

ITERATIVE DIFFERENTIAL GALOIS THEORY IN POSITIVE CHARACTERISTIC: A MODEL THEORETIC APPROACH

JAVIER MORENO

ABSTRACT. This paper introduces a natural extension of Kolchin's differential Galois theory to positive characteristic iterative differential fields, generalizing to the non-linear case the iterative Picard-Vessiot theory recently developed by Matzat and van der Put. We use the methods and framework provided by the model theory of iterative differential fields. We offer a definition of strongly normal extension of iterative differential fields, and then prove that these extensions have good Galois theory and that a G -primitive element theorem holds. In addition, making use of the basic theory of arc spaces of algebraic groups, we define iterative logarithmic equations, finally proving that our strongly normal extensions are Galois extensions for these equations.

1. INTRODUCTION

Differential Galois theory is the study of extensions of differential fields with well-behaved automorphism groups. In contrast to classic algebraic Galois theory, the automorphism groups of differential Galois extensions turn out to be algebraic groups or, in more general settings, differential algebraic groups. The origins of differential Galois theory trace back to the works of Picard and Vessiot in the 1890s studying linear differential equations, but it was Kolchin (following the work of Ritt) who gave the first systematic and modern account of the subject in his seminal book [7]. There he introduced, among other things, the notion of a strongly normal extension of differential fields as a non-linear generalization of the classic extensions discovered by Picard and Vessiot. Modern treatments of Kolchin's theory have been offered in recent years by Magid [9], Kovacic [8] and Umemura [24], among others. The current general reference on the subject is the book by Singer and van der Put [22].

For basic technical reasons regarding the nature of constants in positive characteristic, most of the work on differential Galois theory has been restricted to the context of characteristic zero differential fields, but several attempts have been made to work around this obstacle [1][22]. One of the most popular strategies is replacing the notion of a derivative for that of an iterative (Hasse-Schmidt) derivation. This approach was extensively studied (but with partial success) by Okugawa [12][13] and Shikishima-Tsuji [23],

Date: June, 2009.

2000 Mathematics Subject Classification. Primary 03C98; Secondary 12H05.

This paper contains the results of the author's thesis, which was written under the kind supervision of Anand Pillay. The author would like thank him for his patience, advice and support.

and more recently by Matzat and van der Put [10], who developed a full Picard-Vessiot theory for positive characteristic iterative differential fields with the use of the theory of torsors.

Differential Galois theory and model theory have had a long history. It all started with Poizat's paper *Une théorie de Galois imaginaire* [21] suggesting that Kolchin's main results could be obtained as a consequence of the ω -stability of the theory of differentially closed fields and some work by Zilber and Hrushovski on the definability of automorphism groups [5][26]. After this, several people including Marker, Pillay and Sokolović [14][15][16][18][19] have contributed to the development and even generalization of Kolchin's results making use of these abstract tools from model theory.

Positive characteristic differential Galois theory, however, remained out of reach of model theory until Messmer, Wood and Ziegler proved (strongly based on Delon's work on separably closed fields of positive characteristic [3]) that the theory of fields equipped with stacks of commuting iterative derivations has a stable model companion with quantifier elimination and elimination of imaginaries [11][25]. After this, adapting some of his previous results in characteristic zero, and working along the lines of what Hrushovski suggested in [6], Pillay found alternative proofs of existence and uniqueness of iterative Picard-Vessiot extensions (results already proved by Matzat and van der Put) using now model-theoretic techniques [17].

Following Pillay, this article introduces a theory of strongly normal extensions for iterative differential fields of positive characteristic. These extensions generalize the Picard-Vessiot extensions developed by Matzat and Van Der Put as well as the strongly normal extensions proposed by Okugawa. Our results depend on the model theory of iterative differential fields.

After introducing in section 2 the basic definitions and model theory of iterative differential fields of positive characteristic, in section 3 we define what we mean by an iterative strongly normal extension (Definition 3.1). Then we prove that the Galois group of these extensions is isomorphic to the constant-rational points of an algebraic group defined over the constants of the base field (Theorem 3.5), we have good Galois correspondence (Theorem 3.15), and also what Kolchin called a G -primitive element theorem (Theorem 3.17).

In section 4 we start all over again, this time from the perspective of (logarithmic) differential equations. This requires us to make an overview of the notion of the arc bundle of an algebraic variety (Definition 4.4) and introduce what should be our logarithmic derivation (Definition 4.8). Once there we define what we mean by an iterative differential Galois extension for a given logarithmic differential equation (Definition 4.11) and prove that these extensions exist and are unique modulo isomorphism (Theorem 4.12).

Finally, in section 5, we show that, under certain hypothesis on the base field, iterative strongly normal extensions and iterative differential Galois extensions are just two faces of the same notion (Theorems 5.1 and 5.2).

We assume that the reader has working knowledge of the fundamentals of geometric model theory, and a fair understanding of the terminology of varieties from algebraic geometry and basic differential algebra.

2. ITERATIVE DIFFERENTIAL ALGEBRA: MODEL THEORY AND PRACTICE

The aim of this section is offering a brief introduction to the basic model theory of iterative derivations.

Definition 2.1. Let R be an arbitrary ring. A sequence of maps $\partial = (\partial_i: R \rightarrow R)_{i \in \omega}$ is called a **Hasse-Schmidt derivation** if $\partial_0 = id_R$ and the map

$$\mathbb{D}_\partial: R \rightarrow R[[\epsilon]]: a \mapsto \sum_{i=0}^{\infty} \partial_i(a)\epsilon^i$$

is a ring homomorphism.

If, additionally, for any $i, j \in \omega$ we have that $\partial_i \circ \partial_j = \binom{i+j}{i} \partial_{i+j}$, we say that ∂ is an **iterative Hasse-Schmidt derivation** or simply an **iterative derivation**.

A ring (field) R equipped with an iterative derivation ∂ is what we call an **iterative differential ring (field)** or ID-ring (field) and its **ring (field) of constants**, C_R , is defined as the set where all the ∂_i vanish.

We say that an ID-field F is **non-trivial** if $\partial_1|_F \neq 0$.

Let IDF_p be the first-order theory of fields of characteristic $p > 0$ equipped with an iterative derivation ∂ . The language we will consider is that of fields expanded with a sequence $(\partial_i)_{i < \omega}$ of unary function symbols. This theory has a model companion, SCH_p , the theory of separably closed ID-fields, K , of characteristic p , degree of imperfection 1 (i.e. $[K : K^p] = p$) and $K^p = \{x \in K : \partial_1(x) = 0\}$.

Given a model K of SCH_p , we can see that $C_F = K^{p^\infty}$, an algebraically closed field. This theory is, in some sense, just another version of $SCF_{p,1}$, the theory of separably closed fields of characteristic p and degree of imperfection 1:

Fact 2.2. *Once a p -basis is fixed, every model of $SCF_{p,1}$ can be expanded to a model of SCH_p and, additionally, any highly enough saturated model of SCH_p can be canonically equipped with a p -basis and its corresponding λ -functions are quantifier-free definable.*

Proof. See [25]. □

And, as a consequence of this,

Fact 2.3. *SCH_p is stable (non-superstable) and has quantifier elimination and elimination of imaginaries.*

Proof. See [25]. □

Since SCH_p is stable, we may let (\mathcal{U}, ∂) be a saturated model of SCH_p of large cardinality and \mathcal{C} its field of constants.

