Noname manuscript No.
(will be inserted by the editor)

The Tannakian formalism for modules with a connection, from the model-theoretic point of view

Simon Iosti

the date of receipt and acceptance should be inserted later

Abstract We prove part of the Tannakian duality, namely the fact that one can recover a group from its category of representations, for generalized differential rings — which allows a unified treatment of differential and difference rings. This is achieved using model-theoretic tools such as internality and binding groups, and the analysis of imaginaries. We apply our results to obtain a generalization of Galois-theoretic results on difference fields.

Keywords Tannakian category · binding group · generalized differential ring

Mathematics Subject Classification (2000) 03C60 · 03C98 · 13L05 · 18D10

Introduction

The aim of this work is to prove a model-theoretic version of the Tannakian formalism for the generalized differential rings. The notion of a generalized differential ring is developed in [1], section II. It provides a unified framework for the analysis of structures including both differential and difference rings. In the same article, Yves André also develops the notion of a connection on a module, which is the analogue of the notion of a differential module, and which André uses to prove a Tannakian duality ([1], theorem III.2.1.1 and thereafter). For an exposition of the Tannakian duality, one can consult [5]. The model-theoretic proof of this duality in this general context is inspired by the work of Moshe Kamensky in [8], where the special case of this theorem corresponding to pure fields of characteristic zero is proved using model theory. The proof exposed here, working in a more general framework, is nevertheless

Simon Iosti
Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne cedex, France, E-mail: iosti@math.univ-lyon1.fr

not far from Kamensky's. It is centered around the model-theoretic notions of internality and binding groups, and heavily uses the latter.

Intuitively speaking, the Tannakian formalism, as presented here, says that one can reconstruct an affine algebraic group defined over a given field, considering only the category of its finite-dimensional representations over that field. A major motivation for studying this subject using model theory is that it permits to analyze interdefinability problems between fields — or rings — and groups.

Our methods yield also a modest improvement of a result of [3] (theorem 2.9 there) on difference Galois groups; with relatively little effort, the arguments in [3] and the results about Picard-Vessiot extensions can be generalized to the context of generalized differential fields, and hence hold in particular for the theory $ACFA$.

The plan of the article is as follows. The first section aims at defining stable embedding and internality, in order to prove the (type-)definability of the binding group associated to such an internality. The end of the section presents a Galois correspondence, a particular case of which will be used in section 3. Section 2 presents the notions of a generalized differential ring and a connection as they are presented in [1], sections II.1 and II.2. We define here a generalized differential ring and an appropriate language to turn it into a first order structure. Some hypotheses on the rings in question are also made there. Section 3, which is the central section to this article begins with a presentation of a construction of the Tannakian category generated by a module with a connection satisfying certain hypotheses. Most of the proofs are omitted, since they can essentially be found in [1], section II. This category is then seen as a first order structure containing in particular the generalized differential ring, and a proof of the Tannakian formalism (at least of a certain version of it) is given, based on the observation of the fact that this category is internal to the ring; the construction of the binding group follows. Section 4 compares the different definitions of a Picard-Vessiot extension for generalized differential fields that can be found in [11], [1], and [3], and proves a generalization of a theorem in [3] comparing the Galois groups associated to such extensions.

In the sequel, all the rings will be commutative and unitary, and the theories will be first order theories.

This work was realized during my Ph.D., under the supervision of Tuna Altınel.

1 Stable embedding, internality, and binding groups

The notion of stable embedding of a definable set in a model of a first order theory means intuitively that one can control the parameters involved in the definition of subsets of this set. In a stable theory, every definable set is stably embedded. One can find a proof of the caracterisations of the stable embedding presented below in [4], in the appendix.

Definition 1.1 (Stable embedding) Let T be a first order theory, and let A be a set definable without parameters in a model of this theory. One says that A is *stably embedded* if for every set B definable with parameters, and every $n \in \mathbb{N}$, $A^n \cap B$ is definable with parameters in A.

Lemma 1.2 *Let T be a first order theory, M one of its models, and A definable in M without parameters. The following conditions are then equivalent:*

1. *the set A is stably embedded;*
2. *for all $\alpha \in M$, there exists a subset A_0 of A of cardinality at most $|T|$ such that $tp(\alpha/A_0)$ has the same set of realizations as $tp(\alpha/A)$;*
3. *for all $\alpha \in M$, the type $tp(\alpha/A)$ is definable over a set of parameters $A_0 \subset A$.*

When T has saturated models, the stable embedding of A is characterized by a certain "A-homogeneity" of those models:

Lemma 1.3 *Let T be a first order theory, M a saturated model (in its own cardinality) of T with a regular cardinality, and A a definable set. The following conditions are then equivalent:*

1. *the set A is stably embedded;*
2. *for all $a, b \in M$ such that $tp(a/A) = tp(b/A)$, there exists $\sigma \in Aut(M/A)$ such that $\sigma(a) = b$;*
3. *any automorphism of the structure A lifts to an automorphism of M.*

We will work with the following version of internality:

Definition 1.4 (Internality) Let A and B be two definable sets in a model of a first order theory. The set B is said to be *internal* to A, or *A-internal*, if there exists an injective map $i : B \to A$ which is definable (eventually with parameters).

The definability of the binding group in the frame of an internality to a stably embedded set is proved in [6], proposition 1.6. In fact, a more general result is proved there, namely the definability of the *binding groupoid*. This definability is well-known for certain classes of theories, such as stable theories. One can consult [10], theorem 7.4.8, for a treatment of this case.

Theorem 1.5 (Binding group) *Let T be a first order theory eliminating imaginaries, M a model of T, and A and B two definable sets in M. Assume that A is stably embedded, B is A-internal, and the model M is saturated in its own regular cardinal. Then, the group $Aut(B/A)$ of the functions from $B \cup A$ into itself induced by an automorphism of M fixing A pointwise is type-definable (as well as its action on B) over a set of parameters $A_0 \subset A$ of size at most $|T|$. It is called the binding group of B in A, and is denoted $BG(B/A)$.*

The binding group can be seen as a model-theoretic Galois group, and one can in particular obtain a certain Galois correspondence between its definable subgroups and certain definably closed sets. We will need later a particular case of this correspondence, so we will make its formulation explicit.

The following general and easy group-theoretic lemma will frequently be used in the sequel:

Lemma 1.6 *Let G be a group acting freely on a set X. Then no proper subgroup of G has a G-invariant orbit.*

Proof If H is a subgroup of G with $H.c$ (for some $c \in X$) a G-invariant orbit, then $G.(H.c) = H.c = (GH).c = G.c$. Since the action of G on $G.c$ is free, this proves that $G = H$.

□

The previous lemma is central in the construction of Galois correspondence. We give below the best version we know of such a correspondence in our context. It will not be needed in the sequel.

