Picard-Vessiot categories and Galois groups

Habilitationsschrift

vorgelegt von

Dr. rer. nat. Andreas Maurischat

aus Heidenheim

Contents

1 Introduction **1**

1.1 General overview 2
1.2 Picard-Vessiot theory for linear differential equations 5
1.3 Partial differential equations 10
1.4 Picard-Vessiot theory for iterative differential equations 11
1.5 Picard-Vessiot theory for difference equations 12
1.6 Non-algebraically closed constants 14
1.7 Further transcendental Galois theories 17
1.7.1 Modules with connections 18
1.7.2 Noncommutative differentials and connections 18
1.7.3 Iterative higher differentials and Iterative higher connection 18
1.7.4 Hopf-algebraic approach 18
1.8 The inverse Galois problem 20
1.8.1 In differential Galois theory 20
1.8.2 In iterative differential Galois theory 22
1.8.3 In difference Galois theory 23

2 Categorical Picard-Vessiot theory **24**

2.1 A commutative algebra theorem 25
2.2 Setup and basic properties 28
2.3 $\mathcal{C}$-algebras and base change 33
2.4 Solution rings and Picard-Vessiot rings 36
2.5 Picard-Vessiot rings and fibre functors 45
2.6 Galois group schemes 49
2.7 Galois correspondence 53

3 Picard-Vessiot theory over simple iterative differential rings **56**

3.1 Basic notation 57
3.2 Properties of ID-simple rings 59

3.3 The category of modules with iterative derivation 61
3.4 Picard-Vessiot rings 64
3.5 The differential Galois group scheme 67
3.6 Galois correspondence 69
3.7 Example 74
3.7.1 An ID-simple ring having non-free projective modules . . . 74
3.7.2 A non-free ID-module over S in characteristic zero 75
3.7.3 Picard-Vessiot rings and Galois groups for this ID-module 76
3.7.4 A non-free ID-module over S in positive characteristic . . 78

4 Finite inverse problem in iterative differential Galois theory 80
4.1 Basic notation 81
4.2 Galois theory 84
4.3 Purely inseparable extensions 86
4.4 Finite separable PV-extensions 91
4.5 Finite PV-extensions 92
4.6 Examples 94

5 Realization of Torsion group schemes 97
5.1 Basic notation 99
5.1.1 Picard-Vessiot theory 102
5.2 Iterative derivations compatible with addition 103
5.3 Torsion schemes as Galois group schemes 105
5.4 Extension of iterative derivations 107
5.5 Example 110

Chapter 1

Introduction

chap:intro

1.1 General overview

sec:general-overview

Differential equations arise in many natural sciences, especially physics. Hence, the desire of solving differential equations has a long history, and many important functions are solutions of differential equations. For example, the Gaussian hypergeometric function with parameters a, b and c

$$ {}_2F_1(a,b;c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n $$

is a solution of the second order linear differential equation

$$ z(1-z)\frac{d^2y}{dz^2} + \big(c - (a+b+1)z\big)\frac{dy}{dz} - aby = 0. $$

Here $(a)_n$ etc. denotes the Pochhammer symbol $(a)_n = \prod_{i=0}^{n-1}(a+i)$ for $n \geq 0$.

Apart from explicit descriptions (e.g. in terms of power series), one was also interested in the "nature" of the solutions: Can they be expressed in terms of known functions, like exponentials of rational functions? Are these solutions – or some of them – also solutions of algebraic equations over the field of rational functions?

Differential Galois theory gives answers to these kind of questions, like classical Galois theory does for solutions of algebraic equations. In this thesis, we focus on the case of linear (ordinary as well as partial) differential equations, and more general on linear equations involving other operators like automorphism, endomorphisms or iterative derivations.

For linear differential equations, there are two main approaches to obtain a Galois group. One approach is via minimal extension fields as in the classical Galois theory of algebraic equations, where the Galois group is defined to be the group of differential automorphisms of the field extension, i.e. of those automorphisms which commute with the derivation. This approach is known under the name Picard-Vessiot theory, and is generalized to various other settings which we will describe later on. Another approach is via a Tannakian formalism. Here one considers the "Tannakian category generated by a differential equation" and the Galois group is defined to be the linear algebraic group of automorphisms of the corresponding fibre functor. In [Del90, Sect. 9], Deligne relates these two approaches, and shows that the Galois group of the field extension is just the set of rational points of the Tannakian Galois group. However, the knowledge about this relation seems to be older as Katz already refers to it in [Kat87].

Actually, for differential equations over $\mathbb{C}(x)$ (or a finite extension thereof), there is a third group of interest, the *monodromy group*. This one is obtained via a more analytically geometric context. A linear differential equation $L = 0$ over $\mathbb{C}(x)$ can be considered as a vector bundle over $X = \mathbb{P}^1(\mathbb{C}) \setminus S$ with fixed local

bases together with a connection ∇. Here, S is a finite set of points containing infinity and the points where the coefficients of the differential equation has poles, as well as the zeros of the highest coefficient of the differential equation. By the choice of the exceptional set S, for every point $p \in X$, the differential equation $L = 0$ has a full set of solutions in the ring of holomorphic functions around p, i.e. the set of solutions forms a $\mathbb{C}$-vector space V_p of dimension equal to the order of L. More precisely, the V_p's form a local system on X. General theory of local systems (or just analytic continuation) shows that every path $u : [0, 1] \to X$ from some point $p = u(0)$ to $q = u(1)$ induces an isomorphism $\alpha_u : V_p \to V_q$ which only depends on the homotopy class of the path u. In particular, after fixing a point $p \in X$, one obtains a representation of the fundamental group of X,

$$\pi_1(X, p) \to \mathrm{GL}(V_p), [u] \mapsto \alpha_u,$$

the *monodromy representation*. The *monodromy group* of L is just the image of that representation. Katz showed in [Kat82, Prop. 5.2] that the monodromy group always is a subgroup of the Tannakian Galois group named above. Furthermore in the case that L only has "regular singularities", he even showed that the Tannakian Galois group is the Zariski closure of the monodromy group.

Apart from the question of determining the Galois group of a given linear differential equation, one is also interested in the so-called *inverse problem*: Which linear algebraic groups do occur as Galois groups of linear differential equations? Of course, the answer to this question depends on the base differential field. Over the base $\mathbb{C}(x)$ with the derivation $\frac{\partial}{\partial x}$, this problem has been solved by Tretkoff and Tretkoff [TT79] in the affirmative, i.e. that any linear algebraic group over $\mathbb{C}$ occurs as the differential Galois group of some linear differential equation over the field $\mathbb{C}(x)$. This result has been generalized to the rational function field $C(x)$ for an arbitrary algebraically closed field C by Hartmann in her PhD thesis (see [Har05]), after previous partial results by Singer [Sin93] and Mitchi and Singer [MS96], [MS02]. The monodromy group plays an important role in these results, as it gives a lower bound to the Galois group. We will return to this question in Section 1.8.1, where we consider the inverse problem also for some of the more general settings described in the following.

In the 1960's, differential Galois theory has been generalized to fields of characteristic zero with several operators consisting of derivations and automorphisms (cf. [ByB62]), including a generalization of Picard-Vessiot theory to linear difference equations (see also [Fra63] and [Inf81]). The Picard-Vessiot theory of linear difference equations, i.e. of those equations involving automorphisms, has been generalized to arbitrary characteristic without significant changes (cf. [vdPS97]), but in the differential case characteristic zero remained crucial. A differential theory in positive characteristic was first initiated by Okugawa ([Oku63] and [Oku87]) and later treated systematically by Matzat and van der Put [MvdP03].

The main idea was to replace derivations by iterative derivations (also called iterative Hasse-Schmidt derivations). However, they obtained only a Galois correspondence detecting the intermediate fields over which the Picard-Vessiot field is separable. Actually, Kreimer (see [Kre65a] and [Kre65b]) has also set up a Picard-Vessiot theory for equations with respect to a quite general kind of operators including the iterative differential case with the same restrictions on the Galois correspondence.

Takeuchi [Tak89] gave an approach to Picard-Vessiot theory from a Hopf algebraic point of view which applies to the differential and iterative differential case (even to linear equations of higher derivations) which was later generalized by Amano and Masuoka [AM05] to contain also linear difference equations for automorphisms.

On the other hand, Katz put the Picard-Vessiot theory for linear differential equations into a more geometrical setting of modules with integrable connection (see e.g. [Kat82]). This was later generalized by André [And01] to a theory containing also difference equations where the occurring endomorphisms do not have to be automorphisms. These approaches, however, were restricted to characteristic zero due to the derivations involved, and only adapted to positive characteristic in my PhD thesis [Rös07] using so called higher connections.

One major part of this thesis (see Chapter 2) is the presentation of a categorical approach which unifies the general properties and objects of all these Picard-Vessiot theories. This categorical framework also leads to deeper insight into the structure of all these Picard-Vessiot theories, and establishes a basis for possible further generalizations.
This part also provides a correspondence between isomorphism classes of fibre functors on the full rigid abelian $\otimes$-subcategory generated by one object M and isomorphism classes of Picard-Vessiot rings R for this object M, as well as a canonical isomorphism between the corresponding Tannakian Galois group and the Galois group of the Picard-Vessiot extension. This is the analogue of the correspondence in the differential setting given by Deligne in [Del90] which we mentioned above. This isomorphism has been already given in other settings, too.

Another part of this thesis is a presentation of my developments in the Picard-Vessiot theory in positive characteristic using iterative higher derivations. First at all, the generalization of the iterative differential theory of Matzat and van der Put to obtain a Galois correspondence which includes all intermediate iterative differential fields – even the ones over which the Picard-Vessiot field is inseparable. This generalization works also over constants which are not algebraically closed. Next, the setup of a Picard-Vessiot theory for iterative differential equations over differentially simple rings (instead of over fields). Finally, I discuss the finite inverse problem, i.e. the question which finite group schemes occur as iterative differential Galois groups over a given iterative differential field, and I explicitly

realize torsion group schemes of abelian varieties as iterative differential Galois groups.

The organization of the thesis is not chronological, as the categorical approach was only established, after I generalized the iterative differential Picard-Vessiot theory to work over differentially simple rings. And the investigation of the infinitesimal and the finite inverse problem was even before that.

Actually, the whole story started right after my PhD, when I generalized the iterative differential theory of Matzat and van der Put to obtain a Galois correspondence which includes all intermediate iterative differential fields. This is published in the second part of [Mau10a] (even with a more general kind of operators), and will be recalled here in Section 1.4. The key point is to replace the Galois group by a group scheme whose points over the constants is the original Galois group. One also gets a close relation to the Hopf algebraic approach of Takeuchi.

1.2 Picard-Vessiot theory for linear differential equations

sec:partial-galois

Picard-Vessiot theory was initiated as a Galois theory for linear differential equations over a function field over the complex numbers at the end of the 19th century by Picard [Pic91] and Vessiot [Ves92]. The aim was to describe solutions of linear differential equations by successively taking integrals of known functions (i.e. solutions of $y' = f$) or exponentials of integrals of known functions (i.e. non-zero solutions of $y' = fy$).

This is in analogy to finite Galois theory where one was interested in when polynomial equations are *solvable*, i.e. its zeros are expressible by means of square roots, cubic roots etc.. In finite Galois theory, this turned out to be the case, exactly when the Galois group of the polynomial has a normal series with abelian factors. This property of a group was then named *solvable*.

In Picard-Vessiot theory the Galois groups are linear algebraic groups over the field of constants. Similar to the finite case, a linear differential equation is solvable as described above if and only if the Galois group is a connected solvable algebraic group. As the notation is sometimes not clear and not consistent in the work of Picard and Vessiot, this theorem is attributed to Kolchin who gave a profound setting to the whole theory[Kol48].

The setup used was the following: Let F be a field of characteristic zero with a derivation $\partial : F \to F$, and suppose that its field of constants

$$C := F^{\partial} := \{a \in F \mid \partial(a) = 0\}$$

is algebraically closed. Furthermore, let $L(y) = \partial^n y + a_{n-1}\partial^{n-1}y + \cdots + a_1\partial y + a_0 y$ be a differential polynomial in the indeterminate y with coefficients in F.

Definition 1.2.1. A **Picard-Vessiot extension** E of F for $L(y) = 0$ is a differential field extension with the same field of constants which is generated as a differential field by n solutions of $L(y) = 0$ which are linearly independent over F (or equivalently, linearly independent over C).

One can show that such a Picard-Vessiot extension always exists. If for example $F = \mathbb{C}(x)$ is the field of rational functions on the projective line over $\mathbb{C}$ and the equation $L(y) = 0$ is regular at $r \in \mathbb{C}$, then there is a Picard-Vessiot extension E inside the field of meromorphic functions around r.

Definition 1.2.2. The **Galois group** $\mathrm{Gal}(E/F)$ of a Picard-Vessiot extension E/F is defined to be the group of differential automorphisms of E/F, i.e.

$$\mathrm{Gal}(E/F) := \mathrm{Aut}^{\partial}(E/F) = \{\varphi \in \mathrm{Aut}(E/F) \mid \varphi \circ \partial = \partial \circ \varphi\}$$

is the group of those field automorphisms $\varphi : E \to E$ which fix F pointwise and which commute with the derivation ∂.

It turns out that this group has the structure of (the C-points of) a linear algebraic group over C, and one obtains the following Galois correspondence.

Theorem 1.2.3 (Galois correspondence)**.** *For a Picard-Vessiot extension E/F with Galois group $\mathrm{Gal}(E/F)$ one has a Galois correspondence (i.e. inclusion reversing bijection) between the intermediate differential fields K, $F \leq K \leq E$, and the Zariski closed subgroups H of $\mathrm{Gal}(E/F)$ given by*

$$K \mapsto \mathrm{Gal}(E/K) = \{\varphi \in \mathrm{Gal}(E/F) \mid \forall x \in K : \varphi(x) = x\},$$

and

$$H \mapsto E^H := \{x \in E \mid \forall \varphi \in H : \varphi(x) = x\},$$

respectively.

The structure as a group of matrices becomes more apparent when one considers the matrix differential equation

$$\partial\Big(\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}\Big) = A \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

instead of the differential polynomial L, where

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & \cdots & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_{n\times n}(F)$$

is the companion matrix of L. Solutions η of L correspond to solution vectors ${}^t(\eta, \partial(\eta), \ldots, \partial^{n-1}(\eta))$ [1], and a full system of solutions $\eta_1, \ldots, \eta_n$ corresponds to an invertible matrix

$$Y := \begin{pmatrix} \eta_1 & \ldots & \eta_n \\ \partial(\eta_1) & \ldots & \partial(\eta_n) \\ \vdots & & \vdots \\ \partial^{n-1}(\eta_1) & \ldots & \partial^{n-1}(\eta_n) \end{pmatrix} \in \mathrm{GL}_n(E),$$

a so called *fundamental solution matrix* of the matrix differential equation.

As a Picard-Vessiot extension E is differentially generated over F by $\eta_1, \ldots, \eta_n$, it is a field extension of F generated by the entries of Y. Using this description, the Galois group of E/F is described more easily. Namely, every differential automorphism $\gamma \in \mathrm{Gal}(E/F)$ is determined by the image $\gamma(Y)$ (γ applied entry-wise), hence by the matrix $D_\gamma := Y^{-1}\gamma(Y)$. A priori this matrix has entries in E, however using compatibility with the derivation on E, it is not hard to show that $D_\gamma \in \mathrm{GL}_n(E^\partial) = \mathrm{GL}_n(C)$.

Therefore, one obtains a faithful representation

$$\mathrm{Gal}(E/F) \to \mathrm{GL}_n(C), \gamma \mapsto D_\gamma = Y^{-1}\gamma(Y).$$

Indeed, Kolchin proved that the image of this representation is a Zariski-closed subset of $\mathrm{GL}_n(C)$, and hence $\mathrm{Gal}(E/F)$ has the structure of a linear algebraic group over the algebraically closed field C.

ex:sin-cos-over-cc

Example 1.2.4. *As an example, we consider the differential polynomial $L(y) = \partial^2 y + y$ over the differential field $(F, \partial) = (\mathbb{C}(x), \frac{\partial}{\partial x})$. From basic analysis we know that the analytic functions $\eta_1 = e^{ix}$ and $\eta_2 = e^{-ix}$ are two $\mathbb{C}$-linearly independent solutions of the equation $L(y) = 0$. Hence, the field $E = \mathbb{C}(x)(e^{ix}, e^{-ix}) = \mathbb{C}(x)(e^{ix})$ is a Picard-Vessiot extension of F for L.*

The companion matrix of L is

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and the matrix differential equation is

$$\partial \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

with

$$Y = \begin{pmatrix} \eta_1 & \eta_2 \\ \partial(\eta_1) & \partial(\eta_2) \end{pmatrix} = \begin{pmatrix} e^{ix} & e^{-ix} \\ ie^{ix} & -ie^{-ix} \end{pmatrix}$$

[1] Throughout this thesis, ${}^t(\cdot)$ denotes the transpose of a matrix, i.e. here it is just the column vector with the given entries.

being a fundamental solution matrix. Therefore, we obtain a faithful representation

$$\mathrm{Gal}(E/F) \to \mathrm{GL}_2(\mathbb{C}), \gamma \mapsto D_\gamma = Y^{-1}\gamma(Y).$$

Since γ is supposed to be a field automorphism, the image are exactly those matrices D_γ such that the entries of Y and those of $\gamma(Y) = YD_\gamma$ fulfill the same algebraic relations over F. It is then easy to deduce from the relations $\partial(\eta_1) = i\eta_1$, $\partial(\eta_2) = -i\eta_2$ and $\eta_1\eta_2 = 1$ that the D_γ in the image are of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ for $a \in \mathbb{C}^\times$. As e^{ix} is transcendental over F, there are no further restrictions on a, hence

$$\mathrm{Gal}(E/F) \xrightarrow{\cong} \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) \mid a \in \mathbb{C}^\times \right\} \cong \mathbb{G}_m(\mathbb{C}).$$

We also see in this example that the representation depends on the fundamental solution matrix, but only up to conjugation: Any other fundamental solution matrix Z is of the form $Z = YD$ for some $D \in \mathrm{GL}_2(\mathbb{C})$, e.g.

$$Z = Y \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix} = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix},$$

and the corresponding representation is

$$\mathrm{Gal}(E/F) \to \mathrm{GL}_2(\mathbb{C}), \gamma \mapsto Z^{-1}\gamma(Z) = D^{-1}(Y^{-1}\gamma(Y))D,$$

with image

$$\begin{aligned} & \left\{ \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix}^{-1} \cdot \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix} \,\middle|\, a \in \mathbb{C} \right\} \\ = & \left\{ \begin{pmatrix} \frac{a+a^{-1}}{2} & \frac{a-a^{-1}}{2i} \\ -\frac{a-a^{-1}}{2i} & \frac{a+a^{-1}}{2} \end{pmatrix} \,\middle|\, a \in \mathbb{C}^\times \right\} = \left\{ \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \,\middle|\, c, s \in \mathbb{C}, c^2 + s^2 = 1 \right\} \cong \mathrm{SO}_2(\mathbb{C}). \end{aligned}$$

For theoretical purposes coordinate-free descriptions of the linear differential equations are more convenient:

Definition 1.2.5. A **differential module** over F is a finite dimensional F-vector space M together with a derivation $\partial_M : M \to M$, i.e. an additive map ∂_M satisfying the "Leibniz rule"

$$\partial_M(fm) = \partial(f)m + f\partial_M(m)$$

for all $f \in F$, $m \in M$.

To a matrix differential equation $\partial(\mathbf{y}) = A\mathbf{y}$ with $A \in \mathrm{Mat}_{n\times n}(F)$, one associates a differential module (M, ∂_M) with $\dim_F(M) = n$ and a basis $(b_1, \ldots, b_n)$ of M such that

$$\partial_M(b_j) = -\sum_{i=1}^{n} A_{ij} b_i \quad \text{for all } j = 1, \ldots, n.$$

Then a vector $\mathbf{y} = {}^t(y_1, \ldots, y_n)$ is a solution of the matrix differential equation if and only if $\sum_{j=1}^n y_j b_j$ is a constant vector, i.e. satisfies $\partial_M(\sum_{j=1}^n y_j b_j) = 0$. Hence, the search for a differential extension E of F containing n independent solutions is equivalent to the search for a differential extension E such that the differential module $E \otimes_F M$ over E has a basis of constant vectors.

Differential modules can also be considered as modules over the non-commutative ring $F[\delta]$ of differential operators which are finite-dimensional as F-vector space. Here, $F[\delta]$ equals $\oplus_{n=0}^{\infty} F\delta^n$ as an F-vector space, for some formal elements δ^n with multiplication determined by

$$\delta^k \cdot \delta^l = \delta^{k+l} \quad \text{and} \quad \delta \cdot f = \partial(f) + f \cdot \delta.$$

The multiplication rule in $F[\delta]$ is equivalent to saying that for a $F[\delta]$-module M the map $\partial_M : M \to M, m \mapsto \delta \cdot m$ is a derivation on M as given above. The interpretation as $F[\delta]$-modules also explains the definition of derivations on tensor products $M \otimes_F N$ given by

$$\partial_{M\otimes N}(m \otimes n) = \partial_M(m) \otimes n + m \otimes \partial_N(n) \quad \text{for all } m \in M, n \in N$$

for differential modules (M, ∂_M) and (N, ∂_N). However, we will mostly deal with the notation of a differential module as a pair (M, ∂_M).

In Picard-Vessiot theory, a main role is played by the *Picard-Vessiot ring*. Given a differential module (M, ∂_M), an associated differential equation $\partial(\mathbf{y}) = A\mathbf{y}$ with respect to a basis, and a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$ in a Picard-Vessiot field E, the Picard-Vessiot ring R is the subring of E which is generated as an F-algebra by the entries of Y and its inverse. The importance of the Picard-Vessiot ring R is given by the fact that $\mathrm{Gal}(E/F)$ acts algebraically on R, and even more, that the spectrum $\mathrm{Spec}(R)$ is a torsor of $\mathrm{Gal}(E/F)$ over F. Moreover, the Galois correspondence is more or less a consequence of this torsor property, as by geometric invariant theory, the subfield $E^{\mathcal{H}}$ corresponding to a closed subgroup $\mathcal{H} \leq \mathrm{Gal}(E/F)$ is nothing else than the field of rational functions on the scheme $\mathrm{Spec}(R)/\mathcal{H}$.

One can even define the Picard-Vessiot ring R at first hand:

Definition 1.2.6. A **Picard-Vessiot ring** for a differential module M is a ∂-simple ∂-ring extension R of F with the same constants and which is minimal with the property that $R \otimes_F M$ has a basis of constant elements. Here, ∂-simple means that R has no nontrivial ideals stable under the derivation.

Then for such a Picard-Vessiot ring R, the field of fractions E of R is a Picard-Vessiot field for M, and $\mathrm{Aut}^{\partial}(R/F) = \mathrm{Aut}^{\partial}(E/F)$.

In the categorical setting in Chapter 2, the Picard-Vessiot ring is the main object, since there is no "Picard-Vessiot field".

Apart from the Galois group of the Picard-Vessiot extension, there is also another group attached to a differential module, the so called *Tannakian Galois group*. This group is obtained as follows. The category of differential modules Diff_F over a given differential field F is an abelian category. It is even a symmetric tensor category with tensor product as described above, and moreover, all objects are rigid, i.e. have a dual object. Namely, the dual object of a differential module (M, ∂_M) is just the dual vector space $M^\vee = \mathrm{Hom}_F(M, F)$ with derivation given by

$$\partial_{M^\vee}(f)(m) = \partial_F\big(f(m)\big) - f\big(\partial_M(m)\big)$$

for all $m \in M$, $f \in M^\vee$. Given a fixed differential module M, the full subcategory of Diff_F whose objects are all subobject of direct sums of objects of the form $M^{\otimes n} \otimes (M^\vee)^{\otimes k}$ with $n, k \in \mathbb{N}$, is called the tensor subcategory generated by M, and will be denoted by $\langle\langle M \rangle\rangle$. Assuming that one has a fibre functor $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_C$ to the category vect_C of (finite dimensional) vector spaces over $C = F^\partial$, i.e. a faithful exact additive tensor functor, the category $\langle\langle M \rangle\rangle$ is a neutral Tannakian category. The Tannakian Galois group is then the linear algebraic group of natural automorphisms of this fibre functor ω, and it has a canonical embedding as an algebraic subgroup of $\mathrm{End}(\omega(M)) \cong \mathrm{GL}_n(C)$ where $n = \dim_F(M)$.

Since, the field C is algebraically closed, a fibre functor ω exists, and all fibre functors are isomorphic. All this is explained quite well in [Del90]. Deligne also explains that there is a bijection between isomorphism classes of Picard-Vessiot rings/extensions and isomorphism classes of fibre functors (even if C is not algebraically closed). Furthermore, the Galois groups $\mathrm{Gal}(E/F)$ and $\mathrm{Aut}^\otimes(\omega)$ of a PV-extension E and its corresponding fibre functor are isomorphic.

We will see in Chapter 2 that all these statements are even true in the categorical setting. Hence, they hold in all the settings described in the following paragraphs.

1.3 Partial differential equations

sec:partial-differential

The Picard-Vessiot theory for ordinary differential equations has been generalized to partial differential equations by Kolchin [Kol52]. Here, the base field F is equipped with several commuting derivations $\partial_1, \ldots, \partial_m$ and the modules are finite dimensional F-vector spaces with commuting action of all the derivations. The main parts of the theory stayed the same (see [vdPS03], and for a more detailed description also [Hei07]). Indeed in his setup, Kolchin reduced a lot of proofs to the ordinary differential case.

1.4 Picard-Vessiot theory for iterative differential equations

sec:id-galois

Differential Galois theory does not work well in positive characteristic. This is mainly caused by the fact that in positive characteristic p, every p-th power of an element in a ring is differentially constant, and in particular, every field extension contains new constants.

To overcome this problem, derivations are replaced by so called iterative derivations (cf. [MvdP03]). These are a collection $\theta = \left(\theta^{(n)}\right)_{n\in\mathbb{N}}$ of additive maps satisfying $\theta^{(0)} = \mathrm{id}$, $\theta^{(n)}(ab) = \sum_{i+j=n} \theta^{(i)}(a)\theta^{(j)}(b)$ as well as $\theta^{(n+m)} = \binom{n+m}{n}\theta^{(n)} \circ \theta^{(m)}$ for all $n, m \in \mathbb{N}$. This means, $\partial := \theta^{(1)}$ is a derivation and $\theta^{(n)}$ resembles $\frac{1}{n!}\partial^n$ – the n-th iterate of ∂ devided by n-factorial. Indeed, in characteristic zero, the iterative derivations are determined by the derivation $\partial = \theta^{(1)}$ via $\theta^{(n)} = \frac{1}{n!}\partial^n$. In particular, the differential setting in characteristic zero is a special case of the iterative differential setting.

The constants of an iterative differential field (F, θ) are given by

$$F^\theta := \{x \in F \mid \theta^{(n)}(x) = 0 \,\forall n \geq 1\}.$$

Example 1.4.1. *The standard example is the iterative derivation θ on the rational function field $C(x)$ given by*

$$\theta^{(k)}(x^n) = \binom{n}{k} x^{n-k}$$

and C-linear extension. In characteristic zero, this is exactly the iterative derivation determined by $\theta^{(1)} = \frac{\partial}{\partial x}$. In this case, the constants are just the field C, as one is used from the differential field in characteristic zero.

The basic objects replacing differential modules are iterative differential modules (M, θ_M), i.e. F-vector spaces M with a family $\theta_M = \left(\theta_M^{(n)}\right)_{n\in\mathbb{N}}$ of additive maps $\theta_M^{(n)} : M \to M$ satisfying $\theta_M^{(0)} = \mathrm{id}_M$, $\theta_M^{(n)}(fm) = \sum_{i+j=n} \theta^{(i)}(f)\theta^{(j)}(m)$ for all $f \in F, m \in M$ as well as $\theta^{(n+k)} = \binom{n+k}{n}\theta^{(n)} \circ \theta^{(k)}$ for all $n, k \in \mathbb{N}$.

As in the differential setting, one is interested in minimal iterative differential extensions E of F (with same constants) such that $\dim_{F^\theta}\left((E \otimes_F M)^\theta\right) = \dim_F(M)$. Assuming that $C = F^\theta$ is algebraically closed, a minim

Picard-Vessiot rings and Picard-Vessiot fields for iterative differential modules exist and are unique up to iterative differential isomorphisms.

Matzat and van der Put also defined the Galois group of such a Picard-Vessiot extension E/F as the group of iterative differential automorphisms $\mathrm{Aut}^\theta(E/F)$, and obtained a Galois correspondence. However, as I pointed out in [Mau10a],

and what was independently observed by Amano in [Ama06], this Galois correspondence only takes into account intermediate iterative differential fields over which E is separable.

In the second part of [Mau10a], I was able to remove this defect by considering the Galois group of the extension as an affine group scheme instead of a group, which allowed to take into account nonreduced subgroup schemes on the group side and intermediate extensions L over which the Picard-Vessiot field is inseparable (see also Chapter 4). More explicitly, for a Picard-Vessiot extension E/F with Picard-Vessiot ring R, I defined the Galois group as the group functor

$$\underline{\mathrm{Gal}}(E/F) := \underline{\mathrm{Gal}}(R/F) : \mathsf{Alg}_C \to \mathsf{Groups}, D \mapsto \mathrm{Aut}^\theta(R \otimes_C D/F \otimes_C D)$$

where the C-algebra D is equipped with the trivial iterative derivation, i.e. $R \otimes_C D$ is an extension by constants. This group functor turns out to be representable by $(R \otimes_F R)^\theta$, and hence is an affine group scheme of finite type over $C = F^\theta$.

In general, an iterative differential automorphism of $R \otimes_C D$ does not extend to an automorphism of $E \otimes_C D$, but it extends to the total ring of fractions $\mathrm{Quot}(R \otimes_C D)$, i.e. the localization by all nonzero divisors, a ring which contains E. In particular, for any $g \in \underline{\mathrm{Gal}}(R/F)(D) = \mathrm{Aut}^\theta(R \otimes_C D/F \otimes_C D)$ and $e \in E$, an element $g(e) \in \mathrm{Quot}(R \otimes_C D)$ is well-defined. Therefore, one can define the invariants $E^{\mathcal{H}}$ of E under an algebraic subgroup schemes $\mathcal{H}$ of $\mathcal{G} = \underline{\mathrm{Gal}}(R/F)$ by

$$E^{\mathcal{H}} := \{e \in E \mid \forall D \in \mathsf{Alg}_C, h \in \mathcal{H}(D) : h(e) = e\}.$$

With these definitions, one obtains the desired Galois correspondence with all intermediate iterative differential fields on one hand, and all closed subgroup schemes of $\underline{\mathrm{Gal}}(E/F)$ on the other hand.

If one considers iterative differential fields whose field of constants is not algebraically closed, these definitions still work, and hence [Mau10b] is already written without the assumptions on the constants.

Like the generalization of differential Galois theory to partial differential equations, the iterative differential setting has been generalized to the case of several commuting iterative derivations (called multi-variate iterative derivations) by F. Heiderich in his Master thesis [Hei07]. Apart from some technicalities, it turned out that the theory works very like the case of one iterative derivation. The multivariate setup is recalled in Chapter 4.

1.5 Picard-Vessiot theory for difference equations

sec:sigma-galois

In the Picard-Vessiot theory for difference equations (cf. [vdPS97]), derivations are replaced by automorphisms, and constants are replaced by invariants. One

starts with some field F together with an automorphism $\sigma : F \to F$ and its field of invariant elements $C := F^\sigma := \{x \in F \mid \sigma(x) = x\}$ which is supposed to be algebraically closed. The most prominent examples are the field $\mathbb{C}(z)$ with the shift operator $\sigma(z) = z + 1$ or with the q-difference operator $\sigma(z) = qz$ for some $q \in \mathbb{C}$ which is not a root of unity. In both cases the field of invariants is $\mathbb{C}$.

The basic objects are difference modules (M, σ_M), i.e. F-vector spaces M together with a σ-linear automorphism $\sigma_M : M \to M$. Again, the set of invariants $M^\sigma := \{m \in M \mid \sigma_M(m) = m\}$ is a C-vector space of dimension at most $\dim_F(M)$, and one is interested in a difference extension of F over which the corresponding dimensions are the same. In this setting another aspect appears, since in some situations every solution ring has zerodivisors. Hence, there does not exist a Picard-Vessiot **field** in general. Nevertheless, if C is algebraically closed (as we assume at the moment), there always exists a Picard-Vessiot ring R over F, i.e. a σ-simple σ-ring extension R of F minimal with the property that $R \otimes_F M$ has a basis of invariant elements, and instead of the Picard-Vessiot field one considers $E = \mathrm{Quot}(R)$, the total ring of fractions of R. With these definitions, assuming that F is of characteristic zero, one again obtains a Galois group $\mathrm{Aut}^\sigma(R/F)$ which is the group of C-rational points of a linear algebraic group, as well as a Galois correspondence between closed subgroups of $\mathrm{Aut}^\sigma(R/F)$ and total difference subrings of E containing F.

Example 1.5.1. *The most basic and most prominent example is the one-dimensional difference module $M = \mathbb{C}(z) \cdot b$ over the difference field $F = \mathbb{C}(z)$ with the shift operator $\sigma(z) = z + 1$, where $\sigma_M(b) = \frac{1}{z}b$. Then for a difference ring extensions R of F,*

$$\begin{aligned}(R \otimes_F M)^\sigma &= \{f \cdot b \in R \otimes_F M \mid \sigma_M(fb) = fb\} \\ &= \{f \cdot b \in R \otimes_F M \mid f \in R, \sigma(f) = zf\}.\end{aligned}$$

Since the Gamma function Γ satisfies the functional equation $\Gamma(z + 1) = z\Gamma(z)$, it is a solution to the difference equation $f(z + 1) = \sigma(f)(z) = z \cdot f(z)$. Hence, $R = F[\Gamma, 1/\Gamma]$ is a Picard-Vessiot ring for this difference module inside the ring of meromorphic functions.

The Galois group $\mathrm{Aut}^\sigma(R/F)$ is a priori a Zariski closed subgroup of $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$, and the fact that Γ is transcendental is reflected in the property that $\mathrm{Aut}^\sigma(R/F)$ is not finite, i.e. $\mathrm{Aut}^\sigma(R/F) = \mathbb{C}^\times$.

In positive characteristic, problems with these definitions occur due to inseparability. These can be solved by defining the Galois group as a group scheme quite analogous to the one described in Section 1.4 (cf. [Wib10]). The thesis [Wib10] of Wibmer even considers Galois extensions which are more general than the Picard-Vessiot extensions. But, also for the difference Picard-Vessiot theory, his thesis provides a slight generalization by relaxing several of the assumptions (see

also [OW15, Sect. 2.2]). First at all, he allows the operator σ to be an endomorphism instead of an automorphism. Hence, also the semi-linear operator σ_M on a module M can not be bijective, and the assumption is that the image $\sigma_M(M)$ generates M (which also implies that σ_M is injective). Secondly, he gives credit to the problem that there might be no Picard-Vessiot field. He introduces so-called σ-pseudo fields which are finite products of fields that are still σ-simple. As already observed in [vdPS97], for every difference module M there is always a Picard-Vessiot σ-pseudo field. Wibmer, however, also used a σ-pseudo field as the base difference ring. Such pseudo-fields are also used in [AM05] for a more general kind of operators (cf. Sect. 1.7.4). Both generalizations make some proofs a bit more complicated, but otherwise turned out to work smoothly.

The third generalization – which is a bigger issue – will be explained in more details in the next section, namely that he dropped the assumption that the field of constants is algebraically closed.

