Communications in Algebra®, 33: 3651–3677, 2005

ISSN: 0092-7872 print/1532-4125 online
DOI: 10.1080/00927870500243304

ON THE CONSTRUCTIVE INVERSE PROBLEM IN DIFFERENTIAL GALOIS THEORY#

William J. Cook
Department of Mathematics, North Carolina State University, Raleigh, USA

Claude Mitschi
Institut de Recherche Mathématique Avancée, Université Louis Pasteur, Strasbourg, France

Michael F. Singer
Department of Mathematics, North Carolina State University, Raleigh, USA

We give sufficient conditions for a differential equation to have a given semisimple group as its Galois group. For any group G with $G^0 = G_1 \cdot \cdots \cdot G_r$, where each G_i is a simple group of type A_ℓ, C_ℓ, D_ℓ, E_6, or E_7, we construct a differential equation over $C(x)$ having Galois group G.

Key Words: Galois theory; Inverse problem; Linear differential equations; Picard-Vessiot.

(2000) Mathematics Subject Classification: Primary 34M50; Secondary 12H05, 12H20.

1. INTRODUCTION

In Singer (1993) a large class of linear algebraic groups, including all groups with semisimple identity component, are shown to occur as Galois groups of differential equations $\frac{dY}{dx} = AY$ with A an $n \times n$ matrix with coefficients in $C(x)$, where C is an algebraically closed field of characteristic zero. The proof of this depended heavily on the analytic solution of the Riemann-Hilbert Problem and did not directly give a way of constructing such an equation[1]. Techniques for constructing an equation with a given group have been produced for connected solvable groups by Kovacic (1969, 1971) and for connected groups in general by Mitschi and Singer (1996). For groups that are not connected, Mitschi and Singer (2002) showed that one could construct equations having any solvable-by-finite

Received March 22, 2004; Revised March 22, 2005
#Communicated by R. Piene.
Address correspondence to Michael F. Singer, North Carolina State University, Department of Mathematics, Box 8205, Raleigh, North Carolina 27695-8205, USA; E-mail: singer@math.ncsu.edu

[1]Once one knows that a group G occurs as a differential Galois group over $C(x)$ for C a recursive algebraically closed field of characteristic 0, one can produce an equation with Galois group G by listing all equations and using the algorithm from Hrushovski (2002) to calculate an equation's Galois group to test until one is found. In this article, we are interested in more direct methods.

group as Galois group assuming one could produce (algebraic) equations having any finite group as Galois group. Hartmann (2002) has shown that any linear algebraic group can be realized as the Galois group of a linear differential equation over $C(x)$ and this proof shows that equations can be constructed once one knows how to construct equations for reductive groups (the proof uses the results of Singer, 1993 in this case as well).

In this article, we will give a criterion, Proposition 3.2, for a differential equation to have a given semisimple algebraic group as a Galois group. We will use this proposition to show how one can construct differential equations with Galois group G, where $G = H \ltimes G^0$, H finite and $G^0 = G_1 \cdot \cdots \cdot G_r$ with each G_i of type A_ℓ, C_ℓ, D_ℓ, E_6, or E_7. The rest of the article is organized as follows. In Section 2, we discuss the criteria given by Mitschi and Singer (2002) and by Hrushovski (2002), that allow one to reduce the inverse problem for arbitrary linear algebraic groups over $C(x)$ to finding *equivariant* differential equations with given connected Galois groups over an arbitrary finite Galois extension K of $C(x)$. In Section 3, we develop the necessary group theory and give criteria for a differential equation to have a given semisimple group as its Galois group. In Section 4, we produce equations for the groups described above. In Section 5, we describe an alternate construction for groups of the form $W \ltimes SL_2$, W a finite group.

2. EQUIVARIANT EQUATIONS

Mitschi and Singer (2002) and Hartmann (2002), have shown how to reduce the inverse problem for general groups to the inverse problem for groups of the form $H \ltimes G^0$, where H is a finite group and G^0 is a connected group defined over C. We shall assume that we are given a finite extension K of $C(x)$ with Galois group H and we wish to find a Picard-Vessiot extension E of $C(x)$ containing K with Galois group $H \ltimes G^0$ such that the Galois action of $H \ltimes G^0$ on K factors through the given action of H on K. To attack this problem, the authors introduced the notion of an equivariant equation, which we now review.

Let K be a finite Galois extension of $C(x)$ with Galois group H and let V be a vector space over C that is also a right H-module. Notice that this gives a right action of H on $V(K) = K \otimes V$ given by $f \otimes v \mapsto f \otimes v \cdot h$ for $h \in H$, $f \in K$ and $v \in V$. We will again denote this action by $w \mapsto wh$ for $h \in H$ and $w \in V(K)$. The group H can be seen to also act on the left on $V(K)$ *via* an action defined by $h(f \otimes v) = hf \otimes v$ for $f \in K$ and $v \in V$. We say that an element $w \in V(K)$ is *equivariant* if $hw = wh$ for all $h \in H$ (Hartmann, 2002, Definition 3.5; Mitschi and Singer, 2002, Definition 6.1).

Let us now consider a semidirect product $G = H \ltimes G^0$ of the finite group H and a connected linear algebraic group G^0 (defined over C) with multiplication given by $(h_1, g_1)(h_2, g_2) = (h_1 h_2, h_2^{-1} g_1 h_2 g_2)$. Let $\mathcal{G}$ be the Lie algebra of G^0. For any $h \in H$ the map $g \mapsto h^{-1}gh$ from G^0 to G^0 can be lifted to a map of $\mathcal{G}$ to $\mathcal{G}$, which we shall also denote by $A \mapsto h^{-1}Ah$. In this way, we may consider $\mathcal{G}$ as a *right* H-module. With this convention, we may speak of equivariant elements of $\mathcal{G}(K)$. In concrete terms, an element $A \in \mathcal{G}(K)$ is equivariant if, for any $h \in H$, the result of applying h (as an element of the Galois group of K) to the entries of A is the same as conjugating A by h^{-1}. We will say that a differential equation $Y' = AY$ is equivariant if $A \in \mathcal{G}(K)$ is equivariant. We will use throughout the article, the notation Y' for ∂Y, where ∂ is the unique extension of d/dx on K. Using this notion of equivariance, we have the following criterion (Hartmann, 2002, Proposition 3.10; Mitschi and Singer, 2002, Proposition 6.3).

Proposition 2.1. *Let G and K be as above and let A be an equivariant element of $\mathcal{G}(K)$ such that the Picard-Vessiot extension E of K corresponding to the equation $Y' = AY$ has Galois group G^0. Then E is a Picard-Vessiot extension of $C(x)$ with Galois group G.*

To apply this result, we will need ways of constructing equivariant elements A of $\mathcal{G}(K)$ and criteria to ensure that the equation $Y' = AY$ has the desired Galois group over K. The remainder of this section is devoted to the first task, and the next sections to the second task. In the following, we shall think of C as embedded in the complex numbers and denote by $C\{t\}$ the subring of convergent power series of $C[[t]]$, by $C(\{t\})$ its quotient field, and by $\mathbf{P}^1$ the projective line $\mathbf{P}^1(C)$.

Lemma 2.2. *Let $\pi : \mathbf{C} \to \mathbf{P}^1$ be a covering of the projective line by a curve $\mathbf{C}$ with function field K, such that $C(x) \subset K$ is induced by π. There exists a computable set of points $\mathcal{S} \subset \mathbf{P}^1$ such that the following is true: Given*

1. *an integer M,*
2. *points $p_1, \ldots p_r \in \mathbf{C}$ with $\pi(p_i) \notin \mathcal{S}$ and $\pi(p_i) \neq \pi(p_j)$ for $i \neq j$,*
3. *local parameters t_i at p_i and*
4. *elements $A_1, \ldots, A_r \in \mathcal{G}(C)$,*

there exists an equivariant $A \in \mathcal{G}(K)$ such that at each p_i, we have

$$A = A_i t^M + t^{M+1}(B_i(t)),$$

where $t = t_i$ and $B_i(t) \in \mathcal{G}(C\{t\})$.

Proof. We can consider $\mathcal{G}(C)$ as a *left* H-module under the action $v \mapsto hvh^{-1}$ for any $h \in H$. We define an action of H on $\mathcal{G}(K)$ by the formula $h(f \otimes v) = h(f) \otimes hvh^{-1}$ for $f \in K$, $v \in \mathcal{G}(C)$ and $h \in H$. This action satisfies $h(aw) = h(a)h(w)$ for all $h \in H$, $a \in K$, $w \in \mathcal{G}(K)$ and so, by a result of Kolchin and Lang (Lang, 1993, see Exercises 31 and 32, p. 550), one can construct an invariant basis of $\mathcal{G}(K)$ over K, that is, a basis $\tilde{e}_1, \ldots, \tilde{e}_s$ such that $h(\tilde{e}_i) = \tilde{e}_i$ for $i = 1, \ldots, s$ and for all $h \in H$. This basis is an equivariant basis in the above sense, that is, $h\tilde{e}_i = \tilde{e}_i h$ for all $h \in H$. Fix a basis $e_1, \ldots, e_s$ of $\mathcal{G}(C)$ and define $B \in \mathrm{GL}_s(K)$ such that $(\tilde{e}_1, \ldots, \tilde{e}_s) = (e_1, \ldots, e_s)B$. For any $f_1, \ldots, f_s \in C(x)$, $\sum_{i=1}^s f_i \tilde{e}_i$ is an equivariant element of $\mathcal{G}(K)$. We shall now show how one can select the f_i so that the conclusions of the lemma are satisfied. Let $\mathcal{S}$ be the image under π of those points $p \in \mathbf{C}$ satisfying at least one of the following conditions:

1. p is a singular point of $\mathbf{C}$ or is a ramification point of π, or
2. p is a pole of an entry of B, or
3. $\{\tilde{e}_1(p), \ldots, \tilde{e}_s(p)\}$ fails to be a basis of $\mathcal{G}(C)$, *i.e.*, $\det(B(p)) = 0$.

Note that condition 1. implies that we may select $t = x - \pi(p)$ to be a local coordinate for any point p with $\pi(p) \notin \mathcal{S}$, if $\pi(p)$ is finite, and $t = 1/x$ if $\pi(p)$ is infinite. We shall use these local coordinates. From conditions 1, 2, and 3, above, we see that at each p_i with $\pi(p_i) \notin \mathcal{S}$, there exist coefficients $c_{i,j} \in C$ such that $A_i = \sum_{j=1}^{s} c_{i,j}\tilde{e}_j(p_i)$. Let $f_j \in C(x)$ satisfy $f_j = c_{i,j}t^M + t^{M+1}b_{i,j}$, where $b_{i,j} \in C\{t\}$, when written in local coordinates $t = t_j$ at the point p_j. We then have that $A = \sum_{j=1}^{s} f_j\tilde{e}_j$ satisfies the conclusion of the lemma. □

Corollary 2.3. *Let $\pi : \mathbf{C} \to \mathbf{P}^1$ be a covering of the projective line by a curve $\mathbf{C}$ with function field K such that $C(x) \subset K$ is induced by π. There exists a computable set of points $S \subset \mathbf{P}^1$ such that the following is true:*

Given

1. *integers $M < N$,*
2. *points $p_1, \dots p_r \in \mathbf{C}$ with $\pi(p_i) \notin \mathcal{S}$ and $\pi(p_i) \neq \pi(p_j)$ for $i \neq j$,*
3. *local parameters t_i at p_i and*
4. *for each $i = 1, \dots, r$ elements $A_{i,M}, \dots, A_{i,N} \in \mathcal{G}(C)$,*

there exists an equivariant $A \in \mathcal{G}(K)$ such that at each p_i, we have

$$A = A_{i,M}t^M + \cdots + A_{i,N}t^N + t^{N+1}(B_i(t)),$$

where $t = t_i$ and $B_i(t) \in \mathcal{G}(C\{t\})$.

