

© 2008 Javier A. Moreno

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

BY

JAVIER A. MORENO

DISSERTATION

Submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy in Mathematics  
in the Graduate College of the  
University of Illinois at Urbana-Champaign, 2008

Urbana, Illinois

Doctoral Committee:

Professor C. Ward Henson, Chair  
Professor Lou van den Dries  
Professor Emeritus Anand Pillay  
Professor David Marker, UIC

# Abstract

This thesis 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. Instead of taking an algebraic approach, we use the methods and framework provided by the model theory of iterative differential fields. After defining what we mean by a strongly normal extension of iterative differential fields, we prove that these extensions have good Galois theory and that a G-primitive element theorem holds. Then, 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.

*To Gloria the Wise, Mónica the Silent and Plinio the Cat.  
(And to Alf the Hugger, missing him, everyday.)*

Civilization did not rise and flourish as men hammered out hunting scenes on bronze gates and whispered philosophy under the stars, with garbage as a noisome offshoot, swept away and forgotten. No, garbage rose first, inciting people to build a civilization in response, in self-defense. We had to find ways to discard our waste, to use what we couldn't discard, to reprocess what we couldn't use. Garbage pushed back. It mounted and spread. And it forced us to develop the logic and rigor that would lead to systematic investigations of reality, to science, art, music, mathematics.

Don DeLillo, *Underworld*

# Acknowledgements

Anand Pillay suggested this problem to me when I asked for possible applications of model theory to differential algebra. It was a good pick. For this, and for his constant encouragement, patience, example and support during the course of this thesis, I thank him.

I would like to acknowledge the conversations and e-mail exchanges I had with Clif Ealy, Piotr Kowalski, Sonat Suer, Alf Onshuus, Martin Ziegler, Franck Benoist, Andrés Villaveces, Alex Berenstein, Rodrigo Peláez, Enrique Casanovas and Françoise Delon, among others. I doubt I could have found my way through this dissertation without their help. I also appreciate the suggestions and comments that I got from Lou van den Dries and Dave Marker as members of my defense committee.

Part of this thesis was written during my short visit to the University of Leeds, in Fall 2005. There, I enjoyed the hospitality of Dugald Macpherson and the Leeds Logic Group. In Barcelona, where I live now, I was fortunately adopted by the Model Theory Group at the Universitat de Barcelona. To them, as well as to the whole UIUC Logic Group, I am grateful. I learned lots of mathematics in each of these places.

I am especially indebted to Ward Henson for the permanent guidance and kind help he has given me throughout my graduate career. And also to Dominika, Jana, Ayhan, Francina, Juan, Mercedes and Nano for their friendship and company. My Chambana life was happy, fun and interesting mainly because of them.

I thank my mom, Gloria, for teaching me how to read, giving me books to practice, and supporting me in everything I have done with my life ever since then.

Finally, I thank Mónica, who loves me, bears me, holds my hand, and does not let me cross the street without looking both ways first.

# Table of Contents

<b>Introduction</b> . . . . .	<b>vii</b>
<b>Chapter 1 Background and preliminaries</b> . . . . .	<b>1</b>
1.1 Stability, fields and groups . . . . .	1
1.1.1 Stable theories . . . . .	1
1.1.2 Examples: Some stable fields . . . . .	3
1.1.3 Groups interpretable in stable theories . . . . .	5
1.2 Internality and Galois theory . . . . .	5
1.2.1 Differential Galois theory in characteristic zero . . . . .	6
1.3 Historic and bibliographical notes . . . . .	7
<b>Chapter 2 Iterative differential algebra</b> . . . . .	<b>9</b>
2.1 Basic definitions . . . . .	9
2.2 Model theory of ID-fields . . . . .	12
2.3 Historic and bibliographical notes . . . . .	13
<b>Chapter 3 Iterative strongly normal theory</b> . . . . .	<b>15</b>
3.1 Definition and basic remarks . . . . .	15
3.2 Definability of the Galois group . . . . .	17
3.3 Scaffolding . . . . .	20
3.4 Galois correspondence and a G-primitive element theorem . . . . .	22
3.5 Historic and bibliographical notes . . . . .	25
<b>Chapter 4 Iterative differential Galois extensions</b> . . . . .	<b>27</b>
4.1 Arc bundles and the iterative logarithmic derivative . . . . .	27
4.2 Logarithmic differential equations and Galois extensions . . . . .	30
4.3 Strongly normal extensions revisited . . . . .	33
4.4 Historic and bibliographical notes . . . . .	34
<b>References</b> . . . . .	<b>36</b>
<b>Author's Biography</b> . . . . .	<b>39</b>

# Introduction

What is a repetition? A repetition is a re-enactment of past experience toward the end of isolating the time segment which has lapsed in order that it, the lapsed time, can be savored of itself and without the usual adulteration of events that clog time like peanuts in brittle.

Walker Percy, *The Moviegoer*

In the preface to his book *Differential Algebra and Algebraic Groups* [13], Ellis Robert Kolchin suggested that one way of generalizing to positive characteristic the differential Galois theory in characteristic zero—that he had developed following the works of Ritt, Picard and Vessiot—could be changing the definition of differential ring

by replacing the notion of a derivation  $\delta$  by the notion of a “differentiation”  $(\delta^{(k)})_{k \in \mathbb{N}}$  in the sense of Helmut Hasse and F. K. Schmidt.

There have been several attempts to achieve this goal since then. Kôtarô Okugawa, for instance, restricted himself to the linear (Picard-Vessiot) case in [26] with some success and then, a few years later, offered a first version of a strongly normal theory [27]. More recently, Heinrich Matzat and Marius van der Put came up with a careful and quite complete geometric presentation of the Picard-Vessiot theory for Hasse-Schmidt differentiations (also called iterative derivations) using torsors [19].

The aim of this thesis is to adapt Kolchin’s strongly normal theory to positive characteristic iterative differential algebra using tools provided by model theory and generalizing what Matzat and van der Put did in the linear case.

Differential Galois theory and model theory have had a long history. It all started with Bruno Poizat’s paper *Une théorie de Galois imaginaire* [37] suggesting that Kolchin’s main results could be obtained as a consequence of the  $\omega$ -stability of the theory of differentially closed fields and some work by Boris Zilber and Ehud Hrushovski on the definability of automorphism groups [10][41]. After this, several people including Dave Marker, Anand Pillay and Željko Sokolović 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 Margit Messmer, Carol Wood and Martin Ziegler proved—strongly based on Françoise Delon’s work on separably closed fields

of positive characteristic— that the theory of fields equipped with stacks of commuting iterative derivations had a stable model companion with quantifier elimination and elimination of imaginaries [23][40]. After this, adapting some of his previous results in characteristic zero, and working along the lines of what Ehud Hrushovski suggested in [11], Anand 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 [29]. This thesis is, then, a natural follow-up to what Pillay did.

After introducing in Chapter 1 the tools from model theory that we are going to use and the basics of iterative differential algebra in Chapter 2, we start by defining in Chapter 3 a class of extensions of iterative differential fields (ID-fields, from now on) with well behaved Galois groups. We call them **iterative strongly normal extensions**. In particular we prove (Theorem 3.5) that their Galois groups are isomorphic to algebraic groups:

**1 Theorem** (Definability of  $\text{Gal}(K/F)$ ). *Let  $\mathcal{U}$  be a universal domain for the theory of iterative differential fields where any ID-field mentioned is embedded, and let  $\mathcal{C}$  be its field of constants. Let  $F \subseteq \mathcal{U}$  be an ID-field and let  $K = F\langle a \rangle$  be an iterative strongly normal extension of  $F$ . Then there is an isomorphism*

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

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

Once we have proved that the Galois group is definable inside our model theoretical framework, we also get, making strong use of an associated type-definable totally transcendental structure, a Galois correspondence (Theorem 3.14):

**2 Theorem** (Galois correspondence). *Let  $K$  be a strongly normal extension of  $F$ . Then there is a good Galois correspondence between the set of definably closed subfields of  $K$  containing  $F$  and the set of algebraic subgroups of  $\text{Gal}(K/F)$ .*

Further, we get a version of the  $G$ -primitive element theorem of Kolchin for a particular class of base fields (those relatively algebraically closed inside  $\mathcal{U}$ ) (Theorem 3.15):

**3 Theorem** ( $G$ -primitive element theorem). *Let  $K/F$  be strongly normal and suppose  $F$  is relatively algebraically closed in  $\mathcal{U}$ . Let  $G$  and  $\mu$  be as in the conclusion of Theorem 1. Then there is  $\alpha \in G(K)$  such that  $K = \text{dcl}(F\alpha)$ , and for all  $\sigma \in \text{Gal}(K/F)$  we have that  $\sigma(\alpha) = (\mu(\sigma))^{-1} \cdot \alpha$ .*

Then, in Chapter 4, we turn our emphasis from extensions to equations. For this, we define, making use of the theory of arc spaces of algebraic varieties, the **iterative logarithmic derivative** ( $\ell D$ ) on an algebraic group  $G$  over

the constants of an ID-field  $F$ , and after this we introduce the **iterative logarithmic differential equations**. Given a base ID-field  $F$  and an appropriate iterative logarithmic differential equation, we define the notion of an **iterative differential Galois extension** of  $F$  for the given equation.

Our main result on this topic (Theorem 4.9) goes as follows:

**4 Theorem** (Existence and uniqueness of iterative differential Galois extensions). *If  $G$  is an algebraic group defined over the constants of  $(F, \partial)$  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.*

Finally, we prove that iterative normal extensions and iterative differential Galois extensions coincide under certain extra assumptions (Theorems 4.11 and 4.12).

**5 Theorem.** *Suppose  $K/F$  is an extension of ID-fields.*

1. *On one hand, if  $K/F$  is an iterative differential Galois extension for a given logarithmic differential equation  $\ell D(x) = \alpha$ , then it is also a strongly normal extension.*
2. *On the other hand, if  $F$  is relatively algebraically closed in  $\mathcal{U}$ , and  $K/F$  is a strongly normal extension, then  $K/F$  is an iterative differential Galois extension for some logarithmic differential equation on an algebraic group  $G$  defined over  $C_F$ .*

In the case where  $F$  is relatively algebraically closed in  $\mathcal{U}$ , we also get an equality between the transcendence degree of the extension and the dimension of the Galois group (Theorem 4.13):

**6 Theorem.** *If  $F$  is relatively algebraically closed in  $\mathcal{U}$ , the extension  $K/F$  is strongly normal, and  $G$  is the algebraic group provided by Theorem 1 then*

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

# Chapter 1

## Background and preliminaries

Now, mathematical logic could extricate you from all this nonsensical existence.

