INTRODUCTION TO GALOIS THEORY OF ARTINIAN SIMPLE MODULE ALGEBRAS

by

Florian Heiderich

Abstract. — We give an introduction to a Galois theory of Artinian simple module algebras. To this end, we first recall the Picard-Vessiot theories of differential and difference equations, Umemura's differential Galois theory and Morikawa-Umemura's difference Galois theory. Then we sketch the main ideas of Amano and Masuoka's unification of the Picard-Vessiot theories of differential and difference extensions. We show how the differential Galois theory of Umemura and the difference Galois theory of Morikawa-Umemura can be unified using Artinian simple module algebras in lieu of differential or difference fields, respectively, and remove the restriction to fields of characteristic 0. Finally, we compare this unified theory to the Picard-Vessiot theory of Amano and Masuoka in the case of Picard-Vessiot extensions of Artinian simple module algebras.

Résumé **(Introduction au théorie de Galois des algèbres de modules artiniennes simples)**
Nous donnons une introduction à une théorie de Galois des algèbres de modules artiniennes simples. À cet effet, nous rappelons tout d'abord les théories de Picard-Vessiot des équations différentielles ou aux différences, ainsi que la théorie de Galois différentielle d'Umemura et la théorie de Galois aux différences de Morikawa-Umemura. Nous esquissons ensuite les idées principales de l'unification, due à Amano et Masuoka, des théories de Picard-Vessiot des équations différentielles ou aux différences. Nous montrons alors comment la théorie de Galois différentielle d'Umemura et la théorie de Galois aux différences de Morikawa-Umemura peuvent être unifiées en utilisant les algèbres de modules artiniennes simples à la place, respectivement, des corps différentiels ou aux différences ; de plus, nous supprimons la restriction aux corps de caractéristique nulle. Nous comparons enfin cette théorie unifiée à la théorie de Picard-Vessiot d'Amano et Masuoka, dans le cas des extensions de Picard-Vessiot d'algèbres de modules artiniennes simples.

2000 ***Mathematics Subject Classification.*** — 12H05, 12H10, 13B05, 16T10, 34M15.
Key words and phrases. — Galois theory, module algebra.

The author thanks La Fondation Sciences Mathématiques de Paris for financial support. He was also partially supported by the Spanish grant MTM2009-07024.

Introduction

It was already an aim of Lie to develop a theory analogous to Galois Theory, but for differential equations instead of polynomial equations in one variable. About 100 years ago this goal was achieved for linear differential equations and in honor of its inventors this theory is called Picard-Vessiot theory today. In the middle of the last century Ritt and Kolchin supplied the foundation of this theory: differential algebra. A modern approach to Picard-Vessiot theory of differential equations is provided in [**vdPS03**]. Hasse and Schmidt introduced iterative derivations as a replacement for derivations when working with fields of arbitrary characteristic (cf. [**HS37**]) and using them Okugawa as well as Matzat and van der Put developed a Galois theory of linear differential equations in positive characteristic (cf. [**Oku87**], [**MvdP03**]).

With a delay in time a similar theory was developed for linear difference equations, which is nowadays called Picard-Vessiot theory of difference equations (cf. [**vdPS97**]).

Takeuchi gave a presentation of Picard-Vessiot theory that unifies derivations (for rings including $\mathbb{Q}$) and iterative derivations using so called C-ferential fields, where C is a coalgebra (cf. [**Tak89**]). Inspired by this work, Amano and Masuoka pursued the unification process and developed a theory that not only captures differential fields in characteristic zero and iterative differential fields in arbitrary characteristic, but also inversive difference fields (and more generally direct products of fields together with an automorphism), cf. [**AM05**]. Instead of C-ferential fields, they use D-module algebras, where D is a certain Hopf algebra. Depending on the choice of D one obtains algebras with extra structures, among them derivations, iterative derivations and automorphisms.

Umemura developed a Galois theory for algebraic differential equations (cf. [**Ume96**]) and together with Morikawa he realized an analogous theory for difference equations and applied it to study discrete dynamical systems on algebraic varieties (cf. [**Mor09**], [**MU09**]).

The aim of this survey article is to provide a summary of the above mentioned theories, to show how the theories of Umemura and Morikawa-Umemura can be unified in a similar way as it was done by Amano, Masuoka and Takeuchi in the linear case and how one can overcome the restriction to characteristic zero in the theories of Umemura and Morikawa-Umemura.

In the first part, we recall the Picard-Vessiot theories of differential and difference equations and the theories of Umemura and Morikawa-Umemura for non-linear differential and difference equations, respectively. The second part begins with section 3, where we recall the definition and some results concerning D-module algebras. Section 4 recalls briefly the Picard-Vessiot theory of Amano and Masuoka. In section 5 we show how the theories of Umemura and Morikawa-Umemura can be unified. This unification is described in detail in [**Hei10**]. Additionally, we show that the restriction to extensions of difference fields in the theory of Morikawa-Umemura is not necessary.

Instead, we show how to develop the theory for a certain class of extensions of Artinian simple D-module algebras, where D is a certain bialgebra (cf. also [**Hei**]). By using iterative derivations instead of derivations we also eliminate the restriction to characteristic 0 from the theories of Umemura and Morikawa-Umemura. In the last section we show how this unified theory is related to the Picard-Vessiot theory of Amano and Masuoka by comparing the Umemura functor that we define and the Galois group scheme defined by Amano and Masuoka for Picard-Vessiot extensions.

In [**MU09**] the authors rise the question about the possibility to generalize their results to fields of arbitrary characteristic. We hope that the theory presented here could serve as a framework to tackle these questions.

The proofs for results of sections 5 and 6 that are not provided here can be found in [**Hei10**] and [**Hei**].

Notation. — We assume all rings and algebras to be unital and associative, but not necessarily to be commutative. Homomorphisms of algebras are assumed to preserve the units. We further assume that all coalgebras are counital and coassociative, but not necessarily to be cocommutative. Homomorphisms of coalgebras are assumed to preserve the counits.

If R is a commutative ring, then we denote by $\mathrm{Q}(R)$ the total quotient ring of R, by $\Omega(R)$ the set of minimal prime ideals of R, by $N(R)$ the nilradical of R, i.e. the ideal consisting of all elements $a \in R$ such that there exists a natural number $n > 0$ with $a^n = 0$, and $\pi_R \colon R \to R/N(R)$ denotes the canonical projection. We denote the category of (left) R-modules by ${}_R\mathcal{M}$, and by CAlg_R the category of commutative algebras over R; furthermore we denote by Grp the category of groups.

If $f \colon R \to S$ is a homomorphism of commutative rings and $\boldsymbol{w} = (w_1, \dots, w_n)$ are algebraically independed elements over S, then $f[\![\boldsymbol{w}]\!] \colon R[\![\boldsymbol{w}]\!] \to S[\![\boldsymbol{w}]\!]$ denotes the homomorphism defined by $f[\![\boldsymbol{w}]\!](\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}}\boldsymbol{w}^{\boldsymbol{k}}) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} f(a_{\boldsymbol{k}})\boldsymbol{w}^{\boldsymbol{k}}$.

If C is a category and A and B are objects in C, then we denote the class of morphisms from A to B in C by $\mathsf{C}(A, B)$.

The category of sets is denoted by Set. If A and B are sets and $a \in A$, then we denote by $\mathrm{ev}_a \colon \mathsf{Set}(A, B) \to B$ the evaluation map, i.e. $\mathrm{ev}_a(f) = f(a)$ for all $f \in \mathsf{Set}(A, B)$. We denote by $M_n(A)$ the set of $n \times n$-matrices with coefficients in A and for elements $a, b \in A$ we denote by $\delta_{a,b}$ the Kronecker delta, i.e. $\delta_{a,a} = 1$ and $\delta_{a,b} = 0$ if $a \neq b$.

PART I
DIFFERENTIAL- AND DIFFERENCE GALOIS THEORIES

1. Differential Galois theory

1.1. Galois theory of linear differential equations. — A contemporary exposition of the Galois theory of linear differential equations in characteristic 0 can be found in [**vdPS03**]. The basic object (replacing the field in Galois theory of polynomial equations) is a differential field, i.e. a field together with a derivation on it. Let (K, ∂_K) is a differential field containing $\mathbb{Q}$ and $A \in M_n(K)$ a matrix with coefficients in K. We consider the system of linear differential equations

$$\partial(\boldsymbol{y}) = A\boldsymbol{y}. \tag{1.1}$$

If (L, ∂_L) is a differential extension field of (K, ∂_K), then the *solution space* $\{\boldsymbol{y} \in L^n \mid \partial_L(\boldsymbol{y}) = A\boldsymbol{y}\}$ of (1.1) is a vector space of dimension at most n over the *field of constants*

$$L^{\partial_L} := \{a \in L \mid \partial_L(a) = 0\}.$$

There is a construction analogous to the splitting field of a polynomial:

Proposition 1.1. — *If the field of constants of (K, ∂_K) is algebraically closed and $A \in M_n(A)$, then there is a differential extension field (L, ∂_L) over (K, ∂_K) such that*

(1) the constant field of L is equal to the constant field of K,

(2) there exists a matrix $Y \in \mathrm{GL}_n(L)$ such that $\partial_L(Y) = AY$ and

(3) L is generated as a field over K by the coefficients of Y.

The differential field L with this properties is unique up to differential isomorphism.

This differential extension field (L, ∂_L) of (K, ∂_K) is called a *Picard-Vessiot field* for the equation (1.1) over K and the extension $L|K$ is called a *Picard-Vessiot extension.*

Proposition 1.2. — *For every Picard-Vessiot extension $L|K$ of differential fields, there exists an intermediate differential ring (R, ∂_R) with the following properties:*

(1) (R, ∂_R) is a simple differential ring, i.e. it has no non-trivial differential ideals,

(2) there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$ such that $\partial_R(Y) = AY$ and

(3) the K-algebra R is generated by the coefficients of Y and Y^{-1}.

