Galois Theory of Module Fields

Florian Heiderich

Galois Theory of Module Fields

Florian Heiderich

Universitat de Barcelona
July 2010

Galois Theory of Module Fields

Tesi Doctoral

Programa de doctorat de matemàtiques, curs 2007–2008
Facultat de Matemàtiques, Universitat de Barcelona

Doctorand: Florian Heiderich
Directora de tesi: Teresa Crespo Vicente
Departament d'Àlgebra i Geometria

Acknowledgments

I would like to thank everyone who helped me during the preparation of this thesis.

First, I would like to thank my advisor Teresa Crespo for providing me with the possibility to carry out my studies during the last years that lead to this thesis, for her continuous support and for all our discussions.

Next, I wish to thank my former advisor B. Heinrich Matzat for making two research stays in Heidelberg possible and his working group for providing a pleasant and motivating atmosphere. I am grateful to Andreas Maurischat for making me aware of the work of Takeuchi, Amano and Masuoka.

Further, I would like to thank Leila Schneps for making my research stay in Paris possible and to Daniel Bertrand and Lucia Di Vizio for asking me to speak about my work in their Groupe de travail différentiel in Paris. Also, I want to thank them, Guy Casale and Hiroshi Umemura for several interesting discussions in Paris.

I am grateful to Shigeyuki Kondo and Hiroshi Umemura for making my research stay in Nagoya possible. I would like to thank the latter and Katsunori Saito for interesting discussions during my stay in Nagoya. I profited from discussions with Hiroshi Umemura by obtaining a better understanding of his theory. He also provided me with the idea for the proof of lemma 3.1.1. Also, I would like to thank him and Yukari Ito for inviting me to speak about my work in their Algebraic Geometry seminars at Nagoya University. I thank Shuji Morikawa for providing me with a preliminary version of his article on

the general difference Galois theory, which motivated parts of my research.

My thanks also go to Katsutoshi Amano and Akira Masuoka for inviting me to Tsukuba University to give lectures there.

I am grateful to Paloma Bengoechea and Teresa Crespo for their help with the preparation of the Spanish summary.

I would also like to thank all the other persons I had fruitful mathematical discussions with during several meetings in the last years, especially Michael Wibmer.

After all, I would like to thank my friends at Barcelona, Heidelberg, Paris and Nagoya for their support and for making my stays at the corresponding places each time very enjoyable. Finally, I would like to thank my family for their constant support.

This work was supported by the European Commission under contract MRTN-CT-2006-035495 and by the Japan Society for the Promotion of Science with a JSPS Postdoctoral Fellowship (short-term) for North American and European Researchers. I thank those institutions for financial support.

Contents

Introduction

Galois theory has its roots in the beginning of the 19th century when E. Galois determined group theoretic conditions under which polynomial equations are solvable by radicals. Given a field F and a separable polynomial $f \in F[X]$, there exists an extension field E over F, the so called splitting field of f, which is generated over F by the roots of f. The group $G = \mathrm{Aut}(E/F)$, consisting of all field automorphisms of E fixing F, acts on the set of zeros of f in E. It consists of those permutations of the set of roots of f that respect algebraic relations over F among the roots of f. There exists an inclusion-reversing bijection between the set of subgroups of G and the set of intermediate fields between E and F.

It was the goal of S. Lie to develop a Galois theory for differential equations in place of algebraic equations. The first step was done by E. Picard and E. Vessiot, who developed a Galois theory for linear differential equations, nowadays called Picard-Vessiot theory. Then E. Kolchin extended this theory by developing the differential Galois theory of strongly normal extensions, which include certain extensions of differential fields arising from non-linear differential equations ([Kol76]). Inspired by the work of E. Vessiot ([Ves46]), H. Umemura developed a Galois theory to deal with non-linear algebraic differential equations ([Ume96a]). B. Malgrange developed a theory with a similar aim using the language of differential geometry ([Mal01], [Mal02]). This theory was further studied and applied by G. Casale ([Cas04], [Cas07], [Cas08]). Recently, H. Umemura compared his theory with the one

of B. Malgrange and showed that they are closely connected ([Ume08]).

There exist analog theories for difference equations. First, C. H. Franke developed a Picard-Vessiot theory for difference equations ([Fra63]). Later, R. Infante defined strongly normal extensions of difference fields and developed a Galois theory for them ([Inf80b], [Inf80a]). Recently, S. Morikawa and H. Umemura developed an analogue of the differential Galois theory of the latter for extensions of difference fields ([Mor09], [MU09]). Following B. Malgrange's approach, G. Casale and A. Granier set up Galois theories for nonlinear (q-)difference equations ([Cas06], [Gra09]).

The theories mentioned so far were restricted to fields of characteristic zero. In positive characteristic, derivations turn out not to be adequate and H. Hasse and F. K. Schmidt introduced iterative derivations as a replacement for them when working with fields of arbitrary characteristic ([HS37]). Later, K. Okugawa, B. H. Matzat and M. van der Put developed differential Galois theories in positive characteristic using iterative derivations ([Oku87], [Mat01], [MvdP03]). The theory of B. H. Matzat and M. van der Put was further developed by A. Maurischat and the author ([Rös07], [Hei07], [Mau10a], [Mau10b]). But at least the theories of B. H. Matzat, M. van der Put and the followers are restricted to linear iterative differential equations.

M. Takeuchi gave a Hopf-algebraic approach to Picard-Vessiot theory that unifies the differential Picard-Vessiot theory in characteristic zero and the iterative differential Picard-Vessiot theory in arbitrary characteristic ([Tak89]) using so called C-ferential fields, where C is a certain coalgebra. Recently, K. Amano and A. Masuoka extended the approach of M. Takeuchi using the language of D-module algebras, where D is a certain Hopf-algebra ([Ama05], [AM05], [AMT09]). Their theory unifies the Picard-Vessiot theory of differential equations in characteristic zero, the Picard-Vessiot theory of iterative differential equations in arbitrary characteristic and the Picard-Vessiot theory of difference equations when the difference operator is an automorphism.

To summarize, development in differential and difference Galois theory

went into two directions. On the one hand, H. Umemura and S. Morikawa developed Galois theories that allow the investigation of non-linear differential and difference equations. On the other hand, M. Takeuchi, K. Amano and A. Masuoka developed a unified Galois theory for Picard-Vessiot extensions, i.e. for linear equations (although their approach is more general and does not emphasize the equations).

This thesis has two main purposes. The first is to develop a general Galois theory by combining the capacity of the theories of H. Umemura and S. Morikawa to allow the treatment of very general field extensions with the advantage of the formulation of the theory of M. Takeuchi, K. Amano and A. Masuoka to unify different structures like derivations, iterative derivations and automorphisms. The second purpose is to remove the restriction to characteristic zero from the theories of H. Umemura and S. Morikawa.

We realize our aim by using the language of D-module fields, where D is a cocommutative bialgebra, and iterative derivations and obtain a Galois theory for separable and finitely generated extensions of D-module fields without restrictions on the characteristic. For certain choices of the bialgebra D one recovers the theories of H. Umemura and S. Morikawa, but without the restriction to fields of characteristic zero.

The main tool in the theory of H. Umemura is the homomorphism of differential rings

$$(R,\partial) \to (R[\![t]\!],\partial_t), \quad a \mapsto \sum_{k\in\mathbb{N}} \frac{\partial^k(a)}{k!} t^k$$

associated to a differential ring (R,∂) containing $\mathbb{Q}$, which he calls *universal Taylor homomorphism*. Similarly, in the theory of S. Morikawa the homomorphism of difference rings

$$(R,\sigma) \to (R^{\mathbb{N}},\Sigma), \quad a \mapsto (k \mapsto \sigma^k(a))$$

associated to a difference ring (R,σ), where Σ is the shift operator on $R^{\mathbb{N}}$, plays a central role. This homomorphism is called *universal Euler homo-*

morphism there. Given a commutative ring C, a C-bialgebra D and a C-algebra R, a *D-module algebra structure* on R is a homomorphism of C-modules $\Psi\colon D \otimes_C R \to R$ with certain properties. Given a D-module algebra structure Ψ on R, we obtain a homomorphism of C-algebras

$$R \to \mathsf{Mod}_C(D, R), \quad a \mapsto (d \mapsto \Psi(d \otimes a))$$

having analogous properties as the universal Taylor and universal Euler homomorphisms mentioned before. Given a separable and finitely generated extension of D-module fields L/K, we define the normalization of this extension, namely an extension $\mathcal{L}/\mathcal{K}$ of D-module algebras similar to the normalizations defined by H. Umemura and S. Morikawa. Using this normalization, we introduce an infinitesimal Galois group functor attached to the extension L/K. This functor is a Lie-Ritt functor, i.e. isomorphic to a group functor of infinitesimal transformations fulfilling certain partial differential equations. As Lie-Ritt functors are in general formal group schemes, we see that the infinitesimal Galois group we defined turns out to be a formal group scheme defined over the field L. In order to define the normalization $\mathcal{L}/\mathcal{K}$, H. Umemura and S. Morikawa use a basis of the L-vector space $\mathrm{Der}_K(L)$ consisting of commuting derivations and a Taylor development with respect to this set of derivations. They need to assume that the characteristic is zero. In order to avoid this restriction, we use a multivariate iterative derivation with respect to a separating transcendence basis of L/K instead. In the case of a separable and finitely generated Picard-Vessiot extension of D-module fields L/K in the sense of K. Amano and A. Masuoka ([AM05]), we show that if K is perfect, then after an extension of scalars our infinitesimal Galois group becomes isomorphic to the formal group scheme associated to the Galois group scheme of K. Amano and A. Masuoka.

This thesis is organized as follows: In the first chapter we introduce higher and iterative derivations. Although they can be understood in the framework of module algebras, which we introduce in the second chapter, we devote an own chapter to them due to their importance for this thesis. For the later

use we do not restrict us to the ordinary case, but define multivariate higher and iterative derivations as introduced in ([Hei07]), which are equivalent to a finite set of commuting higher and iterative derivations, respectively. We prove basic properties of higher and iterative differential rings. Some of these properties also hold for module algebras, but others do not hold in the general framework of module algebras anymore.

In the second chapter we first state our convention concerning algebras, coalgebras, and bialgebras and then cover module algebras. Module algebras are used in this thesis as a framework to describe a large family of structures such as derivations, iterative derivations, endomorphisms and automorphisms in a unified way. In section 2.2, we first recall their definition and prove some of their basic properties. At the end of this section, we focus on simple module algebras, which behave particularly well. We close this chapter with examples illustrating the concept of module algebras by defining a number of bialgebras D and explaining D-module algebras in these cases. Most of the bialgebras we explain there are cocommutative, but we also give two examples of non-cocommutative bialgebras. In chapter 3 we make the assumption that the bialgebra is cocommutative. This excludes these bialgebras to be used in our theory, but they are important to describe theories like those of Y. André and C. Hardouin ([And01], [Har10]). Finally, we show how one can associate a bialgebra D to a given iterative Hasse system $\mathcal{D}$ in the sense of R. Moosa and T. Scanlon ([MS10], [MS09]). Then an iterative $\mathcal{D}$-ring poses a canonically associated D-module algebra structure and conversely every commutative D-module algebra becomes an iterative $\mathcal{D}$-ring.

Chapter 3 is the heart of this thesis. We generalize and unify the theories of H. Umemura and M. Morikawa. First, we define the normalization $\mathcal{L}/\mathcal{K}$ of a separable and finitely generated extension of extension of D-module fields L/K. Then we introduce the functor of deformations $\mathcal{F}_{L/K}$ and the infinitesimal Galois group Inf-Gal(L/K) unifying the definitions of H. Umemura and M. Morikawa. We also define Lie-Ritt functors, which have been introduced

by H. Umemura in [Ume96a]. Our treatment of Lie-Ritt functors differs in two points from the one of H. Umemura. First, we use iterative differential rings instead of differential rings to define Lie-Ritt functors in order not to pose unnecessary restrictions on the characteristic. Secondly, certain series appear in the definition of Lie-Ritt functors in [Ume96a] that do not converge. We change the definition in order to avoid this problem.

In the last chapter we compare our general theory with the Picard-Vessiot theory of K. Amano and A. Masuoka. We show that in the case of a separable and finitely generated Picard-Vessiot extension of D-module fields the normalization $\mathcal{L}/\mathcal{K}$ has a particularly easy form and show how the infinitesimal Galois group Inf-Gal(L/K) is related to the Galois group scheme Gal(L/K) defined by K. Amano and A. Masuoka if the field K is perfect.

Since we do not know an adequate reference that covers all we need, we added appendix A on linear topological rings and completed tensor products.

The literature on formal group schemes seems not to be consistent. So we added appendix B about formal schemes, formal group schemes and formal group laws, stating the definitions that we use and showing the relations between the concepts mentioned.

At the end a summary in Spanish is included.

Finally, we mention that we consider the development of the theory that we present here not to be completed. There are several directions for generalizations. To begin with, in their Picard-Vessiot theory, K. Amano and A. Masuoka assume that the bialgebra D is a pointed cocommutative Hopf algebra and that the irreducible component D^1 is of Birkhoff-Witt type. Therefore, theories like those of Y. André ([And01]) and C. Hardouin ([Har10]) are not in the scope of their theory, since the corresponding bialgebras are not cocommutative. It is an interesting question whether a Picard-Vessiot theory using non-cocommutative bialgebras can be developed in order to integrate the theories of Y. André and C. Hardouin. In our theory we do not assume that the bialgebra D is a Hopf algebra, so in contrast to the theory of K. Amano and

A. Masuoka, for example non-inversive difference fields are within our scope. But in this thesis we restrict ourselves to cocommutative bialgebras. The main reason for this is that in this case the dual of the bialgebra becomes a commutative algebra. The algebra $\mathcal{L}$ that we define is a subalgebra of $\mathsf{Mod}_C(D, L)$. If we do not assume that the bialgebra is cocommutative, the latter is in general not commutative anymore. However, if the extension L/K is a Picard-Vessiot extension (though, strictly speaking, there is no definition of Picard-Vessiot extensions in this situation yet), then it is easy to see that $\mathcal{L}$ is still commutative and we can proceed. In the general case this is not at all clear and $\mathcal{L}$ may become non-commutative. H. Umemura shows in [Ume08] that in the case of finitely generated field extensions of $\mathbb{C}$, one can construct the Malgrange groupoid using the spectrum of an algebra that is defined similarly as $\mathcal{L}$. If this algebra is not longer commutative, this is not possible and one can expect objects of a new type. Finally, we would like to mention that the restriction to field extensions in our theory is unpleasant, since for example Picard-Vessiot extensions of difference equations are not, in general, fields. We expect that our theory can be generalized in this direction too.

Notation: *We denote by* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *and* $\mathbb{C}$ *the natural numbers (including zero), integers, rational numbers and complex numbers, respectively. We use standard multiindex notation, namely if* $n \in \mathbb{N}$ *and* $\boldsymbol{k} = (k_i)_{i=1,\dots,n}, \boldsymbol{l} = (l_i)_{i=1,\dots,n} \in \mathbb{Z}^n$ *we write*

$$|\boldsymbol{k}| := \sum_{i=1}^{n} k_i \quad \text{and} \quad \boldsymbol{k} + \boldsymbol{l} := (k_i + l_i)_{i=1,\dots,n}.$$

For $\boldsymbol{k}, \boldsymbol{l} \in \mathbb{N}^n$ *we define*

$$\boldsymbol{k}! := \prod_{i=1}^{n} (k_i)!, \quad \binom{\boldsymbol{k}}{\boldsymbol{l}} := \prod_{i=1}^{n} \binom{k_i}{l_i} \quad \text{and} \quad \boldsymbol{\delta}_i := (\delta_{i,j})_{j=1,\dots,n},$$

where for any set A *and any* $i, j \in A$ *the symbol* $\delta_{i,j}$ *is the Kronecker-*δ*, i.e.* $\delta_{i,j} = 1$ *if* $i = j$ *and* $\delta_{i,j} = 0$ *if* $i \neq j$.

All rings and algebras are assumed to be associative and unital. We denote by $N(A)$ *the nilradical of a commutative ring* A*, i.e. the ideal consisting of all elements* $a \in A$ *such that there exists a natural number* $n > 0$ *with* $a^n = 0$*, and by* π_A *the canonical projection* $A \to A/N(A)$*. The units of a ring* A *are denoted by* $A^\times$*. If* $A[\![\boldsymbol{w}]\!] := A[\![w_1, \dots, w_n]\!]$ *and* $B[\![\boldsymbol{w}]\!] := B[\![w_1, \dots, w_n]\!]$ *are the formal power series rings over commutative rings* A *and* B*, respectively, and if* $\varphi\colon A \to B$ *is a ring homomorphism, then we denote by* $\varphi[\![\boldsymbol{w}]\!]\colon A[\![\boldsymbol{w}]\!] \to B[\![\boldsymbol{w}]\!]$ *the homomorphism defined by* $\varphi[\![\boldsymbol{w}]\!](\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}} \boldsymbol{w}^{\boldsymbol{k}}) := \sum_{\boldsymbol{k}\in\mathbb{N}^n} \varphi(a_{\boldsymbol{k}}) \boldsymbol{w}^{\boldsymbol{k}}$.

If C *is a category and* A *and* B *are objects in* C*, then we denote the set of morphisms from* A *to* B *in* C *by* $\mathsf{C}(A, B)$*. We use the following abbreviations for some basic categories:*

Set	*Sets*
Grp	*Groups*
Rng	*Rings*
CRng	*Commutative rings*
$\mathsf{Mod}_{\mathsf{R}}$	*R-modules, where R is a commutative ring*
$\mathsf{Alg}_{\mathsf{R}}$	*R-algebras, where R is a commutative ring*
$\mathsf{CAlg}_{\mathsf{R}}$	*Commutative R-algebras, where R is a commutative ring*

Chapter 1

Higher and iterative derivations

In this chapter we recall the definition of higher and iterative derivations. In the univariate case they were introduced by H. Hasse and F. K. Schmidt ([HS37]). In [Hei07] the author defined higher and iterative derivations in the multivariate case, which serve as an alternative for systems of commuting derivations in positive characteristic (see also [Rös07] for another generalization of higher and iterative derivations). H. Matsumura proved that univariate higher and iterative derivations extend to 0-étale extensions. We generalize this result to multivariate higher and iterative derivations and show some applications. At the end of this chapter we discuss linearly non-degenerate higher derivations.

Notation: *In this chapter we assume all rings and algebras to be commutative. Let C be a (commutative) ring.*

1.1 Higher and iterative differential rings

Definition 1.1.1. *Let n be a positive natural number and $f\colon R \to \tilde{R}$ be a homomorphism of C-algebras. An* n-variate higher derivation *from R to $\tilde{R}$ over C is a*

homomorphism of C-algebras

$$\theta\colon R \to \tilde{R}[\![t_1,\dots,t_n]\!] =: \tilde{R}[\![\boldsymbol{t}]\!]$$

such that $\varepsilon\circ\theta = f$*, where* ε *is the homomorphism of* $\tilde{R}$*-algebras* $\tilde{R}[\![\boldsymbol{t}]\!] \to \tilde{R}$ *defined by* $\varepsilon(t_i) = 0$ *for* $i = 1,\dots,n$*. For all* $\boldsymbol{k} \in \mathbb{N}^n$ *we denote by* $p_{\boldsymbol{k}}\colon \tilde{R}[\![\boldsymbol{t}]\!] \to \tilde{R}$ *the map sending* $\sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}}\boldsymbol{t}^{\boldsymbol{l}}$ *to* $a_{\boldsymbol{k}}$ *and we define* $\theta^{(\boldsymbol{k})} := p_{\boldsymbol{k}}\circ\theta$*. If there is risk of confusion, we will denote* θ *also by* ${}_{\boldsymbol{t}}\theta$ *in order to indicate the variables of the ring* $\tilde{R}[\![\boldsymbol{t}]\!]$*. An n-variate higher derivation* $\theta\colon R \to R[\![\boldsymbol{t}]\!]$ *from R to R over C is an n-*variate iterative derivation *on R over C if the diagram*

$$\begin{array}{ccc} R & \xrightarrow{{}_{\boldsymbol{t}}\theta} & R[\![\boldsymbol{t}]\!] \\ {\scriptstyle {}_{\boldsymbol{t}}\theta}\downarrow & & \downarrow{\scriptstyle {}_{\boldsymbol{u}}\theta[\![\boldsymbol{t}]\!]} \\ R[\![\boldsymbol{t}]\!] & \xrightarrow{\boldsymbol{t}\mapsto\boldsymbol{t}+\boldsymbol{u}} & R[\![\boldsymbol{t},\boldsymbol{u}]\!]. \end{array}$$

commutes, where the homomorphism ${}_{\boldsymbol{u}}\theta[\![\boldsymbol{t}]\!]\colon R[\![\boldsymbol{t}]\!] \to R[\![\boldsymbol{t},\boldsymbol{u}]\!]$ *is defined by*

$${}_{\boldsymbol{u}}\theta[\![\boldsymbol{t}]\!]\left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\boldsymbol{k}}\boldsymbol{t}^{\boldsymbol{k}}\right) := \sum_{\boldsymbol{k}\in\mathbb{N}^n} {}_{\boldsymbol{u}}\theta(a_{\boldsymbol{k}})\boldsymbol{t}^{\boldsymbol{k}}.$$

We denote by $\mathrm{HD}^n_C(R,\tilde{R})$ *the set of all n-variate higher derivations from R to* $\tilde{R}$ *over C, by* $\mathrm{HD}^n_C(R)$ *the set of all n-variate higher derivations from R to R over C and by* $\mathrm{ID}^n_C(R)$ *the set of all n-variate iterative derivations on R over C.*

Example 1.1.2. *On every C-algebra R there exists for all* $n \in \mathbb{N}$ *an n-variate iterative derivation*

$$\theta_0\colon R \to R[\![t_1,\dots,t_n]\!], \quad r \mapsto r$$

that we call the trivial *n-*variate iterative derivation*.*

Example 1.1.3. *If R is a C-algebra containing the rational numbers* $\mathbb{Q}$ *and* $\partial_1,\dots,\partial_n$ *is a set of commuting C-derivations on R, then*

$$\theta\colon R \to R[\![\boldsymbol{t}]\!], \quad a \mapsto \sum_{\boldsymbol{k}=(k_1,\dots,k_n)\in\mathbb{N}^n} \frac{\partial_1^{k_1}\circ\cdots\circ\partial_n^{k_n}(a)}{\boldsymbol{k}!}\boldsymbol{t}^{\boldsymbol{k}}$$

is an n-variate iterative derivation on R over C.

Definition 1.1.4. *(1) A pair (R,θ), where R is a C-algebra and $\theta \in \mathrm{HD}_C^n(R)$, is called an* ($n$-variate) higher differential ring *(or* HD-ring*) over C. If θ is iterative, (R,θ) is called an* (n-variate) iterative differential ring *(or* ID-ring*) over C.*

(2) Given a HD-ring (R,θ) over C, the set

$$R^\theta := \{a \in R \mid \theta(a) = a\}$$

is a C-subalgebra of R and is called the ring of constants *of (R,θ).*[1]

(3) If (R,θ_R) is a HD-ring (ID-ring) over C and (A,θ_A) is another HD-ring (ID-ring) over C, then we say that (A,θ_A) is a HD-subring *(*ID-subring*) of (R,θ_R) if A is a C-subalgebra of R and if θ_A is the restriction of θ_R to A.*

Definition 1.1.5. *If (R,θ_R) and (S,θ_S) are HD-rings, then a homomorphism of C-algebras $\varphi\colon R \to S$ is called a* homomorphism of HD-rings *over C (or a* HD-homomorphism*) if $\theta_S \circ \varphi = \varphi[\![\boldsymbol{t}]\!] \circ \theta_R$ holds.*

Definition 1.1.6. *Let (R,θ) be a HD-ring over C.*

(1) An ideal A of R is a higher differential ideal *(or* HD-ideal*) of (R,θ) if $\theta(A) \subseteq A[\![\boldsymbol{t}]\!]$ holds.*

(2) The HD-ring (R,θ) is a simple HD-ring *if (0) and R are its only HD-ideals.*

Definition 1.1.7. *Let (S,θ) be a HD-ring, R a HD-subring of S and $A \subseteq S$ a subset. Then we define the* HD-ring generated by A over R *as the smallest HD-subring of S containing R and A and denote it by $R\{A\}_\theta$ (or also by $R\{A\}$ if θ is clear from the context). We denote the smallest HD-ideal of S containing A by $[A]_{(S,\theta)}$ (or also by $[A]_S$ or $[A]$ if there is no risk of confusion).*

[1] There are alternative definitions of constants (see for example [MW95], [Zie03]). Our definition coincides with the more general definition of constants in the context of module algebras (see definition 2.2.12).

Remark 1.1.8. *In the situation of definition 1.1.7 it is easily seen that if S is iterative, then $R\{A\}_\theta$ is generated as C-algebra over R by $\theta^{(\boldsymbol{k})}(a)$ for all $a \in A$ and $\boldsymbol{k} \in \mathbb{N}^n$, i.e we have $R\{A\}_\theta = R[\theta^{(\boldsymbol{k})}(a) \mid a \in A, \boldsymbol{k} \in \mathbb{N}^n]$.*

Example 1.1.9. *Let (R, θ) be an n-variate HD-ring and I be a set. Then we define the* ring of differential polynomials *in variables $(X_i)_{i\in I}$ over (R, θ) as*

$$R\{X_i \mid i \in I\}_{\mathrm{ID}^n} := R[X_i^{(\boldsymbol{k})} \mid i \in I, \boldsymbol{k} \in \mathbb{N}^n]$$

and extend the higher derivation θ to $R\{X_i \mid i \in I\}_{\mathrm{ID}^n}$ by

$$\theta\left(X_i^{(\boldsymbol{k})}\right) := \sum_{\boldsymbol{l}\in\mathbb{N}^n} \binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}} X_i^{(\boldsymbol{l}+\boldsymbol{k})} \boldsymbol{t}^{\boldsymbol{l}}$$

for all $i \in I$ and all $\boldsymbol{k} \in \mathbb{N}^n$. If the higher derivation θ on R is iterative, then the extension to $R\{X_i \mid i \in I\}_{\mathrm{ID}^n}$ is iterative too.

1.2 Extension of higher and iterative derivations

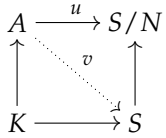
We first recall the following definition of 0-smooth, 0-unramified and 0-étale extensions in terms of the infinitesimal lifting property from [Mat89, p. 193].[2]

Definition 1.2.1. *Let K be a ring. A K-algebra A is called* 0-smooth *over K if for every K-algebra S and every ideal N of S that satisfies $N^2 = 0$, every K-algebra homomorphism $u\colon A \to S/N$ has a lifting $v\colon A \to S$, i.e. for every commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{u} & S/N \\ \uparrow & & \uparrow \\ K & \longrightarrow & S \end{array}$$

[2] These definitions correspond to the formally smooth, formally unramified and formally étale extensions of discrete topological rings, as defined by A. Grothendieck in [Gro64, Définition 19.3.1 and Définition 19.10.2]

there exists a homomorphism $v\colon A \to S$ *making the diagram*



commutative. The K-algebra A is called 0-ramified *if there is at most one such v. It is called* 0-étale *if it is* 0*-smooth and* 0*-ramified.*

The following two propositions specialize to [Mat89, Theorem 27.2] in the case $n = 1$.

Proposition 1.2.2. *Let* $C \to A \xrightarrow{g} B$ *be ring homomorphisms and assume that B is* 0*-étale over A. Let further R be a B-algebra.*

(1) If $\theta\colon A \to R[\![t_1, \dots, t_n]\!]$ *is an n-variate higher derivation from A to R over C, then there exists a unique n-variate higher derivation* $\theta'\colon B \to R[\![t_1, \dots, t_n]\!]$ *from B to R over C such that* $\theta' \circ g = \theta$*.*

(2) If $\theta\colon A \to A[\![t_1, \dots, t_n]\!]$ *is an n-variate iterative derivation on A over C, then the unique extension* $\theta'\colon B \to B[\![t_1, \dots, t_n]\!]$ *of* $g[\![\boldsymbol{t}]\!] \circ \theta$ *is also iterative.*

Proof. For all $\boldsymbol{m} = (m_1, \dots, m_n) \in \mathbb{N}^n$ we construct iteratively a compatible family of homomorphisms

$$B \to R[\![t_1, \dots, t_n]\!]/(t_1^{m_1+1}, \dots, t_n^{m_n+1})$$

making the diagram

$$\begin{array}{ccc} B & \longrightarrow & R[\![t_1, \dots, t_n]\!]/(t_1^{m_1+1}, \dots, t_n^{m_n+1}) \\ {\scriptstyle g}\uparrow & & \uparrow \\ A & \xrightarrow{\theta} & R[\![t_1, \dots, t_n]\!] \end{array} \tag{1.2.1}$$

commutative. For $\boldsymbol{m} = \mathbf{0}$ we note that $R[\![t_1, \ldots, t_n]\!]/(t_1, \ldots, t_n) \cong R$ and we take the structure homomorphism of the B-algebra R. In this case the diagram (1.2.1) becomes

$$\begin{array}{ccc} B & \longrightarrow & R \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle \varepsilon} \\ A & \xrightarrow{\theta} & R[\![t_1, \ldots, t_n]\!], \end{array} \tag{1.2.2}$$

which is commutative, since θ is a higher derivation from A to R. If such a homomorphism is already constructed for some $\boldsymbol{m} \in \mathbb{N}^n$, then, since B is 0-étale over A, for every $i \in \{1, \ldots, n\}$ there exists a unique homomorphism

$$B \to R[\![t_1, \ldots, t_n]\!]/(t_1^{m_1+1}, \ldots, t_i^{m_i+2}, \ldots, t_n^{m_n+1}),$$

making the diagram

$$\begin{array}{ccccc} B & & \longrightarrow & & R[\![t_1, \ldots, t_n]\!]/(t_1^{m_1+1}, \ldots, t_n^{m_n+1}) \\ {\scriptstyle g}\uparrow & \nearrow & & & \uparrow \\ A & \xrightarrow{\theta} & R[\![t_1, \ldots, t_n]\!] & \longrightarrow & R[\![t_1, \ldots, t_n]\!]/(t_1^{m_1+1}, \ldots, t_i^{m_i+2} \ldots, t_n^{m_n+1}) \end{array}$$

commutative. By induction we obtain compatible homomorphisms

$$B \to R[\![t_1, \ldots, t_n]\!]/(t_1^{m_1+1}, \ldots, t_n^{m_n+1})$$

for all $\boldsymbol{m} \in \mathbb{N}^n$ and thus a homomorphism $\theta' \colon B \to R[\![t_1, \ldots, t_n]\!]$ fulfilling our conditions.

To prove the second part, we consider both, ${}_{\boldsymbol{u}}\theta[\![\boldsymbol{t}]\!] \circ {}_{\boldsymbol{t}}\theta \colon A \to A[\![\boldsymbol{t}, \boldsymbol{u}]\!]$ and ${}_{\boldsymbol{t}+\boldsymbol{u}}\theta \colon A \to A[\![\boldsymbol{t}, \boldsymbol{u}]\!]$, as higher derivations on A. By the first part, they uniquely extend to higher derivations on B. Since ${}_{\boldsymbol{u}}\theta[\![\boldsymbol{t}]\!] \circ {}_{\boldsymbol{t}}\theta = {}_{\boldsymbol{t}+\boldsymbol{u}}\theta$, the homomorphisms ${}_{\boldsymbol{u}}\theta'[\![\boldsymbol{t}]\!] \circ {}_{\boldsymbol{t}}\theta' \colon B \to B[\![\boldsymbol{t}, \boldsymbol{u}]\!]$ and ${}_{\boldsymbol{t}+\boldsymbol{u}}\theta' \colon B \to B[\![\boldsymbol{t}, \boldsymbol{u}]\!]$ coincide as well, i.e. θ' is iterative. □

Example 1.2.3. *(1) If A is a ring and $S \subseteq A$ a multiplicative subset of A, then $S^{-1}A$ is 0-étale over A (see [Gro64, Chap. 0, 19.10.3 (ii)]).*

(2) *If K'/K is a finite separable field extension, then K' is 0-étale over K (see [Gro64, Chap. 0, 21.7.4 (iii)]).*

Example 1.2.4. *Let K be a ring.*

(1) *The homomorphism of K-algebras*

$$\theta_{(x_1,\dots,x_n)} \colon K[x_1,\dots,x_n] \to K[x_1,\dots,x_n][t_1,\dots,t_n], \quad x_i \mapsto x_i + t_i$$

defines an n-variate iterative derivation on $K[x_1,\dots,x_n]$ over K.

(2) *If K is a field, then the n-variate iterative derivation $\theta_{(x_1,\dots,x_n)}$ on $K[x_1,\dots,x_n]$ over K extends to $K(x_1,\dots,x_n) = \operatorname{Quot}(K[x_1,\dots,x_n])$ by example 1.2.3 (1) and proposition 1.2.2. We denote this n-variate iterative derivation again by $\theta_{(x_1,\dots,x_n)}$.*

(3) *If K is a field and L/K is a separably and finitely generated field extension with separating transcendence basis $\{x_1,\dots,x_n\}$, then by example 1.2.3 (2) and proposition 1.2.2 the n-variate iterative derivation $\theta_{(x_1,\dots,x_n)} \in \mathrm{ID}^n_K(K(x_1,\dots,x_n))$ constructed above extends uniquely to L and we denote this extension again by $\theta_{(x_1,\dots,x_n)}$.*

In every case we will denote $\theta_{(x_1,\dots,x_n)}$ also by $\theta_{\boldsymbol{x}}$.

Example 1.2.5. (1) *On $R \coloneqq C[\![\boldsymbol{x}]\!] \coloneqq C[\![x_1,\dots,x_n]\!]$ we define an n-variate iterative derivation $\theta_{(x_1,\dots,x_n)} \colon R \to R[\![t_1,\dots,t_n]\!]$ over C by $\theta_{(x_1,\dots,x_n)}(x_i) = x_i + t_i$ for $i \in \{1,\dots,n\}$.*

(2) *By proposition 1.2.2 and example 1.2.3 (1) the iterative derivation $\theta_{(x_1,\dots,x_n)}$ extends uniquely to $R = C[\![\boldsymbol{x}]\!][\boldsymbol{x}^{-1}]$. We denote this extension again by $\theta_{(x_1,\dots,x_n)}$.*

In both cases the constants are C and we denote $\theta_{(x_1,\dots,x_n)}$ also by $\theta_{\boldsymbol{x}}$.

Lemma 1.2.6. *If (R,θ) is an n-variate higher differential ring over C, then θ extends to an n-variate higher derivation $\tilde{\theta}$ on $R[\![\boldsymbol{w}]\!] \coloneqq R[\![w_1,\dots,w_n]\!]$, defined by*

$$\tilde{\theta} \colon R[\![\boldsymbol{w}]\!] \to R[\![\boldsymbol{w},\boldsymbol{u}]\!], \quad w_i \mapsto w_i + u_i \quad \text{for all } i \in \{1,\dots,n\}.$$

If θ is iterative, then $\tilde{\theta}$ is iterative too.

Proof. Since $R[\![\boldsymbol{w},\boldsymbol{u}]\!]$ is complete with respect to the $(\boldsymbol{w},\boldsymbol{u})$-adic topology, there exists a unique continuous homomorphism of R-algebras $\tilde{\theta}\colon R[\![\boldsymbol{w}]\!] \to R[\![\boldsymbol{u},\boldsymbol{w}]\!]$, sending w_i to $w_i + u_i$ for all $i = 1,\dots,n$, where we consider $R[\![\boldsymbol{w}]\!]$ as R-algebra via the inclusion as constants with respect to $\boldsymbol{w}$ and $R[\![\boldsymbol{w},\boldsymbol{u}]\!]$ as R-algebra via the composition of $\theta\colon R \to R[\![\boldsymbol{u}]\!]$ with the inclusion of $R[\![\boldsymbol{u}]\!]$ into $R[\![\boldsymbol{w},\boldsymbol{u}]\!]$ as constants with respect to $\boldsymbol{w}$. Thus, $\tilde{\theta}$ restricts to θ on R. Since $\tilde{\theta}$ is a homomorphism of C-algebras, it is an n-variate higher derivation on $R[\![\boldsymbol{w}]\!]$ over C. Finally, if θ is iterative, then ${}_{\boldsymbol{v}}\tilde{\theta}[\![\boldsymbol{u}]\!] \circ {}_{\boldsymbol{u}}\tilde{\theta}$ and ${}_{\boldsymbol{u}+\boldsymbol{v}}\tilde{\theta}$ coincide by the universal property of the formal power series ring $R[\![\boldsymbol{w}]\!]$, since both are continuous homomorphisms of R-algebras sending w_i to $w_i + u_i + v_i$ for $i = 1,\dots,n$ with respect to the $(\boldsymbol{w})$-adic and $(\boldsymbol{w},\boldsymbol{u},\boldsymbol{v})$-adic topologies on $R[\![\boldsymbol{w}]\!]$ and $R[\![\boldsymbol{w},\boldsymbol{u},\boldsymbol{v}]\!]$, respectively. □

The following proposition is well-known, at least in the univariate case.

Proposition 1.2.7. *Let (R,θ_R) be a simple HD-ring, then*

(1) the ring R is an integral domain and

(2) if $L = \mathrm{Quot}(R)$ is the quotient field of R, then θ_R can be extended to a higher derivation θ_L on L and we have $R^{\theta_R} = L^{\theta_L}$.

Proof. Let P be a prime ideal of R. We define a HD-homomorphism

$$\bar{\theta}_R\colon (R,\theta_R) \to ((R/P)[\![\boldsymbol{t}]\!],\theta_{\boldsymbol{t}})$$

as $\bar{\theta}_R := \pi[\![\boldsymbol{t}]\!] \circ {}_{\boldsymbol{t}}\theta_R$, where $\pi\colon R \to R/P$ is the canonical projection. The kernel of $\bar{\theta}_R$ is a HD-ideal not equal to (1) and, since (R,θ_R) is simple, it has to be trivial. Therefore, $\bar{\theta}_R$ is a monomorphism from R to the integral domain $(R/P)[\![\boldsymbol{t}]\!]$ and thus the ring R does not contain non-trivial zero-divisors.

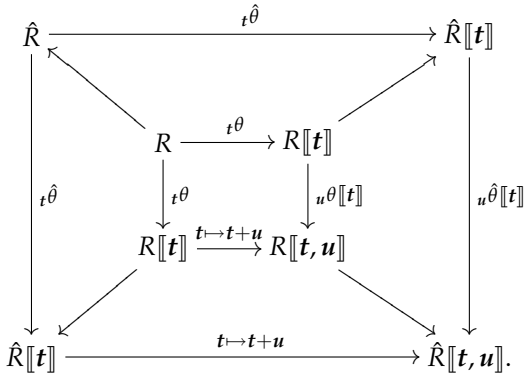
By example 1.2.3 (1) and proposition 1.2.2, the higher derivation θ_R extends to L. For $a \in L^{\theta_L}$ we define $I_a := \{b \in R \mid ab \in R\}$. Since for $b \in I_a$ we also have $a \cdot \theta_R(b) = \theta_R(a \cdot b) \in R[\![\boldsymbol{t}]\!]$, the ideal $I_a \trianglelefteq R$ is a HD-ideal and, since I_a is non-trivial, it is equal to (1). In particular, we obtain $a \in R$. □

Proposition 1.2.8. *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 $R[\![\boldsymbol{t}]\!]$.*

(1) 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.

(2) If θ is iterative, then $\hat{\theta}$ is iterative too.

Proof. The unique extension $\hat{\theta}$ of θ to the completion (see lemma A.1.2) is a higher derivation, since the property $\varepsilon \circ \theta = \mathrm{id}_R$ holds analogously for the extension $\hat{\theta}$ by the uniqueness of the extension. To prove the second part, we consider the diagram



All arrows are continuous homomorphisms and the outer arrows are the unique extensions of the inner ones to the completions. Thus, the commutativity of the outer square follows from the one of the inner square by the uniqueness of the extension of continuous homomorphisms to completions. □

The following proposition was shown already in [Hei07].

Proposition 1.2.9. *Let (R,θ) be a simple n-variate ID-ring with ring of constants R^θ and $x_1,\dots,x_m \in R$. Then the following conditions are equivalent:*

(1) $x_1, \dots, x_m$ *are linearly independent over* R^θ.

(2) $\theta(x_1), \dots, \theta(x_m) \in R[\![t]\!]$ *are linearly independent over* R.

(3) There are $\boldsymbol{d_1}, \dots, \boldsymbol{d_m} \in \mathbb{N}^n$, *such that* $\det\left((\theta^{(\boldsymbol{d_i})}(x_j))_{i,j=1}^m\right) \in R^\times$.

In addition, the implications $(3) \iff (2) \implies (1)$ *also hold if* (R, θ) *is not simple as HD-ring.*

Proof. We show by induction on m that the second condition follows from the first. This is clear for $m = 1$, so let $m > 1$ and $x_1, \dots, x_m$ be linearly independent over C. Then $x_1, \dots, x_{m-1}$ are also linearly independent over C and by the induction hypothesis $\theta(x_1), \dots, \theta(x_{m-1})$ are linearly independent over R. By proposition 1.2.7 the ring R is an integral domain and θ extends to an iterative derivation on $L := \mathrm{Quot}(R)$. Suppose $\theta(x_1), \dots, \theta(x_m)$ were linearly dependent over R, then they would also be linearly dependent over L and we can assume without loss of generality that $\theta(x_m) = \sum_{j=1}^{m-1} a_j \theta(x_j)$ with $a_j \in L$. Then $\theta^{(\boldsymbol{k})}(x_m) = \sum_{j=1}^{m-1} a_j\, \theta^{(\boldsymbol{k})}(x_j)$ for all $\boldsymbol{k} \in \mathbb{N}^n$ and for $\boldsymbol{k} = \boldsymbol{0}$ we obtain the L-linear combination $x_m = \sum_{j=1}^{m-1} a_j x_j$. We will show that a_j are constants of L and thus also of R by proposition 1.2.7 for $j = 1, \dots, m-1$. For $\boldsymbol{i}, \boldsymbol{k} \in \mathbb{N}^n$ we have

$$\begin{aligned}
\binom{\boldsymbol{i}+\boldsymbol{k}}{\boldsymbol{k}} \theta^{(\boldsymbol{i}+\boldsymbol{k})}(x_m) &= \theta^{(\boldsymbol{i})} \circ \theta^{(\boldsymbol{k})}(x_m) \\
&= \sum_{j=1}^{m-1} \theta^{(\boldsymbol{i})}\left(a_j \theta^{(\boldsymbol{k})}(x_j)\right) \\
&= \sum_{j=1}^{m-1} \sum_{\boldsymbol{0} \le \boldsymbol{m} \le \boldsymbol{i}} \theta^{(\boldsymbol{m})}(a_j) \theta^{(\boldsymbol{i}-\boldsymbol{m})} \circ \theta^{(\boldsymbol{k})}(x_j) \\
&= \sum_{j=1}^{m-1} a_j \binom{\boldsymbol{i}+\boldsymbol{k}}{\boldsymbol{k}} \theta^{(\boldsymbol{i}+\boldsymbol{k})}(x_j) + \sum_{j=1}^{m-1} \sum_{\boldsymbol{0} < \boldsymbol{m} \le \boldsymbol{i}} \theta^{(\boldsymbol{m})}(a_j) \binom{\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m}}{\boldsymbol{k}} \theta^{(\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m})}(x_j) \\
&= \binom{\boldsymbol{i}+\boldsymbol{k}}{\boldsymbol{k}} \theta^{(\boldsymbol{i}+\boldsymbol{k})}(x_m) + \sum_{j=1}^{m-1} \sum_{\boldsymbol{0} < \boldsymbol{m} \le \boldsymbol{i}} \binom{\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m}}{\boldsymbol{k}} \theta^{(\boldsymbol{m})}(a_j) \theta^{(\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m})}(x_j)
\end{aligned}$$

and thus

$$\sum_{j=1}^{m-1} \sum_{\mathbf{0}<\boldsymbol{m}\leq\boldsymbol{i}} \binom{\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m}}{\boldsymbol{k}} \theta^{(\boldsymbol{m})}(a_j)\theta^{(\boldsymbol{i}+\boldsymbol{k}-\boldsymbol{m})}(x_j) = 0. \tag{1.2.3}$$

In the next step we show inductively

$$\sum_{j=1}^{m-1} \theta^{(l\boldsymbol{\delta}_\mu)}(a_j)\theta^{(\boldsymbol{k})}(x_j) = 0 \tag{1.2.4}$$

for all $\boldsymbol{k} \in \mathbb{N}^n$, $l \in \mathbb{N}$ and $\mu \in \{1,\dots,n\}$. We fix $\mu \in \{1,\dots,n\}$. For $l = 1$ equation (1.2.4) follows immediately from (1.2.3). Now we assume that for some $\tilde{l} \in \mathbb{N}$ equation (1.2.4) holds for all $0 \leq l \leq \tilde{l}$, all $\boldsymbol{k} \in \mathbb{N}^n$ and all $\mu \in \{1,\dots,n\}$ and show that it also holds for $\tilde{l}+1$, all $\boldsymbol{k} \in \mathbb{N}^n$ and all $\mu \in \{1,\dots,n\}$. From (1.2.3) we obtain for $\boldsymbol{i} = (\tilde{l}+1)\boldsymbol{\delta}_{\boldsymbol{\mu}}$ in particular

$$\sum_{j=1}^{m-1} \sum_{l=1}^{\tilde{l}+1} \binom{(\tilde{l}+1-l)\boldsymbol{\delta}_{\boldsymbol{\mu}}+\boldsymbol{k}}{\boldsymbol{k}} \theta^{(l\boldsymbol{\delta}_\mu)}(a_j)\theta^{((\tilde{l}+1-l)\boldsymbol{\delta}_{\boldsymbol{\mu}}+\boldsymbol{k})}(x_j) = 0.$$

In this sum all partial sums over j with fixed $l \in \{1,\dots,\tilde{l}\}$ are zero by assumption and we obtain $\sum_{j=1}^{m-1} \theta^{((\tilde{l}+1)\boldsymbol{\delta}_\mu)}(a_j)\theta^{(\boldsymbol{k})}(x_j) = 0$ for all $\boldsymbol{k} \in \mathbb{N}^n$. Thus, inductively we obtain (1.2.4) for all $l \in \mathbb{N}$, $\mu \in \{1,\dots,n\}$ and all $\boldsymbol{k} \in \mathbb{N}^n$. Since $\theta(x_1),\dots,\theta(x_{m-1}) \in R[\![\boldsymbol{t}]\!]$ are linearly independent over R, we obtain $\theta^{(l\boldsymbol{\delta}_\mu)}(a_j) = 0$ for all $l \in \mathbb{N}$ and all $\mu \in \{1,\dots,n\}$, and thus $a_j \in R^\theta$ for $j = 1,\dots,m-1$. Consequently, $x_1,\dots,x_m$ are linearly dependent over R^θ in contradiction to our assumption.

