GALOIS THEORY OF ARTINIAN SIMPLE MODULE ALGEBRAS

FLORIAN HEIDERICH

ABSTRACT. This main purpose of this article is the unification of the Galois theory of algebraic differential equations by Umemura and the Galois theory of algebraic difference equations by Morikawa-Umemura in a common framework using Artinian simple D-module algebras, where D is a bialgebra. We construct the Galois hull of an extension of Artinian simple D-module algebras and define its Galois group, which consists of infinitesimal coordinate transformations fulfilling certain partial differential equations and which we call Umemura functor. We eliminate the restriction to characteristic 0 from the above mentioned theories and remove the limitation to field extensions in the theory of Morikawa-Umemura, allowing also direct products of fields, which is essential in the theory of difference equations. In order to compare our theory with the Picard-Vessiot theory of Artinian simple D-module algebras due to Amano and Masuoka, we first slightly generalize the definition and some results about them in order to encompass as well non-inversive difference rings. Finally, we give equivalent characterizations for smooth Picard-Vessiot extensions, describe their Galois hull and show that their Umemura functor becomes isomorphic to the formal scheme associated to the classical Galois group scheme after a finite étale base extension.

INTRODUCTION

The idea behind differential Galois theory, namely to study differential equations using group theoretical methods, dates back to Lie. Picard and Vessiot realized a Galois theory for linear differential equations. Contemporary approaches to this theory can be found for example in [CH11] and [vdPS03]. The Galois groups in this theory are affine group schemes. After an attempt by Drach and work by Vessiot, Umemura developed a Galois theory for non-linear algebraic differential equations (cf. [Ume96]). To an extension of differential fields $L|K$ of characteristic 0 that is finitely generated as an extension of fields he associates a new extension $\mathcal{L}|\mathcal{K}$, the Galois hull of $L|K$, and attaches a group functor to it, the so called the infinitesimal Galois group of $L|K$. The latter is a Lie-Ritt functor, i.e. a group functor of infinitesimal transformations fulfilling certain partial differential equations, which turns out to also be a formal group scheme. A theory with a similar aim was developed by Malgrange in the framework of differential geometry and applied by Casale (cf. [Mal01], [Cas07], [Cas08]).

With a delay in time similar theories were realized for difference equations. The standard reference for Galois theory of linear difference equations is [vdPS97]. Recently, Umemura sketched a difference analogue of his differential Galois theory in [Ume06] and developed it together with Morikawa (cf. [Mor09], [MU09]). To an extension of difference fields $L|K$, i.e. fields equipped with an endomorphism, that is finitely generated as extension of fields they also assign an infinitesimal Galois group, which is a Lie-Ritt functor as in the differential case. Analogues of the theory of Malgrange for non-linear (q-)difference equations have been developed by Casale and Granier (cf. [Cas06], [Gra09]).

The purpose of this article is twofold. On the one hand, we unify the differential Galois theory of Umemura and the difference Galois theory of Morikawa-Umemura by using Artinian simple commutative D-module algebras, where D is a bialgebra. Differential fields and difference fields are special instances of Artinian simple commutative D-module algebras for certain choices of D. At the other hand, we generalize the theories of Morikawa and Umemura. We note first that most of the above mentioned theories have been restricted to characteristic 0. Hasse and Schmidt introduced higher and iterative derivations as a replacement for derivations in positive characteristic (cf. [HS37]) and, using them, differential Galois theories have been developed by Matzat, Okugawa and van der Put (cf. [Oku87], [MvdP03]). We first remove the restriction to characteristic 0 from the theories of Umemura and Morikawa-Umemura using iterative derivations instead of derivations. So our theory could be the starting point to tackle the problem raised by Morikawa and Umemura in [MU09] whether the results they obtain there have analogues in positive characteristic. Second, we eliminate the restriction to fields from the difference Galois theory of Morikawa-Umemura by also allowing direct products of fields equipped with an injective endomorphism (they are Artinian simple commutative D-module algebras for a particular choice of the bialgebra D). This approach is more natural, since the total Picard-Vessiot rings of difference equations are in general not difference fields, but only direct products of fields equipped with an endomorphism. Amano and Masuoka unified the Picard-Vessiot theories for differential and difference extensions by using Artinian simple commutative D-module algebras as well (cf. [AM05]). Though they restrict themselves to Hopf algebras D and therefore non-inversive difference extensions are not within their scope. Here we do not limit ourselves to Hopf algebras and use a broader class of bialgebras such that our theory encompasses as well non-inversive difference rings. In order to compare our general Galois group with the classical Galois group scheme of Picard-Vessiot extensions, we first define Picard-Vessiot extensions of Artinian simple commutative D-module algebras in a slightly more general context than Amano and Masuoka, i.e. without the assumption that D is a Hopf algebra, and show some of their basic properties. Finally, we prove that in the case of smooth Picard-Vessiot extensions of Artinian simple commutative D-module algebras our general Galois group is closely related to the usual Galois group scheme.

More precisely this article is organized as follows: In the first section we recall the definition of D-module algebras and some of their properties, where D is a bialgebra over a field C. We obtain some results about the extension of D-module algebra structures to tensor products and limits, which we need later. We close the section with the definition and equivalent characterizations of Artinian simple D-module algebras, generalizing results of Amano and Masuoka. The second

section is the heart of the article. We explain in detail the above-mentioned unification and generalization of the differential Galois theory of Umemura and the difference Galois theory of Morikawa and Umemura. Let G be a monoid and D^1 an irreducible pointed cocommutative Hopf algebra of Birkhoff-Witt type that is a CG-module bialgebra; we define D to be the smash product $D^1 \# CG$. If $L|K$ is an extension of Artinian simple commutative D-module algebras fulfilling a separability and finiteness condition, then we construct its Galois hull $\mathcal{L}|\mathcal{K}$ and associate to it a group functor $\mathrm{Ume}(L|K)$ on the category of commutative L-algebras that we call the Umemura functor in honor of its inventor in the case of extensions of differential fields. We show that the latter is a Lie-Ritt functor and so in particular a formal group scheme (cf. theorem 2.14). These constructions unify and generalize those of Umemura and Morikawa and, using the language of D-module algebras, arguments become more transparent. In section 3 we define Picard-Vessiot extensions of Artinian simple commutative D-module algebras and prove some of their properties, generalizing results of Amano and Masuoka, cf. [AM05], where they are proven in the case where D is a Hopf algebra satisfying some additional conditions. We close this section with a list of several equivalent characterizations of the property that the principal D-module algebra R of a Picard-Vessiot extension of Artinian simple commutative D-module algebras $L|K$ is smooth over K (cf. proposition 3.8). In the last section we investigate this type of Picard-Vessiot extensions by describing their Galois hull and by comparing the Umemura functor of such an extension with its Galois group scheme. Their Galois hull is of a particularly simple form (cf. lemma 4.1) and we show that the Umemura functor of this kind of extension becomes isomorphic to the formal group scheme associated to its Galois group scheme after a base extension to a finite étale extension of L (cf. theorem 4.3). This demonstrates that the Umemura functor in a way generalizes the Galois group scheme of Amano and Masuoka, though at the cost of generality some information is lost (we do not recover the Galois group scheme itself, but only a base extension of the formal group scheme associated to it). The construction of the Galois hull $\mathcal{L}|\mathcal{K}$, the Umemura functor $\mathrm{Ume}(L|K)$ and the comparison with the classical Galois group scheme $\mathrm{Gal}(L|K)$ are illustrated in two examples of simple Picard-Vessiot extensions of iterative differential fields.

This article develops further results of the authors thesis, where only extensions of D-module fields were considered (cf. [Hei10]).

Notation: *We assume all rings and algebras to be unital and associative, but not necessarily to be commutative. Homomorphisms of algebras are assumed to respect the units. We further assume that all coalgebras are counital and coassociative, but not necessarily to be cocommutative. Homomorphisms of coalgebras are assumed to respect the counits. An algebra (A, m, η) will be abbreviated by A and multiplication and unit will then be denoted by m_A and η_A, respectively. Similarly a coalgebra (D, Δ, ε) will be abbreviated by D and comultiplication and counit will then be denoted by Δ_D and ε_D, respectively. If D is a coalgebra and $d \in D$, then we use the Σ-notation $\Delta_D(d) = \sum_{(d)} d_{(1)} \otimes d_{(2)}$ (cf. [Swe69, Section 1.2] or [Mon93, 1.4.2]).*

If R is a commutative ring, then we denote by $\mathrm{Q}(R)$ the total ring of fractions of R, by $\Omega(R)$ the set of minimal prime ideals of R, by $N(R)$ the nilradical of R and by $\pi_R \colon R \to R/N(R)$ the canonical projection. We denote the category of commutative algebras over R by CAlg_R and the category of left R-modules by $_R\mathcal{M}$; furthermore Grp denotes the category of groups.

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 $\mathsf{C}(A, B)$. We denote the opposite category of C by C^{op}.

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 $f \in \mathsf{Set}(A, B)$. If $A' \subseteq A$ is a subset, then $\mathrm{res}_{A'}^A \colon \mathsf{Set}(A, B) \to \mathsf{Set}(A', B)$ denotes the restriction map. 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 $a \neq b$.

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

1. Module algebras

Notation: *Let C be a commutative ring.*

1.1. **Definitions and basic properties.** We recall that for C-modules A, B and D there is an isomorphism of C-modules

$$(1.1) \qquad {}_C\mathcal{M}(D \otimes_C A, B) \to {}_C\mathcal{M}(A, {}_C\mathcal{M}(D, B)), \quad \Psi \mapsto (a \mapsto (d \mapsto \Psi(d \otimes a))).$$

Lemma 1.1. *If $(D, \Delta_D, \varepsilon_D)$ is a C-coalgebra and (B, m_B, η_B) is a C-algebra, then the C-module ${}_C\mathcal{M}(D, B)$ becomes a C-algebra with respect to the* convolution *product, defined by*

$$f \cdot g := m_B \circ (f \otimes g) \circ \Delta_D$$

for $f, g \in {}_C\mathcal{M}(D, B)$, and unit element given by the composition

$$D \xrightarrow{\varepsilon_D} C \xrightarrow{\eta_B} B.$$

Furthermore, D is cocommutative if and only if ${}_C\mathcal{M}(D, B)$ is commutative for every commutative C-algebra B.

Proof. See for example [BW03, 1.3] $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Proposition 1.2. *Let D be a C-coalgebra and let A and B be C-algebras. If Ψ is an element of ${}_C\mathcal{M}(D \otimes_C A, B)$ and $\rho \in {}_C\mathcal{M}(A, {}_C\mathcal{M}(D, B))$ is the image of Ψ under the isomorphism (1.1), then the following are equivalent:*

(1) *ρ is a homomorphism of C-algebras,*
(2) *for all $d \in D$ and all $a, b \in A$*
  (a) *$\Psi(d \otimes ab) = \sum_{(d)} \Psi(d_{(1)} \otimes a) \Psi(d_{(2)} \otimes b)$ if $\Delta_D(d) = \sum_{(d)} d_{(1)} \otimes d_{(2)}$ and*
  (b) *$\Psi(d \otimes 1_A) = \varepsilon_D(d) 1_B$,*
  hold and
(3) *the diagrams*

$$
\begin{array}{ccccc}
D \otimes_C A \otimes_C A & \xrightarrow{\ \mathrm{id}_D \otimes m_A\ } & D \otimes_C A & \xrightarrow{\quad \Psi \quad} & B \\
{\scriptstyle \Delta_D \otimes \mathrm{id}_A \otimes \mathrm{id}_A} \downarrow & & & & \uparrow {\scriptstyle m_B} \\
D \otimes_C D \otimes_C A \otimes_C A & \xrightarrow{\mathrm{id}_D \otimes \tau \otimes \mathrm{id}_A} & D \otimes_C A \otimes_C D \otimes_C A & \xrightarrow{\ \Psi \otimes \Psi\ } & B,
\end{array}
$$

where $\tau \colon D \otimes_C A \to A \otimes_C D$ *is defined by* $\tau(d \otimes a) = a \otimes d$ *for all* $a \in A$ *and* $d \in D$, *and*

$$
\begin{array}{ccc}
D \otimes_C C & \xrightarrow{\varepsilon_D \otimes \eta_B} & C \otimes_C B \\
{\scriptstyle \mathrm{id}_D \otimes \eta_A} \downarrow & & \downarrow {\scriptstyle \sim} \\
D \otimes_C A & \xrightarrow{\ \Psi\ } & B
\end{array}
$$

commute.

Proof. The equivalence between (1) and (2) can be proven as in [Swe69, Proposition 7.0.1] and the one between (2) and (3) is clear. $\qquad\square$

Definition 1.3. *Let D be a C-coalgebra and A and B be C-algebras. If $\Psi \in {}_C\mathcal{M}(D \otimes_C A, B)$, then we say that Ψ measures A to B if the equivalent conditions in proposition 1.2 are satisfied.*

If A_1, A_2, B_1 and B_2 are C-algebras, $\Psi_1 \colon D \otimes_C A_1 \to B_1$ measures A_1 to B_1 and $\Psi_2 \colon D \otimes_C A_2 \to B_2$ measures A_2 to B_2, then we say that homomorphisms $\varphi_A \colon A_1 \to A_2$ and $\varphi_B \colon B_1 \to B_2$ of C-algebras are compatible with the measurings if the diagram

$$
\begin{array}{ccc}
D \otimes_C A_1 & \xrightarrow{\ \Psi_1\ } & B_1 \\
{\scriptstyle \mathrm{id}_D \otimes \varphi_A} \downarrow & & \downarrow {\scriptstyle \varphi_B} \\
D \otimes_C A_2 & \xrightarrow{\ \Psi_2\ } & B_2
\end{array}
$$

commutes.

The following lemmata are clear from the definition.

Lemma 1.4. *Let D be a C-bialgebra and A be a C-algebra. If $\Psi \in {}_C\mathcal{M}(D \otimes_C A, A)$ and $\rho \colon A \to {}_C\mathcal{M}(D, A)$ is the homomorphism associated to Ψ via (1.1), then Ψ makes A into a D-module if and only if the diagrams*

$$
\begin{array}{ccc}
A & \xrightarrow{\qquad\qquad \rho \qquad\qquad} & {}_C\mathcal{M}(D, A) \\
{\scriptstyle \rho} \downarrow & & \downarrow {\scriptstyle {}_C\mathcal{M}(D, \rho)} \\
{}_C\mathcal{M}(D, A) & \xrightarrow{{}_C\mathcal{M}(m_D, A)} & {}_C\mathcal{M}(D \otimes_C D, A) \cong {}_C\mathcal{M}(D, {}_C\mathcal{M}(D, A))
\end{array}
$$

and

$$
\begin{array}{ccc}
A & \xrightarrow{\ \rho\ } & {}_C\mathcal{M}(D, A) \\
& {\scriptstyle \mathrm{id}} \searrow & \downarrow {\scriptstyle \mathrm{ev}_{1_D}} \\
& & A
\end{array}
$$

commute.

Lemma 1.5. *Let D be a C-coalgebra and A_1, A_2, B_1 and B_2 be C-algebras. If $\Psi_1 \in {}_C\mathcal{M}(D \otimes_C A_1, B_1)$ measures A_1 to B_1 and $\Psi_2 \in {}_C\mathcal{M}(D \otimes_C A_2, B_2)$ measures A_2 to B_2 and ρ_1 and ρ_2 are the associated homomorphisms of C-algebras, then*

homomorphisms of C-algebras $\varphi_A \colon A_1 \to A_2$ and $\varphi_B \colon B_1 \to B_2$ are compatible with the measurings if and only if the diagram

$$\begin{array}{ccc} A_1 & \xrightarrow{\ \rho_1\ } & {}_C\mathcal{M}(D, B_1) \\ \downarrow{\scriptstyle\varphi_A} & & \downarrow{\scriptstyle {}_C\mathcal{M}(D,\varphi_B)} \\ A_2 & \xrightarrow{\ \rho_2\ } & {}_C\mathcal{M}(D, B_2) \end{array}$$

commutes.

Definition 1.6. *Let A be a C-algebra, D be a C-bialgebra and let $\Psi \in {}_C\mathcal{M}(D \otimes_C A, A)$ measure A to A. We say that Ψ is a* (left) D-module algebra structure *on A if Ψ makes A into a D-module (cf. lemma 1.4). The pair (A, Ψ) is then called* (left) D-module algebra.

A commutative D-module algebra *is a D-module algebra (A, Ψ) such that the C-algebra A is commutative.*

A homomorphism of D-module algebras *from (A_1, Ψ_1) to (A_2, Ψ_2) is a homomorphism of C-algebras $\varphi \colon A_1 \to A_2$ that fulfills the equivalent conditions of lemma 1.5 (with $B_1 = A_1$ and $B_2 = A_2$).*

Notation: *If $\Psi \colon D \otimes_C A \to B$ is a homomorphism of C-modules, then we denote by $\rho \colon A \to {}_C\mathcal{M}(D, B)$ the homomorphism corresponding to Ψ under the isomorphism (1.1) and vice versa. If $d \in D$ and $a \in A$, then we denote $\Psi(d \otimes a)$ also by $d.a$ or $d(a)$ if there is no danger of confusion.*

Definition 1.7. *For a C-coalgebra D, a C-module V and $\Psi \in {}_C\mathcal{M}(D \otimes_C V, V)$ we define the* constants *of V with respect to Ψ as*

$$V^\Psi := \{ v \in V \mid \Psi(d \otimes v) = \varepsilon_D(d) v \quad \text{for all } d \in D \}.$$

If $\rho \in {}_C\mathcal{M}(V, {}_C\mathcal{M}(D, V))$ is the element corresponding to Ψ under the isomorphism (1.1), then we denote V^Ψ also by V^ρ. Sometimes we will also denote it by V^D.

Example 1.8. *Let A be a commutative C-algebra.*

(1) *If $D_{der} := C[\mathbb{G}_a]$ is the Hopf algebra on the coordinate ring of the additive group scheme $\mathbb{G}_a$ over C, then D_{der}-module algebra structures on A are in 1-1 correspondence with C-derivations on A.*

If $\mathbb{Q} \subseteq A$, then ${}_C\mathcal{M}(D_{der}, A)$ is isomorphic to the formal power series ring $A[\![w]\!]$. If ∂ is a C-derivation on A, Ψ the corresponding D_{der}-module algebra structure on A and ρ is the homomorphism of C-algebras corresponding to Ψ via (1.1), then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{der}, A) \xrightarrow{\sim} A[\![w]\!]$ is given by $a \mapsto \sum_{k \in \mathbb{N}} \frac{\partial^k(a)}{k!} w^k$. This homomorphism appears in [Ume96] and is called universal Taylor homomorphism there.

In contrast, ${}_C\mathcal{M}(D_{der}, A)$ is not reduced in positive characteristic. It is isomorphic to the ring of so called Hurwitz series as defined by Keigher (cf. [Kei97]).