Theorem 1.7 (Galois correspondence for binding groups) *Let T be a first order theory, M a saturated model (in its own regular cardinality) of T, and A a definable stably embedded set. Assume that M is A-internal, and that this internality is witnessed by an injective map $f_c : M \to A$. Denote by BG the binding group $BG(M/A)$, and assume that it is type-definable over a set of parameters A_0. The application ϕ associating to a subgroup of BG the set of points fixed by this subgroup defines an injection from the set of the definable subgroups of BG into the set of the definable definably closed sets of M containing A; its "inverse" is the application associating to a definable definably closed set D the binding group $BG(M/D)$.*

Proof Denote by $\psi : \left| \begin{array}{c} \{G/G \leq BG\} \to \{dcl(D)/A \subseteq D\} \\ G \mapsto M^G \end{array} \right.$ the application associating to a subgroup G of BG the set of points in M fixed by G (denoted by M^G). We will consider the restriction of this map to the set of definable subgroups of BG, denoting this restriction ϕ, and we will now prove that ϕ is an injection and that for any definable subgroup G of BG, we have $G = BG(M/\phi(G))$.

Remark that ϕ actually takes its values in the definable definably closed sets containing A. Indeed, since BG fixes A, any subgroup of BG fixes A as well, and if an element a is definable over M^G, then it is obviously fixed by G, and is then already in M^G. Moreover, M^G is obviously definable when G is. Every set $\phi(G)$ is then definable, definably closed, and contains A.

Now, we can prove that ϕ is injective. Let G and H be two definable subgroups of BG such that $M^G = M^H$. We want to prove that $G = H$. We will in fact prove that G is the binding group $BG(M/M^G)$, which is enough to conclude (since in this case, H will be the same group). In particular, it also proves the remainder of the theorem. The set M^G is definable and definably closed, hence it is stably embedded: if S is a subset of $(M^G)^n$ definable with parameters in M, then the canonical parameter of S is in $dcl(M^G)$, and is then in M^G. The group $BG(M/M^G)$ is then type-definable (by theorem 1.5), and one has by definition $G \leq BG(M/M^G)$, and G and $BG(M/M^G)$ fix the same elements in M. By lemma 1.6, this implies $G = BG(M/M^G)$. The application ϕ is then injective.

□

2 Generalized differential rings and connections

Recall that all the considered rings are commutative and unitary.

The definitions and the treatment of the generalized differential rings and the connections presented in this section come from [1], sections II.1 and II.2. The rare interventions of model theory are quite natural, and will be useful in the next section. The next proposition is admitted, but one can find in [9], corollary of the theorem 7.12, a proof of the fact that on a commutative (unitary) ring, a finitely presented module is projective if and only if it is flat. The rest of the proof is easier.

Proposition 2.1 *Let A be a commutative noetherian ring, and M an A-module. The module M is faithful, finitely generated and projective if and only if it is faithfully flat and finitely presented.*

Definition 2.2 (Generalized differential ring) We call *generalized differential ring* a ring k, a k-algebra A, and an A-A-bimodule Ω (that is, an abelian group with a left and a right scalar multiplications ${}_{\Omega}\cdot$ and $\cdot_{\Omega}$) together with a bimodule homomorphism $d : A \to \Omega$ (which we will call the *derivation*), satisfying the condition

$$d(ab) = a \ {}_{\Omega}\cdot \ d(b) + d(a) \ \cdot_{\Omega} \ b$$

and such that $ker(d) = k$. The ring k is called the *ring of constants* of A.

Pure rings can be seen as generalized differential rings with $k = \Omega = A$ and $d = 0$. The ordinary differential rings are generalized differential rings, with

$\Omega = A$ and d the usual derivation on A. One can also see a difference ring (A, σ) as a generalized differential ring: put $\Omega = A$ with the usual multiplication as left A-module structure; the multiplication "twisted" by σ as right A-module structure: for $a \in A$ and $\omega \in \Omega$, $\omega \ \cdot_\Omega \ a = \sigma(a) \ {}_\Omega\cdot \ \omega$; and the derivation defined by $d(a) = \sigma(a) - a$.

Let (k, A, Ω, d) be a generalized differential ring.

Hypothesis 1 *Except when otherwise stated, we will need the following assumptions in the sequel :*

1. *A is noetherian;*
2. *the ring k is a field;*
3. *Ω is reduced, that is to say generated (as a left module, or right module, or bimodule, those three conditions being equivalent) by $d(A)$;*
4. *Ω is faithful, projective, and finitely generated over A (or, equivalently by proposition 2.1, is faithfully flat and finitely presented) as a right A-module.*

Consider the following language and theory to describe this structure:

Definition 2.3 The language L is defined as the language containing:

- a sort A endowed with the language of rings;
- a unary predicate k, and ternary predicates $+_k$ and $\times_k$;
- ternary predicates $\cdot_A$, $+_A$ and $\times_A$;
- a n-ary predicate Ω, and $(n+1)$-ary predicates $\cdot_\Omega$, ${}_\Omega\cdot$, a $3n$-ary predicate $+_\Omega$ and a n-ary relation E_Ω;
- a function symbol $d : A \to A^n$.

We define T as the theory of the structure (k, A, Ω, d) in this language, each of the predicate symbol being interpreted in the way suggested by the corresponding symbol.

When the module Ω is finitely presented (hypothesis 1.4), it can be expressed as a quotient of A^n by an equivalence relation E definable (with parameters) in the A-module structure of A^n. The equivalence relation is defined by a finite set of relations which is a presentation of Ω (the parameters involved in the definition of E are then the generators of Ω chosen to make this presentation explicit).

Define now the notion of a connection, which permits to generalize to the case of generalized differential rings the notion of a differential module.

Definition 2.4 (Connection) Consider a finitely generated and projective left A-module M. A *connection* is an additive application $\nabla_M : M \to \Omega \otimes_A M$ satisfying the following relation:

$$\nabla_M(am) = a.\nabla_M(m) + d(a) \otimes m$$

We define in the same way a connection for a right A-module.

If A is a pure ring, then a connection is just a linear application. When A is an ordinary differential ring, a module together with a connection is exactly a differential module.

The derivation is (canonically isomorphic to) a connection on A. If M is a left (or right) A-module, then we can define a connection on M putting $\nabla(am) = (a + d(a)) \otimes m$. Then, for all m, $\nabla(m) = 1_A \otimes m$, and we obtain $\nabla(am) = a\nabla(m) + d(a) \otimes m$. The application ∇ defined this way is then a connection on M. Any connection isomorphic to such a connection is called *trivial connection*. In particular, one can define a connection (on the right or on the left) on Ω this way.

Hypothesis 2 *The module Ω is endowed with the trivial connection, denoted ∇_Ω.*

3 The Tannakian formalism

In this section, we consider a generalized differential ring A in the language defined in the preceding section, satisfying the same hypotheses. The aim of this section is to consider the first-order structure constituted by the category of finite-dimensional representations of an algebraic group, to prove that this whole structure is internal to the field over which the group is defined, and to show that the resulting binding group is actually equal to the original group, using the lemma 1.6 and an analysis of the imaginaries in this category.