To show the converse, suppose that there exist $a_1,\dots,a_m \in R^\theta$, not all zero, such that $\sum_{i=1}^m a_i x_i = 0$. Then $0 = \theta\left(\sum_{i=1}^m a_i x_i\right) = \sum_{i=1}^m a_i \theta(x_i)$ and thus $\theta(x_1),\dots,\theta(x_m)$ are linearly dependent over R^θ and in particular over R.

The equivalence of the second and the third condition is clear. □

Using this characterization of linear independence over constants we obtain the following result, which, in the case of classical derivations and where A is a field, is due to Kolchin ([Kol76, Ch. 2, Corollary 1 to Theorem 1])

Corollary 1.2.10. *Let (R, θ_R) be a simple ID-ring and (A, θ_A) an ID-ring extension of R. Then R and A^{θ_A} are linearly disjoint over R^{θ_R}.*

Proof. Let $a_1, \ldots, a_m \in R$ be linearly independent over R^{θ_R}. Then by proposition 1.2.9 there are $\boldsymbol{d_1}, \ldots, \boldsymbol{d_m} \in \mathbb{N}^n$ such that $\det(\theta^{(\boldsymbol{d_i})}(a_j))_{i,j=1,\ldots,m} \in R^\times$ and by the same proposition we obtain that $a_1 \ldots, a_m$ are linearly independent over A^θ. □

1.3 Linearly non-degenerate higher derivations

The following lemma seems to be well known.

Lemma 1.3.1. *Let L/K be a separable and finitely generated field extension of transcendence degree n and M be an L-algebra. Then the M-module $\mathrm{Der}_K(L, M)$ of K-derivations from L to M is isomorphic to M^n. If $\{x_1, \ldots, x_n\}$ is a separating transcendence basis of L/K, then the K-derivations $\partial_{x_1}, \ldots, \partial_{x_n}$ from L to M, defined by $\partial_{x_i}(x_j) = \delta_{i,j}$ for $i, j \in \{1, \ldots, n\}$, form an M-basis of $\mathrm{Der}_K(L, M)$.*

Proof. Let $x_1, \ldots, x_n$ be a separating transcendence basis of L/K and $(\partial_{x_i} \colon L \to M)_{i=1,\ldots,n}$ be the K-derivations defined by $\partial_{x_i}(x_j) = \delta_{i,j}$ for $i, j \in \{1, \ldots, n\}$. We define two maps

$$\Phi \colon \mathrm{Der}_K(L, M) \to M^n, \quad \partial \mapsto (\partial(x_1), \ldots, \partial(x_n))$$

and

$$\Psi \colon M^n \to \mathrm{Der}_K(L, M), \quad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i \partial_{x_i}.$$

Then for all $\partial \in \mathrm{Der}_K(L, M)$ we have $(\Psi \circ \Phi)(\partial) = \sum_{i=1}^n \partial(x_i)\partial_{x_i}$ and thus $((\Psi \circ \Phi)(\partial))(x_j) = \partial(x_j)$ for all $j \in \{1, \ldots, n\}$. Since $L/K(x_1, \ldots, x_n)$ is finite separable, we obtain $(\Psi \circ \Phi)(\partial) = \partial$ (derivations extend uniquely to finite separable field extensions). It is clear that $\Phi \circ \Psi = \mathrm{id}_{M^n}$. □

Lemma 1.3.2. *Let L/K be a separable and finitely generated field extension with $\mathrm{trdeg}(L/K) = n$ and M be an L-algebra. Then for derivations $\partial_1, \ldots, \partial_n \in \mathrm{Der}_K(L, M)$ the following conditions are equivalent:*

(1) For all separating transcendence bases $\{x_1, \ldots, x_n\}$ *of* L/K *we have*

$$\det((\partial_i(x_j))_{i,j=1,\ldots,n}) \in M^\times.$$

(2) There exists a separating transcendence basis $\{x_1, \ldots, x_n\}$ *of* L/K *such that*

$$\det((\partial_i(x_j))_{i,j=1,\ldots,n}) \in M^\times.$$

(3) The derivations $\partial_1, \ldots, \partial_n$ *form an* M*-basis of* $\mathrm{Der}_K(L, M)$.

Proof. Trivially the first condition implies the second.

Now we assume that there is a separating transcendence basis $\{x_1, \ldots, x_n\}$ of L/K such that

$$\det((\partial_i(x_j))_{i,j=1,\ldots,n}) \in M^\times.$$

Since the K-derivations $\partial_{x_1}, \ldots, \partial_{x_n}$ defined by $\partial_{x_i}(x_j) = \delta_{i,j}$ for $i, j = 1, \ldots, n$ form an M-basis of $\mathrm{Der}_K(L, M)$ by lemma 1.3.1 and since $\partial_i = \sum_{j=1}^n \partial_i(x_j)\partial_{x_j}$ for $i = 1, \ldots, n$, the derivations $\partial_1, \ldots, \partial_n$ form an M-basis of $\mathrm{Der}_K(L, M)$ too.

If we assume (3) to be true and let $\{x_1, \ldots, x_n\}$ be a separating transcendence basis of L/K, then the derivations $\partial_{x_1}, \ldots, \partial_{x_n}$ form an M-basis of $\mathrm{Der}_K(L, M)$ by lemma 1.3.1. Thus, there exists a matrix $A \in \mathrm{GL}_n(M)$ such that $(\partial_1, \ldots, \partial_n)^t = A(\partial_{x_1}, \ldots, \partial_{x_n})^t$. So we obtain $(\partial_i(x_j))_{i,j=1,\ldots,n} = A$ and thus $\det((\partial_i(x_j))_{i,j=1,\ldots,n}) = \det(A) \in M^\times$. □

Definition 1.3.3. *Let* K *be a ring,* L *a* K*-algebra and* M *an* L*-algebra. An* n*-variate higher derivation* $\theta \in \mathrm{HD}_K^n(L, M)$ *is called* linearly non-degenerate *if the derivations* $\theta^{(\delta_1)}, \ldots, \theta^{(\delta_n)} \in \mathrm{Der}_K(L, M)$ *are linearly independent over* M.

In the case of n-variate iterative derivations, this definition coincides with the one given by A. Maurischat in [Mau10b].

Example 1.3.4. *If L/K is a separable and finitely generated field extension with separating transcendence basis $\{x_1, \dots, x_n\}$, then the n-variate iterative derivation $\theta_{(x_1,\dots,x_n)}$ on L over K defined in example 1.2.4 is linearly non-degenerate.*

The following proposition is essentially a concrete version of the formal inverse function theorem (cf. [Haz78, Appendix A, Proposition A.4.5] or [vdE00, Theorem 1.1.2]).

Proposition 1.3.5. *Let R be a ring, $n \in \mathbb{N}$ be a natural number and for $\nu = 1, \dots, n$ let*

$$\sum_{\boldsymbol{i} \in \mathbb{N}^n} a_{\boldsymbol{i}}^{(\nu)} \boldsymbol{t}^{\boldsymbol{i}}, \sum_{\boldsymbol{i} \in \mathbb{N}^n} b_{\boldsymbol{i}}^{(\nu)} \boldsymbol{t}^{\boldsymbol{i}} \in R[\![\boldsymbol{t}]\!] = R[\![t_1, \dots, t_n]\!]$$

be formal power series such that $a_{\boldsymbol{0}}^{(\nu)} = b_{\boldsymbol{0}}^{(\nu)}$ and such that $\det(a_{\delta_\mu}^{(\nu)})_{\nu,\mu=1,\dots,n} \in R^\times$. Then there exist formal power series $\sum_{\boldsymbol{i} \in \mathbb{N}^n} c_{\boldsymbol{i}}^{(\mu)} \boldsymbol{t}^{\boldsymbol{i}} \in R[\![\boldsymbol{t}]\!]$ with $c_{\boldsymbol{0}}^{(\mu)} = 0$ for all $\mu = 1, \dots, n$ such that for $\nu = 1, \dots, n$

$$\sum_{\boldsymbol{i} \in \mathbb{N}^n} a_{\boldsymbol{i}}^{(\nu)} \prod_{\mu=1}^{n} \left(\sum_{\boldsymbol{j} \in \mathbb{N}^n} c_{\boldsymbol{j}}^{(\mu)} \boldsymbol{t}^{\boldsymbol{j}} \right)^{i_\mu} = \sum_{\boldsymbol{j} \in \mathbb{N}^n} b_{\boldsymbol{j}}^{(\nu)} \boldsymbol{t}^{\boldsymbol{j}}. \tag{1.3.1}$$

If in addition $\det(b_{\delta_\mu}^{(\nu)})_{\nu,\mu=1,\dots,n} \in R^\times$, then $\det(c_{\delta_\mu}^{(\nu)})_{\nu,\mu=1,\dots,n} \in R^\times$ holds too.

Proof. Equation (1.3.1) holds if and only if for all $\nu \in \{1, \dots, n\}$ and all $\boldsymbol{j} \in \mathbb{N}^n$

$$b_{\boldsymbol{j}}^{(\nu)} = \sum_{\boldsymbol{i} \in \mathbb{N}^n} a_{\boldsymbol{i}}^{(\nu)} \sum_{\boldsymbol{k}_{1,1}+\dots+\boldsymbol{k}_{1,i_1}+\dots+\boldsymbol{k}_{n,1}+\dots+\boldsymbol{k}_{n,i_n}=\boldsymbol{j}} \prod_{\mu=1}^{n} \prod_{\lambda=1}^{i_\mu} c_{\boldsymbol{k}_{\mu,\lambda}}^{(\mu)}. \tag{1.3.2}$$

For $\boldsymbol{j} = \boldsymbol{0}$ this equation is fulfilled by assumption. We can determine $c_{\boldsymbol{j}}^{(\mu)}$ iteratively from this equation. In fact, the equations for $\nu = 1, \dots, n$ and $\boldsymbol{j} = \boldsymbol{\delta}_\lambda$, $\lambda = 1, \dots, n$ are equivalent to the system of linear equations

$$b_{\delta_\lambda}^{(\nu)} = \sum_{\mu=1}^{n} c_{\delta_\lambda}^{(\mu)} a_{\delta_\mu}^{(\nu)} \qquad \lambda, \nu = 1, \dots, n \tag{1.3.3}$$

for $(c_{\delta_\lambda}^{(\mu)})_{\mu,\lambda=1,\dots,n}$. Since the matrix of coefficients $(a_{\delta_\mu}^{(\nu)})_{\nu,\mu=1,\dots,n}$ is regular by assumption, there exists a unique solution $(c_{\delta_\lambda}^{(\mu)})_{\lambda,\mu=1,\dots,n} \in M_n(R)$. Now let

$\boldsymbol{j} \in \mathbb{N}^n$ and assume by induction that $c_{\tilde{\boldsymbol{j}}}^{(\mu)}$ are already determined for all $\mu = 1, \ldots, n$ and $\tilde{\boldsymbol{j}} < \boldsymbol{j}$. Then the equations (1.3.2) for $\boldsymbol{j}$ and $\nu = 1, \ldots, n$ form a system of linear equations in the unknowns $c_{\boldsymbol{j}}^{(\nu)}$ $(\nu = 1, \ldots, n)$ and the coefficients are again given by the matrix $(a_{\delta_\mu}^{(\nu)})_{\nu,\mu=1,\ldots,n}$. So $c_{\boldsymbol{j}}^{(\nu)}$ $(\nu = 1, \ldots, n)$ are uniquely determined too. The last statement is clear by equation (1.3.3). □

Proposition 1.3.6. *Let L/K be a separable and finitely generated field extension of transcendence degree n, let M be an L-algebra and $\theta_1, \theta_2 \in \mathrm{HD}_K^n(L, M)$ be such that θ_1 is linearly non-degenerate. Then there exists a homomorphism of M-algebras $\varphi\colon M[\![\boldsymbol{w}]\!] \to M[\![\boldsymbol{w}]\!]$ such that $\varphi(\boldsymbol{w})_{|\boldsymbol{w}=\boldsymbol{0}} = 0$ and such that the diagram*

$$\begin{array}{ccc} L & \xrightarrow{\theta_1} & M[\![\boldsymbol{w}]\!] \\ & \searrow^{\theta_2} & \downarrow \varphi \\ & & M[\![\boldsymbol{w}]\!] \end{array}$$

commutes.

Proof. Let $\{x_1, \ldots, x_n\}$ be a separating transcendence basis of L/K and $\tilde{L} \coloneqq K(x_1, \ldots, x_n)$. We define $\theta_1(x_\nu) =: \sum_{\boldsymbol{i} \in \mathbb{N}^n} a_{\boldsymbol{i}}^{(\nu)} \boldsymbol{w}^{\boldsymbol{i}}$ and $\theta_2(x_\nu) =: \sum_{\boldsymbol{i} \in \mathbb{N}^n} b_{\boldsymbol{i}}^{(\nu)} \boldsymbol{w}^{\boldsymbol{i}}$ for $\nu = 1, \ldots, n$. By lemma 1.3.2 and proposition 1.3.5, there exist formal power series $\sum_{\boldsymbol{i} \in \mathbb{N}^n} c_{\boldsymbol{i}}^{(\mu)} \boldsymbol{w}^{\boldsymbol{i}} \in M[\![\boldsymbol{w}]\!]$ with $c_{\boldsymbol{0}}^{(\mu)} = 0$ for $\mu = 1, \ldots, n$ such that for all $\nu = 1, \ldots, n$

$$\sum_{\boldsymbol{i} \in \mathbb{N}^n} a_{\boldsymbol{i}}^{(\nu)} \prod_{\mu=1}^{n} \left(\sum_{\boldsymbol{j} \in \mathbb{N}^n} c_{\boldsymbol{j}}^{(\mu)} \boldsymbol{w}^{\boldsymbol{j}} \right)^{i_\mu} = \sum_{\boldsymbol{i} \in \mathbb{N}^n} b_{\boldsymbol{i}}^{(\nu)} \boldsymbol{w}^{\boldsymbol{i}}.$$

Since $M[\![\boldsymbol{w}]\!]$ is complete with respect to the $(\boldsymbol{w})$-adic topology and since the series $\sum_{\boldsymbol{i} \in \mathbb{N}^n} c_{\boldsymbol{i}}^{(\mu)} \boldsymbol{w}^{\boldsymbol{i}}$ lie in $(\boldsymbol{w})$ for $\mu = 1, \ldots, n$, by the universal property of the formal power series ring $M[\![\boldsymbol{w}]\!]$ (see [Bou81, Chapter IV, §4.3, Proposition 4]) there exists a homomorphism of M-algebras $\varphi\colon M[\![\boldsymbol{w}]\!] \to M[\![\boldsymbol{w}]\!]$ with $\varphi(w_\mu) = \sum_{\boldsymbol{i} \in \mathbb{N}^n} c_{\boldsymbol{i}}^{(\mu)} \boldsymbol{w}^{\boldsymbol{i}}$ for $\mu = 1, \ldots, n$. Since $\varphi \circ \theta_1$ and θ_2 are K-homomorphisms and

$\varphi \circ \theta_1(x_\nu) = \theta_2(x_\nu)$ for $\nu = 1, \ldots, n$, the homomorphisms $\varphi \circ \theta_1$ and θ_2 coincide on $\tilde{L}$, i.e. the diagram

$$\begin{array}{ccc} \tilde{L} & \xrightarrow{\theta_{1|\tilde{L}}} & M[\![\boldsymbol{w}]\!] \\ & \searrow^{\theta_{2|\tilde{L}}} & \downarrow \varphi \\ & & M[\![\boldsymbol{w}]\!] \end{array}$$

commutes. The extension $L/\tilde{L}$ is 0-étale by example 1.2.3 (2). Since $\varphi \circ \theta_1$ and θ_2 are both higher derivations from L to M that extend $\theta_{2|\tilde{L}} = \varphi \circ \theta_{1|\tilde{L}}$, they have to be equal by proposition 1.2.2. □

Corollary 1.3.7. *Let L/K be a separable and finitely generated field extension of transcendence degree n and let $\theta_1, \theta_2 \in \mathrm{HD}^n_K(L)$. If θ_1 is linearly non-degenerate, then for all $\boldsymbol{l} \in \mathbb{N}^n$ the component $\theta_2^{(\boldsymbol{l})}$ of θ is an L-linear combination of $\{\theta_1^{(\boldsymbol{j})} \mid |\boldsymbol{j}| \leq |\boldsymbol{l}|\}$.*

Proof. By proposition 1.3.6, there exists a homomorphism $\varphi \in \mathsf{Alg}_{\mathsf{L}}(L[\![\boldsymbol{w}]\!], L[\![\boldsymbol{w}]\!])$ such that $\theta_2 = \varphi \circ \theta_1$ and $\varphi(\boldsymbol{w})_{|\boldsymbol{w}=\boldsymbol{0}} = 0$. If we write $\varphi(w_i) = \sum_{\boldsymbol{l} \in \mathbb{N}^n} c_{\boldsymbol{l}}^{(i)} \boldsymbol{w}^{\boldsymbol{l}}$ with $c_{\boldsymbol{l}}^{(i)} \in L$ for $i = 1, \ldots, n$, then for all $a \in L$

$$\begin{aligned} \theta_2(a) &= \varphi(\theta_1(a)) \\ &= \sum_{\boldsymbol{j} \in \mathbb{N}^n} \theta_1^{(\boldsymbol{j})}(a) \varphi(w_1)^{j_1} \cdots \varphi(w_n)^{j_n} \\ &= \sum_{\boldsymbol{j} \in \mathbb{N}^n} \theta_1^{(\boldsymbol{j})}(a) \sum_{\boldsymbol{l}_{1,1}, \ldots, \boldsymbol{l}_{1,j_1}, \ldots, \boldsymbol{l}_{n,1}, \ldots, \boldsymbol{l}_{n,j_n} \in \mathbb{N}^n} \prod_{i=1}^{n} \prod_{j=1}^{j_i} c_{\boldsymbol{l}_{i,j}}^{(i)} \boldsymbol{w}^{\boldsymbol{l}_{1,1} + \cdots + \boldsymbol{l}_{1,j_1} + \cdots + \boldsymbol{l}_{n,1} + \cdots + \boldsymbol{l}_{n,j_n}} \end{aligned}$$

Thus, by noting that $c_{\boldsymbol{0}}^{(i)} = 0$ for $i = 1, \ldots, n$, we see that the $\theta_1^{(\boldsymbol{j})}(a)$ occurring in the coefficient of $\boldsymbol{w}^{\boldsymbol{l}}$ for $\boldsymbol{l} \in \mathbb{N}^n$ need to fulfill $|\boldsymbol{j}| \leq |\boldsymbol{l}|$, i.e. $\theta_2^{(\boldsymbol{l})}$ is a linear combination of the $\theta_1^{(\boldsymbol{j})}$ with $|\boldsymbol{j}| \leq |\boldsymbol{l}|$. □

Chapter 2

Module algebras

Since there are different conventions concerning the definition of algebras, coalgebras and bialgebras in the literature, we start this chapter by stating the definitions we use. Next, we recall the definition of module algebras, introduce some new notation concerning them, and prove some of their basic properties. At the end of the chapter we illustrate these concepts by giving several examples, including a comparison to the iterative Hasse systems that have been recently defined by R. Moosa and T. Scanlon.

Notation: *Let C be a commutative ring.*

2.1 Algebras, coalgebras and bialgebras

Although these terms are well known, we recall the notion of C-algebras, C-coalgebras and C-bialgebras as defined in [Bou70] and fix our convention.

Definition 2.1.1. *A* C-algebra *(or algebra over C) is a pair (A, m) consisting of a C-module A together with a homomorphism of C-modules*

$$m\colon A \otimes_C A \to A,$$

called the multiplication *of A. A C-algebra A is* associative *if the diagram*

$$\begin{array}{ccc} A \otimes_C A \otimes_C A & \xrightarrow{m\otimes \mathrm{id}} & A \otimes_C A \\ \downarrow{\scriptstyle \mathrm{id}\otimes m} & & \downarrow{\scriptstyle m} \\ A \otimes_C A & \xrightarrow{m} & A \end{array}$$

commutes. A C-algebra A is commutative *if the diagram*

$$\begin{array}{ccc} A \otimes_C A & \xrightarrow{\tau} & A \otimes_C A \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & A & \end{array}$$

commutes, where

$$\tau\colon A \otimes_C A \to A \otimes_C A \tag{2.1.1}$$

denotes the homomorphism defined by $\tau(a \otimes b) = b \otimes a$ for all $a, b \in A$. A unital C-algebra *is a triple (A, m, η) where (A, m) is a C-algebra and*

$$\eta\colon C \to A$$

is a homomorphism of C-modules, called the unit, *such that the diagram*

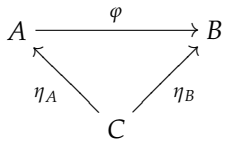
$$\begin{array}{ccccc} C \otimes_C A & \xrightarrow{\eta\otimes \mathrm{id}} & A \otimes_C A & \xleftarrow{\mathrm{id}\otimes \eta} & A \otimes_C C \\ & \searrow & \downarrow{\scriptstyle m} & \swarrow & \\ & & A & & \end{array}$$

commutes, where $C \otimes_C A \to A$ is the canonical isomorphism.

If (A, m_A) and (B, m_B) are C-algebras, a homomorphism of C-algebras *from A to B is a map $\varphi\colon A \to B$ such that the diagram*

$$\begin{array}{ccc} A \otimes_C A & \xrightarrow{\varphi\otimes\varphi} & B \otimes_C B \\ \downarrow{\scriptstyle m_A} & & \downarrow{\scriptstyle m_B} \\ A & \xrightarrow{\varphi} & B \end{array}$$

commutes. If (A, m_A, η_A) *and* (B, m_B, η_B) *are unital* C*-algebras, then a homomorphism of unital* C*-algebras from* (A, m_A, η_A) *to* (B, m_B, η_B) *is a homomorphism of* C*-algebras such that the diagram*



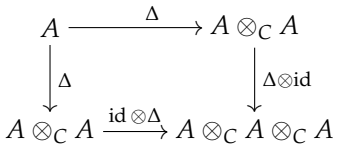
commutes.

Convention: *We assume that every* C*-algebra is associative and unital if not mentioned otherwise explicitly.*

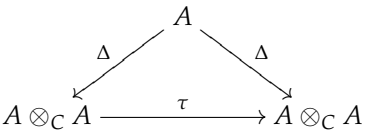
Definition 2.1.2. *A* C-coalgebra *(or* coalgebra *over* C*) is a pair* (A, Δ) *consisting of a* C*-module* A *together with a homomorphism of* C*-modules*

$$\Delta\colon A \to A \otimes_C A,$$

called the comultiplication *of* A*. A* C*-coalgebra* (A, Δ) *is* coassociative *if the diagram*



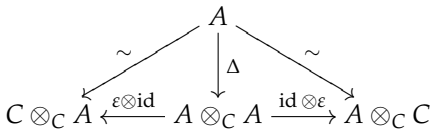
commutes. A C*-coalgebra* (A, Δ) *is* cocommutative *if the diagram*



commutes, where τ *is the homomorphism* (2.1.1)*. A* counital C-coalgebra *is a tuple* (A, Δ, ε) *where* (A, Δ) *is a* C*-coalgebra and*

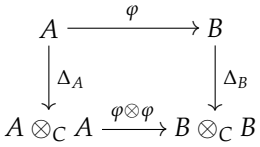
$$\varepsilon\colon A \to C$$

is a homomorphism of C-modules, called the counit, *such that the diagram*

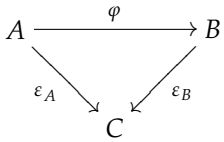


commutes.

If (A, Δ_A) *and* (B, Δ_B) *are C-coalgebras, then a* homomorphism of *C*-coalgebras *from* (A, Δ_A) *to* (B, Δ_B) *is a homomorphism of C-modules* $\varphi\colon A \to B$ *such that the diagram*



commutes; if $(A, \Delta_A, \varepsilon_A)$ *and* $(B, \Delta_B, \varepsilon_B)$ *are counital C-coalgebras, then a homomorphism from the counital C-coalgebra* $(A, \Delta_A, \varepsilon_A)$ *to* $(B, \Delta_B, \varepsilon_B)$ *is a homomorphism of C-coalgebras* φ *such that the diagram*



commutes.

Convention: *We assume that every C-coalgebra is coassociative and counital if not mentioned otherwise explicitly.*

Notation: *We use the Sweedler* Σ*-notation. If A is a C-coalgebra and* $a \in A$*, then we write*

$$\Delta(a) =: \sum_{(a)} a_{(1)} \otimes a_{(2)}$$

(see [Swe69, Section 1.2]).

Definition 2.1.3. *A* C-bialgebra *is a* C*-module* D *with a structure of a (unital, associative)* C*-algebra* (m, η) *and a structure of a (counital, coassociative)* C*-coalgebra* (Δ, ε) *such that the comultiplication* $\Delta\colon D \to D \otimes_C D$ *and the counit* $\varepsilon\colon D \to C$ *are homomorphisms of* C*-algebras.*

A C*-bialgebra is* commutative *(*cocommutative*) if the underlying* C*-algebra is commutative (the underlying* C*-coalgebra is cocommutative).*

A homomorphism of C-bialgebras *is a map that is a homomorphism of* C*-algebras and of* C*-coalgebras.*

Remark 2.1.4. *The condition in definition 2.1.3 that the comultiplication* Δ *and the counit* ε *are homomorphisms of* C*-algebras is fulfilled if and only if the multiplication* $m\colon A \otimes_C A \to A$ *and the unit* $\eta\colon C \to A$ *are homomorphisms of* C*-coalgebras (cf. [Swe69, Proposition 3.1.1]).*

Lemma 2.1.5. *If* (D, Δ) *is a cocommutative* C*-coalgebra, then we have*

$$(\Delta \otimes \Delta) \circ \Delta = (\mathrm{id}_D \otimes \tau \otimes \mathrm{id}_D) \circ (\Delta \otimes \Delta) \circ \Delta.$$

Proof. We have

$$\begin{aligned}(\Delta \otimes \Delta) \circ \Delta &= (\Delta \otimes \mathrm{id}_D \otimes \mathrm{id}_D) \circ (\mathrm{id}_D \otimes \Delta) \circ \Delta \\ &= (\Delta \otimes \mathrm{id}_D \otimes \mathrm{id}_D) \circ (\Delta \otimes \mathrm{id}_D) \circ \Delta \\ &= (\Delta \otimes \mathrm{id}_D \otimes \mathrm{id}_D) \circ (\tau \circ \Delta \otimes \mathrm{id}_D) \circ \Delta \\ &= (\Delta \otimes \mathrm{id}_D \otimes \mathrm{id}_D) \circ (\tau \otimes \mathrm{id}_D) \circ (\Delta \otimes \mathrm{id}_D) \circ \Delta \\ &= (\mathrm{id}_D \otimes \Delta \otimes \mathrm{id}_D) \circ (\Delta \otimes \mathrm{id}_D) \circ \Delta\end{aligned}$$

and so we obtain

$$\begin{aligned}(\Delta \otimes \Delta) \circ \Delta &= (\mathrm{id}_D \otimes \Delta \otimes \mathrm{id}_D) \circ (\Delta \otimes \mathrm{id}_D) \circ \Delta \\ &= (\mathrm{id}_D \otimes \tau \otimes \mathrm{id}_D) \circ (\mathrm{id}_D \otimes \Delta \otimes \mathrm{id}_D) \circ (\Delta \otimes \mathrm{id}_D) \circ \Delta \\ &= (\mathrm{id}_D \otimes \tau \otimes \mathrm{id}_D) \circ (\Delta \otimes \Delta) \circ \Delta.\end{aligned}$$

□

Notation: *For $n \in \mathbb{N}$, C-modules $A_1, \ldots, A_n$ and a permutation*

$$\begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}$$

of the numbers $\{1, \ldots, n\}$ we denote by $(i_1, \ldots, i_n)$ the homomorphism

$$A_1 \otimes_C \cdots \otimes_C A_n \to A_{i_1} \otimes_C \cdots \otimes_C A_{i_n}$$

defined by

$$(i_1, \ldots, i_n)(a_1 \otimes \cdots \otimes a_n) := a_{i_1} \otimes \cdots \otimes a_{i_n}$$

for all $a_1 \in A_1, \ldots, a_n \in A_n$.

Lemma 2.1.6. *If $(D_1, \Delta_1, \varepsilon_1)$ and $(D_2, \Delta_2, \varepsilon_2)$ are C-coalgebras, then $D_1 \otimes_C D_2$ carries a natural C-coalgebra structure with comultiplication and counit given by*

$$\Delta := (\mathrm{id}_{D_1} \otimes \tau \otimes \mathrm{id}_{D_2}) \circ (\Delta_1 \otimes \Delta_2) \qquad \textit{and} \qquad \varepsilon := \varepsilon_1 \otimes \varepsilon_2,$$

respectively. If both, D_1 and D_2, are cocommutative, so is $D_1 \otimes_C D_2$. If in addition D_1 and D_2 are C-bialgebras, then the C-coalgebra $D_1 \otimes_C D_2$ becomes a C-bialgebra with the usual C-algebra structure on the tensor product.

Proof. Since

$$\begin{aligned}(\varepsilon \otimes \mathrm{id}_{D_1 \otimes D_2}) \circ \Delta &= (\varepsilon_1 \otimes \varepsilon_2 \otimes \mathrm{id}_{D_1} \otimes \mathrm{id}_{D_2}) \circ (\mathrm{id}_{D_1} \otimes \tau \otimes \mathrm{id}_{D_2}) \circ (\Delta_1 \otimes \Delta_2) \\ &= ((\varepsilon_1 \otimes \mathrm{id}_{D_1}) \circ \Delta_1) \otimes ((\varepsilon_2 \otimes \mathrm{id}_{D_2}) \circ \Delta_2) \\ &= \mathrm{id}_{D_1} \otimes \mathrm{id}_{D_2},\end{aligned}$$

the homomorphism ε is a counit for Δ. Using the coassociativity of D_1 and D_2 we have

$$\begin{aligned}(\Delta \otimes \mathrm{id}_{D_1 \otimes D_2}) \circ \Delta &= (1,4,2,5,3,6) \circ (\Delta_1 \otimes \mathrm{id}_{D_1} \otimes \Delta_2 \otimes \mathrm{id}_{D_2}) \circ (\Delta_1 \otimes \Delta_2) \\ &= (1,4,2,5,3,6) \circ (\mathrm{id}_{D_1} \otimes \Delta_1 \otimes \mathrm{id}_{D_2} \otimes \Delta_2) \circ (\Delta_1 \otimes \Delta_2) \\ &= (\mathrm{id}_{D_1 \otimes D_2} \otimes \Delta) \circ \Delta.\end{aligned}$$

Thus, the comultiplication Δ is coassociative. If D_1 and D_2 are cocommutative, we have

$$\begin{aligned}\tau_{D_1\otimes D_2}\circ\Delta &= (3,4,1,2)\circ(\mathrm{id}_{D_1}\otimes\tau\otimes\mathrm{id}_{D_2})\circ(\Delta_1\otimes\Delta_2)\\ &= (2,4,1,3)\circ(\Delta_{D_1}\otimes\Delta_2)\\ &= (2,4,1,3)\circ(\tau_{D_1}\circ\Delta_{D_1}\otimes\tau_{D_2}\circ\Delta_2)\\ &= (1,3,2,4)\circ(\Delta_1\otimes\Delta_2)\\ &= \Delta,\end{aligned}$$

where τ denotes the twist homomorphism interchanging the factors of $D_1 \otimes D_2$ and $\tau_{D_1\otimes D_2}$, τ_{D_1} and τ_{D_2} denote the twist homomorphisms on $(D_1 \otimes D_2) \otimes (D_1 \otimes D_2)$, $D_1 \otimes D_1$ and $D_2 \otimes D_2$, respectively. Thus, the comultiplication Δ on $D_1 \otimes_C D_2$ is cocommutative.

If D_1 and D_2 are C-bialgebras, then obviously Δ and ε are homomorphisms of C-algebras and thus $D_1 \otimes_C D_2$ is a C-bialgebra. □

2.2 Module algebras

Next, we recall some definitions and results concerning measuring and module algebras. A standard reference for this material is [Swe69], although there the theory is only developed over fields. Some of the results that we present here might be well known, but since we do not know a reference, we include proofs. Module algebras are fundamental for the formulation of our Galois theory in chapter 3. The usage of module algebras is inspired by the work of M. Takeuchi, K. Amano and A. Masuoka ([Tak89], [AM05]), in which they present generalizations of Picard-Vessiot theory.

2.2.1 Module algebras

We recall that for C-modules A, B and D there is an isomorphism of C-modules

$$\mathsf{Mod}_C(D \otimes_C A, B) \to \mathsf{Mod}_C(A, \mathsf{Mod}_C(D, B)), \quad \Psi \mapsto (a \mapsto (d \mapsto \Psi(d \otimes a))), \tag{2.2.1}$$

which plays a key role in the theory of module algebras and is also fundamentally used in the formulation of our Galois theory in chapter 3 (see [Bou70, Chapter II, §4.1, Proposition 1 a)]).

Lemma 2.2.1. *If $(D, \Delta_D, \varepsilon_D)$ is a C-coalgebra and (B, m_B, η_B) is a C-algebra, then the C-module $\mathsf{Mod}_C(D, B)$ becomes a C-algebra with respect to the* convolution product*, defined by*

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

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

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

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

Proof. See for example [BW03, 1.3] □

Proposition 2.2.2. *Let D be a C-coalgebra and let A and B be C-algebras. If Ψ is an element of $\mathsf{Mod}_C(D \otimes_C A, B)$ and $\rho \in \mathsf{Mod}_C(A, \mathsf{Mod}_C(D, B))$ is the image of Ψ under the isomorphism (2.2.1), 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) $\Psi(d \otimes ab) = \sum_{(d)} \Psi(d_{(1)} \otimes a)\Psi(d_{(2)} \otimes b)$ and

b) $\Psi(d \otimes 1_A) = \varepsilon(d)1_B$,

hold and

(3) the diagrams

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

and

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

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. □

Definition 2.2.3. *Let D be a C-coalgebra and A and B be C-algebras. If $\Psi \in \mathsf{Mod}_C(D \otimes_C A, B)$, then we say that Ψ* measures *A to B if the equivalent conditions in proposition 2.2.2 are satisfied.*

Definition 2.2.4. *Let D be a C-bialgebra and A be a C-algebra. If $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$, we say that Ψ is a D-*module algebra structure *on A if*

(1) Ψ makes A into a D-module and

(2) Ψ measures A to A.

*The pair (A, Ψ) then is called a D-*module algebra*. We will also refer to the D-module algebra (A, Ψ) as (A, ρ), where ρ is the homomorphism of C-algebras associated to Ψ via the isomorphism* (2.2.1)*. If there is no risk of confusion, then we will denote the D-module algebra (A, Ψ) also by A. A D-module algebra (A, Ψ) is called* commutative *if the C-algebra A is commutative.*

If A is a D-module algebra and B is a C-subalgebra of A, we say that B is a D-module subalgebra *of A if the restriction of Ψ to $D \otimes_C B$ induces a homomorphism $D \otimes_C B \to B$ of C-modules that defines a D-module algebra structure on B.*

If B is a D-module subalgebra of A and A' is a subset of A, the D-module subalgebra of A generated by A' over B *is defined as the smallest D-module subalgebra of A containing B and A' and we denote it by $B\{A'\}_\Psi$. If A is a D-module algebra and $B \subseteq A$ a D-module subalgebra, then we say that A is* finitely generated over B as D-module algebra *if there is a finite subset A' of A such that $A = B\{A'\}_\Psi$.*

A D-module field *is a D-module algebra (A, Ψ) such that the C-algebra A is a field. If A is a D-module algebra, then a* D-module subfield *of A is a D-module subalgebra of A that is a D-module field.*

Section 2.3 contains examples of bialgebras illustrating this definition, among them a bialgebra D_{der} such that D_{der}-module algebras are differential rings over C, a bialgebra D_{ID^n} such that D_{ID^n}-module algebras are n-variate iterative differential rings over C and a bialgebra D_{end} such that D_{end}-module algebras are difference rings over C.

We use the isomorphism (2.2.1) a second time in the form

$$\mathsf{Mod}_C(D_1 \otimes_C D_2, A) \xrightarrow{\sim} \mathsf{Mod}_C(D_2, \mathsf{Mod}_C(D_1, A)) \tag{2.2.2}$$

for C-modules D_1, D_2 and A. If D_1 and D_2 are C-coalgebras and A is a C-algebra, then this is in fact a homomorphism of C-algebras with respect to the C-algebra structures induced by lemma 2.2.1 ($D_1 \otimes_C D_2$ carries the C-coalgebra structure defined in lemma 2.1.6). In the following we sometimes implicitly use this isomorphism.

Lemma 2.2.5. *Let D be a C-algebra, A be a C-module and $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$. Then Ψ makes A into a D-module if and only if the homomorphism of C-modules*

$\rho\colon A \to \mathsf{Mod}_C(D, A)$ *associated to* Ψ *via the isomorphism* (2.2.1) *makes the diagrams*

$$\begin{array}{ccc} A & \xrightarrow{\rho} & \mathsf{Mod}_C(D, A) \\ & \searrow^{\mathrm{id}_A} & \downarrow{\scriptstyle \mathrm{ev}_{1_D}} \\ & & A \end{array} \tag{2.2.3}$$

and

$$\begin{array}{ccccc} A & & \xrightarrow{\quad\rho\quad} & & \mathsf{Mod}_C(D, A) \\ \downarrow{\scriptstyle \rho} & & & & \downarrow{\scriptstyle \mathsf{Mod}_C(D,\rho)} \\ \mathsf{Mod}_C(D, A) & \xrightarrow{\mathsf{Mod}_C(m_D, A)} & \mathsf{Mod}_C(D \otimes_C D, A) & \xrightarrow{\sim} & \mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A)). \end{array} \tag{2.2.4}$$

commutative, where the isomorphism at the bottom right is (2.2.2).

Proof. The first diagram commutes if and only if $\Psi(1_D \otimes a) = a$ holds for all $a \in A$ and the second diagram commutes if and only if $\Psi(d_1 d_2 \otimes a) = \Psi(d_1 \otimes \Psi(d_2 \otimes a))$ holds for all $d_1, d_2 \in D$ and all $a \in A$. □

Corollary 2.2.6. *Let D be a C-bialgebra, A be a C-algebra and $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$. Then Ψ is a D-module algebra structure on A if and only if the homomorphism $\rho\colon A \to \mathsf{Mod}_C(D, A)$ associated to Ψ via the isomorphism* (2.2.1) *is a homomorphism of C-algebras and makes the diagrams* (2.2.3) *and* (2.2.4) *commutative.*

Proof. This follows immediately from lemma 2.2.5. □

Lemma 2.2.7. *Let D be a C-bialgebra, A a C-algebra and let $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$ make A into a D-module algebra. If A' is a subset of A, then the D-module subalgebra of A generated by A' over C is the C-subalgebra of A generated by $\Psi(D \otimes_C A')$ over C, i.e.*

$$C\{A'\}_\Psi = C[\Psi(D \otimes_C A')].$$

Proof. Certainly $C[\Psi(D \otimes_C A')]$ is contained in $C\{A'\}_\Psi$. For all $c_1, c_2, d \in D$ and $a_1, a_2 \in A'$ we have

$$d((c_1.a_1)(c_2.a_2)) = \sum_{(d)} d_{(1)}(c_1.a_1) \cdot d_{(2)}(c_2.a_2) = \sum_{(d)} (d_{(1)}c_1).a_1 \cdot (d_{(2)}c_2).a_2$$

and so $d.(ab) \in C[\Psi(D \otimes_C A')]$ for all $a, b \in C[\Psi(D \otimes_C A')]$. Thus, $C[\Psi(D \otimes_C A')]$ is a C-subalgebra and a D-submodule of A, i.e. a D-module subalgebra of A. □

Notation: *If D is a C-bialgebra, A a C-algebra and $\Psi \in \mathsf{Mod}_C(D, A)$ is a D-module algebra structure on A, then we write also $d.a$ or $d(a)$ instead of $\Psi(d \otimes a)$ for $d \in D$ and $a \in A$ if no confusion is possible. If $X = (x_{i,j})_{i,j=1}^n \in M_{n\times m}$ is a matrix with coefficients in A, we denote the matrix $(d.x_{i,j})_{i,j=1}^n$ by $\Psi(d \otimes X)$ and also by $d.X$, $d(X)$ or dX if there is no risk of confusion.*

2.2.2 Homomorphisms, ideals and constants of module algebras

Definition 2.2.8. *Let D be a C-bialgebra. A* homomorphism of D-module algebras *is a map that is a homomorphism of D-modules and of C-algebras. Homomorphisms of D-module fields are homomorphisms of D-module algebras.*

Remark 2.2.9. *If (A_1, Ψ_1) and (A_2, Ψ_2) are D-module algebras and ρ_1 and ρ_2 are the homomorphisms of C-algebras associated to Ψ_1 and Ψ_2 via the isomorphism 2.2.1, respectively, then a homomorphism of C-algebras $f\colon A_1 \to A_2$ is a homomorphism of the D-module algebra (A_1, Ψ_1) to (A_2, Ψ_2) if and only if the diagram*

$$\begin{array}{ccc} A_1 & \xrightarrow{\quad f \quad} & A_2 \\ \downarrow{\scriptstyle \rho_1} & & \downarrow{\scriptstyle \rho_2} \\ \mathsf{Mod}_C(D, A_1) & \xrightarrow{\mathsf{Mod}_C(D,f)} & \mathsf{Mod}_C(D, A_2) \end{array}$$

commutes.

Definition 2.2.10. *If D is a C-bialgebra, (A, Ψ) a D-module algebra and I an ideal in A, then I is called D-*stable *if $\Psi(d \otimes a) \in I$ for all $a \in I$ and all $d \in D$.*

Lemma 2.2.11. *Let D be a C-bialgebra and A be a D-module algebra. If I is a D-stable ideal in A, then there exists a unique D-module algebra structure on A/I such that the canonical projection $A \to A/I$ becomes a homomorphism of D-module algebras.*

Proof. If (A, Ψ) is a D-module algebra and I a D-stable ideal in A, it is clear that

$$\bar{\Psi} \colon D \otimes A/I \to A/I, \quad d \otimes (a + I) \mapsto \Psi(d \otimes a) + I$$

is the unique D-module algebra structure on A/I such that $A \to A/I$ becomes a homomorphism of D-module algebras. □

Definition 2.2.12. *For a C-coalgebra D, a C-module V and $\Psi \in \mathsf{Mod}_C(D \otimes_C V, V)$ we define the* constants *of V with respect to Ψ as*

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

If $\rho \in \mathsf{Mod}_C(D, \mathsf{Mod}_C(D, V))$ is the element corresponding to Ψ under the isomorphism (2.2.1)*, then we denote V^{Ψ} also by V^{ρ}.*[1]

Remark 2.2.13. *K. Amano defines in [Ama05, p. 31] constants for D-modules V, where D is a C-bialgebra. In this case our definitions coincide, when we equip V with the induced C-module structure and define $\Psi \colon D \otimes_C V \to V$ by sending $d \otimes v$ to dv.*

Lemma 2.2.14. *Let D be a C-coalgebra, A be a C-algebra and let $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$ measure A to A.*

(1) Then A^{Ψ} is a C-subalgebra of A.

(2) If moreover A is a field, then A^{Ψ} is a subfield of A.

[1] The constants V^{ρ} are the equalizer in V of ρ and ρ_0, where ρ_0 is the homomorphism defined in lemma 2.2.15.

Proof. For $a, b \in A^\Psi$ we have

$$\Psi(d \otimes (a+b)) = \Psi(d \otimes a) + \Psi(d \otimes b) = \varepsilon(d)(a+b)$$

and, since D measures A to A,

$$\Psi(d \otimes ab) = \sum_{(d)} \Psi(d_{(1)} \otimes a)\Psi(d_{(2)} \otimes b) = \sum_{(d)} \varepsilon(d_{(1)})a\varepsilon(d_{(2)})b = \varepsilon(d)ab$$

If A is a field and a is a non-zero element in A^Ψ, then we have $\rho(a^{-1}) = \rho(a)^{-1} = \rho_0(a)^{-1} = \rho_0(a^{-1})$, so that a^{-1} is constant too. □

Lemma 2.2.15. *Let D be a C-bialgebra and A be a C-algebra.*

(1) There exists a D-module algebra structure $\Psi_0 \in \mathsf{Mod}_C(D \otimes_C A, A)$ on A, defined by

$$\Psi_0 \colon D \otimes_C A \to A, \quad d \otimes a \mapsto \varepsilon_D(d)a.$$

We denote the homomorphism of C-algebras associated to Ψ_0 via the isomorphism (2.2.1) *by ρ_0 and call call Ψ_0 the* trivial D-module algebra structure *on A.*

(2) We have for all $a \in A$ and all $f \in \mathsf{Mod}_C(D, A)$

$$\rho_0(a) * f = af \quad \text{and}$$
$$f * \rho_0(a) = fa,$$

where af and fa are the scalar multiplications of f with a from the left and from the right, respectively, i.e. $(af)(d) = a(f(d))$ and $(fa)(d) = f(d)a$ for all $d \in D$. In particular, $\rho_0(A)$ lies in the center of $(\mathsf{Mod}_C(D, A), \cdot)$ if A is commutative.

