Interpretations and differential Galois extensions.

Moshe Kamensky
Ben-Gurion University of the Negev
email: kamensky@math.bgu.ac.il

Anand Pillay*
University of Notre Dame
email: apillay@nd.edu

December 10, 2015

Abstract

We give accounts and proofs, using model-theoretic methods among other things, of the following results: Suppose $\partial y = Ay$ is a linear differential equation over a differential field K of characteristic 0, and the field C_K of constants of K is existentially closed in K. Then: (i) There exists a Picard-Vessiot extension L of K, namely a differential field extension L of K which is generated by a fundamental system of solutions of the equation, and has no new constants. (ii) If L_1 and L_2 are two Picard Vessiot extensions of K which (as fields) have a common embedding over K into an elementary extension of C_K, then L_1 and L_2 are isomorphic over K as differential fields. (iii) Suppose that C_K is *large* in the sense of Pop [21] and also has only finitely many extensions of degree n for all n (Serre's property (F)). Then K has a Picard-Vessiot extension L such that C_K is existentially closed in L.

In fact we state and prove our results in the more general context of logarithmic differential equations over K on (not necessarily linear)

*Partial support from MSRI and NSF

algebraic groups over C_K, and the corresponding *strongly normal* extensions of K. We make use of interpretations from model theory as well the Galois groupoid, which are related to the Tannakian theory in [3] and [4], but go beyond the linear context. Towards the proof of (iii) we obtain a Galois-cohomological result of possibly independent interest: if k is a field of characteristic 0 with property (F), and G is any algebraic group over k, then $H^1(k, G)$ is countable.

The current paper replaces the preprint [8] which only dealt with the linear differential equations case and had some mistakes.

1 Introduction

Let K be a differential field of characteristic 0 with field of constants C_K, and let $\partial y = Ay$ be a (homogeneous) linear differential equation over K (in vector form). Namely y is a $n \times 1$ column vector of indeterminates and A is an $n \times n$ matrix over K. If L is a differential field extension of K then the solution set of the equation in L is a vector space over C_L of dimension at most n. A *fundamental system of solutions* of this equation, in a differential field L extending K, is by definition a set $Y_1, ..., Y_n$ of solutions in L which form a basis of the C_L-vector space of solutions (which thus has maximal dimension). It is well known that linear independence of $Y_1, .., Y_n$ over C_L is equivalent to the $n \times n$ matrix over L whose columns are $Y_1, .., Y_n$ being nonsingular. In any case by a Picard-Vessiot (or PV) extension of K for the equation we mean a differential field extension L of K which is generated over K by such a fundamental system $Y_1, .., Y_n$ of solutions, and has *no new constants*, i.e. $C_L = C_K$. When C_K is algebraically closed it is well-known that such a PV extension of K exists and is moreover unique up to isomorphism over K (and is generated over K by some/any fundamental system of solutions in the *differential closure* K^{diff} of K, bearing in mind that $C_{K^{diff}} = C_K^{alg} = C_K$). In general ($C_K$ algebraically closed or not) we can always find a fundamental system of solutions in K^{diff}, and the question is whether we can find such a fundamental system Z such that the constants of $K(Z)$ coincide with C_K. Moreover one can ask for uniqueness: for another such Z_1, $K(Z_1)$ is isomorphic to $K(Z_2)$ over K. In general one has neither existence nor uniqueness. Some recent papers [5], [2] give sufficient conditions for the existence of PV-extensions possibly with additional properties, and also uniqueness under additional constraints: In [5] the existence is proved

when C_K is existentially closed in K (as fields). In [2] it is shown that if C_K is a real closed field and K is a formally real field then a formally real PV-extension of K exists, and moreover two formally real extensions of K which are compatible (have common embeddings over K in a common real closed extension of K) are isomorphic over K, as differential fields. Likewise in the p-adic case. These results use the full strength of the theory of Tannakian categories [3] and [4]. The aim of the current paper is to give an account of these results and more, at a somewhat greater level of generality, to which the Tannakian theory, as such, does not apply.

We now discuss logarithmic differential equations on algebraic groups and "strongly normal extensions". The general theory of strongly normal extensions of differential fields was introduced by Kolchin in [10] and further developed in Chapter VI of his book [9]. Another exposition with a scheme-theoretic flavour appears in [11]. Strongly normal extensions of a differential field K generalize Picard-Vessiot extensions of K. In this introduction and in sections 3 and 4 we give an exposition of this theory from the point of view of logarithmic differential equations on algebraic groups, analogous to the way the Picard-Vessiot theory is introduced above via linear differential equations. This point of view appears briefly in Section 7, Chapter VI of [9] on "G-Primitives". However objects such as the"intrinsic" Galois group H^+ described in section 3, and the Galois groupoid, described in section 4, do not make an appearance in the afore-cited works, although they do appear in more general forms in the model-theoretic literature (such as [18], [7]). This explains our somewhat extended exposition.

We start to assume familiarity with differential algebra in the style of Kolchin [9], and in particular with the notion of the differential closure K^{diff} of a differential field K and the fact that the field of constants of K^{diff} is the algebraic closure of the field of constants of K. The reader is also referred to [14] and [15] for basic model theory and the model theory of differential fields. Fix K as above (an arbitrary differential field of characteristic 0) and let G be an algebraic group over C_K which we will take to be connected. By a logarithmic differential equation on G over K, we mean something of the form $(\partial y)y^{-1} = A$ for some $A \in LG(K)$ (where LG denotes the Lie algebra of G), where y ranges over G (i.e. over L-points of G for L any differential field containing K). Here $(\partial y)y^{-1}$ is Kolchin's logarithmic derivative, a crossed homomorphism from G to its Lie algebra, which can be explained as follows: For $g \in G(L)$, ∂g can be considered as a point in the the tangent space to G at g. The tangent bundle TG of G is an algebraic group which splits as the

semidirect product of G and LG. Identifying g with the point $(g, 0)$ of TG, both ∂g and g are points of TG_g so their difference $(\partial g)g^{-1}$ lies in LG.

We will write $dlog_G(-)$ for this logarithmic derivative map from G to LG, where G is an algebraic group over C_K (namely for any differential field L containing K, $dlog_G$ takes $G(L)$ to $LG(L)$). Of course $dlog_G(g) = A$ if and only if $\partial g = Ag$ where the right hand side is multiplication in the sense of the algebraic group TG. We typically write the group operation on LG additively. $dlog_G$ being a crossed homomorphism means that $dlog_G(gh) = dlog_G(g) + (dlog_G(h))^g$. The kernel of $dlog_G$, $\{g : dlog_G(g) = 0\}$ is a subgroup and its points in any differential field $L > K$ coincide with $G(C_L)$. For any $A \in LG$, $\{g \in G : dlog_G(g) = A\}$ is a left coset of the kernel.

When $G = GL_n$, then $dlog_G$ actually coincides with multiplication of matrices $(\partial y)y^{-1}$ in gl_n. When G is an elliptic curve in Weierstrass form the logarithmic derivative coincides with $\partial y/x$. Returning to GL_n we note that if $g \in GL_n(L)$ and A is an $n \times n$ matrix over K and $(\partial g)g^{-1} = A$ then the columns of g form a fundamental system of solutions for the linear differential equation $\partial y = Ay$. Hence seeking a solution of a logarithmic differential equation on an algebraic group G is a generalization of seeking a fundamental system of solutions for a (homogeneous) linear differential equation. The generalization of the notion of Picard-Vessiot extension to this broader class of equations is what is called a "strongly normal" extension. We will present below Kolchin's original definition from [9] so as to keep our notations consistent with the literature. We will work in a "universal differential field" $\mathcal{U}$ (in the sense of Kolchin, or of model theory), and $K, L, ..$ will denote small differential subfields unless we say otherwise. $\mathcal{C}$ denotes the field of constants of $\mathcal{U}$ and C_K the field of constants of K.

Definition 1.1. *Let K, L be differential fields with L finitely generated over K. L is said to be a strongly normal extension of K if*
(i) for each isomorphic copy L_1 of L over K in $\mathcal{U}$, $L_1 \subseteq L(\mathcal{C})$ (the differential field generated over L by $\mathcal{C}$), and
(ii) $C_L = C_K$.

Including (ii) in the definition (as Kolchin does) makes for consistency with the notion of Picard-Vessiot extension. The following is well-known (at least to model theorists, see for example Section 5 of [19]). See also Theorem 6 of Chapter VI of [9].

