

*Pacific  
Journal of  
Mathematics*

**MODULI OF LINEAR DIFFERENTIAL EQUATIONS ON THE  
RIEMANN SPHERE WITH FIXED GALOIS GROUPS**

MICHAEL SINGER

*Pacific  
Journal of  
Mathematics*

**MODULI OF LINEAR DIFFERENTIAL EQUATIONS ON THE  
RIEMANN SPHERE WITH FIXED GALOIS GROUPS**

MICHAEL SINGER

# MODULI OF LINEAR DIFFERENTIAL EQUATIONS ON THE RIEMANN SPHERE WITH FIXED GALOIS GROUPS

MICHAEL F. SINGER

**For fixed  $m$  and  $n$ , we consider the vector space of linear differential equations of order  $n$  whose coefficients are polynomials of degree at most  $m$ . We show that for  $G$  in a large class of linear algebraic groups, if we fix the exponents and determining factors at the singular points (but not the singular points themselves) then the set of such differential equations with this fixed data, fixed Galois group  $G$  and fixed  $G$ -module for the solution space forms a constructible set (i.e., an element of the Boolean algebra generated by the Zariski closed sets). Our class of groups includes finite groups, connected groups, and groups whose connected component of the identity is semisimple or unipotent. We give an example of a group for which this result is false and also apply this result to the inverse problem in differential Galois theory.**

**1. Introduction.** In this paper we consider the set  $\mathcal{L}(n, m)$  of homogeneous linear differential equations

$$(1) \quad L(y) = a_n(x)y^{(n)} + \cdots + a_0(x) = \sum_{i=0}^n \sum_{j=0}^m a_{ij}x^j y^{(i)}$$

of order at most  $n$  whose coefficients are polynomials of degree at most  $m$  with complex coefficients. By identifying  $L \in \mathcal{L}(n, m)$  with the vector  $(a_{ij})$ , one sees that  $\mathcal{L}(n, m)$  may be identified with an affine space  $\mathbb{C}^{(n+1)(m+1)}$ . Let  $G$  be a linear algebraic group and  $V$  a  $G$ -module. One would like to understand the structure of  $\mathcal{L}(n, m, G, V)$ , the set of  $L \in \mathcal{L}(n, m)$  with Galois group  $\text{Gal}(L)$  equal to  $G$  and having solution space  $\text{Soln}(L)$  isomorphic to  $V$  as a  $G$ -module. In general  $\mathcal{L}(n, m, G, V)$  is not a Zariski closed subset of  $\mathcal{L}(n, m)$  or even a constructible subset of  $\mathcal{L}(n, m)$  (i.e. an element of the Boolean algebra generated by the Zariski closed sets). To see this consider the family of equations  $L_c(y) = xy' - cy = 0$ ,  $c \in \mathbb{C}$ . The Galois group is a subgroup of  $\mathbb{C}^*$ , the multiplicative group of nonzero complex numbers. It equals  $\mathbb{C}^*$  if and only if  $c$  is not a rational number. If  $c = p/q$ ,  $p, q \in \mathbb{Z}$ ,  $(p, q) = 1$ , then  $\text{Gal}(L_c) =$

$\mathbb{Z}/q\mathbb{Z}$ . Therefore  $\mathcal{L}(1, 1, \mathbb{C}^*, \mathbb{C})$  is not constructible. Another example is the family  $L_{a,b}(y) = y'' - (a+b)y' + aby = 0$ ,  $a \neq b \in \mathbb{C}$ . A fundamental set of solutions is  $\{e^{ax}, e^{bx}\}$  and  $\text{Gal}(L_{a,b}) \subset \mathbb{C}^* \times \mathbb{C}^*$  with equality if and only if  $a$  and  $b$  are linearly independent over  $\mathbb{Q}$ . Therefore  $\mathcal{L}(2, 0, \mathbb{C}^* \times \mathbb{C}^*, \mathbb{C}^2)$  is not constructible. Note that in the first example  $c$  is an exponent at the singular point 0 and in the second example  $ax$  and  $bx$  are determining factors at infinity (see §2(c) for precise definitions). In this paper we show that for  $G$  in a large class of linear algebraic groups, if we fix the exponents and determining factors at the singular points (but not the singular points themselves) then we can insure constructibility of the set of linear differential equations with this fixed data, fixed Galois group  $G$  and fixed  $G$ -module for the solution space.

To make this precise, let  $\mathcal{W}$  be a finite set consisting of elements of  $\mathbb{C}$ . We denote by  $\mathcal{L}(n, m, \mathcal{W})$  the set of  $L \in \mathcal{L}(n, m)$  such that at any singular point  $\alpha$  of  $L$ , the exponents at  $\alpha$  belong to  $\mathcal{W}$ . We refer to  $\mathcal{W}$  as a set of weak local data.  $\mathcal{L}(n, m, \mathcal{W})$  is a constructible set. Let  $\mathcal{L}(n, m, \mathcal{W}, G, V) = \mathcal{L}(n, m, \mathcal{W}) \cap \mathcal{L}(n, m, G, V)$ . If  $G$  is a linear algebraic group and  $G^\circ$  is its connected component of the identity, we denote by  $\text{Ker } X(G^\circ)$  the intersection of all characters  $\chi: G^\circ \rightarrow \mathbb{C}^*$  of  $G^\circ$ . Theorem 3.14 below implies that if  $G^\circ = \text{Ker } X(G^\circ)$ , then for fixed  $G$ -module  $V$  and fixed  $n, m$  and  $\mathcal{W}$ ,  $\mathcal{L}(n, m, \mathcal{W}, G, V)$  is a constructible set. In particular, if  $G$  is finite or if  $G^\circ$  is semisimple or unipotent, then this result holds. In §3, following this result, we present an example (due to Deligne) of a parameterized family of second order fuchsian linear differential equations with fixed exponents such that for all parameters the Galois group will be a subgroup of  $\mathbb{C}^* \times \mathbb{Z}/2\mathbb{Z}$  but such that the set of parameters for which the Galois group is  $\mathbb{C}^* \times \mathbb{Z}/2\mathbb{Z}$  is not constructible. This shows that if  $G^\circ \neq \text{Ker } X(G^\circ)$ , it is not generally true that  $\mathcal{L}(n, m, \mathcal{W}, G, V)$  is constructible. Nonetheless, we are able to weaken the assumption that  $G^\circ = \text{Ker } X(G^\circ)$  in the following way.

Let  $\mathcal{D}$  be a finite set consisting of elements of  $\mathbb{C}$  and polynomials with coefficients in  $\mathbb{C}$ . We denote by  $\mathcal{L}(n, m, \mathcal{D})$  the set of  $L \in \mathcal{L}(n, m)$  such that at any singular point  $\alpha$  of  $L$ , the exponents and the determining factors at  $\alpha$  belong to  $\mathcal{D}$ . We refer to  $\mathcal{D}$  as a set of local data.  $\mathcal{L}(n, m, \mathcal{D})$  is a constructible set. Let  $\mathcal{L}(n, m, \mathcal{D}, G, V) = \mathcal{L}(n, m, \mathcal{D}) \cap \mathcal{L}(n, m, G, V)$ . Deligne's example shows that, in general,  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is also not constructible. For arbitrary  $G$ ,  $\text{Ker } X(G^\circ)$  is not only a normal sub-

group of  $G^\circ$  but also a normal subgroup of  $G$  and  $G^\circ/\text{Ker } X(G^\circ)$  is a torus. There is a natural action of  $G/G^\circ$  on  $G^\circ/\text{Ker } X(G^\circ)$ . Theorem 3.16 below states that if the action of  $G/G^\circ$  on  $G^\circ/\text{Ker } X(G^\circ)$  is trivial, then for any fixed  $G$ -module  $V$  and fixed  $n, m$  and  $\mathcal{L}$ ,  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is a constructible set. In particular, if  $G$  is connected,  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is constructible. We also give an example to show that one must fix both the exponents and the determining factors and not just the exponents as in Theorem 3.14.

When one restricts oneself to linear differential equations with only regular singular points (the fuchsian equations), the parameters remaining free after one fixes the exponents at the singularities are called accessory parameters (see [HI15] for a discussion of this classical notion). Our main result states that if the action of  $G/G^\circ$  on  $G^\circ/\text{Ker } X(G^\circ)$  is trivial, then when one fixes the exponents of a fuchsian equation, algebraic conditions on the accessory parameters and the singular points determine if the equation has Galois group  $G$ .

Phenomena similar to our main results are known to already occur when one looks at the Lamé equation:

$$L_{n,B,e_3}(y) = f(x)y'' + \frac{1}{2}f'(x)y' - (n(n+1)x + B)y,$$

where  $f(x) = 4(x - e_1)(x - e_2)(x - e_3)$ , the  $e_i$  are distinct,  $e_1$  is fixed and  $e_1 + e_2 + e_3 = 0$ . The exponents at each  $e_i$  are 0 and  $1/2$ . At infinity the exponents are  $-n/2$  and  $(n+1)/2$ . Several authors have investigated the problem of determining those  $n, B$  and  $e_3$  such that  $L_{n,B,e_3}(y) = 0$  has only algebraic solutions. In this case the Galois group  $G \subset \text{GL}(2, \mathbb{C})$  will be finite and coincide with the monodromy group (see [SI81] or the discussion in §4 of this paper). Brioschi showed (see [POO66], §37) that if  $n + \frac{1}{2}$  is an integer, there is a non-zero polynomial  $p \in \mathbb{Q}[u, v]$  of degree  $n + \frac{1}{2}$  in  $v$  such that  $L_{n,B,e_3}(y) = 0$  has only algebraic solutions if and only if  $p(e_3, B) = 0$ . Furthermore, he showed that if this is the case, the image of  $G$  in  $\text{PGL}(2, \mathbb{C})$  is the non-cyclic abelian group of order 4. Baldassari [BA81], [BA89], Chiarellotto [CH89], and Dwork [DW90a] have also studied algebraic solutions of the Lamé equation. Dwork shows that if  $2n$  is not an integer then, for fixed  $n$ , there are only a finite number of pairs  $(e_3, B)$  such that  $G$  is finite. This is a consequence of the following general result of Dwork. Consider the set of second order fuchsian homogeneous linear differential equations with  $m + 1$  singular points. Assume that three are fixed at  $0, 1, \infty$  and that the Wronskian is constant. Fix the exponent differences,  $\mu_1, \dots, \mu_{m+1}$  in  $\mathbb{Q}$  and assume the  $i$ th singular point is apparent

(resp. regular) if  $\mu_i \in \mathbb{Z}$ ,  $\mu_i \geq 2$  (resp.  $\mu_i = 1$ ). Dwork shows that if we fix a finite subgroup  $G'$  of  $\mathrm{PGL}(2, \mathbb{C})$ , then the set of such equations whose Galois group has image  $G'$  in  $\mathrm{PGL}(2, \mathbb{C})$  is a  $\mathbb{Q}$ -constructible set of dimension bounded by  $\mathrm{Inf}(\rho, m - 2)$  where  $\rho$  is the number of  $i$  such that  $\mu_i \in \mathbb{Z}$ ,  $\mu_i \geq 1$ . (For the Lamé equation, if  $2n$  is not an integer, the projective image of the Galois group is either the octahedral or icosahedral group.) Dwork's proof relies heavily on the fact that such an equation must be the weak pullback of a hypergeometric equation whose exponent differences appear in a list compiled originally by H. A. Schwarz. For higher order equations or infinite groups there does not seem to be a similar fact. The proof of our main result proceeds in a different manner, which we now outline.

Let  $G$  be a linear algebraic group,  $\mathscr{W}$  a set of weak local data and  $\mathscr{D}$  a set of local data. One of the key ideas in this paper is that knowing  $n$  and  $m$  and having a bound on the exponents of some  $L \in \mathscr{L}(n, m)$  allows us to bound a priori the exponents and degrees of coefficients of operators  $L_1$  and  $L_2$  such that  $L(y) = L_1(L_2(y))$ . This information also allows us to bound the exponents and degrees of the coefficients of certain auxiliary equations that we construct from  $L$ . This will be used in the following way. For example, it is known that  $\mathrm{Gal}(L) \subset \mathrm{SL}(n)$  if and only if  $\mathrm{Wr}(y_1, \dots, y_n) = R(x) \in \mathbb{C}(x)$  where  $\mathrm{Wr}$  is the Wronskian determinant and  $\{y_1, \dots, y_n\}$  is a basis of  $\mathrm{Soln}(L)$ . Knowing that  $L \in \mathscr{L}(n, m, \mathscr{W})$  allows us to find an  $N$  that bounds the degrees of the numerators and denominators of possible  $R(x) \in \mathbb{C}(x)$  (in fact, to find  $N$  it is enough to assume  $L \in \mathscr{L}(n, m)$  and to have a bound  $B$  on the real parts of exponents of  $L$ ). Therefore for  $L \in \mathscr{L}(n, m, \mathscr{W})$ ,  $\mathrm{Gal}(L) \subset \mathrm{SL}(n)$  is equivalent to the statement "There exists a basis  $\{y_1, \dots, y_n\}$  of  $\mathrm{Soln}(L)$  and a rational function  $R(x)$  whose numerator and denominator have degree  $\leq N$  such that  $\mathrm{Wr}(y_1, \dots, y_n) = R(x)$ ." We use elimination theory to show that this is a constructible condition. We note that we not only use the usual elimination theory for algebraic sets but also use the elimination theory for differential algebraic sets (originally due to Seidenberg, [SEI56]; see §3(a)). In a similar way we can show that for any group  $G$ , the condition " $\mathrm{Gal}(L) \subset G$ " is constructible (Proposition 3.1). This is enough to show that  $\mathscr{L}(n, m, \mathscr{W}, G, V_i)$  is constructible when  $G$  is finite, since  $G$  then has only a finite number of subgroups and constructible sets form a Boolean algebra. This also allows us to show that if  $\mathrm{Gal}(L) \subset G$ , " $\mathrm{Gal}(L)$  is mapped surjectively onto  $G/G^\circ$  by  $\pi: G \rightarrow G/G^\circ$ " is constructible.

Assuming  $\text{Gal}(L) \subset G$ , we then show that “ $\text{Ker } X(G^\circ) \subset \text{Gal}(L)$ ” is a constructible condition. To do this, we need the following concept. If  $V$  is a  $G$ -module and  $\chi$  is a character, we let  $V_\chi = \{v \in V \mid g \cdot v = \chi(g) \cdot v \text{ for all } g \in G\}$ . For distinct  $\chi_1, \chi_2$ ,  $V_{\chi_1}$  and  $V_{\chi_2}$  are independent. Let  $\text{Ch}_G(V) = \bigoplus V_\chi$ , the sum being over all characters. We show that for any  $G$  there is a  $G$ -module  $W$  such that if  $H$  is a subgroup of  $G$ , then  $\text{Ker}(G^\circ) \subset H$  if and only if  $\text{Ch}_{G^\circ}(W) = \text{Ch}_{H \cap G^\circ}(W)$ . We also show that if  $\text{Gal}(L) \subset G$ , then  $W$  is isomorphic to a  $\text{Gal}(L)$  submodule of  $K$ , the Picard-Vessiot extension of  $\mathbb{C}(x)$  associated to  $L$ . Furthermore,  $W = \text{Soln}(\bar{L})$  for some  $\bar{L}$  whose order, degree of coefficients and weak local data can be determined from weak local data for  $L$ . The condition that  $\text{Ch}_{G^\circ}(W) = \text{Ch}_{\text{Gal}(L) \cap G^\circ}(W)$  is then shown to be equivalent to certain factorization properties of  $\bar{L}$  and these are constructible properties because we have bounds on the exponents and degrees of the coefficients of  $\bar{L}$ .

Given the facts that  $\text{Gal}(L) \subset G$ ,  $\text{Gal}(L)$  is mapped surjectively onto  $G/G^\circ$  by  $\pi: G \rightarrow G/G^\circ$  and  $\text{Ker } X(G^\circ) \subset \text{Gal}(L)$ , we need only show that  $\dim(\text{Gal}(L)^\circ/\text{Ker } X(G^\circ)) = \dim(G^\circ/\text{Ker } X(G^\circ))$  to conclude that  $G = \text{Gal}(L)$ . We show that  $\dim(\text{Gal}(L)^\circ/\text{Ker } X(G^\circ)) = \dim(G^\circ/\text{Ker } X(G^\circ))$  is equivalent (under the assumption that  $G/G^\circ$  acts trivially on  $G^\circ/\text{Ker } X(G^\circ)$ ) to the statement that  $K$  contains  $\dim(G^\circ/\text{Ker } X(G^\circ))$  algebraically independent elements  $z_i$  such that  $z'_i/z_i \in \mathbb{C}(x)$ . Knowing local data  $\mathcal{D}$  for  $L$  (and not just a bound) allows us to show that this condition is also constructible.

The rest of the paper is organized as follows. In §2 we present facts from group theory, Galois theory and the structure theory of singular points of linear differential equations that are needed in subsequent sections. In §3 we discuss the elimination theory needed to show sets are constructible, use this to show various subsets of  $\mathcal{L}(n, m)$  are constructible and prove the main results. In §4 we give two applications of Theorem 3.14. In the first, we show, using results of [DW90b] and [KA70], that the set of  $L(y) \in \mathcal{L}(n, m)$  having fixed finite Galois group,  $k$  singular points and fixed exponents has dimension at most  $k$ . In the second application, we are able to show, by refining techniques of [TT79], that for any connected linear algebraic group defined over  $C \subset \mathbb{C}$  and any faithful  $G$ -module  $V$  of dimension  $n$  defined over  $C$ , there is an integer  $m$  and a finite set  $S \subset C$  such that  $\mathcal{L}(n, m, S, G, V)$  is not empty. We show that this in turn implies that any linear algebraic group  $G$ , defined over an algebraically

closed field  $C$  of characteristic zero, with  $G/G^\circ$  acting trivially on  $G^\circ/\text{Ker } X(G^\circ)$ , is the differential Galois group of a homogeneous linear differential equation with coefficients in  $C(x)$ ,  $x' = 1$ . To do this it is important that we show that all the constructible sets we deal with are defined over  $C$ .

The author wishes to thank P. Deligne for many helpful comments on earlier manuscripts. In particular he suggested that one should think of a connected group  $G$  in terms of  $\text{Ker } X(G)$  and  $G/\text{Ker } X(G)$  and that invariant lines in some representation would guarantee that a subgroup of  $G$  contains  $\text{Ker } X(G)$ . B. Dwork also made many helpful comments and suggested the application in §4(a). We would also like to thank A. Duval and M. Loday-Richaud for allowing us to see the preprint [DL89] which contains calculations that helped us formulate Theorem 3.16. Some of the results presented here were formulated and proved at the Université Louis Pasteur in Strasbourg during a visit in May 1989. We would like to thank the mathematicians at this institution, and especially C. Mitschi, J.-P. Ramis and the late J. Martinet for their intellectual as well as financial support.

## 2. Ancillary results.

*a. Group theory.* In this section we investigate the following problem: Given a connected algebraic group  $G$ , does there exist a representation of  $G$  in which we can distinguish  $G$  from *all* of its subgroups  $H$  using invariant subspaces, that is, in which for any subgroup  $H$ , there is an  $H$  invariant subspace not left invariant by  $G$ ? As we shall see (cf. the discussion following Proposition 2.7), this is not true in general. Our main result (Proposition 2.9) implies that we can find a representation such that if  $H$  cannot be distinguished from  $G$  by an invariant line then  $H$  contains the intersection of the kernels of all characters of  $G$ . Let  $C$  be an algebraically closed field of characteristic zero, let  $G$  be a linear algebraic group defined over  $C$  and let  $V$  be a  $G$ -module. In this paper, all  $G$ -modules are assumed to be finite dimensional. If  $\chi: G \rightarrow C^*$  is a character of  $G$ , we define the  $\chi$ -space  $V_\chi$  of  $V$  to be  $\{v \mid g \cdot v = \chi(g) \cdot v \text{ for all } g \in G\}$ . Note that non-zero elements of different  $\chi$ -spaces are linearly independent and therefore that  $V_\chi \neq \{0\}$  for only a finite number of  $\chi$ . The *character submodule*  $\text{Ch}_G(V)$  of  $V$  is defined to be  $\bigoplus V_\chi$  where the sum is over all characters of  $G$ . Let  $X(G)$  be the group of characters of  $G$  and let  $\text{Ker } X(G) = \bigcap_{\chi \in X(G)} \text{Ker}(\chi)$ .  $\text{Ker } X(G)$  is a normal subgroup of  $G$ .  $X(G)$  is a finitely generated abelian group ([HUM81], p. 103)

so  $\text{Ker } X(G) = \bigcap_{i=1}^m \text{Ker}(\chi_i)$  for some finite set of characters. If  $G$  is connected, then  $X(G)$  is torsion free so  $(\chi_1, \dots, \chi_m): G \rightarrow (C^*)^m$  maps  $G$  onto a torus. Therefore, if  $G$  is connected,  $G/\text{Ker } X(G)$  is a torus. If  $V$  is a  $G$ -module and  $H$  is a subgroup of  $G$ , we define  $V^H = \{v | hv = v \text{ for all } h \in H\}$ .

We begin by giving a group theoretical characterization of  $\text{Ker } X(G)$ . A Levi factor of  $G$  is a reductive group  $P$  such that  $G = R_u(G) \rtimes P$  is the semidirect product of  $P$  and the unipotent radical  $R_u(G)$ . In characteristic 0, Levi factors exist and are all conjugate. Furthermore, if  $H$  is a connected reductive subgroup of  $G$ , then  $H$  belongs to some Levi factor of  $G$  ([MO56]).

**LEMMA 2.1.** *Let  $G$  be a connected linear algebraic group,  $R_u(G)$  be its unipotent radical and  $P$  a Levi factor.  $\text{Ker } X(G)$  is the group generated by  $(P, P)$  and  $R_u(G)$ . Furthermore, all characters of  $\text{Ker } X(G)$  are trivial and  $\text{Ker } X(G)$  is connected.*

*Proof.* Any character of  $G$  is trivial on  $(P, P)$  and  $R_u(G)$  so these groups are contained in  $\text{Ker } X(G)$ . To prove the other inclusion note that since  $P$  is reductive,  $P = (P, P) \cdot T$  where  $T$  is a central torus of  $P$  ([HUM81], p. 125 and p. 168). Since  $G = R_u(G) \rtimes P = R_u(G) \rtimes ((P, P) \cdot T)$ , we see that  $R_u(G) \cdot (P, P)$  is a closed normal subgroup of  $G$  such that the quotient is a torus. Therefore  $R_u(G) \cdot (P, P) \supset \text{Ker } X(G)$ . Note that  $(P, P)$  is semisimple so all of its characters are trivial. Since all characters of  $R_u(G)$  are trivial, all characters of  $\text{Ker } X(G)$  are trivial. Since  $R_u(G)$  and  $(P, P)$  are connected,  $\text{Ker } X(G)$  is connected. □

**LEMMA 2.2.** *Let  $G$  be a connected algebraic group and  $V$  a  $G$ -module then  $\text{Ch}_G(V) = V^{\text{Ker } X(G)}$ .*

*Proof.* Since  $\text{Ch}_G(V)$  is the sum  $V_{\chi_1} \oplus \dots \oplus V_{\chi_n}$  of  $\chi$ -spaces and each  $\chi_i$  is trivial on  $\text{Ker } X(G)$ , we have  $\text{Ch}_G(V) \subset V^{\text{Ker } X(G)}$ . On the other hand,  $V^{\text{Ker } X(G)}$  is a  $G$ -submodule of  $V$  and the action of  $G$  on  $V^{\text{Ker } X(G)}$  factors through the action of  $G/\text{Ker } X(G)$  on  $V$ . Since  $G/\text{Ker } X(G)$  is a torus, this action is diagonalizable so  $V^{\text{Ker } X(G)} \subset \text{Ch}_G(V)$ . □

**LEMMA 2.3.** *Let  $G$  be a connected linear algebraic group,  $V$  a  $G$ -module and  $H$  a subgroup of  $G$  such that  $\text{Ker } X(G) \subset H$ . Then  $\text{Ch}_H(V) = \text{Ch}_G(V)$ .*

*Proof.* We have  $\text{Ch}_G(V) \subset \text{Ch}_H(V) \subset \text{Ch}_{\text{Ker } X(G)}$ . Since

$$\text{Ch}_{\text{Ker } X(G)}(V) = V^{\text{Ker } X(G)} = \text{Ch}_G(V),$$

we can conclude  $\text{Ch}_H(V) = \text{Ch}_G(V)$ . □

Our aim now is to show that for an appropriately chosen  $V$ , the converse of Lemma 2.3 is true (Proposition 2.9).

