Abstract

BERMAN, PETER HILLEL. Computing Galois Groups for Certain Classes of Ordinary Differential Equations. (Under the direction of Michael Singer.)

As of now, it is an open problem to find an algorithm that computes the Galois group G of an arbitrary linear ordinary differential operator $L \in \mathcal{C}(x)[D]$. We assume that $\mathcal{C}$ is a computable, characteristic-zero, algebraically closed constant field with factorization algorithm. In this dissertation, we present new methods for computing differential Galois groups in two special cases.

An article by Compoint and Singer presents a decision procedure to compute G in case L is completely reducible or, equivalently, G is reductive. Here, we present the results of an article by Berman and Singer that reduces the case of a product of two completely reducible operators to that of a single completely reducible operator; moreover, we give an optimization of that article's core decision procedure. These results rely on results from cohomology due to Daniel Bertrand.

We also give a set of criteria to compute the Galois group of a differential equation of the form $y^{(3)} + ay' + by = 0,\ a, b \in \mathcal{C}[x]$. Furthermore, we present an algorithm to carry out this computation in case $\mathcal{C} = \bar{\mathbb{Q}}$, the field of algebraic numbers. This algorithm applies the approach used in an article by M. van der Put to study order-two equations with one or two singular points. Each step of the algorithm employs a simple, implementable test based on some combination of factorization properties, properties of associated operators, and testing of associated equations for rational solutions. Examples of the algorithm and a Maple implementation written by the author are provided.

COMPUTING GALOIS GROUPS FOR CERTAIN CLASSES OF ORDINARY DIFFERENTIAL EQUATIONS

by

PETER HILLEL BERMAN

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

MATHEMATICS

Raleigh

2001

APPROVED BY:

Chair of Advisory Committee

In memory of Dan Berman

Biography

Peter Hillel Berman was born in Minneapolis, Minnesota, on August 21, 1969. He graduated from Saint Louis Park Senior High School in Saint Louis Park, Minnesota, in 1987. He received an A.B. degree in mathematics from Washington University in Saint Louis, Missouri, in 1991. He received an A.M. degree in mathematics from Brown University in Providence, Rhode Island, in 1996; his Master's thesis is titled *Dimension Polynomials: Computation and Applications*. He began work in the Department of Mathematics at North Carolina State University in August, 1996. His research interests include differential Galois theory, algebraic groups, and symbolic computation.

Acknowledgements

I would like to express my sincerest gratitude to the following people and groups:

My advisor, Michael Singer, for giving me great ideas and tools for research; for supporting me on numerous research assistantships and conference visits; and for showing enthusiasm, patience and understanding throughout the whole process.

Daniel Bertrand, for his role in developing the material that appears in Chapter 3 of this dissertation. In particular, the new algorithm that appears in Section 3.4 was inspired by a suggestion given to me by Professor Bertrand.

Marius van der Put, for inspiring and helping me with the material that appears in Chapter 4.

Mohan Putcha, for helping with the material on semisimple groups in Section 4.4.

Ron Fulp, Kailash Misra and Larry Norris, for serving on my committee.

The members of the Symbolic Solutions Group at North Carolina State University and the Kolchin Seminar in Differential Algebra at City College of New York for their encouragement and support.

My family and friends, for their love, support and patience which were essential to this project.

Contents

List of Tables

Chapter 1

Introduction

A differential field is a field k equipped with a specified derivation operator. The subfield $\mathcal{C} = \mathcal{C}_k$ of constants in k is assumed to be algebraically closed and of characteristic zero. An equation $L(y) = 0$ corresponds to an element L of the ring of differential operators $k[D]$, which is noncommutative in general. There exists a *Picard-Vessiot extension* K_L/k of differential fields, generated over k by the solution space V_L of L; it is the analogue of a splitting field extension in polynomial Galois theory. The group G_L is the group of differential field automorphisms of K_L/k. This group has a faithful representation as an algebraic subgroup of $\mathrm{GL}(V_L)$; thus, the groups in this case are linear algebraic groups. There is a full Galois correspondence in this setting. See [Mag94] for an extensive introduction to differential Galois theory. Chapter 2 of this dissertation presents basic results and notation from linear algebra, algebraic groups and differential algebra.

As of now, there does not exist an algorithm to compute the group of a differential operator L in general. There exist algorithms to compute the group in certain special cases. There also exist algorithms to perform related tasks. These related tasks include factoring operators, computing associated operators, and testing for rational solutions. See [Sin99] for an overview of these algorithms.

[CS99] presents a decision procedure to compute the group in case L is completely reducible or, equivalently, G is a reductive group. [BS99] shows how to reduce the case of a product of two completely reducible operators to that of a single completely reducible operator; this article relies on results from cohomology presented in [Ber90] and [Ber92]. Chapter 3 of this dissertation presents the results from [BS99] and an optimization of the core decision procedure.

Chapter 3 is organized as follows: Section 3.1 discusses connections and $\mathcal{D}$-modules and their relation to differential equations and systems. Section 3.2 presents the results from Section 2 of [BS99]. This section includes Algorithm I, which computes the group of the inhomogeneous equation $L(y) = b,\ L \in \mathcal{C}(x)[D]$ completely reducible, $b \in \mathcal{C}(x)$. Section 3.3 presents the results from Section 3 of [BS99]. This section includes Algorithm II, which computes the group of $L_1(L_2(y)) = 0,\ L_1, L_2 \in \mathcal{C}(x)$ completely reducible. Algorithm II works by computing an associated inhomogeneous equation $\hat{L}(y) = b$, where $\hat{L}$ is completely reducible, and applying part of Algorithm I to that equation. Section 3.4 presents Algorithm III, an optimization of Algorithm I: Whereas Algorithm I relies on parameterizing all factorizations of L to compute the group of $L(y) = b$, Algorithm III only requires a single expression of L as the least common left multiple of a set of irreducible operators. Note that Algorithm III is presented in terms of inhomogeneous first-order systems rather than inhomogeneous equations; the results of Section 3.1 show that the two settings are interchangeable in our case.

In Chapter 4, we give a set of criteria to compute the Galois group of a differential equation of the form $y^{(3)} + ay' + by = 0,\ a, b \in \mathcal{C}[x]$, where $\mathcal{C}$ is a computable, algebraically closed constant field of characteristic zero. Moreover, we present an algorithm to carry out this computation in case $\mathcal{C} = \bar{\mathbb{Q}}$, the field of algebraic numbers. This algorithm applies the approach used in [dP98b] to study order-two equations with one or two singular points.

Our method relies on a result of Ramis that says that the group of such an equation must be connected and have *defect zero* (c.f. [MS96] and [dP98a]). In Section 4.1, we state this result; we also state the main theorem of Chapter 4. In sections 4.2, 4.3 and 4.4, we enumerate the tori, unipotent groups, and semisimple groups that can be embedded in $\mathsf{SL}_3(\mathcal{C})$ along with their conjugacy classes in $\mathsf{SL}_3(\mathcal{C})$. In Section 4.5, we use the results from Sections 4.2-4.4 to produce a complete list of conjugacy classes of all subgroups of $\mathsf{SL}_3(\mathcal{C})$ that occur as Galois groups of equations of the prescribed form. In Section 4.6, we give an algorithm to compute the group of an equation of this form, in the case where $\mathcal{C} = \bar{\mathbb{Q}}$. Each step of the algorithm employs a simple, implementable test. Examples of this algorithm are given in Section 4.7. The author has implemented this algorithm in Maple. The code is provided in an appendix.

Chapter 2

Basic definitions and facts

2.1 Notation and results from linear algebra

This section is a review of certain facts from basic linear algebra (see, for instance, [HK71]), included here to establish notation for the remainder of the document.

Let V (resp., W) be an m- (resp., n-) dimensional vector space over a field k with ordered basis $\mathcal{E} = \{\mathsf{e}_1, \ldots, \mathsf{e}_m\}$ (resp., $\mathcal{F} = \{\mathsf{f}_1, \ldots, \mathsf{f}_n\}$). For any vector $\mathsf{v} = \sum_{i=1}^m v_i \mathsf{e}_i \in V$, we write

$$[\mathsf{v}]_{\mathcal{E}} = (v_1, \ldots, v_m)^T \in k^m.$$

Given $\phi \in \mathrm{Hom}_k(V, W)$, suppose

$$\phi(\mathsf{e}_i) = \sum_{j=1}^{n} a_{ji} \mathsf{f}_j,\ a_{ji} \in k.$$

Then we define the matrix $[\phi]_{\mathcal{E},\mathcal{F}}$ by

$$[\phi]_{\mathcal{E},\mathcal{F}} = (a_{ij}) \in k^{n \times m};$$

this formula yields the matrix-by-vector multiplication formula

$$[\phi(\mathsf{v})]_{\mathcal{F}} = [\phi]_{\mathcal{E},\mathcal{F}} [\mathsf{v}]_{\mathcal{E}} \quad \text{for all} \quad \mathsf{v} \in V.$$

In the special case $V = W$ (i.e., $\phi \in \mathrm{End}_k(V)$) and $\mathcal{E} = \mathcal{F}$, we write $[\phi]_{\mathcal{E}}$ in place of $[\phi]_{\mathcal{E},\mathcal{F}}$. In the special case $V = W$, $\phi = \mathrm{id}$, $\mathcal{E} \neq \mathcal{F}$, let $P = [\mathrm{id}]_{\mathcal{E},\mathcal{F}}$; we see that P is the change-of-basis matrix from coordinates in $\mathcal{E}$ to coordinates in $\mathcal{F}$.

The following facts are well-known: If X is a k-vector space with ordered basis $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \ldots, \mathsf{b}_q\}$ and $\psi \in \mathrm{Hom}_k(W, X)$, then

$$[\psi \circ \phi]_{\mathcal{E},\mathcal{B}} = [\psi]_{\mathcal{F},\mathcal{B}}[\phi]_{\mathcal{E},\mathcal{F}}.$$

If $V = W$, then $[\mathrm{id}]_{\mathcal{F},\mathcal{E}}$ and $[\mathrm{id}]_{\mathcal{E},\mathcal{F}}$ are inverses of each other and

$$[\phi]_{\mathcal{F}} = [\mathrm{id}]_{\mathcal{E},\mathcal{F}}[\phi]_{\mathcal{E}}[\mathrm{id}]_{\mathcal{F},\mathcal{E}}$$

for arbitrary ϕ.

Next, we make choices for the expression of tensor products of matrices, vector spaces, and transformations. Our choices will correspond to the ordering on

$$\{1, \ldots, m\} \times \{1, \ldots, n\} = \{ik : i \in \{1, \ldots, m\}, k \in \{1, \ldots, n\}\}$$

given by $i_1k_1 \leq i_2k_2$ if $i_1 < i_2$ or $i_1 = i_2, k_1 \leq k_2$. Under this ordering, a column vector $v \in k^{mn\times 1}$ will be written

$$v = (v_{11}, \ldots, v_{1n}, v_{21}, \ldots, v_{2n}, \ldots, v_{m1}, \ldots, v_{mn})^T.$$

Given matrices $A = (a_{ij}) \in k^{m'\times m}, B = (b_{kl}) \in k^{n'\times n}$, we define $A \otimes B = (c_{ik,jl})$, where $c_{ik,jl} = a_{ij}b_{kl}$ for $ik \in \{1, \ldots, m'\} \times \{1, \ldots, n'\}, jl \in \{1, \ldots, m\} \times \{1, \ldots, n\}$. This yields

$$\begin{aligned} A \otimes B &= (a_{ij}b_{kl}) \\ &= \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m'1}B & a_{m'2}B & \cdots & a_{m'm}B \end{bmatrix} \in k^{m'n'\times mn}. \end{aligned} \tag{2.1}$$

For the vector spaces V and W, define the ordered basis $\mathcal{E} \otimes \mathcal{F}$ of $V \otimes W$ by

$$\begin{aligned} \mathcal{E} \otimes \mathcal{F} &= \{e_1 \otimes f_1, \ldots, e_1 \otimes f_n, e_2 \otimes f_1, \ldots, e_2 \otimes f_n, \\ &\quad \ldots, e_m \otimes f_1, \ldots, e_m \otimes f_n\}. \end{aligned} \tag{2.2}$$

Suppose V' and W' are k-vector spaces with bases $\mathcal{E}' = \{e'_1, \ldots, e'_{m'}\}$, $\mathcal{F}' = \{f'_1, \ldots, f'_{n'}\}$, respectively. In the ordered bases $\mathcal{E} \otimes \mathcal{F}$ and $\mathcal{E}' \otimes \mathcal{F}'$ defined according to (2.2), if $T \in \mathrm{Hom}_k(V, V')$ has matrix $[T]_{\mathcal{E},\mathcal{E}'} = A = (a_{ij})$ and $U \in \mathrm{Hom}_k(W, W')$ has matrix $[U]_{\mathcal{F},\mathcal{F}'} = B = (b_{ij})$, then $T \otimes U \in \mathrm{Hom}_k(V \otimes W, V' \otimes W')$ has matrix $[T \otimes U]_{\mathcal{E}\otimes\mathcal{F},\mathcal{E}'\otimes\mathcal{F}'} = A \otimes B$, where $A \otimes B$ is as given in (2.1). Indeed, if $T(e_j) = \sum_i a_{ij} e'_i$ and $U(f_l) = \sum_k b_{kl} f'_k$, then

$$\begin{aligned}(T \otimes U)(e_j \otimes f_l) &= \left(\sum_i a_{ij} e'_i\right) \otimes \left(\sum_k b_{kl} f'_k\right) \\ &= \sum_{i,k} a_{ij} b_{kl} e'_i \otimes f'_k\end{aligned}$$

and therefore the coefficient of $e'_i \otimes f'_k$ in the expansion of $(T \otimes U)(e_j \otimes f_l)$ is $a_{ij} b_{kl}$, as desired.

Finally, we recall the following facts about matrices of dual transformations: Given $T : V \to W$, then the dual transformation $T^* : W^* \to V^*$ is given by $T^*(\psi) = \psi \circ T \in V^*$ for $\psi \in W^*$. Given an ordered basis $\mathcal{E}$ (resp., $\mathcal{F}$) of V (resp., W), suppose $[T]_{\mathcal{E},\mathcal{F}} = A \in k^{m \times n}$. Then we may give V^* (resp., W^*) the ordered basis $\mathcal{E}^*$ (resp., $\mathcal{F}^*$), and we have $[T^*]_{\mathcal{F}^*,\mathcal{E}^*} = A^T$. In particular, if $V = W$ and $T = \mathrm{id}$, we have $T^* = \mathrm{id}$ and

$$[\mathrm{id}]_{\mathcal{F}^*,\mathcal{E}^*} = A^T, \ [\mathrm{id}]_{\mathcal{E}^*,\mathcal{F}^*} = \left(A^T\right)^{-1}. \tag{2.3}$$

2.2 Algebraic groups

The following basic facts are taken from [Hum81]. The material on Levi decomposition is detailed in [Mos56].

We define the following notation: If G is a group and $y \in G$, then $\mathrm{Int}\, y$ is the *inner automorphism* of G defined by $(\mathrm{Int}\, y)(x) = yxy^{-1}$. If H is a normal subgroup of G, then $\mathrm{Int}\, y|_H$ is an automorphism of H. When the context is clear, we will abbreviate $\mathrm{Int}\, y|_H$ as $\mathrm{Int}\, y$.

Throughout this document, $\mathcal{C}$ is an algebraically closed field of characteristic zero. An *algebraic group* over $\mathcal{C}$ is an affine algebraic set defined over $\mathcal{C}$, equipped with group operations which are continuous in the Zariski topology. We suppress the phrase "over $\mathcal{C}$" when the field of definition is clear from context. A morphism in the category of algebraic groups is a Zariski-continuous map which is also a group homomorphism.

Examples of algebraic groups are as follows:

1. $\mathcal{C} = (\mathcal{C}, +)$, the additive group. Note that this group has no proper nontrivial algebraic subgroups.

2. An arbitrary finite-dimensional vector space (e.g., $\mathcal{C}^n$) is generated as an additive algebraic group by an arbitrary vector-space basis; such a group is called a *vector group*. The only closed subgroups of such a group are its vector subspaces.

3. $\mathcal{C}^* = (\mathcal{C} \setminus \{0\}, \cdot)$, the multiplicative group.

4. $\mathsf{GL}_n = \mathsf{GL}_n(\mathcal{C})$, the group of $n \times n$ matrices with nonzero determinant. GL_n is an open subset of affine n^2-space with coordinates $s_{ij}, 1 \leq i, j \leq n$.

5. Any closed subgroup of GL_n. Examples:

   (a) SL_n, the group of $n \times n$ matrices with determinant 1.

   (b) PSL_n, the quotient of SL_n by its center.

   (c) T_n, the group of upper-triangular nonsingular $n \times n$ matrices. We have $\mathsf{T}_n = \{(a_{ij}) \in \mathsf{GL}_n : a_{ij} = 0 \text{ if } j < i\}$.

   (d) U_n, the group of unipotent upper-triangular $n \times n$ matrices. We have $\mathsf{T}_n = \{(a_{ij}) \in \mathsf{T}_n : a_{ii} = 1 \text{ for all } i\}$.

   (e) D_n, the group of diagonal nonsingular $n \times n$ matrices.

   An arbitrary algebraic group G is called a *linear algebraic group* if it is isomorphic to a subgroup of $\mathsf{GL}_n(\mathcal{C})$ for some n.

   Given an n-dimensional $\mathcal{C}$-vector space V, let $\mathcal{E}_0 = \{\mathsf{e}_1, \mathsf{e}_2, \ldots, \mathsf{e}_n\}$ be a fixed basis of V. Then there is a one-to-one correspondence between $\mathsf{GL}(V)$ and GL_n whereby $\phi \in \mathsf{GL}(V)$ corresponds with $[\phi]_{\mathcal{E}_0} \in \mathsf{GL}_n$. This correspondence induces an algebraic group structure on $\mathsf{GL}(V)$. One checks that this structure is independent of choice of basis of V, so that $\mathsf{GL}(V)$ is given a unique structure of linear algebraic group.

   We say that a subgroup $G \subseteq \mathsf{GL}_n$ is the *expression* of the subgroup $\mathsf{G} \subseteq \mathsf{GL}(V)$ in the basis $\mathcal{F}$, and we write $G = [\mathsf{G}]_{\mathcal{F}}$, if $G = \{[\phi]_{\mathcal{F}} : \phi \in \mathsf{G}\}$. It follows from the results of the previous section that two subgroups $G, \tilde{G} \subseteq \mathsf{GL}_n$ are conjugate if and only if there exists a subgroup $\mathsf{G} \subseteq \mathsf{GL}(V)$ and a basis $\mathcal{B}$ of V such that $G = [\mathsf{G}]_{\mathcal{E}_0}, \tilde{G} = [\mathsf{G}]_{\mathcal{B}}$.

   Note that the matrix $P = [\mathrm{id}]_{\mathcal{E},\mathcal{F}}$ centralizes $G = [\mathsf{G}]_{\mathcal{E}}$ (i.e., $PMP^{-1} = M$ for all $M \in G$) if and only if $[\phi]_{\mathcal{E}} = [\phi]_{\mathcal{F}}$ for all $\phi \in \mathsf{G}$.

6. $G \rtimes H = G \rtimes_{\phi} H$, the semidirect product of G by H via ϕ, where G and H are algebraic groups and $\phi : G \times H \to G$ is the mapping corresponding to an *algebraic group action* of H on G (cf. [Hu, Sec. 8.2]) having the property that $\phi(\bullet, y)$ is an automorphism of G for all $y \in H$. As a set, we have $G \rtimes_{\phi} H = G \times H$. The structure of $G \rtimes_{\phi} H$ is given by

$$(x_1, y_1)(x_2, y_2) = (x_1 \phi(x_2, y_1), y_1 y_2)$$

for $(x_i, y_i) \in G \times H, i = 1, 2$. It is easy to see that $G \rtimes H$ includes a copy of G as a normal subgroup and a copy of H as a subgroup and, moreover, that

$$(x, 1)(1, y) = (x, y), \ (\mathrm{Int}(1, y))\,(x, 1) = (\phi(x, y), 1)$$

for all $x \in G, y \in H$.

If the algebraic group A has normal subgroup R and subgroup S with $R \cap S = \{1\}, RS = A$, then one can construct a semidirect product $R \rtimes S$ using inner automorphisms of A. If the map from $R \rtimes S$ to q given by $(r, s) \mapsto rs$ is an isomorphism of algebraic groups, then we say that $A = RS$ is the semidirect product of R by S.

Note that if ψ is an automorphism of H, then $G \rtimes_\phi H$ is isomorphic to $G \rtimes_{\tilde{\phi}} H$, where $\tilde{\phi}(x, y) = \phi(x, \psi(y))$, via the map $(x, y) \mapsto (x, \psi^{-1}(y))$.

Remark: One can show that if $G \simeq \mathcal{C} \rtimes \mathcal{C}^* = \mathcal{C} \rtimes_\phi \mathcal{C}^*$ for some ϕ, then ϕ is given by $(\mathrm{Int}\, y)(x) = \phi(x, y) = y^d x$ for some fixed integer d. One can also show that $C \rtimes_\phi \mathcal{C}^* \simeq C \rtimes_{\tilde{\phi}} \mathcal{C}^*$ if $\phi(x, y) = y^d x$ and $\tilde{\phi}(x, y) = y^{-d} x$ for all $x \in \mathcal{C}, y \in \mathcal{C}^*$.

7. The *group closure* of a subset S (resp., of an element g) of an algebraic group G is the smallest closed subgroup of G including S (resp., containing g), and we denote it $\mathrm{clos}_G(S)$ (resp., $\mathrm{clos}_G(g)$). We will omit the subscript when the context is clear.

8. The centralizer of an element g (resp., an algebraic subset S) of an algebraic group G is an algebraic subgroup of G, and we denote it $\mathrm{Cen}_G(g)$ (resp., $\mathrm{Cen}_G(S)$).

9. The normalizer of an algebraic subgroup H in an algebraic group G is an algebraic subgroup of G, and we denote it $\mathrm{Nor}_G(H)$.

Let G be an algebraic group. The *commutator* (x, y) of two elements x, y in G is the element $(x, y) = xyx^{-1}y^{-1}$. The *commutator subgroup* of G is the group generated by all $(x, y), \ x, y \in G$, and is denoted (G, G). It is a normal algebraic subgroup of G. Define the *derived series* of G to be the series of subgroups

$$G \supseteq \mathcal{D}^1 G \supseteq \mathcal{D}^2 G \supseteq \cdots,$$

where $\mathcal{D}^{i+1} G = (\mathcal{D}^i G, \mathcal{D}^i G)$ for $i \geq 0$. G is *solvable* if its derived series terminates in $\{1\}$. The Lie-Kolchin theorem states that if G is a connected solvable subgroup of $\mathsf{GL}(V)$ for some nontrivial finite-dimensional $\mathcal{C}$-vector space V, then G has a common eigenvector in V.

A corollary states that if G has these properties, then G can be embedded in $\mathsf{T}_n(\mathcal{C})$, where $n = \dim V$.

Let V be a nontrivial finite-dimensional vector space over $\mathcal{C}$. A linear transformation $\phi \in \mathrm{End}(V)$ is *nilpotent* if $\phi^d = 0$ for some $d > 0$. We say ϕ is *unipotent* if $\phi = \mathrm{id}_V + \psi$ for some nilpotent linear transformation $\psi \in \mathrm{End}(V)$. An algebraic subgroup G of $\mathsf{GL}(V)$ is *unipotent* if all of its elements are unipotent. Kolchin's Theorem, an analogue of Engel's theorem for Lie algebras (see [Hum81], Theorem 17.5), states that a unipotent subgroup of $\mathsf{GL}(V)$ has a common eigenvector having eigenvalue 1. A corollary states that such a subgroup can be embedded in $\mathsf{U}(n, \mathcal{C})$.

The *radical* (resp., *unipotent radical*) of an algebraic group G is the maximal connected solvable normal subgroup (resp., the maximal connected unipotent normal subgroup) of G. It is denoted $R(G)$ (resp., $R_u(G)$); it is an algebraic subgroup of G. We say G is *semisimple* (resp., *reductive*) if $R(G)$ (resp., $R_u(G)$) is trivial.

A linear algebraic group G admits a *Levi decomposition* $G = R_u(G)P$ (semidirect product), where P is a maximal reductive subgroup of G. P is called a *Levi subgroup* of G.

An algebraic group G is a *torus* if it is isomorphic to $\mathsf{D}_n(\mathcal{C})$ for some n. A reductive group is the product of its commutator subgroup (which is semisimple) and a torus.

A Borel subgroup of an algebraic group G is a maximal closed connected solvable subgroup. All Borel subgroups of G are conjugate to each other.

Given an algebraic group G and a vector space V, a *representation* of G on V is a morphism from G to $\mathsf{GL}(V)$.

2.3 Differential algebra

The development of the following basic facts is based on [Sin96] and [CS99].

In what follows, unless otherwise specified, all rings are commutative, contain a unit element, and have characteristic zero.

A *derivation* on a ring R is a map $D : R \to R$ such that $D(a + b) = D(a) + D(b)$ and $D(ab) = D(a)\,b + a\,D(b)$ for all $a, b \in R$. We also write a' or $\partial(a)$ for $D(a)$.

A *differential ring* is a pair (R, D), where R is a ring and D a derivation on R. A *differential field* is a differential ring (k, D) such that k is a field. When the derivation is clear from context, we will often abbreviate (R, D) (resp., (k, D)) to R (resp., k). We will often work with the differential field $(\bar{\mathbb{Q}}(x), \frac{d}{dx})$.

A *constant* in a differential field k is an element $c \in k$ such that $c' = 0$. One checks that the set $\mathcal{C} = \mathcal{C}_k \subseteq k$ of constants forms a subfield of k.

In what follows, we assume that $k = (k, D)$ is a differential field and that $\mathcal{C} = \mathcal{C}_k$ is a computable field with factorization algorithm — i.e., that we have algorithms to carry out addition, subtraction, multiplication, division and equality testing in $\mathcal{C}$ and polynomial factorization in $\mathcal{C}[x]$. We moreover assume that $\text{char}(\mathcal{C}) = 0$ and $\mathcal{C} = \bar{\mathcal{C}}$. For example, the algebraic closure of a finitely generated extension of $\mathbb{Q}$ has the above properties; see [dW53]. When appropriate, we will assume that $\mathcal{C} \subsetneq k$.

The *ring of differential operators* over k, written $\mathcal{D} = k[D]$, is the set of polynomials in the indeterminate D with coefficients in k, with a noncommutative multiplication operation $\circ$ determined by the following rule:

$$D \circ f = f \circ D + f' \text{ for all } f \in k.$$

Given $L_1, L_2 \in \mathcal{D}$, we will write either $L_1 \circ L_2$ or $L_1 L_2$ for their product. The ring $\mathcal{D}$ acts on the field k as follows: Given a typical element

$$L = a_n D^n + a_{n-1} D^{n-1} + \cdots + a_1 D + a_0 \in \mathcal{D},\ \ a_i \in k,$$

and an element $y \in k$, then

$$L(y) = a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y.$$

We see that there is a one-to-one correspondence between homogeneous linear ordinary differential equations $L(y) = 0$ over k and elements L of $\mathcal{D}$. The *order* $\text{ord}(L)$ of a differential operator L is defined to be the degree of D in L or, equivalently, the order of the corresponding equation $L(y) = 0$.

The ring $\mathcal{D}$ is a left (resp., right) Euclidean domain. In particular, there is an extended Euclidean algorithm that takes as input $U, V \in \mathcal{D}$ and computes operators $A, B \in \mathcal{D}$ with $\text{ord}\ A < \text{ord}\ V$ and $\text{ord}\ B < \text{ord}\ U$ such that $AU + BV = \text{GCRD}(U, V)$.

Let K/k be an extension of differential fields with $\mathcal{C}_K = \mathcal{C}_k$. Then we may view a homogeneous linear ordinary differential equation over k (resp., an operator $L \in \mathcal{D} = k[D]$) as an equation over K (resp., an operator in $K[D]$). Let $\text{Soln}_K(L)$ denote the set of solutions of $L(y) = 0$ in K. Then $\text{Soln}_K(L)$ is a $\mathcal{C}$-vector space.

Lemma 2.3.1 *Given $L_1, L_2 \in \mathcal{D}$, $ord(L_i) = m_i$ for $i = 1, 2$. Let K/k be a differential field extension with $\mathcal{C}_K = \mathcal{C}_k$. Then, the following statements hold:*

1. $\dim_{\mathcal{C}} \mathrm{Soln}_K(L_1) \leq m_1$.

2. *Suppose* $\dim_{\mathcal{C}} \mathrm{Soln}_K(L_1) = m_1$ *and* $\mathrm{Soln}_K(L_1) \subseteq \mathrm{Soln}_K(L_2)$. *Then* $L_2 = L_3 L_1$ *for some* $L_3 \in \mathcal{D}$.

3. *Suppose* $\dim_{\mathcal{C}} \mathrm{Soln}_K(L_2) = m_2$ *and* $L_2 = L_3 L_1$ *for some* $L_3 \in \mathcal{D}$. *Then:*

   (a) $\dim_{\mathcal{C}} \mathrm{Soln}_K(L_1) = m_1$.

   (b) $\mathrm{Soln}_K(L_1) \subseteq \mathrm{Soln}_K(L_2)$.

Proof. This is Lemma 2.1 of [Sin96].

■

Given $L \in \mathcal{D}$, a *Picard-Vessiot extension* for L is a minimal extension K_L/k of differential fields such that $\mathcal{C}_{K_L} = \mathcal{C}_k$ and $\dim_{\mathcal{C}} \mathrm{Soln}_{K_L}(L) = \mathrm{ord}(L)$. Such an extension exists and is unique up to isomorphism. If K_L/k is a Picard-Vessiot extension, then the *(full) solution set* of L in K_L is $V_L = \mathrm{Soln}_{K_L}(L)$. The *Galois group* $G = G_L = \mathrm{Gal}(K_L/k)$ of L over k is the group of differential automorphisms of K_L which fix k elementwise. An automorphism $\sigma \in G$ maps V_L to itself, and one can show that the action of σ on V_L determines σ uniquely. Thus, there is a faithful representation $G \hookrightarrow \mathsf{GL}(V_L)$ that gives G the structure of linear algebraic group. When discussing this representation, we often say that V is a G-invariant vector space, or *G-module*.

Lemma 2.3.2 *Let* K/k *be a Picard-Vessiot extension,* $G = \mathrm{Gal}(K/k)$.

1. *Let* $V \subseteq K$ *be a finite-dimensional* $\mathcal{C}$*-vector space. Then,* $V = V_L$ *for some* $L \in \mathcal{D}$ *if and only if* V *is* G*-invariant.*

2. *Suppose* $L \in \mathcal{D}$ *is a linear operator with* $V_L \subseteq K$*. Let* $W \subseteq V_L$ *be a* $\mathcal{C}$*-vector subspace. Then* $W = V_{\tilde{L}}$ *for some right factor* $\tilde{L}$ *of* L *if and only if* W *is* G*-invariant.*

Proof. This is Lemma 2.2 of [Sin96] and an easy corollary.

■

Chapter 3

Computing the group of $L_1 \circ L_2,\ L_1, L_2$ completely reducible

3.1 Connections and $\mathcal{D}$-Modules

The following is taken from Sections 2.1-2.3 of [CS99]; see also [Hae87].

A *connection over* k is a pair $(\mathcal{M}, \nabla_{\mathcal{M}})$, where $\mathcal{M}$ is a finite-dimensional k-vector space and $\nabla : \mathcal{M} \to \mathcal{M}$ satisfies the following properties for all $u, v \in \mathcal{M},\ f \in k$:

$$\begin{aligned} \nabla(u+v) &= \nabla(u) + \nabla(v) \\ \nabla(fu) &= f'u + f\nabla(u). \end{aligned}$$

We will omit the phrase "over k" when k is clear from context. We will use $\mathcal{M}$ (resp., ∇) to refer to $(\mathcal{M}, \nabla)$ (resp., $\nabla_{\mathcal{M}}$) when the context is clear. The *dimension* of $(\mathcal{M}, \nabla)$ is the dimension of $\mathcal{M}$ as a k-vector space.

If $(\mathcal{M}_1, \nabla_1)$ and $(\mathcal{M}_2, \nabla_2)$ are connections, then a morphism from $(\mathcal{M}_1, \nabla_1)$ to $(\mathcal{M}_2, \nabla_2)$ is defined to be a map $\phi \in \mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2)$ such that $\nabla_2 \circ \phi = \phi \circ \nabla_1$.

Let $\mathcal{D} = k[D]$. A connection $(\mathcal{M}, \nabla)$ can be given a $\mathcal{D}$-module structure via $D.u = \nabla(u)$ for $u \in \mathcal{M}$. Conversely, a $\mathcal{D}$-module $\mathcal{M}$ can be given a connection structure via $\nabla(u) = D.u$ for $u \in \mathcal{M}$.

One example of a connection is (k^n, ∇_A), where $n \in \mathbb{Z}_{>0},\ A \in k^{n\times n}$ and $\nabla_A(Y) = Y' - AY$ for $Y \in k^n$. Here, Y is viewed as a column vector and AY is the product of multiplication of an $n \times n$ matrix by an $n \times 1$ matrix. We have $\nabla_A(Y) = 0 \Leftrightarrow Y' = AY$, so this connection corresponds to a system of first-order linear differential equations over k. Conversely, given a first-order system of equations

$$Y' = AY,\ Y = (y_1, y_2, \dots, y_n)^T,\ A \in k^{n\times n},$$

we may consider the connection (k^n, ∇_A).

Given a differential field extension K/k with $\mathcal{C}_K = \mathcal{C}_k$, we may view $Y' = AY$ as a system over K. That is, we may consider the connection (K^n, ∇_A). The *solution space* of the system in K^n is the set of all $Y \in K^n$ such that $\nabla_A(Y) = 0$; it is a $\mathcal{C}$-vector space of dimension at most n. A *Picard-Vessiot extension* K/k for the system is a minimal extension containing the full n-dimensional set of solutions of the system. $G = \mathrm{Gal}(K/k)$ acts on K^n by

$$\sigma.\zeta = (\sigma(\zeta_1), \sigma(\zeta_2), \dots, \sigma(\zeta_m)) \tag{3.1}$$

for all $\sigma \in G, \zeta = (\zeta_1, \zeta_2, \dots, \zeta_m) \in K^m$.

Given a connection $(\mathcal{M}, \nabla)$, let $\mathcal{E} = \{e_1, \dots, e_n\}$ be an ordered k-basis of $\mathcal{M}$. For $1 \leq i, j \leq n$, define a_{ij} by

$$\nabla(e_i) = -\sum_{j=1}^{n} a_{ji} e_j.$$

It follows that if $u = \sum_i u_i e_i \in \mathcal{M},\ u_i \in k$, then $\nabla(u) = \sum_i (u_i' - \sum_j a_{ij} u_j) e_i$. We call the matrix $[\nabla]_{\mathcal{E}} = (a_{ij}) \in k^{n\times n}$ the matrix of $(\mathcal{M}, \nabla)$ with respect to $\mathcal{E}$. Observe that if $A = [\nabla]_{\mathcal{E}}$, then $u \mapsto [u_1 u_2 \cdots u_n]^T$ defines an isomorphism from $(\mathcal{M}, \nabla)$ onto (k^n, ∇_A). If $\mathcal{N} \subseteq M$ is a k-subspace such that $\nabla(\mathcal{N}) \subseteq \mathcal{N}$, then $(\mathcal{N}, \nabla\big|_{\mathcal{N}})$ is a connection; moreover, one checks that $(M/\mathcal{N}, \nabla_{M/\mathcal{N}})$ is a connection, where $\nabla_{M/\mathcal{N}}(m + \mathcal{N}) = \nabla(m) + \mathcal{N}$.

In the following observations and definitions, $(\mathcal{M}_1, \nabla_1)$ and $(\mathcal{M}_2, \nabla_2)$ are two connections; $\mathcal{E} = \{e_1, \dots, e_m\}$ (resp., $\mathcal{F} = \{f_1, \dots, f_n\}$) is a basis of $\mathcal{M}_1$ (resp., $\mathcal{M}_2$); $A = (a_{ij}) = [\nabla_1]_{\mathcal{E}}$ and $B = [\nabla_2]_{\mathcal{F}}$.

$(\mathcal{M}_1 \oplus \mathcal{M}_2, \nabla_1 \oplus \nabla_2)$ is a connection.

$(\mathcal{M}_1 \otimes \mathcal{M}_2, \nabla_1 \otimes \mathrm{id}_{\mathcal{M}_2} + \mathrm{id}_{\mathcal{M}_1} \otimes \nabla_2)$ is a connection. It can be shown that $\nabla_{\mathcal{M}_1 \otimes \mathcal{M}_2}$ has matrix

$$[\nabla_{\mathcal{M}_1 \otimes \mathcal{M}_2}]_{\mathcal{E} \otimes \mathcal{F}} \quad = \quad A \otimes I_n + I_m \otimes B$$

$$
= \begin{bmatrix} a_{11}I_n & a_{12}I_n & \cdots & a_{1m}I_n \\ a_{21}I_n & a_{22}I_n & \cdots & a_{2m}I_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}I_n & a_{m2}I_n & \cdots & a_{mm}I_n \end{bmatrix}
+ \begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{bmatrix}. \tag{3.2}
$$

$(\mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2), \nabla_{\mathrm{Hom}})$, where

$$
\nabla_{\mathrm{Hom}}(\phi) = \nabla_2 \circ \phi - \phi \circ \nabla_1,
$$

is a connection. Suppose $\phi \in \mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2)$ is such that $[\phi]_{\mathcal{E},\mathcal{F}} = U$. Then a calculation shows that

$$
[\nabla_{\mathrm{Hom}}(\phi)]_{\mathcal{E},\mathcal{F}} = U' - BU + UA. \tag{3.3}
$$

$(\mathcal{M}_1^*, \nabla^*)$ is a connection, where $\mathcal{M}_1^* = \mathrm{Hom}_k(\mathcal{M}_1, k)$ is the vector space dual of $\mathcal{M}_1$ and $\nabla^*(\phi) = {}' \circ \phi - \phi \circ \nabla_1$. Observe that this definition coincides with the definition of ∇_{Hom} in the case $(\mathcal{M}_2, \nabla_2) = (k, f \mapsto f')$. One checks that $[\nabla^*]_{\mathcal{E}^*} = -A^T$.

There is a natural isomorphism $\Psi : \mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2) \to \mathcal{M}_1^* \otimes \mathcal{M}_2$. Given a homomorphism $\phi \in \mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2)$ with $[\phi]_{\mathcal{E},\mathcal{F}} = U = (u_{ij})$, then $\Psi(\phi) = \sum_{i,j} u_{ji} e_i^* \otimes f_j$. In the ordered basis given by (2.2), we have

$$
\begin{aligned}
[\Psi(\phi)]_{\mathcal{E}^* \otimes \mathcal{F}} &= (u_{11}, u_{21}, \ldots, u_{n1}, u_{12}, u_{22}, \ldots, u_{n2}, \\
&\quad \ldots, u_{1m}, u_{2m}, \ldots, u_{nm})^T \\
&= (U_1^T, U_2^T, \ldots, U_n^T)^T,
\end{aligned} \tag{3.4}
$$

where U_i is the ith column vector of U.

We apply the preceding observations to obtain the following matrix for $\mathcal{M}_1^* \otimes \mathcal{M}_2$:

$$
\begin{aligned}
[\nabla_{\mathcal{M}_1^* \otimes \mathcal{M}_2}]_{\mathcal{E}^* \otimes \mathcal{F}} &= -A^T \otimes I_n + I_m \otimes B \\
&= - \begin{bmatrix} a_{11}I_n & a_{21}I_n & \cdots & a_{m1}I_n \\ a_{12}I_n & a_{22}I_n & \cdots & a_{m2}I_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m}I_n & a_{2m}I_n & \cdots & a_{mm}I_n \end{bmatrix}
\end{aligned}
$$

$$
+\begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{bmatrix}. \tag{3.5}
$$

One checks that a linear transformation $\phi \in \mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2)$ is a morphism of connections if and only if $\nabla_{\mathrm{Hom}}(\phi) = 0$.

Suppose $\phi : \mathcal{M}_1 \to \mathcal{M}_2$ is a vector space isomorphism. Let $\mathcal{E}_1$ (resp., $\mathcal{E}_2$) be a basis of $\mathcal{M}_1$ (resp., $\mathcal{M}_2$). Then one checks that ϕ is an isomorphism of connections if and only if

$$
A_2 = P'P^{-1} + PA_1P^{-1}, \tag{3.6}
$$

where $P = [\phi]_{\mathcal{E}_1,\mathcal{E}_2}$ and $A_i = [\nabla_i]_{\mathcal{E}_i}$ for $i = 1, 2$.

Given an equation $L(y) = 0$, where

$$
L = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 \in \mathcal{D}, \tag{3.7}
$$

we associate the the $\mathcal{D}$-module $\mathcal{M} = (\mathcal{D}/\mathcal{D}L)^*$ and define ∇_L to be the induced connection operator. Let $\mathcal{E} = \left\{1, D, D^2, \ldots, D^{n-1}\right\}$ be a basis of $\mathcal{D}/\mathcal{D}L$, where $n = \mathrm{ord}(L)$. Then one checks that $[\nabla_L]_{\mathcal{E}^*} = A_L$, where

$$
A_L = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{bmatrix}. \tag{3.8}
$$

We see that $((\mathcal{D}/\mathcal{D}L)^*, \nabla_L) \simeq (k^n, A_L)$. So, L corresponds to a first-order system $Y' = A_L Y$. Note that this is the system obtained from $L(y) = 0$ by $Y = (y_1, y_2, \ldots, y_n)^T$, where $y_1 = y$ and $y_i = y'_{i-1}$ for $2 \leq i \leq n$. We call A_L the companion matrix of L.

Given a connection $(\mathcal{M}, \nabla)$, it is a fact ([Kat87]) that if $\mathcal{C}_k \subsetneq k$, then $\mathcal{M}$ contains a *cyclic vector*, i.e., an element $u \in \mathcal{M}$ such that the set

$$
\mathcal{E} = \left\{u, \nabla(u), \nabla^2(u), \ldots, \nabla^{n-1}(u)\right\}
$$

is a basis of $\mathcal{M}$, where $n = \dim(M)$. Applying this fact to $(\mathcal{M}^*, \nabla^*)$, let u^* be an element and

$$
\mathcal{F} = \left\{u^*, \nabla(u^*), \nabla^2(u^*), \ldots, \nabla^{n-1}(u^*)\right\}
$$

a basis of $\mathcal{M}^*$. Then, one checks that

$$[\nabla^*]_{\mathcal{F}} = \begin{bmatrix} 0 & 0 & 0 & \cdots & a_0 \\ -1 & 0 & 0 & \cdots & a_1 \\ 0 & -1 & 0 & \cdots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1} \end{bmatrix}$$

for some $a_0, \ldots, a_{n-1} \in k$. Let $B = [\nabla^*]_{\mathcal{F}}$. It follows that $(\mathcal{M}^{**}, \nabla^{**}) \simeq (\mathcal{M}, \nabla)$ has matrix $[\nabla]_{\mathcal{F}^*} = -B^T = A_L$, where L is given by (3.7); that is, $[\nabla]_{\mathcal{F}^*}$ is the companion matrix of L. We note that there are algorithms to find a cyclic vector for a given system; one of these is given in [Kat87].

Given a homogeneous equation $L(y) = 0,\ L \in \mathcal{D}$, and a system $Y' = AY, A \in k^{n\times n}$, we say that $L(y) = 0$ and $Y' = AY$ are equivalent to each other over k if $(\mathcal{D}/\mathcal{D}L)^*$ and (k^n, ∇_A) are isomorphic connections. Evidently $L(y) = 0$ and $Y' = A_L Y$ are equivalent to each other. If $L(y) = 0$ and $Y' = AY$ are equivalent to each other, then the extension K/k is a Picard-Vessiot extension for $L(y) = 0$ if and only if it is a Picard-Vessiot extension for $Y' = AY$.

We say two operators $L_1, L_2 \in \mathcal{D}$ are equivalent over k if the $\mathcal{D}$-modules $\mathcal{D}/\mathcal{D}L_1$ and $\mathcal{D}/\mathcal{D}L_2$ are isomorphic.

Proposition 3.1.1 *Given $L \in \mathcal{D}$ with $\operatorname{ord}(L) > 0$. Then, there exist $r \in k, L_1, L_2, \ldots, L_m \in \mathcal{D}$, L_i monic and irreducible for $1 \le i \le m$, such that $L = rL_1L_2\cdots L_m$. If $L = \tilde{r}\tilde{L}_1\tilde{L}_2\cdots\tilde{L}_{\tilde{m}}$ is another such factorization, then $r = \tilde{r},\ m = \tilde{m}$, and there exists a permutation $\sigma \in S_m$ such that L_i is equivalent over k to $\tilde{L}_{\sigma(i)}$ for all $i,\ 1 \le i \le m$.*

Proof. This is Proposition 2.11 of [Sin96].

■

We say that the first-order systems $Y' = A_1Y$ and $Y' = A_2Y$ are *equivalent* over k if they have the same order n and the connections (k^n, ∇_{A_1}) and (k^n, ∇_{A_2}) are isomorphic.

Proposition 3.1.2 *Given $L_1, L_2 \in \mathcal{D},\ A_1, A_2 \in k^{n\times n}$. Suppose the equation $L_i(y) = 0$ is equivalent to the system $Y' = A_iY$ for $i = 1, 2$. Let K_i/k (resp., V_i) be the Picard-Vessiot extension (resp., the full solution space) of $L_i(y) = 0$ for $i = 1, 2$. Then, the following are equivalent:*

1. *L_1 and L_2 are equivalent operators.*

2. *There exist operators $R, S \in \mathcal{D}$ of orders less than n such that*

$$\mathrm{GCRD}(R, L_1) = 1, \; L_2 R = S L_1. \tag{3.9}$$

3. *If K/k is a Picard-Vessiot extension containing K_{L_1} and K_{L_2}, then $V_1 \simeq V_2$ as G-modules, where $G = \mathrm{Gal}(K/k)$.*

4. *$Y' = A_1 Y$ and $Y' = A_2 Y$ are equivalent systems.*

5. *There exists a matrix $P \in \mathsf{GL}_n(k)$ such that (3.6) holds.*

Proof. Equivalence of the first three statements is proved in Corollary 2.6 of [Sin96]. Observe that if (3.9) holds, then the map $1 \mapsto R$ yields an isomorphism from $\mathcal{D}/\mathcal{D}L_2$ to $\mathcal{D}/\mathcal{D}L_1$. Equivalence of the first and fourth statements follows from definitions. Equivalence of the fourth and fifth statements follows from the discussion given immediately before and after (3.6).

∎

We define *reducibility* over k in various settings as follows: An operator $L \in \mathcal{D}$ is reducible over k if there exist operators L_1, L_2 of lower order such that $L = L_1 L_2$. A system $Y' = AY$ is reducible over k if it is equivalent over k to a system of the form

$$Y' = \begin{bmatrix} B_1 & 0 \\ B_2 & B_3 \end{bmatrix} Y.$$

A module is reducible if it has a nontrivial proper submodule. A connection $(\mathcal{M}, \nabla)$ is reducible if it includes a proper nontrivial subconnection, i.e., a vector subspace $\mathcal{N} \subseteq \mathcal{M}$ that is closed under ∇. In each setting, we suppress the phrase "over k" when k is clear from context.

Proposition 3.1.3 *Let $Y' = AY$ be a first-order system over k. Let K/k be a Picard-Vessiot extension for this system and $G = \mathrm{Gal}(K/k)$. Let $L \in \mathcal{D}$ be an operator that is equivalent to this system. Then, the following are equivalent:*

1. *The connection (k^n, ∇_A) contains a proper nonzero subconnection.*

2. *The $\mathcal{D}$-module k^n, where $\mathcal{D}Y = \nabla_A(Y)$, is reducible.*

3. *The $\mathcal{D}$-module $\mathcal{D}/\mathcal{D}L$ is reducible.*

4. *L is reducible over k.*

5. *$Y' = AY$ is reducible over k.*

6. *The solution space of $Y' = AY$ in K is a reducible G-module.*

Proof. This is Proposition 2.1 of [CS99]. ■

We define *complete reducibility* over k in various settings as follows: An operator $L \in \mathcal{D}$ is completely reducible over k if is the least common left multiple of irreducible operators. A system $Y' = AY$ is completely reducible over k if it is equivalent over k to a system of the form

$$Y' = \text{diag}(B_1, B_2, \ldots, B_t)Y,$$

where the system $Z' = B_iZ$ is irreducible for $1 \leq i \leq t$. A module is completely reducible if it is the direct sum of irreducible submodules. In each setting, we suppress the phrase "over k" when k is clear from context.