We will consider here categories $\mathbf{C}$ endowed with a bifunctor $\otimes$ satisfying some constraints. An *associativity constraint* is an isomorphism of functors $\phi_{A,B,C} : A\otimes(B\otimes C) \to (A\otimes B)\otimes C$ for which we ensure that the different ways of computing several tensor products are all isomorphic for all A, B, and C. A *commutativity constraint* is an isomorphism of functors $\psi_{A,B} : A\otimes B \to B\otimes A$ for which we ensure that $\psi_{A,B} \circ \psi_{B,A}$ is the identity of A for all objects A, B.

A category is said to be a *tensor category* if it has:

- an identity object $\mathbf{1}$ for $\otimes$;
- an associativity constraint;
- a commutativity constraint;

and these two constraints interact the same way as usual tensor products.

The *internal hom* associated to X and Y is the object $\underline{Hom}(X, Y)$ representing the functor $Z \to Hom(Z \otimes X, Y)$ when it is representable. The dual of X is $X^* = \underline{Hom}(X,\mathbf{1})$, and X is said to be reflexive when X is canonically isomorphic to its bidual X^{**}. The tensor category $\mathbf{C}$ is said to be *rigid* if every internal hom is defined, the morphisms $\underline{Hom}(X, Y) \otimes \underline{Hom}(Z, T) \to \underline{Hom}(X \otimes Z, Y \otimes T)$ are isomorphisms, and every object is reflexive.

It is possible to define easily the notion of tensor functor, that is a functor respecting the structure given by $\otimes$; similarly, one can define a morphism of functors, and an equivalence of tensor categories. In the following, we will consider tensor categories that are also abelian; the typical example is the category Mod_A of finitely generated A-modules over a commutative ring A, endowed with the usual tensor product.

Finally, we define a *fibre functor* on an A-linear tensor category to be a faithful exact A-linear tensor from C to Mod_A, the category of finitely generated A-modules. We can now define a neutral Tannakian category:

Definition 3.1 (Neutral Tannakian category) A category $\mathbf{C}$ is said to be neutral Tannakian over A if it is a A-linear abelian rigid tensor category, endowed with a fibre functor ω.

We will now try to define a first-oder context which will allow us to describe Tannakian categories over a given ring A.

Definition 3.2 We consider the following language $L_{\mathbf{C}}$:

- the language of generalized differential rings for A defined in definition 2.3, with a constant symbol for each element of A;
- a sort S_V for each object V of $\mathbf{C}$, and a function symbol v_f for each arrow f in $\mathbf{C}$ between the corresponding sorts;
- the language of k-vector spaces on each sort S_V;
- a function symbol $b_{V,V'} : S_V \times S_{V'} \to S_{V \otimes_k V'}$ for all V, V'.

If $\mathbf{C}$ is a neutral Tannakian category over A, then we call $T_{\mathbf{C}}$ its elementary theory in the language $L_{\mathbf{C}}$.

When A is noetherian (hypothesis 1.1), we know that a finitely generated module M is noetherian (as a left or right A-module). Hence, any submodule of M is finitely generated; such a submodule is then the quotient of a free finitely generated module by one of its submodules, and this submodule is again finitely generated (by noetherianity); hence, any submodule of M is finitely presented. Moreover, if N and N' are two finitely presented and flat modules, then $N \otimes_A N'$ and $N \oplus N'$ are also finitely presented and flat (and, by proposition 2.1, are finitely generated and projective). The category generated by a module M is the category whose objects are the subquotients of the modules obtained by tensor product, direct sum, and dualization, starting from M. If $\mathbf{C}$ is generated by a unique object M, then we also denote $T_{\mathbf{C}}$ by T_M.

We will now prove a general proposition about imaginaries in a neutral Tannakian category on which a "nice" group acts. This will be fundamental in the proof of the Tannakian formalism, theorem 3.18.

Definition 3.3 (Good polynomials) A language is said to *give good polynomials* if it is the language of rings augmented with unary function symbols.

The *algebra of good polynomials* denoted $A[x]$ over a tuple of variables $x = (x_1, \dots, x_n)$ associated to a structure A in this language is the algebra defined as the set of terms with parameters over A, endowed with the addition, multiplication, and composition of polynomials.

An example of such a language (which is the one we will be interested in) is the language of generalized differential rings. In this case, the polynomials are the generalized differential polynomials. In particular, in the situation of a usual differential ring, the polynomials are the differential polynomials, and in the case of difference rings, the polynomials are the usual difference polynomials.

Proposition 3.4 *Assume that the language of A gives good polynomials. Let H be an affine algebraic group defined over A, and C a Tannakian category over A, over which H acts. Then every H-orbit of the form $H.c$ with c a basis of a module V in C is coded by an element of a projective space associated to an object of C.*

Proof The group H is defined by a polynomial equation on A, say $P(x) = 0$ (x may be a tuple of variables). The basis c permits to identify the set of polynomials $A[x]$ and the symmetric space $S(V^*)$, sending the variable x_i to the i^{th} element of the dual basis of c. We denote by ϕ_c this identification map from $A[x]$ to $S(V^*)$ induced by the basis c. This identifies the ideal $\langle P \rangle$ of $A[x]$ generated by P and an ideal I of $S(V^*)$, generated by the element corresponding to P in $S(V^*)$. If u is an automorphism of the Tannakian structure, then u sends $H.c$ to the set $H.u(c)$. Call I' the image of the ideal $\langle P \rangle$ under the identification $\phi_{u(c)}$ induced by the basis $u(c)$. Then u sends I to I', and u fixes setwise the orbit $H.c$ if and only if $I = I'$, so we will try to find a code for the ideal I.

This ideal being generated by a single element, it is completely determined by its intersection with a finitely generated submodule W of $S(V^*)$, and this intersection $W \cap I$ is itself a finitely generated submodule of $S(V^*)$; the symmetric space $S(V^*)$ is constructed from V using only dualization, direct sums, and tensor products. Consequently, the ideal I is completely determined by its intersection with an object of C, since C is stable under all those operations. Taking the exterior power of W in an appropriate degree, we obtain a new object of C (for the same reasons), such that $W \cap I$ is a submodule of dimension 1 of it. Consequently, $W \cap I$ corresponds to the unique element of the projective space associated to the exterior power of W, and this element is a code for the orbit $H.c$.

□

We will now use this proposition to prove that if G is an affine algebraic group over A, then its category of finitely generated representations over A-

modules is a neutral Tannakian category, and the group of automorphisms of the fibre functor $Aut^{\otimes}(\omega)$ is definably isomorphic to G in A.

3.1 A Tannakian category

To check that a category is a Tannakian category requires to verify various closure properties under tensor products, dualizations, and subquotients; in the case of modules with a connection, the conditions implying these properties were checked by André in [1], and this will be briefly revised in the following subsections for the ease of the reader.