1.6 Non-algebraically closed constants

sec:non-algebr-closed

In the last decade, one has relaxed the conditions on the field of constants/invariants being algebraically closed. However, if the field of constants/invariants C is not algebraically closed (cf. [Dyc08], [Mau10a], and [Wib10]), some things become more involved. We explain these issues in the differential case, but they are present also in the difference case, and the iterative differential case.

In Section 1.2 above, we defined a Picard-Vessiot ring for a differential equation $\partial(\boldsymbol{y}) = A \cdot \boldsymbol{y}$ over F to be a ∂-simple ∂-ring R without new constants such that R contains a fundamental solution matrix Y, and such that R is minimal with these properties. If the constants F^∂ are algebraically closed, the condition"without new constants" is a consequence of the other conditions. Hence, one can construct a Picard-Vessiot ring by first defining a derivation on the localized polynomial ring $U = F[X_{ij}, \det(X)^{-1} \mid i, j = 1, \dots n]$ via $\partial(X) = A \cdot X$, and secondly, taking $R = U/I$ for a maximal ∂-ideal I of U. If F^∂ is not algebraically closed, this construction still provides a minimal ∂-simple ∂-ring R containing a fundamental solution matrix Y, but the constants of R might be a finite extension of F^∂ (see also Prop. 2.4.11 in the categorical setting).

This is the reason that in general, Picard-Vessiot extensions might not exist. Furthermore, there also might be several non-isomorphic Picard-Vessiot extensions for the same equation. These Picard-Vessiot extensions, however, become isomorphic after a finite extension of constants.

ex:sin-cos-over-rr

Example 1.6.1. *We start with an example having two non-isomorphic Picard-Vessiot fields which is due to Dyckerhoff [Dyc08].*

Namely, we are considering the matrix differential equation

$$\partial \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

as in Example 1.2.4, but this time over the differential field $(F, \partial) = (\mathbb{R}(x), \frac{\partial}{\partial x})$. *Although, the matrix*

$$Y = \begin{pmatrix} e^{ix} & e^{-ix} \\ ie^{ix} & -ie^{-ix} \end{pmatrix}$$

provides a fundamental system of solutions, the extension of differential fields $F(e^{ix}, e^{-ix}, ie^{ix}, -ie^{-ix})/F$ *would not be a Picard-Vessiot extension, since the larger field contains new constants, e.g. the imaginary unit* $i = \frac{ie^{ix}}{e^{ix}}$.

However, the matrix

$$Z_1 = Y \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix} = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix},$$

also satisfies $\partial(Z_1) = A \cdot Z_1$ *and a Picard-Vessiot extension for this differential equation is given by* $E_1 = F(\cos(x), \sin(x))$ *with equation* $\cos(x)^2 + \sin(x)^2 = 1$.

Now consider the matrix

$$Z_2 := iZ_1 = \begin{pmatrix} i\cos(x) & i\sin(x) \\ -i\sin(x) & i\cos(x) \end{pmatrix}.$$

This is also a fundamental solution matrix for the given differential equation, and hence the field extension $E_2 = F(i\cos(x), i\sin(x))$ *with equation* $(i\cos(x))^2 + (i\sin(x))^2 = -1$ *is also a Picard-Vessiot field.*

But, the fields E_1 *and* E_2 *are not isomorphic!*
This is seen most easily from the fact, that E_1 *can be ordered (by letting* $\cos(x)$ *and* $\sin(x)$ *be positive), but* E_2 *can't be ordered, since the sum of squares* $(i\cos(x))^2 + (i\sin(x))^2 + 1^2$ *equals zero.*

Example 1.6.2. *An example where no Picard-Vessiot ring/field exists is given by Seidenberg in [Sei56] which we modify here a bit, to fit to the previous example.*

Namely, consider the field $F = \mathbb{R}(x)(w, \partial(w))$ *generated over* $\mathbb{R}(x)$ *by a non-constant solution* w *of the differential equation* $4w^2 + \partial(w)^2 = -1$, *and by its derivative* $\partial(w)$. *One should think of* w *being* $\frac{i}{2}\sin(2x)$ *and* $\partial = \partial_x$.
Then as in the previous example, we consider the matrix differential equation

$$\partial \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix},$$

but this time over the field F.
Morally, $w = \frac{i}{2}\sin(2x) = \frac{i}{2} \cdot 2\sin(x)\cos(x) = i\sin(x)\cos(x)$, *and no matter*

whether we choose $\begin{pmatrix} \cos(x) \\ -\sin(x) \end{pmatrix}$ *or* $\begin{pmatrix} i\cos(x) \\ -i\sin(x) \end{pmatrix}$ *as a solution, the other will also be in the field extension. Hence, the field of constants is* $\mathbb{C}$.

Formally, if E *is a differential field extension of* F *containing a non-trivial solution* ${}^t(y_1, y_2)$*, we have*

$$\partial(y_1^2 + y_2^2) = 2y_1\partial(y_1) + 2y_2\partial(y_2) = 2y_1y_2 - 2y_1y_2 = 0.$$

Hence, $y_1^2 + y_2^2 =: c$ *is a constant.*
If $c = 0$*, then we get* $\left(\frac{y_1}{y_2}\right)^2 = -1 \in \mathbb{R}$*. As elements which are algebraic over constants are constants themselves,* $\frac{y_1}{y_2}$ *is a constant and its square is* -1*. Hence,* $E^\partial \supsetneq \mathbb{R}$.
Now, we assume $c \neq 0$*, and first remark that by differentiating the equation* $4w^2 + \partial(w)^2 = -1$*, we obtain*

$$8w\partial(w) + 2\partial(w)\partial^2(w) = 0 \Rightarrow \partial^2(w) = -4w.$$

Consider now the matrix

$$Z := \begin{pmatrix} 2w & -\partial(w) \\ \partial(w) & 2w \end{pmatrix}^{-1} \cdot \begin{pmatrix} y_1 & -y_2 \\ y_2 & y_1 \end{pmatrix}^2 = \begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(E),$$

for $z_1 = -2w(y_1^2 - y_2^2) - 2y_1y_2\partial(w)$ *and* $z_2 = \partial(w)(y_1^2 - y_2^2) - 4wy_1y_2$.
By differentiating z_1 *and* z_2 *and using the equations above, one obtains that both* z_1 *and* z_2 *are constant. Therefore, also* $\det(Z) = z_1^2 + z_2^2$ *is a constant and*

$$\det(Z) = (4w^2 + \partial(w)^2)^{-1} \cdot (y_1^2 + y_2^2)^2 = -c^2.$$

Hence, $z_1^2 + z_2^2 + c^2 = 0$ *which is not possible if* $z_1, z_2 \in \mathbb{R}$.

To overcome the problem of existence and uniqueness, one possibility is to fix a universal differential overfield, or at least one which is large enough like in the abstract setting in Prop. 2.4.14. In applications of differential equations as well as difference equations, such an overfield is often naturally given, e.g. as a field of meromorphic functions.
In the real and the p-adic case, Crespo, Hajto et al. established results on both existence and uniqueness if the constants of the field F are real closed or p-adically closed, resp. by forcing the extension to be real resp. p-adic, too (see [CHS13] and [CHvdP16]).

Another issue to deal with is that the group of differential automorphisms $\mathrm{Aut}^\partial(E/F)$ respectively difference automorphisms $\mathrm{Aut}^\sigma(E/F)$ might be too small. For example, the differential equation $\frac{\partial}{\partial x}(y) = \frac{1}{3x}y$ over the differential field $(\mathbb{R}(x), \frac{\partial}{\partial x})$ has a solution $z = \sqrt[3]{x}$, hence $E = \mathbb{R}(z)$ is a Picard-Vessiot field, but $\mathrm{Aut}^\partial(E/\mathbb{R}(x)) = \{1\}$, since E does not contain the third roots of unity.

One way to overcome this problem is to consider F-embeddings $E \hookrightarrow E \otimes_C \bar{C}$ instead, or equivalently $\mathrm{Aut}^\partial(E \otimes_C \bar{C}/F \otimes_C \bar{C})$. Another way which fits more in the line of the iterative differential setting, is to replace the automorphism group by a representable group functor $\underline{\mathrm{Gal}}(E/F)$, i.e. an affine group scheme whose group of C-rational points is $\mathrm{Aut}^\partial(E/F)$. Namely by

$$\underline{\mathrm{Gal}}(E/F) := \underline{\mathrm{Gal}}(R/F) : \mathsf{Alg}_C \to \mathsf{Groups}, D \mapsto \mathrm{Aut}^\partial(R \otimes_C D/F \otimes_C D).$$

Then as already described in the iterative differential setting, $\mathrm{Spec}(R)$ is a $\underline{\mathrm{Gal}}(E/F)$-torsor over F and one obtains a Galois correspondence between closed subgroups of $\underline{\mathrm{Gal}}(E/F)$ and differential subfields of E containing F, by defining

$$E^{\mathcal{H}} := \{e = \frac{r}{s} \in E \mid \forall D \in \mathsf{Alg}_C, h \in \mathcal{H}(D) : \frac{h(r \otimes 1)}{h(s \otimes 1)} = \frac{r \otimes 1}{s \otimes 1} \in \mathrm{Quot}(R \otimes_C D)\}$$

for algebraic subgroup schemes $\mathcal{H}$ of $\mathcal{G} = \underline{\mathrm{Gal}}(E/F)$ over C.

In this definition, the detour using the automorphisms of $R \otimes_C D$ is necessary, since the automorphisms of $E \otimes_C D$ are too small in general. The automorphisms of $R \otimes_C D$ only extend uniquely to the total ring of fractions $\mathrm{Quot}(R \otimes_C D)$ which is strictly larger than $E \otimes_C D$ if D/C is not algebraic.

Therefore, on one hand, we need the Picard-Vessiot ring R inside a PV-field for defining the Galois group scheme, since the latter does not act algebraically on the PV-field. On the other hand, one does not get a full Galois correspondence on the ring level.
In geometric terms, $\mathrm{Spec}(R)$ is a $\underline{\mathrm{Gal}}(E/F)$-torsor over F. Hence, for a closed subgroup $\mathcal{H} \leq \underline{\mathrm{Gal}}(E/F)$, one obtains the orbit space $\mathrm{Spec}(R)/\mathcal{H}$, and $E^{\mathcal{H}}$ is just the rational function field of that space, and determines $\mathrm{Spec}(R)/\mathcal{H}$ as a quotient of $\mathrm{Spec}(R)$. The invariant ring $R^{\mathcal{H}}$, however, is the ring of global sections of the orbit space $\mathrm{Spec}(R)/\mathcal{H}$. If the latter is not affine, $R^{\mathcal{H}}$ becomes "too small".
On the ring level, at least one has a restricted Galois correspondence between closed normal subgroups of $\underline{\mathrm{Gal}}(E/F)$ and differential subrings of R containing F which are Picard-Vessiot rings for some ∂-module (see Chapter 3).

In the abstract setting of this article, we will stay on the ring level, since the action of the Galois group is naturally algebraic there.

1.7 Further transcendental Galois theories

The three basic settings described above have been generalised in various ways. On one hand, the operators acting have become more general. On the other hand, the base fields have been replaced by more general bases.

1.7.1 Modules with connections

In [Kat90, Ch. 2], N. Katz considers schemes $\mathcal{X}$ of finite type over a field k of characteristic 0, and obtains Picard-Vessiot extensions for finitely generated $\mathcal{O}_{\mathcal{X}}$-modules with integrable connections.

1.7.2 Noncommutative differentials and connections

André in [And01] used so called noncommutative differentials in characteristic 0. The base is a C-algebra A with a "derivation" $d : A \to \Omega^1$ for some fixed A-A-bimodule Ω^1, i.e. the map d is C-linear and fulfills $d(ab) = a \cdot d(b) + d(a) \cdot b$ for all $a, b \in A$. The "differential modules" are left A-modules M together with a "connection" $\nabla : M \to \Omega^1 \otimes_A M$ verifying the rule $\nabla(am) = a \cdot \nabla(m) + d(a) \otimes m$ for all $a \in A$ and $m \in M$. This setup resembles a collection of derivations and endomorphisms in characteristic 0.

Under the hypothesis that A is commutative and that (A, d) is "simple", as well as some additional assumptions, André shows that a Galois theory works similar as described above. He also describes the relation of the differential Galois group of the extension and the Tannakian Galois group associated to such a module. We show a generalisation of this relation in the categorical setting in Chapter 2.

1.7.3 Iterative higher differentials and Iterative higher connection

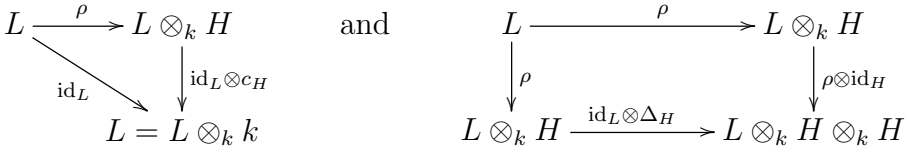
In my PhD thesis [Rös07], I considered regular rings with "(iterative) higher differentials" and modules with "(iterative) higher connections". These higher differentials and iterative higher differentials are analogues in positive characteristic of differentials, similar as higher derivations and iterative higher derivations are analogues in positive characteristic of derivations. I also sketched its generalization to "nice" schemes X. In the second part of [Mau10a], I established the Picard-Vessiot theory over fields with "(iterative) higher differentials" whose constants are a perfect field.

1.7.4 Hopf-algebraic approach

subsec:hopf-algebra

Takeuchi in [Tak89] investigated Picard-Vessiot theory from a purely algebraic point of view. This approach has its origins in a generalisation of classical Galois theory named Hopf-Galois theory (cf. [CS69]): Instead of considering the action of a group on an extension L/K, one considers a co-action of a Hopf-algebra. More precisely, for a commutative base ring k (in our case always a field), one

considers an extension L/K of k-algebras and a co-action of a k-Hopf algebra H on L/K, i.e. a K-linear homomorphism $\rho : L \to L \otimes_k H$ such that the diagrams



commute. Here, $c_h : H \to k$ is the counit of the Hopf algebra and $\Delta_H : H \to H \otimes_k H$ is the comultiplication. The extension L/K is called Hopf-Galois if and only if the ring of coinvariants

$$L^{\mathrm{coH}} := \{l \in L \mid \rho(l) = l \otimes 1\}$$

equals K and the induced homomorphism of L-algebras (with L-action from the left)

$$L \otimes_K L \xrightarrow{\mathrm{id}_L \cdot \rho} L \otimes_k H, l_1 \otimes l_2 \mapsto (l_1 \otimes 1) \cdot \rho(l_2)$$

is an isomorphism.

The classical finite Galois theory for a Galois extension L/K with group G is obtained by taking $k = K$ and H being the K-algebra $K[G]$ of functions $G \to K$ with pointwise multiplication, and comultiplication induced by the multiplication on G. Namely, the condition that the extension L/K is Galois with group G is equivalent to that the homomorphism

$$L \otimes_K L \to L^{|G|}, l_1 \otimes l_2 \mapsto (l_1 \sigma(l_2))_{\sigma \in G}$$

is an isomorphism. But $L^{|G|}$ is naturally isomorphic to $L \otimes_K K[G]$ via

$$(l_\sigma)_{\sigma \in G} \mapsto \sum_{\sigma \in G} l_\sigma \otimes p_\sigma$$

using the standard basis $\{p_\sigma | \sigma \in G\}$ of $K[G]$ where $p_\sigma(\tau) = 1$ for $\tau = \sigma$, and 0 else.

For obtaining a Picard-Vessiot theory from this Hopf algebraic point of view, Takeuchi defines an extension of differential fields L/K to be a Picard-Vessiot extension if they have the same fields of constants k, and if there is a differential subring $R \subseteq L$ such that L is the field of fractions of R and the K-algebra $R \otimes_K R$ is generated by $R \otimes_K K$ and $(R \otimes_K R)^\partial$. He shows that in this case, R/K is a Hopf-Galois extension with k-Hopf algebra $H = (R \otimes_K R)^\partial$. Namely, the two conditions imply that the homomorphism $R \otimes_k H \to R \otimes_K R$ is an isomorphism, and the inverse of this isomorphism is the isomorphism in the definition of a Hopf-Galois extension. In comparison with the differential case over non-algebraically closed constants (Sect. 1.6) or the iterative differential setting

(Sect. 1.4), R is just the Picard-Vessiot ring and H is the Hopf algebra representing the Galois group scheme $\underline{\mathrm{Gal}}(R/K)$. Takeuchi's approach covers the case of constants which are not algebraically closed. He also works in a more general setting, namely with so called *C-ferential fields* which amounts to having a collection of several commuting derivations on L, or several commuting higher derivations in positive characteristic. Here, C stems from the coalgebra of operators acting on L. Since, he didn't suppose the Hopf algebra respectively the extension to be finitely generated, it also covers inductive limits of the usual Picard-Vessiot extensions which would have pro-algebraic groups as Galois groups.

Later Amano and Masuoka in [AM05] have generalised this approach. They extended the kind of operators, and the kind of objects. They replaced the formerly irreducible coalgebra C by a certain Hopf algebra D, and the C-ferential fields by Artinian simple D-module algebras. The first amounts to including also automorphisms as operators, and the second amounts to including not only fields, but also finite products of fields which is necessary in the difference setting (comp. Sect. 1.5).

1.8 The inverse Galois problem

sec:inverse-problem

The inverse Galois problem is about the question which groups respectively group schemes do occur as Galois groups in the various settings. As described above all the Galois groups in the Picard-Vessiot theories are algebraic group schemes over the field of constants/invariants, hence we will only talk about those in the following. Of course the answers to these problems depend on the base differential respectively difference field. The base fields that are of interest are mainly function fields of algebraic varieties ("global fields"), and in particular the rational function field in one variable. Sometimes also "local fields", i.e. Laurent series rings in one or several variables are considered, but mainly to obtain information on the problem in the global case, e.g. do get lower bounds by local-global principles.

1.8.1 In differential Galois theory

subsec:inverse-problem-differential

In differential Galois theory, first results to the inverse Galois problem were established in the "classical case" for the differential field $F = \mathbb{C}(x)$ with $\partial = \frac{d}{dx}$. In this case, Tretkoff and Tretkoff [TT79] solved the question in the affirmative, i.e. they showed that any linear algebraic group over $\mathbb{C}$ occurs as a differential Galois group over $\mathbb{C}(x)$. Their proof uses the analytic theory of monodromy groups mentioned in Section 1.1. Namely, the Riemann-Hilbert correspondence in this case (solved by Plemelj (see[Ple64])) guarantees that for every finitely generated group G, there is a linear differential equation over $\mathbb{C}(x)$ with only

regular singularities such that the monodromy group of this equation equals the given group G. As mentioned earlier, in the case of regular singularities, the monodromy group is Zariski-dense in the differential Galois group. Therefore, the main idea of Tretkoff and Tretkoff was to choose a finitely generated group G which is Zariski-dense in the given linear algebraic group, and consider a linear differential equation corresponding to that group G.

By its analytic nature, this proof was not transferable to rational function fields $F = C(x)$ over other algebraically closed fields of constants C.[2] Singer [Sin93] gave some partial results to the inverse problem using special properties of the groups.

For more general results, other techniques were established, most important an upper bound on the Galois group via its Lie algebra (see [vdPS03, Cor. 4.3]):

Proposition 1.8.1. *Consider a linear differential equation $\partial(\boldsymbol{y}) = A\boldsymbol{y}$ with $A \in \mathrm{Mat}_n(F)$, and let $\mathcal{G} \subseteq \mathrm{GL}_{n,C}$ be a linear algebraic group over C.*
If $A \in \mathrm{Lie}_F(\mathcal{G})$, then the Galois group of the differential equation is (conjugate to) a subgroup of $\mathcal{G}$.

If the cohomological dimension of F is at most one (which is the case for $F = C(x)$), then one also has a partial converse result:

Proposition 1.8.2. *Assume that $\mathrm{cd}(F) \leq 1$, and that $\mathcal{G} \subseteq \mathrm{GL}_{n,C}$ is a connected algebraic group which is the differential Galois group of $\partial(\boldsymbol{y}) = A\boldsymbol{y}$ for some $A \in \mathrm{Mat}_n(F)$. Then the differential equation is conjugate to a differential equation $\partial(\boldsymbol{y}) = B\boldsymbol{y}$ with $B \in \mathrm{Lie}_F(\mathcal{G})$.*

Here, conjugate means that the equation is obtained via a change of bases in F^n, i.e. replacing $\boldsymbol{y}$ by $D^{-1}\boldsymbol{y}$ for some $D \in \mathrm{GL}_n(F)$. In explicit terms, this means that $B = DAD^{-1} + \partial(D)D^{-1}$ for some $D \in \mathrm{GL}_n(F)$.

Using these bounds, Mitchi and Singer [MS96] gave a constructive solution to the inverse problem for connected linear algebraic groups over C, which they later extended to non-connected groups with solvable connected component (cf. [MS02]).

A general result was given by Hartmann in her PhD thesis [Har05] showing that every linear algebraic group is the Galois group of a linear differential equation over $C(x)$, when C is algebraically closed.

Using the so-called *Kovacic trick* (see [BHH16, Thm. 4.12]), one can deduce that the inverse Galois problem also has an affirmative answer for every finitely generated differential field F with algebraically closed constants C. The main ideas for a given linear algebraic group G over C and such a differential field F are the following: Firstly, after a transformation of the derivation, there is some

[2] As noted before, in the differential Galois setting, all fields are assumed to have characteristic zero.

$x \in F$ such that $(C(x), \partial_x)$ is a differential subfield of F. Further, one considers the group G^r for large enough $r \geq 1$, and a Picard-Vessiot extension E over $C(x)$ for G^r, and shows that at least one subextension $\tilde{E}$ of E with group G is linearly disjoint to F.

In the article [Dyc08] in which Dyckerhoff established a Picard-Vessiot theory with non-algebraically closed fields of constants, he also solved the inverse problem over the field $\mathbb{R}(z)$. This was done by descent from the complex case.

In the article [BHH16] mentioned above, the authors solve the inverse Galois problem in the affirmative over any "global" differential field F over C, where the field of constants C is a Laurent series field. In an even more recent paper [BHHP17], they generalize this to such differential fields, where the field of constants is a *large field* of infinite transcendence degree over $\mathbb{Q}$. This includes for example the p-adic numbers $\mathbb{Q}_p$, the reals $\mathbb{R}$, and certain Laurent series fields.

DELETE LOCAL CASE?

In the case of local differential fields, e.g. the Laurent series field $(\mathbb{C}((x)), \partial_x)$, the situation is quite different. Namely, a linear algebraic group G is realisable over $\mathbb{C}((x))$ if and only if G contains a torus T which is normal in G, and such that G/T is topologically generated by one element (see [vdPS03, Section 11.2]).

1.8.2 In iterative differential Galois theory

subsec:inverse-problem-ID

When Matzat and van der Put set up the Galois theory for iterative differential equations in positive characteristic, they also considered the inverse Galois problem in this setting. Of course, they only consider reduced group schemes, since they obtained them from the group C-rational points. As before, C is the field of constants which is assumed to be algebraically closed. By [Mau10a, Cor. 11.7], however, all Galois groups of PV-extension over F are reduced, if $\mathrm{Ker}(\theta_F^{(1)})$ equals F^p. This applies for example to finite extensions of the rational function field $C(x)$ with the standard iterative derivation, or the Laurent series field $C((x))$.

Having this in mind, Matzat and van der Put fully solved the inverse Galois problem for $F = C((x))$ in [MvdP03, Sect. 6]:

Theorem 1.8.3 ([MvdP03, Cor. 6.4 & Thm. 6.6])**.** *A reduced linear algebraic group $\mathcal{G}$ over C is realizable as iterative differential Galois group over $C((x))$ if and only if*

1. *$\mathcal{G}$ is solvable,*
2. *$\mathcal{G}/p(\mathcal{G})$ is commutative, and*
3. *$\mathcal{G}/\mathcal{G}^0$ is an extension of a cyclic group of order prime to p by a p-group.*

Here $\mathcal{G}^0$ is the connected component of the identity element, and $p(\mathcal{G})$ is the normal subgroup generated by elements of p-power order.

For the field $F = C(x)$ or some finite extension of it, they also solved the inverse Galois problem. As in the differential case in characteristic zero, the answer is affirmative, i.e. all reduced linear algebraic groups can be realized as ID-Galois groups over such F.

Matzat: reduced, meine PhD: restricted singularities in reduced connected case; finite problem in Chapter 4

1.8.3 In difference Galois theory

subsec:inverse-problem-difference

??

Chapter 2

Categorical Picard-Vessiot theory

chap:categorical

In this chapter, we present the categorical approach which unifies the general properties and objects of all the Picard-Vessiot theories mentioned in the introduction. This categorical framework also leads to deeper insight into the structure of all these Picard-Vessiot theories, and establishes a basis for possible further generalizations.

The main results are the construction of a universal solution ring for a given "module" M such that all Picard-Vessiot rings (PV-rings) for M are quotients of this ring (Thm. 2.4.7 and Thm. 2.4.12), the existence of PV-rings up to a finite extension of constants (Thm. 2.4.18), and uniqueness of PV-rings inside a given simple solution ring with same constants (Prop. 2.4.14). Furthermore, we prove a correspondence between isomorphism classes of fibre functors $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_{\tilde{k}}$ and isomorphism classes of PV-rings R for $M \otimes_k \tilde{k}$, where k is the field of constants of the base ring S and $\tilde{k}$ is any finite extension of k (Thm. 2.5.5). We also prove that the group scheme of automorphisms $\underline{\mathrm{Aut}}^{\partial}(R/S)$ of R over S that commute with the extra structure, is isomorphic to the affine group scheme of automorphisms $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ of the corresponding fibre functor ω (Cor. 2.6.8). These two statements are direct generalizations of the corresponding facts given for example in [Del90, Ch. 9] or [And01, Sect. 3.4 and 3.5].

Finally, we give a Galois correspondence between closed normal subgroup schemes of the Galois group scheme and subalgebras of the PV-ring which are PV-rings for some other "module".

2.1 A commutative algebra theorem

sec:comm-alg-thm

We will be faced with the question whether there exists a Picard-Vessiot ring up to a finite extension of constants. The following theorem will be a key incredient to the existence proof. All algebras are assumed to be commutative with unit.

thm:abstract-algebra

Theorem 2.1.1. *Let k be a field, S an algebra over k and R a finitely generated flat S-algebra. Furthermore, let ℓ be a field extension of k such that $S \otimes_k \ell$ embeds into R as an S-algebra. Then ℓ is a finite extension of k.*

Proof. The proof is split into several steps:

1) Reduction to S being a field

Choose a minimal prime ideal $\mathfrak{p}$ of S, and let $S_{\mathfrak{p}}$ denote the localization of S at $\mathfrak{p}$. Since localizations are flat, the inclusion of rings $S \subseteq S \otimes_k \ell \subseteq R$ induces an inclusion of rings

$$S_{\mathfrak{p}} \subseteq S_{\mathfrak{p}} \otimes_k \ell \subseteq S_{\mathfrak{p}} \otimes_S R,$$

and $S_{\mathfrak{p}} \otimes_S R$ is a finitely generated $S_{\mathfrak{p}}$-algebra. Since flatness is stable under base change, $S_{\mathfrak{p}} \otimes_S R$ is a flat $S_{\mathfrak{p}}$-algebra.
Since $\mathfrak{p}S_{\mathfrak{p}}$ is the maximal ideal of $S_{\mathfrak{p}}$, $\bar{S} := S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is a field, and $\bar{R} := S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}} \otimes_S R$

is a finitely generated flat algebra over $\bar{S}$. It remains to show that $\bar{S} \otimes_k \ell$ embeds into $\bar{R}$.

Since $S_\mathfrak{p} \otimes_k \ell$ and $S_\mathfrak{p} \otimes_S R$ are both flat over $S_\mathfrak{p}$, the exact sequence $0 \to \mathfrak{p}S_\mathfrak{p} \to S_\mathfrak{p} \to S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p} \to 0$ leads to a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{p}S_\mathfrak{p} \otimes_k \ell & \longrightarrow & S_\mathfrak{p} \otimes_k \ell & \longrightarrow & (S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}) \otimes_k \ell & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{p}S_\mathfrak{p} \otimes_S R & \longrightarrow & S_\mathfrak{p} \otimes_S R & \longrightarrow & (S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}) \otimes_S R & \longrightarrow & 0. \end{array}$$

Then the last vertical arrow is an injection if the left square is a pullback diagram. Hence, we have to proof that any element in $S_\mathfrak{p} \otimes_k \ell$ whose image in $S_\mathfrak{p} \otimes_S R$ actually lies in $\mathfrak{p}S_\mathfrak{p} \otimes_S R$ is an element of $\mathfrak{p}S_\mathfrak{p} \otimes_k \ell$.

Hence, let $z = \sum_{i=1}^n s_i \otimes x_i \in S_\mathfrak{p} \otimes_k \ell$ with k-linearly independent $x_1, \ldots, x_n \in \ell$, and let $w = \sum_{j=1}^m a_j \otimes r_j \in \mathfrak{p}S_\mathfrak{p} \otimes_S R$ such that their images in $S_\mathfrak{p} \otimes_S R$ are the same. Since all elements in $\mathfrak{p}S_\mathfrak{p}$ are nilpotent, there is $e_1 \geq 0$ maximal such that $a_1^{e_1} \neq 0$. Inductively for $j = 2, \ldots, m$, there is $e_j \geq 0$ maximal such that $a_1^{e_1} \cdots a_j^{e_j} \neq 0$. Let $a := \prod_{j=1}^m a_j^{e_j} \in S_\mathfrak{p}$. Then by construction, $a \neq 0$ but $a \cdot w = \sum_{j=1}^m a a_j \otimes r_j = 0$. So $0 = a \cdot z = \sum_{i=1}^n a s_i \otimes x_i$, i.e. $a s_i = 0$ for all i. Since $a \neq 0$, one obtains $s_i \notin (S_\mathfrak{p})^\times$, i.e. $s_i \in \mathfrak{p}S_\mathfrak{p}$.

From now on, we may and will assume that S is a field. In this case R is Noetherian as it is a finitely generated S-algebra.

2) Proof that ℓ is algebraic over k

Assume that ℓ is not algebraic over k, then there is an element $a \in \ell$ transcendental over k. By assumption, a is also transcendental over S inside R, i.e. the polynomial ring $S[a]$ is a subring of R. The image of the corresponding morphism $\psi : \mathrm{Spec}(R) \to \mathrm{Spec}(S[a]) \cong \mathbb{A}^1_S$ is a dense subset of $\mathrm{Spec}(S[a])$, since the ringhomomorphism is an inclusion, and it is locally closed by [Bou98, Cor. 3, Ch. V, §3.1]. Hence, the image is open. But for all $0 \neq f \in k[a]$, the irreducible factors of f in $S[a]$, are invertible in $\ell \subseteq R$. Hence, infinitely many maximal ideals of $\mathrm{Spec}(S[a])$ are not in the image of ψ – contradicting that the image is open.

3) Proof that ℓ is finite over k

For showing that ℓ is indeed finite over k, we give a bound on $[\ell' : k]$ for any $\ell' \subseteq \ell$ which is finite over k, and this bound only depends on data of R. Since ℓ is the union of all its finite subextensions this proves finiteness of ℓ.

For simplicity we again write ℓ for the finite extension ℓ' of k.
Let

$$(0) = \bigcap_{i=1}^c \mathfrak{q}_i$$

be a primary decomposition of the zero ideal $(0) \subseteq R$ and $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ the corresponding prime ideals. Furthermore, let $N_i \in \mathbb{N}$ satisfy $\mathfrak{p}_i^{N_i} \subseteq \mathfrak{q}_i$, i.e. for all

$y_1, \ldots, y_{N_i} \in \mathfrak{p}_i$, one has $y_1 \cdot y_2 \cdots y_{N_i} \in \mathfrak{q}_i$.[1] Furthermore, for each $i = 1, \ldots, c$ let $\mathfrak{m}_i \subseteq R$ be a maximal ideal containing $\mathfrak{p}_i$. Then $d_i := \dim_S R/\mathfrak{m}_i$ is finite for all i.

We claim that $\dim_k(\ell)$ is bounded by $2 \cdot \sum_{i=1}^{c} d_i \cdot N_i$:

First at all $R \to \prod_{i=1}^{c} R/\mathfrak{q}_i$ is an injective S-algebra homomorphism and $R/\mathfrak{q}_i$ is irreducible with unique minimal ideal $\mathfrak{p}_i$.
Letting $\tilde{\mathfrak{q}_i} := \mathfrak{q}_i \cap (S \otimes_k \ell)$, and $\tilde{\mathfrak{p}_i} := \mathfrak{p}_i \cap (S \otimes_k \ell) = \sqrt{\tilde{\mathfrak{q}_i}}$, then $(S \otimes_k \ell)/\tilde{\mathfrak{q}_i}$ embeds into $R/\mathfrak{q}_i$, and $S \otimes_k \ell \to \prod_{i=1}^{c} (S \otimes_k \ell)/\tilde{\mathfrak{q}_i}$ is injective. It therefore suffices to show that $\dim_S ((S \otimes_k \ell)/\tilde{\mathfrak{q}_i}) \leq 2 d_i N_i$ holds for each i. In the following we therefore consider an arbitrary component and will omit the index i.

Since $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is a finite S-algebra, and $\tilde{\mathfrak{p}}$ is its unique minimal prime ideal, $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is a local Artinian algebra with residue field $(S \otimes_k \ell)/\tilde{\mathfrak{p}}$. Since $(S \otimes_k \ell)/\tilde{\mathfrak{p}}$ is a field, the composition

$$(S \otimes_k \ell)/\tilde{\mathfrak{p}} \hookrightarrow R/\mathfrak{p} \to R/\mathfrak{m}$$

is injective. Hence,

$$\dim_S ((S \otimes_k \ell)/\tilde{\mathfrak{p}}) \leq \dim_S (R/\mathfrak{m}) = d.$$

It remains to show that $\dim_{(S \otimes_k \ell)/\tilde{\mathfrak{p}}} ((S \otimes_k \ell)/\tilde{\mathfrak{q}}) \leq 2N$.

As a tensor product of fields and as ℓ/k is finite, $S \otimes_k \ell$ is a finite direct product of local artinian algebras with residue fields being finite extensions of S. The local algebra over some finite extension S' of S is given as $S' \otimes_{k'} \tilde{k}$ for a finite extension k' of k contained in S' and a purely inseparable extension $\tilde{k}/k'$.

In particular, also the algebra $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is of that form (as it is just isomorphic to one factor of $(S \otimes_k \ell)$). Hence, let S', k' and $\tilde{k}$ be such that $(S \otimes_k \ell)/\tilde{\mathfrak{p}} \cong S'$ and $(S \otimes_k \ell)/\tilde{\mathfrak{q}} \cong S' \otimes_{k'} \tilde{k}$. As $\tilde{k}$ is purely inseparable over k', there are $x_1, \ldots, x_t \in \tilde{k}$, $m_1, \ldots, m_t \in \mathbb{N}$ and $a_1, \ldots, a_t \in k'$ such that

$$\tilde{k} = k'[x_1, \ldots, x_t] / \left(x_1^{p^{m_1}} - a_1, \ldots, x_t^{p^{m_t}} - a_t \right).$$

where p denotes the characteristic of the fields. As $S' \otimes_{k'} \tilde{k}$ is local with residue field S', there are also $s_1, \ldots, s_t \in S'$ such that $s_j^{p^{m_j}} = a_j$ for all $j = 1, \ldots, t$, and $S' \otimes_{k'} \tilde{k}$ is given as

$$S' \otimes_{k'} \tilde{k} \cong S'[x_1, \ldots, x_t] / \left((x_1 - s_1)^{p^{m_1}}, \ldots, (x_t - s_t)^{p^{m_t}} \right).$$

In particular its nilradical (corresponding to $\tilde{\mathfrak{p}}$) is generated by $(x_1 - s_1, \ldots, x_t - s_t)$.