Proposition 3.1.4 *Let $Y' = AY$ be a first-order system over k. Let K/k be a Picard-Vessiot extension for this system and $G = \text{Gal}(K/k)$. Let $L \in \mathcal{D}$ be an operator that is equivalent to this system. Then, the following are equivalent:*

1. *The connection (k^n, ∇_A) is completely reducible.*

2. *The $\mathcal{D}$-module k^n, where $\mathcal{D}Y = \nabla_A(Y)$, is completely reducible.*

3. *The $\mathcal{D}$-module $\mathcal{D}/\mathcal{D}L$ is completely reducible.*

4. *L is completely reducible over k.*

5. *$Y' = AY$ is completely reducible over k.*

6. *The solution space of $Y' = AY$ in K is a completely reducible G-module.*

7. *G is a reductive group.*

Proof. This is Proposition 2.2 of [CS99]. ■

3.2 Computing the group of $L(y) = b,\ L$ completely reducible

Consider the inhomogeneous equation $L(y) = b,\ b \in k$. Let $\hat{L} = (D - b'/b) \circ L$. Define the Picard-Vessiot extension K_{I} (resp., the Galois group G_{I}) of $L(y) = b$ to be $K_{\hat{L}}$ (resp., $G_{\hat{L}}$). Note that L is a right factor of $\hat{L}$, so that $V_{\hat{L}} \subseteq K_{\mathrm{I}}$ includes a full solution set of $L(y) = 0$. Thus, we may write $K_{\mathrm{H}} \subseteq K_{\mathrm{I}}$ and $V_L \subseteq V_{\hat{L}}$. Moreover, if $f \in V_{\hat{L}} \setminus V_L$, then there exists a nonzero constant c such that $f_0 = cf$ and $L(f_0) = b$. Since any two solutions of $L(y) = b$ differ by an element of V_L, we see that the full solution set of $L(y) = b$ is $f_0 + V_L$. Moreover, if $\mathcal{E}$ is a basis of V_L, then $\mathcal{E} \cup \{f\}$ is a basis of $V_{\hat{L}}$. It follows that K_{I}/k is the minimal differential field extension containing the full solution set of $L(y) = b$.

Proposition 3.2.1 *Given:*

1. *k a differential field, $\mathcal{C}_k$ algebraically closed of characteristic zero*
2. *$L \in \mathcal{D} = k[D]$ a completely reducible operator*
3. *$b \in k$*
4. *K_{I}/k (resp., $V_{\mathrm{I}},\ G_{\mathrm{I}}$) is the Picard-Vessiot extension (resp., full solution space, group) of $L(y) = b$*
5. *K_{H}/k (resp., $V_{\mathrm{H}},\ G_{\mathrm{H}}$) is the Picard-Vessiot extension (resp., full solution space, group) of $L(y) = 0$*
6. *$L_1, L_0 \in \mathcal{D}$ are monic operators satisfying the following conditions:*
   (a) *$L_1(y) = b$ has a k-rational solution.*
   (b) *$L = L_1 L_0$ for some $L_0 \in \mathcal{D}$.*
   (c) *L_1 is of maximal order.*

Then G_{I} has Levi decomposition $G_{\mathrm{I}} \simeq W \rtimes G_{\mathrm{H}}$, where $W \simeq V_{L_0}$ as vector groups. In addition, the pair (L_1, L_0) given in Item 6 above is unique.

Proof. This is Proposition 2.1 of [BS99]; it is an adaptation of Théorème 1 of [Ber92]. We reproduce it here, with some changes of notation.

First, let $L_1 = 1,\ L_0 = L$. We see that Properties 6(ab) are satisfied, so that there exists a pair (L_1, L_0) satisfying those properties with L_1 of maximal order.

Next, note that if $L = L_1 L_0$, then $K_{\rm I}$ includes the full solution set V_{L_1} (resp., V_{L_0}) of $L_1(y) = 0$ (resp., $L_0(y) = 0$).

Let $f \in K$ be a particular solution of $L(y) = b$. Let $\sigma \in G_{\rm I}$. Then $\sigma(f) - f \in V_{\rm H}$. Thus, we may define $\Phi : G_{\rm I} \to V_L$ by $\Phi(\sigma) = \sigma(f) - f$. Let $H = \mathrm{Gal}(K_{\rm I}/K_{\rm H})$. Then H is normal in $G_{\rm I}$. Since $K_{\rm I}/K_{\rm H}$ is generated by f, we see that Φ is injective on H.

For any $\sigma \in G_{\rm I}, \tau \in H$, we have

$$\begin{aligned}
\Phi(\sigma\tau\sigma^{-1}) &= \sigma\tau\sigma^{-1}(f) - f \\
&= \sigma[\tau(\sigma^{-1}(f) - f) + \tau(f)] - f \\
&= \sigma[\sigma^{-1}(f) - f] + \sigma\tau(f) - f \text{ since } \tau \text{ fixes } V_L \subseteq K_L \text{ elementwise} \\
&= \sigma[\tau(f) - f] \\
&= \sigma\Phi(\tau).
\end{aligned}$$

This calculation (from the proof of Théorèm 1 of [Ber92]) implies that Φ is a $G_{\rm I}$-module morphism, where $G_{\rm I}$ acts on H by conjugation. Therefore, $\Phi(H)$ is a $G_{\rm I}$-invariant subspace $W \subseteq V_{\rm H}$. Since $G_{\rm I}/H$ is isomorphic to the reductive group $G_{\rm H}$ and H is unipotent, it follows that $G_{\rm I}$ has Levi decomposition $G_{\rm I} = HP$ (semidirect product of subgroups), where $H = R_u(G_{\rm I})$ and $P \simeq G_{\rm H}$.

Let $\tilde{L}_0 \in \mathcal{D}$ be the unique monic operator such that $V_{\tilde{L}_0} = W$ and let $\tilde{L}_1 \in \mathcal{D}$ be such that $L = \tilde{L}_1\tilde{L}_0$. Since $\tau(f) - f \in W$ for all $\tau \in H$, we have that $\tilde{L}_0(\tau(f)) = \tilde{L}_0(f)$ for all $\tau \in H$; it follows that $\tilde{L}_0(f) \in K_{\rm H}$. Let $W_1 = V_{\tilde{L}_1} \subseteq K_{\rm H}$ and let $W_{\tilde{L}_0(f)} = W_1 + \mathcal{C}\tilde{L}_0(f) \subseteq K_{\rm H}$. Given $\sigma \in G_{\rm H}$, we have that $\sigma(\tilde{L}_0(f))$ is another particular solution of that $\tilde{L}_1(y) = b$, so that $\sigma(\tilde{L}_0(f)) = \tilde{L}_0(f) + w$ for some $w \in W_1$. It follows that $W_{\tilde{L}_0(f)}$ is $G_{\rm H}$-invariant and, moreover, that $W_{\tilde{L}_0(f)}/W_1$ is a trivial one-dimensional $G_{\rm H}$-module. Since $G_{\rm H}$ is a reductive group, we see that W_1 has a $G_{\rm H}$-invariant complement in $W_{\tilde{L}_0(f)}$. This implies that there exists $f_0 \in K_{\rm H}$ such that $f_0 = \tilde{L}_0(f) + \tilde{w}$ for some $\tilde{w} \in W_1$ and $\sigma(f_0) = f_0$ for all $\sigma \in G_{\rm H}$. From these properties, we conclude that $f_0 \in k$ and $\tilde{L}_1(f_0) = b$.

Now let $L_0, L_1 \in \mathcal{D}$ satisfy Properties 6(abc). Let $\bar{W}_1 = V_{L_1} \subseteq K_{\rm H}$. Since $L_1(L_0(f)) = b$, we have $L_0(f) = f_1 + \bar{w}$ for some $\bar{w} \in \bar{W}_1$. It follows that $L_0(f) \in K_{\rm H}$. Thus, given $\tau \in H$, we have

$$\begin{aligned}
L_0(\Phi(\tau)) &= L_0(\tau(f) - f) = \tau(L_0(f) - f) = \tau(f - f) \\
&= 0.
\end{aligned}$$

This yields $\phi(H) = V_{\tilde{L}_0} \subseteq V_{L_0}$. This implies that $\tilde{L}_0$ divides L_0 on the right. We then see that $\mathrm{ord}(L_1) \leq \mathrm{ord}(\tilde{L}_1)$. In case $\mathrm{ord}(L_1) = \mathrm{ord}(\tilde{L}_1)$ and L_1 is monic, then $\tilde{L}_0 = L_0$ and therefore $L_1 = \tilde{L}_1$.

■

The following examples appeared in [BS99] and were computed by the first author.

Example 3.2.2 Let $k = \mathcal{C}(x)$ and $L = D^2 - 4xD + (4x^2 - 2) = (D - 2x) \circ (D - 2x)$. A basis for the solution space of the equation $L(y) = 0$ is $\{e^{x^2}, xe^{x^2}\}$, so that $G_{\mathrm{H}} \simeq \mathcal{C}^*$.

For any $(c, d) \in \mathcal{C}^2,\ (c, d) \neq (0, 0)$, we have that $(c + dx)e^{x^2}$ is a solution of $L(y) = 0$, so that L has a right factor of the form $D - (2x + \frac{d}{c+dx})$. Furthermore, all right factors of order one are of this form. Therefore the formula

$$L = (D - (2x - \frac{d}{c + dx})) \circ (D - (2x + \frac{d}{c + dx}))$$

with $(c, d) \neq (0, 0)$ yields a parameterization of all irreducible factorizations of L.

We shall now compute the Galois groups of $L(y) = b$ where $b = 4x^2 - 2, 1$ and $\frac{1}{x}$.

(i) $b = 4x^2 - 2$. In this case the equation $L(y) = b$ has the rational solution $y = 1$. This implies that $L_0 = 1$, where L_0 is as defined in Proposition 3.2.1. Thus, V_{L_0} is trivial, and we conclude that the Galois group of $L(y) = b$ is $\mathcal{C}^*$.

(ii) $b = 1$. A partial fraction computation shows that $L(y) = 1$ has no rational solutions. Now let us search for first order left factors L_1 of L such that $L_1 = 1$ has a rational solution. A calculation shows that the equation

$$y' - (2x - \frac{d}{c + dx})y = 1 \tag{3.10}$$

has a rational solution $y = f$ if and only if $z = (c + dx)f$ is a rational solution of

$$z' - 2xz = c + dx \tag{3.11}$$

(c.f., Lemma 3.2.4). The rational solutions of (3.11) must be polynomials, and we see that this has a polynomial solution if and only if $c = 0$. Therefore the operator L_0 as defined in Proposition 3.2.1 is equal to $D - (2x + \frac{1}{x})$; its solution space is spanned by $V_{L_0} = xe^{x^2}$. Therefore the Galois group of $L(y) = 1$ is $\mathcal{C} \rtimes \mathcal{C}^*$, where $t.u = tu$ for $t \in \mathcal{C}^*, u \in \mathcal{C}$.

(iii) $b = \frac{1}{x}$. We shall show that for any $(c, d) \neq (0, 0)$, the equation

$$y' - (2x - \frac{d}{c + dx})y = \frac{1}{x} \tag{3.12}$$

has no rational solution. This implies that $L(y) = \frac{1}{x}$ also has no rational solution and so the W of Proposition 3.2.1 is the full solution space of $L(y) = 0$. Therefore the Galois group of $L(y) = \frac{1}{x}$ is $\mathcal{C}^2 \rtimes \mathcal{C}^*$, where $t.(u, v) = (tu, tv)$ for $t = in\mathcal{C}^*, (u, v) \in \mathcal{C}^2$. Equation (3.12) has a rational solution $y = f$ if and only if $z = (c + dx)f$ is a rational solution of

$$z' - 2xz = \frac{c + dx}{x}. \tag{3.13}$$

If $c \neq 0$ then any rational solution of (3.13) must have a pole at $x = 0$. Comparing orders of the left and right hand side of this equation yields a contradiction. Therefore $c = 0$. Similar considerations show that $z' - 2xz = d$ can never have a rational solution if $d \neq 0$.

■

Proposition 3.2.1 lets us describe K_{I} as follows.

Corollary 3.2.3 *Given $k, L, b, K_{\mathrm{I}}, K_{\mathrm{H}}, L_1, L_0$ as in Proposition 3.2.1. Write*

$$L_0 = D^t - b_{t-1}D^{t-1} - \ldots - b_o,\ \ b_i \in k.$$

Then $K_{\mathrm{I}} = K_{\mathrm{H}}(z_0, z_1, \ldots, z_{t-1})$, where $z_0, z_1, \ldots, z_{t-1}$ are algebraic indeterminates, $z_i' = z_{i+1}$ for $0 \leq i \leq t-2$, and $z_{t-1}' = f_1 + \sum_{i=0}^{t-1} b_i z_i$.

Proof. Let $\hat{L} = (D - b'/b)L$. Then K_{I}/k is a Picard-Vessiot extension for $\hat{L}(y) = 0$, with full solution space $V_{\hat{L}}$. We see that L_0, viewed as a linear operator on K_{I}, maps $V_{\hat{L}}$ onto the full solution space of $\hat{L}_1(y) = 0$, where $\hat{L}_1 = (D - b'/b)L_1$. Therefore, there exists an element $z \in V_{\hat{L}}$ with $L_0(z) = f_1$. We see that $L(z) = b$ and therefore that $K = K_L < z >$. Since $\mathrm{Gal}(K_{\mathrm{I}}/K_{\mathrm{H}})$ is a vector group of dimension t, we have that K is a purely transcendental extension of K_L of transcendence degree t. It follows that $K = K_L(z, z', \ldots, z^{(t-1)})$. The desired result follows easily after setting $z_i = z^{(i)}$. satisfy the conclusion of the Corollary.

■

To compute G_{I} for a given inhomogeneous equation $L(y) = b$ using Proposition 3.2.1, it suffices to perform the following tasks:

1. Compute G_{H}.

2. Find L_1, L_0 satisfying the conditions given in Proposition 3.2.1.

The first of these two tasks is addressed in [CS99] and lies outside the scope of this dissertation. The second task is dealt with in [BS99], and below we summarize the relevant results from that article.

Let $L \in \mathcal{D}$ be completely reducible. Then, by definition, there exist operators $T_1, \ldots, T_s$ such that $L = \mathrm{LCLM}(T_1, \ldots, T_s)$. Proposition 3.1.1 then implies that any left or right factor of L will be equivalent to the least common left multiple of some subset of $\{T_1, \ldots, T_s\}$.

Suppose k is a finite algebraic extension of $\mathcal{C}(x)$, where $\mathcal{C}$ is a computable algebraically closed field of characteristic zero, then (cf. [CS99] and [Sin96]) one can effectively perform the following tasks:

1. Factor an arbitrary element $L \in \mathcal{D} = k[D]$ as a product of irreducible operators.

2. Decide whether L is completely reducible.

3. In case L is completely reducible, compute a set $\{T_1, \ldots, T_s\} \subseteq \mathcal{D}$ such that $L = \mathrm{LCLM}(T_1, \ldots, T_s)$.

The article [BS99] approaches the second task above, as follows. First, find a set $\mathcal{T} = \{T_1, \ldots, T_s\}$ such that $L = \mathrm{LCLM}(T_1, \ldots, T_s)$. If L_1 is a monic left factor of L, then L_1 is equivalent to the least common left multiple of elements from some subset of $\mathcal{T}$. Let $\mathcal{S} = \left\{T_{i_1}, \ldots, T_{i_\mu}\right\} \subseteq \mathcal{T}$ be a fixed subset and let $L_2 = \mathrm{LCLM}(T_{i_1}, \ldots, T_{i_\mu})$. A sequence of lemmas shows that one can:

A. Parameterize the set $\mathcal{M}_{L_2}$ of pairs (L_1, S) with $\mathrm{ord}\ S < \mathrm{ord}\ L_1 = \mathrm{ord}\ L_2$ such that L_1 is a left factor of L and, moreover, (3.9) holds for some R; and

B. Determine whether there exists $(L_1, S) \in \mathcal{M}_{L_2}$ such that $L_1(y) = b$ admits a solution in k.

If these steps are carried out for all subsets $\mathcal{S} \subseteq \mathcal{T}$, then one finds operators L_1, L_0 satisfying conditions 6(abc) of Proposition 3.2.1. [BS99] then shows how to describe the action of G_{H} on V_{L_1}.

Below, Lemmas 3.2.4, 3.2.5, 3.2.6, 3.2.7 describe how to compute $\mathcal{M}_{L_2}$ for a given L_2, and Lemma 3.2.8 will be used to decide whether $L_1(y) = b$ admits a k-rational solution for a given $(L_1, S) \in \mathcal{M}_{L_2}$. Lemmas 3.2.5, 3.2.6 and 3.2.7 are proved by technical means that lie outside the scope of this dissertation; we omit the proofs here.

Lemma 3.2.4 *Given $L_1, L_2, R, S \in \mathcal{D}$ such that* $\mathrm{ord}(L_1) = \mathrm{ord}(L_2) = n$, $\mathrm{ord}(R) < n$, $\mathrm{ord}(S) < n$, *and (3.9) holds. Then, the equation $L_1(y) = b$, $b \in k$ has a solution in k if and only if the equation $L_2(y) = S(b)$ has a solution in k.*

Proof. The extended Euclidean algorithm yields $\tilde{R}$ and $\tilde{L}_1$ in $\mathcal{D}$ such that $\tilde{R}R + \tilde{L}_1 L_1 = 1$ and ord $\tilde{R}_1 <$ ord L_1. The map $v \mapsto R(v)$ is an isomorphism of V_{L_1} onto V_{L_2}, and the map $w \mapsto \tilde{R}(w)$ is the inverse of this isomorphism. Since $L_1\tilde{R}$ and $R\tilde{R} - 1$ vanish on V_{L_2}, we have that L_2 divides both of these operators. Therefore there exist $\tilde{S}$ and $\tilde{L_2} \in \mathcal{D}$ such that $L_1\tilde{R} = \tilde{S}L_2$ and $R\tilde{R} + \tilde{L}_2 L_2 = 1$.

We now claim that $\tilde{S}S + L_1\tilde{L}_1 = 1$. We have that

$$\begin{aligned}
(\tilde{S}S + L_1\tilde{L}_1)L_1 &= \tilde{S}SL_1 + L_1\tilde{L}_1L_1 \\
&= \tilde{S}L_2R + L_1(1 - \tilde{R}R) \\
&= \tilde{S}L_2R + L_1 - L_1\tilde{R}R \\
&= \tilde{S}L_2R + L_1 - \tilde{S}L_2R \\
&= L_1,
\end{aligned}$$

and the equation follows after cancelling L_1 on the right.

To prove one direction of the lemma, suppose $L_1(f) = b$ for some $f \in k$. If $h = R(f) \in k$, then $L_2(h) = SL_1(f) = S(b)$ as desired. To prove the other direction, suppose $L_2(h) = S(b)$ for some $h \in k$. Let $f = \tilde{R}(h) + \tilde{L}_1(b) \in k$. Then

$$\begin{aligned}
L_1(f) &= L_1\tilde{R}(h) + L_1\tilde{L}_1(b) \\
&= \tilde{S}L_2(h) + (1 - \tilde{S}S)(b) \\
&= \tilde{S}S(b) + b - \tilde{S}S(b) \\
&= b,
\end{aligned}$$

completing the proof.

∎

Let $k = \mathcal{C}(x)$. Given $a = \frac{p}{q} \in k$, $p, q \in \mathcal{C}[x]$ with $(p, q) = 1$, define $\deg a$ to be the maximum of $\deg p$ and $\deg q$. Given $L = a_nD^n + a_{n-1}D^{n-1} + \ldots + a_0 \in \mathcal{D}$, define $\deg L = \max_{1 \le i \le n}(\deg a_i)$. Given operators L and L_2, we will want to parameterize all pairs of operators (L_1, S) satisfying:

1. L_1 is a monic operator equivalent to L_2 that divides L on the left, and

2. $\text{ord } S \leq \text{ord } L_2 - 1$ and $L_2 R = S L_1$ for some $R \in \mathcal{D}$, $\text{GCRD}(L_1, R) = 1$.

Lemma 3.2.5 *Let T_1 and T_2 be operators with coefficients in $\mathcal{C}(x)$ of orders n and m and degrees N and M respectively. If T_3 is an operator with coefficients in $\mathcal{C}(x)$ such that $T_3 T_2 = T_1$, then $\deg T_3 \leq (n-m+1)^2 M + N$.*

Proof. See Lemma 2.5 of [BS99].

■

Lemma 3.2.6 *Let $k = \mathcal{C}(x)$ and L, L_2 be monic operators in $\mathcal{D}$ of orders n and m respectively.*

1. *For any i, $0 \leq i \leq \text{ord } L$, one can effectively find an integer n_i such that if $L = L_1 L_0$ with monic $L_1, L_0 \in \mathcal{D}$ and $\text{ord } L_1 = i$, then $\deg L_0 \leq n_i$.*
2. *One can effectively find an integer N such that if $L_2 \tilde{R} = \tilde{S} L$ for some $\tilde{R}, \tilde{S} \in \mathcal{D}$ with $\text{ord } \tilde{R} < \text{ord } L$ and $\text{ord } \tilde{S} < \text{ord } L_2$, then $\deg \tilde{S} \leq N$.*
3. *One can effectively find an integer M such that if L_1 is a monic operator equivalent to L_2, dividing L on the left, then there exist R and S in $\mathcal{D}$ such that $L_2 R = S L_1$, $\text{ord } R < \text{ord } L_1$, $\text{ord } S < \text{ord } L_2$ and $\deg R, \deg S \leq M$.*

Proof. See Lemma 2.6 of [BS99].

■

The next lemma relies on the following notion. Consider the set $\mathcal{F}_{n,m} \subseteq \mathcal{C}(x)[D]$ of operators of order n and degree at most m. We define a bijection between $\mathcal{F}_{n,m}$ and a subset of $\mathcal{C}^{2(n+1)(m+1)}$ as follows: Suppose $L = \sum_{i=0}^{n} a_i D^i \in \mathcal{F}_{n,m}$. Suppose moreover that, for each i, we have

$$a_i = \frac{\sum_{j=0}^{m} b_{i,j} x^j}{\sum_{j=0}^{m} c_{i,j} x^j}, \ b_{i,j}, c_{i,j} \in \mathcal{C}, \ (\sum_j b_{i,j} x^j, \sum_l c_{i,l} x^l) = 1.$$

Then identify L with the vector $(b_{0,0}, b_{0,1}, \ldots, c_{n-1,m}) \in \mathcal{C}^{2(n+1)(m+1)}$. Define a set $\mathcal{L} \subseteq \mathcal{F}_{n,m}$ to be *constructible* if, under this identification, $\mathcal{L}$ corresponds to a constructible subset of $\mathcal{C}^{2(n+1)(m+1)}$.

Lemma 3.2.7 *Let k, L and L_2 be as in the hypotheses of Lemma 3.2.6.*

1. *The set of pairs of monic operators* (L_1, L_0), $\text{ord } L_1 = m$, $\text{ord } L_0 = n - m$ *such that* $L = L_1 L_0$ *forms a constructible set whose defining equations can be explicitly computed.*

2. *Let* n_m *be as in Lemma 3.2.6.1 and* M *be as in Lemma 3.2.6.3. The set* $\mathcal{P}_{L_2}$ *of triples of operators* (L_1, R, S) *where*

   (a) $\text{ord } L_1 = m; \deg L_1 \leq n_m; \text{ ord } R, S \leq m-1; \deg R, S \leq M,$

   (b) L_1 *divides* L *on the the left,*

   (c) $\text{GCRD}(L_1, R) = 1,$

   (d) $L_2 R = S L_1$ *(and so* L_1 *is equivalent to* L_2*)*

   is constructible. Furthermore, one can effectively calculate the defining equations of $\mathcal{P}_{L_2}$.

3. *The set* $\mathcal{M}_{L_2}$ *of pairs* (L_1, S) *such that for some* $R \in \mathcal{D}$, $(L_1, R, S) \in \mathcal{P}_{L_2}$ *is a constructible set. Furthermore, one can effectively calculate the defining equations of* $\mathcal{M}_{L_2}$.

Proof. See Lemma 2.7 of [BS99].

■

Lemma 3.2.8 *Let* $k = \mathcal{C}(x)$, N *an integer and* $L = y^{(n)} + \ldots + a_0 y \in \mathcal{D}$. *The set* $\mathcal{V}$ *of* $(c_0, \ldots, c_N, d_0, \ldots, d_N) \in \mathcal{C}^{2N+2}$ *such that*

$$L(y) = \frac{c_N x^N + \ldots + c_0}{d_N x^N + \ldots + d_0} \tag{3.14}$$

has a solution in k, *is constructible. Furthermore, one can effectively find the defining equations of* $\mathcal{V}$.

Proof. See Lemma 2.8 of [BS99].

■

It is a fact that Lemma 3.2.8 holds in the case where k is an algebraic extension of $\mathcal{C}(x)$ and the parameterized rational function given in the right-hand side of (3.14) is replaced by a parameterized member of k. [BS99] restricts attention to the case where $k = \mathcal{C}(x)$ for convenience. Also remark that the above lemmas represent an extension of known methods for expressing the set of factorizations of a given operator as a constructible set; see [Gri90] and [Tsa96].

The above lemmas now provide sufficient machinery for a decision procedure to calculate the Galois group of $L(y) = b$. Here is the algorithm, as stated in [BS99] with slight modifications:

Algorithm I

Input: A completely reducible nth order operator $L \in \mathcal{C}(x)[D]$ and an element $b \in \mathcal{C}(x)$.

Output: A set of equations in n^2 variables defining the Galois group G_L of $L(y) = 0$, an integer t and a rational homomorphism $\Phi : G_L \to \mathsf{GL}_t(\mathcal{C})$ such that the Galois group G of $L(y) = b$ is $\mathcal{C}^t \rtimes G_L$ where the action of G_L on $\mathcal{C}^t$ by conjugation is given by Φ.

1. Write L as a least common left multiple of a set $\mathcal{T} = \{T_1, \ldots, T_s\}$ of irreducible operators (using, for example, the algorithms in the Appendix of [CS99]).

2. If $L = L_1 L_0$ then complete reducibility implies that L_1 is equivalent to the least common left multiple of some subset of $\mathcal{T}$. Fix some subset of $\mathcal{T}$ and let L_2 be the least common left multiple of its elements. For this operator, apply Lemma 3.2.7.3 to construct the set $\mathcal{M}_{L_2}$.

3. Let $(L_1, S) \in \mathcal{M}_{L_2}$. Lemma 3.2.4 implies that $L_1(y) = b$ has a solution in $\mathcal{C}(x)$ if and only if the equation
$$L_2(y) = S(b) \tag{3.15}$$
has a solution $y \in \mathcal{C}(x)$. Apply Lemma 3.2.8 to equation (3.15) to determine the set of (L_1, S) for which this equation has a rational solution.

4. Repeat steps 2. and 3. until one finds an L_2 of maximal order so that the set $\mathcal{R}_{L_2}$ of $(L_1, S) \in \mathcal{M}_{L_2}$ for which the equation (3.15) has a rational solution is nonempty. In this case, Proposition 3.2.1 implies that there exists a unique L_1 such that $(L_1, S) \in \mathcal{R}_{L_2}$ for some S.

5. We write $L = L_1 L_0$ and let t be the order of L_0. Find defining equations of the Galois group G_L of L with respect to a basis of the solution space that includes a basis of the solution space of $L_0(y) = 0$ (the results of [CS99] allow one to do this). In this basis, an automorphism $\sigma \in G$ will have the form $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$, where A represents the

action of σ on $W = V_{L_0}$. Restriction to the space $W \simeq \mathcal{C}^t$ (i.e., selecting A from σ) yields the desired rational map $\Phi : G_L \to \mathsf{GL}_t(\mathcal{C})$ that gives the action of G_L on $\mathcal{C}^t$ in $\mathcal{C}^t \rtimes G_L$.

■

We make the following additional remarks:

1. The calculations of Example 3.2.2 can be viewed as an application of the above algorithm. In that example, we have $L = (D - 2x) \circ (D - 2x)$, so that all first-order left (resp., right) factors of L are equivalent to $D - 2x$. The set of first-order left factors is $\left\{ L_{1,(c,d)} = D - (2x - \frac{d}{c+dx}) : (c, d) \neq (0, 0) \right\}$. The algorithm calls for deciding whether $L_{1,(c,d)}(y) = b$ admits a k-rational solution for some suitable (c, d). A calculation using Lemma 3.2.4 as in Step 3 of the algorithm shows that the above problem is equivalent to deciding whether $y' - 2xy = (c + dx) \cdot b$ admits a k-rational solution for some $(c, d) \neq (0, 0)$. Lemma 3.2.8 can then be applied to solve that problem.

2. [CS99] presents an algorithm to compute K_{H}/k, the Picard-Vessiot extension of $L(y) = 0$. This algorithm, together with Algorithm 1 above and Corollary 3.2.3, yields an algorithm to compute K_{I}/k, the Picard-Vessiot extension of $L(y) = b$.

3.3 Computing the group of $L_1 \circ L_2,\ L_1, L_2$ completely reducible

The problem of computing the group of $L_1 \circ L_2,\ L_1, L_2$ completely reducible, can be reduced to that of computing the group of $L(y) = b,\ L$ completely reducible. In [Ber90], D. Bertrand accomplishes this in terms of $\mathcal{D}$-modules. In [BS99], the process is made explicit in terms of operators and systems, and a decision procedure is provided. We recapitulate the results from [BS99] below.

First, consider the inhomogeneous first-order system

$$Y' = AY + B,\ Y = (y_1, \ldots, y_n)^T, A \in k^{n \times n}, B = (b_1, \ldots, b_n)^T \in k^n, \tag{3.16}$$

where the y_i are indeterminates. Let K_{H}/k (resp., $V_{\mathrm{H}},\ G_{\mathrm{H}}$) be the Picard-Vessiot extension (resp., the solution space; the group) of the associated homogeneous system $Y' = AY$. Before defining the extension and the group of (3.16), we define a new homogeneous system as follows: Define a new variable y_{n+1}, and consider the following system of equations:

$$Y' = AY + (b_1 y_{n+1}, b_2 y_{n+1}, \ldots, b_n y_{n+1})^T,\ y'_{n+1} = 0.$$

If we define $\tilde{Y} = (y_1, \ldots, y_n, y_{n+1})^T$, we obtain the following homogeneous first-order system:

$$\tilde{Y}' = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix} \tilde{Y}. \tag{3.17}$$

Define the Picard-Vessiot extension K_{I} (resp., the Galois group G_{I}) of (3.16) to be the Picard-Vessiot extension (resp., the group) of (3.17).

Note that if $Y = (y_1, \ldots, y_n) \in V_{\mathrm{H}}$, then $(y_1, \ldots, y_n, 0)$ satisfies (3.17). Thus, we may write $K_{\mathrm{H}} \subseteq K_{\mathrm{I}}$. If $\tilde{\eta} = (\eta_1, \ldots, \eta_n, 1)$ is a solution of (3.17), then $\eta = (\eta_1, \ldots, \eta_n)$ is a solution of (3.16). Any two solutions of (3.16) differ by a member of V_{H}, so that the full solution set of (3.16) is $\eta + V_{\mathrm{H}}$. Moreover, the full solution space of (3.17) over K_{I} is spanned by η and those solutions of the form $(y_1, \ldots, y_n, 0),\ (y_1, \ldots, y_n) \in V_{\mathrm{H}}$. It follows that K_{I}/k is the minimal differential field extension containing the full solution set of (3.16) and that $K_{\mathrm{I}} = K_{\mathrm{H}}\langle \eta_1, \ldots, \eta_n \rangle$.

We define equivalence for inhomogeneous systems as follows: We say that the systems $Y' = A_1 Y + B_1$ and $Y' = A_2 Y + B_2$ are *equivalent* (over k) if they have the same dimension n and there exist isomorphisms $\phi : (k^n, \nabla_{A_1}) \to (k^n, \nabla_{A_2})$ and $\psi : (k^{n+1}, \nabla_{\tilde{A}_1}) \to (k^{n+1}, \nabla_{\tilde{A}_2})$, where

$$\tilde{A}_i = \begin{bmatrix} A_i & B_i \\ 0 & 0 \end{bmatrix}$$

for $i = 1, 2$, such that $\psi\big|_{k^n \oplus 0}$ is identical to ϕ. We see that if $Y' = A_1 Y + B_1$ and $Y' = A_2 Y + B_2$ are equivalent systems, then a Picard-Vessiot extension associated with one system is also a Picard-Vessiot extension for the other system and, moreover, that $Y' = A_1 Y$ and $Y' = A_2 Y$ are equivalent.

We say that the inhomogeneous equation $L(y) = b$ and the system $Y' = AY + B$ are *equivalent* (over k) if the systems $Y' = A_L Y + (0, \ldots, 0, b)^T$ and $Y' = AY + B$ are equivalent (over k).

Given an inhomogeneous first-order system $Y' = AY + B$. We may compute an equivalent equation $L(y) = b$ by the following method: Let $\mathcal{E}$ (resp., $\mathcal{E}^*$) be the standard ordered basis of k^n (resp., of $(k^n)^*$). Find a cyclic vector v of $((k^n)^*, \nabla_A^*)$, so that

$$\mathcal{B}_v = \left\{ v, \nabla_A^*(v), \ldots, (\nabla_A^*)^{n-1}(v) \right\}$$

is an ordered basis of $(k^n)^*$. Using the fact that $[\nabla_A^*]_{\mathcal{E}^*} = -A^T$, compute the matrix

$$P = [\mathrm{id}]_{\mathcal{B}_v,\mathcal{E}^*} = [v|\nabla_A^*(v)|\cdots|(\nabla_A^*)^{n-1}(v)].$$

Note that if $\mathcal{B}_v^*$ is the dual ordered basis of $\mathcal{B}_v$ in k^n, then $[\mathrm{id}]_{\mathcal{E},\mathcal{B}_v^*} = P^T$ by (2.3). Compute $(\nabla_A^*)^n(v)$, then compute the column vector $\bar{v} = [(\nabla_A^*)^n(v)]_{\mathcal{B}_v}$ by solving the matrix equation $P\bar{v} = (\nabla_A^*)^n(v)$. Let $Q = [\nabla_A^*]_{\mathcal{B}_v}$. We see that

$$Q = \begin{bmatrix} 0 & 0 & 0 & \cdots & a_0 \\ -1 & 0 & 0 & \cdots & a_1 \\ 0 & -1 & 0 & \cdots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1} \end{bmatrix},$$

where $\bar{v} = -(a_0,\ldots,a_{n-1})^T$. Define $\tilde{A} = -Q^T = [\nabla_A]_{\mathcal{B}_v^*}$. We claim that $Y' = AY + B$ and $Y' = \tilde{A}Y + \tilde{B}$ are equivalent systems, where $\tilde{B} = P^T B$. Indeed, one checks that the map $\psi : k^{n+1} \to k^{n+1}$ given by

$$\psi(\hat{Y}) = \begin{bmatrix} P^T & 0 \\ 0 & 1 \end{bmatrix} \hat{Y}$$

is an isomorphism that has the properties required for equivalence of inhomogeneous systems. The system $Y' = \tilde{A}Y + \tilde{B}$ has the form

$$Y' = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{bmatrix} Y + \tilde{B}, \tag{3.18}$$

where $a_i \in k$. Write $Y = (y_1,\ldots,y_n)^T$, $\tilde{B} = (\tilde{b}_1,\ldots,\tilde{b}_n)^T$. This yields

$$y_i' = y_{i+1} + \tilde{b}_i \text{ for } 1 \le i \le n-1 \tag{3.19}$$

and

$$y_n' = -\sum_{j=1}^{n} a_j y_j + \tilde{b}_n. \tag{3.20}$$

By solving for y_{i+1} in (3.19) and applying to (3.20), we may eliminate the variable y_{i+1} from (3.20) for $i = n-1, n-2, \ldots, 1$. If we write $y = y_1$, we obtain an equation $L(y) = b$, where $L = D^n + \sum_{i=0}^{n-1} a_i$ and

$$b = \left[\sum_{i=1}^{n} \tilde{b}_i^{(n-i)}\right] + \left[\sum_{j=1}^{n-1} a_j \sum_{i=1}^{j} \tilde{b}_i^{(j+1-i)}\right] \in k. \tag{3.21}$$

We claim that $Y' = \tilde{A}Y + \tilde{B}$ and $Y' = \tilde{A}Y + (0, \ldots, 0, b)^T$ are equivalent systems. Indeed, define a map $\hat{\psi} : k^{n+1} \to k^{n+1}$ given by

$$\hat{\psi}(\hat{Y}) = \begin{bmatrix} I_n & w \\ 0 & 1 \end{bmatrix} \hat{Y},$$

where

$$w = (0, \tilde{b}_1, \tilde{b}_1' + \tilde{b}_2, \tilde{b}_1'' + \tilde{b}_2' + \tilde{b}_3, \ldots, \sum_{i=1}^{n} \tilde{b}_i^{(n-i)})^T;$$

one checks that this mapping is an isomorphism that has the properties required for equivalence of inhomogeneous systems. This shows that $Y' = AY + B$ is equivalent to $L(y) = b$, as desired.

Given a homogeneous equation $L(y) = 0,\ L = L_1 \circ L_2,\ L_2 = D^m + \tilde{a}_{m-1}D^{m-1} + \cdots + \tilde{a}_1 D + \tilde{a}_0,\ L_1 = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0$. Consider the following system of equations in $y_1, \ldots, y_{n+m}$:

$$\begin{aligned} y_m' &= -\sum_{i=1}^{m} \tilde{a}_{i-1} y_i + y_{m+1} \\ y_{n+m}' &= -\sum_{i=1}^{n} a_{i-1} y_{m+i} \\ y_i' &= y_{i+1} \text{ for } i \notin \{m, n+m\}\,. \end{aligned}$$

Written in matrix form, this system is

$$Y' = \begin{bmatrix} A_{L_2} & C_0 \\ 0 & A_{L_1} \end{bmatrix} Y,$$

where $C_0 \in k^{m \times n}$ is the matrix having 1 in the $m, 1$ position and zero everywhere else.

In what follows, we will show how to compute the group of a system of the form

$$Y' = \begin{bmatrix} A_2 & C \\ 0 & A_1 \end{bmatrix} Y, A_2 \in k^{m \times m}, A_1 \in k^{n \times n},\ C \in k^{m \times n}, \tag{3.22}$$

where $Y' = A_i Y$ is completely reducible for $i = 1, 2$ and C is an arbitrary given matrix.

Proposition 3.3.1 *Given a system of the form (3.16). Suppose that the associated homogeneous system $Y' = AY$ is completely reducible. Let $U = \mathrm{Gal}(K_{\mathrm{I}}/K_{\mathrm{H}}) \subseteq G_{\mathrm{I}}$. Then the following statements hold:*

1. *Fix an arbitary particular solution $\eta \in K_{\mathrm{I}}^n$ of $Y' = AY + B$. Then, the map $\Phi_\eta : U \to V_{\mathrm{H}}$ given by $\Phi_\eta(\tau) = \tau.\eta - \eta$ is an injective G_{H}-module homomorphism, where the*

action of G_{H} on U (resp., on V_{H}) is by conjugation (resp., by the usual representation of Galois group on solution space). In particular, U is a vector group over $\mathcal{C}$.

2. *G_{I} is isomorphic to $U \rtimes G_{\mathrm{H}}$, where G_{H} acts on U by conjugation. This is a Levi decomposition of G_{I}, i.e., U is the unipotent radical of G_{I} and G_{I} has a maximal reductive subgroup isomorphic to G_{H}.*

Proof. These statements follow from the proof of Proposition 3.2.1, suitably rewritten in terms of first-order systems.

■

The following result is adapted from Lemma 1 and the discussion in Section 2 of [Ber90]. A *fundamental solution matrix* of a first-order homogeneous system is a matrix whose column vectors form a basis of the solution space.

Lemma 3.3.2 *Let Y_1 (resp., Y_2) be a fundamental solution matrix of $Y' = A_1 Y$ (resp., $Y' = A_2 Y$). Then, the matrix*

$$Y = \begin{pmatrix} Y_2 & UY_1 \\ 0 & Y_1 \end{pmatrix} \tag{3.23}$$

is a fundamental solution matrix of equation (3.22) if and only if U satisfies

$$U' = A_2 U - U A_1 + C. \tag{3.24}$$

Proof. This statement is verified by direct calculation.

■

The following definitions provide an interpretation of (3.24) in terms of connections. Let $\mathcal{M}_i = (\mathcal{D}/\mathcal{D}L_i)^*$ for $i = 1, 2$. Then $[\nabla_{\mathcal{M}_i}]_{\mathcal{E}_i} = A_i$, where $\mathcal{E}_i$ is a suitable basis of $\mathcal{M}_i$ for $i = 1, 2$. Let $\psi_0 : \mathcal{M}_1 \to \mathcal{M}_2$ be such that $[\psi_0]_{\mathcal{E}_1, \mathcal{E}_2} = C$. Applying (3.3), we conclude that (3.24) is a matrix expression of the equation $\nabla_{\mathrm{Hom}}(\phi) = \psi_0$, where ϕ is an unknown member of $\mathrm{Hom}_k(\mathcal{M}_1, \mathcal{M}_2)$.

We compute another matrix expression of this equation as follows: Let K/k be a field extension with $\mathcal{C}_K = \mathcal{C}_k$. Given $V \in K^{m \times n}$, let v_i be the i^{th} column of V. Then define $\tilde{V} \in \mathcal{C}^{mn}$ by $\tilde{V} = (v_1^T, \ldots, v_n^T)^T$. Formulas (3.4) and (3.5) imply that V satisfies $V' = A_2 V - V A_1$ if and only if $\tilde{V}$ satisfies $\tilde{V}' = (-A_1^T \otimes I_m + I_n \otimes A_2)\tilde{V}$. Furthermore, if Y_1

(resp., Y_2) is a fundamental solution matrix of the system $Y' = A_1 Y$ (resp., $Y' = A_2 Y$), then a calculation shows that $(Y_1^{-1})^T \otimes Y_2$ is a fundamental solution matrix of the system $\tilde{V}' = (-A_1^T \otimes I_m + I_n \otimes A_2)\tilde{V}$, where $\tilde{V} \in \mathcal{C}^{mn}$ is a column vector of unknowns. Define $c_i \in \mathcal{C}^m$ to be the ith column vector of C. We see that the equation $\nabla_{\mathrm{Hom}}(\phi) = \psi_0$ also has the matrix expression

$$\tilde{V}' = (-A_1^T \otimes I_m + I_n \otimes A_2)\tilde{V} + \tilde{C}, \tag{3.25}$$

where $\tilde{C} = (c_1^T, \ldots, c_n^T)^T$.

Lemma 3.3.3 *Assume that $\mathcal{C} \subsetneq k$. Let $Y' = A_1 Y$ and $Y' = A_2 Y$ be completely reducible systems and let K/k be the Picard-Vessiot extension of k corresponding to equation (3.22). Let F/k, $F \subset K$, be the Picard-Vessiot extension corresponding to*

$$Y' = \begin{bmatrix} A_2 & 0 \\ 0 & A_1 \end{bmatrix} Y. \tag{3.26}$$

Then, the following statements hold:

1. *The system*

$$\tilde{V}' = (-A_1^T \otimes I_m + I_n \otimes A_2)\tilde{V} \tag{3.27}$$

   admits a full set of F-rational solutions, so there exists a tower of fields $k \subseteq E \subseteq F$ with E/k a Picard-Vessiot extension for (3.27). In particular, $\mathrm{Gal}(E/k)$ *is a quotient of* $\mathrm{Gal}(F/k)$.

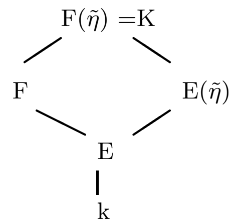
2. *$K = F(\tilde{\eta})$, where $\tilde{\eta}$ is a particular solution of (3.25).*

3. *$E(\tilde{\eta})/k$ is a Picard-Vessiot extension with $\mathrm{Gal}(E(\tilde{\eta})/k) \simeq W \rtimes \mathrm{Gal}(E/k)$, where W is a vector group. Moreover, we have $\mathrm{Gal}(K/k) \simeq W \rtimes \mathrm{Gal}(F/k)$. The action of $\mathrm{Gal}(F/k)$ on W is induced from the action of $\mathrm{Gal}(E/k)$ on W by the equality $\sigma.w = (\sigma|_E).w$ for $\sigma \in \mathrm{Gal}(F/k)$.*

Proof. The first two statements follow immediately from the discussion preceding the Lemma.

We prove the third statement as follows: Complete reducibility of the systems $Y' = A_1 Y$ and $Y' = A_2 Y$ implies that $\mathrm{Gal}(F/k)$ is reductive; it follows that $\mathrm{Gal}(E/k)$ is reductive as well. The first part of the third statement now follows from Proposition 3.3.1.

To prove the second part, we consider the following diagram:



Define $\tilde{W} = \mathrm{Gal}(K/F)$. Define a map $\psi : \tilde{W} \to \mathrm{Gal}(E(\tilde{\eta})/E)$ by composing the inclusion map $\tilde{W} \hookrightarrow \mathrm{Gal}(K/E)$ with the restriction map $\mathrm{Gal}(K/E) \twoheadrightarrow \mathrm{Gal}(E(\tilde{\eta})/E)$. We claim that ψ maps $\tilde{W}$ isomorphically onto W, so that

$$\tilde{W} = \mathrm{Gal}(F(\tilde{\eta})/F) \simeq \mathrm{Gal}(E(\tilde{\eta})/E) \simeq W.$$

To prove this claim, it suffices to show that $F \cap E(\tilde{\eta}) = E$ (see Lemma 5.10 of [Kap76] and its proof). Note that $\mathrm{Gal}(E(\tilde{\eta})/E) \simeq W$ is abelian. It follows that $\mathrm{Gal}(E(\tilde{\eta})/(F \cap E(\tilde{\eta}))$ is a normal subgroup of W and therefore that $(F \cap E(\tilde{\eta}))/E$ is a Picard-Vessiot extension. We have that $\mathrm{Gal}((F \cap E(\tilde{\eta}))/E)$ is a quotient of W and so is unipotent. Since $\mathrm{Gal}(F \cap E(\tilde{\eta})/E)$ is also a quotient of the reductive group $\mathrm{Gal}(F/k)$ it is also reductive and therefore must be trivial. Therefore $F \cap E(\tilde{\eta}) = E$.

Since $\mathrm{Gal}(K/F)/\tilde{W} \simeq G(F/k)$ is reductive, we have that $\tilde{W}$ is the unipotent radical of $\mathrm{Gal}(K/k)$. It follows that $G = \mathrm{Gal}(K/k)$ has Levi decomposition $G = \tilde{W}P$ (semidirect product of subgroups), where the restriction map $G \twoheadrightarrow \mathrm{Gal}(F/k)$ maps $P \subseteq G$ onto $\mathrm{Gal}(F/k)$. Note also that $\mathrm{Gal}(E(\tilde{\eta})/k)$ has Levi decomposition $\mathrm{Gal}(E(\tilde{\eta})/k) = WQ$ (semidirect product of subgroups), where $Q \subseteq \mathrm{Gal}(E(\tilde{\eta})/k)$ is the image of P under the restriction map $G \twoheadrightarrow \mathrm{Gal}(E(\tilde{\eta})/k)$. Moreover, we have natural isomorphisms $Q \simeq \mathrm{Gal}(E/k) \simeq P/P_E$ given by restriction maps.

Let $P_E = P \cap \mathrm{Gal}(K/E)$, so that the image of P_E under the restriction map $G \twoheadrightarrow \mathrm{Gal}(F/k)$ is the subgroup $\mathrm{Gal}(F/E) \subseteq \mathrm{Gal}(F/k)$. We see that P_E is normal in P and so is reductive. The image of P_E under the restriction homomorphism $\mathrm{Gal}(K/E) \twoheadrightarrow \mathrm{Gal}(E(\tilde{\eta})/E) \simeq W$ is a unipotent group and is therefore trivial. This means that P_E fixes $\tilde{\eta}$. Since an automorphism in $\tilde{W} = \mathrm{Gal}(F(\tilde{\eta})/F)$ is determined by its action on $\tilde{\eta}$, we see that P_E commutes elementwise with $\tilde{W}$ and therefore that the conjugation action of P_E on $\tilde{W}$ is trivial. It follows that the map $\psi : \tilde{W} \to W$ is an isomorphism not only of P-modules but of P/P_E-modules. The desired result now follows after considering the natural isomorphism $P/P_E \simeq \mathrm{Gal}(E/k)$.

■

This last result and its proof tell us how to compute the Galois group of equation (3.22) when $k = \mathcal{C}(x)$. Here is the algorithm, followed by examples, as stated in [BS99]:

Algorithm II

Input: A system of linear differential equations (3.22) where $Y' = A_1 Y$ and $Y' = A_2 Y$ are completely reducible with $A_1 \in \mathcal{C}(x)^{n\times n}, A_2 \in \mathcal{C}(x)^{m\times m}$.

