Séminaires & Congrès

COLLECTION SMF

ON THE FINITE INVERSE PROBLEM IN ITERATIVE DIFFERENTIAL GALOIS THEORY

Andreas Maurischat

THÉORIES DE GALOIS GÉOMÉTRIQUE ET DIFFÉRENTIELLE

Numéro 27 D. Bertrand, P. Boalch, J.-M. Couveignes, P. Dèbes, éds.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Séminaires & Congrès
27, 2012, p. 181–189

ON THE FINITE INVERSE PROBLEM IN ITERATIVE DIFFERENTIAL GALOIS THEORY

by

Andreas Maurischat

Abstract. — In positive characteristic, nearly all Picard-Vessiot extensions are inseparable over some intermediate iterative differential extensions. In the Galois correspondence, these intermediate fields correspond to nonreduced subgroup schemes of the Galois group scheme. Moreover, the Galois group scheme itself may be nonreduced, or even infinitesimal. In this article, we investigate which finite group schemes occur as iterative differential Galois group schemes over a given ID-field. For a large class of ID-fields, we give a description of all occuring finite group schemes.

***Résumé* (Sur le problème inverse fini en théorie de Galois des équations différentielles itérées)**

En caractéristique positive, presque toutes les extensions de Picard-Vessiot sont inséparables sur certaines extensions différentielles itérées intermédiaires. Dans la correspondance de Galois, ces extensions intermédiaires correspondent à des sous-schémas en groupes non réduits du schéma en groupes de Galois. De plus, le schéma en groupes de Galois n'est lui-même pas forcément réduit, et peut même être infinitésimal. Dans cet article, nous recherchons quels schémas en groupes finis peuvent apparaître comme schémas en groupes de Galois d'équations différentielles itérées sur un corps aux dérivées itérées donné. Pour une grande classe de tels corps, nous donnons une description de tous les schémas en groupes finis qui apparaissent effectivement.

1. Introduction

Picard-Vessiot theory for iterative differential extensions in positive characteristic as conceived by Matzat and van der Put in [4] was restricted to separable extensions and algebraically closed fields of constants. This restriction was necessary, since the Galois group was given as (the rational points of) a linear algebraic group. Furthermore, intermediate fields over which the Picard-Vessiot ring is inseparable are not

2010 Mathematics Subject Classification. — 12H20, 12F15.
Key words and phrases. — Differential Galois theory, inseparable extensions, finite group schemes.

taken into account in their Galois correspondence. In [5], the Picard-Vessiot theory was extended to perfect fields of constants and to inseparable extensions. This was made possible by constructing the Galois group as an affine group scheme. In the case of a separable PV-extension over an algebraically closed field of constants C, the C-rational points of this group scheme are exactly the original Galois group as defined by Matzat and van der Put.

In this article, we solve the inverse problem for finite group schemes in iterative Picard-Vessiot theory. That is, we give necessary and sufficient conditions for a finite group scheme to be a Galois group scheme over a given ID-field F. The general result which still depends on the inverse problem in classical Galois theory over F is given in Theorem 5.1. In the case where F itself is a PV-extension of an algebraic function field over algebraically closed constants, this classical inverse problem is solved. Therefore, in that case, we can explicitly describe the occuring Galois group schemes (cf. Corollary 5.2).

This article is structured as follows. In Section 2, we describe the notation and results regarding Picard-Vessiot theory in positive characteristic which are required later. Section 3 is dedicated to the case of infinitesimal Galois group schemes (i.e. purely inseparable PV-extensions), whereas results for finite reduced Galois group schemes are given in Section 4. Results from both sections are used in Section 5 to solve the inverse problem for finite group schemes.

Acknowledgements. I thank B. H. Matzat for drawing my attention to the inverse problem for nonreduced group schemes. I also thank E. Dufresne for helpful comments to improve this paper.