Saul Bellow, *Zetland: By A Character Witness*

This first chapter intends to provide the reader with an overview of the model theoretic context on which this work is based. The reader of this thesis is assumed to have a working knowledge of the fundamentals of model theory and also a fair understanding of the terminology of varieties from algebraic geometry. In the last section of this chapter there is a list of general references on these subjects.

### 1.1 Stability, fields and groups

#### 1.1.1 Stable theories

Let  $T$  be an arbitrary first order theory in a language  $\mathcal{L}$  and let  $\mathcal{U}$  be a large saturated model of  $T$ . Unless otherwise specified,  $a, b, c, x, \dots$  will be (possibly infinite although generally finite) tuples of  $\mathcal{U}$ . We will denote small subsets of  $\mathcal{U}$  with capital letters  $(A, B, D, X, Y, \dots)$  and we will reserve  $M$  and  $N$  for small elementary submodels of  $\mathcal{U}$ . Usually  $F$  and  $K$  will be fields (with perhaps additional extra structure),  $G$  and  $H$  groups,  $m$  and  $n$  positive integers, and  $p$  and  $q$  (possibly partial) types.

Since we are going to make regular use of it during this work, let us start by recalling a classical construction due to Makkai: Given a structure  $M$  on the language  $\mathcal{L}$  we define  $M^{eq}$  as follows: for every  $\emptyset$ -definable equivalence relation  $E(x_1, \dots, x_n, y_1, \dots, y_n)$  on  $M^n$ , we add a new sort  $M^n/E$  and a new function symbol  $\pi_E$  to the language  $\mathcal{L}$  for the projection  $M \rightarrow M^n/E$ . We call the elements of the new sorts **imaginary elements** and we denote the resulting many-sorted structure  $M^{eq}$ . If, additionally,  $T$  is the theory of  $M$ , by  $T^{eq}$  we mean the complete theory of  $M^{eq}$  in the new language  $\mathcal{L}^{eq} = \mathcal{L} \cup \{\pi_E : E \text{ as above}\}$ . If  $\mathcal{U}$  is a monster model of  $T$ , then  $\mathcal{U}^{eq}$  turns out to be a monster model of  $T^{eq}$ . By  $dcl^{eq}$  and  $acl^{eq}$  we mean the definable closure and the algebraic closure on this expanded structure.

Given an infinite cardinal  $\lambda$ , we say that  $T$  is  $\lambda$ -**stable** if for any set  $A \subset \mathcal{U}$ , we have that  $|A| \leq \lambda$  if and only if  $S(A) \leq \lambda$ . Additionally, we say that  $T$  is

**stable** if it is  $\lambda$ -stable for some  $\lambda$ .

Among the class of stable theories, the totally transcendental ones, i.e. those with bounded global rank for definable sets, are particularly well behaved:

**1.1 Fact** (Models of totally transcendental theories). *If  $T$  is totally transcendental:*

- *It has a saturated model of any infinite cardinality.*
- *It also has a prime model.*

Recall that a type  $p(x) \in S(A)$  is said to be **definable** if for any formula  $\varphi(x, y)$ , there is a formula  $d\varphi_x(y) \in L(A)$  such that for any  $a \in A$ , we have that  $\varphi(x, a) \in p(x)$  if and only if  $\mathcal{U} \models d\varphi_x(a)$ .

**1.2 Fact.**  *$T$  is stable if and only if any complete type is definable.*

Stable theories are naturally endowed with a notion of independence (non-forking) defined as follows: Suppose  $A \subset \mathcal{U}$  and  $\psi(x, b)$  is a formula. We say that  $\psi(x, b)$  **forks** over  $A$  if there is an  $A$ -indiscernible sequence  $(b_i)_{i < \omega}$  with  $b_0 = b$  such that the set of formulas  $\{\psi(x, b_i) : i < \omega\}$  is inconsistent. Let  $\Pi(x)$  a partial type over  $B \supseteq A$  closed under finite conjunctions. In this case, we say that  $\Pi(x)$  **forks** over  $A$  if there is  $\psi(x, b) \in \Pi(x)$  such that  $\psi(x, b)$  forks over  $A$ . Finally, we say that a tuple  $c$  is **(forking) independent** from  $B$  over  $A$  if  $\text{tp}(c/B)$  does not fork over  $A$  and we denote this by  $c \downarrow_A B$ .

From now on, assume that  $T$  is stable.

**1.3 Fact** (Forking calculus). *Let  $a, b$  be tuples and  $A \subseteq B \subseteq C \subset \mathcal{U}$  be sets.*

- *Existence: If  $p(x) \in S(A)$  there is  $q(x) \in S(B)$ , an extension of  $p(x)$ , such that  $q(x)$  does not fork over  $B$ .*
- *Symmetry:  $a \downarrow_A b$  if and only if  $b \downarrow_A a$ .*
- *Transitivity:  $a \downarrow_A C$  if and only if  $a \downarrow_B C$  and  $a \downarrow_A B$ .*
- *Finite Character:  $a \downarrow_A B$  if and only if  $a \downarrow_A b$  for any finite tuple  $b$  from  $B$ .*

*Proof.* See proposition 2.20, p. 25 of [28] □

A theory is said to be **superstable** if for each  $A$  and  $p \in S(A)$ , there is a finite subset  $A_0 \subset A$  such that  $p$  does not fork over  $A_0$ .

The **multiplicity** of a type  $p \in S(A)$  is defined as the number of extensions of  $p$  to complete types over  $\text{acl}(A)$ . We denote it  $\text{mult}(p)$ . It can be proved that  $\text{mult}(p)$  is equal to the number of non-forking extensions of  $p$  to  $\mathcal{M}$ , for any model  $\mathcal{M}$  containing  $A$ . A complete type is said to be **stationary** if  $\text{mult}(p) = 1$ . In a stable theory any type over an algebraically closed set (in  $\mathcal{U}^{\text{eq}}$ ) is stationary.

**1.4 Fact** (Finite equivalence relation theorem). *Suppose we are in a stable theory. Let  $A \subseteq B$ , a complete type  $p(x) \in S(A)$  and  $q(x), r(x) \in S(B)$  two different non-forking extensions of  $p$ . Then, there is a finite  $A$ -definable equivalence relation  $E$  such that*

$$q(x) \cup r(y) \vdash \neg E(x, y).$$

*In particular, when  $\text{mult}(p)$  is finite there is a finite equivalence relation that distinguishes the non-forking extensions to any algebraically closed set containing  $A$ .*

*Proof.* See lemma 2.11, p. 20 of [28]. □

Let  $X \subset \mathcal{U}$  be a definable set. A possibly imaginary tuple  $c$  is a **canonical parameter** of  $X$  if  $c$  is fixed pointwise by exactly those automorphisms of  $\mathcal{M}$  that fix  $X$  setwise. Clearly, a canonical parameter for a given set  $X$  is unique up to interdefinability. A theory has **elimination of imaginaries** if any definable set has a canonical parameter. In general, however, a canonical parameter of  $X$  is an element in  $\mathcal{M}^{\text{eq}}$ . It is not hard to see that  $T^{\text{eq}}$  has elimination of imaginaries for any given  $T$ .

Consider a stationary type  $p \in S(A)$ . A **canonical base** of  $p$  is a (possibly infinite and imaginary) tuple fixed pointwise by exactly the same set of automorphisms of  $\mathcal{U}$  that fix the global non-forking extension of  $p$  to  $\mathcal{U}$ . Just as with the canonical parameter of a definable set, the canonical base of a stationary type is unique up to interdefinability. By  $\text{Cb}(p)$  we will mean, then, the definable closure of any canonical base of  $p$ . In a stable theory, any stationary type has a canonical base.

**1.5 Fact** (Properties of the canonical base). *Let  $p \in S(A)$  be stationary.*

- $\text{Cb}(p) \subseteq \text{dcl}(A)$ .
- For any  $B \subseteq A$ , the type  $p$  does not fork over  $B$  if and only if  $\text{Cb}(p) \subseteq \text{acl}(B)$ .
- If  $T$  is totally transcendental, the canonical base of  $p$  is interdefinable with a single finite tuple.

*Additionally, in general,  $\text{Cb}(\text{tp}(a/\text{acl}(A))) \subseteq \text{dcl}(Aa)$  for arbitrary  $a$  and  $A$ .*

*Proof.* See remark 2.26, p. 29 of [28]. □

## 1.1.2 Examples: Some stable fields

### Algebraically closed fields and Differentially closed fields

Let  $L_r$  be the language  $\{+, -, \cdot, 0, 1\}$  and let  $p$  be either 0 or a prime number. Let  $\text{ACF}_p$  be the set of  $L_r$ -sentences expressing that its models are algebraically closed fields of characteristic  $p$ .

**1.6 Fact** ( $\text{ACF}_p$ ).  *$\text{ACF}_p$  is complete, totally transcendental, has quantifier elimination and elimination of imaginaries.*

*Proof.* See proposition 1.1 (p. 61), corollary 1.2 (p. 62), and corollary 1.8 (p. 64) of [3].  $\square$

Let  $F$  be an arbitrary field. A **derivation** on  $F$  is an additive function  $\partial: F \rightarrow F$  such that  $\partial(xy) = x\partial(y) + y\partial(x)$  for any  $x, y \in F$ . A field  $F$  equipped with a derivation  $\partial$  is what we call a **differential field**. By **the constants of  $F$** , denoted  $C_F$ , we mean the set of elements in  $F$  where  $\partial$  vanish. Let  $DF_0$  be the set of sentences in the language  $L_{dr} = L_r \cup \{\partial\}$  expressing that its models are differential fields of characteristic 0. Since the time of Robinson we know that  $DF_0$  has a model companion; that is, the class of existentially closed models of  $DF_0$  is axiomatisable. Let  $DCF_0$  be the theory given by this axiomatisation. By a **differentially closed field** (of characteristic 0) we will mean a model of  $DCF_0$ .

**1.7 Fact** ( $DCF_0$ ).  *$DCF_0$  is also complete, totally transcendental, has quantifier elimination and elimination of imaginaries.*

*Proof.* See theorem 1.8 (p. 132), theorem 1.13 (p. 133), and theorem 2.1 (p. 134) of [3].  $\square$

### Separably closed fields

Let  $F$  be a field of characteristic  $p$ . Recall that a polynomial is said to be **separable** if its roots (in the algebraic closure of  $F$ ) are distinct. We say that  $F$  is **separably closed** if any separable polynomial over  $F$  has a root in  $F$ .