Proof. Let $\mathcal{S}$ be as before. We will proceed by induction on $N - M$. Assume that we have found an equivariant $A_0 \in \mathcal{G}(K)$ such that at each p_i, we have

$$A_0 = A_{i,M}t^M + \cdots + A_{i,N-1}t^{N-1} + t^N(B_i(t)),$$

where $t = t_i$ and $B_i(t) \in \mathcal{G}(C\{t\})$. Let C_i be the coefficient of t^N in the expansion of A_0 at p_i. Using Lemma 2.2, we can find an equivariant $\widetilde{A} \in \mathcal{G}(K)$ such that

$$\widetilde{A} = (A_{i,N} - C_i)t^N + t^{N+1}(\widetilde{B}_i(t)),$$

where $t = t_i$ and $\widetilde{B}_i(t) \in \mathcal{G}(C\{t\})$. The element $A = A_0 + \widetilde{A}$ satisfies the conclusion of the corollary. □

Example 2.4. The group $\mathbb{Z}/2\mathbb{Z} \ltimes \mathrm{SL}_2$.

We shall illustrate the above results for this group where $h = -1 \in \mathbb{Z}/2\mathbb{Z}$ acts on SL_2 by sending a matrix to the transpose of its inverse. Note that the action of this element on $\mathfrak{sl}_2$ sends a matrix to the negative of its transpose. Let $K = C(x, \sqrt{x})$ with Galois group $H \simeq \mathbb{Z}/2\mathbb{Z}$. The elements

$$\tilde{e}_1 = \begin{pmatrix} \sqrt{x} & 0 \\ 0 & -\sqrt{x} \end{pmatrix},$$

$$\tilde{e}_2 = \begin{pmatrix} 0 & \sqrt{x} \\ \sqrt{x} & 0 \end{pmatrix}, \quad \text{and}$$

$$\tilde{e}_3 = \begin{pmatrix} 0 & -1 + \sqrt{x} \\ 1 + \sqrt{x} & 0 \end{pmatrix}$$

form an equivariant basis of $\mathfrak{sl}_2(K)$. We will now construct an equivariant element A of $\mathcal{G}(K)$ with the following prescribed principal parts at the points $(4, 2)$, $(9, 3)$ and $(16, 4)$ of the curve $y^2 - x = 0$ (we will see in Section 4 that the equation $Y' = AY$ is then an equivariant equation with Galois group SL_2 over K).

$$\text{At } p_0 = (4, 2), \text{ with } t = x - 4, \ A = \frac{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}{t^2} + \frac{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}{t} \text{ (terms involving } t^j, j \geq 0).$$

$$\text{At } p_1 = (9, 3), \text{ with } t = x - 9, \ A = \frac{\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}}{t} + \text{terms involving } t^j, j \geq 0.$$

$$\text{At } p_2 = (16, 4), \text{ with } t = x - 16, \ A = \frac{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}{t} + \text{terms involving } t^j, j \geq 0.$$

A calculation shows that the following rational functions f_i yield the desired result for $A := f_1\tilde{e}_1 + f_2\tilde{e}_2 + f_3\tilde{e}_3$:

$$f_1 = -\frac{\sqrt{2}}{105}\frac{(x-4)(x-16)}{x-9}$$

$$f_2 = -\frac{1}{240}\frac{(x-9)(x-16)}{(x-4)^2} + \frac{311}{28800}\frac{(x-9)(x-16)}{x-4} - \frac{3}{672}\frac{(x-9)(x-4)}{x-16}$$

$$f_3 = \frac{1}{120}\frac{(x-9)(x-16)}{(x-4)^2} - \frac{43}{7200}\frac{(x-9)(x-16)}{x-4} + \frac{1}{168}\frac{(x-9)(x-4)}{x-16}.$$

□

3. GROUP THEORY AND ITS DIFFERENTIAL CONSEQUENCES

Throughout this section, H stands for any (not necessarily finite) subgroup of a given linear algebraic group G. In what follows, we shall show that for certain algebraic groups H defined over C, we can construct a differential equation, defined over $C(x)$ such that the Galois group of this equation over $\mathbb{C}(x)$ is $H(\mathbb{C})$. By Theorem 2, Section VI.3, of Kolchin (1973) this will imply that the Galois group of the equation over $C(x)$ is $H(C)$.

The principal tool that we shall use is the following result:

Lemma 3.1. *Let $G \subset \mathrm{GL}_n(C)$ be a connected semisimple algebraic group of rank ℓ with Lie algebra $\mathcal{G}$, and let $\mathrm{Ad} : G \to \mathrm{GL}(\mathcal{G})$ be the adjoint representation. Let H be an algebraic subgroup of G and assume:*

1. *H acts reductively on $\mathcal{G}$ via the adjoint representation,*
2. *H contains an element having at least ℓ multiplicatively independent eigenvalues,*
3. *H contains an element u such that $\mathrm{Ad}(u)$ is a unipotent element with an ℓ dimensional eigenspace corresponding to the eigenvalue 1.*

Then $H = G$.

Proof. Let $\mathcal{H}$ be the Lie algebra of H. It is enough to show that $\mathcal{H} = \mathcal{G}$. To do this we will use the following (see Bourbaki, 1990, Exercise 5, p. 246). *If $\mathcal{G}$ is a semisimple*

Lie algebra and $\mathcal{H}$ is a subalgebra acting reductively on $\mathcal{G}$ via the adjoint representation, of the same rank as $\mathcal{G}$, and containing a principal $\mathfrak{sl}_2$-triple of $\mathcal{G}$, then $\mathcal{G} = \mathcal{H}$. We shall show that each of the conditions of the lemma implies the corresponding condition of this latter result.

If H acts reductively on $\mathcal{G}$ then so does $\mathcal{H}$.

Let h be an element of H having ℓ multiplicatively independent eigenvalues. Then h^i has the same property for all $i > 0$, so we may assume that $h \in H^0$. We may write $h = h_s h_u$, where h_s and h_u are the semisimple and unipotent parts of h, respectively. Since the eigenvalues of h and h_s coincide and $h_s \in H^0$, we may assume that h is semisimple and that h lies in some maximal torus T of H. We may assume that T is a subgroup of diagonal matrices and that the ℓ multiplicatively independent eigenvalues of h are the first ℓ entries on the diagonal of h. If χ_i denotes the character that picks out the i^{th} element on the diagonal, we see that no nontrivial power product of $\chi_1, \ldots, \chi_\ell$ is trivial on h. Therefore, $\chi_1, \ldots, \chi_\ell$ are multiplicatively independent on T, and so the dimension of T is greater than or equal to ℓ, that is, the rank of $\mathcal{H}$ is ℓ.

Let $u \in H$ satisfy the property that $\mathrm{Ad}(u)$ is unipotent with an ℓ-dimensional eigenspace corresponding to the eigenvalue 1. Since $\mathrm{Ad}(u) = \mathrm{Ad}(u_s)\mathrm{Ad}(u_u)$, where u_s and u_u are semisimple and unipotent, we have $\mathrm{Ad}(u_s) = 1$ and we can replace u with u_u and assume that u is unipotent. If we let $n = \log(u)$ we have that $\{\exp(an) \mid a \in C\}$ is the unique smallest closed subgroup of H containing u and that $n \in \mathcal{H}$ (see Lemma C, p. 96 and Exercise 11, p. 101 of Humphreys, 1975). This implies that $\mathrm{ad}(n) = \log(\mathrm{Ad}(u))$ and so a calculation implies that the dimension of the nulspace of $\mathrm{ad}(n)$ is ℓ. Since n is nilpotent, the Jacobson-Morozov Theorem (see Bourbaki, 1990, p. 162) implies that n is contained in an $\mathfrak{sl}_2$-triple in $\mathcal{H}$ and, furthermore, this triple is principal in SL_n (*loc. cit.*, p. 166). □

The above lemma gives us the following criterion to ensure that a differential equation has a given semisimple group as its Galois group.

Proposition 3.2. *Let $G \subset \mathrm{GL}_n(C)$ be a connected semisimple linear algebraic group of rank ℓ with Lie algebra $\mathcal{G}$ and $\mathbf{C}$ a curve with function field $K \supset C(x)$. Let $Y' = AY$ be a differential equation with $A \in \mathcal{G}(K)$. Let $H \subset \mathrm{GL}_n(C)$ be the Galois group of $Y' = AY$ over K with respect to a given fundamental solution $y \in G(K)$, and assume that*

1. *H is reductive.*
2. *There exists a point $p_1 \in C$ such that in terms of some local coordinate t at p_1, we can expand $Y' = AY$ as*

$$\frac{dY}{dt} = \left(\frac{A_1}{t} + B_1(t)\right)Y,$$

where A_1 is semisimple and has ℓ eigenvalues that are $\mathbb{Z}$-independent mod $\mathbb{Z}$ and $B_1(t) \in C\{t\}$.

3. *There exists a point $p_2 \in C$ such that in terms of some local coordinate t at p_2, we can expand $Y' = AY$ as*

$$\frac{dY}{dt} = \left(\frac{A_2}{t} + B_2(t)\right)Y,$$

where A_2 is nilpotent and $\mathrm{ad}(A_2)$ *has a kernel in* $\mathcal{G}$ *of dimension* ℓ, *and* $B_2(t) \in C\{t\}$. *Then* $H = G$.

Proof. We know by Proposition 2.1 of Mitschi and Singer (2002) that H is an algebraic subgroup of G. We shall show that it satisfies the hypotheses of Lemma 3.1. Clearly, hypothesis 1 is satisfied.

To see that hypothesis 2 of Lemma 3.1 is satisfied, note that the present hypothesis 2 implies that the distinct eigenvalues of A_1 do not differ by integers. This implies that the equation $Y' = AY$ is equivalent (over $C((t))$ and even $C(\{t\})$) to the equation $Y' = (A_1/t)Y$ whose monodromy matrix at p_1 is $e^{2\pi i A_1}$ (see Section 3 of Babbitt and Varadarajan, 1983, or Sections 3.3. and 5.1.1 of van der Put and Singer, 2003). Note that $e^{2\pi i A_1}$ has at least ℓ multiplicatively independent eigenvalues and that this element belongs to H. Since K-equivalent differential equations have conjugate Galois groups, there exists an element h of H which is conjugate (in $\mathrm{GL}_n(C)$) to $e^{2\pi i A_1}$, and hence satisfies hypothesis 2 of Lemma 3.1.

To verify hypothesis 3, we must argue in a more careful way. For this we use the results of Section 8 of Babbitt and Varadarajan (1983). Since $\mathrm{ad}(A_2)$ is nilpotent, the spectral subspaces $\mathbf{g}_\lambda$ of $\mathrm{ad}(A_2)$ corresponding to all positive integers λ are zero (*loc. cit.,* Section 8.5). Therefore, Proposition 8.5 and Theorem 9.5 of Babbitt and Varadarajan (1983) imply that there exists $g \in G(C\{t\})$ such that the gauge transform of $Y' = AY$ by $Y = gZ$ is $Z' = (A_2/t)Z$, and that A_2 lies in $\mathcal{G}$. We note that $Z' = (A_2/t)Z$ has a fundamental solution matrix of the form $z_0 = e^{A_2 \log t}$ and that z_0 is an element of $G \subset \mathrm{GL}_n$ since $A_2 \in \mathcal{G}(C)$. We therefore have $y = gz_0\gamma$, where γ is a constant matrix belonging to G since y, g, z_0 all are elements of G. The monodromy matrix at p_2 with respect to y is $u = \gamma^{-1}e^{2\pi i A_2}\gamma$. It is an element of the local Galois group of $Y' = AY$ over $C(\{t\})$, hence of the global Galois group H over K with respect to y. Since $\gamma \in G(C)$, the matrices $\mathrm{Ad}(u)$ and $\mathrm{Ad}(e^{2\pi i A_2})$ are conjugate in $\mathrm{GL}(\mathcal{G})$, which implies that $Ad(u)$ has the desired property. □

From Section 2 it is clear that we should have no trouble fulfilling hypotheses 2 and 3 of Proposition 3.2. The difficulty arises in trying to ensure that hypothesis 1 is satisfied. We shall use local properties of the differential equation. As a first step, we will derive a condition on the behavior of a differential equation at *one* singular point to ensure that the Galois group is reductive. We will see that this will only work for SL_n and Sp_n. We will then give a more general criterion that involves the local behavior at several points and this will apply to a larger class of groups.