**LEMMA 2.4.** *Let  $G$  be a connected semisimple linear algebraic group. There exists a  $G$ -module  $V$  such that for any proper connected subgroup  $H$ ,  $\text{Ch}_G(V) \subsetneq \text{Ch}_H(V)$ .*

*Proof.* For any subgroup  $H$  of  $G$ , there exists a  $G$ -module  $W_H$  and a one dimensional subspace  $L_H \subset W_H$  such that  $H = \{g \in G \mid g \cdot L_H = L_H\}$  ([HUM81], p. 80).  $G$  has, up to conjugacy, only finitely many maximal proper closed connected subgroups, say  $H_1, \dots, H_n$  ([DY52]). Since  $G$  is semisimple,  $G = (G, G)$  so any character of  $G$  is trivial. Therefore for any  $G$ -module,  $\text{Ch}_G(V) = V^G$ . This implies  $\text{Ch}_G(W_{H_i}) \subsetneq \text{Ch}_{H_i}(W_{H_i})$  for  $i = 1, \dots, n$ . Therefore  $V = W_{H_1} \oplus \dots \oplus W_{H_n}$  satisfies the conclusion of the lemma. □

**LEMMA 2.5.** *Let  $G$  be a connected reductive group. There exists a  $G$ -module  $V$  such that for any connected subgroup  $H$  of  $G$ , if  $\text{Ch}_H(V) = \text{Ch}_G(V)$ , then  $\text{Ker } X(G) \subset H$ .*

*Proof.* We first note that since  $G$  is reductive,  $R_u(G)$  is trivial. Therefore  $\text{Ker } X(G) = (G, G)$ . Let  $G = (G, G) \cdot T$  where  $T$  is a central torus. Let  $\pi: G \rightarrow G/R(G)$  be the canonical projection and  $H$  a connected subgroup of  $G$  such that  $\pi(H) = \pi(G)$ . We claim that  $\text{Ker } X(G) = (G, G) \subset H$ . To see this let  $y = y_1 y_2 y_1^{-1} y_2^{-1}$ . We write  $y_1 = h_1 c_1$ ,  $y_2 = h_2 c_2$ ,  $h_1, h_2 \in H$ ,  $c_1, c_2 \in T$ . Since the  $c_i$  are central  $y = h_1 h_2 h_1^{-1} h_2^{-1} \in H$ , so  $(G, G) \subset H$ .

To construct  $V$ , note that  $G/R(G)$  is semisimple. Let  $V$  be the  $G/R(G)$  module (and, a fortiori, a  $G$ -module) guaranteed to exist by Lemma 2.4. By the above remarks, for any connected subgroup  $H$  of  $G$  we have that either  $\pi(H)$  is a proper subgroup of  $G/R(G)$  or  $\text{Ker } X(G) = (G, G) \subset H$ . Therefore if  $H$  is a connected subgroup of  $G$  and  $\text{Ch}_H(V) = \text{Ch}_G(V)$ , then  $\pi(H) = G/R(G)$  so  $\text{Ker } X(G) \subset H$ . □

**LEMMA 2.6.** *Let  $G$  be a connected linear algebraic group. There exists a  $G$ -module  $V$  such that if  $H$  is a closed connected subgroup of  $G$  with  $R_u(H) \subsetneq R_u(G)$  then  $\text{Ch}_G(V) \subsetneq \text{Ch}_H(V)$ .*

*Proof.* First assume that the unipotent radical of  $G$  is of the form  $C^n$ , i.e., the  $n$ -fold product of the additive group of the field. Let  $P$  be a Levi factor of  $G$  and write  $G$  as a semidirect product of  $C^n$  and  $P$ ,  $G = C^n \rtimes P$ . Using this decomposition, we can define an action of  $G$  on  $C^n$  as follows. Each element  $p$  of  $P$  induces an automorphism of  $C^n$  via conjugation. For each  $g = (c, p) \in G$  and  $c_0 \in C^n$ , we let  $c_0^g = c + pc_0p^{-1}$ . This defines a group action and so induces an automorphism of  $C[C^n] = C[x_1, \dots, x_n]$  that preserves the degrees of polynomials in this ring. Let  $W$  be the polynomials of degree at most 1 in this ring and let  $V$  be the exterior algebra of  $W$ . We claim that  $V$  satisfies the conclusion of the lemma. To see this, let  $H$  be a connected subgroup of  $G$  such that  $R_u(H) \subsetneq R_u(G)$ . We wish to show  $\text{Ch}_G(V) \subsetneq \text{Ch}_H(V)$ . If  $H_1 = gHg^{-1}$  for some  $g \in G$ , then  $\text{Ch}_{H_1}(V) = g\text{Ch}_H(V)$ . Therefore it is enough to show  $\text{Ch}_G(V) \subsetneq \text{Ch}_{H_1}(V)$  for some conjugate  $H_1$  of  $H$ . In this way we may replace  $H$  by a conjugate and so write  $H = R_u(H) \rtimes P_H$  where  $P_H$  is a Levi factor of  $H$  and  $P_H \subset P$ . Since  $R_u(H) \subsetneq R_u(G)$ , there exist homogeneous linear polynomials  $f_1, \dots, f_m \in W$  such that  $R_u(H)$  is the set of zeros of  $f_1, \dots, f_m$  and such that the span of  $f_1, \dots, f_m$  is invariant under the action of  $H$  but not of  $G$ . Therefore  $f_1 \wedge \dots \wedge f_m \in \wedge^m W$  spans an  $H$ -invariant line that is not  $G$ -invariant. We shall show that  $f_1 \wedge \dots \wedge f_m$  is not in  $\text{Ch}_G(V)$ . Since  $\text{Ch}_G(V) = \bigoplus_{i=1}^n \text{Ch}_G(\wedge_i W)$  it is enough to show that  $f_1 \wedge \dots \wedge f_m \notin \text{Ch}_G(\wedge^m W)$ . By Lemma 2.2  $\text{Ch}_G(\wedge^m W) = (\wedge^m W)^{\text{Ker } X(G)}$ . Since  $R_u(G) \subset \text{Ker } X(G)$ , it is therefore enough to show  $f_1 \wedge \dots \wedge f_m \notin (\wedge^m W)^{R_u(G)}$ .

If  $x_1, \dots, x_n$  are indeterminates, then  $W$  has a basis of the form  $x_0 = 1, x_1, \dots, x_n$ . I claim that  $(\wedge^m W)^{R_u(G)}$  is the span  $\overline{V}$  of  $\{1 \wedge x_{i_2} \wedge \dots \wedge x_{i_m} \mid 0 < i_2 < \dots < i_m\}$ . To see this, let  $g = (c_1, \dots, c_n) \in C^n = R_u(G)$ . We then have  $g(1 \wedge x_{i_2} \wedge \dots \wedge x_{i_m}) = 1 \wedge x_{i_2} \wedge \dots \wedge x_{i_m}$  and, if  $0 < i_1 < \dots < i_m$ , then  $g(x_{i_1} \wedge \dots \wedge x_{i_m}) = x_{i_1} \wedge \dots \wedge x_{i_m} + \sum_{j=1}^m (-1)^{j-1} c_{i_j} (1 \wedge x_{i_1} \wedge \dots \wedge \hat{x}_{i_j} \wedge \dots \wedge x_{i_m})$ . Therefore  $\overline{V} \subset (\wedge^m W)^{R_u(G)}$ . Now let  $v \in (\wedge^m W)^{R_u(G)}$  and assume  $v \notin \overline{V}$ . We may assume  $v = \sum c_I (x_{i_1} \wedge \dots \wedge x_{i_m})$  where the sum is over all  $I = (i_1, \dots, i_m)$  with  $0 < i_1 < \dots < i_m$ . We wish to show  $c_I = 0$  for all such  $I$ . If not, we may assume without loss of generality that  $c_I \neq 0$  for some  $I$  of the form  $(1, i_2, \dots, i_m)$ . Letting  $g = (1, 0, \dots, 0)$  then

$$gv = v + \sum_{\substack{I=(1, i_2, \dots, i_m) \\ 1 < i_2 < \dots < i_m}} c_I (1 \wedge x_{i_2} \wedge \dots \wedge x_{i_m}).$$

Since  $gv = v$ , we must have  $c_I = 0$  for all  $I$  of the form  $(1, i_2, \dots, i_m)$ , a contradiction. Therefore  $\bar{V} = (\bigwedge^m W)^{R_u(G)}$ .

To show that  $f_1 \wedge \dots \wedge f_m \notin (\bigwedge^m W)^{R_u(G)}$  it suffices to note that  $f_1 \wedge \dots \wedge f_m = \sum c_I x_{i_1} \wedge \dots \wedge x_{i_m}$  where the sum is only over  $I$  of the form  $(i_1, \dots, i_m)$ ,  $0 < i_1 < \dots < i_m$ , and so  $f_1 \wedge \dots \wedge f_m$  cannot be in  $\bar{V}$ .

We now remove the assumption that  $R_u(G) = C^n$  and consider the general case. We may assume that  $R_u(G)$  is not trivial, otherwise the lemma becomes trivial. Any maximal subgroup of  $R_u(G)$  has codimension 1 in  $R_u(G)$  and so contains the commutator of  $R_u(G)$ . Let  $F$  be the intersection of all maximal subgroups of  $R_u(G)$ .  $F$  is a characteristic subgroup of  $R_u(G)$  and is therefore normal in  $G$ . Furthermore,  $R_u(G)/F$  is commutative and unipotent, so is isomorphic to  $C^n$  for some  $n \geq 1$ . Therefore  $G/F$  has unipotent radical of the form  $C^n$  and we can use the above to find a  $G/F$ -module satisfying the conclusion of the lemma. This gives the required  $G$ -module.  $\square$

**PROPOSITION 2.7.** *Let  $G$  be a linear algebraic group with  $G^\circ$  being the connected component of the identity. There exists a faithful  $G$ -module  $V$  such that for any closed connected subgroup  $H$  of  $G$ ,  $\text{Ker } X(G^\circ) \subset H$  if and only if  $\text{Ch}_{G^\circ}(V) = \text{Ch}_H(V)$ .*

*Proof.* Since  $G^\circ/R_u(G^\circ)$  is connected and reductive, let  $V_1$  be the  $G^\circ/R_u(G^\circ)$  module guaranteed to exist by Lemma 2.5. Let  $V_2$  be the  $G^\circ$ -module guaranteed to exist by Lemma 2.6. Let  $V_3$  be any faithful  $G^\circ$  module and let  $W = V_1 \oplus V_2 \oplus V_3$ . Let  $g_1 = \text{id}, g_2, \dots, g_m$  be coset representatives in  $G/G^\circ$  and let  $V = g_1 W \oplus \dots \oplus g_m W$  be the induced  $G$ -module. We will show that  $V$  satisfies the conclusion of the proposition.

First note that if  $\text{Ker } X(G^\circ) \subset H$  then Lemma 2.3 implies that  $\text{Ch}_{G^\circ}(V) = \text{Ch}_H(V)$ . Now assume  $\text{Ch}_{G^\circ}(V) = \text{Ch}_H(V)$ . Since  $W$  is  $G^\circ$ -invariant, we also have  $\text{Ch}_{G^\circ}(W) = \text{Ch}_H(W)$ . We shall show from this assumption that  $\text{Ker } X(G^\circ) \subset H$ . To do this, Lemma 2.1 implies that it is enough to show  $R_u(G^\circ) \subset H$  and  $(P, P) \subset H$ , for some Levi factor  $P$  of  $G^\circ$ . Let  $\pi: G^\circ \rightarrow G^\circ/R_u(G^\circ)$  be the canonical projection. Since  $\text{Ch}_{G^\circ}(V_1) = \text{Ch}_H(V_1)$  and  $\tilde{G} = G^\circ/R_u(G^\circ)$  is reductive, Lemma 2.5 implies that  $(\tilde{G}, \tilde{G}) = \text{Ker } X(\tilde{G}) \subset \pi(H)$ . Therefore  $\pi(H)$  is reductive. This implies that  $R_u(H) \subset \text{Ker } \pi = R_u(G^\circ)$ . Since  $\text{Ch}_{G^\circ}(V_2) = \text{Ch}_H(V_2)$ , Lemma 2.6 implies that  $R_u(H) = R_u(G^\circ)$ . Let  $P_H$  be a Levi factor of  $H$  and  $P_{G^\circ}$  a Levi factor of  $G^\circ$  containing  $P_H$ . We may identify  $P_G$  with  $\pi(G^\circ) = \tilde{G}$  and  $P_H$  with  $\pi(H)$ . Since

$(\tilde{G}, \tilde{G}) \subset \pi(H)$ , we have  $(P_{\tilde{G}}, P_{\tilde{G}}) \subset P_H \subset H$ . Therefore Lemma 2.1 implies  $\text{Ker } X(G^\circ) \subset H$ .  $\square$

The above result implies that if  $R_u(G^\circ) = R(G^\circ)$ , then there exists a  $G$ -module  $V$  such that for any connected proper subgroup  $H$  of  $G$ ,  $\text{Ch}_{G^\circ}(V) \subsetneq \text{Ch}_H(V)$ . This follows from the fact that if  $R_u(G^\circ) = R(G^\circ)$  then any Levi factor  $P$  is semisimple so  $P = (P, P)$ . Therefore  $G^\circ = R(G^\circ) \cdot P = R_u(G^\circ) \cdot (P, P)$  so  $G^\circ = \text{Ker } X(G^\circ)$ . If one removes the condition that  $R_u(G^\circ) = R(G^\circ)$  then this conclusion will not hold. For example, if  $G$  is a torus then any representation of  $G$  is diagonalizable so for any  $G$ -module  $V$  and subgroup  $H$ ,  $V = \text{Ch}_G(V) = \text{Ch}_H(V)$ . In fact, one cannot hope to use invariant subspaces to uniformly distinguish a group from its subgroups. To see this let  $T = (C^*)^r$  be a torus of dimension  $r > 1$  and  $V$  be any  $T$ -module.  $T$  is diagonalizable so  $V = V_{\chi_1} \oplus \dots \oplus V_{\chi_n}$  for distinct characters  $\chi_1, \dots, \chi_n$  of  $T$ . For integers  $n_1, \dots, n_r$ , let  $T_{n_1, \dots, n_r} = \{(a_1, \dots, a_r) \in T \mid \prod a_i^{n_i} = 1\}$ . Since any character  $\chi$  of  $T$  is of the form  $\chi(a_1, \dots, a_r) = \prod_{i=1}^r a_i^{m_i}$  for some  $m_i \in \mathbb{Z}$ , we can find  $n_1, \dots, n_r$  such that the  $\chi_1, \dots, \chi_n$  are distinct characters of  $T_{n_1, \dots, n_r}$ . For such a subgroup, any invariant subspace  $W$  will be of the form  $W_1 \oplus \dots \oplus W_n$  where  $W_i \subset V_{\chi_i}$  and so will also be  $T$ -invariant.

To handle proper subgroups of  $G$  that are not connected, we will need the following lemma. This, in turn, depends heavily on the following theorem of Jordan: Let  $C$  be an algebraically closed field of characteristic zero. There exists an integer valued function  $J(n)$ , depending only on  $n$ , such that every finite subgroup of  $\text{GL}(n, C)$  contains an abelian normal subgroup of finite index at most  $J(n)$  (this is shown in [CR62, p. 285], where it is also shown that  $J(n) \leq (\sqrt{8n+1})^{2n^2} - (\sqrt{8n-1})^{2n^2}$ ). The following result is closely related to Proposition 2.2 of [SI81].

**LEMMA 2.8.** *Let  $C$  be an algebraically closed field of characteristic zero. There exists an integer valued function  $N(n)$ , depending only on  $n$ , such that if  $G$  is a subgroup of  $\text{GL}(n, C)$  and  $H$  is a normal subgroup of  $G$  of finite index then there is a normal subgroup  $H'$  of  $G$  such that  $H \subset H'$ ,  $[G : H'] \leq N(n)$ , and  $\text{Ch}_{H'}(C^n) = \text{Ch}_H(C^n)$ .*

*Proof.* We proceed by induction on  $n$ . There are only a finite number of  $\chi$ -spaces for  $H$ . Let  $V_1, \dots, V_k$  be these spaces corresponding

to  $\chi_1, \dots, \chi_k$ . Let  $m = \max\{\dim V_i\}$ . We distinguish between two cases:  $m = n$  and  $m < n$ .

If  $m = n$ , then  $k = 1$  and  $V_1 = C^n$ . In this case  $H$  is a subgroup of  $C_n$ , the group of scalar matrices. Let  $\text{PGL}(n - 1, C) = \text{GL}(n, C)/C_n$ . Note that

$$\text{PGL}(n - 1, C) = \text{SL}(n, C)/(\text{SL}(n, C) \cap C_n).$$

Let  $\phi: \text{GL}(n, C) \rightarrow \text{PGL}(n - 1, C)$  and  $\psi: \text{SL}(n, C) \rightarrow \text{PGL}(n - 1, C)$  be the canonical homomorphisms. The kernel of  $\phi$  contains  $H$ . Therefore,  $\phi(G)$  is finite and so  $\psi^{-1}\phi(G)$  is a finite subgroup of  $\text{SL}(n, C)$ . Jordan's Theorem implies that there exists an abelian normal subgroup  $K$  of  $\psi^{-1}\phi(G)$  of index  $\leq J(n)$ . Let  $H' = \phi^{-1}\psi(K)$ . Some power of each element in  $H'$  is diagonal and  $H'$  is abelian, so we can simultaneously diagonalize all elements of  $H'$ . Therefore,  $C^n$  is the character module of  $H'$  and  $H'$  is normal in  $G$ .

We now turn to the case of  $m < n$ . Since  $H$  is normal in  $G$ ,  $G$  permutes the elements of  $\{V_1, \dots, V_k\}$  and we get a homomorphism of  $G$  into the symmetric group on  $k$  elements. Let  $K$  be the kernel of this homomorphism. Each  $V_i$  is a  $K$ -module and  $H \subset K$ . Since  $\dim V_i < n$ , there are subgroups  $H_i$  of  $K$  such that  $[K : H_i] \leq N(n - 1)$ ,  $H \subset H_i$  and  $V_i$  is contained in the character submodule of  $H_i$  in  $V$ . Let  $\bar{H} = \bigcap H_i$ . We then have  $[K : \bar{H}] \leq \prod [K : H_i] \leq nN(n - 1)$  and  $\text{Ch}_H(V) = \text{Ch}_{\bar{H}}(V)$ . Since  $[G : K] \leq n!$ , we have  $[G : \bar{H}] \leq n(n!)N(n - 1)$ . Let  $G$  act on  $G/\bar{H}$  by multiplication. This induces a map from  $G$  to a permutation group. Let  $H'$  be the kernel of this map.  $H'$  is normal in  $G$  and  $[G : H'] \leq (n(n!)N(n - 1))!$ . Since  $H \subset H' \subset \bar{H}$ , we have  $\text{Ch}_{H'}(V) = \text{Ch}_H(V)$ . □

From these considerations, we see that  $N(n)$  can be defined inductively by  $N(n) = \max\{J(n), (n(n!)N(n - 1))!\}$ . We now generalize Proposition 2.7 to deal with nonconnected subgroups  $H$ .

**PROPOSITION 2.9.** *Let  $G$  be a linear algebraic group with  $G^\circ$  the connected component of the identity. There exists a faithful  $G$ -module  $W$  such that for any closed subgroup  $H$  of  $G$ ,  $\text{Ker } X(G^\circ) \subset H$  if and only if  $\text{Ch}_{G^\circ}(W) = \text{Ch}_{H \cap G^\circ}(W)$ .*

*Proof.* If  $\text{Ker } X(G^\circ) \subset H$ , then Lemma 2.3 implies that for any  $G$ -module  $W$ ,  $\text{Ch}_{G^\circ}(W) = \text{Ch}_{H \cap G^\circ}(W)$ .

To prove the converse, let  $V$  be the  $G$ -module of Proposition 2.7. Let  $V$  have dimension  $n$  and let  $W = \bigoplus_{i=1}^{N(n)} S^i(V)$  where  $S^i(V)$  is the  $i$ th symmetric power of  $V$  and  $N(n)$  is as in Lemma 2.8. We

will show that this choice of  $W$  satisfies the conclusion of Proposition 2.9.

Let  $H$  be a closed subgroup of  $G$  and assume  $\text{Ker } X(G^\circ)$  is not a subgroup of  $H$ . Applying Lemma 2.8 to  $H^\circ \subset G^\circ \cap H$ , we have that there is a normal subgroup  $H'$  of  $G^\circ \cap H$  such that  $\text{Ch}_{H'}(V) = \text{Ch}_{H^\circ}(V)$  and  $[G^\circ \cap H : H'] \leq N(n)$ . Since  $\text{Ker } X(G^\circ)$  is not a subgroup of  $H$ , Proposition 2.7 implies that we have a  $v \in \text{Ch}_{H^\circ}(V) = \text{Ch}_{H'}(V)$  that spans an  $H'$ -invariant subspace that is not in  $\text{Ch}_{G^\circ}(V)$ . Let  $h_1 = \text{id}, \dots, h_m$  be coset representatives of  $G^\circ \cap H/H'$  and let  $w = \prod_{i=1}^m h_i(v) \in S^m(V)$ . Since  $m \leq N(n)$ ,  $w \in W$ . We will now show that  $w \in \text{Ch}_{H \cap G^\circ}(W)$  but  $w \notin \text{Ch}_{G^\circ}(W)$ .

For any  $h \in H \cap G^\circ$ , we have  $h(w) = \prod_{i=1}^m h(h_i(v)) = \prod_{i=1}^m h_i(\tilde{h}_i(v))$  where  $\tilde{h}_i \in H'$ . Since, for each  $i$  we have  $\tilde{h}_i(v) = c_i v$  for some  $c_i \in C$ ,  $h(w) = c \prod_{i=1}^m h_i(w) = cw$  so  $w \in \text{Ch}_{H \cap G^\circ}(W)$ . To see that  $w \notin \text{Ch}_{G^\circ}(W)$ , Lemma 2.2 implies that it suffices to show  $w \notin W^{\text{Ker } X(G^\circ)}$ . Assume, to the contrary that  $g(w) = w$  for all  $g \in \text{Ker } X(G^\circ)$ . Since the symmetric algebra  $S(W)$  of  $W$  is a unique factorization domain, we must have that for each  $i$  there is a  $j$  and a  $c_i \in C$  such that  $g(h_i(v)) = c_i h_j(v)$ . Therefore each  $g$  permutes the lines spanned by the  $h_i(v)$ . For each  $i$ , the set of  $g \in \text{Ker } X(G^\circ)$  such that  $g$  leaves the line spanned by  $h_i(v)$  fixed is a closed subgroup of finite index in  $\text{Ker } X(G^\circ)$ . Since  $\text{Ker } X(G^\circ)$  is connected (Lemma 2.1), we have this subgroup is all of  $\text{Ker } X(G^\circ)$ . In particular,  $h_1 = \text{id}$  so for any  $g \in \text{Ker } X(G^\circ)$  there is a  $c_g \in C$  such that  $g(v) = c_g v$ . The map sending  $g$  to  $c_g$  is a character so Lemma 2.1 implies all  $c_g = 1$ . Therefore  $v \in V^{\text{Ker } X(G^\circ)} = \text{Ch}_{G^\circ}(V)$ , a contradiction.  $\square$

*b. Differential Galois theory.* The basic reference for differential Galois theory is [KO73] (see also [KA57] and [SI89]). Here we recall some facts to be used in this paper. Let  $F$  be a differential field of characteristic zero. The subfield of constants  $C$  of  $F$  is the set of  $c$  in  $F$  such that  $c' = 0$ . If  $F \subset K$  are differential fields and  $y_1, \dots, y_n$  are elements of  $K$ , then  $F\{y_1, \dots, y_n\}$  and  $F\langle y_1, \dots, y_n \rangle$  are the differential ring and differential field, respectively, generated by  $y_1, \dots, y_n$  over  $F$ . If  $C$  is algebraically closed and  $L(y) = 0$  is an  $n$ th order homogeneous linear differential equation with coefficients in  $F$ , there exists an extension  $K$  of  $F$  such that  $K$  and  $F$  have the same subfield  $C$  of constants and  $K = F\langle y_1, \dots, y_n \rangle$  where  $y_1, \dots, y_n$  are solutions of  $L(y) = 0$ , linearly independent over the constants (such a set is called a fundamental set of solutions of  $L(y) = 0$ ). Such a field is unique up to a differential isomorphism that is the identity

on  $F$  and is called the Picard-Vessiot extension of  $F$  associated with  $L(y) = 0$ . A differential automorphism  $\sigma$  of  $K$  leaving  $F$  fixed takes each  $y_i$  to some constant linear combination of  $y_1, \dots, y_n$ . The group of these differential automorphisms is called the Galois group of  $L(y) = 0$  (or the Galois group of  $K$  over  $F$ ) and is denoted by  $\text{Gal}(L)$  or  $\text{Gal}(K/F)$ . It can be identified with a subgroup of  $\text{GL}(n, C)$ . It is known that this group is a Zariski closed subgroup of  $\text{GL}(n, C)$  and so is a linear algebraic group. There is a differential Galois theory that identifies a closed subgroup  $H$  of  $\text{Gal}(L)$  with the intermediate field  $E$ ,  $F \subset E \subset K$ , of elements left fixed by all members of  $H$ . In particular an element  $z \in K$  is in  $F$  if and only if  $\sigma(z) = z$  for all  $\sigma \in \text{Gal}(L)$ . Furthermore, if  $H$  is a closed normal subgroup of  $\text{Gal}(L)$ , then the field  $E$  of elements left fixed by  $H$  is also a Picard-Vessiot extension of  $F$  with Galois group isomorphic to  $\text{Gal}(L)/H$ . Finally, the transcendence degree of  $K$  over  $F$  equals the dimension of  $G$ . We shall also use the fact that elements  $z_1, \dots, z_m$  of a differential field are linearly dependent over the constant subfield if and only if  $\text{Wr}(z_1, \dots, z_m) = 0$  where  $\text{Wr}$  is the Wronskian determinant ([KA57], p. 21). This also implies that if  $L(y)$  has order  $n$ , the dimension of the solution space of  $L(y) = 0$  is at most  $n$ . The following lemma will be used several times.

