note that for $i \neq j$, $a_i y u_i / a_j y u_j = a_i u_i / a_j u_j \notin k$ and $b_i u_i / b_j u_j \notin k$ since the u_i are linearly independent over k. Therefore the discussion in the preceding paragraph implies that for some i and j, we must have $a_i y u_i / b_j u_j \in k$, so $y = d\Pi x_i^{n_i}$.

To prove (b), note that k(E) is finitely generated over k and so can be written as $k(E) = k(x_1, \ldots, x_n)$ for some $x_1, \ldots, x_n \in E$. Therefore part (a) implies that E/k^* is generated by $x_1, \ldots, x_n$.

We now proceed to prove Theorem 4.1. Let $K = k\langle y_1, \ldots, y_n \rangle = k(y_1, \ldots, y_n, \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$. Let $E = \{y \in K \mid y'/y \in k\}$. Proposition 4.2 implies that there exist $x_1, \ldots, x_m \in E$ that generate E/k^*. Therefore $R = k[y_1, \ldots, y_n^{(n-1)}, x_1, \ldots, x_m, x_1^{-1}, \ldots, x_m^{-1}]$ is a finitely generated integral k–algebra. Let $R = k[Y_1, \ldots, Y_s]/P$ where P is a prime ideal. $P = I(V)$ for some Zariski closed set V. For any $\sigma \in G_C$, σ induces an automorphism on R. Since G_C is dense in G, this implies that for any $\sigma \in G$, σ acts on V and we denote this action by $\sigma \cdot v$ for $v \in V$. I will show that for any v_1, v_2 in V there is a unique $\sigma \in G$ such that $\sigma \cdot v_1 = v_2$. Assuming that this is shown, we fix an element v of V. Note that we can find such an element with coefficients in k since we are assuming that k is algebraically closed. The map $\sigma \longrightarrow \sigma \cdot v$ is then an isomorphism of G onto V. This induces a map $\psi: R \longrightarrow k[G]$, which in turn gives the desired map $\psi: K \longrightarrow k(G)$

since K is the quotient field of R.

First we show that for any v_1 and v_2 in V there exists a σ in G such that $\sigma \cdot v_1 = v_2$. To do this it is enough to show that the Zariski closure of $G \cdot v_1$ is all of V (if we select v_1 such that the Zariski closure $\overline{G \cdot v_1}$ of $G \cdot v_1$ has minimal dimension, then $\overline{G \cdot v_1} - G \cdot v_1$ must be empty, so $V = G \cdot v_1$ for this v_1 and so for all $v_1 \in V$). To show that the Zariski closure of $G \cdot v_1 = V$, it is enough to show that the only G–invariant ideals of R are (0) and R. Let $I \neq 0$ be a G–invariant ideal of R. Since the generators of R satisfy homogeneous linear differential equations with coefficients in k, a nonconstructive version of Proposition 2.4 shows that the same is true for all elements in R. Therefore any element v of R lies in a G_C–invariant finite dimensional C–space W. If $v \in I$ then we can assume that $W \subset I$. Let $w_1, \ldots, w_m \in I$ be a basis of such a space. Since I is an ideal, $w = Wr(w_1, \ldots, w_m)$ is in I (we see this by expanding w using minors of the first row). Furthermore, for any $\sigma \in G_C$, $\sigma(w) = c_\sigma w$ for some $c_\sigma \in C$. Therefore, $w'/w \in k$. This means that $w \in E$, so $w^{-1} \in E \subset R$. Again, since I is an ideal, $1 = w \cdot w^{-1} \in I$, so $I = R$.

I will now show that there is at most one $\sigma \in G$ such that $\sigma \cdot v_1 = v_2$. To do this it is enough to show that for any $v \in V$ and $h \in G$ such that $h \cdot v = v$, we have $h = e$, the identity element of G. Let $v = (v_{1,1}, \ldots, v_{n,n}, \ldots)$ and let A be the $n \times n$ matrix $(v_{i,j})$ formed from the first n^2 entries of v. For any $h \in G$ there is an $n \times n$ matrix S such that the first n^2 entries of $h \cdot v$ are gotten from the entries of AS. Since

$Wr(y_1, \ldots, y_n)$ and $1/Wr(y_1, \ldots, y_n) \in R$, we have $\det(y_i^{(j)}) \cdot \det(y_i^{(j)})^{-1} = 1$. Since the a_{ij} satisfy all relations that the $y_i^{(j)}$ satisfy, we have $\det(A) \neq 0$. Since $AS = A$, we have $S =$ the identity matrix. S determines the action of h on V, so $h = e$.

We shall deduce many corollaries from Theorem 4.1.