Output: A system of equations in $m+n$ variables defining the Galois group $G(F/k) \subset \mathsf{GL}_{n+m}(\mathcal{C})$ of the Picard-Vessiot extension corresponding to the system (3.26), an integer t and a rational homomorphism $\Phi : G(F/k) \to \mathsf{GL}_t(\mathcal{C})$ such that the Galois group of (3.22) is $\mathcal{C}^t \rtimes G(F/k)$ where the action of $G(F/k)$ on $\mathcal{C}^t$ by conjugation is given by Φ.

1. One first calculates the Galois group $\tilde{G}$ of equation (3.26) using the results of [CS99]. This Galois group will be represented as matrices acting on $\mathrm{diag}(Y_1, Y_2)$ where Y_1 is a fundamental solution matrix of $Y' = A_1 Y$ and Y_2 is a fundamental solution matrix of $Y' = A_2 Y$. One can easily calculate the action of $G(F/k)$ on $(Y_1^{-1})^T \otimes Y_2$ and so calculate the Galois group $G(E/k)$ of equation (3.27) as well as the map $G(F/k) \to G(E/k)$.

2. Find a scalar equation $\hat{L}(y) = 0$ equivalent to the equation (3.27) as well as an element $\hat{b} \in k$ so that equation (3.25) is equivalent to $\hat{L}(y) = \hat{b}$ (an algorithm to do this is presented in [Kat87]; in the examples below *ad hoc* methods are used). Using the transformation of $Y' = A_{\hat{L}} Y$ to $\tilde{V}' = (-A_1^T \otimes I_n + I_m \otimes A_2)\tilde{V}$ allows us to calculate the action of $G(E/k)$ on the solution space of $\hat{L}(y) = 0$.

3. Proposition 3.2.1 allows us to calculate a vector group W so that the Galois group of $\hat{L}(y) = \hat{b}$ (and so of equation (3.25)) is $W \rtimes G(E/k)$.

4. Lemma 3.3.3 now tells us that the Galois group of equation (3.22) is the group $W \rtimes G(F/k)$ where the action of $G(F/k)$ on W (i.e., the homomorphism Φ) can be calculated from the information we have.

Remark: As in the case of the equation $L(y) = b$, the algorithms of [CS99] can be combined with the above to give a presentation of the Picard-Vessiot extension corresponding to $L_1(L_2(y)) = 0$.

We will now give three examples of this method. In these examples we will start with an equation of the form $L_1(L_2(y)) = 0$ with coefficients in $k = \mathcal{C}(x)$. The Galois group $G(F/k)$ — that is the Galois group of equation (3.26) in Lemma 3.3.3 — is the same as the Galois group of LCLM(L_1, L_2). In the examples we shall apply *ad hoc* methods to calculate this Galois group. We will then calculate a scalar equation equivalent to the system (3.27) as well as the matrix B defining this equivalence. This will allow us to find a scalar equation $\hat{L}(y) = \hat{b}$ equivalent to the system (3.25). We then apply the methods of Section 3.2 to calculate the vector space W.

Example 3.3.4 Consider the equation $L(y) = 0$, where $L = L_1 \circ L_2$, $L_1 = D^2 - x$, $L_2 = D^2 + \frac{1}{x}D + 1$.

The Galois group of this equation is an extension of the Galois group $G_{\tilde{L}}$ of $\tilde{L} =$ LCLM(L_1, L_2). Since L_1 and L_2 are both known to have Galois group isomorphic to $\mathsf{SL}_2(\mathcal{C})$ (L_1 is a form of Airy's equation and L_2 is a Bessel equation), $G_{\tilde{L}}$ is a subgroup of $\mathsf{SL}_2(\mathcal{C}) \times \mathsf{SL}_2(\mathcal{C})$.

We claim that if $G_{\tilde{L}}$ is a *proper* subgroup of $\mathsf{SL}_2(\mathcal{C}) \times \mathsf{SL}_2(\mathcal{C})$, then the operators $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ are equivalent over $\mathcal{C}(x)$. We prove this claim as follows: Let $\{y_1, y_2\}$ (resp., $\{z_1, z_2\}$) be a basis for V_{L_1} (resp., V_{L_2}). Before proceeding, we make the following auxiliary calculations related to the basis $\left\{z_1^2, z_1 z_2, z_2^2\right\}$ of $V_{L_2^{\circledS 2}}$. For $i = 1, 2$, we have

$$\begin{aligned} (z_i^2)' &= 2 z_i z_i' \\ \Rightarrow (z_i^2)'' &= 2(z_i z_i'' + (z_i')^2) \\ &= 2(z_i(-\frac{1}{x} z_i' - z_i) + (z_i')^2), \end{aligned}$$

from which a straightforward simplification yields

$$(z_i')^2 = z_i^2 + \frac{1}{2x}(z_i^2)' + \frac{1}{2}(z_i^2)''. \tag{3.28}$$

A similar set of computations involving the first and second derivatives of $z_1 z_2$ yields

$$z_1' z_2' = z_1 z_2 + \frac{1}{2x}(z_1 z_2)' + \frac{1}{2}(z_1 z_2)''. \tag{3.29}$$

Now suppose $G_{\tilde{L}}$ is a proper subgroup of $\mathsf{SL}_2(\mathcal{C}) \times \mathsf{SL}_2(\mathcal{C})$. Then, according to ([Kol68], p. 1158), there exist a quadratic extension $\tilde{k}/\mathcal{C}(x)$, an element $\alpha \in \tilde{k}$, and a matrix $S = (s_{ij}) \in \mathrm{GL}_2(\mathcal{C}(x))$ such that $\alpha^2 \in \mathcal{C}(x)$ and

$$\mathrm{Wr}(y_1, y_2) = \mathrm{diag}(\alpha, \alpha) \cdot S \cdot \mathrm{Wr}(z_1, z_2).$$

For $i = 1, 2$, we have

$$y_i = \alpha(s_{11} z_i + s_{12} z_i')$$

$$\begin{aligned}
\Rightarrow y_i^2 &= \alpha^2(s_{11}^2 z_i^2 + 2s_{11}s_{12}z_i z_i' + s_{12}^2(z_i')^2) \\
&= \alpha^2(s_{11}^2 z_i^2 + s_{11}s_{12}(z_i^2)' + s_{12}^2(z_i^2 + \frac{1}{2x}(z_i^2)' + \frac{1}{2}(z_i^2)'')) \text{ by (3.28)} \\
&= \alpha^2(s_{11}^2 + s_{12}^2)z_i^2 + \alpha^2(s_{11}s_{12} + \frac{1}{2x}s_{12}^2)(z_i^2)' + \frac{1}{2}\alpha^2 s_{12}^2 (z_i^2)'', \qquad (3.30) \\
y_1 y_2 &= \alpha^2(s_{11}^2 z_1 z_2 + s_{11}s_{12}(z_1 z_2' + z_1' z_2) + s_{12}^2 z_1' z_2') \\
&= \alpha^2(s_{11}^2 z_1 z_2 + s_{11}s_{12}(z_1 z_2)' + s_{12}^2(z_1 z_2 + \frac{1}{2x}(z_1 z_2)' + \frac{1}{2}(z_1 z_2)'')) \text{ by (3.29)} \\
&= \alpha^2(s_{11}^2 + s_{12}^2)z_1 z_2 + \alpha^2(s_{11}s_{12} + \frac{1}{2x}s_{12}^2)(z_1 z_2)' + \frac{1}{2}\alpha^2 s_{12}^2 (z_1 z_2)''. \qquad (3.31)
\end{aligned}$$

From (3.30) and (3.31), it follows that the linear operator

$$\frac{1}{2}\alpha^2 s_{12}^2 D^2 + \alpha^2(s_{11}s_{12} + \frac{1}{2x}s_{12}^2)D + \alpha^2(s_{11}^2 + s_{12}^2) \in \mathcal{C}(x)[D]$$

maps the ordered basis $\{z_1^2, z_1 z_2, z_2^2\}$ of $V_{L_2^{\circledS 2}}$ onto the ordered basis $\{y_1^2, y_1 y_2, y_2^2\}$ of $V_{L_1^{\circledS 2}}$. The claim now follows immediately.

In our case, we claim that $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ are *in*equivalent (and therefore that $G_{\tilde{L}} = \mathsf{SL}_2(\mathcal{C}) \times \mathsf{SL}_2(\mathcal{C})$). The expanded version of *DEtools* developed by Mark van Hoeij for MapleV.5 allows one to calculate symmetric powers, LCLM's and a basis of the ring of $\mathcal{D}$-module endomorphisms of $\mathcal{D}/\mathcal{D}L$ for an operator $L \in \mathcal{D} = \mathcal{C}(x)[D]$. Using this we proceed as follows. A calculation shows that

$$M = \mathrm{LCLM}(L_1^{\circledS 2}, L_2^{\circledS 2})$$

is of order 4. If $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ were equivalent then $\mathcal{D}/\mathcal{D}M$ would be the direct sum of two isomorphic $\mathcal{D}$-modules. The endomorphism ring of $\mathcal{D}/\mathcal{D}M$ would therefore have dimension 4. Using the `eigenring` command in *DEtools* one sees that this ring has dimension 2 and the desired result follows.

We now consider the equation

$$\tilde{V}' = H\tilde{V} + \tilde{C},$$

where

$$\begin{aligned}
H &= -A_1^T \otimes I_2 + I_2 \otimes A_2, \\
A_1 &= \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}, \\
A_2 &= \begin{bmatrix} 0 & 1 \\ -1 & -\frac{1}{x} \end{bmatrix}, \\
\tilde{C} &= (0, 1, 0, 0)^T.
\end{aligned}$$

A cyclic-vector computation shows that the system $\tilde{V}' = H\tilde{V}$ is equivalent to $Z' = KZ$, where

$$
\begin{aligned}
K &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -g_1 & -g_2 & -g_3 & -g_4 \end{bmatrix}, \\
g_1 &= \frac{x^6+3x^5+3x^4+5x^3+6x^2+3x-3}{x(x^3+x^2+1)}, \\
g_2 &= -\frac{x^6+5x^5+3x^3-7x^2-1}{x^3(x^3+x^2+1)}, \\
g_3 &= -\frac{2x^3-2x^2+1}{x^2}, \\
g_4 &= -\frac{x^3-2}{x(x^3+x^2+1)}.
\end{aligned}
$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$
B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -x & 0 \\ -1+x & -\frac{1}{x} & -1 & -2x \\ 2+\frac{1}{x} & \frac{3x^3-x^2+2}{x^2} & 3x-x^2 & 0 \end{bmatrix}.
$$

Therefore, the equation $\tilde{V}' = H\tilde{V} + \tilde{C}$ is equivalent to

$$
Z' = KZ + B\tilde{C}. \tag{3.32}
$$

(The reader can verify that $K = B'B^{-1} + BHB^{-1}$.) Since K is in companion-matrix form, it is easy to convert (3.32) into the inhomogeneous scalar equation $\hat{L}(y) = \hat{b}$, where

$$
\begin{aligned}
\hat{L} &= D^4 + g_4D^3 + g_3D^2 + g_2D + g_1 \qquad (g_i \text{ as above}), \\
\hat{b} &= \frac{x^4+2x^3+x^2+4x+3}{x^3+x^2+1}.
\end{aligned}
$$

Computations using the `DFactor` and `ratsols` commands in *DEtools* show that $\hat{L}$ is irreducible over $\mathcal{C}(x)$ and that this equation admits no rational solutions. Thus, the vector space W referred to in the third statement of Lemma 3.3.3 is all of $\mathcal{C}^4$. We conclude that the Galois group G_L is $(\mathsf{SL}_2(\mathcal{C})) \times \mathsf{SL}_2(\mathcal{C})) \ltimes \mathcal{C}^4$.

Example 3.3.5 Consider the equation $L(y) = 0$, where $L = L_1 \circ L_2$, $L_1 = D^2 + \frac{1}{x}D + 1$, $L_2 = D^2 - D$.

As in the previous example, the Galois group G_L of L is an extension of $G_{\tilde{L}}$, the group of $\tilde{L} = \mathrm{LCLM}(L_1, L_2)$. To calculate $G_{\tilde{L}}$ note that the Galois group G_{L_1} of L_1 is SL_2 and the Galois group G_{L_2} of L_2 is the multiplicative group $\mathcal{C}^*$. The group $G_{\tilde{L}}$ is a subgroup of $G_{L_1} \times G_{L_2}$ that projects surjectively onto each factor. The Theorem of [Kol68] implies that, in this case, $G_{\tilde{L}} = G_{L_1} \times G_{L_2}$.

We now consider the equation

$$\tilde{V}' = H\tilde{V} + \tilde{C},$$

where

$$\begin{aligned} H &= -A_1^T \otimes I_2 + I_2 \otimes A_2, \\ A_1 &= \begin{bmatrix} 0 & 1 \\ -1 & -\frac{1}{x} \end{bmatrix}, \\ A_2 &= \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \\ \tilde{C} &= (0,1,0,0)^T. \end{aligned}$$

A cyclic-vector computation shows that the system $\tilde{V}' = H\tilde{V}$ is equivalent to $Z' = KZ$, where

$$\begin{aligned} K &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -g_1 & -g_2 & -g_3 & -g_4 \end{bmatrix}, \\ g_1 &= \frac{10x^4 + 5x^3 - 6x^2 + 6x + 3}{x^2(5x^2 - 3)}, \\ g_2 &= -\frac{10x^3 + 15x^2 + 9x + 12}{x(5x^2 - 3)}, \\ g_3 &= 3\frac{5x^2 + 5x + 2}{5x^2 - 3}, \\ g_4 &= -2\frac{5x^2 + 5x - 3}{5x^2 - 3}. \end{aligned}$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 1 & \frac{1}{x} & 2 \\ -\frac{1}{x} & -2 & -1 & 3 + \frac{3}{x} \end{bmatrix}.$$

Therefore, the system $\tilde{V}' = H\tilde{V} + \tilde{C}$ is equivalent to

$$Z' = KZ + B\tilde{C}.$$

(The reader can again verify that $K = B'B^{-1} + BHB^{-1}$.) Conversion to an inhomogeneous scalar equation yields $\hat{L}(y) = \hat{b}$, where

$$\begin{aligned} \hat{L} &= D^4 + g_4 D^3 + g_3 D^2 + g_2 D + g_1 \quad (g_i \text{ as above}), \\ \hat{b} &= -2 + \frac{5x^2 + 5x + 12}{5x^2 - 3}. \end{aligned}$$

Using the `eigenring` command of *DEtools*, one sees that the dimension of the endomorphism ring of $\mathcal{D}/\mathcal{D}\hat{L}$ is two. Since $\hat{L}$ is completely reducible, this implies that $\mathcal{D}/\mathcal{D}\hat{L}$ is the direct sum of two nonisomorphic irreducible $\mathcal{D}$-modules. This furthermore implies that $\hat{L}$ has exactly two nontrivial irreducible right (resp., left) factors. A computation using the command `endomorphism_charpoly` yields two different right factors. From these one calculates the unique left factors and then one can show that for neither of these left factors $\bar{L}$ does the equation $\bar{L}(y) = \hat{b}$ have a rational solution. Since $\hat{L}(y) = \hat{b}$ also has no rational solutions, we conclude that G_L is $(\mathsf{SL}_2(\mathcal{C}) \times \mathcal{C}^*) \ltimes \mathcal{C}^4$.

Example 3.3.6 Consider the equation $L(y) = 0$, where $L = L_1 \circ L_2$, $L_1 = \mathrm{LCLM}(D - 2x, D)$, $L_2 = D^2$.

Here it is clear that $G_{\tilde{L}}$, the group of $\tilde{L} = \mathrm{LCLM}(L_1, L_2)$, is $\mathcal{C}^*$.

We now consider the equation

$$\tilde{V}' = H\tilde{V} + \tilde{C},$$

where

$$\begin{aligned} H &= -A_1^T \otimes I_2 + I_2 \otimes A_2, \\ A_1 &= \begin{bmatrix} 0 & 1 \\ 0 & 2x + \frac{1}{x} \end{bmatrix}, \\ A_2 &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ \tilde{C} &= (0, 1, 0, 0)^T. \end{aligned}$$

A cyclic-vector computation shows that the system $\tilde{V}' = H\tilde{V}$ is equivalent to $Z' = KZ$, where

$$
\begin{aligned}
K &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -h_1 & -h_2 \end{bmatrix}, \\
h_1 &= 2\frac{8x^6 - 12x^4 + 18x^2 + 9}{4x^4 + 3}, \\
h_2 &= 4\frac{x(4x^4 - 4x^2 + 3)}{4x^4 + 3}.
\end{aligned}
$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$
B = \begin{bmatrix} 0 & -x & -x & 0 \\ x & -1 & 2x^2 & -x \\ -2x^2 + 1 & 2x & -2x(2x^2 - 1) & 4x^2 \\ 2x(2x^2 - 3) & -6x^2 + 3 & 4x^2(2x^2 - 3) & -6x(2x^2 - 1) \end{bmatrix}.
$$

Therefore, the equation $\tilde{V}' + H\tilde{V} = -\tilde{C}$ is equivalent to

$$
Z' = KZ + B\tilde{C}.
$$

(The reader can once again verify that $K = B'B^{-1} + BHB^{-1}$.) In this example, the equivalent inhomogeneous scalar equation is $\hat{L}(y) = \hat{b}$, where

$$
\begin{aligned}
\hat{L} &= D^4 + h_2 D^3 + h_1 D^2, \\
\hat{b} &= 3 - 6x^2 + 6\frac{4x^4 - 8x^2 - 5}{4x^4 + 3}.
\end{aligned}
$$

The `eigenring` command shows that the corresponding endomorphism ring has dimension 10 and yields a basis of this ring. Applying the command `endomorphism_charpoly` to each of these will yield a list of right factors and a simple calculation yields their corresponding left factors. Despite the fact that in this case there is an infinite set of left factors, there is a third order operator

$$
L_0 = D^3 + \frac{8x^6 - 12x^4 + 6x^2 + 3}{x(4x^4 + 3)}D^2 - 2\frac{8x^6 + 3}{x^2(4x^4 + 3)}D + 2\frac{8x^6 + 12x^4 - 6x^2 + 3}{x^3(4x^4 + 3)}
$$

on this list of left factors such that $L_0(y) = \hat{b}$ admits the rational solution $y = -\frac{1}{4}x(6x^2+5)$. Meanwhile, another computation shows $\hat{L}(y) = \hat{b}$ admits no rational solutions. We are therefore able to avoid a calculation involving parameterized operators. Thus, we have

$$
G_L = \mathcal{C} \rtimes \mathcal{C}^*.
$$

3.4 Computing the group of $Y' = AY + B$, $Y' = AY$ completely reducible

The author would like to thank Daniel Bertrand for suggesting the approach given in this section.

The goal of this section is to present an improvement on Algorithm I. We work in terms of systems in this section, but these are interchangeable with equations provided $C \subsetneq k$.

We begin with two lemmas on modules over reductive groups. The first result is standard; see, e.g., Proposition XVII.1.1 and Lemma XVIII.5.9 of [Lan84].

Lemma 3.4.1 *Let G be a group defined over $\mathcal{C}$, and let V, V_1 and V_2 be irreducible finite-dimensional G-modules. Then:*

1. *If $\phi : V_1 \to V_2$ is a morphism of G-modules, then ϕ is either an isomorphism of V_1 onto V_2 or the zero map.*

2. *If $\psi : V \to V$ is a G-module automorphism, then $\psi = c\,\mathrm{id}_V$ for some $c \in \mathcal{C}$.*

Proof. The first statement of the conclusion is known as Schur's lemma. It follows from the irreducibility hypothesis and the fact that the kernel (resp., the image) of a G-module morphism ϕ is a G-submodule of the domain (resp., the range) of ϕ. The second statement follows from the fact that ψ must have an eigenvalue in the algebraically closed field $\mathcal{C}$; this implies that the corresponding eigenspace is a G-submodule, which must be all of V.

■

Lemma 3.4.2 *Given:*

- *G is a reductive linear algebraic group.*

- *$\hat{V}_1, \hat{V}_2, \ldots, \hat{V}_s$ are finite-dimensional irreducible G-modules that are pairwise nonisomorphic.*

- *V is a finite-dimensional G-module such that*

$$V \simeq \bigoplus_{1 \le i \le s} \hat{V}_i^{\nu_i} = \left\{ (v_{1,1}^T, \ldots, v_{i,j}^T, \ldots, v_{s,\nu_s}^T)^T : v_{i,j} \in \hat{V}_i \right\}.$$

- *W is a submodule of V.*

Then, the following statements hold:

1. *There exist matrices $R_l = (r_{l,ij}) \in \mathcal{C}^{\nu_l \times \nu_l}$ for $1 \le l \le s$ such that*

$$W = \Big\{ v = (v_{1,1}^T, \ldots, v_{l,m}^T, \ldots, v_{s,\nu_s}^T)^T \in V : \sum_{j=1}^{\nu_l} r_{l,mj} v_{l,j} = 0 \text{ for all } l, m,\ 1 \le l \le s,\ 1 \le m \le \nu_l \Big\}.$$

2. *Suppose $s = 1$, and write $\nu = \nu_1, \hat{V} = \hat{V}_1, v_j = v_{1,j}$. Then there exists a vector subspace $\mathcal{S} \subseteq \mathcal{C}^\nu$ such that*

$$W = \left\{ (v_1^T, \ldots, v_\nu^T)^T : \sum_{j=1}^{\nu} c_j v_j = 0 \text{ for all } (c_1, \ldots, c_\nu) \in \mathcal{S} \right\}.$$

We have $W \simeq \hat{V}^{\nu - \dim(\mathcal{S})}$.

Proof. We prove the first statement as follows: Complete reducibility implies that W is the kernel of a projection mapping $\pi : V \to \tilde{W}$ for some subspace $\tilde{W} \subseteq V$. This projection mapping is a morphism of G-modules. Applying a well-known result that characterizes the endomorphism ring of a completely reducible module (see Proposition XVII.1.2 of [Lan84]) and the second statement of Lemma 3.4.1, we see that there exist matrices $R_1, \ldots, R_s$ such that

$$\pi((v_{1,1}^T, \ldots, v_{l,m}^T, \ldots, v_{s,\nu_s}^T)^T) = (\sum_j r_{1,1j} v_{1,j}, \ldots, \sum_j r_{l,mj} v_{l,j}, \ldots, \sum_j r_{s,\nu_s j} v_{s,j}).$$

The first statement of the conclusion of the lemma follows immediately. The second statement then follows after defining $\mathcal{S} \subseteq \mathcal{C}^\nu = \mathcal{C}^{\nu_1}$ to be the row space of the matrix $R = R_1$.

■

We are interested in inhomogeneous systems of the form $Y' = \tilde{A}Y + \tilde{B}$ such that the associated homogeneous system $Y' = \tilde{A}Y$ is completely reducible. A system having this property is equivalent to a system of the form

$$\left.\begin{array}{rcl} Y' &=& AY + B, \\ A &=& \mathrm{diag}(A_1, A_2, \ldots, A_s), \\ B &=& (B_1^T, B_2^T, \ldots, B_s^T)^T, \\ A_i &=& \mathrm{diag}(M_i, \ldots, M_i) \ (\nu_i \text{ copies}), \\ M_i &\in& k^{m_i \times m_i}, \\ \multicolumn{3}{c}{Z' = M_i Z \text{ irreducible}, 1 \le i \le s,} \\ \multicolumn{3}{c}{\text{and pairwise inequivalent}} \end{array}\right\} \quad (3.33)$$

For the remainder of this section, we make the following assumptions:

1. $Y' = AY + B$ is an inhomogeneous system of order n defined over k such that the associated homogeneous system $Y' = AY$ is completely reducible.

2. K_{I}/k (resp., $G_{\mathrm{I}} = \mathrm{Gal}(K_{\mathrm{I}}/k)$) is the Picard-Vessiot extension (resp., the group) of $Y' = AY + B$.

3. K_{H}/k (resp., $V_{\mathrm{H}} \subseteq K_{\mathrm{H}}^n$; $G_{\mathrm{H}} = \mathrm{Gal}(K_{\mathrm{H}}/k)$) is the Picard-Vessiot extension (resp., the full solution set; the group) of the associated homogeneous system $Y' = AY$, with $K_{\mathrm{H}} \subseteq K_{\mathrm{I}}$.

4. U is the subgroup of G_{I} fixing K_{H} elementwise, so that

$$U \simeq \mathrm{Gal}(K_{\mathrm{I}}/K_{\mathrm{H}}) \subseteq G_{\mathrm{I}}$$

and $G_{\mathrm{H}} \simeq G_{\mathrm{I}}/U$.

Lemma 3.4.3 *The following are equivalent for $Y' = AY + B$:*

1. *The system admits a k-rational solution.*

2. *The system admits a K_{H}-rational solution.*

3. *Every solution of the system is K_{H}-rational.*

4. *The subgroup U is trivial, i.e., $K_{\mathrm{H}} = K_{\mathrm{I}}$.*

Proof. It is clear that the first and third statements each imply the second statement. Since the solution set of a system generates that system's Picard-Vessiot extension, it is also clear that the third and fourth statements are equivalent to each other.

Notice that any two solutions of $Y' = AY + B$ differ by an element of $V_{\mathrm{H}} \subseteq K_{\mathrm{H}}^n$. Using this fact, one checks that the second statement implies the third statement.

We now show that the second statement implies the first statement. This implication is proved in Proposition 3.2.1; for convenience we reproduce the proof here using the terminology and notation of systems.

Suppose η is a K_{H}-rational solution of $Y' = AY + B$. Let $W = V_{\mathrm{H}} + \mathrm{span}_{\mathcal{C}}\{\eta\} \subseteq K_{\mathrm{H}}^n$. Since $\sigma \in G_{\mathrm{H}}$ maps η to $\eta + v$ for some element $v \in V_{\mathrm{H}}$, we see that W is G_{H}-invariant and includes V_{H} as a G_{H}-invariant subspace. Moreover, W/V_{H} is a trivial G_{H}-module. Since G_{H} is reductive by assumption, we see that V_{H} has a one-dimensional complement $\tilde{V}$ in W that is trivial as a G_{H}-module. Moreover, since W is spanned by η and V_{H}, we may assume that $\tilde{V}$ is generated by $\tilde{\eta} = \eta + v_0$ for some $v_0 \in V_{\mathrm{H}}$. It follows that $\tilde{\eta}$ is a solution of $Y' = AY + B$ that is fixed by every element of G_{H} and therefore is rational over k. This completes the proof.

■

Lemma 3.4.4 *Assume $Y' = AY + B$ is irreducible. Then, as a G_{H}-module, U is either trivial or isomorphic to V_{H}.*

Proof. If U is nontrivial, then Proposition 3.3.1 implies that U is isomorphic to a nonzero G-submodule of V_{H}. By hypothesis, V_{H} is irreducible; the desired result follows.

■

Lemma 3.4.5 *Suppose $Y' = AY + B$ is of the form (3.33). Then, for each i, the following statements hold:*

1. *There exists a tower of subfields $k \subseteq K_{i,\mathrm{H}} \subseteq K_{\mathrm{H}}$ such that $K_{i,\mathrm{H}}/k$ is the Picard-Vessiot extension for the system $\tilde{Y}' = A_i\tilde{Y}$.*

2. *V_{H} has a ν_i-dimensional G_{H}-invariant subspace $V_{i,\mathrm{H}}$ consisting of vectors of the form $(0, \ldots, 0, Y_i, 0, \ldots, 0)$, where Y_i satisfies $Y_i' = A_iY_i$.*

3. *Let $\tilde{V}_{i,\mathrm{H}} \subseteq K_{i,\mathrm{H}}^{\nu_i}$ be the full solution space of $\tilde{Y}' = A_i\tilde{Y}$. Then there is an isomorphism $\Xi : V_{i,\mathrm{H}} \to \tilde{V}_{i,\mathrm{H}}$. Moreover, we have $V_{\mathrm{H}} \simeq \bigoplus_{i=1}^{s} \tilde{V}_{i,\mathrm{H}}$.*

Proof. Define $\xi_i : V_{\mathrm{H}} \to K_{\mathrm{H}}^{\nu_i}$ by $\xi((Y_1^T, \ldots, Y_s^T)^T) = Y_i$. We see that ξ is a G_{H}-invariant surjection of V_{H} onto $\bar{V}_i$, a full solution space in $K_{\mathrm{H}}^{\nu_i}$ of $\tilde{Y}' = A_i\tilde{Y}$. The first statement of the conclusion of the lemma follows after defining $K_{i,\mathrm{H}}/k$ to be the extension generated by components of vectors in $\bar{V}_i$. The second and third statements then follow easily.

■

Lemma 3.4.6 *Suppose $Y' = AY + B$ is of the form (3.33), and let $K_{i,\mathrm{H}}/k$ and $V_{i,\mathrm{H}}$ be as in Lemma 3.4.5. Write $\eta = (\eta_1^T, \ldots, \eta_s^T)^T$, $\eta_i \in K_{\mathrm{I}}^{\nu_i}$, so that η_i is a particular solution of the system*

$$\tilde{Y}' = A_i\tilde{Y} + B_i. \tag{3.34}$$

Then, for each i, there is a tower of subfields $K_{i,\mathrm{H}} \subseteq K_{i,\mathrm{I}} \subseteq K_{\mathrm{I}}$ with $K_{i,\mathrm{I}}/k$ a Picard-Vessiot extension for the system (3.34), with $K_{i,\mathrm{I}}/K_{i,\mathrm{H}}$ generated by the coordinates of η_i.

Proof. This result is clear from definitions. ■

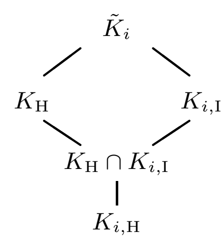
Lemma 3.4.7 *Suppose $Y' = AY + B$ is of the form (3.33). Then $U \simeq \bigoplus_{i=1}^{s} U_i$ (direct sum of G_{H}-modules), where U_i is the unipotent radical of the group of $\tilde{Y}' = A_i\tilde{Y} + B_i$ for $1 \leq i \leq s$.*

Proof. Applying Proposition 3.3.1 to $Y' = AY + B$, we see that there is an embedding $\Phi : U \to V_{\mathrm{H}}$. Let $W = \Phi(U) \subseteq V_{\mathrm{H}}$.

Let $K_{i,\mathrm{H}}/k$ and $V_{i,\mathrm{H}}$ be as in Lemma 3.4.5. Lemma 3.4.5 and basic Galois theory yield $V_{\mathrm{H}} \simeq \bigoplus_{i=1}^{s} \tilde{V}_{i,\mathrm{H}}$ (direct sum of G_{H}-modules), where $\tilde{V}_{i,\mathrm{H}}$ is the solution space of $\tilde{Y}' = A_i\tilde{Y}$. Lemma 3.4.2 implies that $W \simeq \bigoplus_{i=1}^{s} \pi_i(W)$, where $\pi_i : V_{\mathrm{H}} \to \tilde{V}_{i,\mathrm{H}}$ is projection from V_{H} onto $\tilde{V}_{i,\mathrm{H}}$. We need to show that $\pi_i(W) \simeq U_i$.

Fix i, $1 \leq i \leq s$. Consider $\tilde{Y}' = A_i\tilde{Y} + B_i$ as an equation over K_{H} and let $\tilde{K}_i/K_{\mathrm{H}}$ be the Picard-Vessiot extension. We have that $\mathrm{Gal}(\tilde{K}_i/K_{\mathrm{H}})$ is a quotient of U and $\tilde{K}_i/K_{\mathrm{H}}$ is generated by the coordinates of η_i. By considering the map Ξ given in Lemma 3.4.5, one checks that $\mathrm{Gal}(\tilde{K}_i/K_{\mathrm{H}}) \simeq \pi_i(W)$.

Now consider the following diagram:



By definition we have $U_i = \mathrm{Gal}(K_{i,\mathrm{I}}/K_{i,\mathrm{H}})$. Thus, to show that $\pi_i(W) \simeq U_i$, it suffices to show that $\mathrm{Gal}(\tilde{K}_i/K_{\mathrm{H}}) \simeq \mathrm{Gal}(K_{i,\mathrm{I}}/K_{i,\mathrm{H}})$. In turn, to do this it suffices to show that $K_{\mathrm{H}} \cap K_{i,\mathrm{I}} = K_{i,\mathrm{H}}$ (see Lemma 5.10 of [Kap76]).

U_i is a vector group and in particular an abelian group. It follows that $(K_{\mathrm{H}} \cap K_{i,\mathrm{I}})/K_{i,\mathrm{H}}$ is a Picard-Vessiot extension with unipotent Galois group. At the same time, $\mathrm{Gal}((K_{\mathrm{H}} \cap K_{i,\mathrm{I}})/K_{i,\mathrm{H}})$ is a quotient of $\mathrm{Gal}(K_{\mathrm{H}}/K_{i,\mathrm{H}})$, which is a subgroup of the reductive group G_{H} and therefore reductive. This implies that $\mathrm{Gal}((K_{\mathrm{H}} \cap K_{i,\mathrm{I}})/K_{i,\mathrm{H}})$ is also reductive. It follows that $\mathrm{Gal}((K_{\mathrm{H}} \cap K_{i,\mathrm{I}})/K_{i,\mathrm{H}}) = \{1\}$, and we conclude that $K_{\mathrm{H}} \cap K_{i,\mathrm{I}} = K_{i,\mathrm{H}}$ as desired.

■

Lemma 3.4.8 *Assume that* $A = \operatorname{diag}(M, M, \dots, M)$, *where* $M \in k^{m\times m}$ *and there are* $\nu \geq 1$ *copies of* M *along the diagonal. Assume moreover that* $Z' = MZ$ *is an irreducible system. Let* $V_M \subseteq K_{\mathrm{H}}^m$ *be the solution space of* $Z' = MZ$, *so that* $V_{\mathrm{H}} = V_M^\nu$. *Write* $B = (B_1^T, B_2^T, \dots, B_\nu^T)^T$, $B_i \in k^m$. *Let* $\eta = (\eta_1^T, \eta_2^T, \dots, \eta_\nu^T)^T$, $\eta_i \in K_{\mathrm{I}}^m$, *be a fixed particular solution of* $Y' = AY + B$. *Let* $\Phi_\eta : U \to V_{\mathrm{H}}$ *be the map defined in Proposition 3.3.1 and let* $W = \Phi_\eta(U) \subseteq V_{\mathrm{H}}$. *Let* $\mathcal{S} \subseteq \mathcal{C}^\nu$ *be the vector space defined in the second statement of the conclusion of Proposition 3.4.2 (assuming* $V = V_{\mathrm{H}}$*). Define* $\mathcal{T} \subseteq \mathcal{C}^\nu$ *by*

$$\mathcal{T} = \{(c_1, \dots, c_\nu) \in \mathcal{C}^\nu \quad : \quad \text{the system } Z' = MZ + \sum_{j=1}^{\nu} c_j B_j \text{ has a } k\text{-rational solution}\}.$$

Then, the following statements hold:

1. $\mathcal{T}$ *is a* $\mathcal{C}$*-vector space.*

2. $\mathcal{T} = \mathcal{S}$.

3. $U \simeq V_M^{\nu - \dim_{\mathcal{C}} \mathcal{T}}$ *as* G_{H}*-modules.*

Proof. The first statement of the conclusion is easily verified, and the third statement follows directly from the second statement. We prove the second statement as follows:

We see that there is an injection $U \hookrightarrow \oplus_j U_j$, where U_j is the unipotent radical of the group of $Z' = MZ + B_j$. For $1 \leq j \leq \nu$, we have that η_j is a particular solution of $Z' = MZ + B_j$, and we may define $\Phi_{\eta_j} : U_j \to V_M$ by $\Phi_{\eta_j}(\tau) = \tau.\eta_j - \eta_j$ or, equivalently, by writing

$$\Phi(\tau) = (\Phi_{\eta_1}(\pi_1(\tau)), \dots, \Phi_{\eta_\nu}(\pi_\nu(\tau))) \in V_M^\nu = V_{\mathrm{H}},$$

where $\pi_j : U \to U_j$ is projection onto the jth factor. Also observe that, given $c_1, \dots, c_\nu \in \mathcal{C}$, we have that $\sum_j c_j \eta_j$ is a particular solution of the system $Z' = MZ + \sum_j c_j B_j$. We now make the following calculation:

$$\begin{aligned}
(c_1, \dots, c_\nu) \in \mathcal{S} \quad &\Leftrightarrow \quad \sum_j c_j \Phi_{\eta_j}(\tau) = 0 \text{ for all } \tau \in U \\
&\Leftrightarrow \quad \sum_j c_j(\tau.\eta_j - \eta_j) = 0 \text{ for all } \tau \in U \\
&\Leftrightarrow \quad \sum_j c_j \tau.\eta_j = \sum_j c_j \eta_j \text{ for all } \tau \in U
\end{aligned}$$

$$
\begin{aligned}
&\Leftrightarrow \quad \tau.(\sum_j c_j\eta_j) = \sum_j c_j\eta_j \text{ for all } \tau \in U \\
&\Leftrightarrow \quad \sum_j c_j\eta_j \in K_{\mathrm{H}}^m \text{ (since } K_{\mathrm{H}} \text{ is the fixed field of } U) \\
&\Leftrightarrow \quad \text{The system } Z' = MZ + \textstyle\sum_j c_jB_j \text{ has} \\
&\qquad\quad \text{a } k\text{-rational solution (by Lemma 3.4.3)} \\
&\Leftrightarrow \quad (c_1, \ldots, c_\nu) \in \mathcal{T}.
\end{aligned}
$$

This gives us the desired result.

■

For the remainder of this section, assume $k = \mathcal{C}(x)$.

Lemma 3.4.9 *There exists an algorithm that takes as input a matrix $M \in k^{m\times m}$ and a set of vectors $B_1, \ldots, B_\nu \in k^m$ and computes $\dim_{\mathcal{C}}(\mathcal{T})$, where $\mathcal{T} \subseteq \mathcal{C}^\nu$ is the vector space defined in Lemma 3.4.8.*

Proof. Let $A = \mathrm{diag}(M, \ldots, M)$ with ν copies of M on the diagonal, and let $B = (B_1^T, \ldots, B_\nu^T)^T$. Consider the following conceptually simple algorithm:

1. Compute a cyclic vector for the system $Z' = MZ$; obtain a system of the form (3.18), and use this system to define an operator L such that $L(y) = 0$ is equivalent to $Z' = MZ$.

2. For each i, use (3.18) and (3.21) to compute an element $b_i \in k$ such that $Z' = MZ + B_i$ is equivalent to $L(y) = b_i$.

3. Define a new operator $\hat{L}$ by

$$\hat{L} = \mathrm{LCLM}\left(D - \frac{b_1'}{b_1}, \ldots, D - \frac{b_\nu'}{b_\nu}\right) \circ L.$$

4. Compute a basis $\mathcal{F}$ of k-rational solutions of the equation $\hat{L}(y) = 0$. For each element f in this basis, test whether f satisfies $L(f) = 0$.

5. Return the number of elements of $\mathcal{F}$ that are *not* solutions of $L(y) = 0$.

We prove the correctness of this algorithm as follows. For a given $(c_1, \ldots, c_\nu) \in \mathcal{C}^\nu$, we have that $Z' = MZ + \sum_j c_jB_j$ admits a k-rational solution if and only if the equation $L(y) = \sum_j c_jb_j$ does. Suppose $f \in k$ satisfies $L(f) = \sum_j c_jb_j$ for some $(c_1, \ldots, c_\nu) \in \mathcal{C}^\nu$. It follows that $\hat{L}(f) = 0$. Conversely, we see that if $\hat{L}(f) = 0$ and $L(f) \neq 0$, then $L(f) = \sum_j c_j b_j$ for some $(c_1, \ldots, c_\nu) \in \mathcal{C}^\nu$. The desired result now follows easily.

■

We note that it is possible to write a more efficient algorithm than the above, using methods similar to those of Lemma 2.8 of [BS99].

We are now ready to present the main algorithm of this section.

Algorithm III.

Input: A matrix $A \in \mathcal{C}(x)^{n\times n}$ and a vector $B \in \mathcal{C}(x)^n$

Output: An explicit description of the Galois group of the system $Y' = AY + B$

1. Using a cyclic-vector computation, redefine A and compute A_i, B_i, M_i, m_i so that the system (3.33) is equivalent to the original system.

2. For $1 \leq i \leq s$, write $B_i = (B_{i,1}^T, \ldots, B_{i,\nu_i}^T)^T$. Using Lemma 3.4.9, compute $r_i = \dim_{\mathcal{C}} \mathcal{T}_i$, where

$$\mathcal{T}_i = \Big\{(c_{i,1}, \ldots, c_{i,\nu_i}) : \text{ the system } Z' = M_i Z + \sum_j c_{i,j} B_{i,j} \text{ admits a } k\text{-rational solution}\Big\}.$$

   Let $\tilde{r}_i = \nu_i - r_i$.

3. Using [CS99], compute a set $\mathcal{H}$ of defining equations for $\Psi(G_{\mathrm{H}})$, where $\Psi : G_{\mathrm{H}} \to \mathsf{GL}_n(\mathcal{C})$ is a matrix representation of G_{H} on V_{H} with respect to some basis of V_{H} having the following property: Given a matrix $Q = \Psi(\sigma)$, $\sigma \in G_{\mathrm{H}}$, then we have $Q = \mathrm{diag}(Q_1, \ldots, Q_s)$ with $Q_i = \mathrm{diag}(\bar{Q}_i, \ldots, \bar{Q}_i)$ (ν_i copies) and $\bar{Q}_i$ gives the action of σ on V_{M_i} with respect to some fixed basis of V_{M_i} for $1 \leq i \leq s$. Here, V_{M_i} is the solution space of $Z' = M_i Z$.

4. Return $\mathcal{H},\ m_1, \ldots, m_s,\ \tilde{r}_1, \ldots, \tilde{r}_s$. The group of $Y' = AY + B$ is

$$\mathcal{C}^{\sum_i \tilde{r}_i m_i} \rtimes \hat{G}_{\mathrm{H}},$$

   where:

   - $\hat{G}_{\mathrm{H}} \subseteq \mathsf{GL}_n(\mathcal{C})$ is defined by $\mathcal{H}$

- The action of $Q \in \hat{G}_{\mathrm{H}}$ on $v \in \mathcal{C}^{\sum_i \tilde{r}_i m_i}$ is given by $Q.v = \tilde{Q}v$ (matrix-by-vector multiplication), where

$$\begin{aligned} \tilde{Q} &= \operatorname{diag}(\tilde{Q}_1, \ldots, \tilde{Q}_s), \\ \tilde{Q}_i &= \operatorname{diag}(\bar{Q}_1, \ldots, \bar{Q}_1) \ (\tilde{r}_i \text{ copies}), \end{aligned}$$

where $\bar{Q}_i$ is as described above.

We prove the correctness of this algorithm as follows:

Proof. First, we recall that equivalent systems have identical Picard-Vessiot extensions (resp., Galois groups). This algorithm computes the group of (3.33) and thus group of the original system.

Computing G_{H} is accomplished by [CS99], so by Proposition 3.3.1 we need to compute the unipotent radical U and the action of G_{H} on U. Write $U = \bigoplus_i U_i$ as in Lemma 3.4.7. Then Lemma 3.4.8 implies that $U_i \simeq V_{M_i}^{\tilde{r}_i}$ as modules over the group of $\tilde{Y}' = \tilde{A}Y$ and thus over G_{H}. Correctness of Algorithm III is now immediate.

■

We now present examples of this algorithm.

Example 3.4.10 Consider the equation $L(y) = b$, where

$$L = D^2 - 4xD + (4x^2 - 2) = (D - 2x) \circ (D - 2x)$$

and $b \in \mathcal{C}(x)$ as in Example 3.2.2. This equation is equivalent to the system $Y' = AY + B$, where $A = \begin{bmatrix} 0 & 1 \\ -4x^2+2 & 4x \end{bmatrix}$ and $B = (0, b)^T$. A computation shows that another equivalent system is $\tilde{Y}' = \tilde{A}\tilde{Y} + \tilde{B}$, where $\tilde{A} = \operatorname{diag}(2x, 2x)$ and $\tilde{B} = (-xb, b)^T$. The transformation from one system to the other is obtained by writing $\tilde{Y} = PY$, where $P = \begin{bmatrix} 1+2x^2 & -x \\ -2x & 1 \end{bmatrix}$. Applying Lemma 3.4.8, we see that $U \simeq \mathcal{C}^{2-r}$, where

$$\begin{aligned} r \;=\; & \dim_{\mathcal{C}} \Big\{ (c_1, c_2) : y' = 2xy - c_1 xb + c_2 b \\ & \text{admits a } \mathcal{C}(x)\text{-rational solution} \Big\}. \end{aligned}$$

This computation is essentially identical to the one obtained in the first remark at the end of Section 3.2. Thus, for this particular example, Algorithm III essentially coincides with Algorithm I.

Example 3.4.11 Consider the first-order system

$$Y' = \text{diag}(M, M, M, M, M)Y + (0, x^2, 0, x, 0, 1, 0, 1/x, 0, 1/x^2)^T,$$

where $M = \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}$. In this case, we see that G_{H} is the group of the equation $y'' - xy = 0$. From Example 3.3.4 above, we conclude that $G_{\text{H}} \simeq \mathsf{SL}_2$. To compute U, we consider the equation

$$y'' - xy = c_1x^2 + c_2x + c_3 + c_4/x + c_5/x^2.$$

Applying the algorithm given in the proof of Lemma 3.4.9, we consider the equation $\hat{L}(y) = 0$, where

$$\hat{L} = \text{LCLM}(D - 2/x, D - 1/x, D, D + 1/x, D + 2/x) \circ (D^2 - x).$$

A `ratsols` computation in Maple shows that the space of rational solutions of $\hat{L}(y) = 0$ is spanned by the elements 1 and x, which furthermore fail to satisfy $y'' - xy = 0$. Applying Lemma 3.4.8, we now see that $G_{\text{I}} \simeq \mathcal{C}^6 \rtimes \mathsf{SL}_2$, where

$$Q.(v_1^T, v_2^T, v_3^T)^T = \left((Qv_1)^T, (Qv_2)^T, (Qv_3)^T\right)^T$$

for $Q \in \mathsf{SL}_2,\ v_1, v_2, v_3 \in \mathcal{C}^2$, and Qv_i is the standard matrix-by-vector product.

Example 3.4.12 Consider the matrix equation

$$\begin{aligned} Y' &= \text{diag}(A_1, A_2)Y + (B_1^T, B_2^T)^T, \\ A_1 &= \text{diag}(M, M, M, M, M),\ M = \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}, \\ A_2 &= \text{diag}(2x, 2x), \\ B_1 &= (0, x^2, 0, x, 0, 1, 0, 1/x, 0, 1/x^2)^T, \\ B_2 &= (-x, 1)^T. \end{aligned}$$

Evidently G_{H} is the group of the equation $L(y) = 0$, where $L = \text{LCLM}(D^2 - x, D - 2x)$. We see that G_{H} is a subgroup of $\mathsf{SL}_2 \times \mathcal{C}^*$ that projects surjectively onto each factor. As in Example 3.3.5, the Theorem of [Kol68] yields $G_{\text{H}} = \mathsf{SL}_2 \times \mathcal{C}^*$. Next, Lemma 3.4.7 implies that $U \simeq U_1 \oplus U_2$ (direct sum of G_{H}-modules), where U_1 (resp., U_2) is the unipotent radical of the system given in Example 3.4.11 (resp., Example 3.4.10 with $b = 1$). After applying the results of Example 3.4.11 and 3.2.2, we conclude that $G_{\text{I}} \simeq \mathcal{C}^7 \rtimes (\mathsf{SL}_2 \times \mathcal{C}^*)$, where

$$(Q, t).(v_1, v_2, v_3, w)^T = \left((Qv_1)^T, (Qv_2)^T, (Qv_3)^T, tw\right)^T$$

for $(Q,t) \in \mathsf{SL}_2 \times \mathcal{C}^*,\ v_1, v_2, v_3 \in \mathcal{C}^2, w \in \mathcal{C}$.

Note that applying the method of Algorithm I to this system (or rather, more precisely, to an equivalent inhomogeneous scalar equation) would involve computing all factorizations of a twelfth-order completely reducible operator; this step alone would require solving a very large system of equations, in contrast with the simple steps performed above.

Chapter 4

Computing the group of $D^3 + aD + b,\ a, b \in \mathcal{C}[x]$

4.1 Definitions and main results

In this chapter, except where otherwise specified, $\mathcal{C}$ is an algebraically closed constant field of characteristic zero.

We define the *defect* of a connected group, using the definition given in [Sin99], as follows: Assume G is a connected linear algebraic group with Levi decomposition $G = R_u P$ (semidirect product of subgroups), where R_u is the unipotent radical and P a Levi subgroup of G. Note that the group $R_u/(R_u, R_u)$ is commutative and unipotent, hence isomorphic to a vector group $\mathcal{C}^n$ for some n. We see that the conjugation action of P on R_u leaves (R_u, R_u) invariant and therefore induces a representation of P on the vector group $R_u/(R_u, R_u)$. Write $R_u/(R_u, R_u) \simeq U_1^{n_1} \oplus \cdots \oplus U_s^{n_s}$, where each U_i is an irreducible P-module. Suppose U_1 is the trivial one-dimensional P-module. Then the defect of G is the number n_1.