(3) The constants of (A, Ψ_0) are equal to A.

Proof. We note that $\varepsilon_D\colon D \to C$ is the unique homomorphism of C-bialgebras from D to the trivial C-bialgebra C. The C-module homomorphism ρ_0 associated to Ψ_0 via the isomorphism (2.2.1) is given as the composition

$$A \xrightarrow{\sim} \mathsf{Mod}_C(C, A) \xrightarrow{\mathsf{Mod}_C(\varepsilon_D, A)} \mathsf{Mod}_C(D, A).$$

Obviously ρ_0 makes the diagrams

$$\begin{array}{ccc} A & \xrightarrow{\rho_0} & \mathsf{Mod}_C(D, A) \\ & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{ev}_{1_D}} \\ & & A \end{array}$$

and

$$\begin{array}{ccccc} A & & \xrightarrow{\rho_0} & & \mathsf{Mod}_C(D, A) \\ \downarrow{\scriptstyle \rho_0} & & & & \downarrow{\scriptstyle \mathsf{Mod}_C(D, \rho_0)} \\ \mathsf{Mod}_C(D, A) & \xrightarrow{\mathsf{Mod}_C(m_D, A)} & \mathsf{Mod}_C(D \otimes_C D, A) & \xrightarrow{\sim} & \mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A)) \end{array}$$

commutative and thus Ψ_0 is a D-module algebra structure on A. Part (2) follows from

$$(\rho_0(a) * f)(d) = \sum_{(d)} \varepsilon(d_{(1)}) a f(d_{(2)}) = af\left(\sum_{(d)} \varepsilon(d_{(1)}) d_{(2)}\right) = af(d)$$

and

$$(f * \rho_0(a))(d) = \sum_{(d)} f(d_{(1)}) \varepsilon(d_{(2)}) a = f\left(\sum_{(d)} d_{(1)} \varepsilon(d_{(2)})\right) a = f(d)a$$

for all $d \in D$. The last assertion is clear by definition. □

2.2.3 The module algebra structure Ψ_{int}

Lemma 2.2.16. *If D is a C-bialgebra and A a C-algebra, then $\mathsf{Mod}_C(D, A)$ becomes a D-module algebra by the homomorphism of C-modules*

$$\Psi_{int}\colon D \otimes_C \mathsf{Mod}_C(D, A) \to \mathsf{Mod}_C(D, A)$$

which sends $d \otimes f \in D \otimes_C \mathsf{Mod}_C(D, A)$ to the homomorphism of C-modules

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

Furthermore, for any homomorphism of C-algebras $\varphi\colon A \to B$ the induced homomorphism of C-algebras

$$\mathsf{Mod}_C(D, \varphi)\colon \mathsf{Mod}_C(D, A) \to \mathsf{Mod}_C(D, B)$$

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

The constants $\mathsf{Mod}_C(D, A)^{\Psi_{int}}$ are equal to $\rho_0(A)$, where $\rho_0\colon A \to \mathsf{Mod}_C(D, A)$ is the homomorphism associated to the trivial D-module algebra structure Ψ_0 on A (see lemma 2.2.15).

Proof. We note that the homomorphism of C-modules

$$\rho_{int}\colon \mathsf{Mod}_C(D, A) \to \mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A))$$

corresponding to Ψ_{int} via the isomorphism (2.2.1) corresponds to $\mathsf{Mod}_C(m_D, A)$ under the isomorphism of C-algebras (2.2.2) between $\mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A))$ and $\mathsf{Mod}_C(D \otimes_C D, A)$. Since m_D is a homomorphism of C-coalgebras, $\mathsf{Mod}_C(m_D, A)$ and so also ρ_{int} are homomorphisms of C-algebras. The diagram

$$\begin{array}{ccc} \mathsf{Mod}_C(D, A) & \xrightarrow{\rho_{int}} & \mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A)) \\ & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{ev}_{1_D}} \\ & & \mathsf{Mod}_C(D, A) \end{array}$$

obviously commutes. Using again the isomorphism

$$\mathsf{Mod}_C(D, \mathsf{Mod}_C(D, A)) \cong \mathsf{Mod}_C(D \otimes_C D, A),$$

under which ρ_{int} corresponds to $\mathsf{Mod}_C(m_D, A)$, the commutativity of the diagram

$$\begin{array}{ccc} \mathsf{Mod}_C(D,A) & \xrightarrow{\quad\rho_{int}\quad} & \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,A)) \\ \downarrow{\scriptstyle \rho_{int}} & & \downarrow{\scriptstyle \mathsf{Mod}_C(D,\rho_{int})} \\ \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,A)) & \xrightarrow{\mathsf{Mod}_C(m_D,\mathsf{Mod}_C(D,A))} & \mathsf{Mod}_C(D\otimes_C D,\mathsf{Mod}_C(D,A)) \end{array}$$

follows from the one of

$$\begin{array}{ccc} \mathsf{Mod}_C(D,A) & \xrightarrow{\quad\mathsf{Mod}_C(m_D,A)\quad} & \mathsf{Mod}_C(D\otimes_C D,A) \\ \downarrow{\scriptstyle \mathsf{Mod}_C(m_D,A)} & & \downarrow{\scriptstyle \mathsf{Mod}_C(m_D\otimes_C \mathrm{id}_D,A)} \\ \mathsf{Mod}_C(D\otimes_C D,A) & \xrightarrow{\mathsf{Mod}_C(\mathrm{id}_D\otimes_C m_D,A)} & \mathsf{Mod}_C(D\otimes_C D\otimes_C D,A). \end{array}$$

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

$$\begin{array}{ccccc} & & \overset{\mathsf{Mod}_C(m_D,A)}{\frown} & & \\ \mathsf{Mod}_C(D,A) & \xrightarrow{\rho_{int}} & \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,A)) & \xrightarrow{\sim} & \mathsf{Mod}_C(D\otimes_C D,A) \\ \downarrow{\scriptstyle \mathsf{Mod}_C(D,\varphi)} & & \downarrow{\scriptstyle \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,\varphi))} & & \downarrow{\scriptstyle \mathsf{Mod}_C(D\otimes_C D,\varphi)} \\ \mathsf{Mod}_C(D,B) & \xrightarrow{\rho_{int}} & \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,B)) & \xrightarrow{\sim} & \mathsf{Mod}_C(D\otimes_C D,B) \\ & & \underset{\mathsf{Mod}_C(m_D,B)}{\smile} & & \end{array}$$

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

Finally, if $f \in \mathsf{Mod}_C(D, A)$ is constant with respect to Ψ_{int}, then we obtain $f(d) = (\Psi_{int}(d \otimes f))(1) = \varepsilon(d)f(1)$ for all $d \in D$, i.e. $f = \rho_0(f(1))$. □

Remark 2.2.17. *With the notation of lemma 2.2.16 the diagram*

$$\begin{array}{ccccc}
\mathsf{Mod}_C(D,A) & \xrightarrow{\rho_{int}} & \mathsf{Mod}_C(D,\mathsf{Mod}_C(D,A)) & \xrightarrow{\mathsf{Mod}_C(D,\mathrm{ev}_{1_D})} & \mathsf{Mod}_C(D,A) \\
\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \mathrm{id}} \\
\mathsf{Mod}_C(D,A) & \xrightarrow{\mathsf{Mod}_C(m_D,A)} & \mathsf{Mod}_C(D\otimes_C D,A) & \xrightarrow{\mathsf{Mod}_C(\eta_D\otimes \mathrm{id}_D,A)} & \mathsf{Mod}_C(D,A)
\end{array}$$

commutes. Since the composition of the sequence at the bottom is the identity, the composition of the sequence at the top is the identity too.

The following lemma generalizes [Ume96b, Proposition 1.4] and [Mor09, Propositions 2.5 and 2.7].

Lemma 2.2.18. *If D is a C-bialgebra, A a C-algebra and $\Psi \in \mathsf{Mod}_C(D \otimes_C A, A)$ makes A into a D-module algebra, then the homomorphism of C-algebras*

$$\rho\colon A \to \mathsf{Mod}_C(D,A),$$

canonically associated to Ψ by (2.2.1), is a homomorphism from the D-module algebra (A,Ψ) to the D-module algebra $(\mathsf{Mod}_C(D,A),\Psi_{int})$, where Ψ_{int} is the D-module algebra structure on $\mathsf{Mod}_C(D,A)$ introduced in lemma 2.2.16. The homomorphism ρ is universal among all homomorphisms of D-module algebras $\Lambda\colon (A,\Psi) \to (\mathsf{Mod}_C(D,B),\Psi_{int})$, 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 $\Lambda = \mathsf{Mod}_C(D,\lambda)\circ\rho$.

Proof. By lemma 2.2.5, we have that $\mathsf{Mod}_C(D,\rho)\circ\rho$ and $\mathsf{Mod}_C(m_D,A)\circ\rho$ correspond to each other under the isomorphism (2.2.2) and since $\mathsf{Mod}_C(m_D,A)$ corresponds under the isomorphism of C-algebras (2.2.2) to the C-algebra morphism ρ_{int} associated to Ψ_{int} via the isomorphism (2.2.1), we see that ρ is in fact a D-module algebra homomorphism from (A,Ψ) to $(\mathsf{Mod}_C(D,A),\Psi_{int})$. To show the universality of ρ, let $\Lambda\colon (A,\Psi) \to (\mathsf{Mod}_C(D,B),\Psi_{int})$ be a homomorphism of D-module algebras. We define $\lambda\colon A \to B$ as $\lambda := \mathrm{ev}_{1_D}\circ\Lambda$. Then, using the fact that $\mathsf{Mod}_C(D,\Lambda)$ is a homomorphism of D-module algebras and

remark 2.2.17, we have $\mathsf{Mod}_C(D,\lambda)\circ\rho = \mathsf{Mod}_C(D,\mathrm{ev}_{1_D})\circ\mathsf{Mod}_C(D,\Lambda)\circ\rho = \mathsf{Mod}_C(D,\mathrm{ev}_{1_D})\circ\rho_{int}\circ\Lambda = \Lambda$. □

2.2.4 Commuting module algebra structures

Definition 2.2.19. *Let D and D' be C-bialgebras and A a be C-algebra. If $\Psi \in \mathsf{Mod}_C(D\otimes_C A, A)$ and $\Psi' \in \mathsf{Mod}_C(D'\otimes_C A, A)$ are D and D'-module algebra structures on A, respectively, we say that these structures* commute *if the diagram*

$$\begin{array}{ccccc} D\otimes_C D'\otimes_C A & \xrightarrow{\mathrm{id}_D\otimes_C\Psi'} & D\otimes_C A & & \\ \downarrow{\scriptstyle \tau\otimes_C\mathrm{id}_A} & & & \searrow^{\Psi} & \\ D'\otimes_C D\otimes_C A & \xrightarrow{\mathrm{id}_{D'}\otimes_C\Psi} & D'\otimes_C A & \xrightarrow{\Psi'} & A \end{array}$$

commutes, where $\tau\colon D\otimes_C D' \to D'\otimes_C D$ denotes the twist homomorphism defined by $\tau(d\otimes d') = d'\otimes d$ for all $d\in D$ and $d'\in D'$.

Remark 2.2.20. *Let D and D' be C-bialgebras and A a C-algebra. If $\Psi \in \mathsf{Mod}_C(D\otimes_C A, A)$ and $\Psi' \in \mathsf{Mod}_C(D'\otimes_C A, A)$ are D and D'-module algebra structures on A with associated homomorphisms ρ and ρ', respectively, then they commute if and only if the diagram*

$$\begin{array}{ccccc} & & \mathsf{Mod}_C(D,A) & \xrightarrow{\mathsf{Mod}_C(D,\rho')} & \mathsf{Mod}_C(D,\mathsf{Mod}_C(D',A)) \xrightarrow{\sim} \mathsf{Mod}_C(D'\otimes_C D,A) \\ & \overset{\rho}{\nearrow} & & & \downarrow{\scriptstyle \mathsf{Mod}_C(\tau,A)} \\ A & & & & \\ & \underset{\rho'}{\searrow} & & & \\ & & \mathsf{Mod}_C(D',A) & \xrightarrow{\mathsf{Mod}_C(D',\rho)} & \mathsf{Mod}_C(D',\mathsf{Mod}_C(D,A)) \xrightarrow{\sim} \mathsf{Mod}_C(D\otimes_C D',A) \end{array}$$

commutes, where $\tau\colon D\otimes_C D' \to D'\otimes_C D$ is the twist homomorphism defined by $\tau(d\otimes d') = d'\otimes d$ for all $d\in D$ and $d'\in D'$.

Lemma 2.2.21. *Let D_1 and D_2 be C-bialgebras and A be a C-algebra.*

(1) *If* $\Psi_1 \in \mathsf{Mod}_C(D_1 \otimes_C A, A)$ *and* $\Psi_2 \in \mathsf{Mod}_C(D_2 \otimes_C A, A)$ *are commuting* D_1*- and* D_2*-module algebra structures on* A*, respectively, then there is a canonical* $D_1 \otimes_C D_2$*-module algebra structure*

$$\Psi \colon D_1 \otimes_C D_2 \otimes_C A \to A$$

on A*, defined by*

$$\Psi := \Psi_1 \circ (\mathrm{id}_{D_1} \otimes_C \Psi_2) = \Psi_2 \circ (\mathrm{id}_{D_2} \otimes_C \Psi_1) \circ (\tau \otimes_C \mathrm{id}_A). \tag{2.2.5}$$

(2) *Conversely, a* $D_1 \otimes_C D_2$*-module algebra structure* Ψ *on* A *induces commuting* D_1*- and* D_2*-module algebra structures*

$$\Psi_1 \colon D_1 \otimes_C A \to A \quad \textit{and} \quad \Psi_2 \colon D_2 \otimes_C A \to A$$

on A*, defined by*

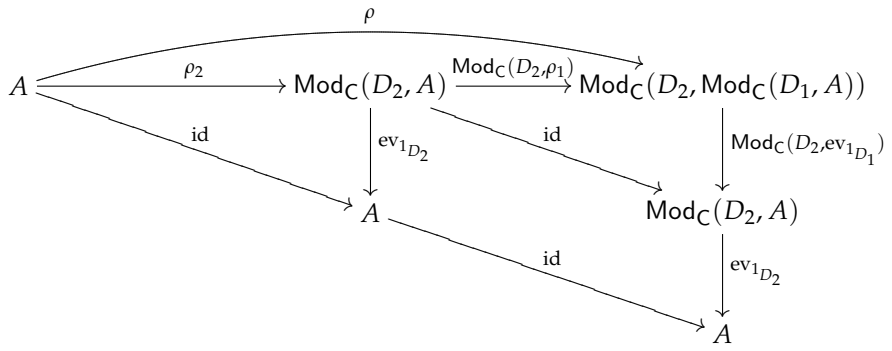
$$\Psi_1(d_1 \otimes a) := \Psi(d_1 \otimes 1 \otimes a) \quad \textit{and} \quad \Psi_2(d_2 \otimes a) := \Psi(1 \otimes d_2 \otimes a),$$

respectively, for $d_1 \in D_1$*,* $d_2 \in D_2$ *and* $a \in A$*.*

Proof. To prove (1), let $\rho_i \colon A \to \mathsf{Mod}_C(D_i, A)$ be the homomorphisms associated to Ψ_i for $i = 1, 2$ and let $\rho \colon A \to \mathsf{Mod}_C(D_1 \otimes_C D_2, A)$ be the homomorphism associated to the homomorphism Ψ defined in (2.2.5) via the isomorphism (2.2.1). We note that ρ is given as the composition

$$A \xrightarrow{\rho_2} \mathsf{Mod}_C(D_2, A) \xrightarrow{\mathsf{Mod}_C(D_2, \rho_1)} \mathsf{Mod}_C(D_2, \mathsf{Mod}_C(D_1, A)) \xrightarrow{\sim} \mathsf{Mod}_C(D_1 \otimes_C D_2, A)$$

and thus is a homomorphism of C-algebras. Since Ψ_1 and Ψ_2 are D_1- and D_2-module algebra structures, respectively, the two small triangles in the diagram



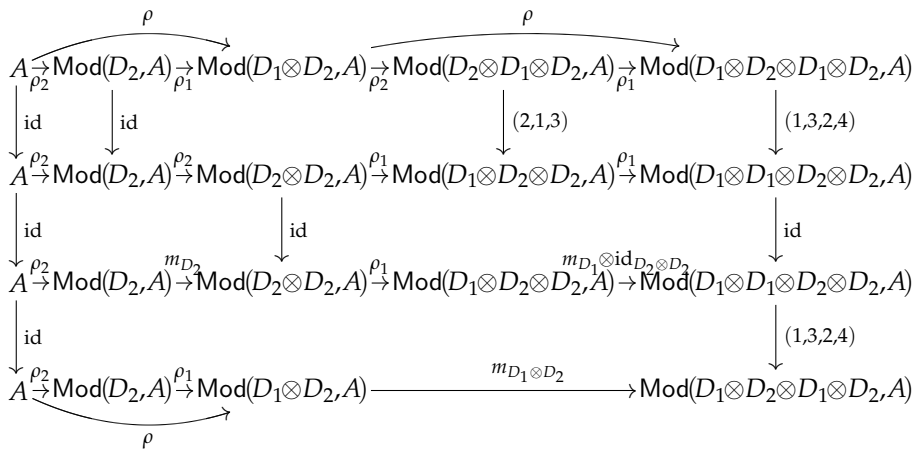
(2.2.6)

commute and thus the big triangle commutes too. In the following diagram we abbreviate the homomorphism

$$\mathsf{Mod}_{\mathsf{C}}(M, \rho_i) \colon \mathsf{Mod}_{\mathsf{C}}(M, A) \to \mathsf{Mod}_{\mathsf{C}}(M, \mathsf{Mod}_{\mathsf{C}}(D, A))$$

as ρ_i for any C-module M and for $i = 1, 2$. For any homomorphism $\varphi \colon M \to N$ of C-modules we abbreviate the homomorphism $\mathsf{Mod}_{\mathsf{C}}(\varphi, A) \colon \mathsf{Mod}_{\mathsf{C}}(N, A) \to \mathsf{Mod}_{\mathsf{C}}(M, A)$ as φ. We also implicitely use the isomorphism (2.2.2). All tensor

products are over C and we write Mod instead of Mod_C.



The rectangle at the top center commutes since Ψ_1 and Ψ_2 commute. The two rectangles in the middle row commute since Ψ_1 and Ψ_2 are D_1- and D_2-module algebra structures on A, respectively, and the rectangle at the bottom row trivially commutes too. Therefore, the big rectangle commutes and together with the commutativity of the big triangle in (2.2.6) and the fact that ρ is a homomorphism of C-algebras we obtain by corollary 2.2.6 that Ψ is a D-module algebra structure on A.

To prove part (2), we denote by ρ the homomorphism of C-algebras $A \to \mathsf{Mod}_C(D, A)$ associated to Ψ via the isomorphism (2.2.1). We define homomorphisms $\rho_1 \colon A \to \mathsf{Mod}_C(D_1, A)$ and $\rho_2 \colon A \to \mathsf{Mod}_C(D_2, A)$ as the compositions

$$\rho_1 \colon A \xrightarrow{\ \rho\ } \mathsf{Mod}_C(D_1 \otimes_C D_2, A) \xrightarrow{\mathsf{Mod}_C(\mathrm{id}_{D_1} \otimes_C \eta_{D_2}, A)} \mathsf{Mod}_C(D_1, A)$$

and

$$\rho_2 \colon A \xrightarrow{\ \rho\ } \mathsf{Mod}_C(D_1 \otimes_C D_2, A) \xrightarrow{\mathsf{Mod}_C(\eta_{D_1} \otimes_C \mathrm{id}_{D_2}, A)} \mathsf{Mod}_C(D_2, A),$$

respectively. Since $\eta_{D_1} \otimes_C \mathrm{id}_{D_2} \colon D_2 \to D_1 \otimes_C D_2$ and $\mathrm{id}_{D_1} \otimes_C \eta_{D_2} \colon D_1 \to D_1 \otimes_C D_2$ are homomorphisms of C-coalgebras, we see that ρ_1 and ρ_2 are in

fact homomorphisms of C-algebras. For all $d, d' \in D_1$ we have $\Psi_1(d \otimes \Psi_1(d' \otimes a)) = \Psi(d \otimes 1_{D_2} \otimes \Psi(d' \otimes 1_{D_2} \otimes a)) = \Psi(dd' \otimes 1_{D_2} \otimes a) = \Psi_1(dd' \otimes a)$ and $\Psi_1(1_{D_1} \otimes a) = \Psi(1_{D_1} \otimes 1_{D_2} \otimes a) = a$. Thus, Ψ_1 makes A into a D_1-module and so Ψ_1 is a D_1-module algebra structure on A. Analogously, one sees that Ψ_2 gives rise to a D_2-module algebra structure on A. Since Ψ is a $(D_1 \otimes_C D_2)$-module algebra structure on A, we have

$$\begin{aligned}\Psi_1(d_1 \otimes \Psi_2(d_2 \otimes a)) &= \Psi((d_1 \otimes 1) \otimes \Psi((1 \otimes d_2) \otimes a)) \\ &= \Psi((d_1 \otimes d_2) \otimes a) \\ &= \Psi((1 \otimes d_2) \otimes \Psi((d_1 \otimes 1) \otimes a)) \\ &= \Psi_2(d_2 \otimes \Psi_1(d_1 \otimes a))\end{aligned}$$

for all $d_1 \in D_1, d_2 \in D_2$ and $a \in A$, i.e. Ψ_1 and Ψ_2 commute. □

Lemma 2.2.22. *Let D and D' be two C-bialgebras, A a C-algebra and $\Psi' \in \mathsf{Mod}_C(D' \otimes_C A, A)$ be a D'-module algebra structure on A. Then $\mathsf{Mod}_C(D, A)$ carries a natural D'-module algebra structure defined by*[2]

$$\begin{aligned}D' \otimes_C \mathsf{Mod}_C(D, A) &\to \mathsf{Mod}_C(D, A) \\ d' \otimes f &\mapsto (d \mapsto \Psi'(d' \otimes f(d)))\end{aligned} \tag{2.2.7}$$

for all $d' \in D'$ and all $f \in \mathsf{Mod}_C(D, A)$.

Proof. If we denote by $\rho' \colon A \to \mathsf{Mod}_C(D', A)$ the homomorphism of C-algebras corresponding to Ψ', then the homomorphism corresponding to (2.2.7) via the isomorphism (2.2.1) is the composition

$$\mathsf{Mod}_C(D,A) \xrightarrow{\mathsf{Mod}_C(D,\rho')} \mathsf{Mod}_C(D, \mathsf{Mod}_C(D',A)) \xrightarrow{\sim} \mathsf{Mod}_C(D', \mathsf{Mod}_C(D,A)),$$

[2] In the case $D = D'$ this D-module algebra structure must not be confused with the one defined in lemma 2.2.16.

which clearly is a homomorphism of C-algebras. Using implicitly the last isomorphism, $\mathsf{Mod}_C(D, \rho')$ makes the diagrams

$$\begin{array}{ccc} \mathsf{Mod}_C(D,A) & \xrightarrow{\mathsf{Mod}_C(D,\rho')} & \mathsf{Mod}_C(D', \mathsf{Mod}_C(D,A)) \\ & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{ev}_{1_{D'}}} \\ & & \mathsf{Mod}_C(D,A) \end{array}$$

and

$$\begin{array}{ccc} \mathsf{Mod}_C(D,A) & \xrightarrow{\mathsf{Mod}_C(D,\rho')} & \mathsf{Mod}_C(D', \mathsf{Mod}_C(D,A)) \\ \downarrow{\scriptstyle \mathsf{Mod}_C(D,\rho')} & & \downarrow{\scriptstyle \mathsf{Mod}_C(D',\mathsf{Mod}_C(D,\rho'))} \\ \mathsf{Mod}_C(D', \mathsf{Mod}_C(D,A)) & \xrightarrow{\mathsf{Mod}_C(m_{D'},\mathsf{Mod}_C(D,A))} & \mathsf{Mod}_C(D' \otimes_C D', \mathsf{Mod}_C(D,A)) \end{array}$$

commutative. Thus, (2.2.7) defines in fact a D'-module algebra structure on $\mathsf{Mod}_C(D, A)$. □

Lemma 2.2.23. *Let D and D' be C-bialgebras, A a C-algebra and let $\Psi' \in \mathsf{Mod}_C(D' \otimes_C A, A)$ be a D'-module algebra structure on A. Then the D-module algebra structure Ψ_{int} on $\mathsf{Mod}_C(D, A)$ defined in lemma 2.2.16 and the D'-module algebra structure induced by Ψ' on $\mathsf{Mod}_C(D, A)$ via lemma 2.2.22 commute, i.e. the diagram*[3]

$$\begin{array}{ccccc} D \otimes_C D' \otimes_C \mathsf{Mod}_C(D,A) & \xrightarrow{\mathrm{id}_D \otimes_C \Psi'} & D \otimes_C \mathsf{Mod}_C(D,A) & & \\ & & & \searrow^{\Psi_{int}} & \\ \downarrow{\scriptstyle \tau \otimes_C \mathrm{id}} & & & & \mathsf{Mod}_C(D,A) \\ & & & \nearrow_{\Psi'} & \\ D' \otimes_C D \otimes_C \mathsf{Mod}_C(D,A) & \xrightarrow{\mathrm{id}_{D'} \otimes_C \Psi_{int}} & D' \otimes_C \mathsf{Mod}_C(D,A) & & \end{array}$$

commutes, where $\tau\colon D \otimes_C D' \to D' \otimes_C D$ denotes the twist map, defined by $\tau(d \otimes d') := d' \otimes d$ for all $d \in D$ and all $d' \in D'$.

[3] By abuse of notation we denote the induced D'-module algebra structure on $\mathsf{Mod}_C(D, A)$, introduced in lemma 2.2.22, again by Ψ'.

Proof. The claim follows from

$$(d(d'.f))(c) = (d'.f)(cd) = d'(f(cd)) = d'((d.f)(c)) = (d'(d.f))(c)$$

for all $c, d \in D$, $d' \in D'$ and $f \in \mathsf{Mod}_{\mathsf{C}}(D, A)$. □

Lemma 2.2.24. *Let D and D' be two C-bialgebras and A be a D'-module algebra via $\Psi' \in \mathsf{Mod}_{\mathsf{C}}(D' \otimes_C A, A)$, then the homomorphism $\rho_0 \colon A \to \mathsf{Mod}_{\mathsf{C}}(D, A)$ associated to the trivial D-module algebra structure Ψ_0 on A (see lemma 2.2.15) is a D'-module algebra homomorphism, where we equip $\mathsf{Mod}_{\mathsf{C}}(D, A)$ with the D'-module algebra structure induced by Ψ' via lemma 2.2.22. In particular, $\rho_0(A)$ is a D'-module subalgebra of $\mathsf{Mod}_{\mathsf{C}}(D, A)$.*

Proof. For all $a \in A$, $d \in D$ and $d' \in D'$ we have

$$(d'.\rho_0(a))(d) = d'(\rho_0(a)(d)) = d'(\varepsilon_D(d)a) = \varepsilon_D(d)d'(a) = (\rho_0(d'.a))(d).$$

□

2.2.5 Extensions of module algebra structures

Proposition 2.2.25. *Let D be a cocommutative C-bialgebra. If*

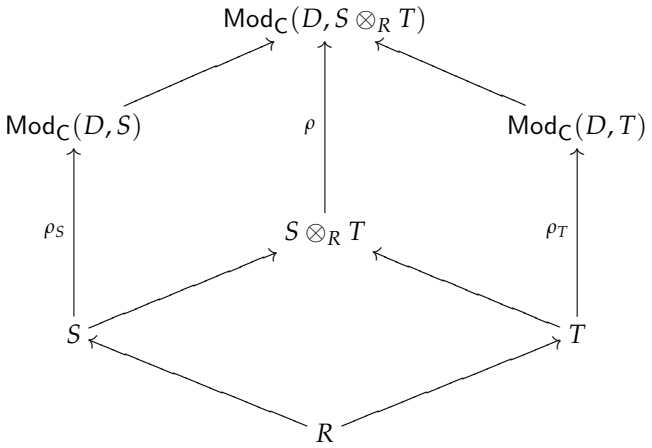
$$(S, \Psi_S) \leftarrow (R, \Psi_R) \rightarrow (T, \Psi_T)$$

is a diagram in the category of commutative D-module algebras, then $S \otimes_R T$ carries a unique D-module algebra structure such that $S \otimes_R T$ becomes the coproduct of (S, Ψ_S) with (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

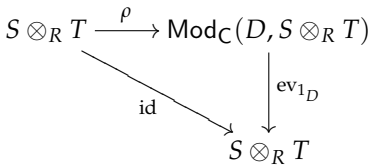
$$\Psi \colon D \otimes_C S \otimes_R T \to S \otimes_R T, \qquad d \otimes s \otimes t \mapsto \sum_{(d)} \Psi_S(d_{(1)} \otimes s) \otimes \Psi_T(d_{(2)} \otimes t). \tag{2.2.8}$$

If ρ_S and ρ_T are the homomorphisms corresponding to Ψ_S and Ψ_T under the isomorphism (2.2.1)*, respectively, then Ψ corresponds to $\rho_S \otimes \rho_T$ under this isomorphism when we identify $\mathsf{Mod}_{\mathsf{C}}(D, S) \otimes_{\mathsf{Mod}_{\mathsf{C}}(D,R)} \mathsf{Mod}_{\mathsf{C}}(D, T)$ with $\mathsf{Mod}_{\mathsf{C}}(D, S \otimes_R T)$.*

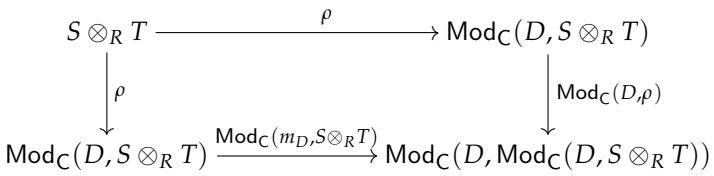
Proof. Since D is cocommutative and R, S and T are commutative C-algebras, the C-algebras $\mathsf{Mod}_{\mathsf{C}}(D,R)$, $\mathsf{Mod}_{\mathsf{C}}(D,S)$ and $\mathsf{Mod}_{\mathsf{C}}(D,T)$ are commutative. We denote the C-algebra homomorphisms corresponding to the D-module algebra structures on R, S and T by ρ_R, ρ_S and ρ_T, respectively. By the universal property of the tensor product $S \otimes_R T$ in the category of commutative C-algebras, there exists a unique homomorphism $\rho\colon S \otimes_R T \to \mathsf{Mod}_{\mathsf{C}}(D, S \otimes_R T)$ of C-algebras that makes the diagram



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



and



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

For any D-module algebra structure Ψ on $S \otimes_R T$ such that $S \to S \otimes_R T, s \mapsto s \otimes 1$ and $T \to S \otimes_R T, t \mapsto 1 \otimes t$ are homomorphisms of D-module algebras, we have $\Psi(d \otimes s \otimes 1) = \Psi_S(d \otimes s) \otimes 1$ and $\Psi(d \otimes 1 \otimes t) = 1 \otimes \Psi_T(d \otimes t)$. Since Ψ measures $S \otimes_R T$ to itself, it follows $\Psi(d \otimes s \otimes t) = \sum_{(d)} \Psi_S(d_{(1)} \otimes s) \otimes \Psi_T(d_{(2)} \otimes t)$. Therefore, (2.2.8) is the unique D-module algebra structure on $S \otimes_R T$ such that $S \to S \otimes_R T$ and $T \to S \otimes_R T$ are D-module algebra homomorphisms. □

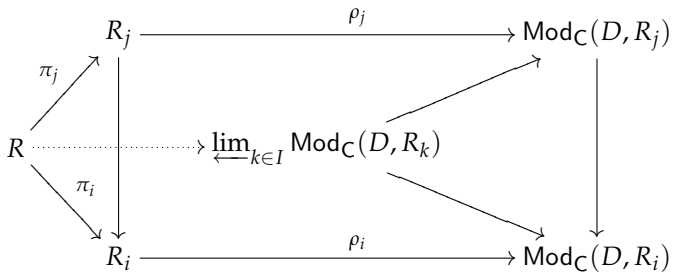
Proposition 2.2.26. *Let D be a cocommutative C-bialgebra and $(R_i, \Psi_i)_{i \in I}$ be an inverse system of commutative C-algebras that are measured by D into themselves such that the homomorphism between the R_i are compatible with the measurings.*

(1) Then D measures the inverse limit $R := \varprojlim_{i \in I} R_i$ (in the category of commutative C-algebras) to itself such that the projections $\pi_i \colon R \to R_i$ are compatible with the measurings.

(2) If in addition all (R_i, Ψ_i) are D-module algebras, then R is also a D-module algebra, the projections $\pi_i \colon R \to R_i$ are homomorphisms of D-module algebras and R is the inverse limit of $(R_i, \Psi_i)_{i \in I}$ in the category of commutative D-module algebras.

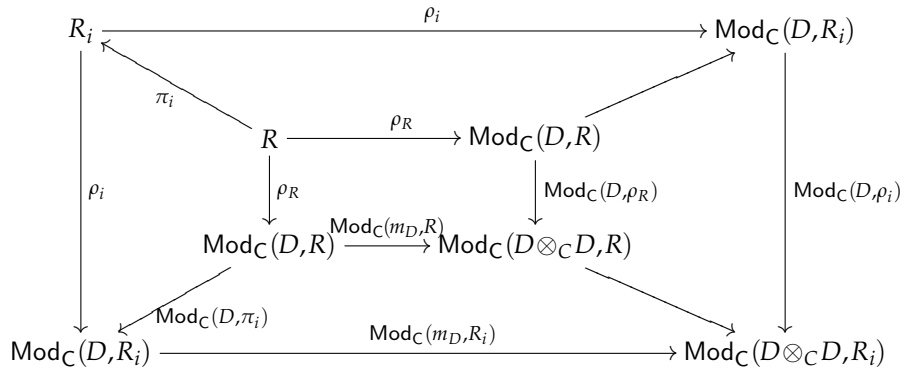
Proof. We denote by $\rho_i \colon R_i \to \mathsf{Mod}_C(D, R_i)$ the homomorphism of C-algebras associated to $\Psi_i \colon D \otimes_C R_i \to R_i$. By the universal property of the inverse limit $\varprojlim_{k \in I} \mathsf{Mod}_C(D, R_k)$ there exists a unique homomorphism of C-algebras

$R \to \varprojlim_{k\in I} \mathsf{Mod}_C(D, R_k)$ such that the diagram



commutes for all $j \to i$. Since $\mathsf{Mod}_C(D, \cdot)$ preserves inverse limits of C-modules, we have an isomorphism of C-modules $\varprojlim_{k\in I} \mathsf{Mod}_C(D, R_k) \cong \mathsf{Mod}_C(D, R)$. This is in fact a homomorphism of C-algebras. Thus, we obtain a homomorphism $\rho_R \colon R \to \mathsf{Mod}_C(D, R)$ of C-algebras, i.e. D measures R to itself.

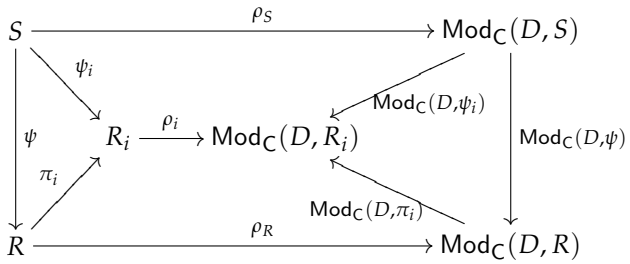
If in addition Ψ_i is a D-module algebra structure on R_i for all $i \in I$, then the outer rectangle in the diagram



commutes for all $i \in I$. The trapezoids commute, since the projections $\pi_i \colon R \to R_i$ are compatible with the measurings. Thus, by the universal property of $\varprojlim_{i\in I} \mathsf{Mod}_C(D \otimes_C D, R_i)$, the inner rectangle also commutes and we see that R is a D-module algebra.

If $\psi_i \colon S \to R_i$ are compatible homomorphisms of D-module algebras, then, by the universal property of $R = \varprojlim_{i\in I} R_i$ in the category of commutative

C-algebras, there exists a homomorphism of C-algebras $\psi\colon S \to R$ such the triangles at the left in the diagrams



commute for all $i \in I$. Thus, the triangle at the right commutes too and the two trapezoids at the top and bottom commute by assumption and by the first part, respectively. By the universal property of $\mathsf{Mod}_C(D, R) = \varprojlim_{i\in I} \mathsf{Mod}_C(D, R_i)$ we obtain $\mathsf{Mod}_C(D, \psi) \circ \rho_S = \rho_R \circ \psi$, i.e. ψ is a homomorphism of D-module algebras. □

Corollary 2.2.27. *Let D be a cocommutative C-bialgebra, I and J be two small categories and F and G be two diagrams in the category of commutative D-module algebras of type I and J, respectively. If $\varphi\colon I \to J$ is a functor from I to J, then every natural transformation from $G \circ \varphi$ to F induces a homomorphism of D-module algebras from the limit of G to the limit of F in the category of commutative D-module algebras.*

2.2.6 Simple module algebras

Definition 2.2.28. *Let D be a C-bialgebra and R be a commutative D-module algebra. Then R is* simple *(as D-module algebra) if (0) and R are its only D-stable ideals.*

We recall the definition of the smash product (cf. [Swe69, Section 7.2])

Definition 2.2.29. *Let D be a C-bialgebra and R be a commutative D-module algebra. We define the* smash product *of R with D, denoted by $R\#_C D$ (or $R\#D$ if there is*

no danger of confusion), as the C-algebra with underlying C-module $R \otimes_C D$, whose elements $a \otimes d$ will be denoted by $a\#d$, and with multiplication given by

$$(a\#c)(b\#d) := \sum_{(c)} a(c_{(1)}b)\#c_{(2)}d$$

for all $a\#c, b\#d \in R\#_C D$ and with unit $1\#1$.

Proposition 2.2.30. *Let D be a commutative C-bialgebra and (R, Ψ_R) be a simple commutative D-module algebra. Then for every $R\#D$-module Y the homomorphism*

$$R \otimes_{R^{\Psi_R}} Y^{\Psi_Y} \to Y, \quad r \otimes y \to ry$$

is injective, where $\Psi_Y \colon D \otimes Y \to Y$ is the D-module structure on Y induced from the $R\#D$-module structure on Y by $\Psi_Y(d \otimes y) := (1\#d)y$.

Proof. See [AM05, Corollary 3.2] or [Ama05, Corollary 3.1.4]. □

Corollary 2.2.31. *If D is a cocommutative C-bialgebra, (R, Ψ_R) a simple commutative D-module algebra and (S, Ψ_S) a commutative D-module algebra extension of (R, Ψ_R), then R and S^{Ψ_S} are linearly disjoint over R^{Ψ_R} and we obtain an injective homomorphism of D-module algebras*

$$R \otimes_{R^{\Psi_R}} S^{\Psi_S} \to S,$$

induced by the multiplication homomorphism in S.

Lemma 2.2.32. *Let D be a C-bialgebra, and (R, Ψ_R) a commutative D-module algebra. Then $\mathsf{Mod}_C(D, R)$ is an $R\#_C D$-module with scalar multiplication*

$$R\#_C D \times \mathsf{Mod}_C(D, R) \to \mathsf{Mod}_C(D, R), \quad (a\#d, f) \mapsto \rho(a) \cdot \Psi_{int}(d \otimes f) \quad (2.2.9)$$

Proof. Obviously (2.2.9) is linear in both arguments. It is also associative, since for $a\#c, b\#d \in R\#_C D$ and $f \in \mathsf{Mod}_{\mathsf{C}}(D, R)$ we have

$$\begin{aligned}((a\#c)(b\#d))f &= \left(\sum_{(c)} ac_{(1)}(b)\#c_{(2)}d\right) f \\ &= \sum_{(c)} \rho(a \cdot c_{(1)}(b)) \cdot (c_{(2)}d)(f) \\ &= \rho(a) \cdot \sum_{(c)} c_{(1)}(\rho(b)) \cdot c_{(2)}(d(f)) \\ &= \rho(a) \cdot c(\rho(b) \cdot d(f)) \\ &= (a\#c)(\rho(b) \cdot d(f)) \\ &= (a\#c)((b\#d)f)\end{aligned}$$

□

Proposition 2.2.33. *Let D be a cocommutative C-bialgebra such that D is free as C-module and (R, Ψ) be a commutative D-module algebra. Then for $a_1, \ldots, a_n \in R$ the following are equivalent:*

(1) $a_1, \ldots, a_n$ are linearly independent over R^{Ψ},

(2) $\rho(a_1), \ldots, \rho(a_n)$ are linearly independent over R, where we consider $\mathsf{Mod}_{\mathsf{C}}(D, R)$ as R-module via the map

$$R \times \mathsf{Mod}_{\mathsf{C}}(D, R) \to \mathsf{Mod}_{\mathsf{C}}(D, R), \quad (a, f) \mapsto \rho_0(a) \cdot f.$$

If R is a field, this is further equivalent to

(3) there exist $d_1, \ldots, d_n \in D$ such that $(d_j(a_i))_{i,j=1}^n \in \mathrm{GL}_n(R)$

Proof. To show that (1) implies (2), we note that by lemma 2.2.32 $\mathsf{Mod}_{\mathsf{C}}(D, R)$ is a $(R\#D)$-module via $(a\#d)f = \rho(a) \cdot \Psi_{int}(d \otimes f)$. By proposition 2.2.30, the

homomorphism

$$R \otimes_{R^\Psi} \mathsf{Mod}_\mathsf{C}(D,R)^{\Psi_{int}} \to \mathsf{Mod}_\mathsf{C}(D,R) \tag{2.2.10}$$

is injective. Let $a_1,\dots,a_n \in R$ be linearly independent over R^Ψ and suppose that there are $b_1,\dots,b_n \in R$, not all equal to zero, such that $\sum_{i=1}^n \rho_0(b_i)\rho(a_i) = 0$. Since $\sum_{i=1}^n \rho_0(b_i)\rho(a_i)$ is the image of the non-zero element $\sum_{i=1}^n a_i \otimes \rho_0(b_i) \in R \otimes_{R^\Psi} \mathsf{Mod}_\mathsf{C}(D,R)$ under the injective homomorphism (2.2.10), this is not possible.

If $\rho(a_1),\dots,\rho(a_n)$ are linearly independent over R and there are $c_1,\dots,c_n \in R^\Psi$ such that $\sum_{i=1}^n c_i a_i = 0$, then it follows $\sum_{i=1}^n \rho_0(c_i)\rho(a_i) = 0$ and thus $c_i = 0$ for all $i = 1,\dots,n$. Thus, (2) implies (1).

If R is a field, the equivalence of (1) and (3) is proven in [Ama05, Proposition 3.1.6]. □

Definition 2.2.34. *Let D be a C-bialgebra and R be a commutative D-module algebra. Then R is* Artinian simple *(or* AS*) if R is simple as D-module algebra and Artinian as a ring.*

Definition 2.2.35. *Let D be a C-bialgebra and S/R be an extension of commutative Artinian simple D-module algebras.*

(1) If B is a subset of S, we denote by $R\langle B\rangle$ the smallest Artinian simple D-module subalgebra of S containing R and B.

(2) We say that S is finitely generated *over R as Artinian simple D-module algebra if there exists a finite subset B of S such that $S = R\langle B\rangle$.*

2.3 Examples

We close this chapter with a list of examples of bialgebras, which illustrate the introduced concepts. The cocommutative ones serve as a pool giving rise to particular instances of our Galois theory (see chapter 3).

2.3.1 Endomorphisms

Endomorphisms on algebras can be considered as module algebra structures for the bialgebra generated as algebra by one groupe-like element. This appeared already in [Swe69, Section 7.0, Example a) on page 139].

Proposition 2.3.1. *(1) The polynomial algebra $C[t]$ over C becomes a C-bialgebra with the usual C-algebra structure and with comultiplication*

$$\Delta\colon C[t] \to C[t] \otimes_C C[t], \quad \Delta(t) \coloneqq t \otimes t$$

and a counit

$$\varepsilon\colon C[t] \to C, \quad \varepsilon(t) \coloneqq 1.$$

We denote this C-bialgebra by D_{end}.

(2) For every C-algebra A there is a bijection between the set $\mathsf{Alg}_C(A, A)$ of endomorphisms of the C-algebra A and the set of D_{end}-module algebra structures on A.