If  $[F : F^p] = p^\nu$ , we call  $\nu$  the **imperfection degree** of  $F$ . A  **$p$ -basis** of  $F$  is a subset  $B = \{b_1, \dots, b_\nu\}$  such that the set of  $p$ -monomials of  $B$  forms a linear basis of  $F$  over  $F^p$ . This is, each  $x \in F$  can be uniquely written as

$$x = \sum_{j \in p^\nu} x_j^p m_j(B),$$

where  $m_j(B) = \prod_{i=1}^\nu b_i^{j(i)}$  for  $j \in p^\nu$ . Let  $f_j: F \rightarrow F: x \mapsto x_j$ .

Fix  $p$ , the integer  $\nu$  and  $B = \{b_1, \dots, b_\nu\}$ . Let  $L_{p,\nu} = L_f \cup B \cup \{f_j: j \in p^\nu\}$  and  $SCF_{p,\nu}$  the  $L_{p,\nu}$ -theory of separably closed fields with imperfection degree  $\nu$ ,  $p$ -basis  $B$  and the  $f_j$ 's as defined above.

**1.8 Fact** ( $SCF_{p,\nu}$ ).  *$SCF_{p,\nu}$  is complete, stable, non-superstable, has quantifier elimination and elimination of imaginaries.*

*Proof.* See theorem 2.1 (p. 146), theorem 2.3 (p. 147), and theorem 2.12 (p. 151) of [3].  $\square$

Separably closed fields are the only fields known to be stable and non-superstable. It is conjectured that they are the only ones.

### 1.1.3 Groups interpretable in stable theories

An  $L$ -structure  $\mathcal{M}$  is **interpretable** in an  $L'$ -structure  $\mathcal{N}$  if the following conditions are satisfied:

- There is a definable set  $V \subset \mathcal{N}^{e_q}$ ;
- for each  $n$ -ary relation  $R \in L$  there is a definable relation  $R' \subset V^n$  in  $\mathcal{N}^{e_q}$ ; and
- for each function  $f: \mathcal{M}^m \rightarrow \mathcal{M}$  in  $L$  there is a definable function  $f': V^m \rightarrow V$  in  $\mathcal{N}^{e_q}$ ; such that
- there is a bijection  $\phi: \mathcal{M} \rightarrow V$  such that  $\phi$  yields an isomorphism  $(\mathcal{M}, R, \dots, f, \dots) \cong (V, R', \dots, f', \dots)$  of  $L$ -structures.

In that case, we say that  $\phi$  is an **interpretation** of  $\mathcal{M}$  in  $\mathcal{N}$ . Additionally, we say that  $\mathcal{M}$  and  $\mathcal{N}$  are **bi-interpretable** if there are interpretations  $\phi$  of  $\mathcal{M}$  in  $\mathcal{N}$  and  $\psi$  of  $\mathcal{N}$  in  $\mathcal{M}$  such that  $\psi \circ \phi$  and  $\phi \circ \psi$  are definable in  $\mathcal{M}$  and  $\mathcal{N}$  respectively.

**1.9 Fact** (Properties preserved under interpretability). *Suppose  $\mathcal{M}$  is interpreted in  $\mathcal{N}$ . If  $\mathcal{N}$  is  $\kappa$ -saturated or  $\kappa$ -stable, so is  $\mathcal{M}$ .*

*Proof.* See lemma 9.19, p. 296 of [35]. □

Finally, let us mention a basic result from the theory of stable groups that we will use in the third chapter.

**1.10 Fact.** *Type-definable groups in totally transcendental theories are definable.*

*Proof.* See corollary 5.19, p. 102 of [36]. □

## 1.2 Internality and Galois theory

The following definition is due to Bruno Poizat. Let  $T$  be a stable theory. Consider  $p$  and  $q$  possibly partial types over  $A$ . We say that  $p$  is  **$q$ -internal (over  $A$ )** (or **internal to  $q$** ) if there is a set  $B$  containing  $A$  such that, for every realization  $a$  of  $p$ , there is a tuple  $b$  of realizations of  $q$  such that  $a \in \text{dcl}(Bb)$ .

Given  $p$   $q$ -internal, we say that a tuple  $a$  of realizations of  $p$  is a **fundamental system of solutions of  $p$  relative to  $q$**  if there exists  $u(\cdot, \cdot)$ , an  $A$ -definable function, such that for any  $b$  realizing  $p$ , we have that  $b = u(a, c)$  for some tuple  $c$  of realisations of  $q$ .

**1.11 Fact** (Existence of a fundamental system of solutions). *If  $p$  is  $q$ -internal and either  $p$  is stationary or  $q$  consists of a single formula, then there is a fundamental system of solutions of  $p$  relative to  $q$ .*

*Proof.* See theorem 2.19, p. 37 of [36]. □

**1.12 Fact (Binding Group).** *Let  $T$  be a stable theory, and let  $\mathcal{U}$  be a large saturated model of  $T$ . Suppose that  $p$  and  $q$  are possibly partial types over  $A$ . Also assume that there is a fundamental system of solutions of  $p$  relative to  $q$ . Let  $P$  be the set of points in  $\mathcal{U}$  satisfying  $p$ , and let  $Q$  be the set of points in  $\mathcal{U}$  satisfying  $q$ . Then the automorphisms of  $\mathcal{U}$  which fix  $A$  and  $Q$  pointwise induce a type-definable group of permutations on  $P$ . This group is called **the binding group between  $p$  and  $q$** .*

*Proof.* For a proof in the case where  $T$  is totally transcendental and  $p$  and  $q$  are formulas, see theorem 2.20, p. 38 of [36]. For a proof in full generality, see theorem 4.8, p. 283 of [28].  $\square$

It is worth pointing out that Udi Hrushovski has shown (Theorem B.1' of [11]) that this theorem can be proved in a far more general setting (only assuming that  $T$  has some elimination of imaginaries and  $P$  and  $P \cup Q$  are stably embedded).

### 1.2.1 Differential Galois theory in characteristic zero

Before finishing this chapter, let us briefly explore a concrete and already quite classical application of internality. Let  $T$  be  $\text{DCF}_0$  and  $\mathcal{U}$  its monster model. Since  $T$  is the model companion of the theory of differential fields, we may assume that any differential field mentioned during this section is embedded in  $\mathcal{U}$ . If  $F$  is a differential field and  $Y$  is a subset of  $\mathcal{U}$ , then  $F\langle Y \rangle$  will denote the differential subfield of  $\mathcal{U}$  generated by  $F$  and the elements in  $Y$ .

Suppose  $F < K$  is an extension of differential fields. We say that  $K$  is a **strongly normal extension of  $F$**  if the following conditions hold:

1.  $C_F = C_K$ , and  $C_F$  is algebraically closed;
2.  $K = F\langle a \rangle$  for some  $a = (a_1, \dots, a_m)$ ; and,
3. Whenever  $\sigma: K \hookrightarrow \mathcal{U}$  is an embedding of  $K$  into  $\mathcal{U}$  over  $F$ , then  $\sigma(K) \subseteq K\langle C_{\mathcal{U}} \rangle$ .

In this case we define  $\text{Gal}(K/F)$  as  $\text{Aut}(K\langle C_{\mathcal{U}} \rangle / F\langle C_{\mathcal{U}} \rangle)$ .

**1.13 Fact.** *If  $K = F\langle a \rangle$  is a strongly normal extension of  $F$ , then  $p = \text{tp}(a/F)$  is  $C_{\mathcal{U}}$ -internal. Moreover,  $a$  is a fundamental system of solutions of  $p$  relative to  $C_{\mathcal{U}}$ .*

*Proof.* Since any  $a' \models p$  is of the form  $\sigma(a)$  for some  $\sigma$  an automorphism of  $\mathcal{U}$  fixing  $F$ , then, by the third condition in the definition of strongly normal extensions,  $a' \in \text{dcl}(F, a, C_{\mathcal{U}})$ . We have that  $a$  is a fundamental system of solutions because of fact 1.11, noting that  $C_{\mathcal{U}}$  is defined by a formula.  $\square$

**1.14 Fact.** *The binding group of  $p$  relative to  $C_{\mathcal{U}}$  is isomorphic to a definable group  $G$  inside  $C_{\mathcal{U}}$  and this group is isomorphic to  $\text{Gal}(K/F)$ .*

*Proof.* The definability of the binding group is a consequence of fact 1.12. In [37] it is proved that the binding group is definable inside  $C_U$ . In the same paper was suggested the isomorphism between the binding group and  $\text{Gal}(K/F)$ . A careful proof of this fact, in a more general setting, can be found in [31].  $\square$

**1.15 Fact** (Galois correspondence). *If  $K$  is a strongly normal extension of  $F$ , then there is a bijective correspondence between the intermediate differential fields and the  $F$ -definable subgroups of  $G$ , with  $G$  as in fact 1.14. Also, if  $L$  is an intermediate differential field, the corresponding subgroup is normal if and only if  $L$  is a strongly normal extension of  $F$ .*

*Proof.* See theorem 1, p. 394 of [13]. For a model theoretic flavored proof, see théorème 16 of [37] or theorem 2.12 of [31].  $\square$

Recall that an **algebraic group** is a variety  $G$  equipped with a group operation such that the function  $G \times G \rightarrow G: (x, y) \mapsto x \cdot y^{-1}$  is a morphism.

**1.16 Fact** (Weil–van den Dries–Hrushovski Theorem). *Groups interpretable in algebraically closed fields are algebraic groups.*

*Proof.* See theorem 4.13, p. 84 of [36]. For van den Dries’ topological proof, see [6].  $\square$

**1.17 Corollary.** *If  $K$  is a strongly normal extension of  $F$ , then  $\text{Gal}(K/F)$  is isomorphic to the  $\mathcal{C}$ -rational points of an algebraic group defined over  $C_F$ .*

*Proof.* A consequence of facts 1.14 and 1.16.  $\square$

### 1.3 Historic and bibliographical notes

As an introduction to model theory, I suggest Wilfrid Hodges’ *A Shorter Model Theory* [9]. There are several excellent introductions to stability theory. Dave Marker’s *Model Theory: An introduction* [22], Bruno Poizat’s *A course in model theory* [35] and John Baldwin’s *Fundamentals of Stability Theory* [1] are three of them. Anand Pillay’s *Geometric Stability Theory* [28] is a quite complete reference on the subject. Enrique Casanova’s *Lecture notes on stability and simplicity* (available online) [4] are also an excellent place to look for detailed proofs. For a careful account of the study of groups in stable theories, you must read *Stable Groups* [36] by Bruno Poizat.