Before we describe criteria in terms of local properties of the differential equation that ensure that hypothesis 1 of Proposition 3.2 is satisfied, we will recall the facts we need relating the local Galois groups and the global Galois group.

Let $\pi : \mathbf{C} \to \mathbf{P}^1$ be a non-singular curve over the projective line and $C(x) \subset K$ the corresponding inclusion of function fields. Let $p \in \mathbf{C}$ and assume that $\mathbf{C}$ is not ramified at p and that $\pi(p) \neq \infty$. What follows can be developed without these assumptions but they simplify the exposition and will hold in our applications. We can embed K into $C((t))$, $t = x - \pi(p)$, by expanding each element of K as a series in t. We shall identify K with its image and write $K \subset C((t))$. In fact, we have that $K \subset C(\{t\}) \subset C((t))$. Any differential equation $Y' = AY$, $A \in \mathfrak{gl}_n(K)$ can be considered as a differential equation over $C((t))$ and so we can form a Picard-Vessiot extension E of $C((t))$ corresponding to this equation. Let y be a fundamental solution of $Y' = AY$ having entries in E, and let $K(y)$ and $C(\{t\})(y)$ denote the fields generated by the entries of y over K and $C(\{t\})$ respectively. We see that $K(y)$ and $C(\{t\})(y)$ are Picard-Vessiot extensions for $Y' = AY$ over K and $C(\{t\})$ respectively. We denote by G, G_{conv} and G_{form} the Galois groups of $K(y)$ over K, of $C(\{t\})(y)$ over $C(\{t\})$ and of E over $C((t))$ respectively. One easily checks that there are natural injections $G_{form} \hookrightarrow G_{conv} \hookrightarrow G$ and that the actions of the former two groups on the solution space of the differential equation coincide with their actions as embedded subgroups of G. These considerations lead to.

Lemma 3.3. *Let $\mathbf{C}$ be a curve with function field $K \supset C(x)$ and let $Y' = AY$ be a differential equation with coefficients in K. If there exists a point $p \in \mathbf{C}$ as above such that the equation is irreducible over $C(\{t\})$, then it is irreducible over K and its Galois group G is reductive. In particular, if it is irreducible over $C((t))$, then G is reductive.*

Proof. A differential equation is irreducible over a differential field with algebraically closed field of constants if and only if its Galois group acts irreducibly on the solution space of the equation in a Picard-Vessiot extension. If $Y' = AY$ is irreducible over $C(\{t\})$, then G_{conv} acts irreducibly on the solutions space. Since $G_{conv} \hookrightarrow G$, we have that G acts irreducibly on this space and so the equation is irreducible over K. We can furthermore conclude that G is reductive since it has an irreducible faithful representation. The final statement follows in a similar manner. □

It is much easier to show that a differential equation is irreducible over $C((t))$ than to show it is irreducible over $C(\{t\})$. Regrettably, from our point of view, irreducibility over $C((t))$ puts severe restrictions on the Galois group of $Y' = AY$ over $C(x)$. One can deduce from Remark 3.34 of van der Put and Singer (2003) that if $Y' = AY$ is irreducible over $C((t))$, then

1. the identity component G^0_{form} of G_{form} is a torus,
2. as a G^0_{form}-module, the solution space is the sum of one dimensional invariant subspaces corresponding to distinct characters of G^0_{form}, and
3. there is an element $\gamma \in G_{form}$ whose action on G^0_{form} by conjugation cyclically permutes the characters of G^0_{form}.

Katz (1987, 3.2.8 and 3.2.9) has shown that a connected algebraic subgroup of SL_n, containing a closed subgroup satisfying the properties 1, 2, and 3 of G_{form} above must be of the form $\prod G_i$, where each G_i is either SL_{n_i} or Sp_{n_i}, n_i even in the latter case, and the n_i are pairwise relatively prime. Katz further shows that the n-space (in our case the solution space) can be written as a tensor product $\otimes V_i$ of representations of these groups where each V_i is the standard or contragredient representation of G_i if $G_i = \mathrm{SL}_{n_i}$ or the standard representation of G_i if $G_i = \mathrm{Sp}_{n_i}$.

Nonetheless, Lemma 3.3 together with Proposition 3.2 will allow us to construct equations $Y' = AY$ having Galois group SL_n or Sp_{2n}. These two results yield the following criteria:

Proposition 3.4. *Let $G \subset \mathrm{SL}_n(C)$ be a connected simple linear algebraic group of rank ℓ with Lie algebra $\mathcal{G}$ and $\mathbf{C}$ a curve with function field $K \supset C(x)$. Let $Y' = AY$ be a* *differential equation with* $A \in \mathcal{G}(K)$. *Let* $H \subset \mathrm{GL}_n(C)$ *be the Galois group of* $Y' = AY$ *over* K *with respect to a given fundamental solution* $y \in G(K)$ *and assume that*

1. *There exists a point* $p_0 \in \mathbf{C}$ *such that the equation* $Y' = AY$ *has a unique slope of the form* $\frac{a}{n}$, $(a, n) = 1$.
2. *There exists a point* $p_1 \in \mathbf{C}$ *such that in terms of some local coordinate* t *at* p_1, *we can expand* $Y' = AY$ *as*

$$\frac{dY}{dt} = \left(\frac{A_1}{t} + B_1(t)\right)Y,$$

where A_1 *is semisimple and has* ℓ *eigenvalues that are* $\mathbb{Z}$*-independent mod* $\mathbb{Z}$ *and* $B_1(t) \in \mathfrak{gl}(C\{t\})$.

3. *There exists a point* $p_2 \in \mathbf{C}$ *such that in terms of some local coordinate* t *at* p_2, *can expand* $Y' = AY$ *as*

$$\frac{dY}{dt} = \left(\frac{A_2}{t} + B_2(t)\right)Y,$$

where A_2 *is nilpotent and the kernel of* $ad(A_2)$ *in* $\mathcal{G}$ *has dimension* ℓ, *and* $B_2(t) \in \mathfrak{gl}_n(C\{t\})$.

Then $H = G$. *Furthermore, if this is the case, then* G *must be either* SL_n *or* Sp_{2n}.

Proof. We refer to Babbitt and Varadarajan (1983), Katz (1987) or van der Put and Singer (2003) for the definition and properties of the slopes of a differential equation at a singular point. From (2.2.8) of Katz (1987) or Remark 3.34 of van der Put and Singer (2003), one sees that hypothesis 1 above implies hypothesis 1 of Proposition 3.2. The last statement follows from the discussion preceding the statement of this proposition. □

To give irreducibility criteria that apply to other groups, we shall show how one can compare the local behavior at several points to ensure irreducibility. These criteria will assume that at several points, the identity component of the local formal Galois groups is a maximal torus of the global Galois group (that is, the Galois group over the function field K of $\mathbf{C}$) and they will give conditions on elements normalizing these tori to ensure irreducibility. We therefore start with the following definition.

We continue the convention that $\pi : \mathbf{C} \to \mathbf{P}^1$ is a non-singular curve over the projective line, $C(x) \subset K$ is the corresponding inclusion of function fields and $p \in \mathbf{C}$ with $\mathbf{C}$ not ramified at p and that $\pi(p) \neq \infty$.

Definition 3.5. Let G be a connected linear algebraic group with Lie algebra $\mathcal{G}$. Let $Y' = AY$ be a differential equation with $A \in \mathcal{G}(K)$. We say that $p \in \mathbf{C}$ is a *maximally toric point* for $Y' = AY$ (with respect to G) if the connected component G^0_{form} of the local formal Galois group G_{form} at p is a maximal torus in G.

The work of Katz quoted above implies that if $p \in \mathbf{C}$ is a point such that the equation has a unique slope of the form a/n, $(a, n) = 1$, then p is a maximally toric point but we shall see that not all maximally toric points need arise in this way.

Let $Y' = AY$ be a differential equation as in Definition 3.5 and let p be a maximally toric point for this equation and let G_{form} be the formal local Galois groups at p. Theorem 11.2 of van der Put and Singer (2003) implies that G_{form}/G^0_{form} is a finite cyclic group. Since G^0_{form} is a maximal torus of G, we may identify the generator g of G_{form}/G^0_{form} with an element of the Weyl group of G. Regrettably, we do not see how to do this in a canonical way so that we can compare the images of elements g for different maximally toric points p of $\mathbf{C}$. Nonetheless, assume that a (and therefore any) maximal torus of G has m weight spaces in the representation of G on the solution space of $Y' = AY$. Since the element g permutes the weight spaces, it can be considered as an element of $\mathfrak{S}_m$, the permutation group on m elements (again, in a non-canonical way). The key fact is that although the image of g in $\mathfrak{S}_m$ may not be uniquely defined, all such images are conjugate in $\mathfrak{S}_m$ since g is determined up to conjugation in G. We refer to this $\mathfrak{S}_m$ conjugacy class as the *permutation conjugacy class* at the toric point p. We now make the following definition.

Definition 3.6. Let $\mathfrak{S}_m$ be the permutation group on m elements, and let $\{C_1, \dots, C_t\}$ be a collection of conjugacy classes in $\mathfrak{S}_m$. We say that the set $\{C_1, \dots, C_t\}$ is *strictly transitive* if for any choice $\tau_i \in C_i$, $i = 1, \dots t$, the subgroup of $\mathfrak{S}_m$ generated by $\{\tau_1, \dots, \tau_t\}$ acts transitively.

Since the conjugacy class of an element of $\mathfrak{S}_m$ is determined by the type of the partition on $\{1, \dots, m\}$ given by its cycle structure, one can see that

Lemma 3.7. *The set $\{C_1, \dots, C_t\}$ of conjugacy classes in $\mathfrak{S}_m$ is strictly transitive if and only if the following holds for some (and therefore any) set of representatives $\{\sigma_1, \dots, \sigma_t\}$ with $\sigma_i \in C_i$: for any i, $1 \le i \le m-1$, there is an element σ_j leaving no set of cardinality i invariant.*

For example, for $m = 6$ the singleton set $\{\overline{(123456)}\}$ and the set $\{\overline{(123)(456)}, \overline{(1234)(56)}\}$ are strictly transitive sets of conjugacy classes (where $\overline{\sigma}$ denotes the conjugacy class of σ). The set $\{\overline{(123)(456)}, \overline{(1)(45)(236)}\}$ is not strictly transitive since each permutation leaves a set of 3 invariant. We are now ready to state the following criterion, which generalizes Proposition 3.4.

Proposition 3.8. *Let $G \subset \mathrm{GL}_n(C)$ be a connected simple linear algebraic group of rank ℓ with Lie algebra $\mathcal{G}$ and $\mathbf{C}$ a curve with function field $K \supset C(x)$. Let $Y' = AY$ be a differential equation with $A \in \mathcal{G}(K)$. Let H be the Galois group of $Y' = AY$ over K and assume that*

1. *There exist maximally toric points $p_1, \dots, p_t \in \mathbf{C}$ for the equation $Y' = AY$ such that the corresponding conjugacy classes form a strictly transitive set.*
2. *There exists a point $p_1 \in \mathbf{C}$ such that in terms of some local coordinate t at p_1, we can expand $Y' = AY$ as*

$$\frac{dY}{dt} = \left(\frac{A_1}{t} + B_1(t)\right)Y,$$

where A_1 is semisimple and has ℓ eigenvalues that are $\mathbb{Z}$-independent mod $\mathbb{Z}$ and $B_1(t) \in \mathfrak{gl}_n(C\{t\})$.

3. *There exists a point* $p_2 \in \mathbf{C}$ *such that in terms of some local coordinate t at* p_2, *we can expand* $Y' = AY$ *as*

$$\frac{dY}{dt} = \left(\frac{A_2}{t} + B_2(t)\right)Y,$$

where A_2 *is nilpotent and the kernel of* $\mathrm{ad}(A_2)$ *has dimension* ℓ *and* $B_2(t) \in \mathfrak{gl}_n(C\{t\})$.

Then $H = G$.