As in the case of characteristic zero differentially closed fields, the field of constants of \mathcal{U} is a pure algebraically closed field, that is, any definable subset is definable in the language of rings. Note that in this case, though, \mathcal{C} is not definable but type-definable:

Fact 2.4. *If $Z \subset \mathcal{U}^m$ is definable in \mathcal{U}^m over A , then $Z \cap \mathcal{C}^m$ is definable in $(\mathcal{C}, +, \cdot)$ over $\text{dcl}(A) \cap \mathcal{C}$.*

Proof. By stability and quantifier elimination. \square

We will now define three different closure operators of algebraic nature.

Definition 2.5. Let $A \subset \mathcal{U}$.

- **The iterative differential closure of A** , denoted $\langle A \rangle$, will be the iterative differential subfield of \mathcal{U} generated by the elements of A . If F is an ID-field and A is a set, by $F\langle A \rangle$ we mean $\langle FA \rangle$.
- **The strict closure of A** , denoted A^s , will be the set obtained after closing A under p th-roots.
- Finally, **the relative algebraic closure of A** , denoted A^a , will be the field theoretic algebraic closure of A inside \mathcal{U} .

Benoist [2] gave useful algebraic characterizations of the model theoretic definable and algebraic closures in \mathcal{U} in terms of these closure operators:

Fact 2.6. Let $A \subset \mathcal{U}$.

- $\text{dcl}(A) = \langle A \rangle^s$
- $\text{acl}(A) = \langle A \rangle^a$

Proof. See Proposition II.2 and Proposition II.3 of [2]. \square

3. ITERATIVE STRONGLY NORMAL EXTENSIONS

From now on, let us fix a prime number $p > 0$. As in the previous chapter, let \mathcal{U} be a saturated model of SCH_p of large cardinality where any ID-field mentioned is embedded and let \mathcal{C} the field of constants of \mathcal{U} .

Let us also assume that (F, ∂) is an iterative differential field with $\partial_1|_F \neq 0$.

3.1. Definition and basic properties.

Definition 3.1. An extension $(F, \partial) < (K, \partial)$ of non-trivial definably closed ID-fields is said to be **strongly normal** if the following conditions hold:

- (1) $C_F = C_K$, and C_F is algebraically closed;
- (2) $K = F\langle a \rangle^s (= \text{dcl}(Fa))$ for some $a = (a_1, \dots, a_m)$;
- (3) Whenever $\sigma: K \hookrightarrow \mathcal{U}$ is an embedding of K into \mathcal{U} over F , then $\sigma(K) \subseteq K\langle \mathcal{C} \rangle$; and finally,
- (4) $F^a \cap K = F\langle d \rangle^s$ for some $d = (d_1, \dots, d_m)$.

Following Kolchin, the **Galois group** of the strongly normal extension K/F , denoted $\text{Gal}(K/F)$ will be $\text{Aut}_\partial(K\langle \mathcal{C} \rangle/F\langle \mathcal{C} \rangle)$. The traditional $\text{Aut}_\partial(K/F)$ will be denoted instead $\text{gal}(K/F)$.

Our definition of a strongly normal theory does not differ much from the original one due to Kolchin in the characteristic zero case. We require, though, one property that in Kolchin's case is automatic: $\text{tp}(a/F)$ should have finite multiplicity. This is going to be crucial to assure the definability of our Galois group. The extra-condition (4) will do this for us:

Fact 3.2. *If $K = F\langle a \rangle^s$ is an iterative strongly normal extension of F , then $\text{tp}(a/F)$ has finite multiplicity.*

This is a corollary of the following general lemma:

Lemma 3.3. *Let T be a stable theory and \mathcal{U} a highly saturated model of T . Then, for any $a \in \mathcal{U}$ and $F \subseteq \mathcal{U}$, we have that $\text{tp}(a/F)$ has finite multiplicity if and only if there exists a finite tuple $c \in \mathcal{U}^{\text{eq}}$ such that $\text{acl}^{\text{eq}}(F) \cap \text{dcl}^{\text{eq}}(aF) = \text{dcl}^{\text{eq}}(Fc)$.*

Proof. \Rightarrow) Let $p = \text{tp}(a/F)$ and let p_1, \dots, p_m be the complete extensions of p to $\text{acl}(F)$, and $p_1 = \text{tp}(a/\text{acl}(F))$. The finite equivalence relation theorem provides us with a single F -definable finite equivalence relation E distinguishing the extensions of p to $\text{acl}(A)$. Let c be the E -class of a . By definition $c \in \text{dcl}^{\text{eq}}(Fa)$, and, since E is an equivalence relation over F with finitely many classes, $c \in \text{acl}^{\text{eq}}(F)$.

On the other hand, let $b \in \text{dcl}^{\text{eq}}(aF) \cap \text{acl}^{\text{eq}}(F)$. Thus we have $b = f(a)$ for some F -definable function f . Let σ be an automorphism of \mathcal{U} fixing Fc . Suppose $\sigma(p_1) \neq p_1$. Then $\sigma(p_1) = p_i$, for some $i \neq 1$ and so $\sigma(c) \neq c$, contradicting the choice of σ . Thus, the formula $\sigma(b) = f(x)$ is still in p_1 . But then, $\sigma(b) = f(a) = b$. This implies that $b \in \text{dcl}^{\text{eq}}(Fc)$.

\Leftarrow) Let $d = \text{Cb}(\text{tp}(a/\text{acl}^{\text{eq}}(F)))$. We know that $d \subseteq \text{acl}^{\text{eq}}(F)$ and it is also clear that $d \subseteq \text{dcl}(Fa)$. Thus $d \subseteq \text{dcl}^{\text{eq}}(Fc)$ for some $c \in \text{acl}^{\text{eq}}(F)$. But this implies that d has finitely many conjugates over A , and so $\text{tp}(a/F)$ has finite multiplicity. \square

One consequence of condition (3) in the definition of iterative strongly normal extensions is the fact that $\text{tp}(a/F)$ is *internal* to \mathcal{C} : If $\text{tp}(b/F) = \text{tp}(a/F)$ then $b \in K\langle\mathcal{C}\rangle = \text{dcl}(F, a, \mathcal{C})$. The fact that the type has finite multiplicity makes this definability uniform, as we show next.

Lemma 3.4. *If $K = F\langle a \rangle^s$ is an iterative strongly normal extension of F , then there exists a function defined over F , let us call it $u(\cdot, \cdot)$, such that for every b with $\text{tp}(b/F) = \text{tp}(a/F)$, there is $c \in \mathcal{C}$ such that $u(a, c) = b$.*

Proof. When $p = \text{tp}(a/F)$ is stationary, this is a standard fact (see, for instance, Theorem 2.19, p. 37, of [20]). For the general case, find a function for each complete extension of p to $\text{acl}(F)$ and then glue them together. \square

3.2. The Galois group is an algebraic group. This subsection is devoted to prove the following key result:

Theorem 3.5. *There is an isomorphism of groups*

$$\mu: \text{Gal}(K/F) \rightarrow G(\mathcal{C}),$$

where G is algebraic group in \mathcal{U} defined over C_F . Furthermore, the action of $\text{Gal}(K/F)$ on $\mathcal{X} = \text{tp}(a/F)^{\mathcal{U}}$ is $(F \cup \{a\})$ -definable.

