Séminaires & Congrès

COLLECTION SMF

UNIPOTENT RADICALS OF TANNAKIAN GALOIS GROUPS IN POSITIVE CHARACTERISTIC

Charlotte Hardouin

ARITHMETIC AND GALOIS THEORY OF DIFFERENTIAL EQUATIONS

Numéro 23

Lucia Di Vizio, Tanguy Rivoal, eds.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Séminaires & Congrès
23, 2011, p. 283–299

UNIPOTENT RADICALS OF TANNAKIAN GALOIS GROUPS IN POSITIVE CHARACTERISTIC

by

Charlotte Hardouin

Abstract. — Let $\mathcal{T}$ be a Tannakian category over a field C of strictly positive characteristic. We show in this note how one can characterize the unipotent radical of the Tannakian Galois group of an object $\mathcal{U}$, extension of the unit object $\mathbf{1}$ by a completely reducible object $\mathcal{Y}$ in terms of the group $Ext^1(\mathbf{1},\mathcal{Y})$ of isomorphism classes of extension of $\mathbf{1}$ by $\mathcal{Y}$. We deduce from our Theorem that, under certain hypothesis, the Tannakian Galois group of a direct sum of extensions is entirely determined by the relations of linear dependence satisfied by these extensions in $Ext^1(\mathbf{1},\mathcal{Y})$. This corollary reduces the computation of an algebraic group to a question of linear algebra. As an application, we show how it gives an alternative proof of the algebraic independence of the Carlitz logarithms of M. Papanikolas ([14]).

Résumé **(Radicaux unipotents de groupes de Galois tannakiens en caractÃŕristique positive)**

Soit $\mathcal{T}$ une catégorie tannakienne sur un corps C de caractéristique strictement positive. Nous montrons dans cette note comment on peut ramener l'étude du radical unipotent d'un groupe de Galois tannakien d'un objet $\mathcal{U}$, extension de l'objet trivial $\mathbf{1}$ par un objet $\mathcal{Y}$ complétement réductible, à celle du groupe $Ext1(\mathbf{1},\mathcal{Y})$ des classes d'isomorphismes d'extensions de $\mathbf{1}$ par $\mathcal{Y}$. Nous déduisons de nôtre théorème que, sous certaines hypothèses, le groupe de Galois tannakien d'une somme directe d'extensions est entièrement déterminé par les relations de dépendance linéaire satisfaites par ces extensions dans $Ext1(\mathbf{1},\mathcal{Y})$. Ce corollaire ramène le calcul des relations algébriques définissant le groupe à une question d'algébre linéaire. Comme application, nous donnons une preuve alternative de l'indépendance algèbrique des logarithmes de Carlitz de M. Papanikolas ([14]).

Introduction

Computation of Tannakian Galois groups. — The theory of Tannakian categories gives a precise answer to the question: "when is a category equivalent to the category Rep_G of finite dimensional representations of an affine group scheme?" By definition, a Tannakian category $\mathcal{T}$ over a field C is a rigid abelian tensor category (see [7, §2.8]).

2000 Mathematics Subject Classification. — 18D10, 39A, 34M15.
Key words and phrases. — Tannakian categories, Unipotent radical, Galois groups, t-motives.

It is said to be neutral if there exists a functor $\omega : \mathcal{T} \to Vect_C$ from $\mathcal{T}$ into the category of finite dimensional C-vector spaces, called "fiber functor", that is C-linear, faithful, exact and tensor compatible (see [7, §1.9]). For instance, the category of differential modules over the differential field $(\mathbb{C}(x), \partial := \frac{d}{dx})$ is a Tannakian category (see [18, §2.2]). The choice of a basis of a differential module $\mathcal{M}$ yields to a differential system $\partial Y = AY$ with $A \in Gl_\nu(\mathbb{C}(x))$. Then, a basis of solutions of this last system provides a fiber functor for the full Tannakian sub-category generated by $\mathcal{M}$. The category of differential modules over a differential field of characteristic zero, the category of iterative differential modules over a field of positive characteristic (see [13]), the category of q-difference modules (see [19]), the category of Frobenius modules (see [12]), which includes isocrystals in the p-adic case and t-motives (see [14]) in the t-adic case are just other examples of Tannakian categories. The fundamental theorem for Tannakian categories is the following

***Theorem 1* (see Theorem 1.12 of [7]).** — *Let $\mathcal{T}$ be a neutral Tannakian category over a field C together with a fiber functor $\omega : \mathcal{T} \to Vect_C$. Then, the functor $Aut^{\otimes}(\omega)$ of tensor compatible automorphisms of ω is representable by an affine group scheme G defined over C and ω induces an equivalence of categories between $\mathcal{T}$ and the category Rep_G of finite dimensional representations of G.*

Then, the Galois group of an object $\mathcal{M}$ of a Tannakian category is defined as follows.