Since $\tilde{\mathfrak{p}}^N \subseteq \tilde{\mathfrak{q}}$, and $(x_1 - s_1)^{p^{m_1}-1} \cdots (x_t - s_t)^{p^{m_t}-1} \neq 0$ we obtain that

$$N > \sum_{j=1}^{t} (p^{m_j} - 1) \geq \sum_{j=1}^{t} \frac{1}{2} p^{m_j} = \frac{1}{2} \dim_{S'} (S' \otimes_{k'} \tilde{k}).$$

[1] This N_i exists since R is Noetherian and therefore $\mathfrak{p}_i$ is finitely generated.

Therefore, we have shown that $\dim_{(S\otimes_k \ell)/\tilde{\mathfrak{p}}}((S\otimes_k \ell)/\tilde{\mathfrak{q}}) < 2N$.

□

2.2 Setup and basic properties

sec:setup

In this section, we set up an abstract framework in which we can prove theorems on Picard-Vessiot extensions, as well as their Galois groups. The theorems thus apply to all kinds of differential and difference Galois theories which match the basic setup given below. The setup therefore provides a uniform approach to the existing theories.

We consider the following setup:

(C1) $\mathcal{C}$ is a locally small abelian symmetric monoidal category with unit object $\mathbb{1} \in \mathcal{C}$. We assume that $\mathbb{1}$ is a simple object in $\mathcal{C}$.

(C2) $\mathcal{C}$ is cocomplete, i.e. $\mathcal{C}$ is closed under small inductive limits.

(F1) There is a scheme $\mathcal{X}$, and an additive tensor functor $\upsilon : \mathcal{C} \to \mathsf{Qcoh}(\mathcal{X})$ from $\mathcal{C}$ to the category of quasi-coherent $\mathcal{O}_\mathcal{X}$-modules which is faithful, exact and preserves small inductive limits. (In particular, $\upsilon(\mathbb{1}) = \mathcal{O}_\mathcal{X}$.)

(F2) $M \in \mathcal{C}$ is dualizable whenever $\upsilon(M)$ is a finitely generated $\mathcal{O}_\mathcal{X}$-module.

Remark 2.2.1. 1. The presence of a faithful functor $\upsilon : \mathcal{C} \to \mathsf{Qcoh}(\mathcal{X})$ as stated in (F1) already implies that all $\mathrm{Mor}_\mathcal{C}(M, N)$ are abelian groups, i.e. that $\mathcal{C}$ is locally small. Hence, we could have ommitted this condition in (C1). However, in this section and Section 2.3, we will not use conditions (F1) and (F2) and therefore need the condition "locally small" in (C1).

2. By an object $M \in \mathcal{C}$ being *dualizable*, we mean that M admits a (right) dual, i.e. an object $M^\vee \in \mathcal{C}$ together with two morphisms $\mathrm{ev}_M : M \otimes M^\vee \to \mathbb{1}$ (*evaluation*) and $\delta_M : \mathbb{1} \to M^\vee \otimes M$ (*coevaluation*) such that the diagrams

$$\begin{array}{ccc} M^\vee \cong \mathbb{1}\otimes M^\vee & \xrightarrow{\delta_M\otimes \mathrm{id}_{M^\vee}} & M^\vee\otimes M\otimes M^\vee \\ & \searrow^{\mathrm{id}_{M^\vee}} & \downarrow{\scriptstyle \mathrm{id}_{M^\vee}\otimes \mathrm{ev}_M} \\ & & M^\vee\otimes\mathbb{1} \cong M^\vee \end{array} \quad \text{and} \quad \begin{array}{ccc} M \cong M\otimes\mathbb{1} & \xrightarrow{\mathrm{id}_M\otimes\delta_M} & M\otimes M^\vee\otimes M \\ & \searrow^{\mathrm{id}_M} & \downarrow{\scriptstyle \mathrm{ev}_M\otimes\mathrm{id}_M} \\ & & \mathbb{1}\otimes M \cong M \end{array}$$

commute.

Example 2.2.2. All the settings mentioned in the introduction are examples for the category $\mathcal{C}$.

In the remainder of this section, $\mathcal{C}$ will be a category satisfying properties (C1) and (C2).

Let $k := \mathrm{End}_{\mathcal{C}}(\mathbb{1})$ denote the ring of endomorphisms of the unit object $\mathbb{1}$. Then by simplicity of $\mathbb{1}$, k is a division ring, and even a field, as $\mathrm{End}_{\mathcal{C}}(\mathbb{1})$ is always commutative.

Let vect_k denote the category of k-vector spaces, and vect_k the subcategory of finite dimensional k-vector spaces. There is a functor $\otimes_k : \mathcal{C} \times \mathsf{vect}_k \to \mathcal{C}$ such that $M \otimes_k k^n = M^n$ and in general $M \otimes_k V \cong M^{\dim(V)}$ (cf. [DM82], p. 21 for details).
As $\mathcal{C}$ is cocomplete, the functor $\otimes_k$ can be extended to $\otimes_k : \mathcal{C} \times \mathsf{vect}_k \to \mathcal{C}$ via

$$M \otimes_k V := \varinjlim_{\substack{W \subset V \\ \text{fin.dim.}}} M \otimes_k W.$$

This functor fulfills a functorial isomorphism of k-vector spaces

$$\mathrm{Mor}_{\mathcal{C}}(N, M \otimes_k V) \cong \mathrm{Mor}_{\mathcal{C}}(N, M) \otimes_k V \text{ for all } M, N \in \mathcal{C}, V \in \mathsf{vect}_k,$$

where the tensor product on the right hand side is the usual tensor product of k-vector spaces. Recall that $\mathrm{Mor}_{\mathcal{C}}(N, M)$ is a k-vector space via the action of $k = \mathrm{End}_{\mathcal{C}}(\mathbb{1})$.

The functor $\otimes_k$ induces a tensor functor $\iota : \mathsf{vect}_k \to \mathcal{C}$ given by $\iota(V) := \mathbb{1} \otimes_k V$, and one obviously has $M \otimes_k V \cong M \otimes \iota(V)$ (the second tensor product taken in $\mathcal{C}$). The functor ι is faithful and exact by construction. Since ι is an exact tensor functor and all finite dimensional vector spaces have a dual (in the categorial sense), all objects $\iota(V)$ for $V \in \mathsf{vect}_k$ are dualizable in $\mathcal{C}$.

There is also a functor $(-)^{\mathcal{C}} := \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, -) : \mathcal{C} \to \mathsf{vect}_k$ from the category $\mathcal{C}$ to the category of all k-vector spaces.

Remark 2.2.3. As already mentioned in the introduction, in the differential case $M^{\mathcal{C}} = M^{\partial}$ is just the k-vector space of constants of the differential module M. In the difference case (with endomorphism σ), $M^{\mathcal{C}}$ equals the invariants M^{σ} of the difference module M.
The functor ι corresponds to the construction of "trivial" differential (resp. difference) modules by tensoring a k-vector space with the differential (resp. difference) base field F.

The following proposition gives some properties of the functors ι and $(-)^{\mathcal{C}}$ which are well known for differential resp. difference modules.

prop:first-properties-cat

Proposition 2.2.4. *Let $\mathcal{C}$ be a category satisfying (C1) and (C2), and let ι and $()^{\mathcal{C}}$ be as above. Then the following hold.*

1. *If $V \in \mathsf{vect}_k$, then any subobject and any quotient of $\iota(V)$ is isomorphic to $\iota(W)$ for some $W \in \mathsf{vect}_k$.*

2. If $V \in \mathsf{vect}_k$, then $\iota(V) \in \mathcal{C}$ has finite length and $\mathrm{length}(\iota(V)) = \dim_k(V)$.

3. If $M \in \mathcal{C}$ has finite length, then $M^{\mathcal{C}} \in \mathsf{vect}_k$ and $\dim_k(M^{\mathcal{C}}) \leq \mathrm{length}(M)$.

Proof. 1. First consider the case that $V \in \mathsf{vect}_k$ is of finite dimension. We show the claim by induction on $\dim(V)$.
The case $\dim(V) = 0$ is trivial. Let $V \in \mathsf{vect}_k$ and $N \in \mathcal{C}$ be a subobject of $\iota(V)$, and let $V' \subseteq V$ be a 1-dimensional subspace. Then one has a split exact sequence of k-vector spaces $0 \to V' \to V \to V/V' \to 0$ and therefore a split exact sequence

$$0 \to \iota(V') \to \iota(V) \to \iota(V/V') \to 0$$

in $\mathcal{C}$. Since N is a subobject of $\iota(V)$, the pullback $N \cap \iota(V')$ is a subobject of $\iota(V') \cong \mathbb{1}$. As $\mathbb{1}$ is simple, $N \cap \iota(V') = 0$ or $N \cap \iota(V') = \iota(V')$.
In the first case, $N \hookrightarrow \iota(V/V')$, and the claim follows by induction on $\dim(V)$.
In the second case, by induction $N/\iota(V')$ is isomorphic to $\iota(W)$ for some subspace $W \subseteq \iota(V/V')$. If W' denotes the preimage of W under the epimorphism $V \to V/V'$, one has a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \iota(V') & \longrightarrow & N & \longrightarrow & \iota(W) & \longrightarrow & 0\,, \\ & & \downarrow\cong & & \downarrow & & \downarrow\cong & & \\ 0 & \longrightarrow & \iota(V') & \longrightarrow & \iota(W') & \longrightarrow & \iota(W) & \longrightarrow & 0 \end{array}$$

and therefore $N \cong \iota(W')$.

If $V \in \mathsf{vect}_k$ has infinite dimension, we recall that $\iota(V) = \varinjlim_{\substack{W \subset V \\ \text{fin.dim.}}} \iota(W)$ and hence, for any subobject $N \subseteq \iota(V)$, one has

$$N = \varinjlim_{\substack{W \subset V \\ \text{fin.dim.}}} N \cap \iota(W).$$

From the special case of finite dimension, we obtain $N \cap \iota(W) = \iota(W')$ for some W' related to W, and therefore

$$N = \varinjlim_{\substack{W \subset V \\ \text{fin.dim.}}} \iota(W') = \iota\left(\varinjlim_{\substack{W \subset V \\ \text{fin.dim.}}} W'\right).$$

Now let $V \in \mathsf{vect}_k$ be arbitrary and, let N be a quotient of $\iota(V)$. Then by the previous, $\mathrm{Ker}(\iota(V) \to N)$ is of the form $\iota(V')$ for some $V' \subseteq V$, and hence $N \cong \iota(V)/\iota(V') \cong \iota(V/V')$, as ι is exact.

2. By part (i), every sequence of subobjects $0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq \iota(V)$ is induced via ι by a sequence of subvector spaces $0 = W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq V$. Hence, $\mathrm{length}(\iota(V)) = \dim_k(V)$.

3. We use induction on the length of M. If M has length 1, then M is a simple object. Since $\mathbb{1}$ also is simple, every morphism in $M^{\mathcal{C}} = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M)$ is either 0 or an isomorphism. In particular, $k = \mathrm{End}_{\mathcal{C}}(\mathbb{1})$ acts transitively on $\mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M)$, which shows that $\dim_k(\mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M))$ is 0 or 1. For the general case, take a subobject $0 \neq N \neq M$ of M. Applying the functor $()^{\mathcal{C}} = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, -)$ to the exact sequence $0 \to N \to M \to M/N \to 0$ leads to an exact sequence

$$0 \to N^{\mathcal{C}} \to M^{\mathcal{C}} \to (M/N)^{\mathcal{C}},$$

as the functor $\mathrm{Mor}_{\mathcal{C}}(X, -)$ is always left-exact.
Hence, $\dim_k(M^{\mathcal{C}}) \leq \dim_k(N^{\mathcal{C}}) + \dim_k((M/N)^{\mathcal{C}})$. Since N and M/N have smaller length than M, we obtain the claim by induction using $\mathrm{length}(M) = \mathrm{length}(N) + \mathrm{length}(M/N)$.

□

prop:adjointness

Proposition 2.2.5. *Let $\mathcal{C}$ be a category satisfying (C1) and (C2) and let ι and $()^{\mathcal{C}}$ be as above. Then the following hold.*

1. *The functor ι is left adjoint to the functor $()^{\mathcal{C}}$, i.e. for all $V \in \mathsf{vect}_k$, $M \in \mathcal{C}$, there are isomorphisms of k-vector spaces $\mathrm{Mor}_{\mathcal{C}}(\iota(V), M) \cong \mathrm{Hom}_k(V, M^{\mathcal{C}})$ functorial in V and M.*

2. *For every $V \in \mathsf{vect}_k$, the homomorphism $\eta_V : V \to (\iota(V))^{\mathcal{C}}$ which is adjoint to $\mathrm{id}_{\iota(V)}$ is an isomorphism.*

3. *For every $M \in \mathcal{C}$, the morphism $\varepsilon_M : \mathbb{1} \otimes_k \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M) = \iota(M^{\mathcal{C}}) \to M$ which is adjoint to $\mathrm{id}_{M^{\mathcal{C}}}$ is a monomorphism.*

rem:iota-full

Remark 2.2.6. 1. Whereas in the differential resp. difference settings, part (i) and (ii) are easily seen, part (iii) amounts to saying that any set $v_1, \ldots, v_n \in M^{\mathcal{C}}$ of constant (resp. invariant) elements of M which are k-linearly independent, are also independent over the differential (resp. difference) field F. This is proven in each setting separately. However, Amano and Masuoka provide an abstract proof (which is given in [Ama05, Prop. 3.1.1]) which relies on the Freyd embedding theorem.

2. The collection of homomorphisms $(\eta_V)_{V \in \mathsf{vect}_k}$ is just the natural transformation $\eta : \mathrm{id}_{\mathsf{vect}_k} \to (-)^{\mathcal{C}} \circ \iota$ (unit of the adjunction) whereas the morphisms ε_M form the natural transformation $\varepsilon : \iota \circ (-)^{\mathcal{C}} \to \mathrm{id}_{\mathcal{C}}$ (counit of the adjunction). By the general theory on adjoint functors, for all $V, W \in \mathsf{vect}_k$, the maps $\mathrm{Hom}_k(V, W) \to \mathrm{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$ induced by applying ι are just the compositions

$$\mathrm{Hom}_k(V, W) \xrightarrow{\eta_W \circ (-)} \mathrm{Hom}_k(V, \iota(W)^{\mathcal{C}}) \xleftarrow[\simeq]{\text{adjunction}} \mathrm{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$$

(cf. [ML98],p. 81,eq. (3) and definition of η). This implies that η_W is a monomorphism for all $W \in \mathsf{vect}_k$ if and only if $\mathrm{Hom}_k(V,W) \to \mathrm{Mor}_{\mathcal{C}}(\iota(V),\iota(W))$ is injective for all $V, W \in \mathsf{vect}_k$, i.e. if ι is a faithful functor. Furthermore, η_W is a split epimorphism for all $W \in \mathsf{vect}_k$ if and only if $\mathrm{Hom}_k(V,W) \to \mathrm{Mor}_{\mathcal{C}}(\iota(V),\iota(W))$ is surjective for all $V, W \in \mathsf{vect}_k$, if and only if ι is a full functor. In particular, η_W being an isomorphism for all $W \in \mathsf{vect}_k$ is equivalent to ι being a fully faithful functor.

Proof of Prop. 2.2.5. 1. For $V \in \mathsf{vect}_k$ and $M \in \mathcal{C}$ we have natural isomorphisms

$$\begin{aligned} \mathrm{Mor}_{\mathcal{C}}(\iota(V), M) &\cong \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M \otimes \iota(V)^\vee) \cong \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M \otimes_k V^\vee) \\ &\cong \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M) \otimes_k V^\vee \cong \mathrm{Hom}_k(V, \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M)) \\ &= \mathrm{Hom}_k(V, M^{\mathcal{C}}) \end{aligned}$$

If V is of infinite dimension the statement is obtained using that $\mathrm{Mor}_{\mathcal{C}}$ and Hom_k commute with inductive limits, i.e.

$$\begin{aligned} \mathrm{Mor}_{\mathcal{C}}(\iota(V), M) &= \mathrm{Mor}_{\mathcal{C}}(\varinjlim_{\substack{W \subset V \\ \text{fin.dim}}} \iota(W), M) = \varprojlim_{\substack{W \subset V \\ \text{fin.dim}}} \mathrm{Mor}_{\mathcal{C}}(\iota(W), M) \\ &\cong \varprojlim_{\substack{W \subset V \\ \text{fin.dim}}} \mathrm{Hom}_k(W, M^{\mathcal{C}}) = \mathrm{Hom}_k(V, M^{\mathcal{C}}). \end{aligned}$$

2. We have, $(\iota(V))^{\mathcal{C}} = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, \mathbb{1} \otimes_k V) \cong \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, \mathbb{1}) \otimes_k V \cong k \otimes_k V = V$, and the morphism $\mathrm{id}_{\iota(V)}$ corresponds to $\mathrm{id}_V : V \xrightarrow{\eta_V} (\iota(V))^{\mathcal{C}} \cong V$ via all these natural identifications.

3. Let $M \in \mathcal{C}$ and $N := \mathrm{Ker}(\varepsilon_M) \subseteq \iota(M^{\mathcal{C}})$. By Prop. 2.2.4(i), there is a subspace W of $M^{\mathcal{C}}$ such that $N = \iota(W)$. Hence, we have an exact sequence of morphisms

$$0 \to \iota(W) \to \iota(M^{\mathcal{C}}) \xrightarrow{\varepsilon_M} M.$$

Since $()^{\mathcal{C}}$ is left exact, this leads to the exact sequence

$$0 \to (\iota(W))^{\mathcal{C}} \to (\iota(M^{\mathcal{C}}))^{\mathcal{C}} \xrightarrow{(\varepsilon_M)^{\mathcal{C}}} M^{\mathcal{C}}$$

But $\eta_V : V \to (\iota(V))^{\mathcal{C}}$ is an isomorphism for all V by part (ii). So we obtain an exact sequence

$$0 \to W \to M^{\mathcal{C}} \xrightarrow{(\varepsilon_M)^{\mathcal{C}} \circ \eta_{M^{\mathcal{C}}}} M^{\mathcal{C}},$$

and the composite $(\varepsilon_M)^{\mathcal{C}} \circ \eta_{M^{\mathcal{C}}}$ is the identity on $M^{\mathcal{C}}$ by general theory on adjoint functors (cf. [ML98, Ch. IV, Thm. 1]). Hence, $W = 0$.

□

2.3 $\mathcal{C}$-algebras and base change

sec:c-algebras

We recall some notation which are already present in [ML65, Ch. 17 & 18], and refer to loc. cit. for more details. The reader should be aware that a "tensored category" in [ML65] is the same as an "abelian symmetric monoidal category" here.

A **commutative algebra in $\mathcal{C}$** (or a **$\mathcal{C}$-algebra** for short) is an object $R \in \mathcal{C}$ together with two morphisms $u_R : \mathbb{1} \to R$ and $\mu_R : R \otimes R \to R$ satisfying several commuting diagrams corresponding to associativity, commutativity and the unit. For instance,

$$\mu_R \circ (u_R \otimes \mathrm{id}_R) = \mathrm{id}_R = \mu_R \circ (\mathrm{id}_R \otimes u_R)$$

says that u_R is a unit for the multiplication μ_R (cf. [ML65, Ch. 17]; although the term "$\mathcal{C}$-algebra" in [ML65] does not include commutativity).

For a $\mathcal{C}$-algebra R we define $\mathcal{C}_R$ to be the category of R-modules in $\mathcal{C}$, i.e. the category of pairs (M, μ_M) where $M \in \mathcal{C}$ and $\mu_M : R \otimes M \to M$ is a morphism in $\mathcal{C}$ satisfying the usual commuting diagrams for turning M into an R-module (cf. [ML65, Ch. 18]).[2] The morphisms in $\mathcal{C}_R$ are morphisms in $\mathcal{C}$ which commute with the R-action. The category $\mathcal{C}_R$ is also an abelian symmetric monoidal category with tensor product $\otimes_R$ defined as

$$M \otimes_R N := \mathrm{Coker}((\mu_M \circ \tau) \otimes \mathrm{id}_N - \mathrm{id}_M \otimes \mu_N : M \otimes R \otimes N \to M \otimes N),$$

where $\tau : M \otimes R \to R \otimes M$ is the twist morphism (see [ML65, Prop. 18.3]).

A **$\mathcal{C}$-ideal** I of a $\mathcal{C}$-algebra R is a subobject of R in the category $\mathcal{C}_R$, and R is called a **simple** $\mathcal{C}$-algebra, if 0 and R are the only $\mathcal{C}$-ideals of R, i.e. if R is a simple object in $\mathcal{C}_R$.

Definition 2.3.1. For a $\mathcal{C}$-algebra R, the additive right-exact functor $()_R : (\mathcal{C}, \otimes) \to (\mathcal{C}_R, \otimes_R), M \mapsto M_R := (R \otimes M, \mu_R \otimes \mathrm{id}_M)$ is called the *base change functor*. It is even a tensor functor, and it is a left adjoint to the forgetful functor $\mathcal{C}_R \to \mathcal{C}$ (see [ML65, Thm. 18.2]).

We can also base change the functors ι and $()^{\mathcal{C}}$. In more details, having in mind that $\mathrm{End}_{\mathcal{C}_R}(R) = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R) = R^{\mathcal{C}}$:

$$\iota_R : \quad \mathrm{mod}\text{-}R^{\mathcal{C}} \to \mathcal{C}_R, V \mapsto R \otimes_{\iota(R^{\mathcal{C}})} \iota(V)$$

and

$$()^{\mathcal{C}_R} : \mathcal{C}_R \to \quad \mathrm{mod}\text{-}R^{\mathcal{C}}, M \mapsto \mathrm{Mor}_{\mathcal{C}_R}(R, M) = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, M) = M^{\mathcal{C}}.$$

A special case is given, if $R = \iota(A)$ for some commutative k-algebra A. In this case, ι_R is "the same" as ι. This case corresponds to an extension by constants in the theory of differential or difference modules.

[2] Most times, we will omit the μ_M in our notation, and just write $M \in \mathcal{C}_R$.

Proposition 2.3.2. *The functor ι_R is left adjoint to the functor $()^{\mathcal{C}_R}$.*

Proof. Let $V \in \ \mathrm{mod}\ _{R^{\mathcal{C}}}$ and $M \in \mathcal{C}_R$, then

$$\mathrm{Mor}_{\mathcal{C}_R}(\iota_R(V), M) = \mathrm{Mor}_{\mathcal{C}_R}(R \otimes_{\iota(R^{\mathcal{C}})} \iota(V), M) = \mathrm{Mor}_{\mathcal{C}_{\iota(R^{\mathcal{C}})}}(\iota(V), M)$$

is the subset of $\mathrm{Mor}_{\mathcal{C}}(\iota(V), M)$ given by all $f \in \mathrm{Mor}_{\mathcal{C}}(\iota(V), M)$ such that the diagram

$$\begin{array}{ccc} \iota(R^{\mathcal{C}}) \otimes \iota(V) & \xrightarrow{\mathrm{id}\otimes f} & \iota(R^{\mathcal{C}}) \otimes M \\ \downarrow{\scriptstyle \iota(\mu_V)} & & \downarrow{\scriptstyle \mu_M} \\ \iota(V) & \xrightarrow{\quad f \quad} & M \end{array}$$

commutes. On the other hand, $\mathrm{Hom}_{R^{\mathcal{C}}}(V, M^{\mathcal{C}_R}) = \mathrm{Hom}_{R^{\mathcal{C}}}(V, M^{\mathcal{C}})$ is the subset of $\mathrm{Hom}_k(V, M^{\mathcal{C}})$ given by all $g \in \mathrm{Hom}_k(V, M^{\mathcal{C}})$ such that the diagram

$$\begin{array}{ccc} R^{\mathcal{C}} \otimes_k V & \xrightarrow{\mathrm{id}\otimes g} & R^{\mathcal{C}} \otimes_k M^{\mathcal{C}} \\ \downarrow{\scriptstyle \mu_V} & & \downarrow{\scriptstyle (\mu_M)^{\mathcal{C}}} \\ V & \xrightarrow{\quad g \quad} & M^{\mathcal{C}} \end{array}$$

commutes. Assume that f and g are adjoint morphisms (i.e. correspond to each other via the bijection $\mathrm{Mor}_{\mathcal{C}}(\iota(V), M) \cong \mathrm{Hom}_k(V, M^{\mathcal{C}})$ of Prop.2.2.5(i)), then the commutativity of the first diagram is equivalent to the commutativity of the second, since the bijection of the hom-sets is natural. □

lemma:ideal-bijection::abstract

Lemma 2.3.3. *Let A be a commutative k-algebra. Then $\iota_{\iota(A)}$ and $()^{\mathcal{C}_{\iota(A)}}$ define a bijection between the ideals of A and the $\mathcal{C}$-ideals of $\iota(A)$.*

Proof. By definition $\iota_{\iota(A)}(I) = \iota(I)$ for any $I \in \ \mathrm{mod}\ _A$. Furthermore, by Prop. 2.2.4(i), ι induces a bijection between the k-subvector spaces of A and the subobjects of $\iota(A)$ in $\mathcal{C}$. The condition on I being an ideal of A (resp. of $\iota(I)$ being an ideal of $\iota(A)$) is equivalent to the condition that the composite $A \otimes_k I \xrightarrow{\mu_A} A \to A/I$ (resp. the composite $\iota(A) \otimes \iota(I) \xrightarrow{\mu_{\iota(A)}} \iota(A) \to \iota(A)/\iota(I)$) is the zero map. Hence, the condition for $\iota(I)$ is obtained from the one for I by applying ι, and using that ι is an exact tensor functor. Since ι is also faithful, these two conditions are indeed equivalent. □

In the special case that A is a field, one obtains the following corollary.

cor:still-simple::abstract

Corollary 2.3.4. *Let ℓ be a field extension of k, then $\iota(\ell)$ is a simple $\mathcal{C}$-algebra.*

Remark 2.3.5. As ι_R and $()^{\mathcal{C}_R}$ are adjoint functors, there are again the unit and the counit of the adjunction. By abuse of notation, we will again denote the unit by η and the counit by ε. There might be an ambiguity which morphism is meant

by ε_M if (M, μ_M) is an object in $\mathcal{C}_R$. However, when M is explicitly given as an object of $\mathcal{C}_R$, then $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \to M$ is meant. This is the case, for example, if $M = N_R$ is the base change of an object $N \in \mathcal{C}$.
In cases where the right meaning of ε_M would not be clear, we always give the source and the target of ε_M.

prop:on-iota-r

Proposition 2.3.6. *Assume that, ι_R is exact and faithful* [3]*, and that any subobject of R^n is of the form $\iota_R(W)$, then the following holds.*

1. *For every $V \in \mathsf{Mod}_{R^{\mathcal{C}}}$, every subobject of $\iota_R(V)$ is isomorphic to $\iota_R(W)$ for some $W \subseteq V$.*

2. *For every $V \in \mathsf{Mod}_{R^{\mathcal{C}}}$, the morphism $\eta_V : V \to (\iota_R(V))^{\mathcal{C}_R}$ is an isomorphism.*

3. *For every $M \in \mathcal{C}_R$, the morphism $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \to M$ is a monomorphism.*

The most important cases where the proposition applies is on the one hand the case $R = \iota(A)$ for some commutative k-algebra A (in which case $\iota_R = \iota$), and on the other hand R being a simple $\mathcal{C}$-algebra.

Proof. 2. We show that $\eta_V : V \to (\iota_R(V))^{\mathcal{C}_R}$ is an isomorphism for all $V \in \mathsf{Mod}_{R^{\mathcal{C}}}$. As ι is faithful by assumption, all η_V are monomorphisms (cf. Rem. 2.2.6). For showing that η_V is an epimorphism, it is enough to show that the natural map

$$R^{\mathcal{C}} \otimes_k V = (R \otimes \iota(V))^{\mathcal{C}_R} \to (\iota_R(V))^{\mathcal{C}_R}$$

is an epimorphism, where on the left hand side, V is considered just as a k-vector space. Saying that this map is epimorphic is equivalent to saying that any morphism $g : R \to \iota_R(V)$ in $\mathcal{C}_R$ can be lifted to a morphism $f : R \to R \otimes \iota(V)$ in $\mathcal{C}_R$. So let $g : R \to \iota_R(V)$ be a morphism in $\mathcal{C}_R$, and let P be the pullback of the diagram

$$\begin{array}{ccc} P & \xrightarrow{\mathrm{pr}_1} & R \\ \downarrow{\scriptstyle \mathrm{pr}_2} & & \downarrow{\scriptstyle g} \\ R \otimes \iota(V) & \xrightarrow{p} & \iota_R(V) \end{array} .$$

Then P is a subobject of $R \oplus (R \otimes \iota(V)) \cong R^{1+\dim_k(V)}$, and hence by assumption, $P = \iota_R(W)$ for some $W \in \mathrm{mod}_{R^{\mathcal{C}}}$. By adjointness, pr_1 corresponds to some $R^{\mathcal{C}}$-homomorphism $q : W \to R^{\mathcal{C}_R} = R^{\mathcal{C}}$, i.e. $\mathrm{pr}_1 = \varepsilon_R \circ \iota_R(q)$. Since

[3] For differential rings this means that the ring R is faithfully flat over $\iota(R^{\mathcal{C}})$.

$\varepsilon_R : R = \iota_R\left(R^{\mathcal{C}_R}\right) \to R$ is the identity, and pr_1 is an epimorphism, faithfulness of ι_R implies that also q is an epimorphism. Therefore, there is a $R^{\mathcal{C}}$-homomorphism $s : R^{\mathcal{C}} \to W$ such that $q \circ s = \mathrm{id}_{R^{\mathcal{C}}}$. Let f be the morphism $f := \mathrm{pr}_2 \circ \iota_R(s) : R \to R \otimes \iota(V)$, then

$$p \circ f = p \circ \mathrm{pr}_2 \circ \iota_R(s) = g \circ \mathrm{pr}_1 \circ \iota_R(s) = g \circ \iota_R(q \circ s) = g.$$

Hence, f is a lift of g.

1. We show that any subobject of $\iota_R(V)$ is of the form $\iota_R(W)$ for some submodule W of V. The case of a quotient of $\iota_R(V)$ then follows in the same manner as in Prop. 2.2.4. Let $N \subseteq \iota_R(V)$ be a subobject in $\mathcal{C}_R$. Then the pullback of N along $p : R \otimes \iota(V) \to \iota_R(V)$ is a subobject of $R \otimes \iota(V)$, hence by assumption of the form $\iota_R(\tilde{W})$ for some $\tilde{W} \subseteq (R^{\mathcal{C}})^{\dim_k(V)}$. Furthermore, as η_V is an isomorphism, the restriction $p|_{\iota_R(\tilde{W})} : \iota_R(\tilde{W}) \to \iota_R(V)$ is induced by some homomorphism $f : \tilde{W} \to V$ (cf. Remark 2.2.6). By exactness of ι_R, we finally obtain $N = \mathrm{Im}(\iota_R(f)) = \iota_R(\mathrm{Im}(f)) = \iota_R(W)$ for $W := \mathrm{Im}(f)$.

3. The proof that $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \to M$ is a monomorphism is the same as in Prop. 2.2.5.

□

lemma:when-eps-is-iso

Lemma 2.3.7. *Let R be a simple $\mathcal{C}$-algebra. Then for $N \in \mathcal{C}_R$, the morphism ε_N is an isomorphism if and only if N is isomorphic to $\iota_R(V)$ for some $V \in \mathsf{Mod}_{R_{\mathcal{C}}}$.*

Proof. If ε_N is an isomorphism, then $N \cong \iota_R(V)$ for $V := N^{\mathcal{C}_R}$. On the other hand, let $N \cong \iota_R(V)$ for some $V \in \mathsf{Mod}_{R_{\mathcal{C}}}$. Since $\iota_R(\eta_V) \circ \varepsilon_{\iota_R(V)} = \mathrm{id}_{\iota_R(V)}$ (cf. [ML98, Ch. IV, Thm. 1]) and η_V is an isomorphism, $\varepsilon_{\iota_R(V)}$ is an isomorphism. Hence, ε_N is an isomorphism. □

prop:subcat-of-trivial-modules

Proposition 2.3.8. *Let R be a simple $\mathcal{C}$-algebra. Then the full subcategory of $\mathcal{C}_R$ consisting of all $N \in \mathcal{C}_R$ such that ε_N is an isomorphism is a monoidal subcategory of $\mathcal{C}_R$ and is closed under taking direct sums, subquotients, small inductive limits, and duals of dualizable objects in $\mathcal{C}_R$.*

Proof. Using the previous lemma, this follows directly from Prop. 2.3.6(i), and the fact that ι_R is an additive exact tensor functor. □

2.4 Solution rings and Picard-Vessiot rings

sec:solution-rings

From now on we assume that $\mathcal{C}$ satisfies all conditions (C1), (C2), (F1) and (F2).

lemma:dualizables-are-projective-of-finite-rank

Lemma 2.4.1. *Let $M \in \mathcal{C}$ be dualizable. Then $v(M)$ is a finitely generated locally free $\mathcal{O}_{\mathcal{X}}$-module of constant rank.*

Proof. If $M \in \mathcal{C}$ is dualizable, then $\upsilon(M)$ is dualizable in $\mathsf{Qcoh}(\mathcal{X})$, since υ is a tensor functor, and tensor functors map dualizable objects to dualizable objects (and their duals to the duals of the images). By [Del90, Prop. 2.6], dualizable objects in $\mathsf{Qcoh}(\mathcal{X})$ are exactly the finitely generated locally free $\mathcal{O}_{\mathcal{X}}$-modules. Hence, $\upsilon(M)$ is finitely generated and locally free whenever M is dualizable.

To see that the rank is constant, let $d \in \mathbb{N}$ be the maximal local rank of $\upsilon(M)$, and consider the d-th exterior power $\Lambda := \Lambda^d(M) \in \mathcal{C}$ which is non-zero by the choice of d. Hence, the evaluation morphism $\mathrm{ev}_\Lambda : \Lambda \otimes \Lambda^\vee \to \mathbb{1}$ is non-zero. Since $\mathbb{1}$ is simple, and the image of ev_Λ is a subobject of $\mathbb{1}$, the morphism ev_Λ is indeed an epimorphism. Hence the evaluation

$$\mathrm{ev}_{\upsilon(\Lambda)} = \upsilon(\mathrm{ev}_\Lambda) : \upsilon(\Lambda) \otimes_{\mathcal{O}_{\mathcal{X}}} \upsilon(\Lambda)^\vee \to \mathcal{O}_{\mathcal{X}}$$

is surjective which implies that $\upsilon(\Lambda) \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X},x} \neq 0$ for any point x of $\mathcal{X}$. But this means that any local rank of $\upsilon(M)$ is at least d, i.e. $\upsilon(M)$ has constant rank d. □

rem:dualizables-are-projective

Remark 2.4.2. With respect to the previous lemma, condition (F2) implies that if $\upsilon(M)$ is finitely generated for some $M \in \mathcal{C}$, then $\upsilon(M)$ is even locally free and of constant rank. This also implies the following:
If M is dualizable, then $\upsilon(M)$ is finitely generated and locally free. Further, for every epimorphic image N of M, the $\mathcal{O}_{\mathcal{X}}$-module $\upsilon(N)$ is also finitely generated and hence, locally free. But then for any subobject $N' \subseteq M$ the sequence $0 \to \upsilon(N') \to \upsilon(M) \to \upsilon(M/N') \to 0$ is split exact, since $\upsilon(M/N')$ as an epimorphic image is locally free. Therefore $\upsilon(N')$ is also a quotient of $\upsilon(M)$, in particular $\upsilon(N')$ is finitely generated and locally free.
So given a dualizable $M \in \mathcal{C}$, all subquotients of finite direct sums of objects $M^{\otimes n} \otimes (M^\vee)^{\otimes m}$ $(n, m \in \mathbb{N})$ are dualizable. Hence, the strictly full tensor subcategory of $\mathcal{C}$ generated by M and $M^\vee$ – which is exactly the full subcategory of $\mathcal{C}$ consisting of all objects isomorphic to subquotients of finite direct sums of objects $M^{\otimes n} \otimes (M^\vee)^{\otimes m}$ $(n, m \in \mathbb{N})$ – is a rigid abelian tensor category and will be denoted by $\langle\langle M \rangle\rangle$. Furthermore by definition, υ is a fibre functor and therefore $\langle\langle M \rangle\rangle$ is even a Tannakian category (cf. [Del90, Section 2.8]).

