Fields Institute Communications
Volume **00**, 0000

Universal Covers and Category Theory in Polynomial and Differential Galois Theory

Andy R. Magid
Department of Mathematics
University of Oklahoma
Norman OK 73019

Abstract. The category of finite dimensional modules for the proalgebraic differential Galois group of the differential Galois theoretic closure of a differential field F is equivalent to the category of finite dimensional F spaces with an endomorphism extending the derivation of F. This paper presents an expository proof of this fact modeled on a similar equivalence from polynomial Galois theory, whose proof is also presented as motivation.

1 Introduction

We begin by recalling some notation, definitions, and standard results:

k denotes a field.

$K \supset k$ is a *splitting field*, or *polynomial Galois* extension, for the degree n monic separable polynomial

$$p = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad a_i \in k$$

if:

1. K is a field extension of k generated over k by $W = \{y \in K \mid p(y) = 0\}$("generated by solutions"); and

2. p is a product of linear factors in $K[X]$ ("full set of solutions").

For polynomial Galois extensions, let $G(K/k) = \mathrm{Aut}_k(K)$; note that $G(K/k) \rightarrow S_n(W)$ is an injection. Then we have the familiar Fundamental Theorem for polynomial Galois extensions:

1991 *Mathematics Subject Classification.* 12H05.

Research supported by the NSF under grant number DMS 0070748.

Theorem (*Fundamental Theorem for Polynomial Galois Extensions*) *Let $K \supset k$ be a polynomial Galois extension. Then $G = G(K/k)$ is a finite group and there is a one-one lattice inverting correspondence between subfields M, $K \supset M \supset k$, and subgroups H of G given by $M \mapsto G(K/M)$ and $H \mapsto K^H$. If M is itself a polynomial Galois extension, then the restriction map $G \to G(M/k)$ is a surjection with kernel $G(K/M)$. If H is normal in G, then K^H is an polynomial Galois extension.*

There is a completely analogous theory for differential fields:

F denotes a differential field of characteristic zero with derivation $D = D_F$ and algebraically closed field of constants C.

$E \supset F$ is a *Picard–Vessiot*, or *Differential Galois*, extension for an order n monic linear homogeneous differential operator

$$L = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y^{(1)} + a_0Y, \quad a_i \in F$$

if:

1. E is a differential field extension of F generated over F by $V = \{y \in E \mid L(y) = 0\}$ ("generated by solutions").

2. The constants of E are those of F ("no new constants").

3. $\dim_C(V) = n$ ("full set of solutions").

For Picard–Vessiot extensions, let $G(E/F) = \mathrm{Aut}_F^{\mathrm{diff}}(E)$; then $G(E/F) \to GL(V)$ is an injection with Zariski closed image.

There is a "Fundamental Theorem" for differential Galois extensions:

Theorem (*Fundamental Theorem for Picard–Vessiot Extensions*) *Let $E \supset F$ be a Picard–Vessiot extension. Then $G = G(E/F)$ has a canonical structure of affine algebraic group and there is a one-one lattice inverting correspondence between differential subfields K, $E \supset K \supset F$, and Zariski closed subgroups H of G given by $K \mapsto G(E/K)$ and $H \mapsto E^H$. If K is itself a Picard–Vessiot extension, then the restriction map $G \to G(K/F)$ is a surjection with kernel $G(E/K)$. If H is normal in G, then E^H is an Picard–Vessiot extension.*

There are Fundamental Theorems for infinite extensions as well:

Theorem (*Fundamental Theorem for Infinite Polynomial Galois Extensions*) *Let k be a field and let $K \supseteq k$ be a directed union of polynomial Galois field extensions of k. Then the group of automorphisms $G = G(K/k)$ has a canonical structure of topological (in fact profinite) group and there is a bijection between the the set of closed subgroups of G, and the set of subfields of K containing k, under which a subgroup H corresponds to the subfield K^H of K fixed element–wise by H and the subfield M corresponds to the subgroup $Aut_M(K)$ of G which fixes each element of M. If M is itself a union of polynomial Galois extensions, then the restriction map $G \to G(M/k)$ is a surjection with kernel $G(K/M)$. If H is (closed and) normal in G, then M^H is a union of polynomial Galois extensions.*

Theorem (*Fundamental Theorem for Infinite Picard–Vessiot Extensions*) *Let $E \supset F$ be a directed union of Picard–Vessiot extensions. Then the group of differential automorphisms $G = G(E/F)$ has a canonical structure of proaffine group and there is a one-one lattice inverting correspondence between differential subfields K, $E \supset K \supset F$, and Zariski closed subgroups H of G given by $K \mapsto G(E/K)$ and $H \mapsto E^H$. If K is itself an infinite Picard–Vessiot extension, then the restriction map $G \to G(K/F)$ is a surjection with kernel $G(E/K)$. If H is (Zariski closed and) normal in G, then K^H is an infinite Picard–Vessiot extension.* [5]

We shall call these theorems (and their finite dimensional versions stated previously) “Correspondence Theorem Galois Theory”. These theorems are about the pair consisting of the base field and the extension . There is a another aspect of Galois theory, which we will call “Universal Cover Galois Theory”, which focuses on the base field and hopes to understand all possible (polynomial or differential) Galois extensions of the base by constructing a closure (or universal cover) and looking at its group of automorphisms.

The field k has a *separable closure*, which can be defined as a union of polynomial Galois extensions of k such that every polynomial Galois extension of k has an isomorphic copy in it. (More generally, every algebraic separable extension of k embeds over k in a separable closure of k.)

For various reasons, the direct analogues of “algebraic closure” and its properties for differential Galois extensions do not hold. However, the following notion is of interest, and can be shown to exist [7]:

A *Picard–Vessiot closure* $E \supset F$ of F is a differential field extension which is a union of Picard–Vessiot extensions of F and such that every such Picard–Vessiot extension of F has an isomorphic copy in E.

For a differential field extension of F to embed in a Picard–Vessiot closure, it is necessary and sufficient that it have the same constants as F and be generated over F as a differential field by elements that satisfy monic linear homogeneous differential equations over F [8, Prop. 13].