3.1.1 The tensor product

Consider ∇_M and ∇_N, two connections on two A-modules M and N. We want to define a connection on the module $M \otimes_A N$ induced by those two connections (recall that the module structures used to construct $M \otimes_A N$ are the left module structure for M and the right module structure for N, so that $a(m \otimes n)b = (am) \otimes (nb)$). If Ω is a commutative bimodule, we can proceed as follows: define $\nabla_{M \otimes_A N}(m \otimes n) = \nabla_M(m) \otimes n + \varphi(m \otimes \nabla_N(n))$, φ being the canonical isomorphism $M \otimes \Omega \otimes N \to \Omega \otimes M \otimes N$. The resulting map is a connection on $M \otimes_A N$.

If Ω is not commutative, then for any A-module with a connection M, we want to build an exchange morphism $\phi : M \otimes \Omega \to \Omega \otimes M$ such that $M \otimes_A N$ becomes a module with a connection. The following proposition adresses this problem:

Proposition 3.5 ([1], Proposition II.4.1.1) *Under the hypothesis 1.3 (Ω is reduced), for any A-module with a connection M, there exists a unique morphism $\phi = \phi_M : M \otimes_A \Omega \to \Omega \otimes_A M$ such that for any A-module with a connection N, the application*

$$\nabla_{M \otimes_A N}(m \otimes n) = \nabla_M(m) \otimes n + (\phi \otimes id_N)(m \otimes \nabla_N(n))$$

is a connection.

3.1.2 Dualization

Definition 3.6 (Rigidity) A module with a connection is said to be *rigid* if it has a dual in the category of the A-modules with a connection.

Recall that $M^* = \underline{Hom}_A(M, A)$ is the dual of M, considered as an A-module.

Proposition 3.7 ([1], Lemma II.3.3.4) *Under the hypothesis 1.3 (Ω is reduced), if the application ϕ_M defined in the proposition 3.5 is invertible, then the application $\nabla_{M^*} : M^* \to \Omega \otimes_A M^*$ defined by*

$$p((id_\Omega \otimes \epsilon)(\nabla_{M^*}(n^*) \otimes m)) = d(n^*(m)) - p((\epsilon \otimes id_\Omega)(n^* \otimes \phi_M^{-1}(\nabla_M(m))))$$

($\epsilon : M^* \otimes M \to A$ being the application of evaluation and p being either one of the two product operations $A \otimes_A M \to M$ or $M \otimes_A A \to M$) is a connection on M^*, and the application ϕ_{M^*} satisfies, for all $m \in M$,

$$p(id_\Omega \otimes \epsilon)(\phi_{M^*}(n^* \otimes \omega) \otimes m) = p(n^* \otimes id_\Omega)(\phi_M^{-1}(\omega \otimes m))$$

The formulas in the preceding proposition can seem obscure, but they are nothing more than the formal translation of the fact that we want to define a connection on the dual of M (see [1] for the details). This proposition permits in particular to prove the following:

Proposition 3.8 ([1], Lemma II.4.2.1) *A module with a connection M is rigid if and only if it is projective and finitely generated and the application $\phi(\nabla_M)$ is invertible.*

3.1.3 Subquotients

To achieve the closure of the category under subquotients, we need the following additional hypothesis :

Hypothesis 3 *Denote by $Q(A)$ the total ring of fractions of A. Assume that $Q(A)$ is semisimple (which means in particular that $Q(A)$ is a finite product of fields), that (A, d) is simple (that is its only differential ideals are 0 and A), and that $\Omega \otimes_A Q(A) \simeq Q(A) \otimes_A \Omega$.*

Proposition 3.9 ([1], Theorem II.5.3.2) *Under the hypotheses 3, 1.1 (A is noetherian), 1.3 (Ω is reduced), and 1.4 (Ω is faithful and projective finitely generated), any subquotient of a finitely generated projective module M with a connection which is rigid is also rigid.*

Under those hypotheses, we define the category $\mathbf{C}_M$ to be the subcategory of the category of A-modules with a connection generated by M and the tensor product, the direct sum, the dualization and the subquotients.

Proposition 3.10 ([1], Theorem II.5.3.2) *Under the hypotheses 3, 1.1 (A is noetherian), 1.3 (Ω is reduced), and 1.4 (Ω is faithful and projectif finitely generated), the category $\mathbf{C}_M$ is abelian, monoidal, symmetric, and rigid. Any set of morphisms has an A-module structure. Moreover, the "forgetful" functor $\omega : \mathbf{C}_M \to Mod_A$ respects the rigid monoidal symmetric structure, and the A-module structure on the sets of morphisms.*

3.2 Model-theoretical study

We will assume in this section that A is a commutative generalized differential ring, and that $\mathbf{C}_M$ is a Tannakian category over A, with M an object generating $\mathbf{C}_M$. We also assume that any object in $\mathbf{C}_M$ is finitely presented, though we will only need this assumption from lemma 3.13. We will study some model-theoretic properties of the resulting theory T_M.

We begin by proving a result about elimination of quantifiers in T_M, though this will not be used in the sequel :

Proposition 3.11 (Elimination of quantifiers for T_M) *The theory T_M eliminates quantifiers for formulas involving any sort but the sort for A.*

Proof The proof uses a back-and-forth argument. Consider a model $\mathbf{C}_M$ of T_M (which we assume to be saturated in a cardinal strictly greater to the cardinal of the substructures we will consider in the following), and two substructures D and D' of $\mathbf{C}_M$, of which the restriction to the sort of A are the same, with an isomorphism $u : D \to D'$ fixing A pointwise. We consider an element $a \in \mathbf{C}_M \setminus D$, and we try to find a' such that we can extend the isomorphism u to an isomorphism between the substructure generated by $D \cup \{a\}$ and the substructure generated by $D' \cup \{a'\}$ sending a on a'.

What is a substructure D of $\mathbf{C}_M$? Each sort in $\mathbf{C}_M$ is nonempty in D since D contains at least the zero vector of each module; by assumption, D also contains the whole sort A. Moreover, the fact that each sort in D is stable by multiplication by a scalar means that each sort of D is a module over A. The choice of an element of $\mathbf{C}_M$ not belonging to D is the same as the choice of an element a in a sort S of $\mathbf{C}_M$ not belonging to the module corresponding to this sort. To choose the image of a, we know that we have to choose it in the same sort, and not belonging to the corresponding module (in D'). Choose such an a', and define $u(a) = a'$. Since each sort in $\mathbf{C}_M$ is endowed with the language of modules, the structure generated by D and a corresponds on the sort S to the module generated by $D|_S$ and a. The application u extends then naturally to all this module, its image being extended to the module generated by $D'|_S$ and a'.

The language of T_M contains — beyond the language of modules on each sort — some symbols of functions between the sorts coding the linear applications, symbols of functions coding the tensor product, and symbols of functions coding the applications ∇. Any of those functions send a to an element $a_{S'}$ in a certain sort S', and we can as above extend u on the modules generated by those elements. The application u obtained is then an isomorphism between the substructure generated by D and a and the substructure generated by D' and a'.