**LEMMA 2.10.** *Let  $F$  be a differential field of characteristic zero with algebraically closed field of constants  $C$  and let  $K$  be a Picard-Vessiot extension of  $F$ . Let  $H$  be a closed subgroup of  $\text{Gal}(K/F)$  and  $E$  the fixed field of  $H$ .*

(i) *If  $V \subset K$  is a finite dimensional vector space over  $C$ , then  $V$  is the solution space of a homogeneous linear differential equation with coefficients in  $E$  if and only if  $V$  is left invariant under the action of  $H$ .*

(ii) *Let  $L(y) = 0$  be a homogeneous linear differential equation with coefficients in  $F$  and with solution space  $W$  in  $K$ . Let  $W_0$  be a subspace of  $W$  left invariant by  $H$ . Then there exist homogeneous linear differential equations  $L_1(y)$  and  $L_0(y)$  with coefficients in  $E$  and with  $L_0$  monic such that  $W_0$  is the solution space of  $L_0(y) = 0$  and  $L(y) = L_1(L_0(y))$ .*

(iii) *For  $z \in K$ ,  $z'/z \in E$  if and only if there is a  $C$ -valued character  $\chi$  of  $\text{Gal}(K/E)$  such that  $\sigma(z) = \chi(\sigma)z$  for all  $\sigma \in \text{Gal}(K/E)$ .*

(iv) *An element  $z \in K$  is algebraic over  $F$  if and only if  $z$  is left fixed by  $\text{Gal}(K/F)^0$ , the connected component of the identity of  $\text{Gal}(K/F)$ .*

*Proof.* (i) If  $V$  is the solution space of  $L(y) = 0$ , then since  $H = \text{Gal}(K/E)$  takes solutions of  $L(y) = 0$  to solutions of the same equation,  $V$  is left invariant by  $\text{Gal}(K/E)$ . If  $V$  is left invariant by  $\text{Gal}(K/E)$ , let  $y_1, \dots, y_n$  be a basis of  $V$ . If  $L(y) = \text{Wr}(y, y_1, \dots, y_n)/\text{Wr}(y_1, \dots, y_n)$  and  $\sigma \in \text{Gal}(K/E)$ , then if we apply  $\sigma$  to the coefficients of  $L(y)$ , we get

$$\begin{aligned} L^\sigma(y) &= \text{Wr}(y, \sigma(y_1), \dots, \sigma(y_n))/\text{Wr}(\sigma(y_1), \dots, \sigma(y_n)) \\ &= \det(\sigma)\text{Wr}(y, y_1, \dots, y_n)/\det(\sigma)\text{Wr}(y_1, \dots, y_n) \\ &= \text{Wr}(y, y_1, \dots, y_n)/\text{Wr}(y_1, \dots, y_n). \end{aligned}$$

Therefore, the coefficients of  $L(y)$  are left fixed by  $\text{Gal}(K/E)$  and so lie in  $E$ .

(ii) By (i), there is a homogeneous linear differential equation  $L_0(y)$  with coefficients in  $E$  whose solution space is  $W_0$ . We may write  $L(y) = L_1(L_0(y)) + R(y)$  where  $L_1(y)$  and  $R(y)$  are homogeneous linear differential equations with coefficients in  $E$  and the order of  $R$  is less than the order of  $L_0(y)$  ([**POO60**]). Since  $R(y) = 0$  for all elements of  $W_0$  and  $\dim W_0$  is larger than the order of  $R(y)$ , we must have  $R \equiv 0$ .

(iii) If  $z'/z = u \in E$ , then  $L(z) = z' - uz = 0$ , so  $z$  spans a one dimensional space invariant under the action of  $\text{Gal}(K/E)$ . Conversely if  $\sigma(z) = \chi(\sigma)z$  for all  $\sigma \in \text{Gal}(K/E)$ , then  $\sigma(z'/z) = z'/z$ , so  $z'/z = u \in E$ .

(iv) If  $z$  is left fixed by  $\text{Gal}(K/F)^0$  then  $z$  lies in the field  $E$  fixed by this group. Since  $\text{Gal}(K/F)^0$  is of finite index in  $\text{Gal}(K/F)$ ,  $E$  has finite degree over  $F$  and so is an algebraic extension ([**KA57**], p. 18). Conversely, if  $z$  is algebraic over  $F$ , then the set of  $\sigma \in G$  such that  $\sigma(z) = z$  is of finite index in  $\text{Gal}(K/F)$  and so must contain  $\text{Gal}(K/F)^0$ . □

*c. Singular points.* Let  $L(y) = a_n(x)y^{(n)} + \dots + a_0(x)y \in \mathcal{L}(n, m)$ ,  $a_n(x) \neq 0$ . If  $a_n(\alpha) = 0$ , we say that  $\alpha$  is a singular point of  $L(y) = 0$ . It is known that  $L(y) = 0$  has a fundamental set of formal solutions of the form

$$y_i = (x - \alpha)^{\rho_i} e^{P_i(1/t)} \left( \sum_{j=1}^{s_i} b_{ij}(t)(\log(x - \alpha))^j \right)$$

$i = 1, \dots, n$  where  $t = (x - \alpha)^{1/n!}$ ,  $P_i$  is a polynomial without

constant term,  $s_i < n$  and  $b_{ij}(t) \in \mathbb{C}[[t]]$  and such that for each  $i$ , some  $b_{ij}(0) \neq 0$  ([LEV75], [MAL79]). If all the  $P_i$  are 0,  $\alpha$  is said to be a regular singular point; otherwise it is called an irregular singular point. If

$$y = (x - \alpha)^\rho e^{P(1/t)} \left( \sum_{j=1}^s b_j(t) (\log(x - \alpha))^j \right),$$

as above, is a solution of  $L(y) = 0$ , then for some  $i$ ,  $\rho = \rho_i$  and  $P = P_i$ . Such a  $P$  is called a *determining factor at  $\alpha$*  and  $\rho$  is called an *exponent at  $\alpha$* .  $P_1, \dots, P_r$  will be the determining factors of  $L(y) = 0$  at  $\alpha$  if and only if  $L_i(y) = e^{P_i(1/t)} L(e^{-P_i(1/t)} y)$  has an indicial polynomial at  $\alpha$  of degree  $d_i > 0$  and  $d_1 + \dots + d_r = n$  (the indicial polynomial  $f(r)$  is the coefficient of the term of lowest degree when  $L((x - \alpha)^r)$  is expanded in powers of  $x - \alpha$  where  $r$  is an indeterminate ([IN56], p. 160)).  $\rho$  is an exponent at  $\alpha$  if and only if, for some  $i$ ,  $\rho$  is the root of the indicial polynomial at  $\alpha$  of  $L_i(y)$ . We note that the indicial polynomial of  $L_i(y)$  has coefficients that are rational functions of the coefficients of  $P_i$  and the coefficients of the  $a_i$ . We define the *local data  $\mathcal{D}_\alpha$  at  $\alpha$*  to be the set  $\{\rho_1, \dots, \rho_n, P_1(x), \dots, P_n(x)\}$ . We define the *weak local data  $\mathcal{W}_\alpha$  at  $\alpha$*  to be a set  $\{\rho_1, \dots, \rho_n\}$  where the  $\rho_i$  are the exponents in  $\mathcal{D}_\alpha$ . Note that if  $\alpha$  is not a singular point, then there exists a fundamental set of solutions at  $\alpha$  of the form  $y_i = (x - \alpha)^{i-1} b_i(x)$ ,  $i = 1, \dots, n$ , where  $b_i(x) \in \mathbb{C}[[x - \alpha]]$  and  $b_i(0) \neq 0$ . At such a point 0 is the only determining factor and the exponents are  $\{0, \dots, n - 1\}$ . Therefore we define the local data at  $\alpha$  to be  $\{0, \dots, n - 1\}$ . One can make similar definitions for the point at infinity by letting  $x = \frac{1}{z}$  and considering  $z = 0$  in the transformed equation. Let  $\mathcal{D}$  be a finite set  $\{\rho_1, \dots, \rho_r, P_1, \dots, P_s\}$  where the  $\rho_i \in \mathbb{C}$  and the  $P_i$  are polynomials without constant terms. We say  $\mathcal{D}$  is *local data for  $L \in \mathcal{L}(n, m)$*  if  $\mathcal{D}_\alpha \subset \mathcal{D}$  for all  $\alpha \in \mathbb{C} \cup \{\infty\}$ . Since any  $L \in \mathcal{L}(n, m)$  has only finitely many singular points, there is always some  $\mathcal{D}$  such that  $\mathcal{D}$  is local data for  $L$ . Similarly, a finite set  $\mathcal{W}$  is *weak local data for  $L$*  if  $\mathcal{W}_\alpha \subset \mathcal{W}$  for all  $\alpha \in \mathbb{C} \cup \{\infty\}$ . We say that a real number  $B$  is a *local bound for  $L$*  if there is a  $\mathcal{W}$  that is weak local data for  $L$  such that  $|\operatorname{Re} \rho| \leq B$  for all  $\rho \in \mathcal{W}$ . Note that the definition of a local bound only refers to the exponents and not the determining factors. We will need a bound on the degrees of the determining factors as well. It is known ([LEV75], [MA79]) that such a bound can be expressed in

terms of the orders at singular points of the coefficient  $a_i$  in  $L$  and  $n$ . These orders can be bounded by  $m$  and so the degrees of the determining factors can be a priori bounded in terms of  $m$  and  $n$  (in fact,  $mn!$  will be such a bound). For fixed  $\mathcal{D}$  (resp.  $\mathcal{W}$ ;  $B$ ) we let  $\mathcal{L}(n, m, \mathcal{D})$  (resp.  $\mathcal{L}(n, m, \mathcal{W})$ ;  $\mathcal{L}(n, m, B)$ ) denote the set of  $L \in \mathcal{L}(m, n)$  with the local data  $\mathcal{D}$  (resp. weak local data  $\mathcal{W}$ ; local bound  $B$ ). For any  $\mathcal{D}$  (resp.  $\mathcal{W}$ ) there exists a  $B$  such that  $\mathcal{L}(n, m, \mathcal{D}) \subset \mathcal{L}(n, m, B)$  (resp.  $\mathcal{L}(n, m, \mathcal{W}) \subset \mathcal{L}(n, m, B)$ ) so having a local bound is weaker than having local data. The following lemma shows that by knowing a local bound  $B$  for  $L \in \mathcal{L}(n, m)$  we can bound in terms of  $n, m, B$ , the degrees of the numerators and denominators of rational functions  $y$  and  $u$  such that  $y$  or  $e^{\int u}$  are solutions of  $L(y) = 0$ . If we furthermore know local data for  $L$ , then we can determine the coefficients in the partial fraction decomposition of a  $u$  up to some finite set of possibilities.

**PROPOSITION 2.11.** (i) *Let  $L \in \mathcal{L}(n, m, B)$ . There exists an integer  $N$ , depending only on  $n, m$  and  $B$  such that if  $y \in \mathbb{C}(x)$ ,  $y \neq 0$ , and  $L(y) = 0$  then  $y$  is the quotient of two polynomials of degree  $\leq N$ .*

(ii) *Let  $L \in \mathcal{L}(n, m, B)$ . There exists an integer  $M$  depending only on  $n, m$  and  $B$  such that if  $u \in \mathbb{C}(x)$  and  $L(e^{\int u}) = 0$  then  $u$  is the quotient of polynomials of degree  $\leq N$ .*

(iii) *Let  $L \in \mathcal{L}(n, m, \mathcal{D})$ . There exists a finite set  $\mathcal{S}$  and an integer  $M$ , both depending only on  $n, m$  and  $\mathcal{D}$  such that if  $u \in \mathbb{C}(x)$  and  $L(e^{\int u}) = 0$  then*

$$(2.11.1) \quad u = \sum_{i=1}^t \left( \sum_{j=1}^{n_i} \frac{a_{ij}}{(x - \alpha_i)^j} \right) + b_s x^s + \dots + b_0$$

where  $s, t \leq M$ ,  $n_i \leq M$  for  $i = 1, \dots, t$  and each  $a_{ij}$  and  $b_j \in \mathcal{S}$ .

*Proof.* (i) Let  $y = \frac{p}{q}$  where  $p, q \in \mathbb{C}[x]$ ,  $(p, q) = 1$  and  $q = \prod (x - \alpha_i)^{n_i}$ . Each  $\alpha_i$  must be a singular point of  $L(y)$  and each  $n_i$  is an exponent at  $\alpha_i$ . Since there are at most  $m$  finite singular points,  $\deg q = \sum n_i \leq mB$ . At infinity  $\deg q - \deg p$  is an exponent so  $\deg p \leq \deg q + B \leq (m + 1)B$ .

(ii) and (iii) Let  $L \in \mathcal{L}(n, m)$  and let  $u$  be as in (2.11.1). For any  $\alpha_i$ , we have  $e^{\int u} = (x - \alpha_i)^{a_{i1}} \exp(\int \sum_{j=2}^{n_i} \frac{a_{ij}}{(x - \alpha_i)^j}) \phi(x)$  where  $\phi(x)$  is

in  $\mathbb{C}[[x - \alpha_i]]$ . Therefore,

$$\sum_{j=2}^{n_i} \frac{a_{ij}}{(x - \alpha_i)^j}$$

is the derivative of a determining factor at  $\alpha_i$  and  $a_{i1}$  is an exponent at  $\alpha_i$ . If  $\alpha_i$  is not a singular point, we have that  $n_i = 1$  and  $a_{i1}$  is a positive integer. At  $\infty$ ,  $b_s x^s + \dots + b_0$  is the derivative of a determining factor and  $-\sum_{i=1}^t a_{i1}$  is an exponent. Therefore if  $L \in \mathcal{L}(m, n, B)$ , each  $n_i$  can be bounded in terms of  $n$  and  $m$  and  $|\sum_{i=1}^t \operatorname{Re} a_{i1}| \leq B$ . If we write  $\sum_{i=1}^t a_{i1} = \sum_{i \in \mathcal{S}} a_{i1} + \sum_{i \in \mathcal{F}} a_{i1}$  where  $\mathcal{S} = \{i | \alpha_i \text{ is a singular point}\}$  and  $\mathcal{F} = \{i | \alpha_i \text{ is not a singular point}\}$ , then we see that  $|\sum_{i \in \mathcal{F}} \operatorname{Re} a_{i1}| \leq B + \sum_{i \in \mathcal{S}} |\operatorname{Re} a_{i1}| \leq B + mB$ . Since each  $a_{i1}$  in the first sum is a positive integer, we can bound the size of  $\mathcal{F}$  and therefore bound  $t$ . Similarly,  $s$  can be determined from the degree of a determining factor at infinity and so can be bounded in terms of  $m$  and  $n$ . Therefore the degrees of the numerator and denominator of  $u$  can be bounded in terms of  $n, m$  and  $B$ .

If  $L \in \mathcal{L}(n, m, \mathcal{D})$ , we can determine for each  $\alpha_i$  that is a singularity of  $L$  the  $a_{ij}$  from the exponents and determining factors. Therefore the  $a_{i1}$  are determined up to some finite set of possibilities from  $\mathcal{D}$ . Similarly the  $b_j$  and  $s$  can be determined from the determining factors at  $\infty$  and so from  $\mathcal{D}$ . Note that  $-(\sum_{i \in \mathcal{S}} a_{i1} + \sum_{i \in \mathcal{F}} a_{i1})$  is an exponent at infinity and that we know the  $a_{i1}$  in the first sum up to some finite set of possibilities. Since the  $a_{i1}$  in the second sum are positive integers, we can determine these up to a finite set of possibilities. □

We close this section by noting that weak local data  $\mathcal{W}$  is an analytic invariant of a differential equation, that is, at any point  $\alpha$  if  $\bar{t} = f(t)$  is an analytic change of coordinates with  $f'(\alpha) \neq 0$ , then  $\mathcal{W}$  will continue to contain the exponents of  $L$ . In contrast, the determining factors themselves need not be preserved under analytic change of coordinates. This is why we show, whenever possible, that our results depend only on knowing weak local data or a local bound  $B$ . This is true for most of our results in §3 (up to Lemma 3.10) but is, regrettably, not true for all our results (see the discussions following to Lemma 3.10 and before Lemma 3.15).

We shall need the following generalization of Fuchs' relation due to Bertrand and Beukers [BB85]. A set of real numbers  $\{r_{\alpha 1}, \dots, r_{\alpha n}\}$  is an *admissible set of exponents for  $L$  at  $\alpha$*  if there exists a fundamental system of solutions whose exponents  $\rho_i$  satisfy  $\operatorname{Re} \rho_i \geq r_{\alpha i}$  for  $i =$

$1, \dots, n$ .  $L$  has rank  $q = \frac{p}{n!}$  at  $\alpha_i$  if the degree of any determining factor is  $\leq p$  Bertrand and Beukers show the following result ([BB85], Theorem 3):

**LEMMA 2.12.** *Let  $\mathcal{S}$  be a finite set of points on the Riemann Sphere containing the singular points and  $\infty$ . For each  $\alpha \in \mathcal{S}$  let the set of real numbers  $\{r_{\alpha 1}, \dots, r_{\alpha n}\}$  be an admissible set of exponents at  $\alpha$  and let  $L$  have rank  $q_\alpha$  at  $\alpha$ . Then*

$$\sum_{\alpha \in \mathcal{S}} \left( \left( \sum_{i=1}^n r_{\alpha i} \right) - (q_\alpha + 1)n(n - 1)/2 \right) \leq -n(n - 1).$$

In subsequent sections we will start with a set of linear differential equations and construct new equations. For example, given  $L_1(y)$  and  $L_2(y)$  we will construct the equation whose solutions are sums of solutions of  $L_1(y) = 0$  and  $L_2(y) = 0$ . These new equations will have singular points that can be determined from the given set of equations and possibly new apparent singularities (singularities where all solutions are analytic). The exponents at the non-apparent singularities will be of the form  $\rho + n$  where  $\rho$  can be determined from the exponents of the given set of equations and  $n$  is a positive integer. We will need to be able to bound such an  $n$  as well as the exponents at apparent singularities (which will be nonnegative integers).

**LEMMA 2.13.** *Let  $L \in \mathcal{L}(n, m)$ ,  $\mathcal{S}$  the set of all singular points of  $L$  and  $R$  a non-negative real number. Assume that at each singular point  $\alpha$  the determining factors of  $L$  have degree  $\leq n!R$  and that the exponents  $\{\rho_{\alpha i}\}$  are of the form  $\rho_{\alpha i} = \widetilde{\rho}_{\alpha i} + n_{\alpha i}$  where  $\text{Re } \widetilde{\rho}_{\alpha i} \geq -R$  and  $n_{\alpha i}$  is a nonnegative integer. Then*

$$\sum_{\alpha \in \mathcal{S}} \sum_{i=1}^n n_{\alpha i} \leq (m + 1)(nR(R + 1)n(n + 1)/2) - n(n - 1).$$

*In particular there are only a finite number of possibilities for  $n_{\alpha i}$  and these are all less than a bound that depends only on  $n, m$  and  $R$ .*

*Proof.*  $\{-R + n_{\alpha i}\}_{i=1}^n$  is an admissible system of exponents at  $\alpha$  and  $L$  has rank  $\leq R$  at  $\alpha$ . Therefore Lemma 2.12 implies

$$\sum_{\alpha \in \mathcal{S}} \left( \sum_{i=1}^n (-R + n_{\alpha i}) - (R + 1)n(n - 1)/2 \right) \leq -n(n - 1).$$

The result follows by noting that  $\mathcal{S}$  has at most  $m + 1$  elements.  $\square$

### 3. Constructible sets of differential equations.

(a) *Basic definitions.* Let  $C \subset \bar{C}$  be fields of characteristic 0 and assume that  $\bar{C}$  is algebraically closed. We start this section by recalling the following definition (cf., [MUM76], p. 37). A subset  $\mathcal{S}$  of  $\bar{C}^n$  is *C-constructible* if it is a union  $T_1 \cup \cdots \cup T_k$  where each  $T_i$  is of the form  $\{c \in \bar{C}^n \mid f_{1i}(c) = \cdots = f_{mi}(c) = 0, \quad g_i(c) \neq 0\}$  for some  $f_{ji}, g_i$  in  $C[x_1, \dots, x_n]$ . The *C-constructible* sets are precisely the elements of the Boolean algebra generated by the Zariski closed sets, defined over  $C$ . It is known that if  $\mathcal{S} \subset \bar{C}^n \times \bar{C}^m = \bar{C}^{n+m}$  is a *C-constructible* set and  $p_2: \bar{C}^n \times \bar{C}^m \rightarrow \bar{C}^m$  is the projection onto the second factor, then  $p_2(\mathcal{S})$  is a *C-constructible* set ([MUM76], p. 37). This fact is very useful in showing that certain sets are constructible and will be used repeatedly in what follows. For example, one can identify the set of polynomial in  $m$  variables of degree  $n$  with coefficients in  $\bar{C}$  with the space  $\bar{C}^N$  of coefficients, where  $N = \binom{n+m}{m}$ . The set of such polynomials that have a factor of degree  $l < n$  with coefficients in  $\bar{C}$  forms a *C-constructible* set. This implies that the set of polynomials of degree  $m$  in  $n$  variables with coefficients in  $\bar{C}$  that are irreducible over  $\bar{C}$  forms a *C-constructible* set for any  $C \subset \bar{C}$ . We shall also need the fact that if a *C-constructible* subset  $\mathcal{S}$  of  $\bar{C}^n$  is nonempty and  $F$  is any algebraically closed field containing  $C$ , then  $\mathcal{S}$  contains a point with coefficients in  $F$ . This is an immediate consequence of the Hilbert Nullstellensatz. In particular, if a *C-constructible* set contains a point in some algebraically closed field containing  $C$ , then it has a point in the algebraic closure of  $C$ .

Let  $\mathcal{L}(n, m)$  be the set of homogeneous linear differential equations as in (1) above. As we have noted,  $\mathcal{L}(n, m)$  may be identified with  $\mathbb{C}^{(n+1)(m+1)}$ . Let  $C$  be a subfield of  $\mathbb{C}$ . A set  $\mathcal{S} \subset \mathcal{L}(n, m)$  of homogeneous linear differential equations is said to be *C-constructible* if it forms a *C-constructible* subset of  $\mathbb{C}^{(n+1)(m+1)}$  under the above identification. For example if we fix integers  $n$  and  $m$  and local data  $\mathcal{D}$  defined over  $C$  then  $\mathcal{L}(n, m, \mathcal{D})$  is a *C-constructible* set. To see this, note that  $L \in \mathcal{L}(n, m, \mathcal{D})$  if and only if for each zero  $\alpha$  of the leading coefficient of  $L$  (and  $\infty$ ) there is a set of determining factors  $P_1, \dots, P_n \in \mathcal{D}$  such that, for  $i = 1, \dots, n$ ,  $e^{P_i(t)} L(e^{-P_i(t)} \bar{y})$ ,  $t = (x - \alpha)^{1/n!}$ , has an indicial equation  $f_\alpha$  of degree  $d_\alpha > 0$  where  $\sum d_\alpha = n$  and the roots of each  $f_\alpha$  lie in  $\mathcal{D}$ . Similarly for fixed  $n, m$  and weak local data  $\mathcal{W}$ ,  $\mathcal{L}(n, m, \mathcal{W})$  is *C-constructible*. Note that  $\mathcal{L}(n, m, B)$  is not a *C-constructible* set (although it is a real semi-

algebraic set when we identify  $\mathbb{C}$  with  $\mathbb{R}^2$  (cf. [BCR87]). Given any set  $X \subset \mathcal{L}(n, m)$  we say that  $Y \subset X$  is a  $C$ -constructible subset of  $X$  if  $Y = X \cap Z$  where  $Z$  is a  $C$ -constructible subset of  $\mathcal{L}(n, m)$ . We will show various sets are  $C$ -constructible. To do this we need a more general notion of constructible which we now describe.