The differential ring R is called the *Picard-Vessiot ring* of the equation (1.1). The *differential Galois group* of the extension $L|K$ is defined as the group functor $\mathrm{Gal}(L|K)$ on the category of commutative K^{∂_K}-algebras such that for every commutative K^{∂_K}-algebra A its A-points are given as the group of differential automorphisms of $R \otimes_{K^{\partial_K}} A$ that leave $K \otimes_{K^{\partial_K}} A$ fixed, where the derivation ∂_R is extended trivially to the right factor of the tensor product $R \otimes_{K^{\partial_K}} A$. It is an affine group scheme over K^{∂_K} with coordinate ring $(R \otimes_K R)^{\partial}$, where ∂ is the derivation induced by the derivation ∂_R on the factors to the tensor product.

In [**vdPS03**, Appendix D] an analogue of this theory for linear partial differential equations of the form $\partial_i(\boldsymbol{y}) = A_i\boldsymbol{y}$ with derivations ∂_i and matrices $A_i \in M_n(K)$ is sketched. This theory is developed in [**Hei07**], also for iterative linear partial differential equations.

1.2. Umemura's Galois theory of non-linear differential equations. — Umemura developed a differential Galois theory, which is aimed at the study of non-linear algebraic differential equations over differential fields of characteristic zero (cf. [**Ume96**]). Starting with an extension of differential fields $L|K$ of characteristic 0 such that L is finitely generated as field over K, he constructs a new extension of partial differential algebras $\mathcal{L}|\mathcal{K}$ and associates to it a group functor on the category of commutative L-algebras whose points turn out to be a group of infinitesimal transformations fulfilling certain partial differential equations, which he calls *infinitesimal Galois group*. In honor of its inventor we will call it the *Umemura functor*. We shortly recall this procedure and the definitions of the objects involved. We do not completely stick to the original definitions in [**Ume96**]. Instead, we incorporate some adaptions, which appeared in [**Ume06**].

Let $L|K$ be an extension of differential fields of characteristic 0 with derivation ∂ that is finitely generated as an extension of abstract fields. We chose a transcendence basis $u_1, \dots, u_n$ of $L|K$ and denote by $\partial_{u_1}, \dots, \partial_{u_n}$ the family of K-derivations on L defined by $\partial_{u_i}(u_j) = \delta_{i,j}$ for $i, j \in \{1, \dots, n\}$; this indeed defines uniquely K-derivations on L, since L is finite separable over $K(u_1, \dots, u_n)$. We extend the derivations ∂_{u_i} to the formal power series ring $L[\![t]\!]$ by their action on the coefficients of formal power series, i.e. for $\sum_{l\in\mathbb{N}} a_l t^l \in L[\![t]\!]$ we define

$$\partial_{u_i}(\sum_{l\in\mathbb{N}} a_l t^l) := \sum_{l\in\mathbb{N}} \partial_{u_i}(a_l) t^l.$$

On $L[\![t]\!]$ there is also the derivation ∂_t with respect to t, which is defined by

$$\partial_t(\sum_{l\in\mathbb{N}} a_l t^l) := \sum_{l\geq 1} a_l l t^{l-1}, \tag{1.2}$$

and the derivations $\partial_t, \partial_{u_1}, \dots, \partial_{u_n}$ commute pairwise. The map

$$\iota\colon L \to L[\![t]\!], \quad a \mapsto \sum_{l\in\mathbb{N}} \frac{\partial^l(a)}{l!} t^l \tag{1.3}$$

is a homomorphism from the differential ring (L, ∂) and $(L[\![t]\!], \partial_t)$ and Umemura calls it the *universal Taylor homomorphism* with respect to ∂. In the notation of [**Hei07**] (cf. also [**Mau10**]) this is the iterative derivation associated to ∂. In fact, the homomorphism ι makes the diagrams

$$
\begin{tikzcd}
L \arrow[r, "\iota"] \arrow[d, "\iota"] & L[\![t]\!] \arrow[d, "\iota[\![t]\!]"] \\
L[\![t]\!] \arrow[r, "t\mapsto t+u"] & L[\![t]\!][\![u]\!]
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
L \arrow[r, "\iota"] \arrow[dr, "\mathrm{id}"'] & L[\![t]\!] \arrow[d, "t\mapsto 0"] \\
 & L
\end{tikzcd}
\tag{1.4}
$$

commutative and a homomorphism of algebras $\iota\colon L \to L[\![t]\!]$ with this property is what we call an *iterative derivation* on L. An equivalent definition uses the properties of the induced maps $(\iota^{(k)}\colon L \to L)_{k\in\mathbb{N}}$ such that $\iota(a) = \sum_{k\in\mathbb{N}} \iota^{(k)}(a)t^k$ for all $a \in L$. In fact, the homomorphism ι is an iterative derivation on L if and only if the maps $(\iota^{(k)})_{k\in\mathbb{N}}$ fulfill the following properties for all $k, l \in \mathbb{N}$ and $a, b \in L$:

(1) $\iota^{(0)} = \mathrm{id}$,

(2) $\iota^{(k)}(a + b) = \iota^{(k)}(a) + \iota^{(k)}(b)$,

(3) $\iota^{(k)}(ab) = \sum_{k=k_1+k_2} \iota^{(k_1)}(a)\iota^{(k_2)}(b)$ and

(4) $\iota^{(k)} \circ \iota^{(l)} = \binom{k}{k+l}\iota^{(k+l)}$.

We define an algebra

$$\mathcal{L} := L\{\iota(L)\}_{\partial_{u_1},\dots,\partial_{u_n}} \subseteq L[\![t]\!],$$

where $L\{\iota(L)\}_{\partial_{u_1},\dots,\partial_{u_n}}$ denotes the differential subalgebra of $(L[\![t]\!], \{\partial_{u_1}, \dots, \partial_{u_n}\})$ generated by L (the constant formal power series) and $\iota(L)$. [(1)] One can easily show that $\mathcal{L}$ is independent of the choice of the transcendence basis $u_1, \dots, u_n$. We further define

$$\mathcal{K} := L[\iota(K)] \subseteq L[\![t]\!].$$

Both, $\mathcal{L}$ and $\mathcal{K}$, are differential subalgebras of $(L[\![t]\!], \{\partial_t, \partial_{u_1}, \dots, \partial_{u_n}\})$. Following Umemura, we define a homomorphism

$$\theta_{\boldsymbol{u}}\colon L \to L[\![w_1, \dots, w_n]\!] = L[\![\boldsymbol{w}]\!], \quad a \mapsto \sum_{\boldsymbol{k}\in\mathbb{N}^n} \frac{\partial_{u_1}^{k_1} \circ \cdots \circ \partial_{u_n}^{k_n}(a)}{\boldsymbol{k}!}\boldsymbol{w}^{\boldsymbol{k}}. \tag{1.5}$$

For every commutative L-algebra A we consider the tensor product

$$L[\![t]\!] \otimes_L A[\![\boldsymbol{w}]\!].$$

where the L-algebra structure on $L[\![t]\!]$ is given by the inclusion of L into $L[\![t]\!]$ as constant formal power series and the one on $A[\![\boldsymbol{w}]\!]$ is given by the composition of $\theta_{\boldsymbol{u}}\colon L \to L[\![\boldsymbol{w}]\!]$ and the homomorphism $L[\![\boldsymbol{w}]\!] \to A[\![\boldsymbol{w}]\!]$ that is induced by the L-algebra structure of A.

This tensor product is a partial differential ring with derivations ∂_t (extended trivially to the right factor) and derivations ∂_i induced by ∂_{u_i} on $L[\![t]\!]$ and ∂_{w_i} on

1. In [**Ume96**], Umemura defined $\mathcal{L}$ to be a field, but later this definition was proposed. So we adopt this definition here.

$A[\![\boldsymbol{w}]\!]$ for each $i = 1, \dots, n$. Since these derivations are continuous, they extend to the completion

$$L[\![t]\!]\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

with respect to the $(\boldsymbol{w})$-adic topology. The algebras $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ and $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ are differential subalgebras of $L[\![t]\!]\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$.

Definition 1.3. — *We define the* Umemura functor *of $L|K$ as a functor*

$$\mathrm{Ume}(L|K)\colon \mathsf{CAlg}_L \to \mathsf{Grp},$$

where for any commutative L-algebra A we define $\mathrm{Ume}(L|K)(A)$ *as the group of automorphisms φ of the differential algebra $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ with respect to the derivations $\partial_t, \partial_1, \dots, \partial_n$ that leave $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ fixed and make the diagram*

$$\begin{tikzcd}
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[d, "\varphi"] \arrow[dr, "\mathrm{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]"] & \\
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[r, "\mathrm{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]"] & \mathcal{L}\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{tikzcd}$$

commutative. If $\lambda\colon A \to B$ is a homomorphism in CAlg_L, we define

$$\mathrm{Ume}(L|K)(\lambda)\colon \mathrm{Ume}(L|K)(A) \to \mathrm{Ume}(L|K)(B)$$

by sending $\varphi \in \mathrm{Ume}(L|K)(A)$ to $\varphi\hat{\otimes}_{A[\![\boldsymbol{w}]\!]}\mathrm{id}_{B[\![\boldsymbol{w}]\!]}$, where we consider $B[\![\boldsymbol{w}]\!]$ as $A[\![\boldsymbol{w}]\!]$-algebra via the homomorphism $\lambda[\![\boldsymbol{w}]\!]\colon A[\![\boldsymbol{w}]\!] \to B[\![\boldsymbol{w}]\!]$.