Proposition 4.1.1 *Given $L \in \mathcal{C}(x)[D]$ of order three such that all singularities of L in the finite plane are apparent singularities and the group G_L of $L(y) = 0$ over $\mathcal{C}(x)$ is included in SL_3. Then G_L is connected and has defect zero.*

Proof. This result follows from Proposition 11.20 and Theorem 11.21 of [dPS].

■

The following well-known result allows us to apply Proposition 4.1.1 to operators of the form $L = D^3 + aD + b, a, b \in \mathcal{C}[x]$.

Lemma 4.1.2 *Given $L = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 \in \mathcal{D}$. Then the group G_L is isomorphic to a subgroup of SL_n if and only if $a_{n-1} = f'/f$ for some $f \in \mathcal{C}(x)$.*

Proof. Let $\mathcal{B} = \{y_1, \ldots, y_n\}$ be a basis of V_L. Then the *fundamental solution matrix* associated to $\mathcal{B}$ is $Z_{\mathcal{B}} = (y_j^{(i-1)}) \in \mathsf{GL}_n$. It is well-known (see, e.g., [Mag94]) that if $Z = Z_{\mathcal{B}}$ is a fundamental solution matrix of L, then a_{n-1} is the logarithmic derivative of $\det Z$. Also, given $\sigma \in G_L$, one checks that $\sigma(\det Z) = \det([\sigma]_{\mathcal{B}}) \det Z$. It then follows from basic Galois theory that $\det Z$ is contained in $\mathcal{C}(x)$ if and only if $\det([\sigma]_{\mathcal{B}}) = 1$ for all $\sigma \in G_L$, i.e., $[G_L]_{\mathcal{B}} \subseteq \mathsf{SL}_n$. The desired result then follows easily.

■

Corollary 4.1.3 *Given $L = D^3 + aD + b \in \mathcal{C}(x)[D], a, b \in \mathcal{C}[x]$. Then G_L is included in SL_3, is connected, and has defect zero.*

Proof. This result follows easily from Proposition 4.1.1 and Lemma 4.1.2.

■

In light of the above results, we define a subgroup $G \subseteq \mathsf{SL}_3$ to be *admissible* if it is connected and has defect zero. Theorem 4.1.5 below enumerates the admissible subgroups of SL_3 up to conjugation.

Before proceeding, we define some specific algebraic subgroups of SL_3 using certain parameterizations. Remark that these parameterizations are noncanonical; we use them in this section for clarity of description only. See Lemmas 4.2.2 and 4.3.1 for equivalent definitions of these subgroups that do not use parameterizations.

$$
\begin{aligned}
T_{(d_1,d_2)} &= \left\{\mathrm{diag}(y^{d_1}, y^{d_2}, y^{-d_1-d_2}) : y \in \mathcal{C}^*\right\}, \\
&\quad\; d_1, d_2 \in \mathbb{Z}, d_1 \geq d_2 \geq 0, d_1 > 0, \mathrm{GCD}(d_1, d_2) = 1 \\
U^1_{(0,0)} &= \left\{ \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : x \in \mathcal{C} \right\}
\end{aligned}
$$

$$U^1_{(1,1)} = \left\{ \begin{bmatrix} 1 & x & \frac{1}{2}x^2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} : x \in \mathcal{C} \right\}$$

$$U^2_{(1,0)} = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathcal{C} \right\}$$

$$U^2_{(0,1)} = \left\{ \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathcal{C} \right\}$$

$$U^2_{(1,1)} = \left\{ \begin{bmatrix} 1 & x & \frac{1}{2}x^2 + y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathcal{C} \right\} = U^1_{(0,0)} U^1_{(1,1)}$$

Let S_3 be the group of permutations of the ordered set $\{1, 2, 3\}$. Given $\sigma \in S_3$, then we define the *permutation matrix* P_σ to be the matrix whose (i, j)th entry is 1 if $i = \sigma(j)$, 0 otherwise.

Given an ordered basis $\mathcal{E} = \{\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3\}$ and a permutation $\sigma \in S_3$, then $\mathcal{E}_\sigma$ is the ordered basis given by

$$\mathcal{E}_\sigma = \left\{ \mathsf{e}_{\sigma^{-1}(1)}, \mathsf{e}_{\sigma^{-1}(2)}, \mathsf{e}_{\sigma^{-1}(3)} \right\}.$$

That is, if $\sigma(I_j) = j$ for $1 \leq j \leq 3$, then $E_\sigma = \{\mathsf{e}_{I_1}, \mathsf{e}_{I_2}, \mathsf{e}_{I_3}\}$. Otherwise stated, if $\mathcal{E}_\sigma = \{\tilde{\mathsf{e}}_1, \tilde{\mathsf{e}}_2, \tilde{\mathsf{e}}_3\}$, then $\mathsf{e}_j = \tilde{\mathsf{e}}_{\sigma(j)}$ for $1 \leq j \leq 3$. It is a fact that $P_\sigma = [\mathrm{id}]_{\mathcal{E}, \mathcal{E}_\sigma}$. For example, if $\sigma = (1\ 2\ 3)$, then $\mathcal{E}_\sigma = \{\mathsf{e}_3, \mathsf{e}_1, \mathsf{e}_2\}$ and

$$P_\sigma = [\mathrm{id}]_{\mathcal{E}, \mathcal{E}_\sigma} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

The following lemma is easily verified.

Lemma 4.1.4 *1. If $[\phi]_{\mathcal{E}} = M$, then $[\phi]_{\mathcal{E}_\sigma} = P_\sigma M P_\sigma^{-1}$.*

2. If $\sigma = \tilde{\omega} \circ \omega$, then $\mathcal{E}_\sigma = (\mathcal{E}_\omega)_{\tilde{\omega}}$ and $P_\sigma = P_{\tilde{\omega}} P_\omega$.

In what follows, the groups $\mathcal{C}, \mathcal{C}^*, \mathsf{U}_3, \mathsf{SL}_2, \mathsf{GL}_2, \mathsf{PSL}_2, \mathsf{SL}_3, \mathsf{T}_3$ and D_3 and the inner automorphism $\mathrm{Int}\, y$, defined for a member y of a group G, are as defined in Section 2.2.

The following result is the main theorem of this chapter.

Theorem 4.1.5 *Let $G \subseteq \mathsf{SL}_3$ be an admissible subgroup. Then G is conjugate to exactly one of the following subgroups of SL_3. The subgroups are classified according to Levi decomposition and decomposition of a reductive group into product of torus and semisimple group; they are also classified in Table 4.1 below by number of invariant subspaces of $\mathcal{C}^3$ of dimension 1 (resp., 2), denoted n_1 (resp., n_2). Assume $G = R_u P$ is a Levi decomposition with P (resp., R_u) a maximal reductive subgroup (resp., the unipotent radical) of G; $H = (P, P)$ is semisimple and $T = Z(P)^\circ$ is a torus.*

1. *Subgroups satisfying $H \simeq 1$.*

   (a) *Subgroups satisfying $T \simeq 1 : \{\mathrm{diag}(1,1,1)\}$. Here, we have $G \simeq \{1\}$ and $n_1 = n_2 = \infty$.*

   (b) *Subgroups satisfying $T \simeq \mathcal{C}^*$.*

      i. *Subgroups satisfying $R_u \simeq 0 : T_{(d_1,d_2)}$. Here, we have $G \simeq \mathcal{C}^*$. If $d_1 > d_2$, then $n_1 = n_2 = 3$; otherwise, $n_1 = n_2 = \infty$.*

      ii. *Subgroups satisfying $R_u \simeq \mathcal{C}$:*

         A. $U^1_{(0,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$, $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1,d_2) = 1, \sigma \in S_3$, $\sigma \in \{\mathrm{id}, (1\ 2), (2\ 3)\}$ *if* $(d_1,d_2) = (1,0)$. *In this case, we have $G \simeq \mathcal{C} \rtimes \mathcal{C}^*$ with*

$$(\mathrm{Int}\, y)(x) = y^{d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(3)}} x \textit{ for } y \in \mathcal{C}^*, x \in \mathcal{C};$$

         we also have $n_1 = n_2 = 2$.

         B. $U^1_{(1,1)} \cdot T_{(1,0)}$. *In this case, we have $G \simeq \mathcal{C} \rtimes \mathcal{C}^*$ with*

$$(\mathrm{Int}\, y)(x) = yx \textit{ for } y \in \mathcal{C}^*, x \in \mathcal{C};$$

         we also have $n_1 = n_2 = 1$.

         C. $U^1_{(0,0)} \cdot T_{(1,1)}$. *In this case, we have $G \simeq \mathcal{C} \rtimes \mathcal{C}^*$ with*

$$(\mathrm{Int}\, y)(x) = y^3 x \textit{ for } y \in \mathcal{C}^*, x \in \mathcal{C};$$

         we also have $n_1 = \infty, n_2 = 2$.

         D. $U^1_{(0,0)} \cdot P_{(1\ 3)} T_{(1,1)} P^{-1}_{(1\ 3)}$. *In this case, we have $G \simeq \mathcal{C} \rtimes \mathcal{C}^*$ with*

$$(\mathrm{Int}\, y)(x) = y^{-3} x \textit{ for } y \in \mathcal{C}^*, x \in \mathcal{C};$$

         we also have $n_1 = 2, n_2 = \infty$.

iii. Subgroups satisfying $R_u \simeq \mathcal{C}^2$:

A. $U^2_{(1,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$, *where* $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1,d_2) = 1$, *and* $\sigma \in \{\mathrm{id}, (1\ 2), (1\ 2\ 3)\}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)(w,x) = (y^{d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(2)}} w, y^{d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(3)}} x)$$

for $y \in \mathcal{C}^*, (w,x) \in \mathcal{C}^2$; *we also have* $n_1 = 1, n_2 = 2$.

B. $U^2_{(0,1)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$, *where* $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1,d_2) = 1$, *and* $\sigma \in \{\mathrm{id}, (2\ 3), (1\ 3\ 2)\}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)(w,x) = (y^{d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(3)}} w, y^{d_{\sigma^{-1}(2)} - d_{\sigma^{-1}(3)}} x)$$

for $y \in \mathcal{C}^*, (w,x) \in \mathcal{C}^2$; *we also have* $n_1 = 2, n_2 = 1$.

C. $U^2_{(1,1)} \cdot T_{(1,0)}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)(w,x) = (yw, y^2 x) \text{ for } y \in \mathcal{C}^*, (w,x) \in \mathcal{C}^2;$$

we also have $n_1 = n_2 = 1$.

D. $U^2_{(1,0)} \cdot P_{(1\ 3)} T_{(1,1)} P^{-1}_{(1\ 3)}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)(w,x) = (y^{-3} w, y^{-3} x) \text{ for } y \in \mathcal{C}^*, (w,x) \in \mathcal{C}^2;$$

we also have $n_1 = 1, n_2 = \infty$.

E. $U^2_{(0,1)} \cdot T_{(1,1)}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)(w,x) = (y^3 w, y^3 x) \text{ for } y \in \mathcal{C}^*, (w,x) \in \mathcal{C}^2;$$

we also have $n_1 = \infty, n_2 = 1$.

iv. Subgroups satisfying $R_u \simeq \mathsf{U}_3$:

A. $\mathsf{U}_3 \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$, $d_1 > d_2 \geq 0$, $\mathrm{GCD}(d_1,d_2) = 1$, $\sigma \in S_3$, $\sigma \in \{\mathrm{id}, (1\ 2), (2\ 3)\}$ *if* $(d_1,d_2) = (1,0)$. *We have* $G \simeq \mathsf{U}_3 \rtimes \mathcal{C}^*$ *with*

$$(\mathrm{Int}\, y)\left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & y^{\kappa_1} v & y^{\kappa_2} w \\ 0 & 1 & y^{\kappa_3} x \\ 0 & 0 & 1 \end{bmatrix},$$

where $\kappa_1 = d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(2)}, \kappa_2 = d_{\sigma^{-1}(1)} - d_{\sigma^{-1}(3)}$,
$\kappa_3 = d_{\sigma^{-1}(2)} - d_{\sigma^{-1}(3)}$, *for*

$$y \in \mathcal{C}^*, \begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3;$$

we also have $n_1 = n_2 = 1$.

B. $\mathsf{U}_3 \cdot P_{(2\ 3)} T_{(1,1)} P_{(2\ 3)}^{-1}$. *We have* $G \simeq \mathsf{U}_3 \rtimes \mathcal{C}^*$ *with*

$$(\operatorname{Int} y)\left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & y^3 v & w \\ 0 & 1 & y^{-3} x \\ 0 & 0 & 1 \end{bmatrix}$$

for

$$y \in \mathcal{C}^*, \begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3;$$

we also have $n_1 = n_2 = 1$.

(c) *Subgroups satisfying* $T \simeq \mathcal{C}^* \times \mathcal{C}^*$.

i. *Subgroups satisfying* $R_u \simeq 0$: $\mathsf{D}_3 \cap \mathsf{SL}_3$. *Here, we have* $G \simeq \mathcal{C}^* \times \mathcal{C}^*$ *and* $n_1 = n_2 = 3$.

ii. *Subgroups satisfying* $R_u \simeq \mathcal{C}$: $U^1_{(0,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$. *Here, we have* $G \simeq \mathcal{C} \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$ *with*

$$(\operatorname{Int}(y_1, y_2))(x) = y_1^2 y_2 x \text{ for } y_1, y_2 \in \mathcal{C}^*, x \in \mathcal{C};$$

we also have $n_1 = n_2 = 2$.

iii. *Subgroups satisfying* $R_u \simeq \mathcal{C}^2$:

A. $U^2_{(1,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$ *with*

$$(\operatorname{Int}(y_1, y_2))(w, x) = (y_1 y_2^{-1} w, y_1^2 y_2 x) \text{ for } y_1, y_2 \in \mathcal{C}^*, w, x \in \mathcal{C};$$

we also have $n_1 = 1, n_2 = 2$.

B. In this case, we have $G \simeq \mathcal{C}^2 \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$ *with*

$$(\operatorname{Int}(y_1, y_2))(w, x) = (y_1^2 y_2 w, y_1 y_2^2 x) \text{ for } y_1, y_2 \in \mathcal{C}^*, w, x \in \mathcal{C};$$

we also have $n_1 = 2, n_2 = 1$.

iv. *Subgroups satisfying* $R_u \simeq \mathsf{U}_3$: $\mathsf{T}_3 \cap \mathsf{SL}_3$. *Here, we have* $G \simeq \mathsf{U}_3 \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$ *with*

$$(\operatorname{Int}(y_1, y_2))\left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & y_1 y_2^{-1} v & y_1^2 y_2 w \\ 0 & 1 & y_1 y_2^2 x \\ 0 & 0 & 1 \end{bmatrix}$$

for

$$y_1, y_2 \in \mathcal{C}^*, \begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3;$$

we also have $n_1 = n_2 = 1$.

2. *Subgroups satisfying* $H \simeq \mathsf{SL}_2$.

   (a) *Subgroups satisfying* $T \simeq 1$.

      i. *Subgroups satisfying* $R_u \simeq 0$:

      $$(t_{ij}) \in \mathsf{SL}_3 : t_{13} = t_{23} = t_{31} = t_{32} = 0, t_{33} = 1.$$

      We have $G \simeq \mathsf{SL}_2$ *and* $n_1 = n_2 = 1$.

      ii. *Subgroups satisfying* $R_u \simeq \mathcal{C}^2$:

         A. $\{(t_{ij}) \in \mathsf{SL}_3 : t_{31} = t_{32} = 0, t_{33} = 1\}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathsf{SL}_2$ *with conjugation given by the unique irreducible representation of* SL_2 *on* $\mathcal{C}^2$; *we also have* $n_1 = 0, n_2 = 1$.

         B. $\{(t_{ij}) \in \mathsf{SL}_3 : t_{21} = t_{31} = 0, t_{11} = 1\}$. *In this case, we have* $G \simeq \mathcal{C}^2 \rtimes \mathsf{SL}_2$ *with conjugation given by the unique irreducible representation of* SL_2 *on* $\mathcal{C}^2$; *we also have* $n_1 = 1, n_2 = 0$.

   (b) *Subgroups satisfying* $T \simeq \mathcal{C}^*$.

      i. *Subgroups satisfying* $R_u \simeq 0$:

      $$\{(t_{ij}) \in \mathsf{SL}_3 : t_{13} = t_{23} = t_{31} = t_{32} = 0\}.$$

      We have $G \simeq \mathsf{GL}_2$ *and* $n_1 = n_2 = 1$.

      ii. *Subgroups satisfying* $R_u \simeq \mathcal{C}^2$:

         A. $\{(t_{ij}) \in \mathsf{SL}_3 : t_{31} = t_{32} = 0\}$. *We have* $G \simeq \mathcal{C}^2 \rtimes \mathsf{GL}_2$ *with conjugation given by*

         $$M.v = (\det M)Mv \text{ for } M \in \mathsf{GL}_2, v \in \mathcal{C}^2;$$

         we also have $n_1 = 0, n_2 = 1$.

         B. $\{(t_{ij}) \in \mathsf{SL}_3 : t_{21} = t_{31} = 0\}$. *We have* $G \simeq \mathcal{C}^2 \rtimes \mathsf{GL}_2$ *with conjugation given by*

         $$M.v = (\det M)^{-1}(M^{-1})^T v \text{ for } M \in \mathsf{GL}_2, v \in \mathcal{C}^2;$$

         we also have $n_1 = 1, n_2 = 0$.

3. Subgroups satisfying $H \simeq \mathsf{PSL}_2$:

$$\{(t_{ij}) \in \mathsf{SL}_3 : \quad t_{12}^2 = t_{11}t_{13},\ t_{21}^2 = 4t_{11}t_{31},\ t_{23}^2 = 4t_{13}t_{33},$$
$$t_{32}^2 = t_{31}t_{33},\ (t_{22}+1)^2 = 4t_{11}t_{33}, (t_{22}-1)^2 = 4t_{13}t_{31}\}.$$

We have $G \simeq \mathsf{PSL}_2$ and $n_1 = n_2 = 0$.

4. Subgroups satisfying $H \simeq \mathsf{SL}_3$: In this case we have $G = \mathsf{SL}_3$ and $n_1 = n_2 = 0$.

n_2	0	1	2	3	∞
n_1 0	PSL_2, SL_3	$\mathcal{C}^2 \rtimes \mathsf{SL}_2$, $\mathcal{C}^2 \rtimes \mathsf{GL}_2$			
1	$\mathcal{C}^2 \rtimes \mathsf{SL}_2$, $\mathcal{C}^2 \rtimes \mathsf{GL}_2$	$\mathcal{C} \rtimes \mathcal{C}^*$ $\mathcal{C}^2 \rtimes \mathcal{C}^*$ $\mathsf{U}_3 \rtimes \mathcal{C}^*$ $\mathsf{T}_3 \cap \mathsf{SL}_3$ SL_2 GL_2	$\mathcal{C}^2 \rtimes \mathcal{C}^*$ $\mathcal{C}^2 \rtimes \mathcal{C}^{*2}$		$\mathcal{C}^2 \rtimes \mathcal{C}^*$
2		$\mathcal{C}^2 \rtimes \mathcal{C}^*$ $\mathcal{C}^2 \rtimes \mathcal{C}^{*2}$	$\mathcal{C} \rtimes \mathcal{C}^*$ $\mathcal{C} \rtimes \mathcal{C}^{*2}$		$\mathcal{C} \rtimes \mathcal{C}^*$
3				$\mathcal{C}^*$ $\mathcal{C}^{*2}$	
∞		$\mathcal{C}^2 \rtimes \mathcal{C}^*$	$\mathcal{C} \rtimes \mathcal{C}^*$		$\mathcal{C}^*$ $\{1\}$

Table 4.1: Admissible subgroups of SL_3. "$\mathcal{C}^{*2}$" stands for $\mathcal{C}^* \times \mathcal{C}^*$.

Below, in Section 4.2 (resp., Section 4.3; Section 4.4), we enumerate the ways in which tori (resp., unipotent groups; semisimple groups) can be embedded in SL_3, up to conjugation. Then, in Section 4.5, we prove Theorem 4.1.5, primarily by considering the ways in which an admissible subgroup can be built from a torus, a semisimple group and a unipotent group. In Section 4.6, we give an algorithm to compute the group of $D^3 + aD + b, a, b \in \mathcal{C}[x]$. The main step of this algorithm relies on Theorem 4.1.5.

4.2 Tori embedded in SL_3

Lemma 4.2.1 *The only (algebraic group) endomorphisms of $\mathcal{C}^*$ are the maps $x \mapsto x^d, d \in \mathbb{Z}$. The only automorphisms of $\mathcal{C}^*$ are the identity and the map $x \mapsto x^{-1}$.*

Proof. The first statement is an easy exercise in the theory of rational functions on $\mathbb{P}^1$. The second statement follows easily from the first statement.

■

Throughout the remainder of this section, $V = \mathcal{C}^3$ is a three-dimensional vector space with fixed basis $\mathcal{E}_0 = \{\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3\}$; this yields a bijection between GL_3 and $\mathsf{GL}(V)$.

Lemma 4.2.2 *Assume $\mathsf{G} \subseteq \mathsf{SL}(V)$ and $\mathcal{F}$ is a basis of V. Let n_i be the number of i-dimensional G-invariant subspaces of V for $i = 1, 2$.*

1. *Define $T_{(d_1,d_2)} = \left\{(t_{ij}) \in \mathsf{D}_3 \cap \mathsf{SL}_3 : t_{11}^{d_2} = t_{22}^{d_1}\right\}, d_1, d_2 \in \mathbb{Z}, d_1 \geq d_2 \geq 0, d_1 > 0$, $\mathrm{GCD}(d_1, d_2) = 1$, and assume $[\mathsf{G}]_{\mathcal{F}} = T_{(d_1,d_2)}$. Then, the following statements hold:*

   (a) $T_{(d_1,d_2)}$ has a faithful parameterization

   $$y \mapsto \mathrm{diag}(y^{d_1}, y^{d_2}, y^{-d_1-d_2}), y \in \mathcal{C}^*,$$

   so in particular $T_{(d_1,d_2)} \simeq \mathcal{C}^*$.

   (b) If $d_1 > d_2$, then the only G-invariant subspaces of V are $\langle \mathsf{f}_1 \rangle, \langle \mathsf{f}_2 \rangle, \langle \mathsf{f}_3 \rangle$, and $\langle \mathsf{f}_i, \mathsf{f}_j \rangle, 1 \leq i < j \leq 3$. In particular, we have $n_1 = n_2 = 3$.

   (c) If $d_1 = d_2 = 1$, then the G-invariant subspaces are $\langle \alpha \mathsf{f}_1 + \beta \mathsf{f}_2 \rangle$, where $(\alpha : \beta) \in \mathbb{P}^1$; $\langle \mathsf{f}_3 \rangle$; $\langle \mathsf{f}_1, \mathsf{f}_2 \rangle$; and $\langle \alpha \mathsf{f}_1 + \beta \mathsf{f}_2, \mathsf{f}_3 \rangle$, where $(\alpha : \beta) \in \mathbb{P}^1$. In particular, we have $n_1 = n_2 = \infty$.

2. *The group $\mathsf{D}_3 \cap \mathsf{SL}_3$ has a faithful parameterization*

   $$(y, z) \mapsto \mathrm{diag}(y, z, (yz)^{-1}), y, z \in \mathcal{C}^*,$$

   so in particular it is isomorphic to $\mathcal{C}^* \times \mathcal{C}^*$. If $[\mathsf{G}]_{\mathcal{F}} = \mathsf{D}_3 \cap \mathsf{SL}_3$, then the G-invariant subspaces are $\langle \mathsf{f}_1 \rangle, \langle \mathsf{f}_2 \rangle, \langle \mathsf{f}_3 \rangle$, and $\langle \mathsf{f}_i, \mathsf{f}_j \rangle, 1 \leq i < j \leq 3$. In particular, we have $n_1 = n_2 = 3$.

Proof. A set of straightforward calculations verifies that each of the given parameterizations is correct for the corresponding algebraic group. The statements about invariant subspaces follow from further calculations. We remark that in the case of $T_{(d_1,d_2)}$, the three integers d_1, d_2 and $-d_1 - d_2$ are distinct if $d_1 \neq d_2$.

■

Lemma 4.2.3 *If $G = [\mathsf{G}]_{\mathcal{E}_0} \subseteq \mathsf{SL}_3$ is isomorphic to a torus, then there exist a basis $\mathcal{F} = \{\mathsf{f}_1, \mathsf{f}_2, \mathsf{f}_3\}$ of V and a unique subgroup $\hat{G} \subseteq \mathsf{SL}_3$ such that $\hat{G} = [\mathsf{G}]_{\mathcal{F}}$ and $\hat{G}$ is one of the following groups:*

1. $1 = \{\mathrm{diag}(1,1,1)\}$.
2. $T_{(d_1,d_2)} \simeq \mathcal{C}^*, d_1, d_2 \in \mathbb{Z}, d_1 \geq d_2 \geq 0, d_1 > 0, \mathrm{GCD}(d_1, d_2) = 1$.
3. $\mathsf{D}_3 \cap \mathsf{SL}_3 \simeq \mathcal{C}^* \times \mathcal{C}^*$.

Proof. It is known ([HK71]) that a commuting group of diagonalizable operators can be simultaneously diagonalized. We may therefore assume that $G \subseteq \mathsf{D}_3$. Since $\mathsf{SL}_3 \cap \mathsf{D}_3 \simeq \mathcal{C}^* \times \mathcal{C}^*$, it follows that G is isomorphic to a torus of dimension at most 2.

Suppose $G \simeq \mathcal{C}^*$. Let $\phi : \mathcal{C}^* \to G$ be an isomorphism. It follows from Lemma 4.2.1 and the fact that $\mathsf{D}_3 \simeq \mathcal{C}^* \times \mathcal{C}^* \times \mathcal{C}^*$ that there exist integers d_1, d_2, d_3 such that $\phi(y) = \mathrm{diag}(y^{d_1}, y^{d_2}, y^{d_3})$ for all $y \in \mathcal{C}^*$. Note that $\phi(\zeta) = \mathrm{diag}(1,1,1)$ if ζ is a dth root of unity, where d is a common divisor of d_1, d_2, d_3. It follows that $\mathrm{GCD}(d_1, d_2, d_3) = 1$. Since $G \subseteq \mathsf{SL}_3$, we also have $d_1 + d_2 + d_3 = 0$. Let σ be the automorphism of $\mathcal{C}^*$ given by $\sigma(x) = x^{-1}$. We have

$$(\phi \circ \sigma)(x) = \mathrm{diag}(x^{-d_1}, x^{-d_2}, x^{-d_3}),\ x \in \mathcal{C}^*.$$

After replacing ϕ with $\phi \circ \sigma$ if necessary, we may assume that two of $\{d_1, d_2, d_3\}$ are nonnegative. After reordering indices if necessary, we may assume that $d_1 \geq d_2 \geq 0 > d_3$. If $d_2 = 0$, then $G = T_{(1,0)}$. If $d_1 = d_2$, then $G = T_{(1,1)}$. Otherwise, $G = T_{(d_1,d_2)}$ with $d_1 > d_2 > 0$.

Next we show that the subgroups $T_{(d_1,d_2)}$ are distinct. Let $T_{(d_1,d_2)}, T_{(\hat{d}_1,\hat{d}_2)}$ be two such subgroups. Define $\phi, \hat{\phi} : \mathcal{C}^* \to \mathsf{SL}_3 \cap \mathsf{D}_3$ by

$$\phi(y) = \mathrm{diag}(y^{d_1}, y^{d_2}, y^{-d_1-d_2}), \hat{\phi}(y) = \mathrm{diag}(y^{\hat{d}_1}, y^{\hat{d}_2}, y^{-\hat{d}_1-\hat{d}_2}),$$

and suppose that $\phi(\mathcal{C}^*) = \hat{\phi}(\mathcal{C}^*)$. It follows that $\phi^{-1} \circ \hat{\phi}$ is an automorphism of $\mathcal{C}^*$. If this map is the identity, then $\phi = \hat{\phi}$. Otherwise, by Lemma 4.2.1, $\phi^{-1} \circ \hat{\phi}$ is the inverse map σ, i.e., $\hat{\phi} = \phi \circ \sigma$. This implies $(d_1, d_2, -d_1 - d_2) = -(\hat{d}_1, \hat{d}_2, -\hat{d}_1 - \hat{d}_2) \in \mathbb{Z}^3$, a contradiction since $d_1, \hat{d}_1 > 0$. We conclude that any two of these parameterizations have distinct images in $\mathsf{D}_3 \cap \mathsf{SL}_3$, and the $T_{(d_1,d_2)}$ are distinct.

It remains to be shown that no two of these subgroups are conjugate. Suppose $T_{(d_1,d_2)}$ and $T_{\left(\tilde{d}_1,\tilde{d}_2\right)}$ are conjugate. Then there exist a basis $\tilde{\mathcal{E}} = \{\tilde{\mathsf{e}}_1, \tilde{\mathsf{e}}_2, \tilde{\mathsf{e}}_3\}$ and a subgroup $\mathsf{G} \subseteq \mathsf{GL}(V)$ such that $T_{(d_1,d_2)} = [\mathsf{G}]_{\mathcal{E}_0}, T_{\left(\tilde{d}_1,\tilde{d}_2\right)} = [\mathsf{G}]_{\tilde{\mathcal{E}}}$. Let $T_{(d_1,d_2)}$ (resp., $T_{\left(\tilde{d}_1,\tilde{d}_2\right)}$) have the parameterization $y \overset{\phi}{\mapsto} \operatorname{diag}\left(y^{d_1}, y^{d_2}, y^{-d_1-d_2}\right)$ (resp., $z \overset{\tilde{\phi}}{\mapsto} \operatorname{diag}\left(z^{\tilde{d}_1}, z^{\tilde{d}_2}, z^{-\tilde{d}_1-\tilde{d}_2}\right)$). Let $P = [\mathrm{id}]_{\mathcal{E}_0,\tilde{\mathcal{E}}}$; define $\omega : \mathsf{GL}_3 \to \mathsf{GL}_3$ by $\omega(M) = PMP^{-1}$, so that $\omega(T_{(d_1,d_2)}) = T_{\left(\tilde{d}_1,\tilde{d}_2\right)}$. Then the map $\tau = \tilde{\phi}^{-1} \circ \omega \circ \phi$ is an automorphism of $\mathcal{C}^*$. As above, Lemma 4.2.1 implies that either $\tau = \mathrm{id}$ or $\tau = \sigma$. We may replace $\tilde{\phi}$ with $\tilde{\phi} \circ \sigma$ if necessary so that $\tau = \mathrm{id}$. This implies that $\tilde{\phi} = \omega \circ \phi$, i.e.,

$$\operatorname{diag}(y^{\tilde{d}_1}, y^{\tilde{d}_2}, y^{-\tilde{d}_1-\tilde{d}_2}) = P \operatorname{diag}(y^{d_1}, y^{d_2}, y^{-d_1-d_2})P^{-1} \text{ for all } y \in \mathcal{C}^*.$$

Now, if V includes infinitely many one-dimensional G-invariant subspaces, then it is easy to see that $T_{(d_1,d_2)} = T_{\left(\tilde{d}_1,\tilde{d}_2\right)} = T_{(1,1)}$. Therefore, we may assume that V includes exactly three one-dimensional G-invariant subspaces. It follows that

$$\tilde{\mathsf{e}}_1 = c_1\mathsf{e}_{j_1}, \tilde{\mathsf{e}}_2 = c_2\mathsf{e}_{j_2}, \tilde{\mathsf{e}}_3 = c_3\mathsf{e}_{j_3}$$

where the c_j are nonzero constants and the ordered 3-tuple (j_1, j_2, j_3) is a permutation of $(1, 2, 3)$. This implies that the change-of-coordinates matrix P is a product of a diagonal matrix by a permutation matrix. From this, we see that

$$\operatorname{diag}(y^{\tilde{d}_1}, y^{\tilde{d}_2}, y^{-\tilde{d}_1-\tilde{d}_2}) = \operatorname{diag}(y^{\bar{d}_1}, y^{\bar{d}_2}, y^{\bar{d}_3})$$

for all $y \in \mathcal{C}^*$, where the ordered 3-tuple $\left(\bar{d}_1, \bar{d}_2, \bar{d}_3\right)$ is a permutation of the ordered 3-tuple $(d_1, d_2, d_3), d_3 = -d_1 - d_2$. This yields $\bar{d}_i = \tilde{d}_i$ for $1 \le i \le 3$. Since $d_1 > d_2 > 0$ and $\tilde{d}_1 > \tilde{d}_2 > 0$, we see that $(d_1, d_2) = (\tilde{d}_1, \tilde{d}_2)$, so that the parameterizations and in particular their images are identical.

Finally, suppose $G \simeq \mathcal{C}^* \times \mathcal{C}^*$. Then $G \subseteq \mathsf{D}_3$ is a two-dimensional connected subgroup of the two-dimensional torus $\mathsf{SL}_3 \cap \mathsf{D}_3$ and therefore must be all of $\mathsf{SL}_3 \cap \mathsf{D}_3$.

■

4.3 Unipotent subgroups of SL_3

As in the previous section, $V = \mathcal{C}^3$ is a three-dimensional vector space with fixed basis $\mathcal{E}_0 = \{\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3\}$, yielding a bijection between GL_3 and $\mathsf{GL}(V)$.

Lemma 4.3.1 *Assume $\mathsf{G} \subseteq \mathsf{SL}(V)$ and $\mathcal{B}$ is a basis of V.*

1. *Define* $U^1_{(0,0)} = \{(t_{ij}) \in \mathsf{U}_3 : t_{12} = 0, t_{23} = 0\}$.

   (a) $U^1_{(0,0)}$ *has a faithful parameterization*

$$x \mapsto \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, x \in \mathcal{C},$$

   so in particular $U^1_{(0,0)} \simeq \mathcal{C}$.

   (b) *If* $[\mathsf{G}]_{\mathcal{B}} = U^1_{(0,0)}$, *then the* G*-invariant subspaces of* V *are:*

   - $\langle \alpha \mathsf{b}_1 + \beta \mathsf{b}_2 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1(\mathcal{C})$; *fixed elementwise*
   - $\langle \mathsf{b}_1, \mathsf{b}_2 \rangle$; *fixed elementwise*
   - $\langle \mathsf{b}_1, \gamma \mathsf{b}_2 + \mathsf{b}_3 \rangle$, *where* $\gamma \in \mathcal{C}$.

2. *Define* $U^1_{(1,1)} = \left\{(t_{ij}) \in \mathsf{U}_3 : t_{12} = t_{23}, t_{13} = \frac{1}{2} t_{12}^2\right\}$.

   (a) $U^1_{(1,1)}$ *has a faithful parameterization*

$$x \mapsto \begin{bmatrix} 1 & x & \frac{1}{2}x^2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} : x \in \mathcal{C},$$

   so in particular $U^1_{(1,1)} \simeq \mathcal{C}$.

   (b) *If* $[\mathsf{G}]_{\mathcal{B}} = U^1_{(1,1)}$, *then the* G*-invariant subspaces of* V *are* $\langle \mathsf{b}_1 \rangle$ *and* $\langle \mathsf{b}_1, \mathsf{b}_2 \rangle$.

3. *Define* $U^2_{(1,0)} = \{(t_{ij}) \in \mathsf{U}_3 : t_{23} = 0\}$.

   (a) $U^2_{(1,0)}$ *has a faithful parameterization*

$$(x, y) \mapsto \begin{bmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, x, y \in \mathcal{C},$$

   so in particular $U^2_{(1,0)} \simeq \mathcal{C}^2$.

   (b) *If* $[\mathsf{G}]_{\mathcal{B}} = U^2_{(1,0)}$, *then the* G*-invariant subspaces are* $\langle \mathsf{b}_1 \rangle$ *and* $\langle \mathsf{b}_1, \alpha \mathsf{b}_2 + \beta \mathsf{b}_3 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1(\mathcal{C})$.

4. *Define* $U^2_{(0,1)} = \{(t_{ij}) \in \mathsf{U}_3 : t_{12} = 0\}$.

(a) $U^2_{(0,1)}$ *has a faithful parameterization*

$$(x,y) \mapsto \begin{bmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}, x, y \in \mathcal{C},$$

so in particular $U^2_{(0,1)} \simeq \mathcal{C}^2$.

(b) *If* $[\mathsf{G}]_{\mathcal{B}} = U^2_{(0,1)}$, *then the* G*-invariant subspaces are* $\langle \alpha \mathsf{b}_1 + \beta \mathsf{b}_2 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1(\mathcal{C})$, *and* $\langle \mathsf{b}_1, \mathsf{b}_2 \rangle$, *all fixed elementwise.*

5. *Define* $U^2_{(1,1)} = \{(t_{ij}) \in \mathsf{U}_3 : t_{12} = t_{23}\}$.

(a) $U^2_{(1,1)}$ *has a faithful parameterization*

$$(x,y) \mapsto \begin{bmatrix} 1 & x & y + \frac{1}{2}x^2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}, x, y \in \mathcal{C},$$

so in particular $U^2_{(1,1)} \simeq \mathcal{C}^2$.

(b) *If* $[\mathsf{G}]_{\mathcal{B}} = U^2_{(1,1)}$, *then the* G*-invariant subspaces are* $\langle \mathsf{b}_1 \rangle$ *and* $\langle \mathsf{b}_1, \mathsf{b}_2 \rangle$.

6. *If* $[\mathsf{G}]_{\mathcal{B}} = \mathsf{U}_3$, *then the* G*-invariant subspaces are* $\langle \mathsf{b}_1 \rangle$ *and* $\langle \mathsf{b}_1, \mathsf{b}_2 \rangle$.

The above listed subgroups are pairwise nonconjugate; in particular, they are distinct.

Proof. These statements are verified by straightforward calculations. ∎

We shall see that every nontrivial unipotent subgroup of SL_3 is conjugate to one of the groups listed above. First we need two technical lemmas.

Lemma 4.3.2 *Given a nontrivial matrix*

$$M = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3, \tag{4.1}$$

then the group closure of M *in* U_3 *is*

$$\mathrm{clos}(M) = \left\{ (t_{ij}) \in \mathsf{U}_3 : \begin{array}{rcl} ct_{12} - at_{23} & = & 0 \\ \frac{1}{2}at_{12}t_{23} + bt_{12} - at_{13} - \frac{1}{2}a^2 t_{23} & = & 0 \\ \frac{1}{2}ct_{12}t_{23} - \frac{1}{2}c^2 t_{12} - ct_{13} + bt_{23} & = & 0 \end{array} \right\}.$$

Moreover, $\mathrm{clos}(M)$ *has a faithful parameterization*

$$x \mapsto \begin{bmatrix} 1 & xa & xb + \frac{x(x-1)}{2}ac \\ 0 & 1 & xc \\ 0 & 0 & 1 \end{bmatrix}, x \in \mathcal{C},$$

so in particular it is isomorphic to $\mathcal{C}$.

Proof. A sequence of straightforward computations shows that the given set is a group containing M, that it has the given parameterization, and that it is isomorphic to $\mathcal{C}$. The desired result then follows from the fact that $\mathcal{C}$ includes no nontrivial proper closed subgroup.

■

Lemma 4.3.3 *Define* $q : \mathsf{U}_3 \to \mathcal{C}^2$ *by*

$$q\left(\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}\right) = (x, z).$$

Then, the following statements hold:

1. q *is an algebraic group homomorphism with kernel* $U^1_{(0,0)}$.

2. $U^1_{(0,0)}$ *is identical to* $(\mathsf{U}_3, \mathsf{U}_3)$, *the commutator subgroup of* U_3.

3. *Two matrices* $M_1, M_2 \in \mathsf{U}_3$ *commute if and only if there is a one-dimensional subspace of* $\mathcal{C}^2$ *containing both* $q(M_1)$ *and* $q(M_2)$, *i.e.,* $q(M_1)$ *and* $q(M_2)$ *differ by a scalar multiple.*

4. $U^1_{(0,0)}$ *is identical to the center of* U_3.

5. *Given a nontrivial matrix* M *of the form (4.1). Then the centralizer of* M *in* U_3 *is*

$$\underset{\mathsf{U}_3}{\mathrm{Cen}}(M) = \mathrm{clos}(M) \cdot U^1_{(0,0)}.$$

   Moreover, this subgroup is isomorphic to $\mathcal{C}^r$, *where* r *is equal to* 1 *if* $\mathrm{clos}(M) = U^1_{(0,0)}$, 2 *otherwise.*

Proof. Item 1 can be verified by direct computation. The reader can verify that if $M_1 = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$, then

$$M_1 M_2 M_1^{-1} M_2^{-1} = \begin{bmatrix} 1 & 0 & a_1c_2 - c_1a_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \tag{4.2}$$

Items 2 and 3 follow easily from this identity. Item 4 follows easily from Item 3. To prove Item 5, let $\tilde{M} \in \mathsf{U}_3$. Suppose $\tilde{M}$ commutes with M. Then, by Item 3, we have

$$\tilde{M} = \begin{bmatrix} 1 & xa & \tilde{b} \\ 0 & 1 & xc \\ 0 & 0 & 1 \end{bmatrix}$$

for some $x, \tilde{b} \in \mathcal{C}$. Write $\tilde{b} = xb + \frac{x(x-1)}{2}ac + \hat{b},\ \hat{b} \in \mathcal{C}$. It is easy to check that

$$\tilde{M} = \begin{bmatrix} 1 & xa & xb + \frac{x(x-1)}{2}ac \\ 0 & 1 & xc \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & \hat{b} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Consider the right-hand side of this identity. By Lemma 4.3.2, the first matrix is a member of $\mathrm{clos}(M)$; by Lemma 4.3.1, the second matrix is a member of $U^1_{(0,0)}$. Thus, $\tilde{M} \in \mathrm{clos}(M) \cdot U^1_{(0,0)}$; this yields one inclusion. To prove the other inclusion, notice that elements of the group closure $\mathrm{clos}(M)$ commute with M; meanwhile, Item 4 of the lemma implies that $U^1_{(0,0)} \subseteq \mathrm{Cen}_{\mathsf{U}_3}(M)$. Moreover, by Lemma 4.3.2 (resp., Lemma 4.3.1), the subgroup $\mathrm{clos}(M)$ (resp., the subgroup $U^1_{(0,0)}$) is isomorphic to $\mathcal{C}$. The desired result now follows easily.

∎

Lemma 4.3.4 *Let $G = [\mathsf{G}]_{\mathcal{E}_0} \subseteq \mathsf{SL}_3$ be a unipotent group. Let $\mathcal{E}' = \{\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3\}$ be such that $G' = [\mathsf{G}]_{\mathcal{E}'} \subseteq \mathsf{U}_3$. Let $q : \mathsf{U}_3 \to \mathcal{C}^2$ be the map defined in Lemma 4.3.3. Then, exactly one of the following cases holds:*

1. *If $q(G') = \mathcal{C}^2$, then $G' = \mathsf{U}_3$.*

2. *Suppose $q(G') = \langle (a, c) \rangle$ is a one-dimensional vector subgroup of $\mathcal{C}^2$ for some $(a : c) \in \mathbb{P}^1$, and $U^1_{(0,0)} \subseteq G'$.*

(a) *If* $a = 0$, *then* $G' = U^2_{(0,1)}$.

(b) *If* $c = 0$, *then* $G' = U^2_{(1,0)}$.

(c) *If* a *and* c *are nonzero, then there exists a basis* $\mathcal{B}$ *such that* $[\mathsf{G}]_{\mathcal{B}} = U^2_{(1,1)}$.

3. *Suppose* $q(G') = \langle (a,c) \rangle$ *is a one-dimensional vector subgroup of* $\mathcal{C}^2$ *for some* $(a:c) \in \mathbb{P}^1$, *and* $U^1_{(0,0)}$ *is not included in* G'.

(a) *If* $a = 0$ *or* $c = 0$, *then there exists a basis* $\mathcal{B}$ *such that* $[\mathsf{G}]_{\mathcal{B}} = U^1_{(0,0)}$.

(b) *If* a *and* c *are both nonzero, then there exists a basis* $\mathcal{B}$ *such that* $[\mathsf{G}]_{\mathcal{B}} = U^1_{(1,1)}$.

4. *Suppose* $q(G') = 0$. *Then either* $G' = U^1_{(0,0)}$ *or* $G' = 1$.

In particular, if G *is nontrivial, then there exists a basis* $\mathcal{B}$ *and a unique subgroup* $\hat{G}$ *such that* $[\mathsf{G}]_{\mathcal{B}} = \hat{G}$ *and* $\hat{G}$ *is one of the subgroups listed in Lemma 4.3.1.*

Proof.

1. Suppose $q(G') = \mathcal{C}^2$. Let $M_1, M_2 \in G'$ be such that $q(M_1) = (1,0), q(M_2) = (0,1)$. It follows from (4.2) that $M_1 M_2 M_1^{-1} M_2^{-1}$ generates $U^1_{(0,0)}$ and therefore that $U^1_{(0,0)} \subseteq G'$. We now see that the closed subgroup G' is three-dimensional, hence identical to U_3.

To prove Items 2 and 3 of the lemma, suppose $q(G') = \langle (a,c) \rangle$ as stated, and let

$$M = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = [\phi]_{\mathcal{E}'} \in G',$$

where $b \in \mathcal{C}$ and $\phi \in \mathsf{G}$. It follows from Item 3 of Lemma 4.3.3 that G' is abelian; it then follows from Item 5 of that lemma that $G' \subseteq \operatorname{clos}(M) \cdot U^1_{(0,0)}$. Since $\operatorname{clos}(M) \cdot U^1_{(0,0)} \simeq \mathcal{C}^2$ and $M \in \operatorname{clos}(M) \subseteq G'$, we see that G' is either $\operatorname{clos}(M)$ or $\operatorname{clos}(M) \cdot U^1_{(0,0)}$.

2. Suppose $U^1_{(0,0)} \subseteq G'$. Here, we see that $G' = \operatorname{clos}(M) \cdot U^1_{(0,0)} \simeq \mathcal{C}^2$.

(a) If $a = 0$, then it's clear that $G' \subseteq U^2_{(0,1)}$; a dimension count yields equality.

(b) If $c = 0$, then it's clear that $G' \subseteq U^2_{(1,0)}$; a dimension count yields equality.

(c) Assume a and c are nonzero. Write

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [\psi_0]_{\mathcal{E}'}, \ \psi_0 \in \mathsf{G},$$

so in particular ϕ, ψ_0 generate G. We may assume without loss of generality that $a = 1$. Let $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3\}$, where $\mathsf{b}_i = \mathsf{e}'_i$ for $i = 1, 2$ and $\mathsf{b}_3 = c^{-1}\mathsf{e}'_3$. Then, one calculates $[\phi]_{\mathcal{B}} = \begin{bmatrix} 1 & 1 & bc^{-1} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ and $[\psi_0]_{\mathcal{B}} \in U^1_{(0,0)}$. This implies $[\mathsf{G}]_{\mathcal{B}} \subseteq U^2_{(1,1)}$, and a dimension count yields equality.

3. Suppose $U^1_{(0,0)}$ is not included in G'. Here, we see that $G' = \operatorname{clos}(M) \simeq \mathcal{C}$ and that G' (resp., G) is generated by M (resp., ϕ).

   (a) If $a = 0$, then let $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3\}$, where $\mathsf{b}_1 = b\mathsf{e}'_1 + c\mathsf{e}'_2$, $\mathsf{b}_2 = \mathsf{e}'_1$, and $\mathsf{b}_3 = \mathsf{e}'_3$ for $i = 1, 3$. Then, one calculates $[\phi]_{\mathcal{B}} \in U^1_{(0,0)}$, and it follows that $[\mathsf{G}]_{\mathcal{B}} = U^1_{(0,0)}$. If $c = 0$, then let $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3\}$, where $\mathsf{b}_1 = \mathsf{e}'_1, \mathsf{b}_2 = a^{-1}b\mathsf{e}'_2 - \mathsf{e}'_3, \mathsf{b}_3 = \mathsf{e}'_2$. In this case also, one calculates $[\phi]_{\mathcal{B}} \in U^1_{(0,0)}$ and obtains $[\mathsf{G}]_{\mathcal{B}} = U^1_{(0,0)}$.