As noted, the goal of what we are calling Universal Cover Galois Theory is produce the (profinite or proalgebraic) Galois group of the (polynomial or differential) universal cover of the base field. In the next section, we will see how this is done in the polynomial case, and then in the following how it is done in the differential case.

1.1 History and Literature. This is an expository article. Section 2 is basically an account of the special (one point) case of A. Grothendieck’s theory of Galois categories and the fundamental group. I learned this material from J. P. Murre’s account of it [9] which is still an excellent exposition. Differential Galois theory is the work of Ellis Kolchin [4]. For a comprehensive modern introduction, see M. van der Put and M. Singer [10]. The survey article by Singer [11] is also a good introduction. Less advanced are the author’s introductory expository lectures on the subject [6], which is a reference for much of the terminology used here. Section 3 is an account of a version of the Tannakian Categories methods in differential Galois Theory. This originated in work of P. Deligne [3]; there are explanations of this in both [11] and [10]. A compact explanation of the theory as well as how to do the Fundamental Theorem in this context is also found in D. Bertrand’s article

[1]. Information about the Picard–Vessiot closure is found in [7] and [8]. And of course the standard reference for Galois theory is categories is F. Borceaux and G. Janelidze [2].

2 The Galois Group of the Separable Closure

The Fundamental Theorems recalled above were called "Correspondence Theorem Galois Theory". Even in their infinite forms, they are just special cases of Categorical Galois Theory [2]. The point of view of Correspondence Theory is from the extension down to the base: somehow the extension has been constructed and the group of automorphisms obtained (if only in principle) and then the lattice of intermediate fields is equivalent to the lattice of subgroups.

Now the naive view of Galois theory, say the one often adopted by students, is often the opposite: the point of view is from the base up. Despite the fact that, as Aurelio Carboni for example has noted, Galois Theory is about *not* solving equations, not about solving equations, the base up point of view begins with the base field, the (polynomial or differential) equation and asks for the solutions. Even though this doesn't work, let us imagine how to conduct such a project. We will deal first with the polynomial situation.

Let $p = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be a separable polynomial over k which we will assume has no repeated irreducible factors (and hence no multiple roots). The set W of roots of p in a separable closure K of k has, by itself, only the structure of a finite set. The elements of W, however, are not completely interchangeable (remember we are taking the point of view of the base k): the elements of W are grouped according to the irreducible factor of p of which they are a root. Within these groupings they are interchangeable, but there are still limitations, namely any multivariable polynomial relations (with k coefficients) should be preserved as well. Of course the "interchanging" we are talking about is the action of the group $\pi_1(k) = G(K/k)$ on W.

(The reader will note the obvious circularity here: we are trying to describe the set of roots of p from the point of view of k, and to do so we introduce the separable closure and its group of k automorphisms. But this means that be have in principle found the roots not only of p but of every (separable) polynomial over of k!).

It is easy to check that the action of $\pi_1(k)$ on W is topological (which means simply that the stabilizers of points are open). And some natural questions arise, for example, do all finite sets with continuous $\pi_1(k)$ action come from polynomials over k, and if so, how? To take up the first, one should consider all finite sets with $\pi_1(k)$ action, and therefore the category $\mathcal{M}(\pi_1(k))$ of all of them, morphisms in the category being $\pi_1(k)$ equivariant maps. (It is a theorem of Grothendieck [9] that $\pi_1(k)$ can be recovered from $\mathcal{M}(\pi_1(k))$, as we will recall later.)

Now let us ask about how finite sets with continuous $\pi_1(k)$ action might come from polynomials. For the set $W = p^{-1}(0) \subset K$ we considered above, we could find p as $\prod_{\alpha \in W}(X - \alpha)$. But suppose we start with an arbitrary finite set X with continuous $\pi_1(k)$ action. If we want to repeat the above construction, then the first thing that should be considered is how to embedd X in K, $\pi_1(k)$ equivariantly of course . While we do not know if such a map even exists, it is clear that no one such should be privileged. Thus the natural thing is to consider the set of all $\pi_1(k)$

equivariant maps $X \to K$. This set is a ring, under pointwise operations on K, and is even a k algebra (the latter sitting in it as constant functions).

We use $C(X, K)$ to denote all the functions from X to K. Then the set $C(X, K)$ is a commutative k algebra under pointwise operations, and $\pi_1(k)$ acts on it via $\sigma \cdot \phi(x) = \sigma(\phi(\sigma^{-1}x))$. We consider the ring of invariants $C(X, K)^{\pi_1(k)}$, which is the ring of $\pi_1(k)$ equivariant functions from X to K. Suppose that ϕ is such a function and x is an element of X. Let $\{x = x_1, \ldots, x_n\}$ be the orbit of x and let H be the intersection of the stabilizers of the x_i. Note that H is closed and normal and of finite index in $\pi_1(k)$. Then all the $\phi(x_i)$ lie in $M = K^H$, which is a polynomial Galois extension of k. Since X is a finite union of orbits, it follows, by taking the compositum of such extensions for each orbit, that there is a finite, normal separable extension $N \supset k$ such that $C(X, K)^{\pi_1(k)} = C(X, N)^{\pi_1(k)}$. Now $C(X, N)$ is a finite product of finite, separable extensions of k, and it follows that its subalgebra $C(X, N)^{\pi_1(k)}$ is as well.