Umemura introduces Lie-Ritt functors in [**Ume96**] and shows that $\mathrm{Ume}(L|K)(A)$ is such a Lie-Ritt functor. He also shows that Lie-Ritt functors give rise to formal group schemes. If $L|K$ is a Picard-Vessiot extension of differential fields with algebraically closed field of constants, then one can show that $\mathrm{Ume}(L|K)$ becomes isomorphic to the formal group scheme associated to the Galois group scheme $\mathrm{Gal}(L|K)$ after a base extension to a finite étale extension of L. We give a definition of Lie-Ritt functors and precise formulations for these claims in a more general framework in sections 5 and 6.

We note that there is another Galois theory in a more geometric setting also aimed at the study of non-linear differential equations by Malgrange (cf. [**Mal01**]).

2. Difference Galois theory

2.1. Galois theory of linear difference equations. — There is a Galois theory of linear difference equations, which is in great parts analogous to the Galois theory of linear differential equations, although there are significant differences. The standard reference is [**vdPS97**].

Let (K, σ_K) be an inversive difference field, i.e. K is a field and σ_K an automorphism of K. For $A \in \mathrm{GL}_n(K)$ we consider the linear difference equation

$$\sigma(\boldsymbol{y}) = A\boldsymbol{y}. \tag{2.1}$$

Proposition 2.1 **([vdPS97]).** — *If the field of constants $K^{\sigma_K} \coloneqq \{a \in K \mid \sigma_K(a) = a\}$ is algebraically closed, then there exists a difference extension ring (R, σ_R) of (K, σ_K) such that*

(1) the difference ring (R, σ_R) is simple, i.e. it has no non-trivial σ_R-stable ideals,

(2) there exists a matrix $Y \in \mathrm{GL}_n(R)$ such that $\sigma_R(Y) = AY$ and

(3) R is generated as K-algebra by the coefficients of Y and Y^{-1}.

A difference ring (R, σ_R) having these properties is unique up to difference isomorphism. If L is the total quotient ring of R, then the constants of L and K are equal.

The ring R is called the *Picard-Vessiot ring* of equation (2.1) and L is called its *total Picard-Vessiot ring.* One main difference to the Picard-Vessiot theory of differential equations is that R is in general not an integral domain, but only a direct product of integral domains, so that L is in general not a field, but only a direct product of fields.

We denote the field of constants K^{σ_K} of K by k. The *difference Galois group* of the equation (2.1) over K (or of the difference ring extension $L|K$) is defined as the group functor $\mathrm{Gal}(L|K)$ on the category of commutative k-algebras such that for every commutative k-algebra A the group $\mathrm{Gal}(L|K)(A)$ consists of the difference automorphisms of $R \otimes_k A$ that leave $K \otimes_k A$ fixed, where the automorphism σ_R is extended trivially to the right factor of the tensor product $R \otimes_k A$.

2.2. Morikawa-Umemura's Galois theory of non-linear difference equations. — Umemura sketched a Galois theory of non-linear algebraic difference equations in characteristic 0 in [**Ume06**, Section 7] and developed it together with Morikawa (cf. [**Mor09**], [**MU09**]). We recall their basic definitions.

Let $L|K$ be an extension of difference fields of characteristic 0 that is finitely generated as a field extension and denote the endomorphism of L by σ. Let $u_1, \dots, u_n$ be a transcendence basis of $L|K$ and $\partial_{u_1}, \dots, \partial_{u_n}$ be the system of K-derivations on L defined by $\partial_{u_i}(u_j) = \delta_{i,j}$ for $i, j \in \{1, \dots, n\}$. On the ring $L^{\mathbb{N}}$ of functions from $\mathbb{N}$ to L we define an endomorphism Σ by

$$\Sigma\colon L^{\mathbb{N}} \to L^{\mathbb{N}}, \quad \Sigma(f)(k) = f(k+1) \text{ for all } f \in L^{\mathbb{N}} \text{ and } k \in \mathbb{N}. \tag{2.2}$$

We extend the derivations $\partial_{u_1}, \dots, \partial_{u_n}$ to $L^{\mathbb{N}}$ by composition, i.e. for $f \in L^{\mathbb{N}}$, $i \in \{1, \dots, n\}$ and $k \in \mathbb{N}$ we define $(\partial_{u_i}(f))(k) \coloneqq \partial_{u_i}(f(k))$. They commute pairwise and also with the endomorphism Σ.

Similarly to the universal Taylor homomorphism (1.3), we define a homomorphism

$$\iota\colon L \to L^{\mathbb{N}}, \quad a \mapsto (k \mapsto \sigma^k(a)), \tag{2.3}$$

which Morikawa and Umemura call *universal Euler morphism*. As in the differential case, one defines

$$\mathcal{L} := L\{\iota(L)\}_{\partial_{u_1},\ldots,\partial_{u_n}} \subseteq L^{\mathbb{N}}$$

as the differential subalgebra of $(L^{\mathbb{N}}, \{\partial_{u_1}, \ldots, \partial_{u_n}\})$ that is generated by $\iota(L)$ and L (the constant functions on $\mathbb{N}$) and similarly

$$\mathcal{K} := L[\iota(K)] \subseteq L^{\mathbb{N}}.$$

Both are differential-difference subalgebras of $(L^{\mathbb{N}}, \{\Sigma, \partial_{u_1}, \ldots, \partial_{u_n}\})$. For any commutative L-algebra A we consider the tensor product

$$L^{\mathbb{N}} \otimes_L A[\![\boldsymbol{w}]\!],$$

where the L-algebra structure on $L^{\mathbb{N}}$ is given by the inclusion of L into $L^{\mathbb{N}}$ as constant functions and the one on $A[\![\boldsymbol{w}]\!]$ is given by $\theta_{\boldsymbol{u}} \colon L \to L[\![\boldsymbol{w}]\!]$ (cf. (1.5)).

We extend the endomorphism Σ (cf. (2.2)) from $L^{\mathbb{N}}$ trivially to the tensor product and denote it again by Σ. For each $i = 1, \ldots, n$ the derivations ∂_{u_i} on $L^{\mathbb{N}}$ and ∂_{w_i} on $A[\![\boldsymbol{w}]\!]$ give rise to a derivation ∂_i on the tensor product, which commute mutually and also commute with the endomorphism Σ.

Since the endomorphism Σ and the derivations ∂_i are continuous, they extend to the completion

$$L^{\mathbb{N}} \hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

with respect to the $(\boldsymbol{w})$-adic topology. The algebras $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ and $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ are differential-difference subalgebras of $(L^{\mathbb{N}}\hat{\otimes}_L A[\![\boldsymbol{w}]\!], \{\Sigma, \partial_1, \ldots, \partial_n\})$.

Definition 2.2. — *The* Umemura functor *of $L|K$ is the functor*

$$\mathrm{Ume}(L|K) \colon \mathsf{CAlg}_L \to \mathsf{Grp},$$

where for every commutative L-algebra A we define $\mathrm{Ume}(L|K)(A)$ to be the group of automorphisms φ of the of differential-difference algebra $(\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!], \{\Sigma, \partial_1, \ldots, \partial_n\})$ that leave $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ fixed and make the diagram

$$\begin{tikzcd}
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[d, "\varphi"] \arrow[dr, "\mathrm{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]"] & \\
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[r, "\mathrm{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]"] & \mathcal{L}\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{tikzcd}$$

commutative. If $\lambda \colon A \to B$ is a homomorphism of commutative L-algebras, we define

$$\mathrm{Ume}(L|K)(\lambda) \colon \mathrm{Ume}(L|K)(A) \to \mathrm{Ume}(L|K)(B)$$

by sending $\varphi \in \mathrm{Ume}(L|K)(A)$ to $\varphi\hat{\otimes}_{A[\![\boldsymbol{w}]\!]} \mathrm{id}_{B[\![\boldsymbol{w}]\!]}$, where we consider $B[\![\boldsymbol{w}]\!]$ as $A[\![\boldsymbol{w}]\!]$-algebra via the homomorphism $\lambda[\![\boldsymbol{w}]\!] \colon A[\![\boldsymbol{w}]\!] \to B[\![\boldsymbol{w}]\!]$.

Morikawa showed that $\mathrm{Ume}(L|K)(A)$ is a Lie-Ritt functor (cf. [**Mor09**]). If $L|K$ is a Picard-Vessiot extension, then $\mathrm{Ume}(L|K)$ becomes isomorphic to the formal group scheme associated to the Galois group scheme $\mathrm{Gal}(L|K)$ after a base extension to a finite étale extension of L. In the sections 5 and 6 we present these results in a more general situation.

As mentioned above, the total Picard-Vessiot rings of linear difference equations are direct products of fields. In section 5 we show how one can remove the restriction that L and K are fields in the theory of Morikawa-Umemura.

We note that following ideas of Malgrange, Galois theories for non-linear (q-)difference equations have been developed by Casale and Granier.

PART II
UNIFIED GALOIS THEORY

In this part we show how the above mentioned theories can be unified.

3. Module algebras

In this section we recall the definition of module algebras and give several examples illustrating them. Let C be a commutative ring, $(D, \Delta_D, \varepsilon_D, m_D, \eta_D)$ be a C-bialgebra and let (A, m_A, η_A) and (B, m_B, η_B) be C-algebras.

Definition 3.1. — *A homomorphism of C-modules $\Psi\colon D \otimes_C A \to A$ is a D-*module algebra structure *(cf.* [**Swe69**]*) on A if for all $d \in D$*

(1) $\Psi(d \otimes ab) = \sum_{(d)} \Psi(d_{(1)} \otimes a)\Psi(d_{(2)} \otimes b)$ for all $a, b \in A$, using the sigma notation $\Delta_D(d) = \sum_{(d)} d_{(1)} \otimes d_{(2)}$ (cf. [**Mon93**, Notation 1.4.2]*)*

(2) $\Psi(d \otimes 1_A) = \varepsilon_D(d)1_A$ and

(3) Ψ makes A into a D-module.

*The pair (A, Ψ) is then called a D-*module algebra.