   (b) If both a and c are nonzero, then we may assume without loss of generality that $a = 1$. Let $\tilde{\mathcal{B}} = \left\{\tilde{\mathsf{b}}_1, \tilde{\mathsf{b}}_2, \tilde{\mathsf{b}}_3\right\}$, where $\tilde{\mathsf{b}}_i = \mathsf{e}'_i$ for $i = 1, 2$ and $\tilde{\mathsf{b}}_3 = c^{-1}\mathsf{e}'_3$. Then one checks that $[\phi]_{\tilde{\mathcal{B}}} = \begin{bmatrix} 1 & 1 & bc^{-1} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Define $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3\}$, where $\mathsf{b}_2 = \tilde{\mathsf{b}}_2 + (bc^{-1} - \frac{1}{2})\tilde{\mathsf{b}}_1$ and $\mathsf{b}_i = \tilde{\mathsf{b}}_i$ for $i = 1, 3$. One calculates

$$[\phi]_{\mathcal{B}} = \begin{bmatrix} 1 & 1 & \frac{1}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

   By Lemmas 4.3.1 and 4.3.2, we see that $U^1_{(1,1)}$ is the group closure of the above matrix; it follows that $[\mathsf{G}]_{\mathcal{B}} = U^1_{(1,1)}$.

4. Item 4 of the lemma follows easily from Item 1 of Lemma 4.3.3.

■

Lemma 4.3.5 *Let $G \subseteq \mathsf{SL}_3$ be one of the two-dimensional unipotent subgroups listed in Lemma 4.3.4.*

1. If $G = U^2_{(1,0)}$, then

$$\operatorname*{Nor}_{\mathsf{GL}_3}(G) = \{(t_{ij}) \in \mathsf{GL}_3 : t_{21} = t_{31} = 0\}$$

and

$$\operatorname*{Nor}_{\mathsf{SL}_3}(G) = \left\{ (t_{ij}) \in \operatorname*{Nor}_{\mathsf{GL}_3}(G) : t_{11}(t_{22}t_{33} - t_{23}t_{32}) = 1 \right\}.$$

2. *If* $G = U^2_{(0,1)}$, *then*

$$\operatorname*{Nor}_{\mathsf{GL}_3}(G) = \{(t_{ij}) \in \mathsf{GL}_3 : t_{31} = t_{32} = 0\}$$

and

$$\operatorname*{Nor}_{\mathsf{SL}_3}(G) = \left\{ (t_{ij}) \in \operatorname*{Nor}_{\mathsf{GL}_3}(G) : (t_{11}t_{22} - t_{12}t_{21})t_{33} = 1 \right\}.$$

3. *If* $G = U^2_{(1,1)}$, *then* $\mathrm{Nor}_{\mathsf{GL}_3}(G) = \mathsf{T}_3$, $\mathrm{Nor}_{\mathsf{SL}_3}(G) = \mathsf{T}_3 \cap \mathsf{SL}_3$.

Proof. These statements are proved by straightforward calculations.

■

4.4 Semisimple subgroups of SL_3

The author would like to thank Mohan Putcha for his help in proving the following lemma.

Lemma 4.4.1 *The only semisimple algebraic groups that can be embedded in* SL_3 *are* SL_2, PSL_2 *and* SL_3.

Proof. This proof relies on results from [FH91] and [Hum81]. The relevant results in [FH91] are stated in [FH91] for the case in which $\mathcal{C} = \mathbb{C}$; these results are known to extend to arbitrary algebraically closed fields of characteristic zero. We will use basic terminology from Lie theory without detailed explanation here, since it is only needed in this section.

Let G be a semisimple group and T a maximal torus of G. Then, the *Weyl group* $\mathcal{W}_G$ is defined in [FH91], Sec. 14.1 to be the group generated by certain vector space involutions on the dual of the Lie algebra of T. G also has a unique *root system* associated to it, and this root system uniquely determines the Weyl group (ibid., Sec. 21.1). It is a fact (ibid, Sec. 23.1) that $\mathcal{W}_G$ is isomorphic to $N_G(T)/T$. If B is a Borel subgroup of G and S is a full set of coset representatives of T in $N_G(T)$, then G has a *Bruhat decomposition* ([Hum81], Sec. 28.3) given by $G = \bigcup_{s \in S} BsB$ (disjoint union).

The group SL_3 has maximal torus $T = \mathsf{D}_3 \cap \mathsf{SL}_3$. Its root system is referred to as (A_2) ([FH91], Sec. 21.1 and 23.1). The reader can verify that $N_{\mathsf{SL}_3}(T)$ is the group of matrices in SL_3 with exactly one nonzero entry in each row (resp., column); it is then easy to show that

$$\mathcal{W}_{\mathsf{SL}_3} \simeq N_{\mathsf{SL}_3}(T)/T \simeq S_3. \tag{4.3}$$

Now, let $G_0 \subseteq \mathsf{SL}_3$ be semisimple, and let T_0 be a maximal torus of G_0. Then T_0 has rank either 1 or 2, i.e., either $T_0 \simeq \mathcal{C}^*$ or $T_0 \simeq \mathcal{C}^* \times \mathcal{C}^*$. In the former case, it follows from (ibid., Sec. 21.1 and 23.1) that G_0 has root system (A_1) and therefore is isomorphic to either SL_2 or PSL_2.

Suppose T_0 has rank 2; we wish to show that $G_0 = \mathsf{SL}_3$. We may assume that T_0 is included in, hence equal to, $\mathsf{D}_3 \cap \mathsf{SL}_3$. Also, by (ibid., Sec. 21.1), the root system of G_0 is one of $(\mathsf{A}_1 \times \mathsf{A}_1),\ (\mathsf{A}_2),\ (\mathsf{B}_2),\ (\mathsf{G}_2)$. By inspection of the diagrams given in (ibid.), the Weyl groups associated to these root systems are dihedral groups of order $4, 6, 8, 12$, respectively.

In our case, we have that $T_0 = T = \mathsf{D}_3 \cap \mathsf{SL}_3$ is the maximal torus of both G_0 and SL_3, so that $\mathcal{W}_{G_0} \simeq N_{G_0}(T)/T$ is isomorphic to a subgroup of $N_{\mathsf{SL}_3}(T)/T$. Of the dihedral groups listed above, the only one whose order divides 6 is the one whose order is exactly 6, i.e., S_3. It now follows from (4.3) that G has root system (A_2), that $\mathcal{W}_{G_0} \simeq \mathcal{W}_{\mathsf{SL}_3}$, and that $N_{G_0}(T) = N_{\mathsf{SL}_3}(T)$.

Since G_0 has the same maximal torus and root system as SL_3, it follows from [Hum81], Sec. 28.1, that G_0 and SL_3 have the same maximal unipotent subgroup U_3 and thus the same Borel subgroup $B = \mathsf{T}_3$. Finally, we see that G_0 and SL_3 have identical Bruhat decompositions, hence are identical.

■

4.5 Admissible subgroups of SL_3

We begin with a technical lemma.

Lemma 4.5.1 *Given:*

- *M is a nontrivial matrix of the form (4.1)*
- *$v \in \mathcal{C}^*$ is a nonroot of unity*
- *d_1, d_2, d_3 are integers such that $d_1 \geq d_2 \geq 0,\ d_1 > 0,\ \mathrm{GCD}(d_1, d_2) = 1,\ d_1 + d_2 + d_3 = 0$*
- *A_1, A_2, A_3 are three distinct integers such that $1 \leq A_i \leq 3$ for $1 \leq i \leq 3$*
- *The matrix Q is given by*

$$Q = \mathrm{diag}\left(v^{d_{A_1}}, v^{d_{A_2}}, v^{d_{A_3}}\right). \tag{4.4}$$

1. *Suppose $QMQ^{-1} \in \mathrm{clos}(M)$. Then, the following statements hold:*

(a) *If* $a = 0, b \neq 0,$ *and* $c \neq 0,$ *then* $d_1 = d_2 = 1$ *and* $A_3 = 3.$

(b) *If* $a \neq 0, b \neq 0,$ *and* $c = 0,$ *then* $d_1 = d_2 = 1$ *and* $A_1 = 3.$

(c) *If* $d_1 > d_2$ *and either* $a = 0$ *or* $c = 0,$ *then two of* $\{a, b, c\}$ *are zero.*

(d) *If* $a \neq 0$ *and* $c \neq 0,$ *then* $d_1 = 1,\ d_2 = 0, A_2 = 2,$ *and* $b = \frac{1}{2}ac.$

2. *Suppose* $QMQ^{-1} \in \mathrm{clos}(M) \cdot U^1_{(0,0)}$ *and* $a \neq 0,\ c \neq 0.$ *Then* $d_1 = 1,\ d_2 = 0,$ *and* $A_2 = 2.$

Proof. We compute

$$QMQ^{-1} = \begin{bmatrix} 1 & v^{d_{A_1} - d_{A_2}} a & v^{d_{A_1} - d_{A_3}} b \\ 0 & 1 & v^{d_{A_2} - d_{A_3}} c \\ 0 & 0 & 1 \end{bmatrix}.$$

Let us first assume that this matrix is a member of $\mathrm{clos}(M)$.

Suppose $a = 0$. Then, by Lemma 4.3.2, there exists $x \in \mathcal{C}$ such that $v^{d_{A_1} - d_{A_3}} b = xb$ and $v^{d_{A_2} - d_{A_3}} c = xc$. If both b and c are nonzero, then $v^{d_{A_1} - d_{A_3}} = x = v^{d_{A_2} - d_{A_3}}$. It quickly follows that $d_{A_1} = d_{A_2}$, which (due to hypotheses on the d_j) implies $d_1 = d_2 = 1$. Also, A_1 (resp., A_2) is either 1 or 2, so that $A_3 = 3$. This proves Item (1a) of the lemma. Item (1b) is proved by similar logic.

Next, suppose $a = 0$ (resp., $c = 0$) and the other two parameters are nonzero. Then Item (1a) (resp., Item (1b)) implies that $d_1 = d_2$. This proves Item (1c) by contrapositive.

Now suppose $a \neq 0$ and $c \neq 0$. In this case, our computation of QMQ^{-1}, together with Lemma 4.3.2, implies that

$$v^{d_{A_1} - d_{A_2}} = x = v^{d_{A_2} - d_{A_3}} \text{ for some } x \in \mathcal{C}. \tag{4.5}$$

This yields $d_{A_1} - 2d_{A_2} + d_{A_3} = 0$, which together with $d_{A_1} + d_{A_2} + d_{A_3} = 0$ implies $d_{A_2} = 0$. The hypotheses on the d_j now easily yield $d_1 = 1, d_2 = 0$. We also have $d_{A_2} = 0,\ d_{A_1} = \epsilon, d_{A_3} = -\epsilon$, where $\epsilon = \pm 1$; this implies $x = v^\epsilon$. Lemma 4.3.2 also implies that the $(1,3)$ coordinate of QMQ^{-1} is

$$v^{d_{A_1} - d_{A_3}} b = xb + \frac{x(x-1)}{2} ac.$$

We may rewrite this identity as

$$v^{2\epsilon} b = v^\epsilon b + \frac{v^{2\epsilon} - v^\epsilon}{2} ac.$$

Item (1d) of the lemma now follows after subtracting $v^\epsilon b$ from both sides and dividing by $v^{2\epsilon} - v^\epsilon$.

To prove Item Two, it follows from Lemma 4.3.3 that

$$\operatorname{clos}(M)\cdot U^1_{(0,0)} = \left\{ \begin{bmatrix} 1 & xa & y \\ 0 & 1 & xc \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathcal{C} \right\}.$$

Therefore, (4.5) holds in this case, and the listed conclusions follow as in the previous case.

■

The following seven lemmas establish conjugacy classes for subgroups having certain Levi decompositions. Lemma 4.5.2 (resp., Lemma 4.5.4; Lemma 4.5.6) enumerates a list of subgroups having trivial semisimple part and describes some of their properties. Lemma 4.5.3 (resp., Lemma 4.5.5; Lemma 4.5.7) shows that these subgroups form a set of conjugacy class representatives. Lemma 4.5.8 addresses the case in which the reductive part is either SL_2 or GL_2 and the unipotent radical is $\mathcal{C}^2$. In each lemma, n_i is the number of i-dimensional G-invariant subspaces for $i = 1, 2$.

Lemma 4.5.2 *Given $G = [\mathsf{G}]_{\mathcal{A}} \subseteq \mathsf{SL}_3$, where G is a subgroup of $\mathsf{SL}_3(V)$ and $\mathcal{A} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3\}$ is a basis of V.*

1. *Suppose $G = U^1_{(0,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}, d_1 > d_2 \geq 0, \mathrm{GCD}(d_1, d_2) = 1, \sigma \in S_3, \sigma \in \{\mathrm{id}, (1\ 2), (2\ 3)\}$ if $(d_1, d_2) = (1, 0)$. Then G has a faithful parameterization*

$$(x, y) \mapsto \begin{bmatrix} y^{d_{I_1}} & 0 & x \\ 0 & y^{d_{I_2}} & 0 \\ 0 & 0 & y^{d_{I_3}} \end{bmatrix},$$

   where $d_3 = -d_1 - d_2$ and $\sigma(I_j) = j$ for $1 \leq j \leq 3$. Under this parameterization, we have $(\mathrm{Int}\, y)(x) = y^{d_{I_1} - d_{I_3}} x$. Moreover, the G-invariant subspaces of V are $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_2 \rangle, \langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_3 \rangle$, so that $n_1 = n_2 = 2$.

2. *Suppose $G = U^1_{(1,1)} \cdot T_{(1,0)}$. Then G has a faithful parameterization*

$$(x, y) \mapsto \begin{bmatrix} y & x & \frac{1}{2}x^2 \\ 0 & 1 & x \\ 0 & 0 & y^{-1} \end{bmatrix}.$$

   Under this parameterization, we have $(\mathrm{Int}\, y)(x) = yx$. The G-invariant subspaces are $\langle \mathsf{a}_1 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, so that $n_1 = n_2 = 1$.

3. *Suppose* $G = U^1_{(0,0)} \cdot T_{(1,1)}$. *Then* G *has a faithful parameterization*

$$(x,y) \mapsto \begin{bmatrix} y & 0 & x \\ 0 & y & 0 \\ 0 & 0 & y^{-2} \end{bmatrix}$$

under which $(\operatorname{Int} y)(x) = y^3 x$. *The* G-*invariant subspaces are* $\langle \alpha \mathsf{a}_1 + \beta \mathsf{a}_2 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1$; $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$; *and* $\langle \mathsf{a}_1, \mathsf{a}_3 \rangle$. *Thus, we have* $n_1 = \infty, n_2 = 2$.

4. *Suppose* $G = U^1_{(0,0)} \cdot P_{(1\ 3)} T_{(1,1)} P^{-1}_{(1\ 3)}$. *Then* G *has a faithful parameterization*

$$(x,y) \mapsto \begin{bmatrix} y^{-2} & 0 & x \\ 0 & y & 0 \\ 0 & 0 & y \end{bmatrix}$$

under which $(\operatorname{Int} y)(x) = y^{-3} x$. *The* G-*invariant subspaces are* $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_2 \rangle$, *and*

$$\langle \mathsf{a}_1, \alpha \mathsf{a}_2 + \beta \mathsf{a}_3 \rangle, (\alpha : \beta) \in \mathbb{P}^1.$$

Thus, we have $n_1 = 2, n_2 = \infty$.

5. *Suppose* $G = U^2_{(1,0)} \cdot P_\sigma T_{(d_1,d_2)} P^{-1}_\sigma$, *where* $d_1 > d_2 \geq 0, \operatorname{GCD}(d_1, d_2) = 1$, *and* $\sigma \in \{\mathrm{id}, (1\ 2), (1\ 2\ 3)\}$. *This group has a faithful parameterization*

$$(w,x,y) \mapsto \begin{bmatrix} y^{d_{I_1}} & w & x \\ 0 & y^{d_{I_2}} & 0 \\ 0 & 0 & y^{d_{I_3}} \end{bmatrix},$$

where $d_3 = -d_1 - d_2$ *and* $\sigma(I_j) = j$ *for* $1 \leq j \leq 3$. *Under this parameterization, we have* $(\operatorname{Int} y)(w,x) = (y^{d_{I_1} - d_{I_2}} w, y^{d_{I_1} - d_{I_3}} x)$. *The* G-*invariant subspaces are* $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ *and* $\langle \mathsf{a}_1, \mathsf{a}_3 \rangle$, *so that* $n_1 = 1, n_2 = 2$.

6. *Suppose* $G = U^2_{(0,1)} \cdot P_\sigma T_{(d_1,d_2)} P^{-1}_\sigma$, *where* $d_1 > d_2 \geq 0, \operatorname{GCD}(d_1, d_2) = 1$, *and* $\sigma \in \{\mathrm{id}, (2\ 3), (1\ 3\ 2)\}$. *Then* G *has a faithful parameterization*

$$(w,x,y) \mapsto \begin{bmatrix} y^{d_{I_1}} & 0 & w \\ 0 & y^{d_{I_2}} & x \\ 0 & 0 & y^{d_{I_3}} \end{bmatrix},$$

where $d_3 = -d_1 - d_2$ *and* $\sigma(I_j) = j$ *for* $1 \leq j \leq 3$. *Under this parameterization, we have* $(\operatorname{Int} y)(w,x) = (y^{d_{I_1} - d_{I_3}} w, y^{d_{I_2} - d_{I_3}} x)$. *The* G-*invariant subspaces are* $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_2 \rangle$ *and* $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, *so that* $n_1 = 2, n_2 = 1$.

7. *Suppose* $G = U^2_{(1,1)} \cdot T_{(1,0)}$. *Then* G *has a faithful parameterization*

$$(w, x, y) \mapsto \begin{bmatrix} y & w & x + \frac{1}{2}w^2 \\ 0 & 1 & w \\ 0 & 0 & y^{-1} \end{bmatrix}.$$

   Under this parameterization, we have $(\operatorname{Int} y)(w, x) = (yw, y^2 x)$. *The* G*-invariant subspaces are* $\langle \mathsf{a}_1 \rangle$ *and* $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, *so that* $n_1 = n_2 = 1$.

8. *Suppose* $G = U^2_{(1,0)} \cdot P_{(1\ 3)} T_{(1,1)} P^{-1}_{(1\ 3)}$. *Then* G *has a faithful parameterization*

$$(w, x, y) \mapsto \begin{bmatrix} y^{-2} & w & x \\ 0 & y & 0 \\ 0 & 0 & y \end{bmatrix}.$$

   Under this parameterization, we have $(\operatorname{Int} y)(w, x) = (y^{-3} w, y^{-3} x)$. *The* G*-invariant subspaces are* $\langle \mathsf{a}_1 \rangle$ *and* $\langle \mathsf{a}_1, \alpha \mathsf{a}_2 + \beta \mathsf{a}_3 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1$. *Thus, we have* $n_1 = 1, n_2 = \infty$.

9. *Suppose* $G = U^2_{(0,1)} \cdot T_{(1,1)}$. *Then* G *has a faithful parameterization*

$$(w, x, y) \mapsto \begin{bmatrix} y & 0 & w \\ 0 & y & x \\ 0 & 0 & y^{-2} \end{bmatrix}.$$

   Under this parameterization, we have $(\operatorname{Int} y)(w, x) = (y^3 w, y^3 x)$. *The* G*-invariant subspaces are* $\langle \alpha \mathsf{a}_1 + \beta \mathsf{a}_2 \rangle$, *where* $(\alpha : \beta) \in \mathbb{P}^1$; *and* $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$. *Thus, we have* $n_1 = \infty, n_2 = 1$.

The above listed subgroups are pairwise nonconjugate; in particular, they are distinct.

Proof. The statements in this lemma are verified by straightforward computations, as is the fact that the above listed sets are subgroups. Nonconjugacy of the various groups follows after studying their actions on invariant subspaces. In Item 1, the stipulation that $\sigma \in \{\mathrm{id}, (1\ 2), (2\ 3)\}$ if $(d_1, d_2) = (1, 0)$ is necessary because $P_{(1\ 3)} T_{(1,0)} P^{-1}_{(1\ 3)} = T_{(1,0)}$. ■

Lemma 4.5.3 *Suppose* $G = [\mathsf{G}]_{\mathcal{E}_0}$ *is a subgroup of* SL_3 *that is isomorphic to* $\mathcal{C}^r \rtimes \mathcal{C}^*$, *where* r *is either* 1 *or* 2. *Let* G *have Levi decomposition* $\mathsf{G} = \mathsf{R_u T}$, *where* $\mathsf{R_u} \simeq \mathcal{C}^r$ *and* $\mathsf{T} \simeq \mathcal{C}^*$. *Let*

$\mathcal{F}$ (resp., $\mathcal{B}$) be a basis of V such that $[\mathsf{T}]_{\mathcal{F}}$ (resp., $[\mathsf{R_u}]_{\mathcal{B}}$) is one of the subgroups listed in Lemma 4.2.3 (resp., Lemmas 4.3.1 and 4.3.4).

1. *Suppose $[\mathsf{T}]_{\mathcal{F}} = T_{(d_1,d_2)}$ for some $d_1, d_2 \in \mathbb{Z}$ with $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1, d_2) = 1$.*

   (a) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(0,0)}$, then there exists a basis $\mathcal{A}$ such that $[\mathsf{G}]_{\mathcal{A}} = U^1_{(0,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$ for some $\sigma \in S_3$. If $(d_1, d_2) = (1, 0)$, then σ can be taken to be one of the permutations $\{\mathrm{id}, (1\ 2), (2\ 3)\}$.*

   (b) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(1,1)}$, then $d_1 = 1$, $d_2 = 0$, and there exists a basis $\mathcal{A}$ such that $[\mathsf{G}]_{\mathcal{A}} = U^1_{(1,1)} \cdot T_{(1,0)}$.*

   (c) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,0)}$, then there exists a permutation $\sigma \in \{\mathrm{id}, (1\ 3), (1\ 2\ 3)\}$ such that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^2_{(1,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$.*

   (d) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(0,1)}$, then there exists a permutation $\sigma \in \{\mathrm{id}, (2\ 3), (1\ 3\ 2)\}$ such that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^2_{(0,1)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$.*

   (e) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,1)}$, then $d_1 = 1$, $d_2 = 0$, and there exists a basis $\mathcal{A}$ such that $[\mathsf{G}]_{\mathcal{A}} = U^2_{(1,1)} \cdot T_{(1,0)}$.*

2. *Suppose $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$. Then $[\mathsf{R_u}]_{\mathcal{B}}$ is one of $\left\{U^1_{(0,0)}, U^2_{(1,0)}, U^2_{(0,1)}\right\}$. Moreover, the following statements hold:*

   (a) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(0,0)}$, then there exist a basis $\mathcal{A}$ and a permutation $\sigma \in \{\mathrm{id}, (1\ 3)\}$ such that $[\mathsf{G}]_{\mathcal{A}} = U^1_{(0,0)} \cdot P_\sigma T_{(1,1)} P_\sigma^{-1}$.*

   (b) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,0)}$, then $[\mathsf{G}]_{\mathcal{F}_{(1\ 3)}} = U^2_{(1,0)} \cdot P_{(1\ 3)} T_{(1,1)} P_{(1\ 3)}^{-1}$.*

   (c) *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(0,1)}$, then $[\mathsf{G}]_{\mathcal{F}} = U^2_{(0,1)} \cdot T_{(1,1)}$.*

In particular, there exists a basis $\mathcal{A}$ and a unique subgroup $\hat{G}$ such that $[\mathsf{G}]_{\mathcal{A}} = \hat{G}$ and $\hat{G}$ is one of the subgroups listed in Lemma 4.5.2.

Proof. By the Lie-Kolchin theorem, there exists a flag

$$0 \subsetneq V_1 \subsetneq V_2 \subsetneq V$$

that is preserved by the action of G.

1. Suppose $[\mathsf{T}]_{\mathcal{F}} = T_{(d_1,d_2)}$ for some $d_1, d_2 \in \mathbb{Z}$ with $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1, d_2) = 1$. Let $d_3 = -d_1 - d_2$. Now, $V_1 \subseteq V$ is a G-invariant subspace and in particular a T-invariant subspace, so that by Lemma 4.2.2 we have $V_1 = \langle \mathsf{f}_{A_1} \rangle$ for some index A_1. An analogous

argument shows that $V_2 = \langle \mathsf{f}_{A_1}, \mathsf{f}_{A_2} \rangle$ for some index A_2. Let $\omega \in S_3$ be the permutation such that $\omega(A_j) = j$ for $j = 1, 2$; define A_3 so that $\omega(A_3) = 3$. Following the notational convention established in Section 2.1, we consider the ordered basis

$$\mathcal{F}_\omega = \{\mathsf{f}_{A_1}, \mathsf{f}_{A_2}, \mathsf{f}_{A_3}\}.$$

Fix a nonroot of unity $v \in \mathcal{C}^*$. From the parameterization given in Lemma 4.2.2, we see that $[\mathsf{T}]_{\mathcal{F}_\omega}$ is generated by the matrix Q, where Q is given by (4.4).

We will next consider the subgroup $[\mathsf{R_u}]_{\mathcal{F}_\omega}$. Since V_1 and V_2 are G-invariant, we see that $[\mathsf{G}]_{\mathcal{F}_\omega} \subseteq \mathsf{T}_3$. This fact, together with the identity

$$[\mathsf{G}]_{\mathcal{F}_\omega} = [\mathsf{R_u}]_{\mathcal{F}_\omega}[\mathsf{T}]_{\mathcal{F}_\omega}, \tag{4.6}$$

implies that $[\mathsf{R_u}]_{\mathcal{F}_\omega} \subseteq \mathsf{U}_3$.

- Assume $\mathsf{R_u} \simeq \mathcal{C}$. Let $\phi \in \mathsf{SL}(V)$ be a generator of $\mathsf{R_u}$. Then $[\mathsf{R_u}]_{\mathcal{F}_\omega}$ is generated by a nontrivial matrix $M = [\phi]_{\mathcal{F}_\omega}$ of the form (4.1). Since (4.6) is a Levi decomposition, we have $QMQ^{-1} \in [\mathsf{R_u}]_{\mathcal{F}_\omega}$, where Q is the generator of $[\mathsf{T}]_{\mathcal{F}_\omega}$ specified above.

  Suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(0,0)}$. Then $[\mathsf{R_u}]_{\mathcal{F}_\omega}$ is conjugate to $U^1_{(0,0)}$. Let $q : \mathsf{U}_3 \to \mathcal{C}^2$ be the mapping defined in Lemma 4.3.3. Then $q(M) = (a, c) \in \mathcal{C}^2$. Since $U^1_{(0,0)}$ is nonconjugate to $U^1_{(1,1)}$ by Lemma 4.3.1, it follows from Item 3 of Lemma 4.3.4 that either $a = 0$ or $c = 0$. Lemma 4.5.1 now implies that two of $\{a, b, c\}$ are zero. Define $\tau \in S_3$ to be $(2\ 3)$ if $a \neq 0$, id if $b \neq 0$, $(1\ 2)$ if $c \neq 0$. Define $\sigma = \tau \circ \omega$. It is now an exercise involving the definitions and Lemma 4.1.4 to check that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^1_{(0,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$. If $(d_1, d_2) = (1, 0)$, then $P_\sigma T_{(1,0)} P_\sigma^{-1}$ is one of the following three groups:

  $$\{t, 1, t^{-1}\} = T_{(1,0)}, \{1, t, t^{-1}\} = P_{(1\ 2)} T_{(1,0)} P^{-1}_{(1\ 2)}, \{t, t^{-1}, 1\} = P_{(2\ 3)} T_{(1,0)} P^{-1}_{(2\ 3)}.$$

  Item 1(a) of the conclusion now follows easily.

  Now suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(1,1)}$, i.e., $a \neq 0$ and $c \neq 0$. Here, Lemma 4.5.1 implies that $d_1 = 1, d_2 = 0, A_2 = 2$, and $b = \frac{1}{2}ac$. Define $\mathcal{A} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3\}$ by $\mathsf{a}_1 = a\mathsf{f}_{A_1}, \mathsf{a}_2 = \mathsf{f}_2, \mathsf{a}_3 = c^{-1}\mathsf{f}_{A_3}$. It is easy to check that $[\phi]_{\mathcal{A}} = \begin{bmatrix} 1 & 1 & 1/2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, from which we obtain $[\mathsf{R_u}]_{\mathcal{A}} = U^1_{(1,1)}$. Next, from $A_2 = 2$ we see that ω is either id or $(1\ 3)$. In either case, we claim that $[\mathsf{T}]_{\mathcal{F}_\omega} = T_{(1,0)}$. Indeed, this statement is trivial in case $\omega = \mathrm{id}$; if $\omega = (1\ 3)$, one checks that

$$P_{(1\ 3)} T_{(1,0)} P^{-1}_{(1\ 3)} = T_{(1,0)},$$

and the claim follows easily in this case as well. From $[\mathsf{T}]_{\mathcal{F}_\omega} = T_{(1,0)}$ we obtain

$$\begin{aligned} [\mathsf{T}]_{\mathcal{A}} &= [\mathrm{id}]_{\mathcal{F}_\omega,\mathcal{A}} [\mathsf{T}]_{\mathcal{F}_\omega} [\mathrm{id}]_{\mathcal{A},\mathcal{F}_\omega} \\ &= \mathrm{diag}(a^{-1}, 1, c) T_{(1,0)} \,\mathrm{diag}(a, 1, c^{-1}) = T_{(1,0)}. \end{aligned}$$

We conclude that $[\mathsf{G}]_{\mathcal{A}} = [\mathsf{R_u}]_{\mathcal{A}} [\mathsf{T}]_{\mathcal{A}} = U^1_{(1,1)} \cdot T_{(1,0)}$ as desired.

- Now assume $\mathsf{R_u} \simeq \mathcal{C}^2$. If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,0)}$, then Lemma 4.3.1 implies that $V_1 = \langle \mathsf{b}_1 \rangle$ and $\mathsf{R_u}$ acts trivially on V/V_1. It follows that b_1 and f_{A_1} differ by a scalar multiple and that $\phi(\mathsf{f}_{A_j}) \in \mathsf{f}_{A_j} + V_1$ for $\phi \in \mathsf{R_u}$ and $j \in \{2, 3\}$. This implies that $[\mathsf{R_u}]_{\mathcal{F}_\omega} = U^2_{(1,0)}$. Moreover, we may swap f_{A_2} and f_{A_3} if necessary so that $A_2 < A_3$. Since $A_j = \sigma^{-1}(j)$, this means that we only need consider the permutations $\mathrm{id}, (1\ 3)$ and $(1\ 2\ 3)$. Item 1(c) of the lemma is now clear.

  If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(0,1)}$, then Lemma 4.3.1 implies that

  $$V_2 = \langle \mathsf{f}_{A_1}, \mathsf{f}_{A_2} \rangle = \langle \mathsf{b}_1, \mathsf{b}_2 \rangle$$

  and $\mathsf{R_u}$ acts trivially on V_2 and V/V_2. It follows that $[\mathsf{R_u}]_{\mathcal{F}_\omega} = U^2_{(0,1)}$. Moreover, in this case, we may swap f_{A_1} and f_{A_2} if necessary so that $A_1 < A_2$. Thus, we need only consider the permutations $\mathrm{id}, (2\ 3)$ and $(1\ 3\ 2)$. Item 1(d) of the lemma follows.

  Next, suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,1)}$. Since $[\mathsf{R_u}]_{\mathcal{F}_\omega} \subseteq \mathsf{U}_3$, the proof of Lemma 4.3.4 implies that $[\mathsf{R_u}]_{\mathcal{F}_\omega} = \mathrm{clos}(M) \cdot U^1_{(0,0)}$ for some matrix M of the form (4.1) with $a \neq 0, c \neq 0$. Here, Lemma 4.5.1 yields $d_1 = 1, d_2 = 0, A_2 = 2$. Define $\mathcal{A} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3\}$ by $\mathsf{a}_1 = a\mathsf{f}_{A_1}, \mathsf{a}_2 = \mathsf{f}_2, \mathsf{a}_3 = c^{-1}\mathsf{f}_{A_3}$. Then, a computation analogous to that used in the case $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(1,1)}$ shows that $[\mathsf{G}]_{\mathcal{A}} = U^2_{(1,1)} \cdot T_{(1,0)}$, as stated in Item 1(e).

2. Suppose $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$, so that $d_1 = d_2 = 1$ and we define $d_3 = -2$. In this case, $[\mathsf{T}]_{\mathcal{F}}$ is generated by a matrix of the form $\mathrm{diag}(v, v, v^{-2}),\ v \in \mathcal{C}^*$ a nonroot of unity. Recall that V_1 is a G-invariant subspace and in particular a T-invariant subspace. Therefore V_1 is either $\langle \mathsf{f}_3 \rangle$ or $\langle \alpha\mathsf{f}_1 + \beta\mathsf{f}_2 \rangle$ for some nonzero (α, β). In order to narrow

down our list of choices, note that our choice of basis $\mathcal{F}$ is arbitrary, so long as $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$. Therefore, in case $V_1 \neq \langle \mathsf{f}_3 \rangle$, we may swap f_1 and f_2 in $\mathcal{F}$ or replace f_1 with $\mathsf{f}_1 + \gamma \mathsf{f}_2$ ($\gamma \in \mathcal{C}$) if necessary so that $V_1 = \langle \mathsf{f}_1 \rangle$; Lemma 4.2.2 then implies that either $V_2 = \langle \mathsf{f}_1, \mathsf{f}_2 \rangle$ or $V_2 = \langle \mathsf{f}_1, \mathsf{f}_3 \rangle$. In case $V_1 = \langle \mathsf{f}_3 \rangle$, we may perform a similar operation if necessary so that $V_2 = \langle \mathsf{f}_2, \mathsf{f}_3 \rangle$. Thus, without loss of generality, we may assume that one of the following holds:

- $V_1 = \langle \mathsf{f}_1 \rangle, V_2 = \langle \mathsf{f}_1, \mathsf{f}_2 \rangle$ $(\omega = \mathrm{id})$
- $V_1 = \langle \mathsf{f}_1 \rangle, V_2 = \langle \mathsf{f}_1, \mathsf{f}_3 \rangle$ $(\omega = (2\ 3))$
- $V_1 = \langle \mathsf{f}_3 \rangle, V_2 = \langle \mathsf{f}_2, \mathsf{f}_3 \rangle$ $(\omega = (1\ 3))$

We now see that $[\mathsf{G}]_{\mathcal{F}_\omega}$ is included in T_3, where ω is the appropriate permutation defined above. Let $A_j = \omega^{-1}(j)$ for $1 \leq j \leq 3$, so that $[\mathsf{T}]_{\mathcal{F}_\omega}$ is generated by a matrix Q of the form (4.4).

- Assume $\mathsf{R_u} \simeq \mathcal{C}$. Let $\phi \in \mathsf{SL}(V)$ be a generator of $\mathsf{R_u}$. Then $[\mathsf{R_u}]_{\mathcal{F}_\omega}$ is generated by a nontrivial matrix $M = [\phi]_{\mathcal{F}_\omega}$ of the form (4.1). Since (4.6) is a Levi decomposition, we have $QMQ^{-1} \in [\mathsf{R_u}]_{\mathcal{F}_\omega}$, where Q is the generator of $[\mathsf{T}]_{\mathcal{F}_\omega}$ specified above.

  Suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(0,0)}$, i.e., either $a = 0$ or $c = 0$. We distinguish three subcases:

  - If $a = c = 0$, then $[\mathsf{R_u}]_{\mathcal{F}_\omega} = U^1_{(0,0)}$ and we have $[\mathsf{G}]_{\mathcal{F}_\omega} = U^1_{(0,0)} \cdot T_{(1,1)}$.
  - If $a = 0, b \neq 0, c \neq 0$, then Lemma 4.5.1 implies that $A_3 = 3$, so that $\omega = \mathrm{id}$ by hypothesis. If we now let $\mathsf{a}_1 = b\mathsf{f}_1 + c\mathsf{f}_2, \mathsf{a}_2 = \mathsf{f}_2, \mathsf{a}_3 = \mathsf{f}_3$, then $[\mathsf{T}]_{\mathcal{A}} = T_{(1,1)}$ since T acts in the same way on all subspaces of the form $\alpha \mathsf{f}_1 + \beta \mathsf{f}_2, \alpha, \beta \in \mathcal{C}$. Meanwhile, it is easy to check that $[\phi]_{\mathcal{A}} \in U^1_{(0,0)}$, so that $[\mathsf{R_u}]_{\mathcal{A}} = U^1_{(0,0)}$; we conclude that $[\mathsf{G}]_{\mathcal{A}} = U^1_{(0,0)} \cdot T_{(1,1)}$.
  - If $a \neq 0, b \neq 0, c = 0$, then Lemma 4.5.1 implies that $A_1 = 3$, so that $\omega = (1\ 3)$ by hypothesis; if we now let $\mathsf{a}_1 = \mathsf{f}_3, \mathsf{a}_2 = a^{-1}b\mathsf{f}_2 - \mathsf{f}_1, \mathsf{a}_3 = \mathsf{f}_2$, then a sequence of calculations similar to the previous case shows that $[\mathsf{G}]_{\mathcal{A}} = U^1_{(0,0)} \cdot P_{(1\ 3)} T_{(1,1)} P_{(1\ 3)}$.

  Each subcase is consistent with Item (2a) of the lemma. Note that $[\mathsf{R_u}]_{\mathcal{B}}$ cannot be $U^1_{(1,1)}$ if $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$, by Item (1d) of Lemma 4.5.1.

- Assume $\mathsf{R_u} \simeq \mathcal{C}^2$.

  Note that $[\mathsf{R_u}]_{\mathcal{B}}$ cannot be $U^2_{(1,1)}$ if $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$, by Item 2 of Lemma 4.5.1.

Suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,0)}$. Then, by Lemma 4.3.4, we have

$$V_1 = \langle \mathsf{b}_1 \rangle = \langle \mathsf{f}_{A_1} \rangle$$

and $\mathsf{R_u}$ acts trivially on V/V_1. We conclude that $[\mathsf{R_u}]_{\mathcal{F}_\omega} \subseteq U^2_{(1,0)}$ and hence $[\mathsf{R_u}]_{\mathcal{F}_\omega} = U^2_{(1,0)}$. A defect argument then implies that $\omega = (1\ 3)$, and we conclude that $[\mathsf{G}]_{\mathcal{F}_{(1\ 3)}} = U^2_{(1,0)} \cdot P_{(1\ 3)} T_{(1,1)} P^{-1}_{(1\ 3)}$.

Suppose $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(0,1)}$. Here, $\mathsf{R_u}$ fixes V_2 elementwise. We conclude that $[\mathsf{R_u}]_{\mathcal{F}_\omega} = U^2_{(0,1)}$. A defect argument implies $\omega = \mathrm{id}$. We conclude that $[\mathsf{G}]_{\mathcal{F}} = U^2_{(0,1)} \cdot T_{(1,1)}$.

■

Lemma 4.5.4 *Given $G = [\mathsf{G}]_{\mathcal{A}} \subseteq \mathsf{SL}_3$, where G is a subgroup of $\mathsf{SL}_3(V)$ and $\mathcal{A} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3\}$ is a basis of V.*

1. *Suppose $G = U^1_{(0,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$. Then G admits a faithful parameterization*

$$(x, y_1, y_2) \mapsto \begin{bmatrix} y_1 & 0 & x \\ 0 & y_2 & 0 \\ 0 & 0 & (y_1 y_2)^{-1} \end{bmatrix},$$

under which $(\mathrm{Int}(y_1, y_2))(x) = y_1^2 y_2 x$. The G-invariant subspaces are $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_2 \rangle, \langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_3 \rangle$, so that $n_1 = n_2 = 2$.

2. *Suppose $G = U^2_{(1,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$. Then G has a faithful parameterization*

$$(w, x, y_1, y_2) \mapsto \begin{bmatrix} y_1 & w & x \\ 0 & y_2 & 0 \\ 0 & 0 & (y_1 y_2)^{-1} \end{bmatrix},$$

under which $(\mathrm{Int}(y_1, y_2))(w, x) = (y_1 y_2^{-1} w, y_1^2 y_2 x)$. The G-invariant subspaces are $\langle \mathsf{a}_1 \rangle, \langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_3 \rangle$, so that $n_1 = 1, n_2 = 2$.

3. *Suppose $G = U^2_{(0,1)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$. Then G has a faithful parameterization*

$$(w, x, y_1, y_2) \mapsto \begin{bmatrix} y_1 & 0 & w \\ 0 & y_2 & x \\ 0 & 0 & (y_1 y_2)^{-1} \end{bmatrix},$$

under which $(\mathrm{Int}(y_1, y_2))(w, x) = (y_1^2 y_2 w, y_1 y_2^2 x)$. The G-invariant subspaces are $\langle \mathsf{a}_1 \rangle$, $\langle \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, so that $n_1 = 2, n_2 = 1$.

The above listed subgroups are pairwise nonconjugate; in particular, they are distinct.

Proof. The statements in this lemma are verified by straightforward computations, as is the fact that the above listed sets are subgroups. Nonconjugacy of the various groups follows after studying their actions on invariant subspaces. ■

Lemma 4.5.5 *Suppose $G = [\mathsf{G}]_{\mathcal{E}_0}$ is a subgroup of SL_3 that is isomorphic to $\mathcal{C}^r \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$, where r is either 1 or 2. Let G have Levi decomposition $\mathsf{G} = \mathsf{R_u}\mathsf{T}$, where $\mathsf{R_u} \simeq \mathcal{C}^r$ and $\mathsf{T} \simeq \mathcal{C}^* \times \mathcal{C}^*$. Let $\mathcal{F}$ (resp., $\mathcal{B}$) be a basis of V such that $[\mathsf{T}]_{\mathcal{F}}$ (resp., $[\mathsf{R_u}]_{\mathcal{B}}$) is $\mathsf{D}_3 \cap \mathsf{SL}_3$ (resp., one of the subgroups listed in Lemmas 4.3.1 and 4.3.4). Then $[\mathsf{R_u}]_{\mathcal{B}}$ is one of $\left\{U^1_{(0,0)}, U^2_{(1,0)}, U^2_{(0,1)}\right\}$. Moreover, the following statements hold:*

1. *If $[\mathsf{R_u}]_{\mathcal{B}} = U^1_{(0,0)}$, then there exists a permutation $\sigma \in S_3$ such that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^1_{(0,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$.*

2. *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(1,0)}$, then there exists a permutation $\sigma \in S_3$ such that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^2_{(1,0)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$.*

3. *If $[\mathsf{R_u}]_{\mathcal{B}} = U^2_{(0,1)}$, then there exists a permutation $\sigma \in S_3$ such that $[\mathsf{G}]_{\mathcal{F}_\sigma} = U^2_{(0,1)} \cdot (\mathsf{D}_3 \cap \mathsf{SL}_3)$.*

In particular, there exists a basis $\mathcal{A}$ and a unique subgroup $\hat{G}$ such that $[\mathsf{G}]_{\mathcal{A}} = \hat{G}$ and $\hat{G}$ is one of the subgroups listed in Lemma 4.5.4.

Proof. By the Lie-Kolchin theorem, there exists a flag

$$0 \subsetneq V_1 \subsetneq V_2 \subsetneq V$$

that is preserved under the action of G.

It follows from Lemma 4.2.2 that (after reordering the basis vectors of $\mathcal{F}$ if necessary) $V_1 = \langle \mathsf{f}_1 \rangle, V_2 = \langle \mathsf{f}_1, \mathsf{f}_2 \rangle$. It follows that $[\mathsf{R_u}]_{\mathcal{F}} \subseteq \mathsf{U}_3$. Let M be a member of $[\mathsf{R_u}]_{\mathcal{F}}$, where M is as described in (4.1). If $[\mathsf{R_u}]_{\mathcal{F}} \neq U^1_{(0,0)}$, then assume $M \notin U^1_{(0,0)}$.

Let $Q = \operatorname{diag}\left(v_1, v_2, (v_1 v_2)^{-1}\right) \in [\mathsf{T}]_{\mathcal{F}}$ with v_2 a nonroot of unity. We compute

$$QMQ^{-1} = \begin{bmatrix} 1 & v_1 v_2^{-1} a & v_1^2 v_2 b \\ 0 & 1 & v_1 v_2^2 c \\ 0 & 0 & 1 \end{bmatrix}.$$

If both a and c are nonzero, then the proof of Lemma 4.3.3 and the fact that $QMQ^{-1} \in [\mathsf{R}_\mathsf{u}]_\mathcal{F}$ imply that $v_1 v_2^{-1} = x = v_1 v_2^2$ for some $x \in \mathcal{C}$, which in turn implies that $v_2^3 = 1$. This contradicts hypothesis on v_2, and we conclude that either $a = 0$ or $c = 0$.

In case $R_u \simeq \mathcal{C}^2$, we may apply Lemma 4.3.3 and its proof to show that $[\mathsf{R}_\mathsf{u}]_\mathcal{F} = \mathrm{clos}(M) \cdot U^1_{(0,0)}$; the desired result then follows easily. In case $R_u \simeq \mathcal{C}$, an additional normalization argument shows that *two* of $\{a, b, c\}$ are zero. Thus, we may reorder the vectors of $\mathcal{F}$ if necessary so that $R'_u = U^1_{(0,0)}$, and the result follows.

■

Lemma 4.5.6 *Given $G = [\mathsf{G}]_\mathcal{A} \subseteq \mathsf{SL}_3$, where G is a subgroup of $\mathsf{SL}_3(V)$ and $\mathcal{A} = \{\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3\}$ is a basis of V.*

1. *Suppose $G = \mathsf{U}_3 \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$, $d_1 > d_2 \geq 0, \mathrm{GCD}(d_1, d_2) = 1$, $\sigma \in S_3, \sigma \in \{\mathrm{id}, (1\ 2), (2\ 3)\}$ if $(d_1, d_2) = (1, 0)$. Then G has a faithful parameterization*

$$\left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}, y \right) \mapsto \begin{bmatrix} y^{d_{I_1}} & v & w \\ 0 & y^{d_{I_2}} & x \\ 0 & 0 & y^{d_{I_3}} \end{bmatrix},$$

where $d_3 = -d_1 - d_2$ and $\sigma(I_j) = j$ for $1 \leq j \leq 3$. Under this parameterization, we have

$$(\mathrm{Int}\, y) \left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & y^{d_{I_1} - d_{I_2}} v & y^{d_{I_1} - d_{I_3}} w \\ 0 & 1 & y^{d_{I_2} - d_{I_3}} x \\ 0 & 0 & 1 \end{bmatrix}.$$

2. *Suppose $G = \mathsf{U}_3 \cdot P_{(2\ 3)} T_{(1,1)} P^{-1}_{(2\ 3)}$. This subgroup has a faithful parameterization*

$$\left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix}, y \right) \mapsto \begin{bmatrix} y & v & w \\ 0 & y^{-2} & x \\ 0 & 0 & y \end{bmatrix}.$$

Under this parameterization, we have

$$(\mathrm{Int}\, y) \left(\begin{bmatrix} 1 & v & w \\ 0 & 1 & x \\ 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & y^3 v & w \\ 0 & 1 & y^{-3} x \\ 0 & 0 & 1 \end{bmatrix}.$$

In either case, the G-invariant subspaces are $\langle \mathsf{a}_1 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, so that $n_1 = n_2 = 1$. These subgroups are pairwise nonconjugate; in particular, they are distinct.

Proof. The statements in this lemma are verified by straightforward computations, as is the fact that the above listed sets are subgroups. Nonconjugacy of the various groups follows after studying their actions on invariant subspaces.

■

Lemma 4.5.7 *Suppose $G = [\mathsf{G}]_{\mathcal{E}_0}$ is a subgroup of SL_3 that is isomorphic to $\mathsf{U}_3 \rtimes \mathcal{C}^*$. Let G have Levi decomposition $\mathsf{G} = \mathsf{R_u T}$, where $\mathsf{R_u} \simeq \mathsf{U}_3$ and $\mathsf{T} \simeq \mathcal{C}^*$. Let $\mathcal{F}$ (resp., $\mathcal{B}$) be a basis of V such that $[\mathsf{T}]_{\mathcal{F}}$ (resp., $[\mathsf{R_u}]_{\mathcal{B}}$) is one of the subgroups listed in Lemma 4.2.3 (resp., U_3).*

1. *If $[\mathsf{T}]_{\mathcal{F}} = T_{(d_1,d_2)}$, $d_1 > d_2 \geq 0$, $\mathrm{GCD}(d_1, d_2) = 1$, then there exists a basis $\mathcal{A}$ such that $[\mathsf{G}]_{\mathcal{A}} = \mathsf{U}_3 \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$ for some $\sigma \in S_3$. If $(d_1, d_2) = (1, 0)$, then we may take σ to be one of $\{\mathrm{id}, (1\ 2), (2\ 3)\}$.*
2. *If $[\mathsf{T}]_{\mathcal{F}} = T_{(1,1)}$, then there exists a basis $\mathcal{A}$ such that $[\mathsf{G}]_{\mathcal{A}} = \mathsf{U}_3 \cdot P_{(2\ 3)} T_{(1,1)} P_{(2\ 3)}^{-1}$.*

In particular, there exists a basis $\mathcal{A}$ and a unique subgroup $\hat{G}$ such that $[\mathsf{G}]_{\mathcal{A}} = \hat{G}$ and $\hat{G}$ is one of the subgroups listed in Lemma 4.5.6.