Remark 1.2. *Suppose $dlog_G(y) = A$ is a logarithmic differential equation on G over K where G is over C_K. Let g be a solution of the equation in $G(\mathcal{U})$*

and let $L = K(g)$ be the (differential) field generated over K by g. Then
(a) Condition (i) in Definition 1.1 is automatically satisfied, as any two solutions differ by an element of $G(\mathcal{C})$.
(b) If L is a strongly normal extension of K (namely condition (ii) is also satisfied) then L is contained in some differential closure of K.
(c) Conversely if L is contained in some differential closure of K and C_K is algebraically closed, then L is a strongly normal extension of K.
(d) As we can always find a solution of $dlog_G(y) = A$ in a differential closure of K, (c) gives the existence of a strongly normal extension of K generated by a solution of the equation, when C_K is algebraically closed.
(e) When C_K is algebraically closed, there is a unique (as differential field, up to isomorphism over K) strongly normal extension of K generated by a solution of $dlog_G(y) = A$.

Remark 1.2 (a) justifies us calling L a *strongly normal extension of K for the equation $dlog_G(y) = A$*, if L is generated over K by a solution $g \in G(L)$ of the equation, and $C_L = C_K$.

From the model-theoretic point of view the question of the existence of such L is an *almost orthogonality* statement: we seek a solution $y \in G(\mathcal{U})$ of the equation such that $tp(y/K)$ has a unique extension to a complete type over $K\mathcal{C}$.

We are here focusing on strongly normal extensions generated by certain kinds of differential equations. But this is close to the general case; see Section 10 of [9] on V-primitives, and our results can suitably be extended to these logarithmic differential equations on principal homogeneous spaces for algebraic groups over the constants.

There is a Galois theory of strongly normal extensions generalizing the linear case. But from our point of view the relevant Galois group intrinsic to the equation $dlog_G(y) = A$ is the group of automorphisms of $K(\mathcal{C})(\mathcal{Y})$ over $K(\mathcal{C})$, where $\mathcal{Y}$ is the solution set of $dlog_G(y) = A$ in $G(\mathcal{U})$, and where the automorphisms should respect the derivation. This is discussed more in section 3.

If $M \subseteq N$ are structures for a common language L, M is said to be existentially closed in N if any quantifier-free formula over M with a solution in N has a solution in M. When we are concerned with fields $K \leq L$ (of characteristic 0 say) in the language of unitary rings, this is equivalent to asking that any algebraic variety V over K (not necessarily affine or irreducible) with an L-rational point, has a K-rational point. M being existentially closed in

N is equivalent to each of the following
(i) N is a model of the universal part of the complete diagram of M,
(ii) N embeds over M into an elementary extension of M.

We now state the main results, as well as giving some comments on the proofs. A logarithmic differential equation

(*) $dlog_G(y) = A$

is fixed in advance, where G is a connected algebraic group over C_K and $A \in LG(K)$.

Theorem 1.3. *Suppose C_K is existentially closed in K (as a field). Then there is a strongly normal extension L of K for the equation (*).*

The idea is as follows. In Section 2 we prove an interpretability result which is roughly that the solution set $\mathcal{Y}$ of (*) in the differentially closed field $\mathcal{U}$, equipped with all relations definable over K in $\mathcal{U}$, is (canonically) interpretable in ACF_K (theory of algebraicallly closed fields with constants for elements of K). Strictly speaking we are interpreting the *theory* of the two sorted structure $(\mathcal{C}, \mathcal{Y})$. We call this interpretation ω. In Section 3 we show that there is a (quantifier-free) formula $O(x)$ in the language of fields with parameters from C_K such that among other things the solutions of $O(x)$ in C_K parametrize the set of strongly normal extensions of K for the given equation (*). Properties of O together with the interpretation ω from Section 2, show that $O(x)$ has a solution in K, so as C_K is existentially closed in K, $O(x)$ has a solution in C_K yielding the desired strongly normal extension of K.

The remainder of the results consist of uniqueness and existence theorems when we demand additional properties of the strongly normal extension L . It is natural to ask for C_K to be also existentially closed in L, so for example if C_K is real closed then we can choose L to be formally real. First the uniqueness theorem, proved in Section 4.

Theorem 1.4. *Suppose that L_1 and L_2 are strongly normal extensions of K for (*) such that there is a common embedding over K of L_1 and L_2 into an elementary extension of C_K (as fields). Then L_1 and L_2 are isomorphic over K (as differential fields).*

The idea of the proof is similar to that of Theorem 1.3. First the field-definable (over C_K) set O obtained earlier is shown to be the set of objects of

the Galois groupoid $\mathcal{G}$ (definable in ACF over C_K) attached to the equation (*). In the same way as the points a of O in C_K parametrize strongly normal extensions of K, morphisms between such points parametrise isomorphisms over K between the corresponding strongly normal extensions. To prove Theorem 1.4, we show that if the strongly normal extensions L_1, L_2 of K correspond to $a_1, a_2 \in O(C_K)$, then the (definable over C_K) set $Mor(a_1, a_2)$ of morphisms between a_1 and a_2 has a point in some elementary extension of C_K (using the interpretation ω), hence has a C_K-point. The above theorem subsumes Theorem 1.2 (2), (3) of [2].

Finally here is the (strong) existence statement, proved in Section 5.

Theorem 1.5. *Suppose again C_K is existentially closed in K. Suppose that C_K is* large *in the sense of [21] and also has only finitely many extensions of degree n for each n (Serre's property (F)). Then there is a strongly normal extension L of K for (*) such that C_K is existentially closed in L.*

Large fields were introduced by Florian Pop, and we refer the reader to his recent survey paper [21] for the basic results and examples. The definition of k being large is that any k-irreducible curve over k with a nonsingular k-point has infinitely many k-points. An equivalent statement (see Proposition 2.6 of [21]) is that any irreducible k-variety with a nonsingular k-point has a Zariski-dense set of k-points. Real closed and p-adically closed fields are large, hence, as they also have property (F), Theorem 1.5 includes the existence result Theorem 1.2 (1) of [2]. Here is a sketch of the proof of Theorem 1.5. First for any $a \in O(C_K)$ there is a smooth variety X_a over K such that the strongly normal extension L of K determined by a is, as a field equal to $K(X_a)$ the function field of X_a over K. If X_a has a point in an elementary extension K_1 of C_K containing K then it will follow from largeness of K_1 that C_K is existentially closed in $L = K(X_a)$. Now the interpretation ω gives rise to $a' \in O(K)$ such that $X_{a'}$ has a K-point. The key issue is to find $a \in O(C_K)$ such that $Mor(a', a)$ has a point in K_1 , giving rise to a K_1-point of X_a as required. This is done by showing, using the (F) property, that $\mathcal{G}(C_K)$ has only finitely many connected components. And this in turn is a consequence of the following result of possibly independent interest (our (Theorem 5.2):
Let k be a field of characteristic 0 with the (F) property. Let G be an algebraic group over k. Then $H^1(k, G)$ is countable.

The notions of Picard-Vessiot and strongly normal extensions of differential fields and their automorphism groups, are a special case of a phenomenon widely studied in model theory, namely "internality" and definable automorphism groups (also called "liason" or "binding" groups). This was initiated by Zilber, with subsequent refinements by Poizat, Hrushovski, and others, including the current authors. Poizat [19] in particular made clear the connection of the general model theoretic constructions with differential Galois theory. A kind of culmination of the model-theoretic perspective appears in [7] where not only a definable automorphism group but also a definable automorphism groupoid, is attached to an "internal cover". This point of view will be present throughout the current paper, but in the concrete context of logarithmic differential equations.

As already mentioned we will assume familiarity with basic model theory from say [14], as well as some basic model theory of differentially closed fields which can be found in [15]. We will on the whole be using elementary model theory, as we aim to give presentation and proofs of the main theorems which will be accessible to a broad audience, including differential algebraists. The exposition is on purpose rather heavy handed, so as to be relatively self-contained and so that a differential algebraist can see the point of view if they so wish. In several places we could have quoted references rather than re-introduce objects ourselves, but the notation may have been different, the references obscure, or, as in the case of the strongly normal theory, the only references are at much greater model-theoretic level of generality. In Section 5 we assume some familiarity with Galois cohomology for which there are of course very elegant sources. We use the expressions "principal homogeneous space" and "torsor" interchangeably.

Our model-theoretic notation is standard. The main complete theories we consider are ACF_0 (theory of algebraically closed fields of characteristic 0 in the language of unitary rings), DCF_0 (theory of differentially closed fields of characteristic 0 in the language of unitary rings with a derivation), and various reducts. Both ACF_0 and DCF_0 are complete with quantifier elimination in their respective languages. For T a complete theory in language L and A a substructure of a model M of T, T_A denotes the complete theory of $(M, a)_{a\in A}$ the expansion of M by adjoining constants for elements of A. When T has quantifier elimination, T_A depends only on T and the isomorphism type of A. When we talk about definability in a given structure M, we allow parameters and try to make it explicit by saying A-definable, $\emptyset$-definable etc...