Hence, the theory T_M eliminates quantifiers in this language as long as the sort for A is not involved.

□

We will now try to build the binding group $BG(\mathbf{C}_M/A)$, which we want to be type-definable in the theory T_M. We need for this to prove that $\mathbf{C}_M$ is internal to A, and that the sort of A is stably embedded in T_M.

Proposition 3.12 (Internality in T_M) *Each sort of T_M is internal to the generalized differential ring A.*

Proof The choice of a generating family of M permits, using the different categorical operations studied above, to deduce a generating family for each module in the category $\mathbf{C}_M$: For the direct sum, this is obvious; for the tensor product, the tensor product of two generating families is a generating family; for the dual, consider the dual family; same thing for the quotient; finally, a submodule of N is the dual of a quotient of N. Hence, the choice of this generating family of M permits to define a definable function from any of the objects of $\mathbf{C}_M$ into the underlying model of T, which gives the internality of T_M into T.

□

We will now prove (proposition 3.15) that the sort of the ring A is stably embedded in T_M, and that any subset of some A^n which is definable in T_M is already definable in A ; in order to do this, we need a description of the terms and the formulas in the language, given in the following lemmas. A term can be seen as a map from a cartesian product of sorts to another sort, $t : \prod_i N_i \to N$. The modules in T_M being finitely presented, there exists isomorphisms $u_i : N_i \to A^{n_i}/I_i$ for all i and $u : N \to A^n/I$, for some integers n_i and n and some finitely generated submodules I_i of A^{n_i} and I of A^n. Note that the equivalence relations defined by the submodules I_i is definable in A, because of the finite generation of these. Hence, the modules A^{n_i}/I_i are in A^{eq}.

Lemma 3.13 (Description of the terms in T_M) *Consider a term t (with parameters in a model of T_M) and the isomorphisms u_i and u with notations as above. Then there exists a first-order formula t_A in the language of A^{eq}, with parameters from A^{eq}, such that the isomorphisms u_i and u realize an isomorphism restricted to the graph of t, with image the set defined by t_A.*

Proof We prove it by induction on the size of the terms.

If the term t consists of only a variable symbol, then it corresponds to the identity on some sort N, and clearly corresponds to the formula t_A in the language of A^{eq} defined by $x = y$ in A^n/I. If the term consists of only a constant symbol c, then t_A is the formula defined by the constant $x = u(c)$ with $u(c)$ an element of A^n/I.

The language 3.2 contains function symbols for the A-module structures on the sorts, for the morphisms in the category $\mathbf{C}_M$, and for the tensor product of any two sorts.

For the A-module structure, consider two terms t and t' with values in N. Then, the term $t +_N t'$ corresponds to the formula $\exists y \in t_A, z \in t'_A, x = y \ +_{A^n/I} \ z$. If t is a term with values in A and t' a term with values in N, then the term $t ._N t'$ corresponds to the formula $\exists y \in t_A, z \in t'_A, x = y \ ._{A^n/I} \ z$.

For the maps in the category $\mathbf{C}_M$, if t is a term with values in N, and f is a function symbol for a map in the category $\mathbf{C}_M$, then the term $f(t)$ corresponds to the formula (with variables x and z) "$\exists y, t_A(x) = y \wedge z = f_A(y)$", where f_A is defined as follows : f being an A-linear map, it is completely determined by the images of some generating family of its domain N in its codomain N' ; so we choose such a generating family $(x_i)_i$, and we associate to it the corresponding tuple $(\bar{x}_i)_i$ with $\bar{x}_i \in A^n/I$ for all i, and we do the same for the family $(f(x_i))_i$ in $A^{n'}/I'$, associating to it the tuple $(\bar{x}'_i)_i$. Then f_A is defined as the definable map sending $(\bar{x}_i)_i$ to $(\bar{x}'_i)_i$, extended by linearity (since the generating family is finite, this can be expressed as a first order term in the language of A^{eq}).

For the tensor product, consider two terms t and t' with values in N and N' respectively. Then the term $b_{N,N'}(t, t')$ corresponds to the formula (with variables x, x', and z) "$\exists y, y', t_A(x) = y \wedge t'_A(x') = y' \wedge z = b_A(y, y')$", where b_A is defined as follows : as above, we choose generating families $(x_i)_i$ and $(x'_j)_j$ for N and N', and consider their images in $N \otimes N'$; to each of these families is associated the corresponding element in A^n/I, $A^{n'}/I$, and $A^{n''}/I''$ (the last one being isomorphic to $N \otimes N'$), and the definable map b_A is defined by extending it by bilinearity.

At this point, all the function symbols in the language of T_M have been taken care of, so by induction on the size of the terms, the lemma is true.

□

Lemma 3.14 (Description of the formulas in T_M) *Using the same notations as above, given a formula $\phi(x_1, \ldots, x_n)$ defining a subset X_ϕ of $\prod_i N_i$, there exists a formula $\psi_\phi(y_1, \ldots, y_n)$ in the language of A^{eq} with parameters from A^{eq} such that the map $\prod_i u_i$ realizes an isomorphism restricted to X_ϕ, with image X_{ψ_ϕ}.*

Proof We prove it by induction on the size of ϕ.

If ϕ is an atomic formula, then it is of the form $t = t'$ for two terms t and t', and by linearity, we may assume that it is of the form $t = 0$. By lemma 3.13, the map $\prod_i u_i$ realize a map between the graph of t and the set defined by t_A in the language of A^{eq} ; hence the formula ψ_ϕ can be taken as being $(x, 0) \in t_A$.

If ϕ and ϕ' are two formulas for which the lemma is true, then clearly the formula $\psi_{\neg\phi}$ is $\neg\psi_\phi$, and the formula $\psi_{\phi\wedge\phi'}$ is the formula $\psi_\phi \wedge \psi_{\phi'}$.

If $\phi(x_1, \ldots, x_n)$ is a formula for which the lemma is true, we seek the formula $\psi_{\exists x_1,\phi}$. In this case, the existential quantifier is over x_1 which is in some sort N_1 corresponding to some A^{n_1}/I_1, so it is enough, when we replace ϕ by ψ_ϕ, to replace the quantification over N_1 by a quantification over A^n/I in A^{eq} ; the formula $\psi_{\exists x_1,\phi}$ is then $\exists y_1, \psi_\phi$, and the induction is done.