A homomorphism from a D-module algebra (A, Ψ_A) to a D-module algebra (B, Ψ_B) is a homomorphism of C-algebras $\varphi\colon A \to B$ such that for all $a \in A$ and $d \in D$ we have $\varphi(\Psi_A(d \otimes a)) = \Psi_B(d \otimes \varphi(a))$.

We illustrate this by examples:

Example 3.2. — *Let A be a commutative C-algebra.*

(1) *Let $D_{der} \coloneqq C[\mathbb{G}_a]$ be the Hopf algebra on the coordinate ring of the additive group scheme $\mathbb{G}_a$ over C. If $D_{der} = C[d]$ with $\Delta(d) = d \otimes 1 + 1 \otimes d$ and $\varepsilon(d) = 0$, then for every D_{der}-module algebra (A, Ψ) we have*

$$\Psi(d \otimes ab) = \Psi(d \otimes a)b + a\Psi(d \otimes b) \quad \text{and} \quad \Psi(d \otimes 1_A) = 0$$

for all $a, b \in A$ and so $\partial\colon A \to A, a \mapsto \Psi(d \otimes a)$ is a C-derivation on A. Conversely, every C-derivation gives rise to a D_{der}-module algebra structure on A, so that D_{der}-module algebra structures on A are in 1-1 correspondence with C-derivations on A.

(2) *Let $D_{aut} \coloneqq C[\mathbb{G}_m]$ be the Hopf algebra on the coordinate ring of the multiplicative group scheme $\mathbb{G}_m$ over C. If $D_{aut} = C[g, g^{-1}]$, $\sigma(g) = g \otimes g$ and $\varepsilon(g) = 1$, then for every D_{aut}-module algebra (A, Ψ) we have*

$$\Psi(g \otimes ab) = \Psi(g \otimes a)\Psi(g \otimes b) \quad \text{and} \quad \Psi(g \otimes 1_A) = 1_A$$

for all $a, b \in A$ and $\sigma\colon A \to A, a \mapsto \Psi(g \otimes a)$ is an automorphism of the C-algebra A. Conversely, every automorphism of the C-algebra A gives rise to a D_{aut}-module algebra structure on A, so that D_{aut}-module algebra structures on A are in 1-1 correspondence with automorphisms of the C-algebra A.

(3) *If D_{end} is the C-bialgebra with underlying C-algebra the polynomial algebra $C[g]$ over C and with coalgebra structure defined by $\Delta(g^n) = g^n \otimes g^n$ and $\varepsilon(g^n) = 1$ for all $n \in \mathbb{N}$, then D_{end}-module algebra structures on A are in 1-1 correspondence with endomorphisms of the C-algebra A.*

(4) *For a monoid G we define a C-bialgebra CG by taking the group algebra CG as the underlying algebra with the coalgebra structure defined by $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ for all $g \in G$. Operations of the monoid G as endomorphisms on the C-algebra A are in 1-1 correspondence with CG-module algebra structure on A.*

If $G = (\mathbb{N}, +)$ is the monoid of natural numbers, then the bialgebra $C\mathbb{N}$ is isomorphic to D_{end}. In the case where $G = (\mathbb{Z}, +)$ is the group of integers, the bialgebra $C\mathbb{Z}$ is isomorphic to D_{aut}.

(5) *We recall that an iterative derivation on A over C is a family $(\theta^{(i)})_{i \in \mathbb{N}}$ of endomorphisms of the C-module A such that $\theta^{(0)} = \mathrm{id}_A$ and for all $a, b \in A$ and all $i, j \in \mathbb{N}$*

$$\theta^{(i)}(ab) = \sum_{i = i_1 + i_2} \theta^{(i_1)}(a)\theta^{(i_2)}(b)$$

and

$$\theta^{(i)} \circ \theta^{(j)} = \binom{i+j}{i} \theta^{(i+j)}$$

hold (cf. [**HS37**] *or* [**Mat89**, §27]*).*

If $D_{ID} \coloneqq C\langle \theta^{(k)} \mid k \in \mathbb{N}\rangle$ is the free C-module with generators $\theta^{(k)}$ for all $k \in \mathbb{N}$ and C-algebra structure defined by

$$\theta^{(i)}\theta^{(j)} \coloneqq \binom{i+j}{i}\theta^{(i+j)} \quad \text{and} \quad 1 \coloneqq \theta^{(0)}$$

and C-coalgebra structure defined by

$$\Delta(\theta^{(i)}) \coloneqq \sum_{i_1+i_2=i} \theta^{(i_1)} \otimes \theta^{(i_2)} \quad \text{and} \quad \varepsilon(\theta^{(i)}) = \delta_{i,0}$$

for all $i, j \in \mathbb{N}$, then D_{ID}-module algebra structures on A are in 1-1 correspondence with iterative derivations on A over C. We also note that D_{ID} is a Hopf algebra (cf. [**Mon93**, Example 5.6.8]*).*

(6) *For each C-bialgebra D, there is a D-module algebra structure $\Psi_0\colon D \otimes_C A \to A$ on A defined as the composition*

$$D \otimes_C A \xrightarrow{\varepsilon_D \otimes \mathrm{id}_A} C \otimes_C A \xrightarrow{\sim} A,$$

which we call the trivial D-module algebra structure *on A.*

If $\Psi\colon D \otimes_C A \to A$ is a homomorphism of C-modules, we denote by $\rho\colon A \to {}_C\mathcal{M}(D, A)$ the homomorphism corresponding to Ψ under the isomorphism

$$ {}_C\mathcal{M}(D \otimes_C A, A) \cong {}_C\mathcal{M}(A, {}_C\mathcal{M}(D, A)). \tag{3.1}$$

We note that the C-module ${}_C\mathcal{M}(D, A)$ carries a C-algebra structure with convolution product

$$(f \cdot g)(d) = \sum_{(d)} f(d_{(1)})g(d_{(2)}) \quad \text{for all } d \in D$$

and unit $\eta_A \circ \varepsilon_D$. The following lemma can be directly verified.

Lemma 3.3. — *The homomorphism Ψ is a D-module algebra structure on A if and only if ρ is a homomorphism of C-algebras and makes the diagrams*

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "\rho"] & {}_C\mathcal{M}(D,A) \arrow[d, "{}_C\mathcal{M}(D,\rho)"] \\ {}_C\mathcal{M}(D,A) \arrow[r, "{}_C\mathcal{M}(m_D,A)"] & {}_C\mathcal{M}(D, {}_C\mathcal{M}(D,A)), \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \arrow[r, "\rho"] \arrow[dr, "\mathrm{id}"] & {}_C\mathcal{M}(D,A) \arrow[d, "\mathrm{ev}_{1_D}"] \\ & A \end{tikzcd} \tag{3.2}$$

commutative, where we identify ${}_C\mathcal{M}(D, {}_C\mathcal{M}(D, A))$ with ${}_C\mathcal{M}(D \otimes_C D, A)$.

Example 3.4. — *In example 3.2 above the algebras ${}_C\mathcal{M}(D, A)$ and the homomorphisms $\rho\colon A \to {}_C\mathcal{M}(D, A)$ associated to the D-module algebra structures $\Psi\colon D \otimes_C A \to A$ on a commutative C-algebra A are well-known:*

(1) *If $\mathbb{Q} \subseteq A$, then ${}_C\mathcal{M}(D_{der}, A)$ is isomorphic to the formal power series ring $A[\![t]\!]$. If ∂ is a C-derivation on A and Ψ the corresponding D_{der}-module algebra structure on A, then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{der}, A) \xrightarrow{\sim} A[\![t]\!]$ is given by $a \mapsto$*

$\sum_{k\in\mathbb{N}} \frac{\partial^k(a)}{k!} t^k$. *This is the universal Taylor homomorphism that we encountered in* (1.3) *and the diagrams* (3.2) *correspond to those in* (1.4).

(2) The C-algebra ${}_C\mathcal{M}(D_{aut}, A)$ is isomorphic to $A^{\mathbb{Z}}$, the ring of maps from the integers to A with pointwise addition and multiplication. If σ is an automorphism of the C-algebra A and Ψ the corresponding D_{aut}-module algebra structure, then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{aut}, A) \xrightarrow{\sim} A^{\mathbb{Z}}$ is given by $a \mapsto (k \mapsto \sigma^k(a))$.

(3) The algebra ${}_C\mathcal{M}(D_{end}, A)$ is isomorphic to $A^{\mathbb{N}}$, the ring of maps from the natural numbers to A with pointwise addition and multiplication. If σ is an endomorphism of the C-algebra A and Ψ the corresponding D_{end}-module algebra structure, then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{end}, A) \xrightarrow{\sim} A^{\mathbb{N}}$ is given by $a \mapsto (k \mapsto \sigma^k(a))$. This homomorphism is the universal Euler homomorphism (2.3).

(4) The C-algebra ${}_C\mathcal{M}(CG, A)$ is isomorphic to A^G, the ring of maps from G to A with pointwise addition and multiplication. If $\Psi\colon CG \otimes_C A \to A$ is the CG-module algebra structure on A corresponding to an operation of G on A and $\rho\colon A \to {}_C\mathcal{M}(CG, A)$ the corresponding homomorphism, then the composition $A \to {}_C\mathcal{M}(CG, A) \to A^G$ is given by $a \mapsto (g \mapsto g.a)$.

(5) The C-algebra ${}_C\mathcal{M}(D_{ID}, A)$ is isomorphic to $A[\![t]\!]$ and if $(\theta^{(k)})_{k\in\mathbb{N}}$ is an iterative derivation on A over C and Ψ the corresponding D_{ID}-module algebra structure on A, then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{ID}, A) \xrightarrow{\sim} A[\![t]\!]$ is given by $a \mapsto \sum_{k\in\mathbb{N}} \theta^{(k)}(a)t^k$. We often denote this homomorphism by θ and refer with it to the corresponding iterative derivation.