Concerning DCF_0, we often work in an ambient "saturated" differentially closed field $\mathcal{U}$ with field $\mathcal{C}$ of constants. We will make use of the following fact, which although well-known to model-theorists, is somewhat subtle and related to stablility theoretic phenomena:

Fact 1.6. *Suppose that F is a differentially closed field, and K is a differential subfield. Then the subsets of Cartesian powers of C_F which are definable with parameters from K in the structure $(F, +, -, \times, 0, 1, \partial)$ are precisely the sets definable with parameters from C_K in the field $(C_F, +, -, 0, 1, \times)$.*

Proof. There is no harm in assuming F to be saturated, and let $\mathcal{C}$ denote its field of constants C_F. Firstly, by quantifier elimination for DCF_0, any subset of $\mathcal{C}^n$ definable (without parameters) in the differential field F is definable (without parameters) in the field $\mathcal{C}$.
Secondly stability of DCF_0 implies that any subset of $\mathcal{C}^n$ definable *with parameters* in the differential field F, is definable *with parameters from* $\mathcal{C}$ in the differential field F.
Putting these two points together, given a subset X of $\mathcal{C}^n$ definable in the differential field F with parameters d from K, there is a formula $\phi(x, e)$ in the language of fields and with parameters e from $\mathcal{C}$ such that X is defined in the field $\mathcal{C}$ by $\phi(x, e)$. So far we have just observed that the field $\mathcal{C}$ is (so-called) *stably embedded* in the differential field F. Now we may assume, by elimination of imaginaries in ACF_0 that e is a canonical parameter for the definable set X in the field $\mathcal{C}$. Now in the saturated differential field F any automorphism which fixes d, fixes X as a set, and hence fixes e. So $e \in dcl(d)$ in the differential field F. But the field K is definably closed in F (again by quantifier elimination), so as d is in K, so is e. Namely $e \in C_K$. So X is definable over C_K in the field $\mathcal{C}$. □

Of course a special case, which is the first step of the proof is that the field of constants of a differentially closed field F with all its "induced structure" is just an algebraically closed field. But we also obtain the following consequence (which the referee pointed out can also be seen from the fact that K and $\mathcal{C}$ are linearly disjoint over their intersection):

Corollary 1.7. *Suppose that K is a (small) differential subfield of $\mathcal{U}$, and that C is a subfield of $\mathcal{C}$ containing C_K. Then the field of constants of the (differential) field $K(C)$ generated by K and C is precisely C.*

Proof. Let $c \in \mathcal{C}$. Then c is a constant of $K(C)$ iff $c \in dcl(K, C)$ in the sense of DCF_0 which by Fact 1.6 is equivalent to $c \in dcl(C)$ in the structure $(\mathcal{C}, +, -, 0, 1, \times)$ expanded by parameters from C_K. But as $C_K \leq C$ this last statement is equivalent to $c \in C$. □

We will use freely facts such as that a definable over k group in an ambient algebraically closed field has a unique structure of algebraic group over k. Also where necessary that a definable (in ACF) subgroup of an algebraic group is an algebraic subgroup. Sometimes we will mention constants in the sense of logic, namely constant symbols, which should not be confused with constants in a differential field.

Acknowledgement. Thanks to the referees, whose reports led to a substantial rewriting of the paper.

2 Interpretations

To a logarithmic differential equation over K we can and will attach a two-sorted structure $(\mathcal{C}, \mathcal{Y})$ consisting of the constants $\mathcal{C}$, and the solution set $\mathcal{Y}$ of the equation, in an ambient differentially closed field, equipped with all relations which are definable over K in the differentially closed field $\mathcal{U}$. The main point of this section is to show that this structure, or rather its first order theory, is interpretable in a rather special way in ACF_K the theory of algebraically closed fields of characteristic 0 with constant symbols for elements of K. Our interpretation result is related to "quantifier-elimination for algebraic ∂-groups" from [12] which implies that the theory of any finite-dimensional differential algebraic group is interpretable in the theory of algebraically closed fields. However in our situation we are dealing with a torsor for a definable group rather than the group itself, which requires a few additional words. On the other hand the relevant definable groups are living in the constants already, yielding simplifications. In any case we cannot simply refer to [12] for our main result, although we will make use of some lemmas from that paper.

The reader is referred to Section 5.3 of [6], Section 3.1 of [16], and Section 9.4 of [20] for the notion of an interpretation of one structure in another structure, and to page 196 in [13] for the (syntatic) notion of the interpretation of a language in another language. We are interested in the related

notion of an interpretation of one theory in another theory, so we give some definitions suitable for our purposes and for establishing notation.

First let L_1, L_2 be possibly many sorted languages which we assume to be relational for simplicity. An interpretation ω of L_1 in L_2 is an assignment, to each sort S of L_1 a formula $\omega(S)$ of L_2. and to each L_1-symbol R, an L_2-formula $\omega(R)$ (appropriately sorted). Note that such an interpretation gives rise, for each formula ϕ of L_1, to a formula $\omega(\phi)$ of L_2. Moreover if ϕ is a sentence, so is $\omega(\phi)$.

Such an interpretation ω also acts on structures: if M is an L_2-structure, then we we obtain an L_1-structure whose sorts are the $\omega(S)(M)$ (interpretation of the formula $\omega(S)$ in M) and relations the $\omega(R)(M)$, and we call this L_1-structure $\omega^*(M)$. So we obtain an interpretation of the L_1-structure $\omega^*(M)$ in M in the sense of the earlier references.

Now suppose that T_1 and T_2 are L_1 and L_2-theories respectively, which need not be complete, and let ω be an interpretation of L_1 in L_2. Then we say that ω is an *interpretation of* T_1 *in* T_2 if for every $\sigma \in T_1$, $\omega(\sigma) \in T_2$. This is *equivalent* to saying that for every model M of T_2, $\omega^*(M)$ is a model of T_1. If T_1 and T_2 happen to be complete theories, then an interpretation of T_1 in T_2 in our sense is determined by (and determines) an interpretation of *some model* M_1 of T_1 in some model M_2 of T_2 (with $M_1 = \omega^*(M_2)$). In any case if T_1 is interpretable in T_2 and M_1 is a model of T_1 then there will be an elementary extension M_1' of M_1 which is of the form $\omega^*(M_2)$ for some model M_2 of T_2.

We now fix, once and for all, the data consisting of a logarithmic differential equation
(*) $dlog_G(y) = A$
where G is a connected algebraic group over C_K, and $A \in LG(K)$.

We will fix a differentially closed field $\mathcal{U}$ containing K. In later sections we may want to apply compactness and so will choose $\mathcal{U}$ to be saturated, but in this section there is no harm in taking $\mathcal{U}$ to be the differential closure K^{diff} of K. Let $\mathcal{C}$ be the field of constants of $\mathcal{U}$ and let $\mathcal{Y}$ be the solution set of (*) in $\mathcal{U}$, namely $\{y \in G(\mathcal{U}) : dlog_G(y) = A\}$. As mentioned earlier $Ker(dlog_G) = G(\mathcal{C})$, and $\mathcal{Y}$ is the left coset (so right torsor) $bG(\mathcal{C})$ for some/any $b \in \mathcal{Y}$.

Let M be $(\mathcal{C}, \mathcal{Y})$ equipped with all relations which are definable over K in $\mathcal{U}$, so a 2-sorted structure. Let $L(M)$ be the language of M, namely with symbols for all these relations. We will show that we can make $(\mathcal{U}, G(\mathcal{U}))$ into an $L(M)$-structure N say in such a way that

(i) $M \prec N$, and
(ii) All the relations on N are definable over K in the algebraically closed field $(\mathcal{U}, +, \cdot)$.

This will yield the interpretation we are looking for. Note that by definition of the language $L(M)$ of M, the subsets of $\mathcal{C}^n$ definable (without parameters) in the structure M are by definition the subsets of $\mathcal{C}^n$ definable over K in the differential field $\mathcal{U}$. Hence by Fact 1.6:

Remark 2.1. *The subsets of $\mathcal{C}^n$ which are $\emptyset$-definable in M are precisely the subsets definable over C_K in the algebraically closed field $(\mathcal{C}, +, \cdot)$.*

To facilitate the construction and proof we will choose some auxiliary languages: $L_{\partial,\mathcal{U}}$ and $L_{\partial,K}$, the languages of (algebraic) ∂-varieties over $\mathcal{U}$ and ∂-varieties over K, respectively (with respect to the "connections" or differential equations $\partial(y) = Ay$ on G, and $\partial(x) = 0$ on $\mathcal{U}$). We refer to [12] for more details and/or background. The reader may also want to refer to Section 4 of [17], in particular the proof of Proposition 4.1, for parts of Remark 2.3 below.