□

Proposition 3.15 (Stable embedding of A in T_M) *The sort of A is stably embedded in T_M, and T_M does not define any new definable set on the models of $Th(A)$.*

Proof Let X_ϕ be a subset of some A^n, definable in T_M by some formula $\phi(x_1, \ldots, x_n)$ whose free variables lie in the sort of A. By lemma 3.14, there exists a formula $\psi_\phi(x_1, \ldots, x_n)$ in the language of A^{eq} over the same variables (since we can obviously choose the isomorphisms u_i to be the identity in this case), such that X_{ψ_ϕ} is equal to X_ϕ. The formula being in the language of A^{eq}, we know by the ^{eq}-construction that there exists a formula $\theta(x_1, \ldots, x_n)$ in the language of A (eventually with parameters from A) such that $\theta(x_1, \ldots, x_n)$ is equivalent modulo $Th(A)$ to $\psi_\phi(x_1, \ldots, x_n)$. Hence, any subset of some A^n definable in T_M with parameters from a model of T_M is in fact definable in the structure of generalized differential ring of A with parameters from A, which concludes the proof.

□

Remark 3.16 We could have done the preceding reasonings, and obtain the same conslusions, for other kinds of categories. What we use there is only the linear or multilinear nature of the function symbols in the theory. So, if we replace the Tannakian category by a category endowed with function symbols being interpreted as multilinear maps (such as the tensor product), and keep assuming the finite presentation of all the modules involved, then the category is still stably embedded in the sort of the ring A, which is stably embedded (and we have a similar description of the terms and formulas in the theory).

3.3 The Tannakian formalism

We can now prove the Tannakian formalism, still following the inspiration given by [8]. We will admit the following proposition, proved in [7], proposition 12, saying that any (type-definable) binding group is in fact an ω-group:

Proposition 3.17 ([7], proposition 12) *Let BG be the binding group associated to the internality of B into A, A being stably embedded, and the internality being witnessed by the function f_c whose parameter c is in the definable* *set C. Then BG is equal to the intersection of the groups of bijections from B to itself fixing a finite subset of the definable sets in B, and each of which is definable.*

Recall that given a group H, a *H-torsor* is a set on which H acts freely and faithfully.

Theorem 3.18 (Tannakian formalism) *Let G be an affine algebraic group in the theory T having a faithful representation in a finitely generated projective A-module with a connection M, this representation generating the category of its finitely generated representations. Then, G is definably (in T_M) isomorphic to the group $Aut^{\otimes}(\omega)$ of the automorphisms (preserving the tensor structure) of the forgetful functor ω from the category of A-modules with a connection to the category of A-modules.*

Proof Under these hypotheses, we can construct the theory T_M as above, and consider its binding group BG associated to the internality of T_M in T (see propositions 3.12 and 3.15). Denote by $\mathbf{C}_M$ the model of T_M considered here, with M the corresponding generator of $\mathbf{C}$. The group BG — which is type-definable (as its action) in T_M — acts by automorphisms on each of the representations of G generated by M, so necessarily, G and its action are type-definably (in T_M) isomorphic to a type-definable subgroup of BG endowed with the induced action.

Start by proving that the subgroup of BG corresponding to G is in fact definable in T_M. By proposition 3.17, there exists a group GL_f of permutations of a model of T_M, definable in T_M, and admitting BG as a subgroup. We can now define the subgroup of BG corresponding to G (that is, the set of elements in BG whose action on a generating family of M corresponds to the action of one of the elements of G) in the following way. The group G is the set of elements of GL_f whose action on a generating family of M is the same as the action of one of the elements of G. The groups GL_f (as a binding group) and G (as an affine group) are both definable in T_M (as is their action), so this group is definable in T_M. We can then suppose that G is a subgroup of BG which is definable, and not only type-definable.

Next, we prove that a torsor of the form $G.c$ is fixed setwise by the group BG. This will permit us to use the lemma 1.6 to prove the equality between G and BG.

By proposition 3.4, and since G is defined by good polynomials, a torsor of G of the form $G.c$ for c a generating family of M is coded by an element a of some projective space. Thus, the element a corresponds then to a representation (which is generated by only one element) of G, and hence is a sort of T_M, since T_M is, by assumption, (equivalent to) the category of finitely generated representations of G on A; in particular, it is a 0-definable set, and BG also stabilizes it. Hence, a is fixed by BG. By lemma 1.6, we have then that $G \simeq BG$. The isomorphism in question is even type-definable, since in order to define it, it is enough to fix a generating family of M and to define the image of $g \in G$ as the element $g' \in BG$ having the same action on this family.

To conclude, consider the forgetful functor $\omega : \mathbf{C}_M \to Mod_A$. By construction of T_M, the binding group BG is necessarily the group $Aut^{\otimes}(\omega)$ of the (tensor) automorphisms of ω: it preserves the operations (used to construct $\mathbf{C}_M$) of tensor product, dual, direct sum and subquotient.

□

We conclude this section by stating the other part of what is usually called the "Tannakian duality", and explaining how it fits into our context.

Proposition 3.19 ([5], theorem 2.11) *If C is a neutral Tannakian category over A, let G be the group $Aut^{\otimes}(\omega)$; then the category of finitely generated representations of G over A is equivalent (as a tensor category) to the category C.*

The obstacle to prove this statement in full generality is the following: if C is a neutral Tannakian category over A, then we can build its associated binding group G in the same way as above, and conclude that it is type-definable and isomorphic to the group $Aut^{\otimes}(\omega)$. We can then build its category of representations, and consider its associated binding group. But in order to prove that these groups are the same, we should use again the lemma 1.6. But not knowing if G is defined by polynomial formulas, we cannot use the proposition 3.4.

We prove below a partial remedy to this obstacle:

Proposition 3.20 *If the group H can be defined by a boolean combination of existential formulas, and if C is a Tannakian category over which H acts, then every H-orbit of the form $G.c$ with c a basis of a module V in C is coded by an element of a projective space associated to an object of C.*

Proof We can assume that H is defined by a formula of the form "$\exists y, \phi(x,y)$", the formula ϕ being a polynomial equation. If H is defined by the formula ϕ, then the reasoning of the proof of proposition 3.4 works identically.

Consider the subset X of A^m defined by $\phi(x,y).c$, m being the number of variables in x and y. The choice of the generating family c of V gives a basis for every object of the Tannakian category under consideration, and there exists such an object W, generated by m elements, such that V is a submodule of W.

The set X is defined by a polynomial equation; it is thus coded by the ideal generated by these polynomials in $A[X_1, \ldots, X_m]$, which corresponds to a finitely generated ideal I of $S(W^*)$. The set S, being the projection of X on the subspace V, is then coded by the quotient of I by the submodule $S(V^*)$, so by a submodule of $S(W^*)/S(V^*)$. Since the Tannakian category is closed under quotienting, we know that this module (or rather again a finitely generated submodule of it) is a sort of the theory T_C (that is, an object of the category C), and the reasoning is the same as in proposition 3.4 to conclude (passing to the exterior power, then to the projective space).