The first chapter of Robin Hartshorne’s *Algebraic Geometry* [7] is a good introduction to the geometry of varieties. I also like to check Igor Shafarevich’s *Basic Algebraic Geometry I* [39] when I’m looking for precise definitions and results. My reference on algebraic groups is James Humphreys’ *Linear Algebraic Groups* [12].

The theory of strongly normal extensions was developed by E. R. Kolchin as a generalization of the late 19th century work of Picard and Vessiot. The main

reference is of course Kolchin's book *Differential Algebra and Algebraic Groups* [13]. Kolchin's work was one of the starting points for the modern study of algebraic groups. A modern treatment of Kolchin's theory is offered, for instance, in A. Magid's *Differential Galois Theory* [17]. An excellent general reference on modern differential Galois theory is the book *Galois Theory of Linear Differential Equations* [38] by Marius van der Put and Michael F. Singer.

As I said in the introduction, it was Bruno Poizat who, in his seminal paper *Une theorie de Galois imaginaire* [37], noticed that Kolchin's Galois theory of differential fields could be presented in model theoretic terms using the work of Zil'ber and Hrushovski on definability of automorphism groups. There was, however, a technical problem: While the Galois group obtained by Kolchin was an algebraic group, the one offered by model theory was merely a definable group in an algebraically closed field. Poizat then posed the conjecture that any such group should be an algebraic group. This was later on proved independently by Lou van den Dries and Ehud Hrushovski using a theorem of Weil.

After this, and making use of the machinery of model theory, Kolchin's strongly normal extensions were extended in Anand Pillay's *Differential Galois Theory I* [31] to a context where the field of constants can be replaced by any definable set. This work has continued in *Differential Galois Theory II* [32] and *Differential Galois Theory III: Some inverse problems* [33] (with Dave Marker).

# Chapter 2

## Iterative differential algebra

So we have a sort of anamorphoscope, more properly no doubt a *paramorphoscope* because it reveals worlds which are set to the side of the one we have taken, until now, to be the only world given us.

Thomas Pynchon, *Against The Day*

The aim of this chapter is offering the reader a brief introduction to the aspects of the algebra and model theory of iterative derivations that are required for this thesis.

### 2.1 Basic definitions

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  $\partial_0 = \text{id}_R$  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. Here we have an alternative definition:

**2.1 Fact.** *Given  $R$  a ring,  $\partial = (\partial_i : R \rightarrow R)_{i \in \omega}$  with  $\partial_0 = \text{id}_R$  is a Hasse-Schmidt derivation if and only if the maps  $\partial_i$  are additive and*

$$\partial_m(xy) = \sum_{i+j=m} \partial_i(x) \partial_j(y).$$

*Proof.* Suppose  $\partial = (\partial_i : R \rightarrow R)_{i \in \omega}$  is a Hasse-Schmidt derivation. Since  $\mathbb{D}_\partial$  is a ring homomorphism,

$$\sum_{i=0}^{\infty} \partial_i(x+y) \epsilon^i = \sum_{i=0}^{\infty} (\partial_i(x) + \partial_i(y)) \epsilon^i.$$

This proves the maps  $\partial_i$  are additive. Likewise, for multiplication we have:

$$\sum_{i=0}^{\infty} \partial_i(xy) \epsilon^i = \sum_{i=0}^{\infty} \left( \sum_{m+n=i} \partial_m(x) + \partial_n(y) \right) \epsilon^i.$$

Observe that these two formulas also prove that if both conditions hold,  $\partial$  is Hasse-Schmidt. □

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  $\partial$  is an **iterative Hasse-Schmidt derivation** or simply an **iterative derivation**. A ring (field)  $R$  equipped with an iterative derivation  $\partial$  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  $\partial_i$  vanish.

**2.2 Fact.** *If  $(R, \partial)$  is an ID-ring, then*

$$\partial_{d_1} \circ \partial_{d_2} \circ \cdots \circ \partial_{d_r} = \frac{(d_1 + \cdots + d_r)!}{d_1! \cdots d_r!} \partial_{d_1 + \cdots + d_r}$$

for all  $d_1, \dots, d_r \in \omega$ .

*Proof.* An easy induction on the number of factors. □

Before continuing, let us take a look at some examples of ID-rings.

**2.3 Example.** 1. *Let  $(R, \delta)$  be an ordinary differential ring of characteristic zero. If we define  $\partial_i = \frac{1}{i!} \delta^i$ , then  $(R, (\partial_i))$  is an ID-ring. We will see later on that this is the only possible example in characteristic zero.*

2. *Let  $F$  be a field of characteristic  $p > 0$  and  $K = F(t)$ , then  $\partial_i(t^m) = \binom{m}{i} t^{m-i}$  and  $\partial_i(a) = 0$  for any  $a \in F$  defines an iterative derivation on  $K$ .*

We will now see that if  $(R, \partial)$  is an ID-ring,  $\partial_1$  is just a derivation. In the case where the characteristic of  $R$  is zero,  $\partial_1$  determines the whole stack of operators. In positive characteristic, though, this is not the case. Infinitely many are necessary:

**2.4 Fact.** *Let  $(R, \partial)$  be an ID-ring.*

1. *If the characteristic of  $R$  is zero,  $\partial$  is completely determined by  $\partial_1$  in the following way:*

$$\partial_m = \frac{1}{m!} \partial_1^m$$

for all  $m \in \omega$ .

2. *If the characteristic of  $R$  is  $p > 0$ , then  $\partial$  is determined by  $(\partial_{p^i})_{i < \omega}$ . Indeed, if  $m = \sum_{j=0}^r d_j p^j$ , with  $0 \leq d_j \leq p-1$ , is the  $p$ -adic representation of  $m$ , then*

$$\partial_1^{d_0} \circ \partial_p^{d_1} \circ \cdots \circ \partial_{p^r}^{d_r} = \left( \frac{m!}{(p!)^{d_1} (p^2!)^{d_2} \cdots (p^r!)^{d_r}} \right) \partial_m.$$

*Proof.* 1. Suppose that the characteristic of  $R$  is zero. We proceed by induction on  $m$ . For  $m = 0$ , the formula is clear. Assume it works for  $m = n$ ,

let us check it for  $m = n + 1$ :

$$\begin{aligned}\partial_{n+1} &= \frac{1}{\binom{n+1}{n}} \partial_n \partial_1 \\ &= \frac{n!}{(n+1)!} \frac{1}{n!} \partial_1^n \partial_1 \\ &= \frac{1}{(n+1)!} \partial_1^{n+1}.\end{aligned}$$

2. Suppose now that the characteristic of  $R$  is  $p$ . Let  $m = \sum_{j=0}^r d_j p^j$  be the  $p$ -adic representation of  $m$ . Let us check the formula by induction on  $r$ . If  $r = 0$ , then  $m = d < p$  and so, as in the characteristic zero case,  $\partial_0^d = d! \partial_d$ . Assume now that the formula works for  $r = l$ , let  $m' = \sum_{j=0}^l d_j p^j$ , and let us check it for  $r = l + 1$ :

$$\begin{aligned}\partial_1^{d_0} \circ \dots \circ \partial_{p^{l+1}}^{d_{l+1}} &= \left( \frac{(m')!}{(p!)^{d_1} \dots (p^l!)^{d_l}} \right) \partial_{m'} \circ \partial_{p^{l+1}}^{d_{l+1}} \\ &= \left( \frac{(m')!}{(p!)^{d_1} \dots (p^l!)^{d_l}} \right) \partial_{m'} \circ \left( \frac{(d_{l+1} p^{l+1})!}{(p^{l+1}!)^{d_{l+1}}} \partial_{d_{l+1} p^{l+1}} \right) \\ &= \left( \frac{(m')! (d_{l+1} p^{l+1})!}{(p!)^{d_1} \dots (p^l!)^{d_l} (p^{l+1}!)^{d_{l+1}}} \right) \binom{m}{m'} \partial_m \\ &= \left( \frac{m!}{(p!)^{d_1} \dots (p^r!)^{d_r}} \right) \partial_m.\end{aligned}$$

In order to make sure this formula works for characteristic  $p$ , we also have to note that, under the hypothesis, the integer

$$T = \frac{m!}{(p!)^{d_1} (p^2!)^{d_2} \dots (p^r!)^{d_r}}$$

is *not* divisible by  $p$ . For this, first recall that if  $m = \sum_{j=0}^r d_j p^j$ , with  $0 \leq d_j \leq p - 1$ , is the  $p$ -adic representation of  $m$ , then the maximum power of  $p$  that divides  $m!$  is of the form  $p^{N(m)}$  where

$$N(m) = \frac{m - \sum_{j=0}^r d_j}{p - 1}$$

(See, for instance, lemme 4.2.1, p. 167 of [5]). Now, this implies that the maximum power of  $p$  that divides  $T$  is

$$\begin{aligned}v_p(T) &= \frac{1}{p-1} \left( m - \sum_{j=0}^r d_j \right) - \frac{1}{p-1} \left( \sum_{j=0}^r d_j (p^j - 1) \right) \\ &= \frac{1}{p-1} \left( \left( m - \sum_{j=0}^r d_j \right) - \left( \sum_{j=0}^r d_j p^j - \sum_{j=0}^r d_j \right) \right) = 0\end{aligned}$$

□

## 2.2 Model theory of ID-fields

Let  $IDF_p$  be the first-order theory of fields of characteristic  $p > 0$  equipped with an iterative derivation  $\partial$ . 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  $K^p = \{x \in K : \partial_1(x) = 0\}$ . Note that each of these properties can be expressed with first order sentences. 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 the already introduced  $SCF_{p,1}$ :

**2.5 Fact.** *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  $\lambda$ -functions are quantifier-free definable.*

*Proof.* See [40]. □

Thus,  $SCH_p$  has good model theoretic properties:

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

*Proof.* See [40]. □

Since  $SCH_p$  is stable, we may let  $(\mathcal{U}, \partial)$  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:

**2.7 Lemma.** *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  $dcl(A) \cap \mathcal{C}$ .*

*Proof.* Suppose  $Z = \phi(\mathcal{U}, a)$  with  $a \in A$ . Let  $p = tp(a/\mathcal{C})$  be the type of  $a$  over  $\mathcal{C}$  and let  $d\phi_x(y)$  be a definition of  $\phi(y, x)$  for this type. This formula exists because of stability and it has parameters in  $dcl(a) \cap \mathcal{C}$ . Clearly,  $\phi(\mathcal{C}, a) = d\phi_x(\mathcal{C})$ . By quantifier elimination,  $d\phi_x(y)$  can be assumed to be a boolean combination of iterative differential polynomials, but all  $\partial_i$  are zero on  $\mathcal{C}$ , thus, making all appearances of  $\partial_i(y)$  zero in  $d\phi_x(y)$ , we have a  $dcl(a) \cap \mathcal{C}$ -definition of  $Z \cap \mathcal{C}^m$  in the field language. □

We will now define three different closure operators of algebraic nature. For this, 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  $\mathcal{U}$ .