Definition 2.2. *(i) By a ∂-subvariety of $\mathcal{U}^n \times G(\mathcal{U})^m$ (over $\mathcal{U}$), we mean an algebraic subvariety X over $\mathcal{U}$, such that $X^\partial =_{def} X \cap (\mathcal{C}^n \times \mathcal{Y}^m)$ is Zariski-dense in X.*
(ii) $L_{\partial,\mathcal{U}}$ is the language with symbols R_X for each such ∂-subvariety, and $L_{\partial,K}$ is the sublanguage consisting of the R_X where X is defined over K.
(iii) $(\mathcal{U}, G)_{L_{\partial,\mathcal{U}}}$ is the $L_{\partial,\mathcal{U}}$ structure with sorts $\mathcal{U}$ and G, and with the tautological interpretations of the R_X. Similarly for $(\mathcal{U}, G)_{L_{\partial,K}}$
(iv) $(\mathcal{C}, \mathcal{Y})_{L_{\partial,\mathcal{U}}}$ is the $L_{\partial,\mathcal{U}}$-structure with sorts $\mathcal{C}$ and $\mathcal{Y}$ and with X^∂ as the interpretation of R_X. Similarly for $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$

Note that according to our definition, a ∂-variety is a special case of an algebraic variety, so definable in algebraically closed fields. Note also that the *structure* $(\mathcal{U}, G)_{L_{\partial,K}}$ is interpretable in the structure $(\mathcal{U}, +, \times, -, 0, 1, a)_{a \in K}$. Analogously for the structure $(\mathcal{U}, G)_{L_{\partial,\mathcal{U}}}$.

Remark 2.3. *(i) The class of ∂-subvarieties of the various Cartesian powers $\mathcal{U}^n \times G(\mathcal{U})^m$ is closed under finite unions, finite intersections, Cartesian products, and passing to irreducible components.*
(ii) If A is a Boolean combination of ∂-subvarieties of $\mathcal{U}^n \times G(\mathcal{U})^m$, then $A^\partial =_{def} A \cap (\mathcal{C}^n \times \mathcal{Y}^m)$ is Zariski-dense in A.

(iii) The ∂-subvarieties of $\mathcal{U}^n$ are precisely the subvarieties defined over $\mathcal{C}$.
(iv) The $\emptyset$-definable sets in the structure $M = (\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ above are precisely the Boolean combinations of the X^∂ for X a ∂ -subvariety defined over K, so from now on we identify M with the $L_{\partial,K}$-structure on $(\mathcal{C}, \mathcal{Y})$. In particular the structure $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ has quantifier-elimination.

Proof. (i) and (ii) are contained in Facts 2.2, Fact 2.3, and Lemma 2.5 of [12]. (iii) is obvious, and (iv) follows from quantifier elimination in DCF_0. □

Lemma 2.4. *The structure $(\mathcal{U}, G)_{L_{\partial,\mathcal{U}}}$ has quantifier elimination.*

Proof. Let us fix a point $d \in \mathcal{Y}$. Let f be translation by d^{-1}, taking G to G. f induces a bijection between $\mathcal{Y}$ and $G(\mathcal{C})$. So for any subvariety X of G, $X \cap \mathcal{Y}$ is Zariski-dense in X if and only if $G(\mathcal{C})$ is Zariski-dense in $f(X)$ if and only if $f(X)$ is defined over $\mathcal{C}$. More generally, fixing n and m,
(**) a subset Z of $\mathcal{U}^n \times G^m$ is a ∂-subvariety if and only if $(id^n, f^m)(Z)$ is a subvariety of $\mathcal{U}^n \times G^m$ which is defined over $\mathcal{C}$.
Now let $W \subseteq \mathcal{U}^n \times G^m$ be ∂-constructible, namely a Boolean combination of ∂-varieties over $\mathcal{U}$. Then (id^n, f^m) is a Boolean combination of subvarieties of $\mathcal{U}^n \times G^m$ which are defined over $\mathcal{C}$. Let π be any projection of $\mathcal{U}^n \times G^m$ onto some coordinate axes, say onto $\mathcal{U}^{n'} \times G^{m'}$. Then by quantifier elimination in algebraically closed fields (rather than differentially closed fields), $\pi \circ (id^n, f^m)(W)$ is also a Boolean combination of subvarieties of $\mathcal{U}^{n'} \times G^{m'}$ defined over $\mathcal{C}$. Applying $(id^{n'}, f^{m'})$ and using (**), we see that $\pi(W)$ is a Boolean combination of ∂-subvarieties of $\mathcal{U}^{n'} \times G^{m'}$, as required. □

Corollary 2.5. *The structure $(\mathcal{U}, G)_{L_{\partial,K}}$ has quantifier elimination.*

Proof. Let $X \subseteq \mathcal{U}^n \times G^m$ be a Boolean combination of ∂-varieties which are defined over K, and let π be some projection on coordinate axes. We have to show that $\pi(X)$ is a Boolean combination of ∂-varieties defined over K. By Lemma 2.4, $\pi(X)$ is a Boolean combination of ∂-varieties which are defined over $\mathcal{U}$, and clearly, $\pi(X)$, as a definable set in $(\mathcal{U}, +, \cdot)$ is invariant under K-automorphisms, as is its Zariski closure $\overline{\pi(X)}$. So it suffices to prove that if $Y \subseteq \mathcal{U}^{n'} \times G^{m'}$ is a Boolean combination of ∂-varieties over $\mathcal{U}$ and is also K-invariant, then Y is a Boolean combination of ∂-varieties over K. And this follows by induction on the dimension of the Zariski closure of Y: by 2.3, $\overline{Y}$ is a ∂-variety, and as it is K-invariant, is a ∂-variety over K. So $\overline{Y} \setminus Y$ is a Boolean combination of ∂-varieties and is K-invariant, so by induction hypothesis is a Boolean combination of ∂-varieties over K. Hence so is Y. □

Corollary 2.6. *$(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ is an elementary substructure of $(\mathcal{U}, G)_{L_{\partial,K}}$*

Proof. First note that by definition $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ is a substructure of $(\mathcal{U}, G)_{L_{\partial,K}}$. Now suppose that Z is a nonempty definable set in $(\mathcal{U}, G)_{L_{\partial,K}}$, defined with parameters from $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$. So Z is definable by a formula $\phi(x, c)$ where c is a tuple from $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$, and $\phi(x, z)$ is a formula in $L_{\partial,K}$. By Definition 2.2(i) the tuple c is itself a (0-dimensional) ∂-variety. By 2.4 (or 2.5), $\phi(x, z)$ defines a Boolean combination of ∂-varieties. By 2.3 (i) (in particular closure under intersections) $\phi(x, z) \wedge z = c$ defines a Boolean combination of ∂-varieties. So by Lemma 2.4, the projection of this set on the x-coordinate, which is precisely Z, is a Boolean combination of ∂-varieties. By 2.3(ii), Z has a point in $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$. The result follows (Tarski-Vaught). □

We deduce immediately:

Theorem 2.7. *The map assigning to each relation symbol $R_X \in L_{\partial,K}$ the formula (over K) defining X in $(\mathcal{U}, +, -, \times, 0, 1)$ is an interpretation of $Th((\mathcal{C}, \mathcal{Y})_{L_{\partial,K}})$ in ACF_K, and we call this interpretation ω.*

Finally we explain how Corollary 2.6 and Theorem 2.7 will be used in practice. Suppose that Z is a $\emptyset$-definable set in the structure $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$. Then Z is defined by an $L_{\partial,K}$-formula ψ say. We let $\omega(Z)$ denote the interpretation of the formula $\omega(\psi)$ in the algebraically closed field $\mathcal{U}$. So $\omega(Z)$ is definable over K in the field $\mathcal{U}$. Moreover $\omega(Z)$ coincides as a set with the interpretation of ψ in the structure $(\mathcal{U}, G(\mathcal{U}))_{L_{\partial,K}}$. One of the main special cases is where Z is defined by the relation symbol R_X with X a ∂-variety over K, in which case $\omega(Z)$ is precisely X. We extend this notation to sets Z definable in $(\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ with parameters. Again a special case is where Z is defined by R_X for X a ∂-variety over $K \cup \mathcal{C} \cup \mathcal{Y}$, in which case $\omega(Z)$ is again X.