Proof. As in the proof of Proposition 3.4, we need only to show that the first condition guarantees that the Galois group H acts irreducibly on the solution space V and so that H is reductive. Let T be a maximal torus of H and assume that T has m distinct weight spaces in the solution space of $Y' = AY$. If W is a proper, non-trivial H-invariant subspace of V, then we can write W as a sum of i, $1 \le i \le m-1$, weight spaces. Since each local formal Galois group $G_{form,j}$ at p_j leaves W invariant, we can conclude that for each j, any generator σ_j of the group $G_{form,j}/G^0_{form,j}$ leaves a set of i weight spaces stable. Therefore, Lemma 3.7 implies that the set of associated conjugacy classes is not strictly transitive is a contradiction. Therefore V is an irreducible H-module. □

We note here that if we can satisfy the first condition of Proposition 3.8, then the representation of $G \subset \mathrm{GL}_n$ is severely restricted. In particular, the Weyl group of G will act transitively on the weights, and so the representation will be a minuscule representation (see Ch.VIII, §7, No. 3 of Bourbaki, 1990, and Katz, 1987, p. 48). This means that if G is a simple group, it must be of type A_ℓ, B_ℓ, C_ℓ, D_ℓ, E_6, E_7 and the representations must have highest weight given in the following list:

$$\begin{array}{rl}
\mathrm{A}_\ell(\ell \ge 1): & \bar{\omega}_1, \bar{\omega}_2, \dots, \bar{\omega}_\ell \\
\mathrm{B}_\ell(\ell \ge 2): & \bar{\omega}_\ell \\
\mathrm{C}_\ell(\ell \ge 2): & \bar{\omega}_1 \\
\mathrm{D}_\ell(\ell \ge 3): & \bar{\omega}_1, \bar{\omega}_{\ell-1}, \bar{\omega}_\ell \\
\mathrm{E}_6: & \bar{\omega}_1, \bar{\omega}_6 \\
\mathrm{E}_7: & \bar{\omega}_7 \\
\mathrm{E}_8, \mathrm{F}_4, \mathrm{G}_2: & \text{no minuscule weights}
\end{array}$$

In fact, we shall see that there are groups of type B_ℓ which have no representation with a strictly transitive set of conjugacy classes in the Weyl group, but we are able to apply the proposition to the rest of the possible types.

To apply Proposition 3.8, we need to ensure that, given a group G with Lie algebra $\mathcal{G}$, we are able to construct an $A \in \mathcal{G}(K)$ having prescribed formal Galois groups at given points. The inverse problem over $C((t))$, $t' = 1$, has been solved and it is known which groups appear as formal Galois groups and how one can even effectively construct equations $Y' = AY$, $A \in \mathfrak{gl}_n(C((t)))$ with allowable formal Galois groups (see Chapter 11.2 of van der Put and Singer, 2003). We will need a small modification of this result to ensure that $A \in \mathcal{G}(C((t)))$, where $\mathcal{G}$ is the Lie algebra of a given group. This is done in Proposition 3.11. We begin with two lemmas. Lemma 3.9 is a slight generalization of Hilbert's Theorem 90.

Lemma 3.9. *Let E be a finite Galois extension of a field F and G a connected linear algebriac group defined over an algebraically closed field $C \subset F$. Assume that the Galois group H of E over F is a finite cyclic group and let $\rho : H \to G(C)$ be a homomorphism. Then there is an element $\eta \in G(F)$ such that $\eta^\tau = \eta \cdot \rho(\tau)$ for all $\tau \in H$, where η^τ denotes the result of applying τ to the entries of η.*

Proof. Since $\rho(H)$ is cyclic, it is contained in a torus T of $G(C)$. There is a C-isomorphism of T with some power of the multiplicative group $G_m(C) = C^*$ of C, so we can assume that $\rho(H) \subset (G_m(C))^r$. The map ρ as a 1-cocycle defines a cohomology class $\overline{\rho} \in H^1(H, (G_m(C))^r) = (H^1(H, G_m(C)))^r$. Hilbert's Theorem 90 (see Chapter VI, §10 of Lang, 1993) implies that $H^1(H, G_m(C)) = 1$ so $\overline{\rho}$ is trivial, that is, ρ is a coboundary. This proves the lemma. □

The following lemma is a distillation and modification of the proof of Theorem 11.2 of van der Put and Singer (2003), included for the convenience of the reader.

Lemma 3.10. *Let T be the group of diagonal elements in $\mathrm{GL}_n(C)$ with Lie algebra $\mathcal{T} \subset \mathfrak{gl}_n(C)$ and $\phi : T \to T$ an automorphism of order m. There exists an $A \in \mathcal{T}(C[t^{-\frac{1}{m}}])$ such that the Galois group of $Y' = AY$ over $C((t^{\frac{1}{m}}))$ is $T(C)$ and such that $A^\gamma = d\phi(A)$ where A^γ denotes the matrix resulting from applying the automorphism of $C((t^{\frac{1}{m}}))$ defined by $\gamma : t^{\frac{1}{m}} \mapsto e^{\frac{2\pi i}{m}} t^{\frac{1}{m}}$ to the entries of A.*

Proof. The map $d\phi : \mathcal{T}(C) \to \mathcal{T}(C)$ is an automorphism of order m and so has eigenvalues that are roots of unity. Let $W_q \subset \mathcal{T}(C)$ be a non-zero eigenspace corresponding to a root of unity $e^{\frac{2\pi i q}{m}}$, where q is an integer $0 \le q < m$ and let $\mathbf{b}_{j,q}$, $1 \le j \le r_q$ be a basis of W_q. Defining

$$A_q = z^{-\frac{q}{m}} \sum_{j=1}^{r_q} z^{-j-1} \mathbf{b}_{j,q}$$

one sees that $A_q^\gamma = d\phi(A_q)$. Let $A = \sum A_q$, where the sum is over all q with $W_q \neq (0)$. We claim that $Y' = AY$ satisfies the conclusion of the lemma. The behavior with respect to γ follows from the construction of A. Since $A \in \mathcal{T}(C((t^{\frac{1}{m}})))$, the Galois group of $Y' = AY$ over $C((t^{\frac{1}{m}}))$ is a subgroup of $T(C)$. A full solution space for this equation is spanned by

$$\left\{ \frac{1}{-\frac{q}{m} - j} e^{z^{-\frac{q}{m} - j}} \mathbf{b}_{j,q} \right\},$$

where q runs over those integers with $W_q \neq (0)$ and $1 \le j \le r_q$. To show that the Galois group is all of $T(C)$, it suffices to show that the elements $\{e^{z^{-\frac{q}{m}-j}}\}$ form an algebraically independent set. The Kolchin-Ostrowski Theorem (Kolchin, 1968) implies that this is the case if there is no non-trivial relation of the form $\sum a_{j,q} z^{-\frac{q}{m}-j-1} = \frac{f'}{f}$, where the $a_{j,q}$ are rational numbers and $f \in C((t^{\frac{1}{m}}))$ (see also Exercise 4, Chapter VI.5 of Kolchin, 1973). Since the order of $\frac{f'}{f}$ is ≥ -1 and the order of a nonzero $\sum a_{j,q} z^{-\frac{q}{m}-j-1}$ is < -1, we see that no such non-trivial relation can exist. □

Proposition 3.11. *Let $G \subset \mathrm{GL}_n$ be a connected linear algebraic group defined over C and $\overline{G} \subset G$ a subgroup with $\overline{G}^0$ a torus and $\overline{G}/\overline{G}^0$ cyclic. Let $\overline{\mathscr{G}}$ be the Lie algebra of $\overline{G}$. There exists an $\overline{A} \in \overline{\mathscr{G}}(C[t, t^{-1}])$ such that the Galois group of $Y' = \overline{A}Y$ over $C((t))$ is $\overline{G}$. Furthermore, this $\overline{A} = \sum_{i=a}^{b} A_i t^i$ can be chosen so that if A is any element of $\mathscr{G}(C((t)))$ such that $A - \overline{A} = \sum_{i=b+1}^{\infty} B_i t^i$, then the Galois group of $Y' = AY$ over $C((t))$ is also $\overline{G}$.*

Proof. We begin by noting that under the assumptions of Proposition 3.11, there is an element $g \in \overline{G}$ of finite order, whose image generates $\overline{G}/\overline{G}^0$ (see Theorem 8.10 of van der Put and Singer, 1997). To see this, let $\overline{g}$ be an element whose image generates $\overline{G}/\overline{G}^0$. If $m = |\overline{G}/\overline{G}^0|$, then $\overline{g}^m \in \overline{G}^0$ and so $\overline{g}$ is semisimple. The Zariski closure Z of the group generated by $\overline{g}$ has only semisimple elements and is therefore diagonalizable. Following Theorem 16.2 of Humphreys (1975) we can write Z as the direct product of a torus and a finite group H. Since $Z/Z^0 \to \overline{G}/\overline{G}^0$ is surjective, there is some element of H that maps to a generator of $\overline{G}/\overline{G}^0$. Let g be this element and assume g has order m'. Note that $m|m'$. We are now going to find elements $\eta, s \in G$ such that the element $(\eta s)' \cdot (\eta s)^{-1}$ of $\mathscr{G}(k_0)$, with $k_0 = C((t))$, satisfies all but the last sentence of the above proposition.

We first select η. Let $k = C((t^{\frac{1}{m}}))$ and $k' = C((t^{\frac{1}{m'}}))$. We may identify k with a subfield of k'. Let H' denote the Galois group of k' over k_0. Since this is a cyclic group of order m', there is a morphism $\rho : H' \to G(C)$ mapping a generator γ' of H' to g. Let $\eta \in G(k')$ be an element, guaranteed to exist by Lemma 3.9, that satisfies $\eta^{\gamma'} = \eta \cdot g$.

We are now ready to select s. Since $\overline{G}^0$ is a torus, we may identify it with the group T of diagonal elements in some $\mathrm{GL}_r(C)$. Conjugation by g induces an automorphism of $\overline{G}^0$ of order m. Lemma 3.10 implies that there is an $\widetilde{A} \in \overline{\mathscr{G}}(k) \subset \mathscr{G}(k)$ such that the Galois group of $Y' = \widetilde{A}Y$ over k is $\overline{G}^0$ and $\widetilde{A}^{\gamma} = g^{-1}\widetilde{A}g$, where γ as before is the k_0-automorphism $t^{\frac{1}{m}} \mapsto e^{\frac{2\pi i}{m}} t^{\frac{1}{m}}$ of k. We shall now consider $\widetilde{A}$ as an element of $\mathscr{G}(k')$ (since $k \subset k'$) and identify γ with an element of H', the Galois group of k' over k_0. Let s be an L-point of $\overline{G}^0$ (in a suitable differential extension L of k) satisfying the differential equation $s' = \widetilde{A}s$ and such that $k'(s)$ is a Picard-Vessiot extension of k' with Galois group $\overline{G}^0$ for this equation.

We now show that $k_0(\eta s)$ is a Picard-Vessiot extension of k_0 with Galois group $\overline{G}$. As in the proof of Proposition 6.3 of Mitschi and Singer (2002) one sees that

1. The element $(\eta, \eta s)$ (denoted there by (w, wg)) satisfies the equation $Y' = BY$, where

$$B = \begin{pmatrix} \eta'\eta^{-1} & 0 \\ 0 & \eta'\eta^{-1} + \eta\widetilde{A}\eta^{-1} \end{pmatrix}.$$

2. Both $\eta'\eta^{-1}$ and $\eta'\eta^{-1} + \eta\widetilde{A}\eta^{-1}$ are in $\overline{G}(k_0)$.
3. The Picard-Vessiot extension $k_0((\eta, \eta s))$ of k_0 has Galois group $\langle g \rangle \ltimes T(C)$, where $\langle g \rangle$ is the cyclic group generated by g.