Corollary 4.3. Let K be a P–V extension of k and assume Const(k) is algebraically closed. The transcendence degree of K over k equals the dimension of $G(K/k)^o$.

To see this, note that if we replace k by its algebraic closure $\tilde{k}$, we have that $K \cdot \tilde{k}$ is a P–V extension of $\tilde{k}$, $tr.deg._k(K) = tr.deg._{\tilde{k}}(K \cdot \tilde{k})$ and $G(K \cdot \tilde{k}/\tilde{k}) = G(K/k)^o$. Therefore we can assume that k is algebraically closed. Theorem 4.1 implies that $K = k(G)$ where $G = G(K/k)$. Since G is a C–closed set and C is algebraically closed, $tr.deg_k k(G) = tr.deg_C C(G) =$ dimension of G.

This result means that the dimension of G(K/k) measures the algebraic dependence among solutions $y_1, \ldots, y_n$ of a homogeneous linear differential equation and their derivatives. For example, one can show that the galois group of $y'' - xy = 0$ over $\mathbb{C}(x)$ is $SL(2,\mathbb{C})$. This implies that for $\{y_1, y_2\}$, a fundamental set of solutions, y_1, y_2, and y_1' are algebraically independent over $\mathbb{C}(x)$. Note that $y_1 y_2' - y_1' y_2 \in \mathbb{C}$.

Corollary 4.4. Let K be a P–V extension of k, an algebraically closed field with constants C, and $G = G(K/k)$.

(a) If $\rho: G \longrightarrow GL(m,C)$ is an irreducible polynomial representation of G then there exists a homogeneous linear differential equation $L(y) = y^{(m)} + a_{m-1}y^{(m-1)} + \ldots + a_0 y = 0$ with the $a_i \in k$ and a fundamental set of solutions $\{y_1, \ldots, y_m\}$ of $L(y) = 0$ in K such that the action of G on the C–span of $\{y_1, \ldots, y_m\}$ is isomorphic to ρ.

(b) If $G = C$, the additive group, then $K = k(y)$ for some $y \in K$ with $y' \in K$.

This corollary is just Proposition 3.2. To prove part (a), we first note that our assumptions imply that $K = k(G)$. Let $\varphi : C^n \longrightarrow C$ be a nonzero linear map. Define $\bar{\varphi} : C^n \longrightarrow k[G]$ by $(\bar{\varphi}(v))(g) = \varphi(\rho(g)v)$. We have $\rho_h^*(\bar{\varphi}(v)(g)) = \bar{\varphi}(v)(gh) = \varphi(\rho(gh)v) = \bar{\varphi}(\varphi(h)v)(g)$. This implies that the kernel of $\bar{\varphi}$ is an invariant subspace of C^n and so $\bar{\varphi}$ is injective. Therefore $\bar{\varphi}$ is an isomorphism of representations. Let V be the image of $\bar{\varphi}$ and let $y_1, \ldots, y_m$ be a basis of V. V is left invariant by G(K/k). Therefore the coefficients of $L(y) = Wr(y, y_1, \ldots, y_m)/Wr(y_1, \ldots, y_m)$ are in k.

To prove part (b), recall from example 4.1.2 that if $G = C$, then $k[G] = k[y]$ for some indeterminate y. For $\sigma \in G_C$, $\rho_\sigma^*(y) = y + c_\sigma$ for some c_σ in C. Therefore, $\sigma(y') = y'$ for all $\sigma \in G(K/k)$. The galois theory implies that $y' \in k$.

Corollary 4.5. Let K be a P–V extension of an algebraically closed field k and let $G = G(K/k)$. $y \in K$ satisfies a homogeneous linear differential equation with coefficients in k if and only if $y \in k[G]$.

Here we are implicitly using Theorem 4.1 to identify K with k(G). Corollary 4.5 appears in [BIA62]. To prove this result, I will first show that k[G] = {y ∈ k(G) | the orbit of y lies in a finite dimensional k–space}. Let k[G] = k[x_1, ... ,x_s]. Since for each g ∈ G, there exist c_{ij} in k such that $\rho^*_g(x_i) = \Sigma c_{ij}x_j$ it is easy to see that for any y ∈ k[G], the orbit of y lies in a finite dimensional space. Conversely, assume y ∈ k(G). We shall use the fact that k[G] consists precisely of those elements of k(G) that are defined everywhere on G, i.e. y ∈ k[G] if and only if for any g ∈ G, there exist u and v ∈ k[G] such that y = u/v and v(g) ≠ 0. Assume that the orbit of y lies in a finite dimensional space W. This implies that there is a proper Zariski closed subset H of G such that for g ∈ G −H, all elements of the orbit are defined at g (let H = zero set of the denominators of a basis of W). On the other hand if y ∉ k[G], then y is not defined at a point g ∈ G. This implies that for any h ∈ G, $\rho^*_{gh^{-1}}(y)$ is not defined at h. When h ∈ G −H, we get a contradiction, showing that y ∈ k[G].