(2) *If $D_{aut} := C[\mathbb{G}_m]$ is the Hopf algebra on the coordinate ring of the multiplicative group scheme $\mathbb{G}_m$ over C, then D_{aut}-module algebra structures on A are in 1-1 correspondence with automorphisms of the C-algebra A.*

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, Ψ the corresponding D_{aut}-module algebra

structure and ρ the associated homomorphism via (1.1), 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) *If $D_{end} := C[t]$ is the polynomial algebra over C with coalgebra structure defined by $\Delta(t^n) = t^n \otimes t^n$ and $\varepsilon(t^n) = 1$ 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.*

The C-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, Ψ the corresponding D_{end}-module algebra structure and ρ the associated homomorphism via (1.1), 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 appears in [Mor09] and is called universal Euler homomorphism there.

(4) *For a monoid G we define a C-bialgebra CG by taking the monoid 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.*

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 $\Psi : CG \otimes_C A \to A$ is the CG-module algebra structure on A corresponding to an operation of G on A and $\rho : A \to {}_C\mathcal{M}(CG, A)$ the corresponding homomorphism, then the composition $A \to {}_C\mathcal{M}(CG, A) \to A^G$ is given by $a \mapsto (g \mapsto g.a)$.

In the cases $G = (\mathbb{N}, +)$ and $G = (\mathbb{Z}, +)$ we recover the situation in (2) and (3), respectively.

(5) *Let D_{ID} be the free C-module with basis consisting of $\theta^{(k)}$ for all $k \in \mathbb{N}$ with C-algebra structure defined by*

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

for all $i, j \in \mathbb{N}$ and C-coalgebra structure defined by

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

for all $i \in \mathbb{N}$. Then D_{ID} becomes a Hopf algebra with antipode defined by $S(\theta^{(i)}) = (-1)^i \theta^{(i)}$ and D_{ID}-module algebra structures on A are in 1-1 correspondence with iterative derivations on A over C (cf. [HS37] or [Mat89, §27]). We note that the bialgebras D_{der} and D_{ID} are isomorphic if $\mathbb{Q} \subseteq C$. Therefore derivations and iterative derivations are equivalent on $\mathbb{Q}$-algebras.

The C-algebra ${}_C\mathcal{M}(D_{ID}, A)$ is isomorphic to $A[\![w]\!]$ and if $(\theta^{(k)})_{k \in \mathbb{N}}$ is an iterative derivation on A over C, Ψ the induced D_{ID}-module algebra structure and ρ the associated homomorphism of C-algebras, then the composition $A \xrightarrow{\rho} {}_C\mathcal{M}(D_{ID}, A) \xrightarrow{\sim} A[\![w]\!]$ is given by $a \mapsto \sum_{k \in \mathbb{N}} \theta^{(k)}(a)w^k$. We will identify an iterative derivation with this homomorphism as in [Hei07].

We note that there are differences in the definition of higher derivations. In [Mat89], [Hei07] and [Hei10] a condition on $\theta^{(0)}$ is posed, which is not present in [Swe69]. Using the definition of Sweedler, higher derivation from

A to another commutative C-algebra B are in 1-1 correspondence with D_{ID}-measurings from A to B. When B is a commutative A-algebra via $A \xrightarrow{g} B$, then higher derivations (of length ∞) in the sense of Matsumura (cf. [Mat89, §27]) are in 1-1 correspondence with D_{ID}-measurings from A to B such that the associated homomorphism of C-algebras $\rho \colon A \to {}_C\mathcal{M}(D, B)$ fulfills $\mathrm{ev}_{1_D} \circ \rho = g$.

(6) For all $m \in \mathbb{N}$ we define $D_{HD_{(m)}}$ as the free C-module with basis consisting of $\theta^{(0)}, \ldots, \theta^{(m)}$ and equip it with a C-coalgebra structure defined by

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

for all $i \in \{0, \ldots, m\}$. Then $D_{HD_{(m)}}$-measurings from A to another commutative C-algebra B are in 1-1 correspondence with higher derivations of length m from A to B over C in the sense of Sweedler (cf. [Swe69]).

Let now B be a commutative A-algebra via $A \xrightarrow{g} B$. Then higher derivations of length m in the sense of Matsumura (cf. [Mat89, §27]) are in 1-1 correspondence with $D_{HD_{(m)}}$-measurings from A to B such that the associated homomorphism of C-algebras $\rho \colon A \to {}_C\mathcal{M}(D, B)$ fulfills $\mathrm{ev}_{1_D} \circ \rho = g$. We note that D_{ID} is isomorphic to $\varinjlim_{m \in \mathbb{N}} D_{HD_{(m)}}$ as C-coalgebra.

The C-algebra ${}_C\mathcal{M}(D_{HD_{(m)}}, B)$ is isomorphic to $B[\![w]\!]/(w^{m+1})$ and if $(\theta^{(k)})_{k=0,\ldots,m}$ is a higher derivation of length m from A to B over C, Ψ is the induced $D_{HD_{(m)}}$-measuring and ρ the associated homomorphism, then the composition $\rho \colon A \to {}_C\mathcal{M}(D_{HD_{(m)}}, B) \xrightarrow{\sim} B[\![w]\!]/(w^{m+1})$ is given by $a \mapsto \sum_{k=0}^{m} \theta^{(k)}(a)w^k + (w^{m+1})$.

(7) For every 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

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

We call Ψ_0 the trivial D-module algebra structure on A.

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 $d \in D$.

If D and D' are C-bialgebras, then $D \otimes_C D'$ becomes a C-bialgebra with the usual C-algebra structure and the coalgebra structure defined by

$$(1.2) \quad \Delta(d \otimes d') \coloneqq \sum_{(d),(d')} d_{(1)} \otimes d'_{(1)} \otimes d_{(2)} \otimes d'_{(2)} \quad and \quad \varepsilon(d \otimes d') \coloneqq \varepsilon(d)\varepsilon(d').$$

A pair of commuting D- and D'-module algebra structures on a C-algebra A gives rise to a $D \otimes_C D'$-module algebra structure on A and vice versa.

For every $n \in \mathbb{N}$ the tensor product $D_{ID^n} \coloneqq D_{ID}^{\otimes_C^n}$ is a cocommutative Hopf algebra and D_{ID^n}-module algebra structures correspond to systems of n commuting iterative derivations, which we call n-variate iterative derivations (cf. [Hei07] or [Mau10]). Furthermore, D_{ID^n}-measures from R to itself such that $1_{D_{ID^n}}.a = a$ for all $a \in R$ correspond 1-1 to n-variate higher derivations on R in the sense

of [Hei07]. Similarly, we define for $n \in \mathbb{N}$ and $\boldsymbol{m} = (m_1, \ldots, m_n) \in \mathbb{N}^n$ the C-coalgebra $D_{HD^n_{(\boldsymbol{m})}} := D_{HD_{(m_1)}} \otimes_C \cdots \otimes_C D_{HD_{(m_n)}}$ and note that D_{ID^n} is isomorphic to $\varinjlim_{\boldsymbol{m} \in \mathbb{N}^n} D_{HD^n_{(\boldsymbol{m})}}$ as C-coalgebra.

Notation: *For C-bialgebras D_1 and D_2 and C-algebras A we often make implicitly use of the isomorphism of C-algebras*

$$(1.3) \qquad {}_C\mathcal{M}(D_2, {}_C\mathcal{M}(D_1, A)) \cong {}_C\mathcal{M}(D_1 \otimes_C D_2, A) \cong {}_C\mathcal{M}(D_1, {}_C\mathcal{M}(D_2, A)).$$

Lemma 1.9. *Let D be a C-bialgebra and A a be C-algebra.*

(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

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

For any homomorphism of C-algebras $\varphi \colon A \to B$ the induced homomorphism of C-algebras

$${}_C\mathcal{M}(D, \varphi) \colon {}_C\mathcal{M}(D, A) \to {}_C\mathcal{M}(D, B)$$

is a homomorphism of D-module algebras with respect to the D-module algebra structures on ${}_C\mathcal{M}(D, A)$ and ${}_C\mathcal{M}(D, B)$ given by Ψ_{int}. Thus, ${}_C\mathcal{M}(D, -)$ is a functor from the category of C-algebras to the category of D-module algebras.

(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 1.8 (7)).*

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

$$(1.4) \qquad {}_C\mathcal{M}(D, \rho') \colon {}_C\mathcal{M}(D, A) \to {}_C\mathcal{M}(D, {}_C\mathcal{M}(D', A)) \cong {}_C\mathcal{M}(D', {}_C\mathcal{M}(D, A)).$$

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.

Proof. We note that the homomorphism of C-modules

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

associated to Ψ_{int} via the isomorphism (1.1), corresponds to

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

under the isomorphism of C-algebras (1.3). Since m_D is a homomorphism of C-coalgebras, ${}_C\mathcal{M}(m_D, A)$ and therefore also ρ_{int} are homomorphisms of C-algebras. The diagram

$$\begin{array}{ccc} {}_C\mathcal{M}(D, A) & \xrightarrow{\ \rho_{int}\ } & {}_C\mathcal{M}(D, {}_C\mathcal{M}(D, A)) \\ & {}_{\text{id}} \searrow & \downarrow {}^{\text{ev}_{1_D}} \\ & & {}_C\mathcal{M}(D, A) \end{array}$$

obviously commutes. Using again the isomorphism (1.3), the commutativity of the diagram

$$
\begin{array}{ccc}
{}_C\mathcal{M}(D,A) & \xrightarrow{\;\;\rho_{int}\;\;} & {}_C\mathcal{M}(D,{}_C\mathcal{M}(D,A)) \\
\downarrow{\scriptstyle\rho_{int}} & & \downarrow{\scriptstyle {}_C\mathcal{M}(D,\rho_{int})} \\
{}_C\mathcal{M}(D,{}_C\mathcal{M}(D,A)) & \xrightarrow{{}_C\mathcal{M}(m_D,{}_C\mathcal{M}(D,A))} & {}_C\mathcal{M}(D\otimes_C D,{}_C\mathcal{M}(D,A))
\end{array}
$$

follows from the associativity of D. Therefore, Ψ_{int} is in fact a D-module algebra structure on ${}_C\mathcal{M}(D,A)$. For a homomorphism of C-algebras $\varphi\colon A \to B$, the big rectangle and the square on the right in the diagram

$$
\begin{array}{ccccc}
 & & & {}_C\mathcal{M}(m_D,A) & \\
{}_C\mathcal{M}(D,A) & \xrightarrow{\rho_{int}} & {}_C\mathcal{M}(D,{}_C\mathcal{M}(D,A)) & \xrightarrow{\;\sim\;} & {}_C\mathcal{M}(D\otimes_C D,A) \\
\downarrow{\scriptstyle {}_C\mathcal{M}(D,\varphi)} & & \downarrow{\scriptstyle {}_C\mathcal{M}(D,{}_C\mathcal{M}(D,\varphi))} & & \downarrow{\scriptstyle {}_C\mathcal{M}(D\otimes_C D,\varphi)} \\
{}_C\mathcal{M}(D,B) & \xrightarrow{\rho_{int}} & {}_C\mathcal{M}(D,{}_C\mathcal{M}(D,B)) & \xrightarrow{\;\sim\;} & {}_C\mathcal{M}(D\otimes_C D,B) \\
 & & & {}_C\mathcal{M}(m_D,B) &
\end{array}
$$

commute and thus the rectangle on the left commutes too, i.e. ${}_C\mathcal{M}(D,\varphi)$ is a homomorphism of D-module algebras with respect to the D-module algebra structures given by Ψ_{int} on ${}_C\mathcal{M}(D,A)$ and ${}_C\mathcal{M}(D,B)$.

To prove part (2), let $f \in {}_C\mathcal{M}(D,A)$. Then f is constant with respect to Ψ_{int} if and only if $f(d) = (\Psi_{int}(d\otimes f))(1) = \varepsilon_D(d)f(1)$ for all $d \in D$, i.e. if and only if $f = \rho_0(f(1))$.

It is clear that ${}_C\mathcal{M}(D,\rho')$ induces a D'-module algebra structure on ${}_C\mathcal{M}(D,A)$, which we denote again by Ψ'. Then we have for all $f \in {}_C\mathcal{M}(D,A), d,\tilde{d} \in D$ and $d' \in D'$

$$
\Psi'(d' \otimes \Psi_{int}(d\otimes f))(\tilde{d}) = \Psi'(d'\otimes f(\tilde{d}d)) = \Psi_{int}(d\otimes \Psi'(d'\otimes f)(\tilde{d})).
$$

$\square$

Lemma 1.10. *Given a C-bialgebra D, a D-module algebra structure $\Psi \in {}_C\mathcal{M}(D\otimes_C A, A)$ on A, the associated homomorphism $\rho\colon A \to {}_C\mathcal{M}(D,A)$ is a homomorphism of D-module algebras from (A,Ψ) to $({}_C\mathcal{M}(D,A),\Psi_{int})$. The homomorphism ρ is universal among all homomorphisms of D-module algebras $\Lambda\colon (A,\Psi) \to ({}_C\mathcal{M}(D,B),\Psi_{int})$, where B is a C-algebra, in the sense that for every such Λ there exists a unique homomorphism of C-algebras $\lambda\colon A \to B$ such that $\Lambda = {}_C\mathcal{M}(D,\lambda) \circ \rho$.*

Proof. Since ${}_C\mathcal{M}(D,\rho) \circ \rho = {}_C\mathcal{M}(m_D,A) \circ \rho$ and since the homomorphism of C-algebras ρ_{int} associated to Ψ_{int} corresponds to ${}_C\mathcal{M}(m_D,A)$ under the isomorphism of C-algebras (1.3), we see that ρ is in fact a D-module algebra homomorphism from (A,Ψ) to $({}_C\mathcal{M}(D,A),\Psi_{int})$. To show the universality of ρ, let $\Lambda\colon (A,\Psi) \to ({}_C\mathcal{M}(D,B),\Psi_{int})$ be a homomorphism of D-module algebras. We define $\lambda := \mathrm{ev}_{1_D} \circ \Lambda$ and obtain ${}_C\mathcal{M}(D,\lambda) \circ \rho = {}_C\mathcal{M}(D,\mathrm{ev}_{1_D}) \circ {}_C\mathcal{M}(D,\Lambda) \circ \rho = {}_C\mathcal{M}(D,\mathrm{ev}_{1_D}) \circ \rho_{int} \circ \Lambda = \Lambda$. $\square$

For $D = D_{der}$ and $D = D_{end}$ one recoveres as corollaries [Ume96, Proposition 1.4] and [Mor09, Propositions 2.5 and 2.7].

1.2. Extensions of module algebra structures.

Proposition 1.11. *Let D be a cocommutative C-bialgebra,*

$$(S, \Psi_S) \leftarrow (R, \Psi_R) \rightarrow (T, \Psi_T)$$

be a diagram in the category of commutative D-module algebras. Then $S \otimes_R T$ carries a unique D-module algebra structure Ψ such that $(S \otimes_R T, \Psi)$ becomes the coproduct of (S, Ψ_S) and (T, Ψ_T) over (R, Ψ_R) in the category of commutative D-module algebras. This D-module algebra structure on $S \otimes_R T$ is given as

$$(1.5) \quad \Psi \colon D \otimes_C S \otimes_R T \rightarrow S \otimes_R T, \qquad d \otimes s \otimes t \mapsto \sum_{(d)} \Psi_S(d_{(1)} \otimes s) \otimes \Psi_T(d_{(2)} \otimes t).$$

Proof. Since D is cocommutative and R, S and T are commutative C-algebras, the C-algebras ${}_C\mathcal{M}(D, R)$, ${}_C\mathcal{M}(D, S)$ and ${}_C\mathcal{M}(D, T)$ are commutative. We denote the C-algebra homomorphisms associated to Ψ_R, Ψ_S and Ψ_T via the bijection (1.1) by ρ_R, ρ_S and ρ_T, respectively. By the universal property of the coproduct $S \otimes_R T$ in the category of commutative C-algebras, there exists a unique homomorphism $\rho \colon S \otimes_R T \rightarrow {}_C\mathcal{M}(D, S \otimes_R T)$ of C-algebras that makes the diagram

$$
\begin{array}{ccc}
& S \xrightarrow{\quad \rho_S \quad} {}_C\mathcal{M}(D, S) & \\
R & S \otimes_R T \xrightarrow{\ \rho\ } {}_C\mathcal{M}(D, S \otimes_R T) & \\
& T \xrightarrow{\quad \rho_T \quad} {}_C\mathcal{M}(D, T) &
\end{array}
$$

commutative. This homomorphism gives rise to a D-module algebra structure on $S \otimes_R T$, since the diagrams

$$
\begin{array}{ccc}
S \otimes_R T & \xrightarrow{\ \rho\ } & {}_C\mathcal{M}(D, S \otimes_R T) \\
& \searrow^{\text{id}} & \downarrow^{\text{ev}_{1_D}} \\
& & S \otimes_R T
\end{array}
$$

and

$$
\begin{array}{ccc}
S \otimes_R T & \xrightarrow{\quad\quad \rho \quad\quad} & {}_C\mathcal{M}(D, S \otimes_R T) \\
\downarrow^{\rho} & & \downarrow^{{}_C\mathcal{M}(D, \rho)} \\
{}_C\mathcal{M}(D, S \otimes_R T) & \xrightarrow{{}_C\mathcal{M}(m_D, S \otimes_R T)} & {}_C\mathcal{M}(D, {}_C\mathcal{M}(D, S \otimes_R T))
\end{array}
$$

commute (which also follows from the universal property of $S \otimes_R T$). Using the universal property of $S \otimes_R T$ again, we see that $(S \otimes_R T, \Psi)$ is in fact the coproduct of (S, Ψ_S) and (T, Ψ_T) over (R, Ψ_R) in the category of commutative D-module algebras.