Proof. The assertion of the first part is easy to verify. The bijection in the second part is given as follows: If $\sigma \in \mathsf{Alg}_C(A, A)$ we define a homomorphism of C-modules $\Psi_\sigma\colon D_{end} \otimes_C A \to A$ by $\Psi_\sigma(t^n \otimes a) \coloneqq \sigma^n(a)$ for all $n \in \mathbb{N}$ and all $a \in A$. Since $\Psi_\sigma(t^n \otimes ab) = \sigma^n(ab) = \sigma^n(a)\sigma^n(b) = \sum_{(t^n)} \Psi_\sigma((t^n)_1 \otimes a)\Psi_\sigma((t^n)_2 \otimes b)$ for all $a, b \in A$ and $n \in \mathbb{N}$, the homomorphism of C-modules Ψ_σ defines in fact a D_{end}-module algebra structure on A. Conversely, for a D_{end}-module algebra structure $\Psi\colon D_{end} \otimes_C A \to A$ on A we define $\sigma_\Psi\colon A \to A$ by $\sigma_\Psi(a) \coloneqq \Psi(t \otimes a)$ for all $a \in A$. From $\sigma_\Psi(ab) = \Psi(t \otimes ab) = \Psi(t \otimes a)\Psi(t \otimes b) = \sigma_\Psi(a)\sigma_\Psi(b)$ we see that σ_Ψ is an endomorphism of the C-algebra A. The maps defined by these assignments give rise to the desired bijection. □

We note that for any C-algebra A the set $A^{\mathbb{N}}$ of maps from $\mathbb{N}$ to A becomes a C-algebra with componentwise addition and multiplication and that there exists a natural endomorphism Σ of $A^{\mathbb{N}}$ defined by

$$(\Sigma(f))(n) = f(n+1) \tag{2.3.1}$$

for all $f \in A^{\mathbb{N}}$ and all $n \in \mathbb{N}$. By proposition 2.3.1, the D_{end}-module algebra structure Ψ_{int} on $\mathsf{Mod}_C(D_{end}, A)$ defined in lemma 2.2.16 gives rise to a C-algebra endomorphism ϕ of $\mathsf{Mod}_C(D_{end}, A)$ which is given by $(\phi(f))(t^n) = f(t^{n+1})$ for $f \in \mathsf{Mod}_C(D_{end}, A)$ and $n \in \mathbb{N}$ when we identify D_{end} with $C[t]$ as in proposition 2.3.1. It is easily seen that there is an isomorphism of C-algebras $\mathsf{Mod}_C(D_{end}, A) \to A^{\mathbb{N}}$ given by sending $f \in \mathsf{Mod}_C(D_{end}, A)$ to $(n \mapsto f(t^n)) \in A^{\mathbb{N}}$. This isomorphism is in fact an isomorphism of difference rings[4], i.e. the diagram

$$\begin{array}{ccc} \mathsf{Mod}_C(D_{end}, A) & \xrightarrow{\sim} & A^{\mathbb{N}} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Sigma} \\ \mathsf{Mod}_C(D_{end}, A) & \xrightarrow{\sim} & A^{\mathbb{N}} \end{array}$$

commutes. From proposition 2.3.1 together with lemma 2.2.18 we obtain for any endomorphism σ of A a homomorphism of D_{end}-module algebras $\rho\colon A \to \mathsf{Mod}_C(D_{end}, A)$. The composition $A \xrightarrow{\rho} \mathsf{Mod}_C(D_{end}, A) \xrightarrow{\sim} A^{\mathbb{N}}$ is the so called *universal Euler homomorphism*, defined by $a \mapsto (n \mapsto \sigma^n(a))$, that S. Morikawa and H. Umemura use in their general difference Galois theory ([Mor09], [MU09]).

2.3.2 Automorphisms

Automorphisms can be described as module algebra structures in a similar way as endomorphisms. We replace the bialgebra $D_{end} = C[t]$ by the localization $C[t, t^{-1}]$ where t is still a group-like element (and thus t^{-1} is group-like too).

Proposition 2.3.2. *We denote by D_{aut} the C-bialgebra underlying the Hopf algebra structure on the coordinate ring $C[\mathbb{G}_m]$ of the multiplicative group scheme $\mathbb{G}_m$ over C (see for example [Wat79, Section 1.4]). For every C-algebra A there is a bijection*

[4] A difference ring is defined as a pair consisting of a ring and an endomorphism of this ring. Morphisms between difference rings are homomorphisms between rings that commute with the endomorphisms on them.

between the set of C-algebra automorphisms of A and the set of D_{aut}-module algebra structures on A.

Proof. We recall that the C-bialgebra structure on $D_{aut} = C[\mathbb{G}_m] \cong C[t, t^{-1}]$ is given by the usual C-algebra structure on $C[t, t^{-1}]$ and the C-coalgebra structure defined by $\Delta(t) := t \otimes t$ and $\varepsilon(t) := 1$. If σ is an automorphism of the C-algebra A, we define a homomorphism of C-modules $\Psi_\sigma \colon D_{aut} \otimes_C A \to A$ by $\Psi(t^n \otimes a) := \sigma^n(a)$ for all $n \in \mathbb{Z}$ and all $a \in A$. As in the proof of proposition 2.3.1 we see that Ψ_σ defines a D_{aut}-module algebra structure on A. Conversely, for a D_{aut}-module algebra structure $\Psi \colon D_{aut} \otimes_C A \to A$ on A we define $\sigma_\Psi \colon A \to A$ by $\sigma_\Psi(a) := \Psi(t \otimes a)$ for all $a \in A$. Then σ_Ψ is an automorphism of the C-algebra A with inverse given by $\sigma_\Psi^{-1}(a) = \Psi(t^{-1} \otimes a)$ for all $a \in A$. The maps defined by these assignments give rise to the desired bijection. □

For any C-algebra A, the set $A^{\mathbb{Z}}$ becomes a C-algebra with componentwise addition and multiplication and there exists a natural automorphism Σ of $A^{\mathbb{Z}}$ defined by $(\Sigma(f))(n) = f(n+1)$ for all $f \in A^{\mathbb{Z}}$ and all $n \in \mathbb{Z}$. By proposition 2.3.2, the D_{aut}-module algebra structure Ψ_{int} on $\mathsf{Mod}_C(D_{aut}, A)$ gives rise to an automorphism ϕ on the C-algebra $\mathsf{Mod}_C(D_{aut}, A)$ given by $(\phi(f))(t^n) = f(t^{n+1})$ for all $f \in \mathsf{Mod}_C(D_{aut}, A)$ and all $n \in \mathbb{Z}$ when we identify D_{aut} with $C[t, t^{-1}]$ as in proposition 2.3.2. There is an isomorphism of C-algebras with automorphism $(\mathsf{Mod}_C(D_{aut}, A), \phi) \to (A^{\mathbb{Z}}, \Sigma)$ given by sending an $f \in \mathsf{Mod}_C(D_{aut}, A)$ to $(n \mapsto f(t^n)) \in A^{\mathbb{Z}}$. By proposition 2.3.2 together with lemma 2.2.18, we obtain for any automorphism σ of a C-algebra A a homomorphism of D_{aut}-module algebras $\rho \colon A \to \mathsf{Mod}_C(D_{aut}, A)$. The composition $A \xrightarrow{\rho} \mathsf{Mod}_C(D_{aut}, A) \xrightarrow{\sim} A^{\mathbb{Z}}$ sends an element $a \in A$ to the map from $\mathbb{Z}$ to A that sends $n \in \mathbb{Z}$ to $\sigma^n(a)$.

2.3.3 Groups acting as algebra endomorphisms

Proposition 2.3.3. *Let G be a group.*

(1) *The group algebra CG over C becomes a cocommutative bialgebra with comultiplication $\Delta\colon CG \to CG \otimes_C CG$ and counit $\varepsilon\colon CG \to C$ given as the C-module homomorphisms defined by*

$$\Delta(g) \coloneqq g \otimes g \quad \textit{and} \quad \varepsilon(g) \coloneqq 1$$

for every $g \in G$.

(2) *For any commutative C-algebra A the set of CG-module algebra structures on A is in bijection with the set of left actions of G as automorphisms on the C-algebra A (i.e. homomorphisms of groups $G \to \mathsf{Alg}_C(A, A)$).*

Proof. The first statement is trivial. For the second, we note that if $\Psi\colon CG \otimes_C A \to A$ is a CG-module algebra structure on A, then $g.a \coloneqq \Psi(g \otimes a)$ for $g \in G$ and $a \in A$ defines a left action of G on A as automorphisms of C-algebras. If conversely $G \times A \to A, (g, a) \mapsto g.a$ is a left action of G on A as automorphisms of C-algebras, then the homomorphism of C-modules $\Psi\colon CG \otimes_C A \to A$ defined by $\Psi(g \otimes a) \coloneqq g.a$ for $g \in G$ and $a \in A$ is a CG-module algebra structure on A. These assignments are inverse to each other and yield the bijection. □

We note that for every commutative C-algebra A there is a natural action of G from the left on the C-algebra $\prod_{g\in G} A$ (with componentwise addition and multiplication) given by

$$G \times \prod_{g\in G} A \to \prod_{g\in G} A, \quad (g, (a_h)_{h\in G}) \mapsto (a_{hg})_{h\in G}.$$

Considering the CG-module algebra $(\mathsf{Mod}_C(CG, A), \Psi_{int})$ as C-algebra with left action of G as automorphisms of C-algebras via proposition 2.3.3, one immediately sees that

$$\mathsf{Mod}_C(CG, A) \to \prod_{g\in G} A, \quad f \mapsto (f(g))_{g\in G} \tag{2.3.2}$$

is an isomorphism of C-algebras with left G-action. If a left action of G as automorphisms on the C-algebra A is given, then the composition of the homomorphism $\rho\colon A \to \mathsf{Mod}_C(CG, A)$, associated to the corresponding CG-module algebra structure on A via the isomorphism (2.2.1), with the isomorphism (2.3.2) is the homomorphism of C-algebras $A \to \prod_{g\in G} A$ sending $a \in A$ to $(g.a)_{g\in G}$.

Remark 2.3.4. *In the case $G = \mathbb{Z}$ the C-bialgebra $C\mathbb{Z}$ is isomorphic to $C[\mathbb{G}_m]$. Since left $\mathbb{Z}$-actions on a commutative C-algebra A correspond to automorphisms of the C-algebra A, proposition 2.3.3 specializes to proposition 2.3.2 in this case.*

2.3.4 Derivations

Derivations can be seen as module algebra structures for a certain bialgebra. This idea appeared in [Swe69, Section 7.0, Example b) on page 139], where the author defined more generally so called g-derivations, where g is a group-like element.

Proposition 2.3.5. *We denote by D_{der} the C-bialgebra underlying the Hopf-algebra structure on the coordinate ring $C[\mathbb{G}_a]$ of the additive group scheme $\mathbb{G}_a$ over C (see for example [Wat79, Section 1.4] or [DG70, Chapitre II, §1, 2.2]). For every C-algebra A, there is a bijection between the set $\mathrm{Der}_C(A)$ of C-derivations on A and the set of D_{der}-module algebra structures on A.*

Proof. We recall that the C-bialgebra structure on $D_{der} = C[\mathbb{G}_a] \cong C[t]$ is given by the usual C-algebra structure on $C[t]$ and the C-coalgebra structure with comultiplication $\Delta\colon C[t] \to C[t] \otimes_C C[t]$ defined by $\Delta(t) := t \otimes 1 + 1 \otimes t$ and counit $\varepsilon\colon C[t] \to C$ defined by $\varepsilon(t) := 0$. If ∂ is a C-derivation on A, then we define

$$\Psi_\partial\colon D_{der} \otimes_C A \to A, \quad \Psi_\partial(t^n \otimes a) := \partial^n(a)$$

for all $n \in \mathbb{N}$ and all $a \in A$. Then obviously A is a D_{der}-module via Ψ_∂ and Ψ_∂ measures A to A since

$$\begin{aligned}\Psi_\partial(t^n \otimes ab) &= \partial^n(ab)\\ &= \sum_{n_1+n_2=n} \binom{n}{n_1} \partial^{n_1}(a)\partial^{n_2}(b)\\ &= \sum_{n_1+n_2=n} \binom{n}{n_1} \Psi_\partial(t^{n_1} \otimes a)\Psi_\partial(t^{n_2} \otimes b)\\ &= \sum_{(t^n)} \Psi_\partial(t^n_{(1)} \otimes a)\Psi_\partial(t^n_{(2)} \otimes b)\end{aligned}$$

and

$$\Psi_\partial(t^n \otimes 1) = \partial^n(1) = \delta_{n,0} = \varepsilon(t^n)1.$$

If, conversely, $\Psi \in \mathsf{Mod}_C(D_{der}, A)$ defines a D_{der}-module algebra structure on A, then we define $\partial_\Psi \colon A \to A$ by $\partial_\Psi(a) := \Psi(t \otimes a)$ for all $a \in A$. Then ∂_Ψ is C-linear and fulfills the Leibniz rule since $\Delta(t) = t \otimes 1 + 1 \otimes t$. These assignments give rise to the asserted bijection. □

Recall that for every commutative C-algebra A the formal power series ring $A[\![x]\!]$ carries a natural derivation ∂_x defined by $\partial_x(\sum_{n\in\mathbb{N}} a_n x^n) := \sum_{n\in\mathbb{N}} a_n n x^{n-1}$ for all $\sum_{n\in\mathbb{N}} a_n x^n \in A[\![x]\!]$. By proposition 2.3.5, the D_{der}-module algebra structure Ψ_{int} on $\mathsf{Mod}_C(D_{der}, A)$ gives rise to a C-derivation ∂_{int} on $\mathsf{Mod}_C(D_{der}, A)$, which is given by $(\partial_{int}(f))(t^n) = f(t^{n+1})$ for all $f \in \mathsf{Mod}_C(D_{der}, A)$ and all $n \in \mathbb{N}$. If A includes $\mathbb{Q}$, there is an isomorphism of differential C-algebras

$$(\mathsf{Mod}_C(D_{der}, A), \partial_{int}) \to (A[\![x]\!], \partial_x), \quad f \mapsto \sum_{n\in\mathbb{N}} \frac{f(t^n)}{n!} x^n.$$

By proposition 2.3.5 together with lemma 2.2.18, every C-derivation ∂ on a C-algebra A gives rise to a homomorphism of D_{der}-module algebras from (A, Ψ_∂) to $(\mathsf{Mod}_C(D_{der}, A), \Psi_{int})$. Thus, if $\mathbb{Q} \subseteq A$, the composition

$$(A, \partial) \xrightarrow{\rho} (\mathsf{Mod}_C(D_{der}, A), \partial_{int}) \xrightarrow{\sim} (A[\![x]\!], \partial_x)$$

is a homomorphism of differential C-algebras given by $a \mapsto \sum_{n\in\mathbb{N}} \frac{\partial^n(a)}{n!}x^n$. This is the iterative derivation associated to ∂, which H. Umemura calls *universal Taylor homomorphism* in his differential Galois theory [Ume96a].

If, however, A is of positive characteristic p, then $\mathsf{Mod}_C(D_{der}, A)$ is not reduced. For example $f \in \mathsf{Mod}_C(D_{der}, A)$ defined by $f(t^p) = 1$ and $f(t^m) = 0$ for $m \neq p$ fulfills $f^p = 0$.

2.3.5 Higher derivations

Higher derivations can also be understood as module algebra structures. In the univariate case ($n = 1$) this idea already appears in [Swe69, Section 7.0, Exercises 1) and 2) on page 140].

Proposition 2.3.6. *(1) For $n \in \mathbb{N}$ we denote by D_{HD^n} the free associative (non-commutative) C-algebra with generators $\theta^{(\boldsymbol{k})}$ for $\boldsymbol{k} \in \mathbb{N}^n \setminus \{\mathbf{0}\}$ and denote $1 \in D_{HD^n}$ also by $\theta^{(\mathbf{0})}$. Then D_{HD^n} becomes a cocommutative C-bialgebra with comultiplication $\Delta\colon D_{HD^n} \to D_{HD^n} \otimes_C D_{HD^n}$ and counit $\varepsilon\colon D_{HD^n} \to C$ defined as the homomorphisms of C-algebras such that*

$$\Delta(\theta^{(\boldsymbol{k})}) = \sum_{\boldsymbol{k}=\boldsymbol{k_1}+\boldsymbol{k_2}} \theta^{(\boldsymbol{k_1})} \otimes \theta^{(\boldsymbol{k_2})} \quad \text{and} \quad \varepsilon(\theta^{(\boldsymbol{k})}) = \delta_{\boldsymbol{k},\mathbf{0}} \quad \text{for all } \boldsymbol{k} \in \mathbb{N}^n. \tag{2.3.3}$$

(2) For every commutative C-algebra A there is a bijection between the set $\mathrm{HD}^n_C(A)$ of n-variate higher derivations on A over C (see chapter 1) and the set of D_{HD^n}-module algebra structures on A.

Proof. By the universal property of the free associative algebra $C\langle\{\theta^{(\boldsymbol{k})} \mid \boldsymbol{k} \in \mathbb{N}^n \setminus \{\mathbf{0}\}\}\rangle$ (see [Bou70, III.2, p. 22, Proposition 7]) there exist unique homomorphisms of C-algebras $\Delta\colon D_{HD^n} \to D_{HD^n} \otimes_C D_{HD^n}$ and $\varepsilon\colon D_{HD^n} \to C$ such that (2.3.3) holds. It is easily seen that Δ and ε make D_{HD^n} into a coassociative, counital and cocommutative C-coalgebra. Since by definition Δ and ε are homomorphisms of C-algebras, D_{HD^n} becomes a cocommutative C-bialgebra. For the proof of the second part, we note that we obtain such a bijection

by assigning to an n-variate higher derivation θ on A over C with components[5] $\theta^{(\boldsymbol{k})}$ the homomorphism of C-modules $\Psi\colon D_{HD^n} \otimes_C A \to A$ defined by $\theta^{(\boldsymbol{k})} \otimes a \mapsto \theta^{(\boldsymbol{k})}(a)$ for all $\boldsymbol{k} \in \mathbb{N}^n$ and all $a \in A$, and by assigning conversely to a D_{HD^n}-module algebra structure $\Psi\colon D_{HD^n} \otimes_C A \to A$ on A a higher derivation $\theta\colon A \to A[\![\boldsymbol{t}]\!]$ on A over C defined by $\theta(a) := \sum_{\boldsymbol{k}\in\mathbb{N}^n} \Psi(\theta^{(\boldsymbol{k})} \otimes a)\boldsymbol{t}^{\boldsymbol{k}}$ for all $a \in A$. □

Remark 2.3.7. *For every $i \in \{1, \dots, n\}$ the sequence $(\theta^{(k\cdot\delta_i)})_{k\in\mathbb{N}}$ in D_{HD^n} is a* divided power sequence *over $\theta^{(\mathbf{0})} \in D_{HD^n}$, as defined for example in [Haz78, 38.2.1].*

2.3.6 Iterative derivations

Iterative derivations can also be regarded as module algebras. The bialgebra used here appears in the univariate case ($n = 1$) for example in [Mon93, Example 5.6.8], where the author shows that this bialgebra is in fact a Hopf algebra.

Proposition 2.3.8. *(1) For $n \in \mathbb{N}$ we define D_{ID^n} as the free C-module with basis $\{\theta^{(\boldsymbol{k})} \mid \boldsymbol{k} \in \mathbb{N}^n\}$. On D_{ID^n} a C-algebra structure can be defined by*

$$1 := \theta^{(\mathbf{0})} \tag{2.3.4}$$

$$\theta^{(\boldsymbol{k})} \cdot \theta^{(\boldsymbol{l})} := \binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}} \theta^{(\boldsymbol{k}+\boldsymbol{l})} \tag{2.3.5}$$

for all $\boldsymbol{k}, \boldsymbol{l} \in \mathbb{N}^n$. Furthermore, D_{ID^n} carries a C-coalgebra structure with comultiplication Δ and counit ε given as the homomorphisms of C-modules defined by

$$\Delta(\theta^{(\boldsymbol{k})}) := \sum_{\boldsymbol{k_1}+\boldsymbol{k_1}=\boldsymbol{k}} \theta^{(\boldsymbol{k_1})} \otimes \theta^{(\boldsymbol{k_2})}$$

and

$$\varepsilon(\theta^{(\boldsymbol{k})}) := \delta_{\boldsymbol{k},\mathbf{0}}$$

[5] By abuse of notation we use the symbol $\theta^{(\boldsymbol{k})}$ for both, the components of the n-variate higher derivation θ and for certain elements in D_{HD^n}.

for all $\boldsymbol{k} \in \mathbb{N}^n$. *In this manner* D_{ID^n} *becomes a commutative, cocommutative* C*-bialgebra.*

(2) *For every commutative* C*-algebra* A *there exists a bijection between the set* $\mathrm{ID}^n_C(A)$ *of* n*-variate iterative derivations on* A *over* C *and the set of* D_{ID^n}*-module algebra structures on* A.

Proof. We first note that the multiplication (2.3.5) is associative, since

$$\begin{aligned}
\theta^{(\boldsymbol{k_1})}(\theta^{(\boldsymbol{k_2})}\theta^{(\boldsymbol{k_3})}) &= \binom{\boldsymbol{k_2}+\boldsymbol{k_3}}{\boldsymbol{k_2}}\theta^{(\boldsymbol{k_1})}\theta^{(\boldsymbol{k_2}+\boldsymbol{k_3})} \\
&= \binom{\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3}}{\boldsymbol{k_1}}\binom{\boldsymbol{k_2}+\boldsymbol{k_3}}{\boldsymbol{k_2}}\theta^{(\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3})} \\
&= \frac{\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3}}{\boldsymbol{k_1}!\boldsymbol{k_2}!\boldsymbol{k_3}!}\theta^{(\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3})} \\
&= \binom{\boldsymbol{k_1}+\boldsymbol{k_2}}{\boldsymbol{k_1}}\binom{\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3}}{\boldsymbol{k_3}}\theta^{(\boldsymbol{k_1}+\boldsymbol{k_2}+\boldsymbol{k_3})} \\
&= \binom{\boldsymbol{k_1}+\boldsymbol{k_2}}{\boldsymbol{k_1}}\theta^{(\boldsymbol{k_1}+\boldsymbol{k_2})}\theta^{(\boldsymbol{k_3})} \\
&= (\theta^{(\boldsymbol{k_1})}\theta^{(\boldsymbol{k_2})})\theta^{(\boldsymbol{k_3})}.
\end{aligned}$$

Obviously D_{ID^n} is commutative and $\theta^{(\boldsymbol{0})}$ is a unit for this multiplication. So D_{ID^n} becomes a commutative C-algebra. It is easily seen that Δ and ε make D_{ID^n} into a coassociative, counital and cocommutative C-coalgebra. We show that Δ and ε are C-algebra homomorphisms. For ε this is clear and for Δ this

follows from

$$\begin{aligned}\Delta(\theta^{(k)})\Delta(\theta^{(l)}) &= \sum_{k_1+k_2=k}\sum_{l_1+l_2=l}(\theta^{(k_1)}\otimes\theta^{(k_2)})(\theta^{(l_1)}\otimes\theta^{(l_2)})\\ &= \sum_{k_1+k_2=k}\sum_{l_1+l_2=l}\binom{k_1+l_1}{k_1}\binom{k_2+l_2}{k_2}(\theta^{(k_1+l_1)}\otimes\theta^{(k_2+l_2)})\\ &= \binom{k+l}{k}\sum_{\mu_1+\mu_2=k+l}\theta^{(\mu_1)}\otimes\theta^{(\mu_2)}\\ &= \binom{k+l}{k}\Delta(\theta^{(k+l)})\\ &= \Delta(\theta^{(k)}\cdot\theta^{(l)})\end{aligned}$$

for all $k, l \in \mathbb{N}^n$. Therefore, D_{ID^n} is a commutative and cocommutative C-bialgebra.

Let θ be an n-variate iterative derivation on a commutative algebra A over C with components $(\theta^{(k)})_{k\in\mathbb{N}^n}$.[6] We define a homomorphism of C-modules $\Psi\colon D_{ID^n}\otimes_C A \to A$ by $\Psi(\theta^{(k)}\otimes a) := \theta^{(k)}(a)$ for all $k \in \mathbb{N}^n$ and $a \in A$. One immediately checks that Ψ defines a D_{ID^n}-module algebra structure on A. Conversely, given a D_{ID^n}-module algebra structure $\Psi\colon D_{ID^n}\otimes_C A \to A$ on A, we define an n-variate iterative derivation $\theta\colon A \to A[\![t]\!]$ on A over C by $\theta(a) := \sum_{k\in\mathbb{N}^n}\Psi(\theta^{(k)}\otimes a)t^k$ for all $a \in A$. □

We recall that for any commutative C-algebra A there is a natural n-variate iterative derivation θ_t on $A[\![t]\!] := A[\![t_1,\dots,t_n]\!]$ over C (cf. example 1.2.5). Considering the D_{ID^n}-module algebra $(\mathsf{Mod}_C(D_{ID^n}, A), \Psi_{int})$ as an n-variate iterative differential ring over C via proposition 2.3.8, we note that there is an isomorphism

$$(\mathsf{Mod}_C(D_{ID^n}, A), \Psi_{int}) \to (A[\![t]\!], \theta_t), \quad f \mapsto \sum_{k\in\mathbb{N}^n} f(\theta^{(k)})t^k \tag{2.3.6}$$

of n-variate iterative differential rings over C. Using proposition 2.3.8 and lemma 2.2.18, we obtain for every n-variate iterative derivation $\theta \in \mathrm{ID}^n_C(A)$ on

[6] Again, by abuse of notation we use the symbol $\theta^{(k)}$ for both, the components of the n-variate iterative derivation θ and for certain elements in D_{ID^n}.

A over C a homomorphism of D_{ID^n}-module algebras $\rho\colon A \to \mathsf{Mod}_C(D_{ID^n}, A)$ and the composition

$$A \xrightarrow{\rho} \mathsf{Mod}_C(D_{ID^n}, A) \xrightarrow{\sim} A[\![\boldsymbol{t}]\!]$$

is again the iterative derivation θ itself. By abuse of notation we sometimes identify ρ and θ using the isomorphism (2.3.6)

2.3.7 σ-derivations

We can also describe σ-derivations in terms of module algebra structures. First, we recall their definition (see for example [And01, 1.4.1]).

Definition 2.3.9. *If A is a C-algebra and σ an endomorphism of A, then a map $\partial\colon A \to A$ is a* σ-derivation *on A over C if*

$$\begin{aligned}\partial(a+b) &= \partial(a) + \partial(b),\\ \partial(ab) &= \partial(a)b + \sigma(a)\partial(b) \text{ and}\\ \partial(\lambda a) &= \lambda\partial(a)\end{aligned}$$

hold for all $a, b \in A$ and $\lambda \in C$.

Proposition 2.3.10. *(1) The free associative (non-commutative) C-algebra*

$$D_{\sigma\text{-}der} := C\langle\sigma, \partial\rangle$$

with generators σ and ∂ becomes a C-bialgebra with coproduct Δ and counit ε given by the C-algebra homomorphisms $\Delta\colon D_{\sigma\text{-}der} \to D_{\sigma\text{-}der} \otimes_C D_{\sigma\text{-}der}$ and $\varepsilon\colon D_{\sigma\text{-}der} \to C$ defined by

$$\Delta(\sigma) = \sigma\otimes\sigma, \quad \Delta(\partial) = \partial\otimes 1 + \sigma\otimes\partial, \quad \varepsilon(\sigma) = 1 \quad \text{and} \quad \varepsilon(\partial) = 0. \tag{2.3.7}$$

The C-bialgebra $D_{\sigma\text{-}der}$ is neither commutative nor cocommutative.

(2) *If A is a C-algebra, then there is a bijection between the set of pairs (σ, ∂), where σ is an endomorphism of the C-algebra A and ∂ is a σ-derivation on A over C, and the set of $D_{\sigma\text{-}der}$-module algebra structures on A.*

Proof. We first note that by the universal property of the free associative (non-commutative) C-algebra $C\langle\sigma, \partial\rangle$ (see for example [Bou70, III.2, p. 22, Proposition 7]) there exist unique homomorphisms of C-algebras $\Delta\colon D_{\sigma\text{-}der} \to D_{\sigma\text{-}der} \otimes_C D_{\sigma\text{-}der}$ and $\varepsilon\colon D_{\sigma\text{-}der} \to C$ fulfilling (2.3.7). Because of

$$(\Delta \otimes \mathrm{id}) \circ \Delta(\partial) = \partial \otimes 1 \otimes 1 + \sigma \otimes \partial \otimes 1 + \sigma \otimes \sigma \otimes \partial = (\mathrm{id} \otimes \Delta) \circ \Delta(\partial)$$
$$(\Delta \otimes \mathrm{id}) \circ \Delta(\sigma) = \sigma \otimes \sigma \otimes \sigma = (\mathrm{id} \otimes \Delta) \circ \Delta(\sigma),$$

the comultiplication Δ is coassociative. From the equations

$$\begin{aligned}(\varepsilon \otimes \mathrm{id}) \circ \Delta(\partial) &= \varepsilon(\partial) \otimes 1 + \varepsilon(\sigma) \otimes \partial = 1 \otimes \partial,\\ (\mathrm{id} \otimes \varepsilon) \circ \Delta(\partial) &= \partial \otimes \varepsilon(1) + \sigma \otimes \varepsilon(\partial) = \partial \otimes 1,\\ (\varepsilon \otimes \mathrm{id}) \circ \Delta(\sigma) &= \varepsilon(\sigma) \otimes \sigma = 1 \otimes \sigma \text{ and}\\ (\mathrm{id} \otimes \varepsilon) \circ \Delta(\sigma) &= \sigma \otimes \varepsilon(\sigma) = \sigma \otimes 1\end{aligned}$$

we see that ε is a counit with respect to Δ on $C\langle\sigma, \partial\rangle$. But if τ is the twist homomorphism on $D_{\sigma\text{-}der} \otimes_C D_{\sigma\text{-}der}$ interchanging the factors, then $\tau \circ \Delta(\partial) = \tau(\partial \otimes 1 + \sigma \otimes \partial) = 1 \otimes \partial + \partial \otimes \sigma \neq \Delta(\partial)$, so the C-bialgebra $C\langle\sigma, \partial\rangle$ is not cocommutative.

To prove part (2), let σ be an endomorphism of the C-algebra A and ∂ a σ-derivation on A over C.[7] We define a C-module homomorphism $\Psi\colon D_{\sigma\text{-}der} \otimes_C A \to A$ by $\Psi(\prod_{i=1}^m \partial^{k_i}\sigma^{l_i} \otimes a) := (\prod_{i=1}^m \partial^{k_i}\sigma^{l_i})(a)$ for all $a \in A$ and $m, k_1, \ldots, k_m, n_1, \ldots, n_m \in \mathbb{N}$. Then it is clear that Ψ measures A to A and that A becomes a $D_{\sigma\text{-}der}$-module via Ψ. If conversely $\Psi\colon D_{\sigma\text{-}der} \otimes_C A \to A$ is a $D_{\sigma\text{-}der}$-module algebra structure on A, then $\sigma\colon A \to A$, defined by $\sigma(a) := \Psi(\sigma \otimes a)$ for all $a \in A$, is an endomorphism of the C-algebra A and

[7] By abuse of notation, we use the symbols σ and ∂ for both, the elements of $D_{\sigma\text{-}der}$ and the endomorphism σ and the σ-derivation ∂.

$\partial\colon A \to A$, defined by $\partial(a) \coloneqq \Psi(\partial \otimes a)$ for all $a \in A$, is a σ-derivation on A over C. □

Later, when defining the infinitesimal Galois group of an extension of D-module fields, where D is a C-bialgebra, we assume that D is cocommutative. This assumption excludes $D_{\sigma\text{-}der}$.

2.3.8 q-skew iterative σ-derivations

C. Hardouin introduced so called *iterative q-difference operators* and developed a Picard-Vessiot for iterative q-difference equations in [Har10]. We show how these operators can be understood in the context of D-module algebras. More precisely, we introduce a bialgebra describing *q-skew iterative σ-derivations*. It turns out that the iterative q-difference operators introduced in [Har10] are a special case of q-skew iterative σ-derivations.

We first recall some q-arithmetical notation. We define in the polynomial algebra $C[\hat{q}]$ over C for $n \in \mathbb{N}$

$$[n]_{\hat{q}} \coloneqq 1 + \hat{q} + \cdots + \hat{q}^{n-1} = \frac{\hat{q}^n - 1}{\hat{q} - 1}.$$

The *$\hat{q}$-factorial* of n will be defined as

$$[0]_{\hat{q}}! := 1 \quad \text{and} \quad [n]_{\hat{q}}! := \prod_{i=1}^{n} [i]_{\hat{q}} \quad \text{for } n > 0.$$

Finally, we define $\hat{q}$-binomial coefficients for natural numbers $m, n \in \mathbb{N}$ by

$$\binom{n}{m}_{\hat{q}} := \begin{cases} \frac{[n]_{\hat{q}}!}{[n-m]_{\hat{q}}![m]_{\hat{q}}!} & \text{if } m \leq n, \\ 0 & \text{if } m > n. \end{cases}$$

They are in fact polynomials in $\hat{q}$ with integer coefficients (see [Kas95, Proposition IV.2.1 (a)])

Lemma 2.3.11 (q-Vandermonde identity). *For $k, l, i \in \mathbb{N}$ with $i \leq k + l$ the identity*

$$\binom{k+l}{i}_{\hat{q}} = \sum_{i_1+i_2=i} \binom{k}{i_1}_{\hat{q}} \binom{l}{i_2}_{\hat{q}} \hat{q}^{i_2(k-i_1)}$$

holds.

Proof. See for example [Kas95, Proposition IV.2.3]. □

For every commutative C-algebra A and every $q \in A$ there is a unique homomorphism of C-algebras from $C[\hat{q}]$ to A sending $\hat{q}$ to q. We denote by $[n]_q$, $[n]_q!$ and $\binom{n}{m}_q$ the images in A of $[n]_{\hat{q}}$, $[n]_{\hat{q}}!$ and $\binom{n}{m}_{\hat{q}}$, respectively.

We recall the definition of iterative q-difference operators given in [Har10, Definition 2.4].

Definition 2.3.12. *Let σ_q be the endomorphism of $C(t)$ defined by*

$$(\sigma_q(f))(t) = f(qt)$$

for all $f \in C(t)$ and let (A, σ_q) be a commutative difference extension ring of $(C(t), \sigma_q)$.[8] *An* iterative q-difference operator *on A is a family $(\delta^{(i)})_{i\in\mathbb{N}}$ of maps from A to itself fulfilling the following properties for all $i, j \in \mathbb{N}$ and all $a, b \in A$*

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

(2) $\delta^{(1)} = \frac{\sigma_q - \mathrm{id}}{(q-1)t}$

(3) $\delta^{(i)}(a + b) = \delta^{(i)}(a) + \delta^{(i)}(b)$,

(4) $\delta^{(i)}(ab) = \sum_{i_1+i_2=i} \sigma_q^{i_2}(\delta^{(i_1)}(a))\delta^{(i_2)}(b)$,

(5) $\delta^{(i)} \circ \delta^{(j)} = \binom{i+j}{i}_q \delta^{(i+j)}$.

[8] By abuse of notation, we denote the endomorphisms of A and of $C(t)$ both by σ_q.

Actually, iterative q-difference operators are a special instance of the more general *q-skew iterative σ-derivations*, which generalize both q-skew σ-derivations and iterative derivations. These are a special case of q-skew higher derivations, which again are a special case of higher σ-derivations (see [Hay08]). Here we restrict ourselves to q-skew iterative σ-derivations, which cover many interesting cases. We first recall the definition (cf. [Hay08]).

Definition 2.3.13. *If A is a commutative C-algebra and $q \in C$, then a* q-skew iterative σ-derivation *of A consists of a C-algebra endomorphism $\sigma \in \mathsf{CAlg}_C(A, A)$ and a family of maps $\theta^{(k)} \colon A \to A$ for all $k \in \mathbb{N}$ such that*

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

(2) $\theta^{(i)}\sigma = q^i \sigma \theta^{(i)}$

(3) $\theta^{(i)}$ *is C-linear*

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

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

for all $i, j \in \mathbb{N}$ and all $a, b \in A$. A homomorphism of commutative C-algebras with q-skew iterative σ-derivations from $(A, \sigma_A, (\theta_A^{(i)})_{i\in\mathbb{N}})$ to $(B, \sigma_B, (\theta_B^{(i)})_{i\in\mathbb{N}})$ is a homomorphism of C-algebras $f \colon A \to B$ such that $f(\sigma_A(a)) = \sigma_B(f(a))$ and $f(\theta_A^{(i)}(a)) = \theta_B^{(i)}(f(a))$ for all $a \in A$ and all $i \in \mathbb{N}$.

Remark 2.3.14. *(1) For any q-skew iterative σ-derivation we obtain from the C-linearity of $\theta^{(i)}$ and σ that $\theta^{(i)}(q) = 0$ for all $i > 0$ and $\sigma(q) = q$, respectively.*

(2) If $(\delta^{(i)})_{i\in\mathbb{N}}$ is an iterative q-difference operator with respect to σ_q such that all $\delta^{(i)}$ are C-linear, then this is a q-skew iterative σ_q-derivation. This follows from [Har10, Lemma 2.6].

(3) There are different definitions of q-skew (iterative) σ-derivations. For example in [Cau03] the condition (2) in definition 2.3.13 is replaced by the relation $\sigma\theta^{(i)} = q\theta^{(i)}\sigma$ (though only classical q-skew σ derivations are treated there

and not q-skew iterative σ-derivations). Having the example of a q-skew σ_q-derivation associated to a q-difference operator σ_q in mind (i.e. the map $\delta^{(1)}$ in definition 2.3.12), we prefer our convention.

Proposition 2.3.15. *For every $q \in C$ the following hold:*

(1) Let $D_{ID_{q,\sigma}}$ be the quotient of the free associative (non-commutative) C-algebra $C\langle\{\sigma\} \cup \{\theta^{(i)} \mid i \in \mathbb{N}\}\rangle$ generated by σ and $\theta^{(i)}$ for $i \in \mathbb{N}$ modulo the ideal I that is generated by

$$\theta^{(0)} - 1, \tag{2.3.8}$$

$$\theta^{(i)}\sigma - q^i\sigma\theta^{(i)} \tag{2.3.9}$$

and

$$\theta^{(i)}\theta^{(j)} - \binom{i+j}{i}_q \theta^{(i+j)} \tag{2.3.10}$$

for all $i, j \in \mathbb{N}$. It becomes a C-bialgebra with comultiplication

$$\Delta\colon D_{ID_{q,\sigma}} \to D_{ID_{q,\sigma}} \otimes_C D_{ID_{q,\sigma}}$$

and counit

$$\varepsilon\colon D_{ID_{q,\sigma}} \to C$$

defined by[9]

$$\Delta(\sigma) := \sigma \otimes \sigma$$
$$\Delta(\theta^{(i)}) := \sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)}$$

and

$$\varepsilon(\sigma) := 1$$
$$\varepsilon(\theta^{(i)}) := \delta_{i,0}$$

for all $i \in \mathbb{N}$, respectively.

[9] By abuse of notation, we denote the images of σ and $\theta^{(i)}$ in $D_{ID_{q,\sigma}}$ by the same symbols.

(2) For any commutative C-algebra A, the set of q-skew iterative σ-derivations on A is in bijection with the set of $D_{ID_{q,\sigma}}$-module algebra structures on A.

Proof. We first define homomorphisms of C-algebras

$$\Delta\colon C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\to C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\otimes_C C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle$$

and

$$\varepsilon\colon C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\to C$$

by

$$\Delta(\sigma)\coloneqq\sigma\otimes\sigma,\quad \Delta(\theta^{(i)})\coloneqq\sum_{i_1+i_2=i}\sigma^{i_2}\theta^{(i_1)}\otimes\theta^{(i_2)}\quad\text{for all } i\in\mathbb{N}$$

and

$$\varepsilon(\sigma)\coloneqq 1,\quad \varepsilon(\theta^{(i)})\coloneqq\delta_{i,0}\quad\text{for all } i\in\mathbb{N},$$

respectively. We show that the image of I under the composition of

$$C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\to C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\otimes_C C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle$$

with

$$C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\otimes_C C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\to D_{ID_{q,\sigma}}\otimes_C D_{ID_{q,\sigma}},$$

which we denote by $\tilde{\Delta}$, and under

$$\varepsilon\colon C\langle\{\sigma\}\cup\{\theta^{(i)}\mid i\in\mathbb{N}\}\rangle\to C$$

is zero and thus these homomorphisms factor through $D_{ID_{q,\sigma}}$. In fact, using

lemma 2.3.11, we have

$$\begin{aligned}
\tilde{\Delta}(\theta^{(i)}\theta^{(j)}) &= \tilde{\Delta}(\theta^{(i)})\tilde{\Delta}(\theta^{(j)}) \\
&= \left(\sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)}\right)\left(\sum_{j_1+j_2=j} \sigma^{j_2}\theta^{(j_1)} \otimes \theta^{(j_2)})\right) \\
&= \sum_{\substack{i_1+i_2=i \\ j_1+j_2=j}} q^{i_1 j_2}\sigma^{i_2+j_2}\binom{i_1+j_1}{i_1}_q \theta^{(i_1+j_1)} \otimes \binom{i_2+j_2}{i_2}_q \theta^{(i_2+j_2)} \\
&= \sum_{\substack{k+l=i+j \\ i_1+i_2=i}} q^{i_1(l-i_2)}\binom{k}{i_1}_q \binom{l}{i_2}_q \sigma^l \theta^{(k)} \otimes \theta^{(l)} \\
&= \sum_{k+l=i+j} \binom{k+l}{i}_q \sigma^l \theta^{(k)} \otimes \theta^{(l)} \\
&= \tilde{\Delta}\left(\binom{i+j}{i}_q \theta^{(i+j)}\right),
\end{aligned}$$

$$\begin{aligned}
\tilde{\Delta}(q^i\sigma\theta^{(i)}) &= q^i\tilde{\Delta}(\sigma)\tilde{\Delta}(\theta^{(i)}) \\
&= q^i(\sigma\otimes\sigma)\sum_{i=i_1+i_2} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)} \\
&= \sum_{i_1+i_2=i} q^{i_1}\sigma^{i_2+1}\theta^{(i_1)} \otimes q^{i_2}\sigma\theta^{(i_2)} \\
&= \left(\sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)}\right)(\sigma\otimes\sigma) \\
&= \tilde{\Delta}(\theta^{(i)}\sigma)
\end{aligned}$$

and

$$\tilde{\Delta}(\theta^{(0)}) = 1 \otimes 1 = \tilde{\Delta}(1).$$

We also have

$$\varepsilon(\theta^{(i)}\theta^{(j)}) = \varepsilon(\theta^{(i)})\varepsilon(\theta^{(j)}) = \delta_{i,0}\delta_{j,0} = \binom{i+j}{i}_q \delta_{i+j,0} = \varepsilon\left(\binom{i+j}{i}_q \theta^{(i+j)}\right),$$
$$\varepsilon(q^i\sigma\theta^{(i)}) = q^i\varepsilon(\sigma)\varepsilon(\theta^{(i)}) = \delta_{i,0} = \varepsilon(\theta^{(i)})\varepsilon(\sigma) = \varepsilon(\theta^{(i)}\sigma)$$

and

$$\varepsilon(\theta^{(0)}) = 1 = \varepsilon(1)$$

and so Δ and ε factor through $D_{ID_{q,\sigma}}$. We denote the induced homomorphisms of C-algebras $D_{ID_{q,\sigma}} \to D_{ID_{q,\sigma}} \otimes_C D_{ID_{q,\sigma}}$ and $D_{ID_{q,\sigma}} \to C$ again by Δ and ε, respectively. Because of

$$\begin{aligned}
(\Delta \otimes \mathrm{id}) \circ \Delta(\theta^{(i)}) &= (\Delta \otimes \mathrm{id}) \left(\sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)} \right) \\
&= \sum_{i_1+i_2=i} \Delta(\sigma^{i_2}\theta^{(i_1)}) \otimes \theta^{(i_2)} \\
&= \sum_{i_1+i_2=i} (\sigma^{i_2} \otimes \sigma^{i_2}) \left(\sum_{i_{11}+i_{12}=i_1} \sigma^{i_{12}}\theta^{(i_{11})} \otimes \theta^{(i_{12})} \right) \otimes \theta^{(i_2)} \\
&= \sum_{i_1+i_2+i_3=i} \sigma^{i_3+i_2}\theta^{(i_1)} \otimes \sigma^{i_3}\theta^{(i_2)} \otimes \theta^{(i_3)} \\
&= \sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \left(\sum_{i_2=i_{21}+i_{22}} \sigma^{i_{22}}\theta^{(i_{21})} \otimes \theta^{(i_{22})} \right) \\
&= (\mathrm{id} \otimes \Delta) \left(\sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)} \otimes \theta^{(i_2)} \right) \\
&= (\mathrm{id} \otimes \Delta) \circ \Delta(\theta^{(i)})
\end{aligned}$$

for all $i \in \mathbb{N}$ and

$$\begin{aligned}
(\Delta \otimes \mathrm{id}) \circ \Delta(\sigma) &= \sigma \otimes \sigma \otimes \sigma \\
&= (\mathrm{id} \otimes \Delta) \circ \Delta(\sigma),
\end{aligned}$$

the comultiplication Δ is coassociative. Furthermore,

$$\begin{aligned}(\varepsilon \otimes \mathrm{id}) \circ \Delta(\theta^{(i)}) &= \sum_{i_1+i_2=i} \varepsilon(\sigma^{i_2}\theta^{(i_1)})\theta^{(i_2)} \\ &= \sum_{i_1+i_2=i} \delta_{i_1,0}\theta^{(i_2)} \\ &= \theta^{(i)} \\ &= \sum_{i_1+i_2=i} \sigma^{i_2}\theta^{(i_1)}\delta_{i_2,0} \\ &= (\mathrm{id} \otimes \varepsilon) \circ \Delta(\theta^{(i)})\end{aligned}$$

and

$$(\varepsilon \otimes \mathrm{id}) \circ \Delta(\sigma) = \varepsilon(\sigma)\sigma = \sigma = \sigma\varepsilon(\sigma) = (\mathrm{id} \otimes \varepsilon) \circ \Delta(\sigma),$$

so that ε is a counit for Δ. This completes the proof of the first part.

The proof of part (2) is analogous to other structures treated before. We just note that the properties (1), (2) and (5) in definition 2.3.13 correspond to the relations (2.3.8), (2.3.9) and (2.3.10), respectively, while the property (4) and the fact that σ is an endomorphism of C-algebras are expressed by the C-coalgebra structure on $D_{ID_{q,\sigma}}$. □

Proposition 2.3.16. *For any commutative C-algebra A and any $q \in C$, let $A^{\mathbb{N}}[\![x]\!]$ be the ring of non-commutative formal power series $\sum_{i\in\mathbb{N}} x^i f_i$ with coefficients $f_i \in A^{\mathbb{N}}$ and with relations $fx = x\Sigma(f)$ for $f \in A^{\mathbb{N}}$, where Σ denotes the shift endomorphism on $A^{\mathbb{N}}$ (see equation (2.3.1)). On $A^{\mathbb{N}}[\![x]\!]$ a q-skew iterative σ-derivation is given by the endomorphism $\tilde{\Sigma}$ on $A^{\mathbb{N}}[\![x]\!]$ defined by*

$$\tilde{\Sigma}\left(\sum_{n\geq 0} x^n f_n\right) := \sum_{n\geq 0} x^n q^n \Sigma(f_n).$$

and maps $\theta^{(i)}$ from $A^{\mathbb{N}}[\![x]\!]$ to itself defined by

$$\theta^{(i)}\left(\sum_{n\geq 0} x^n f_n\right) := \sum_{n\geq 0} \binom{n}{i}_q x^{n-i} f_n$$

for all $i \in \mathbb{N}$ and $\sum_{n\geq 0} x^n f_n \in A^{\mathbb{N}}[\![x]\!]$.