Since G_C is dense in G, to prove the above result it is now enough to show that the set of y in k(G) that satisfy a homogeneous linear differential equation with coefficients in k is precisely the set of y such that the orbit of y under the action of the galois group spans a finite dimensional C–space. Clearly, if y satisfies such a linear differential equation L(y) = 0, then its orbit lies in the solution space of L(y) = 0 and so spans a finite dimension C–space. Conversely, if the orbit of y spans a finite dimensional space V, then V is left invariant by G(K/k). If y_1, ... ,y_n is a basis of V, L(y) = Wr(y,y_1, ... ,y_n)/Wr(y_1, ... ,y_n) has coefficients that are left fixed by G and so lie in k.

Corollary 4.6. Let K be a P–V extension of an algebraically closed field k with with galois group G = G(K/k). If H is a normal subgroup of G, the $H^\sim$ is a P–V extension of k with galois group G/H.

If H is normal in G, the theory of linear algebraic groups tells us that G/H is again a linear algebraic group ([HUM81], p.82). One can show that $H^\sim$ =k(G/H). k[G/H] = k[y_1, ... ,y_n] for some y_i. As noted above the G/H orbits of y_1, ... ,y_n lie in a finite dimensional vector space. If z_1, ... ,z_s form a basis of this space then $H^\sim$ is the P–V extension of k associated with L(y) = Wr(y, z_1, ... ,z_s)/ Wr(z_1, ... ,z_s).

Using the next corollary, I will give a proof of the fact that although sin x satisfies a linear differential equation over ℂ(x), 1/sin x does not.

Definition. Let k be an algebraically closed field a G a linear algebraic group. χ ∈ k[G] is a character if χ(g·h) = χ(g)χ(h) for all g,h ∈ G and χ(e) = 1.

Note that if χ is a character then χ(g) ≠ 0 for all g ∈ G. Conversely, it is known [ROS61], that if f ∈ k[G] and f(g) ≠ 0 for all g ∈ G, then f = a·ξ where ξ is a character and a ∈ k. The following originally appears [HASI85] and again in [SPER86] and [SING86].

Corollary 4.7. Let K be a P–V extension of an algebraically closed field k. If y_1 and y_2 ∈ K satisfy homogeneous linear differential equations over k and $y_1 \cdot y_2 = 1$, then $y_1'/y_1 = y_2'/y_2 \in k$.

We may write $K = k(G)$ where $G = G(K/k)$. Corollary 4.5 implies that $y_1, y_2 \in k[G]$. Since $y_1 \cdot y_2 = 1$, $y_1(g) \neq 0$ for all $g \in G$. Therefore, by the above remark, $g = a\chi(x)$ for some character $\chi(x) \in k[G]$ and $a \in k$. For any $\sigma \in G(K/k)$ $\sigma(y_1) = \sigma(a\chi) = a\chi(\rho_\sigma^*(x)) = a\chi(x)\chi(\sigma)$. Therefore $\sigma(y_1) = c_\sigma y_1$ for some $c_\sigma \in k$. I claim that c_σ is actually in Const(k). To see this let $L(y) = y^{(m)} + a_{m-1}y^{(m-1)} + \ldots + a_0 y$ be of minimal order such that $L(y_1) = 0$ and $a_i \in k$. Since $L(\sigma(y_1)) = 0$, y_1 also satisfies $a_\sigma y^{(m)} + (a_{m-1}a_\sigma + ma'_\sigma)y^{(m-1)} + \ldots = 0$. Therefore, $a_\sigma a_{m-1} = ma'_\sigma + a_{m-1}a_\sigma$. This implies that $a'_\sigma = 0$. Since $a_\sigma \in \text{Const}(k)$, $\sigma(y_1'/y_1) = y_1'/y_1 \in k$.

If $1/\sin x$ satisfied a homogeneous linear differential equation with coefficients in $\mathbb{C}(x)$, then $\sin x$ and $1/\sin x$ would lie in a P–V extension K of $\mathbb{C}(x)$. The above corollary implies that we could then conclude that $(\sin x)'/\sin x = \cot x$ would be algebraic over $\mathbb{C}(x)$. This is a contradiction since the only periodic functions algebraic over $\mathbb{C}(x)$ are constants.

5. Solving Homogeneous Linear Differential Equations in Terms of Linear Differential Equations of Lower Order.

In sections 2 and 3, I discussed the problems of solving homogeneous linear differential equations in terms of first and second order linear differential equations. I am now ready to discuss the general problem mentioned in the title.

