INAUGURAL – DISSERTATION

zur
Erlangung der Doktorwürde
der
Naturwissenschaftlich-Mathematischen Gesamtfakultät
der
Ruprecht - Karls - Universität
Heidelberg

vorgelegt von
Diplom-Mathematikerin Julia Hartmann
aus Kassel
Tag der mündlichen Prüfung: 21.10.2002

Thema

On the Inverse Problem in Differential Galois Theory

Gutachter: Prof. Dr. Bernd Heinrich Matzat

Prof. Dr. G. Kemper

Contents

Introduction

Differential Galois theory is a generalization of the usual Galois theory for polynomials to linear differential equations. The analog of a field in this context is a differential field, i.e., a field with a derivation. There is the notion of a splitting field (a Picard-Vessiot extension) of a linear differential equation and the differential Galois group is the group of automorphisms of this Picard-Vessiot extension over the base differential field which respect the derivation. Just as usual Galois groups come equipped with a standard permutation representation given by the action on the roots of a polynomial defining the extension, the differential Galois groups have a faithful linear representation over the field of constants K of the differential field under consideration, given by the action on the solution space of the differential equation. Moreover, it can be shown that the image of this representation is Zariski-closed, i.e., that any differential Galois group is isomorphic to the set of K-rational points of a linear algebraic group.
Still in analogy with classical Galois theory, it is a very natural question to ask which linear algebraic groups occur in this way as differential Galois groups. This is the so-called *inverse problem*. Even in the most natural setting, namely when the field is just a rational function field $K(t)$ over the algebraically closed field K with derivation $\partial = \frac{d}{dt}$, no general answer was known.
Up to now, several cases of this problem have been solved:

- The *classical case* where $K = \mathbb{C}$, the field of complex numbers, was solved in 1979. Using analytic methods, Tretkoff and Tretkoff showed ([TT79]) that any linear algebraic group occurs as the differential Galois group of some linear differential equation over $\mathbb{C}(t)$. The main idea is to choose a finitely generated Zariski-dense subgroup of the group under consideration and to employ Plemelj's solution to Hilbert's 21st problem (also called the *Riemann-Hilbert problem*) to conclude that this latter group is the monodromy group of a linear differential equation of Fuchsian type. Since for Fuchsian type equations, the monodromy is Zariski-dense in the differential Galois group, this equation will realize the original group.

- In 1993, M. Singer solved the inverse problem for certain classes of groups ([Sin93]) over arbitrary algebraically closed fields of characteristic zero, extending the result of Tretkoff and Tretkoff. The space $\mathcal{L}$ of all linear differential equations of bounded order and with polynomial coefficients of bounded

degree can be identified with an affine space. For a linear algebraic group $\mathcal{G}$, Singer defines $\operatorname{Ker} X(\mathcal{G}^0)$ to be the intersection of the kernels of all linear characters of $\mathcal{G}^0$. He shows that this is a normal subgroup of $\mathcal{G}$, and that $\mathcal{G}^0/\operatorname{Ker} X(\mathcal{G}^0)$ is a torus (in particular, it is abelian). The action of $\mathcal{G}$ on $\mathcal{G}^0$ then induces an action of $\mathcal{G}/\mathcal{G}^0$ on $\mathcal{G}^0/\operatorname{Ker} X(\mathcal{G}^0)$. Singer proves that if this action is trivial, the set of linear differential equations of bounded order with solution space a fixed $\mathcal{G}$-module, bounded polynomial coefficients, and partly prescribed singularities, is a constructible subset of $\mathcal{L}$ (in the sense of algebraic geometry). For such groups, he is then able to vary the coefficient field $\mathbb{C}$ to any algebraically closed field of characteristic zero. In particular, since all linear characters of a semisimple group are trivial, his result implies that any linear algebraic group with semisimple connected component of the identity is a differential Galois group over $K(t)$ (see Theorem 4.3).

- In 1996, C. Mitschi and M. Singer gave a constructive solution of the *connected case* (i.e., the case when the group under consideration is connected), [MS96]. The use of the Lie algebra suggested in Kovacic's ground breaking work ([Kov69], [Kov71]) is the most important tool for their solution: If the matrix defining a differential equation is contained in the Lie algebra of a linear algebraic group, then the differential Galois group is (up to conjugation) a subgroup of that group (Proposition 2.5), and one also has a partial converse (Proposition 2.9). This upper bound reduces the task to finding a sufficiently general element of the Lie algebra as the defining matrix of the differential equation (here the strategy is that the generality of an element should prevent the differential Galois group from being too small). The proof can be simplified by using recent results of T. Oberlies on connected embedding problems ([Obe01]).

- Finally, C. Mitschi and M. Singer found a proof of the fact that all groups with solvable connected component occur as differential Galois groups ([MS00]). This was the first algebraic treatment of non connected groups. Some of the ideas used in this thesis can already be found there. Since the preprint [MS00] is unpublished and not in final form, we give our own proofs of the results we use.

In this context, we also mention that the corresponding inverse problem in positive characteristic differential Galois theory (so-called *iterative differential Galois theory*) has recently been solved by B.H. Matzat ([Mat01]).
The main result of this thesis is the following (Theorem 4.17):

Theorem 1. *Let K be an algebraically closed field of characteristic zero and let $\mathcal{G}$ be a linear algebraic group defined over K. Then there exists a Picard-Vessiot extension $E/K(t)$ such that* $\operatorname{Gal}(E/K(t)) \cong \mathcal{G}(K)$.

This thesis is organized as follows. In Chapter 1, we provide the preliminaries from differential Galois theory needed for the later chapters and thereby introduce the notation we use.
Chapter 2 deals with connected groups. We explain the concept of effectivity and the use of the Lie algebra, and show how this applies to so-called embedding problems. In the last section of Chapter 2, we sketch a proof of the connected inverse problem.
In Chapter 3, we turn to non connected groups. We recall some basic definitions and results from the theory of algebraic groups over non algebraically closed fields. This will be needed for the treatment of split embedding problems with connected kernel and finite cokernel given in the following two sections. In the non connected case, the Lie algebra does not encode enough information about the group. However, if we restrict ourselves to the situation when the connected component of the group has a finite complement, the Lie algebra inherits an action of this complement by conjugation. This action gives rise to a semilinear action which is given by composing the conjugation with a Galois action. In Section 3.2, we show that a necessary condition for a group of the type described above to be a differential Galois group is that there exists a realization of the connected component over its fixed field which is given by a matrix which is invariant under this action (the so-called equivariance condition). Section 3.3 contains a partial converse of this statement, which reduces the realization of such groups to effective equivariant realizations of their connected components over an algebraic extension of the differential field under consideration. The equivariance condition also allows us to generalize some results on embedding problems from the connected case, which is done is Section 3.4. In the last section of the chapter, we state what remains true in the general situation.
The last chapter is devoted to the proof of the above main theorem. We make several reduction steps using the structure theory of linear algebraic groups. These steps are combined in Section 4.4 to prove the main result.
Note: The bibliography is ordered by label.

Acknowledgments

Above all, I feel a deep sense of gratitude for my advisor B.H. Matzat. I thank him for his constant guidance, invaluable support, and for many fruitful mathematical conversations. He introduced me to this subject, suggested this research problem, and gave me new motivation exactly when I needed it.
I owe thanks to Michael Singer for inviting me to a short stay at the MSRI. I have greatly profited from discussions with him and with Claudine Mitschi during this visit. Further, I thankfully acknowledge valuable discussions with Daniel Betrand.
Let me extend my thanks to Larry Smith, who was always there when I needed advice.
Throughout the time of my thesis research, I have been accompanied and supported in many ways by members of the research group of B.H. Matzat and by other people at the IWR. In particular, I would like to mention Gregor Kemper, Jürgen Klüners,

Peter Müller and Thomas Oberlies who helped with critical remarks and comments on various versions of this thesis.
I leave a special note to my parents for many years of unfailing love and patient backing in all things.
Finally, I thank Ulli for believing in me even when I didn't. His love and encouragement were crucial for the completion of this thesis. He is the sunshine of my life.

Chapter 1

Preliminaries

In this chapter, we provide the preliminary material from differential Galois theory which is needed to develop the results of the later chapters. The reader familiar with the concept of Picard-Vessiot extensions and their basic properties may skip this chapter. We do not give proofs of the standard results. As a general reference, we suggest [vdP99].

1.1 Differential Fields and Differential Equations

Definition 1.1. *Let R be a commutative ring with a unit. A map $\partial : R \to R$ is called a* **derivation** *if it is additive and satisfies the Leibnitz rule*

$$\partial(a \cdot b) = \partial(a) \cdot b + a \cdot \partial(b)$$

for all $a, b \in R$. An element of R on which ∂ vanishes is called a **constant**, *and the set of all such elements is denoted by* $\mathrm{Const}(R)$. *A* **differential ring** *is a ring R equipped with a derivation.*

The notion of a differential field is analogous. One easily checks that the set of constants of a differential ring (resp. differential field) forms a subring (resp. subfield).

Definition 1.2. *A ring homomorphism $\varphi \in \mathrm{Hom}(R, S)$ of differential rings (R, ∂_R) and (S, ∂_S) is called a* **differential homomorphism** *if it commutes with the derivations, i.e., if $\varphi \circ \partial_R = \partial_S \circ \varphi$. An ideal in R which is stable under the derivation ∂_R is called a* **differential ideal**.

If R is a differential ring and $0 \notin S \subseteq R$ a multiplicatively closed subset, the derivation on R has a unique extension to $S^{-1}R$. In particular, a differential integral domain allows a unique extension of the derivation to its field of fractions.

Definition 1.3. *Let (F, ∂_F) be a differential field. An element $\ell = \sum_{i=0}^{n} a_i \partial^i \in F[\partial]$ with coefficients $a_i \in F$, $a_n \neq 0$ is called a* **differential operator** *of order n over F.*

Let $(E, \partial_E) \geq (F, \partial_F)$ be a differential field extension (i.e., $E \geq F$ is a field extension and $\partial_E|_F = \partial_F$). An element $y \in E$ such that $\ell(y) = 0$ is called a **solution** *of ℓ in E.*

It is not hard to see that the set of solutions of a differential operator ℓ in a differential extension $E \geq F$ forms a vector space over the field of constants of E of dimension at most the order of ℓ.
A solution $y \in E$ leads to a solution $\mathbf{y} = (y, \partial(y), \partial^2(y), \ldots, \partial^{n-1}(y))^{\mathrm{tr}} \in E^n$ of the matrix differential equation

$$\partial(Y) = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \end{pmatrix} Y$$

(where the differentiation on the left hand side is component-wise). The matrix associated to a differential operator in this way is sometimes called a companion matrix. On the other hand, any matrix $A \in F^{n\times n}$ defines a (matrix) differential equation $\partial(Y) = AY$.
If $B \in \mathrm{GL}_n(F)$ and $\mathbf{y}$ is a solution of $\partial(Y) = AY$, then

$$\partial(B\mathbf{y}) = \partial(B)\mathbf{y} + B\partial(\mathbf{y}) = (\partial(B)B^{-1} + BAB^{-1})B\mathbf{y},$$

i.e., $B\mathbf{y}$ is a solution of the differential equation

$$\partial(X) = (\partial(B)B^{-1} + BAB^{-1})X =: \tilde{A}X.$$

Since the solutions of the differential equations defined by A and $\tilde{A}$ can be transformed into one another by multiplication with a matrix in $\mathrm{GL}_n(F)$, the two differential equations have the same number of $\mathrm{Const}(E)$-linearly independent solutions in every differential field extension $E \geq F$. This motivates the following definition.

Definition 1.4. *Two matrices A and $\tilde{A}$ in $F^{n\times n}$ are called* **equivalent** *if there exists a matrix $B \in \mathrm{GL}_n(F)$ such that*

$$\tilde{A} = \partial(B)B^{-1} + BAB^{-1}.$$

It can be shown (see [Kat87]) that every matrix with coefficients in F is equivalent to the companion matrix of some differential operator over F. Since the matrix form of a differential equation is more suitable for our approach, we will use this formulation for all further considerations.
We will be particularly interested in extensions E of F in which a given differential equation defined by a matrix in $A \in F^{n\times n}$ has n $\mathrm{Const}(E)$-linearly independent solutions, i.e., when the solution space has the largest possible dimension. If $E \geq F$ is such an extension, there exists a matrix $Y \in \mathrm{GL}_n(E)$ satisfying $\partial(Y) = AY$.

Definition 1.5. *A matrix $Y \in \mathrm{GL}_n(E)$ such that $\partial(Y) = AY$ is called a* **fundamental solution matrix** *of the differential equation defined by A.*

One can also translate the above definitions into the setting of differential modules and connections (see, for example, [vdP99], Appendix A.4), but since we will make no use of this theory, we omit its treatment here.

1.2 Picard-Vessiot Extensions

In this section we will define the analog of a splitting field for differential equations and see that such fields always exist.

Definition 1.6. *A* **Picard-Vessiot ring** *for a differential equation defined by the matrix $A \in F^{n\times n}$ is a differential ring $R \geq F$ such that*

1. *R is a simple differential ring (i.e., contains no nontrivial differential ideals),*
2. *there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$ and*
3. *R is generated over F by the coefficients of Y and $\det(Y)^{-1}$.*

It can be shown that because of the first condition, a Picard-Vessiot ring is always an integral domain, which allows us to consider its field of fractions (equipped with the unique extension of the derivation).

Definition 1.7. *The field of fractions of a Picard-Vessiot ring for a differential equation over F is called a* **Picard-Vessiot field**. *We also call such a field a* **Picard-Vessiot extension** *of F without referring to a particular differential equation.*

The first condition of Definition 1.6 also guarantees that the field of constants of a Picard-Vessiot extension of F coincides with that of F ([vdP99], Lemma 3.2). It is shown in [vdP99] (Proposition 3.9), that a differential field extension E/F is a Picard-Vessiot field for a differential equation if and only if E/F is generated by the coefficients of a fundamental solution matrix of this equation and $\mathrm{Const}(E) = \mathrm{Const}(F)$.

Proposition 1.8. *Let F be a differential field with algebraically closed field of constants. Then for every differential equation over F there exists a Picard-Vessiot ring which is unique up to differential isomorphism. The field of constants of the corresponding Picard-Vessiot field coincides with the field of constants of F.*

The idea of construction of a Picard-Vessiot extension is very basic: We consider the coordinate ring $F[\mathrm{GL}_n] = F[X_{ij}, \det(X_{ij})^{-1}]$ of the general linear group and endow it with a derivation given by $\partial(X) = AX$, $X = (X_{ij})$. In this universal solution algebra, the matrix differential equation clearly has a fundamental solution

matrix (namely X). Condition 3 of Definition 1.6 is also satisfied. Factoring by a maximal differential ideal P guarantees differential simplicity and therefore gives the desired Picard-Vessiot ring. For details of the proof, see for example [vdP99], Proposition 3.6.

Remark 1.9. If in the above notation $R = F[\mathrm{GL}_n]/P$ is a Picard-Vessiot ring for a differential equation and $E = \mathrm{Quot}(R)$, the fundamental solution matrix obtained in the construction just described can be considered as an E-rational point of $\mathrm{Spec}(R)$, and then P is the ideal of all $f \in F[\mathrm{GL}_n]$ which vanish on Y.

1.3 The Differential Galois Group

Definition 1.10. *Let E/F be a Picard-Vessiot extension. The set of all differential automorphisms of E over F is called the* **differential Galois group** *of the extension and is denoted by* $\mathrm{Gal}(E/F)$.

In classical Galois theory, Galois groups come with a natural permutation representation given by the action on the roots of a polynomial defining the extension. In differential Galois theory, we have (as seen in Section 1.1) a full K-vector space of solutions with coefficients in a Picard-Vessiot extension E (where K is the common field of constants of E and F) and hence the differential Galois group is equipped with a linear representation. Explicitly, this can be described as follows. Let $A \in F^{n\times n}$ denote the matrix defining the differential equation and let $Y \in \mathrm{GL}_n(E)$ be a fundamental solution matrix. Then since $\sigma \in \mathrm{Gal}(E/F)$ fixes A, it sends Y to another fundamental solution matrix. Therefore, Y and $\sigma(Y)$ can only differ by a constant matrix (this can easily be checked), i.e., $C_\sigma := Y^{-1}\sigma(Y) \in \mathrm{GL}_n(K)$. This defines a faithful representation $\mathrm{Gal}(E/F) \hookrightarrow \mathrm{GL}_n(K)$.

Proposition 1.11. *The image of the differential Galois group under the monomorphism* $\mathrm{Gal}(E/F) \hookrightarrow \mathrm{GL}_n(K)$ *is a closed subgroup of* $\mathrm{GL}_n(K)$. *In particular, there exists a linear algebraic group $\mathcal{G}$ such that* $\mathrm{Gal}(E/F) \cong \mathcal{G}(K)$.