□

This result, however partial, covers an important case. In the article [4], 1.6, it is proved that in $ACFA$, any formula is equivalent to a disjunction of existential formulas. Hence, we obtain the following $ACFA$ version of the Tannakian duality:

Corollary 3.21 *Let C be a neutral Tannakian category over a model K of $ACFA$, and let G be the group $Aut^{\otimes}(\omega)$; then the category of finitely generated representations of G over K is equivalent (as a tensor category) to the category C.*

4 Applications of Tannakian methods

The aim of this section is to generalize some of the results of [3] on difference fields to the case of generalized differential fields, using in this respect the model-theoretic techniques developed in this paper. Namely, we will prove that two distinct ways of defining the Galois group associated to an equation over a generalized differential field lead to essentialy the same Galois group, up to the algebraical closedness of the constants.

In [1], a general notion of a Picard-Vessiot extension associated to module with a connection is introduced. We start the section by stating this definition, and verifying that the notion of a Picard-Vessiot extension defined in [3] is a particular case of it. In the next two subsections, we first verify that our model-theoretical tools fit in the context of [1], and finally state and prove the theorem of comparison of the several notions of Galois groups.

We consider a generalized differential ring A, and a module M with a connection ∇ over A. We denote by $\omega_{A'}$ the functor associating to a module N in the Tannakian category generated by M over A' the module $Ker(\nabla, N)$, and we denote by $< .,. >$ the evaluation map from $M^* \times M$ to A.

Definition 4.1 ([1], definition III.4.1.1) An extension A' of A is called a *Picard-Vessiot extension for M* if:

- A', as a pure ring, is faithfully flat over A;
- A' is simple as a generalized differential ring (that is, has no nontrivial d-invariant ideal);

- the constants $C_{A'}$ of A' are the constants C_A of A;
- the connection on M is trivial when extended to A';
- A', as an A-algebra, is generated by the elements of $< M^*, \omega_{A'}(M) >$ and $< M, \omega_{A'}(M^*) >$.

We will compare this definition with the definition of a Picard-Vessiot extension in [11] (extended to generalized differential rings, instead of difference rings). For this definition, we need to consider an equation of the form $dX = BX$ for some $B \in GL_n(A)$. We recall that a *fundamental system of solutions* of this equation is a matrix $C \in GL_n(A')$ in some extension A' of A such that each column of C is a solution.

Definition 4.2 ([11], definition 1.5) Assume that A is a field. Then a *Picard-Vessiot extension* of the equation is an extension ring A' such that :

- A' is simple as a generalized differential ring;
- A' is generated by a fundamental system of solutions of the equation.

We will prove that a Picard-Vessiot extension of the equation in the sense of definition 4.2 is a Picard-Vessiot extension for the module M generated by a fundamental system of solutions in the sense of definition 4.1, provided that the constants of A are algebraically closed. We assume in the following that A' is a Picard-Vessiot extension in the sense of definition 4.2, and that C_A is algebraically closed.

Proposition 4.3 *If A is a generalized differential field with an algebraically closed field of constants, then any Picard-Vessiot extension of A for some equation over A (in the sense of definition 4.2) is a Picard-Vessiot extension for the module of solutions M (in the sense of definition 4.1).*

Proof First, we note that the simplicity condition appear in both definitions.

We then prove that A' is faithfully flat over A. Since A is a field, A' is an A-vector space, hence it is free, which implies that it is flat. By [2], proposition 1.9, we only need to prove that for every left A-module F, the canonical isomorphism $x \mapsto 1 \otimes x$ from F to $A' \otimes F$ is injective, which is obvious since A is a field and A' and F are A-vector spaces.

The fact that the connection on M is trivial when extended to A' comes from the fact that M is generated by a fundamental system of solutions. The connection on M describes the action of d on the solutions of the equation, hence it is trivial on $M \otimes A'$.

The condition that A' is generated as an A-algebra by $< M^*, \omega_{A'}(M) >$ and $< M, \omega_{A'}(M^*) >$, for the same reason as in the preceding paragraph, is satisfied because A' is generated by a fundamental system of solutions of the equation, since M is generated by such a system.

Finally, the fact that C_A is algebraically closed implies that $C_{A'}$ is equal to it, since $C_{A'}$ is necessarily a finite algebraic extension of C_A (theorem III.4.3.1 of [1]). This completes the proof.

□

4.1 Correspondence between fibre functors and Picard-Vessiot extensions

In [1], theorem III.4.2.3, it is proven that there is an equivalence between the category of the fibre functors on a neutral Tannakian category associated to an equation and the strong Picard-Vessiot extensions of this equation. This equivalence involves the construction of a Picard-Vessiot extension associated to a fibre functor (which we will not discuss here), and the construction of an isomorphism between two particular fibre functors; for this second part of the proof, we can use some of our Tannakian tools to recover this isomorphism.

We first fix a generalized differential field k with algebraically closed constant field, an equation over k, and a Picard-Vessiot extension R associated to this equation. We define the Galois group associated to it :

Definition 4.4 The *strong Galois group of* k is the group of automorphisms of R over k.

If $\mathbf{C}_M$ is a neutral Tannakian category with fibre functor ω, we construct a Picard-Vessiot extension R as it is done in [1], and consider the functor ω_k associated to it (that is, the functor associating to N the C_k-vector space $Ker(\nabla, N \otimes R)$). The aim is then to prove that ω and ω_k are isomorphic.

Note that by proposition 4.3 and lemma III.4.1.4 in [1], we know that ω_k is a fibre functor.

Under the assumptions of proposition 3.20, it is possible to prove the existence of an isomorphism between the groups of tensor automorphisms of the two fibre functors, using as above the proposition 3.4: the group $Aut^{\otimes}(\omega)$ is a subgroup of $Aut^{\otimes}(\omega_k)$, and the latter fixes every torsor for the former since such a torsor is coded by an element of a projective space, which corresponds to a representation of $Aut^{\otimes}(\omega)$; this representation becomes a representation of $Aut^{\otimes}(\omega_k)$ by tensoring by R, and so is fixed by the latter group; we conclude by using the lemma 1.6. This isomorphism gives an isomorphism between the two considered functors, which is what we are aiming at.

4.2 Identification of different Galois groups

In the paper [3], the authors describe, in the context of difference fields, several definitions of the Galois group associated to an equation; they prove that the different suggested definitions lead to the same Galois group, up to an extension of the constants to the algebraic closure of the constants. They then use Tannakian ideas to reprove this statement in a particular case (concerning the field of meromorphic functions over $\mathbb{C}$). Their arguments fit in the context of generalized differential rings and, supported by the model-theoretic techniques we presented above, yield a slight generalization of their theorem 2.9.

We start by recalling another definition of the Galois groups that we will try to compare with those introduced in section 4.1. This one is a Tannakian version, that is the binding group of the category generated by the module generated by a fundamental system of solutions of the considered equation. The one presented in section 4.1 is a more Galois-theoretic version, defined as the group of automorphisms of some generalized difference field fixing a given subfield. For a discussion about the motivation for both of them, we refer to [3].