Let  $F$  be a differential field and  $F\{Y_1, \dots, Y_n\}$  the ring of differential polynomials with coefficients in  $F$ . There exists a differential field  $K$ ,  $F \subset K$ , such that for any  $p_1, \dots, p_m, q$  in  $F\{Y_1, \dots, Y_n\}$ , if  $p_1 = \dots = p_m = 0$ ,  $q \neq 0$  has a solution in some extension of  $F$ , then it has a solution in  $K$  ([KO74]). Further  $K$  and  $F$  have the same field of constants. Kolchin shows that any Picard-Vessiot extension of  $F$  is isomorphic to a unique subfield of  $K$ . We therefore may assume that all Picard-Vessiot extensions we consider are subfields of  $K$ . We say a subset  $\mathcal{S}$  of  $K^n$  is *differentially  $F$ -constructible* if it is the union  $T_1 \cup \dots \cup T_k$  where each  $T_i$  is of the form  $\{\bar{y} \in K^n | p_{1i}(\bar{y}) = \dots = p_{mi}(\bar{y}) = 0, q_i(\bar{y}) \neq 0\}$  for some  $p_{ji}, q_i$  in  $F\{Y_1, \dots, Y_n\}$ . The differentially  $F$ -constructible sets are precisely the elements of the Boolean algebra generated by the differentially Zariski closed sets, defined over  $F$ . It is known that if  $\mathcal{S} \subset K^n \times K^n = K^{n+m}$  is a differentially  $F$ -constructible set and  $p_2: K^n \times K^m \rightarrow K^m$  is the projection onto the second factor, then  $p_2(\mathcal{S})$  is a differentially  $F$ -constructible set ([SE56], [SA72], p. 295, and [GR89]). We shall refer to this fact as Seidenberg's principle and use it frequently in the sequel to show that certain sets are  $C$ -constructible. For example, if one fixes an integer  $N$ , then the set of  $L(y) \in \mathcal{L}(n, m)$  satisfying the following conditions is  $C$ -constructible: there exists a non-zero solution  $y$  of  $L(y) = 0$  such that  $u = y'/y$  satisfies  $p(x, u) = 0$  where  $p$  is a polynomial in  $x$  and  $u$  of degree  $\leq N$ . To see this, let  $p(x, u) = \sum_{i,j=0}^N b_{ij}x^i u^j$  and write  $L(y) = \sum_{i=0}^n \sum_{j=0}^m a_{ij}x^j y^{(i)}$ . Let  $\mathcal{S}$  be the set of  $(a_{ij}, b_{ij}, x, y, u)$  such that  $a'_{ij} = b'_{ij} = 0$ ,  $b_{ij}$  not all zero,  $x' = 1$ ,  $y \neq 0$  satisfies  $L(y) = 0$  for some  $L(y) \in \mathcal{L}(n, m, B)$ ,  $uy = y'$  and  $p(x, u) = 0$ . This is a differentially  $C$ -constructible set. If we project this set onto the  $(a_{ij})$ , Seidenberg's principle tells us that the set of such  $(a_{ij})$  is again differentially  $C$ -constructible. Since the  $a_{ij}$  are also constants, we may replace any occurrence of a derivative of  $a_{ij}$  by 0. Therefore a differentially constructible set of constants is constructible and so the set  $\mathcal{S}$  is a  $C$ -constructible subset of  $\mathcal{L}(n, m)$ .

(b) *Bounds on orders, degrees and exponents.* In this subsection we fix a field  $C \subset \mathbb{C}$  and show that if we start with elements in

$\mathcal{L}(n, m, B)$  or  $\mathcal{L}(n, m, \mathcal{D})$  then we can calculate  $m', n', B'$  and  $\mathcal{D}'$  such that certain associated linear differential equations must lie in  $\mathcal{L}(n', m', B')$  or  $\mathcal{L}(n', m', \mathcal{D}')$ . The results here strengthen results appearing in [SI80] and [SI81] which in turn rely on ideas from [SCH68].

**LEMMA 3.1.** (i) *Let  $AX = 0$  be a system of  $r$  equations in  $s$  unknowns where  $s > r$  and  $A$  has entries in  $C[x]$ ,  $C$  a field. If the degree of each entry in  $A$  is at most  $N$ , then  $AX = 0$  has a non-zero solution in  $C[x]^s$  whose entries have degree at most  $rN$ .*

(ii) *Let  $AX = D$  be a system of  $r$  equations in  $s$  unknowns where  $A$  and  $D$  have entries in  $C[x]$ ,  $C$  a field. If the degree of each entry in  $A$  and  $D$  is at most  $N$  and  $AX = D$  has a solution in  $C(x)^s$  then it has a solution whose entries have numerators and denominators of degree at most  $rN$ .*

*Proof.* (i) By replacing  $AX = 0$  by a smaller system of equations, we may assume that  $A = [a_{ij}]$  has rank  $r$ . Let  $B = [a_{ij}]_{1 \leq i, j \leq r}$ , and we assume, without loss of generality, that  $\det B \neq 0$ . Set each  $x_j = 1$  for  $j > r$  and rewrite the system  $AX = 0$  as  $BX = D$ , for some  $r \times 1$  matrix  $D$ . Using Cramer's rule, we have  $x_j = \det(B_j)/\det(B)$  for  $1 \leq j \leq r$  where  $B_j$  is formed by replacing the  $j$ th column of  $B$  by  $D$ . One sees that the degrees of  $\det(B_j)$  and  $\det(B)$  are bounded by  $rN$  and that  $x_j = \det(B_j)$  for  $1 \leq j \leq r$  and  $x_j = \det(B)$  for  $r + 1 \leq j \leq s$  forms a solution of  $AX = 0$ .

(ii) An application of Cramer's Rule as above yields this result.  $\square$

**LEMMA 3.2.** *Given integers  $n$  and  $m$  one can find integers  $n'$  and  $m'$  such that for any  $L_1$  and  $L_2$  in  $\mathcal{L}(n, m)$  there exist  $L_3, L_4$  and  $L_5$  in  $\mathcal{L}(n', m')$  such that  $\text{Soln}(L_3) = \{y_1 + y_2 | y_1 \in \text{Soln}(L_1), y_2 \in \text{Soln}(L_2)\}$ ,  $\text{Soln}(L_4)$  is spanned by  $\{y_1 \cdot y_2 | y_1 \in \text{Soln}(L_1), y_2 \in \text{Soln}(L_2)\}$  and  $\text{Soln}(L_5) = \{y' | y \in \text{Soln}(L_1)\}$ . Furthermore, given local data  $\mathcal{D}$  (resp. a local bound  $B$ ) there exists local data  $\mathcal{D}'$  (resp. a local bound  $B'$ ) depending only on  $n, m$  and  $\mathcal{D}$  (resp.  $B$ ) such that if  $L_1$  and  $L_2 \in \mathcal{L}(n, m, \mathcal{D})$  (resp.  $\mathcal{L}(n, m, B)$ ) then  $L_3, L_4$  and  $L_5 \in \mathcal{L}(n', m', \mathcal{D}')$  (resp.  $\mathcal{L}(n', m', B')$ ).*

*Proof.* We will prove the existence of  $L_3$ ; the other cases are proved in a similar manner (see [SI80]). Let  $L_1(y) = a_n y^{(n)} + \cdots + a_0 y$  and  $L_2(y) = b_n y^{(n)} + \cdots + b_0 y$  with  $a_i, b_i \in \mathbb{C}[x]$ . We will furthermore assume that  $a_n b_n \neq 0$ ; easy modifications can be made if  $a_n = 0$

or if  $b_n = 0$ . Let  $Y_1$  and  $Y_2$  be differential variables, and formally differentiate  $Y_1 + Y_2$   $2n$  times. Using the relation  $L_1(Y_1) = 0$  and its derivatives, we can replace occurrences of  $Y_1^{(i)}$ ,  $i \geq n$ , with  $C(x)$ -linear combinations of  $Y_1^{(j)}$ ,  $0 \leq j \leq n-1$ . A similar replacement can be made for  $Y_2^{(i)}$ . In this way we get  $2n+1$  expressions  $E_0, \dots, E_{2n}$  in the  $2n$  variables  $Y_1^{(j)}, Y_2^{(j)}$ ,  $0 \leq j \leq n-1$ . Let  $n'$  be the smallest integer such that there exist  $c_0, \dots, c_{n'}$ , in  $\mathbb{C}[x]$ , not all zero such that  $\sum_{i=0}^{n'} c_i(Y_1+Y_2)^{(i)} = 0$ . Clearly any solutions  $y_1, y_2$  of  $L_1(y) = 0$  and  $L_2(y) = 0$  respectively yield a solution  $y_1+y_2$  of  $\sum_{i=0}^{n'} c_i y^{(i)} = 0$ . As in [SI80] one can also show that all solutions of  $\sum_{i=0}^{n'} c_i y^{(i)} = 0$  are of this form.

The  $c_i$  satisfy a system of  $2n+1$  linear homogeneous (algebraic) equations whose coefficients involve the  $a_i$  and  $b_i$  and their derivatives. The degree of the coefficients can be explicitly bounded in terms of the degrees of the  $a_i$  and the  $b_i$  (that is, in terms of  $m$ ). Therefore, by Lemma 3.1, there is a number  $m'$  such that we can find  $c_i$ , not all zero, with the degrees of the  $c_i$  less than  $m'$ .

We have therefore shown that  $y_1+y_2$  satisfies an equation  $L_3(y) = 0$  with  $L_3(y)$  in  $\mathcal{L}(n', m')$  such that every solution of this equation is the sum of a solution of  $L_1(y) = 0$  and a solution of  $L_2(y) = 0$ . Fix some local data  $\mathcal{D}$  and assume that  $L_1, L_2 \in \mathcal{L}(n, m, \mathcal{D})$ . At any point, the determining factors are either those of  $L_1$  or of  $L_2$  and therefore are in  $\mathcal{D}$ . The exponents are of the form  $\rho + t$  where  $\rho$  is an exponent of  $L_1$  or  $L_2$  and  $t$  is a positive integer (the presence of  $t$  is due to the fact that terms may cancel in the sum of solutions of  $L_1(y) = 0$  and  $L_2(y) = 0$ ; this explains why new apparent singularities may enter in  $L_3$ ). If  $B$  is a local bound for  $L_1$  and  $L_2$  then Lemma 2.13 implies that there are only a finite number of possibilities for these non-negative integers and that these only depend on  $n, m$  and  $B$  (or  $\mathcal{D}$ ). This allows us to construct, from  $n, m$  and  $\mathcal{D}$  (resp.  $B$ ) local data  $\mathcal{D}'$  (resp.  $B'$ ) such that  $L_3 \in \mathcal{L}(n, m, \mathcal{D}')$  (resp.  $\mathcal{L}(n', m', B')$ ).

For  $L_4$ , the determining factors will be of the form  $P_1 + P_2$  where  $P_1$  is a determining factor of  $L_1$  and  $P_2$  is a determining factor of  $L_2$ . The exponents will be of the form  $\rho_1 + \rho_2 + t$  where  $\rho_1$  is an exponent of  $L_1$  and  $\rho_2$  is an exponent of  $L_2$  and  $t$  is a non-negative integer. For  $L_5$  the determining factors are the same as those of  $L_1$ . The exponents are of the form  $\rho - (\deg P)(1/n!) - 1 + t$  where  $\rho$  is an exponent of  $L_1$ ,  $P$  is a determining factor of  $L_1$  and  $t$  is a non-negative integer. For both  $L_4$  and  $L_5$  we now proceed as above.  $\square$

LEMMA 3.3. Let  $n$  and  $m$  be integers,  $\mathcal{D}$  local data and  $B \geq 0$ .

(i) Let  $P(Y_1, \dots, Y_t)$  be a differential polynomial in

$$C(x)\{Y_1, \dots, Y_t\}.$$

One can find integers  $n', m'$  such that if  $L_1, \dots, L_t \in \mathcal{L}(n, m)$  then there exists an  $L_P \in \mathcal{L}(n', m')$  having the property that if  $y_i$  satisfies  $L_i(y_i) = 0, i = 1, \dots, t$ , then  $P(y_1, \dots, y_t)$  is a solution of  $L_P(y) = 0$ . Furthermore, one can find local data  $\mathcal{D}'$  (resp. a local bound  $B'$ ) depending only on  $P, n, m$  and  $\mathcal{D}$  (resp.  $B$ ) such that if  $L_i \in \mathcal{L}(n, m, \mathcal{D})$  (resp.  $\mathcal{L}(n, m, B)$ ) then  $L_P$  can be chosen to be in  $\mathcal{L}(n', m', \mathcal{D}')$  (resp.  $\mathcal{L}(n', m', B')$ ).

(ii) Let

$$P(Y_1, \dots, Y_n, C_1, \dots, C_N) \in C(x)\{Y_1, \dots, Y_n, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}.$$

One can find integers  $n'$  and  $m'$  such that for any  $L \in \mathcal{L}(n, m)$  there exists  $L_P \in \mathcal{L}(n', m')$  having the property that if  $y_1, \dots, y_n$  forms a fundamental set of solutions of  $L(y) = 0$  and  $c_1, \dots, c_N$  are constants then  $P(y_1, \dots, y_n, c_1, \dots, c_N)$  is a solution of  $L_P(Y) = 0$ . Furthermore, one can find local data  $\mathcal{D}'$  (resp. a local bound  $B'$ ) depending only on  $P, n, m$  and  $\mathcal{D}$  (resp.  $n, m$  and  $B$ ) such that if  $L \in \mathcal{L}(n, m, \mathcal{D})$  (resp.  $\mathcal{L}(n, m, B)$ ) then  $L_P$  can be chosen to be in  $\mathcal{L}(n', m', \mathcal{D}')$  (resp.  $\mathcal{L}(n', m', B')$ ).

*Proof.* (i) follows from Lemma 3.2 by induction.

(ii) Let  $L(y) \in \mathcal{L}(n, m, \mathcal{D})$  let  $y_1, \dots, y_n$  be a basis for the solution space of  $L(y) = 0$  and let  $Wr$  denote the Wronskian determinant  $\det(y_i^{(j)})$ . If  $L(y) = a_n(x)y^{(n)} + \dots + a_0(x)y$ , then  $Wr'/Wr = -a_{n-1}/a_n$  so  $(Wr)^{-1}$  satisfies  $L_{Wr^{-1}}(y) = 0$  where  $L_{Wr^{-1}} \in \mathcal{L}(1, m)$ . Part (i) of this lemma now implies that there exist  $n', m'$  such that  $P(y_1, \dots, y_n, c_1, \dots, c_N)$  satisfies  $L_P(y) = 0$  for some  $L_P \in \mathcal{L}(n', m')$ .

Now assume  $L \in \mathcal{L}(n, m, \mathcal{D})$ . Part (i) implies that  $\exists n', m', \mathcal{D}'$  such that  $y = Wr$  satisfies  $\bar{L}(y) = 0$  for some  $\bar{L} \in \mathcal{L}(n', m', \mathcal{D}')$ . Therefore  $(Wr)^{-1}$  has exponents of the form  $-\rho$  and determining factors  $-P$  for  $\rho, P \in \mathcal{D}'$ . This implies that  $(Wr)^{-1}$  satisfies  $L_{Wr^{-1}}(y) = 0$  for  $L_{Wr^{-1}} \in \mathcal{L}(1, m, \mathcal{D}'')$  where  $\mathcal{D}'' = -\mathcal{D}'$ . If all we know is that  $L \in \mathcal{L}(n, m, B)$  then a similar argument shows that  $\bar{L} \in \mathcal{L}(n', m', B')$  for some  $B'$  so  $L_{Wr^{-1}} \in \mathcal{L}(1, m, B')$ . □

**LEMMA 3.4.** *Let  $L \in \mathcal{L}(n, m, B)$  and let  $r$  be a positive integer. There exist integers  $N_1$  and  $N_2$  depending only on  $r, n, m$  and  $B$  such that:*

(i) *if  $y$  satisfies  $L(y) = 0$  and  $y$  is algebraic of degree  $r$  over  $\mathbb{C}(x)$  with minimal polynomial  $y^r + b_{r-1}y^{r-1} + \dots + B_0$ ,  $b_i \in \mathbb{C}(x)$ , then the degrees of the numerator and denominator of each  $b_i$  are  $\leq N_1$ .*

(ii) *If  $y$  satisfies  $L(y) = 0$  and  $u = y'/y$  is algebraic of degree  $r$  over  $\mathbb{C}(x)$  with minimal polynomial  $u^r + b_{r-1}u^{r-1} + \dots + b_0$ ,  $b_i \in \mathbb{C}(x)$ , then the degrees of the numerator and denominator of each  $b_i$  are  $\leq N_2$ .*

*Proof.* (i) Since  $f(y) = y^r + b_{r-1}y^{r-1} + \dots + b_0$  is the minimal polynomial of  $y$ , any solution of  $f(y) = 0$  is also a solution of  $L(y) = 0$ . Therefore each  $b_i$  is a known symmetric polynomial of solutions  $u_1, \dots, u_n$  of  $L(y) = 0$ . Lemma 3.3(i) implies the existence of  $n', m', B'$  s.t. each  $b_i$  satisfies  $L_i(b_i) = 0$  for some  $L_i \in \mathcal{L}(n', m', B')$  and Proposition 2.11(i) implies that there exists an integer  $N_1$  such that the degrees of the numerators and denominators of each  $b_i$  are  $\leq N_1$ .

(ii) Since  $g(u) = u^r + b_{r-1}u^{r-1} + \dots + b_0$  is irreducible any solution  $u_i$  of  $g(u) = 0$  is of the form  $u_i = y'_i/y_i$  for some solution  $y_i$  of  $L(y) = 0$ . Note that  $b_{r-1} = -(u_1 + \dots + u_r) = (\prod y_i)' / (\prod y_i) \in \mathbb{C}(x)$ . Let  $P = Y_1 \cdot \dots \cdot Y_r$ . Lemma 3.3(i) implies the existence of  $n', m', B'$  depending only on  $P, n, m$  and  $B$  such that  $P(y_1, \dots, y_r)$  satisfies  $L_P(y) = 0$  for some  $L_P \in \mathcal{L}(n', m', B')$ . Since

$$P'(y_1, \dots, y_r) / P(y_1, \dots, y_r) \in \mathbb{C}(x),$$

Proposition 2.11(ii) implies that there exists an  $M$  such that the degrees of the numerator and denominator of  $b_{r-1} \leq M$ . We furthermore have that  $P(y_1, \dots, y_r)$  satisfies  $\bar{L}(y) = 0$  for some  $\bar{L} \in \mathcal{L}(1, M, B')$ . Therefore  $(\prod y_i)^{-1} = 1/P(y_1, \dots, y_r)$  satisfies  $\bar{\bar{L}}(y) = 0$  for some  $\bar{\bar{L}} \in \mathcal{L}(1, M, B')$ . Each  $b_i, 0 \leq i \leq r - 1$ , is of the form  $P_i(y_1, \dots, y_r)(\prod y_i)^{-1}$  where  $P_i \in \mathbb{C}\{Y_1, \dots, Y_r\}$ . Therefore Lemma 3.3(i) and Proposition 2.11(ii) imply there exists an integer  $N_2$  such that the degrees of the numerators and denominators of the  $b_i \leq N_2$ . □

**LEMMA 3.5.** *Let  $L \in \mathcal{L}(n, m, B)$  and  $r$  be an integer. There exist integers  $n', m'$  such that if  $y$  is a solution of  $L(y) = 0$  and  $y'/y$  is*

algebraic of degree  $\leq r$  over  $\mathbb{C}(x)$  then  $y^{-1}$  satisfies  $\tilde{L}(y^{-1}) = 0$  for some  $\tilde{L} \in \mathcal{L}(n', m', B)$ .

*Proof.* It is enough to prove this lemma assuming that  $y'/y$  has degree  $= r$ . Let  $K$  be the Picard-Vessiot extension of  $L$  over  $\mathbb{C}(x)$ . Lemma 3.4 implies that there exists an  $N$ , depending only on  $r, n, m$ , and  $B$  such that  $u = y'/y$  satisfies  $f(u) = u^r + b_{r-1}u^{r-1} + \dots + b_0 = 0$  where the degrees of the numerators and denominators of the  $b_i \leq N$ . Let  $u_1 = u, u_2, \dots, u_r$  be the conjugates of  $u$ . Each  $u_i$  is of the form  $y'_i/y_i$  for some solution  $y_i$  of  $L(y) = 0$ . The Galois group of  $K$  over  $\mathbb{C}(x)$  acts transitively on the  $u_i$  and permutes them. Let  $v_1 = -u_1, \dots, v_r = -u_r$ . These elements are all conjugate and the minimal polynomial is  $g(v) = (-1)^r v^r + (-1)^{r-1} b_{r-1} v^{r-1} + \dots + b_0$ . Let  $z_i = e^{\int v_i} = y_i^{-1}$  for  $i = 1, \dots, r$ . If  $\sigma \in \text{Gal}(K/\mathbb{C}(x))$  then  $\sigma(e^{\int v_i}) = c_\sigma e^{\int v_{\sigma(i)}}$  for some constant  $c_\sigma$ . Therefore the  $\mathbb{C}$ -span  $V$  of  $z_1, \dots, z_r$  is left invariant by  $\text{Gal}(K/\mathbb{C}(x))$  and so is the solution space of some linear differential equation  $\tilde{L}$  with coefficients in  $\mathbb{C}(x)$ . We will now find  $n', m'$  such that  $\tilde{L} \in \mathcal{L}(n', m', B)$ .

Note that  $z'_i = v_i z_i, z''_i = (v'_i + v_i^2)z_i, \dots, z_i^{(j)} = P_j(v_i)z_i$  where  $P_j(v_i) = (P_{j-1})' + v_i P_{j-1}, P_0 = 1$ . Using  $g(v) = 0$ , we see that there exists an  $M$  depending only on the degrees of the  $b_i$  so that each  $P_j(v)$  may be written as  $P_j(v) = a_{r-1,j}v^{r-1} + \dots + a_{0,j}$  where each  $a_{i,j}$  is the quotient of polynomials of degree  $\leq M$ . Let  $t$  be the smallest integer such that there exist  $c_0, \dots, c_t$  in  $\mathbb{C}[x]$ , not all zero with  $\sum_{j=0}^t c_j P_j(v) = 0$ . Each  $z_i$  will then be a solution of  $\tilde{L}(z) = \sum_{j=0}^t c_j z^{(j)} = 0$ . As in [SI80] one can also show that the  $z_i$  span  $\text{Soln}(\tilde{L})$ . The  $c_j$  satisfy a homogeneous system of linear (algebraic) equations whose coefficients are polynomials of degree  $\leq M$ . Therefore Lemma 3.1 implies that there is an  $M'$  depending only on  $M$  s.t. we can find  $c_i$ , not all zero, with  $\deg c_i \leq M'$ . Therefore  $\tilde{L} \in \mathcal{L}(r, M')$ . To find a local bound for  $\tilde{L}$ , note that at any point  $\alpha$ , each  $u_i$  has an expansion  $u_i = \sum_{j \geq j_0} a_{ij} t^j, t = (z - \alpha)^{1/n'}$ ,  $a_{ij} \in \mathbb{C}$ . Therefore each  $y_i = t^{\rho_i} e^{P_i(t)} \phi_i(t)$  where  $\phi_i \in \mathbb{C}[[t]], \phi_i(0) \neq 0$  and so  $z_i = t^{-\rho_i} e^{-P_i(t)} \psi_i(t), \psi_i(t) \in \mathbb{C}[[t]], \psi_i(0) \neq 0$ . Since the  $z_i$  span  $\text{Soln}(\tilde{L})$ , we have  $\tilde{L} \in \mathcal{L}(r, M', B)$ . □

In Lemma 3.6 we shall deal with the adjoint of a linear differential equation  $L(y) = a_n y^{(n)} + \dots + a_0 y$ . The adjoint is defined to be  $L^*(y) = (-1)^n (a_n y)^{(n)} + (-1)^{(n-1)} (a_{n-1} y)^{(n-1)} + \dots + a_0 y$ . If  $\{y_1, \dots, y_n\}$  form a fundamental set of solutions of  $L(y) = 0$  then

$\{z_1, \dots, z_n\}$  forms a fundamental set of solutions of  $L^*(y) = 0$  where  $z_i = (-1)^{i-1} \text{Wr}(y_1, \dots, \hat{y}_i, \dots, y_n) / \text{Wr}(y_1, \dots, y_n)$  ([SCH68], Vol. I, p. 64). Furthermore, if  $L(y) = L_1(L_2(y))$  then  $L^*(y) = L_2^*(L_1^*(y))$ .

**LEMMA 3.6.** *Given  $n, m$  and  $B$ , there exists a  $B'$  such that if  $L \in \mathcal{L}(n, m, B)$ , then  $L^* \in \mathcal{L}(n, m, B')$ .*

*Proof.* Lemma 3.3(ii) and Lemma 3.2 imply that there exist  $n', m'$  and  $B'$  such that if  $\{y_1, \dots, y_n\}$  is a fundamental set of solutions of  $L(y) = 0$  then there exists an  $\tilde{L} \in \mathcal{L}(n', m', B')$  such that  $\tilde{L}(z_i) = 0$  for  $i = 1, \dots, n$ . Therefore any solution of  $L^*(z) = 0$  is a solution of  $\tilde{L}(z) = 0$  and so  $L^* \in \mathcal{L}(n, m, B')$ .