In classical Galois theory, the permutation representation is only defined after numbering the solutions. In differential Galois theory, the linear representation is only defined up to a choice of basis (since it depends on the fundamental solution matrix, which we can always modify by multiplication with a constant matrix on the right). The differential Galois correspondence works as follows (compare [vdP99], Proposition 3.13.):

Theorem 1.12. *Let F be a differential field with algebraically closed field of constants K, $A \in F^{n\times n}$ and E a Picard-Vessiot extension for A. Let $\mathcal{G}$ be a linear algebraic group over K with* $\mathrm{Gal}(E/F) \cong \mathcal{G}(K)$.

1. *There exists an anti-isomorphism between the lattice of closed subgroups $\mathcal{H}(K)$ of $\mathcal{G}(K)$ and the lattice of intermediate differential fields $E \geq L \geq F$ given by*

$$\mathcal{H}(K) \mapsto E^{\mathcal{H}(K)}, \qquad L \mapsto \mathrm{Gal}(E/L).$$

2. *If $\mathcal{H} \trianglelefteq \mathcal{G}$ is a normal subgroup, $E^{\mathcal{H}(K)}/F$ is a Picard-Vessiot extension with Galois group isomorphic to $(\mathcal{G}/\mathcal{H})(K)$.*

3. *Let $\mathcal{G}^0$ denote the connected component of the identity of $\mathcal{G}$. Then $L := E^{\mathcal{G}^0(K)}$ is a finite Galois extension of F with Galois group isomorphic to $(\mathcal{G}/\mathcal{G}^0)(K)$. Moreover, L is the algebraic closure of F in E.*

In the above theorem, we wrote $E^{\mathcal{H}(K)}$ for the fixed field under $\varphi^{-1}(\mathcal{H}(K))$, where $\varphi : \mathrm{Gal}(E/F) \to \mathcal{G}(K)$ is the given isomorphism. In the sequel, we will also use this notation without further explanation.

1.4 Torsors

For the proof of the above differential Galois correspondence one usually uses a structural theorem which is due to Kolchin (see, for example, [vdP99], Corollary 5.9). It states that after a finite field extension the Picard-Vessiot ring R becomes isomorphic to the coordinate ring of the differential Galois group $\mathcal{G}(K)$. This is a consequence of the fact that the affine scheme $\mathrm{Spec}(R)$ over F is a $\mathcal{G}_F$-torsor (the subscript indicates extension of scalars to F). Since we are going to make use of this latter fact, we include it here.

Definition 1.13. *Let $\mathcal{G}$ be a linear algebraic group defined over the field F. A* **$\mathcal{G}$-torsor** *(or a* **principal homogeneous space over $\mathcal{G}$***) is an affine scheme $\mathcal{X}$ over F with a right $\mathcal{G}$-action*

$$\Gamma : \mathcal{X} \times_F \mathcal{G} \to \mathcal{X}, \qquad (x, g) \mapsto xg$$

such that $\mathrm{id} \times \Gamma : \mathcal{X} \times_F \mathcal{G} \to \mathcal{X} \times_F \mathcal{X}$ *is an isomorphism.*
A $\mathcal{G}$-torsor $\mathcal{X}$ is called a **trivial $\mathcal{G}$-torsor** *if $\mathcal{X} \cong \mathcal{G}$ where the action is given by multiplication.*

Note that a $\mathcal{G}$-torsor $\mathcal{X}$ is trivial if and only if its set of F-rational points $\mathcal{X}(F)$ is non empty. Because of this, an element in $\mathcal{X}(F)$ is sometimes called a trivialization of the torsor.

Theorem 1.14. *Let F be a differential field of characteristic zero with algebraically closed field of constants. Let further $A \in F^{n\times n}$ be the defining matrix of a differential equation with Picard-Vessiot ring R and let $\mathcal{G}$ be a linear algebraic group defined over K such that* $\mathrm{Gal}(\mathrm{Quot}(R)/F) \cong \mathcal{G}(K)$. *Then* $\mathrm{Spec}(R)$ *is a $\mathcal{G}_F$-torsor.*

For a proof, see [vdP99], Theorem 5.6. Since any torsor becomes trivial after a finite field extension, Kolchin's theorem is a direct consequence of Theorem 1.14.
We are also going to use the correspondence between torsors and the first cohomology groups (see for example [Ser97], I.5.2, Prop. 33):

Proposition 1.15. *Let $\mathcal{G}$ be a linear algebraic group defined over F. There is a bijection between the set of $\mathcal{G}$-torsors and $H^1(\mathrm{Gal}(\overline{F}/F), \mathcal{G}(\overline{F}))$ ($\overline{F}$ denotes the algebraic closure of F).*

Chapter 2

Connected Differential Galois Groups

Throughout this chapter, F always denotes a differential field with algebraically closed field of constants K.

2.1 The Notion of Effectivity

Given a linear differential equation in matrix form defined by some matrix $A \in F^{n\times n}$ and a fundamental solution matrix Y with coefficients in a Picard-Vessiot extension E of F, we can recover the original matrix A as $A = \partial(Y)Y^{-1}$. This motivates the following definition.

Definition 2.1. *The map*

$$\lambda : \mathrm{GL}_n(F) \to \mathrm{Mat}_n(F), \qquad X \mapsto \partial(X)X^{-1}$$

is called the **logarithmic derivative**.

The following formula (which can easily be checked) is frequently used for calculations.

Lemma 2.2. *For $A, B \in \mathrm{GL}_n(F)$ we have that $\lambda(AB) = \lambda(A) + A\lambda(B)A^{-1}$.*

If we restrict λ to a linear algebraic group $\mathcal{G} \leq \mathrm{GL}_n$, we can say more about its image. First, we need a definition.

Definition 2.3. *The F-algebra*

$$D := F[X]/(X)^2 = F + Fe, \qquad e^2 = 0$$

is called the **algebra of dual numbers over** F.

Note that the map $F \to D$, $a \mapsto a + \partial(a)e$ is a homomorphism of K-algebras. For a linear algebraic group $\mathcal{G} \leq \mathrm{GL}_{n,F}$ over F the Lie algebra of $\mathcal{G}$ may be defined as the F-vector space

$$\mathrm{Lie}_F(\mathcal{G}) := \left\{ A \in F^{n\times n} \middle| \, 1 + eA \in \mathcal{G}(D) \right\}$$

provided with the Lie bracket

$$[\cdot,\cdot] : \mathrm{Lie}_F(\mathcal{G}) \times \mathrm{Lie}_F(\mathcal{G}) \to \mathrm{Lie}_F(\mathcal{G}), \qquad (A,B) \mapsto [A,B] := AB - BA.$$

It can be shown that the definition given above is equivalent to the usual definition of the Lie algebra as the tangent space at the identity element (in particular, it is independent of the embedding $\mathcal{G} \leq \mathrm{GL}_n$).

Proposition 2.4. *Let $\mathcal{G} \leq \mathrm{GL}_{n,K}$ be a linear algebraic group. Then*

$$\lambda|_{\mathcal{G}} : \mathcal{G}(F) \to \mathrm{Lie}_F(\mathcal{G})$$

is a map from $\mathcal{G}(F)$ to its Lie algebra.

A proof can be found in [Kov69], Section 1. The Lie algebra of a linear algebraic group plays an important role in differential Galois theory, as the following proposition (see [vdP99], Corollary 4.3) indicates.

Proposition 2.5. *Let $\mathcal{G} \leq \mathrm{GL}_{n,K}$ be a linear algebraic group over K and let $A \in \mathrm{Lie}_F(\mathcal{G})$. Then the Galois group of the differential equation defined by A injects into $\mathcal{G}(K)$.*

This proposition is crucial to the approach of the inverse problem, because it reduces the problem to finding a sufficiently general element inside the Lie algebra of the group we want to realize. The main ingredient in the proof is the following lemma, which we will need later. It assures that under the hypothesis of Proposition 2.5, the defining ideal I of $\mathcal{G}$ in $F[\mathrm{GL}_n]$ is a differential ideal with respect to the derivation defined by A. In the construction of the Picard-Vessiot ring sketched in Section 1.2, we may therefore choose the maximal differential ideal so that it contains I. The rest of the proof of Proposition 2.5 is straightforward.

Lemma 2.6. *Let $\mathcal{G} \leq \mathrm{GL}_{n,K}$ be a linear algebraic group over K and let $A \in \mathrm{Lie}_F(\mathcal{G})$. Endow $F[\mathrm{GL}_n] = F[X_{ij}, det(X)^{-1}]$ with the structure of a differential ring via $\partial(X) = AX$, $X = (X_{ij})$. Then the extension of the defining ideal of $\mathcal{G}$ to $F[\mathrm{GL}_n]$ is a differential ideal.*

Combining the above lemma with Remark 1.9, we obtain the following.

Corollary 2.7. *Let $\mathcal{G} \leq \mathrm{GL}_{n,K}$ be a connected linear algebraic group over K and let $A \in \mathrm{Lie}_F(\mathcal{G})$. Let E be the Picard-Vessiot extension defined by A. Then there exists a fundamental solution matrix in $\mathcal{G}(E)$.*

Definition 2.8. *Let $\mathcal{G}$ be a connected linear algebraic group defined over K and let $A \in \mathrm{Lie}_F(\mathcal{G})$. The differential equation defined by A is called* **effective** *if the associated differential Galois group is isomorphic to $\mathcal{G}(K)$. In this case, we also call the defining matrix effective.*
A Picard-Vessiot extension E/F is called **effective** *if it can be defined by an effective equation or matrix, respectively.*

Note that because of Proposition 2.5 and the fact that the Lie algebra of a linear algebraic group coincides with the Lie algebra of its connected component, only connected groups can possibly have effective realizations. Proposition 2.5 has a partial converse if the field F has cohomological dimension at most one. This partial converse is a consequence of the Torsor Theorem (Theorem 1.14) and the fact that over a field of cohomological dimension at most one, all principal homogeneous spaces for a connected group are trivial by the theorem of Springer and Steinberg (see [Ser97], III.2.3, Theorem 1'), combined with Proposition 1.15. If R is a Picard-Vessiot ring for a differential equation with $\mathrm{Quot}(R) = E$ and connected differential Galois group isomorphic to $\mathcal{G}(K)$, it follows that the $\mathcal{G}_F$-torsor $\mathcal{X} = \mathrm{Spec}(R)$ has a trivialization $Z \in \mathcal{X}(F)$. A fundamental solution matrix $Y \in \mathcal{X}(E)$ can then be transformed into $Z^{-1}Y \in \mathcal{G}(E)$, which is a fundamental solution matrix for an equivalent differential equation.

Proposition 2.9. *Suppose that $\mathrm{cd}(F) \leq 1$. Then all Picard-Vessiot extensions of F with connected differential Galois group are effective. Moreover, if E/F is a Picard-Vessiot extension with connected differential Galois group isomorphic to $\mathcal{G}(K)$, there exists a fundamental solution matrix $Y \in \mathcal{G}(E)$.*

For details, see [vdP99], Corollary 5.10.

2.2 Embedding Problems

There is a slightly more general question than the inverse problem which is sometimes called the lifting problem: Given a realization of a quotient of a linear algebraic group by a normal subgroup, is there a realization of the full group containing the given Picard-Vessiot extension as a subfield?

Definition 2.10. *Let*

$$1 \to \mathcal{A} \to \tilde{\mathcal{G}} \to \mathcal{G} \to 1$$

be an exact sequence of linear algebraic groups defined over K (in particular, the maps are morphisms) and suppose that E/F is a Picard-Vessiot extension with differential Galois groups isomorphic to $\mathcal{G}(K)$. The corresponding **embedding problem** *asks for the existence of a Picard-Vessiot extension $\tilde{E}/F$ containing E and a*

monomorphism $\gamma : \mathrm{Gal}(\tilde{E}/F) \to \tilde{\mathcal{G}}(K)$ *such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{G}}(K) & \longrightarrow & \mathcal{G}(K) & \longrightarrow & 1 \\ & & & & \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \cong} & & \\ & & & & \mathrm{Gal}(\tilde{E}/F) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(E/F) & & \end{array}$$

commutes. The kernel of the exact sequence is also called the **kernel of the embedding problem**. *A monomorphism* γ *as above is called a* **solution** *of the embedding problem. It is called* **proper** *if it maps* $\mathrm{Gal}(\tilde{E}/F)$ *onto* $\tilde{\mathcal{G}}(K)$. *The embedding problem is* **effective**, *if* E/F *is an effective extension. If in addition the Picard-Vessiot extension* $\tilde{E}/F$ *is effective we say that the solution is* **effective**. *An embedding problem is called a* **Frattini embedding problem** *if* $\mathcal{A}$ *has no other supplement in* $\tilde{\mathcal{G}}$ *than* $\tilde{\mathcal{G}}$ *itself. We say that an embedding problem is* **connected**, *if all groups in the underlying exact sequence are connected. It is called* **split**, *if the underlying exact sequence splits.*

Note that in case $\tilde{\mathcal{G}}$ is finite, the embedding problem is Frattini if and only if the kernel is contained in the Frattini subgroup $\Phi(\tilde{\mathcal{G}})$ of $\mathcal{G}$ (see [Hal76], Section 10.4). Embedding problems will be a very powerful tool for solving the inverse problem. We require the following lemma.

Lemma 2.11. *Let* $\phi : \tilde{\mathcal{G}} \to \mathcal{G}$ *be a morphism of linear algebraic groups defined over* K, *and let* $d\phi : \mathrm{Lie}_F(\tilde{\mathcal{G}}) \to \mathrm{Lie}_F(\mathcal{G})$ *be the corresponding Lie algebra homomorphism. Then for all* $A \in \mathrm{Lie}_F(\tilde{\mathcal{G}})$, *we have that*

$$\phi(1 + eA) = 1 + ed\phi(A),$$

where we use the dual number definition of the Lie algebra as in Section 2.1 and extend ϕ *and* $d\phi$ *to* $\mathcal{G}(D)$ *and* $\mathrm{Lie}_F(\mathcal{G}) \otimes_F D$ *(by abuse of notation, both identity elements are denoted by* 1*).*

Proof. Suppose that $\tilde{\mathcal{G}} \leq \mathrm{GL}_n$ and $\mathcal{G} \leq \mathrm{GL}_m$, respectively. Let $\tilde{X}_{ij}$ and X_{ij} be the (i,j)-th coordinate functions of $F[\mathrm{GL}_n]$ and $F[\mathrm{GL}_m]$, respectively. Let $\phi_{ij} = \phi^*(X_{ij})$. Then

$$X_{ij}(\phi(1 + eA)) = \phi_{ij}(1 + eA) = \phi_{ij}(1) + e \sum_{r,s=1}^{n} \frac{\partial \phi_{ij}}{\partial \tilde{X}_{rs}}(1) A_{rs} = \delta_{ij} + ed\phi(A)_{ij}$$

from which the claim follows (see [Hum98], Section 5.4, for the computation of the differential of a morphism). □

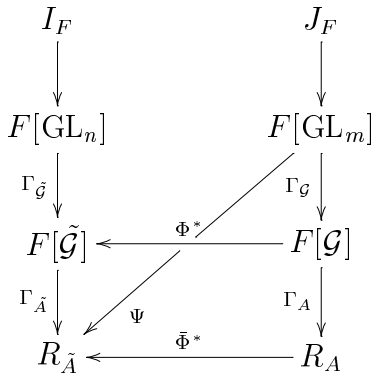
The following proposition makes embedding problems particularly useful when the groups under consideration are connected.