In other words, our search for a polynomial related to X led to a commutative k algebra which is a finite product of finite separable extensions of k. We consider the category of all such:

Let $\mathcal{A}(k)$ be the category whose objects are finite products of finite separable field extensions of k and whose morphisms are k algebra homomorphisms. From the discussion above, we have a contrafunctor

$$\mathcal{U} = C(\cdot, K)^{\pi_1(k)} : \mathcal{M}(\pi_1(k)) \to \mathcal{A}(k).$$

On the other hand, for any object $A = K_1 \times \cdots \times K_n$ in $\mathcal{A}(k)$, we can consider the set $\mathcal{V}(A) = \mathrm{Alg}_k(A, K)$. We have that $\mathcal{V}(A)$ is a finite set (its cardinality is the dimension of A as an k vector space) and there is a left $\pi_1(k)$ action on $\mathcal{F}(A)$, given by following an embeding by an automorphism of K. All the embedings of A into K lie in a fixed finite, separable, normal subextension $K_0 \supseteq k$ of K, and this implies that the action of $\pi_1(k)$ on $\mathcal{V}(A)$ is continuous. Thus we also have a contrafunctor

$$\mathcal{V} = \mathrm{Alg}_k(\cdot, K) : \mathcal{A}(k) \to \mathcal{M}(\pi_1(k))$$

to the category $\mathcal{M}(\pi_1(k))$ of finite sets with continuous $\pi_1(k)$ action.

We will see that $\mathcal{U}$ and $\mathcal{V}$ are equivalences of categories.

Here are some properties of the functor $\mathcal{V}$: if $K_0 \supseteq k$ is a finite separable extension, then $\mathcal{V}(K_0) = \mathrm{Alg}_k(K_0, K)$ has cardinality the dimension of K_0 over k. If $A = K_1 \times \cdots \times K_n$ is a finite product of finite separable extensions of k, then every homomorphism from A to a field must factor through a projection onto a K_i, so it follows that $\mathcal{V}(A)$ is the (disjoint) union $\mathcal{V}(K_1) \amalg \cdots \amalg \mathcal{V}(K_n)$ and hence has cardinality $\sum |\mathcal{V}(K_i)| = \sum \dim_k(K_i) = \dim_k(A)$. We also note that since K is the separable closure of k, $\mathcal{V}(A) = \mathrm{Alg}_k(A, K)$ is always non–empty.

And some properties of the functor $\mathcal{U}$: if X is a finite set with continuous $\pi_1(k)$ action and $X = X_1 \amalg X_2$ is a disjoint union of two proper $\pi_1(k)$ subsets, then the inclusions $X_i \to X$ induce maps $C(X, K) \to C(X_1, K)$ which in turn give an isomorphism $C(X, K) \to C(X_1, K) \times C(X_2, K)$. All these are $\pi_1(k)$ equivariant, and hence give an isomorphism $\mathcal{U}(X) \to \mathcal{U}(X_1) \times \mathcal{U}(X_2)$. Now suppose that X does not so decompose, which means that X is a single orbit, say of the element x with stabilizer H (which is, of course, closed and of finite index in $\pi_1(k)$). Then

$\pi_1(k)$ equivariant maps from X to K are determined by the image of x, which may be any element with stabilizer H. Thus $C(X,K)^{\pi_1(k)} \to K^H$ by $\phi \mapsto \phi(x)$ is a bijection. Combining this observation with the previous then yields the following formula for $\mathcal{U}$: If $X = X_1 \amalg \cdots \amalg X_n$ is a disjoint union of orbits with orbit representatives x_i with stabilizers H_i, then $\mathcal{U}(X) = \prod K^{H_i}$. The index of H_i in $\pi_1(k)$ is both the cardinality of X_i and the dimension of K^{H_i} over k, and it follows that $\dim_k(\mathcal{U}(X)) = |X|$. We also note that $\mathcal{U}(X) = \prod K^{H_i}$ is always non–zero.

Combining, we have cardinality/dimension equalities, $|\mathcal{U}(\mathcal{V}(X))| = |X|$ and $\dim_k(\mathcal{V}(\mathcal{U}(A)) = \dim_k(A)$

We also have "double dual" maps

$$A \to \mathcal{U}(\mathcal{V}(A)) = C(\mathrm{Alg}_k(A,K),K)^{\pi_1(k)} \text{ by } a \mapsto \hat{a}, \text{ where } \hat{a}(\tau) = \tau(a).$$

and

$$X \to \mathcal{V}(\mathcal{U}(X)) = \mathrm{Alg}_k(C(X,K)^{\pi_1(k)},K) \text{ by } x \mapsto \hat{x}, \text{ where } \hat{x}(\phi) = \phi(x).$$

It follows from the cardinality/dimension equalities that in the case that A is a field or X is a single orbit that the double dual maps are bijections, and then that they are bijections in general from the product formulae above.

The above remarks imply that the functors $\mathcal{U}$ and $\mathcal{V}$ give an (anti)equivalence of categories, a result which we now state as a theorem:

Theorem (*Categorical Classification Theorem*) *Let k be a field, let K be a separable closure of k and let $\pi_1(k) = Aut_k(K)$. Then $\pi_1(k)$ has a natural topological structure as a profinite group. Let $\mathcal{A}(k)$ denote the category of commutative k algebras which are finite products of finite separable field extensions of k and k algebra homomorphisms. Let $\mathcal{M}(\pi_1(k))$ denote the category of finite sets with continuous $\pi_1(k)$ action, and $\pi_1(k)$ equivariant functions. Consider the contravariant functors*

$$\mathcal{U} = C(\cdot,K)^{\pi_1(k)} : \mathcal{M}(\pi_1(k)) \to \mathcal{A}(k)$$

and

$$\mathcal{V} = Alg_k(\cdot,K) : \mathcal{A}(k) \to \mathcal{M}(\pi_1(k)).$$

Then both compositions $\mathcal{U}\circ\mathcal{V}$ and $\mathcal{V}\circ\mathcal{U}$ are naturally isomorphic to the identity using the double dual maps, and hence the categories $\mathcal{A}(k)$ and $\mathcal{M}(\pi_1(k))$ are equivalent.