Since $S \rightarrow S \otimes_R T, s \mapsto s \otimes 1$ and $T \rightarrow S \otimes_R T, t \mapsto 1 \otimes t$ are homomorphisms of D-module algebras, we have $\Psi(d \otimes s \otimes 1) = \Psi_S(d \otimes s) \otimes 1$ and $\Psi(d \otimes 1 \otimes t) = 1 \otimes \Psi_T(d \otimes t)$ for all $s \in S, t \in T$ and $d \in D$. Since Ψ measures $S \otimes_R T$ to itself, it follows $\Psi(d \otimes s \otimes t) = \sum_{(d)} \Psi_S(d_{(1)} \otimes s) \otimes \Psi_T(d_{(2)} \otimes t)$. $\qquad\square$

Notation: *In the situation of proposition 1.11 we denote by abuse of notation the D-module algebra structure on $S \otimes_R T$ by $\rho_S \otimes \rho_T$.*

Proposition 1.12. *(1) Let I and J be two small categories,*

$$R\colon J^{op} \to \mathsf{CAlg}_C \quad and \quad S\colon I^{op} \to \mathsf{CAlg}_C$$

be two functors. We write R_j and S_i instead of $R(j)$ and $S(i)$ for $j \in J$ and $i \in I$, respectively. Let Γ be a small category and $\tilde{D}$ be a functor from Γ to the category of cocommutative C-coalgebras and let D be the colimit of $\tilde{D}$, i.e. $D = \varinjlim_{\gamma \in \Gamma} \tilde{D}(\gamma)$. We denote $\tilde{D}(\gamma)$ by D_γ. Let

$$\alpha\colon (I \times \Gamma)^{op} \to J^{op}$$

be a functor and suppose that for every $i \in I$ and every $\gamma \in \Gamma$ the C-coalgebra D_γ measures $R_{\alpha(i,\gamma)}$ to S_i and denote the associated homomorphism of C-algebras by

$$\rho_{i,\gamma}\colon R_{\alpha(i,\gamma)} \to {}_C\mathcal{M}(D_\gamma, S_i).$$

We suppose that these measurings are compatible in the sense that for every morphism $i_1 \to i_2$ in I and $\gamma_1 \to \gamma_2$ in Γ the diagram

$$
\begin{array}{ccc}
R_{\alpha(i_2,\gamma_2)} & \xrightarrow{\;\rho_{i_2,\gamma_2}\;} & {}_C\mathcal{M}(D_{\gamma_2}, S_{i_2}) \\
\downarrow & & \downarrow \\
R_{\alpha(i_1,\gamma_1)} & \xrightarrow{\;\rho_{i_1,\gamma_1}\;} & {}_C\mathcal{M}(D_{\gamma_1}, S_{i_1})
\end{array}
$$

commutes. [1] Then there exists a unique D-measure from $\hat{R} := \varprojlim_{j \in J^{op}} R_j$ to $\hat{S} := \varprojlim_{i \in I^{op}} S_i$ with associated homomorphism $\hat{\rho}\colon \hat{R} \to {}_C\mathcal{M}(D, \hat{S})$ such that

$$
\begin{array}{ccc}
\hat{R} & \xrightarrow{\;\hat{\rho}\;} & {}_C\mathcal{M}(D, \hat{S}) \\
{\scriptstyle \pi_{\alpha(i,\gamma)}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}^D_{D_\gamma} \circ\, {}_C\mathcal{M}(D,\pi_i)} \\
R_{\alpha(i,\gamma)} & \xrightarrow{\;\rho_{i,\gamma}\;} & {}_C\mathcal{M}(D_\gamma, S_i)
\end{array}
$$

commutes for all $i \in I$ and $\gamma \in \Gamma$, where $\pi_j\colon \hat{R} \to R_j$ and $\pi_i\colon \hat{S} \to S_i$ denote the projections.

(2) We assume in addition that there are compatible homomorphisms $\eta_{D_\gamma}\colon C \to D_\gamma$ such that $1_{D_\gamma} := \eta_{D_\gamma}(1_C)$ fulfills $\Delta_{D_\gamma}(1_{D_\gamma}) = 1_{D_\gamma} \otimes 1_{D_\gamma}$ and $\varepsilon_{D_\gamma}(1_{D_\gamma}) = 1_C$ for all $\gamma \in \Gamma$. Furthermore, we assume that there is a natural transformation from the functor $R \circ \alpha$ to S (both are considered as functors from $(I \times \Gamma)^{op}$ to CAlg_C, where S does not depend on the second factor), giving rise to homomorphisms of C-algebras

$$R_{\alpha(i,\gamma)} \to S_i \tag{1.6}$$

for all $i \in I$ and $\gamma \in \Gamma$ and thus to a homomorphism

$$\hat{R} \to \hat{S}. \tag{1.7}$$

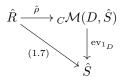[1]This amounts to giving a natural transformation from the functor $R \circ \alpha\colon (I \times \Gamma)^{op} \to \mathsf{CAlg}_C, (i,\gamma) \mapsto R_{\alpha(i,\gamma)}$ to the functor $(I \times \Gamma)^{op} \to \mathsf{CAlg}_C, (i,\gamma) \mapsto {}_C\mathcal{M}(D_\gamma, S_i)$.

If the diagram

$$R_{\alpha(i,\gamma)} \xrightarrow{\rho_{i,\gamma}} {}_C\mathcal{M}(D_\gamma, S_i)$$

$$(1.6) \qquad \downarrow \mathrm{ev}_{1_{D_\gamma}}$$

$$S_i$$

commutes for all $i \in I$ and $\gamma \in \Gamma$, then $\hat{\rho}$ makes the diagram

$$\hat{R} \xrightarrow{\hat{\rho}} {}_C\mathcal{M}(D, \hat{S})$$

$$(1.7) \qquad \downarrow \mathrm{ev}_{1_D}$$

$$\hat{S}$$

commutative.

(3) *We assume furthermore that D is a (cocommutative) C-bialgebra, that $I = J$, that $R = S$ and that there is a functor $\mu \colon \Gamma \times \Gamma \to \Gamma, (\gamma, \tilde{\gamma}) \mapsto \mu_{\gamma\tilde{\gamma}}$ and a natural transformation from $(\tilde{D} \otimes_C \tilde{D}) \colon \Gamma \times \Gamma \to \mathsf{CAlg}_C, (\gamma, \tilde{\gamma}) \mapsto \tilde{D}(\gamma) \otimes_C \tilde{D}(\tilde{\gamma})$ to $\tilde{D} \circ \mu$ inducing homomorphisms $m_{\gamma,\tilde{\gamma}} \colon D_\gamma \otimes_C D_{\tilde{\gamma}} \to D_{\mu_{\gamma,\tilde{\gamma}}}$ that are compatible with the multiplication m_D in the sense that the diagram*

$$(1.8) \qquad \begin{array}{ccc} D \otimes_C D & \xrightarrow{m_D} & D \\ \uparrow & & \uparrow \\ D_\gamma \otimes_C D_{\tilde{\gamma}} & \xrightarrow{m_{\gamma,\tilde{\gamma}}} & D_{\mu_{\gamma,\tilde{\gamma}}} \end{array}$$

commutes for all $\gamma, \tilde{\gamma} \in \Gamma$. If the diagram

$$(1.9) \qquad \begin{array}{ccc} R_{\alpha(\alpha(i,\mu_{\gamma,\tilde{\gamma}}),\mu_{\gamma,\tilde{\gamma}})} \longrightarrow R_{\alpha(\alpha(i,\gamma)),\tilde{\gamma}} \xrightarrow{\rho_{\alpha(i,\gamma),\tilde{\gamma}}} {}_C\mathcal{M}(D_{\tilde{\gamma}}, R_{\alpha(i,\gamma)}) \\ \downarrow \qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow {}_C\mathcal{M}(D_{\tilde{\gamma}},\rho_{i,\gamma}) \\ R_{\alpha(i,\mu_{\gamma,\tilde{\gamma}})} \\ \downarrow \rho_{i,\mu_{\gamma,\tilde{\gamma}}} \\ {}_C\mathcal{M}(D_{\mu_{\gamma,\tilde{\gamma}}}, R_i) \xrightarrow{{}_C\mathcal{M}(m_{\gamma,\tilde{\gamma}},R_i)} {}_C\mathcal{M}(D_\gamma \otimes_C D_{\tilde{\gamma}}, R_i), \end{array}$$

where the vertical homomorphism with source the top left corner is an instance of (1.6), commutes for all $\gamma, \tilde{\gamma} \in \Gamma$ and $i \in I$, then the D-measure from $\hat{R}$ to itself above is a D-module algebra structure.

Furthermore, $(\hat{R}, \hat{\rho})$ has the following universal mapping property: Given a D-module algebra (T, ρ_T) and compatible homomorphisms $(\varphi_i \colon T \to R_i)_{i \in I}$ such that
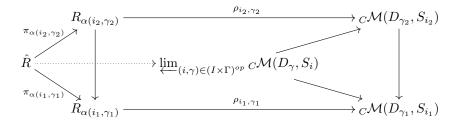
$$(1.10) \qquad \mathrm{res}^D_{D_\gamma} \circ {}_C\mathcal{M}(D, \varphi_i) \circ \rho_T = \rho_{i,\gamma} \circ \varphi_{\alpha(i,\gamma)}$$

for all $i \in I$ and $\gamma \in \Gamma$, there exists a unique homomorphism of D-module algebras $\Phi \colon T \to \hat{R}$ such that $\pi_i \circ \Phi = \varphi_i$ for all $i \in I$.

Proof. The universal mapping property of the limit $\varprojlim_{(i,\gamma)\in(I\times\Gamma)^{op}} {}_C\mathcal{M}(D_\gamma, S_i)$ provides a unique homomorphism of C-algebras

$$(1.11) \qquad \hat{R} \to \varprojlim_{(i,\gamma)\in(I\times\Gamma)^{op}} {}_C\mathcal{M}(D_\gamma, S_i)$$
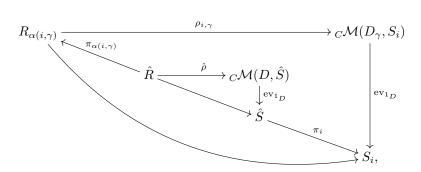
such that the diagram

commutes for all $i_1 \to i_2$ in I and all $\gamma_1 \to \gamma_2$ in Γ. Since the functor ${}_C\mathcal{M}(D,-)$ preserves limits of C-modules and since the functors ${}_C\mathcal{M}(-,S_i)$ turn colimits into limits (cf. [Mac71, V.4]), we have an isomorphism

$$(1.12) \qquad \varprojlim_{(i,\gamma)\in(I\times\Gamma)^{op}} {}_C\mathcal{M}(D_\gamma, S_i) \cong {}_C\mathcal{M}(\varinjlim_{\gamma\in\Gamma} D_\gamma, \varprojlim_{i\in I^{op}} S_i) = {}_C\mathcal{M}(D, \hat{S}),$$

which is a homomorphism of C-algebras. By composing (1.11) and (1.12), we obtain a homomorphism of C-algebras
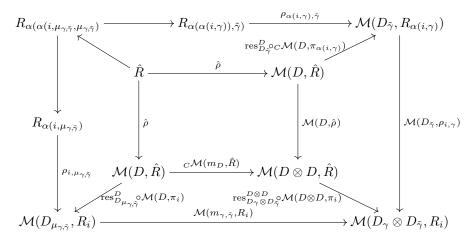
$$\hat{\rho}\colon \hat{R} \to {}_C\mathcal{M}(D, \hat{S}).$$

For the proof of part (2) we note that the outer triangle in the diagram

where the unlabeled arrows are (1.6) and (1.7), commutes by assumption for all $i \in I$ and $\gamma \in \Gamma$. Therefore, the inner triangle also commutes by the universal mapping property of the limit $\hat{S} = \varprojlim_{i\in I^{op}} S_i$.

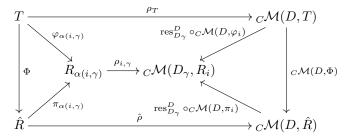By the assumption in part (3) the outer rectangle in the diagram

$$
\begin{array}{ccccc}
R_{\alpha(\alpha(i,\mu_{\gamma,\tilde\gamma},\mu_{\gamma,\tilde\gamma})} & \longrightarrow & R_{\alpha(\alpha(i,\gamma)),\tilde\gamma} & \xrightarrow{\ \rho_{\alpha(i,\gamma),\tilde\gamma}\ } & \mathcal{M}(D_{\tilde\gamma}, R_{\alpha(i,\gamma)}) \\
\end{array}
$$

with $\hat R \xrightarrow{\hat\rho} \mathcal{M}(D,\hat R)$, $\mathrm{res}^D_{D_{\tilde\gamma}}\circ{}_C\mathcal{M}(D,\pi_{\alpha(i,\gamma)})$,

$R_{\alpha(i,\mu_{\gamma,\tilde\gamma})}$, $\hat\rho$, $\mathcal{M}(D,\hat\rho)$, $\mathcal{M}(D_{\tilde\gamma},\rho_{i,\gamma})$,

$\rho_{i,\mu_{\gamma,\tilde\gamma}}$, $\mathcal{M}(D,\hat R) \xrightarrow{{}_C\mathcal{M}(m_D,\hat R)} \mathcal{M}(D\otimes D,\hat R)$,

$\mathrm{res}^D_{D_{\mu_{\gamma,\tilde\gamma}}}\circ\mathcal{M}(D,\pi_i)$, $\mathrm{res}^{D\otimes D}_{D_\gamma\otimes D_{\tilde\gamma}}\circ\mathcal{M}(D\otimes D,\pi_i)$,

$\mathcal{M}(D_{\mu_{\gamma,\tilde\gamma}}, R_i) \xrightarrow{\mathcal{M}(m_{\gamma,\tilde\gamma},R_i)} \mathcal{M}(D_\gamma\otimes D_{\tilde\gamma}, R_i)$

commutes for all $i \in I$ and $\gamma, \tilde\gamma \in \Gamma$, where all tensor products are over C and where we abbreviate ${}_C\mathcal{M}$ by $\mathcal{M}$. The trapezoids commute, since the projections $\pi_i \colon \hat R \to R_i$ are compatible with the D-measurings and since (1.8) commutes. Thus, by the universal mapping property of

$$
{}_C\mathcal{M}(D \otimes_C D, \hat R) \cong \varprojlim_{(i,\gamma,\tilde\gamma)\in(I\times\Gamma\times\Gamma)^{op}} {}_C\mathcal{M}(D_\gamma \otimes_C D_{\tilde\gamma}, R_i),
$$

the inner rectangle also commutes and we see that $\hat R$ is a D-module algebra.

If $\varphi_i \colon T \to R_i$ are compatible homomorphisms such that (1.10) holds, then, by the universal property of $\hat R = \varprojlim_{i\in I^{op}} R_i$ in the category of commutative C-algebras, there exists a homomorphism of C-algebras $\Phi \colon T \to \hat R$ such that $\pi_i \circ \Phi = \varphi_i$ and so the triangles at the left and right in the diagram

$$
\begin{array}{ccc}
T & \xrightarrow{\ \rho_T\ } & {}_C\mathcal{M}(D,T) \\
\end{array}
$$

with $\varphi_{\alpha(i,\gamma)}$, $\mathrm{res}^D_{D_\gamma}\circ{}_C\mathcal{M}(D,\varphi_i)$,

Φ, $R_{\alpha(i,\gamma)} \xrightarrow{\rho_{i,\gamma}} {}_C\mathcal{M}(D_\gamma, R_i)$, ${}_C\mathcal{M}(D,\Phi)$,

$\pi_{\alpha(i,\gamma)}$, $\mathrm{res}^D_{D_\gamma}\circ{}_C\mathcal{M}(D,\pi_i)$,

$\hat R \xrightarrow{\hat\rho} {}_C\mathcal{M}(D,\hat R)$

commute for all $i \in I$. The two trapezoids at the top and bottom commute by assumption and by the previously shown, respectively. By the universal property of ${}_C\mathcal{M}(D,\hat R) \cong \varprojlim_{(i,\gamma)\in(I\times\Gamma)^{op}} {}_C\mathcal{M}(D_\gamma, R_i)$ we obtain ${}_C\mathcal{M}(D,\Phi) \circ \rho_T = \hat\rho \circ \Phi$, i.e. Φ is a homomorphism of D-module algebras. □

Corollary 1.13. *Let D be a cocommutative C-bialgebra. Then small inverse systems of D-module algebras have inverse limits.*

Proof. This follows from proposition 1.12 by taking $I = J$, $R = S$, the category Γ to consists of exactly one object γ and one morphism id_γ and $D_\gamma = D$ and by defining $\alpha \colon I^{op} \times \Gamma^{op} \to I^{op}$ by $\alpha(i,\gamma) = i$ for all $i \in I$. □

Corollary 1.14. *Let R be a linear topological ring with fundamental system of neighborhoods $\mathcal{B}$ of 0. Let Γ be a small category and $\tilde{D}$ be a functor from Γ to the category of cocommutative C-coalgebras and let D be the colimit of $\tilde{D}$, i.e. $D = \varinjlim_{\gamma \in \Gamma} \tilde{D}(\gamma)$. We denote $\tilde{D}(\gamma)$ by D_γ. Let $\Psi \in {}_C\mathcal{M}(D \otimes_C R, R)$ measure R to R and assume that the associated homomorphism of C-algebras $\rho\colon R \to {}_C\mathcal{M}(D, R)$ is continuous with respect to the given topology on R and the linear topology on ${}_C\mathcal{M}(D, R)$ with fundamental system of neighborhoods of 0 given by the ideals*

$$({}_C\mathcal{M}(D, I), \mathrm{Ker}({}_C\mathcal{M}(D, R) \to {}_C\mathcal{M}(D_\gamma, R)))$$

for all $I \in \mathcal{B}$ and $\gamma \in \Gamma$. Then Ψ uniquely extends to a D-measure $\hat{\Psi} \in {}_C\mathcal{M}(D \otimes_C \hat{R}, \hat{R})$ from $\hat{R} := \varprojlim_{I \in \mathcal{B}} R/I$ to itself and the associated homomorphism of C-algebras $\hat{\rho}\colon \hat{R} \to {}_C\mathcal{M}(D, \hat{R})$ is continuous with respect to the induced topology on $\hat{R}$ and the linear topology on ${}_C\mathcal{M}(D, \hat{R})$ with fundamental system of neighborhoods of 0 given by the ideals

$$({}_C\mathcal{M}(D, \hat{I}), \mathrm{Ker}({}_C\mathcal{M}(D, \hat{R}) \to {}_C\mathcal{M}(D_\gamma, \hat{R})))$$

for all $\hat{I} \in \hat{\mathcal{B}}$ and $\gamma \in \Gamma$, where $\hat{\mathcal{B}}$ is a fundamental system of neighborhoods of $0 \in \hat{R}$.

If for every $\gamma \in \Gamma$ there is a homomorphism η_{D_γ} as in proposition 1.12 (2) such that $1_{D_\gamma} := \eta_{D_\gamma}(1_C)$ fulfills $\Psi(1_{D_\gamma} \otimes a) = a$ for all $a \in R$, then $\hat{\Psi}(1_D \otimes a) = a$ holds for all $a \in \hat{R}$.

We furthermore assume the existence of a functor $\mu\colon \Gamma \times \Gamma \to \Gamma$ and homomorphisms $m_{\gamma_1, \gamma_2}\colon D_{\gamma_1} \otimes_C D_{\gamma_2} \to D_{\mu_{\gamma_1, \gamma_2}}$ for all $\gamma_1, \gamma_2 \in \Gamma$ as in proposition 1.12 (3) and that D is a (cocommutative) C-bialgebra. If $\Psi \in {}_C\mathcal{M}(D \otimes_C R, R)$ is a D-module algebra structure on R, then its extension $\hat{\Psi}$ is a D-module algebra structure on $\hat{R}$.