Here is a useful algebraic characterization of the model theoretic definable and algebraic closures in  $\mathcal{U}$  in terms of these closure operators:

**2.8 Fact.** *Let  $A \subseteq \mathcal{U}$ .*

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

*Proof.* See Proposition II.2 and Proposition II.3 of [2]. □

We say that an ID-field  $F$  is non-trivial if  $\partial_1|_F \neq 0$ . Let us close this chapter with a characterization of the relatively algebraically closed ID-subfields of  $\mathcal{U}$ .

**2.9 Lemma.** *If  $F$  is a non-trivial ID-subfield of  $\mathcal{U}$ , and it is relatively algebraically closed inside  $\mathcal{U}$ , then  $F \prec \mathcal{U}$ .*

*Proof.* Since  $\mathcal{U}$  is separably closed and  $F$  is relatively algebraically closed in  $\mathcal{U}$ , then  $F$  is also separably closed.

Let us prove that  $F^p = \{x \in F : \partial_1(x) = 0\}$ : The left to right containment is clear. For the opposite direction, let  $b \in F$  be such that  $\partial_1(b) = 0$ . Then, since  $\mathcal{U} \models \text{SCH}_p$ , we get that  $b = c^p$  for some  $c \in \mathcal{U}$ . But  $F$  is relatively algebraically closed, so  $c \in F$  and  $b \in F^p$ .

In order to finish, we need to prove that  $[F : F^p] = p$ . Since we already proved that  $F^p = \{x \in F : \partial_1(x) = 0\}$  and it is clear by fact 2.4 that  $\partial_1^p \equiv 0$ , this claim is a consequence of theorem 27.3 (i) of [18]. □

## 2.3 Historic and bibliographical notes

Iterative derivations were introduced by Hasse in [8] as a non-trivial generalization of differential algebra for positive characteristic fields. A good introduction to the algebra of iterative derivations is the first chapter of *Differential Galois Theory in Positive Characteristic* [19], by Heinrich Matzat. Another one is Kôtarô Okugawa's paper *Basic properties of differential fields of an arbitrary characteristic and Picard-Vessiot theory* [26]. Section 27 of Matsumara's *Commutative Ring Theory* [18] deals with extensions of traditional derivations to iterative ones.

The model theory of separably closed fields equipped with iterative derivations was originally explored by Margit Messmer and Carol Wood in [23] following previous work on separably closed fields by Françoise Delon. Subsequently, this theory was generalized to several commuting iterative derivations by Martin Ziegler in [40]. Franck Benoist in his PhD thesis [2] made a careful study of the model theory and geometry of these structures. Piotr Kowalski has found a geometric axiomatization of  $\text{SCH}_p$  [14] similar to the one for characteristic zero differentially closed fields. Interesting model theory and applications to algebra have been found making use of this axiomatization. See, for instance, [15].

# Chapter 3

## Iterative strongly normal theory

“To begin with, they are very tall.” I was looking around the room for clues. “They reach way up. Up and up. Toward the sky. They’re so big, some of them, they have to have these supports. To help them hold them up, so to speak.”

Raymond Carver, *Cathedral*

As in the previous chapter, let  $\mathcal{U}$  be a saturated model of  $\text{SCH}_p$  of large cardinality where any ID-field mentioned is embedded and let  $\mathcal{C}$  the field of constants of  $\mathcal{U}$ .

From now on,  $(F, \partial)$  is assumed to be a iterative differential field with  $\partial_1|_F \neq 0$ .

### 3.1 Definition and basic remarks

An extension  $(F, \partial) < (K, \partial)$  of 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.  $K = F\langle \mathbf{a} \rangle^s (= \text{dcl}(F\mathbf{a}))$  for some  $\mathbf{a} = (a_1, \dots, a_m)$ ;
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.  $F^\alpha \cap K = F\langle \mathbf{d} \rangle^s$  for some  $\mathbf{d} = (d_1, \dots, d_m)$ .

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  $\text{gal}(K/F)$ . In lemma 3.6 we show that  $\text{gal}(K/F)$  is in fact a subgroup of  $\text{Gal}(K/F)$ .

**3.1 Example** (Iterative Picard-Vessiot extensions). *The following definitions and facts come from [29]. An algebraic presentation of them can be found in [19].*

Let  $(F, \partial)$  be an ID-field. An **iterative differential module** for  $(F, \partial)$  is an  $F$ -module  $V$  together with a sequence  $D = (D_0, D_1, \dots)$  of additive maps from  $V$  to  $V$  such that

- $D_0$  is the identity,

- $D_m(rv) = \sum_{i+j=m} \partial_i(r)D_j(v)$  for  $r \in F$  and  $v \in V$ , and
- $D_m(D_n(v)) = \binom{m+n}{n} D_{n+m}(v)$  for  $v \in V$ .

Given an  $s$ -dimensional iterative differential module  $(V, D)$  for  $(F, \partial)$ , consider the set

$$V^\partial = \{v \in V : D_m(v) = 0 \text{ for all } m \in \omega\}.$$

It is a fact (Lemma 2.2 of [29]) that  $V^\partial$  is a vector space over  $C_F$  of dimension at most  $s$ .

Suppose now that  $(V, D)$  is a finite-dimensional iterative differential module over  $(F, \partial)$ . After fixing a basis  $(e_1, \dots, e_s)$  of  $V$  over  $F$ , the sequence of equations  $(D_m(v) = 0 : m \in \omega)$  on  $V$  turns into a sequence equations  $(\partial_m(y) = B_m y : m \in \omega)$  on  $F$ . With  $y$  a  $1 \times s$  column vector of variables and  $B_m$  an  $s \times s$  matrix over  $K$ .

We say that a sequence of equations of the form  $(\partial_m(y) = B_m y : m \in \omega)$  is a **consistent linear iterative differential equation** if it comes from an iterative differential module through the process we just described. By a **fundamental system of solutions** of a consistent linear iterative differential equation over  $F$  we mean an invertible matrix  $U \in GL_s(K)$  for some iterative differential field extension  $(K, \partial)$  of  $(F, \partial)$ .

Let  $(F, \partial)$  be an ID-field such that  $C_F$  is algebraically closed. Let

$$(\partial_m(y) = B_m y : m \in \omega)$$

be a consistent linear iterative differential equation over  $F$ . By a **Picard-Vessiot extension** of  $(F, \partial)$  for the given equation we mean an iterative differential field extension  $(K, \partial)$  of  $(F, \partial)$  such that

1.  $C_F = C_K$ ,
2. there is a fundamental matrix  $U$  of solutions of the equation with entries in  $K$ , and
3.  $K = \text{dcl}(FU)$ .

Any iterative Picard-Vessiot extension is a strongly normal extension. The proof of this will be a consequence of the theory developed in the last chapter (see example 4.8).

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:  $\text{tp}(\mathfrak{a}/F)$  should have finite multiplicity. This is going to be important when proving the definability of the Galois group. Our extra-condition (4) will do this for us:

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

This is a corollary of the following general lemma:

**3.3 Lemma.** *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 (Fact 1.4) 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  $\sigma$  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  $\sigma$ . 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.

**3.4 Lemma.** *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.* Suppose that  $p = \text{tp}(a/F)$  has finite multiplicity  $m > 1$ . Let  $a_1, \dots, a_m$  be realisations of the distinct complete extensions of  $p$  to  $\text{acl}(F)$  such that  $a$  is independent from  $(a_1, \dots, a_m)$  over  $F$ . As each of the  $a_i$  realizes  $p$ , for each  $i$  there is a partial function  $f_i(\cdot, \cdot)$  and a constant  $c_i$  such that  $a_i = f_i(a, c_i)$ .

Now let  $b$  realizing  $p$  and take  $b'$  realizing  $\text{tp}(b/\text{acl}(F))$  such that  $b' \downarrow_F ab$ . This implies that  $\text{tp}(ab'/F) = \text{tp}(aa_i/F)$  for some  $i \leq m$  and also  $\text{tp}(bb'/F) = \text{tp}(aa_1/F)$ . Hence, there are constants  $c$  and  $c'$  such that  $f_i(a, c) = b'$  and  $f_1(b', c') = b$ . Thus,  $b = f_1(f_i(a, c), c')$  for some  $i$ . Gluing the  $f_i$ 's together, we obtain the desired function.  $\square$

## 3.2 Definability of the Galois group

Let  $K = F\langle a \rangle^s$  be a strongly normal extension of  $F$ . In this section we will prove the following key result:

**3.5 Theorem** (Definability of  $\text{Gal}(K/F)$ ). *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.

**3.6 Lemma.** *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 a  $\mathcal{U}$ -automorphism fixing  $F\langle\mathcal{C}\rangle$  and taking  $a$  to  $a'$ .

Observe that any of these automorphisms, when restricted to  $K\langle\mathcal{C}\rangle$ , becomes a unique function because the action on this set is already determined by  $\sigma$  and the fact that the new function fixes  $\mathcal{C}$ . This new function, that we will call  $\bar{\sigma}$ , takes  $K\langle\mathcal{C}\rangle$  isomorphically onto  $\sigma(K)\langle\mathcal{C}\rangle$ .

To finish the claim, let us prove that  $\sigma(K)\langle\mathcal{C}\rangle = K\langle\mathcal{C}\rangle$ . One containment ( $\subseteq$ ) is a direct consequence of the third condition of our definition of iterative strongly normal extensions. For the other way around, note that we can substitute  $a$  for any conjugate in the statement of lemma 3.4; that is, for any  $a$  there exists  $c \in \mathcal{C}$  such that  $u(\sigma(a), c) = a$ , and so  $K \subseteq \sigma(K)\langle\mathcal{C}\rangle$ .