Proof. By the Lie-Kolchin theorem, there exists a flag $0 \subsetneq V_1 \subsetneq V_2 \subsetneq V$ that is preserved by the action of G.

Let $\mathcal{F}$ be as in Lemma 4.2.3 and let $[\mathsf{T}]_{\mathcal{F}} = T_{(d_1,d_2)}$ for some $d_1, d_2, d_1 \geq d_2 \geq 0$. If $d_1 > d_2$, then there exists a permutation ω such that $[\mathsf{G}]_{\mathcal{F}_\omega} \subseteq \mathsf{T}_3$. It follows that $[\mathsf{G}]_{\mathcal{F}_\omega}$ is one of the groups listed in Item 1. If $(d_1, d_2) = (1, 0)$, then $P_\omega T_{(1,0)} P_\omega^{-1}$ is one of the following three groups:

$$\left\{t, 1, t^{-1}\right\} = T_{(1,0)}, \left\{1, t, t^{-1}\right\} = P_{(1\ 2)} T_{(1,0)} P_{(1\ 2)}^{-1}, \left\{t, t^{-1}, 1\right\} = P_{(2\ 3)} T_{(1,0)} P_{(2\ 3)}^{-1}.$$

Item 1 of the conclusion now follows easily.

If $d_1 = d_2 = 1$, then we may alter our definition of the basis $\mathcal{F}$ if necessary so that V_1 is generated by either f_1 or f_3. Therefore, there exists a permutation ω such that $[\mathsf{G}]_{\mathcal{F}_\omega} \subseteq \mathsf{T}_3$ in this case as well. Now, a defect argument implies that $\omega = (2\ 3)$, and we conclude that $[\mathsf{G}]_{\mathcal{F}_\omega}$ is the group listed in Item 2.

■

Lemma 4.5.8 *Suppose $G = [\mathsf{G}]_{\mathcal{E}_0}$ is a subgroup of SL_3 that is isomorphic to $\mathcal{C}^2 \rtimes P$, where $P = [\mathsf{P}]_{\mathcal{E}_0}$ is isomorphic to either SL_2 or GL_2. Then there exist a basis $\mathcal{A}$ and a unique subgroup $\hat{G} \subseteq \mathsf{SL}_3$ such that $\hat{G} = [\mathsf{G}]_{\mathcal{A}}$ is one of the following subgroups:*

1. If $P \simeq \mathsf{SL}_2$:

(a) $\{(t_{ij}) \in \mathsf{SL}_3 : t_{31} = t_{32} = 0, t_{33} = 1\} \simeq \mathcal{C}^2 \rtimes \mathsf{SL}_2$, in which conjugation is given by the unique irreducible representation of SL_2 on $\mathcal{C}^2$. In this case, the only G-invariant subspace is $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, so that $n_1 = 0, n_2 = 1$.

(b) $\{(t_{ij}) \in \mathsf{SL}_3 : t_{21} = t_{31} = 0, t_{11} = 1\} \simeq \mathcal{C}^2 \rtimes \mathsf{SL}_2$, in which conjugation is given by the unique irreducible representation of SL_2 on $\mathcal{C}^2$. In this case, the only G-invariant subspace is $\langle \mathsf{a}_1 \rangle$, so that $n_1 = 1, n_2 = 0$.

2. If $P \simeq \mathsf{GL}_2$:

(a) $\{(t_{ij}) \in \mathsf{SL}_3 : t_{31} = t_{32} = 0\} \simeq \mathcal{C}^2 \rtimes \mathsf{GL}_2$, in which conjugation is given by

$$M.v = (\det M)Mv \text{ for } M \in \mathsf{GL}_2, v \in \mathcal{C}^2.$$

In this case, the only G-invariant subspace is $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$, so that $n_1 = 0, n_2 = 1$.

(b) $\{(t_{ij}) \in \mathsf{SL}_3 : t_{21} = t_{31} = 0\} \simeq \mathcal{C}^2 \rtimes \mathsf{GL}_2$, in which conjugation is given by

$$M.v = (\det M)^{-1}(M^{-1})^T v \text{ for } M \in \mathsf{GL}_2, v \in \mathcal{C}^2.$$

In this case, the only G-invariant subspace is $\langle \mathsf{a}_1 \rangle$, so that $n_1 = 1, n_2 = 0$.

Proof. By Lemma 4.3.4, there exists a basis $\mathcal{B}$ such that the subgroup $[\mathsf{R_u}]_{\mathcal{B}}$ is one of $\left\{U^2_{(1,0)}, U^2_{(0,1)}, U^2_{(1,1)}\right\}$. Let $P' = [\mathsf{P}]_{\mathcal{B}}$. Then P' is included in $\mathrm{Nor}_{\mathsf{SL}_3}([\mathsf{R_u}]_{\mathcal{B}})$. The desired result now follows easily from Lemma 4.3.5; note that $[\mathsf{R_u}]_{\mathcal{B}}$ cannot be $U^2_{(1,1)}$ because the normalizer of the latter group is included in T_3 while P cannot be upper-triangularized. The statements about invariant subspaces are verified by calculations.

■

We give one more technical lemma before proceeding.

Lemma 4.5.9 *1. For $d \geq 0$, define $X_d \simeq \mathcal{C}^{d+1}$ to be the space of homogeneous polynomials of degree d in $\mathcal{C}[x, y]$, where x and y are indeterminates. Define*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} .(x^i y^{d-i}) = (ax + cy)^i (bx + dy)^{d-i}$$

for a typical element $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{SL}_2$ and a typical basis vector $x^i y^{d-i}$ of X_d, $0 \leq i \leq d$. Then, up to isomorphism, the induced action of SL_2 on X_d is the unique irreducible

$(d+1)$-dimensional representation of SL_2. If d is odd, then this representation is faithful. If d is even and greater than zero, then the representation has kernel $\{\pm I_2\}$ and thus induces a faithful $(d+1)$-dimensional representation of PSL_2. Moreover, the only nontrivial irreducible representations of PSL_2 are the ones which arise in this way.

2. *If G_0 is an algebraic group and the vector space W is an irreducible G_0-module, then any G_0-module endomorphism of W is a scalar multiple of the identity.*

3. *Given a faithful representation $\mathsf{SL}_2 \to \mathsf{SL}(W)$ with $W \simeq \mathcal{C}^3$. Then there exists a decomposition*

$$W = W_1 + W_2 \text{ (direct sum of } \mathsf{SL}_2\text{-invariant subspaces)},$$

where $W_r \simeq X_{r-1} \simeq \mathcal{C}^r$, X_{r-1} as described in Item 1, for $r = 1, 2$. Moreover, W_1 and W_2 are the only nonzero proper SL_2-invariant subspaces of W.

4. *Let G_0 be one of $\{\mathsf{SL}_2, \mathsf{PSL}_2\}$ and let A be one of $\{\mathcal{C}, \mathcal{C}^*\}$. Then it is impossible to embed $G_0 \times A$ in SL_3.*

Proof. The first statement is proved in Section 23.1 of [FH91]. The second statement is a special case of Lemma 3.4.1.

To prove the third statement, notice that SL_2 is reductive and therefore W is completely reducible over SL_2. Since the representation is faithful, we can rule out $W \simeq X_2$ as well as $W \simeq X_0 \oplus X_0 \oplus X_0$. Thus, we must have $W \simeq X_0 \oplus X_1$; this yields the first part of the statement. To prove the second part, let $w \in W \setminus (W_1 \cup W_2)$; we will show that the smallest SL_2-invariant subspace of W containing w is W itself. Write $w = w_1 + w_2 \in W, w_1 \in W_1, w_2 \in W_2$, and assume $w_1, w_2 \neq 0$. Then, it is easy to show that there exist $\phi_1, \phi_2 \in \mathsf{SL}_2$ such that the set

$$\{w, \phi_1(w) = w_1 + \phi_1(w_2), \phi_2(w) = w_1 + \phi_2(w_2)\}$$

is linearly independent. This proves the desired result.

We prove the fourth statement as follows: In this situation we may identify SL_3 with $\mathsf{SL}(W)$, where $W \simeq \mathcal{C}^3$ is a vector space. Suppose $\Phi : G_0 \times A \to \mathsf{SL}(W)$ is an embedding, where G_0 (resp., A) is one of the groups listed in the statement. Then $\Phi(\{1\} \times A)$ is the group closure of some operator $\psi \in \mathsf{SL}(W)$. Also, $G_0 \simeq G_0 \times \{\text{id}\}$ acts faithfully on W via Φ.

Suppose $G_0 = \mathsf{SL}_2$, so that $W = W_1 + W_2$ as in Item 3 of the lemma. Since $\Phi(\mathsf{SL}_2 \times \{\mathrm{id}\})$ commutes with ψ, we see that $\psi(W_2)$ is a SL_2-invariant subspace of W, which by Item 3 must then be W_2 itself. Moreover, $\psi|_{W_2}$ is a SL_2-module endomorphism. Item 2 of the lemma then implies that $\psi|_{W_2} = \alpha \cdot \mathrm{id}\,|_{W_2}$ for some $\alpha \in \mathcal{C}^*$. It quickly follows that, with respect to some suitable basis $\mathcal{B}$ of W,

$$[\Phi(A)]_{\mathcal{B}} = \left\{ \begin{bmatrix} c^{-2} & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix} : c \neq 0 \right\}.$$

Setting $c = -1$ in the above formula, we see that the matrix $\mathrm{diag}(1, -1, -1)$ is contained in $\Phi(A) \cap \Phi(\mathsf{SL}_2)$, contradicting the hypothesis that the product of G_0 and A is a direct product.

Now suppose $G_0 = \mathsf{PSL}_2$. By Item 1 of the lemma, we see that W is isomorphic to the vector space $X_2 \simeq \mathcal{C}^3$, viewed as a PSL_2-module. In particular, W is irreducible over PSL_2. We also see that ψ is a PSL_2-module endomorphism of W. As in the previous case, Item 2 implies that ψ is a scalar multiple of the identity, so that $\Phi(A) = \mathsf{D}_3$ is the group of scalar matrices. Here, we see that the matrix $\mathrm{diag}(\zeta_3, \zeta_3, \zeta_3)$, where ζ_3 is a primitive cube root of unity, is contained in $\Phi(A) \cap \Phi(\mathsf{PSL}_2)$, contradicting hypothesis as in previous case.

■

We are now ready to prove Theorem 4.1.5.

Proof of Theorem 4.1.5. In what follows, $G \subseteq \mathsf{SL}_3$ is an admissible subgroup; $G = R_u P$ is a Levi decomposition with P (resp., R_u) a maximal reductive subgroup (resp., the unipotent radical) of G; $H = (P, P)$ is semisimple and $T = Z(P)^\circ$ is a torus. Let $G = [\mathsf{G}]_{\mathcal{E}_0}$, where $\mathcal{E}_0 = \{\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3\}$ is a fixed basis of the vector space $V \simeq \mathcal{C}^3$ and $G \subseteq \mathsf{SL}(V)$. Also let $R_u = [\mathsf{R_u}]_{\mathcal{E}_0}, P = [\mathsf{P}]_{\mathcal{E}_0}, H = [\mathsf{H}]_{\mathcal{E}_0}$, and $T = [\mathsf{T}]_{\mathcal{E}_0}$.

By Lemma 4.2.3, there exist a basis $\mathcal{F} = \{\mathsf{f}_1, \mathsf{f}_2, \mathsf{f}_3\}$ and a unique subgroup $T' \subseteq \mathsf{SL}_3$ such that $T' = [\mathsf{T}]_{\mathcal{F}}$ is one of the subgroups listed in Lemma 4.2.3. By Lemma 4.3.4, there exist a basis $\mathcal{B} = \{\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3\}$ and a unique subgroup $R'_u \subseteq \mathsf{SL}_3$ such that $R'_u = [\mathsf{R_u}]_{\mathcal{B}}$ is one of the subgroups listed in Lemma 4.3.4.

We study the admissible subgroups by cases according to decomposition, as follows:

1. $H \simeq 1$.

   (a) $T \simeq 1$. In this case, the zero-defect property of admissible groups implies that

$G \simeq 1$.

(b) $T \simeq \mathcal{C}^*$.

i. $R_u \simeq 0$. Here, $G \simeq \mathcal{C}^*$ is as described in Lemma 4.2.3.

ii. $R_u \simeq \mathcal{C}$. Here, $G \simeq \mathcal{C} \rtimes \mathcal{C}^*$. See Lemma 4.5.3.

iii. $R_u \simeq \mathcal{C}^2$. Here, $G \simeq \mathcal{C}^2 \rtimes \mathcal{C}^*$. See Lemma 4.5.3.

iv. $R_u \simeq \mathsf{U}_3$. Here $G \simeq \mathsf{U}_3 \rtimes \mathcal{C}^*$. See Lemma 4.5.7.

(c) $T \simeq \mathcal{C}^* \times \mathcal{C}^*$.

i. $R_u \simeq 0$. Here, $G \simeq \mathcal{C}^* \times \mathcal{C}^*$ is conjugate to $\mathsf{D}_3 \cap \mathsf{SL}_3$, cf. Lemma 4.2.3.

ii. $R_u \simeq \mathcal{C}$. Here, $G \simeq \mathcal{C} \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$. See Lemma 4.5.5.

iii. $R_u \simeq \mathcal{C}^2$. Then $G \simeq \mathcal{C}^2 \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$. See Lemma 4.5.5.

iv. $R_u \simeq \mathsf{U}_3$. Then $G \simeq \mathsf{U}_3 \rtimes (\mathcal{C}^* \times \mathcal{C}^*)$. In this case, it is clear that G is conjugate to $[\mathsf{G}]_{\mathcal{A}} = \mathsf{T}_3 \cap \mathsf{SL}_3$ for some suitable basis $\mathcal{A}$. The G-invariant subspaces are $\langle \mathsf{a}_1 \rangle$ and $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$.

2. $H \simeq \mathsf{SL}_2$.

(a) $T \simeq 1$.

i. $R_u \simeq 0$. Here, $G \simeq \mathsf{SL}_2$, and it follows from Lemma 4.5.9 that there exists a basis $\mathcal{A}$ of V such that

$$[\mathsf{G}]_{\mathcal{A}} = \left\{ (t_{ij}) \in \mathsf{SL}_3 : \begin{array}{rcl} t_{13} = t_{23} & = & 0 \\ t_{31} = t_{32} & = & 0 \\ t_{33} & = & 1 \end{array} \right\}.$$

By Lemma 4.5.9, the G-invariant subspaces are $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_3 \rangle$.

ii. $R_u \simeq \mathcal{C}$. Here, by Lemma 4.5.9, the only possible conjugation action of SL_2 on $\mathcal{C}$ is the trivial action. Therefore, by hypothesis on the defect of G, we conclude that this case does not arise.

iii. $R_u \simeq \mathcal{C}^2$. See Lemma 4.5.8.

iv. $R_u \simeq \mathsf{U}_3$. In this case, we have $G \simeq \mathsf{U}_3 \rtimes \mathsf{SL}_2$. Then, it is not hard to show that G has Borel subgroup $B \simeq \mathsf{U}_3 \rtimes (\mathsf{T}_2 \cap \mathsf{SL}_2)$. It is also straightforward to show that the unipotent radical R of B is isomorphic to $\mathsf{U}_3 \rtimes \mathsf{U}_2$. If G can be embedded in SL_3, then (by Kolchin's theorem) R can be embedded in U_3. But R has dimension 4; we obtain a contradiction and conclude that this case does not arise.

(b) $T \simeq \mathcal{C}^*$ or $T \simeq \mathcal{C}^* \times \mathcal{C}^*$. By Item 3 of Lemma 4.5.9, V has exactly two nontrivial proper H-invariant subspaces V_1 and V_2, where $V = V_1 + V_2$ (direct sum) and V_r has dimension r for $r = 1, 2$. Since T commutes with H, we have that the image of V_1 (resp., of V_2) under T is an H-invariant subspace of V, which must be either 0 or V_1 or V_2. Moreover, T is a group of automorphisms of V; thus, for $r = 1, 2$, we have that T maps V_r to a subspace of equal dimension; it follows that T maps V_r onto V_r. Item 2 of Lemma 4.5.9 then implies that T acts as scalar multiples of the identity on V_1 (resp., on V_2). Since T is connected, it then follows that $\mathsf{T}|_{V_2} \subseteq \mathsf{GL}(V_2)$ is either 1 or the full group of scalar-multiple operators on V_2. Note that T must act nontrivially on one of V_1, V_2.

Suppose $T \simeq \mathcal{C}^*$. If $\mathsf{T}|_{V_2}$ is trivial, then we see that $\mathsf{T}|_{V_1} \simeq \mathcal{C}^*$; this implies $P \simeq \mathsf{SL}_2 \times \mathcal{C}^*$, an impossibility by Item 4 of Lemma 4.5.9. Assume instead that T acts as the full group of scalar-multiple operators on V_2. In this case, we see that $P|_{V_2} = \mathsf{GL}(V_2)$ and therefore P is conjugate to the subgroup

$$\{(t_{ij}) \in \mathsf{SL}_3 : t_{13} = t_{23} = t_{31} = t_{32} = 0\} \simeq \mathsf{GL}_2. \tag{4.7}$$

Now suppose $T \simeq \mathcal{C}^* \times \mathcal{C}^*$. Since $H \cap T$ is finite, we see that the Levi subgroup $P = HT$ contains a 3-dimensional torus. This contradicts the fact that any torus embedded in SL_3 has dimension at most 2. We conclude that this case does not arise.

We consider the following cases for R_u, assuming $P \simeq \mathsf{GL}_2$:

i. $R_u \simeq 0$. Here, we have $G = P \simeq \mathsf{GL}_2$ conjugate to the group described in (4.7). If $\mathcal{A}$ is a suitable basis, then one checks that the G-invariant subspaces are $\langle \mathsf{a}_1, \mathsf{a}_2 \rangle$ and $\langle \mathsf{a}_3 \rangle$.

ii. $R_u \simeq \mathcal{C}$. Here, we have $G \simeq \mathcal{C} \rtimes \mathsf{GL}_2$. Then G includes a copy of $\mathcal{C} \rtimes \mathsf{SL}_2$. By Item 1 of Lemma 4.5.9, SL_2 can only act trivially on $\mathcal{C}$; it follows that G includes a copy of $\mathcal{C} \times \mathsf{SL}_2$. But (by Item 4 of Lemma 4.5.9) $\mathcal{C} \times \mathsf{SL}_2$ cannot be embedded in SL_3; we obtain a contradiction and conclude that this case does not arise.

iii. $R_u \simeq \mathcal{C}^2$. See Lemma 4.5.8.

iv. $R_u \simeq \mathsf{U}_3$. Here, it follows from our result in the case ($H \simeq \mathsf{SL}_2, T = 1, R_u \simeq \mathsf{U}_3$) that this case does not arise.

3. $H \simeq \mathsf{PSL}_2$. In this case, it follows from Lemma 4.5.9 and its proof that $T = 1$.

(a) $R_u = 0$. Here, $G \simeq \mathsf{PSL}_2$. Lemma 4.5.9 implies that, for some suitable basis $\mathcal{A}$, the subgroup $\hat{G} = [\mathsf{G}]_{\mathcal{A}}$ has a faithful parametrization

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{bmatrix}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{PSL}_2.$$

A calculation shows that this subgroup is cut out of SL_3 by the equations $t_{12}^2 = t_{11}t_{13}$, $t_{21}^2 = 4t_{11}t_{31}$, $t_{23}^2 = 4t_{13}t_{33}$, $t_{32}^2 = t_{31}t_{33}$, $(t_{22}+1)^2 = 4t_{11}t_{33}$, and $(t_{22}-1)^2 = 4t_{13}t_{31}$. It follows from Lemma 4.5.9 that there are no nontrivial proper G-invariant subspaces in this case.

(b) $R_u = \mathcal{C}$ or $R_u = \mathcal{C}^2$ or $R_u = \mathsf{U}_3$. In this case, we have that $G \simeq R_u \rtimes \mathsf{PSL}_2$. Let V be the vector group $R_u/(R_u, R_u)$, and note that V has dimension at most 2. Now consider the representation $\Psi : \mathsf{PSL}_2 \to \mathsf{GL}(V)$ induced by the conjugation action of PSL_2 on R_u. Recall that Item 1 of Lemma 4.5.9 implies that all nontrivial irreducible representations of PSL_2 have dimension at least 3. Since PSL_2 is reductive, it follows that V is built from copies of the trivial representation of PSL_2, i.e., that Ψ is the trivial map. This contradicts the hypothesis that G has defect zero, and we conclude that this case does not arise.

4. $H \simeq \mathsf{SL}_3$. In this case it is clear that $G = \mathsf{SL}_3$ and that there are no nontrivial proper G-invariant subspaces.

This exhausts the possibilities for H, T and R_u, and we conclude that our list of admissible subgroups of SL_3 is complete.

■

4.6 Computing the group of $D^3 + aD + b,\ a, b \in \mathcal{C}[x]$

In this section, unless and until specified otherwise, $\mathcal{C}$ is a computable, algebraically closed constant field of characteristic zero with factorization algorithm; $k = \mathcal{C}(x)$ unless otherwise specified; and $\mathcal{D} = k[D]$.

Given an operator $L = \sum_i f_i D^i \in \mathcal{D}$, define the *adjoint* of L (see [Sin96]) to be $\operatorname{adj} L = \sum_i (-1)^i D^i f_i$. We have that $\operatorname{adj} : \mathcal{D} \to \mathcal{D}$ is an anti-automorphism of $\mathcal{D}$ and that $\mathcal{D}/\mathcal{D} \operatorname{adj} L \simeq (\mathcal{D}/\mathcal{D}L)^*$ as $\mathcal{D}$-modules.

Given an equation $L(y) = 0$, we may define the associated Riccati equation $\operatorname{Ricc} L$ (see [Sin96]) as follows: Formally substitute the formula $y = \exp(\int u)$ into $L(y) = 0$, then divide by $\exp(\int u)$. The resulting nonlinear equation in u is $\operatorname{Ricc} L$. We see that the following are equivalent for a given $f \in k$:

1. f is a solution of $\operatorname{Ricc} L$.

2. F is a solution of $L(y) = 0$, where $F'/F = f$.

3. $D - f$ is a right factor of L.

Given $L \in \mathcal{C}[x]$ of order 3. By computing rational solutions of $\operatorname{Ricc} L$ (resp., $\operatorname{Ricc}(\operatorname{adj} L)$), we can compute n_1, the number of first-order right factors (resp., n_2, the number of first-order left factors — which is also the number of second-order right factors) of L. Corollary 4.1.3 implies that the group of L is one of the groups listed in the appropriate category in Theorem 4.1.5 or, equivalently, the appropriate cell in Table 4.1. The following results enable us to compute the group of a given operator L once n_1 and n_2 are known, in those cases in which there is more than one entry in Table 4.1. Below, Lemma 4.6.1 addresses the case where $n_1 = n_2 = 0$. The remaining lemmas in this section address the case in which G_L is solvable.

Lemma 4.6.1 *Let $L \in \mathcal{D}$ be a third-order differential operator and let G be the group of the equation $L(y) = 0$. Suppose G is known to be isomorphic to either SL_3 or PSL_2. If $L^{\circledS 2}$ has order 5 or factors, then $G \simeq \mathsf{PSL}_2$; otherwise $G \simeq \mathsf{SL}_3$.*

Proof. This is a special case of Theorem 4.7 in [SU93].

■

Before proceeding, remark that if

$$\begin{aligned} L &= D^3 + a_2 D^2 + a_1 D + a_0 \\ &= (D - r_3) \circ (D - r_2) \circ (D - r_1), \end{aligned}$$

where $a_2, a_1, a_0, r_1, r_2, r_3 \in \mathcal{C}(x)$, then a straightforward calculation yields $r_3 = -a_2 - r_1 - r_2$. In particular, suppose $G_L \subseteq \mathsf{SL}_3$, so that $a_2 = h'/h$ for some $h \in \mathcal{C}(x)$ by Lemma 4.1.2; then $r_3 = -r_1 - r_2 + h'/h$.

Lemma 4.6.2 *Given $L = (D + r_1 + r_2 - h'/h) \circ (D - r_2) \circ (D - r_1) \in \mathcal{D},\ r_1, r_2, h \in k$.*

1. *The Picard-Vessiot extension K_L/k is generated by elements R_1, R_2, y_2, ξ, y_3, where:*

   (a) $R_i' = r_i R_i$ *for* $i = 1, 2$

   (b) $y_2' = r_1 y_2 + R_2$

   (c) $\xi' = r_2 \xi + R_1^{-1} R_2^{-1} h$

   (d) $y_3' = r_1 y_3 + \xi$.

   The full solution space V_L has ordered basis $\mathcal{F}_{(r_1, r_2)} = \{y_1, y_2, y_3\}$, where $y_1 = R_1$.

2. *Let $K_1 = k(R_1, R_2) \subseteq K_L$. Then K_1/k is a Picard-Vessiot extension for the operator $L_{\mathrm{red}} = \mathrm{LCLM}(D - r_1, D - r_2, D + r_1 + r_2 - h'/h)$, so that we may write $K_{L_{\mathrm{red}}} = K_1$.*

3. *Define $T = \{\sigma \in G_L : \sigma(y_i)/y_i \in \mathcal{C}^* \text{ for } i = 1, 2, 3\} \subseteq G_L$. Then T is a maximal torus of G_L. We have*

$$\sigma(y_i)/y_i = \sigma(R_i)/R_i, i = 1, 2, 3, \text{ for all } \sigma \in T. \tag{4.8}$$

   The map $\sigma \mapsto \sigma|_{K_{L_{\mathrm{red}}}}$ gives an isomorphism of T onto $G_{L_{\mathrm{red}}}$.

Proof. Items 1 and 2 are proved by straightforward calculations. We prove Item 3 as follows. First note that $V_{D-r_1} = \mathrm{span}_{\mathcal{C}}\{y_1\}$ and $V_{(D-r_2)\circ(D-r_1)} = \mathrm{span}_{\mathcal{C}}\{y_1, y_2\}$ are G_L-invariant subspaces of V_L, so that $[G_L]_{\mathcal{F}_{(r_1,r_2)}} \subseteq \mathsf{T}_3$. It is now clear that $[G_L]_{\mathcal{F}_{(r_1,r_2)}}$ has Levi decomposition

$$[G_L]_{\mathcal{F}_{(r_1,r_2)}} = ([G_L]_{\mathcal{F}_{(r_1,r_2)}} \cap \mathsf{U}_3)([G_L]_{\mathcal{F}_{(r_1,r_2)}} \cap \mathsf{D}_3) \text{ semidirect product of subgroups.}$$

We now see that $T = [G_L]_{\mathcal{F}_{(r_1,r_2)}} \cap \mathsf{D}_3$ is a Levi subgroup of G_L. Next, notice that

$$y_1 = R_1, (D - r_1)(y_2) = R_2, ((D - r_2) \circ (D - r_1))(y_3) = R_1^{-1} R_2^{-1} h.$$

Given $\sigma \in T$, suppose $\sigma(y_i) = t_i y_i$ for some $t_i \in \mathcal{C}^*$ for $i = 1, 2, 3$. We compute

$$\begin{aligned} \sigma(R_2) &= \sigma((D - r_1)(y_2)) \\ &= (D - r_1)(\sigma(y_2)) = (D - r_1)(t_2 y_2) \\ &= t_2 (D - r_1)(y_2) = t_2 R_2, \end{aligned}$$

and a similar computation shows that $\sigma(R_1^{-1} R_2^{-1} h) = t_3 R_1^{-1} R_2^{-1} h$; (4.8) follows easily. The last statement follows from the fact that a member of T (resp., of $G_{L_{\mathrm{red}}}$) is determined by its action on $\mathcal{F}_{(r_1,r_2)}$ (resp., on $\{R_1, R_2, R_1^{-1} R_2^{-1} h\}$).

■

The following three lemmas will be used to decide the Galois group of an operator $L = D^3 + aD + b, a, b \in \mathcal{C}[x]$, in case L has a unique monic factor L_i of order i for $i = 1, 2$ such that G_L is solvable and acts trivially on V_{L_2}/V_{L_1}. Remark that these results can be easily generalized to the case in which L is a third-order operator whose only singularities in the finite plane are apparent singularities and whose Galois group is unimodular.

Lemma 4.6.3 *Let k be a differential field whose constant field is algebraically closed and has characteristic zero. Let $r \in k$. Then there is a unique ring automorphism $\mathrm{shift}_r : k[D] \to k[D]$ such that $\mathrm{shift}_r(D) = D - r$ and $\mathrm{shift}_r(h) = h$ for all $h \in k$. Moreover, if $k(\eta)/k$ is a Picard-Vessiot extension such that $\eta'/\eta = r$, then*

$$\mathrm{shift}_r(L) = \eta \circ L\eta^{-1} \in k(\eta)[D] \text{ for all } L \in k[D].$$

Proof. This lemma is an easy exercise using the relevant definitions.

■

Lemma 4.6.4 *Given: $L = D^3 + aD + b = (D + r_1 + r_2) \circ (D - r_2) \circ (D - r_1), a, b \in \mathcal{C}[x], r_1, r_2 \in \mathcal{C}(x)$, and $g \in \mathcal{C}(x) \setminus \{0\}$ such that $r_2 = g'/g$ and the only monic right factors of L are*

$$1, L_1 = D - r_1, L_2 = (D - r_2) \circ (D - r_1), \text{ and } L.$$

Let y_1, y_2, ξ, y_3 be as defined in Lemma 4.6.2.

1. *Define $\tilde{L}_2 = (D + r_1 + r_2) \circ (D - r_2)$, the unique monic left factor of L of order 2. Then g, ξ span a full set of solutions of $\tilde{L}_2$ in K_L, so we may write $k \subseteq K_{\tilde{L}_2} \subseteq K_L$. $D - r_2$ is the only monic right factor of $\tilde{L}_2$ of order 1.*

2. *Define $L_2^\sharp = (D - 3r_2) \circ (D - r_1 - 2r_2) = \mathrm{shift}_{2r_2}(L_2)$. Then g^2y_1, g^2y_2 span a full set of solutions of $L_2^\sharp$ in K_L, so we may write $k \subseteq K_{L_2^\sharp} \subseteq K_L$. $D - r_1 - 2r_2$ is the only monic right factor of $L_2^\sharp$ of order 1.*

3. *Define $\tilde{L}_2^\sharp = D \circ (D - r_1 - 2r_2) = \mathrm{shift}_{r_1+r_2}(\tilde{L}_2)$. Then $g^2y_1, gy_1\xi$ span a full set of solutions of $\tilde{L}_2^\sharp$ in K_L, so we may write $k \subseteq K_{\tilde{L}_2^\sharp} \subseteq K_L$. $D - r_1 - 2r_2$ is the only monic right factor of $\tilde{L}_2^\sharp$ of order 1.*

4. *Define* $\hat{y}_3 = \frac{1}{2}y_1^{-1}y_2^2$ *and let* $\hat{L} = (D - 2r_2 + r_1) \circ L_2$. *Then* $\hat{\mathcal{B}} = \{y_1, y_2, \hat{y}_3\}$ *is an (ordered) basis of solutions of* $\hat{L}$ *in* K_L, *so we may write* $k \subseteq K_{\hat{L}} \subseteq K_L$.

Proof. These statements are all verified by straightforward computations using known facts.

■

Lemma 4.6.5 *Given:* $L = D^3 + aD + b = (D + r_1 + r_2) \circ (D - r_2) \circ (D - r_1), a, b \in \mathcal{C}[x], r_1, r_2 \in \mathcal{C}(x)$, *and* $g \in \mathcal{C}(x) \setminus \{0\}$ *such that* $r_2 = g'/g$ *and the only monic right factors of* L *are*

$$1, L_1 = D - r_1, L_2 = (D - r_2) \circ (D - r_1), \text{ and } L.$$

Let the elements y_1, y_2, ξ, y_3 *be as defined in Lemma 4.6.2. Let the operators* $\tilde{L}_2, L_2^\sharp, \tilde{L}_2^\sharp$ *and* $\hat{L}$ *be as defined in Lemma 4.6.4.*

1. *There exists a basis* $\mathcal{A} = \{\eta_1, \eta_2, \eta_3\}$ *of* V_L *such that* $[G_L]_\mathcal{A}$ *is one of*

$$\left\{U^1_{(1,1)}T_{(1,0)}, U^2_{(1,1)}T_{(1,0)}, \mathsf{U}_3T_{(1,0)}\right\}.$$

2. *We have* $y_1, y_2, \xi, y_3 \notin \mathcal{C}(x)$.

3. *The following are equivalent:*

   (a) $[G_L]_\mathcal{A} = U^d_{(1,1)}T_{(1,0)}$ *for* $d = 1$ *or* 2.

   (b) $L_2^\sharp$ *is equivalent to* $\tilde{L}_2^\sharp$ *over* $\mathcal{C}(x)$.

   (c) *The equation* $(D - r_1 - 2r_2)(y) = g^3 + c$ *admits a* $\mathcal{C}(x)$*-rational solution for some* $c \in \mathcal{C} \setminus \{0\}$.

   (d) *The equation* $\big(D \circ (D - r_1 - 2r_2)\big)(y) = r_2g^3$ *admits a* $\mathcal{C}(x)$*-rational solution.*

4. *The following are equivalent:*

   (a) $[G_L]_\mathcal{A} = U^1_{(1,1)}T_{(1,0)}$.

   (b) L *and* $\hat{L}$ *are equivalent over* $\mathcal{C}(x)$.

   (c) *The equation* $\big((D - r_1 - 2r_2) \circ (D - 2r_1 - r_2)\big)(y) = g^3 + c$ *admits a* $\mathcal{C}(x)$*-rational solution for some* $c \in \mathcal{C} \setminus \{0\}$.

   (d) *The equation* $\big(D \circ (D - r_1 - 2r_2) \circ (D - 2r_1 - r_2)\big)(y) = r_2g^3$ *admits a* $\mathcal{C}(x)$*-rational solution.*

Proof.

1. By Corollary 4.1.3 and Theorem 4.1.5, there exists a basis $\mathcal{A} = \{\eta_1, \eta_2, \eta_3\}$ of V_L such that $[G_L]_{\mathcal{A}}$ is one of the subgroups listed in Theorem 4.1.5 having exactly one invariant subspace of dimension 1 (resp., 2). Moreover, since L_1 maps V_{L_2} onto $V_{D-r_2} = \text{span}_{\mathcal{C}}\{g\} \subseteq \mathcal{C}(x)$, we see that G_L acts trivially on V_{L_2}/V_{L_1}. The only subgroups listed in Theorem 4.1.5 having these properties are $U^1_{(1,1)}T_{(1,0)}, U^2_{(1,1)}T_{(1,0)}$ and $\mathsf{U}_3T_{(1,0)}$.

2. Let $\mathcal{A} = \{\eta_1, \eta_2, \eta_3\}$ be as described in Item 1 of the conclusion of the lemma. From the possibilities for $[G_L]_{\mathcal{A}}$, we see that there exist $\sigma_0, \tau_0 \in G_L$ such that

$$[\sigma_0]_{\mathcal{A}} = \text{diag}(t_0, 1, t_0^{-1}),\ t_0 \in \mathcal{C}^*,$$

and

$$[\tau_0]_{\mathcal{A}} = \begin{bmatrix} 1 & a_0 & b_0 \\ 0 & 1 & c_0 \\ 0 & 0 & 1 \end{bmatrix},\ a_0, b_0, c_0 \in \mathcal{C}, a_0 \neq 0, c_0 \neq 0.$$

One checks that, for all $v \in V_L \backslash \{0\}$, either $\sigma_0(v) \neq v$ or $\tau_0(v) \neq v$, so that v lies outside the fixed field $\mathcal{C}(x)$ of G_L. This yields $y_1, y_2, y_3 \notin \mathcal{C}(x)$. Finally, notice that L_1 maps $\mathcal{A}$ onto a basis of $V_{\tilde{L}_2}$ and that $L_1(\eta_1) = 0$; it follows that the set $\tilde{\mathcal{A}}_2 = \{L_1(\eta_2), L_1(\eta_3)\}$ is an (ordered) basis of $V_{\tilde{L}_2}$. Moreover, we have that $[\tau]_{\tilde{\mathcal{A}}_2} = \begin{bmatrix} 1 & c_0 \\ 0 & 1 \end{bmatrix}$ with $c_0 \neq 0$; it follows that $V_{\tilde{L}_2} \not\subseteq \mathcal{C}(x)$. By Item 2 of Lemma 4.6.4, another basis of $V_{\tilde{L}_2}$ is $\{g, \xi\}$. Since $g \in \mathcal{C}(x)$ and $V_{\tilde{L}_2} \not\subseteq \mathcal{C}(x)$, we have $\xi \notin \mathcal{C}(x)$.

3. First of all, we show that the first and second conditions are equivalent, as follows. Let $\mathcal{A}_2 = \{\eta_1, \eta_2\}$; it is clear that $\mathcal{A}_2$ is an (ordered) basis of V_{L_2}. We also see that $\mathcal{A}_2^\sharp = \{g^2\eta_1, g^2\eta_2\}$ (resp., $\tilde{\mathcal{A}}_2^\sharp = \{g\eta_1 L_1(\eta_2), g\eta_1 L_1(\eta_3)\}$) is an (ordered) basis of $V_{L_2^\sharp}$ (resp., $V_{\tilde{L}_2^\sharp}$). Let G_L have Levi decomposition $G_L = R_u T$ (semidirect product of subgroups). From Item 1 of the conclusion of the lemma, we see that $[R_u]_{\mathcal{A}} \subseteq \mathsf{U}_3$ and $[T]_{\mathcal{A}} = T_{(1,0)}$. Let σ be a typical element of T, and write

$$[\sigma]_{\mathcal{A}} = \text{diag}(t_\sigma, 1, t_\sigma^{-1}),\ t_\sigma \in \mathcal{C}^*. \tag{4.9}$$

One checks that

$$[\sigma]_{\tilde{\mathcal{A}}_2} = \begin{bmatrix} 1 & 0 \\ 0 & t_\sigma^{-1} \end{bmatrix}, [\sigma]_{\mathcal{A}_2} = [\sigma]_{\mathcal{A}_2^\sharp} = [\sigma]_{\tilde{\mathcal{A}}_2^\sharp} = \begin{bmatrix} t_\sigma & 0 \\ 0 & 1 \end{bmatrix}.$$

It follows that $V_{L_2^\sharp}$ and $V_{\tilde{L}_2^\sharp}$ are isomorphic as T-modules. Thus, they are isomorphic as G_L-modules if and only if they are isomorphic as R_u-modules. Let τ be a typical element of R_u, and write

$$[\tau]_{\mathcal{A}} = \begin{bmatrix} 1 & a_\tau & b_\tau \\ 0 & 1 & c_\tau \\ 0 & 0 & 1 \end{bmatrix}, \ a_\tau, b_\tau, c_\tau \in \mathcal{C}. \tag{4.10}$$

A calculation shows that

$$[\tau]_{\mathcal{A}_2} = [\tau]_{\mathcal{A}_2^\sharp} = \begin{bmatrix} 1 & a_\tau \\ 0 & 1 \end{bmatrix}, [\tau]_{\tilde{\mathcal{A}}_2} = [\tau]_{\tilde{\mathcal{A}}_2^\sharp} = \begin{bmatrix} 1 & c_\tau \\ 0 & 1 \end{bmatrix}.$$

From here, one checks that $V_{L_2^\sharp}$ and $V_{\tilde{L}_2^\sharp}$ are isomorphic as R_u-modules if and only if there exists a nonzero constant α such that $a_\tau = \alpha c_\tau$ for all $\tau \in R_u$. The latter condition holds (with $\alpha = 1$) if $R_u \subseteq U^2_{(1,1)}$ and fails if $R_u = \mathsf{U}_3$. Equivalence of the first two statements is now clear.

Before proceeding, we make some auxiliary computations:

$$\begin{aligned} (D - r_1 - 2r_2)(g^2 y_1) &= (g^2)' y_1 + g^2 y_1' - (r_1 + 2r_2) g^2 y_1 \\ &= 2r_2 g^2 y_1 + r_1 g^2 y_1' - (r_1 + 2r_2) g^2 y_1 \\ &= 0; \end{aligned} \tag{4.11}$$

$$\begin{aligned} (D - r_1 - 2r_2)(g^2 y_2) &= (g^2)' y_2 + g^2 y_2' - (r_1 + 2r_2) g^2 y_2 \\ &= 2r_2 g^2 y_2 + g^2 (r_1 y_2 + g) - (r_1 + 2r_2) g^2 y_2 \\ &= g^3; \end{aligned} \tag{4.12}$$

$$\begin{aligned} (D - r_1 - 2r_2)(g y_1 \xi) &= (g y_1)' \xi + g y_1 \xi' - (r_1 + 2r_2) g y_1 \xi \\ &= (r_1 + r_2) g y_1 \xi + g y_1 (r_2 \xi + g^{-1} y_1^{-1}) - (r_1 + 2r_2) g y_1 \xi \\ &= 1. \end{aligned} \tag{4.13}$$

Next we show that the second condition implies the third condition. Suppose $R, S \in \mathcal{D}$ are operators of order at most 1 such that $L_2^\sharp R = S \tilde{L}_2^\sharp$. Then R maps $V_{\tilde{L}_2^\sharp}$ isomorphically onto $V_{L_2^\sharp}$ in K_L. From Items 3 and 4 of Lemma 4.6.4, we see that R maps $V_{D-r_1-2r_2} = \operatorname{span}_{\mathcal{C}} \{g^2 y_1\}$ isomorphically onto itself; since this is an irreducible G_L-module, it follows that $R|_{V_{D-r_1-2r_2}} = c_0 \operatorname{id}_{V_{D-r_1-2r_2}}$ for some $c_0 \in \mathcal{C} \setminus \{0\}$. This in turn implies that $R = f(D - r_1 - 2r_2) + c_0 \in \mathcal{D}$ for some $f \in \mathcal{C}(x)$. We have that R maps the basis element $g y_1 \xi$ of $V_{\tilde{L}_2^\sharp}$ onto some element of $V_{L_2^\sharp} \setminus V_{D-2r_2}$. Using the basis of $V_{L_2^\sharp}$ given in Item 4 of Lemma 4.6.4, we see that $R(g y_1 \xi) = \alpha g^2 y_1 + \beta g^2 y_2$ for some $\alpha, \beta \in \mathcal{C}, \beta \neq 0$.

We now compute:

$$\begin{aligned} R(gy_1\xi) &= \big(f(D-r_1-2r_2)+c_0\big)(gy_1\xi) \\ &= f(D-r_1-2r_2)(gy_1\xi)+c_0gy_1\xi \\ &= f+c_0gy_1\xi \text{ by (4.13)}, \end{aligned}$$

so that

$$f+c_0gy_1\xi = \alpha g^2y_1+\beta g^2y_2,\ \alpha,\beta\in\mathcal{C},\beta\neq 0.$$

Applying $D-r_1-2r_2$ to each side of this equation yields

$$\begin{aligned} (D-r_1-2r_2)(f)+c_0 &= \alpha(D-r_1-2r_2)(g^2y_1)+\beta(D-r_1-2r_2)(g^2y_2) \\ &= \beta g^3 \text{ by (4.11), (4.12) and (4.13).} \end{aligned}$$

It follows that $y=\beta^{-1}f\in\mathcal{C}(x), c=-\beta^{-1}c_0\in\mathcal{C}\setminus\{0\}$ satisfy

$$(D-r_1-2r_2)(y)=g^3+c,$$

so that the third condition holds.

Next we show that the third condition implies the second condition. Suppose $(D-r_1-2r_2)(f)=g^3+c$ for some $f\in\mathcal{C}(x), c\in\mathcal{C}\setminus\{0\}$. Define $R=f(D-r_1-2r_2)-c\in\mathcal{D}$. The following computations show that R maps $V_{\tilde{L}_2^\sharp}$ isomorphically onto $V_{L_2^\sharp}$, so that the second condition holds. Consider the action of R on the basis $\left\{g^2y_1, gy_1\xi\right\}$ of $V_{\tilde{L}_2^\sharp}$ given in Item 4 of Lemma 4.6.4. First we compute

$$\begin{aligned} R(g^2y_1) &= \big(f(D-r_1-2r_2)-c\big)(g^2y_1) \\ &= -cg^2y_1 \text{ by (4.11).} \end{aligned} \tag{4.14}$$

Next, we claim that $R(gy_1\xi)$ is a solution of the equation $(D-r_1-2r_2)(y)=g^3$. Indeed, we have

$$\begin{aligned} (D-r_1-2r_2)(R(gy_1\xi)) &= \big((D-r_1-2r_2)\circ R\big)(gy_1\xi) \\ &= \Big((D-r_1-2r_2)\circ\big(f(D-r_1-2r_2)-c\big)\Big)(gy_1\xi) \\ &= \Big((D-r_1-2r_2)\circ f(D-r_1-2r_2)\Big)(gy_1\xi)- \\ &\quad c(D-r_1-2r_2)(gy_1\xi) \\ &= (D-r_1-2r_2)(f)-c \text{ by (4.13)} \\ &= (g^3+c)-c \text{ by hypothesis} \\ &= g^3. \end{aligned}$$

This result, together with (4.12), implies that g^2y_2 and $R(gy_1\xi)$ differ by a member of $V_{D-r_1-2r_2}$. By (4.11), we have that $V_{D-r_1-2r_2} = \text{span}_{\mathcal{C}}\left\{g^2y_1\right\}$. Thus, we have

$$R(gy_1\xi) = g^2y_2 + \tilde{c}g^2y_1 \text{ for some } \tilde{c} \in \mathcal{C}. \tag{4.15}$$

By Item 3 of Lemma 4.6.4, we have that $\left\{g^2y_1, g^2y_2\right\}$ is a basis of $V_{L_2^\sharp}$. In light of this fact, we conclude from formulas (4.14) and (4.15) that R maps $\left\{g^2y_1, gy_1\xi\right\}$ onto a basis of $V_{L_2^\sharp}$; the desired result follows.

To prove that the third condition implies the fourth condition, simply differentiate both sides of the equation given in the third condition and divide by 3.

Finally we show that the fourth condition implies the third condition. Suppose

$$(D \circ (D - r_1 - 2r_2))(\bar{f}) = r_2 g^3$$

for some $\bar{f} \in \mathcal{C}(x)$. This condition can be rewritten (after defining $f = 3\bar{f}$) as

$$\left[(D - r_1 - 2r_2)(f)\right]' = [g^3]',$$

or $\left((D-r_1-2r_2)(f) - g^3\right)' = 0$, which in turn implies that $(D-r_1-2r_2)(f) = g^3 + c$ for some $c \in \mathcal{C}$. We must show that $c \neq 0$. Suppose instead that $c = 0$. This yields $(D - r_1 - 2r_2)(f) = g^3$. One then checks that $f \in V_{L_2^\sharp}$. Recall that $g \in \mathcal{C}(x)$ and (by Item 2 of the lemma) $y_1, y_2 \notin \mathcal{C}(x)$. It follows from Item 3 of Lemma 4.6.4 that $V_{L_2^\sharp} \cap \mathcal{C}(x) = \{0\}$, so that $f = 0$. This yields

$$g^3 = (D - r_1 - 2r_2)(f) = 0$$

and therefore $g = 0$, contradicting hypothesis on g. This completes the proof.

4. First of all, we compute a matrix representation of the action of G_L on $V_{\hat{L}}$ with respect to a certain basis; this will be useful in proving that the first two conditions are equivalent. Let $\mathcal{A} = \{\eta_1, \eta_2, \eta_3\}$ be as in Item 1 of the conclusion of the lemma. Let $\hat{\eta}_3 = \dfrac{1}{2}\eta_1^{-1}\eta_2^2$. One checks that $(D - r_1)(\eta_1) = 0$ and $(D - r_1)(\eta_2) = \alpha_0 g$ for some $\alpha_0 \in \mathcal{C} \setminus \{0\}$; using these facts, a straightforward set of computations shows that $\hat{\mathcal{A}} = \{\eta_1, \eta_2, \hat{\eta}_3\}$ is an (ordered) basis of $V_{\hat{L}}$. Let $G_L = R_uT$ be a Levi decomposition as above. Let $\sigma \in T$ and let $t_\sigma \in \mathcal{C}^*$ be as in (4.9). Thus $\sigma(\eta_1) = t_\sigma\eta_1$ and $\sigma(\eta_2) = \eta_2$; it follows that $\sigma(\hat{\eta}_3) = t_\sigma^{-1}\hat{\eta}_3$, so that $[\sigma]_{\hat{\mathcal{A}}} = \text{diag}(t_\sigma, 1, t_\sigma^{-1})$. We conclude that $[T]_{\hat{\mathcal{A}}} = T_{(1,0)}$. Next let $\tau \in R_u$ and let $a_\tau, b_\tau, c_\tau \in \mathcal{C}$ be as in (4.10). Thus $\tau(\eta_1) = \eta_1$

and $\tau(\eta_2) = \eta_2 + a_\tau \eta_1$. We compute

$$\begin{aligned}\tau(\eta_3) &= \frac{1}{2}\eta_1^{-1}(\eta_2 + a_\tau\eta_1)^2 \\ &= \frac{1}{2}\eta_1^{-1}(\eta_2^2 + 2a_\tau\eta_1\eta_2 + a_\tau^2\eta_1^2) \\ &= \hat{\eta}_3 + a_\tau\eta_2 + \frac{1}{2}a_\tau^2\eta_1.\end{aligned}$$

We now see that

$$[\tau]_{\mathcal{A}} = \begin{bmatrix} 1 & a_\tau & \frac{1}{2}a_\tau^2 \\ 0 & 1 & a_\tau \\ 0 & 0 & 1 \end{bmatrix}$$

and therefore that $[R_u]_{\hat{\mathcal{A}}} = U^1_{(1,1)}$. We conclude that $[G_L]_{\hat{\mathcal{A}}} = U^1_{(1,1)}T_{(1,0)}$.