By [Del90, Cor. 6.20], there exists a finite extension $\tilde{k}$ of k and a fibre functor $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_{\tilde{k}}$. In view of Thm. 2.5.5 in Section 2.5, this implies that there is a Picard-Vessiot ring for M over $\tilde{k}$.

We will see later (cf. Cor. 2.4.13) that for every simple minimal solution ring R, the field $R^{\mathcal{C}} = \mathrm{End}_{\mathcal{C}_R}(R)$ is a finite field extension of k.

Definition 2.4.3. Let $M \in \mathcal{C}$.
A *solution ring* for M is a $\mathcal{C}$-algebra R such that the morphism

$$\varepsilon_{M_R} : \iota_R \left((M_R)^{\mathcal{C}_R} \right) \to M_R = R \otimes M$$

is an isomorphism.

A *Picard-Vessiot ring* for M is a minimal solution ring R which is a simple $\mathcal{C}$-algebra, and satisfies $R^{\mathcal{C}} := \mathrm{End}_{\mathcal{C}_R}(R) = k$. Here, *minimal* means that for any solution ring $\tilde{R} \in \mathcal{C}$ that admits a monomorphism of $\mathcal{C}$-algebras to R, this monomorphism is indeed an isomorphism.

Remark 2.4.4. Comparing with the differential setting, $(M_R)^{\mathcal{C}_R}$ is just the so called solution space $(R \otimes_F M)^{\partial}$ of M over R, and ε_{M_R} is the canonical homomorphism $R \otimes_{R^{\partial}} (R \otimes_F M)^{\partial} \to R \otimes_F M$.
When R is a simple $\mathcal{C}$-algebra (i.e. in the differential setting a simple differential ring), then by Prop.2.3.6(iii), ε_{M_R} is always a monomorphism. Hence, for a simple $\mathcal{C}$-algebra R, the condition for being a solution ring means that the solution space is as large as possible, or in other words that $R \otimes M$ has a basis of constant elements, i.e. is a trivial differential module over R.

prop:image-of-solution-rings

Proposition 2.4.5. *Let R be a solution ring for some dualizable $M \in \mathcal{C}$, and let $f : R \to R'$ be an epimorphism of $\mathcal{C}$-algebras. Assume either that R' is a simple $\mathcal{C}$-algebra or that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$-module. Then R' is a solution ring for M as well.*

Remark 2.4.6. If $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$-module, then it is automatically free of finite rank, and the rank is the same as the global rank of $v(M)$ as $\mathcal{O}_{\mathcal{X}}$-module which exists by Lem. 2.4.1.

Proof of Prop. 2.4.5. As $f : R \to R'$ is an epimorphism and M is dualizable, $f \otimes \mathrm{id}_M : R \otimes M \to R' \otimes M$ is an epimorphism, too. As the diagram

$$\begin{array}{ccc} \iota_R\left((R \otimes M)^{\mathcal{C}}\right) & \xrightarrow{\varepsilon_{M_R}} & M_R = R \otimes M \\ \downarrow & & \downarrow{\scriptstyle f \otimes \mathrm{id}_M} \\ \iota_{R'}\left((R' \otimes M)^{\mathcal{C}}\right) & \xrightarrow{\varepsilon_{M_{R'}}} & M_{R'} = R' \otimes M \end{array}$$

commutes and ε_{M_R} is an isomorphism by assumption on R, the morphism $\varepsilon_{M_{R'}}$ is an epimorphism.

If R' is simple, then by Prop. 2.3.6(iii) the morphism $\varepsilon_{M_{R'}}$ is a monomorphism, hence an isomorphism. Therefore, R' is a solution ring.

Assume now, that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$-module of rank n. Then $\iota_R(R \otimes M)^{\mathcal{C}} \cong \iota_R\left((R^{\mathcal{C}})^n\right) = R^n$. Composing with ε_{M_R} leads to an isomorphism $R^n \xrightarrow{\cong} R \otimes M$. We therefore obtain an isomorphism $\alpha : (R')^n \to R' \otimes M$ by tensoring with R'. Applying the natural transformation ε to this isomorphism, we get a commutative square

$$\begin{array}{ccc} R'^n = \iota_{R'}\left((R'^n)^{\mathcal{C}}\right) & \xrightarrow[\cong]{\iota_{R'}(\alpha^{\mathcal{C}})} & \iota_{R'}\left((R' \otimes M)^{\mathcal{C}}\right) \\ \cong\downarrow{\scriptstyle \varepsilon_{R'^n}} & & \downarrow{\scriptstyle \varepsilon_{M_{R'}}} \\ R'^n & \xrightarrow[\cong]{\alpha} & R' \otimes M, \end{array}$$

which shows that $\varepsilon_{M_{R'}}$ is an isomorphism, too. □

thm:exists-sol-ring

Theorem 2.4.7. *Let $M \in \mathcal{C}$ be dualizable. Then there exists a non-zero solution ring for M.*

Proof. We show the theorem by explicitly constructing a solution ring. This construction is motivated by the Tannakian point of view in [DM82] and by Section 3.4 in [And01].
Let $n := \operatorname{rank}(\upsilon(M))$ be the global rank of the $\mathcal{O}_\mathcal{X}$-module $\upsilon(M)$ which exists by Lemma 2.4.1. We then define U to be the residue ring of $\operatorname{Sym}\Big((M \otimes (\mathbb{1}^n)^\vee) \oplus (\mathbb{1}^n \otimes M^\vee)\Big)$ subject to the ideal generated by the image of the morphism

$$\begin{aligned}(-\mathrm{ev}, \mathrm{id}_M \otimes \delta_{\mathbb{1}^n} \otimes \mathrm{id}_{M^\vee}) : M \otimes M^\vee &\to \mathbb{1} \oplus (M \otimes (\mathbb{1}^n)^\vee \otimes \mathbb{1}^n \otimes M^\vee) \\ &\subset \operatorname{Sym}\Big((M \otimes (\mathbb{1}^n)^\vee) \oplus (\mathbb{1}^n \otimes M^\vee)\Big).\end{aligned}$$

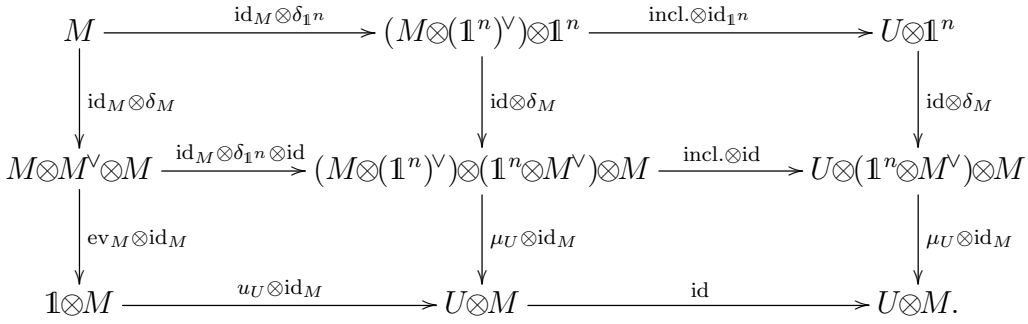
First we show that $U \neq 0$ by showing $\upsilon(U) \neq 0$. By exactness of υ, the ring $\upsilon(U)$ is given as the residue ring of $\operatorname{Sym}\left((\upsilon(M) \otimes_{\mathcal{O}_\mathcal{X}} (\mathcal{O}_\mathcal{X}^n)^\vee) \oplus (\mathcal{O}_\mathcal{X}^n \otimes_{\mathcal{O}_\mathcal{X}} \upsilon(M)^\vee)\right)$ subject to the ideal generated by the image of $(-\mathrm{ev}_{\upsilon(M)}, \mathrm{id} \otimes \delta_{\mathcal{O}_\mathcal{X}^n} \otimes \mathrm{id})$.

Let $\mathcal{U} = \operatorname{Spec}(S) \subseteq \mathcal{X}$ be an affine open subset such that $\tilde{M} := \upsilon(M)(\mathcal{U})$ is free over S. Let $\{b_1, \dots, b_n\}$ be a basis of $\tilde{M}$ and $b_1^\vee, \dots, b_n^\vee \in \tilde{M}^\vee$ the corresponding dual basis. Then $\upsilon(U)(\mathcal{U})$ is generated by $x_{ij} := b_i \otimes e_j^\vee \in \tilde{M} \otimes (S^n)^\vee$ and $y_{ji} := e_j \otimes b_i^\vee \in S^n \otimes (\tilde{M})^\vee$ for $i, j = 1, \dots, n$, where $\{e_1, \dots, e_n\}$ denotes the standard basis of S^n and $\{e_1^\vee, \dots, e_n^\vee\}$ the dual basis. The relations are generated by

$$b_k^\vee(b_i) = \mathrm{ev}_{\tilde{M}}(b_i \otimes b_k^\vee) = (\mathrm{id}_{\tilde{M}} \otimes \delta_{S^n} \otimes \mathrm{id}_{\tilde{M}^\vee})(b_i \otimes b_k^\vee) = \sum_{j=1}^n (b_i \otimes e_j^\vee) \otimes (e_j \otimes b_k^\vee),$$

i.e. $\delta_{ik} = \sum_{j=1}^n x_{ij} y_{jk}$ for all $i, k = 1, \dots, n$. This just means that the matrix $Y = (y_{jk})$ is the inverse of the matrix $X = (x_{ij})$. Hence $\upsilon(U)(\mathcal{U}) = S[X, X^{-1}]$ is the localisation of a polynomial ring over S in n^2 variables.

For showing that U is indeed a solution ring, we consider the following diagram



It is easy to see that the upper left, upper right and lower right squares all commute. The lower left square also commutes by definition of U, since the difference of the two compositions in question is just $(-\mathrm{ev}_M, \mathrm{id}_M \otimes \delta_{\mathbb{1}^n} \otimes \mathrm{id}_{M^\vee}) \otimes \mathrm{id}_M$. Furthermore the composition of the two vertical arrows on the left is just the identity on M by definition of the dual. Tensoring the big square with U leads to the left square of the next diagram

$$\begin{array}{ccccc} U \otimes M & \longrightarrow & U \otimes U \otimes \mathbb{1}^n & \xrightarrow{\mu_U \otimes \mathrm{id}_{\mathbb{1}^n}} & U \otimes \mathbb{1}^n \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}_U \otimes \alpha} & & \downarrow{\scriptstyle \alpha} \\ U \otimes M & \xrightarrow{\mathrm{id}_U \otimes u_U \otimes \mathrm{id}_M} & U \otimes U \otimes M & \xrightarrow{\mu_U \otimes \mathrm{id}_M} & U \otimes M \end{array}$$

where $\alpha := (\mu_U \otimes \mathrm{id}_M) \circ (\mathrm{id} \otimes \delta_M)$. The right square of this diagram also commutes, as is easily checked, and the composition in the bottom row is just the identity according to the constraints on the unit morphism u_U and the multiplication map μ_U. Hence, $\alpha : U \otimes \mathbb{1}^n \to U \otimes M$ is a split epimorphism in $\mathcal{C}$, and even in $\mathcal{C}_U$ (since the right square commutes). Since the rank of $\upsilon(U \otimes \mathbb{1}^n) = \upsilon(U)^n$ and the rank of $\upsilon(U \otimes M)$ as $\upsilon(U)$-modules are both n, the split epimorphism $\upsilon(\alpha)$ is in fact an isomorphism, i.e. α is an isomorphism.

Applying the natural transformation ε, we finally obtain the commutative square

$$\begin{array}{ccc} U^n = \iota_U\big((U \otimes \mathbb{1}^n)^{\mathcal{C}}\big) & \xrightarrow[\cong]{\iota_U(\alpha^{\mathcal{C}})} & \iota_U\big((U \otimes M)^{\mathcal{C}}\big) \\ \cong \downarrow{\scriptstyle \varepsilon_{U^n}} & & \downarrow{\scriptstyle \varepsilon_{M_U}} \\ U^n = U \otimes \mathbb{1}^n & \xrightarrow[\cong]{\alpha} & U \otimes M, \end{array}$$

which shows that ε_{M_U} is an isomorphism. Hence, U is a solution ring for M. □

rem:universal-solution-ring

Remark 2.4.8. In the case of difference or differential modules over a difference or differential field F, respectively, the ring U constructed in the previous proof is just the usual universal solution algebra $F[X, \det(X)^{-1}]$ for a fundamental solution matrix X having indeterminates as entries. We will therefore call U the **universal solution ring** for M.
This is moreover justified by the following theorem which states that U indeed satisfies a universal property.

thm:univ-sol-ring

Theorem 2.4.9. *Let R be a solution ring for M, such that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$-module, and let U be the solution ring for M constructed in Thm. 2.4.7. Then there exists a morphism of $\mathcal{C}$-algebras $f : U \to R$. Furthermore, the image of $\iota(R^{\mathcal{C}}) \otimes U \xrightarrow{\varepsilon_R \otimes f} R \otimes R \xrightarrow{\mu_R} R$ does not depend on the choice of f.*

Proof. By assumption, we have an isomorphism in $\mathcal{C}_R$:

$$\alpha : R^n \xrightarrow{\cong} \iota_R\left((M_R)^{\mathcal{C}_R}\right) = R \otimes_{\iota(R^{\mathcal{C}})} \iota\left((R \otimes M)^{\mathcal{C}}\right) \xrightarrow{\cong} R \otimes M.$$

Since M is dualizable, one has bijections

$$\begin{aligned}\mathrm{Mor}_{\mathcal{C}_R}(R^n, R\otimes M) \simeq \mathrm{Mor}_{\mathcal{C}_R}(R\otimes(\mathbb{1}^n\otimes M^\vee), R) &\simeq \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}^n\otimes M^\vee, R)\\ \alpha \mapsto \tilde{\alpha}_R := (\mathrm{id}_R\otimes \mathrm{ev}_M)\circ(\alpha\otimes \mathrm{id}_{M^\vee}) &\mapsto \tilde{\alpha} := \tilde{\alpha}_R|_{\mathbb{1}^n\otimes M^\vee}\end{aligned}$$

Similarly, for the inverse morphism $\beta := \alpha^{-1} : R\otimes M \to R^n$, one has

$$\begin{aligned}\mathrm{Mor}_{\mathcal{C}_R}(R\otimes M, R^n) \simeq \mathrm{Mor}_{\mathcal{C}_R}(R\otimes(M\otimes(\mathbb{1}^n)^\vee), R) &\simeq \mathrm{Mor}_{\mathcal{C}}(M\otimes(\mathbb{1}^n)^\vee, R)\\ \beta \mapsto \tilde{\beta}_R := (\mathrm{id}_R\otimes \mathrm{ev}_{\mathbb{1}^n})\circ(\beta\otimes \mathrm{id}_{(\mathbb{1}^n)^\vee}) &\mapsto \tilde{\beta} := \tilde{\beta}_R|_{M\otimes(\mathbb{1}^n)^\vee}\end{aligned}$$

Therefore the isomorphism α induces a morphism of $\mathcal{C}$-algebras

$$f : \mathrm{Sym}\Big((M\otimes(\mathbb{1}^n)^\vee)\oplus(\mathbb{1}^n\otimes M^\vee)\Big) \to R.$$

We check that this morphism factors through U, i.e. we have to check that the morphisms

$$M\otimes M^\vee \xrightarrow{\mathrm{id}\otimes\delta_{\mathbb{1}^n}\otimes\mathrm{id}} M\otimes(\mathbb{1}^n)^\vee\otimes\mathbb{1}^n\otimes M^\vee \xrightarrow{\tilde{\beta}\otimes\tilde{\alpha}} R\otimes R \xrightarrow{\mu_R} R$$

and

$$M\otimes M^\vee \xrightarrow{\mathrm{ev}_M} \mathbb{1} \xrightarrow{u_R} R$$

are equal. For this we consider the R-linear extensions in the category $\mathcal{C}_R$. By [Del90, Sect. 2.4], the composition

$$M_R^\vee \xrightarrow{\delta_{R^n}\otimes\mathrm{id}_{M_R^\vee}} (R^n)^\vee\otimes_R R^n\otimes_R M_R^\vee \xrightarrow{\mathrm{id}\otimes\alpha\otimes\mathrm{id}} M_R^\vee\otimes_R M_R\otimes_R (R^n)^\vee \xrightarrow{\mathrm{id}\otimes\mathrm{ev}_{M_R}} (R^n)^\vee$$

is just the transpose ${}^t\alpha : M_R^\vee \to (R^n)^\vee$ of the morphism α, and this equals the contragredient $\beta^\vee$ of $\beta = \alpha^{-1}$.
Hence the equality of the two morphisms reduces to the commutativity of the diagram

$$\begin{array}{ccc} M_R\otimes_R M_R^\vee & \xrightarrow{\beta\otimes\beta^\vee} & R^n\otimes_R (R^n)^\vee \\ & \searrow^{\mathrm{ev}_{M_R}} & \downarrow{\scriptstyle \mathrm{ev}_{R^n}} \\ & & R. \end{array}$$

But by definition of the contragredient (see [Del90, Sect. 2.4]), this diagram commutes.

It remains to show that the image of $\iota(R^{\mathcal{C}})\otimes U \xrightarrow{\varepsilon_R\otimes f} R\otimes R \xrightarrow{\mu_R} R$ does not depend on the chosen morphism $f : U \to R$.
Given two morphism of $\mathcal{C}$-algebras $f, g : U \to R$, let $\tilde{\alpha}_f, \tilde{\alpha}_g \in \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}^n\otimes M^\vee, R)$ be the restrictions of f resp. of g to $\mathbb{1}^n\otimes M^\vee \subseteq U$, and let $\tilde{\beta}_f, \tilde{\beta}_g \in \mathrm{Mor}_{\mathcal{C}}(M\otimes(\mathbb{1}^n)^\vee, R)$ be the restrictions of f resp. of g to $M\otimes(\mathbb{1}^n)^\vee \subseteq U$. Furthermore, let $\alpha_f, \alpha_g \in \mathrm{Mor}_{\mathcal{C}_R}(R^n, M_R)$ and $\beta_f, \beta_g \in \mathrm{Mor}_{\mathcal{C}_R}(M_R, R^n)$ denote the corresponding

isomorphisms. Then by similar considerations as above one obtains that β_f and β_g are the inverses of α_f and α_g, respectively. Then

$$\beta_g \circ \alpha_f \in \mathrm{Mor}_{\mathcal{C}_R}(R^n, R^n) \simeq \mathrm{Hom}_{R^{\mathcal{C}}}((R^{\mathcal{C}})^n, (R^n)^{\mathcal{C}}) \simeq \mathrm{Mor}_{\mathcal{C}_{\iota(R^{\mathcal{C}})}}(\iota(R^{\mathcal{C}})^n, \iota(R^{\mathcal{C}})^n)$$

is induced by an isomorphism on $\iota(R^{\mathcal{C}})^n$ (which we also denote by $\beta_g \circ \alpha_f$). Therefore for the $\iota(R^{\mathcal{C}})$-linear extension $\tilde{\alpha}_{f,\iota(R^{\mathcal{C}})}, \tilde{\alpha}_{g,\iota(R^{\mathcal{C}})} : \iota(R^{\mathcal{C}}) \otimes \mathbb{1}^n \otimes M^\vee \to R$, one has

$$\begin{aligned} \tilde{\alpha}_{f,\iota(R^{\mathcal{C}})} &= (\mathrm{id}_R \otimes \mathrm{ev}_M) \circ (\alpha_f|_{\iota(R^{\mathcal{C}})^n} \otimes \mathrm{id}_{M^\vee}) \\ &= (\mathrm{id}_R \otimes \mathrm{ev}_M) \circ (\alpha_g|_{\iota(R^{\mathcal{C}})^n} \otimes \mathrm{id}_{M^\vee}) \circ ((\beta_g \circ \alpha_f) \otimes \mathrm{id}_{M^\vee}) \\ &= \tilde{\alpha}_{g,\iota(R^{\mathcal{C}})} \circ ((\beta_g \circ \alpha_f) \otimes \mathrm{id}_{M^\vee}) \,. \end{aligned}$$

and similarly,

$$\tilde{\beta}_{f,\iota(R^{\mathcal{C}})} = \tilde{\beta}_{g,\iota(R^{\mathcal{C}})} \circ ((\alpha_g \circ \beta_f) \otimes \mathrm{id}_{M^\vee}) \,.$$

Hence, the morphism $\mu_R \circ (\varepsilon_R \otimes f) : \iota(R^{\mathcal{C}}) \otimes U \to R$ factors through $\mu_R \circ (\varepsilon_R \otimes g)$ and by changing the roles of f and g, the morphism $\mu_R \circ (\varepsilon_R \otimes g)$ factors through $\mu_R \circ (\varepsilon_R \otimes f)$. So the images are equal. □

Remark 2.4.10. In the classical settings, every Picard-Vessiot ring for some module M is a quotient of the universal solution ring U. This is also the case in this abstract setting (see Thm. 2.4.12 below). More generally, we will see that every simple minimal solution ring for M (i.e. without the assumption on the constants) is a quotient of U. Conversely, in Cor. 2.4.16 we show that every quotient of U by a maximal $\mathcal{C}$-ideal $\mathfrak{m}$ is a Picard-Vessiot ring if $(U/\mathfrak{m})^{\mathcal{C}} = k$.
Dropping the assumption $(U/\mathfrak{m})^{\mathcal{C}} = k$, however, one still has a simple solution ring $U/\mathfrak{m}$ (by Prop. 2.4.5), but $U/\mathfrak{m}$ may not be minimal. To see this, let $M = \mathbb{1}$. Then trivially $R := \mathbb{1}$ is a Picard-Vessiot ring for M, and the only one, since it is contained in any other $\mathcal{C}$-algebra.
The universal solution ring for $M = \mathbb{1}$, however, is given by $U \cong \mathbb{1} \otimes_k k[x, x^{-1}]$. Hence, for every maximal ideal I of $k[x, x^{-1}]$, $\mathfrak{m} := \iota(I)$ is a maximal $\mathcal{C}$-ideal of $U = \iota(k[x, x^{-1}])$ by Lemma 2.3.3. But $U/\mathfrak{m} \cong \iota(k[x, x^{-1}]/I)$ is only a minimal solution ring, if $k[x, x^{-1}]/I \cong k$, i.e. $U/\mathfrak{m} \cong \mathbb{1}$.

We continue with properties of quotients of U.
prop:properties-of-quotients-of-U

Proposition 2.4.11. *Let U be the universal solution ring for some dualizable $M \in \mathcal{C}$, and let R be a quotient algebra of U. Then $\upsilon(R)$ is a finitely generated faithfully flat $\mathcal{O}_{\mathcal{X}}$-algebra. If in addition R is a simple $\mathcal{C}$-algebra, then $R^{\mathcal{C}}$ is a finite field extension of k.*

Proof. Since R is a quotient of U, it is a quotient of $T := \mathrm{Sym}\Big((M \otimes (\mathbb{1}^n)^\vee) \oplus (\mathbb{1}^n \otimes M^\vee)\Big)$. Since $\upsilon(M)$ is finitely generated, $\upsilon(T)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$-algebra and therefore also $\upsilon(R)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$-algebra.

Since M is dualizable, $\langle\langle M \rangle\rangle$ is a Tannakian category (see Rem. 2.4.2), and T is an ind-object of $\langle\langle M \rangle\rangle$. Being a quotient of T, R also is an ind-object of $\langle\langle M \rangle\rangle$. Therefore by [Del90, Lemma 6.11], $\upsilon(R)$ is faithfully flat over $\mathcal{O}_\mathcal{X}$.

If in addition R is simple, $\ell := R^\mathcal{C}$ is a field. By exactness of ι and Prop. 2.2.5(iii), we have a monomorphism $\iota(\ell) \hookrightarrow R$, and hence by exactness of υ, an inclusion of $\mathcal{O}_\mathcal{X}$-algebras $\mathcal{O}_\mathcal{X} \otimes_k \ell = \upsilon(\iota(\ell)) \hookrightarrow \upsilon(R)$. After localising to some affine open subset of $\mathcal{X}$, we can apply Thm. 2.1.1, and obtain that ℓ is a finite extension of k. □

thm:simple-minimal-solution-rings-are-quotients

Theorem 2.4.12. *Let M be a dualizable object of $\mathcal{C}$, and let U be the universal solution ring for M. Then every simple minimal solution ring for M is isomorphic to a quotient of the universal solution algebra U. In particular, every Picard-Vessiot ring for M is isomorphic to a quotient of U.*

Proof. Let R be a simple minimal solution ring for M. Since R is simple, $R^\mathcal{C}$ is a field, and therefore $(R \otimes M)^\mathcal{C}$ is a free $R^\mathcal{C}$-module. Hence R fulfills the assumptions of Theorem 2.4.9, and there is a morphism of $\mathcal{C}$-algebras $f : U \to R$. As $(U \otimes M)^\mathcal{C}$ is a free $U^\mathcal{C}$-module, the image $f(U)$ is a solution ring by Prop. 2.4.5. As R is minimal, we obtain $f(U) = R$. Hence, R is the quotient of U by the kernel of f. □

cor:properties-of-simple-minimal-solution-rings

Corollary 2.4.13. *Let $R \in \mathcal{C}$ be a simple minimal solution ring for some dualizable $M \in \mathcal{C}$. Then $\upsilon(R)$ is a finitely generated faithfully flat $\mathcal{O}_\mathcal{X}$-algebra, and $R^\mathcal{C}$ is a finite field extension of k.*

Proof. This follows directly from Thm. 2.4.12 and Prop. 2.4.11. □

prop:unique-pv-inside-simple-sol-ring

Proposition 2.4.14. *Let M be a dualizable object of $\mathcal{C}$, and let R be a simple solution ring for M with $R^\mathcal{C} = k$. Then there is a unique Picard-Vessiot ring for M inside R. This is the image of the universal solution ring U under a morphism $f : U \to R$.*

Proof. As in the proof of Thm. 2.4.12, R fulfills the assumptions of Theorem 2.4.9, so there is a morphism of $\mathcal{C}$-algebras $f : U \to R$. By assumption on R, we have $\iota(R^\mathcal{C}) = \iota(k) = \mathbb{1}$, and hence $\varepsilon_R \otimes f = f : \mathbb{1} \otimes U = U \to R$. So by the second part of Theorem 2.4.9, the image $f(U)$ does not depend on the choice of f. In particular, $f(U)$ (which is a solution ring by Prop. 2.4.5) is the unique minimal solution ring inside R. It remains to show that $f(U)$ is a simple algebra.

Let $I \subseteq U$ be a maximal subobject in $\mathcal{C}_U$ (i.e. an ideal of U), let $R' := U/I$ and let $g : U \to R'$ be the canoncial epimorphism. Furthermore, let $\mathfrak{m} \in \mathcal{C}$ be a maximal ideal of $R' \otimes R$. Since R and R' are simple, the natural morphisms $R \to (R' \otimes R)/\mathfrak{m}$ and $R' \to (R' \otimes R)/\mathfrak{m}$ considered in $\mathcal{C}_R$ and $\mathcal{C}_{R'}$, respectively, are

monomorphisms, and it suffices to show that $\mathbb{1} \otimes f(U) \subseteq (R' \otimes R)/\mathfrak{m}$ is simple.

$$\begin{array}{ccc} U & \xrightarrow{\quad f \quad} & R \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle 1\otimes \mathrm{id}_R} \\ R' & \xrightarrow{\mathrm{id}_{R'}\otimes 1} & (R' \otimes R)/\mathfrak{m} \end{array}$$

$g(U) = R'$ is simple by construction, and so is $g(U) \otimes \mathbb{1} \subseteq (R' \otimes R)/\mathfrak{m}$. By Theorem 2.4.9, we have $\iota(l) \cdot (g(U) \otimes \mathbb{1}) = \iota(l) \cdot (1 \otimes f(U))$, where $l = ((R' \otimes R)/\mathfrak{m})^{\mathcal{C}}$, and l is a field, since $(R' \otimes R)/\mathfrak{m}$ is simple. By Corollary 2.3.4, applied to the category $\mathcal{C}_{R'}$, $\iota(l) \cdot (g(U) \otimes \mathbb{1})$ is also simple, i.e. $\iota(l) \cdot (\mathbb{1} \otimes f(U))$ is simple. Since, $\iota(l) \cdot (\mathbb{1} \otimes f(U)) \cong l \otimes_k f(U)$ is a faithfully flat extension of $f(U)$, this implies that $f(U)$ is also simple. □

Remark 2.4.15. The previous proposition ensures the existence of Picard-Vessiot rings in special cases. For example, in the differential setting over e.g. $F = \mathbb{C}(t)$, if x is a point which is non-singular for the differential equation, then one knows that the ring of holomorphic functions on a small disc around that point is a solution ring for the equation. Hence, there exists a Picard-Vessiot ring (even unique) for the corresponding differential module inside this ring of holomorphic functions.
Similarly, in the case of rigid analytically trivial pre-t-motives (which form a special case of the difference setting) the field of fractions of a given ring of restricted power series is a simple solution ring for all these modules (cf. [Pap08]).

cor:special-quotients-are-pv-rings

Corollary 2.4.16. *Let $M \in \mathcal{C}$ be dualizable, and let $\mathfrak{m}$ be a maximal $\mathcal{C}$-ideal of the universal solution ring U for M such that $(U/\mathfrak{m})^{\mathcal{C}} = k$. Then $U/\mathfrak{m}$ is a Picard-Vessiot ring for M.*

Proof. By Prop. 2.4.5, $U/\mathfrak{m}$ fulfills the conditions of R in the previous propostion. Hence, the image of the morphism $U \to U/\mathfrak{m}$ (which clearly is $U/\mathfrak{m}$) is a Picard-Vessiot ring. □

cor:pv-rings-isom-over-finite-ext

Corollary 2.4.17. *Let $M \in \mathcal{C}$ be dualizable, and let R and R' be two simple minimal solution rings for M. Then there exists a finite field extension ℓ of k containing $R^{\mathcal{C}}$ and $(R')^{\mathcal{C}}$ such that $R \otimes_{R^{\mathcal{C}}} \ell \cong R' \otimes_{(R')^{\mathcal{C}}} \ell$.*

Proof. As in the proof of the previous theorem, let $f : U \to R$ and $g : U \to R'$ be epimorphisms of $\mathcal{C}$-algebras whose existence is guaranteed by Thm. 2.4.12. Let $\mathfrak{m}$ be a maximal $\mathcal{C}$-ideal of $R' \otimes R$, and let $\ell := (R' \otimes R/\mathfrak{m})^{\mathcal{C}}$. Then R' and R embed into $R' \otimes R/\mathfrak{m}$ and hence $(R')^{\mathcal{C}}$ and $R^{\mathcal{C}}$ both embed into ℓ. Furthermore by Thm. 2.4.9, the subrings $\iota(\ell)(g(U) \otimes 1)$ and $\iota(\ell)(1 \otimes f(U))$ are equal. As ℓ contains both $R^{\mathcal{C}}$ and $(R')^{\mathcal{C}}$, one has $\iota(\ell)(g(U) \otimes 1) = \iota(\ell)(R' \otimes 1) \cong R' \otimes_{(R')^{\mathcal{C}}} \ell$ and $\iota(\ell)(1 \otimes f(U)) \cong R \otimes_{R^{\mathcal{C}}} \ell$. Hence, $R' \otimes_{(R')^{\mathcal{C}}} \ell \cong R \otimes_{R^{\mathcal{C}}} \ell$. As in the proof of Prop. 2.4.11, one shows that ℓ is indeed finite over k. □

thm:existence-of-pv-ring

Theorem 2.4.18. *Let $M \in \mathcal{C}$ be dualizable. Then there exists a Picard-Vessiot ring for M up to a finite field extension of k, i.e. there exists a finite field extension ℓ of k and a $\mathcal{C}_{\iota(\ell)}$-algebra R such that R is a PV-ring for $M_{\iota(\ell)} \in \mathcal{C}_{\iota(\ell)}$.*

Proof. Let U be the universal solution ring for M, and let $\mathfrak{m} \subset U$ be a maximal $\mathcal{C}$-ideal of U. Then $R := U/\mathfrak{m}$ is a simple solution ring for M by Prop. 2.4.5, and $\ell := R^{\mathcal{C}}$ is a finite field extension of k by Prop. 2.4.11.
Considering now $M_{\iota(\ell)} \in \mathcal{C}_{\iota(\ell)}$, and R as an algebra in $\mathcal{C}_{\iota(\ell)}$ via $\varepsilon_R : \iota(R^{\mathcal{C}}) = \iota(\ell) \to R$, we obtain that R is a simple solution ring for $M_{\iota(\ell)}$ with $R^{\mathcal{C}} = \ell$. Hence by Prop. 2.4.14, with k replaced by ℓ (and $\mathcal{C}$ by $\mathcal{C}_{\iota(\ell)}$ etc.), there is a unique Picard-Vessiot ring for $M_{\iota(\ell)}$ inside R. Indeed also by Prop. 2.4.14, this Picard-Vessiot ring is R itself, since the canonical morphism $\iota(\ell) \otimes U \to R$ is an epimorphism, and $\iota(\ell) \otimes U$ is easily seen to be the universal solution ring for $M_{\iota(\ell)}$. □

2.5 Picard-Vessiot rings and fibre functors

sec:pv-rings-and-fibre-functors

Throughout this section, we fix a dualizable object $M \in \mathcal{C}$. Recall that we denote by $\langle\langle M \rangle\rangle$ the strictly full tensor subcategory of $\mathcal{C}$ generated by M and $M^\vee$, i.e. the full subcategory of $\mathcal{C}$ containing all objects isomorphic to subquotients of direct sums of objects $M^{\otimes n} \otimes (M^\vee)^{\otimes m}$ for $n, m \geq 0$.

In this section we consider the correspondence between Picard-Vessiot rings R for M and fibre functors $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_k$. The main result is Thm. 2.5.5 which states that there is a bijection between their isomorphism classes. This generalises [And01, Thm. 3.4.2.3] to our abstract setting.

prop:fibre-functor-associated-to-pv-ring

Proposition 2.5.1. *Assume R is a Picard-Vessiot ring for M. Then the functor*

$$\omega_R : \langle\langle M \rangle\rangle \to \mathsf{vect}_k, N \mapsto (R \otimes N)^{\mathcal{C}}$$

is an exact faithful tensor-functor, i.e. a fibre functor.
We call the fibre functor ω_R the **fibre functor associated to** *R.*

Proof. By definition of a Picard-Vessiot ring, the morphism $\varepsilon_{M_R} : R \otimes_k (R \otimes M)^{\mathcal{C}} \to R \otimes M$ is an isomorphism. Hence, by Prop. 2.3.8, ε_{N_R} is an isomorphism for all $N \in \langle\langle M \rangle\rangle$.