Coming back to the proof of the lemma, let  $d$  be a (possibly infinite) tuple from  $K$ . Since  $\mathcal{C}$  is algebraically closed,  $\text{tp}(d/\mathcal{C})$  is stationary. Moreover, because  $\mathcal{C}$  is type definable over the empty set, its canonical base is contained in  $\mathcal{C} \cap \text{dcl}(d) \subseteq C_K (= C_F)$ . Thus, for any such  $d$ , the type  $\text{tp}(d/\mathcal{C})$  is definable over  $C_F$ .

In particular, this applies to the infinite tuples  $aF$  and  $a'F$ , where  $\text{tp}(a'/F) = \text{tp}(a/F)$ . In this case,  $\text{tp}(aF/\mathcal{C})$  and  $\text{tp}(a'F/\mathcal{C})$  are, respectively, the unique non-forking 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 of  $\text{tp}(aF/\mathcal{C})$  and  $\text{tp}(a'F/\mathcal{C})$ .  $\square$

**3.7 Corollary.**  $\mathcal{X}$ , 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 consequence of lemma 3.6: Let  $a'$  and  $a'' \in \mathcal{X}$ . Since they have the same type over  $F$ , let  $\sigma$  be an automorphism of  $\mathcal{U}$  fixing  $F$  that takes  $a'$  to  $a''$ . The lemma then tells us that the restriction of  $\sigma$  to  $K\langle\mathcal{C}\rangle$  is an

element of  $\text{Gal}(K/F)$  and, moreover, that this restriction is unique. This is, for  $a'$  and  $a''$  there is only one  $\sigma \in \text{Gal}(K/F)$  taking  $a'$  to  $a''$ .  $\square$

*Proof of theorem 3.5.* This is a modified version of the general argument for proving the definability of the binding group (fact 1.12). We give the proof here for the sake of completeness.

Let  $Z = \{c \in \mathcal{C} : u(a, c) \in \mathcal{X}\}$ . Observe that by lemma 2.7, this set is type-definable over  $\text{dcl}(a) \cap \mathcal{C}$ , and so over  $F\langle a \rangle^s \cap \mathcal{C} = K \cap \mathcal{C} = C_K$ . Recall that since  $K/F$  is strongly normal,  $C_K$  is equal to  $C_F$ . This is,  $Z$  is type-definable over  $C_F$ .

Consider the equivalence relation  $E$  on  $Z$ , defined by the formula  $u(a, x_1) = u(a, x_2)$ . By the same argument given in the paragraph above,  $E$  is definable over  $C_F$ .

Define  $Y$  to be the quotient of  $Z$  by  $E$ . Because of elimination of imaginaries of algebraically closed fields and the pureness of  $\mathcal{C}$  (lemma 2.7),  $Y$  is a type-definable set in  $\mathcal{C}$  over  $C_F$ . For  $b \in \mathcal{X}$  and  $d \in Y$ , define  $f(b, d) = u(b, c)$  with  $c \in Y_0$  such that  $c/E = d$ .

Note that for any  $b_1$  and  $b_2 \in \mathcal{X}$ , there is only one  $d \in Y$  such that  $f(b_1, d) = b_2$ . This is because if  $f(b_1, d_1) = f(b_2, d_2)$  then  $u(b_1, c_1) = u(b_1, c_2)$  for some  $c_i$  ( $i = 1, 2$ ) such that  $c_i/E = d_i$  and this implies that  $d_1 = d_2$ . Hence we can find  $h(\cdot, \cdot)$  a function such that, for  $b_1$  and  $b_2 \in \mathcal{X}$ , the image of  $(b_1, b_2)$  under  $h$  is the unique  $d \in Y$  for which  $f(b_1, d) = b_2$ .

Consider the function  $\mu: \text{Gal}(K/F) \rightarrow Y: \sigma \mapsto h(a, \sigma(a))$ . The previous paragraph plus corollary 3.7 will allow us to conclude that  $\mu$  is a bijection: Let  $\sigma$  and  $\sigma' \in \text{Gal}(K/F)$  and suppose  $\mu(\sigma) = \mu(\sigma')$ , that is,  $c = h(a, \sigma(a)) = h(a, \sigma'(a))$ . Hence  $\sigma(a) = f(a, c) = \sigma'(a)$  and so,  $\sigma = \sigma'$ . On the other hand, let  $d \in Y$  and consider  $b = f(a, d)$ . Let  $\sigma \in \text{Gal}(K/F)$  such that  $\sigma(a) = b$ . By definition of  $h$ , we have that  $\mu(\sigma) = d$ .

So far, we have managed to find  $Y$  type-definable over  $C_F$  and in bijection with our Galois group. We will now endow  $Y$  with the group operation induced by  $\mu$ . This is, let us define  $d \cdot d' = \mu(\mu^{-1}(d) \cdot \mu^{-1}(d'))$ . Note now that this group operation is definable:

Let  $d_1, d_2 \in Y$  and  $\sigma_i = \mu^{-1}(d_i)$  ( $i = 1, 2$ ). Now,

$$\begin{aligned} \sigma_1 \cdot \sigma_2(a) &= \sigma_1(\sigma_2(a)) \\ &= \sigma_1(f(a, d_2)) \\ &= f(\sigma_1(a), d_2) \\ &= f(f(a, d_1), d_2). \end{aligned}$$

Then, we define  $d_3 = d_1 \cdot d_2 = \mu(\sigma_1 \cdot \sigma_2) = h(a, \sigma_1(\sigma_2(a)))$  as the *unique*  $d_3$  such that  $f(a, d_3) = f(f(a, d_1), d_2)$ .

Moreover, consider now the induced regular action of  $Y$  on  $\mathcal{X}$ . Let  $d \in Y$

and  $\sigma = \mu^{-1}(d)$ . Let  $b \in \mathcal{X}$  and  $d_1 = h(a, b)$  ( $f(a, d_1) = b$ ). Then,

$$\begin{aligned}\sigma(b) &= \sigma(f(a, d_1)) \\ &= f(\sigma(a), d_1) \\ &= f(f(a, d), d_1).\end{aligned}$$

Thus,  $g \cdot b = f(f(a, g), h(a, b))$ , which makes the action  $F \cup \{a\}$ -definable.

Now, since  $\mathcal{C}$  is totally transcendental,  $(Y, \cdot)$  turns out to be not only type-definable but definable with parameters in  $C_F$ , by fact 1.10.

Finally, the Weil-Hrushovski theorem (Fact 1.16) tells us that  $(Y, \cdot)$  is the set of  $\mathcal{C}$ -rational points of an algebraic group  $G$  defined over  $C_F$ .  $\square$

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

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

*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 the characteristic zero case, the model theoretical approach to differential Galois theory heavily depends on the existence of prime models; this is a basic consequence of the fact that  $\text{DCF}_0$  is totally transcendental. Since  $\text{SCH}_p$  is only stable and not even superstable, we need to rely in other tools to deal with the lack of *differential closure*. Just like in the linear case [29], the use of a suitable **auxiliary structure** as a scaffolding to handle the group inside  $\mathcal{U}$  will do the trick.

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  $\mathcal{U}$ .

**3.9 Fact.** *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  $\mathcal{Y}$  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.

**3.10 Fact.**  $\mathcal{M}$  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 3.9.

Observe that  $\mathcal{N}$  is saturated and totally transcendental. Actually,  $\mathcal{N}$  could be simply seen as  $\mathcal{C}$  with names for the elements of  $C_F$ . This is, an algebraically closed field with additional constants. After all, we know that each  $F\langle a \rangle^s$ -definable subset of  $\mathcal{C}$  is  $C_F$ -definable. Its saturation is a consequence of the saturation of  $\mathcal{U}$  itself plus, once again, the pureness of  $\mathcal{C}$  as a field, since definable sets of  $\mathcal{N}$  are partial types of  $\mathcal{U}$ .

These last remarks plus the fact that being totally transcendental and saturation are preserved under taking reducts and interpretability (Fact 1.9), allow us to conclude that  $\mathcal{M}$  is also saturated and totally transcendental.

Finally, let us prove quantifier elimination. Since  $\mathcal{M}$  is saturated, it is enough to prove that it is also quantifier-free homogeneous. This is, once again, a consequence of  $\mathcal{U}$  being saturated (and so homogeneous): 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  $F$ .

**3.11 Lemma.**

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

*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 2.7, 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  $\phi$  is an isolating formula over  $F$ , it must be of the form  $x = c'$  for some  $c' \in C_F$ .  $\square$

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

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.

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

*Proof.* Any  $d \in \mathcal{M}_0^{\text{eq}}$  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  $\text{SCH}_{p,1}$ , it can be assumed that  $E'$  is also an equivalence relation. By elimination of imaginaries in  $\text{SCH}_{p,1}$ , 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  $d = a/E \in \mathcal{M}_0^{\text{eq}}$ . Clearly,  $d$  (seen as an element in  $\mathcal{U}$ ) is interdefinable over  $F$  with  $e$ . □

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

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

**3.13 Lemma.** *If  $K/F$  is strongly normal and  $L$  is an intermediate definably closed ID-field, then  $L$  is finitely generated over  $F$ .*

*Proof.* Consider  $L$  as a definably closed subset in  $\mathcal{M}_0^{\text{eq}}$  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  $\phi$  over  $\text{dcl}(F, b)$ . Clearly,  $d\phi_x(e')$  iff  $e = e'$ , and so  $e \in \text{dcl}(F, b)$ . □

**3.14 Theorem** (Galois correspondence). *Let  $K/F$  be a strongly normal extension of ID-fields. If  $L$  is a definably closed intermediate ID-field in  $K/F$ , then:*

1.  $K/L$  is strongly normal.

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

*Proof.* Let  $L = F\langle b \rangle^s$ .

1. Observe that as  $K/F$  is strongly normal, conditions (1), (2) (by lemma 3.13) and (3) immediately hold in  $K/L$ . Condition (4) requires an explanation:

The correspondence provided by lemma 3.12 allows us to see  $D = \text{acl}(L) \cap K$  as a subset of  $\mathcal{M}_0^{\text{eq}}$ . 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  $\omega$ -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  $\mathcal{M}^{\text{eq}}$ . Let us check that  $L\langle d \rangle^s = D$ :

The left to right containment is clear by the general theory of canonical basis. Suppose then that we have  $e \in \text{acl}(L) \cap K$ . Let  $\psi(a, y)$  witnessing  $e \in \text{dcl}(a, L)$ . Since  $e \in \text{acl}(L)$ , the formula  $\psi(x, e) \in \text{tp}(a/\text{acl}(L))$ . Additionally,  $d$  and  $\text{Cb}(\text{tp}(a/\text{acl}(L)))$  are interdefinable, so there is  $d\psi_x(y)$ , a  $\text{tp}(a/\text{acl}(L))$ -definition of  $\psi(x, y)$  with parameters from  $\text{dcl}(d, L) = L\langle d \rangle^s$ . Since  $\models d\psi_x(y)$  is equivalent to  $\models \psi(a, y)$ , then  $d\psi_x(y)$  is also a definition of  $e$ , this time over  $L \cap \{d\}$ . Thus,  $e \in \text{dcl}(L, d) = L\langle d \rangle^s$ .