Now, suppose the first condition holds. Then, it is clear that the map from V_L to $V_{\hat{L}}$ defined on basis elements by

$$\eta_i \mapsto \eta_i \text{ for } i = 1, 2, \;\; \eta_3 \mapsto \hat{\eta}_3,$$

gives an isomorphism of G_L-modules, so that the second condition holds.

Suppose now that the first condition fails. Then, Item 1 of the conclusion of the lemma implies that the unipotent radical of G_L has dimension 2 or 3. By contrast, we have $[G_L]_{\hat{\mathcal{A}}} = U^1_{(1,1)}T_{(1,0)}$, so that $G_{\hat{L}} \simeq U^1_{(1,1)}T_{(1,0)}$ has a one-dimensional unipotent radical; we now see that the second condition fails. By contrapositive, we conclude that the second condition implies the first condition.

Next we show that the second condition implies the third condition. Let $\Phi, \Psi \in \mathcal{D}$ be operators of order at most 2 such that $\hat{L}\Phi = \Psi L$. We have that V_{L_2} is the unique 2-dimensional G_L-invariant subspace of V_L (resp., of $V_{\hat{L}}$) by hypothesis (resp., by examining $[G_L]_{\hat{\mathcal{A}}}$). It follows that $\Phi|_{V_{L_2}}$ is a G_L-invariant automorphism of V_{L_2}. Thus, we have that $[\Phi]_{\mathcal{A}_2}$ commutes with $[G_L]_{\mathcal{A}_2} = \mathsf{U}_2 T_2$, where $T_2 = \{\mathrm{diag}(t, 1) : t \in \mathcal{C}^*\}$. A straightforward set of computations shows that

$$\begin{aligned}\underset{\mathsf{GL}_2}{\mathrm{Cen}}(\mathsf{U}_2) &= \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} : \alpha \in \mathcal{C}^*, \beta \in \mathcal{C} \right\}, \\ \underset{\mathsf{GL}_2}{\mathrm{Cen}}(T_2) &= \mathsf{D}_2.\end{aligned}$$

Since $[\Phi]_{\mathcal{A}_2}$ is contained in the intersection of these two subgroups of GL_2, we conclude that $\Phi|_{V_{L_2}} = \alpha\, \mathrm{id}_{V_{L_2}}$ for some $\alpha \in \mathcal{C} \setminus \{0\}$. This implies that $\Phi = hL_2 + \alpha$ for some

$h \in \mathcal{C}(x)$. Next we consider the basis $\{y_1, y_2, y_3\}$ of V_L and the basis $\{y_1, y_2, \hat{y}_3\}$ of $V_{\hat{L}}$ as defined in Lemma 4.6.4. Since Φ is an isomorphism that restricts to $\alpha\,\mathrm{id}$ on V_{L_2}, we see that

$$\Phi(y_3) = \beta\hat{y}_3 + y_0 \text{ for some } \beta \in \mathcal{C}^*, y_0 \in V_{L_2}.$$

Before proceeding further, remark that

$$L_2(y_3) = g^{-1}y_1^{-1} \tag{4.16}$$

and

$$L_2(\hat{y}_3) = g^2 y_1^{-1}; \tag{4.17}$$

these equalities can be verified by direct computation. Putting facts together, we obtain

$$\begin{aligned}
L_2(\Phi(y_3)) &= \beta g^2 y_1^{-1} \\
\Rightarrow \beta g^2 y_1^{-1} &= L_2(\Phi(y_3)) = L_2((hL_2 + \alpha)(y_3)) \\
&= (L_2 \circ (hL_2 + \alpha))(y_3) = L_2(hL_2(y_3)) + \alpha L_2(y_3) \\
&= L_2(hg^{-1}y_1^{-1}) + \alpha g^{-1}y_1^{-1} \text{ by (4.16)} \\
\Rightarrow \beta g^3 &= gy_1 L_2(hg^{-1}y_1^{-1}) + \alpha \text{ (after multiplying by } gy_1) \\
&= (gy_1 \circ L_2 \circ g^{-1}y_1^{-1})(h) + \alpha \\
&= (\mathrm{shift}_{r_1+r_2}(L_2))(h) + \alpha.
\end{aligned}$$

The third condition now follows easily after observing that

$$\mathrm{shift}_{r_1+r_2}(L_2) = (D - r_1 - 2r_2) \circ (D - 2r_1 - r_2).$$

Next we show that the third condition implies the second condition. Suppose

$$(\mathrm{shift}_{r_1+r_2}(L_2))(h) = g^3 + c$$

for some $c \in \mathcal{C} \setminus \{0\}$. Define $\Phi = hL_2 - c$. Then $\Phi(y_i) = -cy_i$ for $i = 1, 2$. Also, we compute

$$\begin{aligned}
\Phi(y_3) &= (hL_2 - c)(y_3) = hg^{-1}y_1^{-1} - cy_3 \text{ by (4.16)} \\
\Rightarrow L_2(\Phi(y_3)) &= L_2(hg^{-1}y_1^{-1}) - cg^{-1}y_1^{-1} \text{ by (4.16)} \\
&= g^{-1}y_1^{-1}(gy_1 L_2(hg^{-1}y_1^{-1}) - c)\text{(after distributing out } g^{-1}y_1^{-1})
\end{aligned}$$

$$
\begin{aligned}
&= g^{-1}y_1^{-1}((\mathrm{shift}_{r_1+r_2}(L_2))(h) - c) \\
&= g^{-1}y_1^{-1}((g^3 + c) - c) \text{ by hypothesis} \\
&= g^2 y_1^{-1}.
\end{aligned}
$$

This result, together with (4.17), implies that $\Phi(y_3) = \hat{y}_3 + y_0$ for some $y_0 \in V_{L_2}$. We now see that Φ maps a basis of V_L isomorphically onto a basis of $V_{\hat{L}}$, and the second condition follows.

To prove that the third condition implies the fourth condition, simply differentiate both sides of the equation given in the third condition and divide by 3.

To prove that the fourth condition implies the third condition, suppose

$$(D \circ (D - r_1 - 2r_2) \circ (D - 2r_1 - r_2))(\bar{h}) = r_2 g^3$$

for some $\bar{h} \in \mathcal{C}(x)$. Let $h = 3\bar{h}$. It is then easy to check that

$$((D - r_1 - 2r_2) \circ (D - 2r_1 - r_2))(h) = g^3 + c$$

for some $c \in \mathcal{C}$. We must show that $c \neq 0$. Suppose instead that $c = 0$. Then the rational function $\tilde{h} = (D - 2r_1 - r_2)(h)$ satisfies $(D - r_1 - 2r_2)(\tilde{h}) = g^3$. As in the last step of the proof of Item 3 of the lemma, we see that $\tilde{h} \in V_{L_2^\sharp} \cap \mathcal{C}(x) = \{0\}$ and therefore that $g = 0$, contradicting hypothesis. This completes the proof.

■

Below, we state the Kolchin-Ostrowski theorem (Theorem 4.6.6) and a corollary (Corollary 4.6.7). In case $\mathcal{C} = \bar{Q}$, these results lead to an effective criterion (Lemma 4.6.9) to compute the maximal torus of G_L and its representation $[T]_{\mathcal{F}_{(r_1,r_2)}}$, where T and $\mathcal{F}_{(r_1,r_2)}$ are as defined in Lemma 4.6.2, in case G_L is solvable.

Theorem 4.6.6 *Given a Picard-Vessiot extension K/k and a set $S = \{f_1, \ldots, f_\nu\} \in K$ such that $\frac{f_i'}{f_i} \in k$ for $1 \leq i \leq \nu$. Then S is algebraically dependent over k if and only if there exist integers m_i, not all zero, such that $\prod_{i=1}^{\nu} f_i^{m_i} = g$ for some $g \in k$.*

Proof. This result is stated and proved in [Kol68].

■

Corollary 4.6.7 *Given: L is an operator of the form*

$$L = \mathrm{LCLM}(D - s_1, D - s_2, D + s_1 + s_2 - h'/h),\ \ s_1, s_2, h \in \mathcal{C}(x),$$

such that G_L is isomorphic to either $\mathcal{C}^*$ or $\mathcal{C}^* \times \mathcal{C}^*$. Then, the following are equivalent:

1. $G_L \simeq \mathcal{C}^*$
2. *S_1 and S_2 are algebraically dependent over $\mathcal{C}(x)$, where $S_i'/S_i = s_i$ for $i = 1, 2$*
3. *$m_1 s_1 + m_2 s_2 = \frac{g'}{g}$ for some $m_1, m_2 \in \mathbb{Z}$, not both zero, and $g \in \mathcal{C}(x) \setminus \{0\}$.*

Proof. First, observe that V_L is spanned by S_1, S_2 and $S_1^{-1}S_2^{-1}h$. It follows that K_L/k is generated by S_1 and S_2. Equivalence of the first two conditions now follows from the well-known fact (see, for instance, [Mag94]) that the transcendence degree of a Picard-Vessiot extension is equal to the dimension of the corresponding Galois group. Equivalence of the second and third conditions follows easily from Theorem 4.6.6 after taking logarithmic derivatives.

■

Before proceeding, we provide an example of the criterion for algebraic dependence given in Corollary 4.6.7. Given: S_1, S_2 are members of a Picard-Vessiot extension of $\bar{\mathbb{Q}}(x)$ satisfying

$$\begin{aligned} \frac{S_1'}{S_1} = s_1 &= 6x^2 + \frac{7 + 9\sqrt{2}}{x}, \\ \frac{S_2'}{S_2} = s_2 &= 2x^2 + \frac{1 + 3\sqrt{2}}{x}. \end{aligned}$$

Are S_1 and S_2 algebraically dependent over $\mathbb{Q}(x)$? To answer this question, we write

$$\begin{aligned} s_1 &= \left(\frac{7}{x}\right) + \left(6x^2 + \frac{9\sqrt{2}}{x}\right), \\ s_2 &= \left(\frac{1}{x}\right) + \left(2x^2 + \frac{3\sqrt{2}}{x}\right). \end{aligned}$$

It is now easy to see that $s_1 - 3s_2 = 4/x$ and therefore that $S_1/S_2^3 = x^4$. We conclude that S_1 and S_2 are indeed algebraically dependent over $\mathbb{Q}(x)$.

What follows can be viewed as a generalization of the steps taken in the above example.

Let $\mathcal{C}_0$ be a finite algebraic extension of $\mathbb{Q}$, specified by a set of generators $z_1, \ldots, z_\lambda$ and minimal polynomials

$$p_1 \in \mathbb{Q}[x], p_2 \in \mathbb{Q}(z_1)[x], \ldots, p_\lambda \in \mathbb{Q}(z_1, \ldots, z_{\lambda-1})[x].$$

It is a fact (cf. [Bro96]) that every rational function $f \in \mathcal{C}_0(x)$ admits a unique partial fraction or "PF" decomposition over $\mathcal{C}_0$, written as follows:

$$f = P + \sum_{j=1}^{t} \sum_{d=1}^{\mu_j} \frac{A_{j,d}}{Q_j^d}, \tag{4.18}$$

where:

1. $P \in \mathcal{C}_0[x]$
2. t is a nonnegative integer and μ_j is a positive integer for all j
3. $Q_j \in \mathcal{C}_0[x]$ is monic and irreducible for all j
4. $A_{j,d} \in \mathcal{C}_0[x]$ for all j, d
5. $\deg A_{j,d} < \deg Q_j$ for all j, d.

There are effective algorithms to carry out this decomposition ([Bro96]). We can also carry out the PF decomposition of $f \in \mathcal{C}_0(x)$ over $\bar{\mathbb{Q}}$:

$$f = P + \sum_{i=1}^{s} \sum_{d=1}^{\nu_i} \frac{c_{i,d}}{(x - \alpha_i)^d}, \tag{4.19}$$

where:

1. P is as in (4.18)
2. s is a nonnegative integer and ν_i is a positive integer for all i
3. $\alpha_i \in \bar{\mathbb{Q}}$ for all i
4. $c_{i,d} \in \bar{\mathbb{Q}}$ for all i, d.

Lemma 4.6.8 *Given $f \in \mathcal{C}_0(x)$. Suppose the PF decomposition of f over $\mathcal{C}_0$ (resp., over $\bar{\mathbb{Q}}$) is as given in (4.18) (resp., (4.19)). The following are equivalent:*

1. *$f = g'/g$ for some $g \in \bar{\mathbb{Q}}(x)$*
2. *The following three conditions hold:*

(i) $P = 0$

(ii) $c_{i,d} = 0$ *for all* $d > 1$ *and all* i

(iii) *For all* i*, we have* $c_{i,1} \in \mathbb{Z}$.

3. *The following three conditions hold:*

(i′) $P = 0$

(ii′) $A_{j,d} = 0$ *for all* $d > 1$ *and all* j

(iii′) *For all* j*, there exists* $n_j \in \mathbb{Z}$ *such that* $A_{j,1} = n_j Q_j'$.

4. $f = g'/g$ *for some* $g \in \mathcal{C}_0(x)$

Proof. Equivalence of the conditions numbered 1 and 2 follows after considering Laurent series expansions of the equation $y' - fy = 0$ over $\bar{\mathbb{Q}}(x)$ at its singularities in the finite plane and at infinity.

Next, we show that Condition 2 implies Condition 3. Condition (i′) follows immediately from Condition (i). Condition (ii) implies that the denominator of f is squarefree; this yields Condition (ii′). We prove Condition (iii′) as follows: Condition 2 implies that

$$f = \sum_i \frac{c_i}{x - \alpha_i}, \;\; \alpha_i \in \bar{\mathbb{Q}}, c_i \in \mathbb{Z} \text{ for each } i.$$

We see that for each i, the minimal polynomial of α_i over $\mathcal{C}_0$ is Q_j for some j. Thus, we may write

$$f = \sum_j \sum_{i:Q_j(\alpha_i)=0} \frac{c_i}{x - \alpha_i}. \tag{4.20}$$

We claim that for each j, there exists $n_j \in \mathbb{Z}$ such that $c_i = n_j$ for all i such that $Q_j(\alpha_i) = 0$. Indeed, define $Q = \prod_j Q_j$ and let $\mathcal{C}_Q/\mathcal{C}_0$ be a splitting field extension for Q. Let $\sigma \in \mathrm{Gal}(\mathcal{C}_Q/\mathcal{C}_0)$. We may apply σ to members of $\mathcal{C}_Q(x)$; in particular, we have $\sigma(h) = h$ for all $h \in \mathcal{C}_0(x)$. Applying this fact to (4.20) yields

$$\begin{aligned}
\sum_j \sum_{i:Q_j(\alpha_i)=0} \frac{c_i}{x - \alpha_i} &= f \\
&= \sigma(f) \text{ since } f \in \mathcal{C}_0(x) \\
&= \sum_j \sum_{i:Q_j(\alpha_i)=0} \sigma\left(\frac{c_i}{x - \alpha_i}\right) \\
&= \sum_j \sum_{i:Q_j(\alpha_i)=0} \frac{c_i}{x - \sigma(\alpha_i)}.
\end{aligned}$$

The claim follows easily after observing that $\mathrm{Gal}(\mathcal{C}_Q/\mathcal{C}_0)$ acts transitively on the roots of Q_j for each j.

We now have

$$f = \sum_j \sum_{i:Q_j(\alpha_i)=0} \frac{n_j}{x-\alpha_i}. \tag{4.21}$$

We also have that

$$\begin{aligned} Q_j &= \prod_{i:Q_j(\alpha_i)=0} (x-\alpha_i) \\ \Rightarrow Q_j'/Q_j &= \sum_{i:Q_j(\alpha_i)=0} \frac{1}{x-\alpha_i} \\ \Rightarrow \sum_j n_j Q_j'/Q_j &= \sum_j \sum_{i:Q_j(\alpha_i)=0} \frac{n_j}{x-\alpha_i} \\ &= f. \end{aligned}$$

Condition 3 now follows from uniqueness of PF decomposition over $\mathcal{C}_0$.

Next we show that Condition 3 implies Condition 4. Assume Condition 3 holds and let $g = \prod_j Q_j^{n_j} \in \mathcal{C}_0(x)$. A straightforward calculation implies that $f = g'/g$, so that Condition 4 holds.

Finally, it is clear that Condition 4 implies Condition 1.

■

The following calculations yield an alternative partial fraction or "APF" decomposition for rational functions defined over $\mathcal{C}_0$. As we shall see, the APF decomposition is more useful than the PF decomposition for deciding whether a $\mathbb{Z}$-linear combination of two rational functions is the logarithmic derivative of another rational function; thus, APF is more useful than PF for making Corollary 4.6.7 effective.

Given $f \in \mathcal{C}_0(x)$ having PF decomposition (4.18) over $\mathcal{C}_0$. For each j, compute $\gamma_j \in \mathcal{C}_0,\ B_j \in \mathcal{C}_0[x]$ such that $A_{j,1} = \gamma_j Q_j' + B_j$ and $\deg B_j < \deg Q_j'$. Then compute a decomposition $\gamma_j = \alpha_j + \beta_j$ having the following properties:

1. $\alpha_j \in \mathbb{Q}$

2. β_j is a $\mathbb{Q}$-linear combination of nontrivial power products of the z_i, where $\mathcal{C}_0 = \mathbb{Q}(z_1, \ldots, z_\lambda)$.

This decomposition is unique for a given γ_j. Applying these computations to (4.18) yields

$$
\begin{aligned}
f &= P + \left(\sum_j \frac{A_{j,1}}{Q_j}\right) + \left(\sum_{j,d:d>1} \frac{A_{j,d}}{Q_j^d}\right) \\
&= P + \left(\sum_j \frac{(\alpha_j + \beta_j)Q_j' + B_j}{Q_j}\right) + \left(\sum_{j,d:d>1} \frac{A_{j,d}}{Q_j^d}\right) \\
&= \left(\sum_j \frac{\alpha_j Q_j'}{Q_j}\right) + \left(P + (\sum_j \frac{\beta_j Q_j' + B_j}{Q_j}) + (\sum_{j,d:d>1} \frac{A_{j,d}}{Q_j^d})\right) \\
&= f_{\text{rat}} + f_{\text{irrat}}. \qquad (4.22)
\end{aligned}
$$

We refer to (4.22) as the APF decomposition of f over $\mathcal{C}_0$. Note that this decomposition is unique for a given $f \in \mathcal{C}_0(x)$.

For the remainder of this section, we assume that $\mathcal{C} = \bar{\mathbb{Q}}$.

Before stating the next lemma, we make a new definition which involves a minor abuse of notation: Given $m_1, m_2 \in \mathbb{Z}, \text{GCD}(m_1, m_2) = 1$, define

$$T_{(m_1,m_2)} = \left\{\text{diag}(t^{m_1}, t^{m_2}, t^{-m_1-m_2}) : t \in \mathcal{C}^*\right\} \simeq \mathcal{C}^*.$$

This definition differs from the definition of $T_{(d_1,d_2)}$ given in Lemma 4.2.2 only in that we place fewer restrictions on the subscripts m_1, m_2.

Lemma 4.6.9 *Given L a third-order operator whose only singularities in the finite plane are apparent singularities, such that G_L is nontrivial and $L = (D + r_1 + r_2 - h'/h) \circ (D - r_2) \circ (D - r_1), r_1, r_2, h \in \bar{\mathbb{Q}}(x)$. Let $\mathcal{C}_0/\mathbb{Q}$ be a finite algebraic extension such that $r_1, r_2, h \in \mathcal{C}_0(x)$. Let $r_i = r_{i_{\text{rat}}} + r_{i_{\text{irrat}}}$ be the APF decomposition of r_i over $\mathcal{C}_0(x)$ for $i = 1, 2$. Let $\mathcal{F}_{(r_1,r_2)}, L_{\text{red}}$ and $T \subseteq \mathsf{GL}$ be as defined in Lemma 4.6.2.*

1. *If $r_{1_{\text{irrat}}}$ and $r_{2_{\text{irrat}}}$ are linearly dependent over $\mathbb{Q}$, then there exist $m_1, m_2 \in \mathbb{Z}$ such that $\text{GCD}(m_1, m_2) = 1$ and $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(m_1,m_2)} \simeq \mathcal{C}^*$. The values of m_1, m_2 can be computed as follows:*

   (a) If $r_{2_{\text{irrat}}} = 0$, then $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(1,0)}$.

   (b) If $r_{1_{\text{irrat}}}/r_{2_{\text{irrat}}} = \mu_1/\mu_2 \in \mathbb{Q}, \mu_1, \mu_2 \in \mathbb{Z}, \text{GCD}(\mu_1, \mu_2) = 1$, then $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(\mu_1,\mu_2)}$.

2. *If $r_{1_{\text{irrat}}}$ and $r_{2_{\text{irrat}}}$ are linearly independent over $\mathbb{Q}$ or, equivalently, if $r_{1_{\text{irrat}}}/r_{2_{\text{irrat}}} \notin \mathbb{Q}$, then $[T]_{\mathcal{F}_{(r_1,r_2)}} = \mathsf{D}_3 \cap \mathsf{SL}_3 \simeq \mathcal{C}^* \times \mathcal{C}^*$.*

Proof. First of all, by Lemma 4.6.2, we have that $T \simeq G_{L_{\text{red}}}$. Moreover, after considering Table 4.1, we see that all nontrivial solvable groups listed in Theorem 4.1.5 have Levi subgroup isomorphic to either $\mathcal{C}^*$ or $\mathcal{C}^* \times \mathcal{C}^*$; it follows that T is isomorphic to one of those groups. Thus, we may apply Corollary 4.6.7 to the problem of computing T in this case.

Suppose $r_{2_{\text{irrat}}} = 0$. This yields

$$r_2 = r_{2_{\text{rat}}} = \sum_j \frac{\alpha_j Q_j'}{Q_j},$$

where $\alpha_j \in \mathbb{Q}$ and $Q_j \in \mathcal{C}_0[x]$ is irreducible for each j. We claim that $\alpha_j \in \mathbb{Z}$ for each j. Indeed, if $\alpha_j \in \mathbb{Q} \setminus \mathbb{Z}$ for some j, then we see that $R_2 \in K_2 \setminus k$ for some finite algebraic extension K_2/k, so that T has a finite quotient; this contradicts the fact that T is isomorphic to either $\mathcal{C}^*$ or $\mathcal{C}^* \times \mathcal{C}^*$. We conclude that $R_2 = \prod_j Q_j^{\alpha_j} \in \mathcal{C}_0(x)$, from which Item 1(a) of the conclusion follows easily.

Next suppose $r_{1_{\text{irrat}}}/r_{2_{\text{irrat}}} = \mu_1/\mu_2 \in \mathbb{Q}, \mu_1, \mu_2 \in \mathbb{Z}, \text{GCD}(\mu_1, \mu_2) = 1$. We compute

$$\begin{aligned}
\mu_2 r_{1_{\text{irrat}}} - \mu_1 r_{2_{\text{irrat}}} &= 0 \\
\Rightarrow \mu_2 r_1 - \mu_1 r_2 &= \mu_2 r_{1_{\text{rat}}} - \mu_1 r_{2_{\text{rat}}} \\
&= \sum_j \frac{\alpha_j Q_j'}{Q_j},
\end{aligned}$$

where $\alpha_j \in \mathbb{Q}$ and $Q_j \in \mathcal{C}_0[x]$ is irreducible for each j. As in the previous case, one checks that $\alpha_j \in \mathbb{Z}$ for each j. It follows that $R_1^{\mu_2} R_2^{-\mu_1} = \prod_j Q_j^{\alpha_j} \in \mathcal{C}_0(x)$. This means that, for $\sigma \in T$ with $[\sigma]_{\mathcal{F}_{(r_1,r_2)}} = \text{diag}(t^{m_1}, t^{m_2}, t^{-m_1-m_2})$, t not a root of unity, we have

$$\begin{aligned}
R_1^{\mu_2} R_2^{-\mu_1} &= \sigma\left(R_1^{\mu_2} R_2^{-\mu_1}\right) \\
&= (t^{m_1} R_1)^{\mu_2} (t^{m_2} R_2)^{-\mu_1} \\
&= t^{m_1\mu_2 - m_2\mu_1} R_1^{\mu_2} R_2^{-\mu_1} \\
\Rightarrow 1 &= t^{m_1\mu_2 - m_2\mu_1} \\
\Rightarrow 0 &= m_1\mu_2 - m_2\mu_1 \\
\Rightarrow m_2\mu_1 &= m_1\mu_2 \\
\Rightarrow \frac{\mu_1}{\mu 2} &= \frac{m_1}{m_2}.
\end{aligned}$$

Item 1(b) of the conclusion now follows easily.

Finally, suppose $r_{1_{\text{irrat}}}/r_{2_{\text{irrat}}} \notin \mathbb{Q}$, i.e., $r_{1_{\text{irrat}}}$ and $r_{2_{\text{irrat}}}$ are linearly independent over $\mathbb{Q}$. Then, for all pairs of integers m_1, m_2 not both zero, we have that the APF decomposition of $r = m_1 r_1 + m_2 r_2$ over $\mathcal{C}_0(x)$ satisfies $r_{\text{irrat}} \neq 0$. On the other hand, let $g \in \mathcal{C}_0(x)$

and write $g = \prod_j Q_j^{n_j}, n_j \in \mathbb{Z}, Q_j \in \mathcal{C}_0[x]$ irreducible; then the APF decomposition of $g'/g = \sum_j n_j Q'_j/Q_j$ over $\mathcal{C}_0(x)$ satisfies $(g'/g)_{\text{irrat}} = 0$. It follows that there do *not* exist $(m_1, m_2) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ and $g \in \mathcal{C}(x)$ such that $m_1 r_1 + m_2 r_2 = g'/g$. Corollary 4.6.7 now implies $T \simeq \mathcal{C}^* \times \mathcal{C}^*$. Since T is an algebraic subgroup of $\mathsf{D}_3 \cap \mathsf{SL}_3$, we conclude that $T = \mathsf{D}_3 \cap \mathsf{SL}_3$, and Item 2 of the conclusion is proved.

■

We are now ready to present our algorithm and prove its correctness.

Algorithm IV

Input: Two polynomials $a, b \in \bar{\mathbb{Q}}[x]$, representing the operator $L = D^3 + aD + b \in \bar{\mathbb{Q}}(x)[D]$.

Output: An explicit description of G_L, the group of $L(y) = 0$.

Steps: First compute n_1 and n_2, where n_i is the number of monic ith order right factors of L in $\mathcal{D}$. This step can be carried out by computing rational solutions of $\operatorname{Ricc} L$ and $\operatorname{Ricc}(\operatorname{adj} L)$. Next, if $(n_1, n_2) = \dots$

- $(0,0)$: Compute $L^{\circledS 2}$. If $\operatorname{ord}(L^{\circledS 2}) = 5$, then return $G_L \simeq \mathsf{PSL}_2$. Otherwise, test whether $L^{\circledS 2}$ is reducible. If so, then return $G_L \simeq \mathsf{PSL}_2$; otherwise, return $G_L \simeq \mathsf{SL}_3$.

- $(0,1)$ (resp., $(1,0)$): Here, L has an irreducible (left or right) factor of the form

$$L_2 = D^2 + b_1 D + b_0, \;\; b_0, b_1 \in \bar{\mathbb{Q}}(x). \tag{4.23}$$

  Compute b_1. Test whether $b_1 = \frac{f'}{f}$ for some $f \in \bar{\mathbb{Q}}(x)$. If so, then return $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \mathsf{SL}_2$ with the unique conjugation action; otherwise, return $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \mathsf{GL}_2$ with conjugation as described in Item 2(a) (resp., Item 2(b)) of Lemma 4.5.8.

- $(1,2)$ (resp., $(2,1)$): Compute $r_1, r_2 \in \bar{\mathbb{Q}}(x)$ such that

$$L = (D + r_1 + r_2) \circ (D - r_2) \circ (D - r_1). \tag{4.24}$$

  Apply Lemma 4.6.9 to compute the maximal torus T of G_L. If $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, then return $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes (\bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*)$ with conjugation as described in Item 2 (resp., Item 3) of Lemma 4.5.4. Otherwise, apply Lemma 4.6.9 to compute m_1, m_2 such that $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(m_1,m_2)} \subseteq \mathsf{D}_3 \cap \mathsf{SL}_3$. Return $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$, with:

  1. $(\operatorname{Int} t)(u,v) = (t^{m_1 - m_2} u, t^{2m_1 + m_2} v)$ for $t \in \bar{\mathbb{Q}}^*, u, v \in \bar{\mathbb{Q}}$, in case $(n_1, n_2) = (1,2)$
  2. $(\operatorname{Int} t)(u,v) = (t^{2m_1 + m_2} u, t^{m_1 + 2m_2} v)$ for $t \in \bar{\mathbb{Q}}^*, u, v \in \bar{\mathbb{Q}}$, in case $(n_1, n_2) = (2,1)$.

- $(1, \infty)$ (resp., $(\infty, 1)$): Return $\bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$ with conjugation as described in Item 8 (resp., Item 9) of Lemma 4.5.2.

- $(2, \infty)$ (resp., $(\infty, 2)$): Return $\bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with conjugation as described in Item 4 (resp., Item 3) of Lemma 4.5.2.

- $(2, 2)$: Compute $r_1, r_2 \in \bar{\mathbb{Q}}(x)$ such that (4.24) holds. Apply Lemma 4.6.9 to compute the maximal torus T of G_L. If $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, then return $G_L \simeq \bar{\mathbb{Q}} \rtimes (\bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*)$ with conjugation as described in Item 1 of Lemma 4.5.4. Otherwise, apply Lemma 4.6.9 to compute m_1, m_2 such that $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(m_1,m_2)} \subseteq \mathsf{D}_3 \cap \mathsf{SL}_3$. Compute $n_1^\flat$ (resp., $n_2^\flat$), the number of first-order right factors of $(D - r_2) \circ (D - r_1)$ (resp., of $(D + r_1 + r_2) \circ (D - r_2)$).

  - If $n_1^\flat = 1, n_2^\flat = 2$: Return $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with $(\operatorname{Int} t)(u) = t^{m_1 - m_2} u$.
  - If $n_1^\flat = 2, n_2^\flat = 1$: Return $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with $(\operatorname{Int} t)(u) = t^{m_1 + 2m_2} u$.
  - If $n_1^\flat = 2, n_2^\flat = 2$: Return $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with $(\operatorname{Int} t)(u) = t^{2m_1 + m_2} u$.

- $(3, 3)$: Apply Lemma 4.6.9 to compute the maximal torus T; return $G_L = T$.

- (∞, ∞) : Find the dimension of the $\bar{\mathbb{Q}}$-vector space of $\bar{\mathbb{Q}}(x)$-rational solutions of $L(y) = 0$. If this dimension is 3, then return $G_L \simeq \{1\}$; otherwise, return $G_L \simeq \bar{\mathbb{Q}}^*$.

- $(1, 1)$: Let L_d be the unique monic dth-order right factor of L for $d = 1, 2$.

  1. *If L_1 fails to right-divide L_2* : Then $G_L = G_{L_2}$ is isomorphic to either SL_2 or GL_2. Decide using method given in "(0, 1) or (1, 0)" case.
  2. *If L_1 right-divides L_2* : Compute $r_1, r_2 \in \bar{\mathbb{Q}}(x)$ such that (4.24) holds. Apply Lemma 4.6.9 to compute the maximal torus T of G_L.
     (a) If $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$: Return $G_L \simeq \mathsf{T}_3 \cap \mathsf{SL}_3$.
     (b) If $T \simeq \bar{\mathbb{Q}}^*$: Apply Lemma 4.6.9 to compute the appropriate subgroup $T_{(m_1,m_2)} \subseteq \mathsf{D}_3 \cap \mathsf{SL}_3$. If $T_{(m_1,m_2)} \neq T_{(1,0)}$, then return $G_L \simeq \mathsf{U}_3 \rtimes \bar{\mathbb{Q}}^*$, with conjugation as described in Item 1 or 2 of Lemma 4.5.6. In case $T_{(m_1,m_2)} = T_{(1,0)}$, compute $g \in \bar{\mathbb{Q}}(x)$ such that $g'/g = r_2$. Test whether the equation

$$(D \circ (D - r_1 - 2r_2))(y) = r_2 g^3$$

admits a $\bar{\mathbb{Q}}(x)$-rational solution. If no such solution exists, then return $G_L \simeq \mathsf{U}_3 T_{(1,0)}$. Otherwise, test whether the equation

$$(D \circ (D - r_1 - 2r_2) \circ (D - 2r_1 - r_2))(y) = r_2 g^3$$

admits a $\bar{\mathbb{Q}}(x)$-rational solution. If no such solution exists, then return $G_L \simeq U^2_{(1,1)} T_{(1,0)}$. Otherwise, return $G_L \simeq U^1_{(1,1)} T_{(1,0)}$.

Proof of correctness of algorithm: Corollary 4.1.3 implies that we may apply Theorem 4.1.5. Proposition 3.1.3 and its proof provide a correspondence between right factors of L and G_L-invariant subspaces of V_L. Let $R_1, R_2, y_2, \xi, y_3, T, L_{\text{red}}$ and $\mathcal{F}_{(r_1,r_2)}$ be as defined in Lemma 4.6.2 and let R_u be the unipotent radical of G_L. We consider the various cases according to Table 4.1 as follows.

- $(0,0)$: Correctness in this case follows from Lemma 4.6.1.
- $(0,1)$ or $(1,0)$: Correctness follows from Lemma 4.1.2.
- $(1,2)$: In case $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, correctness follows from the fact that there is only one subgroup listed in Theorem 4.1.5 for which $n_1 = 1, n_2 = 2$ and $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. Suppose now that $T \simeq \bar{\mathbb{Q}}^*$. Note that V_{D-r_1} is the unique 1-dimensional G_L-invariant subspace of V_L. Furthermore, by Theorem 4.1.5, we have that $[G_L]_{\mathcal{F}_{(r_1,r_2)}}$ is conjugate to $U^2_{(1,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$ for some d_1, d_2, σ. From this fact, we see that R_u is two-dimensional and acts trivially on V_L/V_{D-r_1}; we conclude that $[R_u]_{\mathcal{F}_{(r_1,r_2)}} = U^2_{(1,0)}$. Thus, we have $[G_L]_{\mathcal{F}_{(r_1,r_2)}} = U^2_{(1,0)} \cdot T_{(m_1,m_2)}$; correctness now follows after a straightforward calculation.
- $(2,1)$: In case $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, correctness follows from the fact that there is only one subgroup listed in Theorem 4.1.5 for which $n_1 = 2, n_2 = 1$ and $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. Suppose now that $T \simeq \bar{\mathbb{Q}}^*$. Note that $V_{(D-r_2)\circ(D-r_1)}$ is the unique 2-dimensional G_L-invariant subspace of V_L. Furthermore, by Theorem 4.1.5, we have that $[G_L]_{\mathcal{F}_{(r_1,r_2)}}$ is conjugate to $U^2_{(0,1)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$ for some d_1, d_2, σ. From this fact, we see that R_u is two-dimensional and acts trivially on $V_{(D-r_2)\circ(D-r_1)}$; we conclude that $[R_u]_{\mathcal{F}_{(r_1,r_2)}} = U^2_{(0,1)}$. Thus, we have $[G_L]_{\mathcal{F}_{(r_1,r_2)}} = U^2_{(0,1)} \cdot T_{(m_1,m_2)}$; correctness now follows after a straightforward calculation.
- $(2,2)$: In case $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, correctness follows from the fact that there is only one subgroup listed in Theorem 4.1.5 for which $n_1 = n_2 = 2$ and $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. Suppose now

that $T \simeq \bar{\mathbb{Q}}^*$. Then, after considering the relevant subgroups listed in Theorem 4.1.5, we see that $[G_L]_{\mathcal{F}_{(r_1,r_2)}}$ is conjugate to $U^1_{(0,0)} \cdot P_\sigma T_{(d_1,d_2)} P_\sigma^{-1}$ for some d_1, d_2, σ with $d_1 > d_2$. This implies that $[R_u]_{\mathcal{F}_{(r_1,r_2)}} = \text{clos}(M)$ for some $M = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3$ with M conjugate to $M_0 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. We claim that either $a = 0$ or $c = 0$: Indeed, this claim follows easily from Lemma 4.3.4. Applying Item 1 of Lemma 4.5.1 with

$$Q = \text{diag}(t^{m_1}, t^{m_2}, t^{-m_1-m_2}),$$

t some nonroot of unity, we now see that two of a, b, c are zero. It follows that $[R_u]_{\mathcal{F}_{(r_1,r_2)}}$ is one of the following subgroups:

$$U^1_{(1,0)} = \left\{ \begin{bmatrix} 1 & u & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}, U^1_{(0,0)} = \left\{ \begin{bmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}, U^1_{(0,1)} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & u \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$

One checks that the following are equivalent:

1. $[R_u]_{\mathcal{F}_{(r_1,r_2)}} = U^1_{(1,0)}$
2. $y_2 \notin K_{L_{\text{red}}}, \xi \in K_{L_{\text{red}}}$
3. $D - r_1$ is the unique right factor of $(D - r_2) \circ (D - r_1)$, and $(D + r_1 + r_2) \circ (D - r_2)$ is completely reducible
4. $n_1^\flat = 1, n_2^\flat = 2$

In case any of the above equivalent conditions holds, we see that $[G_L]_{\mathcal{F}_{(r_1,r_2)}} = U^1_{(1,0)} \cdot T_{(m_1,m_2)} \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$, and a calculation shows that the conjugation action is as described in the algorithm; thus, the algorithm is correct in this case. Correctness in case $[R_u]_{\mathcal{F}_{(r_1,r_2)}}$ is equal to $U^1_{(0,0)}$ or $U^1_{(0,1)}$ is proved by similar means.

- $(3, 3)$: Correctness is clear in this case.
- (∞, ∞) : Correctness is clear in this case.
- $(1, 1)$: Suppose G_L is isomorphic to either SL_2 or GL_2. Then L_1 fails to right-divide L_2. Correctness then follows from Lemma 4.1.2.

Suppose that G_L is solvable, i.e., L_1 right-divides L_2. In case $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$, correctness follows from the fact that there is only one subgroup listed in Theorem 4.1.5 for which $n_1 = n_2 = 1$ and $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$.

Suppose now that $T \simeq \bar{\mathbb{Q}}^*$. Let $\mathcal{A}$ be a basis of V_L such that $[G_L]_{\mathcal{A}} \subseteq \mathsf{SL}_3$ is one of the relevant subgroups listed in Theorem 4.1.5. Note that each of the solvable subgroups listed in Theorem 4.1.5 satisfying $n_1 = n_2 = 1$ has unipotent radical either $U^1_{(1,1)}, U^2_{(1,1)}$ or U_3. In particular, $[R_u]_{\mathcal{A}}$ includes $U^1_{(1,1)}$; thus, there exists $\tau \in R_u$ such that

$$[\tau]_{\mathcal{A}} = \begin{bmatrix} 1 & 1 & \frac{1}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3.$$

Let $M_0 = [\tau]_{\mathcal{A}}$, and let

$$M = [\tau]_{\mathcal{F}_{(r_1,r_2)}} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in \mathsf{U}_3,\ a, b, c \in \bar{\mathbb{Q}}.$$

We claim that $a \neq 0$ and $c \neq 0$: Indeed, this claim follows easily from Lemma 4.3.4 and the fact that $\mathrm{clos}(M_0) = U^1_{(1,1)}$.

Suppose $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(m_1,m_2)}$ is such that $T_{(m_1,m_2)} \neq T_{(1,0)}$. Then we claim that $[R_u]_{\mathcal{F}_{(r_1,r_2)}} = \mathsf{U}_3$, so that the algorithm is correct in this case. Indeed, if $[R_u]_{\mathcal{F}_{(r_1,r_2)}} \subsetneq \mathsf{U}_3$, then $R_u \simeq \bar{\mathbb{Q}}^d$ for $d = 1$ or 2, and we see by Item 5 of Lemma 4.3.3 that $[R_u]_{\mathcal{F}_{(r_1,r_2)}} \subseteq \mathrm{clos}(M) \cdot U^1_{(0,0)}$. Applying Item 2 of Lemma 4.5.1 with

$$Q = \mathrm{diag}(t^{m_1}, t^{m_2}, t^{-m_1-m_2}),$$

t some nonroot of unity, we obtain $T_{(m_1,m_2)} = T_{(1,0)}$ (note that $T_{(-1,0)} = T_{(1,0)}$), contradicting hypothesis. This proves the claim.

Finally, suppose $T_{(m_1,m_2)} = T_{(1,0)}$. Then one checks that $r_2 = g'/g$ for some $g \in \bar{\mathbb{Q}}(x)$. Correctness now follows from Lemma 4.6.5.

This exhausts the list of subgroups listed in Theorem 4.1.5 satisfying $n_1 = n_2 = 1$.

- $(1, \infty)$ (resp., $(\infty, 1); (2, \infty); (\infty, 2)$): Correctness follows from the fact that there is exactly one subgroup listed in Theorem 4.1.5 having these values for n_1 and n_2.

■

4.7 Examples

Before presenting examples related to this algorithm, we state the following result:

Theorem 4.7.1 *Let G be a connected linear algebraic group defined over an algebraically closed field $\mathcal{C}$ of characteristic zero. Let $d(G)$ (resp., $e(G)$) be the defect (resp., the* excess *— cf. [MS96]) of G. Then G is the Galois group of a Picard-Vessiot extension of $\mathcal{C}(x)$ corresponding to a system of the form*

$$Y' = \left(\frac{A_1}{x - \alpha_1} + \cdots + \frac{A_{d(G)}}{x - \alpha_{d(G)}} + A_\infty \right) Y,$$

where A_i is a constant matrix for $i = 1, \ldots, d(G)$, and A_∞ is a matrix with polynomial entries of degree at most $e(G)$. In particular, the only possible singularities of this system are $d(G)$ regular singular points in the finite plane and a (possibly irregular) singular point at infinity.

Proof. This is Theorem 1.2 in [MS96].

∎

This theorem, suitably rewritten in terms of operators, implies that each algebraic group named in Theorem 4.1.5 arises as the Galois group of a third order operator whose only singularities in the finite plane are apparent singularities.

For each group $G \subseteq \mathsf{SL}_3$ named in Theorem 4.1.5, we would like to find an operator of the form $L = D^3 + aD + b, a, b \in \bar{\mathbb{Q}}[x]$, such that $G_L \simeq G$. Unfortunately, it is not known whether such an operator exists in each case. Below, for each such subgroup $G \subseteq \mathsf{SL}_3$, we name a third-order operator L such that $G_L \simeq G$; L has nonzero D^2 term and one or more apparent singularities in the finite plane in general. In each case, we apply either Algorithm IV or a modified version of Algorithm IV. For each example, n_i denotes the number of ith-order right factors of L for $i = 1, 2$.

1. Examples satisfying $H \simeq 1$.

   (a) Examples satisfying $T \simeq 1$. Let $L = D^3$. Applying Algorithm IV, we compute $n_1 = n_2 = \infty$, and $\left\{1, x, x^2\right\}$ is a basis of $\bar{\mathbb{Q}}(x)$-rational solutions. Algorithm IV then returns the trivial group.

   (b) Examples satisfying $T \simeq \bar{\mathbb{Q}}^*$.

i. Examples satisfying $R_u \simeq 0$. Let

$$\begin{aligned} L &= D^3 + (-a_1^2 - a_1a_2 - a_2^2)D + (a_1^2a_2 + a_1a_2^2) \\ &= (D + a_1 + a_2) \circ (D - a_2) \circ (D - a_1), \\ &\quad a_1, a_2 \in \mathbb{Z} \setminus \{0\}\,,\ \mathrm{GCD}(a_1, a_2) = 1,\ a_1 + a_2 \neq 0, \\ &\quad a_1 \neq -a_1 - a_2,\ a_2 \neq -a_1 - a_2. \end{aligned}$$

One checks that $n_1 = n_2 = 3$. Moreover, we easily see that $G_L \simeq \bar{\mathbb{Q}}^*$. Varying a_1 and a_2 yields the different representations of $\bar{\mathbb{Q}}^*$ described in Lemma 4.2.3.

ii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}$. Here, we seek examples in which $G \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$, as in Items 1-4 of Lemma 4.5.2 and Item 1 of Lemma 4.5.3.

   A. Let

$$\begin{aligned} L &= \mathrm{LCLM}\big((D - a_2x) \circ (D - a_1x), D + (a_1 + a_2)x\big), \\ &\quad a_1, a_2 \in \mathbb{Z} \setminus \{0\}\,,\ \mathrm{GCD}(a_1, a_2) = 1,\ a_1 + a_2 \neq 0, \\ &\quad a_1 \neq -a_1 - a_2,\ a_2 \neq -a_1 - a_2. \end{aligned}$$

   It can be shown that $n_1 = n_2 = 2$, that applying Lemma 4.6.9 yields $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(a_1,a_2)}$, and that $n_1^\flat = 1, n_2^\flat = 2$; we conclude that Return $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with $(\mathrm{Int}\, t)(u) = t^{a_1 - a_2}u$.
   Alternatively, let $R_i \in K_L$ be such that $R_i'/R_i = a_ix$ for $i = 1, 2$. Let $y_2 \in K_L$ be such that $y_2' - a_1xy_2 = R_2$. Then one checks that $\mathcal{F} = \big\{R_1, y_2, R_1^{-1}R_2^{-1}\big\}$ is an ordered basis of V_L. One further checks that $[G_L]_{\mathcal{F}}$ has unipotent radical $U^1_{(1,0)}$ and maximal torus $T_{(a_1,a_2)}$. A computation then shows that $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$, with $(\mathrm{Int}\, t)(u) = t^{a_1 - a_2}u$.
   Note that by varying a_1 and a_2, one can obtain any of the semidirect product structures described in Item 1 of Lemma 4.5.2.

   B. Let $L = D^3 + (-x^2 - 2)D - x = (D + x) \circ D \circ (D - x)$. Maple computations show that $n_1 = n_2 = 1$, that $r_2 = g'/g$ for $g = 1$ and that the equations given in Item 3(d) and 4(d) of Lemma 4.6.5 admit $\bar{\mathbb{Q}}(x)$-rational solutions. We conclude that $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$ with $(\mathrm{Int}\, t)(u) = tu$ as in Item 2 of Lemma 4.5.2.

   C. Let $L = D^3 + (-3x^2 + 3)D + (2x^3 - 6x) = (D - x) \circ (D - x) \circ (D + 2x)$. Maple computations yield $n_1 = 2, n_2 = \infty$, and we conclude that $G_L \simeq \bar{\mathbb{Q}} \rtimes \bar{\mathbb{Q}}^*$, with $(\mathrm{Int}\, t)(u) = t^{-3}u$ as in Item 4 of Lemma 4.5.2. Taking adj L yields the subgroup given in Item 3 of Lemma 4.5.2.

iii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}^2$.

A. Let

$$\begin{aligned} L &= \big(\mathrm{LCLM}(D - a_1 x, D - a_2 x)\big) \circ (D + (a_1 + a_2)x), \quad (4.25) \\ & \quad a_1, a_2 \in \mathbb{Z} \setminus \{0\},\ \mathrm{GCD}(a_1, a_2) = 1,\ a_1 + a_2 \neq 0, \\ & \quad a_1 \neq -a_1 - a_2,\ a_2 \neq -a_1 - a_2. \end{aligned}$$

Here, it can be shown that $n_1 = 1$ and $n_2 = 2$ and that applying Lemma 4.6.9 yields $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(-a_1-a_2,a_1)}$. We conclude that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$ with $(\mathrm{Int}\, t)(u, v) = (t^{a_1-a_2}u, t^{2a_1+a_2}v)$.

Alternatively, let $R_i \in K_L$ be such that $R_i'/R_i = a_i x$ for $i = 1, 2$. Let $y_j \in K_L$ be such that $y_j' + (a_1 + a_2)xy_j = R_{j-1}$ for $j = 2, 3$. Then one checks that $\mathcal{F} = \{R_1^{-1}R_2^{-1}, y_2, y_3\}$ is an ordered basis of V_L. One further checks that $[G_L]_{\mathcal{F}}$ has unipotent radical $U^2_{(1,0)}$ and maximal torus $T_{(-a_1-a_2,a_1)}$. A computation then shows that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$, with

$$(\mathrm{Int}\, t)(u, v) = (t^{-2a_1-a_2}u, t^{-a_1-2a_2}v)$$

for $t \in \bar{\mathbb{Q}}^*, u, v \in \bar{\mathbb{Q}}$.