**LEMMA 3.7.** *Given  $s, n, m$  and  $B$ , there exists an integer  $N$  satisfying the following: if  $L(y) = 0$  is a monic differential equation, with coefficients in  $\mathbb{C}(x)$ , such that  $a \cdot L \in \mathcal{L}(n, m, B)$  for some  $a \in \mathbb{C}[x]$  then if  $L(y) = L_2(L_1(y))$  where  $L_1(y)$  and  $L_2(y)$  are monic linear differential equations with coefficients in an algebraic extension of  $\mathbb{C}(x)$  of degree  $s$ , then each coefficient of  $L_2$  and  $L_1$  satisfies a monic polynomial of degree  $\leq s$  whose coefficients are quotients of polynomials of degree  $\leq N$ . If  $s = 1$  then there exists a  $d \in \mathbb{C}[x]$  such that  $d \cdot L_1 \in \mathcal{L}(n, N, B)$ . Furthermore, if  $a \cdot L \in \mathcal{L}(n, m, \mathcal{D})$  then  $d \cdot L_1 \in \mathcal{L}(n, N, \mathcal{D})$ .*

*Proof.* It is enough to prove this lemma assuming that  $L_1(y)$  has some fixed order  $k < n$ . If  $L_1(y) = y^{(k)} + b_{k-1}y^{(k-1)} + \dots + b_0$ , then  $b_{k-1} = (\text{Wr}(y_1, \dots, y_k))' / \text{Wr}(y_1, \dots, y_k)$  for some solutions  $y_1, \dots, y_k$  of  $L(y) = 0$ . Lemma 3.3 implies that there exist  $n', m', B'$  s.t.  $\text{Wr}(y_1, \dots, y_k)$  satisfies  $L_{k-1}(y) = 0$  for some  $L_{k-1} \in \mathcal{L}(n', m', B')$ . Since  $b_{k-1}$  is algebraic of degree  $\leq s$ , Lemma 3.4 implies that there exists an  $N$  such that  $b_{k-1}$  satisfies a polynomial of degree  $\leq s$  with coefficients in  $\mathbb{C}(x)$  whose numerators and denominators have degree  $\leq N$ . Furthermore, Lemma 3.5 implies there exist  $\tilde{n}, \tilde{m}, \tilde{B}$  such that  $y = 1/\text{Wr}(y_1, \dots, y_k)$  satisfies  $\tilde{L}(y) = 0$  for some  $\tilde{L} \in \mathcal{L}(\tilde{n}, \tilde{m}, \tilde{B})$ . Each  $b_i$  is of the form  $P_i(y_1, \dots, y_k) \cdot (1/\text{Wr}(y_1, \dots, y_k))$  so Lemma 3.2 implies there exist  $n'', m'', B''$  such that each  $b_i$  satisfies  $L_i(y) = 0$  for some  $L_i \in \mathcal{L}(n'', m'', B'')$ . Each  $b_i$  is algebraic of  $\text{deg} \leq s$  so Lemma 3.4 implies there exists an  $M$  such that each  $b_i$  satisfies an irreducible polynomial of degree  $\leq s$

with coefficients in  $\mathbb{C}(x)$  whose numerators and denominators are of degree  $\leq M$ .

Let  $L_2(y) = y^{(n-k)} + a_{n-k-1}y^{(n-k-1)} + \dots + a_0y$ . To handle the coefficients of  $L_2$ , we consider the adjoint operator  $L^* = L_1^*(L_2^*(y))$ . Applying the above considerations and Lemma 3.6 to  $L^*$  we see that there exist  $n'''$ ,  $m'''$ ,  $B'''$  such that each coefficient  $a_i$  of  $L_2^*$  satisfies  $L_i(y) = 0$  for some  $L_i \in \mathcal{L}(n''', m''', B''')$ . Since  $L_2 = (L_2^*)^*$  we see that each  $a_i = P_i(a_1^*, \dots, a_{n-k-1}^*)$  for some  $P_i \in \mathbb{C}\{Y_1, \dots, Y_{n-k-1}\}$  that depends only on  $n-k$  and  $i$ . Therefore Lemma 3.3 implies that there exist  $\tilde{n}$ ,  $\tilde{m}$ ,  $\tilde{B}$  (depending only on  $k, s, n, m$  and  $B$ ) such that  $a_i$  satisfies  $\tilde{L}_i(y) = 0$  for some  $\tilde{L}_i \in \mathcal{L}(\tilde{n}, \tilde{m}, \tilde{B})$ . Since each  $a_i$  is algebraic of degree  $\leq s$ , Lemma 3.4 implies there exists an  $M$  depending only on  $k, s, n, m, B$ , such that each  $a_i$  satisfies an irreducible polynomial whose coefficients have numerators and denominators of degree  $\leq M$ . Letting  $k$  vary from 1 to  $n-1$  yields the result.

If  $s = 1$ , then the bound  $N$  actually bounds the degrees of the numerators and denominators of the coefficients of  $L_1(y)$ . Let  $d$  be the least common multiple of the denominators of these coefficients. Any solution of  $L_1(y) = 0$  is a solution of  $L(y) = 0$  so if  $L \in \mathcal{L}(n, m, B)$  (resp.  $L \in \mathcal{L}(n, N, \mathcal{D})$ ) then  $d \cdot L_1 \in \mathcal{L}(n, 2N, B)$  (resp.  $d \cdot L \in \mathcal{L}(n, 2N, \mathcal{D})$ ).  $\square$

In Proposition 3.9 below we show that a Picard-Vessiot extension  $K$  of  $\mathbb{C}(x)$  contains a copy of any finite dimensional  $G$ -module, where  $G$  is the Galois group of  $K$  over  $\mathbb{C}(x)$ . Before proving this we need some preliminary facts. Let  $G$  be a linear algebraic group defined over a field  $C$  and let  $V$  be a faithful finite dimensional  $G$ -module defined over  $C$ . In [WA79], p. 25, it is shown that every finite dimensional  $G$ -module defined over  $C$  can be constructed from  $V$  by the process of forming tensor products, direct sums, subrepresentations, quotients and duals. If the dimension of  $V$  is  $n$ , we may think of  $G \subset \text{GL}(n, C)$  and consider the one dimensional representation given by  $1/\det(g)$ . Let  $W$  be the associated one dimension  $G$ -module. As noted on p. 26 of [WA79], we do not need duals in the above process if we start with both  $V$  and  $W$ .

We shall also need an observation due to Ritt. Let  $k$  be a differential field and  $Z_1, \dots, Z_n$  differential indeterminates. The order of a differential polynomial  $P \in k\{Z_1, \dots, Z_n\}$  is defined to be the smallest integer  $r$  such that  $P \in k[Z_1, \dots, Z_n, \dots, Z_1^{(r)}, \dots, Z_n^{(r)}]$ . On page 35 of [RI66], Ritt shows the following:

**LEMMA 3.8.** *Let  $k$  be a differential field of characteristic 0 containing an element  $x$  with  $x' = 1$ , let  $Z_1, \dots, Z_n$  be differential indeterminates and let  $P(Z_1, \dots, Z_n) \in k\{Z_1, \dots, Z_n\}$  have order  $r$ . If  $P(Z_1, \dots, Z_n) \neq 0$ , there exists  $d_{ij} \in \mathbb{Q}$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq r$ , such that  $P(\sum_{j=0}^r d_{1j}x^j, \dots, \sum_{j=0}^r d_{nj}x^j) \neq 0$ .*

**PROPOSITION 3.9.** *Let  $C$  be an algebraically closed subfield of  $\mathbb{C}$ ,  $G$  a linear algebraic group defined over  $C$ ,  $V_1$  a faithful  $G$ -module of dimension  $n_1$ , and  $V_2$  a  $G$ -module of dimension  $n_2$ ,  $V_1$  and  $V_2$  defined over  $C$ . There exist integers  $m_2$  and  $N$  and elements  $P_1, \dots, P_{n_2} \in C(x)\{Y_1, \dots, Y_{n_1}, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$ , where  $Y_1, \dots, Y_{n_1}, C_1, \dots, C_N$  are differential indeterminates, satisfying the following: for any  $L_1 \in \mathcal{L}(n_1, m_1)$  whose Galois group  $\text{Gal}(L_1)$  is a  $C$ -subgroup of  $G$  and with  $\text{Soln}(L_1)$   $\text{Gal}(L_1)$ -isomorphic to  $V_1$  and any basis  $y_1, \dots, y_n$  of  $\text{Soln}(L_1)$ , there exist constants  $c_1, \dots, c_N$  such that  $P_1(y_1, \dots, y_{n_1}, c_1, \dots, c_N), \dots, P_{n_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_N)$  form the basis of a  $\text{Gal}(L_1)$  module  $C$ -isomorphic to  $V_2$ . Furthermore given  $m_1$  and  $\mathcal{D}_1$  (resp.  $m_1$  and  $B_1$ ) one can find  $m_2$  and  $\mathcal{D}_2$  (resp.  $m_2$  and  $B_2$ ) such that if  $L_1 \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  (resp.  $L \in \mathcal{L}(n_1, m_1, B_1)$ ) then  $P_1(y_1, \dots, y_{n_1}, c_1, \dots, c_N), \dots, P_{n_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_N)$  form the basis of  $\text{Soln}(L_2)$  for some  $L_2 \in \mathcal{L}(n_2, m_2, \mathcal{D}_2)$  (resp.  $L \in \mathcal{L}(n_2, m_2, B_2)$ ).*

*Proof.* As noted above,  $V_2$  can be identified with a  $G$ -module formed from  $V_1$  and  $(\det V_1)^{-1}$  by taking submodules, direct sums, tensor products and quotients. We shall show that if  $L_1$  is as above then this construction can be carried out inside the Picard-Vessiot extension associated with  $L_1(y) = 0$  and that this can be done in a way that is independent of  $\text{Gal}(L_1) \subset G$ . We shall proceed by induction on the number of these operations required to construct  $V_2$ . We shall assume that  $L_1 \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  (the proof when  $L_1 \in \mathcal{L}(n_1, m_1, B_1)$  is similar). We will start with the operation of taking submodules and prove the following:

Let  $W$  be a  $G$ -module of dimension  $\nu$ ,  $\overline{\mathcal{D}}$  local data,  $N$  and  $m$  integers. Assume there exist

$$w_1, \dots, w_\nu \in C(x)\{Y_1, \dots, Y_{n_1}, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$$

such that if  $L_1(y) \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  then for any basis  $y_1, \dots, y_{n_1}$  of  $\text{Soln}(L_1)$ , there exist constants  $c_1, \dots, c_N$  in  $C$  such that  $w_1(y_i, \dots, y_{n_1}, c_1, \dots, c_N), \dots, w_\nu(y_1, \dots, y_{n_1}, c_1, \dots, c_N)$  is a

basis of a  $\text{Gal}(L_1)$ -module isomorphic to  $W$  and  $W$  that is the solution space of some  $\bar{L} \in \mathcal{L}(\nu, \mu, \mathcal{D})$ . Let  $\tilde{W}$  be a sub- $G$ -module of  $W$  of dimension  $\tilde{\nu}$ . Then there exist integers  $\tilde{N}$  and  $\tilde{\mu}$  and local data  $\tilde{\mathcal{D}}$  and differential polynomials

$$p_1, \dots, p_{\tilde{\nu}} \in C(x)\{Y_1, \dots, Y_{n_1}, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_{\tilde{N}}\}$$

such that if  $L_1 \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  then for any basis  $y, \dots, y_{n_1}$  of  $\text{Soln}(L_1)$  there exist constant  $c_1, \dots, c_{\tilde{N}}$  in  $C$ , such that  $p_1(y_1, \dots, y_{n_1}, c_1, \dots, c_{\tilde{N}}), \dots, p_{\tilde{\nu}}(y_1, \dots, y_{n_1}, c_1, \dots, c_{\tilde{N}})$  is a basis of a  $\text{Gal}(L_1)$ -module isomorphic to  $\tilde{W}$  that is the solution space of some  $\tilde{L} \in \mathcal{L}(\tilde{\nu}, \tilde{\mu}, \tilde{\mathcal{D}})$ .

To see that this is true, let  $(D_{ij})$  be a  $\nu \times \tilde{\nu}$  matrix of new indeterminates and define  $p_1, \dots, p_{\tilde{\nu}}$  by letting

$$(p_1, \dots, p_{\tilde{\nu}}) = (w_1, \dots, w_{\nu})(D_{ij}).$$

If  $y_1, \dots, y_{n_1}, c_1, \dots, c_N$  are chosen so that  $w_1, \dots, w_{\nu}$  is a basis of  $W$ , then there exist constants  $d_{ij}$  in  $C$  so that

$$p_1(y_1, \dots, y_{n_1}, c_1, \dots, c_N, d_{11}, \dots, d_{\nu\tilde{\nu}}), \\ \dots, p_{\tilde{\nu}}(y_1, \dots, y_{n_1}, c_1, \dots, c_N, d_{11}, \dots, d_{\nu\tilde{\nu}})$$

will be a basis for  $\tilde{W}$ . Lemma 2.10(ii) implies that  $\tilde{W} = \text{Soln}(\bar{L})$  where  $L_1(y) = a\bar{L}(\bar{L}(y))$  with  $\bar{L}$  and  $\bar{L}$  monic and having coefficients in  $\mathbb{C}(x)$ . Lemma 3.7 (with  $s = 1$ ) implies that there exists an integer  $\tilde{\mu}$  and  $d \in \mathbb{C}(x)$  such that  $d \cdot \bar{L}(y) \in \mathcal{L}(\tilde{\nu}, \tilde{\mu}, \tilde{\mathcal{D}})$ . To satisfy the conclusion of the above, we let  $\tilde{N} = \nu \cdot \tilde{\nu} + N$  and  $C_{N+1} = D_{11}, \dots, C_{\tilde{N}} = D_{\nu\tilde{\nu}}$ .

We now consider the operations of taking direct sums, tensor products and quotients and show the following:

Let  $W_1$  and  $W_2$  be  $G$ -modules of dimensions  $\nu_1$  and  $\nu_2$ ,  $\mathcal{D}_1$  and  $\mathcal{D}_2$  local data,  $N$ ,  $\mu_1$ , and  $\mu_2$  integers. Assume that there exist  $w_{11}, \dots, w_{1\nu_1}, w_{21}, \dots, w_{2\nu_2}$  in

$$C(x)\{Y_1, \dots, Y_{n_1}, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$$

such that if  $L_1(y) \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  then, for any basis  $y_1, \dots, y_{n_1}$  of the solution space of  $L_1(y)$  there are constants  $c_1, \dots, c_N$  in  $C$  such that

$$w_{11}(y_1, \dots, y_{n_1}, c_1, \dots, c_N), \dots, w_{1\nu_1}(y_1, \dots, y_{n_1}, c_1, \dots, c_N)$$

is the basis of the solution space (isomorphic to  $W_1$ ) of some  $\bar{L}_1(y) \in \mathcal{L}(\nu_1, \mu_1, \mathcal{D}_1)$  and

$$w_{21}(y_1, \dots, y_{n_1}, c_1, \dots, c_N), \dots, w_{2\nu_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_N)$$

is a basis for the solution space (isomorphic to  $W_2$ ) of some  $\bar{L}_2(y) \in \mathcal{L}(\nu_2, \mu_2, \mathcal{D}_2)$ . Then there exist integers  $\bar{m}$  and  $N'$ , and local data  $\bar{\mathcal{D}}$  and differential polynomials  $q_1, \dots, q_{\nu_1+\nu_2}, r_1, \dots, r_{\nu_1 \cdot \nu_2}$  and  $s_1, \dots, s_{\nu_1-\nu_2}$  in  $C(x)\{Y_1, \dots, Y_n, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_{N'}\}$  such that if  $L_1(y) \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$ , then for any basis  $y_1, \dots, y_{n_1}$  of  $\text{Soln}(L_1)$  there are constants  $c_1, \dots, c_{N'}$  in  $C$  such that:

(i)

$$q_1(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'}), \dots, q_{\nu_1+\nu_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'})$$

is a basis of a  $\text{Gal}(L_1)$ -module,  $C$ -isomorphic to  $W_1 \oplus W_2$ , that is the solution space of some  $\bar{L}_3(y) \in \mathcal{L}(\nu_1 + \nu_2, \bar{m}, \bar{\mathcal{D}})$ .

(ii)

$$r_1(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'}), \dots, r_{\nu_1 \cdot \nu_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'})$$

is a basis of a  $\text{Gal}(L_1)$ -module,  $C$ -isomorphic to  $W_1 \otimes W_2$ , that is the solution space of some  $\bar{L}_4(y) \in \mathcal{L}(\nu_1 \cdot \nu_2, \bar{m}, \bar{\mathcal{D}})$ ,

(iii)

$$s_1(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'}), \dots, s_{\nu_1-\nu_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_{N'})$$

is a basis of a  $\text{Gal}(L_1)$ -module,  $C$ -isomorphic to  $W_1/W_2$ , that is the solution space of some  $\bar{L}_5 \in \mathcal{L}(\nu_1 - \nu_2, \bar{m}, \bar{\mathcal{D}})$  (assuming that  $W_2 \subset W_1$ ).

We begin by proving (i). Of course, we would like to claim that  $w_1, \dots, w_{1\nu_1}, w_{21}, \dots, w_{2\nu_2}$  will be a basis of  $W_1 \oplus W_2$ , but this is not necessarily true. We will remedy this by shifting the  $w_{2i}$ . Let  $Z_1, \dots, Z_{\nu_2}$  be differential indeterminates and let  $y_1, \dots, y_{n_1}$  be a basis for the solution space of some  $L_1(y) \in \mathcal{L}(n_1, m_1, \mathcal{D}_1)$  for which there are constants such that

$$\begin{aligned} \tilde{w}_{11} &= w_{11}(y_1, \dots, y_{n_1}, c_1, \dots, c_N) \\ &\quad \vdots \qquad \qquad \qquad \vdots \\ \tilde{w}_{1\nu_1} &= w_{1\nu_1}(y_1, \dots, y_{n_1}, c_1, \dots, c_N) \end{aligned}$$

(resp.

$$\begin{aligned} \tilde{w}_{21} &= w_{21}(y_1, \dots, y_{n_1}, c_1, \dots, c_N) \\ &\quad \vdots \qquad \qquad \qquad \vdots \\ \tilde{w}_{2\nu_2} &= w_{2\nu_2}(y_1, \dots, y_{n_1}, c_1, \dots, c_N) \end{aligned}$$

are linearly independent solutions of some  $\overline{L}_1(y) \in \mathcal{L}(\nu_1, \mu_1, \overline{\mathcal{D}}_1)$  (resp.  $\overline{L}_2(y) \in \mathcal{L}(\nu_2, \mu_2, \overline{\mathcal{D}}_2)$ ). Consider the differential polynomial

$$P(Z_1, \dots, Z_{\nu_2}) = \text{Wr} \left( \tilde{w}_{11}, \dots, \tilde{w}_{1\nu_1}, \sum_{i=1}^{\nu_2} Z_i \tilde{w}_{21}^{(i-1)}, \dots, \sum_{i=1}^{\nu_2} Z_i \tilde{w}_{2\nu_2}^{(i-1)} \right).$$

This is a non-zero polynomial since  $(w_{2j}^{(i-1)})_{1 \leq i, j \leq \nu_2}$  is nonsingular and  $\text{Wr}(\tilde{w}_{11}, \dots, \tilde{w}_{1\nu_1}, Z_1, \dots, Z_{\nu_2})$  is non-zero. Therefore Lemma 3.9 implies that, for some  $M > 0$  and  $d_{ij} \in \mathbb{Q}$ ,

$$P \left( \sum_{j=0}^M d_{1j} x^j, \dots, \sum_{j=0}^M d_{\nu_2 j} x^j \right) \neq 0.$$

Note that  $M$  can be chosen to be any integer bigger than or equal to the order of  $P(Z_1, \dots, Z_{\nu_2})$  and this order can be bounded in terms of  $\nu_1$  and  $\nu_2$ . Letting

$$\begin{aligned} q_1 &= w_{11}, \dots, q_{\nu_1} = w_{1\nu_1}, \\ q_{\nu_1+1} &= \sum_{i=1}^{\nu_2} \left( \sum_{j=0}^M D_{ij} x^j \right) w_{2\nu_1}^{(i-1)} \\ &\quad \vdots \qquad \qquad \qquad \vdots \\ q_{\nu_1+\nu_2} &= \sum_{i=1}^{\nu_2} \left( \sum_{j=0}^M D_{ij} x^j \right) w_{2\nu_2}^{(i-1)} \end{aligned}$$

and  $C_{N+1} = D_{11}, \dots, C_{N'} = D_{\nu_2 M}$  gives us the desired elements of  $C(x)\{Y_1, \dots, Y_{n_1}, (\det(Y_i^{(j)}))^{-1} C_1, \dots, C_{N'}\}$  since the vector space spanned by  $q_{\nu_1+1}, \dots, q_{\nu_1+\nu_2}$  is  $\text{Gal}(L_1)$ -isomorphic to  $W_2$ . Lemma 3.3(b) implies that one can find integers  $n', m'$ , local data  $\mathcal{D}'$  and  $L_{q_i} \in \mathcal{L}(n', m', \mathcal{D}')$  for  $i = 1, \dots, \nu_1 + \nu_2$  such that

$$L_{q_i}(q_i(y_1, \dots, y_n, c_1, \dots, c_N)) = 0.$$

Lemma 3.2 implies that one can find integers  $n'', m''$  local data  $\mathcal{D}''$  and  $L \in \mathcal{L}(n'', m'', \mathcal{D}'')$  such that  $L(q_i(y_1, \dots, y_n, c_1, \dots, c_{N'})) = 0$  for  $i = 1, \dots, \nu_1 + \nu_2$ . Since  $q_1, \dots, q_{\nu_1+\nu_2}$  span a  $\text{Gal}(L_1)$ -invariant subspace of the solution space of  $L(y) = 0$ , we may write  $L(y) = a \cdot \tilde{L}_2(\tilde{L}_1(y))$  where  $\tilde{L}_1(y)$  and  $\tilde{L}_2(y)$  are monic and  $q_1, \dots, q_{\nu_1+\nu_2}$  span the solution space of  $L_1(y) = 0$ . If  $d$  is the least common multiple of the denominators of  $\tilde{L}_1(y)$ , then Lemma 3.8 guarantees that one can find  $\bar{m}$  and a local data  $\bar{\mathcal{D}}$  such that  $\bar{L}_3(y) = d \cdot \tilde{L}_1(y) \in \mathcal{L}(\nu_1 + \nu_2, \bar{m}, \bar{\mathcal{D}})$ . This satisfies (i) above.

To prove (ii), let  $\tilde{w}_{11}, \dots, \tilde{w}_{1\nu_1}, \tilde{w}_{21}, \dots, \tilde{w}_{2\nu_2}$  be as above. Let

$$P(Z_1, \dots, Z_{\nu_2}) = \text{Wr} \left( \tilde{w}_{11} \cdot \left( \sum_{i=1}^{\nu_2} Z_i \cdot w_{21}^{(i-1)} \right), \dots, \tilde{w}_{1\nu_1} \cdot \left( \sum_{i=1}^{\nu_2} Z_i w_{2\nu_2}^{(i-1)} \right) \right).$$

Since  $P$  is a non-zero polynomial, there exists an  $M$  and  $d_{ij} \in \mathbb{Q}$  such that

$$P \left( \sum_{j=0}^M d_{1j} x^j, \dots, \sum_{j=0}^M d_{\nu_2 j} x^j \right) \neq 0.$$

Letting

$$\begin{aligned} r_1 &= w_{11} \cdot \left( \sum_{i=1}^{\nu_2} \left( \sum_{j=0}^M D_{ij} x^j \right) w_{21}^{(i-1)} \right) \\ &\vdots \\ r_{\nu_1 \cdot \nu_2} &= w_{1\nu_1} \cdot \left( \sum_{i=1}^{\nu_2} \left( \sum_{j=0}^M D_{ij} x^j \right) w_{2\nu_2}^{(i-1)} \right) \end{aligned}$$

and  $C_{N+1} = D_{11}, \dots, C_{N'} = D_{\nu_2 M}$  gives us the desired elements. Lemma 3.2, Lemma 3.3 and Lemma 3.7 guarantee the existence of the desired  $\tilde{L}_4(y)$  as above.