Proposition 2.12. *Suppose that $\Phi : \tilde{\mathcal{G}} \to \mathcal{G}$ is a surjective homomorphism of linear algebraic groups defined over K and let $d\Phi : \mathrm{Lie}_F(\tilde{\mathcal{G}}) \to \mathrm{Lie}_F(\mathcal{G})$ be the corresponding Lie algebra homomorphism. Let $\tilde{A} \in \mathrm{Lie}_F(\tilde{\mathcal{G}})$ and define $A := d\Phi(\tilde{A})$. Then the Picard-Vessiot extension $E_{\tilde{A}}$ of F for the differential equation $X' = \tilde{A}X$ contains the Picard-Vessiot extension E_A of F for the differential equation $X' = AX$ (up to differential isomorphism) and there is a commutative diagram*

$$\begin{array}{ccc} \tilde{\mathcal{G}}(K) & \longrightarrow & \mathcal{G}(K) \\ \uparrow & & \uparrow \\ \mathrm{Gal}(E_{\tilde{A}}/F) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(E_A/F) \end{array}$$

where res *denotes the restriction homomorphism and the vertical arrows are the monomorphisms given by Proposition 2.5.*

Proof. On coordinate rings, we obtain the following diagram (the notation will be explained in the course of the proof):



Here $\Gamma_{\tilde{\mathcal{G}}}$ and $\Gamma_{\mathcal{G}}$ denote the canonical projections, I_F and J_F denote the extensions of the defining ideals of the two linear algebraic groups from K to F, so that $I_F = \mathrm{Ker}(\Gamma_{\tilde{\mathcal{G}}})$, $J_F = \mathrm{Ker}(\Gamma_{\mathcal{G}})$, and $\mathrm{Ker}(\Phi^* \circ \Gamma_{\mathcal{G}}) = J_F$ (note that Φ^* is injective because Φ is surjective ([Spr98], 1.9.1)). As explained in Section 1.2, $F[\mathrm{GL}_n]$ can be given a differential ring structure by defining $\partial_{\tilde{A}}(\tilde{X}) = \tilde{A}\tilde{X}$, where $\tilde{X} = (\tilde{X}_{ij})_{i,j=1}^n$ is the matrix of coordinate functions $\tilde{X}_{i,j}$, and $F[\mathrm{GL}_m]$ becomes a differential ring via a derivation ∂_A induced by A in the same fashion. By Lemma 2.6, I_F and J_F are differential ideals and thus $\Gamma_{\tilde{\mathcal{G}}}$ and $\Gamma_{\mathcal{G}}$ are differential epimorphisms with the induced derivations on $F[\tilde{\mathcal{G}}]$ and $F[\mathcal{G}]$, respectively. Further, Φ^* is a differential homomorphism. To see this, let $\tilde{f}_{ij}$ denote the image of the coordinate functions of $F[\mathrm{GL}_n]$ in $F[\tilde{\mathcal{G}}]$, let f_{ij} be the image of the coordinate functions of $F[\mathrm{GL}_m]$ in $F[\mathcal{G}]$,

and compute that for $g \in \tilde{\mathcal{G}}(K)$

$$\begin{aligned}
\left(\Phi^*(f_{ij}) + e\Phi^*(\partial_A f_{ij})\right)(g) &= \Phi^*(1+eA)(f_{ij})(g) \\
&= \Phi^*(1+ed\Phi(\tilde{A}))(f_{ij})(g) \\
&= (1+ed\Phi(\tilde{A}))(f_{ij})(\Phi(g)) \\
&= f_{ij}((1+ed\Phi(\tilde{A}))\Phi(g)) \\
&= f_{ij}(\Phi((1+e\tilde{A})g)) \quad \text{by Lemma 2.11} \\
&= \Phi^*(f_{ij})((1+e\tilde{A})g) \\
&= (1+e\tilde{A})\Phi^*(f_{ij})(g) = \left(\Phi^*(f_{ij}) + e\partial_{\tilde{A}}\Phi^*(f_{ij})\right)(g)
\end{aligned}$$

where we have extended Φ^* to $F[\mathcal{G}] \otimes_F D$ (D is the algebra of dual numbers over F defined in Section 2.1). Comparing the coefficients of e proves the claim.
As a consequence, $\Phi^* \circ \Gamma_{\mathcal{G}}$ is a differential homomorphism with kernel J_F. Let $P \trianglelefteq F[\mathrm{GL}_n]$ be a maximal differential ideal containing I_F. Then $R_{\tilde{A}} := F[\mathrm{GL}_n]/P$ is a Picard-Vessiot ring for the differential equation defined by $\tilde{A}$ as seen in Section 1.2. The map

$$\Gamma_{\tilde{A}} : F[\tilde{\mathcal{G}}] = F[\mathrm{GL}_n]/I_F \to R_{\tilde{A}} = F[\mathrm{GL}_n]/P$$

is the canonical epimorphism, its kernel $\mathrm{Ker}(\Gamma_{\tilde{A}}) \triangleleft F[\tilde{\mathcal{G}}]$ is a differential ideal, and so $\Gamma_{\tilde{A}}$ is a differential homomorphism with the induced derivation on $R_{\tilde{A}}$. Consequently, the map

$$\Psi = \Gamma_A \circ \Phi^* \circ \Gamma_{\mathcal{G}} : F[\mathrm{GL}_m] \to R_{\tilde{A}}$$

obtained by composition is a differential homomorphism with $J_F \subseteq \mathrm{Ker}(\Psi) = Q$, which is a differential ideal. This allows us to define $R_A := F[\mathrm{GL}_m]/Q$ so that Ψ factors through R_A and the map $\bar{\Phi}^* : R_A \hookrightarrow R_{\tilde{A}}$ is a differential monomorphism with the inherited derivation on R_A.
Next, we want to show that R_A is in fact a Picard-Vessiot ring for A. Since R_A includes into the integral domain $R_{\tilde{A}}$, it cannot contain any zero divisors. The differentiation on $F[\mathrm{GL}_m]$ was defined in such a way that the matrix $X = (X_{ij})_{i,j=1}^n$ of the coordinate functions X_{ij} is a fundamental solution matrix, and $F[\mathrm{GL}_m]$ is generated by its entries and the inverse of the determinant. Since Q is a differential ideal, these properties are inherited by R_A. By the remark following Definition 1.7, it remains to check that $E_A = \mathrm{Quot}(R_A)$ does not contain any new constants. This last condition is satisfied since the map $\bar{\Phi}^*$ induces a unique differential monomorphism $\bar{\Phi}^* : E_A \hookrightarrow E_{\tilde{A}} := \mathrm{Quot}(R_{\tilde{A}})$.
We have already defined the required inclusion $E_A \hookrightarrow E_{\tilde{A}}$. By construction, we have an inclusion $\mathrm{Gal}(E_{\tilde{A}}/F) \hookrightarrow \tilde{\mathcal{G}}(K)$ (the maximal ideal contains the defining ideal of the group). The same is true for $\mathrm{Gal}(E_A/F) \hookrightarrow \mathcal{G}(K)$. Finally, we check that the diagram commutes. Again by construction, the fundamental solution matrix $Y_{\tilde{A}} \in \mathrm{Spec}(R_{\tilde{A}}) \subseteq \tilde{\mathcal{G}}(E_{\tilde{A}})$ (which is the image of $\tilde{X}$ modulo P) maps to a matrix Y_A under Φ which is a fundamental solution matrix for E_A/F. Suppose that $\tilde{\sigma}(Y_{\tilde{A}}) =$

$Y_{\tilde{A}}C_{\tilde{\sigma}}$ and $\sigma(Y_A) = Y_A C_\sigma$ for all $\tilde{\sigma} \in \mathrm{Gal}(E_{\tilde{A}}/F)$ and $\sigma \in \mathrm{Gal}(E_A/F)$, respectively ($C_{\tilde{\sigma}} \in \tilde{\mathcal{G}}(K)$, $C_\sigma \in \mathcal{G}(K)$). Then

$$\begin{aligned} Y_A\Phi(C_{\tilde{\sigma}}) &= \Phi(Y_{\tilde{A}}C_{\tilde{\sigma}}) = \Phi(\tilde{\sigma}(Y_{\tilde{A}})) = \tilde{\sigma}(\Phi(Y_{\tilde{A}})) \\ &= \mathrm{res}(\tilde{\sigma})(\Phi(Y_{\tilde{A}})) = \mathrm{res}(\tilde{\sigma})(Y_A) = Y_A C_{\mathrm{res}(\tilde{\sigma})} \end{aligned}$$

for all $\tilde{\sigma} \in \mathrm{Gal}(E_{\tilde{A}}/F)$, from which the claim follows. □

2.3 The Connected Inverse Problem

In this section, we give a sketch of proof of the connected inverse problem over $F = K(t)$ using the technique of embedding problems. The main difference to the solution of the general inverse problem given in Section 4.4 is that the following proposition (see [MS96], Proposition 3.5) provides us with constructive realizations of connected semisimple groups.

Proposition 2.13. *Let $\mathcal{S}$ be a semisimple group. There exist matrices A_0 and A_1 in the Lie algebra $\mathrm{Lie}_K(\mathcal{S})$ such that the matrix $A = A_0 + A_1 t$ realizes $\mathcal{S}(K)$ over F.*

In fact, one chooses A_0 and A_1 to be what is called a *regular pair of generators of the Lie algebra* $\mathrm{Lie}_K(\mathcal{S})$ ([MS96], remarks following Lemma 3.4). In particular, the matrix A is explicitly given.
The step from connected semisimple groups to connected reductive groups is based on the fact that any connected reductive group is the quotient of a direct product of a torus and a semisimple group by a finite group.
The problem is thereby reduced to an embedding problem with unipotent kernel and reductive cokernel. This embedding problem may be decomposed into a split effective embedding problem with unipotent abelian kernel and an effective Frattini embedding problem. The former can be split up further into split embedding problems with so-called minimal unipotent abelian kernel. Such embedding problems have proper effective solutions as shown in [Obe01], Proposition 2.1. Effective Frattini embedding problems always have proper effective solutions (see, for example, [MvdP02], Prop. 4.13), and these results may be combined to yield a solution of the connected inverse problem.

Chapter 3

Non Connected Differential Galois Groups

We have already seen how to realize connected groups as differential Galois groups. One of the most important tools was the Lie algebra and the concept of effectivity. In the non connected case, the Lie algebra does not encode enough information about the group. However, when we are in the lucky situation that the connected component of the group under consideration has a finite complement, i.e., the group is a semidirect product of its connected component by a finite group, we can still recover all the information we need. We will restrict ourselves to this case from Section 3.2 on except for the very last section, where we turn back to the general case.

3.1 Algebraic Groups over non Algebraically Closed Fields

Most of the textbooks that provide material on algebraic groups assume the field of definition to be algebraically closed. The reason is that a linear algebraic group, defined over a non algebraically closed field, might not have enough rational points over that field to completely determine its structure. For example, the elements of a torus need not be diagonalizable over the field of definition of the torus. We find that a good reference for the general case are the additional chapters in the second edition of Springer [Spr98].
An affine variety over a (not necessarily algebraically closed) field F is an algebraic set over the algebraic closure $\overline{F}$ of F (together with its ring of regular functions) whose defining equations have coefficients in F. We will call such a variety an F-variety for short.

Definition 3.1. *Let F be a field and $L \geq F$ be a field extension. A morphism of affine F-varieties which is defined over L is called an* **L-morphism**.

*Let $\mathcal{X}$ be an affine variety defined over the field F. An affine F-variety is called an L/F-***form** *of $\mathcal{X}$ if it is L-isomorphic to $\mathcal{X}$.*

We will only consider the case when L/F is a finite Galois extension. It can be shown that F-isomorphism classes of L/F-forms of an affine F-variety $\mathcal{X}$ are parametrized by the elements of $H^1(\mathrm{Gal}(L/F), \mathrm{Aut}_L(\mathcal{X}))$ (see [Spr98], 11.3.3.).

Definition 3.2. *Let $L \geq F$ be a finite Galois extension and let V be an L-vector space. An action $* : \mathrm{Gal}(L/F) \times V \to V$ is called* **semilinear***, if*

$$\sigma * (\alpha \cdot v) = \sigma(\alpha) \cdot (\sigma * v)$$

for all $\sigma \in \mathrm{Gal}(L/F)$, $\alpha \in L$ and $v \in V$.

Lemma 3.3 (Speiser's Lemma). *Let L/F be a finite Galois extension and let V be an L-vector space on which $\mathrm{Gal}(L/F)$ acts semilinearly. Then $V^{\mathrm{Gal}(L/F)} \otimes_F L = V$. In particular, V has a basis of invariant vectors.*

Proof. Let $v \in V$ be an arbitrary vector. Number the elements of $\mathrm{Gal}(L/F)$ by $1 = \sigma_1, \ldots, \sigma_s$ ($s = [L : F]$) and let $a_1, \ldots, a_s$ be a basis of L over F. Define

$$v_i := \sum_{j=1}^{s} \sigma_j(a_i)\sigma_j(v) = \sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(a_i v),$$

and note that all these vectors are invariant. The automorphisms $\sigma_1, \ldots, \sigma_s$ are linearly independent over F, which implies that the matrix $A = (\sigma_j(a_i))_{i,j=1}^{s}$ is invertible. Let $B = (b_{ij})$ denote its inverse, then

$$\sum_{i=1}^{s} b_{1i} v_i = \sum_{i=1}^{s} \sum_{j=1}^{s} b_{1i}\sigma_j(a_i)\sigma_j(v) = v,$$

which writes v as an L-linear combination of vectors in $V^{\mathrm{Gal}(L/F)}$. □

Definition 3.4. *As before, let L/F be a finite Galois extension. An F-vector space V_0 inside an L-vector space V is called an F-***structure** *on V if the canonical map $V_0 \otimes_F L \to V$ is an isomorphism.*
If A is an L-algebra, and the underlying vector space carries an F-structure which is an F-subalgebra of A, we say that this is an F-structure on A.

As a consequence of Speiser's Lemma 3.3, any semilinear $\mathrm{Gal}(L/F)$-action on an L-vector space defines an F-structure. If a semilinear action on an L-algebra A is by automorphisms of the ring A, it defines an F-structure on A.
Let us close this section by clarifying the connection between F-structures and forms (notation as above): If $\mathcal{X}$ is an affine F-variety, and $L[\mathcal{X}]_0$ is an F-structure on the coordinate ring $L[\mathcal{X}] := L \otimes_F F[\mathcal{X}]$ of $\mathcal{X}$, then by definition $(\mathcal{X}_0)_L \cong \mathcal{X}_L$, where $\mathcal{X}_0$ is the F-variety defined by $L[\mathcal{X}]_0$. That is, $\mathcal{X}_0$ is an L/F-form of $\mathcal{X}$.

3.2 The Equivariance Condition

Assume that we have a Picard-Vessiot extension E/F with non connected differential Galois group isomorphic to $\mathcal{G}(K)$, where $\mathcal{G}$ is a linear algebraic group defined over the field of constants K. Assume further that $\mathcal{G}$ has a decomposition into a semidirect product $\mathcal{G} = \mathcal{G}^0 \rtimes H$ where $\mathcal{G}^0$ is the connected component of $\mathcal{G}$ and H is a finite group. By the Galois correspondence 1.12, the fixed field $L := E^{\mathcal{G}^0(K)}$ is a finite Galois extension of F with Galois group $\mathrm{Gal}(L/F) \cong H$. Consequently, we have two different actions of the finite group H on the Lie algebra $\mathrm{Lie}_L(\mathcal{G}) = \mathrm{Lie}_K(\mathcal{G}) \otimes_K L$: one via conjugation (the adjoint action) and one via the coefficient-wise Galois action. The next proposition shows that in our situation, the two actions must be compatible on the defining matrix of the Picard-Vessiot extension E/L. We pause for a definition.

Definition 3.5. *Let L/F be a finite Galois extension with Galois group isomorphic to H and assume that there is a monomorphism $\chi : \mathrm{Gal}(L/F) \hookrightarrow \mathrm{GL}_n(K)$, $\sigma \mapsto C_\sigma$. A matrix $A \in L^{n\times n}$ is called H-equivariant, if $\sigma(A) = C_\sigma^{-1} A C_\sigma$ for all $\sigma \in \mathrm{Gal}(L/F)$, where the action on the left hand side is the (coefficient-wise) Galois action.*

If the group H is clear from context, we will also just call the matrix equivariant. The condition above will be referred to as the equivariance condition.

Remark 3.6. With notation as above, let $\chi : \mathrm{Gal}(L/F) \to \mathcal{G}(K)$ be the composite $\mathrm{Gal}(L/F) \cong H \xrightarrow{\tau} \mathcal{G}(K)$, where τ is a regular homomorphic section. We define a new action of H on $\mathcal{G}^0(L)$ via

$$\sigma * g = C_\sigma \sigma(g) C_\sigma^{-1}, \qquad g \in \mathcal{G}^0(L),\ \sigma \in \mathrm{Gal}(L/F).$$

The equivariance condition may then be reformulated as an invariance condition:

$$g = \sigma * g \qquad \text{for all } \sigma \in \mathrm{Gal}(L/F) \quad (g \in \mathcal{G}^0(L)).$$

The homomorphism χ defines an element χ in $H^1(\mathrm{Gal}(L/F), \mathcal{G}(L))$. There is a canonical map from $\mathcal{G}$ to its automorphism group sending an element to the inner automorphism it defines. The induced map on cohomology maps χ to an element $\mathrm{Int}(\chi) \in H^1(\mathrm{Gal}(L/F), \mathrm{Aut}_L(\mathcal{G}))$. Any automorphism of $\mathcal{G}$ stabilizes the connected component, i.e., we obtain an element in $H^1(\mathrm{Gal}(L/F), \mathrm{Aut}_L(\mathcal{G}^0))$, which is again denoted by χ.
We may also define a twisted action as above on the coordinate ring $L[\mathcal{G}^0]$ by

$$(\sigma * f)(g) = \sigma(f)(C_\sigma^{-1} g C_\sigma), \quad f \in L[\mathcal{G}^0], g \in \mathcal{G}^0(L)$$

where $\sigma(f)$ denotes the Galois action on the coefficients of f. Note that this $*$-action is semilinear in the sense of Definition 3.2, and thus defines an L/F-form $\mathcal{G}^0_\chi$ of $\mathcal{G}^0$, on which the $*$-action is the Galois action (see also [Spr98], 12.3.7.)