Definition. Let k be a differential field with algebraically closed Const(k). We say that $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots a_0 y$ with $a_i \in k$ can be solved in terms of linear differential equations of lower order if the associated P–V extension K of k lies in a tower of fields $k = k_0 \subset \ldots \subset k_N$ where for each i, $k_i = k_{i-1}(t_i)$ where t_i is algebraic over k_{i-1} or satisfies $y^{(m)} + a_{i,m-1}y^{(m-1)} + \ldots + a_{i,0}y = 0$ for some $a_{i,j} \in k_{i-1}$ and $m < n$.

Let us look at some cases when this can happen. We may assume that k is algebraically closed and by replacing y by $ye^{\int a_{n-1}}$ if necessary assume that $L(y) = y^{(n)} + a_{n-2}y^{(n-2)} + \ldots + a_0 y$, i.e. no $y^{(n-1)}$ term appears in L(y). This does not effect the property of being solvable in terms of lower order linear differential equations. If $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions of $L(y) = 0$, then $L(y) = \text{Wr}(y, y_1, \ldots, y_n)/\text{Wr}(y_1, \ldots, y_n)$. Expanding this we see that $0 = a_{n-1} = W'/W$, where $W = \text{Wr}(y_1, \ldots, y_n)$. Therefore $W \in k$. Since $W = \sigma(W) = \det(\sigma)\, W$ for all $\sigma \in G(K/k)$, we have that $\det(\sigma) = 1$. Therefore $G = G(K/k) \subset SL(n,C)$ where $c = \text{Const}(k)$. Let V be the solution space of $L(y) = 0$ in K.

If G leaves a nontrivial subspace of V invariant, then Proposition 3.5 implies that $L(y) = L_{n-m}(L_m(y))$ for some linear operators of order lower than n. If $n \geq 3$, then this implies that $L(y) = 0$ is solvable in terms of lower order linear differential equations (the $n \geq 3$ requirement is due to the fact that finding solutions of $L(y) = 0$ from solutions of $L_{n-m}(y) = 0$ and $L_m(y) = 0$ requires us to

integrate a certain element. An integral satisfies a first order linear differential equation, but only a second order homogeneous linear differential equation).

Assume that G leaves no nontrivial subspace of V invariant, i.e. G acts irreducibly. From lie theory ([HUM72], p. 102),we know that such a subgroup of SL(n,C) is semisimple. This means ([HUM81],p. 167) that there exist normal Zariski closed simple subgroups H_i such that $G = H_1 \cdots H_s$ (simple means no normal subgroups of positive dimension). Let us assume for a moment that G is itself simple. If there exists a nontrivial representation $\rho: G \longrightarrow GL(m,C)$ with $m < n$, then C^m can be written as the direct sum of minimal invariant subspaces. Each of these yields a representation of smaller size so Proposition 3.2 implies that $L(y) = 0$ is solvable in terms of lower order linear differential equations. But it can happen that $L(y) = 0$ is solvable in terms of linear differential equations of lower order and that G is simple and has no nontrivial representations of dimension less than n. In example 0.3, the galois group of $y''' - 4xy' - 2y = 0$ is PSL(2,C). This has no nontrivial representations of dimension less than three, but this equation is clearly solvable in terms of lower order linear equations. Note that there exists a finite map φ: $SL(2,C) \longrightarrow PSL(2,C)$ and SL(2,C) has a two dimensional representation. In general, if G is simple and there exists a linear algebraic group H and homomorphism $\varphi: H \longrightarrow G$ with finite kernel, such that H has a nontrivial representation of dimension less than n, then $L(y) = 0$ is solvable in terms of lower order linear differential equations. To see this we write $K = k(G)$. k(H) can be thought of as a finite algebraic extension of k(G). One can show ([SING88]) that the derivation on k(G) can be extended to a derivation on k(H) such that H_C is the galois

group of k(H) over k. Furthermore, one can show that k(H) is a P–V extension of k. Since H has a representation of order less than n, it must have an irreducible representation of order less than n (note that H is also simple). Proposition 3.2 implies that k(H) is the P–V extension associated with a homogeneous linear differential equation of order less than n. Therefore $L(y) = 0$ is solvable in terms of linear differential equations of lower order.