Proof. For all $I \in \mathcal{B}$ and $\gamma \in \Gamma$ there exists an ideal $\alpha(I, \gamma)$ in $\mathcal{B}$ such that $\rho(\alpha(I, \gamma)) \subseteq ({}_C\mathcal{M}(D, I), \mathrm{Ker}({}_C\mathcal{M}(D, R) \to {}_C\mathcal{M}(D_\gamma, R)))$ and we obtain homomorphisms of C-algebras $\rho_{I,\gamma}\colon R/\alpha(I, \gamma) \to {}_C\mathcal{M}(D_\gamma, R/I)$, which are compatible in the sense that for all $I_2 \subseteq I_1$ in $\mathcal{B}$ and all $\gamma_1 \to \gamma_2$ in Γ the diagram

$$
\begin{array}{ccc}
R/\alpha(I_2, \gamma_2) & \xrightarrow{\rho_{I_2,\gamma_2}} & {}_C\mathcal{M}(D_{\gamma_2}, R/I_2) \\
\downarrow & & \downarrow \\
R/\alpha(I_1, \gamma_1) & \xrightarrow{\rho_{I_1,\gamma_1}} & {}_C\mathcal{M}(D_{\gamma_1}, R/I_1)
\end{array}
$$

commutes. Then the three claims follow from the corresponding parts of proposition 1.12. $\square$

In the special case of higher and iterative derivations on adic linear topological rings we obtain:

Corollary 1.15. *Let R be a linear topological ring with respect to the I-adic topology on R, where I is an ideal in R, and $\theta\colon R \to R[\![\boldsymbol{t}]\!]$ be an n-variate higher derivation on R that is continuous with respect to the I-adic topology on R and the $(I, \boldsymbol{t})$-adic topology on $R[\![\boldsymbol{t}]\!]$. Then the n-variate higher derivation θ extends uniquely to an n-variate higher derivation $\hat{\theta}\colon \hat{R} \to \hat{R}[\![\boldsymbol{t}]\!]$ on the completion $\hat{R}$, which is again continuous. If θ is iterative, then $\hat{\theta}$ is iterative too.*

Proof. We define $\mathcal{B} := \{I^k \mid k \in \mathbb{N}\}$, $D := D_{ID^n}$, $\Gamma := \mathbb{N}^n$, $D_{\boldsymbol{l}} := D_{HD_{(\boldsymbol{l})}^n}$ for all $\boldsymbol{l} \in \mathbb{N}^n$, $\mu(\boldsymbol{l_1}, \boldsymbol{l_2}) := \boldsymbol{l_1} + \boldsymbol{l_2}$ and let

$$m_{\boldsymbol{l_1}, \boldsymbol{l_2}} \colon D_{HD_{(\boldsymbol{l_1})}^n} \otimes_C D_{HD_{(\boldsymbol{l_2})}^n} \to D_{HD_{(\boldsymbol{l_1}+\boldsymbol{l_2})}^n}$$

be the restriction of the multiplication on D_{ID^n}. Identifying ${}_C\mathcal{M}(D_{ID^n}, R)$ with $R[\![\boldsymbol{t}]\!]$, the ideal $({}_C\mathcal{M}(D, I^k), \mathrm{Ker}({}_C\mathcal{M}(D, R) \to {}_C\mathcal{M}(D_{\boldsymbol{l}}, R)))$ corresponds to the ideal $(I^k, t_1^{l_1+1}, \ldots, t_n^{l_n+1})$ for all $k \in \mathbb{N}$ and $\boldsymbol{l} \in \mathbb{N}^n$, which form a base of neighborhoods of 0 of the linear topological ring $R[\![\boldsymbol{t}]\!]$. Since θ is continuous, there exists for every $k \in \mathbb{N}$ and $\boldsymbol{l} \in \mathbb{N}^n$ an $\ell \in \mathbb{N}$ such that $\theta(I^\ell) \subseteq (I^k, t_1^{l_1+1}, \ldots, t_n^{l_n+1})$. So the claim follows from corollary 1.14. $\qquad\square$

Example 1.16. *Let R be a commutative C-algebra and $n \in \mathbb{N}$. On $R[\boldsymbol{x}]$, where $\boldsymbol{x} = (x_1, \ldots, x_n)$, there is an n-variate iterative derivation $\theta_{\boldsymbol{x}} \colon R[\boldsymbol{x}] \to R[\boldsymbol{x}][\![\boldsymbol{w}]\!]$ (with $\boldsymbol{w} := (w_1, \ldots, w_n)$) defined by $\theta_{\boldsymbol{x}}(x_i) = x_i + w_i$ for $i = 1, \ldots, n$. This n-variate iterative derivation extends uniquely to $R(\boldsymbol{x})$ (cf. [Mat89, Theorem 27.2] or [Hei10, Proposition 1.2.2]) and by corollary 1.15 it uniquely extends to $R[\![\boldsymbol{x}]\!]$. We denote these extensions (and their extensions to formally étale extensions) again by $\theta_{\boldsymbol{x}}$.*

1.3. **The structure of pointed cocommutative Hopf algebras.** In this subsection we recall some definitions and a result about the structure of pointed cocommutative Hopf algebras.

Notation: *Let C be a field.*

Definition 1.17. *If H is a C-bialgebra, then the elements of*

(1) *$G(H) := \{x \in H \mid \Delta(x) = x \otimes x\}$ are called* grouplike *elements of H and the elements of*
(2) *$P(H) := \{x \in H \mid \Delta(x) = x \otimes 1 + 1 \otimes x\}$ are the* primitive *elements of H.*

Definition 1.18. *Let H be a C-coalgebra. The coalgebra H is*

(1) irreducible *if any two subcoalgebras of H have a non-zero intersection,*
(2) simple *if H has no proper subcoalgebras,*
(3) *and* pointed *if every simple subcoalgebra of H is of dimension 1 over C.*

A maximal irreducible subcoalgebra of H is called an irreducible component *of H.*

Definition 1.19. *Let H be a C-bialgebra and A be a commutative left H-module algebra. We define the* smash product *of A with H, denoted by $A\#H$, as the C-algebra with underlying C-module $A \otimes_C H$, whose elements $a \otimes h$ will be denoted by $a\#h$, and with multiplication given by*

$$(a\#g)(b\#h) := \sum_{(c)} a(g_{(1)}b)\#g_{(2)}h$$

for all $a\#g, b\#h \in A\#_C H$ and with unit $1\#1$.

There is the following theorem on the structure of pointed cocommutative Hopf algebras, cf. for example [Mon93, Corollary 5.6.4] or [Swe69, Theorem 8.1.5].

Theorem 1.20. *Let H be a Hopf algebra with set of group like elements G and let H^1 be the irreducible component of H containing 1.*

(1) Then H^1 is a sub-Hopf algebra of H and is a CG-module algebra via

$$(1.13) \qquad g \cdot h := ghg^{-1}$$

for all $g \in G$ and $h \in H^1$.

(2) If H is pointed cocommutative, then there is an isomorphism

$$(1.14) \qquad H^1 \# CG \to H, \quad h\#g \mapsto hg.$$

(3) If $H^1 \# CG$ is equipped with the tensor product coalgebra structure (cf. (1.2)) and the antipode defined by $S(h \otimes g) := (1\#g^{-1})(S(h)\#1)$, then the isomorphism (1.14) is an isomorphism of Hopf algebras.

Definition 1.21. *Let H be a C-bialgebra. Then a* (left) *H-module bialgebra is a C-bialgebra $(A, \Delta, \varepsilon, m, \eta)$ such that Δ, ε, m and η are maps of (left) H-modules, where we equip $A \otimes_C A$ and C with the H-module structures given by*

$$h(a \otimes b) := \sum_{(h)} h_{(1)}a \otimes h_{(2)}b \quad and \quad hc := \varepsilon(h)c$$

for all $h \in H$, $a, b \in A$ and $c \in C$.

Remark 1.22. *In the situation of theorem 1.20, the sub-Hopf algebra H^1 of H is not only a CG-module algebra via (1.13), but in fact a left CG-module bialgebra.*

Definition 1.23. *A pointed irreducible cocommutative bialgebra H is called a* Birkhoff-Witt *bialgebra if an infinite sequence of divided powers lies over each primitive element $a \in P(H)$, i.e. if there is a sequence of elements $(a_n)_{n \in \mathbb{N}}$ in H such that $a_1 = a$ and $\Delta(a_n) = \sum_{i=0}^{n} a_i \otimes a_{n-i}$ for all $n \in \mathbb{N}$.*

For any vector space U over C, Sweedler defined in [Swe69, p. 261-271] the cofree pointed irreducible cocommutative coalgebra $B(U)$ on U. We have the following

Proposition 1.24 ([HS70, Proposition 4.2.10])**.** *A pointed irreducible Hopf algebra H is Birkhoff-Witt if and only if it is isomorphic to $B(U)$ with $U := P(H)$.*

If U is a vector space of finite dimension n over C, then $B(U)^* := {}_C\mathcal{M}(B(U), C)$ is isomorphic to the formal power series ring $C[\![X_1, \dots X_n]\!]$ as C-algebra and in general $B(U)^*$ is a domain, cf. [Swe69, Example-Exercise on p. 278].

1.4. Simple and Artinian simple module algebras.

Definition 1.25. *Let D be a C-bialgebra.*

(1) *A* simple commutative *D-module algebra is a commutative D-module algebra (A, Ψ_A) that has no non-trivial D-stable ideals, i.e. ideals $I \trianglelefteq A$ such that $\Psi_A(D \otimes I) \subseteq I$.*

(2) *An* Artinian simple commutative *D-module algebra is a simple commutative D-module algebra A that is Artinian as a ring.*

Definition 1.26. *Let D be a C-bialgebra.*

(1) *If $L|K$ is an extension of Artinian simple commutative D-module algebras and B is a subset of L, then we denote by $K\langle B \rangle$ the smallest Artinian simple D-module subalgebra of L that contains K and B. The extension $L|K$ is* finitely generated *as extension of Artinian simple commutative D-module algebras if there exists a finite subset B of L such that $L = K\langle B \rangle$.*

(2) If $S|R$ is an extension of commutative D-module algebras and B is a subset of S, then we denote by $R\{B\}_D$ (or also by $R\{B\}_\Psi$, $R\{B\}_\rho$ or $R\{B\}$ if there is no risk of confusion) the smallest D-module subalgebra of S that contains R and B.

Lemma 1.27. *Let D be a C-bialgebra and (A, Ψ_A) be a simple commutative D-module algebra. Then A^{Ψ_A} is a field and for every C-module V and every $\Psi_V \in {}_C\mathcal{M}(A\#D \otimes_C V, V)$ the natural homomorphism*

$$A \otimes_{A^{\Psi_A}} V^{\tilde{\Psi}_V} \to V$$

is injective, where $\tilde{\Psi}_V \colon D \otimes_C V \to V$ is the restriction of Ψ_V.

Proof. Amano and Masuoka prove this in [AM05, Corollary 3.2] under the hypothesis that D is cocommutative and their proof holds also if D is not cocommutative. □

Lemma 1.28. *Let A be a commutative C-algebra, B be a commutative A-algebra and D be a cocommutative C-bialgebra. Then ${}_C\mathcal{M}(D, A)$ and $\rho_0(B)$ are linearly disjoint over $\rho_0(A)$ as subalgebras of ${}_C\mathcal{M}(D, B)$.*

Proof. Let $b_1, \ldots, b_n \in B$ be linearly independent over A. If $f_1, \ldots, f_n \in {}_C\mathcal{M}(D, A)$ are such that $\sum_{i=1}^n f_i \rho_0(b_i) = 0$, it follows $0 = \sum_{i=1}^n (f_i \rho_0(b_i))(d) = \sum_{i=1}^n f_i(d) b_i$ for all $d \in D$. Since $b_1, \ldots, b_n$ are linearly independent over A, we obtain $f_i(d) = 0$ for all $d \in D$ and all $i = 1, \ldots, n$. □

Until the end of this section we make the following

Assumption 1.29. *Let C be a field, G a monoid and D^1 be a pointed irreducible cocommutative Hopf algebra of Birkhoff-Witt type over C such that D^1 is a CG-module bialgebra, where CG is the C-bialgebra defined in example 1.8 (4). We define $D := D^1 \# CG$ and for every submonoid G' of G we define $D(G') := D^1 \# CG'$ (cf. subsection 1.3).*

Lemma 1.30. *The smash product $D^1 \# CG$ becomes a C-bialgebra with the coalgebra structure defined by*

$$\Delta(d\#g) := \sum_{(d)} d_{(1)}\#g \otimes d_{(2)}\#g \quad and \quad \varepsilon(d\#g) := \varepsilon(d)$$

for all $d\#g \in D^1 \# CG$.

Proof. The coalgebra axioms for $D^1\#CG$ follow directly from those of D^1. Since comultiplication and counit of D^1 are CG-module homomorphisms, we obtain

$$\Delta((c\#g)(d\#h)) = \Delta(cg(d)\#gh)$$
$$= \sum_{(cg(d))} (cg(d))_{(1)}\#gh \otimes (cg(d))_{(2)}\#gh$$
$$= \sum_{(c),(g(d))} c_{(1)}(g(d))_{(1)}\#gh \otimes c_{(2)}(g(d))_{(2)}\#gh$$
$$= \sum_{(c),(g(d))} c_{(1)}g(d_{(1)})\#gh \otimes c_{(2)}g(d_{(2)})\#gh$$
$$= \sum_{(c),(d)} (c_{(1)}\#g)(d_{(1)}\#h) \otimes (c_{(2)}\#g)(d_{(2)}\#h)$$
$$= \Delta(c\#g)\Delta(d\#h)$$

and

$$\varepsilon((c\#g)(d\#h)) = \varepsilon(cg(d)\#gh) = \varepsilon(cg(d)) = \varepsilon(c)\varepsilon(g(d)) = \varepsilon(c)\varepsilon(d) = \varepsilon(c\#g)\varepsilon(d\#h)$$

i.e. Δ and ε are multiplicative and obviously they respect the units. $\qquad\square$

Remark 1.31. *If D is a pointed cocommutative Hopf algebra, then by theorem 1.20 it is isomorphic to $D^1\#CG$, where G is the group of grouplike elements of D. Assumption 1.29 is weaker in the sense that we do not assume that G is a group, but only a monoid. Therefore the following results are generalizations of results from [AM05, Section 2], where D is assumed to be a Hopf algebra. This includes in particular the bialgebra D_{end} from example 1.8 (3).*

Proposition 1.32. *Let R be a commutative D-module algebra that is Noetherian as a ring and simple as D-module algebra. We further assume that each $g \in G$ acts as an injective endomorphism on R, i.e. the endomorphism $R \to R, a \mapsto \Psi(g \otimes a)$ is injective (this is the case for example if G is a group or if G is commutative, cf. lemma 1.33). We consider the induced action of G on $\Omega(R)$ from the right defined by $P.g := g^{-1}(P)$ for $g \in G$ and $P \in \Omega(R)$, where $g^{-1}(P)$ denotes the inverse image of P under the endomorphism g, and denote by $G_P := \{g \in G \mid g^{-1}(P) = P\}$ the stabilizer of P in G. Then the following hold:*

(1) *Every $P \in \Omega(R)$ is D^1-stable, so that R/P becomes a $D(G_P)$-module domain. As $D(G_{\Omega(R)})$-module algebra R/P is simple, where $G_{\Omega(R)} := \cap_{Q\in\Omega(R)}G_Q$.*

(2) *The right action of G on $\Omega(R)$ is transitive. Therefore the stabilizers G_P are conjugate to each other.*

(3) *There is a natural isomorphism $R \cong \prod_{P\in\Omega(R)} R/P$.*

Proof. The proof is similar to the one of [AM05, Proposition 2.4], but some modifications are necessary due to the fact that in general the $g \in G$ do not act as automorphisms on R. We first note that the set $\Omega(R)$ of minimal prime ideals of R is finite. Since R is reduced, $\cap_{Q\in\Omega(R)}Q = 0$ and since all $g \in G$ act as injective endomorphisms on R, it follows

$$\cap_{Q\in\Omega(R)}g^{-1}(Q) = \cap_{Q\in\Omega(R)}Q = 0.$$

Therefore $g^{-1}(Q) \in \Omega(R)$ for all $Q \in \Omega(R)$ and all $g \in G$. Since $[G : G_Q] \le |\Omega(R)|$, the index $[G : G_Q]$ is finite for all $Q \in \Omega(R)$ and hence is $[G : G_{\Omega(R)}]$.

To prove (1), we denote by $\rho_1 \colon R \to {}_C\mathcal{M}(D^1, R)$ the homomorphism of C-algebras associated to the restriction of the D-module algebra structure to a D^1-module algebra structure. Then the inverse image $\rho_1^{-1}({}_C\mathcal{M}(D^1, P))$ is a D^1-stable prime ideal of R that is included in P. Since P is a minimal prime ideal, it follows $P = \rho_1^{-1}({}_C\mathcal{M}(D^1, P))$ and so P is D^1-stable.

Let J be a proper $D(G_{\Omega(R)})$-stable ideal of R containing P. Let $1 = g_1, \ldots, g_\nu$ be a system of representatives of the cosets $G/G_{\Omega(R)}$. Then $\cap_{i=1}^\nu g_i^{-1}(J)$ is D-stable and thus equal to (0), since R is a simple D-module algebra. Since P is a prime ideal, there exists an $i \in \{1, \ldots, \nu\}$ such that $g_i^{-1}(J) \subseteq P$. Together with our assumption $P \subseteq J$ we obtain $g_i^{-1}(P) \subseteq g_i^{-1}(J) \subseteq P$. Since P is a minimal prime ideal, it follows $g_i^{-1}(P) = P$, i.e. $i = 1$ and thus $J = P$. Therefore R/P is a simple $D(G_{\Omega(R)})$-module algebra.

To prove (2), let $P \in \Omega(R)$. By part (1), $g^{-1}(P)$ is D^1-stable for all $g \in G$. Therefore the intersection $\cap_{g \in G/G_P} g^{-1}(P)$ is D-stable and thus we have

$$\cap_{Q \in \Omega(R)} Q = (0) = \cap_{g \in G/G_P} g^{-1}(P),$$

since R is a simple D-module algebra. It follows $\{g^{-1}(P) \mid g \in G/G_P\} = \Omega(R)$.