2. As  $b \in K$ , let  $b = t(a)$  for some  $F$ -definable function  $t$ . Observe that  $g \in G_L$  iff  $t(a) = b = g \cdot b = g \cdot t(a) = t(g \cdot a)$ . Thus,  $G_L$  is definable.

Consider  $\sigma \in \text{Gal}(K/L)$  and let  $g = \mu(\sigma) \in G(\mathcal{C})$ . Then  $t(a) = t(\sigma(a)) = t(g \cdot a)$ . This is,  $g \in G_L$ . If, on the other hand,  $g \in G_L$ , then,  $\mu^{-1}(g)(L) = L$ , thus  $\mu^{-1}(g) \in \text{Gal}(K/L)$ .

3. Let  $H$  any  $C_F$ -definable subgroup of  $G(\mathcal{C})$ . Since the group action is  $K$ -definable,  $Ha$  is  $K$ -definable. If  $b$  is the canonical parameter for  $Ha$ , then,  $b \in K$  (since  $K$  is definably closed). Consider  $L = F\langle b \rangle^s$ . By the first part,  $K/L$  is strongly normal with Galois group  $G_L$ . To finish, we prove that  $G_L$  is equal to  $H$ :

Let  $g \in H$ . Clearly,  $g \cdot Ha = Ha$ , then,  $g \cdot b = b$  (considering  $g$  as an element of  $\text{Gal}(K/F)$ ). This implies that  $g \in G_L$ . On the other hand, if  $g \cdot b = b$ , then  $g \cdot Ha = Ha$  and so  $g \cdot a = h \cdot a$  for some  $h \in H$ . This implies (by regularity of the action of  $\text{Gal}(K/F)$  on  $\mathcal{X}$ ) that  $g = h \in H$ .

4. 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 fact,  $N = G_{L'}$  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,  $\sigma(d) \in L(\mathcal{C})$  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  $\text{Gal}(K/F)$  because of lemma 3.6. Let  $d \in L$ , we need to show that  $\sigma(d) \in L(\mathcal{C})$ : 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  $\tau$  is arbitrary, this implies that  $\sigma(d)$  belongs to the set fixed by  $\text{Gal}(K/L)$ , which is precisely  $L(\mathcal{C})$ .

Finally, consider the restriction map

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

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

□

**3.15 Theorem** (G-Primitive Element Theorem). *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  $a \downarrow_F b$ ,  $a \downarrow_F c$  and  $c \downarrow_F b$ . 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  $\alpha$  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  $\text{tp}(ac/F) = \text{tp}(c\sigma(a)/F)$  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. □

It is worth noticing that, because of lemma 2.9, we have that  $F$  is a model of  $\text{SCH}_p$ . We have left the statement of the theorem as it is only to suggest that the same proof could work if we consider, instead, several commuting iterative derivations.

### 3.5 Historic and bibliographical notes

This chapter is motivated by Anand Pillay's papers *Differential Galois Theory I* [31] and *Two remarks on differential fields* [29]. The first one offers a generalization of Kolchin's strongly normal extensions in characteristic zero making use of the model theory of differential fields. The second one gives a model-theoretic proof of the existence and uniqueness of a Picard-Vessiot extension for an iterative linear differential equation in positive characteristic. The idea of using an appropriate totally transcendental type-definable structure as a scaffolding comes from there.

As I mentioned in the introduction, Okugawa offered in [27] a first version of a strongly normal theory for ID-fields. His approach and techniques followed very closely those of Kolchin for characteristic 0 differential fields given in [13]. In particular, he proved that his corresponding Galois group for a given strongly normal extension is a  $\mathcal{C}$ -group in the sense of Kolchin (Chapter 5, Theorem 6, p. 135 of [27]) and he also found a Galois correspondence (Chapter 5, Theorem 7, p. 144 of [27]). These two results are equivalent to our theorems 3.5 and 3.14 respectively.

Our  $G$ -primitive element theorem (Theorem 3.15) is a version for positive characteristic of Theorem 6 (Chapter IV, Section 7) of [13]. For a model theoretic

version of that result see proposition 0.3 of [34].

# Chapter 4

## Iterative differential Galois extensions

Por eso hay que repetir, eterna y disparatadamente hay que repetir: desde el primer vocablo, desde el primer balbuceo humano y aun desde el primer dedo índice que señaló sin decir. Una y otra vez, e inútilmente una vez más.

J. Marías, *Tu Rostro Mañana*

In the previous chapter 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. We will prove that their Galois extensions are strongly normal (Theorem 4.11) and that, sometimes, strongly normal extensions can be seen as Galois extensions for appropriate differential equations (Theorem 4.12).

### 4.1 Arc bundles and the iterative logarithmic derivative

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  $a \mapsto a + 0\epsilon + \dots + 0\epsilon^m$ .

Let  $X$  be an algebraic variety over  $F$  and define, for any field  $k$  extending  $F$  the  $m^{\text{th}}$  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  $(k^{m+1})$ . Locally, this implies that if

$$X = \text{Spec}(F[x_1, \dots, x_l]/(\{f_j\}_{j \in J})) (\subseteq \mathbb{A}^l),$$

then

$$\mathcal{A}_m X = \text{Spec}(F[(x_{i,s})_{1 \leq i \leq l, 0 \leq s \leq m}]/(\{f_{j,t}\})) (\subseteq \mathbb{A}^{l(m+1)})$$

where  $f_{j,t} \in F[(x_{i,s})_{1 \leq i \leq l, 0 \leq s \leq m}]$  is defined by the identity

$$f_j\left(\sum_{t=0}^m x_{i,t} \epsilon^t\right)_{1 \leq i \leq l} = \sum_{t=0}^m f_{j,t}((x_{i,s})_{1 \leq i \leq l, 0 \leq s \leq m}) \epsilon^t$$

computed in the ring  $F[(x_{i,s})_{1 \leq i \leq l, 0 \leq s \leq m}, \epsilon]/(\epsilon^{m+1})$ .

**4.1 Example.** Let  $X$  be the algebraic variety defined by the equation  $x = y^2$ . The equations defining  $\mathcal{A}_1(X)$ , a variety in  $\mathbb{A}^4$  with local coordinates  $(x_0, x_1, y_0, y_2)$ , are  $x_0 - y_0^2 = 0$  and  $x_1 - 2y_0y_2 = 0$ . In general, the equations defining  $\mathcal{A}_m(X)$  (with coordinates  $(x_0, \dots, x_m, y_0, \dots, y_m)$ ) are those of  $\mathcal{A}_{m-1}(X)$  plus

$$x_m - (y_n^2 + 2 \sum_{\substack{i+j=m \\ 0 \leq i < j}} y_i y_j) = 0,$$

if  $m$  is even and equal to  $2n$ , and

$$x_m - 2 \sum_{\substack{i+j=m \\ 0 \leq i < j}} y_i y_j = 0,$$

otherwise.

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  $X(k^{(m)})$ .

**4.2 Fact.** 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  $\rho_n$ . For  $a \in X(k)$ , the  $n^{\text{th}}$  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  $a$ .

Finally, define  $\mathcal{A}X(k)$ , **the full arc bundle of  $X$  over  $k$** , as the inverse limit of  $(\mathcal{A}_i X(k))_{i \in \omega}$  and 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  $\text{SCH}_{p,1}$ .

**4.3 Lemma.** *Let  $X$  be an algebraic variety defined over  $C_F$ .*

*If  $\mathbf{a} \in X(\mathcal{U})$ , then  $\nabla_X(\mathbf{a}) = (\partial_0(\mathbf{a}), \partial_1(\mathbf{a}), \dots) \in \mathcal{A}X(\mathcal{U})$  and in particular  $\nabla_{X,m}(\mathbf{a}) = (\partial_0(\mathbf{a}), \dots, \partial_m(\mathbf{a})) \in \mathcal{A}_m X(\mathcal{U})$  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  $\nabla_X(\mathbf{a})$  is just another way of presenting  $\mathbb{D}_\partial(\mathbf{a})$  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  $\mathbf{a} \in X(\mathcal{U})$ , then  $p(\mathbb{D}_\partial(\mathbf{a})) = 0$ . Which is another way of saying that  $\nabla_X(\mathbf{a}) \in \mathcal{A}X(\mathcal{U})$ .

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

**4.4 Corollary.** *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  $\nabla_G \circ \cdot = \mathcal{A}(\cdot) \circ \nabla_{G \times G}$ .  $\square$

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  $\pi$  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  $\pi$ . 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:

**4.5 Fact.** *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

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

□

Define **the iterative logarithmic derivative** as the map

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

**4.6 Fact.** *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 4.5. □

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:

**4.7 Example.** *Let  $G = \mathbb{G}_\alpha$ , the additive group. Then  $\mathcal{A}(G) = \sum_{i=0}^{\infty} \mathbb{G}_\alpha$  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

Given an algebraic group defined over the constants of  $(F, \partial)$  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  $\ell D$  is defined as in the previous section and  $\alpha \in \mathcal{A}G_e(F)$  is an element contained in the image of  $\ell D$ .

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  $C_F = C_K$ .

**4.8 Example** (Back to iterative Picard-Vessiot equations). *Let  $G = GL_s$ , the general linear group of dimension  $s$ . Let*

$$\lambda_m: G(\mathcal{U}) \rightarrow \mathcal{U}^{s \times s}: A \mapsto \partial_m(A)A^{-1}.$$

*Note that by section 2.3 in [19]  $\ell D(A)$  can be identified with the sequence  $(\lambda_m(A): m \in \omega)$ , and so an iterative logarithmic differential equation over  $F$  can be seen as a sequence of equations of the form*

$$(\partial_m(Y)Y^{-1} = B_m: m \in \omega)$$

*with  $B_m \in F^{s \times s}$ .*

*Additionally, by theorem 2.11 of [19],  $(B_m: m \in \omega)$  is in the image of  $\ell D$  if the sequence of linear iterative differential equations*

$$(\partial_m(Y) = B_m Y: m \in \omega)$$

*is consistent in the sense of example 3.1.*

*This in particular implies that a Picard-Vessiot extension of  $(F, \partial)$  for a given linear iterative differential equation (recall example 3.1) is precisely an iterative differential Galois extension  $K$  of  $F$  for the corresponding iterative logarithmic differential equation on the general linear group.*

**4.9 Theorem** (Existence and Uniqueness of iterative differential Galois extensions). *If  $G$  is an algebraic group defined over the constants of  $(F, \partial)$  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  $\mathcal{U}$ .