2. Basic notation

All rings are assumed to be commutative with unit. We will use the following notation (see also [6]). An iterative derivation on a ring R is a homomorphism of rings $\theta : R \to R[[T]]$, such that $\theta^{(0)} = \mathrm{id}_R$ and for all $i, j \geq 0$, $\theta^{(i)} \circ \theta^{(j)} = \binom{i+j}{i}\theta^{(i+j)}$, where the maps $\theta^{(i)} : R \to R$ are defined by $\theta(r) =: \sum_{i=0}^{\infty} \theta^{(i)}(r)T^i$. The pair (R, θ) is then called an ID-ring and $C_R := \{r \in R \mid \theta(r) = r\}$ is called the **ring of constants** of (R, θ). An iterative derivation θ resp. the ID-ring (R, θ) is called **nontrivial**, if $C_R \neq R$. An ideal $I \trianglelefteq R$ is called an **ID-ideal** if $\theta(I) \subseteq I[[T]]$ and R is **ID-simple** if R has no proper nontrivial ID-ideals. An ID-ring which is a field is called an **ID-field**. Iterative derivations are extended to localisations by $\theta(\frac{r}{s}) := \theta(r)\theta(s)^{-1}$ and to tensor products by

$$\theta^{(k)}(r \otimes s) = \sum_{i+j=k} \theta^{(i)}(r) \otimes \theta^{(j)}(s)$$

for all $k \geq 0$.

If R is an integral domain of positive characteristic p, the iterative derivation induces a family of ID-subrings given by

$$R_\ell := \bigcap_{0<j<p^\ell} \mathrm{Ker}(\theta^{(j)}),$$

($\ell \in \mathbb{N}$) and also a family of ID-overrings $R_{[\ell]} := (R_\ell)^{p^{-\ell}}$ ($\ell \in \mathbb{N}$) in some inseparable closure with iterative derivation given by

$$\theta_{R_{[\ell]}}(x) := \left(\theta_R(x^{p^\ell})\right)^{p^{-\ell}}.$$

Notation *From now on, (F,θ) denotes an ID-field of positive characteristic p, and $C = C_F$ its field of constants. We assume that C is a perfect field, and that θ is* non-degenerate*, i. e., that $\theta^{(1)} \neq 0$.*

Remark 2.1. — In this setting, F_ℓ is an ID-subfield with $C_{F_\ell} = C$, and since $\theta^{(p^\ell)}$ is a nilpotent $F_{\ell+1}$-linear endomorphism of F_ℓ and $\theta^{(p^\ell)}$ is of nilpotence order p with 1-dimensional kernel, one has $[F_\ell : F_{\ell+1}] = p$. Therefore, one obtains $[F : F_\ell] = p^\ell$ for all ℓ.

Furthermore, $F_{[\ell]}$ is an ID-extension of F with same constants (since C is perfect), and $[F_{[\ell]} : F] = p^{\ell(m-1)}$, where m denotes the degree of imperfection of F (possibly infinite).

In [6], Prop. 4.1, it is shown that $F_{[\ell]}/F$ is the maximal purely inseparable ID-extension of F of exponent $\leq \ell$.

We now recall some definitions from Picard-Vessiot theory:

Definition 2.2. — Let $A = \sum_{k=0}^{\infty} A_k T^k \in \mathrm{GL}_n(F[[T]])$ be a matrix with $A_0 = \mathbb{1}_n$ and for all $k, l \in \mathbb{N}$, $\binom{k+l}{l} A_{k+l} = \sum_{i+j=l} \theta^{(i)}(A_k) \cdot A_j$. An equation

$$\theta(\boldsymbol{y}) = A\boldsymbol{y},$$

where $\boldsymbol{y}$ is a vector of indeterminants, is called an **iterative differential equation (IDE)**.

Remark 2.3. — The condition on the A_k is equivalent to the condition that

$$\theta^{(k)}(\theta^{(l)}(Y_{ij})) = \binom{k+l}{k} \theta^{(k+l)}(Y_{ij})$$

holds for a matrix $Y = (Y_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(E)$ satisfying $\theta(Y) = AY$, where E is some ID-extension of F. (Such a Y is called a **fundamental solution matrix**) . The condition $A_0 = \mathbb{1}_n$ is equivalent to $\theta^{(0)}(Y_{ij}) = Y_{ij}$, and already implies that the matrix A is invertible.