The following lemma and its corollary, both crucial in the proof of this theorem, clarify the nature of $\text{Gal}(K/F)$ and its relation with the associated strongly normal extension. In particular, the lemma tells us that $\text{gal}(K/F) < \text{Gal}(K/F)$.

Lemma 3.6. *Any embedding of K into \mathcal{U} over F can be uniquely extended to an automorphism of $K\langle\mathcal{C}\rangle$ fixing \mathcal{C} pointwise.*

Proof. It is enough to show that for any $a' \in \mathcal{U}$ such that $\text{tp}(a'/F) = \text{tp}(a/F)$, we have $\text{tp}(a'/F\langle\mathcal{C}\rangle) = \text{tp}(a/F\langle\mathcal{C}\rangle)$. To see this, take $\sigma: K \rightarrow \mathcal{U}$ an

embedding of ID-fields fixing F . Since $\text{tp}(a/F) = \text{tp}(\sigma(a)/F)$, our assumption tells us that $\text{tp}(a/F\langle\mathcal{C}\rangle) = \text{tp}(\sigma(a)/F\langle\mathcal{C}\rangle)$ and this, by homogeneity of \mathcal{U} and stability of the theory, provides us with $\bar{\sigma}$, a \mathcal{U} -automorphism fixing $F\langle\mathcal{C}\rangle$ and taking a to a' . Note that $\bar{\sigma}|_{K\langle\mathcal{C}\rangle}: K\langle\mathcal{C}\rangle \rightarrow \sigma(K)\langle\mathcal{C}\rangle$. Note also that $\sigma(K)\langle\mathcal{C}\rangle = K\langle\mathcal{C}\rangle$.

In order to prove the claim, consider the infinite tuples aF and $a'F$, where $\text{tp}(a'/F) = \text{tp}(a/F)$. Since \mathcal{C} is algebraically closed and type-definable over the empty set, $\text{tp}(aF/\mathcal{C})$ and $\text{tp}(a'F/\mathcal{C})$ are, respectively, the unique nonforking extensions of $\text{tp}(aF/C_F)$ and $\text{tp}(a'F/C_F)$. However, $\text{tp}(aF/C_F)$ and $\text{tp}(a'F/C_F)$ are equal, and, in consequence, the same is true about $\text{tp}(aF/\mathcal{C})$ and $\text{tp}(a'F/\mathcal{C})$. \square

Corollary 3.7. \mathcal{X} , the set of realisations of $\text{tp}(a/F)$ in \mathcal{U} , is a principal homogeneous space for $\text{Gal}(K/F)$.

Proof. As $\mathcal{X} \subset K\langle\mathcal{C}\rangle$, then $\text{Gal}(K/F)$ acts on \mathcal{X} . The fact that the action on \mathcal{X} is transitive and free is a direct consequence of the previous lemma. \square

Proof of theorem 3.5. This is a modified version of the general argument for proving the definability of the binding group.

Let $Y = Z/E$ where $Z = \{c \in \mathcal{C} : u(a, c) \in \mathcal{X}\}$ and E is an equivalence relation on Z defined by the formula $u(a, x_1) = u(a, x_2)$. Because of elimination of imaginaries of the theory of algebraically closed fields and the pureness of \mathcal{C} , Y is a type-definable set in \mathcal{C} over $dcl(a) \cap \mathcal{C} \subset C_F$.

For $b \in \mathcal{X}$ and $d \in Y$, define $f(b, d) = u(b, c)$ with $c \in Y_0$ such that $c/E = d$, and note that for any b_1 and $b_2 \in \mathcal{X}$, there is only one $d \in Y$ such that $f(b_1, d) = b_2$.

Consider the function $\mu: \text{Gal}(K/F) \rightarrow Y: \sigma \mapsto h(a, \sigma(a))$. Corollary 3.7 then tells us that μ is a bijection. Endow Y with the group operation induced by μ . This is, let us define $d \cdot d' = \mu(\mu^{-1}(d) \cdot \mu^{-1}(d'))$. Note that this group operation is definable. Moreover, the induced action of Y on \mathcal{X} turns out to be $F \cup a$ -definable.

Finally, the fact that \mathcal{C} is totally transcendental plus the Weil-Van den Dries-Hrushovski theorem (See Theorem 4.13, p. 84 of [20], or [4]) tells us that (Y, \cdot) is definably isomorphic to the set of \mathcal{C} -rational points of an algebraic group G defined over C_F . Identify $G(\mathcal{C})$ and Y . \square

In addition, μ takes $\text{gal}(K/F)$ to the C_F -rational points of G .

Fact 3.8. $\mu(\text{gal}(K/F)) = G(C_F)$

Proof. First, observe that for any $\sigma \in \text{Gal}(K/F)$, we have that $\sigma(a) \in F\langle a, \mu(\sigma) \rangle^s$ and $\mu(\sigma) \in F\langle a, \sigma(a) \rangle^s \cap \mathcal{C}$. Now, if $\sigma(a) \in K$, then $\mu(\sigma) \in F\langle a \rangle^s \cap \mathcal{C} = C_K = C_F$.

On the other hand, if $\mu(\sigma) \in C_F$, then, $\sigma(a) \in F\langle a \rangle^s = K$. \square

3.3. Scaffolding. In characteristic zero, the model theoretic approach to differential Galois theory [16] heavily depends on the existence of prime models, a basic consequence of the fact that DCF_0 is totally transcendental. Since SCH_p is only stable and not even superstable, we need to rely in other tools to deal with the lack of decent *differential closure*. Just like in the linear

case [17], the use of a suitable auxiliary structure as a scaffolding to handle the group inside \mathcal{U} will do the trick.

Definition 3.9. Let K/F be an iterative strongly normal extension, with $K = F\langle a \rangle^s$. Now define \mathcal{M} as the two-sorted structure $(\mathcal{X}, \mathcal{C})$, with relations induced by F -definable relations in \mathcal{U} .

Fact 3.10. Let \mathcal{N} be the structure whose universe is \mathcal{C} , with relations induced by the $F\langle a \rangle^s$ -definable sets in \mathcal{U} . Then (\mathcal{M}, a) is bi-interpretable with \mathcal{N} .

Proof. On one hand, any intersection of \mathcal{C} and a $F\langle a \rangle^s$ -definable set in \mathcal{U} is, inside \mathcal{M} , an a -definable set. The other direction depends on the definability of the Galois group from the previous section.

As in the proof of theorem 3.5, let us define Y as the quotient of Z by E , where Z is the type-definable set $\{c \in \mathcal{C} : u(a, c) \in \mathcal{X}\}$ and E is given by the formula $u(a, x_1) = u(a, x_2)$. By the proof of theorem 3.5 we know that Y is a C_F -definable set in \mathcal{C} .