Proof. Let $n, m \in \mathbb{N}$ and $f, g \in A^{\mathbb{N}}$. First, the map $\tilde{\Sigma}$ is multiplicative, since

$$\begin{aligned}\tilde{\Sigma}(x^n f x^m g) &= \tilde{\Sigma}(x^{n+m}\Sigma^m(f)g)\\ &= x^{n+m}q^{n+m}\Sigma^{m+1}(f)\Sigma(g)\\ &= x^n q^n \Sigma(f) x^m q^m \Sigma(g)\\ &= \tilde{\Sigma}(x^n f)\tilde{\Sigma}(x^m g).\end{aligned}$$

Using lemma 2.3.11 we have for all $i, j \in \mathbb{N}$

$$\begin{aligned}\sum_{i_1+i_2=i} \tilde{\Sigma}^{i_2}(\theta^{(i_1)}(x^n f))\theta^{(i_2)}(x^m g) &= \sum_{i_1+i_2=i} \tilde{\Sigma}^{i_2}\left(\binom{n}{i_1}_q x^{n-i_1} f\right)\binom{m}{i_2}_q x^{m-i_2} g\\ &= \sum_{i_1+i_2=i}\binom{n}{i_1}_q\binom{m}{i_2}_q q^{(n-i_1)i_2} x^{n-i_1}\Sigma^{i_2}(f)x^{m-i_2}g\\ &= \binom{n+m}{i}_q x^{n+m-i}\Sigma^m(f)g\\ &= \theta^{(i)}(x^{n+m}\Sigma^m(f)g)\\ &= \theta^{(i)}(x^n f x^m g)\end{aligned}$$

and

$$\begin{aligned}\theta^{(i)}\theta^{(j)}(x^n f) &= \theta^{(i)}\left(\binom{n}{j}_q x^{n-j} f\right)\\ &= \binom{n}{j}_q\binom{n-j}{i}_q x^{n-j-i} f\\ &= \binom{i+j}{i}_q\binom{n}{i+j}_q x^{n-j-i} f\\ &= \binom{i+j}{i}_q \theta^{(i+j)}(x^n f)\end{aligned}$$

and so we see that $\tilde{\Sigma}$ together with $(\theta^{(i)})_{i\in\mathbb{N}}$ is a q-skew iterative σ-derivation on $A^{\mathbb{N}}[\![x]\!]$. □

Proposition 2.3.17. *For any $q \in C$ and any commutative C-algebra A there is an isomorphism of C-algebras with q-skew iterative σ-derivations (with $A^{\mathbb{N}}[\![x]\!]$ as*

defined in proposition 2.3.16)

$$\varphi\colon \mathsf{Mod}_{\mathsf{C}}(D_{ID_{q,\sigma}}, A) \xrightarrow{\sim} A^{\mathbb{N}}[\![x]\!],$$

defined by $\varphi(f) \coloneqq \sum_{i\geq 0} x^i (n \mapsto f(\sigma^n \theta^{(i)}))$ *for all* $f \in \mathsf{Mod}_{\mathsf{C}}(D_{ID_{q,\sigma}}, A)$.

Proof. Obviously φ is C-linear. It is also multiplicative since for $f, g \in \mathsf{Mod}_{\mathsf{C}}(D, A)$ we have

$$\begin{aligned}
\varphi(f)\varphi(g) &= \left(\sum_{i_1\geq 0} x^{i_1}(n \mapsto f(\sigma^n \theta^{(i_1)}))\right)\left(\sum_{i_2\geq 0} x^{i_2}(n \mapsto g(\sigma^n \theta^{(i_2)}))\right) \\
&= \sum_{i_1,i_2\geq 0} x^{i_1+i_2}\Sigma^{i_2}(n \mapsto f(\sigma^n \theta^{(i_1)}))(n \mapsto g(\sigma^n \theta^{(i_2)})) \\
&= \sum_{i_1,i_2\geq 0} x^{i_1+i_2}(n \mapsto f(\sigma^{n+i_2} \theta^{(i_1)}) g(\sigma^n \theta^{(i_2)})) \\
&= \sum_{i\geq 0} x^i (n \mapsto (fg)(\sigma^n \theta^{(i)})) \\
&= \varphi(fg).
\end{aligned}$$

From

$$\begin{aligned}
\varphi(\sigma.f) &= \sum_{i\geq 0} x^i (n \mapsto f(\sigma^n \theta^{(i)} \sigma)) \\
&= \sum_{i\geq 0} x^i q^i (n \mapsto f(\sigma^{n+1} \theta^{(i)})) \\
&= \tilde{\Sigma}(\varphi(f))
\end{aligned}$$

and

$$\begin{aligned}
\theta^{(j)}(\varphi(f)) &= \theta^{(j)}\left(\sum_{i\geq 0} x^i (n \mapsto f(\sigma^n\theta^{(i)}))\right) \\
&= \sum_{i\geq 0} \binom{i}{j}_q x^{i-j} (n \mapsto f(\sigma^n\theta^{(i)})) \\
&= \sum_{i\geq 0} \binom{i+j}{j}_q x^i (n \mapsto f(\sigma^n\theta^{(i+j)})) \\
&= \sum_{i\geq 0} x^i (n \mapsto f(\sigma^n \binom{i+j}{j}_q \theta^{(i+j)})) \\
&= \sum_{i\geq 0} x^i (n \mapsto f(\sigma^n\theta^{(i)}\theta^{(j)})) \\
&= \varphi(\theta^{(j)}.f)
\end{aligned}$$

for all $f \in \mathsf{Mod}_C(D_{ID_{q,\sigma}}, A)$ we obtain that φ is a homomorphism of C-algebras with q-skew iterative σ-derivation. It is clear that φ is an isomorphism since $D_{ID_{q,\sigma}}$ is a free C-module with basis $\{\sigma^n\theta^{(i)} \mid i, n \in \mathbb{N}\}$. □

The composition

$$A \xrightarrow{\rho} \mathsf{Mod}_C(D_{ID_{q,\sigma}}, A) \xrightarrow{\sim} A^{\mathbb{N}}[\![x]\!]$$

is a homomorphism of C-algebras with q-skew iterative σ-derivations that generalizes the corresponding homomorphisms in subsection 2.3.4 (in the case of characteristic 0) and in subsubsection 2.3.6. When we compose this homomorphism with the homomorphism

$$A^{\mathbb{N}}[\![x]\!] \to A[\![x]\!], \quad \sum_{i\geq 0} x^i f_i \mapsto \sum_{i\geq 0} x^i f_i(0)$$

we obtain a homomorphism $A \to A[\![x]\!]$, which in the case of iterative q-difference operators is closely related to the homomorphism **T** defined in [Har10, Definition 2.15].

2.3.9 $\mathcal{D}$-rings

In [MS09] R. Moosa and T. Scanlon introduce Hasse systems $\mathcal{D}$ and, given such a Hasse system, they define $\mathcal{D}$-rings, generalizing rings with higher derivation as introduced in chapter 1. They also introduce iterative Hasse systems and, given such an iterative Hasse system $\mathcal{D}$, they define iterative Hasse rings. We show that to every iterative Hasse system $\mathcal{D}$ there is canonically associated a cocommutative C-bialgebra D such that iterative $\mathcal{D}$-rings and D-module algebras are in bijection to each other. We refer to [MS10] and [MS09] for notation concerning Hasse systems $\mathcal{D}$ and $\mathcal{D}$-rings.

Remark 2.3.18. *Although the authors do not specify it, we assume that all ring schemes occurring in the definition of Hasse systems are commutative.*

Proposition 2.3.19. *Let $\mathcal{D} = (\mathcal{D}_n)_{n\in\mathbb{N}}$ be an iterative Hasse system over C with respect to $\Delta = (\Delta_{(m,n)}\colon \mathcal{D}_{m+n} \to \mathcal{D}_{(m,n)})_{m,n\in\mathbb{N}}$ (see [MS09, Definition 2.1 and 2.13]). Then*

$$D \coloneqq \varinjlim_{n\in\mathbb{N}} \mathcal{D}_n(C)^*,$$

where we denote by $\mathcal{D}_n(C)^*$ the dual $\mathsf{Mod}_C(\mathcal{D}_n(C), C)$ of the C-module $\mathcal{D}_n(C)$, becomes naturally a cocommutative C-bialgebra and for every commutative C-algebra R there is an isomorphism of C-algebras

$$\mathsf{Mod}_C(D, R) \cong \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R). \tag{2.3.11}$$

Proof. We denote the transition maps of $\mathcal{D}$ by $\pi_{m,n}\colon \mathcal{D}_m \to \mathcal{D}_n$ for all $m, n \in \mathbb{N}$ with $m \geq n$. The structure of a commutative C-algebra on $\mathcal{D}_n(C)$ induces a structure of a cocommutative C-coalgebra on the dual $\mathcal{D}_n(C)^*$ for all $n \in \mathbb{N}$ and the homomorphisms of C-algebras $\pi_{m,n}(C)\colon \mathcal{D}_m(C) \to \mathcal{D}_n(C)$ induce homomorphisms of C-coalgebras $\pi_{m,n}(C)^*\colon \mathcal{D}_n(C)^* \to \mathcal{D}_m(C)^*$ forming a direct system in the category of C-coalgebras. These C-coalgebra structures induce a

C-coalgebra structure on $D := \varinjlim_{n\in\mathbb{N}} \mathcal{D}_n(C)^*$, which again is cocommutative. We recall that there is a canonical isomorphism

$$\mathcal{D}_{(m,n)}(C) \xrightarrow{\sim} \mathcal{D}_m(C) \otimes_C \mathcal{D}_n(C) \tag{2.3.12}$$

(cf. [MS10, Remark 4.10]). The homomorphisms of C-algebras

$$\mathcal{D}_{m+n}(C) \xrightarrow{\Delta_{(m,n)}(C)} \mathcal{D}_{(m,n)}(C) \xrightarrow{\sim} \mathcal{D}_m(C) \otimes_C \mathcal{D}_n(C)$$

induce homomorphisms of C-coalgebras

$$\mathcal{D}_m(C)^* \otimes_C \mathcal{D}_n(C)^* \xrightarrow{\sim} \mathcal{D}_{(m,n)}(C)^* \xrightarrow{\Delta_{(m,n)}(C)^*} \mathcal{D}_{m+n}(C)^*$$

for all $m, n \in \mathbb{N}$. These give rise to a homomorphism of C-coalgebras

$$m\colon D \otimes_C D \to D,$$

which makes the diagram

$$\begin{array}{ccc} D \otimes_C D & \xrightarrow{\quad m \quad} & D \\ \uparrow & & \uparrow \\ \mathcal{D}_m(C)^* \otimes_C \mathcal{D}_n(C)^* & \xrightarrow{\Delta_{(m,n)}(C)^*} & \mathcal{D}_{m+n}(C)^* \end{array}$$

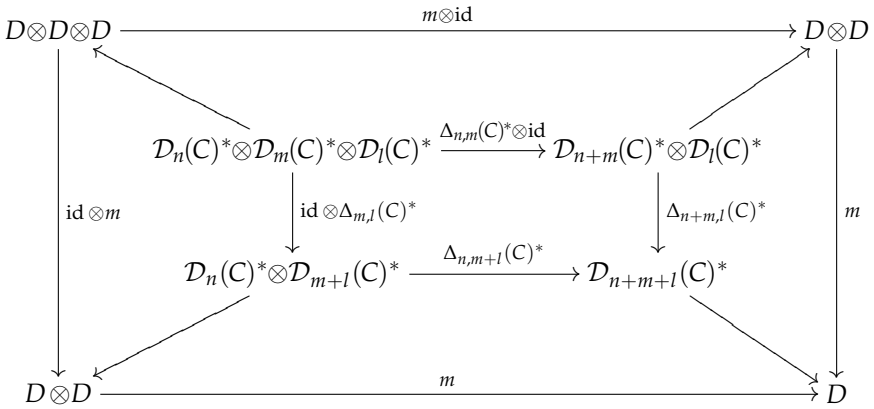
commutative for all $m, n \in \mathbb{N}$. The homomorphisms of C-algebras

$$\pi_{n,0}(C)\colon \mathcal{D}_n(C) \to \mathcal{D}_0(C) = C$$

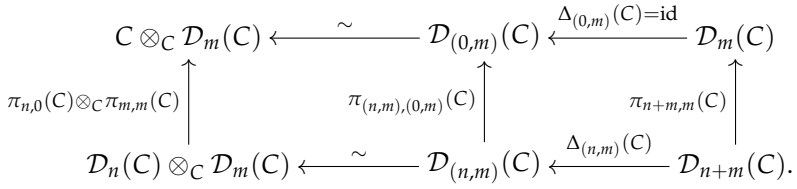
give rise to homomorphisms of C-coalgebra $C \to \mathcal{D}_n(C)^*$ and thus to $\eta\colon C \to \mathcal{D}_n(C)^* \to D$ (this composition does not depend on $n \in \mathbb{N}$). From the properties of iterative Hasse systems (cf. [MS09, Definition 2.13 (b)]) we see, using implicitely the isomorphisms (2.3.12), that the diagram

$$\begin{array}{ccc} \mathcal{D}_n(C) \otimes_C \mathcal{D}_m(C) \otimes_C \mathcal{D}_l(C) & \xleftarrow{\Delta_{n,m}(C)\otimes_C \mathrm{id}} & \mathcal{D}_{n+m}(C) \otimes_C \mathcal{D}_l(C) \\ \uparrow{\scriptstyle \mathrm{id}\otimes_C \Delta_{m,l}(C)} & & \uparrow{\scriptstyle \Delta_{n+m,l}(C)} \\ \mathcal{D}_n(C) \otimes_C \mathcal{D}_{m+l}(C) & \xleftarrow{\Delta_{n,m+l}(C)} & \mathcal{D}_{n+m+l}(C) \end{array}$$

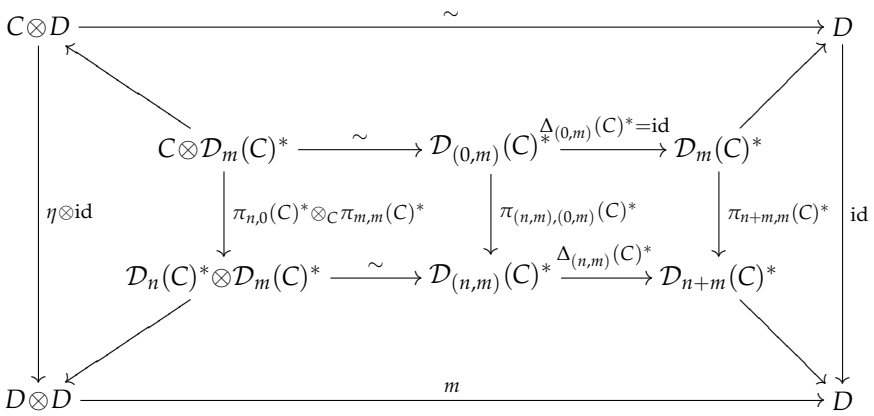
commutes for all $m, n, l \in \mathbb{N}$ and thus dually the inner rectangle of



commutes too (all tensor products are over C). From the universal property of the direct limit we obtain that the outer rectangle also commutes, i.e. that m is associative. Again by the properties of iterative Hasse systems (cf. [MS09, Definition 2.13 (a) and (c)]), the diagram



commutes for all $m, n \in \mathbb{N}$. Therefore, dually the inner rectangles of



commute and, again by the universal property of the direct limit, the outer rectangle commutes too. This means that η is a left unit for the multiplication m. Similarly, one can show that η is a right unit. Finally, for every commutative C-algebra R we have

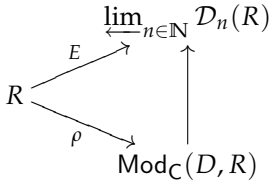
$$\begin{aligned}
\mathsf{Mod}_C(D, R) &= \mathsf{Mod}_C(\varinjlim_{n \in \mathbb{N}} \mathcal{D}_n(C)^*, R) \\
&\cong \varprojlim_{n \in \mathbb{N}} \mathsf{Mod}_C(\mathcal{D}_n(C)^*, R) \\
&\cong \varprojlim_{n \in \mathbb{N}} \mathcal{D}_n(C) \otimes_C R \\
&\cong \varprojlim_{n \in \mathbb{N}} \mathcal{D}_n(R).
\end{aligned}$$

□

Remark 2.3.20. *Let $\mathcal{D} = (\mathcal{D}_n)_{n \in \mathbb{N}}$ be a Hasse system over C. Then there is a bijection between the set of $\mathcal{D}$-rings as defined in [MS09, Definition 2.2] and the set of pairs (R, E) where R is a C-algebra and $E \colon R \to \varprojlim_{n \in \mathbb{N}} \mathcal{D}_n(R)$ is a C-algebra homomorphism such that the composition $R \xrightarrow{E} \varprojlim_{n \in \mathbb{N}} \mathcal{D}_n(R) \to \mathcal{D}_0(R) = R$ is the identity on R.*

Proposition 2.3.21. *Let $\mathcal{D}$ be an iterative Hasse system over C and $D = \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(C)^*$ the associated C-bialgebra (see proposition 2.3.19).*

(1) If (R, E) is an iterative $\mathcal{D}$-ring over C with $E = (E_n \colon R \to \mathcal{D}_n(R))_{n\in\mathbb{N}}$ (see [MS09, Definition 2.2 and 2.13]), then to E there is associated canonically a D-module algebra structure $\rho \colon R \to \mathsf{Mod}_C(D, R)$ on R and the diagram



is commutative, where the vertical arrow is the isomorphism (2.3.11) from proposition 2.3.19 and the homomorphism $E \colon R \to \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R)$ is induced by the homomorphisms $E_n \colon R \to \mathcal{D}_n(R)$ (see remark 2.3.20).[10]

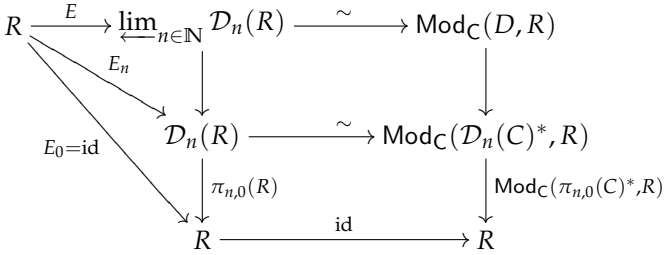
(2) Conversely, to every commutative D-module algebra (R, ρ) there is canonically associated an iterative $\mathcal{D}$-ring structure on R.

The constructions in (1) and (2) are inverse to each other.

Proof. Given an iterative $\mathcal{D}$-ring (R, E), we define $\rho \colon R \to \mathsf{Mod}_C(D, R)$ as the composition

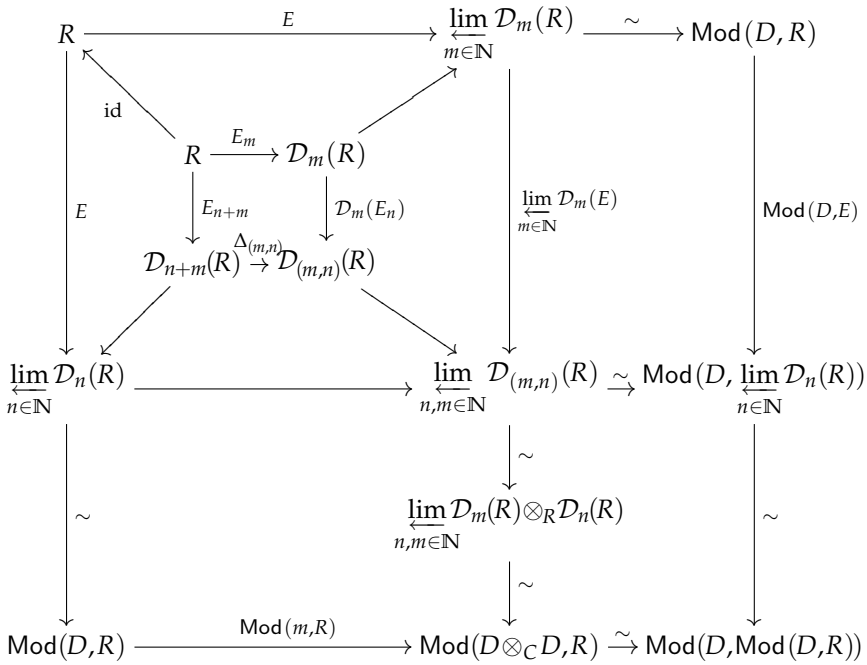
$$R \xrightarrow{E} \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R) \xrightarrow{\sim} \mathsf{Mod}_C(D, R).$$

Then the diagram



[10] By abuse of notation we use E for both, the homomorphism $R \to \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R)$ induced by the E_n and for the family $(E_n)_{n\in\mathbb{N}}$.

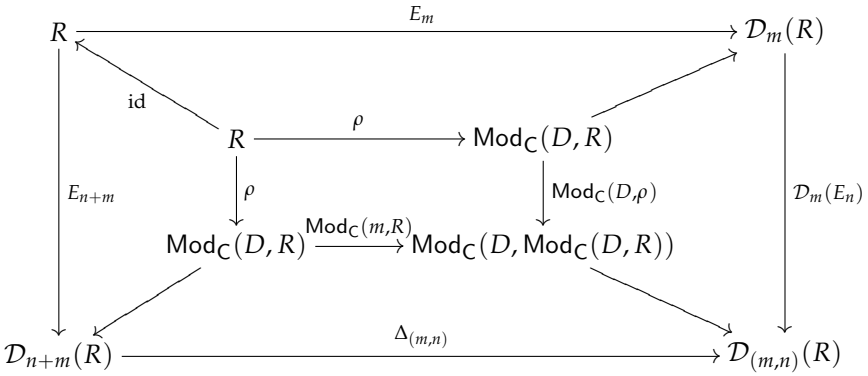
commutes. Furthermore, by the definition of the multiplication m of D, the diagram



commutes, where we denote Mod_C by Mod for short. From the commutativity of these diagrams we obtain that $\rho\colon R \to \mathsf{Mod}_C(D,R)$ is a D-module algebra structure on R.

If, conversely, $\rho\colon R \to \mathsf{Mod}_C(D,R)$ is a D-module algebra structure on R, then for every $n \in \mathbb{N}$ we define a homomorphism of C-algebras $E_n\colon R \to \mathcal{D}_n(R)$ as the composition $R \xrightarrow{\rho} \mathsf{Mod}_C(D,R) \xrightarrow{\sim} \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R) \to \mathcal{D}_n(R)$. Then by definition the maps E_n fulfill the relations $E_n = \pi_{m,n}(R) \circ E_m$ for all $m \geq n$ and $E_0 = \mathrm{ev}_{1_D} \circ \rho = \mathrm{id}_R$. Consequently, the family $E = (E_n)_{n\in\mathbb{N}}$ defines a $\mathcal{D}$-ring structure on R. Since ρ defines a D-module algebra structure,

the inner rectangle in the diagram



commutes, and thus also the outer for all $n, m \in \mathbb{N}$. This means that (R, E) is an iterative $\mathcal{D}$-ring.

Using the identification described in remark 2.3.20, we see that the passage between the iterative $\mathcal{D}$-ring structure E on R and the D-module algebra structure ρ on R is given by composition with the isomorphism $\varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R) \xrightarrow{\sim} \mathsf{Mod}_C(D, R)$ and its inverse. Therefore, the constructions in (1) and (2) are inverse to each other. □

In [MS09] the authors do not define morphisms between $\mathcal{D}$-rings over C. Though, if $\mathcal{D} = (\mathcal{D}_n)_{n\in\mathbb{N}}$ is a Hasse system over C and (R, E) and (S, F) are $\mathcal{D}$-rings, then a morphism from (R, E) and (S, F) can be defined as a homomorphism of C-algebras $\varphi\colon R \to S$ such that $\mathcal{D}_n(\varphi) \circ E_n = F_n \circ \varphi$ holds for all $n \in \mathbb{N}$. Then a homomorphism of C-algebras φ is a morphism of $\mathcal{D}$-rings if and only if the induced morphism $\varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(\varphi)\colon \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R) \to \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(S)$ fulfills $F \circ \varphi = \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(\varphi) \circ E$.

If $\mathcal{D}$ is an iterative Hasse system over C and D is the C-bialgebra associated

to $\mathcal{D}$ by proposition 2.3.19, then the diagram

$$\begin{array}{ccc} \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(R) & \xrightarrow{\sim} & \mathsf{Mod}_{\mathsf{C}}(D,R) \\ \downarrow{\scriptstyle \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(\varphi)} & & \downarrow{\scriptstyle \mathsf{Mod}_{\mathsf{C}}(D,\varphi)} \\ \varprojlim_{n\in\mathbb{N}} \mathcal{D}_n(S) & \xrightarrow{\sim} & \mathsf{Mod}_{\mathsf{C}}(D,S), \end{array}$$

commutes, where the horizontal arrows are the isomorphisms from proposition 2.3.19. So we see that there is a bijection between homomorphisms between the iterative $\mathcal{D}$-rings (R,E) and (S,F) and homomorphisms between the D-module algebras R and S. Together with proposition 2.3.21 we see that the category of $\mathcal{D}$-rings and the category of commutative D-module algebras are isomorphic.

Chapter 3

The infinitesimal Galois group

In this chapter we define a normalization $\mathcal{L}/\mathcal{K}$ for a given extension of D-module fields with certain properties. Using this normalization, we define a functor of infinitesimal deformations and the infinitesimal Galois group functor. The former turns out to be a principal homogeneous space for the infinitesimal Galois group. We also give a definition of Lie-Ritt functors and show that the infinitesimal Galois group is a Lie-Ritt functor and thus a formal group scheme.

Notation: *Let C be a commutative ring and D be a cocommutative C-bialgebra. Let L be a D-module field via $\Psi \in \mathsf{Mod}_C(D \otimes_C L, L)$ and K a D-module subfield such that the field extension L/K is separable and finitely generated*[1]*. We denote the homomorphism of D-module algebras associated to Ψ via the isomorphism (2.2.1) by $\rho\colon L \to \mathsf{Mod}_C(D, L)$. Let $\boldsymbol{u} = (u_1, \ldots, u_n)$ be a separating transcendence basis of L/K, $\theta_{\boldsymbol{u}}$ be the associated n-variate iterative derivation on L over K (see example 1.2.4) and $\Psi_{\boldsymbol{u}} \in \mathsf{Mod}_C(D_{ID^n} \otimes_C L, L)$ the corresponding D_{ID^n}-module field structure on L (see proposition 2.3.8). Furthermore, we denote the trivial D-module algebra structure on L (see lemma 2.2.15) by Ψ_0 and the homomorphism associated to Ψ_0 via the isomorphism* (2.2.1) *by ρ_0. If nothing else is mentioned, then we consider*

[1] Under these conditions a separating transcendence basis of L/K exists (see for example [Bou81, Chapitre V, §16.7, Theorem 5]).

$\mathsf{Mod}_C(D, L)$ as a D- and D_{ID^n}-module algebra with the D-module algebra structure Ψ_{int} introduced in lemma 2.2.16 and the D_{ID^n}-module algebra structure induced from $\Psi_{\boldsymbol{u}}$ on $\mathsf{Mod}_C(D, L)$ by lemma 2.2.22, which we also denote by $\Psi_{\boldsymbol{u}}$.

3.1 The rings $\mathcal{L}$ and $\mathcal{K}$ associated to L/K

In this section we define two rings, $\mathcal{L}$ and $\mathcal{K}$, which are associated to the extension of D-module fields L/K. The passage from L/K to $\mathcal{L}/\mathcal{K}$ can be interpreted as a normalization process. The motivation for this is explained in the articles [Ume06] and [Ume07].

Lemma 3.1.1. *The D_{ID^n}-module subalgebra $\rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{u}}}$ of $\mathsf{Mod}_C(D, L)$, generated by $\rho(L)$ over $\rho_0(L)$, is independent of the separating transcendence basis $\boldsymbol{u}$ of L/K.*

Proof. Let $\boldsymbol{v} = (v_1, \ldots, v_n)$ be another separating transcendence basis of L/K and $\Psi_{\boldsymbol{v}}$ be the D_{ID^n}-module algebra structure corresponding to the n-variate iterative derivation $\theta_{\boldsymbol{v}}$ on L (see example 1.2.4). We have

$$\rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{u}}} = \rho_0(L)[\Psi_{\boldsymbol{u}}(D_{ID^n} \otimes_C \rho(L))]$$

and

$$\rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{v}}} = \rho_0(L)[\Psi_{\boldsymbol{v}}(D_{ID^n} \otimes_C \rho(L))]$$

by lemma 2.2.7. Thanks to corollary 1.3.7 there exist for every $\boldsymbol{k} \in \mathbb{N}^n$ elements $c_{\boldsymbol{k},\boldsymbol{l}} \in L$ for all $\boldsymbol{l} \in \mathbb{N}^n$, almost all equal to zero, such that $\theta_{\boldsymbol{v}}^{(\boldsymbol{k})} = \sum_{\boldsymbol{l}\in\mathbb{N}^n} c_{\boldsymbol{k},\boldsymbol{l}}\theta_{\boldsymbol{u}}^{(\boldsymbol{l})}$. Therefore, we obtain $\rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{v}}} = \rho_0(L)[\Psi_{\boldsymbol{v}}(D_{ID^n} \otimes \rho(L))] \subseteq \rho_0(L)[\Psi_{\boldsymbol{u}}(D_{ID^n} \otimes \rho(L))] = \rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{u}}}$. By symmetry, the claim follows. □

Definition 3.1.2. *We define $\mathcal{K}$ as the subalgebra $\rho_0(L)[\rho(K)]$ of $\mathsf{Mod}_C(D, L)$, generated by $\rho_0(L)$ and $\rho(K)$, and $\mathcal{L}$ as the D_{ID^n}-module subalgebra $\rho_0(L)\{\rho(L)\}_{\Psi_{\boldsymbol{u}}}$ of $\mathsf{Mod}_C(D, L)$, generated by $\rho_0(L)$ and $\rho(L)$.*

Lemma 3.1.3. *The L-algebras $\mathcal{K}$ and $\mathcal{L}$ are $D \otimes_C D_{ID^n}$-module subalgebras of* $\mathsf{Mod}_{\mathsf{C}}(D,L)$.

Proof. Since K is a D-module subfield of L, the image $\rho(K)$ of K under the homomorphism of D-module algebras $\rho\colon (L,\Psi) \to (\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{int})$ is a D-module subalgebra of $(\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{int})$. The image $\rho_0(L)$ of L under the homomorphism ρ_0 is a D-module subalgebra of $(\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{int})$, since it consists of constants. Since the elements of K are constant with respect to $\Psi_{\boldsymbol{u}}$ and K is a D-module subfield of L, the image $\rho(K)$ consists of constants with respect to $\Psi_{\boldsymbol{u}}$ and is thus a D_{ID^n}-module subalgebra of $(\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{\boldsymbol{u}})$. By lemma 2.2.24, the image $\rho_0(L)$ is a D_{ID^n}-module subalgebra of $(\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{\boldsymbol{u}})$. Since $D \otimes_C D_{ID^n}$ measures $\mathsf{Mod}_{\mathsf{C}}(D,L)$ to itself, we see that $\mathcal{K}$ is a $D \otimes_C D_{ID^n}$-module subalgebra of $\mathsf{Mod}_{\mathsf{C}}(D,L)$. Furthermore, it is clear that the C-subalgebra of $\mathsf{Mod}_{\mathsf{C}}(D,L)$ generated by $\Psi_{\boldsymbol{u}}(D_{ID^n} \otimes_C \rho(L))$ is a D_{ID^n}-module subalgebra and it is also a D-module subalgebra by lemma 2.2.23. Therefore, $\mathcal{L}$ is also a $D \otimes_C D_{ID^n}$-module subalgebra of $\mathsf{Mod}_{\mathsf{C}}(D,L)$, since $D \otimes_C D_{ID^n}$ measures $\mathsf{Mod}_{\mathsf{C}}(D,L)$ to itself. □

Lemma 3.1.4. *The subalgebras $\rho_0(L)$ and $\rho(K)$ of $\mathcal{K}$ are linearly disjoint over $\rho_0(K^\Psi)$ and the multiplication homomorphisms of $\mathcal{K}$ induces an isomorphism of $D \otimes_C D_{ID^n}$-module algebras*

$$\rho_0(L) \otimes_{\rho_0(K^\Psi)} \rho(K) \to \mathcal{K}.$$

Proof. We consider the extension of D-module algebras $\rho(K) \subseteq \mathcal{K}$. Corollary 2.2.31 implies that the multiplication homomorphism

$$\rho(K) \otimes_{\rho_0(K^\Psi)} \mathcal{K}^{\Psi_{int}} \to \mathcal{K}$$

is injective. Since $\mathcal{K}^{\Psi_{int}} = \rho_0(L)$ by lemma 2.2.16, we obtain the injection

$$\rho(K) \otimes_{\rho_0(K^\Psi)} \rho_0(L) \to \mathcal{K}, \tag{3.1.1}$$

which is surjective by definition of $\mathcal{K}$. We note that in the tensor product $\rho(K) \otimes_{\rho_0(K^\Psi)} \rho_0(L)$ the left factor consists of constants with respect to $\Psi_{\boldsymbol{u}}$, and the right, with respect to Ψ_{int}. Both factors are $D \otimes_C D_{ID^n}$-module algebras. Obviously (3.1.1) is a homomorphism of $D \otimes_C D_{ID^n}$-module algebras. □

3.2 Lie-Ritt functors

Lie-Ritt functors have been introduced by H. Umemura in [Ume96a]. The infinitesimal Galois group that we define below turns out to be a Lie-Ritt functor, like those defined by H. Umemura and S. Morikawa. Since we do not restrict the characteristic to be zero, we have to adapt the definition of H. Umemura by using iterative derivations instead of classical derivations. We state some basic properties of Lie-Ritt functors, most of which are stated in [Ume96a]. For the sake of simplicity, proofs there are sometimes just given in the case $n = 1$, so we include complete proofs here.

Definition 3.2.1. *Let A be a commutative ring and $n \in \mathbb{N}$. We define the set of all infinitesimal coordinate transformations of n variables over A as*

$$\Gamma_n(A) := \{\Phi = (\varphi_i)_{i=1,\dots,n} \in (A[\![\boldsymbol{x}]\!])^n \mid \varphi_i \equiv x_i \mod N(A)[\![\boldsymbol{x}]\!] \ \forall\, i = 1,\dots,n\},$$

where we denote $(x_1,\dots,x_n)$ by $\boldsymbol{x}$.

In the following we show that $\Gamma_n(A)$ carries a group structure.

Lemma 3.2.2. *Let A be a commutative ring. For elements $\Phi = (\varphi_1,\dots,\varphi_n)$ and $\Psi = (\psi_1,\dots,\psi_n)$ in $\Gamma_n(A)$ the composition $\Phi \circ \Psi = (\varphi_1(\Psi),\dots,\varphi_n(\Psi))$ is well defined and an element of $\Gamma_n(A)$.*

Proof. Since $\Psi(\mathbf{0})$ and $\Phi(\mathbf{0})$ are both elements of $N(A)^n$, the elements ψ_i and φ_i are topologically nilpotent in $A[\![\boldsymbol{x}]\!]$ for $i = 1,\dots,n$ (see [Bou81, Chapter IV, §4.2, Corollary]). Thus, by [Bou81, Chapter IV, §4.3, Proposition 4], Ψ and Φ define homomorphisms

$$A[\![\boldsymbol{x}]\!] \to A[\![\boldsymbol{x}]\!], \quad x_i \mapsto \psi_i(\boldsymbol{x}) \quad \text{and} \quad A[\![\boldsymbol{x}]\!] \to A[\![\boldsymbol{x}]\!], \quad x_i \mapsto \varphi_i(\boldsymbol{x}),$$

respectively, which are continuous with respect to the $(\boldsymbol{x})$-adic topology and are congruent to the identity modulo $N(A)[\![\boldsymbol{x}]\!]$. Therefore, their composition, sending x_i to $\varphi_i(\Psi)$ for $i = 1, \ldots, n$, is also a continous homomorphism of A-algebras, which is congruent to the identity modulo $N(A)[\![\boldsymbol{x}]\!]$. In particular, $\varphi_i(\Psi)$ is well defined and congruent to x_i modulo $N(A)[\![\boldsymbol{x}]\!]$ for $i = 1, \ldots, n$. □

Lemma 3.2.3. *Let A be a commutative ring and $n \in \mathbb{N}$. Then for all $\Phi, \Psi, \Theta \in \Gamma_n(A)$ we have $\Phi \circ (\Psi \circ \Theta) = (\Phi \circ \Psi) \circ \Theta$.*

Proof. See [Bou81, Chapter IV, §4, 3.]. □

We often make use of the following well-known fact, which we recall for the reader's convenience.

Lemma 3.2.4. *Let A be a commutative ring, $u \in A^\times$ a unit and $a \in A$ such that $a \equiv u \mod N(A)$, then a is also a unit in A.*

Proof. There exists an $m \in \mathbb{N}$ such that $(a-u)^m = 0$. Therefore,

$$0 = \sum_{i=0}^{m} \binom{m}{i} a^i (-u)^{m-i} = (-u)^m + a \left(\sum_{i=1}^{m} a^{i-1} (-u)^{m-i} \right)$$

and we see that a is invertible in A. □

The following lemma is similar to proposition 1.3.5. It is a restricted, but also refined version of the formal inverse function theorem.

Lemma 3.2.5. *For any commutative ring A and any $\Phi \in \Gamma_n(A)$ there exists $\Psi \in \Gamma_n(A)$ such that $\Psi \circ \Phi(\boldsymbol{x}) = \boldsymbol{x}$.*

Proof. Writing

$$\Phi(\boldsymbol{x}) = (\varphi_1(\boldsymbol{x}), \ldots, \varphi_n(\boldsymbol{x})) = \left(\sum_{\boldsymbol{k} \in \mathbb{N}^n} a_{1,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}, \ldots, \sum_{\boldsymbol{k} \in \mathbb{N}^n} a_{n,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \right)$$

we see that $(x_1 - a_{1,\boldsymbol{0}}, \ldots, x_n - a_{n,\boldsymbol{0}}) \circ \Phi = (\sum_{\boldsymbol{k}>\boldsymbol{0}} a_{1,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}, \ldots, \sum_{\boldsymbol{k}>\boldsymbol{0}} a_{n,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}})$, and so by lemma 3.2.3 we can assume that $a_{i,\boldsymbol{0}} = 0$ for $i = 1, \ldots, n$. Since $a_{i,\boldsymbol{\delta}_j} \equiv \delta_{i,j}$

mod $N(A)$ for $i,j=1,\dots,n$ we have $\det((a_{i,\delta_j})_{i,j=1}^n) \equiv 1 \mod N(A)$ and thus $\det((a_{i,\delta_j})_{i,j=1}^n) \in A^\times$. We are looking for an element

$$\Psi = (\psi_1,\dots,\psi_n) = \left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} c_{1,\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}},\dots,\sum_{\boldsymbol{k}\in\mathbb{N}^n} c_{n,\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}\right) \in \Gamma_n(A)$$

such that for all $\lambda = 1,\dots,n$

$$\sum_{\boldsymbol{l}\in\mathbb{N}^n} c_{\lambda,\boldsymbol{l}} \prod_{\mu=1}^{n} \left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{\mu,\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}\right)^{l_\mu} = x_\lambda. \tag{3.2.1}$$

This is equivalent to the following system of linear equations in the unknowns $\{c_{\lambda,\boldsymbol{l}} \mid \boldsymbol{l}\in\mathbb{N}^n\}$

$$\sum_{\boldsymbol{l}\in\mathbb{N}^n} c_{\lambda,\boldsymbol{l}} \sum_{\boldsymbol{k}_{1,1}+\dots,\boldsymbol{k}_{1,l_1}+\dots+\boldsymbol{k}_{n,1}+\dots+\boldsymbol{k}_{n,l_n}=\boldsymbol{i}} \prod_{\mu=1}^{n}\prod_{\nu=1}^{l_\mu} a_{\mu,\boldsymbol{k}_{\mu,\nu}} = \begin{cases} 1 & \text{if } \boldsymbol{i}=\boldsymbol{\delta}_\lambda, \\ 0 & \text{otherwise} \end{cases} \tag{3.2.2}$$

for all $\boldsymbol{i}\in\mathbb{N}^n$ and all $\lambda\in\{1,\dots,n\}$. Note that in this sum only terms with $|\boldsymbol{l}| \le |\boldsymbol{i}|$ occur, since if $|\boldsymbol{l}| > |\boldsymbol{i}|$ then in the decomposition $\boldsymbol{k}_{1,1}+\dots+\boldsymbol{k}_{1,l_1}+\dots+\boldsymbol{k}_{n,1}+\dots+\boldsymbol{k}_{n,l_n}$ of $\boldsymbol{i}$ at least one $\boldsymbol{k}_{\mu,\nu}$ must be zero and $a_{\mu,\boldsymbol{0}}$ was assumed to be zero. Therefore, we can construct a solution for (3.2.1) by solving by induction on κ the equations (3.2.2) in the unknowns $\{c_{\lambda,\boldsymbol{l}} \mid |\boldsymbol{l}| = \kappa\}$ for all $\boldsymbol{i}$ with $|\boldsymbol{i}| = \kappa$ and all $\lambda\in\{1,\dots,n\}$. From (3.2.2) for $\boldsymbol{i}=\boldsymbol{0}$ we obtain $c_{\lambda,\boldsymbol{0}} = 0$ for all $\lambda = 1,\dots,n$. By induction we assume that for some κ the elements $(c_{\lambda,\boldsymbol{l}})_{|\boldsymbol{l}|<\kappa,\lambda=1,\dots,n}$ are solutions of (3.2.2) for $|\boldsymbol{i}| < \kappa$. We have to solve the equations (3.2.2) for all $\boldsymbol{i}$ with $|\boldsymbol{i}| = \kappa$ in the unknowns $c_{\lambda,\boldsymbol{l}}$ with $|\boldsymbol{l}| = \kappa$ and $\lambda\in\{1,\dots,n\}$. This is a system of linear equations with coefficient matrix $D = (D_{\boldsymbol{i},\boldsymbol{l}})_{|\boldsymbol{i}|=|\boldsymbol{l}|=\kappa}$ given by $D_{\boldsymbol{i},\boldsymbol{l}} = \sum_{\boldsymbol{k}_{1,1}+\dots+\boldsymbol{k}_{1,l_1}+\dots+\boldsymbol{k}_{n,1}+\dots+\boldsymbol{k}_{n,l_n}=\boldsymbol{i}} \prod_{\mu=1}^{n}\prod_{\nu=1}^{l_\mu} a_{\mu,\boldsymbol{k}_{\mu,\nu}}$ for all $\boldsymbol{i},\boldsymbol{l}\in\mathbb{N}^n$ with $|\boldsymbol{i}| = |\boldsymbol{l}| = \kappa$. Since

$$a_{\mu,\boldsymbol{k}_{\mu,\nu}} \equiv \begin{cases} 1 \mod N(A) & \text{if } \boldsymbol{k}_{\mu,\nu} = \boldsymbol{\delta}_\mu \\ 0 \mod N(A) & \text{otherwise,} \end{cases}$$

we have $D_{\boldsymbol{i},\boldsymbol{l}} \equiv \delta_{\boldsymbol{i},\boldsymbol{l}} \mod N(A)$ for all $\boldsymbol{i},\boldsymbol{l}\in\mathbb{N}^n$ with $|\boldsymbol{i}| = |\boldsymbol{l}| = \kappa$. So $\det\left((D_{\boldsymbol{i},\boldsymbol{l}})_{|\boldsymbol{i}|=|\boldsymbol{l}|=\kappa}\right) \equiv 1 \mod N(A)$ and thus $\det(D)\in A^\times$, i.e. $D\in \mathrm{GL}_n(A)$.

So we can uniquely solve this system of linear equations and obtain by induction on κ a solution for (3.2.1). □

Proposition 3.2.6. *Let A be a commutative ring and $n \in \mathbb{N}$. Then the set $\Gamma_n(A)$ carries a group structure with composition given by*

$$\Psi \circ \Phi = (\psi_i(\varphi_1, \dots, \varphi_n))_{i=1,\dots,n} \tag{3.2.3}$$

for elements $\Psi = (\psi_i)_{i=1,\dots,n}$ and $\Phi = (\varphi_i)_{i=1,\dots,n}$ of $\Gamma_n(A)$ and identity element $\boldsymbol{x} \in \Gamma_n(A) \subseteq (A[\![\boldsymbol{x}]\!])^n$.

Proof. By lemma 3.2.2, equation (3.2.3) defines a composition law on $\Gamma_n(A)$. Since $\boldsymbol{x} \circ \Phi = \Phi = \Phi \circ \boldsymbol{x}$, the tuple $\boldsymbol{x}$ is a left- and right-unit and the lemmas 3.2.3 and 3.2.5 show that this composition law is associative and has left inverses. Since the left inverses are also right inverses, the composition law (3.2.6) makes $\Gamma_n(A)$ into a group. □

Definition 3.2.7. *Let R be a commutative ring and $n \in \mathbb{N}$. We define the* Lie-Ritt functor of all infinitesimal transformations of n variables defined over R *as the functor*

$$\boldsymbol{\Gamma}_{nR} \colon \mathsf{CAlg}_R \to \mathsf{Grp},$$

that has $\Gamma_n(A)$ as A-points for every commutative R-algebra A and for every homomorphism $\varphi \colon A \to B$ of commutative R-algebras we define $\boldsymbol{\Gamma}_{nR}(\varphi) \colon \boldsymbol{\Gamma}_{nR}(A) \to \boldsymbol{\Gamma}_{nR}(B)$ to be the map induced by $(\varphi[\![\boldsymbol{w}]\!])^n \colon (A[\![\boldsymbol{w}]\!])^n \to (B[\![\boldsymbol{w}]\!])^n$.