The proofs of the assertions summarized as the Categorical Classification Theorem depended on the Fundamental Theorem of Galois Theorem. Conversely, the Categorical Classification Theorem can be used to prove the Fundamental Theorem:

Suppose $K_0 \supset k$ is a finite, normal, separable extension, and that $\tau : K_0 \to K$ is an embeding over k. By normality, $\mathcal{V}(K_0) = \mathrm{Alg}_k(K_0,K)$ is a single orbit, and the stabilizer H of τ is a closed normal subgroup of $\pi_1(k)$ with $\pi_1(k)/H$ isomorphic to $G = \mathrm{Aut}_k(K_0)$. Also, $\mathcal{V}(k) = \{\mathrm{id}_k\}$ is a final object. The transitive $\pi_1(k)$ sets X which fit into a diagram $\mathcal{V}(K_0) \to X \to \mathcal{V}(k)$ are the $\pi_1(k)$ sets between $\pi_1(k)/H$ and $\pi_1(k)/\pi_1(k)$, namely those of the form $\pi_1(k)/K$ where K is a closed subgroup of $\pi_1(k)$ containing H, and thus correspond one–one to subgroups of $\pi_1(k)/H$. The quotients of $\mathcal{V}(K_0)$ correspond, by $\mathcal{U}$, to the subobjects of E. Thus once the Categorical Classification Theorem is available, the Fundamental Theorem of Galois Theory (for finite field extensions) translates into the simple correspondence between (homogeneous) quotients of a finite homogeneous space and the subgroups of the transformation group. We state this result, noting that it implies the Fundamental Theorem of Galois Theory:

Theorem (Fundamental Theorem for Faithful Transitive G Sets) *Let G be a finite group and regard G as a finite set on which G acts transitively and with trivial stabilizers, and let e be the identity of G. Let Z be a one point set and $p : X \to Z$ a map. Then transitive G sets Y and classes of G equivariant surjective maps $q : G \to Y$ which factor through p are in one–one correspondence with subgroups H of G as follows: to the subgroup H, make correspond the G set G/H and the map $G \to G/H$ by $g \mapsto gH$; to the surjective G map $q : G \to X$, make correspond the stabilizer H of $q(e)$.*

3 The Galois Group of the Picard–Vessiot Closure

In the preceding section, we saw how the category $\mathcal{M}(\pi_1(k))$ of finite sets on which the profinite Galois group of the separable closure of k acts continuously was (anti)equivalent to a category of k algebras. And we recalled that for any profinite group, the category of finite sets on which it acts continuously determines it. A similar statement is true about proalgebraic groups: such a group is determined by the category of vector spaces (or modules) on which it acts algebraically (this is the general Tannaka Duality Theorem [3]). The group of differential automorphisms $\Pi(F) = G(E/F)$ of the Picard–Vessiot closure E of the differential field F is a proalgebraic group, and it is therefore natural to consider the analogue of the functors of the preceding section in the differential case.

Thus we consider the category $\mathcal{M}(\Pi(F))$ of finite dimensional, algebraic, $\Pi(F)$ modules, and the functor $\mathrm{Hom}_{\Pi(F)}(\cdot, E)$ defined on it. The proalgebraic group $\Pi(F)$ is over the field C of constants of F, and the vector spaces in $\mathcal{M}(\Pi(F))$ are over C. The field E is not a $\Pi(F)$ module, although of course $\Pi(F)$ acts on it, since not every element in E has a $\Pi(F)$ orbit that spans a finite dimensional C vector space. Those elements that do form an F subalgebra S of E, which is additionally characterized by the fact that it consists of the elements of E which satisfy a linear homogeneous differential equation over F (see [6, Prop. 5.1, p.61], and [8]). Any $\Pi(F)$ equivariant homomorphism from an algebraic $\Pi(F)$ module to E must have image in S, so the functor to be considered is actually $\mathcal{V}(U) = \mathrm{Hom}_{\Pi(F)}(U, S)$.

It is clear that $\mathcal{V}(U)$, for U an object of $\mathcal{M}(\Pi(F))$, is an abelian group under pointwise addition of of functions. It is also true that $\mathcal{V}(U)$ is an F vector space via multiplication in the range of functions. We will see below that $\mathcal{V}(U)$ is finite dimensional over F. The derivation D of E preserves S, and this derivation of S defines an operator, which we also call D, on $\mathcal{V}(U)$ as follows: let $f \in \mathcal{V}(U)$ and let $u \in U$. Then $D(f)(u)$ is defined to be $D(f(u))$. It is easy to check that D on $\mathcal{V}(U)$ is additive and in fact is C linear. It is not F linear, but we do have the following formula: for $\alpha \in F$ and $f \in \mathcal{V}(U)$, $D(\alpha f) = D(\alpha)f + \alpha D(f)$.

This suggests we consider the category $\mathcal{M}(F \cdot D)$ of finite dimensional F vector spaces V equipped with C linear endomorphisms D_V (usually abbreviated D) such that for $\alpha \in F$ and $v \in V$, $D(\alpha v) = D(\alpha)v + \alpha D(v)$, morphisms being F linear maps which commute with D action. We call objects of $\mathcal{M}(F \cdot D)$ *$F \cdot D$ modules*, and morphisms of $\mathcal{M}(F \cdot D)$ *$F \cdot D$ morphisms.* (Sometimes $F \cdot D$ modules are known as connections [11, 2.4.1 p.536].) The contrafunctor $\mathcal{V}$ sends all objects and morphisms $\mathcal{M}(\Pi(F))$ to $\mathcal{M}(F \cdot D)$ (we still have to establish that $\mathcal{V}(U)$ is always finite dimensional over F). We note that, except for the finite dimensionality, S is like an object in $\mathcal{M}(F \cdot D)$ in that it has an operator D satisfying the appropriate relation, and for an object in $\mathcal{M}(F \cdot D)$ we will use $\mathrm{Hom}_{F \cdot D}(V, S)$ to denote the F linear D preserving homomorphisms from V to S.

It is clear that $\mathrm{Hom}_{F \cdot D}(V, S)$ is an abelian group under pointwise addition of functions, and a C vector space under the usual scalar multiplication operation.

The group $\Pi(F)$ acts on $\mathrm{Hom}_{F \cdot D}(V, S)$: for $\sigma \in \Pi(F), T \in \mathrm{Hom}_{F \cdot D}(V, S)$, and $v \in V$, define $\sigma(T)(v) = \sigma(T(v))$. We will see later that $\mathrm{Hom}_{F \cdot D}(V, S)$ is a finite dimensional C vector space, and that the action of $\Pi(F)$ on it is algebraic. Thus we will have a contrafunctor $\mathcal{U}(V) = \mathrm{Hom}_{F \cdot D}(V, S)$ from $\mathcal{M}(F \cdot D)$ to $\mathcal{M}(\Pi(F))$.