Note that \mathcal{X} and Y are isomorphic. Indeed, for each $b \in \mathcal{X}$ assign the class \bar{c}_b of $c \in \mathcal{C}$ such that $u(a, c) = b$. This map is one-to-one and onto by construction. Now, suppose that you have $D \subset \mathcal{M} \cap \mathcal{X}$ definable in (\mathcal{M}, a) . By definition, D is $F\langle a \rangle^s$ -definable in $\mathcal{U} \cap \mathcal{X}$. The map given between \mathcal{X} and Y is also $F\langle a \rangle^s$ -definable; thus the image of D , now inside the quotient set, is also $F\langle a \rangle^s$ -definable. This makes D definable inside \mathcal{N} . \square

Now we can check that, although we are working in a stable, non-superstable theory, the auxiliary structure we built is totally transcendental.

Fact 3.11. \mathcal{M} is saturated and its theory $\text{Th}(\mathcal{M})$ has quantifier elimination and is totally transcendental.

Proof. Let \mathcal{N} be just as in fact 3.10.

Since \mathcal{N} can be seen as \mathcal{C} with names for the elements of C_F , then it is saturated and totally transcendental. The fact that being totally transcendental and saturation are preserved under taking reducts and interpretability, allow us to conclude that \mathcal{M} is also saturated and totally transcendental.

Since \mathcal{M} is saturated, for quantifier elimination it is enough to prove that it is also quantifier-free homogeneous. Indeed, if d_1 and d_2 are two finite tuples from \mathcal{M} with the same quantifier-free type, then, seeing them as tuples from \mathcal{U} , they have the same type over F . The homogeneity of \mathcal{U} then provide us with an automorphism of \mathcal{U} over F taking one to the other. As it fixes F , this function is also an automorphism of \mathcal{M} when restricted to its domain. \square

Given that $\text{Th}(\mathcal{M})$ is totally transcendental, let \mathcal{M}_0 be its prime model over the empty set. This structure will play the role of the differential closure of F .

Lemma 3.12.

$$\mathcal{M}_0 \cap \mathcal{C} = C_F$$

Proof. Let $c \in \mathcal{M}_0 \cap \mathcal{C}$ and consider p , the type of c over the empty set in the language of \mathcal{M} . Since \mathcal{M}_0 is prime, p is isolated by a formula $\phi(x)$.

By lemma 2.4, the set that this formula defines inside \mathcal{C} is also defined by a formula in the language of rings and with parameters in $F \cap \mathcal{C} = C_F$. However, being algebraically closed, C_F is an elementary substructure of \mathcal{C} (in the language of rings), and so $\phi(\mathcal{C}) \cap C_F$ is not empty. This implies that, as ϕ is an isolating formula over F , it must be of the form $x = c'$ for some $c' \in C_F$. \square

The following fact tells us that the whole extension can be somehow interpreted, in a multi-sorted way, inside \mathcal{M}_0 , as if it were an scaffolding built on its side.

Lemma 3.13. *There is a bijection between the set of definably closed subsets of \mathcal{M}_0^{eq} and the set of definably closed ID-fields lying between F and K .*

Proof. Any $d \in \mathcal{M}_0^{eq}$ is of the form a'/E where E , by quantifier elimination, is a quantifier free \emptyset -definable equivalence relation in \mathcal{M} . This means that, in \mathcal{U} , we have that E is the intersection of \mathcal{X} and some F -definable set E' in \mathcal{U} . By stability of $SCH_{p,1}$, it can be assumed that E' is also an equivalence relation. By elimination of imaginaries in $SCH_{p,1}$, we know that a'/E' is interdefinable over F in \mathcal{U} with some tuple $e \in \text{dcl}(F, a')$. Note that, since there is $c \in \mathcal{C} \cap \mathcal{M}_0 = C_F$ such that $a' = u(a, c)$, then, $e \in \text{dcl}(F, a) = K$. Thus, d is interdefinable over F in \mathcal{U} with a tuple in K .

Let now $e \in K$. Then, $e = f(a)$ for some F -definable function f . Let $E(x, y)$ be $f(x) = f(y)$. The restriction of E is \emptyset -definable in \mathcal{M}_0 and $d = a/E \in \mathcal{M}_0^{eq}$. Clearly, d (seen as an element in \mathcal{U}) is interdefinable over F with e . \square

3.4. Galois correspondence and a G -primitive element theorem.

Let K a strongly normal extension of F and G the algebraic group whose \mathcal{C} -rational points are isomorphic to $\text{Gal}(K/F)$, as provided by theorem 3.5. As in the previous subsection, let \mathcal{M} the scaffolding built for the extension K/F and \mathcal{M}_0 its prime model over the empty set.

Definition 3.14. Given L a definably closed subfield of K containing F , let

$$G_L = \{g \in G(\mathcal{C}) : g(c) = c \text{ for all } c \in L\}.$$

Theorem 3.15. *Let K/F be a strongly normal extension of ID-fields. If L is a definably closed intermediate ID-field in K/F , then:*

- (i) K/L is strongly normal.
- (ii) G_L is a C_F -definable subgroup of $G(\mathcal{C})$ and is isomorphic to $\text{Gal}(K/L)$.
- (iii) The correspondence $L \mapsto G_L$ between intermediate ID-fields and C_F -definable subgroups of G is an injection.
- (iv) L/F is strongly normal if and only if G_L is a normal subgroup of $G(\mathcal{C})$. In this case, $G(\mathcal{C})/G_L \cong \text{Gal}(L/F)$.

Before proving the theorem, let us observe that definably closed intermediate fields of a strongly normal extension are finitely generated over the base field. More precisely:

Lemma 3.16. *If K/F is strongly normal and L is an intermediate definably closed ID-field, then $L = F\langle b \rangle^s$ for some $b = (b_1, \dots, b_m)$.*

Proof. Consider L as a definably closed subset in \mathcal{M}_0^{eq} and let $p = \text{tp}(a/L)$. Since $\text{Th}(\mathcal{M})$ is totally transcendental, there is a finite tuple b such that p is the unique non-forking extension over L of $\text{tp}(a/Fb)$. This b is the tuple of the canonical bases of each of the finitely many complete extensions of p to $\text{acl}(L)$. We claim $F\langle b \rangle^s = L$.

The left to right containment is clear. On the other hand, if $e \in L$, let $g(\cdot)$ an F -definable function such that $g(a) = e$. Consider the formula $\phi(x, y)$ defined as $g(x) = y$ and let $d\phi_x(y)$ be the $\text{tp}(a/\text{acl}(L))$ -definition of ϕ over $\text{dcl}(F, b)$. Clearly, $d\phi_x(e')$ iff $e = e'$, and so $e \in \text{dcl}(F, b)$. \square

Proof of theorem 3.15. Let $L = F\langle b \rangle^s$.

(ii) and (iii) are easy.

For (i), observe that as K/F is strongly normal, conditions (1), (2) (by lemma 3.16) and (3) of the definition of strongly normal extensions immediately hold in K/L . Condition (4) requires an explanation:

The correspondence provided by lemma 3.13 allows us to see $D = \text{acl}(L) \cap K$ as a subset of \mathcal{M}_0^{eq} . Consider then, in \mathcal{M} , the type $\text{tp}(a/D)$. Since $K = L\langle a \rangle^s$, the canonical base of $\text{tp}(a/\text{acl}(L))$ is contained inside D . By ω -stability of $\text{Th}(\mathcal{M})$, we have that $\text{Cb}(\text{tp}(a/\text{acl}(L)))$ is interdefinable with d , a single finite tuple in \mathcal{M}^{eq} . It is easy to check that $L\langle d \rangle^s = D$.