We are therefore left with two cases. Either G is semisimple but not simple or G is simple and there does not exist a linear algebraic group H and a finite–to–one homomorphism $\varphi: H \longrightarrow G$ such that H has a representation of lower dimension. If the first case holds, then one can show that $G = H_1 \cdots H_s$, $s > 1$, and for each i, there is a linear algebraic group H_i' and a finite–to–one homomorphism $\varphi_i: H_i' \longrightarrow H_i$ such that H_i has a nontrivial irreducible representation of dimension less than n ([SAM69], p. 109). If we let $G_i = H_1 \cdots H_{i-1} H_{i+1} \cdots H_s$, then G_i is a normal subgroup of G and $G_i^{\sim}$ is a P–V extension with galois group G/G_i. This latter group is a quotient of H_i and so is simple. We have a map $\varphi_i': H_i' \longrightarrow G/G_i$ so by the discussion above $G_i^{\sim}$ is generated by solutions of a linear differential equation of order less than n. Therefore, $L(y) = 0$ is solvable in terms of linear differential equations of lower order.

The above discussion outlines a proof of half of the following (a complete proof is contained in [SING88]):

Theorem 5.1. Let k be a differential field with algebraically closed field of constants C and let $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y$

with $a_i \in k$. $L(y) = 0$ is NOT solvable in terms of linear differential equations of lower order if and only if the associated P–V extension has galois group G whose connected component G^o of the identity is

(i) simple, and

(ii) there does not exist a linear algebraic group H with finite–to–one homomorphism $\varphi: H \longrightarrow G^o$ such that H has a nontrivial representation of dimension less than n.

There is a cleaner statement of this result if one uses the language of lie algebras. Given a linear algebraic group G, one can associate to G a lie algebra g, the tangent space at the identity of G. There is a map $A \longmapsto \exp(A)$ sending g to a neighborhood of the identity. For example, the group SL(n,C) is associated with the lie algebra $sl(n,C) = \{n\times n \text{ matrices } A \mid tr(A) = 0\}$. Zariski closed connected normal subgroups of G correspond to ideals in g. Therefore simple groups have simple lie algebras. If $\varphi: H \longrightarrow G$ is a finite to one map then H and G have the same lie algebra. If $\rho: G \longrightarrow GL(n,C)$ is a rational representation then ρ induces a lie algebra homomorphism $\bar{\rho}: g \longrightarrow gl(n,C)$ = the lie algebra of all n×n matrices. Conversely, if g is simple and if $\bar{\rho}: g \longrightarrow gl(n,C)$ is a lie algebra homomorphism, then there exists a linear algebraic group H, a finite–to–one homomorphism $\varphi: H \longrightarrow GL(n,C)$ and a representation $\rho: H \longrightarrow GL(n,C)$ such that $\bar{\rho}$ is induced by ρ. Using this latter fact, we have:

Theorem 5.1 (bis). Let k be a differential field with algebraically closed field of constants C and let $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y$ with $a_i \in k$. $L(y) = 0$ is NOT solvable in terms of linear differential equations of lower order if and only if the associated P–V extension has galois group G such that G^o has a lie algebra g that is simple and such that if $\rho: g \longrightarrow gl(m,C)$ is a lie algebra homomorphism with $m < n$, the $\rho \equiv 0$.

For future reference, we list the simple lie algebras. There are the following infinite families:

(i) $sl(n) = \{ A \in gl(n,C) \mid tr(A) = 0 \}$ $n \geq 2$.

(ii) $sp(2n) = \{A \in gl(2n,C) \mid A^tJ + JA = 0\}$ $n \geq 2$, where $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$ and I_n is the identity matrix.

(iii) $o(n) = \{A \in gl(n,C) \mid A^t + A = 0\}$, $n \geq 7$.

There are 5 more exceptional simple lie algebras and these appear as algebras of n×n matrices for certain $n > 7$. We shall not need these later. In (iii) above, the condition that $n \geq 7$ is given because $o(2)$ is abelian, $o(3) \cong sl(2)$, $o(4) \cong sl(2) \oplus sl(2)$, $o(5) \cong sp(4)$ and $o(6) \cong sl(4)$.

6. Algebraic Relations Among Solutions of Homogeneous Linear Differential Equations.

In this section I shall assume that the reader is familiar with the definition of projective space $\mathbb{P}^n(C)$ and the basic properties of its Zariski closed subsets (see [HUM81], Ch. 1).

In 1883, Fuchs considered the following situation. Let $L(y) = 0$ be a homogeneous linear differential equation with coefficients in $\mathbb{C}(x)$. In a neighborhood $\mathcal{O}$ of any nonsingular point, there exist analytic

functions $y_1(x)$, $y_2(x)$, and $y_3(x)$ forming a fundamental set of solutions of $L(y) = 0$. The assignment $x \longmapsto (y_1(x), y_2(x), y_3(x))$ defines a map $Y: \mathcal{O} \longrightarrow \mathbb{P}^2(\mathbb{C})$. Fuchs showed

Theorem 6.1. If the image of Y lies on an algebraic curve in $\mathbb{P}^2(\mathbb{C})$, then either

(i) all solutions of $L(y) = 0$ are liouvillian over $\mathbb{C}(x)$, or

(ii) there is a second order linear differential equation $y'' + Py' + Qy = 0$, $P,Q \in \mathbb{C}(x)$, and linearly independent solutions z_1, z_2 such that $\{z_1^2, z_1z_2, z_2^2\}$ is a fundamental set of solutions of $L(y) = 0$.