We claim that the Picard-Vessiot extension $k_0(\eta s)$ has Galois group $\overline{G}$. Note that since $k_0(\eta s) \subset k_0((\eta, \eta s))$, the Galois group of $k_0(\eta s)$ is isomorphic to the quotient of $\langle g\rangle \ltimes T(C)$ by the subgroup of its elements that leave ηs fixed. An element (a, b) of $\langle g\rangle \ltimes T(C)$ maps ηs to ηsab. Therefore (a, b) leaves ηs fixed if and only if $ab = 1$. The set of such elements is the same as the kernel of the homomorphism $\langle g\rangle \ltimes T(C) \to \langle g\rangle T(C) = \overline{G}$ that sends (a, b) to ab. Therefore, the Galois group of $k_0(\eta s)$ is $\overline{G}$.

As noted above, $(\eta s)'(\eta s)^{-1}$ is an element of $\mathcal{G}(k_0)$. If we write it as $\sum_{i=p}^{\infty} A_i t^i$, then the results of Sections 6 and 7 of Babbitt and Varadarajan (1983) imply that one can effectively find an integer q such that the canonical form of the equation $Y' = (\sum_{i=p}^{\infty} A_i t^i)Y$ is determined by $\sum_{i=p}^{q} A_i t^i$ and so is its formal Galois group. Therefore, for $\overline{A} = \sum_{i=p}^{q} A_i t^i$, the proposition is proven. □

Example 3.12. We shall illustrate the above proposition for $G = \mathrm{SL}_2$. Let

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

The identity component $\overline{G}^0$ is a maximal torus and $\overline{G}/\overline{G}^0$ is the cyclic group of order two. The element

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

is an element of order 4, whose image generates the group $\overline{G}/\overline{G}^0$. Let $k' = C((t^{\frac{1}{4}}))$ and

$$\eta = \frac{1}{2} \begin{pmatrix} t^{\frac{1}{4}} + t^{-\frac{1}{4}} & \sqrt{-1}(-t^{\frac{1}{4}} + t^{-\frac{1}{4}}) \\ \sqrt{-1}(t^{\frac{1}{4}} - t^{-\frac{1}{4}}) & t^{\frac{1}{4}} + t^{-\frac{1}{4}} \end{pmatrix}.$$

If γ' is the generator of the Galois group of k' over $C((t))$, then one sees that $\eta^{\gamma'} = \eta g$. Now define

$$s = \begin{pmatrix} e^{t^{-1/2}} & 0 \\ 0 & e^{-t^{-1/2}} \end{pmatrix}.$$

One sees that s satisfies the differential equation $s' = \widetilde{A}s$, where

$$\widetilde{A} = \begin{pmatrix} \frac{-1}{2t^{3/2}} & 0 \\ 0 & \frac{1}{2t^{3/2}} \end{pmatrix},$$

and that ηs satisfies the equation $(\eta s)' = \overline{A}(\eta s)$, where

$$\overline{A} = \begin{pmatrix} -\frac{t+1}{4t^2} & \frac{-\sqrt{-1}(2t-1)}{4t^2} \\ \frac{\sqrt{-1}}{4t^2} & \frac{t+1}{4t^2} \end{pmatrix}.$$

The proposition assures us that the equation $Y' = \overline{A}Y$ has Galois group $\overline{G}$. □

4. EQUIVARIANT EQUATIONS FOR $G^0 = G_1 \cdots G_r$, WHERE EACH G_i IS A SIMPLE GROUP OF TYPE A_ℓ, C_ℓ, D_ℓ, E_6, or E_7

In the previous section, we gave criteria which guarantee that a given equation has given Galois group. Here we shall show how one can construct equations meeting these criteria. In this section, G is a given linear algebraic group with identity component G^0 and H, as in Section 2, denotes a finite subgroup of G. Let K be a Galois extension of $C(x)$ with Galois group H. We will begin by showing that it suffices to accomplish this task for *simply connected* groups G_i. We shall then show how to find equivariant equations for simply connected groups of each of the types mentioned above and then for products of these groups.

To reduce the inverse problem in our situation to an inverse problem for simply connected groups, we proceed as follows. Let $G = H \ltimes G^0$ with G^0 a semisimple group. From Theorem 5.1 of Hochschild (1976) there exist a simply connected group $\widetilde{G^0}$ and a morphism $\rho : \widetilde{G^0} \to G^0$ with finite kernel. Theorem 5.5 of the same reference implies that every morphism $\sigma : G^0 \to G^0$ lifts to a *unique* morphism $\tilde{\sigma} : \widetilde{G^0} \to \widetilde{G^0}$ such that $\rho\tilde{\sigma} = \sigma\rho$. In particular, this implies that the action of H on G^0 lifts to an action of H on $\widetilde{G^0}$ such that $\mathrm{id} \times \rho : H \ltimes \widetilde{G^0} \to H \ltimes G^0$ is a morphism. Therefore, if we can find an H-equivariant $\tilde{A} \in \tilde{\mathcal{G}}(K)$ (where $\tilde{\mathcal{G}}$ is the Lie algebra of $\widetilde{G^0}$) such that the Galois group of $Y' = AY$ is $H \ltimes \widetilde{G^0}$, then $d\rho(A)$ is H-equivariant and by Proposition 5.3 of Mitschi and Singer (2002) the Galois group of $Y' = d\rho(A)Y$ is G.

4.1. Equivariant Equations for Simply Connected Groups of Type A_ℓ, C_ℓ, D_ℓ, E_6, or E_7

In this section, we shall apply Propositions 3.4 and 3.8 to construct equivariant equations with groups of the above types. In fact, we shall show

Proposition 4.1. *Let G be a simply connected group of type A_ℓ, C_ℓ, D_ℓ, E_6 or E_7. There is a representation $\rho : G \to \mathrm{GL}_N$ with associated representation $d\rho : \mathcal{G} \to \mathfrak{gl}_N$ of its Lie algebra, and elements $B_1, B_2, \ldots, B_m \in d\rho(\mathcal{G})[t^{-1}, t]$ such that*

1. *for any covering $\pi : \mathbf{C} \to \mathbf{P}^1$ of the projective line by a non-singular curve $\mathbf{C}$ with $C(x) \subset K$, the corresponding extension of function fields, and points $q_1, \ldots q_m \in \mathbf{C}$ that are not ramification points and such that $\pi(q_i) \neq \infty$ for $i = 1, \ldots, m$, and*
2. *any element $B \in d\rho(\mathcal{G})(K)$ such that $B = B_i +$(terms of order higher than $\deg(B_i)$) in a local coordinate t at q_i, for $i = 1, \ldots, m$,*

the equation $Y' = BY$ has Galois group G over K. Furthermore, at least one of the q_i is an irregular singular point of $Y' = BY$.

In fact, for simple groups under consideration, m can be chosen to be 3 or 4.

We note that once the proposition has been established, a simple application of Corollary 2.3 yields an equivariant equation. We will prove Proposition 4.1 by showing that one can select the B_i so that the conditions of Propositions 3.4 or 3.8 are satisfied. We first show how conditions 2 and 3 of these propositions can be fulfilled and then turn to condition 1.

Condition 2. If G is a linear algebraic group of rank ℓ, then, by definition, G contains a torus T of dimension ℓ. Any torus contains elements g that generate each a Zariski dense subgroup of T. Such an element must be semisimple and have ℓ multiplicatively independent eigenvalues. We may write $g = e^{A_1}$ for some $A_1 \in \mathcal{T}(C) \subset \mathcal{G}(C)$. One sees that A_1 will also be semisimple and have ℓ eigenvalues that are $\mathbb{Z}$-independent *mod* $\mathbb{Z}$. For example, let $r_1, \ldots, r_{n-1} \in C$ be $\mathbb{Z}$-linearly independent *mod* $\mathbb{Z}$ and let $r_n = -\sum r_i$. If $G^0 = \mathrm{SL}_n$ let $A_1 = \mathrm{diag}(r_1, \ldots, r_n) \in \mathfrak{sl}_n(C)$. If $G^0 = \mathrm{Sp}_n$, let $A_1 = \mathrm{diag}(\mathrm{diag}(r_1, \ldots, r_n), -\mathrm{diag}(r_1, \ldots, r_n)) \in \mathfrak{sp}_n(C)$. We let $B_1 = A_1/t$.

Condition 3. The element A_2 will be a principal nilpotent element of the Lie algebra. By Proposition 8, p. 166, of Bourbaki (1990), any semisimple Lie algebra of rank ℓ contains principal nilpotent elements u. These can be constructed by decomposing the algebra as the sum of a Cartan subalgebra and nonzero root spaces $\mathfrak{g}_\alpha$ and letting $u = \sum_{\alpha \in \Phi^+} v_\alpha$, where v_α is a nonzero element of $\mathfrak{g}_\alpha$ for each positive root $\alpha \in \Phi^+$ (*loc. cit.* Proposition 10, p. 168). For example, in $\mathfrak{sl}_n(C)$ we can take the matrix $u = (a_{i,j})$, where $a_{i,j} = 0$ if $i \geq j$ and $a_{i,j} = 1$ if $i < j$. We let A_2 be such an element and $B_2 = A_2/t$.

Condition 1. Unlike conditions 2 and 3, we are unable to satisfy condition 1 (in either Proposition 3.4 or 3.8) without taking into account the particular representation of our group. In all cases, we will need to select an appropriate representation that will allow us to ensure that the conjugacy classes of selected elements $\{\sigma_1, \ldots, \sigma_m\}$ of the Weyl group of a maximal torus T give rise to a strictly transitive set. As noted before, this representation must be minuscule. Using Proposition 3.11 and Corollary 2.3, we can guarantee that we can construct a differential equation $Y' = AY$ having singular points $p_1, \ldots p_m$ so that the local formal Galois group at p_i is isomorphic to the group generated by σ_i and T. Since the set $\{\overline{\sigma_1}, \ldots, \overline{\sigma_m}\}$ will, by construction, be a strictly transitive set, condition 1 of Proposition 3.8 will be met. In fact, for simply connected groups of type A_ℓ and C_ℓ (*i.e.*, $\mathrm{SL}_{\ell+1}$ and $\mathrm{Sp}_{2\ell}$) we will only need to use one element from the Weyl group, and the construction can be made so explicit that Proposition 3.4 can be applied. We now complete this argument for each of the above types of groups.

4.1.1. Proof of Proposition 4.1 for the Type A_ℓ. The simply connected group of type A_ℓ is $\mathrm{SL}_{\ell+1}$. We shall consider the usual representation of this group acting on a vector space of dimension $\ell + 1$ (in fact, all the fundamental representations are minuscule, but we will only consider this one). In this representation, the diagonal elements form a maximal torus T and there are $\ell + 1$ distinct weights. The Weyl group is isomorphic to the group of unimodular permutation matrices, that is, to $\mathfrak{S}_{\ell+1}$, and its action on the weights is the usual action of this permutation group on $\ell + 1$ elements. In particular, there is an element σ_1 of the Weyl group that cyclically permutes the roots. Clearly, $\{\overline{\sigma_1}\}$ forms a strictly transitive set. Using Proposition 3.11, we can find an element $\overline{A} \in \mathfrak{sl}_{\ell+1}(C[t, t^{-1}])$ such that the Galois group of $Y' = \overline{A}Y$ is the group generated by σ_1 and T. Letting $B_3 = \overline{A}$, we see from Proposition 3.8 that together with the matrices B_1 and B_2 already constructed, the set $\{B_1, B_2, B_3\}$ satisfies Proposition 4.1.

The groups $SL_{\ell+1}$ are particularly transparent, but this is not the case of the other groups we will consider. For simply connected groups of the remaining types, the action of the Weyl group on weights for a given representation is best described in Lie-theoretic terms. We will, in each case, identify the Weyl group with the group generated by reflections associated to a set of simple roots in the Lie algebra. To prepare the reader for this discussion, we will show how one can find the element σ_1 above using the Lie-theoretic description of the Weyl group. To do this, we now fix some notation.

Let $\mathfrak{g}$ be a semisimple Lie algebra of rank ℓ with Cartan subalgebra $\mathfrak{h}$ and $\{\epsilon_1, \dots, \epsilon_\ell\}$ a basis of the dual vector space $\mathfrak{h}^*$. We will use an inner product on $\mathfrak{h}^*$ for which the ϵ_i form an orthogonal basis and write weights in terms of the ϵ_i in order to do our calculations.