Let R be a commutative ring and A a commutative R-algebra. We equip the ring $A[\![\boldsymbol{x}]\!] \coloneqq A[\![x_1, \dots, x_n]\!]$ with the n-variate iterative derivation $\theta \colon A[\![\boldsymbol{x}]\!] \to A[\![\boldsymbol{x}]\!][\![\boldsymbol{w}]\!]$ over A defined by

$$\theta\left(\sum_{j \in \mathbb{N}^n} a_j \boldsymbol{x}^j\right) \coloneqq \sum_{k,j \in \mathbb{N}^n} \binom{j}{k} a_j \boldsymbol{x}^{j-k} \boldsymbol{w}^k$$

for all $\sum_{j \in \mathbb{N}^n} a_j \boldsymbol{x}^j \in A[\![\boldsymbol{x}]\!]$ (see example 1.2.5). We extend it to

$$A[\![\boldsymbol{x}]\!]\{\boldsymbol{y}\} \coloneqq A[\![x_1, \dots, x_n]\!][y_i^{(k)} \mid i = 1, \dots, n, \boldsymbol{k} \in \mathbb{N}^n]$$

and finally to the completion

$$A[\![\boldsymbol{x}]\!]\{\{\boldsymbol{y}\}\} \coloneqq A[\![x_1,\dots,x_n]\!][\![y_i^{(\boldsymbol{k})} \mid i=1,\dots,n,\boldsymbol{k}\in\mathbb{N}^n]\!].$$

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

$$\theta\left(y_i^{(\boldsymbol{k})}\right) \coloneqq \sum_{\boldsymbol{l}\in\mathbb{N}^n}\binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}} y_i^{(\boldsymbol{k}+\boldsymbol{l})}\boldsymbol{w}^{\boldsymbol{l}}.$$

We denote by $A[\![\boldsymbol{x}]\!]\{A[\![\boldsymbol{y}]\!]\}$ the HD-subring of $A[\![\boldsymbol{x}]\!]\{\{\boldsymbol{y}\}\}$ generated by $A[\![\boldsymbol{x},\boldsymbol{y}]\!]$. For $F\in A[\![\boldsymbol{x}]\!]\{A[\![\boldsymbol{y}]\!]\}$ and $\Phi=(\varphi_1,\dots,\varphi_n)\in\boldsymbol{\Gamma}_{nR}(A)\subseteq A[\![\boldsymbol{x}]\!]^n$ we define $F_{|\boldsymbol{y}=\Phi}$ by replacing $y_i^{(\boldsymbol{k})}$ in F with $\theta^{(\boldsymbol{k})}(\varphi_i)$, i.e. if

$$F=\sum_{\substack{j\in\mathbb{N}^n\\ \boldsymbol{k}\in\mathbb{N}^{\{1,\dots,n\}\times\mathbb{N}^n}}} a_{j,\boldsymbol{k}}\boldsymbol{x}^j \prod_{(i,\boldsymbol{l})\in\{1,\dots,n\}\times\mathbb{N}^n}\left(y_i^{(\boldsymbol{l})}\right)^{\boldsymbol{k}(i,\boldsymbol{l})}\in A[\![\boldsymbol{x}]\!]\{A[\![\boldsymbol{y}]\!]\}$$

then

$$F_{|\boldsymbol{y}=\Phi}=\sum_{\substack{j\in\mathbb{N}^n\\ \boldsymbol{k}\in\mathbb{N}^{\{1,\dots,n\}\times\mathbb{N}^n}}} a_{j,\boldsymbol{k}}\boldsymbol{x}^j \prod_{(i,\boldsymbol{l})\in\{1,\dots,n\}\times\mathbb{N}^n}\left(\theta^{(\boldsymbol{l})}(\varphi_i)\right)^{\boldsymbol{k}(i,\boldsymbol{l})}\in A[\![\boldsymbol{x}]\!]. \tag{3.2.4}$$

Definition 3.2.8. *Let R be a commutative ring. A* Lie-Ritt functor *over R is a group functor G on the category CAlg_R isomorphic to a subfunctor of $\boldsymbol{\Gamma}_{nR}$ for some $n\in\mathbb{N}$ that is defined by a HD-ideal of $R[\![\boldsymbol{x}]\!]\{R[\![\boldsymbol{y}]\!]\}$, i.e. there is a HD-ideal $I\trianglelefteq R[\![\boldsymbol{x}]\!]\{R[\![\boldsymbol{y}]\!]\}$ such that $G(A)\cong Z(I)(A)$, where $Z(I)$ is defined by*

$$Z(I)(A)\coloneqq\{\Phi\in\boldsymbol{\Gamma}_{nR}(A)\mid F_{|\boldsymbol{y}=\Phi}=0\ \forall\ F\in I_A\}$$

for all commutative R-algebras A, where I_A denotes the HD-ideal generated by I in $A[\![\boldsymbol{x}]\!]\{A[\![\boldsymbol{y}]\!]\}$.[2]

Example 3.2.9. *We define a subgroup functor G_+ of $\boldsymbol{\Gamma}_{1\mathbb{Z}}$ as*

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

[2] In [Ume96a] Lie-Ritt functors over R are defined using ideals in $R[\![\boldsymbol{x}]\!]\{\{\boldsymbol{y}\}\}$. Since the term in (3.2.4) is not well defined for elements $F\in R[\![\boldsymbol{x}]\!]\{\{\boldsymbol{y}\}\}$ in general, we change the definition.

for all commutative rings A. Let I be the HD-ideal in $\mathbb{Z}[\![x]\!]\{\mathbb{Z}[\![y]\!]\}$ generated by $y^{(1)} - 1$ and $y^{(k)}$ for all $k \geq 2$. Then G_+ is the Lie-Ritt functor over $\mathbb{Z}$ defined by the ideal I. Furthermore, G_+ is isomorphic to $\hat{\mathbb{G}}_a$ (see example B.2.5).

Proof. If A is a commutative ring and $\varphi(x) = \sum_{i\geq 0} a_i x^i \in Z(I)(A)$, then $1 = \theta^{(1)}(\varphi) = \sum_{i\geq 1} a_i i x^{i-1}$, and thus $a_1 = 1$. For all $k \geq 2$ the ideal I contains $y^{(k)}$. So we obtain $0 = \theta^{(k)}(\varphi) = \sum_{i\geq k} \binom{i}{k} a_i x^{i-k}$ and thus $a_k = 0$. Since there are no restrictions on $a_0 \in N(A)$, the claim follows. □

The analog of this example in the setting of H. Umemura appeared in [Ume96a, Example 1.9 (i)]. Since he works over $\mathbb{Q}$, it is sufficient to consider the equation $y^{(1)} - 1$. In the general case we have to add the equations $y^{(k)}$ for $k > 2$.

Similarly, the result corresponding to the following proposition in the setting of H. Umemura (which means in particular that the characteristic is zero) can be found in [Ume96a, p. 71].

Proposition 3.2.10. *Let R be a commutative ring and $n \in \mathbb{N}$. Given an n-dimensional formal group law F over R, the associated group functor $\mathbf{F}$ (see remark B.2.4) is isomorphic to the Lie-Ritt functor $Z(I) \subseteq \mathbf{\Gamma}_{nR}$ defined by the HD-ideal*

$$I := [\theta^{(\boldsymbol{k})}(F(\boldsymbol{y}, \Psi(\boldsymbol{x}))) \mid \boldsymbol{k} \in \mathbb{N}^n \setminus \{\mathbf{0}\}]_{R[\![\boldsymbol{x}]\!]\{R[\![\boldsymbol{y}]\!]\}}, \tag{3.2.5}$$

where Ψ is as in lemma B.2.3.

Proof. Let A be a commutative R-algebra and $\Phi \in \mathbf{\Gamma}_{nR}(A)$. If $H_{|\boldsymbol{y}=\Phi} = 0$ for all $H \in I_A$, then we have in particular for all $\boldsymbol{k} \in \mathbb{N}^n \setminus \{\mathbf{0}\}$

$$\theta^{(\boldsymbol{k})}(F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x}))) = \left(\theta^{(\boldsymbol{k})}(F(\boldsymbol{y}, \Psi(\boldsymbol{x})))\right)_{|\boldsymbol{y}=\Phi(\boldsymbol{x})} = \mathbf{0}.$$

This implies that there exists an $\boldsymbol{a} \in A^n$ such that

$$F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x})) = \boldsymbol{a}.$$

Since

$$\boldsymbol{a} = F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x})) \equiv F(\boldsymbol{x}, \Psi(\boldsymbol{x})) = \mathbf{0} \mod N(A)[\![\boldsymbol{x}]\!],$$

it follows $\boldsymbol{a} \in N(A)^n$. Thus, we obtain a map $\pi : Z(I)(A) \to N(A)^n$ by sending Φ to $\boldsymbol{a}$.

Conversely, for $\boldsymbol{a} \in N(A)^n$ we define $\Phi(\boldsymbol{x}) := F(\boldsymbol{a}, \boldsymbol{x})$. Then $\Phi(\boldsymbol{x}) = F(\boldsymbol{a}, \boldsymbol{x}) \equiv F(\boldsymbol{0}, \boldsymbol{x}) = \boldsymbol{x} \mod N(A)[\![\boldsymbol{x}]\!]$, i.e. $\Phi \in \boldsymbol{\Gamma}_{nR}(A)$ and we have

$$F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x})) = F(F(\boldsymbol{a}, \boldsymbol{x}), \Psi(\boldsymbol{x})) = F(\boldsymbol{a}, F(\boldsymbol{x}, \Psi(\boldsymbol{x}))) = F(\boldsymbol{a}, \boldsymbol{0}) = \boldsymbol{a}.$$

It follows $(\theta^{(\boldsymbol{k})}(F(\boldsymbol{y}, \Psi(\boldsymbol{x}))))_{|\boldsymbol{y}=\Phi(\boldsymbol{x})} = \theta^{(\boldsymbol{k})}(F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x}))) = \boldsymbol{0}$ for all $\boldsymbol{k} \in \mathbb{N}^n \setminus \{\boldsymbol{0}\}$ and thus also $H(\Phi(\boldsymbol{x})) = \boldsymbol{0}$ for all $H \in I_A$. Consequently, we obtain a map $N(A)^n \to Z(I)(A)$ that sends $\boldsymbol{a} \in N(A)^n$ to Φ.

Since $F(F(\boldsymbol{a}, \boldsymbol{x}), \Psi(\boldsymbol{x})) = F(\boldsymbol{a}, F(\boldsymbol{x}, \Psi(\boldsymbol{x}))) = F(\boldsymbol{a}, \boldsymbol{0}) = \boldsymbol{a}$ for all $\boldsymbol{a} \in N(A)^n$ and $F(F(\Phi(\boldsymbol{x}), \Psi(\boldsymbol{x})), \boldsymbol{x}) = F(\Phi(\boldsymbol{x}), F(\Psi(\boldsymbol{x}), \boldsymbol{x})) = F(\Phi(\boldsymbol{x}), \boldsymbol{0}) = \Phi(\boldsymbol{x})$ for all $\Phi(\boldsymbol{x}) \in \boldsymbol{\Gamma}_{nR}(A)$, this map is inverse to π and we obtain a bijection $N(A) \cong Z(I)(A)$.

Finally, π is a group homomorphism: For $\Phi_1, \Phi_2 \in Z(I)(A)$ there are $\boldsymbol{a}_i \in N(A)^n$ such that $F(\Phi_i, \Psi) = \boldsymbol{a}_i$ and thus $\Phi_i(\boldsymbol{x}) = F(\boldsymbol{a}_i, \boldsymbol{x})$ for $i = 1, 2$. Consequently, we obtain $(\Phi_1 \circ \Phi_2)(\boldsymbol{x}) = F(\boldsymbol{a}_1, F(\boldsymbol{a}_2, \boldsymbol{x})) = F(F(\boldsymbol{a}_1, \boldsymbol{a}_2), \boldsymbol{x})$, i.e. $\pi(\Phi_1 \circ \Phi_2) = F(\boldsymbol{a}_1, \boldsymbol{a}_2)$. □

It is easy to see that in the case of example 3.2.9 the generators of the ideal I in (3.2.5) are exactly $y^{(1)} - 1$ and $y^{(k)}$ for $k > 1$.

Proposition 3.2.11. *Every Lie-Ritt functor over a commutative ring R is isomorphic to a formal group scheme over R.*

Proof. First, we consider the Lie-Ritt functor $\boldsymbol{\Gamma}_{nR}$ of all infinitesimal transformations of n variables defined over R. For every commutative R-algebra A we have an isomorphism

$$\boldsymbol{\Gamma}_{nR}(A) \to \widehat{\mathbb{A}}_R^{\{1,\dots,n\}\times\mathbb{N}^n}(A), \quad \left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} a_{i,\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}\right)_{i=1,\dots,n} \mapsto \left(a_{i,\boldsymbol{k}} - \delta_{\boldsymbol{k},\delta_i}\right)_{(i,\boldsymbol{k})\in\{1,\dots,n\}\times\mathbb{N}^n}$$

so that $\boldsymbol{\Gamma}_{nR}$ is isomorphic to the formal scheme $\widehat{\mathbb{A}}_R^{\{1,\dots,n\}\times\mathbb{N}^n}$.

Let A be a commutative R-algebra and let $\Psi = (\psi_1, \dots, \psi_n)$ and $\Phi = (\varphi_1, \dots, \varphi_n)$ be elements of $\mathbf{\Gamma}_{nR}(A)$. We write $\varphi_i = \sum_{\boldsymbol{k} \in \mathbb{N}^n} a_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ and $\psi_i = \sum_{\boldsymbol{k} \in \mathbb{N}^n} b_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ for all $i \in \{1, \dots, n\}$. Then for all $\boldsymbol{l} \in \mathbb{N}^n$ the coefficient of $\boldsymbol{x}^{\boldsymbol{l}}$ in $\psi_i(\Phi)$ is

$$\sum_{\boldsymbol{k} \in \mathbb{N}^n} b_{i,\boldsymbol{k}} \sum_{\substack{\boldsymbol{l}_{1,1}, \dots, \boldsymbol{l}_{1,k_1}, \dots, \boldsymbol{l}_{n,1}, \dots, \boldsymbol{l}_{n,k_n} \in \mathbb{N}^n \\ \sum_{\mu=1}^{n} \sum_{\nu=1}^{k_\mu} \boldsymbol{l}_{\mu,\nu} = \boldsymbol{l}}} \prod_{\mu=1}^{n} \prod_{\nu=1}^{k_\mu} a_{\mu, \boldsymbol{l}_{\mu,\nu}}$$

Thus, there exist formal power series $(f_{i,\boldsymbol{l}})_{i \in \{1,\dots,n\}, \boldsymbol{l} \in \mathbb{N}^n}$ in variables $u_{j,\boldsymbol{k}}, v_{j,\boldsymbol{k}}$ with $j \in \{1, \dots, n\}$ and $\boldsymbol{k} \in \mathbb{N}^n$, coefficients in $\mathbb{Z}$ and constant term equal to zero such that $\psi_i(\Phi) = \sum_{\boldsymbol{l} \in \mathbb{N}^n} f_{i,\boldsymbol{l}}((a_{j,\boldsymbol{k}}, b_{j,\boldsymbol{k}})_{(j,\boldsymbol{k}) \in \{1,\dots,n\} \times \mathbb{N}^n}) \boldsymbol{x}^{\boldsymbol{l}}$. The formal power series $(f_{i,\boldsymbol{l}})_{(i,\boldsymbol{l}) \in \{1,\dots,n\} \times \mathbb{N}^n}$ give rise to a morphism $\widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n} \times \widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n} \to \widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n}$ of formal schemes over R, which defines a group law on $\widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n}$ such that $\widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n}$ becomes a formal group scheme over R. Then by construction the group functor $\mathbf{\Gamma}_{nR}$ is isomorphic to the formal group scheme $\widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n}$.

Now let $G \subseteq \mathbf{\Gamma}_{nR}$ be an arbitrary Lie-Ritt functor over R and $I \trianglelefteq R[\![\boldsymbol{x}]\!]\{R[\![\boldsymbol{y}]\!]\}$ be such that $G(A) \cong Z(I)(A)$ for all commutative R-algebras A. Let $\Phi = (\varphi_1, \dots, \varphi_n) \in \mathbf{\Gamma}_{nR}(A)$ and $\varphi_i = \sum_{\boldsymbol{k} \in \mathbb{N}^n} a_{i,\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ 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 $\widehat{\mathbb{A}}_R^{\{1,\dots,n\} \times \mathbb{N}^n}$ defined by the polynomials h_λ for all $h \in I$ and $\lambda \in \Lambda_h$. □

3.3 The functor $\mathcal{F}_{L/K}$ of infinitesimal deformations

In the following we often consider subalgebras of the completed tensor product

$$\mathsf{Mod}_{\mathsf{C}}(D, L) \hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

for commutative L-algebras A. If not mentioned otherwise, the L-algebra structure on $\mathsf{Mod}_{\mathsf{C}}(D, L)$ is given by $\rho_0 \colon L \to \mathsf{Mod}_{\mathsf{C}}(D, L)$ and the one on

$A[\![\boldsymbol{w}]\!]$ is given by the composition of $\theta_{\boldsymbol{u}}\colon L \to L[\![\boldsymbol{w}]\!]$ and $L[\![\boldsymbol{w}]\!] \to A[\![\boldsymbol{w}]\!]$ and the completion is with respect to the topology on the tensor product induced by the discrete topology on $\mathsf{Mod}_{\mathsf{C}}(D,L)$ and the $(\boldsymbol{w})$-adic topology on $A[\![\boldsymbol{w}]\!]$ (see proposition A.2.1).

Lemma 3.3.1. *Let A be a commutative L-algebra.*

(1) There exists a D-module algebra structure on the completed tensor product $\mathsf{Mod}_{\mathsf{C}}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ induced by the D-module algebra structure on the tensor product $\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!]$ that is induced by

$$(\mathsf{Mod}_{\mathsf{C}}(D,L),\Psi_{int}) \xleftarrow{\rho_0} (L,\Psi_0) \xrightarrow{\theta_{\boldsymbol{u}}} (A[\![\boldsymbol{w}]\!],\Psi_0) \tag{3.3.1}$$

via proposition 2.2.25.

(2) There exists a D_{ID^n}-module algebra structure on the completed tensor product $\mathsf{Mod}_{\mathsf{C}}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ induced by the D_{ID^n}-module algebra structure on the tensor product $\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!]$ that is induced by

$$(\mathsf{Mod}_{\mathsf{C}}(D,L),\mathsf{Mod}_{\mathsf{C}}(D,\theta_{\boldsymbol{u}})) \xleftarrow{\rho_0} (L,\theta_{\boldsymbol{u}}) \xrightarrow{\theta_{\boldsymbol{u}}} (A[\![\boldsymbol{w}]\!],\theta_{\boldsymbol{w}}) \tag{3.3.2}$$

via proposition 2.2.25.

These D- and D_{ID^n}-module algebra structures commute with each other so that we obtain a $D\otimes_C D_{ID^n}$-module algebra structure on $\mathsf{Mod}_{\mathsf{C}}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$.

Proof. By proposition 2.2.25, there is a unique D-module algebra structure on $\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!]$ such that this tensor product becomes the coproduct of the diagram (3.3.1) in the category of commutative D-module algebras. The ideals in $\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!]$ generated by $(1\otimes \boldsymbol{w}^{\boldsymbol{k}})$ for $\boldsymbol{k}\in\mathbb{N}^n$ are D-stable and thus $((\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!])/(1\otimes \boldsymbol{w}^{\boldsymbol{k}}))_{\boldsymbol{k}\in\mathbb{N}^n}$ forms an inverse system of D-module algebras. By proposition 2.2.26, the inverse limit

$$\mathsf{Mod}_{\mathsf{C}}(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!] = \varprojlim_{\boldsymbol{k}\in\mathbb{N}^n} (\mathsf{Mod}_{\mathsf{C}}(D,L)\otimes_L A[\![\boldsymbol{w}]\!])/(1\otimes \boldsymbol{w}^{\boldsymbol{k}})$$

becomes a D-module algebra.

The proof of the second part is similar using the fact that continuous n-variate iterative derivations extend to completions (see proposition 1.2.8).

It is clear the the D- and D_{ID^n}-module algebra structures commute with each other. □

Lemma 3.3.2. *For any commutative L-algebra A there exists an injective homomorphism of $D \otimes_C D_{ID^n}$-module algebras*

$$\mu_{A,\boldsymbol{u}} \colon \mathsf{Mod}_C(D,L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \to \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!]) \tag{3.3.3}$$
$$\sum_{\boldsymbol{i}\in\mathbb{N}^n} f_{\boldsymbol{i}} \otimes a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}} \mapsto \sum_{\boldsymbol{i}\in\mathbb{N}^n} \mathsf{Mod}_C(D,\theta_{\boldsymbol{u}})(f_{\boldsymbol{i}}) \cdot \rho_0(a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}}),$$

where we consider $\mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$ as D-module algebra via Ψ_{int} and as D_{ID^n}-module algebra via the D_{ID^n}-module algebra structure induced by $\theta_{\boldsymbol{w}}$ on $A[\![\boldsymbol{w}]\!]$ to $\mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$ via lemma 2.2.22.

Proof. We first consider the homomorphism

$$\mathsf{Mod}_C(D,L) \otimes_L A[\![\boldsymbol{w}]\!] \to \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!]) \tag{3.3.4}$$

that is given as the composition of

$$\mathsf{Mod}_C(D,L) \otimes_L A[\![\boldsymbol{w}]\!] \xrightarrow{\mathsf{Mod}_C(D,\theta_{\boldsymbol{u}})\otimes\rho_0} \mathsf{Mod}_C(D, L[\![\boldsymbol{w}]\!]) \otimes_L \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$$

and the restriction of the multiplication map on $\mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$

$$\mathsf{Mod}_C(D, L[\![\boldsymbol{w}]\!]) \otimes_L \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!]) \xrightarrow{\mathrm{m}} \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!]).$$

Since

$$\mathsf{Mod}_C(D,\theta_{\boldsymbol{u}}) \colon \mathsf{Mod}_C(D,L) \to \mathsf{Mod}_C(D, L[\![\boldsymbol{w}]\!])$$

and

$$\rho_0 \colon A[\![\boldsymbol{w}]\!] \to \mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$$

are homomorphisms of $D \otimes_C D_{ID^n}$-module algebras, where $A[\![\boldsymbol{w}]\!]$ is equipped with the trivial D-module algebra structure, $\mathsf{Mod}_C(D,\theta_{\boldsymbol{u}}) \otimes \rho_0$ is one too by

proposition 2.2.25. Since $D \otimes_C D_{ID^n}$ measures $\mathsf{Mod}_C(D, A[\![\boldsymbol{w}]\!])$ to itself, m is also a homomorphism of $D \otimes_C D_{ID^n}$-module algebras. Therefore, (3.3.4) is a homomorphism of $D \otimes_C D_{ID^n}$-module algebras too. Using proposition 2.2.26 (2) we extend (3.3.4) to (3.3.3). Note that by corollary 2.2.31 the subalgebras $\mathsf{Mod}_C(D, \theta_{\boldsymbol{u}})(\mathsf{Mod}_C(D, L))$ and $\rho_0(A[\![\boldsymbol{w}]\!])$ are linearly disjoint over $\rho_0(\theta_{\boldsymbol{u}}(L))$. Thus, the homomorphism (3.3.4) is injective and so is (3.3.3). □

Notation: *We denote by* $i\colon \mathcal{L} \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ *the homomorphism sending* $a \in \mathcal{L}$ *to* $a \otimes 1 \in \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$.

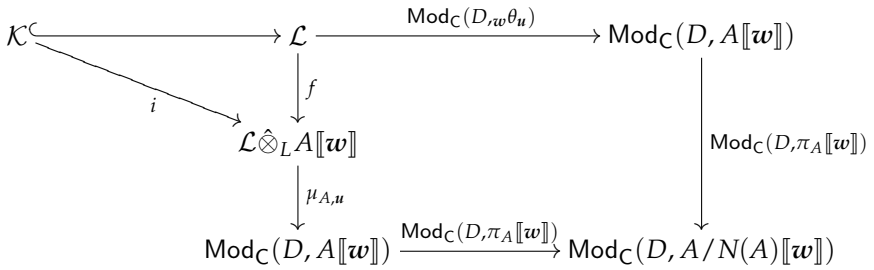
Definition 3.3.3. *We define the functor*

$$\mathcal{F}_{L/K,\boldsymbol{u}}\colon \mathsf{CAlg}_{\mathsf{L}} \to \mathsf{Set}$$

of infinitesimal deformations of *i as follows: For a commutative L-algebra A we define* $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$ *to be the set of all homomorphisms*

$$f\colon \mathcal{L} \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

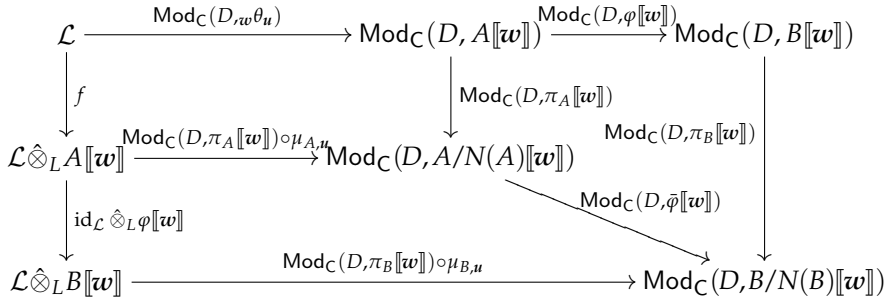
of $D \otimes_C D_{ID^n}$*-module algebras such that the diagram*



commutes, where $\pi_A\colon A \to A/N(A)$ *denotes the canonical projection. If* $\varphi\colon A \to B$ *is a homomorphism of commutative L-algebras, we define*

$$\mathcal{F}_{L/K,\boldsymbol{u}}(\varphi)\colon \mathcal{F}_{L/K,\boldsymbol{u}}(A) \to \mathcal{F}_{L/K,\boldsymbol{u}}(B)$$

by sending an $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ to $(\mathrm{id}_{\mathcal{L}} \hat{\otimes}_L \varphi[\![\boldsymbol{w}]\!]) \circ f$. This is well-defined, since the diagram



commutes, where $\bar{\varphi}\colon A/N(A) \to B/N(B)$ is the homomorphism of L-algebras induced by φ.

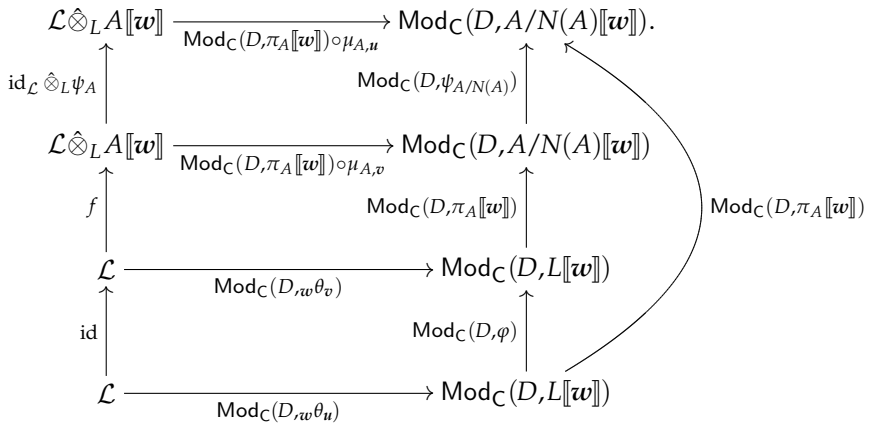
Our definition of the functor $\mathcal{F}_{L/K}$ of infinitesimal transformations differs slightly from the definition of H. Umemura. Mainly, the target of the homomorphisms we consider is $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$, while H. Umemura considers the composition with $\mu_{A,\boldsymbol{u}}$.

The functor $\mathcal{F}_{L/K,\boldsymbol{u}}$ is essentially independent of the separating transcendence basis $\boldsymbol{u}$ of L over K. In fact, we have the following lemma, which specializes to [Ume96a, Proposition 4.1] and [Mor09, Lemma 2.14] in the case where the characteristic of K is zero and where the C-bialgebra D is equal to D_{der} (see subsection 2.3.4) and D_{end} (see subsection 2.3.1), respectively.

Lemma 3.3.4. *If $\boldsymbol{u}$ and $\boldsymbol{v}$ are separating transcendence bases of L/K, then $\mathcal{F}_{L/K,\boldsymbol{u}}$ and $\mathcal{F}_{L/K,\boldsymbol{v}}$ are naturally isomorphic.*

Proof. By proposition 1.3.6, there is an automorphism φ of the L-algebra $L[\![\boldsymbol{w}]\!]$ such that $\varphi(\boldsymbol{w})_{|\boldsymbol{w}=\boldsymbol{0}} = 0$ and $\varphi \circ \theta_{\boldsymbol{u}} = \theta_{\boldsymbol{v}}$. Then $\psi := \varphi^{-1}$ also fulfills $\psi(\boldsymbol{w})_{|\boldsymbol{w}=\boldsymbol{0}}$, i.e. ψ is continous with respect to the $(\boldsymbol{w})$-adic topology. For every commutative L-algebra A we extend ψ first A-linearly to an automorphism ψ_A of $A[\![\boldsymbol{w}]\!]$ and then further $\mathsf{Mod}_{\mathsf{C}}(D, L)$-linearly to an automorphism of $\mathsf{Mod}_{\mathsf{C}}(D, L)\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$, which we denote by $\mathrm{id}_{\mathsf{Mod}_{\mathsf{C}}(D,L)} \hat{\otimes}_L \psi_A$. It is easy to

see that this automorphism restricts to an automorphism of $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$, which we denote by $\mathrm{id}_{\mathcal{L}}\hat{\otimes}_L\psi_A$. If $f \in \mathcal{F}_{L/K,\boldsymbol{v}}(A)$, then the diagram



commutes.[3] We note that $(\mathrm{id}_{\mathcal{L}}\hat{\otimes}_L\psi_A)\circ f\colon \mathcal{L}\to\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ is a $D\otimes_C D_{ID^n}$-homomorphism, where the D_{ID^n}-module algebra structure on $\mathcal{L}$ is given by $\theta_{\boldsymbol{u}}$ and the one on $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ by $\theta_{\boldsymbol{u}}\hat{\otimes}\theta_{\boldsymbol{w}}$. From the commutativity of the big rectangle we obtain that $(\mathrm{id}_{\mathcal{L}}\hat{\otimes}_L\psi_A)\circ f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ and thus a natural transformation from $\mathcal{F}_{L/K,\boldsymbol{v}}$ to $\mathcal{F}_{L/K,\boldsymbol{u}}$. Similarly, by sending an $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ to $(\mathrm{id}_{\mathcal{L}}\hat{\otimes}_L\varphi_A)\circ f \in \mathcal{F}_{L/K,\boldsymbol{v}}(A)$, we obtain a natural transformation from $\mathcal{F}_{L/K,\boldsymbol{u}}$ to $\mathcal{F}_{L/K,\boldsymbol{v}}$, which is inverse to the other. □

If the characteristic of K is zero, the following proposition specializes to [Ume96a, Lemma 4.5] and [Mor09, Lemma 2.15] in the case where $D = D_{der}$ and $D = D_{end}$, respectively.

Proposition 3.3.5. *For every commutative L-algebra A and every $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ there exists a unique $\Phi \in \mathbf{\Gamma}_{nL}(A)$ such that for all $a \in L$*

$$f(\rho(a)) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \mathsf{Mod}_C(D,\theta_{\boldsymbol{u}}^{(\boldsymbol{k})})(\rho(a))\otimes(\Phi-\boldsymbol{w})^{\boldsymbol{k}}.$$

[3] Note that the L-algebra structures on the right factors in the two completed tensor products at the top left are different. The one at the very top is given by $\theta_{\boldsymbol{u}}$, while the one at second from the top is given by $\theta_{\boldsymbol{v}}$.

Thus, we obtain an injective map $\mathcal{F}_{L/K,\boldsymbol{u}}(A) \to \mathbf{\Gamma}_{nL}(A)$ giving rise to a natural transformation $\mathcal{F}_{L/K} \to \mathbf{\Gamma}_{nL}$.

Proof. For $i = 1, \dots, n$, we define

$$\varphi_i \coloneqq \mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ f \circ \rho(u_i) - u_i \in A[\![\boldsymbol{w}]\!],$$

where $\mathrm{ev}_{1_D} \colon \mathsf{Mod}_{\mathsf{C}}(D, A[\![\boldsymbol{w}]\!]) \to A[\![\boldsymbol{w}]\!]$ denotes the evaluation map at $1_D \in D$. Then $\Phi \coloneqq (\varphi_1, \dots, \varphi_n)$ is an element of $\mathbf{\Gamma}_{nL}(A)$, since

$$\varphi_i \equiv \mathrm{ev}_{1_D} \circ \mathsf{Mod}_{\mathsf{C}}(D, {}_{\boldsymbol{w}}\theta_{\boldsymbol{u}}) \circ \rho(u_i) - u_i = w_i \mod N(A)[\![\boldsymbol{w}]\!].$$

We define two homomorphisms of C-algebras $F, G \colon L \to A[\![\boldsymbol{w}]\!]$ by

$$F \coloneqq \mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ f \circ \rho$$

and

$$G \coloneqq \mathrm{ev}_{1_D} \circ \mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}}) \circ \rho.$$

For $a \in K$ we have $F(a) = a = G(a)$ and for $i = 1, \dots, n$

$$\begin{aligned} G(u_i) &= \mathrm{ev}_{1_D} \circ \mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}}) \circ \rho(u_i) \\ &= u_i + \varphi_i \\ &= u_i + \mathrm{ev}_{1_D} \circ \mu_{A,\boldsymbol{u}} \circ f \circ \rho(u_i) - u_i \\ &= F(u_i). \end{aligned}$$

So F and G coincide on $K(\boldsymbol{u})$ and, since L is 0-étale over $K(\boldsymbol{u})$, they also coincide on L.

Finally, we show $\mu_{A,\boldsymbol{u}} \circ f \circ \rho = \mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}}) \circ \rho$. Using that f, ρ, $\mu_{A,\boldsymbol{u}}$ and $\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})$ are homomorphisms of D-module algebras (see lemma 2.2.18

and lemma 3.3.2) and that F and G are equal, we obtain

$$\begin{aligned}(\mu_{A,\boldsymbol{u}} \circ f \circ \rho(a))(d) &= (d.(\mu_{A,\boldsymbol{u}} \circ f \circ \rho(a)))(1_D) \\ &= (\mu_{A,\boldsymbol{u}} \circ f \circ \rho(d.a))(1_D) \\ &= (\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(d.a)))(1_D) \\ &= (d.(\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a))))(1_D) \\ &= (\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a)))(d).\end{aligned}$$

Since

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

and since $\mu_{A,\boldsymbol{u}}$ is injective, the claim follows. □

Lemma 3.3.6. *Let A be a commutative L-algebra and $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$. If we denote by $\varepsilon\colon A[\![\boldsymbol{w}]\!] \to A$ the homomorphism of A-algebras sending w_i to 0 for $i = 1, \ldots, n$, then for any $0 \neq a \in \mathcal{L}$ the element $\mathsf{Mod}_{\mathsf{C}}(D, \varepsilon) \circ \mu_{A,\boldsymbol{u}} \circ f(a) \in \mathsf{Mod}_{\mathsf{C}}(D, A)$ is not zero. In particular, f is injective.*

Proof. For $0 \neq a \in \mathcal{L}$ there exists $c \in \mathsf{Mod}_{\mathsf{C}}(D, N(A)[\![\boldsymbol{w}]\!])$ such that

$$(\mu_{A,\boldsymbol{u}} \circ f)(a) = \mathsf{Mod}_{\mathsf{C}}(D, {}_{\boldsymbol{w}}\theta_{\boldsymbol{u}})(a) + c$$

and thus for any $d \in D$ we have $(\mu_{A,\boldsymbol{u}} \circ f)(a)(d)_{|\boldsymbol{w}=\boldsymbol{0}} = a(d) + c(d)_{|\boldsymbol{w}=\boldsymbol{0}}$. If $\mathsf{Mod}_{\mathsf{C}}(D, \varepsilon) \circ \mu_{A,\boldsymbol{u}} \circ f(a)$ would be zero, we would obtain $a(d) = -c(d)_{|\boldsymbol{w}=\boldsymbol{0}} \in L \cap N(A) = \{0\}$ for all $d \in D$, i.e. $a = 0$ in contradiction to our assumption. □

3.4 The infinitesimal Galois group

Definition 3.4.1. *We define a functor*

$$\text{Inf-Gal}(L/K)\colon \mathsf{CAlg}_{\mathsf{L}} \to \mathsf{Grp}$$

as follows. For any commutative L-algebra A we define $\text{Inf-Gal}(L/K)(A)$ *to be the group of automorphisms* φ *of the of* $D \otimes_C D_{ID^n}$*-module algebra of* $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ *that make the diagram*

$$\begin{array}{ccccc}
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\text{id}} & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \\
\downarrow{\scriptstyle \text{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \text{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]} \\
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\text{id}_{\mathcal{L}}\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]} & \mathcal{L}\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{array}$$

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

$$\text{Inf-Gal}(L/K)(\lambda)\colon \text{Inf-Gal}(L/K)(A) \to \text{Inf-Gal}(L/K)(B)$$

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

Definition 3.4.2. *For any commutative L-algebra A and any* $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ *we define*

$$\psi_f\colon \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

as the extension of the homomorphism of $D \otimes_C D_{ID^n}$*-module algebras*

$$(\text{id}_{\mathcal{L}} \otimes_L \text{m}_{A[\![\boldsymbol{w}]\!]}) \circ (f \otimes_L \text{id}_{A[\![\boldsymbol{w}]\!]})\colon \mathcal{L} \otimes_L A[\![\boldsymbol{w}]\!] \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

to the completion with respect to the $(1 \otimes \boldsymbol{w})$*-adic topology, which again is a homomorphism of* $D \otimes_C D_{ID^n}$*-module algebras (see corollary 2.2.27).*

Lemma 3.4.3. *For any commutative L-algebra A and any* $f \in \mathcal{F}_{L/K}(A)$ *the homomorphism*

$$\psi_f\colon \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$$

is injective.

Proof. Let $\sum_{\boldsymbol{i}\in\mathbb{N}^n} g_{\boldsymbol{i}} \otimes a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}}$ be a non-zero element of $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ and let $\boldsymbol{i_0} \in \mathbb{N}^n$ be minimal among all $\boldsymbol{i} \in \mathbb{N}^n$ with the property that $g_{\boldsymbol{i}} \otimes a_{\boldsymbol{i}}\boldsymbol{w}^{\boldsymbol{i}} \neq 0$. We write

$\psi_f(\sum_{i\in\mathbb{N}^n} g_i \otimes a_i \boldsymbol{w}^i) = \sum_{i\in\mathbb{N}^n} h_i \otimes b_i \boldsymbol{w}^i$, where the term of smallest possible order that can occur is $h_{i_0} \otimes b_{i_0} \boldsymbol{w}^{i_0}$. From lemma 3.3.6 we know that there exists a $d \in D$ such that $(\mathsf{Mod}_{\mathsf{C}}(D,\varepsilon) \circ \mu_A \circ f(g_{i_0}))(d) \neq 0$, where $\varepsilon\colon A[\![\boldsymbol{w}]\!] \to A$ is the homomorphism sending all w_i to 0. In fact, this element is given as the sum of $g_{i_0}(d)$ and a nilpotent element from A and thus it is invertible in A. Thus, we see that $\mu_A(h_{i_0} \otimes a_{i_0} \boldsymbol{w}^{i_0})(d) = (\mathsf{Mod}_{\mathsf{C}}(D,\varepsilon) \circ \mu_A \circ f(g_{i_0}))(d) \cdot a_{i_0} \boldsymbol{w}^{i_0}$ is non-zero in $A[\![\boldsymbol{w}]\!]$. In particular, $h_{i_0} \otimes a_{i_0} \boldsymbol{w}^{i_0}$ cannot be zero and thus ψ_f is injective. □

In order to prove lemma 3.4.6, we first need some other lemmata.

Lemma 3.4.4. *Let A be a commutative ring and $\theta_{\boldsymbol{w}}$ be the canonical n-variate iterative derivation on $A[\![\boldsymbol{w}]\!]$ with respect to $\boldsymbol{w}$. Then for $g(\boldsymbol{w}) \in A[\![\boldsymbol{w}]\!]$ and $\Phi(\boldsymbol{w}) \in A[\![\boldsymbol{w}]\!]^n$ with $\Phi(\mathbf{0}) \in N(A)^n$ we have*

$$g(\Phi(\boldsymbol{w})) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})}(g(\boldsymbol{w}))(\Phi(\boldsymbol{w}) - \boldsymbol{w})^{\boldsymbol{k}}.$$

Proof. Since $\Phi(\mathbf{0}) \in N(A)^n$, the components of $\Phi(\boldsymbol{w})$ are topologically nilpotent in $A[\![\boldsymbol{w}]\!]$ with respect to the $(\boldsymbol{w})$-adic topology. So writing $g(\boldsymbol{w}) = \sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}} \boldsymbol{w}^{\boldsymbol{l}}$ we have

$$\begin{aligned}
\sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})}(g(\boldsymbol{w}))(\Phi(\boldsymbol{w}) - \boldsymbol{w})^{\boldsymbol{k}} &= \sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})} \left(\sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}} \boldsymbol{w}^{\boldsymbol{l}} \right) (\Phi(\boldsymbol{w}) - \boldsymbol{w})^{\boldsymbol{k}} \\
&= \sum_{\boldsymbol{k}\in\mathbb{N}^n} \left(\sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}} \binom{\boldsymbol{l}}{\boldsymbol{k}} \boldsymbol{w}^{\boldsymbol{l}-\boldsymbol{k}} \right) (\Phi(\boldsymbol{w}) - \boldsymbol{w})^{\boldsymbol{k}} \\
&= \sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}} \left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} \binom{\boldsymbol{l}}{\boldsymbol{k}} \boldsymbol{w}^{\boldsymbol{l}-\boldsymbol{k}} (\Phi(\boldsymbol{w}) - \boldsymbol{w})^{\boldsymbol{k}} \right) \\
&= \sum_{\boldsymbol{l}\in\mathbb{N}^n} a_{\boldsymbol{l}} (\Phi(\boldsymbol{w}))^{\boldsymbol{l}} \\
&= g(\Phi(\boldsymbol{w})).
\end{aligned}$$

□

Corollary 3.4.5. *For any commutative L-algebra A and any* $\Phi = \Phi' + \boldsymbol{w}, \Psi = \Psi' + \boldsymbol{w} \in \mathbf{\Gamma}_{nL}(A)$ *we have for all* $\boldsymbol{l} \in \mathbb{N}^n$

$$(\Psi'(\Phi))^{\boldsymbol{l}} = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})}(\Psi'^{\boldsymbol{l}})\Phi'^{\boldsymbol{k}}.$$

Proof. By lemma 3.4.4 we have

$$(\Psi'(\Phi))^{\boldsymbol{l}} = \left(\sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})}(\Psi')\Phi'^{\boldsymbol{k}}\right)^{\boldsymbol{l}} = ({}_{\Phi'}\theta_{\boldsymbol{w}}(\Psi'))^{\boldsymbol{l}} = {}_{\Phi'}\theta_{\boldsymbol{w}}(\Psi'^{\boldsymbol{l}}) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \theta_{\boldsymbol{w}}^{(\boldsymbol{k})}(\Psi'^{\boldsymbol{l}})\Phi'^{\boldsymbol{k}}.$$

□

Lemma 3.4.6. *Let A be a commutative L-algebra. If* $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ *and* $\Phi \in \mathbf{\Gamma}_{nL}(A)$ *is such that*

$$f(\rho(a)) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}}^{(\boldsymbol{k})})(\rho(a)) \otimes (\Phi - \boldsymbol{w})^{\boldsymbol{k}}$$

holds for all $a \in L$ *(see proposition 3.3.5) and* $g\colon \rho(L) \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ *is a map such that*

$$g(\rho(a)) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}}^{(\boldsymbol{k})})(\rho(a)) \otimes (\Psi - \boldsymbol{w})^{\boldsymbol{k}},$$

holds for some $\Psi \in \mathbf{\Gamma}_{nL}(A)$ *and all* $a \in L$*, then*

$$\psi_f \circ g(\rho(a)) = \sum_{\boldsymbol{l}\in\mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}}^{(\boldsymbol{l})})(\rho(a)) \otimes (\Phi(\Psi) - \boldsymbol{w})^{\boldsymbol{l}}$$

holds for all $a \in L$*.*

Proof. With the notation $\Phi' = \Phi - \boldsymbol{w}$ and $\Psi' = \Psi - \boldsymbol{w}$, we have for all $a \in L$,

using $\Phi(\Psi) - w = \Psi' + \Phi'(\Psi)$ and corollary 3.4.5,

$$\begin{aligned}
(\psi_f \circ g)(\rho(a)) &= \psi_f \left(\sum_{k \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k)})(\rho(a)) \otimes \Psi'^k \right) \\
&= \sum_{k \in \mathbb{N}^n} \theta^{(k)} \left(\sum_{l \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(l)})(\rho(a)) \otimes \Phi'^l \right) (1 \otimes \Psi'^k) \\
&= \sum_{k_1, k_2, l \in \mathbb{N}^n} \left(\mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k_1)} \circ \theta_u^{(l)})(\rho(a)) \otimes \theta_w^{(k_2)}(\Phi'^l) \right) (1 \otimes \Psi'^{k_1 + k_2}) \\
&= \sum_{k_1, k_2, l \in \mathbb{N}^n} \left(\binom{k_1 + l}{l} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k_1 + l)})(\rho(a)) \otimes \theta_w^{(k_2)}(\Phi'^l) \right) (1 \otimes \Psi'^{k_1 + k_2}) \\
&= \sum_{m, k_2, l \in \mathbb{N}^n} \binom{m}{l} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(m)})(\rho(a)) \otimes \theta_w^{(k_2)}(\Phi'^l) \Psi'^{m - l + k_2}) \\
&= \sum_{m, l \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(m)})(\rho(a)) \otimes \binom{m}{l} \Psi'^{m-l} (\Phi'(\Psi))^l \\
&= \sum_{n \in \mathbb{N}^m} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(n)})(\rho(a)) \otimes (\Phi(\Psi) - w)^m.
\end{aligned}$$

□

Corollary 3.4.7. *Let A be a commutative L-algebra. If $f, g \in \mathcal{F}_{L/K,u}(A)$ are such that*

$$f(\rho(a)) = \sum_{k \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k)})(\rho(a)) \otimes \Phi'^k$$

and

$$g(\rho(a)) = \sum_{k \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k)})(\rho(a)) \otimes \Psi'^k$$

hold for all $a \in L$ with some $\Phi = \Phi' + w, \Psi = \Psi' + w \in \mathbf{\Gamma}_{nL}(A)$ (see proposition 3.3.5), then we have

$$(\psi_f \circ \psi_g)(\rho(a) \otimes 1) = \sum_{k \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_u^{(k)})(\rho(a)) \otimes (\Phi(\Psi) - w)^k$$

for all $a \in L$.