All of this translates to the Lie algebra: The respective action on the Lie algebra (defined in the very same way as on the group) is also semilinear and therefore defines an F-structure $\mathrm{Lie}_L(\mathcal{G})_\chi$ on $\mathrm{Lie}_L(\mathcal{G})$. In fact, we have $\mathrm{Lie}_L(\mathcal{G})_\chi = \mathrm{Lie}_L(\mathcal{G}_\chi)$. To see this, use the dual number definition of the Lie algebra given in Section 2.1: For a matrix A, we have that $1 + eA$ is in $\mathcal{G}(L[e])$ and equivariant for some e with $e^2 = 0$ if and only if $1 + eA$ is in $\mathcal{G}(L[e])$ and A is equivariant.
Therefore, equivariant elements in $\mathrm{Lie}_L(\mathcal{G})$ are the same as $*$-invariant elements in $\mathrm{Lie}_L(\mathcal{G})$ which in turn are just F-rational points of $\mathrm{Lie}_L(\mathcal{G}_\chi)$.

Let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be the semidirect product of a connected group by a finite group, both defined over K. In the sequel, we will assume that we have fixed a regular homomorphic section $\tau : H \to \mathcal{G}$. If we are further given a finite Galois extension of F with Galois group isomorphic to H, equivariance is to be understood as equivariance with respect to the representation of H defined by τ.
The following statement (in slightly different form) can also be found in [MS00].

Proposition 3.7. *Let $\mathcal{G} = \mathcal{G}^0 \rtimes H \leq \mathrm{GL}_{n,K}$ be a linear algebraic group defined over K, and assume that $\mathrm{cd}(F) \leq 1$. Suppose that E/F is a Picard-Vessiot extension with Galois group isomorphic to $\mathcal{G}(K)$. Then $E^{\mathcal{G}^0(K)} =: L$ is a finite Galois extension of F with Galois group isomorphic to H. Further, E/L is a Picard-Vessiot extension of a differential equation given by a matrix $A \in \mathrm{Lie}_L(\mathcal{G}^0)$ which is equivariant.*

Proof. Since $\mathcal{G}^0(K)$ is normal in $\mathcal{G}(K)$, L is a Picard-Vessiot extension of F and E is a Picard-Vessiot extension of L by the Galois correspondence 1.12. Also by the Galois correspondence, L/F is a finite Galois extension with Galois group isomorphic to $(\mathcal{G}/\mathcal{G}^0)(K) \cong H$. This proves the first claim.
Let $\tau : H \to \mathcal{G}$ be a regular homomorphic section. Let $\tilde{Y}$ be a fundamental solution matrix for the equation given over F on which the Galois group acts via $\eta(\tilde{Y}) = \tilde{Y}C_\eta$, $\eta \in \mathrm{Gal}(E/F)$, $C_\eta \in \mathcal{G}(K)$. The isomorphism $\chi : \mathrm{Gal}(L/F) \to \tau(H)$, $\sigma \mapsto C_\sigma$ defines a cocycle $\chi \in H^1(\mathrm{Gal}(L/F), \mathrm{GL}_n(K))$. By Hilbert's Theorem 90 ([Ser97], III.1.1, Lemma 1), this cocycle is trivial, i.e., there exists an element $Z \in \mathrm{GL}_n(L)$ with the property $\sigma(Z) = ZC_\sigma$ for all $\sigma \in \mathrm{Gal}(L/F)$. As a consequence, the logarithmic derivative of Z has coefficients in F. This shows that $F(Z)$ is a Picard-Vessiot extension of F, and it is clearly contained in L. No element of $\mathrm{Gal}(L/F)$ fixes Z, from which we conclude that $L = F(Z)$.
We claim that $Y := Z^{-1}\tilde{Y}$ is a fundamental solution matrix for E/L. Clearly, we have that $E = L(Y)$. For $\eta \in \mathrm{Gal}(E/L)$, the restriction of the representation above to $\mathrm{Gal}(E/L)$ shows that $\eta(Y) = YC_\eta$, $C_\eta \in \mathcal{G}^0(K)$. Consequently, the logarithmic derivative of Y has coefficients in L and defines a differential equation with Picard-Vessiot extension E/L. Note that Y satisfies the equivariance condition (although Y does not have coefficients in L, this statement makes sense since we may consider $\mathrm{Gal}(L/F)$ as a subgroup of $\mathrm{Gal}(E/F)$):

$$\sigma(Y) = \sigma(Z^{-1})\sigma(\tilde{Y}) = C_\sigma^{-1}Z^{-1}\tilde{Y}C_\sigma = C_\sigma^{-1}YC_\sigma, \qquad \sigma \in \mathrm{Gal}(L/F).$$

Let R be a Picard-Vessiot ring for the extension E/L. The ring R may be obtained from $L[\mathrm{GL}_n]$ as the quotient by the maximal differential ideal $P = \{f \in L[\mathrm{GL}_n] | f(Y) = 0\}$ (this follows from the construction explained in Section 1.2, see also Remark 1.9). We can define a twisted action on $L[\mathrm{GL}_n]$ via

$$(\sigma * f)(g) = \sigma(f)(C_\sigma^{-1} g C_\sigma), \qquad f \in L[\mathrm{GL}_n],\ g \in \mathrm{GL}_n(L),$$

and this induces an F-structure on R since $\sigma * P \subseteq P$ for all $\sigma \in \mathrm{Gal}(L/F)$. Namely, for $\sigma \in \mathrm{Gal}(L/F)$ and $f \in P$ we have that

$$(\sigma * f)(Y) = \sigma(f)(C_\sigma^{-1} Y C_\sigma) = \sigma(f)(\sigma(Y)) = \sigma(f(Y)) = \sigma(0) = 0$$

since Y is equivariant.
By Theorem 1.14, $\mathcal{X} := \mathrm{Spec}(R)$ is a $\mathcal{G}_L^0$-torsor. The F-structure on R defines a form $\mathcal{X}_\chi$ of $\mathcal{X}$ and we also have a form $\mathcal{G}_\chi^0$ as explained in Remark 3.6 above. Moreover, $\mathcal{X}_\chi$ is a $\mathcal{G}_\chi^0$-torsor. To see this, we need to define a morphism

$$\Gamma : \mathcal{X}_\chi \times \mathcal{G}_\chi^0 \to \mathcal{X}_\chi, \quad (x, g) \mapsto x \cdot g,$$

which gives $\mathcal{X}_\chi$ the structure of a $\mathcal{G}_\chi^0$-variety. To define Γ, we use the restriction of the $\mathcal{G}_L^0$-variety structure.
For elements $x, x' \in \mathcal{X}(\overline{F})$, there exists an element $g \in \mathcal{G}^0(\overline{F})$ such that $x \cdot g = x'$. Suppose that both x and x' are invariant under the $*$-action. Then $x \cdot g = x' = \sigma * x' = (\sigma * x) \cdot (\sigma * g) = x \cdot (\sigma * g)$ and thus $g = \sigma * g$ for all $\sigma \in \mathrm{Gal}(L/F)$ because $\mathcal{X}$ is a $\mathcal{G}_L^0$-torsor. This shows that $\mathcal{X}_\chi$ is in fact a $\mathcal{G}_\chi^0$-torsor.
Since $\mathcal{G}_\chi^0$ is connected and $\mathrm{cd}(L) \leq 1$, there exists an F-rational point $B \in \mathcal{X}_\chi(F)$ by the theorem of Springer and Steinberg ([Ser97], III.2.3., Theorem 1') in combination with Propositon 1.15; and $\mathcal{X}_\chi(F) = B\mathcal{G}_\chi^0(F)$. The matrix Y satisfies the equivariance condition and is by the above equivariantly equivalent to an equivariant matrix in $\mathcal{G}^0(E)$: We can replace Z by ZB and Y by $B^{-1}Y$, and the action of the Galois groups $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(E/F)$, respectively, remain unchanged. In particular, ZB and $B^{-1}Y$ have the same properties stated above for Z and Y. The logarithmic derivative A of $B^{-1}Y$ is then an equivariant matrix in $\mathrm{Lie}(\mathcal{G}^0(L))$ as claimed:

$$C_\sigma \sigma(A) C_\sigma^{-1} = C_\sigma \sigma(\lambda(B^{-1}Y)) C_\sigma^{-1} = C_\sigma \sigma(\lambda(B^{-1})) C_\sigma^{-1} + C_\sigma \sigma(B^{-1}\lambda(Y)B) C_\sigma^{-1} = A$$

for all $\sigma \in \mathrm{Gal}(L/F)$. □

Remark 3.8. The corresponding (weaker) statement for general non connected groups can be found in Section 3.5.

3.3 Embedding Problems with Finite Cokernel

Let us begin this section by stating one of the consequences of the equivariance condition.

Lemma 3.9. *Let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be a linear algebraic group defined over K with a regular homomorphic section $\tau : H \to \mathcal{G}$. Suppose that L/F is a Galois extension with Galois group isomorphic to $\tau(H)$ via $\sigma \mapsto C_\sigma$. Let $A \in \mathrm{Lie}_L(\mathcal{G})$ be an equivariant matrix defining a Picard-Vessiot extension E of L with fundamental solution matrix $Y \in \mathcal{G}^0(E)$ (see Corollary 2.7).*

1. *There exists a matrix $Z \in \mathrm{GL}_n(L)$ such that $L = F(Z)$ and $\sigma(Z) = ZC_\sigma$ for all $\sigma \in \mathrm{Gal}(L/F)$.*
2. *The differential equation defined by A descends to a differential equation given by $\tilde{A} = \lambda(Z) + ZAZ^{-1} \in F^{n\times n}$ over F, and $\tilde{Y} := ZY$ is a fundamental solution matrix for this equation.*
3. *We have $E = F(\tilde{Y})$, i.e., the Picard-Vessiot extension of F defined by $\tilde{A}$ is E. In particular, $\tilde{A}$ defines a Picard-Vessiot extension of F which contains L.*

Proof. The first part is shown as in Proposition 3.7.
The second claim follows from straightforward calculation:

$$\sigma(\tilde{A}) = Z'C_\sigma C_\sigma^{-1}Z^{-1} + ZC_\sigma\sigma(A)C_\sigma^{-1}Z^{-1} = \tilde{A} \quad \text{for all } \sigma \in \mathrm{Gal}(L/F),$$

i.e., $\tilde{A}$ has coefficients in F. Moreover,

$$\tilde{Y}' = (ZY)' = Z'Y + ZY' = Z'Y + ZAY = (Z'Z^{-1} + ZAZ^{-1})ZY = \tilde{A}\tilde{Y},$$

i.e., the matrix $\tilde{Y} = ZY \in \mathrm{GL}_n(E)$ is a fundamental solution matrix for the differential equation given by $\tilde{A}$.
Next, we want to show that E is in fact a Picard-Vessiot extension of F. To this end, consider the block diagonal matrix

$$\begin{pmatrix} \tilde{A} & 0 \\ 0 & \lambda(Z) \end{pmatrix} \in F^{2n\times 2n}.$$

Let $\tilde{E}/F$ be the Picard-Vessiot extension defined by this matrix. Over L, the matrix is equivalent to A (or rather to the block diagonal matrix $A \oplus 0$), from which we conclude that $\tilde{E}L = E$. Since $\tilde{E}$ contains L by construction, this implies $\tilde{E} = E$.
Clearly, we have that $F(\tilde{Y})$ is a Picard-Vessiot extension and it is contained in E. To prove the last part, it is therefore sufficient to show that no (nontrivial) element of the Galois group $\mathrm{Gal}(E/F)$ fixes $\tilde{Y}$. First, no nontrivial element of $\mathrm{Gal}(E/L)$ fixes $\tilde{Y}$, since for $1 \neq \varepsilon \in \mathrm{Gal}(E/L)$, we have that $\varepsilon(\tilde{Y}) = \varepsilon(ZY) = Z\varepsilon(Y) = ZYC_\varepsilon = \tilde{Y}C_\varepsilon$ for some matrix $C_\varepsilon \in \mathcal{G}^0(K)$ with $C_\varepsilon \neq 1$. Suppose that $\varepsilon \in \mathrm{Gal}(E/F) \setminus \mathrm{Gal}(E/L)$ fixes $\tilde{Y}$. Then the restriction $\mathrm{res}(\varepsilon)$ of ε to L is nontrivial, and we have that $\varepsilon(\tilde{Y}) = \mathrm{res}(\varepsilon)(Z)\varepsilon(Y) = ZC_{\mathrm{res}(\varepsilon)}\varepsilon(Y)$. We conclude that $C_{\mathrm{res}(\varepsilon)} = Y\varepsilon(Y)^{-1}$. Since $Y \in \mathcal{G}^0(E)$ and $\mathcal{G}^0$ is defined over K, we have that $\varepsilon(Y) \in \mathcal{G}^0(E)$, and thus $C_{\mathrm{res}(\varepsilon)} \in \mathcal{G}^0(K)$. But we also have $C_{\mathrm{res}(\varepsilon)} \in \tau(H)$, from which we conclude that $C_{\mathrm{res}(\varepsilon)} = 1$ and thus $\mathrm{res}(\varepsilon)$ is trivial, a contradiction. □

The following proposition will be the main ingredient for solving the inverse problem. It may be obtained as a corollary of Proposition 3.12, but to make clear how the action of the finite part on the connected part is obtained in this special situation we give an independent proof (which we believe is more conceptual). This proposition may also be seen as a partial converse to Proposition 3.7 (see also [MS00], Prop. 4.3)

Proposition 3.10. *Let $\mathcal{G} = \mathcal{G}^0 \rtimes H \leq \mathrm{GL}_{n,K}$ be a linear algebraic group defined over K with a regular homomorphic section $\tau : H \to \mathcal{G}$. Suppose that L/F is a finite Galois extension with an isomorphism $\alpha : \mathrm{Gal}(L/F) \cong H$. Let $\chi := \tau \circ \alpha : \mathrm{Gal}(L/F) \to \mathcal{G}(K)$, $\sigma \mapsto C_\sigma$, be the composite. Consider the associated embedding problem*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{G}^0(K) & \longrightarrow & \mathcal{G}(K) & \underset{\tau}{\overset{\beta}{\rightleftarrows}} & H & \longrightarrow & 1 \\ & & & & & & \alpha \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(L/F) & & \end{array}$$

Let $Z \in \mathrm{GL}_n(L)$ be a fundamental solution matrix for L/F such that $\sigma(Z) = ZC_\sigma$ for all $\sigma \in \mathrm{Gal}(L/F)$ (see Lemma 3.9).

1. *Let E/L be a Picard-Vessiot extension with Galois group isomorphic to $\mathcal{G}^0(K)$ via an isomorphism*

$$\gamma : \mathrm{Gal}(E/L) \xrightarrow{\cong} \mathcal{G}^0(K) \trianglelefteq \mathcal{G}(K), \qquad \varepsilon \mapsto C_\varepsilon.$$

   Then there exists an element $Y \in \mathcal{G}^0(E)$ satisfying $\varepsilon(Y) = YC_\varepsilon$ for all $\varepsilon \in \mathrm{Gal}(E/L)$ and $E = L(Y)$, i.e., Y is a fundamental solution matrix for the extension E/L on which the Galois group $\mathrm{Gal}(E/F)$ acts via γ.

2. *Suppose in addition that the logarithmic derivative A of Y is equivariant. Then E/F is a Picard-Vessiot extension with Galois group isomorphic to $\mathcal{G}(K)$ and $\tilde{Y} := ZY$ is a fundamental solution matrix for this extension. The isomorphism γ of part 1 may be extended to an isomorphism*

$$\tilde{\gamma} : \mathrm{Gal}(E/F) \to \mathcal{G}(K) \quad \textit{with} \quad \alpha \circ \mathrm{res} = \beta \circ \tilde{\gamma},$$

   *i.e., $\tilde{\gamma}$ is a proper solution of the above embedding problem (*res *denotes the restriction homomorphism $\mathrm{Gal}(E/F) \xrightarrow{\mathrm{res}} \mathrm{Gal}(L/F)$).*

Proof. For Part 1, we have to show that the representation can be adjusted. Let $\hat{Y} \in \mathrm{GL}_m(E)$ be a fundamental solution matrix for the differential equation defining the extension E/L, and suppose that the differential Galois group acts on $\hat{Y}$ via a representation $\rho : \mathcal{G}^0 \to \mathrm{GL}_m$ such that $\varepsilon(\hat{Y}) = \hat{Y}\rho(\gamma(\varepsilon)) = \hat{Y}\rho(C_\varepsilon)$ for all $\varepsilon \in \mathrm{Gal}(E/L)$. Since $\mathrm{cd}(L) = \mathrm{cd}(F) \leq 1$ and $\rho(\mathcal{G}^0)$ is connected, Proposition 2.9 implies that we may assume without loss of generality that $\hat{Y} \in \rho(\mathcal{G}^0(E))$. Setting $Y = \rho^{-1}(\hat{Y}) \in \mathcal{G}^0(E)$, we have $\varepsilon(Y) = YC_\varepsilon$ as desired.