Recall $R \otimes_k (R \otimes N)^{\mathcal{C}} = \iota_R((N_R)^{\mathcal{C}}) = \iota_R(\omega_R(N))$ for all N.

As $\upsilon(R)$ is faithfully flat over $\mathcal{O}_{\mathcal{X}} = \upsilon(\mathbb{1})$ by Cor. 2.4.13, the functor $N \mapsto R \otimes N$ is exact and faithful. Hence, given a short exact sequence $0 \to N' \to N \to N'' \to 0$ in $\langle\langle M \rangle\rangle$, the sequence

$$0 \to R \otimes N' \to R \otimes N \to R \otimes N'' \to 0$$

is exact, and $R \otimes N = 0$ if and only if $N = 0$. Using the isomorphisms ε_{N_R} etc. the sequence

$$0 \to R \otimes_k \omega_R(N') \to R \otimes_k \omega_R(N) \to R \otimes_k \omega_R(N'') \to 0$$

is exact. As ι_R is exact and faithful, this implies that

$$0 \to \omega_R(N') \to \omega_R(N) \to \omega_R(N'') \to 0$$

is exact. Furthermore, $\omega_R(N) = 0$ if and only if $R \otimes_k \omega_R(N) = 0$ if and only if $R \otimes N = 0$ if and only if $N = 0$.

It remains to show that ω_R is a tensor-functor which is already done by showing that $\varepsilon_{(N\otimes N')_R}$ is an isomorphism if ε_{N_R} and $\varepsilon_{N'_R}$ are. □

Given a fibre functor $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_k$, we want to obtain a Picard-Vessiot ring associated to ω.
Apparently, this Picard-Vessiot ring is already given in the proof of [DM82, Thm. 3.2], although the authors don't claim that it is a Picard-Vessiot ring. We will recall the construction to be able to prove the necessary facts:
For $N \in \langle\langle M \rangle\rangle$, one defines P_N to be the largest subobject of $N \otimes_k \omega(N)^\vee$ such that for all $n \geq 1$ and all subobjects $N' \subseteq N^n$, the morphism

$$P_N \to N \otimes_k \omega(N)^\vee \xrightarrow{\text{diag}} N^n \otimes_k \omega(N^n)^\vee \to N^n \otimes_k \omega(N')^\vee$$

factors through $N' \otimes_k \omega(N')^\vee$.
For monomorphisms $g : N' \to N$ and epimorphisms $g : N \to N'$, one obtains morphisms $\phi_g : P_N \to P_{N'}$, and therefore

$$R_\omega := \varinjlim_{N \in \langle\langle M \rangle\rangle} P_N^\vee \in \mathrm{Ind}(\langle\langle M \rangle\rangle) \subseteq \mathcal{C}$$

is welldefined. The multiplication $\mu_{R_\omega} : R_\omega \otimes R_\omega \to R_\omega$ is induced by the natural morphisms $P_{N\otimes L} \to P_N \otimes P_L$ via dualizing and taking inductive limits.

lem:R-omega-representing

Lemma 2.5.2. *The functor $\mathcal{C}-\mathsf{Alg} \to \mathsf{Sets}$ which associates to each $\mathcal{C}$-algebra R' the set of natural tensor-transformations from the functor $R' \otimes (\iota \circ \omega) : \langle\langle M \rangle\rangle \to \mathcal{C}_{R'}$ to the functor $R' \otimes \mathrm{id}_{\langle\langle M \rangle\rangle} : \langle\langle M \rangle\rangle \to \mathcal{C}_{R'}$ is represented by the $\mathcal{C}$-algebra R_ω, i.e. there is a natural bijection between the natural transformations $R' \otimes (\iota \circ \omega) \to R' \otimes \mathrm{id}_{\langle\langle M \rangle\rangle}$ of tensor functors and the morphisms of $\mathcal{C}$-algebras $R_\omega \to R'$.*

Proof. Let R' be a $\mathcal{C}$-algebra, and let α be a natural transformation not necessarily respecting the tensor structure. Then for every $N \in \langle\langle M \rangle\rangle$ one has a morphism

$$\begin{aligned} \alpha_N &\in \mathrm{Mor}_{\mathcal{C}_{R'}}(R' \otimes \iota(\omega(N)), R' \otimes N) \simeq \mathrm{Mor}_{\mathcal{C}}(\iota(\omega(N)), R' \otimes N) \\ &\simeq \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes N \otimes \iota(\omega(N))^\vee) = (R' \otimes N \otimes \iota(\omega(N))^\vee)^{\mathcal{C}} \end{aligned}$$

It is straight forward to check that such a collection of morphisms $(\alpha_N)_N$ where $\alpha_N \in \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes N \otimes \iota(\omega(N))^\vee)$ defines a natural transformation if and only if $\alpha_N \in \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes P_N)$ for all N, and $\alpha_{N'} = (\mathrm{id}_{R'} \otimes \phi_g) \circ \alpha_N$ whenever $\phi_g : P_N \to P_{N'}$ is defined.
On the other hand, one has

$$\begin{aligned} \mathrm{Mor}_{\mathcal{C}}(R_\omega, R') &= \mathrm{Mor}_{\mathcal{C}}(\varinjlim_{N \in \langle\langle M \rangle\rangle} P_N^\vee, R') \\ &= \varprojlim_{N \in \langle\langle M \rangle\rangle} \mathrm{Mor}_{\mathcal{C}}(P_N^\vee, R') \simeq \varprojlim_{N \in \langle\langle M \rangle\rangle} \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes P_N) \end{aligned}$$

Hence, giving such a compatible collection of morphisms α_N is equivalent to giving a $\mathcal{C}$-morphism $R_\omega \to R'$.
It is also not hard to check that the natural transformations that respect the tensor structure correspond to morphisms of $\mathcal{C}$-algebras $R \to R'$ under this identification. □

Before we show that R_ω is a simple solution ring for M, we need some more results from [DM82] resp. from [Del90]:
As ω has values in k-vector spaces, $\langle\langle M \rangle\rangle$ together with ω is a neutral Tannakian category (see [Del90]), and therefore equivalent to the category of representations of the algebraic group scheme $G = \underline{\mathrm{Aut}}^{\otimes}(\omega)$.
This also induces an equivalence of their ind-categories, and R_ω corresponds to the group ring $k[G]$ with the right regular representation (cf. proof of [DM82, Theorem 3.2]).

prop:pv-ring-associated-to-fibre-functor

Proposition 2.5.3. *The object $R_\omega \in \mathrm{Ind}(\langle\langle M \rangle\rangle) \subseteq \mathcal{C}$ associated to ω is a simple solution ring for M, and satisfies $(R_\omega)^{\mathcal{C}} = k$.*

rem:pv-ring-associated-to-fibre-functor

Remark 2.5.4. By Prop. 2.4.14, R_ω therefore contains a unique Picard-Vessiot ring for M. This Picard-Vessiot ring will be called the **PV-ring associated to** ω. Indeed, R_ω is already minimal and hence a Picard-Vessiot ring itself. This will be seen at the end of the proof of Thm. 2.5.5. There is also a way of directly showing that R_ω is isomorphic to a quotient of the universal solution ring for M which would also imply that R_ω is a PV-ring (cf. Cor. 2.4.16). But we don't need this here, so we will omit it.

Proof. As ω defines an equivalence of categories $\langle\langle M \rangle\rangle \to \mathrm{Rep}_k(G)$ (and also of their ind-categories), and $\omega(R_\omega) = k[G]$, one obtains

$$(R_\omega)^{\mathcal{C}} = \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, R_\omega) \simeq \mathrm{Hom}_G(k, k[G]) = k[G]^G = k.$$

For showing that R_ω is simple, let $I \neq R_\omega$ be an ideal of R_ω in $\mathcal{C}$. We even have $I \in \mathrm{Ind}(\langle\langle M \rangle\rangle)$, as it is a subobject of R_ω. By the equivalence of categories $\omega(I)$

belongs to $\mathrm{Ind}(\mathrm{Rep}_k(G))$, and $\omega(I)$ is an ideal of $\omega(R_\omega) = k[G]$. But $k[G]$ does not have non-trivial G-stable ideals. Hence, $\omega(I) = 0$, and therefore $I = 0$.

As seen in Lemma 2.5.2, $\mathrm{id}_{R_\omega} \in \mathrm{Mor}_{\mathcal{C}}(R_\omega, R_\omega)$ induces a natural transformation $\alpha : R_\omega \otimes (\iota \circ \omega) \to R_\omega \otimes \mathrm{id}_{\langle\langle M \rangle\rangle}$, in particular it induces a $\mathcal{C}_{R_\omega}$-morphism $\alpha_M : R_\omega \otimes \iota(\omega(M)) \to R_\omega \otimes M$. By [DM82, Prop. 1.13], such a natural transformation is an equivalence, as $\langle\langle M \rangle\rangle$ is rigid[4]. Therefore, the morphism α_M is an isomorphism. As $R_\omega \otimes \iota(\omega(M)) = \iota_{R_\omega}(\omega(M))$, Lemma 2.3.7 implies that ε_{M_R} is an isomorphism.
Hence, R_ω is a solution ring for M.

□

thm:pv-rings-equiv-to-fibre-functors

Theorem 2.5.5. *Let $M \in \mathcal{C}$ be dualizable, and let ℓ be a field extension of k. Then there is a bijection between isomorphism classes of Picard-Vessiot rings R for $M_{\iota(\ell)}$ over $\widetilde{\mathbb{1}} := \iota(\ell)$ and isomorphism classes of fibre functors ω from $\langle\langle M_{\iota(\ell)} \rangle\rangle$ into ℓ-vector spaces.*
This bijection is induced by $R \mapsto \omega_R$ and $\omega \mapsto$ (PV-ring inside R_ω) given in Prop. 2.5.1 and Rem. 2.5.4, respectively.

Proof. Clearly isomorphic Picard-Vessiot rings give rise to isomorphic fibre functors and isomorphic fibre functors give rise to isomorphic Picard-Vessiot rings. Hence, we only have to show that the maps are inverse to each other up to isomorphisms.
By working directly in the category $\mathcal{C}_{\iota(\ell)}$ we can assume that $\ell = k$.

On one hand, for given ω and corresponding PV-ring R, one has natural isomorphisms

$$\iota_R(\omega(N)) = R \otimes_k \omega(N) \to N_R$$

(see proof of Prop. 2.5.3). By adjunction these correspond to natural isomorphisms

$$\lambda_N : \omega(N) \cong (N_R)^{\mathcal{C}} = \omega_R(N),$$

i.e. the functors ω and ω_R are isomorphic.

Conversely, given a Picard-Vessiot ring R and associated fibre functor ω_R, let R_ω be the simple solution ring constructed above.
As $\iota_R = R \otimes \iota$ and $(N_R)^{\mathcal{C}_R} = \omega_R(N)$ for all $N \in \langle\langle M \rangle\rangle$, the natural isomorphisms $\varepsilon_{N_R} : \iota_R\left((N_R)^{\mathcal{C}_R}\right) \to N_R$ form a natural transformation $R \otimes (\iota \circ \omega_R) \to R \otimes \mathrm{id}_{\langle\langle M \rangle\rangle}$. By Lemma 2.5.2, this natural transformation corresponds to a morphism of $\mathcal{C}$-algebras $\varphi : R_\omega \to R$. As R_ω is a simple $\mathcal{C}$-algebra, φ is a monomorphism. But R is a minimal solution ring, and hence φ is even an isomorphism. Therefore, R_ω is isomorphic to R and already minimal, i.e. R_ω is a Picard-Vessiot ring itself. □

[4]Rigidity of the target category which is assumed in loc. cit. is not needed. See also [Bru94, Prop. 1.1].

2.6 Galois group schemes

sec:galois-groups

Given a dualizable object $M \in \mathcal{C}$ and a Picard-Vessiot ring R for M, one considers the group functor

$$\underline{\mathrm{Aut}}_{\mathcal{C}-\mathrm{alg}}(R) : \mathsf{Alg}_k \to \mathsf{Groups}$$

which associates to each k-algebra D the group of automorphisms of $R \otimes_k D$ as an algebra in $\mathcal{C}_{\iota(D)}$, i.e. the subset of $\mathrm{Mor}_{\mathcal{C}_{\iota(D)}}(R \otimes_k D, R \otimes_k D)$ consisting of all isomorphisms which are compatible with the algebra structure of $R \otimes_k D$.
This functor is called the **Galois group of** R over $\mathbb{1}$.

On the other hand, given a fibre functor $\omega : \langle\langle M \rangle\rangle \to \mathsf{vect}_k$, one considers the group functor

$$\underline{\mathrm{Aut}}^{\otimes}(\omega) : \mathsf{Alg}_k \to \mathsf{Groups}$$

which associates to each k-algebra D the group of natural automorphisms of the functor $D \otimes_k \omega : N \mapsto D \otimes_k \omega(N)$.
As $\langle\langle M \rangle\rangle$ together with the fibre functor ω is a neutral Tannakian category, this group functor is called the **Tannakian Galois group** of $(\langle\langle M \rangle\rangle, \omega)$. In [Del90] it is shown that this group functor is indeed an algebraic group scheme.

The aim of this section is to show that both group functors are isomorphic algebraic group schemes if $\omega = \omega_R$ is the fibre functor associated to R.

We start by recalling facts about group functors, (commutative) Hopf-algebras and affine group schemes. All of this can be found in [Wat79].

A group functor $\mathsf{Alg}_k \to \mathsf{Groups}$ is an affine group scheme over k if it is representable by a commutative algebra over k. This commutative algebra then has a structure of a Hopf-algebra. The group functor is even an algebraic group scheme (i.e. of finite type over k) if the corresponding Hopf-algebra is finitely generated. The category of commutative Hopf-algebras over k and the category of affine group schemes over k are equivalent. This equivalence is given by taking the spectrum of a Hopf-algebra in one direction and by taking the ring of regular functions in the other direction.
For a Hopf-algebra H over k, and corresponding affine group scheme $\mathcal{G} := \mathrm{Spec}(H)$, the category $\mathsf{Comod}(H)$ of right comodules of H and the category $\mathrm{Rep}(\mathcal{G})$ of representations of $\mathcal{G}$ are equivalent. This equivalence is given by attaching to a comodule V with comodule map $\rho : V \to V \otimes_k H$ the following representation $\varrho : \mathcal{G} \to \mathrm{End}(V)$ of $\mathcal{G}$: For any k-algebra D and $g \in \mathcal{G}(D) = \mathrm{Hom}_{k-\mathrm{alg}}(H, D)$, the endomorphism $\varrho(g)$ on $V \otimes_k D$ is the D-linear extension of

$$g \circ \rho : V \to V \otimes_k H \to V \otimes_k D.$$

On the other hand, for any representation $\varrho : \mathcal{G} \to \mathrm{End}(V)$, the universal element $\mathrm{id}_H \in \mathrm{Hom}_{k-\mathrm{alg}}(H, H) = \mathcal{G}(H)$ gives a H-linear homomorphism $\varrho(\mathrm{id}_H) : V \otimes_k H \to V \otimes_k H$, and its restriction to $V \otimes 1$ is the desired comodule map $\rho : V \to V \otimes_k H$.

For showing that the group functors $\underline{\mathrm{Aut}}_{\mathcal{C}-\mathrm{alg}}(R)$ and $\underline{\mathrm{Aut}}^{\otimes}(\omega_R)$ are isomorphic algebraic group schemes, we show that they are both represented by the k-vector space $H := (R \otimes R)^{\mathcal{C}} = \omega_R(R)$. The next lemma shows that H is a finitely generated (commutative) k-Hopf-algebra, and hence $\mathrm{Spec}(H)$ is an algebraic group scheme over k.

Remark 2.6.1. This fact is shown for differential modules over algebraically closed constants in [vdPS03, Thm. 2.33], and for t-motives in [Pap08, Sections 3.5-4.5].

`lemma:H-is-Hopf-algebra`

Lemma 2.6.2. *Let R be a PV-ring for M and $H := \omega_R(R) = (R \otimes R)^{\mathcal{C}}$.*

1. *The morphism $\varepsilon_{R_R} : R \otimes_k H \to R_R = R \otimes R$ is an isomorphism in $\mathcal{C}_R$ (with R-module structure on $R \otimes R$ given on the first factor).*

2. *H is a finitely generated commutative k-algebra where the structure maps $u_H : k \to H$ (unit), $\mu_H : H \otimes_k H \to H$ (multiplication) are given by*

$$u_H := \omega_R(u_R) \quad \textit{and} \quad \mu_H := \omega_R(\mu_R),$$

   respectively.

3. *The k-algebra H is even a Hopf-algebra where the structure maps $c_H : H \to k$ (counit), $\Delta : H \to H \otimes_k H$ (comultiplication) and $s : H \to H$ (antipode) are given as follows: Counit and antipode are given by*

$$c_H := (\mu_R)^{\mathcal{C}} \quad \textit{and} \quad s := (\tau)^{\mathcal{C}},$$

   respectively, where $\tau \in \mathrm{Mor}_{\mathcal{C}}(R \otimes R, R \otimes R)$ denotes the twist morphism. The comultiplication is given by

$$\Delta := \omega_R\big(\varepsilon_{R_R}^{-1} \circ (u_R \otimes \mathrm{id}_R)\big)$$ [5]

Remark 2.6.3. The definition of Δ might look strange. Compared to other definitions (e.g. in [Tak89, Sect. 2]), where Δ is the map on constants/invariants induced by the map $R \otimes R \to R \otimes R \otimes R, a \otimes b \mapsto a \otimes 1 \otimes b$, one might think that Δ should be defined as $(\mathrm{id}_R \otimes u_R \otimes \mathrm{id}_R)^{\mathcal{C}} = \omega_R(u_R \otimes \mathrm{id}_R)$. The reason for the difference is that in [Tak89] and others, one uses $(R \otimes R) \otimes_R (R \otimes R) \cong R \otimes R \otimes R$ with right-R-module structure on the left tensor factor $(R \otimes R)$ and left-R-module structure on the right tensor factor $(R \otimes R)$.
In our setting, however, we are always using left-R-modules. In particular, the natural isomorphism $\omega_R(R) \otimes_k \omega_R(R) \to \omega_R(R \otimes R)$ reads as

$$\mathrm{Mor}_{\mathcal{C}_R}(R, R \otimes R) \otimes_k \mathrm{Mor}_{\mathcal{C}_R}(R, R \otimes R) \to \mathrm{Mor}_{\mathcal{C}_R}(R, R \otimes R \otimes R)$$

[5] Hence, Δ is the image under ω_R of the morphism $R \xrightarrow{u_R \otimes \mathrm{id}_R} R \otimes R \xrightarrow{\varepsilon_{R_R}^{-1}} R \otimes_k H$

where the left hand side is isomorphic to $\mathrm{Mor}_{\mathcal{C}_R}(R, (R\otimes R)\otimes_R (R\otimes R))$. But here, this is the tensor product of left-R-modules.
The additional $\varepsilon_{R_R}^{-1}$ in the definition of Δ solves the problem. It is also implicitly present in the identification $H\otimes_k H \cong (R\otimes R\otimes R)^{\mathcal{C}}$ in [Tak89] (cf. proof of Lemma 2.4(b) loc. cit.).

Proof of Lemma 2.6.2. As R is an object of $\mathrm{Ind}(\langle\!\langle M\rangle\!\rangle)$, part (i) follows from Prop. 2.3.8. As ω_R is a tensor functor, it is clear that the structure of a commutative algebra of R induces a structure of a commutative algebra on $\omega_R(R) = H$ via the maps u_H and μ_H defined in the lemma. As in the proof of Prop. 2.4.11, one verifies that $H = \omega_R(R)$ is finitely generated as k-algebra.
Part (iii) is obtained by checking that the necessary diagrams commute. We only show that Δ is coassociative, i.e. that $(\Delta\otimes_k \mathrm{id}_H)\circ\Delta = (\mathrm{id}_H\otimes_k\Delta)\circ\Delta$, and leave the rest to the reader.

As $\Delta = \omega_R\big(\varepsilon_{R_R}^{-1}\circ(u_R\otimes\mathrm{id}_R)\big)$, $\Delta\otimes_k\mathrm{id}_H = \omega_R\big((\varepsilon_{R_R}^{-1}\otimes_k\mathrm{id}_H)\circ(u_R\otimes\mathrm{id}_R\otimes_k\mathrm{id}_H)\big)$ and $\mathrm{id}_H\otimes_k\Delta = \omega_R(\mathrm{id}_R\otimes_k\Delta)$, it suffices to show that the morphisms

$$(\varepsilon_{R_R}^{-1}\otimes_k\mathrm{id}_H)\circ(u_R\otimes\mathrm{id}_R\otimes_k\mathrm{id}_H)\circ\varepsilon_{R_R}^{-1}\circ(u_R\otimes\mathrm{id}_R) \quad\text{and}$$

$$(\mathrm{id}_R\otimes_k\Delta)\circ\varepsilon_{R_R}^{-1}\circ(u_R\otimes\mathrm{id}_R)$$

are equal. This is seen by showing that the following diagram commutes:

$$\begin{array}{ccccc}
R & \xrightarrow{u_R\otimes\mathrm{id}_R} & R\otimes R & \xrightarrow{\varepsilon_{R_R}^{-1}} & R\otimes_k H \\
\downarrow{\scriptstyle u_R\otimes\mathrm{id}_R} & & \downarrow{\scriptstyle u_R\otimes\mathrm{id}_{R\otimes R}} & & \downarrow{\scriptstyle u_R\otimes\mathrm{id}_{R\otimes_k H}} \\
R\otimes R & \xrightarrow{\mathrm{id}_R\otimes u_R\otimes\mathrm{id}_R} & R\otimes R\otimes R & \xrightarrow{\mathrm{id}_R\otimes\varepsilon_{R_R}^{-1}} & R\otimes R\otimes_k H \\
\downarrow{\scriptstyle \varepsilon_{R_R}^{-1}} & & & & \downarrow{\scriptstyle \varepsilon_{R_R}^{-1}\otimes_k\mathrm{id}_H} \\
R\otimes_k H & & \xrightarrow{\mathrm{id}_R\otimes_k\Delta=\iota_R(\Delta)} & & R\otimes_k H\otimes_k H
\end{array}$$

Obviously the upper squares commute. Let $\delta := \varepsilon_{R_R}^{-1}\circ(u_R\otimes\mathrm{id}_R)$. Then the middle horizontal morphism equals $\mathrm{id}_R\otimes\delta$ and the lower horizontal morphism is $\iota_R(\Delta) = \iota_R((\mathrm{id}_R\otimes\delta)^{\mathcal{C}_R})$. As ε is a natural transformation $\iota_R\circ()^{\mathcal{C}_R}\to\mathrm{id}_{\mathcal{C}_R}$, and as $\varepsilon_{R_R}^{-1}\otimes_k\mathrm{id}_H = \varepsilon^{-1}_{(R\otimes_k H)_R}$, also the lower square commutes.

□

thm:Aut-R-represented-by-H

Theorem 2.6.4. *Let R be a PV-ring for M. Then the group functor*

$$\underline{\mathrm{Aut}}_{\mathcal{C}-alg}(R) : \mathsf{Alg}_k \to \mathsf{Groups}$$

is represented by the Hopf-algebra $H = \omega_R(R) = (R\otimes R)^{\mathcal{C}}$. Furthermore $\mathrm{Spec}(\upsilon(R))$ *is a torsor of $\underline{\mathrm{Aut}}_{\mathcal{C}-alg}(R)$ over X.*

Proof. This is shown similar to [Mau10a, Prop.10.9] or [Dyc08]. One has to use that

$$\delta : R \xrightarrow{u_R \otimes \mathrm{id}_R} R \otimes R \xrightarrow{\varepsilon_{R_R}^{-1}} R \otimes_k H$$

defines a right coaction of H on R. The property of a right coaction, however, is given by the commutativity of the diagram in the proof of Lemma 2.6.2.

The torsor property is obtained by the isomorphism $\upsilon(\varepsilon_{R_R}^{-1}) : \upsilon(R) \otimes_{\mathcal{O}_\mathcal{X}} \upsilon(R) \to \upsilon(R) \otimes_k H$. □

thm:H-acting-on-omega_R

Theorem 2.6.5. *Let R be a PV-ring for M and $H = \omega_R(R)$.*

1. *For all $N \in \langle\langle M \rangle\rangle$, $\rho_N : \omega_R(N) \to H \otimes_k \omega_R(N)$ given by*

$$\rho_N := \omega_R\big(\varepsilon_{N_R}^{-1} \circ (u_R \otimes \mathrm{id}_N)\big)$$ [6]

   defines a left coaction of H on $\omega_R(N)$.

2. *The collection $\rho := (\rho_N)_{N \in \langle\langle M \rangle\rangle}$ is a natural transformation of tensor functors $\omega_R \mapsto H \otimes_k \omega_R$, where $H \otimes_k \omega_R$ is a functor $\langle\langle M \rangle\rangle \to \mathsf{Mod}_H$.*

Remark 2.6.6. By going to the inductive limit one also gets a map $\rho_R : \omega_R(R) \to H \otimes_k \omega_R(R)$. This map is nothing else then the comultiplication $\Delta : H \to H \otimes_k H$.

Proof of Thm. 2.6.5. Part (i) is proven in the same manner as the coassociativity of Δ. For proving the second part, recall that ε is a natural transformation. Hence, for every morphism $f : N \to N'$ the diagram

$$\begin{array}{ccccc} N & \xrightarrow{u_R \otimes \mathrm{id}_N} & R \otimes N & \xrightarrow{\varepsilon_{N_R}^{-1}} & R \otimes_k \omega_R(N) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_R \otimes f} & & \downarrow{\scriptstyle \iota_R((\mathrm{id}_R \otimes f)^\mathcal{C})} \\ N' & \xrightarrow{u_R \otimes \mathrm{id}_{N'}} & R \otimes N' & \xrightarrow{\varepsilon_{N'_R}^{-1}} & R \otimes_k \omega_R(N') \end{array}$$

commutes. As $\iota_R((\mathrm{id}_R \otimes f)^\mathcal{C}) = \mathrm{id}_R \otimes_k \omega_R(f)$, applying ω_R to the diagram gives the desired commutative diagram for ρ being a natural transformation. Compatibility with the tensor product is seen in a similar way. □

thm:Aut-omega_R-represented-by-H

Theorem 2.6.7. *Let R be a PV-ring for M and $H = \omega_R(R)$. Then the group functor*

$$\underline{\mathrm{Aut}}^\otimes(\omega_R) : \mathsf{Alg}_k \to \mathsf{Groups}$$

is represented by the Hopf-algebra H. [7]

[6] The map $\varepsilon_{N_R}^{-1} \circ (u_R \otimes \mathrm{id}_N)$ is a morphism in $\mathcal{C}$: $N \to R \otimes N \to R \otimes_k \omega_R(N)$

[7] As shown in the following proof, the representing Hopf-algebra naturally is the coopposite Hopf-algebra H^{cop} of H. However, the antipode s is an isomorphism of Hopf-algebras $s : H \to H^{\mathrm{cop}}$, hence $H^{\mathrm{cop}} \cong H$.

Proof. As $\rho := (\rho_N)_{N \in \langle\langle M \rangle\rangle}$ defines a left coaction of H on the functor ω_R by natural transformations, one obtains a right action of $\mathrm{Spec}(H)$ on ω_R. Composing with the antipode (i.e. taking inverse group elements), one therefore gets a homomorphism of group functors

$$\varphi : \mathrm{Spec}(H) \to \underline{\mathrm{Aut}}^{\otimes}(\omega_R).$$

Explicitly, for any k-algebra D and $h \in H(D) = \mathrm{Hom}_{k-\mathrm{alg}}(H, D)$, one defines $\varphi(h) \in \underline{\mathrm{Aut}}^{\otimes}(\omega_R)(D) = \mathrm{Aut}^{\otimes}(D \otimes_k \omega_R)$ as the natural transformation which for $N \in \langle\langle M \rangle\rangle$ is the D-linear extension of the composition

$$\omega_R(N) \xrightarrow{\rho_N} H \otimes_k \omega_R(N) \xrightarrow{s \otimes \mathrm{id}_{\omega_R(N)}} H \otimes_k \omega_R(N) \xrightarrow{h \otimes \mathrm{id}_{\omega_R(N)}} D \otimes_k \omega_R(N).$$

For showing that the homomorphism φ is indeed an isomorphism, we give the inverse map:
For any k-algebra D and $g \in \underline{\mathrm{Aut}}^{\otimes}(\omega_R)(D)$, one has the homomorphism $g_R \in \mathrm{End}_D(D \otimes_k \omega_R(R)) = \mathrm{End}_D(D \otimes_k H)$, and one defines $\psi(g) \in H(D)$ as the composition

$$H \xrightarrow{s} H \xrightarrow{u_D \otimes \mathrm{id}_H} D \otimes_k H \xrightarrow{g_R} D \otimes_k H \xrightarrow{\mathrm{id}_D \otimes c_H} D.$$

It is a straight forward calculation to check that $\psi(g)$ is indeed a homomorphism of k-algebras and that φ and ψ are inverse to each other. □

cor:auts-are-isomorphic

Corollary 2.6.8. *The affine group schemes* $\underline{\mathrm{Aut}}_{\mathcal{C}\text{-}\mathsf{Alg}}(R)$ *and* $\underline{\mathrm{Aut}}^{\otimes}(\omega_R)$ *are isomorphic.*

Proof. By Thm. 2.6.4 and Thm. 2.6.7 both functors are represented by the Hopf-algebra $H = \omega_R(R)$. □

2.7 Galois correspondence

sec:galois-correspondence

In this section we will establish a Galois correspondence between subalgebras of a PV-ring and closed subgroups of the corresponding Galois group. As in [Mau14], the Galois correspondence will only take into account subalgebras which are PV-rings themselves on the one hand, and normal subgroups on the other.

We start by recalling facts about sub-Hopf-algebras and closed subgroup schemes which can be found in [Wat79].

In the equivalence of affine group schemes and Hopf-algebras, closed subgroup schemes correspond to Hopf-ideals, and closed normal subgroup schemes correspond to so called normal Hopf-ideals. As there is a correspondence between closed normal subgroup schemes and factor group schemes of $\mathcal{G}$ by taking the

cokernel and the kernel, respectively, there is also a correspondence between normal Hopf-ideals and sub-Hopf-algebras ([Tak72, Thm. 4.3]). This correspondence is given by

$$I \mapsto H(I) := \mathrm{Ker}\left(H \xrightarrow{\Delta - \mathrm{id}_H \otimes u_H} H \otimes_k H \to H \otimes_k (H/I)\right),$$

for a normal Hopf-ideal I, and by

$$H' \mapsto (H')^+ H,$$

for a sub-Hopf-algebra H', where $(H')^+$ is defined to be the kernel of the counit $c_{H'} : H' \to k$.

Furthermore, for a sub-Hopf-algebra $H' \subseteq H$, the category $\mathsf{Comod}(H')$ embeds into $\mathsf{Comod}(H)$ as a full subcategory.

thm:galois-correspondence-cat

Theorem 2.7.1. *Let $M \in \mathcal{C}$ be dualizable, R a PV-ring for M (assuming it exists), $\omega = \omega_R$ the corresponding fibre functor, $H = \omega_R(R)$, and $\mathcal{G} = \mathrm{Spec}(H) = \underline{\mathrm{Aut}}_{\mathcal{C}\text{-}\mathsf{Alg}}(R) = \underline{\mathrm{Aut}}^{\otimes}(\omega)$ the corresponding Galois group. Then there is a bijection between*

$$\mathfrak{T} := \{T \in \mathcal{C}\text{-}\mathsf{Alg} \mid T \subseteq R \text{ is PV-ring for some } N \in \langle\langle M \rangle\rangle\}$$

and

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

given by $\Psi : \mathfrak{T} \to \mathfrak{N}, T \mapsto \underline{\mathrm{Aut}}_{\mathcal{C}_T\text{-}\mathsf{Alg}}(R)$ resp. $\Phi : \mathfrak{N} \to \mathfrak{T}, \mathcal{N} \mapsto R^{\mathcal{N}}$.

Here, the ring of invariants $R^{\mathcal{N}}$ is the largest subobject T of R such that for all k-algebras D and all $\sigma \in \mathcal{N}(D) \subset \mathrm{Aut}_{\mathcal{C}_{\iota(D)}}(R \otimes_k D)$, one has $\sigma|_{T \otimes_k D} = \mathrm{id}_{T \otimes_k D}$. Equivalently, $R^{\mathcal{N}}$ is the equalizer of the morphisms $\mathrm{id}_R \otimes u_{k[\mathcal{N}]} : R \to R \otimes_k k[\mathcal{N}]$ [8] and $R \xrightarrow{\delta} R \otimes_k H \twoheadrightarrow R \otimes_k k[\mathcal{N}]$, where $\delta = \varepsilon_{R_R}^{-1} \circ (u_R \otimes \mathrm{id}_R)$ is the comodule map of R as H-comodule, and $H \twoheadrightarrow k[\mathcal{N}]$ is the canonical epimorphism.

Proof of Thm. 2.7.1. The functor ω_R is an equivalence of categories

$$\omega_R : \langle\langle M \rangle\rangle \to \mathsf{comod}(H),$$

and also of their ind-categories.[9] Hence, it provides a bijection between subalgebras of R in $\mathcal{C}$ and subalgebras of H stable under the left comodule structure. We will show that under this bijection sub-PV-rings correspond to sub-Hopf-algebras and that this bijection can also be described as given in the theorem.

[8] $k[\mathcal{N}] := \mathcal{O}_{\mathcal{N}}(\mathcal{N})$ denotes the ring of regular functions on the affine scheme $\mathcal{N}$.

[9] Here, $\mathsf{comod}(H)$ denotes the category of left-H-comodules which are finite-dimensional as k-vector spaces.

First, let $T \subseteq R$ be a PV-ring for some $N \in \langle\langle M \rangle\rangle$. Then $\langle\langle N \rangle\rangle$ is a full subcategory of $\langle\langle M \rangle\rangle$, and the fibre functor $\omega_T : \langle\langle N \rangle\rangle \to \mathsf{vect}_k$ corresponding to T is nothing else than the restriction of ω_R to the subcategory $\langle\langle N \rangle\rangle$, as T is a subobject of R. Hence, $H' := \omega_R(T) = \omega_T(T)$ is a sub-Hopf-algebra of H. Therefore, we obtain a closed normal subgroup scheme of $\mathcal{G} = \mathrm{Spec}(H)$ as the kernel of $\mathrm{Spec}(H) \twoheadrightarrow \mathrm{Spec}(H')$. As $\mathrm{Spec}(H) = \underline{\mathrm{Aut}}_{\mathcal{C}\text{-}\mathsf{Alg}}(R)$ and $\mathrm{Spec}(H') = \underline{\mathrm{Aut}}_{\mathcal{C}\text{-}\mathsf{Alg}}(T)$, this kernel is exactly $\underline{\mathrm{Aut}}_{\mathcal{C}_T\text{-}\mathsf{Alg}}(R)$.

On the other hand, let $\mathcal{N}$ be a closed normal subgroup scheme of $\mathcal{G} = \mathrm{Spec}(H)$ defined by a normal Hopf-ideal I of H, and

$$H' = \mathrm{Ker}\left(H \xrightarrow{\Delta - \mathrm{id}_H \otimes u_H} H \otimes_k H \twoheadrightarrow H \otimes_k (H/I)\right)$$

the corresponding sub-Hopf-algebra of H.
The subcategory $\mathsf{comod}(H')$ is generated by one object V (as every category of finite comodules is), and the object $N \in \langle\langle M \rangle\rangle$ corresponding to V via ω_R, has a PV-ring T inside R by Thm. 2.4.18, since R is a simple solution ring for N with $R^{\mathcal{C}} = k$. Furthermore, since T is the PV-ring corresponding to the fibre functor $\omega_R : \langle\langle N \rangle\rangle \to \mathsf{comod}(H')$, we have $\omega_R(T) = H'$.