To prove (iii), we may assume that  $\nu_2 > \nu_1$  and  $w_{21} = w_{11}, \dots, w_{2\nu_2} = w_{1\nu_2}$ . Let  $\tilde{w}_{11}, \dots, \tilde{w}_{1\nu_1}$  be as above. We know that there is some  $\bar{L}_1 \in \mathcal{L}(\nu_1, \mu_1, \bar{\mathcal{D}}_1)$  such that  $\bar{L}_1(\tilde{w}_{11}) = \dots = \bar{L}_1(\tilde{w}_{1\nu_1}) = 0$  and an  $\bar{L}_2 \in \mathcal{L}(\nu_2, \mu_2, \bar{\mathcal{D}}_2)$  such that  $\bar{L}_2(\tilde{w}_{11}) = \dots = \bar{L}_2(\tilde{w}_{1\nu_2}) = 0$ . Since every solution of  $\bar{L}_2(y) = 0$  is a solution of  $\bar{L}_1(y) = 0$ , there is a linear operator  $L_3$ , with coefficients in  $\mathbb{C}(x)$  such that  $\bar{L}_1(y) = L_3(\bar{L}_2(y))$ . Therefore  $\bar{L}_2(\tilde{w}_{1\nu_2+1}), \dots, \bar{L}_2(\tilde{w}_{1\nu_2})$  forms a basis of a

Gal( $L_1$ )-module isomorphic to  $W_1/W_2$ . We can therefore let

$$s_1 = \sum_{i=0}^{\nu_2} \left( \sum_{j=0}^{\bar{\mu}_2} D_{ij} x^j \right) w_{1\nu_2+1}^{(i)}, \dots, s_{\nu_1-\nu_2} = \sum_{i=0}^{\nu_2} \left( \sum_{j=0}^{\bar{\mu}_2} D_{ij} x^j \right) w_{1\nu_1}^{(i)}.$$

Setting  $C_{N+1} = D_{00}, \dots, C_{N'} = D_{\nu_2 \bar{\mu}_2}$ , we can apply Lemmas 3.2, 3.3 and 3.7 to conclude that the  $s_i$  satisfy (iii). □

**LEMMA 3.10.** *Let  $n, m$  be integers,  $\mathcal{D}$  local data, and  $P_1, \dots, P_t \in \mathbb{C}\{Y_1, \dots, Y_n, C_1, \dots, C_N, \det(Y_i^{(j)})^{-1}\}$ . One can find an integer  $M$ , depending only on  $n, m, \mathcal{D}$  and  $P_1, \dots, P_t$  satisfying the following:*

*For any  $L(y) \in \mathcal{L}(n, m, \mathcal{D})$ ,  $c_1, \dots, c_N \in \mathbb{C}$  and  $\{y_1, \dots, y_n\}$ , a fundamental set of solutions of  $L(y) = 0$  such that*

$$(P_i(y_1, \dots, y_n, c_1, \dots, c_N))' / P_i(y_1, \dots, y_n, c_1, \dots, c_N) \in \mathbb{C}(x),$$

*for  $i = 1, \dots, r$ , we have that*

$$P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, P_r(y_1, \dots, y_n, c_1, \dots, c_N)$$

*are algebraically dependent over  $\mathbb{C}(x)$  if and only if there exist integers  $m_1, \dots, m_r$ , not all zero, with  $|m_i| \leq M$  such that*

$$\prod_{i=1}^r (P_i(y_1, \dots, y_n, c_1, \dots, c_N))^{m_i} = R(x)$$

*where  $R(x) \in \mathbb{C}(x)$  and  $\deg(R(x)) \leq M$ .*

*Proof.* If  $\prod_{i=1}^r (P_i(y_1, \dots, y_n, c_1, \dots, c_N))^{m_i} = R(x)$  as above, then the  $P_i(y_1, \dots, y_n, c_1, \dots, c_N)$  are algebraically dependent. Conversely, if  $P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, P_r(y_1, \dots, y_n, c_1, \dots, c_N)$  are algebraically dependent over  $\mathbb{C}(x)$ , then the Kolchin-Ostrowski Theorem [KO68] implies that there exist integers  $m_1, \dots, m_r$  not all zero such that

$$(3.9.1) \quad \prod_{l=1}^r (P_l(y_1, \dots, y_n, c_1, \dots, c_N))^{m_l} = R(x)$$

for some rational function  $R(x) \in \mathbb{C}(x)$ . Lemma 3.2 and Lemma 2.10(ii) imply that we can find  $s, t, n_i$  and a finite set  $\mathcal{S}$  depending only on  $n, m, \mathcal{D}$  and  $P_1, \dots, P_t$  such that

$$\frac{P'_l}{P_l} = \sum_{i=1}^t \sum_{j=1}^{n_i} \frac{a_{ijl}}{(x - \alpha_{il})^j} + b_{sl} x^s + \dots + b_{0l}$$

for  $l = 1, \dots, r$  where  $a_{ijl}, b_{sl} \in \mathcal{S}$ . Let  $R(x) = \prod_{i=1}^d (x - \gamma_i)^{\overline{m}_i}$ . Taking the logarithmic derivative of (3.9.1), we have

$$(3.9.2) \quad \sum_{l=1}^r m_l \left( \sum_{i=1}^t \sum_{j=1}^{n_i} \frac{a_{ijl}}{(x - \alpha_{il})^j} + b_{sl}x^s + \dots + b_{0l} \right) = \sum_{i=1}^d \frac{\overline{m}_i}{(x - \gamma_j)}$$

Comparing positive powers of  $x$ , we have

$$(3.9.3) \quad \sum_{l=1}^r m_l b_{kl} = 0$$

for  $l = 1, \dots, r$ . Let  $\beta_1, \dots, \beta_q$  be the distinct elements among the  $\alpha_{il}$  and  $\gamma_j$ . Fix some  $\beta_i$ , say  $\beta_1$ . Comparing coefficients of  $(x - \beta_1)^{-1}$ , we have

$$(3.9.4) \quad \sum_{l=1}^r \sum_{\alpha_{il}=\beta_1} m_l a_{i1l} = \overline{m}_j$$

where  $\gamma_j = \beta_1$ . Comparing coefficients of  $(x - \beta_1)^{-j}$ ,  $j > 1$ , we have for each such  $j$

$$(3.9.5) \quad \sum_{l=1}^r \sum_{\alpha_{il}=\beta_1} m_l a_{ijl} = 0.$$

We get similar equations for each  $\beta_i$ . Note that the formation of the equations (3.9.3), (3.9.4) and (3.9.5) depends firstly only on the partition of the elements  $\alpha_{ij}$  and  $\gamma_i$  (according to which are equal) and not on the particular values of the  $\beta_i$  and secondly on a choice of the  $a_{ijl}$  and  $b_{jl}$  from the finite set  $\mathcal{S}$ . Furthermore, any choice of integers  $m_i$  and  $\overline{m}_i$  (not all zero) satisfying these equations will yield a solution of (3.9.1) (for a particular choice of  $\alpha_{ij}$  and  $\gamma_i$ ). Since there are only a finite number of partitions and only a finite number of choices for the  $a_{ijl}$  and  $b_{ijl}$ , we can find an integer  $M$  such that if there exist  $m_i$  satisfying (3.9.1) for some  $R(x)$ , then there exist such  $m_i$  with  $|m_i| \leq M$ .  $\square$

We note that, unlike the previous lemmas and propositions, the hypotheses in Lemma 3.10 cannot be weakened to assume  $L \in \mathcal{L}(n, m, B)$  for some local bound  $B$ . An example showing that we need to know the exponents is  $y' - (\alpha/x)y = 0$ . Let  $r = 1, P_1 = y$ .

Letting  $\alpha = (1/m)$  shows that as  $\alpha \rightarrow 0$  we must let  $m \rightarrow \infty$  to guarantee  $y^m \in \mathbb{C}(x)$ . An example showing that we need to know the determining factors and not just a bound on their degrees is given by  $y'' - (\alpha_1 + \alpha_2)y' + (\alpha_1\alpha_2)y = 0$ ,  $\alpha_1 \neq \alpha_2 \in \mathbb{C}$ . The solutions are  $y_1 = e^{\alpha_1 x}$ ,  $y_2 = e^{\alpha_2 x}$ , so  $\alpha_1 x$  are determining factors at  $\infty$ . Letting  $P_1 = y_1$ ,  $P_2 = y_2$ , and  $\alpha_2 = (1/n)\alpha_1$ , then  $P_1 P_2^n \in \mathbb{C}(x)$  with  $n \rightarrow \infty$  and a suitable choice of the coefficient of the determining factors.

(c) *Main Theorem.* In this section we show that certain sets of linear differential equations are constructible. Throughout this section  $C \subset \mathbb{C}$  is a fixed algebraically closed field.

**PROPOSITION 3.11.** *Let  $n$  and  $m$  be integers and  $B \geq 0$  a real number.*

(i) *Let  $G$  be a linear algebraic group and  $V$  a faithful  $G$ -module of dimension  $n$  both defined over  $C$ . The set of  $L \in \mathcal{L}(n, m, B)$  such that  $\text{Gal}(L) \subset G$  and  $\text{Soln}(L)$  is  $\text{Gal}(L)$ -isomorphic over  $C$  to  $V$  is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ .*

(ii) *If  $G$  is a finite group and  $V$  a faithful  $G$ -module, then  $\mathcal{L}(n, m, B, G, V)$  is  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ . Therefore, for any weak local data  $\mathcal{W}$ ,  $\mathcal{L}(n, m, \mathcal{W}, G, V)$  is a  $C$ -constructible set.*

*Proof.* (i) We start with some notation. Let  $f_1, \dots, f_t \in C[x_{11}, \dots, x_{nn}]$  generate the ideal of polynomials vanishing on  $G$ . If we select enough generators, we may assume that the  $C$ -span  $W$  of  $f_1, \dots, f_t$  is  $G$ -invariant under  $\lambda_g(f) = f((g)^{-1} \cdot (x_{ij}))$  and that  $G = \{g \in \text{GL}(n, \mathbb{C}) \mid \lambda_g W = W\}$ . Let  $Y = (Y_i^{(j)})$  and  $s = (s_{ij})$  where the  $Y_i^{(j)}$  and the  $s_{ij}$  are variables. For  $r = 1, \dots, t$ , let  $F_r(Y_i^{(j)}, s_{ij}) = f_r((Y^{-1} \cdot s)_{ij})$ . For  $L(y) \in \mathcal{L}(n, m, B)$  and  $y_1, \dots, y_n$  a fundamental set of solutions of  $L(y) = 0$ , let  $\tilde{Y} = (y_i^{(j)})$  and  $\tilde{F}_r(s_{ij}) = F_r(y_i^{(j)}, s_{ij})$  for  $r = 1, \dots, t$ . Note that the action of  $g \in G$  on  $\tilde{Y}$  is given by  $g(\tilde{Y}) = \tilde{Y} \cdot (g_{ij})$  for some  $(g_{ij}) \in \text{GL}(n, \mathbb{C})$ .

We first note that  $\tilde{F}_r(y_i^{(j)}) = f_r(\text{id}) = 0$ ,  $r = 1, \dots, t$ , where  $\text{id}$  is the identity matrix. Secondly, any  $g \in \text{Gal}(L)$  acts on the coefficients of  $\tilde{F}_r(s_{ij})$  via

$$\tilde{F}_r^g(s_{ij}) = g(\tilde{F}_r(s_{ij})) = f_r(g((y_i^{(j)})^{-1}) \cdot (s_{ij})) = \lambda_g f_r((y_i^{(j)})^{-1} \cdot (s_{ij})).$$

Therefore,  $\tilde{F}_r^g(y_i^{(j)}) = f_r(g^{-1})$ . We claim that the  $\mathbb{C}$ -span  $V$  of  $\{\tilde{F}_1, \dots, \tilde{F}_t\}$  is left invariant by  $\text{Gal}(L)$  if and only if  $\text{Gal}(L) \subset G$ .

To see this first assume that  $\text{Gal}(L) \subset G$ . For each  $g \in \text{Gal}(L)$ , we have

$$\tilde{F}_r^g(s_{ij}) = \lambda_g f_r((y_i^{(j)})^{-1} \cdot (s_{ij})) = \sum_k c_{rk}^g f_k((y_i^{(j)})^{-1} \cdot (s_{ij}))$$

for some  $c_{ij}^g$  in  $\mathbb{C}$ , since the span of the  $f_i$  is left invariant by  $G$ . Therefore  $\tilde{F}_r^g(s_{ij}) = \sum_k c_{rk}^g \tilde{F}_k(s_{ij})$ . Now assume that  $V$  is left invariant by  $\text{Gal}(L)$ . This implies that  $\tilde{F}_r^g(s_{ij}) = \sum_k c_{rk}^g \tilde{F}_k(s_{ij})$  for some constants  $c_{ij}^g$ . Therefore  $\tilde{F}_r^g(y_i^{(j)}) = 0$ , so  $f_r(g^{-1}) = 0$  and  $g$  is in  $G$ .

Therefore, to reach the desired conclusion we must show that the property “the  $\mathbb{C}$ -span  $V$  of  $\{\tilde{F}_1, \dots, \tilde{F}_t\}$  is left invariant by  $\text{Gal}(L)$ ” is  $C$ -constructible. To see this we consider each  $F_r(Y_i^{(j)}, s_{ij})$  as a polynomial in the  $s_{ij}$  with coefficients in  $C(Y_i^{(j)})$ . In such a polynomial the coefficient of each power product of the  $s_{ij}$  is of the form  $(\det(Y_i^{(j)}))^{-N} q(Y_i^{(j)})$ , where  $q$  is a polynomial. Therefore we may multiply the  $F_r$  by a sufficiently high power of  $\det(Y_i^{(j)})$  and assume that these coefficients are differential polynomials in  $C\{Y_1, \dots, Y_n\}$ . Assume that there are at most  $M$  power products of the  $s_{ij}$  in each  $F_r$  and order these products in some manner. We may identify each  $F_r$  with its vector of coefficients  $(P_{rl})_{1 \leq l \leq M}$ , where each  $P_{rl} \in C\{Y_1, \dots, Y_n\}$ . Let  $p_{rl} = P_{rl}\{y_1, \dots, y_n\}$ . Note  $(p_{rl})$  is the vector of coefficients of  $\tilde{F}_r$ . Let  $P$  be the  $t \times M$  matrix formed by these rows. Assume that the rank of  $P$  is  $t_1$  and let  $Q = (q_{ij})$  be the  $t_1 \times M$  matrix formed by using a maximal set of independent rows of  $P$ . Clearly  $V$  is left invariant by  $\text{Gal}(L)$  if and only if for any  $g \in \text{Gal}(L)$  there is an  $A_g \in \text{GL}(t_1, \mathbb{C})$  such that  $gQ = A_g \cdot Q$ . We shall show that this latter condition is  $C$ -constructible.

First note that Lemma 3.2 and Lemma 3.3 imply that there exist integers  $\bar{n}$  and  $\bar{m}$  and a local bound  $\bar{B}$  (depending only on  $n, m$  and  $B$ ) and an element  $\bar{L} \in \mathcal{L}(\bar{n}, \bar{m}, \bar{B})$  such that  $\bar{L}(q_{ij}) = 0$  for all entries  $q_{ij}$  of  $Q$ . Let  $\alpha$  be a point that is not a singular point of  $\bar{L}$  (i.e.  $\alpha$  is not a zero of the leading coefficient of  $\bar{L}$ ), let  $\nu_j = (j - 1)\bar{n}$  and let  $R = \sum_{j=1}^M (x - \alpha)^{\nu_j} Q_j$  where  $Q_j$  is the  $j$ th column of  $Q$ . We claim that the entries of  $R$  are linearly independent over  $\mathbb{C}$ . To see this, assume that we have  $c_i \in \mathbb{C}$ ,  $i = 1, \dots, t_1$ , such that

$$0 = \sum_{i=1}^{t_1} c_i \left( \sum_{j=1}^M (x - \alpha)^{\nu_j} q_{ij} \right) = \sum_{j=1}^M (x - \alpha)^{\nu_j} \left( \sum_{i=1}^{t_1} c_i q_{ij} \right).$$

For each  $j$ ,  $\sum_{i=1}^{t_1} c_i q_{ij}$  is a solution of  $\bar{L}(y) = 0$  analytic at  $\alpha$  which vanishes at  $\alpha$  to order at most  $\bar{n} - 1$ . Therefore the order of each non-zero term  $(x - \alpha)^{\nu_j} (\sum_{i=1}^{t_1} c_i q_{ij})$  is between  $(j - 1)\bar{n}$  and  $j\bar{n} - 1$ . Since the sum of these terms is zero we must have each  $\sum_{i=1}^{t_1} c_i q_{ij} = 0$ . Since the rows of  $Q$  are linearly independent, we must have that each  $c_i = 0$ .

We will now show that the statement that for any  $g \in \text{Gal}(L)$  there is an  $A_g \in \text{GL}(t_1, \mathbb{C})$  such that  $gQ = A_g \cdot Q$  is equivalent to the following:

(a) The entries of  $R$  form a basis for the solution space of some  $L$  in  $\mathcal{L}(\tilde{n}, \tilde{m}, \tilde{B})$  where  $\tilde{n}, \tilde{m}, \tilde{B}$  depend only on  $n, m$  and  $S$ .

(b)  $Q = WZ$  where  $W = (R, R', \dots, R^{(t_1-1)})$  and  $Z$  is a  $t_1 \times M$  matrix with entries that are rational functions (whose degrees can be a priori bounded in terms of  $n, m$  and  $B$ ).

Once we have shown this equivalence we will be done since Seidenberg's principle implies that (a) and (b) define  $C$ -constructible sets.

Let us start by assuming that for each  $g \in G$  there is an  $A_g \in \text{GL}(t_1, \mathbb{C})$  such that  $gQ = A_g \cdot Q$ . Since  $R = Q \cdot X$  where  $X = ((x - \alpha)^{\nu_1}, \dots, (x - \alpha)^{\nu_{t_1}})^T$  we see that the entries of  $R$  span a  $\text{Gal}(L)$  invariant space. Since these entries are linearly independent, Lemma 2.10(i), Lemma 3.2, Lemma 3.3, and Lemma 3.7 imply that there exist integers  $\tilde{n}$  and  $\tilde{m}$  and a local bound  $\tilde{B}$  (depending only on  $n, m$  and  $B$ ) such that these entries form a basis of the solution space of some  $\tilde{L} \in \mathcal{L}(\tilde{n}, \tilde{m}, \tilde{B})$ . Therefore (a) holds.

To see that (b) holds, let  $g \in \text{Gal}(L)$ . Since  $gR = g(Q \cdot X) = A_g R$ , we have  $gW = A_g W$ . Since  $W$  is the Wronskian matrix of the entries of  $R$ ,  $W$  is invertible. Therefore  $Z = W^{-1}Q$  is left invariant by  $\text{Gal}(L)$  and its entries so must lie in  $\mathbb{C}(x)$ . Lemma 3.2, Lemma 3.3 and Proposition 2.11(i) imply that we can a priori bound the degrees of  $Z$  in terms of  $n, m$  and  $B$  so (b) holds.

Conversely assume that (a) and (b) hold. (a) implies that for any  $g \in \text{Gal}(L)$  there exists an  $A_g \in \text{GL}(t_1, \mathbb{C})$  such that  $gR = A_g R$ . From (b) we deduce that  $gQ = A_g Q$ .

(ii) Let  $G$  be a finite group and  $H_1, \dots, H_t$  all the subgroups of  $G$ . We then have that

$$\begin{aligned} \mathcal{L}(n, m, B, G, V) &= \{L \in \mathcal{L}(n, m, B) \mid \text{Gal}(L) \subset G\} \\ &\quad - \bigcup_{i=1}^t \{L \in \mathcal{L}(n, m, B) \mid \text{Gal}(L) \subset H_i\}. \end{aligned}$$

Since  $C$ -constructible sets form a boolean algebra, this latter set is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ .  $\square$

Of course if  $L \in \mathcal{L}(n, m, B, G, V)$  for a finite group  $G$ , all solutions of  $L(y) = 0$  will be algebraic so  $L$  will have only regular singular points and rational exponents.

**PROPOSITION 3.12.** *Let  $n$  and  $m$  be integers and  $B$  a real number. Let  $G$  be a linear algebraic group with  $G^0$  the connected component of the identity and  $V$  a faithful  $G$ -module of dimension  $n$ , all defined over  $C$ . The set of  $L$  in  $\mathcal{L}(n, m, B)$  such that*

(i)  $\text{Gal}(L) \subset G$  and  $\text{Soln}(L)$  is isomorphic to  $V$  over  $C$  as  $\text{Gal}(L)$ -modules.

(ii) The map  $\pi: G \rightarrow G/G^0$  is surjective when restricted to  $\text{Gal}(L)$  is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ .

*Proof.* Let  $W$  be a faithful  $G/G^0$ -module. By Proposition 3.9 there exist  $P_1, \dots, P_t \in \mathbb{C}(x)\{Y_1, \dots, Y_n, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$  such that if  $L \in \mathcal{L}(n, m, B)$  and  $\text{Gal}(L) \subset G/G^0$  with  $\text{Soln}(L)$  isomorphic to  $W$  as a  $\text{Gal}(L)$ -module then for any basis  $\{y_1, \dots, y_n\}$  of  $\text{Soln}(L)$ , there exist constants  $c_1, \dots, c_N$  such that

$$P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, P_t(y_1, \dots, y_n, c_1, \dots, c_N)$$

generate a  $\text{Gal}(L)$ -module isomorphic to  $W$ . Furthermore, there exist  $n', m', B'$  depending only on  $n, m, B$  and the  $P_i$  such that  $W = \text{Soln}(L')$  for some  $L' \in \mathcal{L}(n', m', B)$ . Therefore (ii) is equivalent to: (ii') there exists a basis  $\{y_1, \dots, y_n\}$  and constants  $c_1, \dots, c_N$  such that  $P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, P_t(y_1, \dots, y_n, c_1, \dots, c_N)$  is a basis of  $\text{Soln}(L')$  for some  $L' \in \mathcal{L}(n', m', B', G/G^0, W)$ . Proposition 3.12(i) implies that (i) above defines a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ . Proposition 3.12(ii) implies that (ii') defines a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ . Therefore Seidenberg's principle implies that the set defined in the proposition is a  $C$ -constructible set of  $\mathcal{L}(n, m, B)$ .  $\square$

**PROPOSITION 3.13.** *Let  $n$  and  $m$  be integers and  $B$  a real number. Let  $G$  be a linear algebraic group,  $G^0$  its connected component of the identity and  $V$  a faithful  $G$ -module of dimension  $n$ , all defined over  $C$ . The set of  $L \in \mathcal{L}(n, m, B)$  such that*

(i)  $\text{Gal}(L) \subset G$  and  $\text{Soln}(L)$  is isomorphic to  $V$  over  $C$  as  $\text{Gal}(L)$ -modules.

(ii)  $\text{Ker } X(G^0) \subset \text{Gal}(L)$

is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ .

*Proof.* Proposition 3.11 implies that (i) defines a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$  so we only need to show that under the assumption that (i) is true, condition (ii) defines a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ . To see this, let  $W$  be the faithful  $G$ -module guaranteed to exist by Proposition 2.9. Let  $k = \dim W$ ,  $r = \dim(\text{Ch}_{G^0}(W))$ , and let  $s = [G : G^0]$ . Let  $V_1 = V$  and  $V_2 = W$  and let  $n_2, m_2, B_2$  and  $P_1, \dots, P_k \in \mathbb{C}(x)\{Y_1, \dots, Y_k, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$  be the elements guaranteed to exist by Proposition 3.9. We will show that (assuming (i) holds) (ii) is equivalent to the following condition and that this condition defines a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ :

(ii') There exists a basis  $\{y_1, \dots, y_n\}$  of  $\text{Soln}(L)$  and constants  $c_1, \dots, c_N$  such that

$$\{P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, P_k(y_1, \dots, y_n, c_1, \dots, c_N)\}$$

forms the basis of  $\text{Soln}(L_2)$  for some  $L_2 \in \mathcal{L}(n_2, m_2, B_2)$  with

(a)  $L_2(y) = L_{k-r}(L_r(y))$  where  $L_{k-r}(y)$  and  $L_r(y)$  have coefficients in an algebraic extension of  $\mathbb{C}(x)$  of degree  $\leq s$ .

(b) If  $L_2(y) = 0$  and  $y'/y$  is algebraic over  $\mathbb{C}(x)$  of degree  $\leq s$ , then  $L_r(y) = 0$ .

Assume (i) and (ii) hold so  $\text{Ker } X(G^0) \subset \text{Gal}(L)$ . Proposition 2.9 implies that  $\text{Ch}_{G^0}(W) = \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$ .  $\text{Ch}_{\text{Gal}(L) \cap G^0}(W)$  is a  $\text{Gal}(L) \cap G^0$  invariant subspace of  $W$  of dimension  $r$  so Lemma 2.10(ii) implies that  $L_2(y) = L_{k-r}(L_r(y))$  where

$$\text{Soln}(L_r) = \text{Ch}_{\text{Gal}(L) \cap G^0}(W),$$

and  $L_{k-r}$  and  $L_r$  have coefficients in the fixed field of  $\text{Gal}(L) \cap G^0$ . Since  $[\text{Gal}(L) : \text{Gal}(L) \cap G^0] \leq [G : G^0]$ , this fixed field is an algebraic extension of  $\mathbb{C}(x)$  of degree at most  $s$ . Therefore (a) is true. If  $L_2(y) = 0$  and  $y'/y$  is algebraic over  $\mathbb{C}(x)$ , then  $y'/y$  is left fixed by  $\text{Gal}(L)^0$ . Since  $\text{Ker } X(G^0) \subset \text{Gal}(L)^0$  we have  $\text{Ch}_{\text{Gal}(L)^0}(W) = \text{Ch}_{G^0}(W) = \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$ . Therefore  $y \in \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$  so  $L_r(y) = 0$ .