Note that if Z happens to be the set of $\mathcal{C}$ points of an algebraic variety defined over $\mathcal{C}$ then $\omega(Z)$ is precisely the set of $\mathcal{U}$-points of that variety. So we write $\omega(Z)$ as $Z(\mathcal{U})$. Likewise if Z is a constructible subset of some $\mathcal{C}^m$.

Give this notation, we will use 2.6 to transfer facts expressed by first order sentences, from $(\mathcal{C}, \mathcal{Y})$ to the algebraically closed field $\mathcal{U}$.

3 The Galois group and the proof of Theorem 1.3

We remain in the general setup of the previous section, namely a connected algebraic group G over C_K, and a logarithmic differential equation $dlog_G(-) = A$ over K, and again we take $\mathcal{Y}$ to be the solution set in $\mathcal{U}$, an ambient differentially closed field extending K, which we will now take to be saturated. $\mathcal{C}$ denotes the constants of $\mathcal{U}$ as before. Note that $\mathcal{Y}$ is a subset of $G(\mathcal{U})$ and as noted earlier is also a left coset $bG(\mathcal{C})$ of $G(\mathcal{C})$.

By $Aut(\mathcal{Y}/K(\mathcal{C}))$ we mean the group of permutations of $\mathcal{Y}$ induced by automorphisms of $\mathcal{U}$ which fix $K(\mathcal{C})$ pointwise. Equivalently, via quantifier-elimination it is the simply the group of automorphisms of the differential field $K(\mathcal{C})(\mathcal{Y})$ which fix the differential subfield $K(\mathcal{C})$ pointwise.

We will work in the structure $\mathcal{U}$ (as a differential field). The aim (accomplished in Lemma 3.4) is to obtain a K-definable function f from $\mathcal{Y}$ to $\mathcal{C}^m$ (some m) such that for each $b \in \mathcal{Y}$, b is "constrained over $K(\mathcal{C})$" by some differential equations and inequations over $K(f(b))$. Or in model-theoretic notation $tp(b/K(\mathcal{C}))$ is isolated by a formula over $K(f(b))$. It will follow that $C_{K(b)} = C_{K(f(b))}$ as also noted in Lemma 3.4 below.

Lemma 3.1. *$\mathcal{Y}$ is contained in any differential closure of $K(\mathcal{C})$ in $\mathcal{U}$. In particular for all $b \in \mathcal{Y}$, $tp(b/K(\mathcal{C}))$ is isolated.*

Proof. Let us fix a solution $b_1 \in \mathcal{Y}$ in some differential closure K_1 of $K(\mathcal{C})$ in $\mathcal{U}$. Any other $b \in \mathcal{Y}$ differs from b_1 by an element of $G(\mathcal{C})$ so is also in K_1. □

We first describe the "intrinsic" Galois group of the equation (*) (which does *not* appear explicitly in the differential algebraic literature on strongly normal extensions).

Lemma 3.2. *Let $b \in \mathcal{Y}$ and $\sigma \in Aut(\mathcal{Y}/K(\mathcal{C}))$. Then $\sigma(b)b^{-1}$ (multiplication in the group G) does not depend on b*

Proof. Let b_1 be another element of $\mathcal{Y}$. As $\mathcal{Y}$ is a left coset of $G(\mathcal{C})$ there is $d \in G(\mathcal{C})$ such that $b = b_1 d$. Applying σ we get $\sigma(b) = \sigma(b_1)d$. So $\sigma(b)b^{-1} = \sigma(b_1)dd^{-1}b_1^{-1} = \sigma(b_1)b_1^{-1}$. □

Lemma 3.3. *(i) The map ρ from $Aut(\mathcal{Y}/K(\mathcal{C}))$ to G taking σ to $\sigma(b)b^{-1}$ (for some/any $b \in \mathcal{Y}$) is an isomorphism between $Aut(\mathcal{Y}/K(\mathcal{C}))$ and a definable*

over K subgroup H^+ of G.
(ii) This is also an isomorphism of group actions where the action of H^+ on $\mathcal{Y}$ is by left multiplication in G (so $\mathcal{Y}$ is a union of right cosets of H^+).

Proof. (i) By Lemma 3.2, $\rho(\sigma) = \sigma(b)b^{-1}$ does not depend on the choice of $b \in \mathcal{Y}$. Given $\sigma, \tau \in Aut(\mathcal{Y}/K(\mathcal{C})$, and $b \in \mathcal{Y}$, let $b_1 = \tau(b)$. So $\rho(\sigma\tau) = \sigma\tau(b)b^{-1} = \sigma(b_1)b_1^{-1}b_1b = \sigma(b_1)b_1^{-1}\tau(b)b^{-1} = \rho(\sigma)\rho(\tau)$. So ρ is a homomorphism. If $\sigma(b) = b$ then clearly σ is the identity, so σ is an isomorphism with its image, which we call H^+. Now H^+ is definable, for example as $\{yb^{-1} :\models \phi_b(y)\}$ where $\phi_b(y)$ isolates $tp(b/K(\mathcal{C}))$. As H^+ is also invariant under $Aut(\mathcal{U}/K)$ it is defined over K.
(ii) $\sigma(b) = \sigma(b)b^{-1}b$.

□

Hence we see that the group $Aut(\mathcal{Y}/K(\mathcal{C}))$ together with its action, is definable over K in the differentially closed field $\mathcal{U}$. In particular it is a differential algebraic subgroup of G.

We now construct the function $f : \mathcal{Y} \to \mathcal{C}^m$, definable over K in $\mathcal{U}$. In fact the key object will be the set $\mathcal{Y}/H^+$ of *right* cosets of H^+ in $\mathcal{Y}$, equivalently orbits under the action of H^+ on $\mathcal{Y}$ by left multiplication in G. $\mathcal{Y}/H^+$ is interpretable over K in $\mathcal{U}$. Note also that $\mathcal{Y}/H^+$ is fixed pointwise by $Aut(\mathcal{U}/K(\mathcal{C}))$. So by compactness and elimination of imaginaries in DCF_0, $\mathcal{Y}/H^+$ is in definable (over K) bijection with a K-definable subset of $\mathcal{C}^m$ which we call O. By Fact 1.6, O is definable over C_K in the algebraically closed field $\mathcal{C}$. In other words we have a K-definable map f from $\mathcal{Y}$ onto a C_K-definable subset O of $\mathcal{C}^m$ such that for $b_1, b_2 \in \mathcal{Y}$, $f(b_1) = f(b_2)$ iff $b_1 = hb_2$ for some $h \in H^+$. This f is the required function. Here are some of its properties:

Lemma 3.4. *(i) Let $a \in O$. Then the formula "$y \in \mathcal{Y}$" $\wedge f(y) = a$ isolates a complete type over $K(\mathcal{C})$, which of course is $tp(b/K(\mathcal{C}))$ for some/any $b \in \mathcal{Y}$ such that $f(b) = a$.*
(ii) For any $a \in O$ and b with $f(b) = a$, the field of constants of the (differential) field $K(b)$ is precisely $C_K(a)$.
(iii) In particular if $a \in O(C_K)$, namely has coordinates in C_K and $f(b) = a$, then $K(b)$ is a strongly normal extension of K (for the equation (*)).

Proof. (i) By definition as well as Lemma 3.3, $f^{-1}(a)$ is an orbit under $Aut(\mathcal{Y}/K(\mathcal{C})$ so all elements of $f^{-1}(a)$ have the same type over $K(\mathcal{C})$.

(ii) Note that as $a = f(b)$ and f is definable over K, $a \in K(b)$, so $a \in C_{K(b)}$ (or rather the coordinates of a are in $C_{K(b)}$). Conversely, suppose d is a constant in $K(b)$. So $d = g(b)$ for some K-definable function g and $d \in \mathcal{C}$. By (i) the following sentence (over $K(a)$) is true in $\mathcal{U}$:
$\forall y \in \mathcal{Y}(f(y) = a \rightarrow g(y) = d)$. Hence $d \in dcl(K(a)) = K(a)$ so is a constant in $C_{K(a)}$ which equals $C_K(a)$ by 1.7.
(iii) follows immediately from (ii). □

Conclusion of proof of Theorem 1.3.
Let f be the function we have just constructed. So f is $\emptyset$-definable in the structure $M = (\mathcal{C}, \mathcal{Y})_{L_{\partial,K}}$ discussed in Section 2. We have already remarked that the image O is definable (so constructible) over C_K in the algebraically closed field $\mathcal{C}$. We now apply the interpretation ω, or more precisely Corollary 2.6, as described at the end of Section 2. $\omega(O)$ is just $O(\mathcal{U})$, the interpretation of the field formula defining O in $\mathcal{U}$. Let $F = \omega(f)$. Then $F : G \rightarrow O(\mathcal{U})$ is definable over K in the algebraically closed field $\mathcal{U}$. In particular, as the identity e of G has coordinates in C_K, $F(e) \in O(K)$. So $O(K) \neq \emptyset$. As O is definable over C_K and C_K is existentially closed in K (as fields), $O(C_K)$ is nonempty. By Lemma 3.4 (iii), this gives rise to a strongly normal extension of K for the given logarithmic differential equation.