Definition 2.4. — An ID-ring $(R, \theta_R) \geq (F, \theta)$ is called a **Picard-Vessiot ring** (PV-ring) for the IDE $\theta(\boldsymbol{y}) = A\boldsymbol{y}$, if the following holds:

1. R is an ID-simple ring.

2. There is a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$, i. e., an invertible matrix satisfying $\theta(Y) = AY$.
3. As an F-algebra, R is generated by the coefficients of Y and by $\det(Y)^{-1}$.
4. $C_R = C_F = C$.

The quotient field $E = \mathrm{Quot}(R)$ (which exists, since such a PV-ring is always an integral domain) is called a **Picard-Vessiot field** (PV-field) for the IDE $\theta(\boldsymbol{y}) = A\boldsymbol{y}$.[(1)]

For a PV-ring R/F one defines the functor

$$\underline{\mathrm{Aut}}^{ID}(R/F) : (\mathsf{Algebras}/C) \to (\mathsf{Groups}), D \mapsto \mathrm{Aut}^{ID}(R \otimes_C D/F \otimes_C D)$$

where D is equipped with the trivial iterative derivation. In [5], Sect. 10, it is shown that this functor is representable by a C-algebra of finite type, and hence, is an affine group scheme of finite type over C. This group scheme is called the (iterative differential) **Galois group scheme** of the extension R over F – denoted by $\underline{\mathrm{Gal}}(R/F)$ –, or also, the Galois group scheme of the extension E over F, $\underline{\mathrm{Gal}}(E/F)$, where $E = \mathrm{Quot}(R)$ is the corresponding PV-field.

Furthermore, $\mathrm{Spec}(R)$ is a $(\underline{\mathrm{Gal}}(R/F) \times_C F)$-torsor and the corresponding isomorphism of rings

$$\gamma : R \otimes_F R \to R \otimes_C C[\underline{\mathrm{Gal}}(R/F)] \tag{1}$$

is an R-linear ID-isomorphism. Again, $C[\underline{\mathrm{Gal}}(R/F)]$ is equipped with the trivial iterative derivation.

This torsor isomorphism (1) is the key tool to establish the Galois correspondence between the closed subgroup schemes of $\mathcal{G} = \underline{\mathrm{Gal}}(R/F)$ and the intermediate ID-fields of the extension E/F, in more detail:

Theorem 2.5. — **(Galois correspondence)** *Let E/F be a PV-extension with PV-ring R and Galois group scheme $\mathcal{G}$.*

Then there is an inclusion reversing bijection between

$$\mathfrak{H} := \{\mathcal{H} \mid \mathcal{H} \leq \mathcal{G} \text{ closed subgroup scheme of } \mathcal{G}\}$$

and

$$\mathfrak{M} := \{M \mid F \leq M \leq E \text{ intermediate ID-field}\}$$

given by $\Psi : \mathfrak{H} \to \mathfrak{M}, \mathcal{H} \mapsto E^{\mathcal{H}}$ and $\Phi : \mathfrak{M} \to \mathfrak{H}, M \mapsto \underline{\mathrm{Gal}}(E/M)$.
With respect to this bijection, $\mathcal{H} \in \mathfrak{H}$ is a normal subgroup of $\mathcal{G}$, if and only if $E^{\mathcal{H}}$ is a PV-field over F. In this case the Galois group scheme $\underline{\mathrm{Gal}}(E^{\mathcal{H}}/F)$ is isomorphic to $\mathcal{G}/\mathcal{H}$.

(1) The PV-rings and PV-fields defined here were called pseudo Picard-Vessiot rings (resp. pseudo Picard-Vessiot fields) in [5] and [6]. This definition, however, is the most natural generalisation of the original definition of PV-rings and PV-fields to non algebraically closed fields of constants.