Now we prove (3): By the previous we have a bijection $G/G_P \cong \Omega(R)$ for every $P \in \Omega(R)$. If Q and Q' are distinct elements of $\Omega(R)$, then $(Q \subsetneq) Q + Q' = R$, since R/Q is a simple $D(G_{\Omega(R)})$-module algebra. Hence $R \to \prod_{Q \in \Omega(R)} R/Q \cong \prod_{g \in G/G_P} R/g^{-1}(P)$ is an isomorphism by the Chinese remainder theorem. $\square$

Lemma 1.33. *If the monoid G is commutative and R is a commutative D-module algebra, then the kernel $\operatorname{Ker} g$ of each $g \in G$, considered as an endomorphism of R, is a D-stable ideal of R. In particular, if R is a simple commutative D-module algebra, then all $g \in G$ act as injective endomorphisms of R.*

Proof. We note that for all $g \in G$ and $\sum_{i=1}^n d_i \# h_i \in D^1 \# CG$ we have

$$(1 \# g)(\sum_{i=1}^n d_i \# h_i) = \sum_{i=1}^n g(d_i) \# g h_i = \sum_{i=1}^n g(d_i) \# h_i g = (\sum_{i=1}^n g(d_i) \# h_i)(1 \# g).$$

So for $a \in \operatorname{Ker} g$ we have $(1 \# g)(\sum_{i=1}^n d_i \# h_i)(a) = (\sum_{i=1}^n g(d_i) \# h_i)(1 \# g)(a) = 0$, and thus $(\sum_{i=1}^n d_i \# h_i)(a) \in \operatorname{Ker}(g)$. Therefore $\operatorname{Ker}(g)$ is a D-stable ideal of R. $\square$

Proposition 1.34. *Let R be a Noetherian simple commutative D-module algebra. If furthermore each $g \in G$ acts as an injective endomorphism on R, then the following are equivalent:*

(1) R is total,
(2) R/P is a field for every $P \in \Omega(R)$,
(3) The Krull dimension of R is zero and
(4) R is Artinian as a ring.

In this case every R-module is projective.

Proof. Since $R \cong \prod_{P \in \Omega(R)} R/P$ by proposition 1.32 (3), R is total if and only if R/P is total for every $P \in \Omega(R)$ and since R/P is an integral domain, this is the case if and only if R/P is a field. The Krull dimension of R is zero if and only if each $P \in \Omega(R)$ is a maximal ideal, i.e. if R/P is a field. Since R is Noetherian, it

is Artinian if and only if its Krull dimension is 0 (cf. [Bou85, Chapitre IV, §2.5, Proposition 9]).

In this case R is semi-simple and so every R-module is projective (cf. [Bou85, Chapitre I, §2.4]). $\qquad\square$

If G is a group, then we recover the first part of [AM05, Corollary 2.5] from proposition 1.34.

2. Galois theory of Artinian simple module algebras

2.1. **Notation.** As in assumption 1.29, let C be a field, G be a monoid and let CG be the C-bialgebra defined in example 1.8 (4). Let further D^1 be a pointed irreducible cocommutative Hopf algebra of Birkhoff-Witt type over C such that D^1 is a CG-module bialgebra. We define $D := D^1 \# CG$ and consider it as a C-bialgebra as in lemma 1.30.

Remark 2.1. *These conditions allow for example the choices D_{end}, D_{aut} or D_{ID^n} for D (cf. example 1.8). The pointed irreducible cocommutative Hopf algebra D_{der} is of Birkhoff-Witt type if $\mathbb{Q} \subseteq C$. Another example is provided by the Hopf algebra constructed by Masuoka in [Mas10], describing iterative q-difference operators as introduced by Hardouin in [Har10].*

Let $L|K$ be an extension of Artinian simple commutative D-module algebras such that the elements $g \in G \subseteq D$ act as injective endomorphisms on L. By proposition 1.34, L and K have Krull dimension 0, are total and the monoid G acts transitively on $\Omega(L)$ and $\Omega(K)$ (cf. proposition 1.32 (2)). If $Q \in \Omega(L)$ and $P \in \Omega(K)$, then we denote by G_Q and G_P the stabilizers in G of Q and P, respectively. It follows $\Omega(L) \cong G/G_Q$, $\Omega(K) \cong G/G_P$ and by proposition 1.32 (3) we have

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

We assume that for every $Q \in \Omega(L)$ the field extension L/Q over $K/(K \cap Q)$ is separable and finitely generated and that its degree of transcendence is the same for every Q, say n. Let $\boldsymbol{u}^Q = (u_1^Q, \ldots, u_n^Q)$ be a separating transcendence basis of it and let $\theta_{\boldsymbol{u}^Q} : L/Q \to L/Q[\![\boldsymbol{w}]\!]$ 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 $i = 1, \ldots, n$ (cf. example 1.16). By corollary 1.13, there exists a unique n-variate iterative derivation

$$(2.1) \qquad\qquad\qquad \theta_{\boldsymbol{u}} : L \to L[\![\boldsymbol{w}]\!]$$

on the product $L \cong \prod_{Q \in \Omega(L)} L/Q$ over K such that the projections to all factors L/Q are iterative differential homomorphisms. We extend $\theta_{\boldsymbol{u}}$ to $_C\mathcal{M}(D, L)$ as in (1.4) and by abuse of notation we denote this n-variate iterative derivation again by $\theta_{\boldsymbol{u}}$. By [Gro64, Chapitre 0, 21.7.4], L/Q is formally étale over $(K/(Q \cap K))(\boldsymbol{u}^Q)$ for all $Q \in \Omega(L)$. We define $u_i := (u_i^Q)_{Q \in \Omega(L)} \in L$ for all $i \in \{1, \ldots, n\}$ and $\boldsymbol{u} := (u_1, \ldots, u_n)$. Then L is formally étale over $\prod_{Q \in \Omega(L)} (K/(Q \cap K))(\boldsymbol{u}^Q)$. We denote the latter by $K(\boldsymbol{u})$.

Remark 2.2. *Our conditions allow it to consider the theories in [Ume96] and [Mor09] as special cases:*

(1) In [Ume96], *Umemura starts with an extension of differential fields of characteristic zero that is finitely generated as extension of fields. This situation is recovered by setting $D^1 := D_{der}$ and $G = \{1\}$.*

(2) In [Mor09], *Morikawa starts with an extension of difference fields $L|K$ of characteristic zero that is finitely generated as extension of fields. This situation is recovered by setting $D^1 := C$ and $G := (\mathbb{N}, +)$, such that $D \cong D_{end}$.*

In both cases all of our further conditions are automatically fulfilled.

But our conditions also allow to consider finite direct products of fields equipped with an injective endomorphism, as they appear in the study of (linear) difference equations, cf. for example [vdPS97]. The factors in this direct product correspond to the minimal prime ideals of the ring.

2.2. The Galois hull $\mathcal{L}|\mathcal{K}$ of an extension $L|K$ of Artinian simple D-module algebras.

Lemma 2.3. *If $\boldsymbol{u^Q} = (u_1^Q, \ldots, u_n^Q)$ and $\boldsymbol{v^Q} = (v_1^Q, \ldots, v_n^Q)$ are separating transcendence bases of L/Q over $K/(Q \cap K)$ for all $Q \in \Omega(L)$ and $\theta_{\boldsymbol{u}}$ and $\theta_{\boldsymbol{v}}$ are the associated n-variate iterative derivations on L over K as defined in (2.1), then there exists an automorphism φ of the L-algebra $L[\![\boldsymbol{w}]\!]$ such that $\theta_{\boldsymbol{v}} = \varphi \circ \theta_{\boldsymbol{u}}$ and the iterative differential subalgebras of $_C\mathcal{M}(D, L)$ generated by $\rho(L)$ and $\rho_0(L)$, once with respect to $\theta_{\boldsymbol{u}}$, once with respect to $\theta_{\boldsymbol{v}}$, are equal, i.e.*

$$\rho_0(L)\{\rho(L)\}_{\theta_{\boldsymbol{u}}} = \rho_0(L)\{\rho(L)\}_{\theta_{\boldsymbol{v}}}.$$

Proof. We first show that for each $Q \in \Omega(L)$ there exists an automorphism φ_Q of the L/Q-algebra $(L/Q)[\![\boldsymbol{w}]\!]$ such that $\theta_{\boldsymbol{v}Q} = \varphi_Q \circ \theta_{\boldsymbol{u}Q}$. In fact, the set of formal power series $(\theta_{\boldsymbol{u}Q}(v_i^Q) - v_i^Q)_{i=1,\ldots,n}$ has an invertible Jacobian matrix $(\theta_{\boldsymbol{u}Q}^{(\boldsymbol{\delta}_j)}(v_i^Q))_{i,j=1}^n$ and by the formal inverse function theorem (cf. for example [Haz78, A.4]) there exists a continuous homomorphism of L/Q-algebras $\varphi_Q \colon (L/Q)[\![\boldsymbol{w}]\!] \to (L/Q)[\![\boldsymbol{w}]\!]$ such that $\varphi_Q(\theta_{\boldsymbol{u}Q}(v_i^Q) - v_i^Q) = w_i = \theta_{\boldsymbol{v}Q}(v_i^Q) - v_i^Q$ and thus also $\varphi_Q(\theta_{\boldsymbol{u}Q}(v_i^Q)) = \theta_{\boldsymbol{v}Q}(v_i^Q)$ for all $i = 1, \ldots, n$, so that $\varphi_Q \circ \theta_{\boldsymbol{u}Q}$ and $\theta_{\boldsymbol{v}Q}$ coincide on $K(v_1^Q, \ldots, v_n^Q)$. Since L/Q is a formally étale extension of $(K/(Q \cap K))(v_1^Q, \ldots, v_n^Q)$, they coincide on L/Q as well (cf. [Mat89, Theorem 27.2] or [Hei10, Proposition 1.2.2]). The automorphisms $(\varphi_Q)_{Q \in \Omega(L)}$ induce an automorphism φ of the L-algebra $L[\![\boldsymbol{w}]\!]$ such that $\theta_{\boldsymbol{v}} = \varphi \circ \theta_{\boldsymbol{u}}$. The last claim is a direct consequence of this. $\square$

We define

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

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. Both are $D \otimes_C D_{ID^n}$-module subalgebras of $(_C\mathcal{M}(D, L), \rho_{int} \otimes \theta_{\boldsymbol{u}})$ and by the previous lemma $\mathcal{L}$ does not depend on the choice of $\boldsymbol{u}$.[2] We call the extension $\mathcal{L}|\mathcal{K}$ the *Galois hull* of $L|K$.

Example 2.4. *Let K be a field and $L = K(y)$ be a purely transcendental extension field of K. We define an iterative derivation θ_y on L as the K-linear homomorphism*

---

[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] when $D = D_{end}$ and L and K are fields.

$\theta_y \colon L \to L[\![t]\!]$ *fulfilling* $\theta_y(y) \coloneqq y + t$ *(cf. example 1.16). We chose* $\{u = y\}$ *as separating transcendence basis of* L *over* K. *Then* $\mathcal{L} = L[K(y+t)]$ *and* $\mathcal{K} = L$.

Example 2.5. *Let* K *be a field containing* $\mathbb{Q}$ *and* $L = K(y)$ *be a purely transcendental extension field of* K. *We define an iterative derivation* θ_y *on* L *as the* K-*linear homomorphism* $\theta \colon L \to L[\![t]\!]$ *fulfilling* $\theta(y) \coloneqq y \exp(t)$. *We chose* $\{u = y\}$ *as separating transcendence basis of* L *over* K. *Then* $\mathcal{L} = L[K(y \exp(t))]$ *and* $\mathcal{K} = L$.

2.3. **The Umemura functor.** 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 structures on $_C\mathcal{M}(D, L)$ and on $A[\![\boldsymbol{w}]\!]$ are given by $\rho_0 \colon L \to {}_C\mathcal{M}(D, L)$ (cf. example 1.8 (7)) and by $\theta_{\boldsymbol{u}} \colon L \to L[\![\boldsymbol{w}]\!]$ (cf. (2.1)), respectively. This tensor product carries D and D_{ID^n}-module algebra structures ρ and θ, induced by

$$(2.2) \qquad (_C\mathcal{M}(D, L), \rho_{int}, \theta_{\boldsymbol{u}}) \xleftarrow{\ \rho_0\ } (L, \rho_0, \theta_{\boldsymbol{u}}) \xrightarrow{\ \theta_{\boldsymbol{u}}\ } (A[\![\boldsymbol{w}]\!], \rho_0, \theta_{\boldsymbol{w}})$$

using proposition 1.11. The corresponding homomorphism

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

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 $D \otimes_C D_{ID^n}$-module algebra structure extends to the completion

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

with respect to the $(\boldsymbol{w})$-adic topology by corollary 1.14. 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 2.6. *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 of* $D \otimes_C D_{ID^n}$-*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*

$$
\begin{array}{ccc}
\mathcal{L} \hat{\otimes}_L A[\![\boldsymbol{w}]\!] & & \\
\Big\downarrow{\scriptstyle \varphi} & \searrow^{\mathrm{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]} & \\
\mathcal{L} \hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\mathrm{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]} & \mathcal{L} \hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{array}
$$

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* $\lambda[\![\boldsymbol{w}]\!] \colon A[\![\boldsymbol{w}]\!] \to B[\![\boldsymbol{w}]\!]$.

2.4. **Lie-Ritt functors.** Umemura defines Lie-Ritt functors in [Ume96]. Here we use a slightly changed version of them.

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

The *infinitesimal coordinate transformations of n variables over A*

$$\mathbf{\Gamma}_{nL}(A) := \{(\varphi_1, \ldots, \varphi_n) \in (A[\![\boldsymbol{w}]\!])^n \mid \varphi_i \equiv w_i \mod N(A)[\![\boldsymbol{w}]\!] \; \forall \, i \in \{1, \ldots, n\}\},$$

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

We equip the ring $A[\![\boldsymbol{w}]\!]$ with the n-variate iterative derivation θ over A with respect to $\boldsymbol{w}$ (cf. example 1.16) and we extend it to

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

with elements $(Y_i^{(\boldsymbol{k})})_{i \in \{1,\ldots,n\}, \boldsymbol{k} \in \mathbb{N}^n}$, algebraically independent over $A[\![\boldsymbol{w}]\!]$, by

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

for all $\boldsymbol{l} \in \mathbb{N}^n$. 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 n-tuple $(Y_1^{(\boldsymbol{0})}, \ldots, Y_n^{(\boldsymbol{0})})$. For $F \in A[\![\boldsymbol{w}]\!]\{A[\![\boldsymbol{Y}]\!]\}_\theta$ and $\Phi = (\varphi_1, \ldots, \varphi_n) \in \mathbf{\Gamma}_{nL}(A)$ we denote by $F_{|\boldsymbol{Y}=\Phi}$ the image of F under the homomorphism of $A[\![\boldsymbol{w}]\!]$-algebras $A[\![\boldsymbol{w}]\!]\{A[\![\boldsymbol{Y}]\!]\}_\theta \to A[\![\boldsymbol{w}]\!]$ that sends $Y_i^{(\boldsymbol{k})}$ to $\theta^{(\boldsymbol{k})}(\varphi_i)$.

Definition 2.7. *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 $I \lhd L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta$ such that $G(A) \cong Z(I)(A)$ for every commutative L-algebra A, where*

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

Remark 2.8. *In [Ume96, Definition 1.8] Lie-Ritt functors over L are defined using ideals in $L[\![\boldsymbol{w}]\!]\{\{\boldsymbol{Y}\}\}$ instead of $L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta$. 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 above definition instead.*

Example 2.9. *We define a subgroup functor G_+ of $\mathbf{\Gamma}_{1\mathbb{Z}}$ as*

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

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 $\varphi(w) = \sum_{i \geq 0} (a_i + \delta_{i,1}) w^i \in \mathbf{\Gamma}_{1\mathbb{Z}}(A)$ lies in $Z(I)(A)$ if and only if $1 = \theta^{(1)}(\varphi) = \sum_{i \geq 1} (a_i + \delta_{i,1}) i w^{i-1}$ and for all $k \geq 2$ the equation $0 = \theta^{(k)}(\varphi) = \sum_{i \geq k} \binom{i}{k} (a_i + \delta_{i,1}) w^{i-k}$ holds. This is the case if and only if $a_k = 0$ for all $k \geq 1$, i.e. if $\varphi(w) = a_0 + w$ for some $a_0 \in N(A)$. $\qquad\square$

Example 2.10. *We define a subgroup functor G_* of $\mathbf{\Gamma}_{1\mathbb{Z}}$ as*

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

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 $\varphi(w) = \sum_{i \geq 0}(a_i + \delta_{i,1})w^i \in \mathbf{\Gamma}_{1\mathbb{Z}}(A)$ lies in $Z(I)(A)$ if and only if $w\sum_{i \geq 1} i(a_i + \delta_{i,1})w^{i-1} = \sum_{i \geq 0}(a_i + \delta_{i,1})w^i$ and $\theta^{(k)}(\sum_{i \geq 0}(a_i + \delta_{i,1})w^i) = 0$ 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 $\varphi(w) \in G_*(A)$. $\qquad\square$

Example 2.11. *Let L be a field and $0 \neq y \in L$. We define a subgroup functor $\tilde{G}_*$ of $\mathbf{\Gamma}_{1L}$ as*

$$\tilde{G}_*(A) := \{ya_1 + (1 + a_1)w \mid a_0 \in N(A)\}$$

for all commutative L-algebras A. Then $\tilde{G}_*$ is a Lie-Ritt functor over L and $\tilde{G}_* = Z(I)$, where $I = (\{(y + w)Y^{(1)} - Y - y, Y^{(k)} \mid k \geq 2\})$.

Furthermore, $\tilde{G}_*$ is isomorphic to the Lie-Ritt functor G_* in example 2.10 and thus also to the multiplicative formal group scheme $\hat{\mathbb{G}}_m$.

Proof. An element $\varphi(w) = \sum_{i \geq 0}(a_i + \delta_{i,1})w^i \in \mathbf{\Gamma}_{1L}(A)$ lies in $Z(I)(A)$ if and only if $(y+w)\sum_{i \geq 1} i(a_i + \delta_{i,1})w^{i-1} - \sum_{i \in \mathbb{N}}(a_i + \delta_{i,1})w^i - y = 0$ and $\theta^{(k)}(\sum_{i \geq 0}(a_i + \delta_{i,1})w^i) = 0$ hold for all $k \geq 2$. This is the case if and only if $a_0 = ya_1$ and $a_k = 0$ for all $k \geq 2$, i.e. if $\varphi(w) \in \tilde{G}_*(A)$.