Motivated by this result, Fano [FANO00] considered the following situation. Given $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0y = 0$ with $a_i \in \mathbb{C}(x)$, there exist functions $y_1(x), \ldots, y_n(x)$, analytic in the neighborhood $\mathcal{O}$ of a nonsingular point, such that $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions of $L(y) = 0$. We can define a function $Y(x) = (y_1(x), \ldots, y_n(x)) : \mathcal{O} \longrightarrow \mathbb{P}^{n-1}(\mathbb{C})$. He showed

Theorem 6.2. If the image of Y lies on an algebraic curve then either

(i) all solutions of $L(y) = 0$ are liouvillian over $\mathbb{C}(x)$, or

(ii) there is a second order linear differential equation $y'' + Py' + Qy = 0$, $P,Q, \in \mathbb{C}(x)$, and linearly independent solutions z_1, z_2 such that $\{z_1^{n-1}, z_1^{n-1}z_2, \ldots, z_2^{n-1}\}$ forms a fundamental set of solutions of $L(y) = 0$.

These results suggest that one could ask the following question: If the image of Y lies on a proper algebraic subset V of $\mathbb{P}^{n-1}(\mathbb{C})$, can $L(y) = 0$ be solved in terms of linear differential equations of lower order? Fano investigated in [FANO00] this question and showed that if $n = 3$, 4, or 5, then the answer is yes. He also got some positive partial results when $n = 6$. Furthermore, he was able to show that the answer was yes for all n if the dimension of V is 1 or 2 and partial positive results if the dimension of V is 3. In [SIN88], I showed that the answer is yes for all $n \leq 6$, but for all $n \geq 7$, there exists an n^{th} order homogeneous linear differential equation $L_n(y) = 0$ with coefficients in $\mathbb{C}(x)$ such that $L_n(y) = 0$ is not solvable in terms of linear differential equations of lower order and that for some fundamental set of solutions $\{y_1, \ldots, y_n\}$, we have $y_1^2 + \ldots + y_n^2 = 0$. Using the results of section 5, I will prove this below. Notice that we need only consider $n \geq 3$ since linearly independent solutions of a second order homogeneous linear differential equation can never satisfy a homogeneous equation $f(y_1,y_2) = 0$ with coefficients in $\mathbb{C}$.

Proposition 6.3. Let n be a positive integer ≤ 6. Let k be a differential field with algebraically closed field of constants C and let $L(y)$ be a homogeneous linear differential equation with coefficients in k. If $L(y) = 0$ is not solvable in terms of lower order linear differential equations, then for any fundamental set of solutions $\{y_1, \ldots, y_n\}$ and homogeneous polynomial $0 \neq P \in C[Y_1, \ldots, Y_n]$, we have $P(y_1, \ldots, y_n) \neq 0$.

Using Theorem 5.1 (bis), it is enough to show that, for $n \leq 6$, if

the lie algebra g of the connected component of the galois group G of the P–V extension associated with L(y) = 0 is (i) simple, and (ii) g has no nontrivial lie algebra representation of dimension less than n, then G leaves invariant no proper algebraic subset of $\mathbb{P}^{n-1}(\mathbb{C})$. We list below the lie algebras and corresponding groups satisfying (i) and (ii)

n	Lie Algebra	Group
3	$sl(3,\mathbb{C})$	SL(3,ℂ)
4	$sl(4,\mathbb{C})$,$sp(4,\mathbb{C})$	SL(4,ℂ),SP(4,ℂ)
5	$sl(5,\mathbb{C})$	SL(5,ℂ)
6	$sl(6,\mathbb{C})$,$sp(6,\mathbb{C})$	SL(6,ℂ),SP(6,ℂ)

SP(2n,ℂ) is the group on 2n×2n matrices satisfying $A^t\begin{bmatrix} 0 & J \\ -J & 0 \end{bmatrix}A = \begin{bmatrix} 0 & J \\ -J & 0 \end{bmatrix}$, where $J = \begin{bmatrix} & & 1 \\ & \cdot^{\cdot} & \\ 1 & & \end{bmatrix}$. It is well known ([JAC74], p.360 and p.374) that SL(n,ℂ) and SP(2n,ℂ) act transitively on $\mathbb{C}^n$ and $\mathbb{C}^{2n}$ respectively and so have no invariant algebraic subsets of $\mathbb{P}^{n-1}(\mathbb{C})$.