It remains to show that $T = R^{\mathcal{N}}$, i.e. that

$$T = \mathrm{Ker}\left(R \xrightarrow{\delta - \mathrm{id}_R \otimes_k u_H} R \otimes_k H \twoheadrightarrow R \otimes_k k[\mathcal{N}] = R \otimes_k (H/I)\right).$$

As ω_R is an equivalence of categories, this is equivalent to

$$\omega_R(T) = \mathrm{Ker}\left(\omega_R(R) \xrightarrow{\omega_R(\delta) - \omega_R(\mathrm{id}_R) \otimes_k u_H} \omega_R(R) \otimes_k H \twoheadrightarrow \omega_R(R) \otimes_k (H/I)\right).$$

But, as $\omega_R(T) = H'$, $\omega_R(R) = H$ and $\omega_R(\delta) = \Delta$, this is just the definition of H'. $\square$

Chapter 3

Picard-Vessiot theory over simple iterative differential rings

chap:id-simple-rings

Like fields are simple rings having only (0) and (1) as ideals, the Picard-Vessiot ring is a differentially simple ring, i.e. a differential ring having only (0) and (1) as differential ideals. Having in mind that the classical Galois theory is a theory of extensions of fields, i.e. of simple rings, it is quite natural to ask whether one can also set up a Picard-Vessiot theory where the base is not a differential field, but more general a differentially simple ring. Giving a positive answer to this question, i.e. setting up such a differential Galois theory is the task of this chapter.

We follow here [Mau14], but have adapted it to make use of the categorical setting. A major change to [Mau14] is the notion of a solution ring. The one used here is compatible with the notion of a solution ring in the categorical setting, whereas a *solution ring* in [Mau14] is a *simple solution ring having the same constants*, here.

3.1 Basic notation

sec:notation

We review the basic notation of iterative differential rings.

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

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

for all $k \geq 0$.

A homomorphism of ID-rings $f : S \to R$ is a ring homomorphism $f : S \to R$ s.t. $\theta_R^{(n)} \circ f = f \circ \theta_S^{(n)}$ for all $n \geq 0$. If $\tilde{R}$ is an ID-ring extension of R. Then an element $r \in \tilde{R}$ is called **ID-finite** over R if the R-submodule of $\tilde{R}$ generated by $\{\theta^{(k)}(r) \mid k \geq 0\}$ is finitely generated.

For an ID-ring (R, θ), an **iterative derivation** on an R-module M is an additive map $\theta_M : M \to M[[T]]$ such that $\theta_M(rm) = \theta(r)\theta_M(m)$, $\theta_M^{(0)} = \mathrm{id}_M$ and $\theta_M^{(i)} \circ \theta_M^{(j)} = \binom{i+j}{i}\theta_M^{(i+j)}$ for all $i, j \geq 0$. We will refer to such a pair (M, θ_M) as a **module with iterative derivation**.

An **ID-module** (M, θ_M) over R is a module with iterative derivation which is finitely generated as an R-module.

A subset $N \subseteq M$ of an ID-module (M, θ_M) is called **ID-stable**, if $\theta^{(n)}(N) \subseteq N$ for all $n \geq 0$. An **ID-submodule** of (M, θ_M) is an ID-stable R-submodule N of

M which is finitely generated as R-module.[1] For an ID-module (M, θ_M) and an ID-stable R-submodule $N \subseteq M$, the factor module M/N is again an ID-module with the induced iterative derivation.

The free R-module R^n is an example of an ID-module over R with iterative derivation given componentwise. An ID-module (M, θ_M) over R is called **trivial** if $M \cong R^n$ as ID-modules, i.e. if M has a basis of constant elements.

For modules with iterative derivation (M, θ_M), (N, θ_N), the **direct sum** $M \oplus N$ is a module with iterative derivation where the iterative derivation given componentwise, and the **tensor product** $M \otimes_R N$ is a module with iterative derivation $\theta_\otimes$ given by $\theta_\otimes^{(k)}(m \otimes n) := \sum_{i+j=k} \theta_M^{(i)}(m) \otimes \theta_N^{(j)}(n)$ for all $k \geq 0$.

For modules with iterative derivation (M, θ_M), (N, θ_N), a **morphism** $f : (M, \theta_M) \to (N, \theta_N)$ is a homomorphism $f : M \to N$ of the underlying modules such that $\theta_N^{(k)} \circ f = f \circ \theta_M^{(k)}$ for all $k \geq 0$. For a morphism $f : (M, \theta_M) \to (N, \theta_N)$, the kernel $\mathrm{Ker}(f)$ and the image $\mathrm{Im}(f)$ are ID-stable R-submodules of M resp. N.

ex:ID-rings

Example 3.1.1. 1. For any field C and $R := C[t]$, the homomorphism of C-algebras $\theta_t : R \to R[[T]]$ given by $\theta_t(t) := t + T$ is an iterative derivation on R with field of constants C. This iterative derivation will be called the **iterative derivation with respect to** t. R is indeed an ID-simple ring, since for any polynomial $0 \neq f \in R$ of degree n, $\theta^{(n)}(f)$ equals the leading coefficient of f, and hence is invertible in $R = C[t]$.

item:der by t

2. For any field C, $C[[t]]$ also is an ID-ring with the iterative derivation with respect to t, given by $\theta_t(f(t)) := f(t + T)$ for $f \in C[[t]]$. The constants of $(C[[t]], \theta_t)$ are C, and $(C[[t]], \theta_t)$ also is ID-simple, since for $f = \sum_{i=n}^{\infty} a_i t^i \in C[[t]]$ with $a_n \neq 0$, one has

$$\theta_t^{(n)}(f) = \sum_{i=n}^{\infty} a_i \binom{i}{n} t^{i-n} \in C[[t]]^\times.$$

Hence, every non-zero ID-ideal contains a unit. This ID-ring will play an important role, since every ID-simple ring can be ID-embedded into $C[[t]]$ for an appropriate field C (comp. Thm. 3.2.4).

3. For any ring R, there is the **trivial** iterative derivation on R given by $\theta_0 : R \to R[[T]], r \mapsto r \cdot T^0$. Obviously, the ring of constants of (R, θ_0) is R itself.

4. Given a differential ring (R, ∂) containing the rationals (i.e. a $\mathbb{Q}$-algebra R with a derivation ∂), then $\theta^{(n)} := \frac{1}{n!}\partial^n$ defines an iterative derivation on R. On the other hand, for an iterative derivation θ, the map $\theta^{(1)}$ always

[1] Since R may not be Noetherian, R-submodules of finitely generated modules may not be finitely generated.

is a derivation. Hence, differential rings containing $\mathbb{Q}$ are special cases of ID-rings.
Since for a differentially simple ring in characteristic zero, its ring of constants always is a field (same proof as for ID-simple rings), we see that the Picard-Vessiot theory for ID-simple rings, we provide here, contains a Picard-Vessiot theory for differentially simple rings in characteristic zero as a special case.

rem:id-finiteness-questions

Remark 3.1.2. We will not assume our rings to be Noetherian. Hence, for an ID-module over an ID-ring R, there might exist R-submodules which are stable under the iterative derivation, but are not finitely generated as R-module, and therefore are not ID-modules in our definition. In particular, the kernel of a morphism of ID-modules is not an ID-module in general.
Another problem that might occur is concerned with ID-finiteness of elements. In general, the set of ID-finite elements in a ring extension $\tilde{R}$ does not have any extra structure (sums and products of ID-finite elements may be not ID-finite). Furthermore, there might be elements $r \in R$ which are not ID-finite over R, since the ideal generated by all $\theta^{(k)}(r)$ $(k \geq 0)$ does not need to be finitely generated.

For ID-simple rings, however, both points will work out fine as we will see in Cor. 3.3.5, resp. in Prop. 3.2.2, and Cor. 3.3.6.

prop:constants-of-triv-ext

Proposition 3.1.3. *Let (R, θ) be an ID-ring with constants C and let D/C be a ring extension such that D is free as C-module, and let D be equipped with the trivial iterative derivation $\theta_D(d) = d \in D[[T]]$ for all $d \in D$. Then the constants of $R \otimes_C D$ are exactly the elements $1 \otimes d$, $d \in D$.*

Proof. By definition all elements $1 \otimes d$ are constant. For proving that there are no others, let $(d_i)_{i \in I}$ be a basis of D as C-module, and consider an arbitrary constant element $\sum_{i \in I} r_i \otimes d_i \in R \otimes_C D$ (almost all r_i equal to 0). Then for all $k \geq 0$,

$$0 = \theta^{(k)}(\sum_{i \in I} r_i \otimes d_i) = \sum_{i \in I} \theta^{(k)}(r_i) \otimes d_i.$$

Therefore, all r_i are constant, i.e. $r_i \in C$.
Hence, $\sum_{i \in I} r_i \otimes d_i = 1 \otimes (\sum_{i \in I} r_i d_i)$. □

3.2 Properties of ID-simple rings

We first summarize some properties of ID-simple rings:

prop:first-properties-ID

Proposition 3.2.1. *Let (S, θ) be an ID-simple ring. Then*

1. *S is an integral domain.*

2. *The field of fractions of S has the same constants as S.*

3. *The ring of constants of S is a field.*

Proof. i) and ii) are proved in [MvdP03, Lemma 3.2]. However, ii) also follows as a special case of Prop. 3.2.2, since constants are ID-finite elements. Part iii) follows from ii), since the inverses of constants are constants, and hence the ring of constants of an ID-field is indeed a field.

□

prop:ID-finite

Proposition 3.2.2. *Let (S, θ) be an ID-simple ring. Then an element $x \in \mathrm{Quot}(S)$ is ID-finite over S if and only if $x \in S$.*

Proof. If $x \in S$, then $I := \langle \theta^{(n)}(x) \mid n \in \mathbb{N} \rangle_S$ is an ID-ideal of S, hence $I = \{0\}$ or $I = S = \langle 1 \rangle_S$. In both cases I is finitely generated, and hence x is ID-finite.

Now assume $x \in \mathrm{Quot}(S)$ is ID-finite over S, so by definition the S-module $M := \langle \theta^{(n)}(x) \mid n \in \mathbb{N} \rangle_S \subseteq \mathrm{Quot}(S)$ is finitely generated. M is also stable under the iterative derivation, as is easily verified by calculation. The ideal $I := \{s \in S \mid sm \in S \ \forall m \in M\}$ is non-zero, since it contains the product of the denominators of generators of M.
We will show that I is an ID-ideal. From this the claim follows, since by ID-simplicity of S, this will imply $I = S$, and hence $1 \cdot x \in S$.
For all $s, m \in \mathrm{Quot}(S)$, $n \in \mathbb{N}$ the equation

$$\theta^{(n)}(s \cdot m) = \sum_{i+j=n} \theta^{(i)}(s)\theta^{(j)}(m) = \theta^{(n)}(s) \cdot m + \sum_{i=0}^{n-1} \theta^{(i)}(s)\theta^{(n-i)}(m)$$

holds. In particular, for all $s \in I$, $m \in M$ we inductively obtain for all $n \in \mathbb{N}$:

$$\theta^{(n)}(s) \cdot m = \theta^{(n)}(\underbrace{s \cdot m}_{\in S}) - \sum_{i=0}^{n-1} \underbrace{\theta^{(i)}(s)}_{\in I \text{ by ind.hyp.}} \underbrace{\theta^{(n-i)}(m)}_{\in M} \in S,$$

and hence, $\theta^{(n)}(s) \in I$. Therefore, I is an ID-ideal. □

prop:ideal-bijection

Proposition 3.2.3. *Let (S, θ) be an ID-simple ring with field of constants $C = C_S$, let D be a finitely generated C-algebra equipped with the trivial iterative derivation. Then there is a bijection*

$$\begin{array}{rcl} \mathcal{I}(D) & \longleftrightarrow & \mathcal{I}^{\mathrm{ID}}(S \otimes_C D) \\ I & \longmapsto & S \otimes_C I \\ J \cap (1 \otimes_C D) & \longmapsfrom & J \end{array}$$

between the ideals of D and the ID-ideals of $S \otimes_C D$.

Proof. cf. [Mau10a, Lemma 10.7]. □

thm:embedding

Theorem 3.2.4. *Let (S, θ) be an ID-simple ring, $\mathfrak{m} \trianglelefteq S$ a maximal ideal, and $C = S/\mathfrak{m}$ the residue field. Then (S, θ) can be embedded into $(C[[t]], \theta_t)$ as ID-ring.*

Proof. The iterative derivation θ induces an injective ring homomorphism $\tilde{\theta} : S \to S[[t]], x \mapsto \sum_{n=0}^{\infty} \theta^{(n)}(x)t^n$, and it is easy to check, that $\tilde{\theta}$ is indeed an ID-homomorphism $(S, \theta) \to (S[[t]], \theta_t)$ where θ_t denotes the iterative derivation with respect to t (comp. Example 3.1.12). Since $\mathfrak{m}[[t]]$ is an ID-ideal of $S[[t]]$ and S is ID-simple, also $\bar{\theta} : S \to (S/\mathfrak{m})[[t]] = C[[t]]$ is injective which is the desired ID-embedding. □

3.3 The category of modules with iterative derivation

From now on, let (S, θ) denote an ID-simple ring.

We will consider the category $\mathcal{C}$ whose objects are pairs (N, θ_N) where N is an S-module and θ_N is an iterative derivation on N, and whose morphisms are morphisms of modules with iterative derivations.

It is easy to verify that the category $\mathcal{C}$ verifies (C1) and (C2) given in Section 2.2, with the tensor structure given in 3.1, and unit object $\mathbb{1} = (S, \theta)$. This can also be seen by recognizing that an S-module with iterative derivation is nothing else than a module over the non-commutative ring $S[\theta^{(n)} | n \in \mathbb{N}]$ with $\theta^{(i)} \cdot \theta^{(j)} = \binom{i+j}{i} \theta^{(i+j)}$ and

$$\theta^{(n)} \cdot s = \sum_{i=0}^{n} \theta^{(i)}(s) \cdot \theta^{(j)}$$

for all $n \in \mathbb{N}$ and $s \in S$ (cf. [MvdP03]).

There is an obvious additive tensor functor $v : \mathcal{C} \to \mathsf{Mod}(S)$ from $\mathcal{C}$ to the category of S-modules which is faithful, exact and preserves small inductive limits, namely the one which "forgets" the iterative derivation. Hence, the category $\mathcal{C}$ also satisfies (F1).

In the following, we will show that also (F2) is satisfied.

Remark 3.3.1. For a finitely generated S-module M, the following conditions are equivalent (see [Bou98, Section II.5.2, Theorem 1]):

1. M is projective.
2. M is finitely presented and locally free in the weaker sense, i.e. for every prime ideal $P \trianglelefteq S$ the localisation $M_P = S_P \otimes_S M$ is a free S_P-module.

3. M is locally free in the stronger sense: there exist $x_1, \ldots, x_r \in S$, generating the unit ideal, such that for each i, $M[\frac{1}{x_i}]$ is a free $S[\frac{1}{x_i}]$-module.

Furthermore, Cartier showed in [Car58, Appendice, Lemme 5], that the condition "finitely presented" in ii) is superfluous if S is an integral domain.

Since, ID-simple rings are integral domains by Proposition 3.2.1, in our situation the conditions *projective*, *locally free in the weaker sense* and *locally free in the stronger sense* are equivalent for finitely generated modules.

lem:M-free

Lemma 3.3.2. *Assume that S is a local ring with maximal ideal $\mathfrak{m}$ and let (M, θ_M) be an ID-module over (S, θ). Then M is a free S-module.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a minimal set of generators of M, and assume that this set is S-linearly dependent, i.e. there are $r_i \in S$ (not all of them equal to 0) such that $r_1x_1 + \cdots + r_nx_n = 0$. Since S is ID-simple, for each r_i there is some $k_i \in \mathbb{N}_0$ such that $\theta^{(k_i)}(r_i) \notin \mathfrak{m}$, i.e. $\theta^{(k_i)}(r_i) \in S^\times$. Take $k \in \mathbb{N}_0$ maximal such that for all $j < k$ and all $i = 1, \ldots, n$: $\theta^{(j)}(r_i) \in \mathfrak{m}$. W.l.o.g. $\theta^{(k)}(r_1) \in S^\times$. Then one obtains:

$$\begin{aligned} 0 &= \theta_M^{(k)}(r_1x_1 + \cdots + r_nx_n) = \sum_{i=1}^{n} \left(\sum_{j=0}^{k} \theta^{(j)}(r_i)\theta_M^{(k-j)}(x_i) \right) \\ &\equiv \sum_{i=1}^{n} \theta^{(k)}(r_i)x_i \mod \mathfrak{m}M \end{aligned}$$

Since $\theta^{(k)}(r_1)$ is invertible, this implies $x_1 \in \langle x_2, \ldots, x_n\rangle + \mathfrak{m}M$, hence $\langle x_2, \ldots, x_n\rangle + \mathfrak{m}M = M$, and by Nakayama's lemma $\langle x_2, \ldots, x_n\rangle = M$ contradicting the assumption that $\{x_1, \ldots, x_n\}$ was minimal.

Hence, $\{x_1, \ldots, x_n\}$ is linearly independent, and therefore a basis of M. □

thm:M-projective

Theorem 3.3.3. *If (M, θ_M) is an ID-module over (S, θ), then M is a projective S-module.*

Proof. For every prime ideal $P \trianglelefteq S$ the localisation S_P is a local ring and an ID-simple ring, and $M_P = S_P \otimes_S M$ is an ID-module over S_P. By the previous lemma, M_P is free for all P, i.e. M is locally free in the weaker sense, hence projective. □

Now we are able to show the non-trivial part of (F2), namely that every finitely generated module with iterative derivation, i.e. every ID-module, has a dual in the category $\mathcal{C}$.

thm:dual-ID-module

Theorem 3.3.4. *The dual ID-module of an ID-module (M, θ_M) is defined to be $(M^\vee, \theta_{M^\vee})$ where $M^\vee = \mathrm{Hom}_S(M, S)$ is the dual module of M, and $\theta_{M^\vee}$ is given by*

$$\theta^{(n)}_{M^\vee}(f) = \sum_{j=0}^{n} (-1)^j \theta^{(n-j)} \circ f \circ \theta^{(j)}_M$$

for all $f \in M^\vee$ and $n \in \mathbb{N}_0$.

The evaluation homomorphism $\mathrm{ev}_M : M \otimes M^\vee \to S$ and the coevaluation homorphism $\delta_M : S \to M^\vee \otimes M$ of the projective S-module M are then morphisms of ID-modules.

Hence, $(M^\vee, \theta_{M^\vee})$ is a dual object of (M, θ_M) in the category $\mathcal{C}$.

Proof. This is the same computation as in [Mat01] for ID-modules over ID-fields. □

From Remark 2.4.2 in the categorical setup, we obtain that ID-stable S-submodules of ID-modules are again finitely generated which we state as a corollary here.

`cor:submodule-is-fin-gen`

Corollary 3.3.5. *Let (M, θ_M) be an ID-module over (S, θ). Then every ID-stable S-submodule of M is a finitely generated S-module, and hence an ID-submodule of M.*

This enables us to prove the last point mentioned in Remark 3.1.2.

`cor:ID-finite-subalgebra`

Corollary 3.3.6. *Let (R, θ) be an ID-ring extension of (S, θ). Then the set of elements in R which are ID-finite over S is an S-subalgebra of R.*

Proof. By Prop. 3.2.2, all elements in S are ID-finite over S. So it remains to show that for ID-finite elements $x, y \in R$ also $x + y$ and $x \cdot y$ are ID-finite.

Since x and y are ID-finite over S, the S-modules $\langle \theta^{(n)}(x) \mid n \in \mathbb{N} \rangle_S$ and $\langle \theta^{(n)}(y) \mid n \in \mathbb{N} \rangle_S$ are finitely generated. But then also $M := \langle \theta^{(n)}(x) \mid n \in \mathbb{N} \rangle_S + \langle \theta^{(n)}(y) \mid n \in \mathbb{N} \rangle_S$ is finitely generated as well as $N := \langle \theta^{(n)}(x)\theta^{(m)}(y) \mid n, m \in \mathbb{N} \rangle_S$. Therefore, M and N are ID-modules over S. Using additivity of the $\theta^{(n)}$ resp. the generalized Leibniz rule, one obtains that $\langle \theta^{(n)}(x+y) \mid n \in \mathbb{N} \rangle_S$ and $\langle \theta^{(n)}(x \cdot y) \mid n \in \mathbb{N} \rangle_S$ are ID-stable S-submodules of M resp. of N, and hence by Cor. 3.3.5, they are both finitely generated as S-modules. Therefore $x + y$ and $x \cdot y$ are ID-finite over S. □

We end the considerations on the structure of ID-modules by looking at the special case of the ID-simple ring $(S, \theta) = (C[[t]], \theta_t)$ (comp. Example 3.1.12).

`thm:trivial-over-ct`

Theorem 3.3.7. *Let C be a field. Then every ID-module over $(C[[t]], \theta_t)$ is trivial.*

Proof. Let (M, θ_M) be an ID-module over $(C[[t]], \theta_t)$. Since, $C[[t]]$ is a local ring, M is a free $C[[t]]$-module by Lemma 3.3.2. Hence, let $\boldsymbol{b} = (b_1, \dots, b_r)$ be a basis of M and $A(t,T) \in \mathrm{Mat}_{r\times r}(C[[t]][[T]])$ be such that $\theta_M(\boldsymbol{b}) = \boldsymbol{b}A(t,T)$.[2] Since $\theta^{(0)} = \mathrm{id}_M$, one has $A(t,0) = \mathbb{1}_r \in \mathrm{GL}_r(C[[t]])$ which implies that $A(t,T)$ is invertible, i.e. $A(t,T) \in \mathrm{GL}_r(C[[t]][[T]])$. Therefore, also $Y(t) := A(t,-t) \in \mathrm{Mat}_{r\times r}(C[[t]])$ is invertible, since $Y(0) = A(0,0) = \mathbb{1}_r \in \mathrm{GL}_r(C)$. We claim that $\boldsymbol{b}Y(t)$ is a basis of constant vectors in M, and hence $M \cong S^r$ as ID-modules.
Since, $\theta_M(\boldsymbol{b}Y(t)) = \theta_M(\boldsymbol{b})\theta_t(Y(t)) = \boldsymbol{b}A(t,T)Y(t+T)$, we have to show that

$$Y(t) = A(t,T)Y(t+T).$$

Since the iteration rule $\theta_M^{(i)} \circ \theta_M^{(i)} = \binom{i+j}{i}\theta_M^{(i+j)}$ holds, one has the following commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{{}_U\theta_M} & M[[U]] \\ & \searrow^{{}_{T+U}\theta_M} & \downarrow{\scriptstyle \theta_M[[U]]} \\ & & M[[T,U]] \end{array}$$

(which indeed is equivalent to the iteration rule; cf. [Mat89, §27]). Here ${}_U\theta_M$ and ${}_{T+U}\theta_M$ are the iterative derivations on M with T replaced by U resp. by $T+U$, i.e. ${}_U\theta_M : M \xrightarrow{\theta_M} M[[T]] \xrightarrow{T\mapsto U} M[[U]]$. The map $\theta_M[[U]]$ denotes the extension of θ_M to $M[[U]]$ by applying θ_M to each coefficient, i.e. $\theta_M[[U]]\left(\sum_{i=0}^{\infty} m_i U^i\right) := \sum_{i=0}^{\infty} \theta_M(m_i)U^i \in M[[T,U]]$.

Applying this to our setting, we obtain

$$\begin{aligned} \boldsymbol{b}A(t,T+U) &= {}_{T+U}\theta_M(\boldsymbol{b}) = \theta_M[[U]]\left({}_U\theta_M(\boldsymbol{b})\right) \\ &= \theta_M[[U]]\left(\boldsymbol{b}A(t,U)\right) = \boldsymbol{b}A(t,T)A(t+T,U), \end{aligned}$$

hence $A(t,T+U) = A(t,T)A(t+T,U)$. Specializing U to $-t-T$, we finally get

$$Y(t) = A(t,-t) = A(t,T)A(t+T,-t-T) = A(t,T)Y(t+T).$$

□

3.4 Picard-Vessiot rings

sec:pv-rings-id

Throughout the section, let (S,θ) denote an ID-simple ring, and (M,θ_M) an ID-module over S. In the categorical setting we have already defined solution rings and Picard-Vessiot rings. We recall their definition in this special case for the sake of readability.

[2] When we apply θ resp. θ_M to a tuple or a matrix, it is meant to apply θ resp. θ_M to each entry. Then the equation has to be read as a matrix identity, i.e. $\theta_M(b_i) = \sum_{j=1}^{r} b_j A(t,T)_{ji}$ for $A(t,T)_{ji}$ being the (j,i)-th entry of $A(t,T)$.

def:pv-ring

Definition 3.4.1. A **solution ring** for M is an ID-ring extension (R, θ_R) of (S, θ) s.t. the natural homomorphism

$$R \otimes_{C_R} C_{R \otimes_S M} \to R \otimes_S M$$

is an isomorphism. A **Picard-Vessiot ring** (PV-ring) for M is a *minimal* solution ring (R, θ_R) such that

(i) R is ID-simple,

(ii) $C_R = C_S$.

Here, *minimal* means that if $(\tilde{R}, \theta_{\tilde{R}})$ is another solution ring, then any injective ID-homomorphism of S-algebras $g : \tilde{R} \to R$ (if it exists) is an isomorphism.

prop:ct-is-simple-sol-ring

Proposition 3.4.2. *Let $\mathfrak{m}$ be a maximal ideal of S and $C = S/\mathfrak{m}$. Then $C[[t]]$ is a simple solution ring for any ID-module M where $S \hookrightarrow C[[t]]$ is given as in Thm. 3.2.4.*

Proof. Let $\hat{M} := C[[t]] \otimes_S M$. We then have to verify that $C[[t]] \otimes_C C_{\hat{M}} \to \hat{M}$ is an isomorphism. But this just means that $\hat{M}$ is a trivial ID-module over $C[[t]]$ which is given by Thm. 3.3.7. □

Remark 3.4.3. Assume that M is a free S-module with basis $\boldsymbol{b} = (b_1, \ldots, b_r)$.

1. If R is a solution ring for M, then there is a matrix $Y \in \mathrm{GL}_r(R)$ s.t. $\boldsymbol{b}Y$ is a basis of constant elements in $R \otimes_S M$. Such a matrix will be called a **fundamental solution matrix** for M (with respect to $\boldsymbol{b}$).

2. The universal solution ring U defined in the categorical setting in Thm. 2.4.7 is in this case nothing else than the localized polynomial ring $S[X, \det(X)^{-1}]$ in r^2-variables x_{ij} and the iterative derivation is given in such a way that X is a fundamental solution matrix for M.

The next proposition implies that in case of an ID-module M which is free as S-module, our definition of PV-ring coincides with the usual one given for example in [MvdP03, Sect. 3] (if the constants are algebraically closed) resp. in [Mau10b, Def. 2.3].

prop:generated-by-fsm

Proposition 3.4.4. *Assume that M is free as an S-module, and let R be a simple solution ring for M such that $C_R = C_S$. Then there is a unique Picard-Vessiot ring $\tilde{R}$ inside R. This is the S-subalgebra of R generated by the coefficients of a fundamental solution matrix and the inverse of its determinant.*

Proof. This is just Prop. 2.4.14 □

We now turn to the construction of a PV-ring for a general ID-module.
thm:explicit-pv-ring

Theorem 3.4.5. *Let M be an ID-module over S, R a simple solution ring for M with $C_R = C_S$, and let $\boldsymbol{e} = (e_1, \dots, e_r)$ be an R-basis of $R \otimes_S M$ consisting of ID-constant elements. Furthermore, let $x_1, \dots, x_l \in S$ such that $\langle x_1, \dots, x_l \rangle_S = S$ and $M[\frac{1}{x_i}]$ is free over $S[\frac{1}{x_i}]$ for all $i = 1, \dots, l$.*[3] *For all i let $\boldsymbol{b_i}$ be a basis of $M[\frac{1}{x_i}]$ over $S[\frac{1}{x_i}]$ consisting of elements in M, and $Y_i \in \mathrm{Mat}_{r\times r}(R)$ s.t. $\boldsymbol{b_i} = \boldsymbol{e}Y_i$ $(i = 1, \dots, l)$. Furthermore, choose $n_i \in \mathbb{N}$ such that $x_i^{n_i} M \subseteq \langle \boldsymbol{b_i} \rangle_S$.*

Then there is a unique Picard-Vessiot ring $\tilde{R}$ for M inside R, and it is explicitly given by $\tilde{R} := S[Y_j, \det(x_j^{n_j} Y_j^{-1}) \mid j = 1, \dots l]$.

Proof. First at all, since $\langle x_1, \dots, x_l \rangle_S = S$ and therefore $\langle x_1^{n_1}, \dots, x_l^{n_l} \rangle_S = S$, there exist $a_1, \dots, a_l \in S$ s.t. $\sum_{i=1}^{l} a_i x_i^{n_i} = 1$. This also implies that $\boldsymbol{b_1} \cup \dots \cup \boldsymbol{b_l}$ is a set of generators for M. Hence, $\boldsymbol{b_1} \cup \dots \cup \boldsymbol{b_l}$ is a set of generators for $R \otimes_S M$, and there also is a matrix $\tilde{Y} \in \mathrm{Mat}_{rl\times r}(R)$ s.t. $\boldsymbol{e} = (\boldsymbol{b_1}, \dots, \boldsymbol{b_l})\tilde{Y}$. The proof now procedes in three steps:

Step 1: We show that $\tilde{R} = S[Y_j, \det(x_j^{n_j} Y_j^{-1}) \mid j = 1, \dots l] \subseteq R$:
Since $x_j^{n_j} M \subseteq \langle \boldsymbol{b_j} \rangle_S$ and $\boldsymbol{b_i} x_j^{n_j} = \boldsymbol{b_j} x_j^{n_j} Y_j^{-1} Y_i$, the matrix $(x_j^{n_j} Y_j^{-1} Y_i)$ has coefficients in S for all i, j. Then

$$\begin{aligned} \boldsymbol{e} x_j^{n_j} &= (\boldsymbol{b_1}, \dots, \boldsymbol{b_l})\tilde{Y} x_j^{n_j} = (\boldsymbol{b_1} x_j^{n_j}, \dots, \boldsymbol{b_l} x_j^{n_j})\tilde{Y} \\ &= \boldsymbol{b_j}(x_j^{n_j} Y_j^{-1} Y_1, \dots, x_j^{n_j} Y_j^{-1} Y_l)\tilde{Y} \in \langle \boldsymbol{b_j} \rangle_R \end{aligned}$$

and $\boldsymbol{e} x_j^{n_j} = \boldsymbol{b_j}(x_j^{n_j} Y_j^{-1})$. Therefore, $x_j^{n_j} Y_j^{-1} \in \mathrm{Mat}_{r\times r}(R)$. Therefore we obtain $\tilde{R} = S[Y_j, \det(x_j^{n_j} Y_j^{-1})] \subseteq R$.

Step 2: $\tilde{R}$ is a simple solution ring for M:
$\tilde{R}$ is ID-simple, since all the localisations $\tilde{R}[\frac{1}{x_i}]$ are ID-simple by the consideration of the special case of a free ID-module, because they are just Picard-Vessiot rings for the free $S[\frac{1}{x_i}]$-modules $M[\frac{1}{x_i}]$. (Y_i^{-1} is a fundamental solution matrix for $M[\frac{1}{x_i}]$.)
Furthermore, $\tilde{R} \otimes_S M$ contains the basis $\boldsymbol{e}$, since

$$\boldsymbol{e} = \boldsymbol{e} \cdot \sum_{j=1}^{l} a_j x_j^{n_j} = \sum_{j=1}^{l} \boldsymbol{b_j}(x_j^{n_j} Y_j^{-1}) a_j \in \langle \boldsymbol{b_1} \cup \dots \cup \boldsymbol{b_l} \rangle_{\tilde{R}} = \tilde{R} \otimes_S M.$$

Hence, $\tilde{R} \otimes_S M$ is a trivial ID-module and therefore $\tilde{R}$ is a solution ring for M.

Step 3: $\tilde{R}$ is a Picard-Vessiot ring for M, and the unique one inside R:
The steps 1 and 2 work for any solution ring R, in particular for a Picard-Vessiot ring $R' \subseteq R$. In this case, by minimality of R', and $\tilde{R} \subseteq R'$, we obtain that $R' = \tilde{R}$. Therefore $\tilde{R}$ is a Picard-Vessiot ring, and the unique one inside R. □

[3] The x_i exist, since M is projective by Theorem 3.3.3, hence locally free in the stronger sense.

From the explicit description above or directly from the categorical case (see Thm. 2.4.12), we obtain

cor:faithful-flatness

Corollary 3.4.6. *Let (R, θ_R) be a Picard-Vessiot ring for M. Then:*

(a) All $r \in R$ are ID-finite over S.

(b) R/S is faithfully flat.

We end this section with two theorems on the existence and uniqueness of Picard-Vessiot rings. The first one follows from the general case (Thm. 2.4.18 and Cor. 2.4.17), and the second one from the considerations above.

thm:c-alg-closed

Theorem 3.4.7. *Let M be an ID-module over S. If the constants C of S are algebraically closed, then there exists a Picard-Vessiot ring for M and it is unique up to ID-isomorphism.*

thm:pv-ring-exists

Theorem 3.4.8. *Let S have a maximal ideal $\mathfrak{m}$ satisfying $S/\mathfrak{m} \cong C = C_S$, and let $S \hookrightarrow C[[t]]$ be the embedding given in Thm. 3.2.4. Then for any ID-module M over S there exists a unique Picard-Vessiot ring R for M inside $C[[t]]$.*

Proof. By Prop. 3.4.2, $C[[t]]$ is a simple solution ring for M. By assumption it constants C equal the constants of S. Hence by Theorem 3.4.5, there exists a unique Picard-Vessiot ring for M inside $C[[t]]$). □

3.5 The differential Galois group scheme

In this and the next section we introduce the Galois group scheme and establish the Galois correspondence for a Picard-Vessiot extension analogous to the classical ones. The ideas are the same as in [Dyc08, Sect. 2] resp. in [Mau10a, Sect. 10/11]. But we have to do a bit more work, since our modules are not free.

Although the main result follows from the categorical setting, we give the proofs here, because they also give more explicit descriptions.

thm:torsor-isomorphism

Theorem 3.5.1. *Let M be an ID-module over S, R' a simple solution ring for M with $C_{R'} = C_S$ and R a PV-ring for M. Then the map*

$$\alpha : R' \otimes_C C_{R' \otimes_S R} \longrightarrow R' \otimes_S R, r \otimes a \mapsto (r \otimes 1) \cdot a$$

is an ID-isomorphism. Furthermore, $C_{R' \otimes_S R}$ is a finitely generated C-algebra.