An isomorphism $G_* \to \tilde{G}_*$ is given by sending $(1 + a_1)w \in G_*(A)$ to $ya_1 + (1 + a_1)w \in \tilde{G}_*(A)$, which is multiplicative since if $(1 + b_1)w$ is another element of $G_*(A)$, then the product of $(1+a_1)w$ and $(1+b_1)w$ in $G_*(A)$ is $(1+a_1)(1+b_1)w = (1+a_1+b_1+a_1b_1)w$, which has as image in $\tilde{G}_*(A)$ the element $y(a_1+b_1+a_1b_1)+(1+a_1+b_1+a_1b_1)w$. At the other hand, the product of $ya_1+(1+a_1)w$ and $yb_1+(1+b_1)w$ in $\tilde{G}_*(A)$ is $ya_1+(1+a_1)(yb_1+(1+b_1)w) = y(a_1+b_1+a_1b_1)+(1+a_1+b_1+a_1b_1)w$. $\quad\square$

The analogues of example 2.9 and 2.10 in the setting of Umemura appeared in [Ume96, Example 1.9(i) and (ii)]. Since he assumes $\mathbb{Q} \subseteq L$, it is sufficient for him to use the equation $Y^{(1)} - 1$ and $wY^{(1)} - Y$ as generators of I in the first and second example, respectively. In the general case we have to add the equations $Y^{(k)}$ for $k \geq 2$.

Proposition 2.12. *Every Lie-Ritt functor over L is isomorphic to a formal group scheme over L.*

Proof. Let A be a commutative L-algebra. Then for every $n \in \mathbb{N}$ we have an isomorphism

$$\mathbf{\Gamma}_{nL}(A) \to \widehat{\mathbb{A}}_L^{\{1,\ldots,n\} \times \mathbb{N}^n}(A), \quad \left(\sum_{\boldsymbol{k} \in \mathbb{N}^n}(a_{i,\boldsymbol{k}} + \delta_{\boldsymbol{k},\boldsymbol{\delta}_i})\boldsymbol{w}^{\boldsymbol{k}}\right)_{i=1,\ldots,n} \mapsto (a_{i,\boldsymbol{k}})_{(i,\boldsymbol{k}) \in \{1,\ldots,n\} \times \mathbb{N}^n},$$

which is natural in A. It gives rise to an isomorphism from $\mathbf{\Gamma}_{nL}$ to the formal scheme $\widehat{\mathbb{A}}_L^{\{1,\ldots,n\} \times \mathbb{N}^n}$, which has as A-points the set $N(A)^{\{1,\ldots,n\} \times \mathbb{N}^n}$.

There exist formal power series $(f_{i,\boldsymbol{l}})_{i \in \{1,\ldots,n\}, \boldsymbol{l} \in \mathbb{N}^n}$ in variables $u_{j,\boldsymbol{k}}, v_{j,\boldsymbol{k}}$ with $j \in \{1,\ldots,n\}$ and $\boldsymbol{k} \in \mathbb{N}^n$, coefficients in $\mathbb{Z}$ and constant terms equal to zero

defined by

$$f_{i,\boldsymbol{l}}((u_{j,\boldsymbol{k}},v_{j,\boldsymbol{k}})_{(j,\boldsymbol{k})\in\{1,\dots,n\}\times\mathbb{N}^n}) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} v_{i,\boldsymbol{k}} \sum_{\substack{\boldsymbol{l}_{1,1},\dots,\boldsymbol{l}_{1,k_1},\dots,\boldsymbol{l}_{n,1},\dots,\boldsymbol{l}_{n,k_n}\in\mathbb{N}^n \\ \sum_{\mu=1}^{n}\sum_{\nu=1}^{k_\mu}\boldsymbol{l}_{\mu,\nu}=\boldsymbol{l}}} \prod_{\mu=1}^{n}\prod_{\nu=1}^{k_\mu} u_{\mu,\boldsymbol{l}_{\mu,\nu}}$$

such that for all elements $\Psi = (\psi_1,\dots,\psi_n)$ and $\Phi = (\varphi_1,\dots,\varphi_n)$ of $\boldsymbol{\Gamma}_{nL}(A)$ with $\varphi_i = \sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{i,\boldsymbol{k}}\boldsymbol{w}^{\boldsymbol{k}}$ and $\psi_i = \sum_{\boldsymbol{k}\in\mathbb{N}^n} b_{i,\boldsymbol{k}}\boldsymbol{w}^{\boldsymbol{k}}$ for all $i \in \{1,\dots,n\}$ we have

$$\psi_i(\Phi) = \sum_{\boldsymbol{l}\in\mathbb{N}^n} f_{i,\boldsymbol{l}}((a_{j,\boldsymbol{k}},b_{j,\boldsymbol{k}})_{(j,\boldsymbol{k})\in\{1,\dots,n\}\times\mathbb{N}^n})\boldsymbol{w}^{\boldsymbol{l}}.$$

The formal power series $f_{i,\boldsymbol{j}}$ have the *monomials have finite support condition* (cf. [Haz79, Definition 7.2]) and since the multiplication in $\boldsymbol{\Gamma}_{nL}(A)$ is associative and unital, with unit the tuple $(w_1,\dots,w_n)$, we see that $f_{i,\boldsymbol{l}}$ give rise to an (infinite dimensional) formal group law in the sense of Hazewinkel (cf. [Haz79, Definition 7.5]). They also give rise to a morphism

$$\widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n} \times \widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n} \to \widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n}$$

of formal schemes over L, which defines a group law on $\widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n}$ such that $\widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n}$ becomes a formal group scheme over L, which is isomorphic to the group functor $\boldsymbol{\Gamma}_{nL}$.

Let G be an arbitrary Lie-Ritt functor over L and let $I \trianglelefteq L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta$ be such that $G \cong Z(I)$. Let $\Phi = (\varphi_1,\dots,\varphi_n) \in \boldsymbol{\Gamma}_{nL}(A)$ and $\varphi_i = \sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{i,\boldsymbol{k}}\boldsymbol{w}^{\boldsymbol{k}}$ for all $i \in \{1,\dots,n\}$. For $h \in I$ the condition $h(\Phi) = 0$ is equivalent to a system of polynomial equations $(h_\lambda)_{\lambda\in\Lambda_h}$ among the coefficients $a_{i,\boldsymbol{k}}$. Thus, G is isomorphic to the closed formal subgroup scheme of $\widehat{\mathbb{A}}_L^{\{1,\dots,n\}\times\mathbb{N}^n}$ defined by the polynomials h_λ for all $h \in I$ and $\lambda \in \Lambda_h$. $\qquad\square$

2.5. The Umemura functor as a Lie-Ritt functor. Notation: *In this subsection we assume that $L|K$ is as in subsection 2.1.*

Lemma 2.13. *For any commutative L-algebra A there exists an injective homomorphism of $D \otimes_C D_{ID^n}$-module algebras*

$$(2.3)\qquad \mu_{A,\boldsymbol{u}}\colon {}_C\mathcal{M}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \to {}_C\mathcal{M}(D,A[\![\boldsymbol{w}]\!])$$

$$\sum_{\boldsymbol{i}\in\mathbb{N}^n} f_{\boldsymbol{i}} \otimes a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}} \mapsto \sum_{\boldsymbol{i}\in\mathbb{N}^n} \theta_{\boldsymbol{u}}(f_{\boldsymbol{i}}) \cdot \rho_0(a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}}),$$

where we consider ${}_C\mathcal{M}(D,A[\![\boldsymbol{w}]\!])$ as D-module algebra via Ψ_{int} and as D_{ID^n}-module algebra with the D_{ID^n}-module algebra structure induced by $\theta_{\boldsymbol{w}}$ on $A[\![\boldsymbol{w}]\!]$ to ${}_C\mathcal{M}(D,A[\![\boldsymbol{w}]\!])$ via lemma 1.9 (3).

Proof. The composition of homomorphisms of $D \otimes_C D_{ID^n}$-module algebras

$${}_C\mathcal{M}(D,L)\otimes_L A[\![\boldsymbol{w}]\!] \xrightarrow{\theta_{\boldsymbol{u}}\otimes\rho_0} {}_C\mathcal{M}(D,L[\![\boldsymbol{w}]\!])\otimes_{LC}\mathcal{M}(D,A[\![\boldsymbol{w}]\!]) \xrightarrow{m} {}_C\mathcal{M}(D,A[\![\boldsymbol{w}]\!]),$$

is injective by lemma 1.28. We extend this homomorphism to the completion ${}_C\mathcal{M}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$. This extension is again injective, since the inverse image of ${}_C\mathcal{M}(D,(\boldsymbol{w}^{\boldsymbol{k}}))$ is ${}_C\mathcal{M}(D,L)\otimes(\boldsymbol{w}^{\boldsymbol{k}})$ and their intersection over all $\boldsymbol{k} \in \mathbb{N}^n$ is (0). $\quad\square$

The following theorem generalizes [Ume96, Lemma 5.9] and [Mor09, Theorem 2.22].

Theorem 2.14. *The functor* $\mathrm{Ume}(L|K)$ *is a Lie-Ritt functor over* L.

Proof. For a commutative L-algebra A we consider the map

(2.4)
$$\mathrm{Ume}(L|K)(A) \longrightarrow \boldsymbol{\Gamma}_{nL}(A)$$
$$\varphi \longmapsto (\mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ \varphi(\rho(u_i) \otimes 1) - u_i)_{i=1,\ldots,n}.$$

Let $\varphi \in \mathrm{Ume}(L|K)(A)$ and define

$$\Phi := (\varphi_1,\ldots,\varphi_n) := (\mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ \varphi(\rho(u_i) \otimes 1) - u_i)_{i=1,\ldots,n}.$$

Then we have

$$\mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ \varphi(\rho(u_i) \otimes 1) - u_i \equiv w_i \quad \mathrm{mod}\ N(A)[\![\boldsymbol{w}]\!],$$

so that (2.4) is well defined. We define

$$F \colon L \to A[\![\boldsymbol{w}]\!], \quad a \mapsto \mathrm{ev}_{1_D} \circ_\Phi \theta_{\boldsymbol{u}} \circ \rho(a),$$

where ${}_\Phi\theta_{\boldsymbol{u}} \colon L \to A[\![\boldsymbol{w}]\!]$ is the composition of $\theta_{\boldsymbol{u}}$ with the endomorphism of $A[\![\boldsymbol{w}]\!]$ sending w_i to φ_i for all $i \in \{1,\ldots,n\}$, and

$$G \colon L \to A[\![\boldsymbol{w}]\!], \quad a \mapsto \mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ \varphi(\rho(a) \otimes 1).$$

Trivially F and G coincide on K and for all $i = 1,\ldots,n$ we have

$$F(u_i) = \mathrm{ev}_{1_D} \circ_\Phi \theta_{\boldsymbol{u}} \circ \rho(u_i) = u_i + \varphi_i = u_i + \mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ \varphi(\rho(u_i) \otimes 1) - u_i = G(u_i).$$

Since L is formally étale over $K(u_1,\ldots,u_n)$, F and G coincide also on L. Since $\rho, \varphi, \mu_{A,\boldsymbol{u}}$ and ${}_\Phi\theta_{\boldsymbol{u}}$ are homomorphisms of D-module algebras, it follows that for all $a \in L$

$$
\begin{aligned}
(\mu_{A,\boldsymbol{u}} \circ \varphi(\rho(a) \otimes 1))(d) &= (d.(\mu_{A,\boldsymbol{u}} \circ \varphi(\rho(a) \otimes 1)))(1_D) \\
&= (\mu_{A,\boldsymbol{u}} \circ \varphi(\rho(d.a) \otimes 1))(1_D) \\
&= ({}_\Phi\theta_{\boldsymbol{u}}(\rho(d.a)))(1_D) \\
&= (d.({}_\Phi\theta_{\boldsymbol{u}}(\rho(a))))(1_D) \\
&= ({}_\Phi\theta_{\boldsymbol{u}}(\rho(a)))(d),
\end{aligned}
$$

i.e. $\mu_{A,\boldsymbol{u}} \circ \varphi(\rho(a) \otimes 1) = {}_\Phi\theta_{\boldsymbol{u}}(\rho(a))$. Using that for all $a \in L$

$$\mu_{A,\boldsymbol{u}}\left(\sum_{\boldsymbol{k} \in \mathbb{N}^n} \theta_{\boldsymbol{u}}^{(\boldsymbol{k})}(\rho(a)) \otimes (\Phi - \boldsymbol{w})^{\boldsymbol{k}}\right) = {}_\Phi\theta_{\boldsymbol{u}}(\rho(a))$$

and the injectivity of $\mu_{A,\boldsymbol{u}}$, this implies

(2.5)
$$\varphi(\rho(a) \otimes 1) = \sum_{\boldsymbol{k} \in \mathbb{N}^n} \theta_{\boldsymbol{u}}^{(\boldsymbol{k})}(\rho(a)) \otimes (\Phi - \boldsymbol{w})^{\boldsymbol{k}}.$$

Next, we show that the natural transformation induced by (2.4) respects the group structures. To this end, let $\psi \in \mathrm{Ume}(L|K)(A)$ and let Ψ be the image of it under (2.4). By equation (2.5) we obtain, using the abbreviations $\Phi' = \Phi - \boldsymbol{w}$ and

$\Psi' = \Psi - \boldsymbol{w}$, that for all $a \in L$

$$
\begin{aligned}
\varphi \circ \psi(\rho(a) \otimes 1) &= \varphi\left(\sum_{\boldsymbol{k} \in \mathbb{N}^n} \theta_{\boldsymbol{u}}^{(\boldsymbol{k})}(\rho(a)) \otimes (\Psi - \boldsymbol{w})^{\boldsymbol{k}} \right) \\
&= \sum_{\boldsymbol{k} \in \mathbb{N}^n} \theta^{(\boldsymbol{k})} \left(\sum_{\boldsymbol{l} \in \mathbb{N}^n} \theta_{\boldsymbol{u}}^{(\boldsymbol{l})}(\rho(a)) \otimes \Phi'^{\boldsymbol{l}} \right) (1 \otimes \Psi'^{\boldsymbol{k}}) \\
&= \sum_{\boldsymbol{k_1}, \boldsymbol{k_2}, \boldsymbol{l} \in \mathbb{N}^n} \left(\binom{\boldsymbol{k_1} + \boldsymbol{l}}{\boldsymbol{l}} \theta_{\boldsymbol{u}}^{(\boldsymbol{k_1} + \boldsymbol{l})}(\rho(a)) \otimes \theta_{\boldsymbol{w}}^{(\boldsymbol{k_2})}(\Phi'^{\boldsymbol{l}}) \right) (1 \otimes \Psi'^{\boldsymbol{k_1} + \boldsymbol{k_2}}) \\
&= \sum_{\boldsymbol{m}, \boldsymbol{k_2}, \boldsymbol{l} \in \mathbb{N}^n} \binom{\boldsymbol{m}}{\boldsymbol{l}} \theta_{\boldsymbol{u}}^{(\boldsymbol{m})}(\rho(a)) \otimes \theta_{\boldsymbol{w}}^{(\boldsymbol{k_2})}(\Phi'^{\boldsymbol{l}}) \Psi'^{\boldsymbol{m} - \boldsymbol{l} + \boldsymbol{k_2}}) \\
&= \sum_{\boldsymbol{m}, \boldsymbol{l} \in \mathbb{N}^n} \theta_{\boldsymbol{u}}^{(\boldsymbol{m})}(\rho(a)) \otimes \binom{\boldsymbol{m}}{\boldsymbol{l}} \Psi'^{\boldsymbol{m} - \boldsymbol{l}} (\Phi'(\Psi))^{\boldsymbol{l}} \\
&= \sum_{\boldsymbol{m} \in \mathbb{N}^m} \theta_{\boldsymbol{u}}^{(\boldsymbol{m})}(\rho(a)) \otimes (\Phi(\Psi) - \boldsymbol{w})^{\boldsymbol{m}}.
\end{aligned}
$$

It follows that the image of $\varphi \circ \psi$ in $\boldsymbol{\Gamma}_{nL}(A)$ is $\Phi(\Psi)$.

It remains to show that the image of the natural transformation induced by (2.4) is of the form $Z(I)$ for some ideal I of $L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta$. For all $m \in \mathbb{N}$, elements $a_1, \ldots, a_m \in L$, iterative differential polynomials $F(X_{a_1}, \ldots, X_{a_m}) \in \mathcal{K}\{X_{a_1}, \ldots, X_{a_m}\}_{D_{ID^n}}$ with coefficients in $\mathcal{K}$ and in iterative differential variables $X_{a_1}, \ldots, X_{a_m}$ fulfilling $F(\rho(a_1), \ldots, \rho(a_m)) = 0$ (with respect to the iterative derivation $\theta_{\boldsymbol{u}}$) and for all $d \in D$ we define

$$
F_d := F^{\theta_{\boldsymbol{u}}}(\boldsymbol{Y} \theta_{\boldsymbol{u}}(\rho(a_1)), \ldots, \boldsymbol{Y} \theta_{\boldsymbol{u}}(\rho(a_m)))(d)
$$

as an element of $L[\![\boldsymbol{w}]\!]\{L[\![\boldsymbol{Y}]\!]\}_\theta$, where $\boldsymbol{Y}$ is considered as an n-tuple of iterative differential variables and $F^{\theta_{\boldsymbol{u}}}$ denotes the differential polynomial in $X_{a_1}, \ldots, X_{a_m}$ obtained from F by applying $\theta_{\boldsymbol{u}}$ to its coefficients. Let I be the ideal generated by all such F_d. Then the image of (2.4) is equal to $Z(I)$. $\qquad \square$

Corollary 2.15. *The functor* $\mathrm{Ume}(L|K)$ *is a formal group scheme over* L.

Proof. This follows from theorem 2.14 and proposition 2.12. $\qquad \square$

Example 2.16. *In the situation of example 2.4 the Umemura functor* $\mathrm{Ume}(L|K)$ *is isomorphic to the functor* G_+ *(cf. example 2.9) and thus to the additive formal group scheme* $\hat{\mathbb{G}}_a$.