By Lemma 3.9, $\tilde{A} := Z'Z^{-1} + ZAZ^{-1}$ has coefficients in F, the matrix $\tilde{Y} = ZY \in \mathrm{GL}_n(E)$ is a fundamental solution matrix for the differential equation given by $\tilde{A}$, and $E = F(\tilde{Y})$.
Any element $\sigma \in \mathrm{Gal}(L/F)$ defines an automorphism of $\mathcal{G}^0$ by conjugation with C_σ and hence an automorphism of $K[\mathcal{G}^0]$ in the standard way. This extends to an automorphism $\tilde{\sigma}$ of $L[\mathcal{G}^0] = L \otimes_K K[\mathcal{G}^0]$ via

$$\begin{aligned} \tilde{\sigma}(f_{ij})(D) &= f_{ij}(C_\sigma^{-1} D C_\sigma), & D &\in \mathcal{G}^0(K), \\ \tilde{\sigma}(f) &= \sigma(f), & f &\in L, \end{aligned}$$

where $f_{ij} \in K[\mathcal{G}^0]$ denotes the (i,j) coordinate function (compare Remark 3.6). Since $\mathcal{G}^0$ is connected, L is algebraically closed in E by the Galois correspondence 1.12 and $E = \mathrm{Quot}(L[\mathcal{G}^0])$ by Kolchin's Theorem (see Section 1.4). Consequently, $\tilde{\sigma}$ uniquely extends to E.
By definition, $\tilde{\sigma}|_L = \sigma$, and in particular, F remains fixed under $\tilde{\sigma}$. Further, $\tilde{\sigma}$ commutes with the derivation: Any element σ of $\mathrm{Gal}(L/F)$ is a differential automorphism and the same is true for conjugation with constant matrices. Consequently, $\tilde{\sigma} \in \mathrm{Gal}(E/F)$ is a differential automorphism and it is easy to see that we have in fact defined a monomorphism

$$\varphi : \mathrm{Gal}(L/F) \hookrightarrow \mathrm{Gal}(E/F), \qquad \sigma \mapsto \tilde{\sigma}$$

which is a section to the restriction homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(L/F)$. This implies that $\mathrm{Gal}(E/F) = \mathrm{Gal}(E/L) \rtimes \mathrm{Gal}(L/F)$. On the fundamental solution matrix, the action is then

$$\tilde{\sigma}(\tilde{Y}) = \sigma(Z)\tilde{\sigma}(Y) = ZC_\sigma C_\sigma^{-1} Y C_\sigma = \tilde{Y} C_\sigma$$

for $\sigma \in \mathrm{Gal}(L/F)$ since $Y \in \mathcal{G}^0(E)$.
Next, we check that the Galois group $\mathrm{Gal}(E/F)$ is in fact the correct semidirect product $\mathcal{G}^0(K) \rtimes H$. To this end, we consider the action on $\tilde{Y}$:

$$(\varepsilon_1, \tilde{\sigma}_1)(\tilde{Y}) = \sigma_1(Z)\varepsilon_1\tilde{\sigma}_1(Y) = ZC_{\sigma_1}\varepsilon_1(C_{\sigma_1}^{-1} Y C_{\sigma_1}) = ZYC_{\varepsilon_1}C_{\sigma_1} = \tilde{Y}C_{\varepsilon_1}C_{\sigma_1},$$

and similarly

$$(\varepsilon_2, \tilde{\sigma}_2)(\varepsilon_1, \tilde{\sigma}_1)(\tilde{Y}) = \tilde{Y} C_{\varepsilon_2} C_{\varepsilon_1}^{C_{\sigma_2}^{-1}} C_{\sigma_2} C_{\sigma_1},$$

for $\varepsilon_1, \varepsilon_2 \in \mathrm{Gal}(E/L)$, $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/F)$, which proves the claim (the superscript denotes conjugation).
Defining $\tilde{\gamma} : \mathrm{Gal}(E/F) = \mathrm{Gal}(E/L) \rtimes \mathrm{Gal}(L/F) \xrightarrow{\cong} \mathcal{G}(K)$, $(\varepsilon, \tilde{\sigma}) \mapsto C_\varepsilon C_\sigma$, we find

$$\beta \circ \tilde{\gamma}(\varepsilon, \tilde{\sigma}) = \beta(C_\sigma) = \beta(\chi(\sigma)) = \beta(\tau(\alpha(\sigma))) = \alpha(\sigma) = \alpha \circ \mathrm{res}(\varepsilon, \tilde{\sigma}),$$

which shows that $\tilde{\gamma}$ is a proper solution of the embedding problem. □

3.4 Equivariant Embedding Problems

In Section 2.2, we encountered embedding problems for connected groups. Using the equivariance condition defined in Section 3.2, we can generalize this machinery to the type of groups under consideration (semidirect products of connected groups by finite groups).
To be able to translate the results from the connected case, one has to ensure that the equivariance condition is preserved when solving an embedding problem. We start by setting up the stage. Let H be a finite group defined over K.

Definition 3.11. *Let L/F be a finite Galois extension with Galois group isomorphic to H. Let*

$$1 \to \mathcal{A}(K) \to \tilde{\mathcal{B}}(K) \to \mathcal{B}(K) \to 1$$

be an exact sequence of connected linear algebraic groups defined over K and suppose that each of the groups carries an action of (a group isomorphic to) H by conjugation. Assume moreover that all homomorphisms in this sequence are defined over K and are equivariant with respect to these actions (this will ensure that they are equivariant under the corresponding twisted actions as well). Suppose further that N/L is a Picard-Vessiot extension with Galois group isomorphic to $\mathcal{B}(K)$, and that this Picard-Vessiot extension is defined by some equivariant matrix in $\mathrm{Lie}_L(\mathcal{B})$. An embedding problem of this kind is called an **equivariant embedding problem**. *It is called a* **split equivariant embedding problem**, *if the underlying exact sequence splits and the section is H-equivariant. An effective solution of such an embedding problem which is given by an equivariant matrix will be called an* **equivariant solution**. *The kernel of a split equivariant embedding problem is called* **minimal**, *if it has no proper subgroup which is both $\tilde{\mathcal{B}}$-stable and H-stable.*

The above definition allows us to formulate a generalization of Proposition 2.12 to non connected groups.

Proposition 3.12. *Let L/F be a finite Galois extension with Galois group isomorphic to H. Let*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) & \xrightarrow{\pi} & \mathcal{B}(K) & \longrightarrow & 1 \\ & & & & & & \phi \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(N/L) & & \end{array}$$

be a connected H-equivariant embedding problem. Assume that this embedding problem has an effective equivariant solution defined by an equivariant matrix $A_{\tilde{\mathcal{B}}} \in \mathrm{Lie}_L(\tilde{\mathcal{B}})$ with Picard-Vessiot extension $\tilde{N} \geq N$. Suppose further that $d\pi(A_{\tilde{\mathcal{B}}}) = A_{\mathcal{B}} \in \mathrm{Lie}_L(\mathcal{B})$ is the matrix which realizes N/L.

Then $\tilde{N}$ is a Picard-Vessiot extension of F and $\mathrm{Gal}(\tilde{N}/F)$ injects into $\tilde{\mathcal{B}}(K) \rtimes H$. Moreover, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) \rtimes H & \xrightarrow{\tilde{\pi}} & \mathcal{B} \rtimes H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow \iota & & \uparrow \tilde{\phi} \cong & & \\ 1 & \longrightarrow & \mathrm{Gal}(\tilde{N}/N) & \longrightarrow & \mathrm{Gal}(\tilde{N}/F) & \xrightarrow{\mathrm{res}_N} & \mathrm{Gal}(N/F) & \longrightarrow & 1 \end{array}$$

where $\tilde{\phi}$ is the isomorphism given by Proposition 3.10. (Note that the definition of an equivariant embedding problem requires actions of the finite group H on $\tilde{\mathcal{B}}$ and $\mathcal{B}$, respectively. The semidirect products are defined with respect to these actions.)

Proof. Let $\tilde{\tau} : H \to \tilde{\mathcal{B}} \rtimes H$ and $\tau : H \to \mathcal{B} \rtimes H$ denote the given regular homomorphic sections (which define the equivariance condition) and let $\alpha : \mathrm{Gal}(L/F) \to H$ be the given isomorphism. Let $\tilde{\chi} := \tilde{\tau} \circ \alpha$ and $\chi := \tau \circ \alpha$ be the composites. The homomorphism $\tilde{\pi}$ in the above diagram is defined by $\tilde{\pi}(b \cdot \tilde{\tau}(h)) = \pi(b) \cdot \tau(h)$ for $b \in \tilde{\mathcal{B}}$, $h \in H$. Note that this is a homomorphism because π is equivariant. Moreover, we have $\tilde{\pi} \circ \tilde{\chi} = \tilde{\pi} \circ (\tilde{\tau} \circ \alpha) = \tau \circ \alpha = \chi$.
By Lemma 3.9, there exists matrices $\tilde{Z} \in \mathrm{GL}_n(L)$ and $Z \in \mathrm{GL}_m(L)$ such that $\sigma(\tilde{Z}) = \tilde{Z}\tilde{\chi}(\sigma)$ and $\sigma(Z) = Z\chi(\sigma)$ for all $\sigma \in \mathrm{Gal}(L/F)$, and $\tilde{N}/F$ is a Picard-Vessiot extension with fundamental solution matrix $\tilde{Z}Y_{\tilde{\mathcal{B}}}$, where $Y_{\tilde{\mathcal{B}}} \in \tilde{\mathcal{B}}(\tilde{N})$ is a fundamental solution matrix for the differential equation defined by $A_{\tilde{\mathcal{B}}}$ over L.
Since $L \leq N \leq \tilde{N}$ is a tower of Picard-Vessiot extensions, we have restriction homomorphisms $\mathrm{res}_L : \mathrm{Gal}(\tilde{N}/F) \to \mathrm{Gal}(L/F)$ and $\mathrm{res}_N : \mathrm{Gal}(\tilde{N}/F) \to \mathrm{Gal}(N/F)$, respectively. For σ in $\mathrm{Gal}(\tilde{N}/F)$, there exists a $C_\sigma \in \mathrm{GL}_n(K)$ such that $\sigma(Y) = YC_\sigma$. We want to show that $C_\sigma \in \tilde{\mathcal{B}}(K) \rtimes H$ for all $\sigma \in \mathrm{Gal}(\tilde{N}/F)$. We have that

$$YC_\sigma = \sigma(Y) = \sigma(\tilde{Z}Y_{\tilde{\mathcal{B}}}) = \mathrm{res}_L(\sigma)(\tilde{Z})\sigma(Y_{\tilde{\mathcal{B}}}) = \tilde{Z}\tilde{\chi}(\mathrm{res}_L(\sigma))\sigma(Y_{\tilde{\mathcal{B}}})$$

from which we conclude that

$$C_\sigma = Y_{\tilde{\mathcal{B}}}^{-1}\tilde{\chi}(\mathrm{res}_L(\sigma))\sigma(Y_{\tilde{\mathcal{B}}}).$$

We have written C_σ as a product of matrices in $(\tilde{\mathcal{B}} \rtimes H)(\tilde{N})$, but it also has constant coefficients, which proves that $\mathrm{Gal}(\tilde{N}/F) \hookrightarrow \tilde{\mathcal{B}}(K) \rtimes H$ via a homomorphism ι given by the formula $\iota(\sigma) = Y^{-1}\sigma(Y)$.
It remains to check that the diagram commutes. The fundamental solution matrix $Y_{\tilde{\mathcal{B}}}$ maps to a fundamental solution matrix $Y_{\mathcal{B}} \in \mathcal{B}(N)$ for $A_{\mathcal{B}}$ under π as seen in the proof of Proposition 2.12. From the proof of Proposition 3.10, it follows that $ZY_{\mathcal{B}}$ is a fundamental solution matrix for N/F with Galois group acting as $\mathcal{B}(K) \rtimes H$ via $\tilde{\phi}$. For $\sigma \in \mathrm{Gal}(\tilde{N}/F)$, we have that

$$\begin{aligned} (\tilde{\pi} \circ \iota)(\sigma) &= \tilde{\pi}(Y^{-1}\sigma(Y)) = \tilde{\pi}(Y_{\tilde{\mathcal{B}}}^{-1}\tilde{Z}^{-1}\,\mathrm{res}_L(\sigma)(\tilde{Z})\sigma(Y_{\tilde{\mathcal{B}}})) \\ &= \pi(Y_{\tilde{\mathcal{B}}}^{-1})\tilde{\pi}\left(\tilde{\chi}(\mathrm{res}_L(\sigma))\right)\sigma(\pi(Y_{\tilde{\mathcal{B}}})) = Y_{\mathcal{B}}^{-1}\chi(\mathrm{res}_L(\sigma))\,\mathrm{res}_N(\sigma)(Y_{\mathcal{B}}) \\ &= Y_{\mathcal{B}}^{-1}Z^{-1}\,\mathrm{res}_L(\sigma)(Z)\,\mathrm{res}_N(\sigma)(Y_{\mathcal{B}}) = (ZY_{\mathcal{B}})^{-1}\,\mathrm{res}_N(\sigma)(ZY_{\mathcal{B}}) \\ &= (\tilde{\phi} \circ \mathrm{res}_N)(\sigma) \end{aligned}$$

which proves the claim (there is then a canonical way to define the arrows on the left hand side so that the big diagram commutes). □

Note 3.13. In the above proof, we identified $\tilde{\mathcal{B}}$ with its image in $\tilde{\mathcal{B}} \rtimes H$ (and $\mathcal{B}$ with its image in $\mathcal{B} \rtimes H$). This might require an adjustment of the fundamental solution matrix (to the new representation). Since $\tilde{\mathcal{B}}$ is connected and the fundamental solution matrix can be chosen as a rational point of this group in some extension of F, this is always possible (as seen in the proof of Proposition 3.10). Moreover, the homomorphisms in the exact sequence as well as the equivariance carry over to the new representations. In the sequel, we will make this kind of identification without further indication.

In the special case when $\mathcal{B} = 1$, we obtain a Kovacic-type result (cf. Proposition 2.9) in the non connected case.

Corollary 3.14. *Let $\mathcal{G} = \mathcal{G}^0 \rtimes H$ be a linear algebraic group defined over K and let L/F be a finite Galois extension with Galois group isomorphic to H. Let further $A \in \mathrm{Lie}_L(\mathcal{G}^0)$ be an equivariant matrix. Then the Picard-Vessiot extension N/L defined by A is also a Picard-Vessiot extension of F and $\mathrm{Gal}(N/F)$ injects into $\mathcal{G}(K)$. Moreover, we have a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{G}^0(K) & \longrightarrow & \mathcal{G}(K) & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow \cong & & \\ 1 & \longrightarrow & \mathrm{Gal}(N/L) & \longrightarrow & \mathrm{Gal}(N/F) & \longrightarrow & \mathrm{Gal}(L/F) & \longrightarrow & 1 \end{array}$$

Remark 3.15. Although the above diagram commutes, $\mathrm{Gal}(N/F)$ need not be a semidirect product of $\mathrm{Gal}(N/L)$ and $\mathrm{Gal}(L/F)$, i.e., the lower sequence does *not* necessarily split.

3.5 Non-split Extensions

We conclude this chapter by briefly mentioning what happens if the group under consideration is a nontrivial extension of its connected component by a finite group.

Proposition 3.16. *Let $\mathcal{G}$ be a linear algebraic group defined over K and let R/F be a Picard-Vessiot ring with field of fractions E. Suppose that $\mathrm{Gal}(E/F) \cong \mathcal{G}(K)$, and let $\mathcal{X} = \mathrm{Spec}(R)$.*

1. *$E^{\mathcal{G}^0(K)} =: L/F$ is a finite Galois extension with Galois group $\mathrm{Gal}(L/F) \cong (\mathcal{G}/\mathcal{G}^0)(K)$ and E/L is a Picard-Vessiot extension with $\mathrm{Gal}(E/L) \cong \mathcal{G}^0(K)$.*
2. *Let $\tilde{Y}$ be a fundamental solution matrix for the extension E/F. There exists a fundamental solution matrix $Y \in \mathcal{G}^0(E)$ for the extension E/L and $Z := \tilde{Y}Y^{-1}$ is an L-rational point of $\mathcal{X}$.*

3. The assignment

$$\sigma \mapsto \chi(\sigma) = Z^{-1}\sigma(Z)$$

defines a cocycle $\chi \in Z^1(\mathrm{Gal}(L/F), \mathcal{G}(L))$.