(6) The homomorphism $\rho_0\colon A \to {}_C\mathcal{M}(D, A)$ associated to the trivial D-module algebra structure Ψ_0 is given by $\rho_0(a)(d) = \varepsilon_D(d)a$ for all $a \in A$ and $d \in D$.

We note that D_{der} and D_{ID} are isomorphic if $\mathbb{Q} \subseteq C$. This explains why derivations and iterative derivations are equivalent on commutative $\mathbb{Q}$-algebras. In contrast, ${}_C\mathcal{M}(D_{der}, A)$ is not reduced in positive characteristic. It is isomorphic to the ring of Hurwitz series as defined by Keigher (cf. [**Kei97**]).

If D_1 and D_2 are C-bialgebras, then $D_1 \otimes_C D_2$ becomes a C-bialgebra in a natural way. Commuting D_1- and D_2-module algebra structures on A give rise to a $D_1 \otimes_C D_2$-module algebra structure on A and vice versa.

In particular, $D_{ID^n} := {D_{ID}}^{\otimes n}$-module algebra structures correspond to systems of n commuting iterative derivations, which we call *n-variate iterative derivations* as in [**Hei07**] (cf. also [**Mau10**]). Let A be a commutative C-algebra. Then we have

$$ {}_C\mathcal{M}(D_{ID^n}, A) \cong A[\![w_1, \ldots, w_n]\!] =: A[\![\boldsymbol{w}]\!]. \tag{3.3}$$

Let $(\theta_1^{(k)})_{k\in\mathbb{N}}, \ldots, (\theta_n^{(k)})_{k\in\mathbb{N}}$ be commuting iterative derivations on A over C, i.e. $\theta_i^{(k)} \circ \theta_j^{(l)} = \theta_j^{(l)} \circ \theta_i^{(k)}$ for all $i, j \in \{1, \ldots, n\}$ and $k, l \in \mathbb{N}$, and $\rho\colon A \to {}_C\mathcal{M}(D_{ID^n}, A)$ be the homomorphism of C-algebras associated to the corresponding D_{ID^n}-module algebra structure on A. If we denote by $\theta\colon A \to A[\![\boldsymbol{w}]\!]$ the composition of ρ and the isomorphism (3.3) and by $\theta^{(\boldsymbol{k})}$ the homomorphisms of the C-module A such that $\theta(a) = \sum_{\boldsymbol{k}\in\mathbb{N}} \theta^{(\boldsymbol{k})}(a)\boldsymbol{w}^{\boldsymbol{k}}$ holds for all $a \in A$ and $\boldsymbol{k} \in \mathbb{N}^n$, then they fulfill

$$\theta^{(\boldsymbol{0})} = \mathrm{id}_A, \theta^{(\boldsymbol{k})}(ab) = \sum_{\boldsymbol{k}=\boldsymbol{k_1}+\boldsymbol{k_2}} \theta^{(\boldsymbol{k_1})}(a)\theta^{(\boldsymbol{k_2})}(b) \text{ and } \theta^{(\boldsymbol{k})} \circ \theta^{(\boldsymbol{l})} = \binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}}\theta^{(\boldsymbol{k}+\boldsymbol{l})} \tag{3.4}$$

for all $a, b \in A$ and $\boldsymbol{k}, \boldsymbol{l} \in \mathbb{N}^n$ (cf. [**Hei07**]). Both $\theta\colon A \to A[\![\boldsymbol{w}]\!]$ and the maps $(\theta^{(\boldsymbol{k})})_{\boldsymbol{k}\in\mathbb{N}^n}$ determine the n-variate iterative derivation uniquely, so one could define n-variate iterative derivations on A over C also as a homomorphism $\theta\colon A \to A[\![\boldsymbol{w}]\!]$ such that

$$\begin{tikzcd} A \arrow[r, "\theta"] \arrow[dr, "\mathrm{id}"'] & A[\![\boldsymbol{w}]\!] \arrow[d, "\varepsilon"] \\ & A \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \arrow[r, "\theta"] \arrow[d, "\theta"] & A[\![\boldsymbol{w}]\!] \arrow[d, "\theta[\![\boldsymbol{w}]\!]"] \\ A[\![\boldsymbol{w}]\!] \arrow[r, "w_i\mapsto w_i+v_i"] & A[\![\boldsymbol{w}]\!][\![\boldsymbol{v}]\!], \end{tikzcd}$$

commute, where $\varepsilon\colon A[\![\boldsymbol{w}]\!] \to A$ denotes the homomorphism of A-algebras defined by $\varepsilon(w_i) = 0$ for all $i = \{1, \dots, n\}$, or as a system of endomorphisms $(\theta^{(\boldsymbol{k})})_{\boldsymbol{k}\in\mathbb{N}^n}$ of the C-module A such that (3.4) holds. Therefore we also use $\theta\colon A \to A[\![\boldsymbol{w}]\!]$ or the family $(\theta^{(\boldsymbol{k})})_{\boldsymbol{k}\in\mathbb{N}}$ to refer to an n-variate iterative derivation.

Definition 3.5. — *The* constants *of a D-module algebra (A, Ψ) are defined as*

$$A^\Psi := \{a \in A \mid \Psi(d \otimes a) = \varepsilon(d)a \quad \text{for all } d \in D\}.$$

They will also be denoted by A^ρ, where ρ is the homomorphism associated to Ψ via (3.1).

Example 3.6. — *If R is a commutative ring, $n \in \mathbb{N}$ and S is one of the rings $R[\boldsymbol{x}], R[\![\boldsymbol{x}]\!]$ or $R(\boldsymbol{x})$, where $\boldsymbol{x} = (x_1, \dots, x_n)$ is an n-tuple of algebraically independent elements over R. Then there is a unique n-variate iterative derivation on S over R such that the associated homomorphism $\theta_{\boldsymbol{x}}\colon S \to S[\![\boldsymbol{w}]\!]$ (with $\boldsymbol{w} := (w_1, \dots, w_n)$) fulfills $\theta_{\boldsymbol{x}}(x_i) = x_i + w_i$ for all $i \in \{1, \dots, n\}$. The components $\theta_{\boldsymbol{x}}^{(\boldsymbol{l})}$ of $\theta_{\boldsymbol{x}}$ fulfill $\theta_{\boldsymbol{x}}^{(\boldsymbol{l})}(\boldsymbol{x}^{\boldsymbol{k}}) = \binom{\boldsymbol{k}}{\boldsymbol{l}}\boldsymbol{x}^{\boldsymbol{k}-\boldsymbol{l}}$. They uniquely extend to n-variate iterative derivations over R on formally étale extension of S by* [**Mat89**, Theorem 27.2], *which we again denote by $\theta_{\boldsymbol{x}}$.*

Lemma 3.7. — *(1) The C-algebra ${}_C\mathcal{M}(D, A)$ becomes a D-module algebra by the homomorphism of C-modules*

$$\Psi_{int}\colon D \otimes_C {}_C\mathcal{M}(D, A) \to {}_C\mathcal{M}(D, A)$$

that sends $d \otimes f \in D \otimes_C {}_C\mathcal{M}(D, A)$ to the homomorphism of C-modules

$$\Psi_{int}(d \otimes f)\colon D \to A, \quad \bar{d} \mapsto f(\bar{d}d) \quad \text{for all } \bar{d} \in D.$$

(2) *The constants* ${}_C\mathcal{M}(D,A)^{\Psi_{int}}$ *are equal to* $\rho_0(A)$*, where* $\rho_0\colon A \to {}_C\mathcal{M}(D,A)$ *is the homomorphism associated to the trivial* D*-module algebra structure* Ψ_0 *on* A *(cf. example 3.4 (6)).*

(3) *If* D' *is another* C*-bialgebra and* (A,Ψ') *is a* D'*-module algebra with associated homomorphism* $\rho'\colon A \to {}_C\mathcal{M}(D',A)$*, then* ${}_C\mathcal{M}(D,A)$ *has a* D'*-module algebra structure with associated homomorphism given by*

$$ {}_C\mathcal{M}(D,\rho')\colon {}_C\mathcal{M}(D,A) \to {}_C\mathcal{M}(D,{}_C\mathcal{M}(D',A)) \cong {}_C\mathcal{M}(D',{}_C\mathcal{M}(D,A)). \tag{3.5}$$

This D'*-module algebra structure commutes with the* D*-module algebra structure* Ψ_{int} *on* ${}_C\mathcal{M}(D,A)$ *and thus* ${}_C\mathcal{M}(D,A)$ *becomes a* $D\otimes_C D'$*-module algebra.*

For the bialgebras D_{der} and D_{end} the first part of the last lemma has the following concrete form:

(1) If A is a commutative C-algebra containing $\mathbb{Q}$, then under the isomorphism ${}_C\mathcal{M}(D_{der},A) \cong A[\![t]\!]$ the D_{der}-module algebra structure Ψ_{int} on ${}_C\mathcal{M}(D_{der},A)$ corresponds the derivation ∂_t with respect to t (cf. (1.2)).

(2) The D_{end}-module algebra structure Ψ_{int} on ${}_C\mathcal{M}(D_{end},A)$ corresponds to the shift endomorphism Σ (cf. (2.2)) under the isomorphism ${}_C\mathcal{M}(D_{end},A) \cong A^{\mathbb{N}}$.

Notation. — By lemma 3.3, all information about a D-module algebra structure Ψ is encoded also in the associated homomorphism ρ. Therefore, we will also use (A,ρ) to refer to a D-module algebra (A,Ψ).

4. Picard-Vessiot extensions of Artinian simple module algebras

Amano and Masuoka unified the Picard-Vessiot theories of differential equations and difference equations using Artinian simple commutative D-module algebras (cf. [**AM05**]). But they restrict themselves to the case where D is a Hopf algebra fulfilling some additional hypothesis. We sketch how their definitions and some of their results can be generalized so that the bialgebra D_{end} is also within our scope.