Now assume (i) and (ii') hold. We will show  $\text{Ch}_{\text{Gal}(L) \cap G^0}(W) = \text{Ch}_{G^0}(W)$  so by Proposition 2.9,  $\text{Ker } X(G^0) \subset \text{Gal}(L)$ . Let  $t = \dim \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$  and let  $\{\tilde{y}_1, \dots, \tilde{y}_t\}$  be a basis of  $\text{Ch}_{\text{Gal}(L) \cap G^0}(W)$  where each  $\tilde{y}_i$  spans a  $\text{Gal}(L) \cap G^0$ -invariant subspace of  $W$ . For each  $i$ ,  $\tilde{y}'_i/\tilde{y}_i$  will be  $\text{Gal}(L) \cap G^0$ -invariant and so be algebraic over

$\mathbb{C}(x)$  of degree at most  $s$ . Therefore (b) implies that each  $\hat{y}_i$  satisfies  $L_r(\hat{y}_i) = 0$ . This implies  $t \leq r$ . Since  $\text{Gal}(L) \cap G^0 \subset G^0$ , we have  $\text{Ch}_{G^0}(W) \subset \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$  so we must have  $t = r$  and  $\text{Ch}_{G^0}(W) = \text{Ch}_{\text{Gal}(L) \cap G^0}(W)$ .

Therefore, assuming (i), (ii) and (ii') are equivalent. To see that (ii') is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$  note that Lemma 3.7 implies that there exists an  $M$  depending only on  $n_2, m_2$  and  $B_2$  (and so only on  $N, m$  and  $B$ ) such that the coefficients of  $L_{k-r}$  and  $L_r$  satisfy irreducible polynomials over  $\mathbb{C}(x)$  whose coefficients are quotients of polynomials of degree  $\leq M$ . Furthermore Lemma 3.4(ii) implies that there exists an  $\tilde{M}$  such that if  $y$  is as in (b) then  $y'/y$  will satisfy an irreducible polynomial whose coefficients are quotients of polynomials of degree  $\leq \tilde{M}$ . Using Seidenberg's principle we see that (ii') defines a  $C$ -constructible set.  $\square$

**THEOREM 3.14.** *Let  $n$  and  $m$  be integers and  $B$  a real number. Let  $G$  be a linear algebraic group,  $G^0$  its connected component of the identity and  $V$  a faithful  $G$ -module of dimension  $n$ , all defined over  $C$ . The set of  $L \in \mathcal{L}(n, m, B)$  such that*

(i)  $\text{Gal}(L) \subset G$  and  $\text{Soln}(L)$  is isomorphic to  $V$  over  $C$  as  $\text{Gal}(L)$ -modules.

(ii)  $\pi: G \rightarrow G/G^0$  is surjective when restricted to  $\text{Gal}(L)$ .

(iii)  $\text{Ker } X(G^0) \subset \text{Gal}(L)$

is a  $C$ -constructible subset of  $\mathcal{L}(n, m, B)$ . Therefore, if  $G^0 = \text{Ker } X(G^0)$  and  $\mathcal{W}$  is weak local data, then the set of  $L \in \mathcal{L}(n, m, \mathcal{W}, G, V)$  is a  $C$ -constructible set.

*Proof.* The first statement follows from Propositions 3.12 and 3.13. To prove the second statement, note that if  $\text{Ker } X(G^0) = G^0$ , then conditions (i), (ii), (iii) imply that  $\text{Gal}(L) = G$ .  $\mathcal{L}(n, m, \mathcal{W})$  is always  $C$ -constructible so the conclusion follows.  $\square$

We note that the condition  $\text{Ker } X(G^0) = G^0$ , is equivalent to the condition that  $R_u(G^0) = R(G^0)$ . To see this note that Lemma 2.4 implies that  $\text{Ker } X(G^0) = R_u(G) \rtimes (P, P)$  for some Levi factor  $P$  of  $G^0$ . Therefore if  $G^0 = \text{Ker } X(G^0)$  then  $G^0/R_u(G^0)$  is semisimple so  $R_u(G^0) = R(G^0)$ . Conversely, assume  $R_u(G^0) = R(G^0)$ . Any character  $\chi$  of  $G^0$  is trivial on  $R_u(G^0)$  so becomes a character on  $G^0/R_u(G^0)$ . Since  $R_u(G^0) = R(G^0)$ ,  $G^0/R_u(G^0)$  is semisimple so  $\chi$  is trivial on  $G^0/R_u(G^0)$  as well. Therefore any character of  $G^0$  is trivial, i.e.,  $G^0 = \text{Ker } X(G^0)$ . Examples of groups satisfying

$R_u(G^0) = R(G^0)$  are finite groups and groups where  $G^0$  is semisimple or unipotent.

We also note that  $\mathcal{L}(n, m, B)$  is a real semi-algebraic set when we identify  $\mathbb{C}$  with  $\mathbb{R}^2$ . Therefore the set defined by (i), (ii) and (iii) in Proposition 3.13 is a real semi-algebraic set.

Finally we note here that the last part of Theorem 3.14 is not true in general without some assumption on  $G$ . The following example (due to Deligne) shows that for  $G = \mathbb{C}^* \rtimes (\mathbb{Z}/2\mathbb{Z})$  there is a  $G$ -module  $V$ , integers  $n$  and  $m$  and local data  $\mathcal{D}$  such that  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is not constructible. This example is constructed by first constructing a differential equation on a torus (with differential Galois group  $\mathbb{C}^*$ ) and then projecting onto the Riemann Sphere.

Let  $E$  be an elliptic curve. Given any two points  $p$  and  $q$  on  $E$ , there exists a holomorphic 1-form  $\omega$  with poles only at  $p$  and  $q$  and at these points the poles are simple with residues  $-1$  and  $+1$  respectively ([FO81], Corollary 18.12, p. 152). Any two such 1-forms differ by a holomorphic 1-form, so there is a one-parameter family of such forms. If we fix  $p$  to be  $O$ , the identity element in the group structure of  $E$  and let  $q$  be a variable point, we get a two parameter family of forms  $\omega(q, t)$ .

Consider the family of differential equations

$$(3.14.1) \quad \frac{dZ}{Z} = \omega(q, t)$$

parameterized by  $q$  and  $t$ . Assume that for some fixed  $q \in E$  and  $t \in \mathbb{C}$  this has a solution  $Z = z(x)$  algebraic over  $\mathbb{C}(E)$ , the function field of  $E$ . Since  $z'/z$  will be in  $\mathbb{C}(E)$ , the Kolchin-Ostrowski Theorem [KO68] implies that  $z^N \in \mathbb{C}(E)$  for some  $N \in \mathbb{Z} - \{0\}$ . The divisor of  $z^N$  will be  $-N \cdot O + N \cdot q$ . Abel's Theorem implies that such a divisor is the divisor of a meromorphic function if and only if  $-N \cdot O + N \cdot q = O$  where  $+$  is now interpreted as addition on  $E$  ([FO81], 20.8, p. 165). Therefore, if equation (3.14.1) has a solution, algebraic over  $\mathbb{C}(E)$ , for some  $t$ , then  $q$  must be a point of finite order in  $E$ . Conversely, if  $q$  is a point of order  $N$  in  $E$ , let  $w \in \mathbb{C}(E)$  be a function whose divisor is  $-N \cdot O + N \cdot q$  and let  $z = \sqrt[N]{w}$ . One sees that  $z$  is a solution of (3.14.1) for some (unique) value of  $t$ . Therefore the set  $A$  of  $(q, t) \in E \times \mathbb{C}$  such that (3.14.1) has an algebraic solution is not a constructible set since the points of finite order on  $E$  are not constructible. If  $(q, t) \notin A$ , then a solution  $z$  of (3.14.1) is transcendental over  $\mathbb{C}(E)$ . Since such a solution satisfies  $z'/z \in \mathbb{C}(E)$ , the Galois group is  $\mathbb{C}^*$ . Furthermore note that (3.14.1)

has only regular singular points and that the exponents of (3.14.1) are  $\{\pm 1\}$  independent of  $q$  and  $t$ . We therefore have an example of a parameterized family of equations on  $E$ , with regular singular points and fixed exponents, which for almost all parameters has Galois group  $\mathbb{C}^*$  but such that the set of parameters corresponding to equations with Galois group  $\mathbb{C}^*$  is not constructible.

One can project this example down to the Riemann Sphere. If one considers  $E$  as a two sheeted cover of  $\mathbb{P}^1$  then the Galois group of  $\mathbb{C}(E)$  over  $\mathbb{C}(x)$  is  $\mathbb{Z}/2\mathbb{Z}$ . Let  $\sigma$  be a generator of this group and  $z_1 = e^{\int \omega}$  be a multivalued solution of (3.14.1). Let  $z_2 = e^{\int \sigma(\omega)}$ . We then have that  $L(Y) = \text{Wr}(Y, z_1, z_2)/\text{Wr}(z_1, z_2)$  is a parameterized family of second order linear differential equations with coefficients that are meromorphic functions on the Riemann Sphere (i.e., rational functions).  $L(Y)$  is parameterized by the projection  $\pi(q)$  and  $t$ . Its Galois group will generically be  $\mathbb{C}^* \rtimes \mathbb{Z}/2\mathbb{Z}$  and will be finite (for some value of  $t$ ) if and only if  $\pi(q)$  lies under a point of finite order. This family will have regular singular points with fixed exponents  $\mathcal{D}$  and so the set  $\mathcal{L}(2, m, \mathcal{D}, \mathbb{C}^* \rtimes \mathbb{Z}/2\mathbb{Z}, \mathbb{C}^2)$  is not  $C$ -constructible.

Note that in the above example the action of  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{C}^*$  is not trivial. We show in Theorem 3.16 that if the action of  $G/G^0$  on  $G^0/\text{Ker } X(G^0)$  is trivial, one can indeed extend Theorem 3.14 and show that for fixed  $n, m$  and local data  $\mathcal{D}$ , the set  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is  $C$ -constructible. We note that it is not enough to fix a local bound  $B$  or weak local data  $\mathcal{W}$  but rather one must fix local data  $\mathcal{D}$  to make this result true. To see this consider again the example  $L_\alpha(y) = y' - (\alpha/x)y = 0$ ,  $\alpha \in \mathbb{C}$ . For any  $B$ , the set of  $\alpha$  such that  $|\text{Re } \alpha| \leq B$  and  $\text{Gal}(L_\alpha) = \mathbb{C}^*$  is not a constructible set of the parameter space. Even if we fix the exponents, one must know the determining factors and not just a bound on their degrees. To see this consider again  $L_{\alpha_1, \alpha_2}(y) = y'' - (\alpha_1 + \alpha_2)y' + \alpha_1\alpha_2y$ ,  $\alpha_1, \alpha_2 \in \mathbb{C}$ .  $\text{Gal}(L_{\alpha_1, \alpha_2}) = \mathbb{C}^* \times \mathbb{C}^*$  if and only if  $\alpha_1$  and  $\alpha_2$  are linearly independent over  $\mathbb{Q}$  but the only singular points is infinity and there the determining factors have degree 1.

To prove Theorem 3.16 we need the following technical lemma. Let  $G$  be a linear algebraic group.  $\text{Ker } X(G^0)$  is not only a normal subgroup of  $G^0$ , but it is also normal in  $G$ . We therefore have the following exact sequence

$$1 \rightarrow G^0/\text{Ker } X(G^0) \rightarrow G/\text{Ker } X(G^0) \rightarrow G/G^0 \rightarrow 1.$$

Since  $G^0/\text{Ker } X(G^0)$  is abelian, this sequence defines an action of  $G/G^0$  on  $G^0/\text{Ker } X(G^0)$ .

LEMMA 3.15. (i) *Let*

$$1 \rightarrow K \rightarrow G \xrightarrow{\pi} Q \rightarrow 1$$

*be an exact sequence of linear algebraic groups where  $K$  is abelian and  $Q$  is finite. If the action of  $Q$  on  $K$  is trivial, then  $G = H \cdot K$  where  $H$  is a finite normal subgroup of  $G$ .*

(ii) *If  $G$  is a linear algebraic group and  $G/G^0$  acts trivially on  $G/\text{Ker } X(G^0)$  then there is a surjective map  $\phi: G \rightarrow T$  where  $T$  is a torus and  $\dim T = \dim G^0/\text{Ker } X(G)$ .*

*Proof.* (i)  $G = H \cdot G^0$  for some finite subgroup  $H$  of  $G$  ([WE73], p. 142). Since  $Q$  is finite,  $G^0 \subset K$  so  $G = H \cdot K$  as well. Since the action of  $Q$  on  $K$  is trivial,  $K$  is central so  $H$  is normal.

(ii) Write  $G/\text{Ker } X(G^0)$  as  $H \cdot K$ ,  $K = G^0/\text{Ker } X(G^0)$  and  $H$  is finite and normal. Let  $\psi: G/\text{Ker } X(G^0) \rightarrow H \cdot K/H = K/K \cap H$ . Note that  $K/K \cap H = T$  is a torus and, since  $\text{Ker } \psi$  is finite,  $\dim T = \dim G^0/\text{Ker } X(G^0)$ . Let  $\phi = \psi \circ \pi$  where  $\pi: G \rightarrow G/\text{Ker } X(G^0)$  is the canonical projection. □

**THEOREM 3.16.** *Let  $n$  and  $m$  be integers and  $\mathcal{D}$  local data defined over  $C$ . Let  $G$  be a linear algebraic group,  $G^0$  its connected component of the identity and  $V$  a faithful  $G$ -module, all defined over  $C$ . If  $G/G^0$  acts trivially on  $G/\text{Ker } X(G^0)$ , then  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is  $C$ -constructible.*

*Proof.* Let  $\psi: G \rightarrow T$  be the map defined in Lemma 3.15(ii). Let  $\dim T = k$  and let  $\chi = (\chi_1, \dots, \chi_t)$  be an isomorphism of  $T$  with  $(\mathbb{C}^*)^t$ . Note that the  $\chi_i$  are multiplicatively independent characters of  $G$ . Proposition 3.9 gives us polynomials  $P_1, \dots, P_t$  in  $\mathbb{C}(x)\{Y_1, \dots, Y_n, (\det(Y_i^{(j)}))^{-1}, C_1, \dots, C_N\}$  such that if  $\text{Gal}(L) \subset G$  and  $\{y_1, \dots, y_n\}$  is a basis for  $\text{Soln}(L)$  then there exist constants  $c_1, \dots, c_N$  such that for each  $i$ ,  $i = 1, \dots, t$ ,  $P_i(y_1, \dots, y_n, c_1, \dots, c_N)$  spans a one dimensional  $\text{Gal}(L)$  module corresponding to  $\chi_i$ . Let  $\mathcal{S}$  be the set of  $L \in \mathcal{L}(n, m, \mathcal{D})$  such that

(i)  $\text{Gal}(L) \subset G$  and  $\text{Soln}(L)$  is a  $\text{Gal}(L)$ -module isomorphic to  $V$ .

(ii)  $\text{Ker } X(G^0) \subset G$

(iii)  $\pi: G \rightarrow G/G^0$  maps  $\text{Gal}(L)$  surjectively onto  $G/G^0$ .

(iv) There exists a basis  $\{y_1, \dots, y_n\}$  of  $\text{Soln}(L)$  and constants  $c_1, \dots, c_N$  such that  $p_1 = P_1(y_1, \dots, y_n, c_1, \dots, c_N), \dots, p_t = P_t(y_1, \dots, y_n, c_1, \dots, c_N)$  are algebraically independent.

We claim that  $\mathcal{S} = \mathcal{L}(n, m, \mathcal{D}, G, V)$ . If  $L \in \mathcal{L}(n, m, \mathcal{D}, G, V)$  then  $\text{Gal}(L) = G$  so (i), (ii) and (iii) obviously hold. Furthermore, each  $p_i$  spans a one dimensional  $G$ -space corresponding to  $\chi_i$ . If the  $p_i$  are algebraically dependent, then the Kolchin-Ostrowski Theorem implies that  $p_1^{m_1} \cdots p_t^{m_t} = 1$  for some integers  $m_i$  not all zero. This in turn implies  $\chi_1^{m_1} \cdots \chi_t^{m_t} = 1$ , contradicting the multiplicative independence of the  $\chi_i$ .

Conversely, assume (i), (ii), (iii) and (iv) hold. For  $g \in \text{Gal}(L)$ ,  $g(p_i) = \chi_i(g)p_i$ . Therefore each  $p_i$  is in the fixed field  $K_0$  of  $\text{Ker } X(G^0)$  (which is a subgroup of  $\text{Gal}(L)$  by (ii)). The Galois group of  $K_0$  over  $\mathbb{C}(z)$  is  $\text{Gal}(L)/\text{Ker } X(G^0)$ . Since the  $p_i$  are algebraically independent,  $\text{tr.deg.}_{\mathbb{C}(z)} K_0 \geq t$ , so  $\dim_{\mathbb{C}}(\text{Gal}(L)/\text{Ker } X(G^0)) \geq t$ . Since  $\text{Gal}(L)^0 \subset G^0$  and  $\dim_{\mathbb{C}}(G^0/\text{Ker } X(G^0)) = t$ , we have  $\text{Gal}(L)^0 = G^0$ . By (iii) we have  $\text{Gal}(L) = G$ .

All that remains is to show that (i)–(iv) define a  $C$ -constructible set. Theorem 3.14 implies that (i)–(iii) define a constructible set. To see that in addition (iv) defines a  $C$ -constructible set first note that since (i) holds, each  $p_i$  spans a one dimensional  $\chi_i$ -space so  $p'_i/p_i \in \mathbb{C}(x)$ . Proposition 3.11 implies that there exists an  $M$  depending only on  $n, m$  and  $\mathcal{D}$  such that the  $p_i$  are algebraically dependent if and only if  $\prod_{i=1}^t p_i^{m_i} = R(x)$  for some integers  $m_i$ , not all zero, with  $|m_i| \leq M$  and rational function  $R(x)$  that is the quotient of polynomials of degrees at most  $M$ . This implies that “the  $p_i$  are algebraically dependent” is a  $C$ -constructible condition. Seidenberg’s principle implies that  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is  $C$ -constructible.  $\square$

Note that if  $G/G^0$  does not act trivially on  $G^0/\text{Ker } X(G^0)$  then we can still produce  $p_1, \dots, p_t$  in the Picard-Vessiot extension of  $\mathbb{C}(x)$  corresponding to  $L$  such that each  $p'_i/p_i$  is left fixed by  $G^0$  (but not necessarily by  $G$ ). As Deligne’s example shows, Proposition 3.11 is no longer true if  $\mathbb{C}(x)$  is replaced by an algebraic extension of  $\mathbb{C}(x)$ . Therefore, we are forced to have some hypothesis on  $G$  in Theorem 3.16 because for a non-trivial algebraic extension  $K$  of  $\mathbb{C}(x)$  the condition “ $p'_i/p_i \in K$  for  $i = 1, \dots, t$  and  $p_1, \dots, p_t$  are algebraically independent” is no longer constructible.

Theorem 3.16 implies that if  $G$  is connected then  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is a  $C$ -constructible set. Deligne’s example again

shows that this result does not extend when we consider differential equations over Riemann surfaces of genus  $\geq 1$  instead of the Riemann sphere. The reason is the same as above.

#### 4. Applications.

*a. Finite Galois groups.* In this section we show how our results combined with results of Katz and Dwork imply that if  $G$  is a finite group then the dimension of the set linear differential equations of order  $n$  with  $k$  distinct regular singular points, fixed exponents and Galois group  $G$  is a constructible set of dimension at most  $k$ . We shall show that if one furthermore fixes the singular points as well, then this set is finite. We thank B. Dwork for pointing out how the arguments of [DW90b] can be used to prove this result.

We first review some facts about differential operators in characteristic  $p$  (cf. [KA70], [HO81], [DW90]). Let  $K$  be a field of characteristic  $p$  and let  $L = D^n + a_{n-1}D^{n-1} + \cdots + a_0$  be a differential operator with coefficients in  $K(x)$ ,  $D = \frac{d}{dx}$ . We say that  $L$  has nilpotent  $p$ -curvature if  $D^{p\mu} \in K(x)[D]L$  for some positive integer  $\mu$ . One can define regular singular points and exponents as in the characteristic 0 case (using Fuchs' criteria). It is known ([KA70], [HO81]) that if  $L$  has nilpotent  $p$ -curvature then it has only regular singular points and its exponents are in  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . Fix integers  $n$  and  $k$  and consider the set  $V_N^p$  of operators having order  $n$ ,  $k+1$  regular singular points (including  $\infty$ ) and nilpotent  $p$ -curvature. Note that Fuchs' relation implies that there is a bound  $m$ , depending on  $n$  and  $k$ , such that the coefficients of  $L$  are quotients of polynomials of degrees  $\leq m$ . We denote a point in  $V_N^p$  by  $(\gamma, \nu)$  where  $\gamma$  is the vector of  $k$  finite singular points and  $\nu$  is the vector of remaining parameters. Dwork [DW90] showed that  $V_N^p$  is a constructible set and that if  $(\gamma, \nu) \in V_N^p$ , then  $\nu$  is integral over  $\mathbb{F}_p[\gamma]$ .

Finally, we need the following facts. Let  $F$  be a number field and  $L$  a differential operator with coefficients in  $F(x)$ . For almost all primes  $\mathfrak{p}$  of  $F$  we can reduce the coefficients of  $L \pmod{\mathfrak{p}}$  and get an operator  $L_{\mathfrak{p}}$  with coefficients in  $F_{\mathfrak{p}}(x)$ , where  $F_{\mathfrak{p}}$  is the residue field of  $\mathfrak{p}$ . It is known (cf. [KA70], [HO81]) that if  $L(y) = 0$  has  $n$  linearly independent solutions algebraic over  $F(x)$ , then for almost all primes  $\mathfrak{p}$ ,  $L_{\mathfrak{p}}(y) = 0$  has  $n$  linearly independent solutions in  $F_{\mathfrak{p}}(x)$  and that this implies that  $L_{\mathfrak{p}}$  has nilpotent  $p$ -curvature.

To prove our assertion, we may assume that one of the singular points is always  $\infty$ . Let  $\mathcal{S}$  be the set of linear differential equa-

tions of order  $n$  with  $k + 1$  distinct regular singular points (including  $\infty$ ), fixed exponents, and Galois group  $G$ . We will show that the dimension of  $\mathcal{F}$  is at most  $k$ . We may further assume that the representation of  $G$  is fixed, since  $G$  has only a finite number of inequivalent representations of any finite dimension. Therefore  $\mathcal{F}$  is a constructible subset of  $\mathcal{L}(m, n, S, G, V)$  for some  $m, S$  and  $V$ . As in the characteristic  $p$  case, we associate an element  $L \in \mathcal{F}$  with  $(\gamma, \nu)$  where  $\gamma$  is the vector of  $k$  finite singular points and refer to  $L$  as  $L_{\gamma, \nu}$ . Let  $(\gamma, \nu)$  be a generic point of some irreducible components of  $\mathcal{F}$ . We shall show that there is a constructible set  $V$  defined over  $\mathbb{Q}$  with  $(\gamma, \nu) \in V$  such that, for almost all primes  $p$ ,  $V_p$ , the mod  $p$  reduction of  $V$ , lies in  $V_N^p$ . Since for almost all  $p$ , the dimension of  $V_p$  is the same as the dimension of  $V$ , the result of Dwork quoted above shows that  $\nu$  is algebraic over  $\mathbb{Q}[\gamma]$ , so  $\dim \mathcal{F} \leq k$ . Furthermore, if the singular points are fixed, there can be only finitely many such  $\nu$ .

To produce the desired constructible set  $V$  we first consider the following set. For fixed  $m, n$  and  $M$ , let  $V_{n, m, M}$  be the set of elements  $(a, c)$  where  $a = (a_{ij}), c = (c_{ijl})$  such that

- (i) for  $i = 1, \dots, n, f_i = \sum_{j=0}^M \sum_{l=0}^M c_{ijl} x^j y^l$  is irreducible in  $\mathbb{C}[x, y]$ ,
- (ii)  $f_i(y) = 0$  implies that  $L_a(y) = \sum_{j=0}^n \sum_{i=0}^m a_{ij} x^i y^{(j)} = 0$ , and
- (iii) There exist  $y_1, \dots, y_n$  such that  $f_i(y_i) = 0$  and  $\text{Wr}(y_1, \dots, y_n) \neq 0$ .