We will use the description of A_ℓ given on Planche I of Bourbaki (1990). The simple roots are given as

$$\alpha_i = \epsilon_i - \epsilon_{i+1}, \quad i = 1, \dots, \ell.$$

We will only look at the minuscule representation $V(\bar{\omega}_1)$, whose highest weight is $\bar{\omega}_1 = \epsilon_1 - \frac{1}{\ell+1}\sum_{j=1}^{\ell+1}\epsilon_j$. This is the standard representation and it is of dimension $\ell + 1$. We wish to now determine which weights appear in this representation and how the Weyl group permutes them. We denote by S_i the reflection associated with the simple root α_i, that is

$$S_i(v) = v - \frac{2(v, \alpha_i)}{(\alpha_i, \alpha_i)}\alpha_i.$$

Define $w_j = \epsilon_j - \frac{1}{\ell+1}\sum_{j=1}^{\ell+1}\epsilon_j$ and note that $w_1 = \bar{\omega}_1$. We also note that for all i, $1 \leq i \leq \ell$, we have $(\alpha_i, \alpha_i) = 2$, so

$$\begin{aligned}
(1 \leq i \leq \ell) \quad S_i(w_j) &= w_j - (w_j, \alpha_i)\alpha_i \\
&= w_j - \left(\epsilon_j - \frac{1}{\ell+1}\sum_{j=1}^{\ell+1}\epsilon_j, \epsilon_i - \epsilon_{i+1}\right)(\epsilon_i - \epsilon_{i+1}) \\
&= \begin{cases} w_j & \text{if } j \neq i, i+1 \\ w_j - (\epsilon_i - \epsilon_{i+1}) & \text{if } j = i \\ w_j + (\epsilon_i - \epsilon_{i+1}) & \text{if } j = i+1 \end{cases} \\
&= \begin{cases} w_j & \text{if } j \neq i, i+1 \\ w_{j+1} & \text{if } j = i \\ w_{j-1} & \text{if } j = i+1. \end{cases}
\end{aligned}$$

Since $V(\omega_1)$ is minuscule, the set of weights appearing in this representation is precisely the orbit of $\bar{\omega}_1$ under the Weyl group. The previous calculation shows that $\{w_i\}_{i=1}^{\ell+1}$ are among these and, comparing dimensions, we have that this set is precisely the set of weights. Again from this calculation, we see that $S_i = (i, i+1)$, where we are thinking of S_i as a permutation of the (subscripts of the) weights. A calculation shows that $S_1 S_2 \cdot \cdots \cdot S_\ell = (1, 2, \dots, \ell, \ell+1)$. Let σ_1 be an element of the normalizer of a maximal torus corresponding to this latter permutation (this can be found once one has elements corresponding to the reflections S_i, see Exercise 23.22 of Fulton and Harris, 1991). This is the element σ_1 introduced in the first paragraph.

We finish our discussion of $\mathrm{SL}_{\ell+1}$ by showing how we can make the above construction even more explicit. Prior to our work on Proposition 3.8, the late A. Bolibrukh and R. Schäfke showed us how to explicitly construct differential equations with irreducible local Galois groups. Using their ideas in combination with the Weyl group approach, we may proceed as follows. Let $A_{0.1} = (a_{i,j})$ be the matrix defined by $a_{i+1,i} = 1$ for $i = 1, \ldots, \ell$ and $a_{i,j} = 0$ if $j + 1 \neq i$ and let $A_{0,2}$ be the matrix with 1 as the $(1, \ell + 1)$ entry and zero everywhere else. Note that $A_{0,1} + A_{0,2}$ is a matrix whose eigenvalues are the $(\ell + 1)^{st}$ roots of 1. We now apply Corollary 2.3. Select three points p_0, p_1, p_3 not in $\mathcal{S}$, with distinct projections on $\mathbf{P}^1$. Let $A_1 = \mathrm{diag}(r_1, \ldots, r_{\ell+1})$ where $r_1, \ldots, r_\ell$ are $\mathbb{Z}$-linearly independent *mod* $\mathbb{Z}$ and $r_{\ell+1} = -\sum_{j=1}^{\ell}$. Let $A_2 = (a_{i,j})$ where $a_{i,j} = 0$ if $i \geq j$ and $a_{i,j} = 1$ if $i < j$. Corollary 2.3 implies that one can produce an $A \in \mathcal{G}(K)$ such that in terms of the local coordinate t at these points, the equation $Y' = AY$ has the following local expansions:

$$\text{At } p_0, \frac{dY}{dt} = \left(\frac{A_{0,1}}{t^2} + \frac{A_{0,2}}{t} + \text{terms involving } t^j, j \geq 0\right)Y. \tag{1}$$

$$\text{At } p_1, \frac{dY}{dt} = \left(\frac{A_1}{t} + \text{terms involving } t^j,\ j \geq 0\right)Y. \tag{2}$$

$$\text{At } p_2, \frac{dY}{dt} = \left(\frac{A_2}{t} + \text{terms involving } t^j, j \geq 0\right)Y. \tag{3}$$

We will now check that the conditions of Proposition 3.4 hold. To see that there is a unique slope at p_0, let $g = \mathrm{diag}\ (1, t^{1/(\ell+1)}, t^{2/(\ell+1)}, \ldots, t^{\ell/(\ell+1)})$. Note that for any matrix $(a_{i,j})$, we have that

$$g(a_{i,j})g^{-1} = \left(t^{\frac{i-j}{\ell+1}} a_{i,j}\right).$$

Therefore

$$g[A] = gAg^{-1} + g'g^{-1} = \frac{A_{0.1} + A_{0,2}}{t^{2-\frac{1}{\ell+1}}} + \text{ terms involving } t^j, j \geq 2 - \frac{1}{\ell+1}.$$

This is a so-called *shearing-transform* of the equation $dY/dt = AY$ at p_0. Since the matrix $A_{0,1} + A_{0,2}$ is semisimple, there will be a unique slope, equal to $2 - 1/(\ell + 1)$ (Babbitt and Varadarajan, 1983, Proposition 4.2 and the subsequent paragraphs). Therefore, as noted before, the equation will be irreducible over $C((t))$.

Finally, at p_1 and p_2 the required conditions are obviously satisfied. Therefore, the equivariant equation $Y' = AY$ has Galois group G^0 over K and so using the techniques of Mitschi and Singer (2002) or Hartmann (2002) one can construct an equation having Galois group $H \ltimes G^0$ over $C(x)$. In particular, the example given in Section 2 was constructed in the above manner and so was Galois group SL_2 over $K = C(x, \sqrt{x})$ (another example with this group is given *via* an *ad hoc* construction by Hartmann (2002), p. 42, and in Section 5).

4.1.2. Proof for C_ℓ. The simply connected groups of this type are the groups $\mathrm{Sp}_{2\ell}$ (see the tables for (C_l) given by Tits, 1967, p. 32). A set of simple roots of C_ℓ are

$$\alpha_i = \epsilon_i - \epsilon_{i+1}, \qquad i = 1, \ldots, \ell - 1,$$
$$\alpha_\ell = 2\epsilon_\ell$$

(see Planche III of Bourbaki, 1990). The only minuscule weight is $\bar{\omega}_1 = \epsilon_1$, corresponding to the standard representation $V(\bar{\omega}_1)$ of $\mathrm{Sp}_{2\ell}$, which has dimension 2ℓ. We again denote by S_i the reflection across the simple root α_i and will calculate the action of these reflections on the ϵ_i. Noting that for $1 \le i \le \ell - 1$, $(\alpha_i, \alpha_i) = 2$ and $(\alpha_\ell, \alpha_\ell) = 4$, we have

$$(1 \le i \le \ell - 1) \qquad S_i(\epsilon_j) = \epsilon_j - (\epsilon_j, \epsilon_i - \epsilon_{i+1})(\epsilon_i - \epsilon_{i+1})$$
$$= \begin{cases} \epsilon_j & \text{if } j \ne i, i+1 \\ \epsilon_{i+1} & \text{if } j = 1 \\ \epsilon_i & \text{if } j = i+1 \end{cases}$$
$$S_\ell(\epsilon_j) = \epsilon_j - \frac{2(\epsilon_j, 2\epsilon_\ell)}{4} 2\epsilon_\ell$$
$$= \begin{cases} \epsilon_j & \text{if } j \ne \ell \\ -\epsilon_\ell & \text{if } j = \ell. \end{cases}$$

Since $V(\bar{\omega}_1)$ is minuscule, the set of weights appearing is precisely the orbit of $\bar{\omega}_1$ under the Weyl group. The above calculation shows that this orbit contains $\{\pm\epsilon_i\}_{i=1}^{\ell}$ and so by comparing dimensions, we see that it is precisely the set of weights. Let us give the labels $\epsilon_1 = 1, \ldots, \epsilon_\ell = \ell, -\epsilon_1 = \ell + 1, \ldots, -\epsilon_\ell = 2\ell$. Rewriting the S_i as permutations of these weights, the above calculation shows that $S_1 \cdot \cdots \cdot S_{\ell-1} = (1, 2, \ldots, \ell)(\ell + 1, \ldots, 2\ell)$ and $S_1 \cdot \cdots \cdot S_\ell = (1, 2, \ldots, 2\ell)$. Let σ_1 be an element of the normalizer of a maximal torus of $\mathrm{Sp}_{2\ell}$ that yields this latter permutation. We see that σ_1 acts transitively on the set of weights and so $\{\overline{\sigma_1}\}$ forms a strictly transitive set. One now proceeds as in the first paragraph of the discussion of A_ℓ.

We note that we can make this as explicit as the example in the discussion of A_ℓ. To do this we let $U = (a_{i,j})$ be the matrix defined by $a_{i+1,i} = 1$ for $i = 1, \ldots, \ell - 1$ an $a_{i,j} = 0$ if $j + 1 \ne i$. and let V be the matrix with 1 as the $(1, \ell)$ entry and zero everywhere else. Let

$$A_{0,1} = \begin{pmatrix} U & 0 \\ V & -U \end{pmatrix}$$
$$A_{0,2} = \begin{pmatrix} 0 & (-1)^\ell V \\ 0 & 0 \end{pmatrix}.$$

Note that each of these matrices is in $\mathrm{Sp}_{2\ell}$ and $A_{0,1} + A_{0,2}$ is a matrix whose eigenvalues are the 2ℓth roots of unity. We also define $A_1 = \mathrm{diag}(\mathrm{diag}(r_1, \ldots, r_\ell), -\mathrm{diag}(r_1, \ldots, r_\ell))$, where $r_1, \ldots, r_{\ell-1} \in C$ are $\mathbf{Z}$-linearly independent *mod.* $\mathbf{Z}$ and $r_n = -\sum r_i$. Finally, we let A_2 be any nilpotent matrix in $Sp_{2\ell}$ such that $Ad(u)$ has an r-dimensional eigenspace corresponding to 1. One then proceeds as in the case of A_ℓ.

4.1.3. Proof for D_ℓ. The simply connected groups of this type are the groups $Spin_{2\ell}$. These are double covers of the groups $SO_{2\ell}$. We claim that it suffices to prove the analog of Proposition 4.1 for all (non simply connected) groups $SO_{2\ell}$. To see this, assume that we have verified the result of Proposition 4.1 for one of these groups, say G. Let $\pi : G' \to G$ be a simply connected covering with $d\pi : \mathcal{G}' \to \mathcal{G}$ the associated map of Lie algebras and $\rho' : G' \to GL_{N'}$ be a faithful representation. The map $d\pi$ will be an isomorphism from $\mathcal{G}'$ onto $\mathcal{G}$. Let $B'_i = d\pi^{-1}(B_i)$. We claim that the B'_i satisfy the conclusions of Proposition 4.1. Let $B' \in \mathfrak{gl}_{N'}(K)$ satisfy hypotheses 1 and 2 of the proposition and let $K(g)$ be a Picard-Vessiot extension for $Y' = B'Y$ with $g \in G'$. Then $\pi(g)$ satisfies $Y' = d\pi(B)Y$ and this latter equation has Galois group G by the above proposition. Since the only subgroup of G' mapping onto G *via* π is G', Proposition 5.3 of Mitschi and Singer (2002) implies that the Galois group of $K(g)$ over K is G'.