Notation. — Let C be a field, G be a monoid and let D^1 be an irreducible pointed cocommutative Hopf algebra of Birkhoff-Witt type, i.e. D^1 is of the form $B(U)$, where U is a C-vector space and $B(U)$ is the cofree pointed irreducible cocommutative coalgebra on U as defined in [**Swe69**, pp. 261-271]. We assume that D^1 is a CG-module algebra, where CG is the bialgebra introduced in example 3.2 (4), and define D as the smash product $D^1\#CG$.

Remark 4.1. — *These conditions allow to chose* D *for example as* D_{end}*,* D_{aut} *or* D_{ID}*. The cocommutative pointed irreducible commutative Hopf algebra* D_{der} *is of Birkhoff-Witt type if* $\mathbb{Q}\subseteq C$ *(and then* $D_{der}\cong D_{ID}$*).*

Definition 4.2. — *An* Artinian simple commutative D-module algebra *is a commutative D-module algebra that is simple as D-module algebra, i.e. it has no non-trivial D-stable ideals, and Artinian as a ring.*

Definition 4.3. — *An extension of Artinian simple commutative D-module algebras $(L, \rho_L)|(K, \rho_K)$ is* Picard-Vessiot *if the following hold:*

(1) The constants L^{ρ_L} of L coincide with the constants K^{ρ_K} of K.

(2) There exists an intermediate D-module algebra (R, ρ_R) of $K \subseteq L$ such that the total quotient ring $\mathrm{Q}(R)$ of R is equal to L and such that the K^{ρ_K}-subalgebra

$$H := (R \otimes_K R)^{\rho_R \otimes \rho_R}$$

of $R \otimes_K R$ generates $R \otimes_K R$ as left (or equivalently right) R-algebra, i.e.

$$R \cdot H = R \otimes_K R \quad (\textit{or } H \cdot R = R \otimes_K R). \tag{4.1}$$

We note that the Picard-Vessiot extensions in the differential and difference context mentioned in the first part are examples of Picard-Vessiot extensions of Artinian simple commutative module algebras. In fact, the Picard-Vessiot ring R fulfills the conditions in (2), where the statement (4.1) (or more precisely the statement (4.2) below following from it) is a theorem in the Picard-Vessiot theories of differential and difference equations, stating that $\operatorname{Spec} R$ is a $\operatorname{Gal}(L|K)$-torsor.

Proposition 4.4. — *Let $(L, \rho_L)|(K, \rho_K)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras with constants $k := L^{\rho_L} = K^{\rho_K}$ and (R, ρ_R) and H be as in definition 4.3. Then the following hold:*

(1) The homomorphism

$$\mu\colon (R \otimes_k H, \rho_R \otimes \rho_0) \to (R \otimes_K R, \rho_R \otimes \rho_R), \quad a \otimes h \mapsto (a \otimes 1) \cdot h \tag{4.2}$$

is an isomorphism of D-module algebras.

(2) The k-algebra H carries a Hopf algebra structure induced by the R-coalgebra structure on $R \otimes_K R$, given by the counit

$$\varepsilon\colon R \otimes_K R \to R, \quad a \otimes b \mapsto ab$$

and the comultiplication

$$\Delta\colon R \otimes_K R \to (R \otimes_K R) \otimes_R (R \otimes_K R), \quad a \otimes b \mapsto (a \otimes 1) \otimes (1 \otimes b).$$

The antipode S on H is induced by the map

$$\tau\colon R \otimes_K R \to R \otimes_K R, \quad a \otimes b \mapsto b \otimes a.$$

(3) The intermediate D-module algebra (R, ρ_R) satisfying condition (2) in definition 4.3 is unique.

Proof. — This can be proven as [**AM05**, Proposition 3.4], only the proof of part (3) requires a small modification, cf. [**Hei**]. □

Definition 4.5. — *If $L|K$ is a Picard-Vessiot extension of Artinian simple commutative D-module algebras, then R and H in definition 4.3 are called the* principal D-module algebra *and the* Hopf algebra of a Picard-Vessiot extension $L|K$*, respectively. If we want to indicate R and H, we denote the Picard-Vessiot extension $L|K$ also by $(L|K, R, H)$.*

Definition 4.6. — *If $(L|K, R, H)$ is a Picard-Vessiot extension of Artinian simple commutative D-module algebras, then we define the* Galois group scheme $\mathrm{Gal}(L|K)$ *of $L|K$ to be the affine group scheme $\operatorname{Spec} H$ over the constants $K^{\Psi_K} = L^{\Psi_L}$.*

Proposition 4.7. — *Let $L|K$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras with principal D-module algebra (R, ρ_R), Hopf algebra H and constants $k := L^{\Psi_L}$. Then for any commutative k-algebra A the group of A-points of $\mathrm{Gal}(L|K) = \operatorname{Spec} H$ is isomorphic to the group of automorphisms of the D-module algebra $(R \otimes_k A, \rho_R \otimes \rho_0)$ that leave $K \otimes_k A$ fixed.*

Proof. — The proof of [**AM05**, Remark 3.11] also holds in our situation. □

Amano and Masuoka also establish a Galois correspondence for Picard-Vessiot extensions of Artinian simple commutative D-module algebras, D being a Hopf algebra fulfilling some additional conditions.

5. Generalized Galois theory of Artinian simple module algebras

Now we show that the theories of Umemura and Morikawa, which we sketched in part I, can be unified in a similar manner as the Picard-Vessiot theories for differential and difference equations that have been unified by Amano, Masuoka and Takeuchi (cf. [**Tak89**], [**AM05**]). In this unified theory we do not assume that the module algebras are fields (as in the difference Galois theory of Morikawa-Umemura) and we make no assumption on the characteristic, though we make a separability assumption.

As in section 4, let C be a field, G be a monoid and let D^1 be an irreducible pointed cocommutative Hopf algebra of Birkhoff-Witt type such that D^1 is a CG-module algebra, where CG is the bialgebra introduced in example 3.2 (4). We define D to be the smash product $D^1 \# CG$.

Let $L|K$ be an extension of Artinian simple commutative D-module algebras such that all $g \in G$ operate as injective endomorphisms on L. Then L and K are both direct products of fields (cf. [**Hei**]). In fact

$$L \cong \prod_{Q \in \Omega(L)} L/Q \quad \text{and} \quad K \cong \prod_{P \in \Omega(K)} K/P.$$

We assume for every $Q \in \Omega(L)$ the field L/Q is a separable and finitely generated over $K/(Q\cap K)$ and that its transcendence degree is the same for all $Q \in \Omega(L)$, say n. Let $\boldsymbol{u}^{(Q)} = (u_1^{(Q)}, \dots, u_n^{(Q)})$ be a separating transcendence basis of the extension L/Q of $K/(Q\cap K)$ and $\theta_{\boldsymbol{u}^{(Q)}} : L/Q \to L/Q[\![\boldsymbol{w}]\!]$ be the associated n-variate iterative derivation of L/Q over $K/(Q \cap K)$ defined by $\theta_{\boldsymbol{u}^{(Q)}}(u_i^{(Q)}) = u_i^{(Q)} + w_i$ for all $i = 1, \dots, n$ (cf. example 3.6). There exists an n-variate iterative derivation on the product $L \cong \prod_{Q\in\Omega(L)} L/Q$ over K such that the projections to all factors become iterative differential homomorphisms (cf. [**Hei10**, Proposition 2.2.26]). We denote this n-variate iterative derivation by $\theta_{\boldsymbol{u}}$.

5.1. The Umemura functor. — We denote by $\rho\colon L \to {}_C\mathcal{M}(D, L)$ the homomorphism of C-algebras associated to the given D-module algebra structure on L and the one associated to the trivial D-module algebra structure on L by ρ_0. We define

$$\mathcal{L} \coloneqq \rho_0(L)\{\rho(L)\}_{\theta_{\boldsymbol{u}}} \qquad \text{and} \qquad \mathcal{K} \coloneqq \rho_0(L)[\rho(K)]$$

as the iterative differential subalgebras of $({}_C\mathcal{M}(D, L), \theta_{\boldsymbol{u}})$ generated by $\rho_0(L)$ and $\rho(L)$ and by $\rho_0(L)$ and $\rho(K)$, respectively. The algebra $\rho_0(L)[\rho(K)]$ is in fact already closed with respect to $\theta_{\boldsymbol{u}}$ and $\mathcal{L}$ does not depend on the choice of the separating transcendence bases $\boldsymbol{u}^{(Q)}$ of L/Q over $K/(K \cap Q)$. Both are $D \otimes_C D_{ID^n}$-module subalgebras of $({}_C\mathcal{M}(D, L), \rho_{int} \otimes \theta_{\boldsymbol{u}})$. [2]

For every commutative L-algebra A we consider the tensor product

$${}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!],$$

where the L-algebra structure on ${}_C\mathcal{M}(D, L)$ is given by $\rho_0\colon L \to {}_C\mathcal{M}(D, L)$ (cf. example 3.2 (6)) and the one on $A[\![\boldsymbol{w}]\!]$ is given by the composition of $\theta_{\boldsymbol{u}}\colon L \to L[\![\boldsymbol{w}]\!]$ and the homomorphism $L[\![\boldsymbol{w}]\!] \to A[\![\boldsymbol{w}]\!]$ induced by the L-algebra structure of A. This tensor product carries a $D \otimes_C D_{ID^n}$-module algebra structure $\rho \otimes \theta$, induced by

$$({}_C\mathcal{M}(D, L), \rho_{int} \otimes \theta_{\boldsymbol{u}}) \xleftarrow{\rho_0} (L, \rho_0 \otimes \theta_{\boldsymbol{u}}) \xrightarrow{\theta_{\boldsymbol{u}}} (A[\![\boldsymbol{w}]\!], \rho_0 \otimes \theta_{\boldsymbol{w}}). \tag{5.1}$$

The homomorphism

$$\rho \otimes \theta\colon {}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!] \to {}_C\mathcal{M}(D \otimes_C D_{ID^n}, {}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!])$$

is continuous with respect to the $(\boldsymbol{w})$-adic topology on ${}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!]$ and the $(\boldsymbol{w}, \boldsymbol{T})$-adic topology on

$${}_C\mathcal{M}(D, {}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!])[\![\boldsymbol{T}]\!] \cong {}_C\mathcal{M}(D \otimes_C D_{ID^n}, {}_C\mathcal{M}(D, L) \otimes_L A[\![\boldsymbol{w}]\!]).$$

Therefore, this $D \otimes D_{ID^n}$-module algebra structure extends to the completion

$${}_C\mathcal{M}(D, L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

2. Originally Umemura defined $\mathcal{L}$ to be a field, but later the definition was changed. The definition we give here coincides with the definition in [**Mor09**] if $D = D_{end}$ and if L and K are fields.

with respect to the $(\boldsymbol{w})$-adic topology. The algebras $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ and $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ are $D \otimes_C D_{ID^n}$-module subalgebras.