Proof. The first claim follows from the Galois correspondence 1.12. Since $\mathcal{G}^0$ is connected, there exists by 2.9 a fundamental solution matrix $Y \in \mathcal{G}^0(E)$ for the extension E/L. By definition, $Z \in \mathcal{X}(E)\mathcal{G}^0(E) \subseteq \mathcal{X}(E)\mathcal{G}(E) = \mathcal{X}(E)$ (recall that $\mathcal{X}$ is a $\mathcal{G}_F$-torsor by Theorem 1.14). A computation then shows that Z is fixed by $\mathrm{Gal}(E/L) \cong \mathcal{G}^0(K)$, i.e., has coefficients in L:

$$\varepsilon(Z) = \varepsilon(\tilde{Y}Y^{-1}) = \tilde{Y}C_\varepsilon C_\varepsilon^{-1}Y^{-1} = Z$$

for all $\varepsilon \in \mathrm{Gal}(E/L)$ with image $C_\varepsilon \in \mathcal{G}^0(K)$. To see the last claim, let $\sigma, \varepsilon \in \mathrm{Gal}(L/F)$. Then

$$\chi(\sigma\varepsilon) = Z^{-1}\sigma\varepsilon(Z) = Z^{-1}\sigma(Z)\sigma(Z)^{-1}\sigma\varepsilon(Z) = \chi(\sigma)\sigma(\chi(\varepsilon))$$

as we had to show. □

Chapter 4

The Inverse Problem

In this chapter, we solve the inverse problem over the differential field $(F, \partial) = (K(t), \partial_t = \frac{d}{dt})$, where K is an algebraically closed field of characteristic zero. Our approach consists of three main steps, which correspond to the first three sections of this chapter:
The connected component of the identity of a linear algebraic group is a normal subgroup of finite index, in particular, the quotient of the algebraic group by this normal subgroup is finite. Since finite groups are realizable over fields of the type under consideration, the inverse problem will be solved once we can solve embedding problems with connected kernel and finite cokernel. A theorem of Borel and Serre will allow the reduction to the case of split embedding problems of this type. As seen in Chapter 3, such embedding problems can be solved by finding equivariant realizations of the connected components.
Every linear algebraic group may be decomposed as the semidirect product of a unipotent group (the unipotent radical) by a maximal reductive subgroup (a so-called Levi factor). Consequently, the realization of arbitrary linear algebraic groups can be split into the equivariant realization of a maximal connected reductive subgroup and the solution of equivariant embedding problems with unipotent kernel. This will be the subject of the second and third section, respectively.
In the fourth section, we will combine the previous results to prove the main theorem. The last section of this chapter is devoted to some concluding remarks on the proof and possible generalizations.

4.1 A First Reduction

Our first reduction is based on the following theorem ([BS64], Lemme 5.11):

Theorem 4.1. *Let $\mathcal{G}$ be a linear algebraic group defined over an algebraically closed field of characteristic zero. Then $\mathcal{G}$ contains a finite supplement to the connected component of the identity, i.e., there exists a finite subgroup H of $\mathcal{G}$ such that $\mathcal{G}$ is generated as a linear algebraic group by $\mathcal{G}^0$ and H.*

For our purposes, we need to find a supplement which satisfies an additional condition, namely, which respects the semidirect product decomposition of the connected component into unipotent radical and Levi factor.

Lemma 4.2. *Let $\mathcal{G}$ be a linear algebraic group defined over K. Then there exists a decomposition $\mathcal{G}^0 = \mathcal{U} \rtimes \mathcal{P}$ of $\mathcal{G}^0$ into unipotent radical $\mathcal{U}$ and maximal reductive subgroup $\mathcal{P}$, and a finite supplement H of $\mathcal{G}^0$ in $\mathcal{G}$ which normalizes $\mathcal{P}$.*

Proof. By [Mos56] (first theorem of the article, whose theorems are unfortunately not numbered), $\mathcal{G}$ can be decomposed into the semidirect product $\mathcal{G} = \mathcal{U} \rtimes \mathcal{G}^{\mathrm{red}}$ of its unipotent radical $\mathcal{U}$ by a maximal reductive subgroup $\mathcal{G}^{\mathrm{red}}$. The connected component of the identity $\mathcal{P}$ of $\mathcal{G}^{\mathrm{red}}$ is then a complement to $\mathcal{U}$ in $\mathcal{G}^0$. By Theorem 4.1 above, $\mathcal{P}$ has a finite supplement H in $\mathcal{G}^{\mathrm{red}}$. This supplement H is likewise a supplement to $\mathcal{G}^0$ in $\mathcal{G}$. In addition, it normalizes the connected reductive group $\mathcal{P}$. □

4.2 Realization of Reductive Groups

In this section, $\mathcal{G}$ denotes a reductive linear algebraic group over K which is the semidirect product of its connected component of the identity $\mathcal{P} \trianglelefteq \mathcal{G}$ by a finite group H. By [Spr98], Cor. 8.1.6, $\mathcal{P}$ can be written as the product $\mathcal{T} \cdot \mathcal{S}$ of a torus $\mathcal{T}$, the radical of $\mathcal{P}$, and the commutator subgroup $\mathcal{S}$, which is semisimple.
Moreover, both subgroups are stabilized by H (the radical $\mathcal{T}$ is a characteristic subgroup and $\mathcal{S}$ is a commutator subgroup). This allows us to consider the two groups $\mathcal{S} \rtimes H$ and $\mathcal{T} \rtimes H$.

4.2.1 Equivariant Realizations of Semisimple Groups

As before, let $\mathcal{S} \rtimes H$ be a semidirect product of a connected semisimple group by a finite group. We are going to make use of the following theorem which is a consequence of [Sin93], Theorem 4.4 (using that all linear characters of a semisimple group are trivial).

Theorem 4.3. *Groups with semisimple connected component of the identity are realizable over F.*

By the above theorem, there exists a Picard-Vessiot extension E/F with differential Galois group $\mathcal{S}(K) \rtimes H$. The fixed field $L := E^{\mathcal{S}(K)}$ under $\mathcal{S}(K)$ is a finite Galois extension of F with Galois group (isomorphic to) H. By Proposition 3.7, there exists a matrix $A_{\mathcal{S}} \in \mathrm{Lie}_L(\mathcal{S})$ which defines the Picard-Vessiot extension E/L and is equivariant in the sense of Definition 3.5. We have thus shown:

Lemma 4.4. *Let $\mathcal{S} \rtimes H$ be the semidirect product of a connected semisimple linear algebraic group by a finite group, both defined over K. There exists a finite Galois extension L/F with Galois group isomorphic to H and an effective equivariant realization of $\mathcal{S}$ over L.*

4.2.2 Equivariant Realizations of Tori

Next, we turn to the torus $\mathcal{T}$.

Definition 4.5. *An element x of a torus is called* **regular** *if no nontrivial character of the torus evaluates to 1 on x. Similarly, an element of the Lie algebra is called regular if no differential of a nontrivial character vanishes on this element.*

It is more or less folklore that to realize a torus, it is (up to a slight modification) sufficient to use a regular element of the Lie algebra of the torus as the defining matrix of the differential equation. For our purposes, we need a regular element which also satisfies the equivariance condition. The existence of such an element is guaranteed by the next lemma.

Lemma 4.6. *Let $\mathcal{T} \rtimes H$ be the semidirect product of a torus by a finite group, both defined over K. Let L/F be a finite Galois extension with Galois group isomorphic to H. Then the set of equivariant matrices in* $\mathrm{Lie}(\mathcal{T}(L))$ *contains a regular element.*

Proof. Let $w_1, \ldots, w_r$ be a normal basis of L/F, $r := [L : F]$ (see, for example, [Lan84], Theorem 13.1), and let $d := \dim(\mathcal{T})$. We claim that the elements of the set $\{t^i w_j | i = 1, \ldots, d; j = 1, \ldots, r\}$ are linearly independent over $\mathbb{Q}$. To see this, suppose that $\sum_{i,j} \beta_{ij} t^i w_j = 0$ is a relation with coefficients $\beta_{ij} \in \mathbb{Q}$, then

$$\sum_{j=1}^{r} \left(\sum_{i=1}^{d} \beta_{ij} t^i \right) w_j = 0,$$

which implies that $\sum_{i=1}^{d} \beta_{ij} t^i = 0$ for $j = 1, \ldots, r$ since the w_j are linearly independent over $F = K(t) > \mathbb{Q}(t)$. This, in turn, may only happen if all β_{ij} are zero (compare coefficients).
Let $\tau : H \to \mathcal{T} \rtimes H$ be a regular homomorphic section. For $\sigma \in \mathrm{Gal}(L/F)$, denote by C_σ the image of σ in $\tau(H)$, and let $\chi : \mathrm{Gal}(L/F) \to \mathrm{Aut}(\mathrm{Lie}_L(\mathcal{T}))$ be the homomorphism given by $\chi(\sigma)(g) = C_\sigma \sigma(g) C_\sigma^{-1}$, $g \in \mathrm{Lie}_L(\mathcal{T})$.
Let

$$\Phi : \mathcal{T}(L) \to \mathbb{G}_m^d(L), \qquad x \mapsto (\chi_1(x), \ldots, \chi_d(x))$$

be an isomorphism and define $b := (d\Phi)^{-1}(tw_1, \ldots, t^d w_1)$. Let moreover $\tilde{b} = \sum_{\sigma \in \mathrm{Gal}(L/F)} \chi(\sigma(b))$. We claim that $\tilde{b}$ is a regular element (its equivariance is clear).
We need to show that no differential of a character of $\mathcal{T}$ vanishes on $\tilde{b}$. Suppose that κ is a character, then $\sigma^{-1}\kappa\chi(\sigma)$ is again a character: κ is a rational function in the coordinate functions f_{ij}, consequently, $\sigma^{-1}\kappa\chi(\sigma)(f_{ij}) = \kappa(C_\sigma(f_{ij})C_\sigma^{-1})$ and this is again a rational function in the f_{ij}. Therefore, we may write $\sigma^{-1}\kappa\chi(\sigma) = \prod_{i=1}^{d} \chi_i^{\alpha_i(\sigma)}$

for exponents $\alpha_i(\sigma) \in \mathbb{Z}$. Moreover, $\sigma^{-1}d\kappa\chi(\sigma) = d(\sigma^{-1}\kappa\chi(\sigma)) = \sum_{i=1}^{d} \alpha_i(\sigma)d\chi_i$. Here the first equality is valid since

$$\begin{aligned}(d(\sigma^{-1}\kappa\chi(\sigma))(a_{ij})) &= \sum_{i,j} \frac{\partial(\sigma^{-1}\kappa\chi(\sigma))}{\partial f_{ij}}(1)a_{ij} \\ &= \sum_{i,j} \frac{\sigma^{-1}\partial(\kappa)}{\partial\chi(\sigma)(f_{ij})}(1)f_{ij}(\chi(\sigma)(a_{ij})) = (\sigma^{-1}d\kappa\chi(\sigma))(a_{ij})\end{aligned}$$

for $(a_{ij}) \in \mathrm{Lie}(\mathcal{T}(L))$ (see [Hum98], Section 5.4 for the computation of the differential of a morphism). The second equality just uses the fact that the differential of multiplication in the group is addition in the Lie algebra. Consequently, we find that

$$\begin{aligned}d\kappa(\tilde{b}) &= \sum_{\sigma\in\mathrm{Gal}(L/F)} d\kappa(\chi(\sigma)(b)) \\ &= \sum_{\sigma\in\mathrm{Gal}(L/F)} \sigma\left(\sum_{i=1}^{d} \alpha_i(\sigma)d\chi_i(b)\right) = \sum_{\sigma\in\mathrm{Gal}(L/F)} \sum_{i=1}^{d} \alpha_i(\sigma)\sigma(t^i w_1)\end{aligned}$$

and this is nonzero since the elements $t^i w_j$ are linearly independent over $\mathbb{Q}$ as shown above. □

With this at hand, we can prove the following (compare to [MS00], 5.1):

Lemma 4.7. *Let $\mathcal{T} \rtimes H$ be the semidirect product of a torus and a finite group, both defined over K. Let L/F be a finite Galois extension with Galois group isomorphic to H. Then there exists an effective equivariant realization of $\mathcal{T}(K)$ over L.*

Proof. Assume without loss of generality that L/F is unramified at ∞ (replace t by a linear fractional transformation of t). Let $A_{\mathcal{T}}$ be a regular equivariant element in $\mathrm{Lie}(\mathcal{T}(L))$ (such an element exists by Lemma 4.6 above), and let $\Phi : \mathcal{T}(L) \to \mathbb{G}_m^d(L)$, $x \mapsto (\chi_1(x), \ldots, \chi_d(x))$ be an isomorphism, where $d := \dim(\mathcal{T})$. As a consequence of Proposition 2.12, the Galois group G of the differential equation $X' = d\Phi(A_{\mathcal{T}})X$ has dimension less than or equal to the Galois group of the equation $X' = A_{\mathcal{T}}X$ (compare transcendence degrees of the corresponding fields over L), which in turn has dimension at most d. Since $A_{\mathcal{T}}$ is regular, the values $g_i \in L$ of the $d\chi_i$ on $A_{\mathcal{T}}$ are linearly independent over $\mathbb{Z}$. By [MS96], Prop. 2.10, G has dimension d if every relation of the form $\alpha_1 g_1 + \ldots + \alpha_d g_d = f'/f$ with coefficients $\alpha_i \in \mathbb{Z}$ and $f \in L$ is trivial. After replacing $A_{\mathcal{T}}$ by an F-multiple if necessary, we may assume that the g_i in such a relation are regular except for points above ∞ and that they have poles at points above ∞. This adjustment of the matrix changes neither its equivariance nor its regularity. Every element of the form f'/f has a zero at points above ∞. Thus a relation of the form above implies a $\mathbb{Z}$-linear dependence of the g_i, which

shows that the relation has to be trivial. Consequently, the dimension of G is in fact d and hence the same holds for the dimension of the Galois group we are interested in. Since it is contained in the connected group $\mathcal{T}(K)$ of the same dimension, it has to equal $\mathcal{T}(K)$ as required. □

4.2.3 Realizations of Arbitrary Reductive Groups

Combining the results on semisimple groups and tori, we obtain the following proposition.

Proposition 4.8. *Let $\mathcal{P} \rtimes H$ be the semidirect product of a connected reductive linear algebraic group and a finite group, both defined over K. Then there exists a finite Galois extension L/F with Galois group isomorphic to H and an effective equivariant realization of $\mathcal{P}$ over L.*

Proof. Let $\tau : H \to \mathcal{P} \rtimes H$ be a regular homomorphic section. By [Spr98], Corollary 8.1.6., $\mathcal{P}$ is the product of a semisimple group $\mathcal{S}$ and a torus $\mathcal{T}$ both normalized under $\tau(H)$, and we have a surjective homomorphism $\pi : \mathcal{T} \times \mathcal{S} \to \mathcal{P}$ with finite kernel given by multiplication in $\mathcal{P}$.
Both $\mathcal{S}$ and $\mathcal{T}$ are closed in $\mathcal{P}$, ([Hum98], 17.2. and [Spr98], 6.4.14., respectively), which implies that the inclusions of these subgroups are morphisms of linear algebraic groups. Consequently, the composition of the inclusions and multiplications π is also a morphism.
We consider the semidirect products $\mathcal{S} \rtimes H$ and $\mathcal{T} \rtimes H$ as subgroups of $\mathcal{P} \rtimes H$, so that we can work with the same section τ as above. By Lemma 4.4, there exists a finite Galois extension L/F with Galois group isomorphic to H and an equivariant matrix $A_{\mathcal{S}} \in \mathrm{Lie}_L(\mathcal{S})$ which realizes $\mathcal{S}$. By Lemma 4.7, there exists an equivariant matrix $A_{\mathcal{T}} \in \mathrm{Lie}_L(\mathcal{T})$ which realizes $\mathcal{T}(K)$ over L. It is shown in [MS96], Prop. 2.10, that the block diagonal matrix $A_{\mathcal{S}} \oplus A_{\mathcal{T}}$ then realizes the direct product $\mathcal{T}(K) \times \mathcal{S}(K)$ over L.
By Lemma 2.12, the matrix $d\pi(A_{\mathcal{T}} \oplus A_{\mathcal{S}}) = A_{\mathcal{T}} + A_{\mathcal{S}} \in \mathrm{Lie}_L(\mathcal{P})$ realizes $\mathcal{G}$ over L, and as a sum of equivariant matrices (with respect to the same section), this matrix is equivariant. □

All in all, we have found equivariant realizations of connected reductive groups over L. Before turning to the remaining part, namely the solution of equivariant embedding problems with unipotent kernel, we state the following partial solution of the inverse problem.