**4.10 Lemma.**  *$\mathcal{M}$  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 3.10, 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 4.5). 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 3.9. 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 3.10 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 3.11.  $\square$

We now go back to the proof of theorem 4.9:

*Proof of theorem 4.9. (Existence)* Consider  $a \in \mathcal{M}_0 \cap \mathcal{X}$ . We claim  $K = F\langle a \rangle^s$  is an iterative differential Galois extension of  $F$  for the given equation. For this, we only need to prove that  $C_F = C_K$ .

Let  $b \in C_K$ . Then  $b = f(a)$  for some  $F$ -definable function  $f$ . The intersection of the graph of  $f$  with  $\mathcal{X} \times \mathcal{C}$  is the graph of a  $\emptyset$ -definable function in  $\mathcal{M}$ , so  $b = f(a) \in \mathcal{M}_0 \cap \mathcal{C}$ . Finally,  $b \in C_F$  by the last part of lemma 4.10.

*(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  $a'$ . We claim that  $\mathcal{M}_1 \cap \mathcal{C} = C_F$ :

Indeed, let  $b \in \mathcal{M}_1 \cap \mathcal{C}$  and  $p = \text{tp}(b/a')$  in  $\mathcal{M}$ . Since  $\mathcal{M}_1$  is prime,  $p$  is isolated by  $\psi(x)$ , an  $a'$ -definable subset of  $\mathcal{C}$ . Since  $\text{Th}(\mathcal{M})$  has quantifier elimination, and by lemma 2.7, we get that  $\psi(x)$  is definable over some  $c \in \mathcal{C}$  in the structure  $(\mathcal{C}, +, \cdot)$  where  $c \in \text{dcl}(Fa')$ . This is  $c \in K' \cap \mathcal{C}$ , which is precisely  $C_F$  by the definition of ID-Galois extensions. As in the proof of lemma 3.11, this proves that  $b \in C_F$ , finishing the proof of the claim.

Now, since the type of  $a$  is principal, 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  $a'' \cdot g = a'$  but this implies that  $\text{dcl}(Fa') = \text{dcl}(Fa'')$ .

Now, since  $\text{tp}(a) = \text{tp}(a'')$  in  $\mathcal{M}$ , then  $\text{tp}(a/F) = \text{tp}(a''/F)$  in  $\mathcal{U}$  and so, by saturation, there is an automorphism fixing  $F$  and sending  $a$  to  $a''$ . This automorphism, restricted to  $\text{dcl}(Fa)$ , provides us with an isomorphism of ID-fields between  $\text{dcl}(Fa)$  and  $\text{dcl}(Fa'')$ .  $\square$

Finally, we observe that the ID-Galois extensions just defined are strongly normal extensions:

**4.11 Theorem.** *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 4.6. 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 3.14.  $\square$

### 4.3 Strongly normal extensions revisited

Now let us go back to our strongly normal extensions and see that, under the hypothesis of the primitive element theorem (Thm. 3.15), they are ID-Galois extensions for an appropriate iterative logarithmic differential equation over the base field:

**4.12 Theorem.** *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  $\alpha$  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 4.6 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  $\sigma$  induces an isomorphism between  $K$  and  $K'$ . Thus  $K$  is isomorphic to a Galois differential extension of  $F$  for an appropriate logarithmic

differential equation. □

To conclude, let us prove, under the same hypothesis 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. More precisely:

**4.13 Theorem.** *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  $\alpha$  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  $\alpha$ , which are all in  $F$ . This in particular implies that  $\text{tr.deg}(K/F) = \text{tr.deg}(F(a)/F)$ .

Secondly, by fact 4.6, 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,  $\text{tr.deg}(K/F) = \text{tr.deg}(\mathcal{X}) = \text{tr.deg}(G(\mathcal{C})) = \dim(G(\mathcal{C}))$ . □

## 4.4 Historic and bibliographical notes

Arc spaces were introduced by Nash in [24] to study resolution of singularities. Later, they were used by Kontsevich as the basis for his theory of motivic integration. Eduard Looijenga's *Motivic measures* [16] is a good reference if you want to learn more about them and their uses. In the context of iterative derivations, arc spaces and prolongation spaces, which are closely related, play an important role in Piotr Kowalski's work on the geometric axiomatization of existentially closed ID-fields [14].

Anand Pillay's paper *Algebraic D-groups and Differential Galois theory* [30] motivated most of the results from this chapter.

Turn up your nose at things in general, and when you let slip any thing a little *too* absurd, you need not be at the trouble of scratching it out, but just add a foot-note and say that you are indebted for the above profound observation to the "*Kritik der reinen Vernunft*", or to the "*Metaphysische Anfangsgründe der Naturwissenschaft*". This will look erudite and —and— frank.

Edgar Allan Poe, *How to Write a Blackwood Article*

# References

- [1] J. Baldwin, *Fundamentals of Stability Theory*. Springer, 1988.
- [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] E. Bouscaren, ed. *Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*. Springer, 1999.
- [4] E. Casanovas, *Lecture notes on stable and simple theories*. Available online at <http://www.ub.es/modeltheory/documentos/stability.pdf>.
- [5] B. Diarra, *Cours d'Analyse p-Adique*. Available online at <http://www.maths.univ-bpclermont.fr/~diarra/coursDEA.pdf>.
- [6] 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).
- [7] R. Hartshorne, *Algebraic Geometry*. Springer, 1977.
- [8] H. Hasse, *Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik*. Journ. reine angew. Math., vol. 175, 1936 (pp. 50-54).
- [9] W. Hodges, *A Shorter Model Theory*. Cambridge, 1997.
- [10] E. Hrushovski, *Unidimensional theories are superstable*. Annals of Pure and Applied Logic 50, 1990 (pp 117-138).
- [11] 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).
- [12] J.E. Humphreys, *Linear Algebraic Groups*. Springer, 1998.
- [13] E.R. Kolchin, *Differential Algebra and Algebraic Groups*. Academic Press, 1973.
- [14] P. Kowalski, *Geometric axioms for existentially closed fields with Hasse derivations*. Annals of Pure and Applied Logic 135, 2005 (pp. 286-302).
- [15] P. Kowalski and A. Pillay, *On the isotriviality of projective iterative  $\delta$ -varieties*. 2006. Preprint available online at <http://www.math.uni.wroc.pl/~pkowa/prace.html>.

- [16] E. Looijenga, *Motivic measures*. Séminaire Bourbaki Vol 1999/2000, Astérisque No. 276, 2002 (pp. 267-297).
- [17] A. Magid, *Differential Galois Theory*. Mem. AMS, 1994.
- [18] H. Matsumara, *Commutative Ring Theory*. Cambridge University Press, 1986.
- [19] H. Matzat, *Differential Galois theory in positive characteristic*, notes written by Julia Hartmann. Preprint, 2001.
- [20] H. Matzat and M. van der Put, *Iterative differential equations and the Abhyankar conjecture*. J. reine angew. Math. 257, 2003 (pp. 1-52).
- [21] D. Marker, *Model Theory: An Introduction*. Springer, 2002.
- [22] D. Marker, *Manin kernels*. Quaderni di matematica, Vol. 6 (Connections Between Model Theory and Algebraic and Analytic Geometry), 2000.
- [23] M. Messmer and C. Wood, *Separably closed fields with higher derivations*. Journal of Symbolic Logic, Vol. 60, n. 3, Sep. 1995 (pp. 898-910).
- [24] J. Nash, *Arc structure of singularities*. Duke Math. J. 81, 1995 (pp. 31-38).
- [25] R. Moosa, A. Pillay and T. Scanlon, *Differential arcs and regular types in differential fields*. Preprint, 2004.
- [26] 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).
- [27] K. Okugawa, *Differential Algebra of Nonzero Characteristic*. Lectures in Mathematics 16. Kinokuniya Company Ltd., Tokyo, 1987
- [28] A. Pillay, *Geometric Stability Theory*. Oxford Logic Guides, 1996.
- [29] A. Pillay, *Two remarks on differential fields*. Quaderni di matematica, Vol. 11 (Model Theory and Applications), 2002.
- [30] A. Pillay, *Algebraic D-groups and differential Galois theory*. Pacific J. Math 216, 2004 (pp. 343-360).
- [31] A. Pillay, *Differential Galois theory I*. Illinois Journal of Mathematics, Vol. 42, n. 4, Winter 1998 (pp. 678-699).
- [32] A. Pillay, *Differential Galois theory II*. Annals of Pure and Applied Logic 88, 1997 (pp. 181-191).
- [33] A. Pillay and D. Marker, *Differential Galois theory III: Some inverse problems*. Illinois Journal of Mathematics, Vol. 3, 1997 (pp. 453-461).
- [34] A. Pillay and Ž. Sokolović, *Superstable differential fields*. Journal of Symbolic Logic, Vol. 56, n. 1, Mar 1992 (pp. 97-108).
- [35] B. Poizat, *A Course in Model Theory*. Springer, Universitext Series, 2000.
- [36] B. Poizat, *Stable Groups*. AMS, 2001.
- [37] B. Poizat, *Une théorie de Galois imaginaire*. Journal of Symbolic Logic, Vol. 48, n. 4, Dec 1983 (pp. 1151-1170).

- [38] M. van der Put and M. Singer, *Galois Theory of Linear Differential Equations*. Springer, 2003.
- [39] I. Shafarevich, *Basic Algebraic Geometry I*. Springer, 1994.
- [40] M. Ziegler, *Separably closed fields with Hasse derivations*. Journal of Symbolic Logic, Vol. 68, n. 1, Dec 2003 (pp. 311-318).
- [41] 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).

# Author's Biography

Javier Arturo Moreno was born in Bogotá, Colombia, in 1977. He graduated from the Universidad Nacional de Colombia on May 2001 and began graduate studies at UIUC a few months later. He finished this thesis, after some struggle, on January 2008, and currently lives in Barcelona, Spain, with Mónica, his wife, and Plinio, their yellow cat.

He enjoys staring at the sea, cooking, reading fiction, and writing short stories.