A set of simple roots in the case of $SO_{2\ell}$ is

$$\alpha_1 = \epsilon_1 - \epsilon_2, \ldots, \alpha_{\ell-1} = \epsilon_{\ell-1} - \epsilon_\ell, \alpha_\ell = \epsilon_{\ell-1} + \epsilon_\ell$$

(see Planche IV of Bourbaki, 1990) We shall only consider the representation $V(\bar{\omega}_1)$ corresponding to $\bar{\omega}_1 = \epsilon_1$. This is the standard representation of $SO_{2\ell}$ of dimension 2ℓ (and is not a faithful representation of $Spin_{2\ell}$). Noting that $(\alpha_i, \alpha_i) = 2$ for $i = 1, \ldots, \ell$, we again make the calculation

$$\begin{aligned} (1 \le i \le \ell - 1) \quad S_i(\epsilon_j) &= \epsilon_j - (\epsilon_j, \epsilon_i - \epsilon_{i+1})(\epsilon_i - \epsilon_{i+1}) \\ &= \begin{cases} \epsilon_j & \text{if } j \neq i, i+1 \\ \epsilon_{i+1} & \text{if } j = 1 \\ \epsilon_i & \text{if } j = i+1 \end{cases} \\ S_\ell(\epsilon_j) &= \epsilon_j - (\epsilon_j, \epsilon_{\ell-1} + \epsilon_\ell)(\epsilon_{\ell-1} + \epsilon_\ell) \\ &= \begin{cases} \epsilon_j & \text{if } j \neq \ell, \ell - 1 \\ -\epsilon_\ell & \text{if } j = \ell - 1 \\ \epsilon_{\ell-1} & \text{if } j = \ell. \end{cases} \end{aligned}$$

Once again, we can conclude that the orbit of $\bar{\omega}_1$ is $\{\pm\epsilon_i\}_{i=1}^{\ell}$. If we give the labels $\epsilon_1 = 1, \ldots, \epsilon_\ell = \ell, -\epsilon_1 = \ell + 1, \ldots, -\epsilon_\ell = 2\ell$, then the S_i correspond to the following permutations:

$$\begin{aligned} S_i &= (i, i+1)(\ell + i, \ell + i + 1), \qquad 1 \le i \le \ell - 1, \\ S_\ell &= (\ell - 1, 2\ell)(\ell, 2\ell - 1). \end{aligned}$$

From this, one can show

$$\begin{aligned} S_1 S_2 \cdot \cdots \cdot S_{\ell-1} &= (1, \ldots, \ell)(\ell + 1, \ldots, 2\ell), \\ S_1 S_2 \cdot \cdots \cdot S_\ell &= (1, \ldots, \ell - 1, \ell + 1, \ldots, 2\ell - 1)(\ell, 2\ell). \end{aligned}$$

Let σ_1 and σ_2 be elements of the normalizer of a maximal torus T of $SO_{2\ell}$ that yield these permutations. Then $\{\overline{\sigma_1}, \overline{\sigma_2}\}$ is a strictly transitive set.

We construct B_3, B_4 for the groups generated by σ_1 and T, by σ_2 and T respectively. We then have that B_1, B_2, B_3, B_4 yield the conclusion of Proposition 4.1.

4.1.4. Proof for E_6. The positive roots and a choice of simple roots are given on Planche V of Bourbaki (1990) but it is slightly easier to make the computation using the form given by Fulton and Harris (1991, pp. 332–333), (where L_i is used for ϵ_i and ω is used for $\bar{\omega}$). There are two possible minuscule representations: those having highest weight $\bar{\omega}_1 = \frac{2\sqrt{3}}{3}L_6$ and $\bar{\omega}_6 = L_5 + \frac{\sqrt{3}}{3}$ (*loc. cit.*, formulas for (E_6) p. 333 and p. 528). We will consider the 27-dimensional representation corresponding to ω_1. According to the tables for (E_7) given by Tits (1967, p. 47), the representation associated to ω_1 is a faithful representation of the simply connected group of this type.

Using a Maple package developed by the first author (see the link `www.math.ncsu.edu/~singer/papers/weyl_permutation.html` to download the software and reproduce the calculation), we calculated the 27 weights associated with this representation and calculated the permutations induced by the reflections given by the simple roots. We were able to determine the cycle structure of all elements in the permutation group generated by these elements and found that there were elements with cycle structure [12, 12, 3] (that is, a product of two 12-cycles and one 3-cycle) and [9, 9, 9]. A simple calculation shows that the associated conjugacy classes act strictly transitively. We refer to the above web page for details of the computation. Letting σ_1 and σ_2 be elements of the normalizer of a maximal torus having these cycle structures, we proceed as above to find the B_i.

4.1.5. Proof for E_7. We use again the positive roots and a choice of simple roots as given by Fulton and Harris (1991, p. 333). There is only one possible minuscule representation: the representation having highest weight $\omega_7 = L_6 + \frac{\sqrt{2}}{2}L_7$. This representation has dimension 56 and is a faithful representation of the associated simply connected group, as appears in the tables p. 47 of Tits (1967). A calculation similar to the one above shows that there are two elements of the Weyl group whose permutation structure is given by [18, 18, 18, 2] and [14, 14, 14] respectively. The associated conjugacy classes are strictly transitive. We again refer to the web page for the details.

4.1.6. Proof for other types. Groups of type G_2, F_4, and E_8 do not have minuscule representations and so the above methods do not apply. The spin representation (corresponding to highest weight ω_ℓ) is a minuscule representation for groups of type B_ℓ. We have calculated the action of the Weyl group on the weights of this representation and are able to produce strictly transitive sets of permutation conjugacy classes for B_2, B_3, B_5 and B_7 and can show that such sets do not exist for B_4. We do not have definitive results for general groups of type B_ℓ.

4.2. Equivariant Equations for $G^0 = G_1 \cdot \cdots \cdot G_r$, Where Each G_i Is of Type A_ℓ, C_ℓ, D_ℓ, E_6 or E_7

At the beginning of this section, we showed how one can reduce the problem under consideration to finding equivariant equations for *simply connected* groups of the same type, that is groups $G^0 = \prod G_i$, where each G_i is simply connected and of type $A_\ell, C_\ell, D_\ell, E_6$ or E_7. We shall restrict ourselves to groups of this form. Let $\mathscr{G}_i$ denote the Lie algebra of G_i and $\mathscr{G} = \bigoplus_{i=1}^r \mathscr{G}_i$. For each i, let $B_{i,1}, \ldots, B_{i,m_i}$ be the elements guaranteed to exist by Proposition 4.1. Let $\{p_{i,1}, \ldots, p_{i,m_i}\}_{i=1}^r$ be points on $\mathbf{C}\backslash\mathscr{S}$ having distinct projections. Corollary 2.3 implies that one can find an equivariant $B = \text{diag}(B_1, \ldots B_r) \in \mathscr{G}(K) = \bigoplus \mathscr{G}_i(K)$ with $B_i \in \mathscr{G}_i(K)$ such that in terms of the local coordinate t at the point $p_{i,j}$, the equation $Y' = B_iY$ has the form $dY/dt = (B_{i,j} +$ higher order terms$)Y$ and such that the equation is non-singular at the points $p_{j,k}$ for $j \neq i$.

Let E be the Picard-Vessiot extension of K corresponding to $Y' = BY$. Since $B \in \mathscr{G}(K)$, the proof of Proposition 1.31 of van der Put and Singer (1993) shows that we can assume that E is generated by the entries of an element $g \in G^0(E)$ such that $g' = Bg$. Writing $g = (g_1, \ldots, g_m)$, where each g_i is in G_i, we have that $g_i' = B_ig_i$ and so E contains the Picard-Vessiot extension $E_i = K(g_i)$ of K corresponding to each of the equations. From Proposition 4.1, we know that the Galois group of $Y' = B_iY$ over K is G_i. We shall now show that the Galois group G' of $Y' = BY$ over K is G^0.

Since $A \in \mathscr{G}(K)$, we have that $G' \subset G$ (see Proposition 1.31 of van der Put and Singer, 2003). Assume that $G' \neq G$. We will show that this implies that there exist indices $i \neq j$ such that E_i lies in an algebraic extension of E_j. We will see that comparing the local behavior of solutions of the corresponding differential equations at some $p_{i,k}$ will yield a contradiction.

A result of Kolchin (1968) (see also Exercise 8, Chapter V.23 of Kolchin, 1973) implies that there are indices $i \neq j$ and a homomorphism (defined over C) $f : G_i \to G_j/Z(G_j)$, where $Z(G_j)$ is the center of G_j, such that for every $h = (h_1, \ldots, h_m) \in G'$, $f(h_i) = \pi(h_j)$, where π is the canonical homomorphism $G_j \to G_j/Z(G_j)$. Note that since G_i and G_j are simple, the kernels of f and π are finite.

We now apply the maps f and π to the element $g = (g_1, \ldots, g_m) \in G^0(E)$ defined above. Since $f(g_i) = \pi(g_j)$, we have that E_i and E_j share the common subfield $K(f(g_i)) = K(\pi(g_j))$. Furthermore, E_i and E_j are algebraic extensions of this field since the kernels of f and π are finite. Therefore E_i is contained in an algebraic extension of E_j.

By construction, $Y' = B_jY$ is non-singular at each of the $p_{i,k}$ and so the solutions of $Y' = B_jY$ at $p_{i,k}$ have components in $C((t))$, where t is the local parameter at $p_{i,k}$. Therefore, we can embed E_j into $C((t))$. This implies that $Y' = B_iY$ has a fundamental set of solutions in an algebraic extension of $C((t))$ and so must be regular singular at this point (see Exercise 3.29 of van der Put and Singer, 2003). By construction, one of the points $p_{i,k}$ is not a regular singular point and so this is a contradiction. Therefore the Galois group of $Y' = BY$ is G.

5. AN ALTERNATE CONSTRUCTION FOR FINITE EXTENSIONS OF SL_2

In this section, we present an alternate method for constructing linear differential equations whose Galois groups are finite extensions of SL_2. In the previous sections, we considered groups of the form $H \ltimes G^0$, H a finite group and G^0 of the type considered above, and showed that for any realization of H as a Galois group of an extension K of $C(x)$, we could find an equivariant A such that $Y' = AY$ had Galois group G^0 over K. The construction described here begins by constructing a suitable K and so does not work over any such K. On the other hand, it introduces fewer singularities and uses group theoretic facts that may be of independent interest. This construction was motivated by the Example given by Julia Hartmann (2002, p. 42).

We begin with a modification of Lemma 5.11 of Bore and Serre (1964) (see also Lemma 10.10 of Wehrfritz, 1973). For any algebraic group G we define $\mathrm{Int}: G \to \mathrm{Aut}(G^0)$ to be the map that sends an element to the automorphism resulting from conjugation by that element.

Lemma 5.1. *Let G be a linear algebraic group, B a Borel subgroup of G and T a maximal torus of B.*

1. *There exists a finite subgroup W of G such that W normalizes B and T, and the natural projection $W \to G/G^0$ is surjective.*
2. *If, in addition, G^0 is semisimple and all automorphisms of G^0 are inner, then $\mathrm{Int}(W) \subset \mathrm{Int}(T)$ and so $\mathrm{Int}(W)$ is a finite abelian group. If $G^0 = \mathrm{SL}_2$ or PSL_2, then $\mathrm{Int}(W)$ is cyclic.*

Proof. 1. Let $N_G(B)$ be the normalizer of B in G and $N_G(B, T)$ be the subgroup of elements of $N_G(B)$ that normalize T as well. Since all Borel subgroups of G lie in G^0 and are conjugate in G^0 (see Humphreys, 1975, Theorem 21.3), we have that for any $g \in G$ there exists an $h \in G^0$ such that $gBg^{-1} = hBh^{-1}$. Therefore $h^{-1}g \in N_G(B)$ and we can conclude that $G = N_G(B) \cdot G^0$. Using the fact that the maximal tori of B are all conjugate in B (*loc. cit.* Theorem 19.3), we also have that $N_G(B) = N_G(B, T) \cdot B$. Lemma 10.10 of Wehrfritz (1973) implies that there exists a finite subgroup W of $N_G(B, T)$ such that the natural projection $W \to N_G(B, T)/N_G(B, T)^0$ is surjective. We then have that the projection $W \to G/G^0$ is surjective as well.