Theorem 3.4.8. *For any commutative L-algebra A, the set $\mathcal{F}_{L/K,u}(A)$ is a principal homogeneous space for the group* Inf-Gal$(L/K)(A)$.

Proof. We define a map

$$\text{Inf-Gal}(L/K)(A) \times \mathcal{F}_{L/K,\boldsymbol{u}}(A) \to \mathcal{F}_{L/K,\boldsymbol{u}}(A)$$

by sending a pair $(\varphi, f) \in \text{Inf-Gal}(L/K)(A) \times \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ to $\varphi \circ f$. This is in fact well-defined: Since f and φ are $D \otimes_C D_{ID^n}$-module algebra homomorphisms, so is $\varphi \circ f$. We consider the diagram

$$\begin{array}{ccccc}
\mathcal{K} & \longrightarrow & \mathcal{L} & \xrightarrow{\mathsf{Mod}_{\mathsf{C}}(D,{}_{\boldsymbol{w}}\theta_{\boldsymbol{u}})} & \mathsf{Mod}_{\mathsf{C}}(D, A[\![\boldsymbol{w}]\!]) \\
\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathsf{Mod}_{\mathsf{C}}(D,\pi_A[\![\boldsymbol{w}]\!])} \\
\mathsf{Mod}_{\mathsf{C}}(D,{}_{\boldsymbol{w}}\theta_{\boldsymbol{u}}) & & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\mathsf{Mod}_{\mathsf{C}}(D,\pi_A[\![\boldsymbol{w}]\!])\circ\mu_{A,\boldsymbol{u}}} & \mathsf{Mod}_{\mathsf{C}}(D, A/N(A)[\![\boldsymbol{w}]\!]) \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}} \\
\mathsf{Mod}_{\mathsf{C}}(D, A[\![\boldsymbol{w}]\!]) & \xleftarrow{\mu_{A,\boldsymbol{u}}} & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\mathsf{Mod}_{\mathsf{C}}(D,\pi_A[\![\boldsymbol{w}]\!])\circ\mu_{A,\boldsymbol{u}}} & \mathsf{Mod}_{\mathsf{C}}(D, A/N(A)[\![\boldsymbol{w}]\!]).
\end{array}$$

By definition of $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$ and $\text{Inf-Gal}(L/K)(A)$, the two squares on the right commute. Since $f(a) \in \mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ for $a \in \mathcal{K}$ and φ is a $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$-homomorphism, we have $\mu_{A,\boldsymbol{u}} \circ \varphi \circ f(a) = \mu_{A,\boldsymbol{u}} \circ f(a) = \mathsf{Mod}_{\mathsf{C}}(D, {}_{\boldsymbol{w}}\theta_{\boldsymbol{u}})(a)$ for all $a \in \mathcal{K}$, i.e. the rectangle at the left commutes too. Thus, $\varphi \circ f$ is also an element of $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$. It is clear that this defines in fact an operation of $\text{Inf-Gal}(L/K)(A)$ on $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$ from the left.

In order to show that this operation makes $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$ into a principal homogeneous space for $\text{Inf-Gal}(L/K)(A)$, we have to prove that for any $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ there exists a unique automorphism $\psi_f \in \text{Inf-Gal}(L/K)(A)$ such that

$$\psi_f \circ i = f, \tag{3.4.1}$$

where $i\colon \mathcal{L} \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ is the homomorphism defined before definition 3.3.3. The automorphism ψ_f of the $D \otimes_C D_{ID^n}$-module algebra $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ in definition 3.4.2 fulfills (3.4.1) by definition and by lemma 3.4.3 it is injective. It remains to show that ψ_f is unique and that it is an automorphism. By propo-

sition 3.3.5, there exists a $\Phi \in \mathbf{\Gamma}_{nL}(A)$ such that for all $a \in L$

$$f(\rho(a)) = \sum_{\boldsymbol{k} \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}}^{(\boldsymbol{k})})(\rho(a)) \otimes (\Phi - \boldsymbol{w})^{\boldsymbol{k}}.$$

We define Ψ as the inverse Φ^{-1} of Φ in the group $\mathbf{\Gamma}_{nL}(A)$. We claim that the assignment

$$\rho(a) \mapsto \sum_{\boldsymbol{k} \in \mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}}^{(\boldsymbol{k})})(\rho(a)) \otimes (\Psi - \boldsymbol{w})^{\boldsymbol{k}}$$

defines a $\mathcal{K}$-homomorphism $g\colon \mathcal{L} \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ of $D \otimes_C D_{ID^n}$-module algebras. Since $\mathcal{L}$ is differentially generated by $\rho(L)$ over $\mathcal{K}$ with respect to the n-variate iterative derivation $\theta_{\boldsymbol{u}}$, we only have to show that this is well-defined, i.e. that if $F \in \mathcal{K}\{X_1, \dots, X_m\}_{D_{ID^n}}$ is a differential polynomial with coefficients in $\mathcal{K}$ such that $F(\rho(a_1), \dots, \rho(a_m)) = 0$ for certain elements $a_1, \dots, a_m \in L$, then $F(g(\rho(a_1)), \dots, g(\rho(a_m)))$ vanishes too. By lemma 3.4.6, we have

$$\psi_f \circ g(\rho(a)) = \rho(a) \otimes 1$$

for all $a \in \mathcal{L}$. Since ψ_f is a $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$-homomorphism of $D \otimes_C D_{ID^n}$-module algberas, we obtain

$$\begin{aligned}\psi_f(F(g(\rho(a_1)), \dots, g(\rho(a_m)))) &= F(\psi_f \circ g(\rho(a_1)), \dots, \psi_f \circ g(\rho(a_m))) \\ &= F(\rho(a_1) \otimes 1, \dots, \rho(a_m) \otimes 1) \\ &= 0\end{aligned}$$

Because ψ_f is injective by lemma 3.4.3, it follows

$$F(g(\rho(a_1)), \dots, g(\rho(a_m))) = 0$$

and thus $g\colon \mathcal{L} \to \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ is a well-defined homomorphism of $\mathcal{K}$-algebras. It is clear that g is a homomorphism of $D \otimes_C D_{ID^n}$-module algebras. By corollary 3.4.7, ψ_g is the inverse of ψ_f, i.e. ψ_f is an automorphism. The homomorphism ψ_f is unique with the property that $\psi_f(a \otimes 1) = f(a)$ for all $a \in \mathcal{L}$, since elements of Inf-Gal$(L/K)(A)$ are determined by their values on $\mathcal{L} \otimes 1$. □

Remark 3.4.9. *In [Ume96a, Theorem 5.10] the author shows that $\mathcal{F}_{L/K}$ is a principal homogeneous space for* Inf-Gal(L/K). *The operation defined there is an operation from the right, while ours is from the left.*

Corollary 3.4.10. *For any commutative L-algebra A there is an isomorphism*

$$\text{Inf-Gal}(L/K)(A) \xleftrightarrow{\sim} \mathcal{F}_{L/K,\boldsymbol{u}}(A)$$

given by

$$\varphi \mapsto \varphi \circ i$$
$$\psi_f \hookleftarrow f$$

This isomorphism is functorial in A, i.e. we obtain a natural isomorphism of Set*-functors on the category* $\mathsf{CAlg}_{\mathsf{L}}$

$$\text{Inf-Gal}(L/K) \cong \mathcal{F}_{L/K,\boldsymbol{u}}.$$

Proposition 3.4.11. *There exists an ideal $I \trianglelefteq L[\![\boldsymbol{x}]\!]\{L[\![\boldsymbol{y}]\!]\}$ such that*

$$\mathcal{F}_{L/K,\boldsymbol{u}}(A) \cong Z(I)(A)$$

for any commutative L-algebra A.

Proof. Proposition 3.3.5 provides for every commutative L-algebra A a map from $\mathcal{F}_{L/K,\boldsymbol{u}}(A)$ to $\mathbf{\Gamma}_{nL}(A)$. We have to show that there exists an ideal I such that its image is of the form $Z(I)(A)$. Since $\mathcal{L} = \mathcal{K}\{\rho(a) \mid a \in L\}_{\Psi_{\boldsymbol{u}}}$, we have

$$\mathcal{L} \cong \mathcal{K}\{X_a \mid a \in L\}_{\mathrm{ID}^n}/J$$

with

$$J = \Big\{F(X_{a_1}, \ldots, X_{a_m}) \in \mathcal{K}\{X_a \mid a \in L\}_{\mathrm{ID}^n} \mid F(\rho(a_1), \ldots, \rho(a_m)) = 0\Big\}.$$

Elements $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ are determined by their values on $\rho(a)$ with $a \in L$. If $\Phi \in \mathbf{\Gamma}_{nL}(A)$, then there exists an $f \in \mathcal{F}_{L/K,\boldsymbol{u}}(A)$ such that $f(\rho(a)) = \sum_{\boldsymbol{k}\in\mathbb{N}^n} \mathsf{Mod}_{\mathsf{C}}(D, \theta^{(\boldsymbol{k})})(\rho(a)) \otimes (\Phi - \boldsymbol{w})^{\boldsymbol{k}}$ for all $a \in L$ if for all $F(X_{a_1}, \ldots, X_{a_m}) \in J$ we have

$$F^{\mathsf{Mod}_{\mathsf{C}}(D,\boldsymbol{w}\theta_{\boldsymbol{u}})}(\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a_1)), \ldots, \mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a_m))) = 0.$$

We define for $F(X_{a_1}, \ldots, X_{a_m}) \in J$ and $d \in D$ an element $F_d \in L[\![\boldsymbol{w}]\!]\{L[\![\Phi]\!]\}$ as

$$F_d := F^{\mathsf{Mod}_{\mathsf{C}}(D,\boldsymbol{w}\theta_{\boldsymbol{u}})}(\mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a_1)), \ldots, \mathsf{Mod}_{\mathsf{C}}(D, {}_{\Phi}\theta_{\boldsymbol{u}})(\rho(a_m)))(d).$$

Then the image of $\mathcal{F}_{L/K,\boldsymbol{u}}$ in $\mathbf{\Gamma}_{nL}$ is given as $Z(I)$, where I is the ideal generated by F_d for all $F \in J$ and all $d \in D$. In the notation of definition 3.2.8, the variables w_i correspond to x_i and φ_i corresponds to y_i for all $i \in \{1, \ldots, n\}$. □

Corollary 3.4.12. *The functor* Inf-Gal(L/K) *is a Lie-Ritt functor over* L.

Proof. For any commutative L-algebra A we obtain from corollary 3.4.10 and proposition 3.4.11 an ideal $I \trianglelefteq L[\![\boldsymbol{x}]\!]\{[\![\boldsymbol{y}]\!]\}$ and isomorphisms

$$\text{Inf-Gal}(L/K)(A) \xrightarrow{\sim} \mathcal{F}_{L/K,\boldsymbol{u}}(A) \xrightarrow{\sim} Z(I)(A).$$

The composition is a group homomorphism by corollary 3.4.7. □

Corollary 3.4.13. *The infinitesimal Galois group* Inf-Gal(L/K) *is a formal group scheme.*

Proof. This follows from corollary 3.4.12 and proposition 3.2.11. □

Example 3.4.14. *If* Ψ *is the trivial* D*-module algebra structure on* L*, then* $\mathcal{L} = \mathcal{K} = \rho_0(L)$ *and both* $\mathcal{F}_{L/K}$ *and* Inf-Gal(L/K) *are trivial.*

Chapter 4

Picard-Vessiot theory

In this chapter we consider finitely generated Picard-Vessiot extensions L/K of D-module fields in the sense of K. Amano and A. Masuoka ([AM05]). For such an extension we give a description of the extension of algebras $\mathcal{L}/\mathcal{K}$ associated to L/K, as defined in chapter 3, and show that there is a close connection between the Galois group scheme $\mathrm{Gal}(L/K)$ of the Picard-Vessiot extension L/K, as defined by K. Amano and A. Masuoka, and the infinitesimal Galois group $\text{Inf-Gal}(L/K)$ of the extension L/K.

Notation: *Let C be a commutative ring and D be a cocommutative C-bialgebra. Although many results hold more generally, we assume additionally, as in [AM05], that D is a pointed Hopf-algebra and that the irreducible component D^1 is of Birkhoff-Witt type. Given an extension of commutative D-module algebras $R \subseteq S$, we denote by $\mathrm{Aut}_D(S/R)$ the group of automorphisms of the D-module algebra S that leave R fixed.*

4.1 Picard-Vessiot extensions of Artinian simple module algebras

We recall the definition of Picard-Vessiot extensions of commutative Artinian simple module algebras and basic properties of finitely generated Picard-Vessiot extensions from [AM05]. Alternative references for this material are [Ama05] and [AMT09].

Definition 4.1.1. *An extension of commutative Artinian simple D-module algebras* $(L, \rho_L)/(K, \rho_K)$ *is* Picard-Vessiot *if the following hold:*

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

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

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

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

$$R \cdot H = R \otimes_K R \quad (\text{or } H \cdot R = R \otimes_K R).$$

Proposition 4.1.2 ([AM05, Proposition 3.4])**.** *Let* $(L, \rho_L)/(K, \rho_K)$ *be a Picard-Vessiot extension of commutative Artinian simple D-module algebras with constants* $k := L^{\rho_L} = K^{\rho_K}$ *and* (R, ρ_R) *and* H *be as in definition 4.1.1. Then the following hold:*

(1) The intermediate D-module algebra (R, ρ_R) *satisfying condition (2) in definition 4.1.1 is unique.*

(2) The homomorphism

$$\mu \colon (R \otimes_k H, \rho_R \otimes \rho_0) \to (R \otimes_K R, \rho_R \otimes \rho_R), \quad a \otimes h \mapsto (a \otimes 1) \cdot h \tag{4.1.1}$$

is an isomorphism of D-module algebras.

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

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

and the comultiplication

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

The antipode S on H is induced by the twist map

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

Definition 4.1.3. *If L/K is a Picard-Vessiot extension of commutative Artinian simple D-module algebras, then R and H in definition 4.1.1 are called the* principal *D*-module algebra *and the* Hopf algebra of a Picard-Vessiot extension *L/K, respectively. If we want to indicate R and H, we denote the Picard-Vessiot extension L/K also by $(L/K, R, H)$.*

Definition 4.1.4. *If $(L/K, R, H)$ is a Picard-Vessiot extension of commutative Artinian simple D-module algebras, then we define the* Galois group scheme $\mathrm{Gal}(L/K)$ *of L/K to be the affine group scheme* $\operatorname{Spec} H$ *over the constants $K^\Psi = L^\Psi$.*

Remark 4.1.5. *Let $(L/K, R, H)$ be a Picard-Vessiot extension of commutative Artinian simple D-module algebras with constants $k := L^\Psi = K^\Psi$. Then for any commutative k-algebra A the A-points of* $\mathrm{Gal}(L/K) = \operatorname{Spec} H$ *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 (see [AM05, Remark 3.11]).*

Theorem 4.1.6 ([AM05, Theorem 4.6])**.** *If $(L, \rho_L)/(K, \rho_K)$ is a Picard-Vessiot extension of commutative Artinian simple D-module algebras that is finitely generated as Artinian simple D-module algebra, then there exists a matrix $X \in \mathrm{GL}_n(L)$ such that $L = K\langle X\rangle := K\langle\{x_{i,j} \mid i, j \in \{1, \dots, n\}\}\rangle$ and for every $d \in D$ the coefficients*

of $(dX)X^{-1}$ *are in* K*. Furthermore, the principal* D*-module algebra* R *of* L/K *is of the form*

$$R = K[X, X^{-1}]$$

and the Hopf algebra H *of* L/K *is of the form*

$$H = k[(X^{-1} \otimes 1)(1 \otimes X), (1 \otimes X^{-1})(X \otimes 1)],$$

where $k := L^{\Psi} = K^{\Psi}$.[1]

4.2 The general Galois theory in the linear case

In this section we examine the extension $\mathcal{L}/\mathcal{K}$ defined in chapter 3 in the case where L/K is a finitely generated Picard-Vessiot extension of D-module fields and compare the infinitesimal Galois group Inf-Gal(L/K) with the Galois group scheme Gal(L/K) of L/K as defined by K. Amano and A. Masuoka in [AM05].

Lemma 4.2.1. *Let* $(L/K, R, H)$ *be a Picard-Vessiot extension of* D*-module fields such that* L/K *is separable and finitely generated as a field extension. Let* $\boldsymbol{u} = (u_1, \ldots, u_n)$ *be a separating transcendence basis of* L/K*. Then the subring of* $\mathsf{Mod}_{\mathsf{C}}(D, L)$ *generated by* $\rho_0(L)$ *and* $\rho(L)$ *is closed under the extension* $\mathsf{Mod}_{\mathsf{C}}(D, \theta_u)$ *of the* n*-variate iterative derivation* $\theta_{\boldsymbol{u}}$ *from* L *to* $\mathsf{Mod}_{\mathsf{C}}(D, L)$ *(via lemma 2.2.22) and* $\rho_0(L)$ *and* $\rho(L)$ *are linearly disjoint over the field of constants* $k := L^{\Psi} = K^{\Psi}$*. We thus have an isomorphism*

$$\mathcal{L} = \rho_0(L)[\rho(L)] \cong \rho_0(L) \otimes_k \rho(L) \tag{4.2.1}$$

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

$$\rho_0(L)[\rho(R)] \cong \rho_0(L) \otimes_k \rho(R). \tag{4.2.2}$$

[1] Usually such a matrix $X \in \mathrm{GL}_n(L)$ is called *fundamental solution matrix*.

Proof. By theorem 4.1.6, there exists a matrix $X \in \mathrm{GL}_n(L)$ such that $L = K\langle X\rangle$, $R = K[X, X^{-1}]$ and such that $d(X)X^{-1} \in M_n(K)$ for all $d \in D$. Thus, the element $Z := \rho(X)\rho_0(X)^{-1}$ lies in $\mathrm{GL}_n(\mathsf{Mod}_{\mathsf{C}}(D, K))$. Therefore, and since $\mathcal{K}[\rho(X), \rho(X)^{-1}] = \mathcal{K}[Z\rho_0(X), \rho_0(X)^{-1}Z^{-1}] = \mathcal{K}[Z, Z^{-1}]$, we see that $\rho_0(L)[\rho(R)] = \mathcal{K}[\rho(R)] = \mathcal{K}[\rho(X), \rho(X)^{-1}]$ is closed under the D_{ID^n}-module algebra structure on $\mathsf{Mod}_{\mathsf{C}}(D, L)$ induced by $\theta_{\boldsymbol{u}}$.

Since $\rho(L) = \mathrm{Quot}(\rho(R))$, it is sufficient to show that the images $\mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}})(a)$ of non-zero elements a of $\rho(R)$ are invertible in $(\rho_0(L)[\rho(L)])[\![\boldsymbol{w}]\!]$. Since formal power series are invertible if and only if their constant term is invertible and since the constant term of $\mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}})(a)$ is the non-zero (and hence invertible) element $a \in \rho(L)$, we see that $\mathsf{Mod}_{\mathsf{C}}(D, \theta_{\boldsymbol{u}})(a)$ is invertible in $(\rho_0(L)[\rho(L)])[\![\boldsymbol{w}]\!]$. Thus, $\rho_0(L)[\rho(L)]$ is closed with respect to the D_{ID^n}-module algebra structure induced by $\theta_{\boldsymbol{u}}$.

We consider $\rho(L)$ as subalgebra of $\mathcal{L}$. It follows from corollary 2.2.31 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. The linear disjointness of $\rho_0(L)$ and $\rho(R)$ over k and thus the isomorphism (4.2.2) also follows from corollary 2.2.31. □

The following lemma is well-known in the Picard-Vessiot theories of differential and difference equations.

Lemma 4.2.2. *Let $(L, \rho)/(K, \rho_K)$ be a finitely generated Picard-Vessiot extension of commutative Artinian simple D-module algebras with field of constants $k := L^{\rho_L} = K^{\rho_K}$. If $X \in \mathrm{GL}_n(L)$ is such that $L = K\langle X\rangle$ and $(dX)X^{-1} \in M_n(K)$ for all $d \in D$ (see theorem 4.1.6), then for all commutative k-algebras A and all automorphisms σ of the D-module algebra $(L \otimes_k A, \rho_L \otimes \rho_0)$ fixing $K \otimes_k A$ there exists a matrix $C_\sigma \in \mathrm{GL}_n((L \otimes_k A)^{\rho_L \otimes \rho_0})$ such that*

$$\sigma(X \otimes 1) = (X \otimes 1)C_\sigma$$

and the map

$$\mathrm{Aut}_D(L \otimes_k A/K \otimes_k A) \to \mathrm{GL}_n((L \otimes_k A)^{\rho_L \otimes \rho_0}), \quad \sigma \mapsto C_\sigma \tag{4.2.3}$$

is a homomorphism of groups.

Proof. For every $\sigma \in \mathrm{Aut}_D(L \otimes_k A, K \otimes_k A)$ we define $C_\sigma := (X \otimes 1)^{-1}\sigma(X \otimes 1)$. Then C_σ is constant with respect to $\rho_L \otimes \rho_0$, since with $Z := \rho(X)\rho_0(X)^{-1}$ we have

$$\begin{aligned}(\rho_L \otimes \rho_0)(C_\sigma) &= (\rho_L \otimes \rho_0)((X^{-1} \otimes 1) \cdot \sigma(X \otimes 1)) \\ &= (\rho_L(X) \otimes 1)^{-1} \cdot (\rho_L \otimes \rho_0)(\sigma(X \otimes 1)) \\ &= (\rho_0(X)^{-1}Z^{-1} \otimes 1) \cdot \mathsf{Mod}_{\mathsf{C}}(D, \sigma)(Z\rho_0(X) \otimes 1) \\ &= \rho_0(X^{-1} \otimes 1) \cdot \rho_0(\sigma(X \otimes 1)) \\ &= \rho_0(C_\sigma).\end{aligned}$$

Because of

$$C_{\sigma\tau} = (X \otimes 1)^{-1} \cdot (\sigma\tau)(X \otimes 1) = (X^{-1} \otimes 1) \cdot \sigma((X \otimes 1)C_\tau) = C_\sigma C_\tau,$$

the map (4.2.3) is a homomorphism of groups. □

For a finitely generated Picard-Vessiot extension $(L/K, R, H)$ of commutative Artinian simple D-module algebras and a commutative L-algebra A the groups $\mathrm{Aut}_D(L \otimes_k A/K \otimes_k A)$ and $\mathrm{Aut}_D(R \otimes_k A/K \otimes_k A)$ are in general not isomorphic. But the following is still true:

Lemma 4.2.3. *Let $(L, \rho_L)/(K, \rho_K)$ be a finitely generated Picard-Vessiot extension of commutative Artinian simple D-module algebras with field of constants $k := L^{\rho_L} = K^{\rho_K}$ and let (R, ρ_R) be the principal D-module algebra of L/K. On the category CAlg_k two group functors G and H are defined by*

$$G(A) := \mathrm{Ker}\left(\mathrm{Aut}_D(L \otimes_k A/K \otimes_k A) \to \mathrm{Aut}_D(L \otimes_k A/N(A)/K \otimes_k A/N(A))\right)$$

and

$$H(A) := \mathrm{Ker}\left(\mathrm{Aut}_D(R \otimes_k A/K \otimes_k A) \to \mathrm{Aut}_D(R \otimes_k A/N(A)/K \otimes_k A/N(A))\right),$$

respectively, for all commutative k-algebras A, where the homomorphisms between the automorphism groups are induced by the natural projection $\pi_A \colon A \to A/N(A)$ and

where the D-module algebra structures on $L \otimes_k A$ and $R \otimes_k A$ are given by $\rho_L \otimes \rho_0$ and $\rho_R \otimes \rho_0$, respectively. Then the functors G and H are naturally isomorphic.

Proof. We first recall that by theorem 4.1.6 there exists a matrix $X \in \mathrm{GL}_n(L)$ such that $(dX)X^{-1} \in M_n(K)$ for all $d \in D$ and such that $L = K\langle X \rangle$ and $R = K[X, X^{-1}]$. By lemma 4.2.2, there exists for every $\sigma \in \mathrm{Aut}_D(L \otimes_k A/K \otimes_k A)$ a matrix $C_\sigma \in \mathrm{GL}_n((L \otimes_k A)^{\rho_L \otimes \rho_0}) = \mathrm{GL}_n(k \otimes_k A)$ such that $\sigma(X \otimes 1) = (X \otimes 1)C_\sigma$. It follows

$$\begin{aligned}\sigma(R \otimes_k A) &= \sigma(K[X, X^{-1}] \otimes_k A) \\ &= \sigma(K \otimes_k A)[\sigma(X \otimes 1), \sigma(X^{-1} \otimes 1)] \\ &= (K \otimes_k A)[(X \otimes 1)C_\sigma, C_\sigma^{-1}(X^{-1} \otimes 1)] \\ &= R \otimes_k A.\end{aligned}$$

Thus, σ restricts to an automorphism of the D-module algebra $(R \otimes_k A, \rho_R \otimes \rho_0)$ and trivially the image of it in $\mathrm{Aut}_D(R \otimes_k A/N(A)/K \otimes_k A/N(A))$ is the identity. Therefore, we obtain a homomorphism of groups $G(A) \to H(A)$.

Let, conversely, $\sigma \in H(A)$ and $a \in R$ be a non-zero divisor. Then $\sigma(a \otimes 1)$ is congruent to $a \otimes 1$ modulo $R \otimes_k N(A)$ and thus also with respect to $N(L \otimes_k A) \supseteq N(R \otimes_k A) \supseteq R \otimes_k N(A)$. Therefore, $\sigma(a \otimes 1)$ is invertible in $L \otimes_k A$ and consequently σ extends to an automorphism $\tilde{\sigma}$ on $L \otimes_k A$. If $a/a' \in L = \mathrm{Q}(R)$ and $b \in A$, then $\tilde{\sigma}(a/a' \otimes b) = \sigma(a \otimes b)/\sigma(a' \otimes 1)$. Since $\sigma(a \otimes b) \equiv a \otimes b \mod R \otimes_k N(A)$ we also have $\tilde{\sigma}(a/a' \otimes b) \equiv a/a' \otimes b \mod L \otimes_k N(A)$ and so we obtain a homomorphism of groups from $H(A)$ to $G(A)$.

It is clear that these homomorphisms of groups are inverse to each other. □

We have the following similar result for the infinitesimal Galois group.

Lemma 4.2.4. *Let $(L/K, R, H)$ be a Picard-Vessiot extension of D-module fields with field of constants k such that the field extension L/K is separable and finitely generated. Similarly as in definition 3.4.1 we define a group functor* Inf-Gal(R/K)

on the category CAlg_L *by defining* Inf-Gal$(R/K)(A)$ *for every commutative* L*-algebra* A *to be the group of automorphisms* φ *of the* $D \otimes_C D_{ID^n}$*-module algebra* $\rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ *that make the diagram*

$$\begin{array}{ccccc}
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\mathrm{id}} & \rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \\
\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}\,\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]} \\
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\mathrm{id}\,\hat{\otimes}\pi_A[\![\boldsymbol{w}]\!]} & \rho_0(L)[\rho(R)]\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!],
\end{array}$$

commutative. Then the functors Inf-Gal(L/K) *and* Inf-Gal(R/K) *are naturally isomorphic.*

Proof. Let A be a commutative L-algebra. Using the isomorphism (4.2.2) in lemma 4.2.1, we obtain an isomorphism of algebras

$$\rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \cong (R \otimes_k A)[\![\boldsymbol{w}]\!]. \tag{4.2.4}$$

Similarly, from the isomorphism (4.2.1) we obtain an isomorphism

$$\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \cong (L \otimes_k A)[\![\boldsymbol{w}]\!]. \tag{4.2.5}$$

If φ is an element of Inf-Gal$(R/K)(A)$, then

$$\varphi(\rho(a) \otimes 1) \equiv \rho(a) \otimes 1 \mod \rho_0(L)[\rho(R)]\hat{\otimes}_L N(A)[\![\boldsymbol{w}]\!]$$

for all $a \in R$. Therefore, the element $\varphi(\rho(a) \otimes 1)$ corresponds under the isomorphism (4.2.4) to an element in $(R \otimes_k A)[\![\boldsymbol{w}]\!]$ congruent to $a \otimes 1$ modulo $(R \otimes_k N(A))[\![\boldsymbol{w}]\!]$ and thus is invertible in $(L \otimes_k A)[\![\boldsymbol{w}]\!]$. Using the isomorphism (4.2.5), we see that φ can be extended to an automorphism on $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$.

Conversely, given an element $\varphi \in$ Inf-Gal$(L/K)(A)$, one easily sees from the formulas in lemma 3.4.6 and lemma 4.2.1 that φ restricts to an automorphism of the $D \otimes_C D_{ID^n}$-module algebra $\rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$. □

Lemma 4.2.5. *Let $(L/K, R, H)$ be a finitely generated Picard-Vessiot extension of D-module fields with field of constants k and $X \in \mathrm{GL}_n(L)$ be as in theorem 4.1.6. Then there exists a finite field extension K' of K, a matrix $A \in \mathrm{GL}_n(K')$ and a left K-linear and 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*

$$\gamma(X \otimes 1 \otimes 1) := (X \otimes 1 \otimes 1)(1 \otimes X^{-1} \otimes 1)(1 \otimes 1 \otimes A). \tag{4.2.6}$$

Proof. Let $\theta\colon (R, \rho_R) \to (R \otimes_k H, \rho_R \otimes \rho_0)$ be the homomorphism of D-module algebras defined by $\theta(a) := \mu^{-1}(1 \otimes a)$ for all $a \in R$, where $\mu\colon (R \otimes_k H, \rho_R \otimes \rho_0) \to (R \otimes_K R, \rho_R \otimes \rho_R)$ is the isomorphism of D-module algebras (4.1.1) defined in proposition 4.1.2. Then θ fulfills

$$\theta(X) = (X \otimes (1 \otimes 1))(1 \otimes (X^{-1} \otimes 1)(1 \otimes X)). \tag{4.2.7}$$

Let I be a maximal ideal of R and let $\pi\colon R \to R/I$ be the canonical projection from R to $K' := R/I$. Since R is a finitely generated K-algebra, $K' = R/I$ is a finite field extension of K by Hilbert's Nullstellensatz (see for example [Wat79, Appendix 8]). We extends the composition

$$R \xrightarrow{\theta} R \otimes_k H \hookrightarrow R \otimes_k R \otimes_K R \xrightarrow{\mathrm{id}_R \otimes_k \mathrm{id}_R \otimes_K \pi} R \otimes_k R \otimes_K K'$$

right $R \otimes_K K'$-linearly to an endomorphism γ of $R \otimes_k R \otimes_K K'$ and we define $A \in \mathrm{GL}_n(K')$ to be the image of X under the homomorphism π. Then from equation (4.2.7) the defining identity (4.2.6) for γ follows and clearly γ is a homomorphism of D-module algebras. The antipode S of the Hopf algebra H fulfills $S((X^{-1} \otimes 1)(1 \otimes X)) = (1 \otimes X^{-1})(X \otimes 1)$. The inverse of γ is given by the right $R \otimes_K K'$-linear extension of

$$R \xrightarrow{\theta} R \otimes_k H \xrightarrow{\mathrm{id} \otimes_k S} R \otimes_k H \hookrightarrow R \otimes_k R \otimes_K R \xrightarrow{\mathrm{id}_R \otimes_k \mathrm{id}_R \otimes_K \pi} R \otimes_k R \otimes_K K',$$

to an endomorphism of $R \otimes_k R \otimes_K K'$, which sends $X \otimes 1 \otimes 1$ to $(X \otimes 1 \otimes 1)(1 \otimes 1 \otimes A^{-1})(1 \otimes X \otimes 1)$.

□

Theorem 4.2.6. *Let $(L, \rho_L)/(K, \rho_K)$ be a Picard-Vessiot extension of D-module fields with principal D-module algebra (R, ρ_R) and field of constants $k := L^{\rho_L} = K^{\rho_K}$ such that the field L is finitely generated and over K and such that K is perfect. Then there exists a finite separable field extension L' of L such that for any commutative L'-algebra A there is an isomorphism of groups*

$$\mathrm{Ker}\left(\mathrm{Gal}(L/K)(A) \to \mathrm{Gal}(L/K)(A/N(A))\right) \cong \text{Inf-Gal}(L/K)(A),$$

where the homomorphism $\mathrm{Gal}(L/K)(A) \to \mathrm{Gal}(L/K)(A/N(A))$ is induced by the canonical projection $\pi_A \colon A \to A/N(A)$.

Proof. First, we recall the isomorphism

$$\mathrm{Gal}(L/K)(A) \cong \mathrm{Aut}_D(R \otimes_k A/K \otimes_k A)$$

for every commutative k-algebra A (remark 4.1.5). By lemma 4.2.4, we know that Inf-Gal(L/K) is isomorphic to the functor Inf-Gal(R/K) defined there. We will thus show that there exists a finite separable field extension L' of L such that Inf-Gal$(R/K)(A)$ is isomorphic to

$$\mathrm{Ker}\left(\mathrm{Aut}_D(R \otimes_k A/K \otimes_k A) \to \mathrm{Aut}_D(R \otimes_k A/N(A)/K \otimes_k A/N(A))\right) \quad (4.2.8)$$

for every commutative L'-algebra A. Let $X \in \mathrm{GL}_n(L)$ be as in theorem 4.1.6, so that $R = K[X, X^{-1}]$. By lemma 4.2.5, there exists a finite field extension K' over K and a right $R \otimes_K K'$-linear and left 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

$$\gamma(X \otimes 1 \otimes 1) := (X \otimes 1 \otimes 1)(1 \otimes X^{-1} \otimes 1)(1 \otimes 1 \otimes A)$$

for a certain matrix $A \in \mathrm{GL}_n(K')$. Since K is perfect, the field K' is finite separable over K and thus there exists a finite separable field extension L' of L containing K'. Then γ induces a left K-linear and right L'-linear automorphism $\bar{\gamma}$ of the D-module algebra $(R \otimes_k L', \rho_R \otimes \rho_0)$ defined by $\bar{\gamma}(X \otimes 1) := (X \otimes 1)(1 \otimes X^{-1}A)$. We denote the unique extension of the

n-variate iterative derivation $\theta_{\boldsymbol{u}}$ from L to L' 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 corollary 2.2.31; we have an isomorphism of D-module algebras

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

where the D-module algebra structure on $\bar{\gamma}(R \otimes_k 1) \otimes_k (1 \otimes_k L')$ is $\rho_R \otimes_k \rho_0 \otimes_k \rho_R \otimes_k \rho_0$. By lemma 4.2.1, we have isomorphisms of D-module algebras

$$R \otimes_k L \xrightarrow{\rho \otimes_k \rho_0} \rho(R) \otimes_k \rho_0(L) \xrightarrow{m} \rho_0(L)[\rho(R)], \tag{4.2.9}$$

which extend L'-linearly to

$$R \otimes_k L' \xrightarrow{\rho \otimes_k \rho_0} \rho(R) \otimes_k \rho_0(L') \xrightarrow{m} \rho_0(L')[\rho(R)], \tag{4.2.10}$$

where $R \otimes_k L'$ carries the D-module algebra structure $\rho_R \otimes_k \rho_0$ and m is the restriction of the multiplication homomorphism in $\rho_0(L')[\rho(R)] \subseteq \mathsf{Mod}_{\mathsf{C}}(D, L')$. 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 $Z \coloneqq \rho(X)\rho_0(X)^{-1}\rho_0(A)$ and the image of $1 \otimes_k L'$ under this isomorphism is $\rho_0(L')$. Thus, we obtain an isomorphism

$$R \otimes_k L' \xrightarrow{(\bar{\gamma} \circ i_1) \otimes i_2} \bar{\gamma}(R \otimes_k 1) \otimes_k (1 \otimes_k L') \xrightarrow{m \circ (\rho \otimes \rho_0) \otimes m \circ (\rho \otimes \rho_0)} \rho(K)[Z, Z^{-1}] \otimes_k \rho_0(L') \xrightarrow{m} \rho_0(L')[\rho(R)], \tag{4.2.11}$$

where the homomorphism $i_1 \colon R \to R \otimes_k L'$ is defined by $i_1(a) = a \otimes 1$ for all $a \in R$ and $i_2 \colon L' \to R \otimes_k L'$ is defined by $i_2(a) = 1 \otimes a$ for all $a \in L'$. Note that the isomorphism (4.2.11) is different from (4.2.10). Since $\rho(K)[Z, Z^{-1}]$ is a subring of $\mathsf{Mod}_{\mathsf{C}}(D, K')$, it is constant with respect to the D_{ID^n}-module algebra structure $\theta_{\boldsymbol{u}}$ on $\mathsf{Mod}_{\mathsf{C}}(D, L')$. At the other hand, $\rho_0(L')$ is trivial with respect to the D-module algebra structure Ψ_{int} on $\mathsf{Mod}_{\mathsf{C}}(D, L')$. Thus, the isomorphisms in (4.2.11) are isomorphisms of $D \otimes_C D_{ID^n}$-module algebras, where the D-module algebra structure on $R \otimes_k L'$ is given by $\rho_R \otimes_k \rho_0$, on $\bar{\gamma}(R \otimes_k 1) \otimes_k (1 \otimes_k L')$ by $\rho_R \otimes_k \rho_0 \otimes_k \rho_R \otimes_k \rho_0$, on $\rho(K)[Z, Z^{-1}] \otimes_k \rho_0(L)$ by $\rho_{int} \otimes \rho_0$ (which

is equal to $\rho_{int} \otimes \rho_{int}$ there) and on $\rho_0(L')[\rho(R)]$ by ρ_{int}, and the D_{ID^n}-module algebra structure on $R \otimes_k L'$ is given by $\theta_0 \otimes_k \theta_{\boldsymbol{u}}$, on $\bar{\gamma}(R \otimes_k 1) \otimes_k (1 \otimes_k L')$ by $(\theta_0 \otimes_k \theta_0) \otimes_k (\theta_0 \otimes_k \theta_{\boldsymbol{u}})$, on $\rho(K)[Z, Z^{-1}] \otimes_k \rho_0(L')$ by $\theta_0 \otimes_k \theta_{\boldsymbol{u}}$ (which is equal to $\theta_{\boldsymbol{u}} \otimes_k \theta_{\boldsymbol{u}}$ there) and on $\rho_0(L')[\rho(R)]$ by $\theta_{\boldsymbol{u}}$, where θ_0 denotes the trivial n-variate iterative derivations on the corresponding rings.

For every commutative L'-algebra A, the isomorphism (4.2.11) gives rise to an isomorphism of $D \otimes_C D_{ID^n}$-module algebras

$$\rho_0(L)[\rho(R)]\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \to \rho_0(L')[\rho(R)]\hat{\otimes}_{L'} A[\![\boldsymbol{w}]\!] \to (R \otimes_k L')\hat{\otimes}_{L'} A[\![\boldsymbol{w}]\!] \to (R \otimes_k A)[\![\boldsymbol{w}]\!]. \tag{4.2.12}$$

Given a commutative L'-algebra A and a $\varphi \in \text{Inf-Gal}(R/K)(A)$, we obtain by composition with the vertical isomorphisms of $D \otimes_C D_{ID^n}$-module algebras, given by (4.2.12), in the diagram

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

an automorphism of the $D \otimes_C D_{ID^n}$-module algebra $(R \otimes_k A)[\![\boldsymbol{w}]\!]$, where the D-module algebra structure is given by $\rho \otimes_k \rho_0$ on the coefficients with respect to $\boldsymbol{w}$ (as in lemma 2.2.22) and the D_{ID^n}-module algebra structure is given by the n-variate iterative derivation $\theta_{\boldsymbol{w}}$. This automorphism restricts to an automorphism σ of the D-module algebra $R \otimes_k A$ of D_{ID^n}-constants of $(R \otimes_k A)[\![\boldsymbol{w}]\!]$, so that the automorphism of the $D \otimes_C D_{ID^n}$-module algebra $(R \otimes_k A)[\![\boldsymbol{w}]\!]$ is given as $\sigma[\![\boldsymbol{w}]\!]$. Since under the vertical isomorphisms $\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ is isomorphic to $(K \otimes_k A)[\![\boldsymbol{w}]\!]$ and since φ is congruent to the identity modulo $\rho_0(L)[\rho(R)]\hat{\otimes}_L N(A)[\![\boldsymbol{w}]\!]$, we see that σ lies in fact in the kernel (4.2.8).

If, conversely, σ is an element of the kernel (4.2.8), then $\sigma[\![\boldsymbol{w}]\!]$ is an automorphism of the $D \otimes_C D_{ID^n}$-module algebra $(R \otimes_k A)[\![\boldsymbol{w}]\!]$ and using the vertical isomorphisms in the diagram above we obtain an element of $\text{Inf-Gal}(R/K)(A)$.

It is clear that these constructions are inverse to each other, yielding an isomorphism of groups between Inf-Gal$(R/K)(A)$ and (4.2.8). □

Corollary 4.2.7. *Let L/K be a Picard-Vessiot extension of D-module fields such that K is perfect and such that the field L is finitely generated over K. We denote the field of constants by k and by $G := \mathrm{Gal}(L/K)$ the Galois group scheme of L/K. Then there exists a finite separable field extension L' of L such that* Inf-Gal$(L/K) \times_L L'$ *is isomorphic to the formal group scheme $\hat{G}_{L'}$ associated to the base extension $G_{L'} = G \times_k L'$ of G.*

Proof. This follows from theorem 4.2.6 and proposition B.3.2. □

Corollary 4.2.8. *Under the assumptions of corollary 4.2.7 there exists a finite separable field extension L' of L and an isomorphism*

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

Proof. This follows immediately from theorem 4.2.6 by taking $A = L'[\varepsilon]/(\varepsilon^2)$, noting that

$$\mathrm{Lie}(\mathrm{Gal}(L/K)) \otimes_k L' \cong \mathrm{Ker}\left(\mathrm{Gal}(L/K)(L'[\varepsilon]/(\varepsilon^2)) \to \mathrm{Gal}(L/K)(L')\right).$$

□

In the case where $D = D_{end}$, the statement of corollary 4.2.8 is similar to the one of [Mor09, Theorem 3.3]. The statement of the latter is stronger, namely the claim is that Inf-Gal$(L/K)(L[\varepsilon]/(\varepsilon^2))$ is isomorphic to the Lie algebra of $\mathrm{Gal}(L/K) \otimes_k L$, but the proof given there is difficult to follow. Taking $D = D_{der}$, it provides a similar result as [Ume96a, Theorem 5.15] in the case of finitely generated Picard-Vessiot extensions of differential fields in characteristic zero.

Appendices

Appendix A

Linear topological rings

Since we do not know an adequate reference that covers all we need, we give a short introduction to linear topological rings, their completions and (completed) tensor products of these rings here.

Notation: *In this appendix we assume that all rings are commutative.*

A.1 Linear topological rings and their completion

First, we recall the definition of topological rings (see [Bou71, Chapitre III, §6.3]) and linear topological rings (see [Bou85, Chapitre III, §4.2] or [Gro60, Chapitre 0, 7.1.1]).

Definition A.1.1. *A* topological ring *is a set A carrying a ring structure and a topology such that the maps*

$$\begin{aligned} A \times A \to A \quad (x, y) \mapsto x + y, \\ A \to A \quad x \mapsto -x \end{aligned}$$

and

$$A \times A \to A \quad (x, y) \mapsto xy$$

are continuous. A topological ring A is said to be linearly topologized *(and then A is called a* linear topological ring*) if there exists a fundamental system of neighborhoods of 0 consisting of ideals of A.*

Let A be a linear topological ring and $\mathcal{B}$ a fundamental system of neighborhoods of 0 consisting of ideals of A. Then the elements of $\mathcal{B}$ are open and closed in A (see [Bou71, Chapter III, §2.1, Corollaire to Proposition 4]) and the system $(A/I)_{I\in\mathcal{B}}$ together with the canonical homomorphisms $A/I \to A/J$ for $I \subseteq J$ forms an inverse system of discrete topological rings (where $\mathcal{B}$ is ordered by inclusion). With this notation, the inverse limit

$$\hat{A} \coloneqq \varprojlim_{I\in\mathcal{B}} A/I$$

is the completion *of A.*

There exists a canonical homomorphism $A \to \hat{A}$ such that for every open ideal $I \trianglelefteq A$ the composition $A \to \hat{A} \to A/I$ is the canonical projection $A \to A/I$. So there exists an ideal $\bar{I} \trianglelefteq \hat{A}$ such that $\hat{A}/\bar{I} \cong A/I$. The ideals $\bar{I}$ form a filtered system and we give $\hat{A}$ the linear topology such that they form a base of neighborhoods of zero. We say that A is complete *(or a* formal ring*, cf. [Str99]) if the homomorphism $A \to \hat{A}$ is an isomorphism.*

We denote by LRng *the category of linear topological rings with morphisms the continuous ring homomorphism and by* FRng *the full subcategory of* LRng *consisting of formal rings.*

Lemma A.1.2. *For every morphism $f\colon R \to S$ in* LRng *there exists a unique $\hat{f}\colon \hat{R} \to \hat{S}$ such that the diagram*

$$\begin{array}{ccc} \hat{R} & \xrightarrow{\hat{f}} & \hat{S} \\ \uparrow & & \uparrow \\ R & \xrightarrow{f} & S \end{array} \tag{A.1.1}$$

commutes.