Proof. By definition α is an ID-homomorphism.
First we show injectivity: Since α is an ID-homomorphism, $\mathrm{Ker}(\alpha)$ is an ID-ideal of $R' \otimes_C C_{R' \otimes_S R}$. Since R' is ID-simple, $\mathrm{Ker}(\alpha)$ is generated by elements in $C_{R' \otimes_S R}$

by Proposition 3.1.3. But $C_{R'\otimes_S R}$ embeds in $R'\otimes_S R$. Hence, $\mathrm{Ker}(\alpha)=\{0\}$. For showing surjectivity, we use the notation of Theorem 3.4.5. So let $x_1,\dots,x_l\in S$ be such that $\langle x_1,\dots,x_l\rangle_S = S$ and $M[\frac{1}{x_i}]$ is free as $S[\frac{1}{x_i}]$-module for all $i=1,\dots,l$, and let $\boldsymbol{b_i}$ be a basis of $M[\frac{1}{x_i}]$ consisting of elements of M, and $n_i\in\mathbb{N}$ such that $x_i^{n_i}M\subseteq\langle \boldsymbol{b_i}\rangle_S$. Furthermore, let $\boldsymbol{e}$ resp. $\boldsymbol{e}'$ be a basis of constant elements in $R\otimes_S M$ resp. $R'\otimes_S M$. Additionally, let $Y_i\in \mathrm{Mat}_r(R)$ and $X_i\in\mathrm{Mat}_r(R')$ such that $\boldsymbol{b_i}=\boldsymbol{e}Y_i=\boldsymbol{e}'X_i$. Then R is generated over S by the entries of Y_i and $x_i^{n_i}Y_i^{-1}$, and by R'-linearity of α it is enough to show that these entries are in $\mathrm{Im}(\alpha)$.

$\boldsymbol{e}$ and $\boldsymbol{e}'$ can also be viewed as bases of the free $(R'\otimes_S R)$-module $(R'\otimes_S R)\otimes_S M$.[4] Hence, there is a matrix $Z\in\mathrm{GL}_r(R'\otimes_S R)$ such that $\boldsymbol{e}Z=\boldsymbol{e}'$. Since both $\boldsymbol{e}$ and $\boldsymbol{e}'$ consist of constant vectors the entries of Z are also constant, and the same holds for its inverse $Z^{-1}\in\mathrm{GL}_r(R'\otimes_S R)$. Hence, $Z\in\mathrm{GL}_r(C_{R'\otimes_S R})$.

For all i we have $\boldsymbol{e}Y_i=\boldsymbol{b_i}=\boldsymbol{e}'X_i=\boldsymbol{e}ZX_i$ and hence $Y_i=ZX_i\in\mathrm{Mat}_r(R'\otimes_S R)$, as well as $x_i^{n_i}Y_i^{-1}=(x_i^{n_i}X_i^{-1})Z^{-1}$. Hence, the entries of all Y_i and of all $x_i^{n_i}Y_i^{-1}$ are in the image of α.

Finally, as just seen, the restriction of α to $R'\otimes_C C[Z,Z^{-1}]\subseteq R'\otimes_C C_{R'\otimes_S R}$ is also surjective. But α is an isomorphism and hence, $R'\otimes_C C[Z,Z^{-1}]=R'\otimes_C C_{R'\otimes_S R}$. Therefore, $C[Z,Z^{-1}]=C_{R'\otimes_S R}$, and $C_{R'\otimes_S R}$ is a finitely generated C-algebra. □

Proposition 3.5.2. *Let M be an ID-module over S, and let R,R' be PV-rings for M. Furthermore, let D be a C-algebra equipped with the trivial iterative derivation. Then any $(S\otimes_C D)$-linear ID-homomorphism $R\otimes_C D\to R'\otimes_C D$ is an isomorphism.*

Proof. Let $\beta: R\otimes_C D\to R'\otimes_C D$ be an $(S\otimes_C D)$-linear ID-homomorphism. As in the previous proof, $\mathrm{Ker}(\beta)$ is generated by constants and hence is trivial. For the surjectivity, we remark that $\beta(R)$ and R' are both PV-rings for M. As in the previous proof, there are bases of constant elements $\boldsymbol{e}$ and $\boldsymbol{e}'$ in $\beta(R)\otimes_S M$ resp. $R'\otimes_S M$ which can both be viewed as bases of the free $(R'\otimes_C D)$-module $(R'\otimes_C D)\otimes_S M$.

The same arguments as in the previous proof (with R and R' switched) show that R' is contained in the subring $\beta(R\otimes_C D)=\beta(R)\cdot D$ of $R'\otimes_C D$. Hence by D-linearity β is surjective. □

thm:the-scheme-isom

Theorem 3.5.3. *Let M be an ID-module over S, and let R',R be PV-rings for M. Then the functor*

$$\underline{\mathrm{Isom}}_S^{ID}(R,R'):\mathsf{Alg}_C\longrightarrow\mathsf{Sets},\ D\mapsto \mathrm{Isom}_S^{ID}(R\otimes_C D,R'\otimes_C D)$$

is represented by $\mathrm{Spec}(C_{R'\otimes_S R})$. *In particular, it is an affine scheme of finite type over C.*

[4] R and R' both embed into $R'\otimes_S R$, since they are both ID-simple.

Proof. Using the previous proposition and theorem, the proof is exactly the same as in [Dyc08, Cor. 2.11], or in [Mau10a, Prop. 10.9.]. □

As a special case for $R' = R$ we obtain the representability of $\underline{\mathrm{Aut}}^{ID}(R/S)$.

cor:galois-group-scheme

Corollary 3.5.4. *For a PV-extension R/S, the group functor $\underline{\mathrm{Aut}}^{ID}(R/S)$ is represented by $\mathcal{G} := \mathrm{Spec}(C_{R\otimes_S R})$, and thus $\mathcal{G} \cong \underline{\mathrm{Aut}}^{ID}(R/S)$ is an affine group scheme of finite type over C.*

Definition 3.5.5. We call $\mathcal{G} = \underline{\mathrm{Aut}}^{ID}(R/S)$ the **ID-Galois group (scheme)** of R/S and denote it by $\underline{\mathrm{Gal}}(R/S)$.

Proposition 3.5.6. *Let R/S be a PV-extension and $\mathcal{G} = \underline{\mathrm{Gal}}(R/S)$ the ID-Galois group. Denote $\mathcal{G}_S := \mathcal{G} \times_C \mathrm{Spec}(S)$ the extension of $\mathcal{G}$ by scalars. Then $\mathrm{Spec}(R)$ is a $\mathcal{G}_S$-torsor.*

Proof. The inverse of the isomorphism α of Theorem 3.5.1 for $R' = R$ induces an isomorphism of affine schemes

$$\mathrm{Spec}(R) \times_{\mathrm{Spec}(S)} \mathcal{G}_S = \mathrm{Spec}(R) \times_C \mathcal{G} \longrightarrow \mathrm{Spec}(R) \times_{\mathrm{Spec}(S)} \mathrm{Spec}(R).$$

By bookkeeping of the identifications one verifies that this map is indeed the isomorphism $(x, g) \mapsto (x, g(x))$ indicating that $\mathrm{Spec}(R)$ is a $\mathcal{G}_S$-torsor. □

3.6 Galois correspondence

We will now describe the Galois correspondence given in the categorical setting in a more explicit way. For that, we need a definition of functorial invariants (comp. [Mau10a, Sect. 11]):

Let $\mathcal{H} \leq \mathcal{G}$ be a subgroup functor of $\mathcal{G} = \underline{\mathrm{Gal}}(R/S)$, i. e. for every C-algebra D, the set $\mathcal{H}(D)$ is a group acting on $R_D := R \otimes_C D$ and this action is functorial in D. An element $r \in R$ is then called **invariant** under $\mathcal{H}$ if for all D, the element $r \otimes 1 \in R_D$ is invariant under $\mathcal{H}(D)$. The ring of invariants is denoted by $R^{\mathcal{H}}$. (In [Jan03, I.2.10] the invariant elements are called "fixed points".)

rem:rho

Remark 3.6.1. Let $\gamma : R \otimes_S R \to R \otimes_C C[\mathcal{G}]$ denote the inverse of the isomorphism α. The action of $\mathcal{G} := \underline{\mathrm{Gal}}(R/S)$ on R is fully described by the ID-homomorphism $\rho := \gamma|_{1\otimes R} : R \to R \otimes_C C[\mathcal{G}]$. Namely, for a C-algebra D and $g \in \mathcal{G}(D)$ with corresponding $\tilde{g} \in \mathrm{Hom}(C[\mathcal{G}], D)$, one has $g(r \otimes 1) = (1 \otimes \tilde{g})(\rho(r)) \in R \otimes_C D$ for all $r \in R$.
Furthermore, for a closed subgroup scheme $\mathcal{H} \leq \mathcal{G}$, defined by an ideal $I \subseteq C[\mathcal{G}]$, one has $r \in R^{\mathcal{H}}$ if and only if, $\rho(r) \equiv r \otimes 1 \mod R \otimes I$, resp. if $\pi^{\mathcal{G}}_{\mathcal{H}}(\rho(r)) = r \otimes 1 \in R \otimes_C C[\mathcal{H}]$ where $\pi^{\mathcal{G}}_{\mathcal{H}} : C[\mathcal{G}] \to C[\mathcal{G}]/I = C[\mathcal{H}]$ denotes the canonical projection.

prop:R^G=S

Proposition 3.6.2. *Let R/S be a PV-extension and $\mathcal{G} = \underline{\mathrm{Gal}}(R/S)$ the ID-Galois group. Then $R^{\mathcal{G}} = S$.*

Proof. By the previous remark, $r \in R^{\mathcal{G}}$ if and only if $\rho(r) = r \otimes 1$. This means that $\gamma(r \otimes 1) = r \otimes 1 = \gamma(1 \otimes r)$ which is equivalent to $r \in \mathrm{Quot}(S)$. Since, R/S is faithfully flat by Cor. 3.4.6, we obtain $r \in S$. □

rem:converse-to-R^G=S

Remark 3.6.3. The converse conclusion to Proposition 3.6.2, i.e. that $R^{\mathcal{H}} = S$ for $\mathcal{H} \leq \mathcal{G}$ implies $\mathcal{H} = \mathcal{G}$, is not true. For example, if $\mathcal{G} = \mathrm{GL}_n(C)$ and $\mathcal{H}$ is taken to be a Borel subgroup, then $R \cong S[\mathrm{GL}_n]$ by Hilbert 90, and $R^{\mathcal{H}} \cong S[\mathrm{GL}_n]^{\mathcal{H}} = S$. The geometrical reason is that $R^{\mathcal{H}}$ is the ring of global sections of the scheme $\mathrm{Spec}(R)/\mathcal{H}$. In case of $\mathcal{H}$ being the Borel subgroup this is a projective scheme over S.

Before we come to the Galois correspondence, we need some lemmas and propositions. We start with a condition on an ID-simple ring ensuring that it is a PV-ring.

lem:torsor-is-pv-ring

Lemma 3.6.4 (analog of [Mau10a, Prop. 10.12])**.** *Let R/S be a faithfully flat extension of ID-simple rings with $C_R = C_S = C$. Assume there exists an affine group scheme $\mathcal{G}$ of finite type over C such that $\mathrm{Spec}(R)$ is a $\mathcal{G}_S$-torsor and the corresponding isomorphism of S-algebras $\gamma : R \otimes_S R \to R \otimes_C C[\mathcal{G}]$ is an ID-isomorphism. Here, as usual $C[\mathcal{G}]$ is equipped with the trivial iterative derivation. Then R is a Picard-Vessiot ring over S.*

Proof. The proof goes similar to [Tak89], proof of Thm. 3.3(a)⇒(b).

Since, $\mathrm{Spec}(R)$ is a $\mathcal{G}_S$-torsor, R is finitely generated over S, and we can choose C-linear independent elements $u_1, \ldots, u_r \in R$ such that R is generated over S by these elements. By possibly increasing the set of u's we can assume that $\rho(\langle u_1, \ldots, u_r \rangle_C) \subseteq \langle u_1, \ldots, u_r \rangle_C \otimes_C C[\mathcal{G}]$, since by general theory on comodules, every element is contained in a finite dimensional comodule (cf. [Swe69, Thm. 2.1.3]).[5] Then there are $b_{ij} \in C[\mathcal{G}]$ $(i, j = 1, \ldots, r)$ such that $\rho(u_j) = \sum_{i=1}^{r} u_i \otimes b_{ij}$ for all $j = 1, \ldots, r$, or written in matrix notation:

$$\rho(u_1, \ldots, u_r) = (u_1, \ldots, u_r) \otimes B,$$

for $B = (b_{ij})_{1 \leq i,j \leq r}$.
Since, ρ is a homomorphism of ID-rings, we also obtain for all $n \in \mathbb{N}$ that

$$\rho(\theta^{(n)}(u_1), \ldots, \theta^{(n)}(u_r)) = (\theta^{(n)}(u_1), \ldots, \theta^{(n)}(u_r)) \otimes B.$$

[5] As in Remark 3.6.1, $\rho := \gamma|_{1 \otimes R}$ denotes the coaction of $C[\mathcal{G}]$ on R corresponding to the action of $\mathcal{G}$.

Now, let $M \subseteq R^r$ be the S-module generated by all vectors $(\theta^{(n)}(u_1), \ldots, \theta^{(n)}(u_r))$ $(n \geq 0)$. Then M is an ID-stable subset of R^r by definition and an S-module.

We will show that M is finitely generated as S-module, that $R \otimes_S M = R \cdot M = R^r$, as well as that for any $\tilde{R} \subsetneqq R$, the standard basis of R^r is not contained in $\tilde{R} \otimes_S M$.
The first shows that M is indeed an ID-module over S, the second that R is a solution ring for M, and the third that R is a minimal solution ring, hence a Picard-Vessiot ring for M.

We consider the matrices

$$W(k_1, \ldots, k_r) := \begin{pmatrix} \theta^{(k_1)}(u_1) & \ldots & \theta^{(k_1)}(u_r) \\ \vdots & & \vdots \\ \theta^{(k_r)}(u_1) & \ldots & \theta^{(k_r)}(u_r) \end{pmatrix} \in \mathrm{Mat}_{r \times r}(R)$$

for $(k_1, \ldots, k_r) \in \mathbb{N}^r$, and the ideal

$$I := \langle \det(W(k_1, \ldots, k_r)) \mid (k_1, \ldots, k_r) \in \mathbb{N}^r \rangle_R \subseteq R$$

generated by all the determinants of all these matrices.

Since $\{u_1, \ldots, u_r\}$ are C-linearly independent, $\{\theta(u_1), \ldots, \theta(u_r)\} \subseteq R[[T]]$ are R-linearly independent (cf. [Tak89, Prop. 1.5]), and therefore, there is a matrix $W(k_1, \ldots, k_r)$ having full rank. In particular, $I \neq \{0\}$. Furthermore, using the Leibniz determinant formula and the product rule for iterative derivations one obtains

$$\theta^{(n)}(\det(W(k_1, \ldots, k_r))) = \sum_{n_1 + \cdots + n_r = n} \binom{k_1+n_1}{k_1} \cdots \binom{k_r+n_r}{k_r} \det(W(k_1+n_1, \ldots, k_r+n_r)).$$

Hence, I is an ID-ideal, and since R is ID-simple, we have $I = R$. Therefore, there exist matrices $W_1, \ldots, W_l \in \{W(k_1, \ldots, k_r) \mid (k_1, \ldots, k_r) \in \mathbb{N}^r\}$ and $a_1, \ldots, a_l \in R$ such that $1 = \sum_{i=1}^{l} a_i \det(W_i)$. Using the adjugate matrices $W_i^{\#}$ of the W_i we get

$$\mathbb{1}_r = \sum_{i=1}^{l} a_i \det(W_i) \mathbb{1}_r = \sum_{i=1}^{l} a_i W_i^{\#} W_i.$$

This means that the standard basis of R^r is obtained as an R-linear combination of the rows of the W_i, and hence $R \cdot M = R^r$.

For the finite generation of M, we take $W = W(k_1, \ldots, k_r)$ of full rank, and observe that $\rho(W) = W \otimes B$, $\rho(\det(W)) = \det(W) \otimes \det(B)$ and $\rho(W^{\#}) = (1 \otimes B^{\#}) \cdot (W^{\#} \otimes 1)$, by using $WW^{\#} = \det(W)\mathbb{1}_r$. Write $\theta^{(n)}(\boldsymbol{u}) := (\theta^{(n)}(u_1), \ldots, \theta^{(n)}(u_r))$,

then we get

$$\begin{aligned}\gamma(\det(W)\otimes\theta^{(n)}(\boldsymbol{u})W^{\#}) &= \det(W)(\theta^{(n)}(\boldsymbol{u})\otimes B)(1\otimes B^{\#})(W^{\#}\otimes 1)\\ &= (\det(W)\theta^{(n)}(\boldsymbol{u})\otimes\det(B)\mathbb{1}_r)(W^{\#}\otimes 1)\\ &= \theta^{(n)}(\boldsymbol{u})W^{\#}\det(W)\otimes\det(B)\\ &= \gamma(\theta^{(n)}(\boldsymbol{u})W^{\#}\otimes\det(W))\end{aligned}$$

Since, γ is an isomorphism, we have $\theta^{(n)}(\boldsymbol{u})W^{\#}\otimes\det(W) = \det(W)\otimes\theta^{(n)}(\boldsymbol{u})W^{\#}$, and since the tensor product is taken over S, each entry of $\theta^{(n)}(\boldsymbol{u})W^{\#}$ is a $\mathrm{Quot}(S)$-multiple of $\det(W)$. So there is a vector $\boldsymbol{s} = (s_1,\dots,s_r)\in S^r$ and $t\in S$ such that $t\cdot\theta^{(n)}(\boldsymbol{u})W^{\#} = \boldsymbol{s}\det(W)$, and hence

$$t\cdot\theta^{(n)}(\boldsymbol{u}) = \boldsymbol{s}W.$$

This shows that all the vectors $\theta^{(n)}(\boldsymbol{u})$ are S-linearly dependent to the rows of W. Recalling that the rows of W were R-linearly independent, this show that for any S-module N generated by vectors $\theta^{(n)}(\boldsymbol{u})$ for several $n\in\mathbb{N}$ containing the rows of W, one has $R\otimes_S N = R\cdot N$.
Applying this to the S-module M and to the S-module N generated by the rows of the W_i $(i=1,\dots,l)$ above, we see that $R\otimes_S N = R^r = R\otimes_S M$. Hence by faithful flatness of R/S, $M=N$ and M is a finitely generated S-module.

Finally, we observe that for any solution ring $\tilde{R}$ inside R, the standard basis of R^r must be contained in $\tilde{R}\otimes_S M\subseteq R^r$, as it is a basis of constant vectors. Since $(u_1,\dots,u_r) = \sum_{i=1}^r u_i e_i\in M$, we get that $u_i\in\tilde{R}$. Hence, $\tilde{R}=R$. □

prop:equivalent-conditions

Proposition 3.6.5. *Let R/S be a PV-extension with Galois group scheme $\mathcal{G}$. For an ID-ring T with $S\subseteq T\subseteq R$ the following are equivalent:*

1. *T is a Picard-Vessiot ring over S for some ID-module.*
2. *T is ID-simple and stable under the action of $\mathcal{G}$, i.e. $\rho(T)\subseteq T\otimes_C C[\mathcal{G}]$.*
3. *There is a normal subgroup scheme $\mathcal{H}$ of $\mathcal{G}$ such that $T = R^{\mathcal{H}}$.*

If the equivalent conditions are fulfilled, the normal subgroup scheme $\mathcal{H}$ in iii) can be taken to be $\mathcal{H} = \underline{\mathrm{Gal}}(R/T)$.

Proof. i)⇒ii): (cf. [Mau10b, proof of Prop. 3.4])
Since, T is a PV-extension over S, we obtain a commutative diagram

$$\begin{array}{ccc} T\otimes_S T & \xrightarrow{\cong} & T\otimes_C C[\underline{\mathrm{Gal}}(T/S)] = T\otimes_C C_{T\otimes_S T}\\ \downarrow & & \downarrow\\ R\otimes_S R & \xrightarrow{\cong} & R\otimes_C C[\mathcal{G}] = R\otimes_C C_{R\otimes_S R}\end{array}$$

where the vertical maps are just the inclusions. But this implies $\rho(T) \subseteq T \otimes_C C_{T\otimes_S T} \subseteq T \otimes_C C[\mathcal{G}]$, i. e. T is stable under the action of $\mathcal{G}$.

ii)⇒iii): Since R also is a PV-ring over T for $T \otimes_S M$, the Galois group $\mathcal{H} := \underline{\mathrm{Gal}}(R/T)$ exists, and by Prop. 3.6.2, we have $R^{\mathcal{H}} = T$. The group scheme $\mathcal{H}$ is indeed a closed subgroup scheme of $\mathcal{G}$: $R \otimes_T R$ is a factor ring of $R \otimes_S R$ by an ID-ideal I. Since $\gamma : R \otimes_S R \to R \otimes_C C[\mathcal{G}]$ is an isomorphism, one has $\gamma(I) = R \otimes_C J$ for an ideal $J \trianglelefteq C[\mathcal{G}]$ by Prop. 3.2.3. Hence, $C[\mathcal{H}] = C_{R\otimes_T R} = C_{(R\otimes_S R)/I} = C[\mathcal{G}]/J$. Furthermore, since T is stable under the $\mathcal{G}$-action, for all C-algebras D and $g \in \mathcal{G}(D)$, $h \in \mathcal{H}(D) \subseteq \mathcal{G}(D)$, also $g^{-1}hg$ fixes the elements of $T \otimes_C D$, i.e. $g^{-1}hg \in \mathcal{H}(D)$. Hence, $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$.

iii)⇒i): (comp. [Mau10a, proof of Thm. 11.5(ii)])
First at all we show that T has constants C, that T/S is faithfully flat, and that $T = R^{\mathcal{H}}$ is ID-simple. As $C = C_S \subseteq C_T \subseteq C_R = C$, we have $C_T = C$. Faithful flatness is clear by the proof of Cor. 3.4.6, since $T \subseteq R$ consists of ID-finite elements. The isomorphism $\gamma : R \otimes_S R \to R \otimes_C C[\mathcal{G}]$ is $\mathcal{H}$-equivariant, considered by the action of $\mathcal{H}$ on the right tensor factor, and hence we get an ID-isomorphism

$$R \otimes_S R^{\mathcal{H}} \cong R \otimes_C C[\mathcal{G}]^{\mathcal{H}}.$$

Since $\mathcal{H}$ is normal, $\mathcal{G}/\mathcal{H}$ is an affine group scheme with $C[\mathcal{G}/\mathcal{H}] \cong C[\mathcal{G}]^{\mathcal{H}}$ (cf. [DG70, III,§3, Thm. 5.6 and 5.8]). Furthermore, $C[\mathcal{G}]^{\mathcal{H}} \subseteq C[\mathcal{G}]$ is faithfully flat. But then also $R \otimes_C C[\mathcal{G}]^{\mathcal{H}} \subseteq R \otimes_C C[\mathcal{G}]$ is faithfully flat, i.e. $R \otimes_S R^{\mathcal{H}} \subseteq R \otimes_S R$ is faithfully flat. But as $S \subseteq R$ is faithfully flat, this implies that $R^{\mathcal{H}} \subseteq R$ is also faithfully flat.
If $I \trianglelefteq T$ is an ID-ideal, then $RI \trianglelefteq R$ is an ID-ideal, and hence, RI equals $\{0\}$ or R. As R is faithfully flat over $R^{\mathcal{H}}$ this implies I equals $\{0\}$ or $R^{\mathcal{H}} = T$. Hence, T is ID-simple.
Taking again invariants on both sides of the isomorphism $R \otimes_S R^{\mathcal{H}} \cong R \otimes_C C[\mathcal{G}]^{\mathcal{H}}$ (this time $\mathcal{H}$ is only acting on the first tensor factor), this isomorphism restricts to an isomorphism

$$R^{\mathcal{H}} \otimes_S R^{\mathcal{H}} \cong R^{\mathcal{H}} \otimes_C C[\mathcal{G}]^{\mathcal{H}} = R^{\mathcal{H}} \otimes_C C[\mathcal{G}/\mathcal{H}].$$

By construction it is an ID-isomorphism, and it is the isomorphism corresponding to the map $\mathrm{Spec}(R^{\mathcal{H}}) \times_S (\mathcal{G}/\mathcal{H})_S \to \mathrm{Spec}(R^{\mathcal{H}}) \times_S \mathrm{Spec}(R^{\mathcal{H}})$ indicating that $\mathrm{Spec}(R^{\mathcal{H}})$ is a $(\mathcal{G}/\mathcal{H})_S$-torsor. Therefore, by Lemma 3.6.4, $T = R^{\mathcal{H}}$ is a PV-ring over S.

The statement on the choice of $\mathcal{H}$ has already been seen in the proof of the implication ii)⇒iii). □

thm:galois-correspondence-ID

Theorem 3.6.6. *(Galois correspondence) Let R/S be a PV-extension for some ID-module and $\mathcal{G} = \underline{\mathrm{Gal}}(R/S)$. Then there is a bijection between*

$$\mathfrak{T} := \{T \mid S \subseteq T \subseteq R \text{ intermediate PV-ring}\}$$

and

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

given by $\Psi : \mathfrak{T} \to \mathfrak{H}, T \mapsto \underline{\mathrm{Gal}}(R/T)$ *resp.* $\Phi : \mathfrak{H} \to \mathfrak{T}, \mathcal{H} \mapsto R^{\mathcal{H}}$.

Remark 3.6.7. The maps Ψ and Φ can be defined between all intermediate ID-rings and all closed subgroups of $\mathcal{G}$. But contrary to the Galois correspondences in [Mau10a] and others, one does not get a full bijection, as we only consider the rings and not the fields of fractions. Remark 3.6.3 provides an example that the extension Φ would not be injective in general.
Maybe, one would get a full bijection when considering schemes with ID-simple structure sheaves, because $\mathcal{G}/\mathcal{H}$, and therefore $\mathrm{Spec}(R)/\mathcal{H}$ is a non-affine scheme in general.

Proof of Thm. 3.6.6. Prop. 3.6.5 already shows most things: If $\mathcal{H}$ is a normal subgroup scheme of $\mathcal{G}$, then $R^{\mathcal{H}}$ is a PV-ring. Hence Φ is welldefined. If T is an intermediate PV-ring, the group scheme $\mathcal{H} := \underline{\mathrm{Gal}}(R/T)$ is a closed normal subgroup scheme of $\mathcal{G}$. Hence, Ψ is welldefined. Furthermore, $R^{\underline{\mathrm{Gal}}(R/T)} = T$ showing $\Phi \circ \Psi = \mathrm{id}$.

It remains to show that $\underline{\mathrm{Gal}}(R/R^{\mathcal{H}}) = \mathcal{H}$ for all closed normal subgroup schemes $\mathcal{H}$ of $\mathcal{G}$. In the proof of Prop. 3.6.5, it is shown that $\underline{\mathrm{Gal}}(R^{\mathcal{H}}/S) \cong \mathcal{G}/\mathcal{H}$. Furthermore, the projection map $\mathcal{G} \to \mathcal{G}/\mathcal{H}$ corresponds to the map $\underline{\mathrm{Gal}}(R/S) \to \underline{\mathrm{Gal}}(R^{\mathcal{H}}/S)$ given by restricting the automorphisms in $\underline{\mathrm{Gal}}(R/S)$ to $R^{\mathcal{H}}$. Hence, $\underline{\mathrm{Gal}}(R/R^{\mathcal{H}})$ is the kernel of this map, i.e. equals $\mathcal{H}$. □

3.7 Example

sec:example

We now give an example of an ID-module which is not free as a module. Therefore, we first need an ID-simple ring for which non-free projective modules exist. The most standard examples for non-free projective modules are non-principle ideals of Dedekind domains. This will be our example after having attached iterative derivations to the Dedekind domain as well as the module.

3.7.1 An ID-simple ring having non-free projective modules

Let C be any field and let

$$S := C[s, t, \frac{1}{3s^2 - 1}]/(s^3 - s - t^2),$$

which is the localisation of an integral extension of $C[t]$ of degree 3. S is integrally closed, and hence S is a Dedekind domain.

Since we inverted $3s^2-1$, S is étale over $C[t]$, and hence the iterative derivation θ_t by t on $C[t]$ can be uniquely extended to an iterative derivation θ on S (cf. [Mat89, Thm. 27.2]). The $\theta^{(n)}(s)$ can be computed successively using the equation

$$\theta(s)^3-\theta(s)=\theta(t)^2=(t+T)^2,$$

obtained from $s^3-s=t^2$ by applying θ. In particular,

$$\theta^{(1)}(s)=\frac{2t}{3s^2-1}.$$

Proposition 3.7.1. *The ID-ring (S,θ) is ID-simple.*

Proof. If $0\neq I\lneq S$ is an ideal, then $I\cap C[t]$ is an ideal of $C[t]$. Since, S is the localisation of an integral extension, the ideal $I\cap C[t]$ also is nontrivial. Furthermore, if I is an ID-ideal, then obviously $I\cap C[t]$ is also ID-stable, hence an ID-ideal of $C[t]$. But $(C[t],\theta_t)$ is ID-simple by Example 3.1.1. Hence, S also contains no nontrivial ID-ideals. □

3.7.2 A non-free ID-module over S in characteristic zero

We first restrict to the case of $\mathrm{char}(C)=0$. In this case, an iterative derivation θ_M on M is uniquely determined by the derivation $\partial_M:=\theta_M^{(1)}$.

We consider the S-module M generated by two elements f_1 and f_2 subject to the relations $tf_1-sf_2=0$ and $(s^2-1)f_1-tf_2=0$. As S-module M is isomorphic to the ideal $I=\langle s,t\rangle_S\subseteq S$ by mapping f_1 to s and f_2 to t. Since I is a non-principal ideal of S, I and hence M is a non-free projective S-module of rank 1.

Theorem 3.7.2. *For any $b\in S$,*

$$\partial_M(f_1):=bf_1+\frac{3s^2+1}{3s^2-1}f_2\quad\text{ and }\quad\partial_M(f_2):=sf_1+bf_2$$

defines a derivation on M.
Furthermore, every derivation on M can be written in this form.

Proof. Using the definition, one obtains

$$\begin{aligned}\partial_M(tf_1-sf_2) &= \partial(t)f_1+t\partial_M(f_1)-\partial(s)f_2-s\partial_M(f_2)\\ &= f_1+tbf_1+t\frac{3s^2+1}{3s^2-1}f_2-\frac{2t}{3s^2-1}f_2-s^2f_1-sbf_2\\ &= b(tf_1-sf_2)+(1-s^2)f_1+\left(\frac{3s^2+1}{3s^2-1}-\frac{2}{3s^2-1}\right)tf_2\\ &= b(tf_1-sf_2)-\big((s^2-1)f_1-tf_2\big)=0,\end{aligned}$$

and similarly $\partial_M((s^2-1)f_1 - tf_2) = 0$. Hence, the derivation is a well-defined derivation on M.

On the other hand, given a derivation ∂_M on M, we obtain a derivation on the $\mathrm{Quot}(S)$-vector space $\tilde{M} := \mathrm{Quot}(S) \otimes_S M$ by scalar extension. The element f_2 is a basis of that vector space, and $f_1 = \frac{s}{t} f_2 \in \tilde{M}$.
Hence, $\partial_M(f_2) = af_2$ for some $a \in \mathrm{Quot}(S)$ which can also be written as $\partial_M(f_2) = sf_1 + bf_2$ for $b = a - \frac{s^2}{t}$.
Then

$$\begin{aligned}\partial_M(f_1) &= \partial_M\left(\frac{s}{t}f_2\right) = \partial\left(\frac{s}{t}\right)f_2 + \frac{s}{t}\partial_M(f_2) = \frac{\frac{2t}{3s^2-1}t - s}{t^2}f_2 + \frac{s}{t}(sf_1 + bf_2) \\ &= \left(\frac{2}{3s^2-1} - \frac{s}{t^2}\right)f_2 + \frac{s^3}{t^2}f_2 + bf_1 = bf_1 + \frac{3s^2+1}{3s^2-1}f_2.\end{aligned}$$

Therefore, ∂_M is of the form above for some $b \in \mathrm{Quot}(S)$. But, M is stable under this derivation if and only if $bf_2 \in M$ as well as $bf_1 \in M$. So M is stable under the derivation if and only if $bM \subseteq M$, i.e. $b \in S$. □

3.7.3 Picard-Vessiot rings and Galois groups for this ID-module

The ID-ring S has a C-rational point, e.g. the ideal $\mathfrak{m} = (s-1, t)$, and we obtain an ID-embedding $S \to (S/\mathfrak{m})[[t]] \cong C[[t]]$.[6] So by Thm. 3.4.8 there exists a Picard-Vessiot ring for M inside $C[[t]]$, and we follow the explicit description of the Picard-Vessiot ring given in Thm. 3.4.5.

First at all, we choose $x_1 := s$ and $x_2 := s^2 - 1$. Then $M[\frac{1}{x_1}]$ is free over $S[\frac{1}{x_1}]$ with basis $b_1 := f_1$, and $M[\frac{1}{x_2}]$ is free over $S[\frac{1}{x_2}]$ with basis $b_2 := f_2$. Further, $x_1 M = sM \subseteq \langle b_1 \rangle_S$ and $x_2 M = (s^2-1)M \subseteq \langle b_2 \rangle_S$, hence we can choose $n_1 = n_2 = 1$.

Let $0 \neq e \in C[[t]] \otimes_S M$ be a constant element, and $y \in C[[t]]$ such that $f_1 = ye$. As $s \notin \mathfrak{m}$, s is invertible in $S_{\mathfrak{m}} \cong C[[t]]$, and $f_2 = \frac{t}{s} f_1 \in C[[t]] \otimes_S M$. In particular, f_1 is a basis of $C[[t]] \otimes_S M$. Actually, this also implies that y is invertible in $C[[t]]$, as it is the base change matrix between the bases f_1 and e of $C[[t]] \otimes_S M$. As

$$\partial(y)e = \partial_M(ye) = \partial(f_1) = bf_1 + \frac{3s^2+1}{3s^2-1}f_2 = \left(b + \frac{3s^2+1}{3s^2-1}\frac{t}{s}\right)ye,$$

y is a solution of the differential equation

$$\partial(y) = \left(b + \frac{3s^2+1}{3s^2-1}\frac{t}{s}\right)y.$$

[6] Using the variable t in the power series ring is justified by the fact, that $t \in S$ indeed maps to $t \in C[[t]]$ via the given embedding.

Furthermore with notation as in Thm. 3.4.5, we get $Y_1 = y, Y_2 = \frac{yt}{s}$, $\det(x_1^{n_1}Y_1^{-1}) = \frac{s}{y}$ as well as $\det(x_2^{n_2}Y_2^{-1}) = \frac{(s^2-1)s}{yt} = \frac{t}{y}$. Hence,

$$R = S[y, \frac{yt}{s}, \frac{s}{y}, \frac{t}{y}].$$

Be aware that the inverse of y is not in R.

As M is a module of rank 1, the Galois group is a subgroup of $\mathrm{GL}_1 = \mathbb{G}_m$. Hence, the Galois group is $\mathbb{G}_m$ or one of the groups μ_n of n-th roots of unity. The Galois group is $\mathbb{G}_m$ if y is transcendental over S, and it is μ_n if n is the least positive integer such that $y^n \in S$.

Whether y is transcendental over S or not, depends on the choice of b.

1. If we take, $b = \frac{-3st}{3s^2-1}$, then $\partial(y) = \frac{t}{(3s^2-1)s}y$, and hence

$$\partial\left(\frac{y^2}{s}\right) = \frac{2y\partial(y)}{s} - \frac{y^2\partial(s)}{s^2} = 0.$$

   Therefore, $\frac{y^2}{s}$ is a constant, i.e. y is a square root in $C[[t]]$ of cs for some $0 \neq c \in C$. Actually, any $c \neq 0$ such that cs is a square in $C[[t]]$ will do, as different choices just correspond to different choices of the constant basis e. As in $C[[t]]$, $s \equiv 1 \mod t$, there exists a square root $\sqrt{s} \in C[[t]]$ of s with $\sqrt{s} \equiv 1 \mod t$. Hence, we can choose $c = 1$, and $y = \sqrt{s}$, and obtain

$$R = S\left[\sqrt{s}, \frac{t}{\sqrt{s}}\right],$$

   an extension of degree 2 and Galois group μ_2.