4 The Galois groupoid and proof of Theorem 1.4

We elaborate on the map $f : \mathcal{Y} \rightarrow O$ defined in the previous section. For $a \in O$ we write $\mathcal{Y}_a$ for the fibre $f^{-1}(a)$. We feel free to identify H^+ (acting by left multiplication on $\mathcal{Y}$) with $Aut(\mathcal{Y}/K(\mathcal{C}))$. Multiplication is always meant in the sense of the ambient group G.

Definition 4.1. *For $a_1, a_2 \in O$, let $H_{a_1,a_2} = \{b_1^{-1}b_2 : b_1 \in \mathcal{Y}_{a_1}, b_2 \in \mathcal{Y}_{a_2}\}$.*

Remark 4.2. *Given $a_1, a_2 \in O$, fix $b_1 \in \mathcal{Y}_{a_1}$ and fix $b_2 \in \mathcal{Y}_{a_2}$. Then $H_{a_1,a_2} = \{b_1^{-1}b : b \in \mathcal{Y}_{a_2}\} = \{b^{-1}b_2 : b \in \mathcal{Y}_{a_1}\}$.*

Proof. Let $c \in \mathcal{Y}_{a_1}$, and $b \in \mathcal{Y}_{a_2}$, then using the definition of f, $b_1c^{-1} \in H^+$, and hence $b_1c^{-1}b = d \in \mathcal{Y}_{a_2}$, whereby $c^{-1}b = b_1^{-1}d$ as required. Similarly for the second equality.

□

We write H_a for $H_{a,a}$ and record some key facts.

Lemma 4.3. *(i) H_{a_1,a_2} is a subset of $G(\mathcal{C})$ which is definable over C_K, a_1, a_2 in the algebraically closed field $\mathcal{C}$ and uniformly so (as a_1, a_2 vary).*
(ii) For any $a_1, a_2 \in O$ and $c \in H_{a_1,a_2}$ (right) multiplication by c defines a bijection between $\mathcal{Y}_{a_1}$ and $\mathcal{Y}_{a_2}$.
(iii) For $a \in O$, H_a is a group, and for any $b \in \mathcal{Y}_a$, $bH_a = \mathcal{Y}_a = H^+b$, whereby $bH_ab^{-1} = H^+$.
(iv) For $a \in O$ and $b \in \mathcal{Y}_a$, the map taking σ to $b^{-1}\sigma(b)$ is a group isomorphism between $Aut(\mathcal{Y}/K(\mathcal{C}))$ and H_a.
(v) For any $a_1, a_2, a_3 \in O$, $H_{a_1,a_3} = H_{a_1,a_2} \cdot H_{a_2,a_3} =_{def} \{cd : c \in H_{a_1,a_2}, d \in H_{a_2,a_3}\}$. In particular H_{a_1,a_2} is a right coset (or left torsor) of H_{a_1} and left coset (right torsor) of H_{a_2}

Proof. For (i), note that $\{(a_1, a_2, c) : a_1, a_2 \in O,\ c \in H_{a_1,a_2}\}$ is a subset of a suitable Cartesian power of $\mathcal{C}$ which is definable in the differentially closed field $\mathcal{U}$ over K. So apply 1.6 to see that this set is definable in the algebraically closed field $\mathcal{C}$ over C_K which is precisely the meaning of statement (i). The rest of the Lemma, although very important, consists of easy computations, using the definitions and Remark 4.2 where needed. □

Remark 4.4. *For $a \in O$, H_a is of course an algebraic subgroup of $G(\mathcal{C})$ and is the "usual" Galois group of the equation (*) (as an algebraic group in the constants).*

We briefly recall groupoids. We follow the formalism of section 2 of [7] and repeat the definitions. A category is considered as a 2-sorted structure with sorts Ob for the objects, Mor for the morphisms and maps $i_0, i_1 : Mor \to Ob$, a partially defined composition $\circ : Mor \times Mor \to Mor$, and identity $Id : Ob \to Mor$. So for example if $x \in Mor$ then x will be a morphism between the objects $i_0(x)$ and $i_2(x)$. We write $Mor(a, b)$ for the set of morphisms between a and b, and unless we say otherwise, if $x \in Mor(a, b)$ and $y \in Mor(b, c)$ we write $xy \in Mor(a, c)$ for their composition. A groupoid is a category where every morphism x has a 2-sided inverse x^{-1}. For a, b objects of the groupoid $\mathcal{G}$, write $a \sim b$ if $Mor(a, b) \neq \emptyset$. Then $\sim$ is an equivalence relation and the classes are called the connected components of $\mathcal{G}$. As a groupoid is in particular a category, and is already considered as a structure by our conventions, it makes sense to speak of a groupoid $\mathcal{G}$ being definable (or interpretable) in a given structure over a set of parameters

A. Namely $Ob, Mor, i_0, i_1, \circ, Id$ should all be definable over A in the given structure

We return to the earlier discussion and notation, and we obtain from Lemma 4.3:

Lemma 4.5. *(i) The category whose set of objects is O and such that for $a_1, a_2 \in O$, the set $Mor(a_1, a_2)$ of morphisms between a_1 and a_2 is H_{a_1,a_2}, and where we define composition of morphisms to be multiplication in $G(\mathcal{C})$, is a connected groupoid, $\mathcal{G}$ say, which we call the Galois groupoid of the equation (*).*
(ii) Moreover $\mathcal{G}$ is definable over C_K in the algebraically closed field $\mathcal{C}$.

Now as ACF_{C_K} has quantifier elimination, $\mathcal{G}$ is quantifier-free definable, hence for any field C containing C_K we can consider $\mathcal{G}(C)$, the category with objects $O(C)$ and for $a_1, a_2 \in O(C)$, morphisms $Mor(a_1, a_2)(C)$. $\mathcal{G}(C)$ is clearly a groupoid but is not necessarily connected. The following shows that $\mathcal{G}(C_K)$ parametrizes the family of strongly normal extensions of K, in a strong sense.

Proposition 4.6. *There is a natural one-one correspondence between:*
(a) The set of strongly normal extensions of K for (*) up to isomorphism over K as differential fields, and
(b) The set of connected components of the groupoid $\mathcal{G}(C_K)$.

Proof. Given $a \in O_{C_K}$, pick any $b \in \mathcal{Y}_a$, and by Lemma 3.4(iii) we obtain a strongly normal extension $K(b)$ of K. Conversely if $b \in \mathcal{Y}$ and $K(b)$ is a strongly normal extension of K then $f(b) \in O(C_K)$ as K and $K(b)$ have the same constants. Hence it suffices to prove that if $a_1, a_2 \in O(C_K)$ and $b_i \in \mathcal{Y}_{a_i}$ for $i = 1, 2$, then $Mor(a_1, a_2)(C_K)$ is nonempty if and only if $K(b_1)$ and $K(b_2)$ are isomorphic over K as differential fields. First suppose $K(b_1)$ is isomorphic to $K(b_2)$ over K. Applying an automorphism of $\mathcal{U}$ over K (which of course fixes a_1 and a_2) we may assume that $K(b_1) = K(b_2) = L$, say. Now $b_2^{-1}b_1 \in G(C_L) = G(C_K)$, and is also in $Mor(a_1, a_2)$. So $Mor(a_1, a_2)(C_K) \neq \emptyset$.
Conversely, suppose that $c \in Mor(a_1, a_2)(C_K)$. By definition $c = b_1'^{-1}b_2'$ for some $b_i' \in \mathcal{Y}_{a_i}$, $i = 1, 2$. So clearly $K(b_1') = K(b_2')$. As b_1 and b_1' are both in $\mathcal{Y}_{a_1}$, by Lemma 3.4(i), $tp(b_1/K) = tp(b_1'/K)$ (in DCF) so $K(b_1)$ and $K(b_1')$ are isomorphic over K as differential fields. Likewise $K(b_2)$ and $K(b_2')$ are isomorphic over K. So therefore are $K(b_1)$ and $K(b_2)$. □

It is convenient at this point to record some facts about the interpretation ω. We fix some notation, bearing in mind the discussion at the end of section 2.