Proof. Since f is continuous, for every open ideal $J \trianglelefteq S$ there exists an open ideal $I \trianglelefteq R$ such that $f(I) \subseteq J$ and thus we obtain a homomorphism $R/I \to$

S/J. By composition with the canonical projection $\hat{R} \to R/I$ we obtain a family of compatible homomorphisms $\hat{R} \to S/J$ for every open ideal J in S. By the universal property of the inverse limit $\hat{S} = \varprojlim S/J$ we obtain a unique homomorphism $\hat{f}\colon \hat{R} \to \hat{S}$ such that the compositions $\hat{R} \to \hat{S} \to S/J$ and $\hat{R} \to R/I \to S/J$ coincide for all open ideals J in S. For every open ideal $J \trianglelefteq S$ the composition $R \xrightarrow{f} S \to \hat{S} \to S/J$ coincides with $R \to \hat{R} \xrightarrow{\hat{f}} \hat{S} \to S/J$ by definition of $\hat{f}$. Thus, by the universal property of $\hat{S} = \varprojlim S/J$ both families give rise to the same morphism from R to $\hat{S}$. But these are exactly the two morphisms $R \to \hat{R} \xrightarrow{\hat{f}} \hat{S}$ and $R \xrightarrow{f} S \to \hat{S}$ in diagram A.1.1. □

Proposition A.1.3. *The functor* LRng $\to$ FRng *sending R to $\hat{R}$ and f to $\hat{f}$ is left adjoint to the inclusion of* FRng *in* LRng.

Proof. See for example [Str99, Proposition 4.21 (d)]. □

A.2 The completed tensor product of linear topological rings

Next, we treat tensor products of linear topological rings and their completions. References for this material include [BH96] and [Gro60, Chapitre 0, §7.7].

Proposition A.2.1. *If $S \leftarrow R \to T$ is a diagram in* LRng, *the tensor product $S \otimes_R T$ has a structure of a linear topological ring with a fundamental system of neighborhoods of 0 given by the ideals $I \otimes_R T + S \otimes_R J$ for open ideals $I \trianglelefteq S$ and $J \trianglelefteq T$. Furthermore, $S \otimes_R T$ is the coproduct of S and T over R in* LRng.

Proof. This can be proven as in [Gro60, Chapitre 0, 7.7.6]. □

Proposition A.2.2. *The tensor product of linear topological rings defined in proposition A.2.1 is associative.*

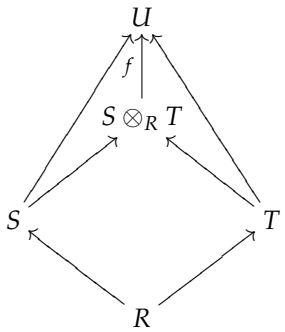
Proof. Let $S_1 \leftarrow R_1 \to S_2 \leftarrow R_2 \to S_3$ be a diagram in LRng. It is well known that $(S_1 \otimes_{R_1} S_2) \otimes_{R_2} S_3$ and $S_1 \otimes_{R_1} (S_2 \otimes_{R_2} S_3)$ are isomorphic as rings. They

are also homeomorphic since if $\mathfrak{a}_1 \trianglelefteq S_1$, $\mathfrak{a}_2 \trianglelefteq S_2$ and $\mathfrak{a}_3 \trianglelefteq S_3$ run through bases of neighborhoods of 0 of the corresponding linear topological rings, then the systems of ideals given by $(\mathfrak{a}_1 \otimes S_2 + S_1 \otimes \mathfrak{a}_2) \otimes S_3 + (S_1 \otimes S_2) \otimes \mathfrak{a}_3$ and $\mathfrak{a}_1 \otimes (S_2 \otimes S_3) + S_1 \otimes (\mathfrak{a}_2 \otimes S_3 + S_2 \otimes \mathfrak{a}_3)$ are bases of neighborhoods of 0 in $(S_1 \otimes_{R_1} S_2) \otimes_{R_2} S_3$ and $S_1 \otimes_{R_1} (S_2 \otimes_{R_2} S_3)$ respectively. □

Definition A.2.3. *For a diagram $S \leftarrow R \rightarrow T$ in* LRng *we define $S \hat{\otimes}_R T$ as the completion of the linear topological ring $S \otimes_R T$ defined in proposition A.2.1 and call it the* completed tensor product.

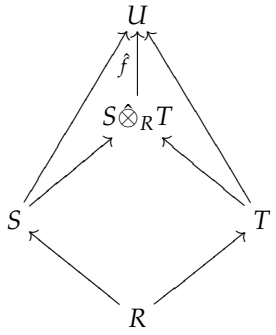
Proposition A.2.4. *For a diagram $S \leftarrow R \rightarrow T$ in* FRng *the completed tensor product $S \hat{\otimes}_R T$ is the coproduct of S and T over R in* FRng.

Proof. Let $U \in$ FRng and let $S \rightarrow U$ and $T \rightarrow U$ be two morphisms in FRng such that the compositions $R \rightarrow T \rightarrow U$ and $R \rightarrow S \rightarrow U$ coincide. By proposition A.2.1 the tensor product $S \otimes_R T$ is the coproduct of $S \leftarrow R \rightarrow T$ in LRng and so there exists a unique homomorphism $f\colon S \otimes_R T \rightarrow U$ such that the diagram



commutes. By lemma A.1.2 there exists a unique extension $\hat{f}\colon S \hat{\otimes}_R T \rightarrow U$ of

f such that the diagram



commutes. Using the uniqueness of the extension of continuous homomorphisms to completions again, we see that $S \to S\hat{\otimes}_R T \leftarrow T$ in fact becomes the coproduct of S and T over R in FRng. □

Lemma A.2.5. *For a diagram $S \leftarrow R \to T$ in LRng we have $\hat{S}\hat{\otimes}_R T \cong S\hat{\otimes}_R T \cong S\hat{\otimes}_R \hat{T}$.*

Proof. The claim follows from the isomorphisms $\hat{S}\hat{\otimes}_R T = \varprojlim_{\bar{I},J} \hat{S}/\bar{I} \otimes_R T/J \cong \varprojlim_{I,J} S/I \otimes_R T/J = S\hat{\otimes}_R T \cong \varprojlim_{I,\bar{J}} S/I \otimes_R \hat{T}/\bar{J} = S\hat{\otimes}_R \hat{T}$, where I (resp. $\bar{I}$, J, $\bar{J}$) runs through a base of neighborhoods of 0 in S (resp. $\hat{S}$, T, $\hat{T}$). □

Proposition A.2.6. *The completed tensor product is associative, i.e. given a diagram $S_1 \leftarrow R_1 \to S_2 \leftarrow R_2 \to S_3$ in LRng we have*

$$(S_1\hat{\otimes}_{R_1} S_2)\hat{\otimes}_{R_2} S_3 \cong S_1\hat{\otimes}_{R_1}(S_2\hat{\otimes}_{R_2} S_3)$$

Proof. Using lemma A.2.5 and proposition A.2.2 we have

$$\begin{aligned}(S_1\hat{\otimes}_{R_1} S_2)\hat{\otimes}_{R_2} S_3 &= (S_1 \otimes_{R_1} S_2)\hat{\otimes}_{R_2} S_3 \\ &= \widehat{(S_1 \otimes_{R_1} S_2)} \otimes_{R_2} S_3 \\ &= S_1 \otimes_{R_1} \widehat{(S_2 \otimes_{R_2} S_3)} \\ &= S_1\hat{\otimes}_{R_1}(S_2 \otimes_{R_2} S_3) \\ &= S_1\hat{\otimes}_{R_1}(S_2\hat{\otimes}_{R_2} S_3).\end{aligned}$$

□

Lemma A.2.7. *Let $S \leftarrow R \rightarrow T$ be a diagram in* CRng*, then*

$$S\hat{\otimes}_R T[\![\boldsymbol{w}]\!] \cong (S \otimes_R T)[\![\boldsymbol{w}]\!] \cong S[\![\boldsymbol{w}]\!]\hat{\otimes}_R T,$$

where we consider S and T as discrete topological rings and $S[\![\boldsymbol{w}]\!]$, $T[\![\boldsymbol{w}]\!]$ and $(S \otimes_R T)[\![\boldsymbol{w}]\!]$ as topological rings with their $(\boldsymbol{w})$-adic topologies.

Proof. Since $\varprojlim_{n\in\mathbb{N}}(S \otimes_R T)[\![\boldsymbol{w}]\!]/(\boldsymbol{w})^n \cong (S \otimes_R T)[\![\boldsymbol{w}]\!]$ the claim follows from the isomorphisms

$$\begin{aligned} S\hat{\otimes}_R T[\![\boldsymbol{w}]\!] &\cong \varprojlim_{n\in\mathbb{N}} (S \otimes_R T[\![\boldsymbol{w}]\!])/(S \otimes_R (\boldsymbol{w})^n) \\ &\cong \varprojlim_{n\in\mathbb{N}} (S \otimes_R T)[\![\boldsymbol{w}]\!]/(\boldsymbol{w})^n \\ &\cong \varprojlim_{n\in\mathbb{N}} (S[\![\boldsymbol{w}]\!] \otimes_R T)/((\boldsymbol{w})^n \otimes_R T) \\ &\cong S[\![\boldsymbol{w}]\!]\hat{\otimes}_R T. \end{aligned}$$

□

Remark A.2.8. *We make frequent use of the following fact: If $S_1 \leftarrow R \rightarrow S_2$ and $T_1 \leftarrow R \rightarrow T_2$ are diagrams in* LRng *and $f_i : S_i \rightarrow T_i$ are morphisms in* LRng *over R, then there exists a morphism $f : S_1\hat{\otimes}_R S_2 \rightarrow T_1\hat{\otimes}_R T_2$ such that the following diagram*

$$\begin{array}{ccc} S_1\hat{\otimes}_R S_2 & \xrightarrow{\hat{f}} & T_1\hat{\otimes}_R T_2 \\ \uparrow & & \uparrow \\ S_i & \xrightarrow{f_i} & T_i \end{array}$$

commutes for $i = 1, 2$. This is clear since we have a homomorphism of R-algebras $S_1 \otimes_R S_2 \rightarrow T_1 \otimes_R T_2$, which we can extend by lemma A.1.2 to a morphism $S_1\hat{\otimes}_R S_2 \rightarrow T_1\hat{\otimes}_R T_2$ in LRng *over R.*

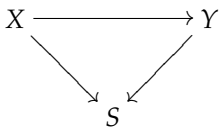
Appendix B

Formal schemes, formal group schemes and formal group laws

In this appendix we recall some basic definitions and facts concerning formal schemes, formal group schemes and formal group laws. We follow mainly [Str99].

B.1 Formal schemes and formal group schemes

Definition B.1.1. *A* formal scheme *is a functor* $X\colon \mathsf{CRng} \to \mathsf{Set}$ *that is a small filtered colimit of affine schemes. Morphisms between formal schemes are natural transformations. We denote by* FSch *the category of formal schemes. Given a formal scheme* S*, we define the category of* formal schemes over S *by taking as objects all morphisms* $X \to S$ *of formal schemes and as morphisms between* $X \to S$ *and* $Y \to S$ *all morphisms* $X \to Y$ *of formal schemes such that*



commutes. We denote the category of formal schemes over X by FSch_X. We call formal schemes over $\operatorname{Spec} R$ *also formal schemes over R and denote the category of formal schemes over R by FSch_R.*

Example B.1.2. *Let R be a commutative ring and I be a set. For $\alpha \in \mathbb{N}^I$ we define $R_\alpha := R[x_i \mid i \in I]/(x_i^{\alpha(i)+1} \mid i \in I)$. Then the filtered colimit*

$$\widehat{\mathbb{A}}_R^I := \varinjlim_{\alpha \in \mathbb{N}^I} \operatorname{Spec} R_\alpha$$

exists and is given by $\widehat{\mathbb{A}}_R^I(A) = N(A)^I$ for any commutative R-algebra A. Therefore, $\widehat{\mathbb{A}}_R^I$ is a formal scheme over $\operatorname{Spec} R$*. In the special case $I = \{1, \dots, n\}$ for $n \in \mathbb{N}$ we denote $\widehat{\mathbb{A}}_R^{\{1,\dots,n\}}$ also by $\widehat{\mathbb{A}}_R^n$.*

Definition B.1.3. *A morphism of formal schemes $f\colon X \to Y$ is a* closed inclusion *if it is a regular monomorphism in* FSch *(i.e. the equalizer of two arrows $Y \rightrightarrows Z$). A* closed formal subscheme *of a formal scheme Y is a subfunctor X of Y such that X is a formal scheme and such that the inclusion $X \hookrightarrow Y$ is a closed inclusion.*

Definition B.1.4. *A* formal group scheme *over a formal scheme S is a group object in* FSch_S.

Proposition B.1.5. *Let R be a commutative ring and $f\colon X \times \widehat{\mathbb{A}}^n \to X \times \widehat{\mathbb{A}}^m$ be a morphism of formal schemes over $X = \operatorname{Spec} R$. Then there exist unique formal power series $f_1, \dots, f_m \in R[\![x_1, \dots, x_n]\!]$ such that for all R-algebras A and all $(u, a_1, \dots, a_n) \in X(A) \times \widehat{\mathbb{A}}^n(A)$ we have*

$$f(u, a_1, \dots, a_n) = (u, (uf_1)(a_1, \dots, a_n), \dots, (uf_m)(a_1, \dots, a_n)) \tag{B.1.1}$$

such that $f_i(0, \dots, 0)$ are nilpotent for $i = 1, \dots, n$.

Conversely, given $f_1, \dots, f_m \in R[\![x_1, \dots, x_n]\!]$ with nilpotent constant terms the formula (B.1.1) *defines a morphism $X \times \widehat{\mathbb{A}}^n \to X \times \widehat{\mathbb{A}}^m$ of formal schemes over X.*

Proof. See [Str06, Prop. 5.6] □

Remark B.1.6. *Let R be a commutative ring. Then there is a natural equivalence between the category* $\mathsf{CAlg}_R\mathsf{Set}$ *of functors from* CAlg_R *to* Set *and the category* $(\mathsf{CRngSet})_{\operatorname{Spec} R}$ *of objects of* $\mathsf{CRngSet}$ *over* $\operatorname{Spec} R$.

Proof. See for example [DG70, I, §1, 6.2] □

B.2 Formal groups laws and their associated formal group schemes

Definition B.2.1. *Let $n \in \mathbb{N} \cup \{\infty\}$. An* n-dimensional formal group law *on a commutative ring R is an n-tuple*

$$F = (f_1, \ldots, f_n) \in R[\![u_1, \ldots, u_n, v_1, \ldots, v_n]\!]^n$$

if $n \in \mathbb{N}$ or an element of $(R[\![u_i, v_i \mid i \in \mathbb{N}]\!])^{\mathbb{N}}$ if $n = \infty$ such that

(1) $F(\boldsymbol{u}, \mathbf{0}) = \boldsymbol{u}$, $F(\mathbf{0}, \boldsymbol{v}) = \boldsymbol{v}$ *and*

(2) $F(\boldsymbol{u}, F(\boldsymbol{v}, \boldsymbol{w})) = F(F(\boldsymbol{u}, \boldsymbol{v}), \boldsymbol{w})$,

where $\boldsymbol{u}$, $\boldsymbol{v}$ and $\boldsymbol{w}$ denote the tuples $(u_1, \ldots, u_n)$, $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_n)$ if $n \in \mathbb{N}$ and $(u_i)_{i\in\mathbb{N}}$, $(v_i)_{i\in\mathbb{N}}$ and $(w_i)_{i\in\mathbb{N}}$ if $n = \infty$, respectively.

Example B.2.2. *For every natural number $n \in \mathbb{N}$ an n-dimensional formal group law is given over every commutative ring R by*

$$f_i(\boldsymbol{u}, \boldsymbol{v}) = u_i + v_i \quad \text{for all } i = \{1, \ldots, n\}.$$

This formal group law is called the additive formal group law *of dimension n over R.*

Lemma B.2.3. *If $n \in \mathbb{N}$ and F is an n-dimensional formal group law on a commutative ring R, there exists $\Psi \in R[\![u_1, \ldots, u_n]\!]^n$ such that $\Psi(\mathbf{0}) = \mathbf{0}$ and $F(\boldsymbol{u}, \Psi(\boldsymbol{u})) = \mathbf{0} = F(\Psi(\boldsymbol{u}), \boldsymbol{u})$.*

Proof. See [Ser65, LG 4.15–4.16]. □

Remark B.2.4. *To an n-dimensional formal group law F on a commutative ring R we associate a formal group scheme over* $\operatorname{Spec} R$ *as follows: We define a functor* $\mathbf{F}\colon \mathsf{CAlg}_R \to \mathsf{Grp}$ *by* $\mathbf{F}(A) := N(A)^n$ *for every commutative R-algebra A. The group multiplication on* $N(A)^n$ *is defined by* $\boldsymbol{ab} := F(\boldsymbol{a}, \boldsymbol{b})$ *for* $\boldsymbol{a}, \boldsymbol{b} \in N(A)^n$ *and the unit is given by* $\mathbf{0} \in N(A)^n$*. Note that this defines in fact a morphism* $\mathbf{F} \times \mathbf{F} \to \mathbf{F}$ *of formal schemes over* $\operatorname{Spec} R$ *by proposition B.1.5 and* $\mathbf{F}$ *becomes a group object in* FSch_R*. As a formal scheme* $\mathbf{F}$ *is isomorphic to* $\widehat{\mathbb{A}}^n_R$*.*

Example B.2.5. *Let R be a commutative ring. We define the* additive formal group scheme *of dimension n, denoted by* $\hat{\mathbb{G}}^n_{a,R}$*, to be the formal group scheme over* $\operatorname{Spec} R$ *induced by the additive formal group law in example B.2.2 via remark B.2.4. Then for every commutative R-algebra A the group multiplication on* $\hat{\mathbb{G}}^n_{a,R}(A) = N(A)^n$ *is given by componentwise addition and the unit is given by* $\mathbf{0} \in N(A)^n$*. If the ring R is equal to $\mathbb{Z}$ or clear from the context, we will denote* $\hat{\mathbb{G}}_{a,R}$ *also by* $\hat{\mathbb{G}}_a$*.*

B.3 The formal group scheme attached to a group scheme

Definition B.3.1. *Let R be a commutative ring and G be an affine group scheme over R. We define a formal scheme $\hat{G}$ over R as*

$$\hat{G} := \varinjlim_{n \in \mathbb{N}} \operatorname{Spec} C[G]/m_e^n,$$

where $C[G]$ is the coordinate ring of G and m_e is the kernel of the counit $\varepsilon\colon C[G] \to R$.

Proposition B.3.2. *Let R be a commutative ring and G be a Noetherian affine group scheme over R. Then for the formal scheme $\hat{G}$ associated to G there is an isomorphism*

$$\hat{G}(A) \cong \operatorname{Ker}(G(A) \to G(A/N(A)))$$

for every commutative R-algebra A.

Proof. For all commutative R-algebras A we have

$$\begin{aligned}
\hat{G}(A) &= \varinjlim_{n\in\mathbb{N}} \mathrm{Spec}(C[G]/m_e^n)(A) \\
&\cong \varinjlim_{n\in\mathbb{N}} \mathsf{CAlg}_R(C[G]/m_e^n, A) \\
&\cong \varinjlim_{n\in\mathbb{N}} \{f \in \mathsf{CAlg}_R(C[G], A) \mid f(m_e^n) = 0\} \\
&\cong \{f \in \mathsf{CAlg}_R(C[G], A) \mid \exists n \in \mathbb{N} : f(m_e^n) = 0\} \\
&= \{f \in \mathsf{CAlg}_R(C[G], A) \mid \exists n \in \mathbb{N} : f(m_e)^n = 0\}.
\end{aligned} \tag{B.3.1}$$

At the other side, for every commutative R-algebra A the kernel of $G(A) \to G(A/N(A))$ consists of all elements f of $\mathsf{CAlg}_R(C[G], A)$ that make the diagram

$$\begin{array}{ccc}
C[G] & \xrightarrow{\quad f \quad} & A \\
\downarrow{\scriptstyle \varepsilon} & & \\
R & & \downarrow{\scriptstyle \pi_A} \\
\downarrow & & \\
A & \xrightarrow{\quad \pi_A \quad} & A/N(A),
\end{array}$$

commutative, where $\varepsilon\colon C[G] \to R$ denotes the counit of $C[G]$. Thus, it remains to show that for $f \in \mathsf{CAlg}_R(C[G], A)$ this diagram commutes if and only if $f(m_e)^n = 0$ for some $n \in \mathbb{N}$. Since $C[G]/m_e \cong R$, we have an isomorphism of R-modules $C[G] \cong R \oplus m_e$. The compositions of the homomorphisms in the diagram coincide when restricted to $R \subseteq C[G]$. Since $\pi_A \circ \varepsilon(m_e) = 0$, the diagram commutes if and only if $\pi_A \circ f(m_e) = 0$, i.e. if $f(m_e) \subseteq N(A)$. Since $C[G]$ is Noetherian, the ideal m_e is finitely generated and thus $f(m_e) \subseteq N(A)$ if and only if $f(m_e)^n = 0$ for some $n \in \mathbb{N}$. □

Proposition B.3.3. *If R is a commutative ring and G an affine group scheme over R, then $\hat{G}$ is a formal group scheme over R and we call it the* formal group scheme associated to *G.*

Proof. We only have to show that $\hat{G}$ is a group object in FSch_R. From proposition B.3.2 one easily sees that $\hat{G}(A)$ is a group for all commutative R-algebras A. Since finite fiber products exist in FSch_R and coincide with those in RngSet by [Str99, Proposition 4.12], we see that $(\hat{G} \times_R \hat{G})(A) = \hat{G}(A) \times_R \hat{G}(A)$ for all R-algebras A and from the group multiplication in $\hat{G}(A)$ we obtain a morphism $m\colon \hat{G} \times_R \hat{G} \to \hat{G}$. From the unit in $\hat{G}(A)$ for all R-algebras A we obtain a morphism $e\colon \operatorname{Spec} R \to \hat{G}$. Then $(\hat{G}, m, e)$ is easily seen to be a group object in FSch_R. □

Example B.3.4. *For every commutative ring R and every $n \in \mathbb{N}$, the formal group scheme associated to the n-dimensional additive affine group scheme $\mathbb{G}_a^n$ over R is isomorphic to the additive formal group scheme that is associated to the n-dimensional additive formal group law over R (cf. examples B.2.2 and B.2.5).*

Resumen en castellano

Introducción

La teoría de Galois se remonta a principios del siglo XIX cuando E. Galois determinó condiciones en términos de teoría de grupos para la resolubilidad por radicales de ecuaciones polinomiales. Dado un cuerpo K y un polinomio separable $f \in K[X]$ existe un cuerpo L, extensión de K, llamado cuerpo de descomposición de f, que está generado sobre K por las raíces de f. El grupo $G = \mathrm{Aut}(L/K)$ de los automorfismos del cuerpo L que dejan fijo el cuerpo K opera sobre el conjunto de las raíces de f. Se pueden interpretar los elementos de G como permutaciones de las raíces de f que respetan las relaciones algebraicas sobre K entre las raíces de f. Existe una biyección entre los subgrupos de G y los cuerpos intermedios de la extensión L/K.

El desarrollo de una teoría de Galois para ecuaciones diferenciales análoga a la de ecuaciones polinomiales fue ya un objectivo de S. Lie. El primer paso en esta dirección, debido a E. Picard y E. Vessiot, fue el desarrollo de una teoría de Galois para ecuaciones diferenciales lineales. Desde los años cuarenta del siglo XX se desarrolló esta teoría que figura ya en libros de texto como [vdPS03] o [CH07], por mencionar sólo los dos últimos publicados. A mediados del siglo pasado E. Kolchin definió extensiones fuertemente normales de cuerpos diferenciales y desarrolló una teoría de Galois para estas extensiones, que incluyen ciertas extensiones de cuerpos diferenciales que provienen de ecuaciones diferenciales no lineales ([Kol76]). Inspirado en el trabajo de E. Vessiot ([Ves46]),

H. Umemura desarrolló una teoría de Galois para tratar ecuaciones diferenciales algebraicas no lineales ([Ume96a]). Unos años más tarde, B. Malgrange, con un fin parecido, publicó su propia teoría de Galois diferencial usando el lenguaje de la geometría diferencial ([Mal01], [Mal02]). G. Casale siguió desarrollando y aplicando esta teoría ([Cas04], [Cas07], [Cas08]). Recientemente, H. Umemura comparó su teoría con la de B. Malgrange y mostró que están estrechamente relacionadas ([Ume08]).

Existen también teorías análogas para ecuaciones en diferencias. Su elaboración fue iniciada por C. H. Franke, quien desarrolló una teoría de Galois para ecuaciones lineales en diferencias ([Fra63]), llamada también teoría de Picard-Vessiot.[1] Más tarde, R. Infante definió extensiones fuertemente normales de cuerpos en diferencias y desarrolló una teoría de Galois para estas extensiones ([Inf80b], [Inf80a]). Últimamente, S. Morikawa y H. Umemura elaboraron una teoría análoga a la de éste último para ecuaciones algebraicas no lineales en diferencias ([Mor09], [MU09]). Siguiendo el enfoque de B. Malgrange, G. Casale y A. Granier desarrollaron teorías de Galois para ecuaciones no lineales en (q-)diferencias ([Cas06], [Gra09]).

Las teorías mencionadas hasta ahora se restringían a cuerpos de característica cero. En característica positiva las derivaciones clásicas no se comportan bien. H. Hasse y F. K. Schmidt introdujeron derivaciones iterativas ([HS37]) como alternativa a las derivaciones clásicas. Posteriormente, K. Okugawa, B. H. Matzat y M. van der Put desarrollaron teorías de Galois para ecuaciones diferenciales en característica positiva usando derivaciones iterativas ([Oku87], [Mat01], [MvdP03]). Recientemente, A. Maurischat y el autor ampliaron la teoría de B. H. Matzat y M. van der Put ([Rös07], [Hei07], [Mau10a], [Mau10b]). Estas teorías se restringen a ecuaciones diferenciales iterativas *lineales*.

M. Takeuchi desarrolló una teoría de Picard-Vessiot que unifica las teorías de Picard-Vessiot para ecuaciones diferenciales en característica cero y pa-

[1] Se suele llamar a las teorías de Galois en situaciones "lineales" *teorías de Picard-Vessiot*.

ra ecuaciones diferenciales iterativas en característica arbitraria usando cuerpos C-ferenciales, donde C es una cierta coálgebra ([Tak89]). Recientemente, K. Amano y A. Masuoka ampliaron la teoría de M. Takeuchi usando D-módulo álgebras, donde D es cierta álgebra de Hopf ([Ama05], [AM05], [AMT09]). Su teoría unifica las teorías de Picard-Vessiot para ecuaciones diferenciales en característica cero y para ecuaciones diferenciales iterativas en característica arbitraria, así como también para ecuaciones en diferencias en el caso en que el operador en diferencias es un automorfismo.

En resumen, el desarrollo de la teoría de Galois diferencial y en diferencias tomó dos direcciones. Por un lado se crearon teorías para tratar extensiones de cuerpos más generales debido a H. Umemura y S. Morikawa. Por otro lado M. Takeuchi, K. Amano y A. Masuoka unificaron las teorías de Picard-Vessiot de extensiones de cuerpos (y ciertos anillos) diferenciales, dotados de una derivación iterativa y dotados de un automorfismo.

Esta tesis tiene dos objetivos principales. El primero es el desarrollo de una teoría de Galois más general que combine la capacidad de las teorías de H. Umemura y S. Morikawa, que permite tratar extensiones de cuerpos de gran generalidad, con la ventaja de la formulación de K. Amano y A. Masuoka que unifica estructuras como las derivaciones y los automorfismos. El segundo objetivo es el de eliminar la restricción a cuerpos de característica cero de las teorías de H. Umemura y S. Morikawa.

Resumen de los contenidos

Capítulo 1

En el primer capítulo introducimos derivaciones superiores y derivaciones iterativas. H. Hasse y F. K. Schmidt definieron derivaciones superiores y derivaciones iterativas sobre un anillo R como una sucesión de aplicaciones $\partial^{(k)}\colon R \to R$ para cada $k \in \mathbb{N}$ que cumplen ciertas propiedades. Estas aplicaciones dan lugar a un homomorfismo de anillos $\theta\colon R \to R[\![t]\!]$ que envía $a \in R$

a la serie formal $\sum_{k\in\mathbb{N}} \partial^{(k)}(a)t^k$. De hecho, dar una derivación superior en R es equivalente a dar un homomorfismo de anillos

$$\theta\colon R \to R[\![t]\!], \tag{1}$$

y dar una derivación iterativa es equivalente a dar un homomorfismo de anillos $\theta\colon R \to R[\![t]\!]$ que cumple condiciones adicionales. Si R contiene $\mathbb{Q}$, las derivaciones iterativas $(\partial^{(k)})_{k\in\mathbb{N}}$ están determinadas por $\partial^{(1)}$ y el homomorfismo correspondiente es

$$\theta\colon R \to R[\![t]\!], \quad a \mapsto \sum_{k\in\mathbb{N}} \frac{{\partial^{(1)}}^k(a)}{k!}t^k \tag{2}$$

Definimos *derivaciones superiores n-variadas* como homomorfismos de anillos $R \to R[\![t_1, \dots t_n]\!]$ y *derivaciones iterativas n-variadas* como derivaciones superiores n-variadas que cumplen condiciones adicionales que generalizan las condiciones del caso univariado. Mostramos propiedades fundamentales de estas derivaciones superiores e iterativas n-variadas. Por ejemplo demostramos que se extienden a extensiones étales. De esto se deduce que las derivaciones iterativas con respecto a las variables de los anillos de polinomios se extienden al cuerpo de funciones racionales y por tanto obtenemos una derivación iterativa $\theta_{\boldsymbol{u}}$ para cada base de trascendencia separable $\boldsymbol{u} = (u_1, \dots, u_n)$ de una extensión separable y finitamente generada de cuerpos.

Capítulo 2

En el segundo capítulo introducimos el concepto de módulo álgebras. Sea C un álgebra conmutativa, D una biálgebra y R una C-álgebra conmutativa. Recordemos que se tiene la biyección

$$\mathsf{Mod}_C(D \otimes_C R, R) \to \mathsf{Mod}_C(R, \mathsf{Mod}_C(D, R)), \quad \Psi \mapsto (a \mapsto (d \mapsto \Psi(d \otimes a))). \tag{3}$$

Si $\Psi \in \mathsf{Mod}_C(D \otimes_C R, R)$ y ρ es el elemento en $\mathsf{Mod}_C(R, \mathsf{Mod}_C(D, R))$ que corresponde a Ψ por esta biyección, ρ es un homomorfismo de C-álgebras (con

respecto a la estructura de álgebra en $\mathsf{Mod}_C(D,R)$ inducida por la estructura de coálgebra de D) si y solo si Ψ cumple para cada $d \in D$ y $a, b \in R$ las dos condiciones siguientes

(1) $\Psi(d \otimes ab) = \sum_{(d)} \Psi(d_{(1)} \otimes a)\Psi(d_{(2)} \otimes b)$

(2) $\Psi(d \otimes 1) = \varepsilon(d)1$.

Si además Ψ induce una estructura de D-módulo en R, decimos que Ψ es una *estructura de D-módulo álgebra* en R. La C-álgebra $\mathsf{Mod}_C(D,R)$ posee una estructura de D-módulo álgebra

$$\Psi_{int} \colon D \otimes_C \mathsf{Mod}_C(D,R) \to \mathsf{Mod}_C(D,R)$$

definida por

$$\Psi_{int}(d \otimes f) \colon D \to R, \quad c \mapsto f(cd) \quad \text{para cada } c \in D$$

para cada $d \otimes f \in D \otimes \mathsf{Mod}_C(D,R)$.

Ejemplo: *Si D_{der} es la C-biálgebra subyacente al álgebra de Hopf $C[\mathbb{G}_a] =: C[x]$, entonces dotar a R de una estructura de D_{der}-módulo álgebra es equivalente a dotarla de una C-derivación. Dada una C-derivación ∂ en R, se obtiene una estructura de D_{der}-módulo álgebra Ψ en R, definida por $\Psi(x \otimes a) := \partial(a)$ para $a \in R$. Si R contiene $\mathbb{Q}$, entonces $\mathsf{Mod}_C(D_{der}, R)$ es isomorfo a $R[\![t]\!]$ y la composición*

$$R \xrightarrow{\rho} \mathsf{Mod}_C(D_{der}, R) \longrightarrow R[\![t]\!]$$

es la derivación iterativa (2) *inducida por la derivación ∂.*

También se pueden describir derivaciones superiores, derivaciones iterativas, endomorfismos de álgebras, automorfismos de álgebras, σ-derivaciones y otras estructuras en términos de módulo álgebras.

Mostramos propiedades de módulo álgebras que usamos en el capítulo 3 y damos una lista de biálgebras que dan lugar a módulo álgebras interesantes.

Capítulo 3

El tercer capítulo es la parte principal de la tesis. Dada cierta extensión de módulo cuerpos (es decir, módulo álgebras, que son cuerpos) definimos una normalización de esta extensión y un grupo de Galois infinitesimal.

Sea C un álgebra conmutativa, D una C-biálgebra coconmutativa y L/K una extensión de D-módulo cuerpos tal que L/K sea finitamente generada y separable. Entonces L posee una base de transcendencia separante $\boldsymbol{u} = (u_1, \ldots, u_n)$. Sea $\theta_{\boldsymbol{u}}$ la derivación iterativa n-variada con respecto a esta base de transcendencia separante. Entonces $\theta_{\boldsymbol{u}}$ induce una derivación iterativa n-variada en $\mathsf{Mod}_{\mathsf{C}}(D, L)$. Definimos $\mathcal{K}$ como la subálgebra de $\mathsf{Mod}_{\mathsf{C}}(D, L)$ generada por $\rho_0(L)$ y $\rho(K)$ (donde $\rho_0 \colon L \to \mathsf{Mod}_{\mathsf{C}}(D, L)$ está definido por $(\rho_0(a))(d) = \varepsilon(d)a$ para cada $d \in D$ y $a \in L$). Entonces $\mathcal{K}$ es una D-módulo subálgebra de $\mathsf{Mod}_{\mathsf{C}}(D, \Psi_{int})$ estable por la derivación iterativa n-variada $\theta_{\boldsymbol{u}}$. Definimos también $\mathcal{L}$ como subálgebra diferencial iterativa de $\mathsf{Mod}_{\mathsf{C}}(D, L)$ generada por $\rho_0(L)$ y $\rho(L)$. La extensión $\mathcal{L}/\mathcal{K}$ es la normalización mencionada anteriormente. Definimos el grupo de Galois infinitesimal como el funtor $\text{Inf-Gal}(L/K) \colon \mathsf{CAlg}_{\mathsf{L}} \to \mathsf{Grp}$ que tiene como A-puntos el grupo de automorfismos φ de la $D \otimes_C D_{ID^n}$-módulo álgebra[2] $\mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!]$ que hacen conmutativo el diagrama

$$\begin{array}{ccccc}
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\text{id}} & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] \\
\downarrow{\scriptstyle \text{id}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \text{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]} \\
\mathcal{K}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \hookrightarrow & \mathcal{L}\hat{\otimes}_L A[\![\boldsymbol{w}]\!] & \xrightarrow{\text{id}_{\mathcal{L}} \hat{\otimes} \pi_A[\![\boldsymbol{w}]\!]} & \mathcal{L}\hat{\otimes}_L (A/N(A))[\![\boldsymbol{w}]\!].
\end{array}$$

Demostramos que el funtor $\text{Inf-Gal}(L/K)$ es un funtor de Lie-Ritt y por tanto un esquema formal en grupos.

Nuestros resultados recuperan los de H. Umemura y S. Morikawa al restringirse a las situaciones correspondientes.

[2] D_{ID^n} es una C-biálgebra tal que las D_{ID^n}-módulo álgebras son equivalentes a derivaciones iterativas n-variadas sobre C.

Capítulo 4

En el cuarto capítulo describimos explícitamente el álgebra $\mathcal{L}$ y comparamos el esquema en grupos de una extensión de Picard-Vessiot de módulo cuerpos con el grupo de Galois infinitesimal definido anteriormente.

Sea L/K una extensión de D-módulo cuerpos separable, finitamente generada y de Picard-Vessiot en el sentido de Amano-Masuoka ([AM05]) con álgebra principal R y cuerpo de constantes k. Mostramos lo siguiente:

(1) El álgebra $\rho_0(L)[\rho(L)]$ es cerrada por θ_u, es decir $\mathcal{L} = \rho_0(L)[\rho(L)]$, y las subálgebras $\rho_0(L)$ y $\rho(L)$ son linealmente disjuntas sobre k; se tiene por tanto un isomorfismo de D-módulo álgebras

$$\mathcal{L} = \rho_0(L)[\rho(L)] \cong \rho_0(L) \otimes_k \rho(L). \tag{4}$$

(2) Análogamente $\rho_0(L)[\rho(R)]$ es cerrado por θ_u y las álgebras $\rho_0(L)$ y $\rho(R)$ son linealmente disjuntas sobre k; tenemos un isomorfismo de D-módulo álgebras

$$\rho_0(L)[\rho(R)] \cong \rho_0(L) \otimes_k \rho(R). \tag{5}$$

(3) Sea $G \coloneqq \mathrm{Gal}(L/K)$ el esquema en grupos de Galois de la extensión de Picard-Vessiot L/K. Si K es perfecto, entonces existe un cuerpo L', extensión finita separable de L, tal que $\text{Inf-Gal}(L/K) \otimes_L L'$ es isomorfo al esquema en grupos formal $\hat{G}_{L'}$ asociado a la extensión de base $G_{L'} = G \times_k L'$ de G.

Apéndices

En el apéndice A recopilamos definiciones sobre anillos topológicos lineales y productos tensoriales completados y en el apéndice B fijamos las definiciones concernientes a esquemas formales, esquemas formales en grupos, y leyes formales de grupos.

Bibliography

[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. `arXiv:math/0503291`.

[AMT09] Katsutoshi Amano, Akira Masuoka, and Mitsuhiro Takeuchi. Hopf algebraic approach to Picard-Vessiot theory. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 127–171. Elsevier/North-Holland, Amsterdam, 2009. Available from: `http://dx.doi.org/10.1016/S1570-7954(08)00204-0`, `doi:10.1016/S1570-7954(08)00204-0`.

[And01] Yves André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Ann. Sci. École Norm. Sup. (4)*, 34(5):685–739, 2001.

[BH96] George M. Bergman and Adam O. Hausknecht. *Cogroups and corings in categories of associative rings*, volume 45 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1996.

[Bou70] Nicolas Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3*. Hermann, Paris, 1970.

[Bou71] N. Bourbaki. *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*. Hermann, Paris, 1971.

[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.

[Cas04] Guy Casale. *Sur le groupoïde de Galois d'un feuilletage*. PhD thesis, Université Paul Sabatier, Toulouse, 2004.

[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 groupoïde de Galois de P_1 et son irréductibilité. *Comment. Math. Helv.*, 83(3):471–519, 2008.

[Cau03] Gérard Cauchon. Effacement des dérivations et spectres premiers des algèbres quantiques. *J. Algebra*, 260(2):476–518, 2003. Available from: `http://dx.doi.org/10.1016/S0021-8693(02)00542-2`, `doi:10.1016/S0021-8693(02)00542-2`.

[CH07] Teresa Crespo and Zbigniew Hajto. *Introduction to Differential Galois Theory*. Wydawnictwo PK, Cracow, 2007.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris, 1970. Avec un appendice *Corps de classes local* par Michiel Hazewinkel.

[Fra63] Charles H. Franke. Picard-Vessiot theory of linear homogeneous difference equations. *Trans. Amer. Math. Soc.*, 108:491–515, 1963.

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

[Gro60] Alexander Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[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.

[Har10] Charlotte Hardouin. Iterative q-difference galois theory. *J. Reine Angew. Math.*, 2010. Ahead of Print. Available from: `http://dx.doi.org/10.1515/CRELLE.2010.053`.

[Hay08] Heidi Haynal. PI degree parity in q-skew polynomial rings. *J. Algebra*, 319(10):4199–4221, 2008. Available from: `http://dx.doi.org/10.1016/j.jalgebra.2008.01.036`, `doi:10.1016/j.jalgebra.2008.01.036`.

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

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

[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.

[Inf80a] Ronald P. Infante. Strong normality and normality for difference fields. *Aequationes Math.*, 20(2-3):159–165, 1980. Available from: `http://dx.doi.org/10.1007/BF02190510`, `doi:10.1007/BF02190510`.

[Inf80b] Ronald R. Infante. The structure of strongly normal difference extensions. *Aequationes Math.*, 21(1):16–19, 1980. Available from: `http://dx.doi.org/10.1007/BF02189335`, `doi:10.1007/BF02189335`.

[Kas95] Christian Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Kol76] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1976.

[Mal01] Bernard Malgrange. Le groupoïde 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.

[Mal02] Bernard Malgrange. On nonlinear differential Galois theory. *Chinese Ann. Math. Ser. B*, 23(2):219–226, 2002. Dedicated to the memory of Jacques-Louis Lions.

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

[Mat01] Bernd Heinrich Matzat. *Differential Galois Theory in Positive Characteristic*. 2001. IWR-Preprint No. 2001-35. Available from: `http://www.iwr.uni-heidelberg.de/organization/sfb359/Preprints2001.html`.

[Mau10a] Andreas Maurischat. Galois theory for iterative connections and nonreduced Galois groups. *Trans. Amer. Math. Soc.*, 362:5411–5453, 2010.

[Mau10b] Andreas Maurischat. Infinitesimal group schemes as iterative differential Galois groups. *J. Pure Appl. Algebra*, 214:2092–2100, 2010.

[Mon93] Susan Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1993.

[Mor09] Shuji Morikawa. On a general difference Galois theory I. *Ann. Inst. Fourier (Grenoble)*, 59(7):2709–2732, 2009. Available from: `http://aif.cedram.org/aif-bin/item?id=AIF_2009__59_7_2709_0`.

[MS09] Rahim Moosa and Thomas Scanlon. Generalised Hasse varieties and their jet spaces. 2009. `arXiv:0908.4230v1`.

[MS10] Rahim Moosa and Thomas Scanlon. Jet and prolongation spaces. *J. Inst. Math. Jussieu*, 9(2):391–430, 2010. Available from: `http://dx.doi.org/10.1017/S1474748010000010`, `doi:10.1017/S1474748010000010`.

[MU09] Shuji Morikawa and Hiroshi Umemura. On a general difference Galois theory II. *Ann. Inst. Fourier (Grenoble)*, 59(7):2733–2771, 2009. Available from: `http://aif.cedram.org/aif-bin/item?id=AIF_2009__59_7_2733_0`.

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

[MW95] Margit Messmer and Carol Wood. Separably closed fields with higher derivations. I. *J. Symbolic Logic*, 60(3):898–910, 1995.

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

[Rös07] Andreas Röscheisen. *Iterative Connections and Abhyankar's Conjecture*. PhD thesis, Universität Heidelberg, Fakultät für Mathematik und Informatik, 2007.

[Ser65] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1964 of *Lectures given at Harvard University*. W. A. Benjamin, Inc., New York-Amsterdam, 1965.

[Str99] Neil P. Strickland. Formal schemes and formal groups. In *Homotopy invariant algebraic structures (Baltimore, MD, 1998)*, volume 239 of *Contemp. Math.*, pages 263–352. Amer. Math. Soc., Providence, RI, 1999.

[Str06] Neil P. Strickland. Formal groups, 2006. Available at `http://neil-strickland.staff.shef.ac.uk/courses/formalgroups/fg.pdf`.

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

[Tak89] Mitsuhiro Takeuchi. A Hopf algebraic approach to the Picard-Vessiot theory. *J. Algebra*, 122(2):481–509, 1989.

[Ume96a] Hiroshi Umemura. Differential Galois theory of infinite dimension. *Nagoya Math. J.*, 144:59–135, 1996.

[Ume96b] Hiroshi Umemura. Galois theory of algebraic and differential equations. *Nagoya Math. J.*, 144:1–58, 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.

[Ume07] Hiroshi Umemura. Invitation to Galois theory. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 269–289. Eur. Math. Soc., Zürich, 2007.

[Ume08] Hiroshi Umemura. Sur l'équivalence des théories de Galois différentielles générales. *C. R. Math. Acad. Sci. Paris*, 346(21-22):1155–1158, 2008.

[vdE00] Arno van den Essen. *Polynomial automorphisms and the Jacobian conjecture*, volume 190 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000.

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

[Ves46] Ernest Vessiot. Sur une théorie générale de la réductibilité des équations et systèmes d'équations finies ou différentielles. *Ann. Sci. École Norm. Sup. (3)*, 63:1–22, 1946.

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

[Zie03] Martin Ziegler. Separably closed fields with Hasse derivations. *J. Symbolic Logic*, 68(1):311–318, 2003.

Index