***Definition 1* (see Theorem 3.2.1.1 of [3]).** — *Let $(\mathcal{T}, \omega)$ be a neutral Tannakian category defined over a field C. We denote by $\langle \mathcal{M} \rangle^{\otimes}$ the full Tannakian sub-category generated by $\mathcal{M}$ in $\mathcal{T}$. Then,*

- *there exists an affine group scheme $G_{\mathcal{M}}$ defined over C, together with a closed immersion ι from $G_{\mathcal{M}}$ into $Gl(\omega(\mathcal{M}))$, such that $\omega_{|\mathcal{M}} : \langle \mathcal{M} \rangle^{\otimes} \to Vect_C$ induces a $\otimes$-tensor equivalence of categories between $\langle \mathcal{M} \rangle^{\otimes}$ and the category $Rep_{G_{\mathcal{M}}}$;*
- *the image of ι is the closed sub-group of $Gl(\omega(\mathcal{M}))$ which stabilizes all the sub-objects $\mathcal{N}$ contained in any finite sum $\bigoplus_{i,j}(\mathcal{M}^{\otimes i} \otimes (\mathcal{M}^*)^{\otimes j})$, where $\mathcal{M}^*$ denotes the dual of $\mathcal{M}$.*

We call $G_{\mathcal{M}}$ the Galois group of $\mathcal{M}$.

For a differential module $\mathcal{M}$ over $\mathbb{C}(x)$, the linear algebraic group $G_{\mathcal{M}}$ is defined over $\mathbb{C}$ and isomorphic to the differential Galois group attached to $\mathcal{M}$ by Picard-Vessiot constructions (see [18, Definition 1.25]). Its dimension over $\mathbb{C}$ is equal to the transcendence degree of the field generated over $\mathbb{C}(x)$ by a basis of solutions of a differential system attached to $\mathcal{M}$. In [3, Theorem 3.4.2.3], it is shown that, for an object $\mathcal{M}$ in a neutral Tannakian category of either differential or difference modules over C, there is a one to one correspondence between fiber functors over $\langle \mathcal{M} \rangle^{\otimes}$, Picard-Vessiot extensions of $\mathcal{M}$ (roughly, C-algebras generated by a basis of solution of $\mathcal{M}$ plus some minimality conditions) and $G_{\mathcal{M}}$-torsors. Specifically, this implies that the algebraic relations between the solutions of $\mathcal{M}$ are controlled by the

Galois group of $\mathcal{M}$. The Tannakian categories are thus strongly related to questions of functional transcendence and the computation of Tannakian Galois groups is a powerful tool since it reduces these questions to the computation of a linear algebraic group.

There exist some algorithms to compute Galois groups of Tannakian objects but they are, most of the time, specific to the Tannakian category considered. For instance, in [10], E. Hrushovski proves that one can compute the Galois group of a linear differential equation over $\overline{Q}(x)$. In the first part of this note, we present some theorems of computation for Tannakian Galois groups, which generalize those mentioned in [16]. Even if they requires some technical hypothesis, these theorems are valid for any Tannakian category in positive characteristic and they may thus apply, for instance, as well for iterative differential equations as for Frobenius difference equations.

We detail below the results of the first section of this note. Let C be a field and let $(\mathcal{T}, \omega)$ be a neutral Tannakian category over C. Let $\mathbf{1}$ be the unit object for the tensor product. Let $\mathcal{Y}$ be a completely reducible object of $\mathcal{T}$, *i.e.* $\mathcal{Y}$ is a direct sum of finitely many irreducible objects. We say that $\mathcal{U}$, an object of $\mathcal{T}$, is an extension of $\mathbf{1}$ by $\mathcal{Y}$ if there exists an exact sequence in $\mathcal{T}$ such that

$$0 \to \mathcal{Y} \to \mathcal{U} \to \mathbf{1} \to 0.$$

To consider extensions of $\mathbf{1}$ by $\mathcal{Y}$ is a way to build "logarithms of the solutions" of $\mathcal{Y}$. For instance, if $\mathcal{Y}$ is a differential module over $(\mathbb{C}(x), \frac{d}{dx})$ associated to the differential system $\frac{d}{dx}Y(x) = A(x)Y(x)$ with $A(x) \in Gl_\nu(\mathbb{C}(x))$, then an extension of $\mathbf{1}$ by $\mathcal{Y}$ corresponds to a differential system of the form $\frac{d}{dx}Z(x) = A(x)Z(x) + B(x)$ with $B(x) \in (\mathbb{C}(x))^\nu$.

Using Levi decomposition, we see that the Galois group $G_\mathcal{Y}$ of an extension $\mathcal{U}$ of $\mathbf{1}$ by $\mathcal{Y}$ a completely reducible object, may be written as the semi-direct product $G_\mathcal{U} = R_u(G_\mathcal{U}) \rtimes G_\mathcal{Y}$ where $R_u(G_\mathcal{U})$ stands for the unipotent radical of $G_\mathcal{U}$. Then, if we assume that $G_\mathcal{Y}$ is given, the computation of $G_\mathcal{U}$ is reduced to the computation of the unipotent radical of $G_\mathcal{U}$. If the characteristic of C is equal to zero, it is proved in [9, Theorem 2.1] that the unipotent radical of $G_\mathcal{U}$ is isomorphic to a vectorial subgroup of the fiber $\omega(\mathcal{Y})$, entirely determined by the structure of $Ext^1(\mathbf{1}, \mathcal{Y})$, the group of isomorphism classes of extensions of $\mathbf{1}$ by $\mathcal{Y}$ in $\mathbf{T}$. The proof extends and follows closely the kummerian arguments of [5] and [4]. If the characteristic of C is strictly positive, one has to be more careful ; first of all, it may happen that the Galois groups are not reduced and, secondly, the image of a vectorial group by a group morphism is not necessarily a vectorial group. Then, if $\mathbf{G}_m$ denotes the multiplicative group over C, we have