Corollary 4.9. *Let $\mathcal{G}$ be a reductive linear algebraic group. Then $\mathcal{G}$ is realizable as a differential Galois group over F.*

Proof. By Theorem 4.1, there exists a finite subgroup H of $\mathcal{G}$ which is a supplement for $\mathcal{G}^0$ in $\mathcal{G}$. Let $\tilde{\mathcal{G}} = \mathcal{G}^0 \rtimes H$ be the semidirect product. Note that we have a morphism of linear algebraic groups $\pi : \tilde{\mathcal{G}} \twoheadrightarrow \mathcal{G}$ with finite kernel $H \cap \mathcal{G}^0$ given by

inclusion of the two closed subgroups and multiplication. By Proposition 4.8, there exists a finite Galois extension L/F and an effective equivariant realization of $\mathcal{G}^0$ over L. By Proposition 3.10, this gives a realization of $\tilde{\mathcal{G}}(K)$ over F as the Galois group of some Picard-Vessiot extension $\tilde{N}/F$. By the Galois correspondence, the fixed field $N \leq \tilde{N}$ under $\mathrm{Ker}(\pi)$ is a Picard-Vessiot extension of F with differential Galois group isomorphic to $\mathcal{G}(K)$. □

4.3 Equivariant Embedding Problems with Unipotent Kernel

Throughout this section, L/F denotes a finite Galois extension of F with Galois group isomorphic to the finite K-group H.
Let us consider the connected split equivariant embedding problem

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{U}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) & \underset{\leftarrow}{\overset{\pi}{\longrightarrow}} & \mathcal{B}(K) & \longrightarrow & 1 \\ & & & & & & \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(M/L) & & \end{array} \tag{4.10}$$

with unipotent kernel $\mathcal{U}$ and reductive cokernel $\mathcal{B}$. The aim of this section is to show that embedding problems of this type have proper effective equivariant solutions. To this end, we will break up this embedding problem into smaller ones as follows. The commutator subgroup $\mathcal{U}' := (\mathcal{U},\mathcal{U})$ is normal in $\tilde{\mathcal{B}}$. We obtain two new short exact sequences

$$1 \to \mathcal{U}/\mathcal{U}' \to \tilde{\mathcal{B}}/\mathcal{U}' \to \mathcal{B} \to 1 \tag{4.11}$$

and

$$1 \to \mathcal{U}' \to \tilde{\mathcal{B}} \to \tilde{\mathcal{B}}/\mathcal{U}' \to 1. \tag{4.12}$$

Since $\mathcal{U}'$ is stable under H (it is a commutator subgroup), the quotients $\tilde{\mathcal{B}}/\mathcal{U}'$ and $\mathcal{U}/\mathcal{U}'$ inherit an action of H by conjugation. Note that by definition, all homomorphisms in the two exact sequences are equivariant homomorphisms with respect to this action.
It is well known that in the above situation, it suffices to solve the two embedding problems associated to the new exact sequences separately. Namely, if we find a proper effective solution of the embedding problem associated to the sequence (4.11) with some Picard-Vessiot extension N of L containing M, and then a proper effective solution of the embedding problem associated to the sequence (4.12) (with $\left(\tilde{\mathcal{B}}/\mathcal{U}'\right)(K) \cong \mathrm{Gal}(N/L)$), this will be a proper effective solution of the initial embedding problem. Moreover, if the matrices in both steps are equivariant, we will have solved the initial problem by an equivariant matrix.

4.3.1 Equivariantly Split Embedding Problems with Unipotent Abelian Kernel

First, we turn to the embedding problem associated to the sequence (4.11). This sequence splits and the section is H-equivariant. The kernel of this embedding problem is unipotent abelian and stable under the H-action. Since $\delta(\mathcal{B}) \rtimes H \leq \tilde{\mathcal{B}} \rtimes H$ is reductive (this group is defined since δ is equivariant), we may write

$$\mathcal{U}/\mathcal{U}' \cong \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$$

where the $\mathcal{A}_i$ are minimal $\delta(\mathcal{B}) \rtimes H$-stable direct sums of additive groups. Note that this decomposition is a decomposition as linear algebraic groups (i.e., the isomorphism is in fact a morphism) and exists over the algebraically closed field K. In particular, all $\mathcal{A}_i$ are defined over K.
As before, we may successively factor by such $\mathcal{A}_i$ and reduce the problem to an embedding problem with a lower dimensional kernel. The key observation is that all resulting embedding problems are split by H-equivariant sections (with the inherited action on the factor groups).

Lemma 4.13. *Let*

$$1 \to \mathcal{A}_1 \times \mathcal{A}_2 \xrightarrow{\alpha} \tilde{\mathcal{B}} \underset{\leftarrow}{\overset{\psi}{\underset{\delta}{\rightleftarrows}}} \mathcal{B} \to 1$$

be a split exact sequence of connected linear algebraic groups, and suppose that each of the groups in the exact sequence carries an action of the finite group H by K-automorphisms. Suppose further that α, δ and ψ are equivariant with respect to these actions. Moreover, assume that the direct sum decomposition is $\delta(\mathcal{B})$-stable and H-stable (in particular, this forces $\mathcal{A}_1$ to be normal in $\tilde{\mathcal{B}}$). Then the sequences

$$1 \to \mathcal{A}_2 \xrightarrow{\alpha_1} \tilde{\mathcal{B}}/\mathcal{A}_1 \xrightarrow{\psi_1} \mathcal{B} \to 1$$

and

$$1 \to \mathcal{A}_1 \xrightarrow{\alpha_2} \tilde{\mathcal{B}} \xrightarrow{\psi_2} \tilde{\mathcal{B}}/\mathcal{A}_1 \to 1$$

also split, and the sections are H-equivariant (with respect to the induced H-action on the factor groups).

Proof. Note that since all groups under consideration are defined over K, it suffices to define the homomorphisms on K-rational points and to make sure they are morphism. Define a section δ_1 to ψ_1 by the composite

$$\delta_1 : \mathcal{B} \xrightarrow{\delta} \tilde{\mathcal{B}} \xrightarrow{\psi_2} \tilde{\mathcal{B}}/\mathcal{A}_1,$$

this is a section since $\psi_1(\delta_1(b)) = \psi_1(\psi_2(\delta(b))) = \psi(\delta(b)) = b$ for $b \in \mathcal{B}(K)$. As a composition of morphisms, δ_1 is a morphism. As a composition of H-equivariant maps, it is H-equivariant.

Next, we define a section to ψ_2. Since $\tilde{\mathcal{B}}/\mathcal{A}_1 \cong \mathcal{A}_2 \rtimes \mathcal{B}$ (H-equivariantly) as shown above, we can define $\delta_2 : \tilde{\mathcal{B}}/\mathcal{A}_1 \cong \mathcal{A}_2 \rtimes \mathcal{B} \to \tilde{\mathcal{B}} = (\mathcal{A}_1 \times \mathcal{A}_2) \rtimes \mathcal{B}$ by $(a_2, b) \mapsto (1 \times a_2, b)$, $a_2 \in \mathcal{A}_2(K)$, $b \in \mathcal{B}(K)$. Note that this a morphism of linear algebraic groups and gives a section to ψ_2.
Finally, we check that

$$\begin{aligned}\delta_2(a_2, b)^h &= (1 \times a_2, b)^h = (1 \times a_2^h, b^h) \\ &= \delta_2(a_2^h, b^h) = \delta_2((a_2, b)^h)\end{aligned}$$

for $a_2 \in \mathcal{A}_2(K)$, $b \in \mathcal{B}(K)$ and $h \in H$ (the superscript stands for the corresponding H-actions), i.e., δ_2 is H-equivariant. □

By induction on the dimension of the kernel, the above lemma allows the reduction to a split equivariant embedding problem with minimal unipotent abelian kernel. It remains to show that such embedding problems have proper equivariant (effective) solutions. This is the aim of the following proposition which mimics Proposition 2.1 of [Obe01].

Proposition 4.14. *A split equivariant embedding problem*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) & \underset{\delta}{\overset{\longleftarrow}{\longrightarrow}} & \mathcal{B}(K) & \longrightarrow & 1 \\ & & & & & & \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(N/L) & & \end{array}$$

with minimal unipotent abelian kernel has an effective proper equivariant solution.

Proof. Let $\tilde{\tau} : H \to \tilde{\mathcal{B}} \rtimes H$ be the regular homomorphic section defining the equivariance condition for $\tilde{\mathcal{B}}$. Let $A_{\mathcal{B}} \in \mathrm{Lie}_L(\delta(\mathcal{B}))$ be an equivariant matrix realizing N/L. Let $Y_{\mathcal{B}} \in \delta(\mathcal{B})(N)$ be a fundamental solution matrix for the differential equation defined by $A_{\mathcal{B}}$, and let $\Phi : \mathcal{A}(L) \to L^m$ be an isomorphism (which exists since $\mathcal{A}$ is commutative). Let $d\Phi$ be the associated homomorphism of Lie algebras. Conjugation with elements of $\delta(\mathcal{B}) \rtimes H \leq \tilde{\mathcal{B}} \rtimes H$ on $\mathcal{A}(L)$ induces an automorphism of L^m, the corresponding representation $\delta(\mathcal{B}) \rtimes H \to \mathrm{GL}_m$ will be denoted by ρ (this is indeed a morphism because it is given by conjugation). We have a twisted action of H on L^m via $\sigma * a := \rho(C_\sigma)\sigma(a)$ ($\sigma \in \mathrm{Gal}(L/F)$, C_σ the corresponding element of $\tilde{\tau}(H)$, $a \in L^m$) induced by the twisted action on $\mathrm{Lie}_L(\mathcal{A})$. This action is clearly semilinear, and a vector invariant under this action is the image of an equivariant element in $\mathrm{Lie}_L(\mathcal{A})$ under $d\Phi$. Therefore, we will call such vectors equivariant.
Assume for a moment that there exists a vector $a \in L^m$ which is equivariant such that the differential equation $X' = \rho(Y_{\mathcal{B}})^{-1}a$ has no solution with coefficients in N. Set $\tilde{X} := \rho(Y_{\mathcal{B}})X$. A calculation shows that

$$\begin{aligned} X' = \rho(Y_{\mathcal{B}})^{-1}a &\iff (\rho(Y_{\mathcal{B}})^{-1}\tilde{X})' = \rho(Y_{\mathcal{B}})^{-1}a \\ &\iff (\rho(Y_{\mathcal{B}})^{-1})'\tilde{X} + \rho(Y_{\mathcal{B}})^{-1}\tilde{X}' = \rho(Y_{\mathcal{B}})^{-1}a \\ &\iff \tilde{X}' - d\rho(A_{\mathcal{B}})\tilde{X} = a, \end{aligned}$$

so by assumption, the latter equation has no solution with coefficients in N. Let b be a solution in an extension field of N. Let $\Phi^{-1}(b) =: Y_{\mathcal{A}} \in \mathcal{A}(N)$ and $A_{\mathcal{A}} := d\Phi^{-1}(a) \in \mathrm{Lie}_L(\mathcal{A})$. Note that $A_{\mathcal{A}}$ is equivariant by definition of the twisted action on L^m: Since

$$d\Phi(A_{\mathcal{A}} - C_\sigma \sigma(A_{\mathcal{A}}) C_\sigma^{-1}) = a - \rho(C_\sigma)\sigma(a) = a - a = 0$$

and $d\Phi$ is an isomorphism, we have that $C_\sigma \sigma(A_{\mathcal{A}}) C_\sigma^{-1} = A_{\mathcal{A}}$ for all $\sigma \in \mathrm{Gal}(L/F)$ with image $C_\sigma \in \tilde{\tau}(H)$. Moreover, we have that (compare [MS00], remark following Proposition 3.7)

$$\begin{aligned} d\Phi(A_{\mathcal{A}}) &= \Phi(Y_{\mathcal{A}})' - d\rho(A_{\mathcal{B}})\Phi(Y_{\mathcal{A}}) \\ &= \rho(Y_{\mathcal{B}}) \left(\rho(Y_{\mathcal{B}})^{-1} \Phi(Y_{\mathcal{A}})' - \rho(Y_{\mathcal{B}})^{-1} \rho(Y_{\mathcal{B}})' \rho(Y_{\mathcal{B}})^{-1} \Phi(Y_{\mathcal{A}}) \right) \\ &= \rho(Y_{\mathcal{B}}) \left(\rho(Y_{\mathcal{B}})^{-1} \Phi(Y_{\mathcal{A}}) \right)' = \rho(Y_{\mathcal{B}}) \Phi(Y_{\mathcal{B}} Y_{\mathcal{A}} Y_{\mathcal{B}}^{-1})' \\ &= \rho(Y_{\mathcal{B}}) d\Phi(\lambda(Y_{\mathcal{B}} Y_{\mathcal{A}} Y_{\mathcal{B}}^{-1})) = d\Phi(Y_{\mathcal{B}}^{-1} \lambda(Y_{\mathcal{B}} Y_{\mathcal{A}} Y_{\mathcal{B}}^{-1}) Y_{\mathcal{B}}) \end{aligned}$$

from which we conclude that

$$A_{\mathcal{A}} = Y_{\mathcal{B}}^{-1} \lambda(Y_{\mathcal{B}} Y_{\mathcal{A}} Y_{\mathcal{B}}^{-1}) Y_{\mathcal{B}} = -A_{\mathcal{B}} + Y_{\mathcal{A}} Y_{\mathcal{A}}' + Y_{\mathcal{A}} A_{\mathcal{B}} Y_{\mathcal{A}}$$

since $d\Phi$ is an isomorphism. With the help of the last equality, it can easily be checked that the matrix $Y_{\mathcal{A}} Y_{\mathcal{B}}$ is a fundamental solution matrix of the differential equation $X' = (A_{\mathcal{A}} + A_{\mathcal{B}})X$. Let $\tilde{N}/L$ be the corresponding Picard-Vessiot extension with $N \lneq \tilde{N}$ so that $Y_{\mathcal{A}} Y_{\mathcal{B}} \in \tilde{\mathcal{B}}(\tilde{N})$.
The matrix $A_{\mathcal{A}} + A_{\mathcal{B}}$ is equivariant, so by Proposition 3.10, the extension descends to a Picard-Vessiot extension of F. By Proposition 3.12, $\mathrm{Gal}(\tilde{N}/F)$ injects into $\tilde{\mathcal{B}}(K) \rtimes H$ and we obtain a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) \rtimes H & \xrightarrow{\pi} & \mathcal{B}(K) \rtimes H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow \iota & & \uparrow \varphi \cong & & \\ 1 & \longrightarrow & \mathrm{Gal}(\tilde{N}/N) & \longrightarrow & \mathrm{Gal}(\tilde{N}/F) & \longrightarrow & \mathrm{Gal}(N/F) & \longrightarrow & 1 \end{array} .$$

Since $\mathrm{Gal}(\tilde{N}/N)$ is normal in $\mathrm{Gal}(\tilde{N}/F)$ and normal in $\mathcal{A}(K)$ (recall that this is a commutative group), it must be normal in $\tilde{\mathcal{B}}(K) \rtimes H$ (which is generated by the two groups). In particular, it is $\tilde{\mathcal{B}}$-stable and H-stable. Consequently, $\mathrm{Gal}(\tilde{N}/N) \cong \mathcal{A}(K)$ by minimality. The five lemma then implies that $\mathrm{Gal}(\tilde{N}/L) \cong \tilde{\mathcal{B}}(K)$.
It remains to show the existence of the vector a as above. Let $\tilde{a}$ be any nonzero equivariant vector in L^m (which exists, for example, by Speiser's Lemma 3.3) and let $(\rho(Y_{\mathcal{B}})^{-1}\tilde{a})_i$ be a non vanishing component of $\rho(Y_{\mathcal{B}})^{-1}\tilde{a}$. By Lemma A.1 of the Appendix, there exists a $c \in K$ such that $X' = \frac{(\rho(Y_{\mathcal{B}})^{-1}\tilde{a})_i}{t-c}$ has no solution in N. Let $a := \frac{1}{t-c} \cdot \tilde{a}$ and note that this vector is still equivariant by semilinearity. Then $X' = \rho(Y_{\mathcal{B}})^{-1} a$ has no solution with coefficients in N. □

4.3.2 Equivariant Frattini Embedding Problems

Let us now consider the embedding problem associated to the sequence (4.12)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{U}'(K) & \longrightarrow & \tilde{\mathcal{B}}(K) & \longrightarrow & (\tilde{\mathcal{B}}/\mathcal{U}')(K) & \longrightarrow & 1 \\ & & & & & & \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(N/L) & & \end{array}$$

which is an equivariant Frattini embedding problem (see [Kov69], Lemma 2). The following proposition guarantees that this problem has a proper equivariant solution.

Proposition 4.15. *An equivariant Frattini embedding problem has a proper (effective) equivariant solution.*

Proof. We keep the notation we have been using in this chapter. Let

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A}(K) & \longrightarrow & \tilde{\mathcal{B}}(K) & \xrightarrow{\pi} & \mathcal{B}(K) & \longrightarrow & 1 \\ & & & & & & \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(N/L) & & \end{array}$$

be an equivariant Frattini embedding problem, and suppose that $\mathrm{Gal}(N/L)$ is realized by an equivariant matrix $B \in \mathrm{Lie}_L(\mathcal{B})$. Since π is H-equivariant and defined over K (in particular, it commutes with the Galois action), the fiber $d\pi^{-1}(B)$ is closed under the twisted action of H. Consequently, if we let B' be any element in this fiber, we may define

$$\tilde{B} := \frac{1}{|\mathrm{Gal}(L/F)|} \sum_{\sigma \in \mathrm{Gal}(L/F)} C_\sigma \sigma(B') C_\sigma^{-1} \in d\pi^{-1}(B),$$

where as usual C_σ is the image of σ in the given representation of H. Note that $\tilde{B}$ is equivariant by definition. By Proposition 2.12, $\tilde{B}$ defines an equivariant solution of the embedding problem which is proper since the problem is a Frattini problem. □

4.3.3 The General Case

From the results above, we immediately obtain the following

Proposition 4.16. *A split equivariant embedding problem of the form (4.10) with unipotent kernel and reductive cokernel has a proper effective equivariant solution.*

4.4 The Main Result

We have now collected all necessary ingredients to prove the main result of this thesis.