Finally, for (iv), suppose that L/F is strongly normal and let N be the normalizer of $\text{Gal}(K/L)$ in $\text{Gal}(K/F)$. As both $\text{Gal}(K/L)$ and $\text{Gal}(K/F)$ are definable, so is N . Thus, by part (3) of the present theorem, $N = G_{L'}$ for some L' such that $F < L' < L$. We will prove that $N = \text{Gal}(K/F)$:

Let $\sigma \in \text{Gal}(K/F)$, an automorphism $\tau \in \text{Gal}(K/L)$ and $d \in L$. Since L/F is strongly normal, $\sigma(d) \in L\langle \mathcal{C} \rangle$ and so $\tau\sigma(d) = \sigma(d)$. This implies that $\sigma^{-1}\tau\sigma(d) = d$ and thus we conclude that $\sigma^{-1}\tau\sigma \in \text{Gal}(K/L)$ and, moreover, $\sigma \in N$ as $\tau \in \text{Gal}(K/L)$ is arbitrary.

Assume now that $G_L = \text{Gal}(K/L)$ is a normal subgroup of $\text{Gal}(K/F)$. Conditions (1), (2) and (4) from the definition of strongly normal extensions are clear for L/F . We need to prove (3): Let $\sigma: L \hookrightarrow \mathcal{U}$ be an embedding of L into \mathcal{U} over F . Because of saturation of \mathcal{U} and quantifier elimination, there is $\bar{\sigma}$ an embedding of K into \mathcal{U} over F such that $\sigma = \bar{\sigma}|_L$. Since K/F is strongly normal, $\bar{\sigma}$ can be seen as an element of $\text{Gal}(K/F)$ (lemma 3.6). Let $d \in L$, we need to show that $\sigma(d) \in L\langle \mathcal{C} \rangle$: Consider $\tau \in \text{Gal}(K/L)$ and observe that, as $\text{Gal}(K/L)$ is normal in $\text{Gal}(K/F)$, we have that

$$\bar{\sigma}^{-1}\tau\bar{\sigma}(d) = \sigma^{-1}\tau\sigma(d) = d.$$

That is, $\tau(\sigma(d)) = \sigma(d)$. As τ is arbitrary, this implies that $\sigma(d)$ belongs to the set fixed by $\text{Gal}(K/L)$, which is precisely $L\langle \mathcal{C} \rangle$.

Finally, consider the restriction map

$$|_{L\langle \mathcal{C} \rangle}: \text{Gal}(K/F) \rightarrow \text{Gal}(L/F).$$

This map is onto because of saturation of \mathcal{U} and quantifier elimination, and its kernel is $\text{Gal}(K/L)$. This implies that $G(\mathcal{C})/G_L \cong \text{Gal}(L/F)$. \square

Theorem 3.17. *Let K/F be a strongly normal extension of ID-fields. Suppose F is relatively algebraically closed in \mathcal{U} . Then, there is $\alpha \in G(K)$ such that $K = F\langle \alpha \rangle$, and for all $\sigma \in \text{Gal}(K/F)$, we have that*

$$\sigma(\alpha) = (\mu(\sigma))^{-1} \cdot \alpha.$$

Proof. Let $b, c \in \mathcal{U}$ with $\text{tp}(b/F) = \text{tp}(a/F) = \text{tp}(c/F)$ such that $a \perp_F b$, $a \perp_F c$ and $c \perp_F b$. Using the notation from the proof of 3.5, it is clear that

$$h(a, b), h(a, c), h(c, b) \in G(\mathcal{U})$$

and

$$h(a, c) \cdot h(c, b) = h(a, b).$$

Replacing a, b, c by a, b, c plus finitely many derivations and p th-roots, we may assume h is rational. Since b is algebraically independent of a and c over F and F is relatively algebraically closed in \mathcal{U} , we can find $d \in F$ such that

$$h(a, d), h(c, d), h(a, c) \in G(\mathcal{U}),$$

and

$$h(a, c) \cdot h(c, d) = h(a, d). \quad (\star)$$

Let $\alpha = h(a, d)$. Observe first that α is interdefinable with a over F (because of the way h is defined) and so $K = F\langle\alpha\rangle$. Additionally, as $a, d \in K$, we have that $\alpha \in K$. Finally, let $\sigma \in \text{Gal}(K/F)$ and pick $c \perp_F \sigma(a)$. Then $\text{tp}(a, c/F) = \text{tp}(c, \sigma(a)/F)$ by stationarity. So

$$h(c, \sigma(a)) \cdot h(\sigma(a), d) = h(c, d).$$

But this, combined with (\star) implies that

$$h(a, c) \cdot h(c, \sigma(a)) \cdot h(\sigma(a), d) = h(a, d).$$

Now, $h(a, c) \cdot h(c, \sigma(a)) = \mu(\sigma)$ and $h(\sigma(a), d) = \sigma(\alpha)$ (because $\sigma(d) = d$). So, we have

$$\mu(\sigma) \cdot \sigma(\alpha) = \alpha.$$

Which is what was left to prove. \square

4. ITERATIVE DIFFERENTIAL GALOIS EXTENSIONS

In the previous section we introduced a class of ID-field extensions with well behaved Galois groups. Now, we will concentrate on the differential equations that under suitable conditions have good Galois theory.

4.1. Arc bundles and the iterative logarithmic derivative.

Definition 4.1. For a natural number m and an arbitrary field k , define $k^{(m)}$ as the ring $k[\epsilon]/(\epsilon^{m+1})$. View $k^{(m)}$ as a k -algebra under the natural map $a \mapsto a + 0\epsilon + \dots + 0\epsilon^m$.

Definition 4.2. Let X be an algebraic variety over F and define, for any field k extending F **the m^{th} arc bundle of X over k** , denoted $\mathcal{A}_m X(k)$, as the set of $k^{(m)}$ -rational points of X . This can be seen as an actual algebraic variety by identifying points in $k^{(m)}$ with points in (k^{m+1}) .

Now, if $f: X \rightarrow Y$ a (regular) map of algebraic varieties over F , then define

$$\mathcal{A}_m(f): \mathcal{A}_m X \rightarrow \mathcal{A}_m Y$$

as the map which is given, on k -points, by evaluating f on $X(k^{(m)})$.

Fact 4.3. Let X, Y and Z be algebraic varieties over F .

- (1) $\mathcal{A}_m(X) \times \mathcal{A}_m(Y)$ is naturally isomorphic to $\mathcal{A}_m(X \times Y)$.

- (2) Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are regular maps defined over F , then $\mathcal{A}_m(g \circ f) = \mathcal{A}_m(g) \circ \mathcal{A}_m(f)$. This is, \mathcal{A}_m is a functor from the category of algebraic varieties with regular maps over F to itself.
- (3) If (G, \cdot) is an algebraic group defined over F , then so is $(\mathcal{A}_m G, \mathcal{A}_m(\cdot))$.