Proof. Let A be a commutative L-algebra. Then every $\varphi \in \mathrm{Ume}(L|K)(A)$ is determined by $\varphi(\rho(y) \otimes 1)$. The relation $\theta_y^{(1)}(\rho(y)) = 1$ implies

$$
(2.6) \qquad\qquad\qquad \theta^{(1)}(\varphi(\rho(y) \otimes 1)) = 1,
$$

where θ denotes the iterative derivation on $\mathcal{L} \hat{\otimes}_L A[\![w]\!]$ induced by $\theta_u (= \theta_y)$ on $\mathcal{L}$ and θ_w on $A[\![w]\!]$. Since for all $k \geq 2$ we have $\theta_y^{(k)}(\rho(y)) = 0$, it follows

$$
(2.7) \qquad\qquad\qquad \theta^{(k)}(\varphi(\rho(y) \otimes 1)) = 0.
$$

By theorem 2.14, there exists a $\Phi \in \Gamma_{1L}(A)$ such that $\varphi(\rho(y) \otimes 1) = \sum_{k \in \mathbb{N}} \theta_y^{(k)}(\rho(y)) \otimes (\Phi - w)^k$, cf. equation (2.5). In our situation this becomes

$$\varphi(\rho(y) \otimes 1) = \sum_{k \in \mathbb{N}} \theta_y^{(k)}(\rho(y)) \otimes (\Phi - w)^k = \rho(y) \otimes 1 + 1 \otimes (\Phi - w).$$

Therefore, if we write $\Phi = \sum_{i \in \mathbb{N}} a_i w^i$, then

$$\varphi(\rho(y) \otimes 1) = (y + t) \otimes 1 + 1 \otimes (\sum_{i \in \mathbb{N}} a_i w^i - w).$$

From (2.6) and (2.7) we obtain $\sum_{i \geq 1} a_i i w^{i-1} = 1$ and $\sum_{i \in \mathbb{N}} a_i \theta_w^{(k)}(w^i) = 0$, which implies $a_1 = 1$ and $a_k = 0$ for all $k \geq 2$. Hence $\varphi(\rho(y) \otimes 1) = \rho(y) \otimes 1 + 1 \otimes a_0$ and $\Phi = a_0 + w$ with $a_0 \in N(A)$. The elements $\Phi \in \Gamma_{1L}(A)$ of this form are the elements of $G_+(A)$. Conversely, the automorphisms φ of the form $\varphi(\rho(y) \otimes 1) = \rho(y) \otimes 1 + 1 \otimes a_0$ belong to $\mathrm{Ume}(L|K)(A)$. $\qquad\square$

Example 2.17. *In the situation of example 2.5 the Umemura functor* $\mathrm{Ume}(L|K)$ *is isomorphic to the functor* $\tilde{G}_*$ *(cf. example 2.11) and thus to the multiplicative formal group scheme* $\hat{\mathbb{G}}_m$.

Proof. Let A be a commutative L-algebra. Then every $\varphi \in \mathrm{Ume}(L|K)(A)$ is determined by $\varphi(\rho(y) \otimes 1)$. The relations $\rho(y) = y\theta_y^{(1)}(\rho(y))$ and $\theta_y^{(k)}(\rho(y)) = 0$ imply

$$\varphi(\rho(y) \otimes 1) = (y \otimes 1)\theta^{(1)}(\varphi(\rho(y) \otimes 1)) \quad \text{and} \quad \theta^{(k)}(\varphi(\rho(y) \otimes 1)) = 0$$

for all $k \geq 2$. By theorem 2.14 there exists a $\Phi \in \Gamma_1(A)$ such that

$$\varphi(\rho(y) \otimes 1) = \sum_{k \in \mathbb{N}} \theta_y^{(k)}(\rho(y)) \otimes (\Phi - w)^k,$$

cf. equation (2.5), which becomes

$$\varphi(\rho(y) \otimes 1) = \rho(y) \otimes 1 + \rho(y)/y \otimes (\Phi - w)$$

here. It follows

$$\rho(y) \otimes 1 + \rho(y)/y \otimes (\Phi - w) = (y \otimes 1)(\theta^{(1)}(\rho(y) \otimes 1 + \rho(y)/y \otimes (\Phi - w)))$$
$$= \rho(y) \otimes 1 + \rho(y) \otimes (\theta^{(1)}(\Phi) - 1))$$

and therefore

$$\Phi = (y + w)\theta^{(1)}(\Phi) - y.$$

$\qquad\square$

3. 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 D-module algebras (cf. [AM05]), where D is a bialgebra over a field C. They restrict themselves to the case where the bialgebra D is a pointed cocommutative Hopf algebra such that its irreducible component of 1 is of Birkhoff-Witt type. This excludes bialgebras such as D_{end} (cf. example 1.8 (3)). Here we sketch how their definitions and some of their results can be generalized to include this case as well.

Notation: *Let C be a field, G be a monoid and D^1 be a pointed irreducible cocommutative Hopf algebra of Birkhoff-Witt type over C such that D^1 is a CG-module bialgebra. We define $D := D^1 \# CG$ and consider it as a bialgebra as in lemma 1.30.*

Definition 3.1. *An extension of Artinian simple commutative D-module algebras $(L, \rho_L)|(K, \rho_K)$ is* Picard-Vessiot *if the following hold:*

(1) *The elements $g \in G$ operate as injective endomorphisms on L.*

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

(3) *There exists an intermediate D-module algebra (R, ρ_R) of $K \subseteq L$ such that the total ring of fractions $\mathrm{Q}(R)$ 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 R-algebra, i.e.
$$R \cdot H = R \otimes_K R.$$

The Picard-Vessiot extension $L|K$ is called finitely generated *if it is finitely generated as extension of Artinian simple D-module algebras.*

Proposition 3.2. *Let $L|K$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras with constants $k := L^\rho$ and (R, ρ_R) and H be as in definition 3.1. Then the following hold:*

(1) *The homomorphism*

(3.1) $$\mu \colon R \otimes_k H \to R \otimes_K R, \quad a \otimes h \mapsto (a \otimes 1) \cdot h$$

is an isomorphism of D-module algebras, where $R \otimes_k H$ carries the D-module algebra structure induced by ρ_R on R and ρ_0 on H and $R \otimes_K R$ the one induced by ρ_R on both factors.

(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 of H is induced by the homomorphism
$$\tau \colon R \otimes_K R \to R \otimes_K R, \quad a \otimes b \mapsto b \otimes a.$$

(3) *The intermediate D-module algebra (R, ρ_R) satisfying condition (3) in definition 3.1 is unique.*

Proof. This can be proven essentially as [AM05, Proposition 3.4], only the proof of (3) needing a slight adaption:

If R_1 and R_2 satisfy condition (3) in definition 3.1, then $R_1 R_2$ satisfies it too. Therefore we can assume that R_1 is included in R_2. We denote by H_1 and H_2 the constants of the D-module algebras $R_1 \otimes_K R_1$ and $R_2 \otimes_K R_2$, where the D-module algebra structures are induced by ρ_{R_1} and ρ_{R_2} on both factors, respectively. Then H_1 is a Hopf subalgebra of H_2 and thus H_2 is faithfully flat over H_1 by [Wat79, Chapter 14]. Therefore $L \otimes_k H_2$ is faithfully flat over $L \otimes_k H_1$. By proposition 1.34, the K-module L is projective and so in particular flat. By [Bou85, Chapitre 1, §3.5,

Proposition 9], L is also faithfully flat over K and therefore $L \otimes_K R_1$ is faithfully flat over R_1 (cf. [Bou85, Chapitre 1, §3.3, Proposition 5]). Since by the above $L \otimes_K R_2 \cong L \otimes_k H_2$ is faithfully flat over $L \otimes_K R_1 \cong L \otimes_k H_1$, $L \otimes_K R_2$ is also faithfully flat over R_1 (cf. [Bou85, Chapitre I, §3.4, Proposition 7]) and hence R_2 is faithfully flat over R_1. Thus for each $r_1 \in R_1$ we have $r_1 R_1 = r_1 R_2 \cap R_1$. For any $r_2 \in R_2$ there exists a non-zero divisor $r_1 \in R_1$ such that $r_1 r_2 \in R_1$, since $R_2 \subseteq L = Q(R_1)$, and so $r_1 r_2 \in r_1 R_2 \cap R_1 = r_1 R_1$. Therefore $r_2 \in R_1$, i.e. $R_2 = R_1$. $\qquad\square$

Definition 3.3. *If $L|K$ is a Picard-Vessiot extension of Artinian simple commutative D-module algebras, then R and H in definition 3.1 are called the* principal *D-module algebra[3] and the* Hopf algebra *of $L|K$, respectively. If we want to indicate R and H, we denote the Picard-Vessiot extension $L|K$ also by $(L|K, R, H)$.*

Definition 3.4. *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 $\mathrm{Spec}\, H$ over L^ρ.*

Proposition 3.5. *Let $(L|K, R, H)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras with constants $k := L^\rho$. Then for any commutative k-algebra A the A-points of $\mathrm{Gal}(L|K) = \mathrm{Spec}\, H$ are isomorphic to the group of automorphisms of the D-module algebra $(R \otimes_k A, \rho \otimes \rho_0)$ that leave $K \otimes_k A$ fixed.*

Proof. This can be proven as [Ama05, Theorem 3.6.1]. $\qquad\square$

Proposition 3.6. *Let $(L|K, R, H)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras.*

    (1) Then R is a simple D-module algebra.
    (2) The ring R is isomorphic to $\prod_{P \in \Omega(L)} R/(P \cap R)$.

Proof.   (1) This can be proven as [AM05, Corollary 3.12] (cf. also [Ama05, Proposition 3.5.9]). In its proof [AM05, Proposition 3.10 (i)] is used, which also holds in our generalized setting.

    (2) The ring L is a localization of R and thus $\Omega(L) \to \Omega(R), P \mapsto P \cap R$ is an injection. We obtain an injective homomorphism

$$(3.2) \qquad\qquad R \to \prod_{P \in \Omega(L)} R/(P \cap R).$$

    If for minimal prime ideals $P, Q \in \Omega(L)$, the ideal $J := (P \cap R) + (Q \cap R)$ would be strictly smaller than R, then as in the proof of 1.32 (1), using that R is simple as a D-module algebra, one can show that $J = P \cap R = Q \cap R$, i.e. that $P = Q$. Therefore (3.2) is an isomorphism.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Proposition 3.7. *Let $(L|K, R, H)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras. Let further $\Omega(K) = \{P_1, \ldots, P_m\}$ and for all $i \in \{1, \ldots, m\}$ let $Q_{i,1}, \ldots, Q_{i,r_i}$ be the minimal prime ideals of L lying over P_i. We define $L_i := \prod_{j=1}^{r_i} L/Q_{i,j}$, $R_i := \prod_{j=1}^{r_i} R/(Q_{i,j} \cap R)$, $K_i := K/P_i$, $L_{i,j} := L/Q_{i,j}$ and $R_{i,j} := R/(Q_{i,j} \cap R)$ for all $j \in \{1, \ldots, r_i\}$. We denote by k the field of constants*

---

    [3]In Picard-Vessiot theory of differential and difference equations, this algebra is usually called *Picard-Vessiot ring.*

of L. Then $(L_i|K_i, R_i, H)$ is a Picard-Vessiot extension of Artinian simple $D(G_{P_i})$-module algebras for all $i \in \{1, \ldots, m\}$.

Proof. For each $i \in \{1, \ldots, m\}$ we denote by $\pi_i \colon R \to R_i$ the canonical homomorphism. Since L has Krull dimension 0, we see that $Q_{i,j_1} + Q_{i,j_2} = L$ and thus $(Q_{i,j_1} \cap R) + (Q_{i,j_2} \cap R) = R$ for all $j_1 \neq j_2 \in \{1, \ldots, r_i\}$. Hence π_i is surjective. If we denote by μ_i the homomorphism $R_i \otimes_k H \to R_i \otimes_{K_i} R_i, r_i \otimes h \mapsto (r_i \otimes 1)h$, then the diagram

$$
\begin{array}{ccc}
R \otimes_k H & \xrightarrow{\ \mu\ } & R \otimes_K R \\
\downarrow{\scriptstyle \pi_i \otimes \mathrm{id}} & & \downarrow{\scriptstyle \pi_i \otimes \pi_i} \\
R_i \otimes_k H & \xrightarrow{\ \mu_i\ } & R_i \otimes_{K_i} R_i
\end{array}
$$

commutes and since μ is an isomorphism, μ_i is an isomorphism too. We note that also $L_i^{D(G_{P_i})} = L^D = K^D = K_i^{D(G_{P_i})}$. Finally, also $\mathrm{Q}(R_i) = L_i$, since if S is the set of non-zero divisors of R, then $(S^{-1}R)/S^{-1}(Q_{i,j} \cap R) \cong \bar{S}^{-1}(R/(Q_{i,j} \cap R))$, where $\bar{S}$ is the image of S under $R \to R/(Q_{i,j} \cap R)$. We note that $S^{-1}(Q_{i,j} \cap R) = Q_{i,j}$ and that $\bar{S}$ is the set of non-zero divisors of $R_{i,j}$. Therefore $\mathrm{Q}(R_{i,j}) \cong L_{i,j}$ and thus $\mathrm{Q}(R_i) \cong L_i$. $\qquad\square$

Proposition 3.8. *Let $(L|K, R, H)$ be a Picard-Vessiot extension of Artinian simple commutative D-module algebras such that R is a finitely generated K-algebra and H is a finitely generated k-algebra. Then with the notation of proposition 3.7 we have:*

(1) The following conditions are equivalent:
  (a) R is smooth over K,
  (b) R_i is smooth over K_i for all $i \in \{1, \ldots, m\}$,
  (c) H is smooth over k and
  (d) $\mathrm{Gal}(L|K)$ is smooth over k.
(2) The following conditions are also equivalent:
  (e) L_i is separable over K_i for all $i \in \{1, \ldots, m\}$,
  (f) R_i is separable over K_i for all $i \in \{1, \ldots, m\}$ and
  (g) $\bar{k} \otimes_k H$ is reduced.
(3) The equivalent conditions in (1) imply those of (2). If k is perfect, then the converse holds and these conditions are further equivalent to the following:
  (h) H is reduced and
  (i) $R \otimes_K R$ is reduced.

Proof. We first prove (d) $\Leftrightarrow$ (c) $\Leftrightarrow$ (a) $\Leftrightarrow$ (b) $\Rightarrow$ (e) $\Leftrightarrow$ (f) $\Leftrightarrow$ (g):

The equivalence of (c) and (d) is clear.

By [Gro67, Chapitre IV, 17.7.3 (ii)], $R \otimes_K R$ is smooth over R if and only if R is smooth over K. In the same way H is smooth over k if and only if $R \otimes_k H$ is smooth over R. Since $R \otimes_K R \cong R \otimes_k H$, we conclude that R is smooth over K if and only if H is smooth over k.

Since smoothness is a local property (cf. [Gro67, Chapitre IV, 17.3.2 (iii)]) and since $R \cong \prod_{i=1}^m R_i$ and $K \cong \prod_{i=1}^m K_i$, R is smooth over K if and only if R_i is smooth over K_i for all $i \in \{1, \ldots, m\}$.

If R_i is smooth over K_i, then L_i is formally smooth over K_i, since as a localization L_i is formally étale over R_i. By [Gro67, Chapitre IV, 17.1.6] we see that L_i is

formally smooth over K_i if and only if $L_{i,j}$ is formally smooth over K_i for all $j \in \{1, \ldots, r_i\}$. By the theorem of Cohen (cf. [Gro64, Chapitre 0, 19.6.1]) $L_{i,j}$ is formally smooth over K_i if and only if it is separable over K_i. The product $L_i = \prod_{j=1}^{r_i} L_{i,j}$ is separable over K_i if and only if each $L_{i,j}$ is separable over K_i. Thus L_i is formally smooth over K_i if and only if it is separable over K_i.

If L_i is separable over K_i, then obviously R_i is also separable over K_i and the converse holds too (cf. [Bou81, Chapitre V, §15.2, Proposition 4]).

By proposition 3.7, $(L_i|K_i, R_i, H)$ is a Picard-Vessiot extension of $D(G_{P_i})$-module algebras for all $i \in \{1, \ldots, m\}$. Therefore we have an isomorphism

$$R_i \otimes_{K_i} R_i \cong R_i \otimes_k H.$$

Let $\mathfrak{m}_i$ be a maximal ideal of R_i. Then $R_i/\mathfrak{m}_i$ can be embedded into an algebraic closure $\bar{K}_i$ of K_i by Hilbert's Nullstellensatz. We extend the induced isomorphism

$$R_i/\mathfrak{m}_i \otimes_{K_i} R_i \cong R_i/\mathfrak{m}_i \otimes_k H.$$

to an isomorphism

$$\overline{K_i} \otimes_{K_i} R_i \cong \overline{K_i} \otimes_k H.$$

Since R_i is separable over K_i if and only if $\overline{K_i} \otimes_{K_i} R_i$ is reduced, and since $\overline{K_i} \otimes_k H$ is reduced if and only if $\bar{k} \otimes_k H$ is reduced, the equivalence of (f) and (g) follows.

We now prove that (c) $\Leftrightarrow$ (g) $\Leftrightarrow$ (h) $\Leftrightarrow$ (i) if k is perfect:

Since k is perfect, the affine group scheme $\mathrm{Gal}(L|K) = \mathrm{Spec}\, H$ is smooth over k if and only if $\bar{k} \otimes_k H$ is reduced (cf. [Wat79, 11.6]) if and only if H is reduced (cf. [Bou81, Chapitre V, §15.2, Proposition 5]). Since R is reduced, H is reduced if and only if $R \otimes_k H \cong R \otimes_K R$ is reduced. $\square$

4. Comparison with Picard-Vessiot theory

In this section we examine the Galois hull $\mathcal{L}|\mathcal{K}$ defined above in the case where $(L|K, R, H)$ is a finitely generated Picard-Vessiot extension of Artinian simple commutative D-module algebras such that R is smooth over K 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.

Notation: *Let C be a field, G be a monoid and D^1 be a pointed irreducible cocommutative Hopf algebra of Birkhoff-Witt type over C such that D^1 is a CG-module bialgebra. We define $D := D^1 \# CG$. 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, then this is the case by [AM05, Theorem 4.6]). Let $\Omega(K) = \{P_1, \ldots, P_m\}$ be the set of minimal prime ideals of K and for each $i \in \{1, \ldots, m\}$ let $Q_{i,1}, \ldots, Q_{i,r_i}$ be the minimal prime ideals of L lying over P_i. We define $K_i := K/P_i$, $L_{i,j} := L/Q_{i,j}$, $L_i := \prod_{j=1}^{r_i} L/Q_{i,j}$ and $R_i := \prod_{j=1}^{r_i} R/(Q_{i,j} \cap R)$. By proposition 3.8, L_i is separable over K_i for all $i \in \{1, \ldots, m\}$ and thus all $L_{i,j}$ ($j \in \{1, \ldots, r_i\}$) are separable over K_i. We assume that the transcendence degree of $L_{i,j}$ over K_i is the same for all $i \in \{1, \ldots, m\}$ and all $j \in \{1, \ldots, r_i\}$, say n. Let $\boldsymbol{u}^{(i,j)} = (u_1^{(i,j)}, \ldots, u_n^{(i,j)})$ be a separating transcendence basis for the extension $L_{i,j}$ over K_i and let $\theta_{\boldsymbol{u}}$ be the n-variate iterative derivation (2.1) on L over K. We denote by Ψ the D-module algebra structure on L, by ρ the associated homomorphism of C-algebras and by $k := L^\rho$ the field of constants of L.*

Lemma 4.1. *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; i.e. with the notation of subsection 2.2 there is an isomorphism*

$$(4.1) \qquad \mathcal{L} = \rho_0(L)[\rho(L)] \cong \rho_0(L) \otimes_k \rho(L)$$

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. there is an isomorphism of D-module algebras

$$(4.2) \qquad \rho_0(L)[\rho(R)] \cong \rho_0(L) \otimes_k \rho(R).$$

Proof. The element $Z := \rho(X)\rho_0(X)^{-1}$ lies in $\mathrm{GL}_n(_C\mathcal{M}(D, K))$ and so

$$\rho_0(L)[\rho(R)] = \mathcal{K}[\rho(R)] = \mathcal{K}[\rho(X), \rho(X)^{-1}] = \mathcal{K}[Z, Z^{-1}]$$

is closed under $\theta_{\boldsymbol{u}}$. Since $\rho(L) = \mathrm{Q}(\rho(R))$, for every non-zero divisor $a \in R$ the element $\theta_{\boldsymbol{u}}(\rho(a))$ is invertible in $\rho_0(L)[\rho(L)][\![\boldsymbol{w}]\!]$ by [Swe69, Lemma 9.2.3]. Thus, $\rho_0(L)[\rho(L)]$ is also closed under $\theta_{\boldsymbol{u}}$.