Definition 5.1. — *The* Umemura functor *of $L|K$ is the functor*

$$\mathrm{Ume}(L|K)\colon \mathsf{CAlg}_L \to \mathsf{Grp},$$

where for each commutative L-algebra A we define $\mathrm{Ume}(L|K)(A)$ *to be the group of automorphisms φ of the $D \otimes_C D_{ID^n}$-module algebra $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ that leave $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ fixed and make the diagram*

$$\begin{tikzcd}
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[d, "\varphi"] \arrow[dr, "\mathrm{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]"] & \\
\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \arrow[r, "\mathrm{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]"] & \mathcal{L}\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{tikzcd}$$

commutative. If $\lambda\colon A \to B$ is a homomorphism of commutative L-algebras, we define

$$\mathrm{Ume}(L|K)(\lambda)\colon \mathrm{Ume}(L|K)(A) \to \mathrm{Ume}(L|K)(B)$$

by sending $\varphi \in \mathrm{Ume}(L|K)(A)$ to $\varphi\hat{\otimes}_{A[\![\boldsymbol{w}]\!]}\mathrm{id}_{B[\![\boldsymbol{w}]\!]}$, where we consider $B[\![\boldsymbol{w}]\!]$ as $A[\![\boldsymbol{w}]\!]$-algebra via the homomorphism $\lambda[\![\boldsymbol{w}]\!]\colon A[\![\boldsymbol{w}]\!] \to B[\![\boldsymbol{w}]\!]$.

5.2. Lie-Ritt functors. — Umemura defines Lie-Ritt functors in [**Ume96**]. Here we use a slightly changed version of Lie-Ritt functors, which we define now.

Notation. — In this subsection let L be an arbitrary commutative ring and A be a commutative L-algebra.

The set of all *infinitesimal coordinate transformations of n variables over A*

$$\boldsymbol{\Gamma}_{nL}(A) \coloneqq \{\Phi = (\varphi_i)_{i=1,\dots,n} \in (A[\![\boldsymbol{w}]\!])^n \mid \varphi_i \equiv w_i \mod N(A)[\![\boldsymbol{w}]\!] \text{ for all } i = 1,\dots,n\},$$

where $n \in \mathbb{N}$ and where $\boldsymbol{w}$ denotes the tuple $(w_1,\dots,w_n)$, is a group with multiplication given by composition, i.e. if $\Phi = (\varphi_1,\dots,\varphi_n), \Psi \in \boldsymbol{\Gamma}_{nL}(A)$, then $\Phi\cdot\Psi$ is defined as $(\varphi_1(\Psi),\dots,\varphi_n(\Psi))$ (cf. [**Bou81**, Chapitre IV, §4.3 and §4.7]).

We equip the ring $A[\![\boldsymbol{w}]\!] \coloneqq A[\![w_1,\dots,w_n]\!]$ with the n-variate iterative derivation θ over A with respect to $\boldsymbol{w}$ (cf. example 3.6) and we extend it to

$$A[\![\boldsymbol{w}]\!]\{\{\boldsymbol{Y}\}\} \coloneqq A[\![w_1,\dots,w_n]\!][\![Y_i^{(\boldsymbol{k})} \mid i = 1,\dots,n, \boldsymbol{k} \in \mathbb{N}^n]\!]$$

with variables $Y_i^{(\boldsymbol{k})}$ for $i \in \{1,\dots,n\}$ and $\boldsymbol{k} \in \mathbb{N}^n$ by

$$\theta^{(\boldsymbol{l})}\left(Y_i^{(\boldsymbol{k})}\right) \coloneqq \binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}} Y_i^{(\boldsymbol{k}+\boldsymbol{l})}.$$

We denote by $A[\![\boldsymbol{w}]\!]\{A[\![\boldsymbol{Y}]\!]\}_\theta$ the iterative differential subring of $A[\![\boldsymbol{w}]\!]\{\{\boldsymbol{Y}\}\}$ generated by $A[\![\boldsymbol{w},\boldsymbol{Y}]\!]$, where $\boldsymbol{Y}$ denotes the tuple $(Y_1^{(\boldsymbol{0})},\dots,Y_n^{(\boldsymbol{0})})$. For $F \in A[\![\boldsymbol{x}]\!]\{A[\![\boldsymbol{Y}]\!]\}_\theta$

and $\Phi = (\varphi_1, \dots, \varphi_n) \in \mathbf{\Gamma}_{nL}(A)$ we denote by $F_{|\boldsymbol{Y}=\Phi}$ the image of F under the homomorphism $A[\![\boldsymbol{w}]\!]\{A[\![\boldsymbol{Y}]\!]\}_\theta \to A[\![\boldsymbol{w}]\!]$ that sends $Y_i^{(\boldsymbol{k})}$ to $\theta^{(\boldsymbol{k})}(\varphi_i)$.

Definition 5.2. — *A* Lie-Ritt functor *over L is a group functor G on the category of commutative L-algebras such that there exists an $n \in \mathbb{N}$ and an ideal $I \trianglelefteq L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta = L[\![w_1, \dots, w_n]\!]\{L[\![Y_1, \dots, Y_n]\!]\}_\theta$ such that $G(A) \cong Z(I)(A)$ for every commutative L-algebra A, where*

$$Z(I)(A) \coloneqq \{\Phi \in \mathbf{\Gamma}_{nL}(A) \mid F_{|\boldsymbol{Y}=\Phi} = 0 \ \textit{ for all } \ F \in I\}.$$

Remark 5.3. — *In* [**Ume96**, Definition 1.8] *Lie-Ritt functors over L are defined using ideals in $L[\![\boldsymbol{w}]\!]\{\{\boldsymbol{Y}\}\}$. Since the term $F_{|\boldsymbol{Y}=\Phi}$ is not well defined for elements $F \in L[\![\boldsymbol{w}]\!]\{\{\boldsymbol{Y}\}\}$ in general, we use the definition above instead.*

Example 5.4. — *We define a subgroup functor G_+ of $\mathbf{\Gamma}_{1\mathbb{Z}}$ as*

$$G_+(A) \coloneqq \{a_0 + w \mid a_0 \in N(A)\}$$

for all commutative rings A. Let I be the ideal in $\mathbb{Z}[\![w]\!]\{\mathbb{Z}[\![Y]\!]\}_\theta$ generated by $Y^{(1)} - 1$ and $Y^{(k)}$ for all $k \geq 2$. Then $G_+ = Z(I)$, i.e. G_+ is a Lie-Ritt functor over $\mathbb{Z}$. Furthermore, G_+ is isomorphic to the additive formal group scheme $\hat{\mathbb{G}}_a$.

Proof. — Let A be a commutative ring. An element $\varphi(w) = \sum_{i \geq 0} a_i w^i \in \mathbf{\Gamma}_{1\mathbb{Z}}$ lies in $Z(I)$ if and only if $1 = \theta^{(1)}(\varphi) = \sum_{i \geq 1} a_i i w^{i-1}$ and for all $k \geq 2$ the equation $0 = \theta^{(k)}(\varphi) = \sum_{i \geq k} \binom{i}{k} a_i w^{i-k}$ holds. This is the case if and only if $a_1 = 1$ and $a_k = 0$ for all $k \geq 2$. □

Example 5.5. — *We define a subgroup functor G_* of $\mathbf{\Gamma}_{1\mathbb{Z}}$ as*

$$G_*(A) \coloneqq \{(1 + a_1)w \mid a_1 \in N(A)\}$$

for all commutative rings A. Then G_* is a Lie-Ritt functor over $\mathbb{Z}$ and $G_* = Z(I)$, where $I = (\{wY^{(1)} - Y, Y^{(k)} \mid k \geq 2\})$. Furthermore, G_* is isomorphic to the multiplicative formal group scheme $\hat{\mathbb{G}}_m$.

Proof. — An element $\varphi(w) = \sum_{i \geq 0} a_i w^i \in \mathbf{\Gamma}_{1\mathbb{Z}}$ lies in $Z(I)(A)$ if and only if $w \sum_{i \geq 1} i a_i w^{i-1} = \sum_{i \geq 0} a_i w^i$ and $\theta^{(k)}(\sum_{i \geq 0} a_i w^i) = 0$ hold for all $k \geq 2$. This is the case if and only if $a_0 = 0$ and $a_k = 0$ for all $k \geq 2$, i.e. if φ lies in $G_*(A)$. □

The analogs of these examples in the setting of Umemura appeared in [**Ume96**, Example 1.9(i) and (ii)]. Since he works over $\mathbb{Q}$, it is sufficient to consider the equation $Y^{(1)} - 1$ and $wY^{(1)} - Y$ in the first and second example, respectively. In the general case we have to add the equations $Y^{(k)}$ for $k \geq 2$.