$V_{n, m, M}$  is a  $\mathbb{Q}$ -constructible set. Furthermore, there exists a  $p_0$  such that for any prime  $p > p_0$  we have  $(\tilde{a}, \tilde{c}) \in (V_{n, m, M})_p$  the mod  $p$  reduction of  $V_{n, m, M}$  if and only if conditions (i), (ii) and (iii) hold over  $\mathbb{F}_p(\tilde{a}, \tilde{c})(x)$  (where  $\mathbb{C}[x, y]$  is replaced by  $K[x, y]$ ,  $K$  being the algebraic closure of  $\mathbb{F}_p(\tilde{a}, \tilde{c})$ ), that is,  $(\tilde{a}, \tilde{c}) \in (V_{n, m, M})_p$  if and only if  $L_{\tilde{a}}(y) = 0$  has  $n$  independent solutions in some algebraic extension of  $\mathbb{F}_p(\tilde{a}, \tilde{c})(x)$ . For  $(a, c) \in V_{n, m, M}$ , define  $\pi(a, c) = a$ . Let  $V = \pi(V_{n, m, M})$ . For sufficiently large  $p$ , we have  $V_p$ , the mod  $p$  reduction of  $V$ , is the same as  $\pi((V_{n, m, M})_p)$ . Therefore any point in  $V_p$  corresponds to a linear differential equation having only algebraic solutions and so, as noted above, it must have nilpotent  $p$ -curvature. Therefore  $V_p \subset V_N^p$ . Since  $(\gamma, \nu) \in V$ , we have produced the desired constructible set  $V$ .

*b. The inverse problem.* In this section we show (Theorem 4.3) that for any linear algebraic group  $G$  defined over an algebraically

closed field  $C \subset \mathbb{C}$  and a faithful  $n$ -dimensional  $G$ -module  $V$ , there exists an integer  $m$  and local data  $\mathcal{D}$  defined over  $C$  such that  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is not empty. In fact, we will select  $\mathcal{D}$  having no determining factors, so any  $L \in \mathcal{L}(n, m, \mathcal{D}, G, V)$  is of fuchsian type, that is, will have only regular singular points. When  $G$  has the property that  $G/G^0$  acts trivially on  $G^0/\text{Ker } X(G^0)$ , Theorem 3.16 implies that  $\mathcal{L}(n, m, \mathcal{D}, G, V)$  is a  $C$ -constructible set and the Hilbert Nullstellensatz implies that  $\mathcal{L}(n, m, S, G, V)$  contains a point with coefficients in  $C$ . This allows us to show that for any algebraically closed field  $C$  of characteristic zero and connected linear algebraic group defined over  $C$ , there is a Picard-Vessiot extension of  $C(x)$  having  $G$  as its Galois group (Theorem 4.4).

The proof of Theorem 4.3 follows ideas presented in [TT79]. In that paper the authors show that any linear algebraic group  $G \subset \text{GL}(n, \mathbb{C})$  is the Galois group of a Picard-Vessiot extension of  $\mathbb{C}(x)$ . To do this, they select a finitely generated Zariski dense subgroup  $G^*$  of  $G$  and use the solution of Hilbert's Twenty-First Problem [KAT79] to conclude that there is a homogeneous linear differential equation  $L(y) = 0$  of fuchsian type whose monodromy group is given by  $G^*$ . For equations of fuchsian type, the monodromy group is Zariski dense in the Galois group, so the Galois group must be  $G$  [TT79]. Since their proof relies heavily on analytic techniques, it does not immediately apply to fields of the form  $C(x)$ , where  $C$  is any algebraically closed field of characteristic zero, but the machinery developed above will allow us to transfer their result to such fields. The following two lemmas allow us to modify the argument of [TT79] to insure that the differential equation produced via the solution of Hilbert's Twenty-First Problem has exponents in a designated field  $C$ .

**LEMMA 4.1.** *Let  $G \subset \text{GL}(n, C)$  be a connected solvable linear algebraic group defined over an algebraically closed field  $C \subset \mathbb{C}$ . There exists a finite set  $X = \{g_1, \dots, g_t\} \subset G$ , such that*

- (i) *The subgroup generated by  $X$  is Zariski dense in  $G$ ,*
- (ii)  $\prod_{i=1}^t g_i = 1$ ,
- (iii) *For any  $g \in X$ , the eigenvalues of  $g$  are of the form  $e^{2\pi i \zeta}$  with  $\zeta \in C$ .*

*Proof.* Since  $G$  is connected and solvable, we may assume that the elements of  $G$  have been simultaneously triangularized and that  $G = T \cdot U$ , where  $T$  is a maximal torus and  $U$  is unipotent. All elements of  $U$  satisfy (iii). Inductively choose  $g_1, g_2, \dots \in U$  such

that the Zariski closure of the group generated by  $g_1, \dots, g_i$  has dimension  $i \leq$  dimension of  $U$ . In this way we can find  $g_1, \dots, g_s$  that generate a group that is Zariski dense in  $U$ . We next consider  $T \subset D(n, C)$ , the group of diagonal elements of  $GL(n, C)$ . Assume  $T$  has dimension  $r$ . Let  $\chi_i$  be the character on  $D(n, C)$  that picks out the  $i$ th diagonal element. There exist ([HUM81], p. 104) characters  $\varphi_j = \prod_{i=1}^n \chi_i^{n_{ij}}$ , with  $n_{ij} \in \mathbb{Z}$  and  $j = 1, \dots, r$  such that  $\Phi = (\varphi_1, \dots, \varphi_r)$  maps  $T$  isomorphically onto  $(\mathbb{C}^*)^r$ . Let  $\zeta_1, \dots, \zeta_r \in \overline{\mathbb{Q}}$  be linearly independent over  $\mathbb{Q}$ . We then have that  $a = (e^{2\pi i \zeta_1}, \dots, e^{2\pi i \zeta_r})$  generates a Zariski dense subgroup of  $(\mathbb{C}^*)^r$ , since  $\chi(a) \neq 1$  for any character on  $(\mathbb{C}^*)^r$ . Therefore,  $g_{s+1} = \Phi^{-1}(a)$  is an element of  $T$  satisfying (iii) that generates a Zariski dense subgroup of  $T$ . We have now constructed  $g_1, \dots, g_s, g_{s+1}$  satisfying (i) and (iii) for  $G$ . Since we are assuming that the elements of  $G$  are upper triangular matrices, one sees that  $h = (\prod_{i=1}^{s+1} g_i)$  also satisfies (iii). Therefore  $S = \{g_1, \dots, g_{s+1}, g_{s+2} = h^{-1}\}$  satisfies conditions (i), (ii), and (iii).  $\square$

LEMMA 4.2. *Let  $G \subset GL(n, C)$  be a linear algebraic group defined over an algebraically closed field  $C \subset \mathbb{C}$ . Then there exists a finite set  $X = \{g_1, \dots, g_t\} \subset G$ , such that*

- (i) *The subgroup generated by  $X$  is Zariski dense in  $G$ ,*
- (ii)  $\prod_{i=1}^t g_i = 1$ ,
- (iii) *For any  $g \in G$ , the eigenvalues of  $G$  are of the form  $e^{2\pi i \zeta}$  with  $\zeta \in C$ .*

*Proof.* First assume  $G$  is connected. We claim there exist two Borel subgroups  $B_1$  and  $B_2$  of  $B$  such that  $B_1 \cup B_2$  generates a Zariski dense subgroup of  $G$ . To see this let  $R(G)$  be the radical of  $G$  and let  $\pi: G \rightarrow G/R(G)$ . Let  $B$  be a Borel subgroup of  $G/R(G)$ . By ([HUM81], p. 174),  $B \cup B^-$  is Zariski dense in  $G/R(G)$ , where  $B^-$  is the opposite Borel subgroup of  $G$ .  $B_1 = \pi^{-1}(B)$  and  $B_2 = \pi^{-1}(B^-)$  satisfy the conclusion of our claim.

Lemma 4.1 now guarantees the existence of a set  $\{g_1^1, \dots, g_t^1\}$  and  $\{g_1^2, \dots, g_t^2\}$  satisfying (i), (ii), (iii) with respect to  $B_1$  and  $B_2$  respectively.  $X = \{g_1^1, \dots, g_t^1, g_1^2, \dots, g_t^2\}$  satisfies the conclusion of Lemma 4.2.

Now assume that  $G$  is not necessarily connected and let  $G^0$  be the connected component of the identity of  $G$ . We may write  $G = H \cdot G^0$  for some finite subgroup  $H$  of  $G$  ([WE73], p. 142). For any  $h \in H$ , the eigenvalues of  $h$  are of the form  $e^{2\pi i r}$  for some

$r \in \mathbb{Q}$ . Let  $\{q_1, \dots, q_t\}$  satisfy (i), (ii), (iii) with respect to  $G^0$ .  $X = \{q_1, \dots, q_t\} \cup H$  satisfies (i), (ii) and (iii) with respect to  $G$ .  $\square$

The proof of the Theorem 4.3 depends on the solution of Hilbert's Twenty-First Problem for a multiply punctured sphere, (cf., [KAT76], [TT79]). This result states that if  $z_1, \dots, z_{s+1}$  are points on the Riemann Sphere  $S^2$ , then any representation of the fundamental group  $\pi_1(S^2 - \{z_1, \dots, z_{s+1}\})$  in  $\text{GL}(n, \mathbb{C})$  can be obtained as the monodromy representation of a fuchsian differential equation with coefficients in  $\mathbb{C}(x)$  (possibly having additional apparent singular points). Note that  $\pi_1(S^2 - \{z_0, \dots, z_s\})$  is isomorphic to the free group on  $s+1$  generators  $\gamma_0, \dots, \gamma_s$  modulo the relation  $\gamma_0 \cdots \gamma_s = 1$ . Therefore a representation of  $\pi_1(S^2 - \{z_0, \dots, z_s\})$  is defined once we have specified  $s+1$  matrices  $g_0, \dots, g_s$  such that  $g_0 \cdots g_s = 1$ .

**THEOREM 4.3.** *Let  $G$  be a linear algebraic group and let  $V$  be a faithful  $n$ -dimensional  $G$ -module all defined over an algebraically closed field  $C \subset \mathbb{C}$ . There exists an integer  $m$  and a finite set  $S \subset C$  such that  $\mathcal{L}(n, m, S, G, V)$  is not empty.*

*Proof.* The action of  $G$  on  $V$  allows us to consider  $G$  as a subgroup of  $\text{GL}(n, C)$ . Let  $\{g_1, \dots, g_t\}$  be a subset of  $G$  satisfying Lemma 4.2 and let  $z_1, \dots, z_t$  be distinct points on  $S^2$ . These allow us to define a representation of  $\pi_1(S^2 - \{z_1, \dots, z_t\})$  into  $G \subset \text{GL}(n, \mathbb{C})$ . Using the solution of Hilbert's Twenty-First Problem, there is a fuchsian differential equation  $L(y) = 0$  having this as its monodromy representation. Since  $\{g_1, \dots, g_t\}$  generates a dense subgroup of  $G$ , the Galois group of  $L(y) = 0$  is  $G$  and the solution space is isomorphic to  $V$ . Let  $S$  be the set of exponents of  $L(y)$ . The singular points of  $L(y)$  are either among the  $z_i$  or are apparent singularities. At the  $z_i$  the exponents are  $(1/2\pi i)$  times the logarithms of eigenvalues of  $g_i$  and so lie in  $C$ . At the apparent singularities, the exponents are integers. Therefore  $S \subset C$ . Let  $m$  be the maximum of the degrees of the coefficients of  $L(y)$ . We then have that  $\mathcal{L}(n, m, S, G, V)$  is nonempty.  $\square$

**THEOREM 4.4.** *Let  $G$  be a linear algebraic group defined over an algebraically closed field  $C$  of characteristic zero such that  $G/G^0$  acts trivially on  $G^0/\text{Ker } X(G^0)$ . There exists a fuchsian differential equation  $L(y) = 0$  with coefficients in  $C(x)$  such that the Galois group of  $L(y)$  is  $G$ .*

*Proof.* If the cardinality of  $C$  is at most the cardinality of  $\mathbb{C}$ , we can assume that  $C \subset \mathbb{C}$ . Theorem 4.3, Theorem 3.14, Theorem 3.16 and Hilbert's Nullstellensatz imply that there is a fuchsian linear differential equation  $L(y) = 0$  with coefficients in  $C(x)$  such that the Galois group of  $L(y)$  over  $\mathbb{C}(x)$  is  $G$ . Since  $C$  is algebraically closed, the Picard-Vessiot extension  $K_0$  of  $\mathbb{C}(x)$  associated with  $L(y) = 0$  is isomorphic to  $K \otimes_C \mathbb{C}$ , where  $K$  is the Picard-Vessiot extension of  $C(x)$  associated with  $L(y) = 0$ . One then sees that the Galois group of  $K$  over  $C(x)$  is  $G$ .

If the cardinality of  $C$  is larger than the cardinality of  $\mathbb{C}$ , we can assume that  $\mathbb{C} \subset C$  and that  $G$  is defined over  $\mathbb{C}$ . The preceding paragraph shows that there is a Picard-Vessiot extension  $K_0$  of  $\mathbb{C}(x)$ , associated with a fuchsian equation  $L(y) = 0$ , such that the Galois group of  $K_0$  over  $\mathbb{C}(x)$  is  $G$ .  $K = K_0 \otimes_{\mathbb{C}} C$  is the Picard-Vessiot extension of  $C(x)$  associated with  $L(y) = 0$  and its Galois group is also  $G$ .  $\square$

As mentioned earlier, when  $C = \mathbb{C}$  this result (for arbitrary  $G$ ) appears in [TT79]. Kovacic in [KOV69] and [KOV71] deals with the general problem of when an algebraic group is the Galois group of a differential field  $k$ . One of his results is that if  $G$  is a connected solvable linear algebraic group defined over an algebraically closed field  $C$  and  $k$  is a finitely generated proper differential extension of  $C$  with constant field  $C$ , then there exists a Picard-Vessiot extension of  $k$  having Galois group  $G$ . Ramis [RA88] has shown that any semisimple connected linear algebraic group is the Galois group of a linear differential equation with coefficients in  $\mathbb{C}(x)$  with precisely one regular singular point and one irregular singular point. These results are not constructive and it should be noted that other authors have shown that certain groups occur as Galois groups of linear differential equations by explicitly calculating the Galois groups of certain classes of equations ([BH87], [BBH88], [DM89], [KAT87], [KP87], [MI89]) and by showing that certain groups can be realized by specializing generic equations ([GOL57], [MIL70]).

#### REFERENCES

- [BA81] F. Baldassari, *On algebraic solutions of Lamé's differential equations*, J. Differential Equations, **41** (1981), 44–58.
- [BA89] ———, *Towards a Schwarz list for Lamé differential operators via division points on elliptic curves*, preprint, University of Padua, 1989.
- [BE90] D. Bertrand, Personal Communication, 1990.

- [BB85] D. Bertrand and F. Beukers, *Équations Différentielles Linéaires et Majorations de Multiplicités*, Ann. Sci. École Norm. Sup., 4 série, t. 18, (1985), 181–192.
- [BH87] F. Beukers and G. Heckman, *Monodromy for the Hypergeometric Function  ${}_nF_{n-1}$* , Preprint Nr. 483, University of Utrecht, 1987.
- [BBH88] F. Beukers, D. Brownawell and G. Heckman, *Siegel normality*, Ann. Math., **127** (1988), 279–308.
- [BCR87] J. Bochnak, M. Coste and M.-F. Roy, *Geométrie Algébrique Réelle*, Ergebnisse der Mathematik, Springer-Verlag, Berlin, 1987.
- [CH89] B. Chiarellotto, *On Lamé operators which are pull-back of hypergeometric ones*, preprint, University of Padua, 1989.
- [CR62] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, New York, 1962.
- [DL89] A. Duval and M. Loday-Richaud, *A Propos de l'Algorithm de Kovacic*, preprint 89-12, Univ. de Paris-Sud, 1989.
- [DM88] A. Duval and C. Mitschi, *Matrices de Stokes et Groupe de Galois des Equations Hypergéométriques Confluentes Généralisées*, Pacific J. Math., **138**, no. 1, (1989), 25–56.
- [DW90a] B. Dwork, *On the moduli of second order differential equations on the Riemann sphere which are weak pullbacks of the hypergeometric equation*, preprint, Princeton University, 1990.
- [DW90b] —, *Differential operators with nilpotent  $p$ -curvature*, Amer. J. Math., **112** (1990), 749–786.
- [DY52] E. Dynkin, *Maximal subgroups of the classical groups*, Trudy Moskov. Mat. Obschestva, **1**, pp. 39–160; Amer. Math. Soc. Transl., Ser. 2, **6** (1957), 245–378.
- [FO81] O. Foster, *Lectures on Riemann Surfaces*. Springer-Verlag, New York, 1981.
- [GOL57] L. Goldman, *Specializations and Picard-Vessiot theory*, Trans. Amer. Math. Soc., **85** (1957), 327–356.
- [GR89] D. Yu. Grigor'ev, *Complexity of quantifier elimination in the theory of ordinary differential equations*, AAEC-6, Lecture Notes in Computer Science, vol. 357, Springer-Verlag, New York, 1989.
- [HI15] E. Hilb, *Lineare Differentialgleichungen in komplexen Gebiet*, Encyclopedie der mathematischen Wissenschaften, Vol. IIB5, Teubner, Leipzig, 1915.
- [HUM81] J. E. Humphreys, *Linear Algebraic Groups*, Second Edition, Springer-Verlag, New York, 1981.
- [HO81] T. Honda, *Algebraic differential equations*, Symp. Math., **24**, Academic Press, N.Y., (1981), 169–204.
- [KA57] I. Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris, 1957.
- [KA70] N. Katz, *Nilpotent connections and the Monodromy Theorem; applications of a result of Turittin*, Pub. Math. IHES, **39** (1970), 176–232.
- [KAT76] —, *An Overview of Deligne's Work on Hilbert's Twenty-First Problem*, Mathematical Developments Arising From Hilbert Problems, Amer. Math. Soc., Providence, RI, 1976.
- [KAT87] —, *On the calculation of some differential Galois groups*, Inv. Math., **87** (1987), 13–61.
- [KP87] N. Katz and R. Pink, *A note on pseudo-CM representations and differential Galois groups*, Duke Math. J., **54**, No. 1, (1987), 57–65.
- [KO68] E. R. Kolchin, *Algebraic groups and algebraic dependence*, Amer. J. Math., **90** (1968), 1151–1164.

- [KO73] —, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.
- [KO74] —, *Constrained extensions of differential fields*, *Adv. in Math.*, **12** (1974), 141–170.
- [KOV69] J. Kovacic, *The inverse problem in the Galois theory of differential fields*, *Ann. of Math.*, **89** (1969), 583–608.
- [KOV71] —, *On the inverse problem in the Galois theory of differential fields*, *Ann. of Math.*, **93** (1971), 269–284.
- [LEV75] A. H. M. Levelt, *Jordan decomposition for a class of singular differential operators*, *Ark. Math.*, **13** (1975), 1–27.
- [MAL79] B. Malgrange, *Sur la Réduction Formelle des Équations à Singularités Irrégulières*, Grenoble preprint, 1979.
- [MI89] C. Mitschi, *Groupes de Galois différentiels des équations hypergéométriques confluentes généralisées*, *C.R. Acad. Sci., Paris*, **309**, Serie I, (1989), 217–220.
- [MIL70] J. Miller, *On Differentially Hilbertian Differential Fields*, Ph.D. Thesis, Columbia University, 1970.
- [MO56] G. D. Mostow, *Fully reducible subgroups of algebraic groups*, *Amer. J. Math.*, **78** (1956), 200–221.
- [MUM76] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Springer-Verlag, New York, 1976.
- [POO60] E. G. C. Poole, *Introduction to the Theory of Linear Differential Equations*, Dover Publications, New York, 1960.
- [RI66] J. F. Ritt, *Differential Algebra*, Dover Publications, New York, 1966.
- [SA72] G. Sachs, *Saturated Model Theory*, W. A. Benjamin, New York, 1972.
- [SCH68] L. Schlesinger, *Handbuch der Theorie der linearen Differentialgleichungen*, Johnson Reprint Corporation, New York, 1968.
- [SEI56] A. Seidenberg, *An Elimination Theory for Differential Algebra*, *Univ. Calif. Publ. Math. (N.S.)*, **3** (1956), 31–66.
- [SI80] M. F. Singer, *Algebraic Solutions of  $n$ th Order Linear Differential Equations*, *Proceedings of the 1979 Queens University Conference on Number Theory, Queens Papers in Pure and Applied Math.*, **54** (1980), 379–420.
- [SI81] —, *Liouvillian solutions of  $n$ th order linear differential equations*, *Amer. J. Math.*, **103** (1981), 661–682.
- [SI89] —, *An Outline of Differential Galois Theory*, *Computer Algebra and Differential Equations*, E. Tournier, Ed., Academic Press, London, (1989), 3–57.
- [TT79] C. Tretkoff and M. Tretkoff, *Solution of the inverse problem of differential Galois theory in the classical case*, *Amer. J. Math.*, **101** (1979), 1327–1332.
- [WA79] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag, New York, 1979.
- [WE73] B. A. F. Wehrfritz, *Infinite Linear Groups*, *Ergebnisse der Mathematik*, Springer-Verlag, Berlin, 1973.

Received October 21, 1991. The preparation of this paper was partially supported by NSF grants DMS-88-03109 and DMS-90-24624.



# PACIFIC JOURNAL OF MATHEMATICS

Founded by

E. F. BECKENBACH (1906–1982) F. WOLF (1904–1989)

## EDITORS

S. Y. A. CHANG  
(Managing Editor)  
University of California  
Los Angeles, CA 90024-1555  
chang@math.ucla.edu

F. MICHAEL CHRIST  
University of California  
Los Angeles, CA 90024-1555  
christ@math.ucla.edu

HERBERT CLEMENS  
University of Utah  
Salt Lake City, UT 84112  
clemens@math.utah.edu

THOMAS ENRIGHT  
University of California, San Diego  
La Jolla, CA 92093  
tenright@ucsd.edu

NICHOLAS ERCOLANI  
University of Arizona  
Tucson, AZ 85721  
ercolani@math.arizona.edu

R. FINN  
Stanford University  
Stanford, CA 94305  
finn@gauss.stanford.edu

VAUGHAN F. R. JONES  
University of California  
Berkeley, CA 94720  
vfr@math.berkeley.edu

STEVEN KERCKHOFF  
Stanford University  
Stanford, CA 94305  
spk@gauss.stanford.edu

MARTIN SCHARLEMANN  
University of California  
Santa Barbara, CA 93106  
mgscharl@henri.ucsb.edu

HAROLD STARK  
University of California, San Diego  
La Jolla, CA 92093

V. S. VARADARAJAN  
University of California  
Los Angeles, CA 90024-1555  
vsv@math.ucla.edu

## SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA  
UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
UNIVERSITY OF MONTANA  
UNIVERSITY OF NEVADA, RENO  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON  
UNIVERSITY OF SOUTHERN CALIFORNIA  
STANFORD UNIVERSITY  
UNIVERSITY OF HAWAII  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON

---

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

---

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1991 *Mathematics Subject Classification* scheme which can be found in the December index volumes of *Mathematical Reviews*. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Julie Honig, University of California, Los Angeles, California 90024-1555.

There are page-charges associated with articles appearing in the *Pacific Journal of Mathematics*. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 75 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

---

The *Pacific Journal of Mathematics* (ISSN 0030-8730) is published monthly except for July and August. Regular subscription rate: \$200.00 a year (10 issues). Special rate: \$100.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to *Pacific Journal of Mathematics*, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

---

The *Pacific Journal of Mathematics* at P.O. Box 969, Carmel Valley, CA 93924 (ISSN 0030-8730) is published monthly except for July and August. Second-class postage paid at Carmel Valley, California 93924, and additional mailing offices. Postmaster: send address changes to *Pacific Journal of Mathematics*, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

This publication was typeset using  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{T}\mathcal{E}\mathcal{X}$ ,  
the American Mathematical Society's  $\mathcal{T}\mathcal{E}\mathcal{X}$  macro system.  
Copyright © 1993 by Pacific Journal of Mathematics

# PACIFIC JOURNAL OF MATHEMATICS

Volume 160    No. 2    October 1993

---

A note on Morton's conjecture concerning the lowest degree of a 2-variable knot polynomial	201
PETER RICHARD CROMWELL	
The soft torus and applications to almost commuting matrices	207
RUY EXEL	
A continuation principle for periodic solutions of forced motion equations on manifolds and applications to bifurcation theory	219
M. FURI and MARIA PATRIZIA PERA	
Positive 2-spheres in 4-manifolds of signature $(1, n)$	245
KAZUNORI KIKUCHI	
Tau functions for the Dirac operator in the Euclidean plane	259
JOHN NELSON PALMER	
Moduli of linear differential equations on the Riemann sphere with fixed Galois groups	343
MICHAEL SINGER	