It follows from lemma 1.27 that $\rho(L)$ and $\rho_0(L)$ are linearly disjoint over k and thus that $\mathcal{L}$ and $\rho_0(L) \otimes_k \rho(L)$ are isomorphic as D-module algebras. Since $\rho(R)$ is a subalgebra of $\rho(L)$, the algebras $\rho(R)$ and $\rho_0(L)$ are also linearly disjoint over k and we obtain the isomorphism (4.2). $\qquad\square$

Lemma 4.2. *We assume that the field of constants k is perfect. Then there exists a finite étale extension K' of K, a matrix $B \in \mathrm{GL}_n(K')$ and a right $R \otimes_K K'$-linear automorphism γ of the D-module algebra $(R \otimes_k R \otimes_K K', \rho \otimes \rho_0 \otimes \rho_0)$, defined by*

$$(4.3) \qquad \gamma(X \otimes 1 \otimes 1) := (X \otimes 1 \otimes 1)(1 \otimes X^{-1} \otimes 1)(1 \otimes 1 \otimes B).$$

Proof. Let $\eta \colon (R, \rho_R) \to (R \otimes_k H, \rho_R \otimes \rho_0)$ be the homomorphism of D-module algebras defined by $\eta(a) := \mu^{-1}(1 \otimes a)$ for all $a \in R$, where $\mu \colon R \otimes_k H \to R \otimes_K R$ is the isomorphism of D-module algebras (3.1). Then η fulfills

$$(4.4) \qquad \eta(X) = (X \otimes (1 \otimes 1))(1 \otimes (X^{-1} \otimes 1)(1 \otimes X)).$$

By proposition 3.7, $L_i|K_i$ is a Picard-Vessiot extension for all $i \in \{1, \ldots, m\}$ and by proposition 3.8, $\mathrm{Gal}(L_i|K_i)$ is smooth over k. Since the K_i-algebra R_i is finitely generated, $\mathrm{Spec}\, R_i$ has a point in the algebraic closure of K_i by Hilbert's Nullstellensatz. Since $\mathrm{Spec}\, R_i$ is a principal homogeneous space for the smooth affine group scheme $\mathrm{Gal}(L_i|K_i)$, it has in fact a point in a finite separable field extension of K_i (cf. [Wat79, 18.5]). Together they provide a point $\nu \colon R \to K'$ of $\mathrm{Spec}\, R = \mathrm{Spec} \prod_{i=1}^m R_i$ in a finite étale extension K' of K. We extend the composition

$$R \xrightarrow{\eta} R \otimes_k H \hookrightarrow R \otimes_k R \otimes_K R \xrightarrow{\mathrm{id}_R \otimes_k \mathrm{id}_R \otimes_K \nu} R \otimes_k R \otimes_K K'$$

right $R \otimes_K K'$-linearly to an endomorphism γ of $R \otimes_k R \otimes_K K'$ and we define $B := \nu(X)$. Then the defining identity (4.3) for γ follows from equation (4.4) and clearly γ is a homomorphism of D-module algebras. The inverse of γ is given by the right $R \otimes_K K'$-linear extension of

$$R \xrightarrow{\eta} R \otimes_k H \xrightarrow{\mathrm{id}_R \otimes_k S} R \otimes_k H \hookrightarrow R \otimes_k R \otimes_K R \xrightarrow{\mathrm{id}_R \otimes_k \mathrm{id}_R \otimes_K \nu} R \otimes_k R \otimes_K K'$$

to an endomorphism of $R \otimes_k R \otimes_K K'$, where S is the antipode of H.

$\square$

Theorem 4.3. *If the field of constants k 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. Let A be a commutative L-algebra. By remark 3.5, $\mathrm{Gal}(L|K)(A)$ is isomorphic to the group $\mathrm{Aut}_D(R \otimes_k A | K \otimes_k A)$ of automorphisms of the D-module algebra $R \otimes_k A$ that leave $K \otimes_k A$ fixed. Thus $\widehat{\mathrm{Gal}(L|K)}(A)$ is isomorphic to the kernel

$$(4.5) \qquad \mathrm{Ker}\left(\mathrm{Aut}_D(R \otimes_k A | K \otimes_k A) \to \mathrm{Aut}_D(R \otimes_k A/N(A) | K \otimes_k A/N(A))\right).$$

The isomorphisms (4.1) and (4.2) induce isomorphisms of algebras

$$(4.6) \qquad\qquad\qquad \mathcal{L} \hat{\otimes}_L A[\![\boldsymbol{w}]\!] \cong (L \otimes_k A)[\![\boldsymbol{w}]\!]$$

and

$$(4.7) \qquad\qquad\qquad \rho_0(L)[\rho(R)] \hat{\otimes}_L A[\![\boldsymbol{w}]\!] \cong (R \otimes_k A)[\![\boldsymbol{w}]\!].$$

Using these isomorphisms it is easy to see that $\mathrm{Ume}(L|K)(A)$ is isomorphic to the group of automorphisms of the $D \otimes_C D_{ID^n}$-module algebra $\rho_0(L)[\rho(R)] \hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ that leave $\mathcal{K} \hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ fixed and are congruent to the identity modulo $\rho_0(L)[\rho(R)] \hat{\otimes}_L N(A)[\![\boldsymbol{w}]\!]$. We denote the latter by $\mathrm{Ume}(R|K)(A)$.

By lemma 4.2, there exists a finite étale extension K' of K, a matrix $B \in \mathrm{GL}_n(K')$ and a right $R \otimes_K K'$-linear automorphism γ of the D-module algebra $(R \otimes_k R \otimes_K K', \rho \otimes \rho_0 \otimes \rho_0)$ defined by

$$\gamma(X \otimes 1 \otimes 1) \coloneqq (X \otimes 1 \otimes 1)(1 \otimes X^{-1} \otimes 1)(1 \otimes 1 \otimes B).$$

There exists a finite étale extension L' of L containing K' and γ induces a left K-linear and right L'-linear automorphism $\bar{\gamma}$ of the D-module algebra $(R \otimes_k L', \rho \otimes \rho_0)$ defined by $\bar{\gamma}(X \otimes 1) \coloneqq (X \otimes 1)(1 \otimes X^{-1}B)$. The n-variate iterative derivation $\theta_{\boldsymbol{u}}$ extends uniquely from L to L' (cf. [Mat89, Theorem 27.2] or [Hei10, Proposition 1.2.2]) and we denote it again by $\theta_{\boldsymbol{u}}$. The ring $R \otimes_k L'$ is generated by $\bar{\gamma}(R \otimes_k 1)$ and $1 \otimes_k L'$, which are linearly disjoint over k by lemma 1.27 (note that by proposition 3.6, the D-module algebra R is simple); we have an isomorphism of D-module algebras

$$(4.8) \qquad\qquad R \otimes_k L' = \bar{\gamma}(R \otimes_k 1)[1 \otimes_k L'] \cong \bar{\gamma}(R \otimes_k 1) \otimes_k L',$$

where the D-module algebra structure on $\bar{\gamma}(R \otimes_k 1) \otimes_k L'$ is $\rho \otimes_k \rho_0 \otimes_k \rho_0$. The isomorphism (4.2) of D-module algebras extends L'-linearly to an isomorphism

$$(4.9) \qquad\qquad R \otimes_k L' \xrightarrow{\rho \otimes_k \rho_0} \rho(R) \otimes_k \rho_0(L') \xrightarrow{\ m\ } \rho_0(L')[\rho(R)],$$

where $R \otimes_k L'$ carries the D-module algebra structure $\rho \otimes_k \rho_0$ and m is the restriction of the multiplication homomorphism of $\rho_0(L')[\rho(R)]$. The image of $\bar{\gamma}(R \otimes_k 1)$ under this isomorphism in $\rho_0(L')[\rho(R)]$ is $\rho(K)[Z, Z^{-1}]$ with $Z \coloneqq \rho(X)\rho_0(X)^{-1}\rho_0(B)$ and the image of $1 \otimes_k L'$ under it is $\rho_0(L')$. Thus, we obtain an isomorphism of

$D \otimes_C D_{ID^n}$-module algebras

$$(4.10) \qquad R\otimes_k L' \longrightarrow \bar\gamma(R\otimes_k 1)\otimes_k L' \xrightarrow{m\circ(\rho\otimes\rho_0)\otimes\rho_0} \rho(K)[Z,Z^{-1}]\otimes_k \rho_0(L') \xrightarrow{m} \rho_0(L')[\rho(R)],$$

$$\rho\otimes\rho_0 \qquad\qquad \rho\otimes\rho_0\otimes\rho_0 \qquad\qquad\qquad \rho_{int}\otimes\rho_{int} \qquad\qquad \rho_{int}$$

$$\theta_0\otimes\theta_{\boldsymbol u} \qquad\qquad (\theta_0\otimes\theta_0)\otimes\theta_{\boldsymbol u} \qquad\qquad\qquad \theta_{\boldsymbol u}\otimes\theta_{\boldsymbol u} \qquad\qquad \theta_{\boldsymbol u}$$

where the isomorphism at the left is (4.8) and the D- and D_{ID^n}-module algebra structures are indicated in the two rows below the isomorphisms (θ_0 denotes the trivial n-variate iterative derivation). For every commutative L'-algebra A, the isomorphism (4.10) gives rise to an isomorphism of $D \otimes_C D_{ID^n}$-module algebras

(4.11)

$$\rho_0(L)[\rho(R)]\hat\otimes_L A[\![\boldsymbol w]\!] \to \rho_0(L')[\rho(R)]\hat\otimes_{L'} A[\![\boldsymbol w]\!] \to (R\otimes_k L')\hat\otimes_{L'} A[\![\boldsymbol w]\!] \to (R\otimes_k A)[\![\boldsymbol w]\!],$$

where on $(R \otimes_k A)[\![\boldsymbol w]\!]$ the D-module algebra structure is given by $\rho \otimes_k \rho_0$ on the coefficients with respect to $\boldsymbol w$ (as in (1.4)) and the D_{ID^n}-module algebra structure is given by the n-variate iterative derivation $\theta_{\boldsymbol w}$ (cf. 1.16).

Given a $\varphi \in \mathrm{Ume}(R|K)(A)$, we obtain by composition with the vertical isomorphisms of $D \otimes_C D_{ID^n}$-module algebras, given by (4.11), in the diagram

$$
\begin{array}{ccc}
\rho_0(L)[\rho(R)]\hat\otimes_L A[\![\boldsymbol w]\!] & \xrightarrow{\ \varphi\ } & \rho_0(L)[\rho(R)]\hat\otimes_L A[\![\boldsymbol w]\!] \\
\downarrow{\scriptstyle\sim} & & \uparrow{\scriptstyle\sim} \\
(R\otimes_k A)[\![\boldsymbol w]\!] & \xrightarrow{\ \sigma[\![\boldsymbol w]\!]\ } & (R\otimes_k A)[\![\boldsymbol w]\!],
\end{array}
$$

an automorphism of the $D \otimes_C D_{ID^n}$-module algebra $(R \otimes_k A)[\![\boldsymbol w]\!]$, which is of the form $\sigma[\![\boldsymbol w]\!]$, where σ is an automorphism of the D-module algebra $R \otimes_k A$ of constants of the iterative derivation $\theta_{\boldsymbol w}$ on $(R \otimes_k A)[\![\boldsymbol w]\!]$. Then σ is an element of the kernel (4.5) and this yields an isomorphism of groups between $\mathrm{Ume}(R|K)(A)$ and (4.5). □

Corollary 4.4. *Under the assumptions of theorem 4.3 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 4.3 by taking $A = L'[\varepsilon]/(\varepsilon^2)$. □

In the case where $D = D_{end}$, the statement of corollary 4.4 is similar to the one of [Mor09, Theorem 3.3] and to [Ume]. Taking $D = D_{der}$, it provides a similar result as [Ume96, Theorem 5.15] in the case of finitely generated Picard-Vessiot extensions of differential fields in characteristic zero.

Example 4.5. *Let $L|K$ be the extension of example 2.4 (resp. example 2.5). It is a Picard-Vessiot extension, in theorem 4.3 the extension L' can be chosen to be L and for every commutative L-algebra A, the element $\varphi \in \mathrm{Ume}(L|K)(A)$ given by $\varphi(\rho(y)\otimes 1) = \rho(y)\otimes 1 + 1\otimes a_0$ for some $a_0 \in N(A)$ (resp. $\varphi(\rho(y)\otimes 1) = \rho(y)\otimes(1+a_1)$ for some $a_1 \in N(A)$) corresponds under the isomorphism in theorem 4.3 to the automorphism $\sigma \in \widehat{\mathrm{Gal}(L|K)}(A)$ that fulfills $\sigma(y \otimes 1) = y \otimes 1 + 1 \otimes a_0$ (resp. $\sigma(y \otimes 1) = y \otimes (1+a_1)$).*

Acknowledgements. I thank Hiroshi Umemura for helpful discussions on the topic of the article.

References

[AM05]   Katsutoshi Amano and Akira Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *J. Algebra*, 285(2):743–767, 2005.

[Ama05]   Katsutoshi Amano. Relative invariants, difference equations, and the Picard-Vessiot theory. 2005, math/0503291.

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

[Bou85]   Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 1 à 4. [Commutative algebra. Chapters 1–4], Reprint.

[BW03]   Tomasz Brzezinski and Robert Wisbauer. *Corings and comodules*, volume 309 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[Cas06]   Guy Casale. Enveloppe galoisienne d'une application rationnelle de $\mathbb{P}^1$. *Publ. Mat.*, 50(1):191–202, 2006.

[Cas07]   Guy Casale. The Galois groupoid of Picard-Painlevé VI equation. In *Algebraic, analytic and geometric aspects of complex differential equations and their deformations. Painlevé hierarchies*, RIMS Kôkyûroku Bessatsu, B2, pages 15–20. Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.

[Cas08]   Guy Casale. Le groupoï de de Galois de P_1 et son irréductibilité. *Comment. Math. Helv.*, 83(3):471–519, 2008.

[CH11]   Teresa Crespo and Zbigniew Hajto. *Algebraic groups and differential Galois theory*, volume 122 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[Gra09]   Anne Granier. *Un D-groupoï de de Galois pour les équations aux q-différences*. PhD thesis, Institut de Mathématiques de Toulouse, Université Paul Sabatier, Toulouse, 2009.

[Gro64]   Alexander Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I. *Inst. Hautes Études Sci. Publ. Math.*, (20):259, 1964.

[Gro67]   Alexander Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[Har10]   Charlotte Hardouin. Iterative q-difference galois theory. *J. Reine Angew. Math.*, 644:101–144, 2010.

[Haz78]   Michiel Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[Haz79]   Michiel Hazewinkel. Infinite-dimensional universal formal group laws and formal A-modules. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 124–143. Springer, Berlin, 1979.

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

[Hei10]   Florian Heiderich. *Galois Theory of Module Fields*. PhD thesis, Universitat de Barcelona, Departament d'Àlgebra i Geometria, 2010. Available from: `http://hdl.handle.net/10803/674`.

[HS37]   Helmut Hasse and Friedrich Karl Schmidt. Noch eine Begründung der Theorie des höheren Differentialquotienten in einem algebraischen Funktionenkörper in einer Unbestimmten. *J. Reine Angew. Math.*, 177:215–237, 1937.

[HS70]   Robert G. Heyneman and Moss E. Sweedler. Affine Hopf algebras. II. *J. Algebra*, 16:271–297, 1970.

[Kei97]   William F. Keigher. On the ring of Hurwitz series. *Comm. Algebra*, 25(6):1845–1859, 1997.

[Mac71] Saunders MacLane. *Categories for the working mathematician*. Springer-Verlag, New York, 1971. Graduate Texts in Mathematics, Vol. 5.

[Mal01] Bernard Malgrange. Le groupoï de de Galois d'un feuilletage. In *Essays on geometry and related topics, Vol. 1, 2*, volume 38 of *Monogr. Enseign. Math.*, pages 465–501, Geneva, 2001. Enseignement Math.

[Mas10] Akira Masuoka. The $\times_r$-bialgebra associated with an iterative q-difference ring. preprint, 2010.

[Mat89] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, Cambridge-New York, 1989.

[Mau10] Andreas Maurischat. Infinitesimal group schemes as iterative differential Galois groups. *J. Pure Appl. Algebra*, 214(11):2092–2100, 2010.

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

[Mor09] Shuji Morikawa. On a general difference Galois theory I. *Ann. Inst. Fourier (Grenoble)*, 59(7):2709–2732, 2009.

[MU09] Shuji Morikawa and Hiroshi Umemura. On a general difference Galois theory II. *Ann. Inst. Fourier (Grenoble)*, 59(7):2733–2771, 2009.

[MvdP03] Bernd Heinrich Matzat and Marius van der Put. Iterative differential equations and the Abhyankar conjecture. *J. Reine Angew. Math.*, 557:1–52, 2003.

[Oku87] Kôtaro Okugawa. *Differential Algebra of Nonzero Characteristic*, volume 16 of *Lectures in Mathematics*. Kinokuniya Company Ltd., Tokyo, 1987.

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

[Ume] Hiroshi Umemura. Picard-Vessiot theory in general Galois theory. preprint.

[Ume96] Hiroshi Umemura. Differential Galois theory of infinite dimension. *Nagoya Math. J.*, 144:59–135, 1996.

[Ume06] Hiroshi Umemura. Galois theory and Painlevé equations. In *Théories asymptotiques et équations de Painlevé*, volume 14 of *Sémin. Congr.*, pages 299–339, Paris, 2006. Soc. Math. France.

[vdPS97] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[vdPS03] Marius van der Put and Michael F. Singer. *Galois Theory of Linear Differential Equations*. Springer, Berlin, 2003.

[Wat79] William C. Waterhouse. *Introduction to Affine Group Schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU, CASE 247, UNIVERSITÉ PIERRE ET MARIE CURIE, 4 PLACE JUSSIEU, 75252 PARIS CEDEX 05

E-mail address: `heiderich@math.jussieu.fr`