Proof. (1) and (2) are immediate consequences of the given definition of \mathcal{A} , and (3) follows from those two. For instance, for associativity, consider the commutative diagram,

$$\begin{array}{ccc} (g_1, g_2, g_3) & \xrightarrow{\quad} & (g_1 \cdot g_2, g_3) \\ \downarrow & & \downarrow \\ (g_1, g_2 \cdot g_3) & \xrightarrow{\quad} & (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \end{array}$$

and then apply \mathcal{A}_m . □

For $n > m$, the quotient map $k^{(n)} \rightarrow k^{(m)}$ induces a projection

$$\rho_{n,m}: \mathcal{A}_n X \rightarrow \mathcal{A}_m X.$$

Identifying \mathcal{A}_0 with the identity functor we will write $\rho_{n,0}$ as ρ_n .

Definition 4.4. For $a \in X(k)$, the n^{th} arc space $\mathcal{A}_n X_a$ of X at a is defined as the fibre of $\rho_n: \mathcal{A}_n X \rightarrow X$ over a .

Additionally, define $\mathcal{A}X(k)$, the full arc bundle of X over k , as the inverse limit of $(\mathcal{A}_i X(k))_{i \in \omega}$.

Observe that $\mathcal{A}X(k)$ can be identified with the $k[[\epsilon]]$ -rational points of X .

Let us consider now the case when F is a ID -field of positive characteristic. As before, assume \mathcal{U} is a highly saturated model of $SCH_{p,1}$.

Lemma 4.5. Let X be an algebraic variety defined over C_F .

If $a \in X(\mathcal{U})$, then $\nabla_X(a) = (\partial_0(a), \partial_1(a), \dots) \in \mathcal{A}X(\mathcal{U})$ and in particular $\nabla_{X,m}(a) = (\partial_0(a), \dots, \partial_m(a)) \in \mathcal{A}_m X(\mathcal{U})$ for any m .

Additionally, if Y is an algebraic variety, $f: X \rightarrow Y$ is a morphism and both are also defined over C_F , then $\mathcal{A}(f) \circ \nabla_X = \nabla_Y \circ f$.

Proof. Before starting, observe that $\nabla_X(a)$ is just another way of presenting $\mathbb{D}_\partial(a)$ once you identify, as suggested above, $\mathcal{A}X(\mathcal{U})$ and $X(\mathcal{U}[[\epsilon]])$.

For the first part, recall that $\mathbb{D}_\partial: \mathcal{U} \rightarrow \mathcal{U}[[\epsilon]]: x \rightarrow \sum_{i=0}^{\infty} \partial_i(x)\epsilon^i$ is a ring homomorphism. Then, working locally, if $p(x)$ is one of the defining polynomials of X and $a \in X(\mathcal{U})$, then $p(\mathbb{D}_\partial(a)) = 0$. Which is another way of saying that $\nabla_X(a) \in \mathcal{A}X(\mathcal{U})$.

For the second part, note that \mathbb{D}_∂ is not only a ring homomorphism but a \mathcal{C} -algebra homomorphism. Thus, again locally, if $q(x)$ is a polynomial with constant coefficients, then $\mathbb{D}_\partial(q(x)) = q(\mathbb{D}_\partial(x))$. □

Corollary 4.6. If (G, \cdot) is an algebraic group defined over the constants of F , then $(\mathcal{A}G, \mathcal{A}(\cdot))$ is also a group and $\nabla_G: G \rightarrow \mathcal{A}(G)$ is a group embedding.

Proof. Since (G, \cdot) is an inverse limit of algebraic groups, it is a pro-algebraic group. For the second part, the previous lemma gives us that $\nabla_G \circ \cdot = \mathcal{A}(\cdot) \circ \nabla_{G \times G}$. □

Let G be an algebraic group defined over C_F and consider the following exact sequence of groups:

$$\{(e, 0)\} \longrightarrow \mathcal{A}_e(G) \xrightarrow{i} \mathcal{A}(G) \xrightarrow{\pi} G \longrightarrow \{e\},$$

where i is the natural inclusion and π the canonical projection. Note that $s: G \rightarrow \mathcal{A}(G): g \mapsto (g, 0, 0, \dots)$ is a group embedding and so a homomorphic section of π . Recall also that the existence of such a homomorphic section provides us with an isomorphism $\mathcal{A}(G) \cong \mathcal{A}_e(G) \rtimes G$. Thus, we can identify G with its image under s . Let $h: \mathcal{A}(G) \rightarrow \mathcal{A}_e(G)$ be the projection induced by this isomorphism. Given $(g, u) \in \mathcal{A}(G)$, we have that $(g, u) = ((g, u) \cdot s(g^{-1})) \cdot s(g)$, so $h((g, u)) = (g, u) \cdot s(g^{-1})$.

Although h is not a group homomorphism, we have:

Fact 4.7. *If $h((g, u)) = h((l, v))$ then $h((g, u)^{-1} \cdot (l, v)) = (e, 0)$.*

Proof. Since $h((g, u)) = h((l, v))$, then, by definition,

$$(g, u) \cdot s(g^{-1}) = (l, v) \cdot s(l^{-1}).$$

Reorganizing the equation, we get

$$(g, u)^{-1} \cdot (l, v) = s(g^{-1}) \cdot s(l).$$

Now, applying h to both sides, we obtain

$$h((g, u)^{-1} \cdot (l, v)) = h(s(g^{-1}l)) = s(g^{-1}l) \cdot s(l^{-1}g) = (e, 0).$$

□

Definition 4.8. Define the **iterative logarithmic derivative** be the map

$$\ell D: G(\mathcal{U}) \rightarrow \mathcal{A}G_e(\mathcal{U}): g \mapsto h(\nabla(g)).$$

Fact 4.9. *If G is defined over C_F , then $\text{Ker}(\ell D) = G(\mathcal{C})$. Furthermore, if $\ell D(x) = \ell D(y)$, then $x^{-1} \cdot y \in G(\mathcal{C})$.*

Proof. If $\ell D(g) = (e, 0)$, then $\nabla(g) \cdot (g^{-1}, 0) = (e, 0)$. Thus $\nabla(g) = (g, 0)$, which implies that $\partial_i(g) = 0$ for any i . That is, $g \in G(\mathcal{C})$.

The additional remark is a direct consequence of fact 4.7. □

The logarithmic derivative in the (differential) characteristic zero case, defined as a map from G to $\mathcal{L}(G)$, the Lie algebra of G , is surjective. In our setting, that is not the case:

Example 4.10. Let $G = \mathbb{G}_a$, the additive group. Then $\mathcal{A}(G) = \sum_{i=0}^{\infty} \mathbb{G}_a$ and

$$\ell D(g) = (g, \partial_1(g), \dots) - (g, 0, \dots) = (0, \partial_1(g), \partial_2(g), \dots).$$

Thus, $\text{Im}(\ell D)$ is contained in the set

$$\{(x_i): x_0 = 0 \text{ and, for } i > 0, \partial_j(x_i) = \binom{i+j}{i}(x_{i+j})\},$$

which is clearly not equal to $\mathcal{A}_e(G)$.

4.2. Logarithmic differential equations and Galois extensions.

Definition 4.11. Given an algebraic group defined over the constants of (F, ∂) a (non-trivial) definably closed ID -field of characteristic p with algebraically closed constant field, by a **consistent logarithmic differential equation** over F we mean something of the form

$$\ell D(x) = \alpha,$$

where ℓD is defined as in the previous section and $\alpha \in \mathcal{AG}_e(F)$ is an element contained in the image of ℓD .