The pair of functors $\mathcal{U}$ and $\mathcal{V}$, therefore, are the analogues for the differential Galois case of the corresponding functors in the polynomial Galois case. And we will see that, as in the polynomial Galois case, both $\mathcal{V}(\cdot)$ and $\mathcal{U}(\cdot)$ are equivalences.

We begin by describing the $\Pi(F)$-module structure of S, and for this we now fix the following notation:

Notation 1 *Let* Π *denote* $\Pi(F)$*, the differential Galois group of the Picard–Vessiot closure* E *of* F*, and let* Π^0 *denote its identity component and* $\overline{\Pi} = \Pi/\Pi^0$ *the profinite quotient. .*

We denote the algebraic closure of F by $\overline{F}$. We regard $\overline{F}$ as emdedded in S, where it is a Π submodule and, since also $\overline{F} = S^{\Pi^0}$, a $\overline{\Pi}$ module. Therefore, when we need to regard $\overline{F}$ as a trivial Π module we will denote it $\overline{F}_t$.

Proposition 1 *In Notation* (1)*,*

1. $\overline{F}_t \otimes_F S \cong \overline{F}_t \otimes_C C[\Pi]$ *as* $\overline{F}_t$ *algebras and* Π *modules*

2. $S \cong \overline{F} \otimes_C C[\Pi^0]$ *as* $\overline{F}$ *algebras and* Π^0 *modules*

Proof Statement (1) is the infinite version of Kolchin's Theorem, [9, Thm. 5.12, p.67]. Since E is also a Picard–Vessiot closure of $\overline{F}$, whose corresponding ring is S as an $\overline{F}$ algebra, statement (2) is Kolchin's Theorem as well. □

We can analyze the functor $\mathcal{V} : \mathcal{M}(\Pi) \to \mathcal{M}(F \cdot D)$ using the structural description of the preceding theorem: since $\mathcal{V}(U) = \mathrm{Hom}_{\Pi}(U, S)$ we have

$$\begin{aligned} \mathcal{V}(U) = \mathrm{Hom}_{\Pi}(U, S) &= (\mathrm{Hom}_{\Pi^0}(U, S))^{\overline{\Pi}} \\ &= (\mathrm{Hom}_{\Pi^0}(U, \overline{F} \otimes_C C[\Pi^0]))^{\overline{\Pi}} \\ &= (\overline{F} \otimes_C \mathrm{Hom}_{\Pi^0}(U, C[\Pi^0]))^{\overline{\Pi}} \qquad (\mathcal{V}\text{ factor}) \end{aligned}$$

(For the third equality of ($\mathcal{V}$ factor) we used the isomorphism of Proposition (1)(2), and for the final equality of ($\mathcal{V}$ factor), we used the fact that U was finite dimensional.)

Using the decomposition ($\mathcal{V}$ factor), it is a simple matter to see that $\mathcal{V}$ is exact:

Proposition 2 *The contrafunctor* $\mathcal{V} : \mathcal{M}(\Pi) \to \mathcal{M}(F \cdot D)$ *is exact. Moreover,* $\mathcal{V}(U)$ *is* F *finite dimensional with* $dim_F(\mathcal{V}(U)) = dim_C(U)$

Proof In ($\mathcal{V}$ factor), we have factored $\mathcal{V}$ as the composition of four functors: first the forgetful functor from Π modules to Π^0 modules, then $U \mapsto \mathrm{Hom}_{\Pi^0}(U, C[\Pi^0])$, $(\cdot) \mapsto \overline{F} \otimes_C (\cdot)$, and $(\cdot) \mapsto (\cdot)^{\overline{\Pi}}$. The first of these is obviously exact. For exactness of the second, we use that $C[\Pi^0]$ is an injective Π^0 module (in fact, for any finite dimensional algebraic Π^0 module W the map $\mathrm{Hom}_{\Pi^0}(W, C[\Pi^0]) \to (W)^*$ by evaluation at the identity is a C isomorphism to the C linear dual of W). The third functor is also obviously exact. Since our modules are over a field of characteristic zero, taking invariants by a profinite group is also exact, and hence the final functor is exact as well.

To compute dimensions, we note that $\dim_F(\mathcal{V}(U)) = \dim_{\overline{F}}(\mathcal{V}(U) \otimes_F \overline{F})$, then that $\mathcal{V}(U) \otimes_F \overline{F} = \mathrm{Hom}_\Pi(U, S) \otimes_F \overline{F} = \mathrm{Hom}_\Pi(U, \overline{F}_t \otimes_F S)$, and by Proposition (1)(1), this latter is $\mathrm{Hom}_\Pi(U, \overline{F}_t \otimes_C C[\Pi]) = \mathrm{Hom}_\Pi(U, C[\Pi]) \otimes_C \overline{F} = U^* \otimes_C \overline{F}$, which has the same dimension over $\overline{F}$ as U does over C. □

Now we turn to the functor $\mathcal{U} = \mathrm{Hom}_{F \cdot D}(\cdot, S)$, and we will see that it also is exact and preserves dimensions. For both of these, we will need a few comments about cyclic $F \cdot D$ modules:

Remark 1 *An $F \cdot D$ module W is* cyclic*, generated by x, if W is the smallest $F \cdot D$ submodule of W containing x. For any $F \cdot D$ module V and any element $x \in V$, the F span of its derivatives $\sum_{i \geq 0} FD^i(x)$ is a cyclic $F \cdot D$ module, generated by x. If $n = dim_F(V)$, and $\{D^0 x, D^1 x, \ldots, D^{k-1} x\}$ is a maximal linearly independent set, then there are elements $\alpha_i \in F$ with $D^k x + \alpha_{k-1} D^{k-1} x + \cdots + \alpha_0 D^0 x = 0$. Note that $k \leq n$. We refer to the differential operator $L = Y^{(k)} + \alpha_{k-1} Y^{(k-1)} + \cdots + \alpha_0 Y$ as the* differential operator corresponding to *x in V.*