By varying a_1 and a_2, one can obtain any of the semidirect product structures described in Item 5 of Lemma 4.5.2.

B. Let $\bar{L} = \mathrm{adj}\, L$, where L is as defined in (4.25). Arguments similar to those used in computing G_L show that $G_{\bar{L}} \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$ is as described in Item 6 of Lemma 4.5.2.

C. Let $L = D^3 + (-x^4 - 5x)D + (-3x^3 - 3) = (D + x^2) \circ (D + 1/x) \circ (D - x^2 - 1/x)$. Maple computations show that $n_1 = n_2 = 1$, that $r_2 = g'/g$ for $g = 1/x$, that the equation given in Item 3(d) of Lemma 4.6.5 admits a $\bar{\mathbb{Q}}(x)$-rational solution but the equation given in Item 4(d) of that lemma does not. We conclude that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$, with $(\mathrm{Int}\, t)(u, v) = (tu, t^2 v)$ as in Item 7 of Lemma 4.5.2.

D. Let

$$\begin{aligned} L &= D^3 + (-3x^4 + 6x)D + (2x^6 - 12x^3 + 4) \\ &= (D - x^2) \circ (D - x^2) \circ (D + 2x^2). \quad (4.26) \end{aligned}$$

Maple computations show that $n_1 = 1, n_2 = \infty$, and we conclude that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$, with $(\operatorname{Int} t)(u, v) = (t^{-3}u, t^{-3}v)$ as described in Item 8 of Lemma 4.5.2.

E. Let $\bar{L} = \operatorname{adj} L$, where L is as defined in (4.26). Arguments similar to those used in computing G_L show that $G_{\bar{L}} \simeq \bar{\mathbb{Q}}^2 \rtimes \bar{\mathbb{Q}}^*$ is as described in Item 9 of Lemma 4.5.2.

iv. Examples satisfying $R_u \simeq \mathsf{U}_3$.

A. Let

$$\begin{aligned} L &= (D + (a_1 + a_2)x) \circ (D - a_2 x) \circ (D - a_1 x), \\ & \quad a_1, a_2 \in \mathbb{Z} \setminus \{0\}\,,\ \operatorname{GCD}(a_1, a_2) = 1,\ a_2 \neq 0. \end{aligned}$$

It can be shown that $n_1 = n_2 = 1$ and that applying Lemma 4.6.9 yields $[T]_{\mathcal{F}_{(r_1,r_2)}} = T_{(a_1,a_2)}$. We conclude that $G_L \simeq \mathsf{U}_3 \cdot T_{(a_1,a_2)}$.
Alternatively, it can be shown that K_L/k is generated by elements R_1, R_2, y_2, ξ, $y_3 \in K_L$ satisfying $R_i'/R_i = a_i x$ for $i = 1, 2$, $y_2' - a_1 x y_2 = R_2$, $\xi' - a_2 x \xi = R_1^{-1} R_2^{-1}$ and $y_3' - a_1 x y_3 = \xi$. It can moreover be shown that V_L has ordered basis $\mathcal{B} = \{R_1, y_2, y_3\}$; that $[G_L]_{\mathcal{B}}$ has maximal torus $T_{(a_1,a_2)}$ and unipotent radical U_3. These facts yield $G_L \simeq \mathsf{U}_3 \cdot T_{(a_1,a_2)}$.
Varying a_1 and a_2 yields the different conjugation actions described in Item 1 of Lemma 4.5.6.

B. Let

$$\begin{aligned} L &= D^3 + (-x^4 - 2x^3 - x^2 - 5x - 3)D + (-3x^3 - 5x^2 - 2x - 3) \\ &= (D + x^2 + x) \circ (D + 1/x) \circ (D - x^2 - x - 1/x). \end{aligned}$$

Maple computations show that $n_1 = n_2 = 1$, that $r_2 = g'/g$ for $g = 1/x$, and that the equation given in Item 3(d) of Lemma 4.6.5 fails to admit a $\bar{\mathbb{Q}}(x)$-rational solution. We conclude that $G_L \simeq \mathsf{U}_3 \rtimes \bar{\mathbb{Q}}^*$, with

$$(\operatorname{Int} t)\left(\begin{bmatrix} 1 & b & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & tb & t^2 c \\ 0 & 1 & td \\ 0 & 0 & 1 \end{bmatrix}$$

as in Lemma 4.5.6 with $\sigma = \operatorname{id}, T_{(d_1,d_2)} = T_{(1,0)}$.

(c) Examples satisfying $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$.

i. Examples satisfying $R_u \simeq 0$. Let $L = \mathrm{LCLM}(D-x, D-1, D+x+1)$. Here, it is easy to see that $G_L \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$.

ii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}$. Let $L = \mathrm{LCLM}((D-x)\circ(D-1), D+x+1)$. A Maple computation shows that $n_1 = n_2 = 1$. It is easy to see that $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. We conclude from Theorem 4.1.5 that $G_L \simeq \bar{\mathbb{Q}} \rtimes (\bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*)$, with $(\mathrm{Int}(t_1,t_2))(u) = t_1^2 t_2 u$ as in Item 1 of Lemma 4.5.4.

iii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}^2$. Let $L = (\mathrm{LCLM}(Dx-x, Dx-1))\circ(D+x+1)$. A Maple computation shows that $n_1 = 1, n_2 = 2$. It is easy to see that $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. We conclude from Theorem 4.1.5 that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes (\bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*)$, with $(\mathrm{Int}(t_1,t_2))(u,v) = (t_1 t_2^{-1} u, t_1^2 t_2 v)$ as in Item 2 of Lemma 4.5.4. Similar computations show that the group of $\mathrm{adj}\, L$ is as described in Item 3 of Lemma 4.5.4.

iv. Examples satisfying $R_u \simeq \mathsf{U}_3$. Let $L = D^3 + (-x^2-x-2)D + (x^2+x+1) = (D+x+1)\circ(D-x)\circ(D-1)$. Maple computations show that $n_1 = n_2 = 1$ and that $T \simeq \bar{\mathbb{Q}}^* \times \bar{\mathbb{Q}}^*$. We conclude that $G_L \simeq \mathsf{T}_3 \cap \mathsf{SL}_3$.

2. Examples satisfying $H \simeq \mathsf{SL}_2$.

(a) Examples satisfying $T \simeq 1$.

i. Examples satisfying $R_u \simeq 0$. Let $L = \mathrm{LCLM}(D^2 - x, D)$. A Maple computation shows that $n_1 = n_2 = 1$; we see that G_L is nonsolvable and that $G_{D^2-x} \simeq \mathsf{SL}_2$. From Theorem 4.1.5 we conclude that $G_L \simeq \mathsf{SL}_2$.

ii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}^2$. Let $L = D^3 - xD - 1 = D\circ(D^2 - x)$. Maple computations show that $n_1 = 1, n_2 = 0$, and $G_{D^2-x} \simeq \mathsf{SL}_2$; we conclude that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \mathsf{SL}_2$, with the unique conjugation action. Similar computations show that $\mathrm{adj}\, L$ satisfies $n_1 = 0, n_2 = 1$ and also has group $\bar{\mathbb{Q}}^2 \rtimes \mathsf{SL}_2$ with the unique conjugation action. See Lemma 4.5.8.

(b) Examples satisfying $T \simeq \bar{\mathbb{Q}}^*$, so that $P \simeq \mathsf{GL}_2$.

i. Examples satisfying $R_u \simeq 0$. Let $L = D^3 + (-3x^2+1)D + (2x^3 - 4x) = \mathrm{LCLM}(D^2 + xD - 2x^2, D - x)$. Maple computations show that $n_1 = n_2 = 1$, that G_L is nonsolvable and that $G_{D^2+xD-2x^2} \simeq \mathsf{GL}_2$. We conclude that $G_L \simeq \mathsf{GL}_2$.

ii. Examples satisfying $R_u \simeq \bar{\mathbb{Q}}^2$. Let $L = D^3 + (-x^4 + 2x + 1)D - x^2 = (D - x^2)\circ(D^2 + x^2 D + 1)$. Maple computations show that $n_1 = 1, n_2 = 0$.

It is easy to see that $G_L \simeq \bar{\mathbb{Q}}^2 \rtimes \mathsf{GL}_2$ with $M.v = (\det M)^{-1}(M^{-1})^T v$ as in Item 2(b) of Lemma 4.5.8. Similar computations show that the group of $\operatorname{adj} L$ is as described in Lemma 4.5.8.

3. Examples satisfying $H \simeq \mathsf{PSL}_2$. Let $L = D^3 - 4xD - 2 = (D^2 - x)^{\circledS 2}$. A Maple computation shows that $L^{\circledS 2}$ has order 5. We conclude that $G_L \simeq \mathsf{PSL}_2$.

4. Examples satisfying $H \simeq \mathsf{SL}_3$. Let $L = D^3 - x$. A Maple computation shows that $L^{\circledS 2}$ is irreducible of order 6. We conclude that $G_L \simeq \mathsf{SL}_3$.

Chapter 5

Bibliography

Bibliography

[Ber90] Daniel Bertrand. Extensions de d-modules et groupes de Galois différentiels. In F.B. et al., editor, *P-adic analysis (Trento, 1989)*, volume 1454 of *Lecture Notes in Mathematics*, pages 125–141, Berlin, 1990. Springer.

[Ber92] Daniel Bertrand. Un analogue différentiel de la théorie de kummer. In P. Philippon, editor, *Approximations Diophantiennes et Nombres Transcendents, Luminy 1990*, pages 39–49, Berlin, 1992. Walter de Gruyter.

[Bro96] Manuel Bronstein. *Symbolic Integration I: Transcendental Functions.* Algorithms and Computation in Mathematics. Springer, Berlin, 1996.

[BS99] Peter Berman and Michael Singer. Calculating the Galois group of $L_1(L_2(y)) = 0$, L_1, L_2 completely reducible operators. *Journal of Pure and Applied Algebra*, 139:3–23, 1999.

[CS99] Elie Compoint and Michael Singer. Calculating Galois groups of completely reducible linear operators. *Journal of Symbolic Computation*, 28(4-5):473–494, 1999.

[FH91] W. Fulton and J. Harris. *Representation Theory: A First Course.* Readings in Mathematics. Springer, New York, 1991.

[Gri90] D. Y. Grigoriev. Complexity of factoring and calculating the gcd of linear ordinary differential operators. *Journal of Symbolic Computation*, 10(1):7–38, 1990.

[Hae87] A. Haefliger. Local theory of meromorphic connections in dimension one (Fuchs theory). In Borel et al., editor, *Algebraic D-Modules*, pages 129–149. Academic Press, 1987.

[HK71] K. Hoffman and R. Kunze. *Linear Algebra.* Prentice Hall, Englewood Cliffs, New Jersey, second edition, 1971.

[Hum81] James Humphreys. *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer, New York, 1981.

[Kap76] I. Kaplansky. *An Introduction To Differential Algebra, 2nd ed.* Hermann, Paris, 1976.

[Kat87] Nicholas Katz. A simple algorithm for cyclic vectors. *Amer. J. Math*, 109:65–70, 1987.

[Kol68] E. Kolchin. Algebraic groups and algebraic dependence. *Amer. J. Math*, 90:1151–1164, 1968.

[Lan84] S. Lang. *Algebra.* Addison-Wesley, Menlo Park, California, second edition, 1984.

[Mag94] Andy R. Magid. *Lectures on Differential Galois Theory*, volume 7 of *University Lecture Series.* American Mathematical Society, Providence, Rhode Island, 1994.

[Mos56] G. D. Mostow. Fully reducible subgroups of algebraic groups. *Amer. J. Math*, 78:211–264, 1956.

[MS96] C. Mitschi and M. Singer. Connected linear groups as differential Galois groups. *Jour. Alg.*, 184:333–361, 1996.

[dP98a] M. van der Put. Recent work in differential Galois theory. In *Séminaire Bourbaki: volume 1997/1998*, Astérisque. Société Mathématique de France, Paris, 1998.

[dP98b] M. van der Put. Symbolic analysis of differential equations. In Cohen et. al., editor, *Some Tapas of Computer Algebra.* Springer, 1998.

[dPS] M. van der Put and M.F. Singer. Differential Galois Theory. Manuscript, 2001.

[Sin96] Michael Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Appl. Algebra Eng. Commun. Comput.*, 7:77–104, 1996.

[Sin99] Michael Singer. Direct and inverse problems in differential Galois theory. In Cassidy Bass, Buium, editor, *Selected Works of Ellis Kolchin with Commentary*, pages 527–554. American Mathematical Society, 1999.

[SU93] Michael Singer and Felix Ulmer. Galois groups of second and third order linear differential equations. *Journal of Symbolic Computation*, 16:9–36, 1993.

[Tsa96] S. P. Tsarev. An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator. In L.Y.N., editor, *Proc. 1996 Internat. Symp. on Symbolic and Algebraic Computation*, pages 226–231, New York, 1996.

[dW53] B. L. van der Waerden. *Modern Algebra.* Frederick Ungar Publishing Co., New York, second edition, 1953.

Appendix

Appendix A

Maple code, documentation

A.1 README file

```
File o3np.README: information about o3np.mpl, by Peter Berman.
Version 1.0. July 23, 2001. Compatible with Maple 6.


EXAMPLES:

> read("o3np.mpl");
Warning, the protected names norm and trace have been redefined and
unprotected
Warning, the name adjoint has been redefined

> dom := [Dx,x];
                                dom := [Dx, x]

> L := mult(Dx^2 - 2*x, Dx, dom);
                                       3
                               L := Dx  - 2 x Dx

> order_3_no_pole(-2*x,0,x);
The group of Dx^3-2*x*Dx is a semidirect product of C^2 by SL2.
    The conjugation action of SL2 on C^2 is given as follows:
    M.v = multiply( transpose(v), inverse(M) )
       for M in SL2, v in C^2.
       (multiplication of vector transpose by matrix inverse).

> # Note: The third argument, x, is the independent variable
> o3np(-2*x,0,x);
                  [C^2, SL2, vector_transpose_matrix_inverse]
```

```
> order_3_no_pole(2*x,1,x);
The group of Dx^3+2*x*Dx+1 is PSL2.

> o3np(2*x,1,x);
                                [0, PSL2, 0]
```

```
To use o3np.mpl, make sure that your copy of that file is
in a directory that's accessible to MAPLE, then type

    > read("o3np.mpl");

from the MAPLE command line.  The file contains code for
initialization and function defitions.


The remainder of this README file contains the declarations
and comment lines for the two main functions defined in the
o3np file.
```

```
order_3_no_pole := proc( f, g, x )
  #
  # This procedure takes as input the polynomials f and g in x,
  # and returns as output a paragraph describing the Galois group
  # of the operator D^3 + fD + g over C(x), where C is the
  # field of algebraic numbers.
  #
  # It is a wrapper function for o3np, providing a text description
  # for the output of that procedure; see o3np code and comments
  # for details.
  #


o3np := proc( a, b, x )
  #
  #
  #
  #
  # Takes as input the polynomials a and b in the
  # indeterminate x, with algebraic number coefficients.
  #
  #
  # Computes the Galois group of Dx^3 + a*Dx + b over the field
  # of rational functions with algebraic number coefficients.
```

```
#
#
# Returns as output a list of the form
#
#         [ U, P, Conj ].
#
# where U is the name of a unipotent group, P is the name of a
# reductive group, and the conjugation action of P on U is
# described by Conj.
#
#
# A nontrivial unipotent group U is one of the following:
#
#    "U3", "C^2", "C", "0".
#
#
# A reductive group P is one of the following:
#
#    "SL3", "PSL2", "GL2", "SL2", "C*^2" (i.e., C* x C*), "C*", "1".
#
#
#
# The conjugation action Conj for a semidirect product
# is represented in one of the following ways, depending on U and P:
#
#    *** If U = 0, then Conj = "0"
#
#    *** C^2 by SL2 or GL2:
#        Conj = "matrix_vector" or "vector_transpose_matrix_inverse"
#
#    *** C by C*:
#        Conj = d, where t.u = t^d * u for t in C*, u in C
#
#    *** C by C*^2:
#        Conj = [d1,d2], where (t1,t2).u = t1^d1 * t2^d2 * u
#        for t1, t2 in C*, u in C
#
#    *** C^2 by C*:
#        Conj = [d1,d2], where t.(u1,u2) = (t^d1 * u1, t^d2 * u2)
#        for t in C*, u1, u2 in C
#
#    *** C^2 by C*^2:
#        Conj = [ [d1,d2], [e1,e2] ] where
#
#           (t1,t2).(u,v) = ( t1^d1 * t2^d2 * u, t1^e1 * t2^e2 * v )
#
#        for t1, t2 in C*, u, v in C
#
#    *** U3 by C*:
```

```
  #         Conj. = [d1, d2], where C* embeds in SL3 via
  #         t  |-->  diag( t^d1, t^d2, t^(-d1-d2) ) and
  #         U3 is the group of upper triangular matrices in SL3 with
  #         1s along the diagonal.
  #
  #     *** U3 by C*^2:
  #         Conj. = "standard". In this case, the group is conjugate to
  #         T3 intersect SL3, the group of upper triangular matrices in
  #         SL3.  Thus there is only one possible conjugation action.
  #
  #
```

A.2 Maple code

```
# File o3np.mpl
# by Peter Berman.
# Version 1.0. July 23, 2001. Compatible with Maple 6.


#
# CONTENTS:
#
# I.   Initialization, general tools
# II.  compute_torus code
# III. o3np code
# IV.  order_3_no_pole code
#





#
# I.  Initialization, general tools
#


with(linalg):
with(DEtools):



logDiff := proc( f, x );
  #
  # logDiff stands for LOGarithmic DIFFerentiation
  #
```

```
  return  diff( f, x ) / f ;
end:


rfldtest := proc( f, x )
  #
  # rfld stands for Rational Function Logarithmic Derivative.
  # This procedure returns TRUE if f = g'/g for some rational
  # function g, FALSE otherwise.
  #
  local s;
  s := ratsols(diff(y(x),x) - f*y(x), y(x));
  if not ( s = [] ) then
    return  true ;
  fi;
  return  false ;
end:


numES := proc( L, dom )
  #
  # numES stands for NUMber of Exponential Solutions.
  # This procedure returns either a nonnegative integer
  # or infinity, equal to the number of solutions of
  # L(y) = 0 of the form exp(int(g)), g a rational function.
  #
  local Lde, es, esx, esld, n, i, j, y, t, x;
  Lde := diffop2de( L, y(t), dom );
  es := expsols( Lde = 0, y(t) );
  n := nops( es );
  if ( n = 0 ) then
    return  0 ;
  fi;
  x := op( 2, dom );
  esx := subs( t=x, es );
  esld := map( logDiff, esx, x );
  for i from 1 to n do
    for j from (i+1) to n do
      if ( rfldtest( op(i, esld) - op(j, esld), x ) ) then
        return  infinity ;
      fi;
    od;
  od;
  return  n ;
end:
```

```
#
# II. compute_torus code
#
```

```
make_monic := proc( Llist, dom )
  #
  # Input:  Llist, a list of three first-order
  #         operators over the domain dom whose
  #         product is monic
  #
  # Converts Llist to a list of monic first-order operators
  # whose product is also equal to L. (Note: This
  # is a precautionary measure. The elements of Llist
  # are assumed to have been computed using the DEtools
  # DFactor command, which might automatically return
  # its factor list in this form.)
  #
  # Output: a list M of three monic first-order
  #         operators such that
  #         mult(Llist[1], Llist[2], Llist[3], dom) =
  #         mult(M[1], M[2], M[3], dom).
  #
  #
  local M, f, s, Dx, x;
  Dx := dom[1];
  x := dom[2];
  f := map( coeff, Llist, Dx, 1 );
  s := map( coeff, Llist, Dx, 0 );
  if ( f = [1,1,1] ) then return  Llist ; fi;
  M := [0,0,0];
  M[1] := Dx + s[1]/f[1] + logDiff( f[2]*f[3], x );
  M[2] := Dx + s[2]/f[2] + logDiff( f[3], x );
  M[3] := Dx + s[3]/f[3];
  M;
end:
```

```
Llist2rlist := proc( Llist, dom )
  #
  # Input: Llist, a list [L3, L2, L1] of first-order operators
  #        over dom, such that
  #
  #         Dx^3 + a*Dx + b = mult(L3,L2,L1,dom)
```

```
  #
  # Output: A list [r3, r2, r1] of rational functions such that
  #
  # mult( L3, L2, L1, dom ) = mult( Dx - r3, Dx - r2, Dx - r1, dom )
  #
  local Mlist, Rlist, Dx, x;
  Dx := dom[1];
  x := dom[2];
  Mlist := make_monic( Llist, dom );
  Rlist := map( coeff, Mlist, Dx, 0 );
  Rlist := map( x -> (-1)*x, Rlist );
  Rlist;
end:



cf2 := proc( fn )
  #
  # Helper function; see coefficient_field below.
  # This function recursively computes and returns a set
  # containing all RootOfs appearing in fn.
  #
  local u, s;
  if type( fn, RootOf ) then
    return  { fn } ;
  fi;
  if nops( fn ) = 1 then
      return  {} ;
  fi;
  s := {};
  for u in fn do
    s := s union cf2( u );
  od;
  s;
end:



coefficient_field := proc( f )
  #
  # Takes as input either a rational function with
  # algebraic-number coefficients -- i.e., a function
  # built up from rational numbers, RootOfs and symbols
  # using addition, subtraction, multiplication and addition --
  # or a list or set of such functions.
  #
  # Returns an ordered list [ s[1], s[2], ..., s[n] ]
  # of the RootOfs that appear in f.
  # s[j] fails to appear in s[i] if i < j.
```

```
  #
  local fcollection, g, gnormal, s;
  if type( f, list ) or type( f, set ) then
    fcollection := f;
  else
    fcollection := { f };
  fi;
  s := {};
  for g in fcollection do
    gnormal := evala( Normal ( g ) );
    s := s union cf2( gnormal );
  od;
  s := [op(s)];
  s := sort( s, proc(a,b) return  not evalb( has( a, b ) ) end );
  s;
end:


parfrac_summand_decomp := proc( f, x, C_0 )
  #
  # Takes as input f, a summand of a partial fraction decomposition
  # in the indeterminate x over the field C_0. It is assumed that
  # f has nontrivial denominator. That is, it is assumed that we can
  # write f = N/Q^d, where:
  #
  #    * N and Q are polynomials over C_0
  #    * degree(N) < degree(Q)
  #    * Q is monic and irreducible over C_0
  #    * d is an integer, d >= 1
  #
  # Returns as output the list [N, Q, d].
  #
  local N1, D1, L, u, Q1, d, c;
  N1 := numer( f );
  D1 := denom( f );
  L := evala( Factors( D1, C_0 ) );
  u := L[1];
  if nops( L[2] ) > 1 then
    error  "Too many factors in denominator of \
            partial fractions summand %1" , f ;
  fi;
  Q1 := L[2][1][1];
  d := L[2][1][2];
  # f = N1 / (u*Q1^d)
  c := lcoeff( Q1, x );
  # f = N1 / (u*(c*Q2)^d) = N1 / (u * c^d * Q2^d)
  #   = (N1 / u / c^d) / Q2^d
  return  [ N1/u/c^d, Q1/c, d ] ;
end:
```

```
rational_number_summand_in := proc( a_input )
  #
  # Takes as input an algebraic number a_input. Suppose
  # a_input = a1 + a2, where a1 is a rational number and
  # a2 is a Q-linear combination of nontrivial power products
  # of RootOfs.  Then this procedure returns a1.
  #
  local a_normal, u;
  a_normal := evala( Normal( a_input ) );
  if not type( a_normal, algnum ) then
    error   "%1 is not an algebraic number", a_input;
  fi;
  if not type( a_normal, `+` ) then
    #
    # There is only one summand in  a_normal.  Replace  a_normal
    # with  { a_normal } so that the subsequent loop through the
    # operands of  a_normal  treats  a_normal as a summand.
    #
    a_normal := { a_normal };
  fi;
  #
  # a_normal is an expanded element of the polynomial algebra
  # determined by the RootOfs that appear in a_input.  The
  # following loop searches the operands that appear in a_normal.
  # If one of the summands is a rational number, then the procedure
  # returns this number (which is unique); otherwise the procedure
  # returns zero.
  #
  for u in  a_normal  do
    if type( u, rational ) then
      return  u ;
    fi;
  od;
  return  0 ;
end:



ratfun_relation := proc( s1, s2, x )
  #
  # Takes the rational functions s1 and s2 with algebraic number
  # coefficients as input.
  #
  # It is assumed that the distinct RootOfs appearing in s1 and s2
  # are independent.
  #
```

```
# Returns as output a list [j1,j2] of integers such that
#
#          j1*s1 + j2*s2 = h'/h
#
# for some rational function h.
#
# The list will be nonzero if possible; i.e., if there exist
# integers n1, n2, not both zero, such that n1*s1 + n2*s2 = g'/g
# for some rational function g, then the output of
# ratfun_relation is UNEQUAL to [0,0].
#
# If j1,j2 are not both zero, then [j1,j2] will be
# in lowest possible terms. That is, if [j1,j2] = [c*k1,c*k2]
# for some integers c, k1, k2 such that k1*s1 + k2*s2 = f'/f
# for some rational function f, then c is equal to
# either 1 or -1.
#
local C_0, sp, i, u, s_fld, s_cancel, psd, A, Q, Qprime,
   alpha, B, alpha1, alpha2, scq, fld_denoms, n;
if  s1 = 0 then return  [1,0] ; fi;
if  s2 = 0 then return  [0,1] ; fi;
C_0 := coefficient_field( [ s1, s2 ] );
sp := [0,0];
s_fld := [0,0];
s_cancel := [0,0];
fld_denoms := [{},{}];
#
#
# sp will be a two-element list consisting of the
# partial-fraction decompositions of s1 and s2 over C_0.
# s_fld (for Fraction of a Logarithmic Derivative) will be
# a two-element list such that s_fld[i] is the "part" of
# sp[i] which is the log-derivative of an nth root of a
# rational function over C_0 for some n.  s_cancel will be a
# two-element list such that
#
#      sp[i] = s_fld[i] + s_cancel[i];
#
# we will want s_cancel[1] and s_cancel[2] to "cancel" in
# the sense that some Z-linear combination of these two
# rational functions should be zero; i.e., that they differ
# multiplicatively by a rational number.
#
#
sp[1] := convert( s1, parfrac, x, C_0 );
sp[2] := convert( s2, parfrac, x, C_0 );
for i from 1 to 2 do
  if not type( sp[i], `+` ) then
    #
```

```
    # There is only one summand in the partial-fraction
    # decomposition of s_i. Replace s_i with { s_i } so that
    # the subsequent loop through the operands of s_i treats
    # s_i as a summand.
    #
    sp[i] := { sp[i] };
  fi;
  for u in sp[i] do
    if type( u, polynom ) then
      #
      # Summand is of the form c*x^d with d >= 0;
      # place in s_cancel[i]
      #
      s_cancel[i] := s_cancel[i] + u;
      next;
    fi;
    psd := parfrac_summand_decomp( u, x, C_0 );
    if psd[3] > 1 then
      #
      # Summand is of the form A/Q^d with d > 1;
      # place in s_cancel[i]
      #
      s_cancel[i] := s_cancel[i] + u;
    else
      #
      # Summand is of the form A/Q, Q irreducible over C_0;
      # write A = alpha*diff(Q,x) + B, where deg B < deg Q'.
      # Then write alpha = alpha1 + alpha2, where
      # alpha1 is a rational number and alpha2 is a
      # Q-linear combination of nontrivial power products of
      # RootOfs.  Then,
      #
      #  A/Q = ((alpha1+alpha2)*Q' + B)/Q
      #      = (alpha1 * Q' / Q) + (alpha2*Q'+B)/Q
      #      = f1 + f2.
      #
      # Add f1 to s_fld[i], f2 to s_cancel[i].
      #
      #
      #
      A := psd[1];
      Q := psd[2];
      Qprime := diff( Q, x );
      alpha := quo( A, Qprime, x, 'B' );
      if degree( alpha, x ) > 0 then
        error "Unexpected high-degree numerator in \
               partial fractions summand %1", A/Q;
      fi;
      alpha1 := rational_number_summand_in( alpha );
```

```
        fld_denoms[i] := fld_denoms[i] union { denom( alpha1 ) };
        alpha2 := alpha - alpha1;
        s_fld[i] := s_fld[i] + alpha1 * Qprime / Q;
        s_cancel[i] := s_cancel[i] + (alpha2 * Qprime + B)/Q;
      fi;
    od;
  od;
  if s_cancel[1] = 0 then
    return  [ lcm(op(fld_denoms[1])), 0 ] ;
  fi;
  if s_cancel[2] = 0 then
    return  [0, lcm(op(fld_denoms[2]))] ;
  fi;
  scq := evala( Normal( s_cancel[1]/s_cancel[2] ) );
  if type( scq, rational ) then
    #
    # The s_cancel parts differ by a multiplicative rational number, scq.
    # Say scq = n1/n2; then s_cancel[1]/s_cancel[2] = n1/n2, so that
    # n2*s_cancel[1] - n1*s_cancel[2] = 0 and therefore (by hypotheses)
    # n2*s1 - n1*s2 is the log-derivative of the nth root of
    # a rational function, so that
    # n*n2*s1 - n*n1*s2 is the log-derivative of a rational function.
    # Here, n is the LCM of the denominators of the rational numbers
    # alpha1 found above.
    #
    n := lcm( op(fld_denoms[1]), op(fld_denoms[2]) );
    return  [ n * denom( scq ), (-1) * n * numer( scq ) ] ;
  else
    #
    # The s_cancel parts fail to cancel
    #
    return  [0, 0] ;
  fi;
end:


compute_torus := proc( r1, r2, x )
  #
  # This procedure assumes that r1 and r2 are rational functions
  # in the indeterminate x satisfying the following property:
  # Let
  #
  #      L = mult( Dx + r1 + r2, Dx - r2, Dx - r1, dom ),
  #
  # where dom = [Dx,x].  Then there exist polynomials a, b
  # such that
  #
  #      L = Dx^3 + a*Dx + b.
```

```
#
# This procedure computes the group of
#
#     Lred = LCLM( Dx + r1 + r2, Dx - r2, Dx - r1, dom).
#
# Moreover, if this group is a one-dimensional torus, then
# the procedure computes the matrix representation
# of this group on the solution space of Lred, relative to
# the ordered basis {R1, R2, 1/R1/R2}.  Here, R_i is a
# function whose logarithmic derivative is r_i for i = 1,2.
# This ordered basis is chosen because it corresponds
# with a basis of the solution space of L, relative to which
# the group of L is upper-triangular. In particular, R1
# is a solution of L.
#
#
# This procedure returns as output a list of one of
# the following types:
#
#
# [0] -- if the group of Lred is trivial (0-dimensional).
#
#
# [2] -- if the group of Lred is C* x C* (2-dimensional).
#        In this case, the group is represented as
#
#             { diag( u, v, w ) : uvw = 1}.
#
#
# [1, [e1, e2]] -- if the group of Lred is C* (1-dimensional).
#                In this case, the matrix representation
#                referred to above has image
#
#                   { diag(u,v,w): u^e2 = v^e1, uvw = 1 }.
#
#                Moreover, it is parameterized by the mapping
#
#                   t |--> diag( t^e1, t^e2, t^(-e1-e2) )
#
#                for t in C*.  Also, e1 >= 0; this is
#                guaranteed in the procedure by replacing
#                (e1, e2) with (-e1, -e2) if necessary.
#
#
local jlist, elist;
  if ( rfldtest( r1, x ) and rfldtest( r2, x ) ) then
    #
    # group is trivial
    #
```

```
      return  [0] ;
    fi;
    jlist := ratfun_relation( r1, r2, x );
    if ( jlist = [0, 0] ) then
      #
      # group is C* x C*
      #
      return  [2] ;
    fi;
    #
    # ratfun_relation returns [j1, j2] such that j1*r1 + j2*r2 = h'/h
    # for some rational function h, i.e., R1^j1 * R2^j2 = h.
    #
    # Define [e1,e2] = [-j2, j1], so that replacing R1 with t^e1 * R1
    # and R2 with t^e2 * R2 preserves the relation R1^j1 * R2^j2 = h.
    # Then make sure that e1 >= 0.
    #
    elist := [ (-1) * jlist[2], jlist[1] ];
    if elist[1] < 0 then
      elist := [ (-1)*elist[1], (-1)*elist[2] ];
    fi;
    [ 1, elist ];
  end:


#
# III. o3np code
#


sl2test := proc( L, dom )
  #
  # Input:  L, an irreducible
  #         second-order differential operator
  #         over dom whose group is known to be
  #         either SL_2 or GL_2
  #
  # Output: Returns true if the group is SL_2,
  #         false if GL_2
  #
  local x, Dx, f;
  Dx := dom[1];
  x := dom[2];
  f := coeff( L, Dx );
  rfldtest( f, x );
end:
```

```
o3np := proc( a, b, x )
  #
  #
  #
  #
  # Takes as input the polynomials a and b in the
  # indeterminate x, with algebraic number coefficients.
  #
  #
  # Computes the Galois group of Dx^3 + a*Dx + b over the field
  # of rational functions with algebraic number coefficients.
  #
  #
  # Returns as output a list of the form
  #
  #         [ U, P, Conj ].
  #
  # where U is the name of a unipotent group, P is the name of a
  # reductive group, and the conjugation action of P on U is
  # described by Conj.
  #
  #
  # A nontrivial unipotent group U is one of the following:
  #
  #    "U3", "C^2", "C", "0".
  #
  #
  # A reductive group P is one of the following:
  #
  #    "SL3", "PSL2", "GL2", "SL2", "C*^2" (i.e., C* x C*), "C*", "1".
  #
  #
  #
  # The conjugation action Conj for a semidirect product
  # is represented in one of the following ways, depending on U and P:
  #
  #    *** If U = 0, then Conj = "0"
  #
  #    *** C^2 by SL2 or GL2:
  #        Conj = "matrix_vector" or "vector_transpose_matrix_inverse"
  #
  #    *** C by C*:
  #        Conj = d, where t.u = t^d * u for t in C*, u in C
  #
  #    *** C by C*^2:
  #        Conj = [d1,d2], where (t1,t2).u = t1^d1 * t2^d2 * u
```

```
#        for t1, t2 in C*, u in C
#
#    *** C^2 by C*:
#        Conj = [d1,d2], where t.(u1,u2) = (t^d1 * u1, t^d2 * u2)
#        for t in C*, u1, u2 in C
#
#    *** C^2 by C*^2:
#        Conj = [ [d1,d2], [e1,e2] ] where
#
#           (t1,t2).(u,v) = ( t1^d1 * t2^d2 * u, t1^e1 * t2^e2 * v )
#
#        for t1, t2 in C*, u, v in C
#
#    *** U3 by C*:
#        Conj. = [d1, d2], where C* embeds in SL3 via
#        t  |-->  diag( t^d1, t^d2, t^(-d1-d2) ) and
#        U3 is the group of upper triangular matrices in SL3 with
#        1s along the diagonal.
#
#    *** U3 by C*^2:
#        Conj. = "standard". In this case, the group is
#        conjugate to T3 intersect SL3,
#        the group of upper triangular matrices in SL3.
#        Thus there is only one possible conjugation action.
#
#
local Dx, dom, L, Ladj, Lfactors, rlist, r1, r2, r3, L1, L2,
  L2sharp, Ltest, n1, n2, Ls2, Ls2factors,
  t, GredList, f, g, s, Ltemp, Ltemp1, elist;
dom := [Dx, x];
L := Dx^3 + a*Dx + b;
Ladj := DEtools[adjoint]( L, dom );
Lfactors := DFactor( L, dom );
n1 := numES( L, dom );
n2 := numES( Ladj, dom );
if ( n1 = 0 ) then
  if ( n2 = 0 ) then
    #
    # n1 = n2 = 0
    #
    Ls2 := symmetric_power(L, 2, dom);
    if ( degree( Ls2, Dx ) = 5 ) then
      return  [ "0", "PSL2", "0" ] ;
    fi;
    Ls2factors := DFactor( Ls2, dom );
    if ( nops( Ls2factors ) > 1 ) then
      return  [ "0", "PSL2", "0" ] ;
    else
      return  [ "0", "SL3", "0" ] ;
```

```
    fi;
  elif ( n2 = 1 ) then
    #
    # n1 = 0, n2 = 1
    #
    L2 := Lfactors[2];
    if ( sl2test( L2, dom ) ) then
      return  [ "C^2", "SL2", "matrix_vector" ] ;
    else
     return  [ "C^2", "GL2", "matrix_vector" ] ;
     fi;
  else
    error "for n1 = 0, unexpected n2: %1", n2;
  fi;
elif ( n1 = 1 ) then
  if ( n2 = 0 ) then
    #
    # n1 = 1, n2 = 0
    #
    L2 := Lfactors[1];
    if ( sl2test( L2, dom ) ) then
      return  [ "C^2", "SL2", "matrix_vector" ] ;
    else
      return  [ "C^2", "GL2", "vector_transpose_matrix_inverse" ] ;
    fi;
  elif ( n2 = 1 ) then
    #
    # n1 = n2 = 1
    #
    if ( nops( Lfactors ) = 2 ) then
      #
      # L is a LCLM of an irreducible 2nd-order and a
      # 1st-order operator
      #
      L1 := Lfactors[1];
      L2 := Lfactors[2];
      #
      # Define Ltest to be the second-order factor of L,
      # then apply sl2test.  NOTE: Could also seek rational
      # solutions of the first-order factor of L
      #
      #
      if ( degree( L1, Dx ) = 2 ) then
        Ltest := L1;
      else
        Ltest := L2;
      fi;
      if ( sl2test( Ltest, dom ) ) then
        return  [ "0", "SL2", "0" ] ;
```

```
    else
      return  [ "0", "GL2", "0" ] ;
    fi;
  else
    #
    # L is a product of three first-order operators
    #
    rlist := Llist2rlist( Lfactors, dom );
    r2 := rlist[2];
    r1 := rlist[3];
    GredList := compute_torus( r1, r2, x );
    if ( GredList[1] = 2 ) then
      #
      # torus is C*^2
      #
      return  [ "U3", "C*^2", "standard" ] ;
    elif (GredList[1] = 1 ) then
      #
      # torus is C*
      #
      elist := GredList[2];
      if ( elist[2] = 0 ) then
        #
        # Torus representation is t |--> [t,1,1/t]
        #
        g := ratsols( diff(y(x),x) - r2*y(x), y(x) )[1];
        #
        # The next line rules out the case where g is a constant.
        # This ensures that the subsequent calls to ratsols will be
        # for inhomogeneous differential equations.
        #
        if ( diff( g, x ) = 0 ) then
          return  [ "C", "C*", 1 ] ;
        fi;
        Ltemp := mult(Dx,Dx-r1-2*r2,dom);
        Ltemp1 := diffop2de(Ltemp,y(x),dom);
        s := ratsols( Ltemp1 = r2*g^3,y(x) );
        if ( nops(s) = 1 ) then
          #
          # inhomogeneous equation has no rational solutions;
          # Maple has returned only a list of solutions to the
          # homogeneous equation
          #
          return  [ "U3", "C*", [ 1, 0 ] ] ;
        else
          #
          # decide between C and C^2 for unipotent radical
          #
          Ltemp := mult(Dx,Dx-r1-2*r2,Dx-2*r1-r2,dom);
```

```
          Ltemp1 := diffop2de(Ltemp,y(x),dom);
          s := ratsols( Ltemp1 = r2*g^3, y(x) );
          if ( nops(s) = 1 ) then
            #
            # inhomogeneous equation has no rational solutions;
            # Maple has returned only a list of solutions to
            # the homogeneous equation
            #
            return  [ "C^2", "C*", [ 1, 2 ] ] ;
          else
            return  [ "C", "C*", 1 ] ;
          fi;
        fi;
      else
        #
        # Torus representation is NOT [t,1,1/t];
        # unipotent radical must be U3
        #
        return  [ "U3", "C*", elist ] ;
      fi;
    else
      error  "unexpected trivial torus in case n1 = n2 = 1" ;
    fi;
  fi;
elif ( n2 = 2 ) then
    #
    # n1 = 1, n2 = 2
    #
    rlist := Llist2rlist( Lfactors, dom );
    r2 := rlist[2];
    r1 := rlist[3];
    GredList := compute_torus( r1, r2, x );
    if ( GredList[1] = 2 ) then
      #
      # torus is C*^2
      #
      return  [ "C^2", "C*^2", [ [1, -1], [2, 1] ] ] ;
    elif ( GredList[1] = 1 ) then
      #
      # torus is C*
      #
      elist := GredList[2];
      return  [ "C^2", "C*", [ elist[1] - elist[2], \
              2*elist[1] + elist[2] ] ] ;
    else
      error  "unexpected trivial torus in case n1 = 1, n2 = 2" ;
    fi;
elif ( n2 = infinity ) then
  #
```

```
      # n1 = 1, n2 = infinity
      #
      return  [ "C^2", "C*", [ -3, -3 ] ] ;
    else
      error  "for n1 = 1, unexpected n2: %1", n2 ;
    fi;
  elif ( n1 = 2 ) then
    if ( n2 = 1 ) then
      #
      # n1 = 2, n2 = 1
      #
      rlist := Llist2rlist( Lfactors, dom );
      r2 := rlist[2];
      r1 := rlist[3];
      GredList := compute_torus( r1, r2, x );
      if ( GredList[1] = 2 ) then
          #
          # torus is C*^2
          #
          return  [ "C^2", "C*^2", [ [ 2, 1 ], [ 1, 2 ] ] ] ;
      elif (GredList[1] = 1 ) then
          #
          # torus is C*
          #
          elist := GredList[2];
          return  [ "C^2", "C*", [ 2*elist[1] + elist[2], \
             elist[1] + 2*elist[2] ] ] ;
      else
        error  "unexpected trivial torus in case n1 = 2, n2 = 1" ;
      fi;
    elif ( n2 = 2 ) then
      #
      # n1 = n2 = 2
      #
      rlist := Llist2rlist( Lfactors, dom );
      r2 := rlist[2];
      r1 := rlist[3];
      GredList := compute_torus( r1,r2, x );
      if ( GredList[1] = 2 ) then
          #
          # torus is C*^2
          #
          return  [ "C", "C*^2", [ 2, 1 ] ] ;
      elif ( GredList[1] = 1 ) then
          #
          # torus is C*
          #
          elist := GredList[2];
          L2 := mult( Lfactors[2], Lfactors[3], dom);
```

```
        L2sharp := mult( Lfactors[1], Lfactors[2], dom);
        if ( numES( L2, dom)  = 1 ) then
          return  [ "C", "C*", elist[1] - elist[2] ] ;
        elif ( numES( L2sharp, dom)  = 1 ) then
          return  [ "C", "C*", elist[1] + 2*elist[2] ] ;
        fi;
        return  [ "C", "C*", 2*elist[1] + elist[2] ];
      else
        error  "unexpected trivial torus in case n1 = 2, n2 = 2";
      fi;
    elif ( n2 = infinity ) then
      #
      # n1 = 2, n2 = infinity
      #
      return  [ "C", "C*", -3 ] ;
    else
      error  "for n1 = 2, unexpected n2: %1", n2;
    fi;
  elif ( n1 = 3 ) then
    if ( n2 = 3 ) then
      #
      # n1 = n2 = 3
      #
      rlist := Llist2rlist( Lfactors, dom );
      r2 := rlist[2];
      r1 := rlist[3];
      GredList := compute_torus( r1,r2, x );
      if ( GredList[1] = 2 ) then
        return  [ "0", "C*^2", "0" ] ;
      elif ( GredList[1] = 1 ) then
        return  [ "0", "C*", "0" ] ;
      else
        error  "unexpected trivial torus in case n1 = 3, n2 = 3" ;
      fi;
    else
      error  "for n1 = 3, unexpected n2: %1", n2 ;
    fi;
  else
    if ( n2 = 1 ) then
      #
      # n1 = infinity, n2 = 1
      #
      return  [ "C^2", "C*", [ 3, 3 ] ] ;
    elif ( n2 = 2 ) then
      #
      # n1 = infinity, n2 = 2
      #
      return  [ "C", "C*", 3 ] ;
    elif ( n2 = infinity ) then
```

```
      #
      # n1 = n2 = infinity
      #
      rlist := Llist2rlist( Lfactors, dom );
      r2 := rlist[2];
      r1 := rlist[3];
      GredList := compute_torus( r1, r2, x );
      if ( GredList[1] = 1 ) then
        return  [ "0", "C*", "0" ] ;
      elif ( GredList[1] = 0 ) then
        return  [ "0", "1", "0" ] ;
      else
        error  "unexpected 2-dimensional torus in case\
           n1 = n2 = infinity";
      fi;
    else
      error "for n1 = infinity, unexpected n2: %1", n2 ;
    fi;
  fi;
end:




#
# IV.  order_3_no_pole code
#


translate_matrix_text := proc( s, txt )
  #
  # This procedure takes as input s, a Maple name that describes
  # a certain type of conjugation action.  See the comments
  # for o3np, under conjugation action of SL2 or GL2 on C^2.
  #
  # It returns as output an English-language description
  # of that action.
  #
  if ( s = "matrix_vector" ) then
    return  cat( "M.v = Mv for M in ", txt, ", v in C^2.\
      (matrix-vector multiplication)") ;
  elif ( s = "vector_transpose_matrix_inverse" ) then
    return  cat( "M.v = multiply( transpose(v), inverse(M) )\n\
       for M in ",txt, ", v in C^2.\n (multiplication of vector\
       transpose by matrix inverse)" ) ;
  else
    error "Incorrect call to translate_matrix_text";
  fi;
end:
```

```
order_3_no_pole := proc( f, g, x )
  #
  # This procedure takes as input the polynomials f and g in x,
  # and returns as output a paragraph describing the Galois group
  # of the operator D^3 + fD + g over C(x), where C is the
  # field of algebraic numbers.
  #
  # It is a wrapper function for o3np, providing a text description
  # for the output of that procedure; see o3np code and comments
  # for details.
  #
  local G, L, Dx, U, P, Conj, ConjText;
  G := o3np( f, g, x );
  L := Dx^3 + f*Dx + g;
  U := G[1];
  P := G[2];
  Conj := G[3];
  if ( U = "0" ) then
    printf("\nThe group of %A is %A.\n\n", L, G[2] );
    return;
  fi;
  if ( U = "U3" ) then
    if ( P = "C*" ) then
      printf( "\nThe group of %A is a semidirect product\
        of U3 by C*.\nIt is isomorphic to the subgroup of\
        GL3 given by\nthe equations t21 = t31 = t32 = 0,\
        t11 * t22 * t33 = 1, t11^%d = t22^%d.\n\n",
        L, Conj[2], Conj[1] );
        return ;
    elif ( P = "C*^2" ) then
      printf( "\nThe group of %A is a semidirect product\
        of U3 by C* x C*.\nIt is isomorphic to T3 intersect SL3,\
        i.e., the subgroup of GL3 given by\nthe equations\
        t21 = t31 = t32 = 0, t11 * t22 * t33 = 1.\n\n", L );
      return ;
    else
      error "In case U = U3, unexpected reductive subgroup: %1", P;
    fi;
  elif ( U = "C" ) then
    if ( P = "C*" ) then
      ConjText := sprintf( "t.u = t^%d * u for t in C*, u in C", Conj );
    elif( P = "C*^2" ) then
      ConjText := sprintf( "(t1, t2).u = t1^%d * t2^%d * u\n\
         for t1, t2 in C*, u in C", Conj[1], Conj[2] );
    else
      error "In case U = C, unexpected reductive subgroup: %1", P;
    fi;
```

```
  elif ( U = "C^2" ) then
    if ( P = "GL2" or P = "SL2" ) then
      ConjText := translate_matrix_text( Conj, convert(P,string) );
    elif ( P = "C*^2" ) then
      ConjText := sprintf( "(t1,t2).(u,v) = (t1^%d * t2^%d * u,\
        t1^%d * t2^%d * v)\nfor t1, t2 in C*, u, v in C",\
        Conj[1][1], Conj[1][2], Conj[2][1], Conj[2][2] );
    elif ( P = "C*" ) then
      ConjText := sprintf( "t.(u,v) = (t^%d * u, t^%d * v)\n\
        for t in C*, u, v in C", Conj[1], Conj[2] );
    else
      error "In case U = C^2, unexpected reductive subgroup: %1", P;
    fi;
  else
    error  "Unexpected unipotent subgroup: %1", U ;
  fi;
  printf("\nThe group of %A is a semidirect product of %A by %A.\n\
      The conjugation action of %A on %A is given as follows:\n\
      %s.\n\n", L, U, P, P, U, ConjText );
end:
```