Notation.
F denotes $\omega(f)$, a function from G to $O(\mathcal{U})$ definable over K in the algebraically closed field $\mathcal{U}$, and we write X_a for $F^{-1}(a)$, $a \in O(\mathcal{U})$.
H denotes the Zariski closure of H^+, an algebraic subgroup of G, defined over K.
We write $\mathcal{G}(\mathcal{U})$ for $\omega(\mathcal{G})$, as $\mathcal{G}$ is definable in $\mathcal{C}$ over C_K.

Lemma 4.7. *(i) Let $h : \mathcal{Y} \times \mathcal{Y} \to G(\mathcal{C})$ be $h(x, y) = x^{-1}y$. Then $\omega(h) : G \times G \to G$ is also the map taking $(x, y) \to (x^{-1}y)$.*
(ii) The fibres X_a for $a \in O(\mathcal{U})$ are the right cosets of H in G, in particular smooth algebraic subvarieties of G. (So $O(\mathcal{U})$" = "G/H .)
(iii) For $a \in O(C_K)$, X_a is K-irreducible, and the strongly normal extension L of K corresponding to a is, as a field, precisely the function field $K(X_a)$ of X_a over K.
(iv) $Mor(\mathcal{U})(a_1, a_2) = \{b_1^{-1}b_2 : b_1 \in X_{a_1}, b_2 \in X_{a_2}$, for $a_1, a_2 \in O(\mathcal{U})\}$.

Proof. (i) If Z is the graph of the map taking $(x, y) \in G \times G$ to $x^{-1}y \in G$, then $Z \cap (\mathcal{Y} \times \mathcal{Y} \times G(\mathcal{C}))$ is Zariski-dense in Z, so Z is a ∂-variety over K, and so $Z = \omega(graph(h))$ as required.
(ii) Fix $b \in \mathcal{Y}$, let $h_b : \mathcal{Y} \to G(\mathcal{C})$ taking y to $b^{-1}y$, then $\omega(h_b) : G \to G$ is again premultiplication by b^{-1}. Let $f_1 = f \circ h_b^{-1} : G(\mathcal{C}) \to O$. So by 2.6, $F_1 =_{def} \omega(f_1) = F \circ \omega(h_b^{-1})$ (as $\omega(f_1)$ is the interpretation in $(\mathcal{U}, G)$ of the formula defining f_1 in $(\mathcal{C}, \mathcal{Y})$ etc.). Let $f(b) = a \in O(\mathcal{C})$. Then the fibres of $f_1 : G(\mathcal{C}) \to O$ are clearly the right cosets of H_a. Hence as all this is definable in the algebraically closed field $\mathcal{C}$, the fibres of $F_1 : G \to O(\mathcal{U})$ are the right cosets of $H_a(\mathcal{U})$. Hence the fibres of $F : G \to O(\mathcal{C})$ are the right cosets of $bH_a(\mathcal{U})b^{-1}$. But notice that $bH_ab^{-1} = H^+$ (by 4.3), so by taking Zariski closures $bH_a(\mathcal{U})b^{-1} = H$, and we have proved (ii).
(iii) Let $a \in O(C_K)$ (in fact even in $O(\mathcal{C})$) and let $b \in \mathcal{Y}_a$. We have seen in the proof of (ii) that $X_a = Hb$ where H is the Zariski closure of H^+. As $\mathcal{Y}_a = H^+b$ it follows that X_a is the Zariski closure of $\mathcal{Y}_a$. Now suppose $a \in O(C_K)$. As all elements of $\mathcal{Y}_a$ have the same type over K (in DCF_0 so also in ACF_0) it follows that X_a which is clearly an algebraic variety over K is K-irreducible. In particular b is a generic point of X_a over K, whereby $K(b)$ is the function field of X_a over K.
(iv) This is a direct application of 2.6, using (i), (ii): In the $L_{\partial,K}$-structure

$(\mathcal{C}, \mathcal{Y})$ the following holds: For all $a_1, a_2 \in O$, $Mor(a_1, a_2) = \{b_1^{-1} b_2 : b_1 \in f^{-1}(a_1), b_2 \in f^{-1}(a_2)\}$. So apply the interpretation ω, 2.6, and parts (i) and (ii) to get the desired conclusion.

□

Proof of Theorem 1.4.
Let L_1, L_2 be strongly normal extensions of K. By Proposition 4.6 they correspond to $a_1, a_2 \in O(C_K)$. Assuming that L_1 and L_2 have a common embedding (as fields) over K into an elementary extension of C_K we need, by Proposition 4.6, to show that $Mor(a_1, a_2)$ has a C_K-point. Suppose $L_i = K(b_i)$ where $f(b_i) = a_i$ for $i = 1, 2$. So $F(b_i) = a_i$. By hypothesis we can find a subfield L_3 of $\mathcal{U}$ containing K which is an elementary extension of C_K, and embeddings h_i of L_1 into L_3 for $i = 1, 2$. Let $b_i' = h_i(b_i)$ for $i = 1, 2$. As F is field-definable over K in $\mathcal{U}$, $F(b_i') = a_i$ for $i = 1, 2$. Then $b_1'^{-1} b_2' \in Mor(a_1, a_2)(L_3)$. As C_K is an elementary substructure of L_3 and $Mor(a_1, a_2)$ is quantifier-free field definable over C_K, it follows that $Mor(a_1, a_2)(C_K)$ is nonempty, as required.

5 Galois cohomology and the proof of Theorem 1.5

To prove Theorem 1.5, we will need to know, among other things, that if C_K has the (F)-property then $\mathcal{G}(C_K)$ has only finitely many connected components, where $\mathcal{G}$ is the Galois groupoid defined in the previous section. To prove this we will go through Galois cohomology. In fact in the linear case (when $G = GL_n$), then assuming $\mathcal{G}(C_K)$ to be nonempty, and choosing $a \in \mathcal{G}(C_K)$, the set of connected components of $\mathcal{G}(C_K)$ will be in natural one-one correspondence with $H^1(C_k, H_a)$, which follows from 4.6 together with results in [3] and [4].(See Propositions 1.5 and 1.6 of [2].) This is no longer the case for G an arbitrary algebraic group, but the set of connected components of $\mathcal{G}(C_K)$ will be a "definable" part of $H^1(C_K, H_a)$, so we will be able to deduce the required finiteness result from *countability* of the Galois cohomology group as we explain later.

For convenience, all our fields will be of characteristic 0. We will be making use of

Fact 5.1. *Suppose k has the (F) property, then so does any field elementarily*

equivalent to k. Moreover if $k \prec K$ then the natural map from $Gal(K^{alg}/K) \to Gal(k^{alg}/k)$ is an isomorphism of profinite groups.

Explanation. This should be considered folklore, but see Section 2 of [1] for coding of finite field extensions and Galois groups.

Galois cohomology is well-known and Serre's book [22] is the established reference. For G an algebraic group over k, $H^1(k, G)$ denotes $H^1(Gal(k^{alg}/k), G(k^{alg}))$, the first cohomology set of the profinite group $Gal(k^{alg}/k)$, acting on the discrete group $G(k^{alg})$. (Here k^{alg} denotes the algebraic closure of k.) One of the main points for us is that $H^1(k, G)$ classifies the set of principal homogeneous spaces for G defined over k up to k-isomorphism (section I.5.2 of [22]). In section 4 of Chapter III of [22] the (F) property is introduced, namely that $Gal(k^{alg}/k)$ has finitely many open subgroups of index n for each n. Equivalently k has only finitely many extensions of degree n for each n. It is proved there that if k has property (F) then for any *linear* algebraic group G over k, $H^1(k, G)$ is finite. The following theorem gives an extension to arbitrary algebraic groups G. We make one reference to the proof of Theorem 1.1 in [2], but it is an elementary observation in the cohomology of groups.

Theorem 5.2. *Let k be a field (of characteristic 0) which has property (F) and G an arbitrary algebraic group over k. Then $H^1(k, G)$ is countable.*

Proof. Let G be an algebraic group over k. We have the exact sequence (of pointed sets): $H^1(k, G^0) \to H^1(k, G) \to H^1(k, G/G^0)$. As the latter is finite (Proposition 8, Chapter III of [22]), we may assume G to be connected. In that case we have the exact sequence $1 \to L \to G \to A \to 1$, where L is linear, and A an abelian variety, all over k. By Exercise 1 in section 4.4 of Chapter III of [22], the induced map from $H^1(k, G)$ to $H^1(k, A))$ is finite-to-one. So it suffices to prove that $H^1(k, A)$ is countable when A is an abelian variety.