By an **iterative differential Galois extension** of F for that given logarithmic differential equation we mean $K = F\langle a \rangle^s$, where $\ell D(a) = \alpha$ and $C_F = C_K$.

Theorem 4.12 (Existence and Uniqueness of iterative differential Galois extensions). *If G is an algebraic group defined over the constants of (F, ∂) and $\ell D(x) = \alpha$ is a (consistent) logarithmic differential equation over F , then there exists an iterative differential Galois extension of F for the given equation. Furthermore, any two such extensions are isomorphic over F as ID -fields.*

Once again, we will depend on the use of an appropriate auxiliary structure in order to prove this. Let \mathcal{M} be the two-sorted structure $(\mathcal{X}, \mathcal{C})$, where \mathcal{X} is the set of solutions in \mathcal{U} of the equation $\ell D(x) = \alpha$, and the relations of \mathcal{M} are those induced by F -definable sets in \mathcal{U} .

Lemma 4.13. *\mathcal{M} is saturated, its theory $\text{Th}(\mathcal{M})$ has quantifier elimination, it is totally transcendental and, additionally,*

$$\mathcal{M}_0 \cap \mathcal{C} = C_F.$$

Proof. Just as in the proof of fact 3.11, this depends on the bi-interpretability of an expansion of \mathcal{M} by a constant and another simpler structure. Let a' be any solution of the given logarithmic differential equation and let \mathcal{N} be the structure whose universe is \mathcal{C} and whose relations are induced by the $F\langle a' \rangle$ -definable sets in \mathcal{U} . We will see that \mathcal{N} is bi-interpretable with (\mathcal{M}, a') :

Let $Y = G(\mathcal{C})$. As a subset of \mathcal{N} , we have that Y is definable. Observe that there is a one-to-one correspondence between \mathcal{X} and Y . This is given by the fact that, for any $b \in \mathcal{X}$, there is $g \in G(\mathcal{C})$ such that $g \cdot a' = b$ (a corollary of fact 4.7). Note that such g is unique given b and a' . Let $f: Y \rightarrow \mathcal{X}: g \mapsto g \cdot a'$. The fact that \mathcal{X} and Y are isomorphic via this function is proved as in fact 3.10. This shows that \mathcal{X} (and so \mathcal{M}) is interpretable in \mathcal{N} . The fact that \mathcal{N} is interpreted in (\mathcal{M}, a) is clear.

Note that \mathcal{N} is, once again, totally transcendental and saturated, and thus the argument used to prove fact 3.11 applies. Hence, \mathcal{M} is also saturated and totally transcendental. The same is true for proving that \mathcal{M} has quantifier elimination.

The proof that $\mathcal{M}_0 \cap \mathcal{C} = C_F$ is exactly the same given for lemma 3.12. \square

We now go back to the proof of theorem 4.12:

Proof of theorem 4.12. (Existence) Let $a \in \mathcal{M}_0 \cap \mathcal{X}$ and $K = F\langle a \rangle^s$. It is not hard to see that $C_F = C_K$.

(*Uniqueness*) Let $a' \in \mathcal{X}$ be such that $K' = F\langle a' \rangle^s$ is another iterative differential Galois extension of F for the given equation.

Consider \mathcal{M}_1 prime over a' . Note that $\mathcal{M}_1 \cap \mathcal{C} = C_F$. Let $a'' \in \mathcal{M}_1$ with the same type as a over the empty set. As $\mathcal{M}_1 \prec \mathcal{M}$, there is $g \in \mathcal{M}_1 \cap \mathcal{C} = C_F$ such that $a'' \cdot g = a'$. This implies that $\text{dcl}(Fa') = \text{dcl}(Fa'')$.

Finally, since $\text{tp}(a) = \text{tp}(a'')$ in \mathcal{M} , then $\text{tp}(a/F) = \text{tp}(a''/F)$ in \mathcal{U} . This, by saturation, implies that $\text{dcl}(Fa)$ is isomorphic to $\text{dcl}(Fa'') = \text{dcl}(Fa')$. \square

5. WHAT GOES AROUND COMES AROUND

Section 3 introduced a class of extensions of differential fields with good Galois theory. Section 4 provided us with extensions of differential fields related to iterative logarithmic differential equations. In this section we will prove that, under certain conditions on the base field, these two notions coincide.

Theorem 5.1. *If K is an iterative differential Galois extension of F for a given logarithmic differential equation $\ell D(x) = \alpha$, then K/F is a strongly normal extension.*

Proof. The first two conditions of the definition of strongly normal extensions are explicitly stated in our definition of ID -Galois extensions. For the third one, let $K = F\langle a \rangle^s$, and $\text{tp}(a'/F) = \text{tp}(a/F)$. Since $\alpha \in \mathcal{AG}_e(F)$ and $\ell D(a) = \alpha$, we have that $\ell D(a') = \alpha$, and this implies that $a^{-1}a' \in G(\mathcal{C})$ by fact 4.9. So, $a' = a \cdot d$ for some $d \in G(\mathcal{C})$ and thus $a' \in K\langle \mathcal{C} \rangle$. Finally, for the fourth condition, the argument goes exactly as in the proof of the first part of theorem 3.15. \square

Theorem 5.2. *Suppose F is relatively algebraically closed in \mathcal{U} and K/F is a strongly normal extension. Let G be the algebraic group over C_F that is provided by theorem 3.5 whose set of \mathcal{C} -rational points is isomorphic to $\text{Gal}(K/F)$. Then K/F is an iterative differential Galois extension for some logarithmic differential equation on G .*

Proof. Let K/F be a strongly normal extension and G as in the statement. Let

$$\mu: \text{Gal}(K/F) \rightarrow G(\mathcal{C})$$

witness the isomorphism.

Since F is relatively algebraically closed in \mathcal{U} , the primitive element theorem provides us with $a \in G(K)$ such that $K = F\langle a \rangle$ and, for any $\sigma \in \text{Gal}(K/F)$, we have that $\sigma(a) = (\mu(\sigma))^{-1} \cdot a$.

Let $\alpha = \ell D(a)$ and note that α is fixed by any automorphism of \mathcal{U} fixing F : let $\bar{\xi} \in \text{Aut}(\mathcal{U}/F)$; since K/F is strongly normal, lemma 3.6 tells us that $\xi = \bar{\xi}|_{K(\mathcal{C})} \in \text{Gal}(K/F)$, and so $\xi(a) \cdot a^{-1} = (\mu(\xi))^{-1} \in G(\mathcal{C}) = \text{Ker}(\ell D)$. Thus,

$$\bar{\xi}(\alpha) = \ell D(\xi(a)) = \ell D(a) = \alpha.$$

Since F is relatively algebraically closed in \mathcal{U} , we get that $\alpha \in \mathcal{AG}_e(F)$.