Now we turn to exactness of $\mathcal{U}$

Proposition 3 *The contrafunctor $\mathcal{U} : \mathcal{M}(F \cdot D) \to \mathcal{M}(\Pi)$ is exact.*

Proof Since $\mathcal{U}$, being a "Hom into" functor, is right exact, what we need to show is that it carries monomorphisms $V_1 \to V_2$ into epimorphisms. We can assume that the monomorphism is an inclusion and that V_2 is generated over V_1 by a single element x (that is, that V_2 is the sum of V_1 and the cyclic submodule of V_2 generated by x.) We suppose given an $F \cdot D$ morphism $T_1 : V_1 \to S$. We consider the symmetric algebras over F on V_1 and V_2, which we denote $F[V_1]$ and $F[V_2]$. The D operators on the V_i extend to derivations of the $F[V_i]$, and T_1 extends to a differential homomorphism $h : F[V_1] \to S$. We have $F[V_1] \subset F[V_2]$ (this is split as a extension of polynomial algebras over F), and $F[V_2]$ is generated over $F[V_1]$ as a differential algebra by x, which is denoted $F[V_2] = F[V_1]\{x\}$. We will also use h for the extension of h to the quotient field E of S. Let P be the kernel of h, let $\overline{F[V_1]} = F[V_1]/P$ and let $\overline{F[V_2]} = F[V_2]/PF[V_2]$. (Since $PF[V_2]$ is a differential ideal, this latter is a differential algebras.) If $\overline{x}$ denotes the image of x in $\overline{F[V_2]}$, then $\overline{F[V_2]} = \overline{F[V_1]}\{\overline{x}\}$. Now we extend scalars to E:

$$R = E \otimes_{\overline{F[V_1]}} \overline{F[V_1]}\{\overline{x}\}.$$

Note that R is finitely generated as an algebra over E. This implies that if Q is any maximal differential ideal of R, then the quotient field K of R/Q is a differential field extension of E with the same constant field C [6, Cor. 1.18, p. 11]. By construction, K is generated over E as a differential field by the image y of $\overline{x}$. Now x, and hence $\overline{x}$ and y, is the zero of a linear differential operator L of order k, the operator corresponding to x defined above in Remark (1). On the other hand, E already contains a Picard–Vessiot extension of F for L, and hence a full set of zeros of L (that is, of dimension k over C). Since K has no new constants, the zero y of L must belong to this set and hence $y \in E$. But this then implies $K = E$. Thus we have a differential F algebra homomorphism $f : F[V_2] \to \overline{F[V_2]} \to R \to R/Q \to E$, and by construction f restricted to $F[V_1]$ is h. Moreover, the image y of x lies in S (since it satisfies a differential equation over F) and hence f has image in S. Finally, the restriction T_2 of f to V_2 is an $F \cdot D$ morphism from V_2 to S extending $T_1 : V_1 \to S$. It follows that $\mathcal{U}$ is left exact, as desired. □

Using exactness, we can also show how $\mathcal{U}$ preserves dimension:

Proposition 4 *$\mathcal{U}(V)$ is C finite dimensional with $dim_C(\mathcal{U}(V)) = dim_F(V)$*

Proof By Proposition (3), $\mathcal{U}$ is exact, and since dimension is additive on exact sequences, we can reduce to the case that the $F{\cdot}D$ module V is cyclic with generator x. Then, by Remark (1), V has F basis $\{D^0x, D^1x, \dots, D^{k-1}x\}$ and corresponding linear operator $L = Y^{(k)} + \alpha_{k-1}Y^{(k-1)} + \cdots + \alpha_0 Y$. Then an $F \cdot D$ morphism $V \to S$ is determined by the image of x, which is an element of S sent to zero by L, and every such element of S determines a morphism. Thus $\mathcal{U}(V)$ is the zeros of L in S, which is the same as the zeros of L in E. Since E contains a Picard–Vessiot extension of F for L, and hence a complete set of solutions, we have $\dim_C(\mathcal{U}(V)) = \dim_C(L^{-1}(0)) = k = \dim_F(V)$. □

Both $\mathcal{U}$ and $\mathcal{V}$ involve a "duality" into S, and hence a "double duality" which we now record, and use to prove that the functors are equivalences.

Theorem 1 1. *The function $V \to \mathcal{V}(\mathcal{U}(V)) = Hom_\Pi(Hom_{F.D}(V,S),S)$ by $v \mapsto \hat{v}$, $\hat{v}(T) = T(v)$ is an $F \cdot D$ isomorphism natural in V.*

2. *The function $U \to \mathcal{U}(\mathcal{V}(U)) = Hom_{F.D}(Hom_\Pi(U,S),S)$ by $u \mapsto \hat{u}$, $\hat{u}(\phi) = \phi(u)$ is a Π isomorphism natural in U.*

In particular, $\mathcal{U}$ and $\mathcal{V}$ are category equivalences between the categories $\mathcal{M}(F{\cdot}D)$ and $\mathcal{M}(\Pi(F))$.