Following the terminology of [3], we define another notion of Picard-Vessiot extensions to which we will associate their Galois groups:

Definition 4.5 ([3], definition 2.1) We call *weak Picard-Vessiot ring of the equation* over k a ring R extending k such that:

- $C_R = C_k$, and
- $R = k[Z, \det(Z)^{-1}]$ for a $Z \in GL_n(R)$ whose columns are solutions of the equation.

If R is the quotient field of such a ring, still with the same constants as k, then R is called a *weak Picard-Vessiot field of the equation*. The *weak Galois group* of k is defined to be the group of automorphisms of R over k when R is a weak Picard-Vessiot field.

We will try to compare these two Galois groups by realizing them as binding groups of a particular Tannakian category. One of them will be a subgroup of the other, and a reasoning as in the preceding section will allow us to identify them in some situations. We assume in all of the following that the constants C_k of k are algebraically closed.

Given a finitely generated module with a connection M over k, call $\mathbf{C}_M$ the category generated by M using the direct sum, the dualization, the subquotienting and the tensor product. If K is a field extension of k, then call M_K the module $M \otimes_k K$, and $\mathbf{C}_{M_K}$ the corresponding category. We will define a fibre functor associated to each of these categories, so that we will be able to build the binding group associated to it, and define them as the strong and weak Galois group of the equation, then proving equality of these groups when we extend the constants to their algebraic closure.

From now on, we assume that there exists a weak Picard-Vessiot extension field R of the equation, and a Picard-Vessiot extension R' of the extension (which has been proven to exist when $\mathbf{C}_M$ is Tannakian by [1], theorem III.4.2.3).

We define ω_K in the same way we defined ω_k in the previous section, with the notations above, and the same reasoning proves that it is also a fibre functor. Finally, both $\mathbf{C}_M$ and $\mathbf{C}_{M_K}$ endowed with these functors are neutral Tannakian categories, and we can build their binding groups G_M and G_{M_K}.

We now prove the following theorem:

Theorem 4.6 ([3], theorem 2.9) *The groups G_M and G_{M_K} are identified respectively with the group of the k-automorphisms of R, and the group of the K-automorphisms of R'. We have*

$$G_M \otimes \overline{C_K} = G_{M_K} \otimes \overline{C_K}$$

Proof To prove that the binding groups can be identified with the automorphisms groups of the different kinds of Picard-Vessiot extensions, we use theorem 3.2 in [5]: for any fibre functor η of $\mathbf{C}_M$ over k, the functor $N \mapsto Hom^{\otimes}(\omega_N, \eta_N)$ is representable by $Spec(R)$, and similarly for $\mathbf{C}_{M_K}$. Hence, each of the groups G_M and G_{M_K} can be identified with the corresponding group of automorphisms of the (weak) Picard-Vessiot extension.

To prove the equality between these groups over the algebraic closure of the constants, we first extend the functor ω_k to the category $\mathbf{C}_{M_K}$ by putting $\bar{\omega_k}(N) = ker(\delta, N \otimes_K (R \otimes_k K))$. We will first prove that $Aut^{\otimes}(\omega_k) \otimes C_K = Aut^{\otimes}(\bar{\omega_k})$. Since any tensor automorphism of $\bar{\omega_k}$ induces an automorphism of ω_k fixing the constants of K, we see immediately that $Aut^{\otimes}(\bar{\omega_k}) \subseteq Aut^{\otimes}(\omega_k) \otimes C_K$. Moreover, the group $Aut^{\otimes}(\bar{\omega_k})$ being a binding group, the proposition 3.17 implies that it is equal to an intersection of definable subgroups of $Aut^{\otimes}(\omega_k) \otimes C_K$. We will prove that each of them is equal to $Aut^{\otimes}(\omega_k) \otimes C_K$, which will prove the desired equality. Let G be one of these definable subgroups.

We can now use the same reasoning as in theorem 3.18 to prove equality between G and $Aut^{\otimes}(\omega_k) \otimes C_K$: if we consider a G-torsor, then by proposition 3.4, it is coded by an element of some projective space of an object in the category $\mathbf{C}_{M_K}$; this element corresponds to a subrepresentation of the group G over C_K, and is then fixed by the group $Aut^{\otimes}(\omega_k) \otimes C_K$. The lemma 1.6 then proves that the two groups are equal.

We will now prove that the group $Aut^{\otimes}(\bar{\omega_k})$ is equal to the group $G_{M_K} = Aut^{\otimes}(\omega_K)$ when we extend the constants to their algebraic closure. But ω_K and $\bar{\omega_k}$ are two fiber functors over C_K for the category $\mathbf{C}_{M_K}$. As in the proof of the theorem 3.1 of [3], we use the fact that these functors become isomorphic over the algebraic closure of the base field to say that the two groups, tensored by $\overline{C_K}$, are isomorphic. This concludes the proof of the theorem.

□

In particular, we know that the existence of the different Picard-Vessiot extensions considered here is ensured when we are in the situation of a difference field, or a differential field. The theorem above is then true in these situations, permitting in particular to recover the theorem 2.9 of [3].

Acknowledgements

The author would like to thank its supervisor Tuna Altınel for the large amount of time he devoted to this work, and for his help and discussions, and Meghan Anderson for bringing to its attention the article [1].

References

[1] Yves André, *Différentielles non-commutatives et théorie de Galois différentielle ou aux différences*, Annales Scientifiques de l'École Normale Supérieure, 4^{th} series, t. 34, 2001, pp. 685 to 739.

[2] N. Bourbaki, *Algèbre commutative*, Actualités Scientifiques et Industrielles, No. 1290, Herman, Paris, 1961.

[3] Zoé Chatzidakis, Charlotte Hardouin, and Michael Singer, *On the definitions of difference Galois groups*, http://arxiv.org/abs/0705.2975, 2007.

[4] Zoé Chatzidakis and Ehud Hrushovski, *Model Theory of Difference Fields*, Transactions of the American Mathematical Society, vol. 351, n. 8, 1999, pp. 2997 to 3071.

[5] Pierre Deligne and James S. Milne, "Tannakian categories", in *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, 1981, Volume 900, pp. 101-228.

[6] Ehud Hrushovski, *Groupoids, Imaginaries and Internal Covers*, http://arxiv.org/pdf/math/0603413, 2009.

[7] Moshe Kamensky, *Definable Groups of Partial Automorphisms*, Selecta Mathematica, New Series, vol. 15, 2009, pp. 295-341, www.nd.edu/~mkamensk/papers/defaut.pdf

[8] Moshe Kamensky, *Model Theory of Tannakian Categories*, unknown date, www.nd.edu/~mkamensk/lectures/tanakmod.pdf

[9] Hideyuki Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics, vol. 8 (2nd ed.), Cambridge University Press, Cambridge, 1989.

[10] Anand Pillay, *Geometric Stability Theory*, Oxford Logic guides, vol. 32, Oxford Science Publications, Oxford, 1996.

[11] Michael Singer and Marius van der Put, *Galois theory of difference equations*, Lecture Notes in Mathematics, Volume 1666, 1997.