Let k_0 be a countable elementary substructure of k over which A is defined. By Fact 5.1, the natural map from $Gal(k^{alg}/k)$ to $Gal(k_0^{alg}/k_0)$ is a bijection. Now part (2) of the proof of Theorem 1.1 in [2] says that in this situation, for any commutative algebraic group C over k_0, the natural map $H^n(k_0, C) \to H^1(k, C)$ is bijective, for all $n > 0$. In particular the natural map $H^1(k_0, A) \to H^1(k, A)$ is bijective. As $H^1(k_0, A)$ is clearly countable, so is $H^1(k, A)$. □

Corollary 5.3. *Let k be a field with property (F), and $\mathcal{G}$ a connected groupoid definable over k in ACF (namely a groupoid definable over k in some algebraically closed field containing k). Then $\mathcal{G}(k)$ has finitely many connected components.*

Proof. We may assume that $O(k)$ is nonempty, and let $a \in O(k)$. So $H_a = Mor(a, a)$ is an algebraic group over k. For any $b \in O(k)$, $Mor(a, b)$ is a (left) principal homogeneous space for H_a defined over k,
Claim. Let $b, c \in O(k)$. Then $Mor(a, b)$ and $Mor(a, c)$ are isomorphic over k (as left torsors for H_a) iff $Mor(b, c)(k) \neq \emptyset$.
Proof of claim. If $h \in Mor(b, c)(k)$, then the map (bijection) taking any $h_1 \in Mor(a, b)$ to $h_1 h \in Mor(a, c)$ is k-definable and commutes with the left action of H_a.
Conversely, if χ is an isomorphism over k between $Mor(a, b)$ and $Mor(a, c)$, let $h \in Mor(a, b)$ (in the ambient algebraically closed field) and consider $h^{-1}\chi(h) \in Mor(b, c)$. We claim it is defined over k. Let σ be an automorphism (of the ambient algebraically closed field) fixing k pointwise, and let $h_1 = \sigma(h) \in Mor(a, b)$, so $h_1 = h_2 h$ for some $h \in H_a$. Then $\sigma(h^{-1}\chi(h)) = h_1^{-1}\chi(h_1) = h^{-1}h_2^{-1}\chi(h_2 h) = h^{-1}h_2^{-1}h_2\chi(h) = h^{-1}\chi(h)$. So $h^{-1}\chi(h) \in Mor(b, c)(k)$ as required.

It follows from the claim that the set of connected components of $\mathcal{G}(k)$ embeds into $H^1(k, H_a)$. Supposing for a contradiction that $\mathcal{G}(k)$ had infinitely many connected components, then by compactness, there would be an elementary extension K of k such that $\mathcal{G}(K)$ has uncountably many connected components. But then by the previous sentence applied to K, we conclude that $H^1(K, H_a)$ is uncountable, contradicting Theorem 5.2, bearing in mind 5.1. □

We now prove Theorem 1.5.

Proof. Before starting the proof it is worth remarking how the largeness assumption is used, which is as follows: Suppose X is a smooth variety over a large field k, which is k-irreducible. Then from the existence of a k-rational point of X we deduce from largeness that $X(k)$ is Zariski-dense in X from which we conclude that k is existentially closed in the function field $k(X)$. See Fact 2.3 of [21].
We use notation from Lemma 4.7 and just before. We aim for:

Main Claim. There is $a \in O(C_K)$ such that X_a has a point in some elementary extension K_1 of C_K which contains K.

Let us suppose first that we have the Main Claim. By 4.7 the strongly normal extension of K corresponding to a is precisely the function field $K(X_a)$ of the algebraic variety X_a over K. Let K_1 be the elementary extension of C_K containing K such that X_a has a K_1-point. Notice that X_a, being a coset of an algebraic group, is equidimensional, and a disjoint union of its irreducible components, all of which are smooth. Let Z be a K-irreducible component of X_a such that $Z(K_1) \neq \emptyset$. By Proposition 2.1 of [21], K_1 is large. Hence as Z is smooth and has a K_1-rational point, K_1 is existentially closed in the function field $K_1(Z)$ (using again Fact 2.3 of [21]). As C_K is an elementary substructure of K_1, C_K is existentially closed in $K_1(Z)$. But the embedding of K in K_1 extends to an embedding of $K(X_a)$ in $K_1(Z)$. Hence C_K is existentially closed in the strongly normal extension $K(X_a)$ of K, as required.

So it remains to prove the Main Claim. We already know from Theorem 1.3 that $O(C_K)$ is nonempty. We again consider $F = \omega(f) : G \to O(\mathcal{U})$ and let again $F(e) = a' \in O(K)$. Note that $X_{a'}$ is precisely H, by 4.7(ii). As C_K is existentially closed in K, let K_1 be an elementary extension of C_K containing K which we may assume is a subfield of $\mathcal{U}$. So $a' \in O(K_1)$. By Corollary 5.3, $\mathcal{G}(C_K)$ has only finitely many connected components. As K_1 is an elementary extension of C_K there is $a \in O(C_K)$ such that $Mor(a, a')(K_1)$ is nonempty. By 4.7 (iv) we obtain a (field-) definable over K_1 bijection between X_a and X'_a. But $X_{a'}(K_1) = H(K_1)$ is nonempty (as it contains the identity). Hence $X_a(K_1)$ is nonempty, as required. This completes the proof of the main claim and hence of Theorem 1.5. □

References

[1] Z. Chatzidakis, Notes on the talk: "Independence in (unbounded) PAC fields, and imaginaries" from Leeds meeting 2008, http://www.logique.jussieu.fr/ zoe/papiers/Leeds08.pdf

[2] T. Crespo, Z. Hajto, and M. van der Put, Real and p-adic Picard-Vessiot fields, preprint July 2013, arXiv 1307.2388, to appear in Math. Annalen.

[3] P. Deligne, Catégories tannakiennes, in *Grothendieck Festschrift*, vol II, Progress in Mathematics 87, Birkhauser, 1990.

[4] P. Deligne and J.S. Milne, Tannakian Categories, in *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics 900, Springer, 1982.

[5] H. Gillet, S. Gorchinskiy, and A. Ovchinnikov, Parametrized Picard-Vessiot extensions and Atiyah extensions, Advances in Math., 238 (2013), 322-411.

[6] W. A. Hodges, *Model Theory*, Cambridge University Press, 1993.

[7] E. Hrushovski, Groupoids, imaginaries, and internal covers, arXiv: math.LO/0603413, and Turkish Journal of Mathematics, 36(2), (2012), 173-198.

[8] M. Kamensky, Picard-Vessiot structures, preprint 2013.

[9] E. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973.

[10] E. Kolchin, Galois theory of differential fields, American Journal of Math. 75 (1953), 753-824.

[11] J. Kovacic, The differential Galois theory of strongly normal extensions, Transactions AMS 355 (2003), 4475-4522.

[12] P. Kowalski and A. Pillay, Quantifier elimination for algebraic D-groups, Trans. AMS, 358.1 (2006), 167-181.

[13] M. Makkai and G. E. Reyes, *First order categorical logic*, Lecture Notes in Mathematics 611, Springer, 1977.

[14] D. Marker, *Model Theory: An Introduction*, Springer, 2002.

[15] D. Marker, Model theory of differential fields, in *Model theory of fields*, edited Marker, Messmer, Pillay, Lecture Notes in Logic 5, ASL-Peters, 2006.

[16] A. Pillay, *Geometric Stability Theory*, Oxford University Press, 1996.

[17] A. Pillay, Two remarks on differential fields, in *Model Theory and Applications*, Quaderni di Matematica, vol 11, Caserta 2002.

[18] A. Pillay, Algebraic D-groups and differential Galois theory, Pacific J. Math., vol. 216 (2004) 343-360.

[19] B. Poizat, Une théorie de Galois imaginaire, Journal Symbolic Logic, 48.4 (1983), 1151-1170.

[20] B. Poizat, *A Course in Model Theory*, Springer, 2000.

[21] F. Pop, Little survey of large fields - Old and New -, in *Valuation Theory in Interaction*, edited by Campillo Lopez, Kuhlmann, Teissier, EMS series of Congress reports, European Math Soc., 2014.

[22] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math, no. 5, Springer, 1973.