Theorem 4.17. *Let $\mathcal{G}$ be a linear algebraic group defined over K. There exists a Picard-Vessiot extension of $K(t)$ with differential Galois group (isomorphic to) $\mathcal{G}(K)$.*

Proof. By Lemma 4.2, the connected component of the identity $\mathcal{G}^0(K)$ has a decomposition $\mathcal{G}^0 = \mathcal{U} \rtimes \mathcal{P}$ into unipotent radical and reductive complement, and there exists a finite supplement H in $\mathcal{G}$ which normalizes $\mathcal{P}$. Consequently, we have

$$\tilde{\mathcal{G}} := (\mathcal{U} \rtimes \mathcal{P}) \rtimes H = \mathcal{U} \rtimes (\mathcal{P} \rtimes H).$$

By Proposition 4.8, there exists a finite Galois extension L/F with Galois group isomorphic to H and an equivariant realization of $\mathcal{P}$ over L as the Galois group of some Picard-Vessiot extension M/L. By Proposition 4.16, the resulting split equivariant embedding problem

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{U}(K) & \longrightarrow & \mathcal{G}^0(K) & \underset{\leftarrow}{\longrightarrow} & \mathcal{P}(K) & \longrightarrow & 1 \\ & & & & & & \uparrow \cong & & \\ & & & & & & \mathrm{Gal}(M/L) & & \end{array}$$

has a proper effective equivariant solution. All in all, we obtain an equivariant realization of $\mathcal{G}^0(K)$ as the differential Galois group of some Picard-Vessiot extension $\tilde{E}$ of L. By Proposition 3.10, $\tilde{E}$ is also a Picard-Vessiot extension of F with Galois group isomorphic to $\tilde{\mathcal{G}}(K)$. Let $\tilde{\gamma} : \mathrm{Gal}(\tilde{E}/F) \to \tilde{\mathcal{G}}(K)$ be the corresponding isomorphism. Let further $\pi : \tilde{\mathcal{G}}(K) \to \mathcal{G}(K)$ denote the morphism of algebraic groups given by composition of the inclusion of the closed subgroups $\mathcal{G}^0$ and H with multiplication. Then $E = \tilde{E}^{\mathrm{Ker}(\pi)}$ is the desired Picard-Vessiot extension with $\mathrm{Gal}(E/F) \cong \mathcal{G}(K)$ by the Galois correspondence 1.12. □

4.5 Concluding Remarks

The main result of this thesis (or rather its proof) has two drawbacks. First, it is not constructive. In particular, the use of Singer's result (Theorem 4.3) fixes the finite extension we work over, and we have no control what this extension looks like. To have a constructive proof at least in the split case one would have to find (constructive) equivariant realizations of connected semisimple groups. There is some evidence that an approach similar to the one given by Mitschi and Singer in [MS96] might also work in this more general setting. Namely, the Lie algebra decomposition they use can be performed equivariantly; in particular, there exists

a regular pair of generators of the Lie algebra *over* L which is equivariant (this can be seen using Theorem 13.3.6 of [Spr98] in combination with Speiser's Lemma 3.3). Although we don't know how to prove that a suitable F-linear combination of these matrices provides us with a realization of arbitrary connected semisimple groups, we can at least give an ad hoc proof for the case of SL_2 over $L = K(\sqrt{t})$.

Example. The group SL_2 is the natural example of a semisimple group. There is only one nontrivial class (modulo inner automorphisms) of outer automorphisms, a representative of which is given by the matrix $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This matrix generates an order two subgroup of GL_2. Let us consider the quadratic extension $L = K(\sqrt{t})/F$ with Galois group isomorphic to the copy of $\mathbb{Z}/2$ in GL_2 just described.

We work with the standard representation of SL_2 and the standard (diagonal) torus $\mathcal{T} \leq \mathrm{SL}_2$. The adjoint representation of $\mathcal{T}$ on $\mathrm{Lie}_K(\mathrm{SL}_2)$ gives a decomposition

$$\mathrm{Lie}_K(\mathrm{SL}_2) = \mathrm{Lie}_K(\mathcal{T}) \oplus X_- \oplus X_+$$

where X_- and X_+ are the two root spaces associated to the nontrivial roots.

Note that the action of $\mathbb{Z}/2$ stabilizes the maximal torus $\mathcal{T}$ and therefore also stabilizes this decomposition. Moreover, the matrix $A_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in X_- \oplus X_+$ together with any regular element of $\mathrm{Lie}_K(\mathcal{T})$ forms a regular pair of generators for $\mathrm{Lie}_K(\mathrm{SL}_2)$ (compare [MS96], considerations following Lemma 3.4.). Note that A_0 is equivariant with respect to the given $\mathbb{Z}/2$-actions (indeed, it is fixed by the Galois action as well as by conjugation with σ). It is of course not possible to find a regular equivariant element in $\mathrm{Lie}_K(\mathcal{T})$, but we may choose $A_1 = \begin{pmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{pmatrix} \in \mathrm{Lie}_L(\mathcal{T})$.

We define $A := \frac{1}{2}(A_0 + \frac{1}{t}A_1)$ and claim that the differential Galois group given by this matrix over L is $\mathrm{SL}_2(K)$.

Let $u = \sqrt{t}$ and consider the matrix $\tilde{A} = A_0 + A_1$ over the differential field $(K(u), \partial_u = \frac{\partial}{\partial u})$. By the calculation in [MS96], Example 2, $\tilde{A}$ realizes SL_2 over $K(u)$. Let Y be a fundamental solution matrix for this equation and let $C = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Then

$$\partial_t(CY) = \partial_u(CY)\frac{1}{2u} = \frac{1}{2u}C\tilde{A}C^{-1}(CY) = A(CY)$$

which shows that the differential Galois group defined by A over $(K(u), \partial_t)$ is also SL_2 (the matrices CY and Y define the same Picard-Vessiot extension of L).

As noted above, the lack of a constructive way of realizing semisimple groups makes it impossible to control the finite extension we work with, and therefore implies the second drawback of our approach: It does not generalize to fields of higher transcendence degree over K.

In any case, it remains an interesting problem to find a completely constructive proof of Theorem 4.17.

Appendix

Since we make use of a Lemma of T. Oberlies which hasn't been published so far, we include the proof here (compare [Obe01], Prop. 2.2.).

Lemma A.1. *Let E/F be a Picard-Vessiot extension and $w \in E$. There exist infinitely many elements $c_1, \ldots, c_r \in K$ such that the solutions y_i of $y_i' = \frac{w}{t-c_i}$ are algebraically independent over $K(t)$. In particular, there exists a $c \in K$ such that $y' = \frac{w}{t-c}$ has no solution in E.*

Proof. Let T be a transcendence basis of K over $\mathbb{Q}$ and let $Q := \mathbb{Q}(T)$. Then Q is a Hilbertian field ([FJ86], Theorem 12.9). Let $n \in \mathbb{N}$ be minimal such that $w^{(n)}$ is algebraic over $Q(t, w, \ldots, w^{(n-1)})$ (such n exists since E is of finite transcendence degree over $K(t)$ and thus also over $Q(t)$). Consider the minimal polynomial of $w^{(n)}$ over $Q(t, w, \ldots, w^{(n-1)})$ and clear denominators to obtain an equation of the form

$$\sum_{i=1}^{r} g_i (w^{(n)})^i = 0$$

with coefficients $g_i \in Q[t, w, \ldots, w^{(n-1)}]$. Applying the derivation to this equation gives

$$\sum_{i=1}^{r} g_i' (w^{(n)})^i + w^{(n+1)} \underbrace{\sum_{i=1}^{r} g_i i (w^{(n)})^{i-1}}_{h} = 0, \qquad (*)$$

which shows that $w^{(n+1)} \in F := Q(t, w, \ldots, w^{(n)})$, i.e., F is a differential subfield of E. Let $N := Q(w, \ldots, w^{(n-1)})$. Then $v := g_r w^{(n)}$ is integral over $N[t, v]$.
We claim that there exist infinitely many $c \in Q$ such that $(t-c)N[t, v]$ is a prime ideal. Assuming this, we proceed as follows. Given $m \in \mathbb{N}$, we choose $c_i \in Q$ $(i = 1, \ldots, m)$ such that $(t-c_i)N[t, v]$ is prime and $g_r, h \notin (t-c_i)N[t, v]$. Let y_i be a solution of the differential equation $y_i' = \frac{w}{t-c_i}$ $(i = 1, \ldots, m)$ and assume that the y_i are algebraically dependent over $Q(t)$. Then they are also algebraically dependent over F. By the Kolchin-Ostrowski-Theorem ([Kol76], Section 2) this implies the existence of a relation of the form

$$\sum_{i=1}^{m} d_i y_i' = f'$$

for some $f \in F$ and coefficients $d_i \in \mathbb{Z}$ which are not all zero. Without loss of generality we may assume that $d_1 \neq 0$. Let S be the multiplicatively closed subset of $N[t,v]$ generated by h, g_r and $\{t-c_i, i \geq 2\}$. Note that $N[t,v]$ is not a differential ring, but $S^{-1}N[t,v]$ is a differential ring because of equation $(*)$ above. Moreover, $(t-c_1)S^{-1}N[t,v]$ is a prime ideal. Since the quotient field of $S^{-1}N[t,v]$ is F, we may write $f = (t-c_1)^z \frac{p}{q}$ where $p, q \in S^{-1}N[t,v] \setminus (t-c)S^{-1}N[t,v]$ and $z \in \mathbb{Z}$. Substituting this into the relation above and multiplying by q^2, we find that

$$q^2 w \sum_{j=1}^{m} \frac{d_j}{t-c_j} = z(t-c_1)^{z-1}pq + (t-c_1)^z(p'q - pq') \qquad (**).$$

If $z < 0$, we multiply $(**)$ with $(t-c_1)^{1-z}$ to conclude that $zpq \in (t-c_1)S^{-1}N[t,v]$, which is a contradiction since the ideal is prime. Therefore we conclude that $z \geq 0$. Multiplying $(**)$ with $(t-c_1)$ then shows that $q^2 w d_1 \in (t-c_1)S^{-1}N[t,v]$ (note that for $z = 0$, the first term on the right hand side vanishes). If $n > 0$, we obtain a contradiction since $w \in N$ in this case. If $n = 0$, w is algebraic over $Q(t)$ and $N = Q$. Then if $w \in (t-c)S^{-1}Q[t,v]$, there exists an element $s \in S$ such that $sw \in (t-c)Q[t,v]$ and since this is a prime ideal, $w \in (t-c)Q[t,v]$. Note that $w = v/g_r \in N[t,v]$. Consequently, $v \in (t-c)Q[t,v]$, i.e., there exists an element $k \in Q[t,v]$ such that $v = k(t-c)$. Since v is integral of degree r over $Q[t]$, we may write $k = \sum_{i=1}^{r-1} l_i v^i$ for polynomials $l_i \in Q[t]$. Then we consider the coefficient of v to obtain $1 = (t-c)l_1$, which is a contradiction.

It remains to prove the claim. Consider the integral closure $\mathcal{O}_M$ of $N[t]$ in $M := \mathrm{Quot}(N[t,v])$. Note that since v is integral over $N[t]$, $\mathcal{O}_M$ contains $N[t,v]$. We prove the claim in two steps.

First, we show that there are infinitely many $c \in Q$ such that $(t-c)\mathcal{O}_M$ is prime. The minimal polynomial f_v of v in $N[t,X] = Q(w, \ldots, w^{(n-1)})[t,X]$ is irreducible of degree r and since Q is Hilbertian, f_v remains irreducible for infinitely many specializations $t \mapsto c$. We claim that for all such specializations, $(t-c)\mathcal{O}_M$ is prime. Let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}_M$ in the decomposition of $(t-c)\mathcal{O}_M$ ($\mathcal{O}_M$ is a Dedekind ring). The reduction of f_v modulo $(t-c)$ is irreducible over $N[t]/(t-c)$ and has root v modulo $\mathfrak{p}$ in $\mathcal{O}_M/\mathfrak{p}\mathcal{O}_M$, consequently, the residue classe degree equals the degree r of the extension of $N[t]$ defined by f_v, which by the product formula implies that $(t-c)\mathcal{O}_M$ has to be prime.

The second part is to show that for all but finitely many $c \in Q$, if $(t-c)\mathcal{O}_L$ is prime, then so is $(t-c)N[t,v]$. Since $\mathcal{O}_M$ is finite over $N[t,v]$ ([Mat86], Lemma 33.1), and $N[t,v]$ contains generators for M, there exists an element $a \in N[t,v]$ such that $a\mathcal{O}_M \subseteq N[t,v]$. There are only finitely many $c \in Q$ such that the norm $\mathcal{N}_{M/N[t]}(a) \in (t-c)N[t]$. We want to show that for all other c, $(t-c)N[t,v]$ is prime. Let $x, y \in N[t,v]$ such that $xy \in (t-c)N[t,v]$. Since the extension of the ideal to $\mathcal{O}_M$ is prime, we may without loss of generality assume that $x \in (t-c)\mathcal{O}_M$. Then $ax \in (t-c)N[t,v]$. The elements $1, v, \ldots, v^{r-1}$ form a basis of L over $N(t)$

as a vector space. Let $\mathbf{x}$ be the vector representing x in this basis. Consider the linear transformation on L given by multiplication with a. Since v is integral over $N[t]$, all coefficients of the matrix representation T of this transformation in the given basis are in $N[t]$. By assumption, $T\mathbf{x}$ reduces to zero modulo $(t-c)$, but $\det(T) = \mathcal{N}_{M/N(t)}$ is nonzero when reduced modulo $(t-c)$ by the choice of c. This implies that $\mathbf{x}$ reduces to zero, proving that $x \in (t-c)N[t,v]$. $\square$

Bibliography

[BS64] A. Borel and J.-P. Serre. Théorèmes de finitude en cohomologie galoisienne. *Comment. Math. Helv.*, 39:111–164, 1964.

[FJ86] M.D. Fried and M. Jarden. *Field Arithmetic.* Springer–Verlag, Berlin, Heidelberg, 1986.

[Hal76] M. Hall. *The Theory of Groups.* Chelsea Publishing Company, New York, 1976.

[Hum98] J.E. Humphreys. *Linear Algebraic Groups.* Springer–Verlag, New York, Berlin, Heidelberg, 1998. Fifth corrected printing.

[Kat87] N. Katz. A simple algorithm for cyclic vectors. *Am. J. Math.*, 109:65–70, 1987.

[Kol76] E.R. Kolchin. Algebraic groups and algebraic dependence. *Am. J. Math.*, 90:1151–1164, 1976.

[Kov69] J. Kovacic. The inverse problem in the Galois theory of differential fields. *Ann. Math.*, 89:583–608, 1969.

[Kov71] J. Kovacic. On the inverse problem in the Galois theory of differential fields. *Ann. Math.*, 93:269–284, 1971.

[Lan84] S. Lang. *Algebra.* Addison-Wesley Publishing Company, Menlo Park, 1984.

[Mat86] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, Cambridge, UK, 1986.

[Mat01] B.H. Matzat. Differential Galois theory in positive characteristic. Preprint 2001-35, IWR, 2001.

[Mos56] G.D. Mostow. Fully reducible subgroups of algebraic groups. *Am. J. Math.*, 78:200–221, 1956.

[MS96] C. Mitschi and M. Singer. Connected groups as differential Galois groups. *J. Algebra*, 184:333–361, 1996.

[MS00] C. Mitschi and M. Singer. Solvable by finite groups as differential Galois groups. Preliminary version, 2000.

[MvdP02] B.H. Matzat and M. van der Put. Constructive differential Galois theory. Preprint 2002-02, IWR, 2002.

[Obe01] T. Oberlies. Connected embedding problems. Preliminary version, 2001.

[Ser97] J.-P. Serre. *Galois Cohomology*. Springer-Verlag, Berlin Heidelberg, 1997.

[Sin93] M. Singer. Moduli of linear differential equations on the Riemann sphere with fixed Galois groups. *Pac. J. Math.*, 106:343–395, 1993.

[Spr98] T.A. Springer. *Linear Algebraic Groups*. Birkhäuser, Boston, 2nd edition, 1998.

[TT79] C. Tretkoff and M. Tretkoff. Solution of the inverse problem of differential Galois theory in the classical case. *Am. J. Math.*, 101:1327–1332, 1979.

[vdP99] M. van der Put. Galois theory of differential equations, algebraic groups and Lie algebras. *J. Symb. Comput.*, 28(4–5):441–472, 1999.