Consider the iterative logarithmic differential equation $\ell D(x) = \alpha$. Let $K' = \text{dcl}(Fa')$ be the *unique* iterative differential Galois extension of F for the given equation. Note that, since $\ell D(a) = \ell D(a')$, fact 4.9 tells us that

there exists $g \in G(\mathcal{C})$ such that $a' = g^{-1} \cdot a$. Since $g \in G(\mathcal{C})$ there is $\sigma \in \text{Gal}(K/F)$ such that $\mu(\sigma) = g$. So, by the way a was chosen,

$$a' = ((\mu(\sigma))^{-1} \cdot a = \sigma(a),$$

which implies that σ induces an isomorphism between K and K' . Thus K is isomorphic to a Galois differential extension of F for an appropriate logarithmic differential equation. \square

To conclude, let us prove, under the same assumption on the base field, that a desirable equality between the transcendence degree of a strongly normal extension and the dimension of its Galois group holds. To be precise:

Theorem 5.3. *Suppose F is relatively algebraically closed in \mathcal{U} , the extension K/F is strongly normal, and G is an algebraic group over C_F such that $G(\mathcal{C})$ is isomorphic to $\text{Gal}(K/F)$. Then,*

$$\dim(G(\mathcal{C})) = \text{tr. deg}(K/F).$$

Proof. By the previous result, we know that K is an iterative differential Galois extension of F for a consistent logarithmic differential equation $\ell D(x) = \alpha$ on $G(\mathcal{U})$ with α in F . That is, there is $a \in G(K)$ such that $\ell D(a) = \alpha$ and $K = F\langle a \rangle^s$.

First note that $K = F(a)^s$. To prove this, it is enough to see that $\partial_n(a) \in F(a)$ for all $n \in \omega$. However, by the definition of the logarithmic derivative, we know that $\nabla(a) = \alpha \cdot (a, 0, 0, \dots)$, thus coordinate by coordinate, we obtain that $\partial_n(a)$ is a rational function of a and the coefficients of α , which are all in F . This in particular implies that $\text{tr. deg}(K/F) = \text{tr. deg}(F(a)/F)$.

Secondly, by fact 4.9, we know that for each $a', a'' \in \mathcal{X}$, where \mathcal{X} is the solution set in $G(\mathcal{U})$ of the equation, there is $g \in G(\mathcal{C})$ such that $g \cdot a' = a''$. Since $G(\mathcal{C})$ is precisely our isomorphic copy of $\text{Gal}(K/F)$, this implies that, in \mathcal{U} , any $a' \in \mathcal{X}$ has the same type as a over F . Thus, $\text{tr. deg}(K/F)$ is in fact equal to $\text{tr. deg}(\mathcal{X})$.

Finally, observe that, after naming $a \in \mathcal{X}$, there is a rational bijection between \mathcal{X} and $G(\mathcal{C})$ given by $a' \mapsto a^{-1} \cdot a'$. So, $\text{tr. deg}(K/F) = \text{tr. deg}(\mathcal{X}) = \text{tr. deg}(G(\mathcal{C})) = \dim(G(\mathcal{C}))$. \square

REFERENCES

- [1] Y. André, *Différentielles non-commutatives et théorie de Galois différentielle ou aux différences*, Annales Scientifiques de l'Ecole Normale Supérieure, Vol. 34, n. 5, September 2001 (pp. 685-739).
- [2] F. Benoist, *Théorie des modèles des corps munis d'une dérivation de Hasse*. PhD. Thesis, Équipe de Logique Mathématique, Université Paris 7 - Denis Diderot, 2005. Available online at <http://tel.archives-ouvertes.fr/tel-00134889>.
- [3] F. Delon, *Separably Closed Fields*, in *Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*. Springer, 1999.
- [4] L.P.D. van den Dries, *Weil's group chunk theorem: A topological setting*. Illinois Journal of Mathematics, Vol. 34, n. 1, Spring 1990 (pp. 127-139).
- [5] E. Hrushovski, *Unidimensional theories are superstable*. Annals of Pure and Applied Logic 50, 1990 (pp 117-138).
- [6] E. Hrushovski, *Computing the Galois group of a linear differential equation*. Differential Galois theory (Bedlewo, 2001), Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002 (pp. 97-138).

- [7] E.R. Kolchin, *Differential Algebra and Algebraic Groups*. Academic Press, 1973.
- [8] J. Kovacic, *The differential Galois theory of strongly normal extensions*, Transactions of the American Mathematical Society, vol. 355, n. 11, 2003 (pp. 4475-4522).
- [9] A. Magid, *Differential Galois Theory*. Mem. AMS, 1994.
- [10] H. Matzat, *Differential Galois theory in positive characteristic*, notes written by Julia Hartmann. Preprint, 2001.
- [11] M. Messmer and C. Wood, *Separably closed fields with higher derivations*. Journal of Symbolic Logic, Vol. 60, n. 3, Sep. 1995 (pp. 898-910).
- [12] K. Okugawa, *Basic properties of differential fields of arbitrary characteristic and the Picard-Vessiot theory*. Journal of mathematics of Kyoto University, Vol. 2, n. 3, 1963 (pp. 294-322).
- [13] K. Okugawa, *Differential Algebra of Nonzero Characteristic*. Lectures in Mathematics 16. Kinokuniya Company Ltd., Tokyo, 1987
- [14] A. Pillay and D. Marker, *Differential Galois theory III: Some inverse problems*. Illinois Journal of Mathematics, Vol. 3, 1997 (pp. 453-461).
- [15] A. Pillay, *Differential Galois theory II*. Annals of Pure and Applied Logic 88, 1997 (pp. 181-191).
- [16] A. Pillay, *Differential Galois theory I*. Illinois Journal of Mathematics, Vol. 42, n. 4, Winter 1998 (pp. 678-699).
- [17] A. Pillay, *Two remarks on differential fields*. Quaderni di matematica, Vol. 11 (Model Theory and Applications), 2002.
- [18] A. Pillay, *Algebraic D-groups and differential Galois theory*. Pacific J. Math 216, 2004 (pp. 343-360).
- [19] A. Pillay and Ž. Sokolović, *Superstable differential fields*. Journal of Symbolic Logic, Vol. 56, n. 1, Mar 1992 (pp. 97-108). Universitext Series, 2000.
- [20] B. Poizat, *Stable Groups*. AMS, 2001.
- [21] B. Poizat, *Une théorie de Galois imaginaire*. Journal of Symbolic Logic, Vol. 48, n. 4, Dec 1983 (pp. 1151-1170).
- [22] M. van der Put and M. Singer, *Galois Theory of Linear Differential Equations*. Springer, 2003.
- [23] K. Shikishima-Tsuji, *Galois theory of differential fields of positive characteristic*. Pacific J. Math, Vol. 138, n. 1, 1989 (pp. 151-168).
- [24] H. Umemura, *Galois theory and Painlevé equations*. Séminaires & Congrès 14, 2006 (pp. 299-339).
- [25] M. Ziegler, *Separably closed fields with Hasse derivations*. Journal of Symbolic Logic, Vol. 68, n. 1, Dec 2003 (pp. 311-318).
- [26] B. Zilber, *Totally categorical theories: structural properties and non-finite axiomatizability in Model theory of algebra and arithmetic* (ed. L. Pacholski et al.). Springer, 1980 (pp. 381-410).

INSTITUT CAMILLE JORDAN, UNIVERSITÉ CLAUDE BERNARD LYON 1, 43 BOULEVARD
DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE CEDEX, FRANCE

E-mail address: moreno@math.univ-lyon1.fr

URL: <http://math.univ-lyon1.fr/~moreno/>