Notice that $o(n,\mathbb{C})$ does not appear on this list because the list stops before n = 7. $O(n,\mathbb{C}) = \{A \mid A^tA = I\}$ leaves the zero set of $Y_1^2 + \ldots + Y_n^2$ invariant. This observation is crucial to the following

Proposition 6.4. For all $n \geq 7$, there exists a homogeneous linear differential equation $L_n(y) = 0$ with coefficients in ℂ(x) such that $L_n(y)$ is not solvable in terms of lower order linear differential equations, but for some fundamental set of solutions $\{y_1, \ldots, y_n\}$ we have $y_1^2 + \ldots + y_n^2 = 0$.

The proof depends of a result from [TT79]: Given any linear algebraic group $G \subset GL(n,\mathbb{C})$, there is a homogeneous linear differential equation $\tilde{L}_n(y) = 0$ with coefficients in ℂ(x) such that the galois group of the associated P–V extension K is G. Therefore, there exist homogeneous linear differential equations $\tilde{L}(y) = 0$ with galois group $O(n,\mathbb{C})$. Let $\{z_1, \ldots, z_n\}$ be a fundamental set of solutions of such an equation such that $z_1^2 + \ldots + z_n^2$ is left fixed by G. For i = 1, ... ,n, let $y_i = u_1z_i + u_2z_i' + u_3z_i''$ with the u_i to be determined. $y_1^2 + \ldots + y_n^2 = Q(u_1,u_2,u_3)$ is a homogeneous quadratic form in u_1,u_2,u_3 whose coefficients are left fixed by G and so lie in ℂ(x). It is known ([GRE69], p.22) that this implies that there exist a_1, a_2, a_3, not all zero, in ℂ(x) such that $Q(a_1, a_2, a_3) = 0$. Replacing each u_j with a_j in all y_i, we get y_i in K. The y_i are linearly independent since if $\Sigma c_iy_i = 0$, we have $\sum_{j=1}^{3} a_j (\Sigma c_iz_i) = 0$, so $\tilde{L}(y) = 0$ and $a_3y'' + a_2y' + a_1y = 0$ have a space of common solutions. This space would be invariant under $O(n,\mathbb{C})$ and so must be {0}. This implies that each $c_i = 0$. Therefore the y_i satisfy the homogeneous linear differential equation $L(y) = Wr(y,y_1, \ldots ,y_n)/Wr(y_1, \ldots ,y_n) = 0$, which has coefficients in ℂ(x). Differentiating the relations $y_i = a_1z_i + a_2z_i' + a_3z_i''$ n–1 times allows one to conclude that $(y_i^{(j)}) = A \cdot (z_i^{(j)})$ where A is an n×n matrix with coefficients in ℂ(x). Since the matrices $(y_i^{(j)})$ and $(z_i^{(j)})$ are invertible, A is invertible. Therefore, $\mathbb{C}(x)\langle y_1, \ldots ,y_n\rangle = \mathbb{C}(x)\langle z_1, \ldots ,z_n\rangle$, and L(y) = 0 has the desired properties.

REFERENCES

[BADW79] F. Baldassarri, B. Dwork, On second order linear differential equations with algebraic solutions, Amer. J. Math., 101, 1979.

[BBH88] F. Beukers, W.D. Brownawell, G. Heckman, Siegel Normality, to appear in Annals of Math.

[BEHE87] F. Beukers, G. Heckman, Monodromy for the Hypergeometric Function ${}_nF_{n-1}$, University of Utrecht Preprint No. 483, 1987.

[BIA62] A. Bialynicki–Birula, On Galois theory of fields with operators, Am. J. Math., 84, 1962.

[BOU98] A. Boulanger, Contributions à l'étude des équations différentielles linéaires homogènes intégrables algébriquement, J. de l'Ecole Poly., 2^e Ser. 4, 1898.

[DAV84] J. H. Davenport, A Liouville principle for linear differential equations, to appear in Proc. Journees equations differentielles dans les champs complex, 1984.

[DAV85] J. H. Davenport, Closed form solutions of ordinary differential equations, Second RIKEN International Symposium on Symbolic and Algebraic Computation by Computers, World Scientific Publ., 1985

[DASI86] J. H. Davenport, M. F. Singer, Elementary and liouvillian solutions of linear differential equations, J. Symb. Comp., 2, 1986.

[DEL70] P. Deligne, Equations différentielles à points singuliers reguliers, Lecture Notes in Mathematics 163, Springer Verlag, Berlin–Heidelberg–New York, 1970.