Theorem 2. — *Let $\mathcal{Y}$ be an object of $\mathbf{T}$, and let $\mathcal{U}$ be an extension of $\mathbf{1}$ by $\mathcal{Y}$. Assume that*

1. *every $G_\mathcal{Y}$-module is completely reducible,*
2. *the center of $G_\mathcal{Y}$ contains $\mathbf{G}_m$,*

3. *the action of* $\mathbf{G}_m$ *on* $\omega(\mathcal{Y})$ *is isotypic* [(1)]*,*
4. $G_{\mathcal{U}}$ *is reduced.*

Then, there exists a smallest sub-object $\mathcal{V}$ *of* $\mathcal{Y}$ *such that* $\mathcal{U}/\mathcal{V}$ *is a trivial extension of* $\mathbf{1}$ *by* $\mathcal{Y}/\mathcal{V}$*. The unipotent radical of the Galois group* $G_{\mathcal{U}}$ *is then equal to* $\omega(\mathcal{V})$*.*

First of all, we just want to emphasize the fact that every diagonal C-group scheme satisfy the first hypothesis (see [11, p.35]). Secondly, the third hypothesis may be removed if one thinks in terms of weights of the characters of $\mathbf{G}_m$ acting on each isotypical components of $\omega(Y)$. But, for simplicity of exposition, we assume that the action of $\mathbf{G}_m$ is isotypic, *i.e.* involves one single character. As a corollary of Theorem 2, we show

Corollary 1. — *Let* $\mathcal{Y}$ *be an object of* $\mathbf{T}$*. Let* Δ *be the ring* $End(\mathcal{Y})$*, and let* $\mathcal{E}_1, ..., \mathcal{E}_n$ *be extensions of* $\mathbf{1}$ *by* $\mathcal{Y}$*. Assume that*

1. *every* $G_{\mathcal{Y}}$*-module is completely reducible,*
2. *the center of* $G_{\mathcal{Y}}$ *contains* $\mathbf{G}_m$*,*
3. *the action of* $\mathbf{G}_m$ *on* $\omega(\mathcal{Y})$ *is isotypic,*
4. $G_{\mathcal{E}_1}, ..., G_{\mathcal{E}_n}$ *are reduced.*

Then, if $\mathcal{E}_1, ..., \mathcal{E}_n$ *are* Δ*-linearly independent in* $Ext^1(\mathbf{1}, \mathcal{Y})$*, the unipotent radical of* $G_{\mathcal{E}_1 \oplus ... \oplus \mathcal{E}_n}$ *is isomorphic to* $\omega(\mathcal{Y})^n$*.*

The meaning of this corollary is the following. Algebraic relations between the extensions occur if and only if the group $G_{\mathcal{E}_1 \oplus ... \oplus \mathcal{E}_n}$ is not as big as possible, i.e. , if and only if its unipotent radical is strictly contained in $\omega(\mathcal{Y})^n$. Corollary 1 then states that algebraic relations are exactly given by the relations of linear dependence. As for Theorem 2, this corollary holds in characteristic zero (see [9, Cor. 2.2]). Even if, in full generality, the criteria of linear dependency of the extensions shall seem rather complicated, it reduces most of the time, to a question of existence of a rational solution of a given equation.

An application to the transcendency of periods of Drinfeld module. — In the second section, we show how the computation theorems of the first section may apply to the Tannakian category of t-motives defined by M. Papanikolas in [14] and thus to the study of the transcendence properties of some periods of Drinfeld modules.

Let $\mathbf{F}_q$ be the field of q elements, where q is a power of a prime p. Let $k := \mathbf{F}_q(\theta)$, where θ is transcendental over $\mathbf{F}_q$. Define a valuation $|.|_\infty$ at the infinite place of k such that $|\theta|_\infty = q$. Let $k_\infty := \mathbf{F}_q((1/\theta))$ be the ∞-adic completion of k, let $\overline{k_\infty}$ be an algebraic closure of k_∞, let $\mathbf{K}$ be the ∞-adic completion of $\overline{k_\infty}$, and let $\overline{k}$ be the algebraic closure of k in $\mathbf{K}$. One call "numbers " the elements of $\mathbf{K}$. A number which is not in $\overline{k}$ is a transcendent number. Let $\mathbf{K}[\tau]$ be the twisted polynomial ring in τ over $\mathbf{K}$ subject to the relation $\tau c = c^q \tau$ for all $c \in \mathbf{K}$. Now, let t be an

(1) We recall that the action of a group G on a module V is isotypic if the module V is the direct sum of irreducible isomorphic G-modules.