Proposition 5.6. — *Every Lie-Ritt functor over a commutative ring L is isomorphic to a formal group scheme over L.*

Proof. — This is shown in [**Ume96**] in the case of Lie-Ritt functors that are subgroup functors of infinitesimal transformations of one variable. The general case is proven in [**Hei10**]. □

5.3. The Umemura functor as a Lie-Ritt functor. —

Notation. — We now continue to use the notation from the beginning of this section.

Theorem 5.7. — *The functor* $\mathrm{Ume}(L|K)$ *is a Lie-Ritt functor over* L.

Idea of proof. — Let A be a commutative L-algebra A. There exists an injective homomorphism

$$\begin{aligned} \mu_{A,\boldsymbol{u}}\colon {}_C\mathcal{M}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!] &\to {}_C\mathcal{M}(D,A[\![\boldsymbol{w}]\!]) \\ \sum_{\boldsymbol{i}\in\mathbb{N}^n} f_{\boldsymbol{i}}\otimes a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}} &\mapsto \sum_{\boldsymbol{i}\in\mathbb{N}^n}\theta_{\boldsymbol{u}}(f_{\boldsymbol{i}})\cdot\rho_0(a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}}). \end{aligned} \tag{5.2}$$

We consider the map

$$\begin{aligned} \mathrm{Ume}(L|K)(A) &\longrightarrow \boldsymbol{\Gamma}_{nL}(A) \\ \varphi &\longmapsto (\mathrm{ev}_{1_D}\circ\mu_{A,\boldsymbol{u}}\circ\varphi(\rho(u_i)\otimes 1)-u_i)_{i=1,\dots,n}. \end{aligned} \tag{5.3}$$

Then one shows that it is well defined, i.e. that the image of φ is an element of $\boldsymbol{\Gamma}_{nL}(A)$, that it respects the group structures and that its image is of the form $Z(I)$. For details we refer to [**Hei10**] or [**Hei**]. □

6. Comparison of the general theory with Picard-Vessiot theory

In this section we examine the extension $\mathcal{L}|\mathcal{K}$ defined above in the case where $L|K$ is a finitely generated Picard-Vessiot extension of Artinian simple commutative D-module algebras and compare the Umemura functor $\mathrm{Ume}(L|K)$ with the Galois group scheme $\mathrm{Gal}(L|K)$ of $L|K$ as defined by Amano and Masuoka in [**AM05**].

Notation. — Let C and D be as in section 5 and let $(L|K,R,H)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras such that $R|K$ is smooth. We further assume that there exists a matrix $X\in\mathrm{GL}_n(R)$ such that $R=K[X,X^{-1}]$ and $d(X)X^{-1}\in M_n(K)$ for all $d\in D$ (if D is a Hopf algebra as in [**AM05**], then this is the case, cf. ibid., Theorem 4.6). For every (minimal) prime ideal Q of L the field L/Q is separable and finitely generated over $K/(Q\cap K)$ (cf. [**Gro64**, Chapitre 0, Théorème 19.6.1]). We assume that the transcendence degree of L/Q over $K/(K\cap Q)$ is the same for all $Q\in\Omega(L)$, say n. Let $\boldsymbol{u}^{(Q)}=(u_1^{(Q)},\dots,u_n^{(Q)})$ be a separating transcendence basis of this extension and let $\theta_{\boldsymbol{u}}$ be the n-variate iterative derivation on L over K as defined at the beginning of section 5. We denote the homomorphism associated to the D-module algebra structure on L by $\rho\colon L\to {}_C\mathcal{M}(D,L)$.

In the case of Picard-Vessiot extensions the algebra $\mathcal{L}$ has a particularly simple form. By using the existence of the principal D-module algebra R for the extension $L|K$ and its properties (cf. theorem 4.4) and linear disjointness from constants (cf. [**AM05**, Corollary 3.2] or [**Hei**]), one obtains the following lemma.

Lemma 6.1. — *The subring of ${}_C\mathcal{M}(D,L)$ generated by $\rho_0(L)$ and $\rho(L)$ is closed under the n-variate iterative derivation $\theta_{\boldsymbol{u}}$ and $\rho_0(L)$ and $\rho(L)$ are linearly disjoint over the field of constants $k \coloneqq L^\rho$. We thus have an isomorphism*

$$\mathcal{L} = \rho_0(L)[\rho(L)] \cong \rho_0(L) \otimes_k \rho(L) \tag{6.1}$$

of D-module algebras. Similarly, $\rho_0(L)[\rho(R)]$ is closed under $\theta_{\boldsymbol{u}}$ and $\rho_0(L)$ and $\rho(R)$ are linearly disjoint over k, i.e.

$$\rho_0(L)[\rho(R)] \cong \rho_0(L) \otimes_k \rho(R). \tag{6.2}$$

Theorem 6.2. — *If the field of constants $k \coloneqq L^\rho$ is perfect, then there exists a finite étale extension L' of L such that $\mathrm{Ume}(L|K) \times_L L'$ is isomorphic to the formal group scheme $\widehat{\mathrm{Gal}(L|K)}_{L'}$ associated to the base extension $\mathrm{Gal}(L|K)_{L'} = \mathrm{Gal}(L|K) \times_k L'$ of the Galois group scheme $\mathrm{Gal}(L|K)$.*

Proof. — The proof can be found in [**Hei**]. In the case where L and K are fields a slightly weaker version of this result was already shown in [**Hei10**]. □

Corollary 6.3. — *Under the assumptions of theorem 6.2 there exists a finite étale extension L' of L and an isomorphism*

$$\mathrm{Ume}(L|K)(L'[\varepsilon]/(\varepsilon^2)) \cong \mathrm{Lie}(\mathrm{Gal}(L|K)) \otimes_k L'.$$

Proof. — This follows immediately from theorem 6.2 by taking $A = L'[\varepsilon]/(\varepsilon^2)$. □

In the case $D = D_{end}$ the statement of corollary 6.3 is similar to the one of [**Mor09**, Theorem 3.3] and to [**Ume**]. Taking $D = D_{der}$, this corollary provides a similar result as [**Ume96**, Theorem 5.15] in the case of finitely generated Picard-Vessiot extensions of differential fields in characteristic zero.

References

[AM05] K. Amano & A. Masuoka – "Picard-Vessiot extensions of Artinian simple module algebras", *J. Algebra* **285** (2005), no. 2, p. 743–767.

[Bou81] N. Bourbaki – *Éléments de mathématique*, Lecture Notes in Mathematics, vol. 864, Masson, Paris, 1981, Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7].

[Gro64] A. Grothendieck – "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I", *Inst. Hautes Études Sci. Publ. Math.* (1964), no. 20, p. 259.

[Hei] F. Heiderich – "Galois theory of Artinian simple module algebras", submitted.

[Hei07] ______, *Picard-Vessiot Theorie für lineare partielle Differentialgleichungen*, Diplomarbeit, Universität Heidelberg, Fakultät für Mathematik und Informatik, 2007.

[Hei10] ______, "Galois theory of module fields", Ph.D. Thesis, Universitat de Barcelona, Departament d'Àlgebra i Geometria, 2010, Available from: `http://hdl.handle.net/10803/674`.

[HS37] H. Hasse & F. K. Schmidt – "Noch eine Begründung der Theorie des höheren Differentialquotienten in einem algebraischen Funktionenkörper in einer Unbestimmten", *J. Reine Angew. Math.* **177** (1937), p. 215–237.

[Kei97] W. F. Keigher – "On the ring of Hurwitz series", *Comm. Algebra* **25** (1997), no. 6, p. 1845–1859.

[Mal01] B. Malgrange – "Le groupoïde de Galois d'un feuilletage", in *Essays on geometry and related topics, Vol. 1, 2* (Geneva), Monogr. Enseign. Math., vol. 38, Enseignement Math., 2001, p. 465–501.

[Mat89] H. Matsumura – *Commutative ring theory*, Cambridge University Press, Cambridge-New York, 1989.

[Mau10] A. Maurischat – "Infinitesimal group schemes as iterative differential Galois groups", *J. Pure Appl. Algebra* **214** (2010), no. 11, p. 2092–2100.

[Mon93] S. Montgomery – *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, vol. 82, American Mathematical Society, Providence, RI, 1993.

[Mor09] S. Morikawa – "On a general difference Galois theory I", *Ann. Inst. Fourier (Grenoble)* **59** (2009), no. 7, p. 2709–2732.

[MU09] S. Morikawa & H. Umemura – "On a general difference Galois theory II", *Ann. Inst. Fourier (Grenoble)* **59** (2009), no. 7, p. 2733–2771.

[MvdP03] B. H. Matzat & M. van der Put – "Iterative differential equations and the Abhyankar conjecture", *J. Reine Angew. Math.* **557** (2003), p. 1–52.

[Oku87] K. Okugawa – *Differential algebra of nonzero characteristic*, Lectures in Mathematics, vol. 16, Kinokuniya Company Ltd., Tokyo, 1987.

[Swe69] M. E. Sweedler – *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969.

[Tak89] M. Takeuchi – "A Hopf algebraic approach to the Picard-Vessiot theory", *J. Algebra* **122** (1989), no. 2, p. 481–509.

[Ume] H. Umemura – "Picard-Vessiot theory in general Galois theory", preprint.

[Ume96] ______, "Differential Galois theory of infinite dimension", *Nagoya Math. J.* **144** (1996), p. 59–135.

[Ume06] ______, "Galois theory and Painlevé equations", in *Théories asymptotiques et équations de Painlevé* (Paris), Sémin. Congr., vol. 14, Soc. Math. France, 2006, p. 299–339.

[vdPS97] M. van der Put & M. F. Singer – *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997.

[vdPS03] ______, *Galois theory of linear differential equations*, Springer, Berlin, 2003.

Florian Heiderich, Institut de Mathématiques de Jussieu, Case 247, Université Pierre et Marie Curie, 4 place Jussieu, 75252 Paris Cedex 05 • *E-mail :* `heiderich@math.jussieu.fr`