[DUMI88] A. Duval, C. Mitschi, Matrices de Stokes et groupe de Galois des équations hypergéométriques confluentes generalisées, Publ. de l'IRMA, Univ. de Strasbourg, 1988.

[FANO00] G. Fano, Ueber lineare Differentialgleichungen mit algebraischen Relationen Zwischen den Fundamentalloesungen, Math. Ann., 53, 1900.

[GRE69] M. J. Greenberg, Lectures on Forms in Many Variables, W.A. Benjamin, New York, 1969.

[GRI88] D. Yu. Grigor'ev, Complexity of factoring and calculating the GCD of linear ordinary differential operators, preprint, 1988.

{HASI85] W.A. Harris, Y. Sibuya, The reciprocals of solutions of linear ordinary differential equations, Adv. in Math., 85, 1985.

[HUM72] J. E. Humphreys, Introduction to Lie Algebras and Representation Theory, Springer–Verlag, New York, 1976.

[HUM81] J. E. Humphreys, Linear Algebraic Groups, Springer–Verlag, New York, 1981.

[JAC74] N. Jacobson, Basic Algebra I, W.H. Freeman, San Fransisco, 1974.

[KAP57] I. Kaplansky, An Introduction to Differential Algebra, Hermann, Paris 1957.

[KATZ82] N. M. Katz, A conjecture in the arithmetic theory of differential equations, Bull. Soc. Math. Fr., 110, 1982.

[KATZ87a] N. M. Katz, On the calculation of some differential galois groups, Inventiones Math., 87, 1987.

[KATZ87b] N. M. Katz, On the monodromy groups attached to certain families of exponential sums, Duke Math. J. 54, No.1, 1987.

[KAPI87] N. M. Katz, R. Pink, A note on Pseudo–CM representations and differential galois groups, Duke Math. J., 54, No. 1, 1987.

[KOL73] E. R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.

[KOLA58] E. R. Kolchin, S. Lang, Algebraic groups and the galois theory of differential fields, Am. J. Math., 80, 1958.

[KOV86] J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, J. Symb. Comp., 2, No. 1, 1986.

[MAR98] F. Marotte, Les equations differentielles lineaires et la theorie des groupes, Ann. Fac. Sci. Univ. Toulouse (1), 12, 1898.

[RAM85a] J. P. Ramis, Phenomene de Stokes et filtration Gevrey sur le groupe de Picard–Vessiot, C. R. Acad. Sci. Paris, 301, Ser. 1, No. 5, 1985.

[RAM85b] J. P. Ramis, Filtration Gevrey sur le group de Picard–Vessiot d'une equation differentielle irreguliere, Informes de matematica, IMPA, Serie a–045/85, 1985.

[ROS61] M. Rosenlicht, Toroidal algebraic groups, Proc. Amer. Math. Soc., 12, 1961.

[ROS80] M. Rosenlicht, Initial results in the theory of linear algebraic groups, in Studies in Algebraic Geometry, A. Seidenberg, ed., MAA Studies in Math., 20, 1980.

[SAM69] H. Samelson, Notes on Lie Algebras, Van Nostrand Reinhold, New York, 1969.

[SCH95] L. Schlesinger, Handbuch der Theorie der linearen Differentialgleichungen, Teubner, Leipzig, 1895.

[SING80] M.F. Singer, Algebraic solutions of n^{th} order linear differential equations, Proc. 1979 Queens Conference on Number Theory, Queens Papers in Pure and Applied Math., 54, 1980.

[SING81] M. F. Singer, Liouvillian solutions of n^{th} order linear differential equations, Amer. J. Math., 103, 1981.

[SING85] M. F. Singer, Solving homogeneous linear differential equations in terms of second order linear differential equations, Amer. J. Math, 107, 1985.

[SING86] M. F. Singer, Algebraic relations among solutions of linear differential equations, Trans. Am. Math. Soc., 295, 1986.

[SING88a] M. F. Singer, Algebraic relations among solutions of linear differential equations: Fano's Theorem. Amer. J. Math., 110, 1988.

[SING88b] M. F. Singer, Liouvillian solutions of linear differential equations with liouvillian coefficients, preprint, 1988.

[SPER86] S. Sperber, On solutions of differential equations which satisfy certain algebraic relations, Pac. J. of Math., 124, 1986.

[SPR81] T. A. Springer, Linear Algebraic Groups, Birkhaeuser, Boston/Basel/Stuttgart, 1981.

[TOU87] E. Tournier, Solutions formelles d'équations différentielles, These pour Docteur d'Etat, Grenoble, 1987.

[TT79] C. Tretkoff, M. Tretkoff, Solution of the inverse problem of differential galois theory in the classical case, Am. J. Math., 101, 1979.