Proof We leave to the reader to check that the maps $v \mapsto \hat{v}$ and $u \mapsto \hat{u}$ are well defined and natural in V and U. To see that they are isomorphisms, we use the fact that $\mathcal{V} \circ \mathcal{U}$ and $\mathcal{U} \circ \mathcal{V}$ are exact to reduce to the case of checking the isomorphism for non–zero simple modules, and then use the fact that $\mathcal{V} \circ \mathcal{U}$ and $\mathcal{U} \circ \mathcal{V}$ preserve dimension to reduce to showing that both double dual maps are non–zero. For (1), this means that there is a non–zero $T \in \mathrm{Hom}_{F.D}(V,S) = \mathcal{U}(V)$. But since $\dim_C(\mathcal{U}(V)) = \dim_F(V) \neq 0$, this holds. For (2), this means that there is a non–zero $\phi \in \mathrm{Hom}_\Pi(U,S) = \mathcal{V}(U)$. Since $\dim_F(\mathcal{V}(U)) = \dim_C(U) \neq 0$, this holds as well. Thus the theorem is proved. □

Theorem (1) tells us that the category of $\Pi(F)$ modules is equivalent to the category of $F{\cdot}D$ modules. As we mentioned above, the proalgebraic group $\Pi(F)$ can be recovered from its category of modules $\mathcal{M}(\Pi(F))$ by the Tannaka Duality. We review this construction briefly: a *tensor automorphism* of $\mathcal{M}(\Pi(F))$ is a family of vector space automorphisms $\sigma_U, U \in |\mathcal{M}(\Pi(F))|$, one for each object in $\mathcal{M}(\Pi(F))$, such that

1. For any $\Pi(F)$ homomorphism $\phi : U \to U'$ we have $\sigma_{U'}\phi = \phi\sigma_U$, and

2. For any $\Pi(F)$ modules U and U', we have $\sigma_{U \otimes U'} = \sigma_U \otimes \sigma_{U'}$

An example of a tensor automorphism is $\mathrm{Id}_U, U \in |\mathcal{M}(\Pi(F))$.

The composition of tensor automorphisms are tensor automorphisms (composition of $\sigma_U, U \in |\mathcal{M}(\Pi(F))|$. and $\tau_U, U \in |\mathcal{M}(\Pi(F))|$ is $\sigma_U \tau_U, U \in |\mathcal{M}(\Pi(F))|$) and so are inverses, and the tensor automorphism $\mathrm{Id}_U, U \in |\mathcal{M}(\Pi(F))|$ is an identity for composition. Thus the tensor automorphisms form a group, denoted $\mathrm{Aut}_\otimes(\Pi(F))$. For notational convenience, we will denote the element of $\mathrm{Aut}_\otimes(\Pi(F))$ given by $\sigma_U, U \in |\mathcal{M}(\Pi(F))|$ simply as σ

If $U \in |\mathcal{M}(\Pi(F))|$, and $u \in U$ and $f \in U^*$, then we can define a function $m_{u,f}$ on $\mathrm{Aut}_\otimes(\Pi(F))$ by $m_{u,f}(\sigma) = f(\sigma_U(u))$. The C algebra of all such functions is denoted $C[\mathrm{Aut}_\otimes(\Pi(F))]$. One shows, as part of Tannaka Duality, that $C[\mathrm{Aut}_\otimes(\Pi(F))]$ is the coordinate ring of a proalgebraic group structure on $\mathrm{Aut}_\otimes(\Pi(F))$.

For any $g \in \Pi(F)$ and any $U \in |\mathcal{M}(\Pi(F))|$, let $L(g)_U$ denote the left action of g on U. Then $L(g)_U, U \in |\mathcal{M}(\Pi(F))|$ is a tensor automorphism, and $L : \Pi(F) \to \mathrm{Aut}_\otimes(\Pi(F))$ is a group homomorphism. Tannaka duality proves that L is actually a group isomorphism (of proalgebraic groups). Thus the proalgebraic group $\Pi(F)$ is recovered from the category $\mathcal{M}(\Pi(F))$ modules. (This procedure works for any proalgebraic group.)

Because of the importance of the tensor product in the Tannaka Duality, we record how the tensor products in $\mathcal{M}(F \cdot D)$ and $\mathcal{M}(\Pi)$ interact with the functors $\mathcal{U}$ and $\mathcal{V}$.

Proposition 5 *There are natural (and coherent) isomorphisms*

1. $\mathcal{V}(U_1) \otimes_F \mathcal{V}(U_2) \to \mathcal{V}(U_1 \otimes_C U_2)$, *and*

2. $\mathcal{U}(V_1) \otimes_C \mathcal{U}(V_2) \to \mathcal{U}(V_1 \otimes_F V_2)$.

Proof The map in (1) is defined as follows: if $\phi_i \in \mathrm{Hom}_\Pi(U_i, S)$, then $\phi_1 \otimes_F \phi_2$ is sent to the function in $\mathrm{Hom}_\Pi(U_1 \otimes_C U_2, S)$ given by $u_1 \otimes u_2 \mapsto \phi_1(u_1)\phi_2(u_2)$. Since $\mathcal{V}(U_1) \otimes_F \mathcal{V}(U_2)$ and $\mathcal{V}(U_1 \otimes_C U_2)$ have the same dimension over F (namely that of $U_1 \otimes_C U_2$ over C), to see that the map is an isomorphism it suffices to see that it is injective. To that end, we tensor it over F with $\overline{F}_t$. Then we consider successively:

$$(\mathrm{Hom}_\Pi(U_1, S) \otimes_F \mathrm{Hom}_\Pi(U_2, S)) \otimes_F \overline{F}_t \to \mathrm{Hom}_\Pi(U_1 \otimes_C U_2, S) \otimes_F \overline{F}_t$$

we distribute $\overline{F}_t$ over the tensors and inside the Hom's

$$(\mathrm{Hom}_\Pi(U_1, S) \otimes_F \overline{F}_t) \otimes_{\overline{F}_t} (\mathrm{Hom}_\Pi(U_2, S)) \otimes_F \overline{F}_t) \to \mathrm{Hom}_\Pi(U_1 \otimes_C U_2, S \otimes_F \overline{F}_t)$$

then we apply Proposition (1) (1)

$$\mathrm{Hom}_\Pi(U_1, \overline{F}_t \otimes_C C[\Pi]) \otimes_{\overline{F}_t} \mathrm{Hom}_\Pi(U_2, \overline{F}_t \otimes_C C[\Pi])) \to \mathrm{Hom}_\Pi(U_1 \otimes_C U_2, \overline{F}_t \otimes_C C[\Pi])$$

and finally use that spaces of Π maps into $C[\Pi]$ are duals

$$(\mathrm{Hom}_C(U_1, \overline{F}_t) \otimes_{\overline{F}_t} \mathrm{Hom}_C(U_2, \overline{F}_t) \to \mathrm{Hom}_C(U_1 \otimes_C U_2, \overline{F}_t).$$

And this final map is, of course, an isomorphism. This proves (1).