2. We refer to the proof of Theorem 27.4 of Humphreys (1975). Since all automorphisms of G^0 are inner, for any element $w \in W$ there is an element $h \in G^0$ such that for all $g \in G^0$, $wgw^{-1} = hgh^{-1}$. Since w normalizes B and T, we have that $\mathrm{Int}(W) \subset \mathrm{Int}(N_{G^0}(B, T))$. Since B is a Borel subgroup, we have that $N_{G^0}(B, T) \subset N_{G^0}(B) = B$. An element of B that normalizes T must lie in T (*loc. cit.* Proposition 19.4, Corollary 26.2A) so $\mathrm{Int}(W) \subset \mathrm{Int}(T)$. The final statement follows from the fact that a maximal torus of these groups has dimension 1. □

Let G be a linear algebraic group with G^0 semisimple and let $\mathcal{G}$ be its Lie algebra. If T is a maximal torus of G^0, then its Lie algebra $\mathcal{T}$ is a Cartan subalgebra of $\mathcal{G}$ and we can decompose

$$\mathcal{G} = \mathcal{T} \oplus \prod_{\alpha \in \Phi} \mathcal{G}_\alpha,$$

where Φ are the roots of $\mathcal{G}$, which we consider as multiplicative characters on T. If W is the finite group described in Corollary 5.1, then for any $\alpha \in \Phi$ and $w \in W$ we define $\alpha(w) = \alpha(t)$ for any $t \in T$ such that $\mathrm{Int}(w) = \mathrm{Int}(t)$. Since the elements of Φ factor through $\mathrm{Int}: G \to \mathrm{Aut}(G)$, each root in this way defines a multiplicative character on W.

Example 5.2. Let $G^0 = \mathrm{SL}_2$ and assume that T is the subgroup of diagonal matrices. As usual, we let

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

$\mathcal{T}$ is spanned by h and there are two roots α and $-\alpha$ with $\mathcal{G}_\alpha$ being spanned by e and $\mathcal{G}_{-\alpha}$ by f. Furthermore, considering the roots as characters on T, we have that

$$\alpha\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = a^2,$$

$$-\alpha\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = a^{-2}.$$

Let $G = \mathrm{SL}_2 \ltimes \{1, -1\}$, where the action of -1 on SL_2 is given by conjugation by the matrix

$$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}.$$

We then have that $\mathrm{Int}(W) = \mathrm{Int}(H)$, where $W = \{1, -1\}$ and H is the order four cyclic subgroup of SL_2 generated by the above matrix. Note that α can be considered as the character on W given by $\alpha(-1) = -1$. □

Let G be an algebraic group with $G^0 = \mathrm{SL}_2$ and let W be as in Lemma 5.1. We shall construct a differential equation having $W \ltimes G^0$ as its Galois group over $C(x)$. The group G will then be the Galois group of a subfield $\widetilde{E}$ of the Picard-Vessiot extension E of $C(x)$ corresponding to this former equation.

We now use the notation G to denote the group $\mathrm{SL}_2 \ltimes W$, and $\mathcal{G}$ to denote the Lie algebra of G. Conjugation by an element of W induces an automorphism of G and also an automorphism of $\mathcal{G}$, which we again denote by conjugation. If K is any field containing C and $X = ah + be + cf \in \mathcal{G}(K)$, $a, b, c \in K$, then, for $w \in W$

$$w^{-1}Xw = ah + b\alpha(w^{-1})e + c(-\alpha(w^{-1})f).$$

Note that if the image of W in $\mathrm{Aut}(G)$ has order n, then α maps W onto the group of nth roots of unity. We identfy this with the Galois group of $C(x, x^{1/n})$. Let K be a Galois extension of $C(x)$ with Galois group W such that the fixed field of the kernel of α is $C(x, x^{1/n})$, $x' = 1$ and the action of W on this latter field is given by α. Theorem 7.13 of Volklein (1996) implies that such a field exists. Let

$$\widetilde{A} = x^{-1/n}e + x^{1/n}f + x^2h.$$

To construct a differential equation whose Galois group is G, Proposition 5.2 of Mitschi and Singer (2002) implies that it is enough to prove the following proposition.

Proposition 5.3. *$\widetilde{A}$ is equivariant and the differential Galois group of $Y' = \widetilde{A}Y$ over $C(x, x^{1/n})$ is SL_2.*

Proof. To prove the claim about the Galois group, we make a change of variables $x = z^n$. We then get a new equation $\frac{dY}{dz} = AY$, where

$$A = n(z^{n-2}e + z^n f + z^{3n-1}h).$$

We will use the techniques of Mitschi and Singer (1996) to show that $\frac{dY}{dz} = AY$ has differential Galois group SL_2 over $C(z)$.

Assuming that this latter fact is true, we claim that the differential Galois group of $Y' = \widetilde{A}Y$ over $C(x, x^{1/n})$ is SL_2. To see this, let K be a Picard-Vessiot extension of $C(z) = C(x^{1/n})$ for $\frac{dY}{dz} = AY$. Since K has no new $\frac{d}{dz}$-constants, it has no new $\frac{d}{dx}$-constants. Furthermore, since the elements of SL_2 commute with $\frac{d}{dz}$ and leave $C(z)$ fixed, they will commute with $\frac{d}{dx} = \frac{1}{nz^{n-1}}\frac{d}{dz}$. Therefore, SL_2 is a subgroup of the differential Galois group G of $K/C(z)$ with respect to $\frac{d}{dx}$. From the form of $\widetilde{A}$, we see that $G \subset \mathrm{SL}_2$, so the claim is proven.

We now proceed to show that $\frac{dY}{dz} = AY$ has differential Galois group SL_2 over $C(z)$. Since C^2 is a Chevalley module for SL_2, Lemma 3.3 of Mitschi and Singer (1996) implies that it is enough to show that if

$$c = c_{3n-1}z^{3n-1} + \cdots + c_0 \in C[z] \text{ and } w = w_m z^m + \cdots + w_0 \in C^2 \otimes C[z]$$

and

$$w' - n[z^{n-2}e + z^n f + z^{3n-1}h - cI]w = 0, \tag{4}$$

then $w = 0$.

To simplify notation, we let $u = \binom{1}{0}$ and $v = \binom{0}{1}$. These generate the root spaces of SL_2 and $eu = 0$, $ev = u$, $fu = v$, $fv = 0$, and u, v are eigenvectors of h. The proof of the above fact proceeds by considering the coefficients of powers of z in Eqn. (4). The highest power of z that can appear is z^{3n-1+m} and its coefficient is

$$n(c_{3n-1}I - h)w_m = 0.$$

We therefore have that w_m is an eigenvector of h and so we can assume that $w_m = u$, $c_{3n-1} = 1$ or $w_m = v$, $c_{3n-1} = -1$. Let us assume that $w_m = u$ and $c_{3n-1} = 1$. We shall write $w = pu + qv$, where $p, q \in C[z]$, $p = z^m +$ lower degree terms, and $q =$ a polynomial of degree at most $m - 1$. Substituting $w = pu + qv$ into Eqn. (4), we have

$$(p' - nz^{n-2}q - nz^{3n-1}p + ncp)u + (q' - nz^n p + nz^{3n-1}q + nqc)v = 0$$

and therefore

$$p' - n(z^{3n-1} - c)p = nz^{n-2}q, \tag{5}$$

$$q' + n(z^{3n-1} + c)q = nz^n p. \tag{6}$$

The right hand side of Eqn. (6) has degree $n + m$. Since $z^{3n-1} + c$ has degree $3n - 1$, q must have degree $m - 2n + 1$. Therefore, the right hand side of Eqn. (5)

has degree $m-n-1$, while the degree of $(z^{2n-1}-c)p$ is at least m if $z^{3n-1}-c \neq 0$. Therefore, we have $c = z^{3n-1}$ and $p' = nz^{n-2}q$. Comparing degrees in this last equation, we have $m-1 = n-2+m-2n+1 = m-n-1$ so $n=0$, a contradiction, unless $w=0$. If $w_m = v$ and $c_{3m-1} = -1$ one argues in a similar way to also show that $w=0$. □

ACKNOWLEDGMENTS

We wish to thank the late A. Bolibrukh and R. Schäfke for showing us how to select the local form of a differential equation so that Katz's Criterion ensures it is irreducible.

The third author would like to thank the Institut de Recherche Mathématique Avancée, Université Louis Pasteur et C.N.R.S., for its hospitality and support during the preparation of this article. The preparation was also supported by NSF Grant CCR- 0096842.

REFERENCES

Babbitt, D. G., Varadarajan, V. S. (1983). Formal reduction of meromorphic differential equations: a group theoretic view. *Pacific J. Math.* 109(1):1–80.

Bore, A., Serre, J.-P. (1964). Théorèmes de finitude en cohomologie galoisienne. *Comment. Math. Helv.* 39:111–164.

Bourbaki, N. (1990). *Groupes et Algèbres de Lie, Chaps. 4,5 and 6*. Paris: Masson.

Bourbaki, N. (1990). *Groupes et Algèbres de Lie, Chaps. 7 and 8*. Paris: Masson.

Fulton, W., Harris, J. (1991). *Representation Theory. A First Course*. Vol. 129. of Graduate Texts in Mathematics. New York: Springer.

Hartmann, J. (2002). On the Inverse Problem in Differential Galois Theory. Ph.D. Thesis, University of Heidelberg. Available at www.ub.uni-heidelberg.de/archiv/3085).

Hochschild, G. (1976). *Basic Theory of Algebraic Groups and Lie Algebras*. Vol. 75. Graduate Texts in Mathematics. Berlin: Springer Verlag.

Hrushovski, E. (2002). Computing the Galois group of a linear differential equation. *Differential Galois Theory*. Vol. 58 of Banach Center Publications. Warszawa: Institute of Mathematics. Polish Academy of Sciences, pp. 97–138.

Humphreys, J. (1975). *Linear Algebraic Groups*. Graduate Texts in Mathematics. New York: Springer-Verlag.

Katz, N. (1987). On the calculation of some differential Galois groups. *Inventiones Mathematicae* 87:13–61.

Kolchin, E. R. (1968). Algebraic groups and algebraic dependence. *Am. J. Math.* 90:1151–1164.

Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups*. New York: Academic Press.

Kovacic, J. (1969). The inverse problem in the Galois theory of differential fields. *Ann. Math.* 89:583–608.

Kovacic, J. (1971). On the inverse problem in the Galois theory of differential fields. *Ann. Math.* 93:269–284.

Lang, S. (1993). *Algebra*. 3rd ed. New York: Addison Wesley.

Mitschi, C., Singer, M. F. (1996). Connected linear groups as differential Galois groups. *J. Alg.* 184:333–361.

Mitschi, C., Singer, M. F. (2002). Solvable-by-finite groups as differential Galois groups. *Ann. Fac. Sci. Toulouse* XI(3):403–423.

van der Put, M., Singer, M. F. (1997). *Galois Theory of Difference Equations*. Vol. 1666 of Lecture Notes in Mathematics. Heidelberg: Springer-Verlag.

van der Put, M., Singer, M. F. (2003). *Galois Theory of Linear Differential Equations*. Vol. 328 of Grundlehren der Mathematischen Wissenshaften. Heidelberg: Springer.

Singer, M. F. (1993). Moduli of linear differential equations on the Riemann sphere with fixed Galois group. *Pac. J. Math.* 106(2):343–395.

Tits, J. (1967). *Tabellen zu den einfachen Lie Gruppen und ihren Darstellungen*. Vol. 40 of Lecture Notes in Mathematics. Heidelberg: Springer-Verlag.

Volklein, H. (1996). *Groups as Galois Groups*. Vol. 53 of Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press.

Wehrfritz, B. A. F. (1973). *Infinite Linear Groups*. Ergebnisse der Mathematik. Berlin: Springer-Verlag.