The map in (2) is defined similarly: if $T_i \in \mathrm{Hom}_{F \cdot D}(V_i, S)$ then $T_1 \otimes_F T_2$ is sent to the function in $\mathrm{Hom}_{F \cdot D}(V_1 \otimes V_2, S)$ given by $v_1 \otimes v_2 \mapsto T_1(v_1)T_2(v_2)$.

To prove (2), we may assume that $V_i = \mathcal{V}(U_i)$, so we are trying to show that $\mathcal{U}(\mathcal{V}(U_1)) \otimes_C \mathcal{U}(\mathcal{V}(U_2)) \to \mathcal{U}(\mathcal{V}(U_1) \otimes_F \mathcal{V}(U_2))$ is an isomorphism. Note that the domain is, by Theorem (1) (2), $U_1 \otimes_C U_2$. On the other hand, if we apply $\mathcal{V}$ to (1), then we have an isomorphism $\mathcal{U}(\mathcal{V}(U_1 \otimes_C U_2)) \to \mathcal{U}(\mathcal{V}(U_1) \otimes_F \mathcal{V}(U_2))$. Here again, by Theorem (1) (2) the domain is $U_1 \otimes_C U_2$. It is a simple matter to check that both maps are the same, and hence conclude (2). □

4 Conclusion

We try to set some of the above in perspective. We consider the problem of understanding the proalgebraic differential Galois group $\Pi(F)$ of a Picard–Vessiot closure of F. By Tannaka Duality, $\Pi(F)$ is determined by and recoverable from its category $\mathcal{M}(\Pi(F))$ of finite dimensional over C algebraic modules – the tensor product over C in $\mathcal{M}(\Pi(F))$ being an essential part of the structure. The (anti)equivalence $\mathcal{U}$ and its inverse $\mathcal{V}$ show that the category $\mathcal{M}(F \cdot D)$ of finite dimensional F spaces with an endomorphism compatible with the derivation on F is (anti)equivalent to the category $\mathcal{M}(\Pi(F))$. In other words, we might say that every finite dimensional $F \cdot D$ module has a "secret identity" as a $\Pi(F)$ module (more appropriately, perhaps, a "dual secret identity", since the equivalences are contravariant). And this identification includes converting tensors over F of $F \cdot D$ modules into tensors over C for $\Pi(F)$ modules. It follows, at least in principle, that the group $\Pi(F)$ is determined by, and determines, the category of $F \cdot D$ modules. So everything that could be learned about F from the group $\Pi(F)$ can be learned by studying $F \cdot D$ modules.

We would also like to tie this observation about differential Galois theory with our earlier discussion of polynomial Galois theory. In that case, we began by considering sets of solutions of polynomial equations in isolation, that is, simply as finite sets, and then found that the structure necessary to tell these "disembodied sets of solutions" from unstructured finite sets was an action of the Galois group of the separable closure. In the same way, modules for the differential Galois group are like "disembodied sets of solutions" for differential equations. But unlike the situation with the polynomial equations, where duality with respect to the closure leads from solution sets to extension fields (actually finite products of extension fields), in the differential case duality with respect to the closure lead from solution spaces to $F \cdot D$ modules, which are more like "disembodied differential equations" (see Remark (1)) than extensions. There is a way to pass from $F \cdot D$ modules to extensions (we saw some of this construction in the proof of Proposition (3)): for an $F \cdot D$ module V, we form the F symmetric algebra $F[V] = S_F[V]$. This F algebra has a derivation extending that of F, and if we mod out by a maximal differential ideal Q we obtain a differential F integral domain whose quotient field has the same constants as F. One can then show that this domain embeds in a Picard–Vessiot closure of F [8, Prop. 13], and in particular into a Picard–Vessiot extension of F. Different choices of Q are possible, of course. But each arises from a differential F algebra homomorphism from $F[V]$ to the Picard–Vessiot closure of F and hence from differential F algebra homomorphisms $F[V] \to S$. (Since these latter correspond to $F \cdot D$ module homomorphisms $V \to S$, we see our functor $\mathcal{U}$.) One should regard the whole collection of these homomorphisms, or at least all their images, as the corresponding object to the (finite product of) field extensions in the polynomial case.

References

[1] Bertrand, D. *Review of Lectures on Differential Galois Theory by A. Magid*, Bull. (New Series) Amer. Math. Soc. **33** (1966) 289–294.

[2] Borceau, F. and Janelidze, G. *Galois Theories*, Cambridge Studies in Advanced Mathematics **72**, Cambridge University Press, Cambridge, 2001.

[3] Deligne, P. *Catégories tannakiennes* in Carties P., et. al, eds, Grothendieck Festschrift, Vol. 2, Progress in Mathematics **87**, Birkhauser, Boston, 1990, 111–195.

[4] Kolchin, E. *Selected Works*, Amer. Math. Soc., Providence, 1999.

[5] Kovacic, J. *Pro-algebraic groups and the Galois theory of differential fields*, Amer. J. Math. **95** (1973), 507–536.

[6] Magid, A. *Lectures on Differential Galois Theory*, University Lecture Series **7**, American Mathematical Society, Providence RI, 1997 (second printing with corrections).

[7] Magid, A. *The Picard-Vessiot Antiderivative Closure*, J. of Algebra **244** (2001), 1–18.

[8] Magid, A. *The Picard–Vessiot closure in differential Galois theory* in Diferential Galois Theory, Banach Center Publications **58**, Polish Academy of Sciences, Warsaw, 2002, 157–164.

[9] Murre, J. P. *Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group*, Tata Institute of Fundamental Research, Bombay, 1967.

[10] van der Put, M. and Singer, M. *Differential Galois Theory* Springer–Verlag, New York, 2003.

[11] Singer, M. *Direct and inverse problems in differential Galois theory* in H. Bass et al, eds, Selected Works of Ellis Kolchin with Commentary, Amer. Math. Soc., Providence, 1999, 527–554.