   If we would have taken the maximal ideal to be $\mathfrak{m} = (s+1, t)$, and the corresponding embedding $S \hookrightarrow (S/\mathfrak{m})[[t]] \cong C[[t]]$, then in the last step $s \equiv -1 \mod t$ inside $C[[t]]$, and we have a square root $\sqrt{-s}$ of $-s$ in $C[[t]]$ with $\sqrt{-s} \equiv 1 \mod t$. This leads to the Picard-Vessiot ring

$$R_2 = S\left[\sqrt{-s}, \frac{t}{\sqrt{-s}}\right],$$

   which is not isomorphic as an S-algebra to R above, if -1 is not a square in $C^\times$. The Galois group, however, is again μ_2.

2. If we take, $b = 0$, then inside $\mathrm{Quot}(S)$ we have

$$\partial\left(\frac{y}{s}\right) = \frac{\partial(y)}{s} - y\frac{\partial(s)}{s^2} = \frac{(3s^2+1)t}{(3s^2-1)s}\frac{y}{s} - \frac{2t}{(3s^2-1)s}\frac{y}{s} = \frac{t}{s}\frac{y}{s}$$

If $\frac{y}{s}$ was not transcendental over Quot(S), then some n-th power $w = \left(\frac{y}{s}\right)^n$ would be in Quot(S). For w we get the differential equation

$$\partial(w) = \frac{nt}{s} w.$$

Writing $w = w_0(s) + w_1(s)t$ with $w_0, w_1 \in C(s)$, we calculate

$$\begin{aligned} \partial(w) &= \partial(w_0(s)) + \partial(w_1(s))t + w_1(s) \\ &= w_0'(s)\frac{2t}{3s^2-1} + w_1'(s)\frac{2t}{3s^2-1}t + w_1(s) \\ &= \left(w_1(s) + w_1'(s)\frac{2(s^3-s)}{3s^2-1}\right) + \frac{2w_0'(s)}{3s^2-1}t, \end{aligned}$$

as well as

$$\frac{nt}{s} w = \frac{nt}{s} w_0(s) + \frac{nt^2}{s} w_1(s) = n(s^2-1)w_1(s) + \frac{nw_0(s)}{s} t.$$

Here $w_0'(s)$ and $w_1'(s)$ denote the usual derivatives of rational functions. By comparing coefficients of t, we obtain

$$\begin{aligned} \frac{nw_0(s)}{s} &= \frac{2w_0'(s)}{3s^2-1} \quad \text{and} \\ (ns^2 - n - 1)w_1(s) &= w_1'(s)\frac{2(s^3-s)}{3s^2-1}. \end{aligned}$$

If $w_0, w_1 \neq 0$, this implies

$$\deg_s(w_0(s)) = \deg_s\left(\frac{nw_0(s)}{s}\right) + 1 = \deg_s\left(\frac{2w_0'(s)}{3s^2-1}\right) + 1 = \deg_s(w_0'(s)) - 1,$$

and

$$\begin{aligned} \deg_s(w_1(s)) &= \deg_s\left((ns^2-n-1)w_1(s)\right) - 2 \\ &= \deg_s\left(w_1'(s)\frac{2(s^3-s)}{3s^2-1}\right) - 2 = \deg_s(w_1'(s)) - 1. \end{aligned}$$

But $\deg_s(f'(s)) \leq \deg_s(f(s)) - 1$ for all $0 \neq f(s) \in C(s)$, and hence $w_0(s) = w_1(s) = 0$, i.e. $w = 0$ which is impossible.
Hence, there is no such w, and $\frac{y}{s}$ and also y are transcendental over S.

3.7.4 A non-free ID-module over S in positive characteristic

Finding an example in positive characteristic is harder, since one is not done by giving just $\theta_M^{(1)}$, but by giving all $\theta_M^{(p^j)}$ which moreover have to commute and have to be nilpotent of order p.

We will follow a different approach here. We start with the example in characteristic zero given in the previous paragraph.

The iterative derivation on $C[t]$ is already defined on $\mathbb{Z}[t]$ and extends to the ring $S_{\mathbb{Z}} := \mathbb{Z}[s,t,\frac{1}{3s^2-1}]/(s^3-s-t^2)$, since the latter is étale over the former.

Therefore, the ID-ring S from above (with constants C) is obtained as $S = C \otimes_{\mathbb{Z}} S_{\mathbb{Z}}$. And this holds in any characteristic. For constructing an ID-module M over S, one can start with a projective module M' over $S_{\mathbb{Z}}$, and define a derivation on $M := S \otimes_{S_{\mathbb{Z}}} M'$. If the corresponding iterative derivation stabilizes M', one can reduce modulo p, to obtain an iterative derivation on M'/pM'. This is then an ID-module over $\mathbb{F}_p \otimes_{\mathbb{Z}} S_{\mathbb{Z}}$.

Therefore take the ID-module over $S_{\mathbb{Q}}$ from above with $b = \frac{-3st}{3s^2-1}$. Then we know that $e = \frac{1}{y} f_1$ is a constant basis of $R \otimes M$, where $y = \sqrt{s}$.

Hence, $\theta_M(f_1) = \theta_M(ye) = \theta(y)e = \frac{\theta(y)}{y} f_1$. Replacing y by $\sqrt{s}$ and using the chain rule (cf. [Rös07, Prop. 7.2]) one obtains:

$$\theta(\sqrt{s}) = \theta_s(\sqrt{s})|_{T=\theta(s)-s} = (s+T)^{\frac{1}{2}}|_{T=\theta(s)-s} = \sqrt{s} \cdot \sum_{k=0}^{\infty} \binom{1/2}{k} \left(\frac{\theta(s)}{s} - 1\right)^k.$$

Therefore, all appearing rational numbers only have powers of 2 in the denominator, and we can reduce modulo any prime p different from 2, obtaining a non-free ID-module in characteristic p.

Chapter 4

Finite inverse problem in iterative differential Galois theory

chap:finite-inverse

In this chapter, we prove a necessary and sufficient condition to decide whether a finite group scheme occurs as Galois group scheme of a PicardVessiot extension over a given ID-field or not. In particular, this solves the inverse ID-Galois problem for finite group schemes. Furthermore, the part on infinitesimal group schemes gives a tool to tell whether all purely inseparable ID-extensions are in fact PicardVessiot extensions.

This part is published in [Mau10b] and [Mau13]. Take care that the Picard-Vessiot rings and fields were called pseudo Picard-Vessiot rings and pseudo Picard-Vessiot fields in[Mau10b], since at that time the point theoretic definition of Galois extensions was more popular.

In this part, we are even dealing with several commuting iterative derivations (called multivariate iterative derivations) instead of only one iterative derivation, because the general case is not more difficult than the special case of one iterative derivation.

4.1 Basic notation

basics

All rings are assumed to be commutative with unit. We use the usual notation for multiindices, namely $\binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}} = \prod_{\mu=1}^{m} \binom{i_\mu+j_\mu}{i_\mu}$ and $\boldsymbol{T}^{\boldsymbol{i}} = T_1^{i_1} T_2^{i_2} \cdots T_m^{i_m}$ for $\boldsymbol{i} = (i_1, \ldots, i_m), \boldsymbol{j} = (j_1, \ldots, j_m) \in \mathbb{N}^m$ and $\boldsymbol{T} = (T_1, \ldots, T_m)$.

An **m-variate iterative derivation** on a ring R is a homomorphism of rings $\theta : R \to R[[T_1, \ldots, T_m]]$, such that $\theta^{(\boldsymbol{0})} = \mathrm{id}_R$ and for all $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^m$, $\theta^{(\boldsymbol{i})} \circ \theta^{(\boldsymbol{j})} = \binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}} \theta^{(\boldsymbol{i}+\boldsymbol{j})}$, where the maps $\theta^{(\boldsymbol{i})} : R \to R$ are defined by $\theta(r) =: \sum_{\boldsymbol{i} \in \mathbb{N}^m} \theta^{(\boldsymbol{i})}(r) \boldsymbol{T}^{\boldsymbol{i}}$ (cf. [Hei07], Ch. 4). In the case $m = 1$ this is equivalent to the usual definition of an iterative derivation used earlier here. The pair (R, θ) is then called an ID-ring and $C_R := \{r \in R \mid \theta(r) = r\}$ is called the **ring of constants** of (R, θ). An ideal $I \trianglelefteq R$ is called an **ID-ideal** if $\theta(I) \subseteq I[[\boldsymbol{T}]]$ and R is **ID-simple** if R has no nontrivial ID-ideals. Iterative derivations are extended to localizations by $\theta(\frac{r}{s}) := \theta(r)\theta(s)^{-1}$ and to tensor products by

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

for all $\boldsymbol{k} \in \mathbb{N}^m$. The m-variate iterative derivation θ is called **non-degenerate** if the m additive maps $\theta^{(1,0,\ldots,0)}, \theta^{(0,1,0,\ldots,0)}, \ldots, \theta^{(0,\ldots,0,1)}$ (which actually are derivations on R) are R-linearly independent.

Given an ID-ring (R, θ_R) over an ID-field (F, θ), we call an element $x \in R$ **differentially finite over** F if the F-vector space spanned by all $\theta^{(\boldsymbol{k})}(x)$ ($\boldsymbol{k} \in \mathbb{N}^m$) is finite dimensional - quite as we did in Section 3.1. The same calculation as in the proof of Corollary 3.3.6 shows that the set of elements which are differentially finite over F form an ID-subring of R that contains F.

rem-on-IDs

Remark 4.1.1. (see also [Hei07], Ch. 4)

Given an m-variate iterative derivation θ on a ring R, one obtains a set of m (1-variate) iterative derivations $\theta_1, \ldots, \theta_m$ by defining

$$\theta_1^{(k)} := \theta^{(k,0,\ldots,0)}, \quad \theta_2^{(k)} := \theta^{(0,k,0,\ldots,0)}, \quad \ldots, \quad \theta_m^{(k)} := \theta^{(0,\ldots,0,k)}$$

for all $k \in \mathbb{N}$. By the iteration rule for θ these iterative derivations commute, i. e. satisfy the condition $\theta_i^{(k)} \circ \theta_j^{(l)} = \theta_j^{(l)} \circ \theta_i^{(k)}$ for all $i, j \in \{1, \ldots, m\}, k, l \in \mathbb{N}$. On the other hand, given m commuting 1-variate iterative derivations $\theta_1, \ldots, \theta_m$ one obtains an m-variate iterative derivation θ by defining

$$\theta^{(\boldsymbol{k})} := \theta_1^{(k_1)} \circ \cdots \circ \theta_m^{(k_m)}$$

for all $\boldsymbol{k} = (k_1, \ldots, k_m) \in \mathbb{N}^m$.

Using the iteration rule one sees that the m-variate iterative derivation θ is determined by the derivations $\theta_1^{(1)}, \ldots, \theta_m^{(1)}$ if the characteristic of R is zero, and by the set of maps $\{\theta_1^{(p^\ell)}, \ldots, \theta_m^{(p^\ell)} \mid \ell \in \mathbb{N}\}$ if the characteristic of R is $p > 0$. Furthermore, θ is non-degenerate if and only if for all $j = 1, \ldots, m$ the derivation $\theta_j^{(1)}$ is nontrivial on $\bigcap_{i=1}^{j-1} \operatorname{Ker}(\theta_i^{(1)})$.

Notation *From now on, (F, θ) denotes an ID-field of positive characteristic p, and $C = C_F$ its field of constants. We assume that C is perfect, and that the m-variate iterative derivation θ is non-degenerate.*

With these assumptions, the derivations $\theta_1^{(1)}, \ldots, \theta_m^{(1)}$ are nilpotent C_F-endomorphisms of F. Since they commute and θ is non-degenerate, there exist $x_1, \ldots, x_m \in F$ such that $\theta_i^{(1)}(x_j) = \delta_{ij}$ for all i, j, where δ_{ij} denotes the Kronecker delta. Therefore $\{x_1^{e_1} \cdots x_m^{e_m} \mid 0 \leq e_j \leq p-1\}$ is a basis of F as a vector space over $F_1 := \bigcap_{i=1}^m \operatorname{Ker}(\theta_i^{(1)})$. Hence F/F_1 is a field extension of degree p^m. Furthermore, the maps $\theta_1^{(p)}, \ldots, \theta_m^{(p)}$ are derivations on F_1, they also are nilpotent and commute, and

$$\theta_i^{(p)}(x_j^p) = \left(\theta_i^{(1)}(x_j)\right)^p = \delta_{ij}.$$

So by the same argument, F_1 is a vector space over $F_2 := F_1 \cap \bigcap_{i=1}^m \operatorname{Ker}(\theta_i^{(p)})$ and $[F_1 : F_2] = p^m$. Repeating this, one obtains a descending sequence of subfields $F_\ell := F_{\ell-1} \cap \bigcap_{i=1}^m \operatorname{Ker}(\theta_i^{(p^{\ell-1})})$ satisfying $[F_{\ell-1} : F_\ell] = p^m$.

This sequence will be useful in Section 4.3.

Definition 4.1.2.
Let (F, θ) be an ID-field, and let $A = \sum_{\boldsymbol{k} \in \mathbb{N}^m} A_{\boldsymbol{k}} \boldsymbol{T}^{\boldsymbol{k}} \in \mathrm{GL}_n(F[[\boldsymbol{T}]])$ be a matrix satisfying the properties $A_{\boldsymbol{0}} = \mathbb{1}_n$ and $\binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{l}} A_{\boldsymbol{k}+\boldsymbol{l}} = \sum_{\boldsymbol{i}+\boldsymbol{j}=\boldsymbol{l}} \theta^{(\boldsymbol{i})}(A_{\boldsymbol{k}}) A_{\boldsymbol{j}}$ for all $\boldsymbol{k}, \boldsymbol{l} \in \mathbb{N}^m$. Then an equation

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

where $\boldsymbol{y}$ is a vector of indeterminants, is called an **iterative differential equation** (IDE) over F.[1]

[1] As before, iterative derivations are applied componentwise to vectors and matrices.

Picard-Vessiot rings in this setting are defined the same way as in the univariate setting. There is also the following explicit description.

Definition 4.1.3. An ID-ring $(R, \theta_R) \geq (F, \theta)$ is called a **Picard-Vessiot ring** (PV-ring) for $\theta(\boldsymbol{y}) = A\boldsymbol{y}$ if the following holds:

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

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

`ide-condition`

Remark 4.1.4. The condition on the $A_{\boldsymbol{k}}$ given in the definition of the IDE is equivalent to the condition that $\theta_R^{(\boldsymbol{k})}(\theta_R^{(\boldsymbol{l})}(Y_{ij})) = \binom{\boldsymbol{k}+\boldsymbol{l}}{\boldsymbol{k}} \theta_R^{(\boldsymbol{k}+\boldsymbol{l})}(Y_{ij})$ holds for a fundamental solution matrix $Y = (Y_{ij})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(R)$.

Furthermore, the condition $A_{\boldsymbol{0}} = \mathbb{1}_n$ already implies that the matrix A is invertible.

A PV-ring has a nice characterization inside the PV-field.

`diff-finite`

Proposition 4.1.5. *Let (R, θ_R) be a PV-ring over F for an IDE $\theta(\boldsymbol{y}) = A\boldsymbol{y}$ and $E = \mathrm{Quot}(R)$. Then R is equal to the set of elements in E which are differentially finite over F.*

Proof. (Compare [Mat01], Thm. 4.9, for the case when C is algebraically closed and θ is univariate.)
Let $Y \in \mathrm{GL}_n(R)$ be a fundamental solution matrix for the IDE. Then by definition $\theta^{(\boldsymbol{k})}(Y) = A_{\boldsymbol{k}} Y$ and hence for all i, j and all $\boldsymbol{k} \in \mathbb{N}^m$ the derivatives $\theta^{(\boldsymbol{k})}(Y_{ij})$ are in the F-vector space spanned by all Y_{ij}, i. e. all Y_{ij} are differentially finite. Furthermore, one has $\theta(\det(Y)^{-1}) = \det(\theta(Y))^{-1} = \det(AY)^{-1} = \det(A)^{-1} \det(Y)^{-1}$, i. e. $\det(Y)^{-1}$ is differentially finite. Therefore, R is generated by differentially finite elements, and since the differentially finite elements form a ring, all elements of R are differentially finite.

On the other hand, let $x \in E$ be differentially finite over F and let $W_F(x)$ be the F-vector space spanned by all $\theta^{(\boldsymbol{k})}(x)$ ($\boldsymbol{k} \in \mathbb{N}^m$). Then the set $I_x := \{r \in R \mid r \cdot W_F(x) \subseteq R\}$ is an ID-ideal of R. Since $W_F(x)$ is finite dimensional and E is the quotient field of R, one has $I_x \neq 0$. Since R is ID-simple, this implies $I_x = R$. Hence $1 \cdot W_F(x) \subseteq R$, and in particular $1 \cdot x = x \in R$. □

From this characterization of the PV-ring as the ring of differentially finite elements, we immediately get the following.

unique-PV-ring

Corollary 4.1.6. *Let E be a PV-field over F for several IDEs. Then the PV-ring inside E is unique and independent of the particular IDE.*

4.2 Galois theory

galois-theory

The Galois theory for a PV-extension works the same as in the univariate case, since it is also an instance of the abstract setting.

However, as in the classical differential setting, we get a full Galois correspondence using the PV-field.

For a PV-ring R/F the Galois group scheme is again defined as the functor

$$\underline{\mathrm{Gal}}(R/F) : \mathsf{Alg}_C \to \mathsf{Groups}, L \mapsto \mathrm{Aut}^{\mathrm{ID}}(R \otimes_C L/F \otimes_C L)$$

where L is provided with the trivial iterative derivation, i. e. the iterative derivation on L given by $a \mapsto a \in L \subseteq L[[\boldsymbol{T}]]$.

As before (see also [Mau10a], Sect. 10) the functor $\mathcal{G} := \underline{\mathrm{Gal}}(R/F)$ is representable by a C-algebra of finite type and hence $\mathcal{G}$ is an affine group scheme of finite type over C. We sometimes also refer to it as the Galois group scheme of the extension E over F, $\underline{\mathrm{Gal}}(E/F)$, where $E = \mathrm{Quot}(R)$ is the corresponding PV-field. This is justified by the fact given in Corollary 4.1.6 that the PV-ring can be recovered from the PV-field without regarding an IDE. Also take care that the functor $\underline{\mathrm{Aut}}^{\mathrm{ID}}(E/F)$ is not isomorphic to $\underline{\mathrm{Aut}}^{\mathrm{ID}}(R/F)$. Hence the Galois group scheme of E/F has to be defined using the PV-ring.

Directly from the abstract setting, we get that $\mathrm{Spec}(R)$ is a $(\mathcal{G} \times_C F)$-torsor and the corresponding isomorphism of rings

$$\gamma : R \otimes_F R \to R \otimes_C C[\mathcal{G}] \tag{4.1}$$

is an R-linear ID-isomorphism. Here again, $C[\mathcal{G}]$ is equipped with the trivial iterative derivation, and equals $C_{R \otimes_F R}$.

For later use, we remark that the comultiplication on $C[\mathcal{G}]$ is induced via the isomorphism γ by the map

$$R \otimes_F R \longrightarrow (R \otimes_F R) \otimes_R (R \otimes_F R), a \otimes b \mapsto (a \otimes 1) \otimes (1 \otimes b),$$

and the counit map $ev : C[\mathcal{G}] \to C$ is induced by the multiplication

$$R \otimes_F R \longrightarrow R, a \otimes b \mapsto ab.$$

(see also [Tak89]).

We recall that for a subgroup functor $\mathcal{H} \leq \mathcal{G}$, an element $r \in R$ is called **invariant** under $\mathcal{H}$ if for all L, the element $r \otimes 1 \in R_L$ is invariant under $\mathcal{H}(L)$. The ring of invariants is denoted by $R^{\mathcal{H}}$. (In [Jan03], I.2.10 the invariant elements are called "fixed points".)

More generally, let $E = \mathrm{Quot}(R)$ be the quotient field and for all L let $\mathrm{Quot}(R \otimes_C L)$ be the localization by all nonzero divisors. Since every automorphism of $R \otimes_C L$ extends uniquely to an automorphism of $\mathrm{Quot}(R \otimes_C L)$, the functor $\underline{\mathrm{Aut}}(R/F)$ is a subgroup functor of the group functor

$$\mathsf{Alg}_C \to \mathsf{Groups}, L \mapsto \mathrm{Aut}(\mathrm{Quot}(R \otimes_C L)/\,\mathrm{Quot}(F \otimes_C L)).$$

In this sense, we call an element $e = \frac{r}{s} \in E$ **invariant** under $\mathcal{H}$, if for all C-algebras L and all $h \in \mathcal{H}(L)$,

$$\frac{h(r \otimes 1)}{h(s \otimes 1)} = \frac{r \otimes 1}{s \otimes 1} = e \otimes 1.$$

The ring of invariants of E is denoted by $E^{\mathcal{H}}$.

rho

Remark 4.2.1. The action of $\mathcal{G} := \underline{\mathrm{Gal}}(R/F)$ on R is fully described by the ID-homomorphism $\rho := \gamma|_{1 \otimes R} : R \to R \otimes_C C[\mathcal{G}]$. Namely, for a C-algebra L and $g \in \mathcal{G}(L)$ with corresponding $\tilde{g} \in \mathrm{Hom}(C[\mathcal{G}], L)$, one has $g(r \otimes 1) = (1 \otimes \tilde{g})(\rho(r)) \in R \otimes_C L$ for all $r \in R$.

Similar to Proposition 3.6.5 we have

Proposition 4.2.2. *Let E/F be a PV-extension with PV-ring R and Galois group scheme $\mathcal{G}$. An ID-field $\tilde{F}$, with $F \leq \tilde{F} \leq E$, is a PV-field over F, if and only if it is stable under the action of $\mathcal{G}$, i. e. if $\rho(R \cap \tilde{F}) \subseteq (R \cap \tilde{F}) \otimes C[\mathcal{G}]$.*

Proof. If $\tilde{F}$ is a PV-field, its PV-ring $\tilde{R}$ is the set of elements in $\tilde{F}$ which are differentially finite over F (cf. Prop 4.1.5), in particular we have $\tilde{R} = \tilde{F} \cap R$. Hence we obtain a commutative diagram:

$$\begin{array}{ccc} \tilde{R} \otimes_F \tilde{R} & \xrightarrow{\cong} & \tilde{R} \otimes_C C[\underline{\mathrm{Gal}}(\tilde{R}/F)] = \tilde{R} \otimes_C C_{\tilde{R} \otimes_F \tilde{R}} \\ \downarrow & & \downarrow \\ R \otimes_F R & \xrightarrow{\cong} & R \otimes_C C[\mathcal{G}] = R \otimes_C C_{R \otimes_F R}\ , \end{array}$$

where the vertical maps are induced by the inclusion $\tilde{R} \subseteq R$, and the horizontal maps are the isomorphisms γ for $\tilde{R}$ respectively for R. But this implies $\rho(\tilde{R}) \subseteq \tilde{R} \otimes_C C_{\tilde{R} \otimes_F \tilde{R}} \subseteq \tilde{R} \otimes_C C[\mathcal{G}]$, i. e. $\tilde{F}$ is stable under the action of $\mathcal{G}$.

The converse is stated in Theorem 4.2.3,iii). □

galois_correspondence

Theorem 4.2.3. (Galois correspondence) *Let E/F be a PV-extension with PV-ring R and Galois group scheme $\mathcal{G}$.*

1. *There is an antiisomorphism of the lattices*

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

and

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

given by $\Psi : \mathfrak{H} \to \mathfrak{M}, \mathcal{H} \mapsto E^{\mathcal{H}}$ *and* $\Phi : \mathfrak{M} \to \mathfrak{H}, M \mapsto \underline{\mathrm{Gal}}(E/M)$.

normal_subgroup

2. *If* $\mathcal{H} \leq \mathcal{G}$ *is normal, then* $E^{\mathcal{H}} = \mathrm{Quot}(R^{\mathcal{H}})$ *and* $R^{\mathcal{H}}$ *is a PV-ring over* F *with Galois group scheme* $\underline{\mathrm{Gal}}(R^{\mathcal{H}}/F) \cong \mathcal{G}/\mathcal{H}$.

3. *If* $M \in \mathfrak{M}$ *is stable under the action of* $\mathcal{G}$*, then* $\mathcal{H} := \Phi(M)$ *is a normal subgroup scheme of* $\mathcal{G}$*,* M *is a PV-extension of* F *and* $\underline{\mathrm{Gal}}(M/F) \cong \mathcal{G}/\mathcal{H}$.

4. *For* $\mathcal{H} \in \mathfrak{H}$*, the extension* $E/E^{\mathcal{H}}$ *is separable if and only if* $\mathcal{H}$ *is reduced.*

Proof. See [Mau10a], Thm. 11.5. □

4.3 Purely inseparable extensions

purely-insep

As in the previous section, F denotes a field of positive characteristic p with a non-degenerate m-variate iterative derivation θ and a perfect field of constants $C = C_F$.

Recall that a field extension E/F is **purely inseparable**, if for every $r \in E$ there exists $e \in \mathbb{N}$ such that $r^{p^e} \in F$, where p denotes the characteristic of F. The minimal number $e \in \mathbb{N}$ such that $r^{p^e} \in F$ for all $r \in E$ (if it exists) is called the **exponent** of the extension, and is denoted by $\mathrm{e}(E/F)$. In our cases, E/F is finitely generated – and therefore finite – and so the exponent $\mathrm{e}(E/F)$ exists.

An affine group scheme $\mathcal{G}$ over C is called **infinitesimal**, if the kernel of the counit map $ev : C[\mathcal{G}] \to C$, denoted by $C[\mathcal{G}]^+$, contains only nilpotent elements. The minimal number $h \in \mathbb{N}$ such that $x^{p^h} = 0$ for all $x \in C[\mathcal{G}]^+$ (if it exists) is called the **height** of $\mathcal{G}$, denoted by $\mathrm{h}(\mathcal{G})$. In our cases, $\mathcal{G}$ is of finite type over C, so $C[\mathcal{G}]$ is a finitely generated C-algebra, and the height $\mathrm{h}(\mathcal{G})$ exists.

Examples of infinitesimal group schemes are given by Frobenius kernels. For example for any $\ell \in \mathbb{N}$, $\boldsymbol{\alpha}_{p^\ell} := \mathrm{Ker}(\mathbb{G}_a \to \mathbb{G}_a, a \mapsto a^{p^\ell})$ is an infinitesimal group scheme with coordinate ring $C[\boldsymbol{\alpha}_{p^\ell}] \cong C[X]/X^{p^\ell}$, and $\boldsymbol{\mu}_{p^\ell} := \mathrm{Ker}(\mathbb{G}_m \to \mathbb{G}_m, a \mapsto a^{p^\ell})$ is an infinitesimal group scheme with coordinate ring $C[\boldsymbol{\mu}_{p^\ell}] \cong C[X, \frac{1}{X}]/(X^{p^\ell} - 1)$.

infinitesimal_group

Corollary 4.3.1. *Let* E/F *be a PV-extension with Galois group scheme* $\mathcal{G}$*. Then* E/F *is a purely inseparable extension if and only if* $\mathcal{G}$ *is an infinitesimal group scheme. In this case, the exponent* $\mathrm{e}(E/F)$ *and the height* $\mathrm{h}(\mathcal{G})$ *are equal.*

Proof. Let $\mathcal{G}$ be infinitesimal of height h and let $ev : C[\mathcal{G}] \to C$ denote the counit map corresponding to the neutral element $1_{\mathcal{G}}$ of the group. Then by Remark 4.2.1, for any $\frac{r}{s} \in E$, we have

$$(\mathrm{id} \otimes ev)(\gamma(r \otimes s - s \otimes r)) = (r \otimes 1)1_{\mathcal{G}}(s) - (s \otimes 1)1_{\mathcal{G}}(r) = rs - sr = 0,$$

that is $\gamma(r \otimes s - s \otimes r) \in R \otimes_C C[\mathcal{G}]^+$. Since $\mathcal{G}$ is of height h, we obtain $(r \otimes s - s \otimes r)^{p^h} = 0$. Therefore $r^{p^h} \otimes s^{p^h} = s^{p^h} \otimes r^{p^h} \in R \otimes_F R$ which means that $\frac{r^{p^h}}{s^{p^h}} \in F$. So E/F is purely inseparable of exponent $\leq h$. On the other hand, let E/F be purely inseparable of exponent e. For arbitrary $x \in C[\mathcal{G}]^+$, let $\gamma^{-1}(1 \otimes x) =: \sum_j r_j \otimes s_j$. Then

$$1 \otimes x^{p^e} = \gamma\left(\sum_j r_j^{p^e} \otimes s_j^{p^e}\right) = \gamma\left(\sum_j r_j^{p^e} s_j^{p^e} \otimes 1\right) = \sum_j r_j^{p^e} s_j^{p^e} \otimes 1.$$

Hence (e.g. by applying $\mathrm{id} \otimes ev$), one obtains $\sum_j r_j^{p^e} s_j^{p^e} = 0$ and $x^{p^e} = 0$. Therefore $\mathcal{G}$ is infinitesimal of height $\leq e$. □

Notation *For all $\ell \in \mathbb{N}$, let $J_\ell := \left\{(j_1, \ldots, j_m) \in \mathbb{N}^m \setminus \{\mathbf{0}\} \mid \forall\, i : j_i < p^\ell\right\}$ and let*

$$F_\ell := \bigcap_{\boldsymbol{j} \in J_\ell} \mathrm{Ker}(\theta_F^{(\boldsymbol{j})}).$$

Actually, the subfields F_ℓ are the same as the ones defined in Remark 4.1.1.

Since $\theta_F(F_\ell) \subseteq F_\ell[[T_1^{p^\ell}, \ldots, T_m^{p^\ell}]]$, one obtains an iterative derivation on $F_{[\ell]} := (F_\ell)^{p^{-\ell}}$ by $\theta_{F_{[\ell]}}(x) := \left(\theta_F(x^{p^\ell})\right)^{p^{-\ell}}$. This is the unique iterative derivation which turns $F_{[\ell]}$ into an ID-extension of F, since every such iterative derivation has to coincide with θ_F on F_ℓ.

leq-ell

max-id-extension

Proposition 4.3.2. *1. For all $\ell \in \mathbb{N}$, $F_{[\ell]}$ is the unique maximal purely inseparable ID-extension of F of exponent $\leq \ell$.*

formula

2. For all $\ell_1, \ell_2 \in \mathbb{N}$, $(F_{[\ell_1]})_{[\ell_2]} = F_{[\ell_1+\ell_2]}$.

trivial

3. If $F_{[1]} = F$ then $F_{[\ell]} = F$ for all $\ell \in \mathbb{N}$.

eq-ell

4. If $F_{[1]} \neq F$ and θ is non-degenerate, then for all $\ell \in \mathbb{N}$, the exponent of $F_{[\ell]}/F$ is exactly ℓ.

Proof. For the proof of part 1, we have already seen that $F_{[\ell]}/F$ is an ID-extension, and by definition it is purely inseparable of exponent $\leq \ell$. If E is a purely inseparable ID-extension of F of exponent $\leq \ell$, then $E^{p^\ell} \subseteq F \cap E_\ell \subseteq F_\ell$ and therefore $E \subseteq F_{[\ell]}$. Hence $F_{[\ell]}$ is the unique maximal ID-extension of this kind.

By definition $(F_{[\ell_1]})_{[\ell_2]}$ is an ID-extension of F of exponent $\leq \ell_1 + \ell_2$. Hence by part 1, we have $(F_{[\ell_1]})_{[\ell_2]} \subseteq F_{[\ell_1+\ell_2]}$. On the other hand $\left(F_{[\ell_1+\ell_2]}\right)^{p^{\ell_1+\ell_2}} \subseteq F$ and so $\left(F_{[\ell_1+\ell_2]}\right)^{p^{\ell_2}} \subseteq F_{[\ell_1]}$. Hence $F_{[\ell_1+\ell_2]}$ is an ID-extension of $F_{[\ell_1]}$ of exponent $\leq \ell_2$ and therefore contained in $(F_{[\ell_1]})_{[\ell_2]}$. This proves part 2.

Part 3 is a direct consequence of part 2. So it remains to prove 4. For this it suffices to show that $F_{[\ell+1]} \neq F_{[\ell]}$ for all ℓ, because this implies that $\mathrm{e}(F_{[\ell]}/F) \geq \mathrm{e}(F_{[\ell-1]}/F) + 1 \geq \cdots \geq \mathrm{e}(F_{[1]}/F) + \ell - 1 = \ell$.

By Remark 4.1.1, one has $\dim_{F_{\ell+1}}(F_\ell) = p^m$, since θ is non-degenerate. Assume that $F_{[\ell+1]} = F_{[\ell]}$. Then $F_{\ell+1} = \left(F_{[\ell+1]}\right)^{p^{\ell+1}} = \left(F_{[\ell]}\right)^{p^{\ell+1}} = (F_\ell)^p$ and therefore F is a finite extension of $(F_\ell)^p$ of degree $[F : (F_\ell)^p] = [F : F_{\ell+1}] = p^{(\ell+1)m}$. On the other hand,

$$[F : (F_\ell)^p] = [F : F^p] \cdot [F^p : (F_\ell)^p] = [F : F^p] \cdot [F : F_\ell] = p^{\ell m}[F : F^p].$$

Hence $[F : F^p] = p^m = [F : F_1]$, and $F_1 = F^p$, in contradiction to $F_{[1]} \neq F$. □

frob-pullback

Theorem 4.3.3. *Let E/F be a PV-extension and let $\ell \in \mathbb{N}$. Then $E_{[\ell]}/F_{[\ell]}$ is a PV-extension, and its Galois group scheme is related to $\underline{\mathrm{Gal}}(E/F)$ by $(\mathbf{Frob}^\ell)^* \left(\underline{\mathrm{Gal}}(E_{[\ell]}/F_{[\ell]})\right) \cong \underline{\mathrm{Gal}}(E/F)$, where* **Frob** *denotes the Frobenius morphism on* $\mathrm{Spec}(C)$.

Proof. Let $R \subseteq E$ be the corresponding PV-ring and $Y \in \mathrm{GL}_n(R)$ a fundamental solution matrix for a corresponding IDE $\theta(\boldsymbol{y}) = A\boldsymbol{y}$. Since the m-variate iterative derivation is non-degenerate on F, on has $[F : F_\ell] = p^{m\ell} = [E : E_\ell]$. Hence, there is a matrix $D \in \mathrm{GL}_n(F)$ such that $\tilde{Y} := D^{-1}Y \in \mathrm{GL}_n(R_\ell)$. The matrix $\tilde{Y}$ satisfies

$$\theta(\tilde{Y}) = \theta(D^{-1}Y) = \theta(D)^{-1}AD\tilde{Y},$$

that is, it is a fundamental solution matrix for the IDE $\theta(\boldsymbol{y}) = \tilde{A}\boldsymbol{y}$, where $\tilde{A} = \theta(D)^{-1}AD \in \mathrm{GL}_n(F[[\boldsymbol{T}]])$.

We first show that $\tilde{A} \in \mathrm{GL}_n(F_\ell[[T_1^{p^\ell}, \ldots, T_m^{p^\ell}]])$: Clearly $\tilde{A} \in \mathrm{GL}_n(F[[\boldsymbol{T}^{p^\ell}]])$, since $\theta^{(\boldsymbol{k})}(\tilde{Y}) = 0$ for all $\boldsymbol{k} \in J_\ell$ and since θ is iterative. Then for all $\boldsymbol{j} \in \mathbb{N}^m$ and all $\boldsymbol{k} \in J_\ell$ we have

$$\theta^{(\boldsymbol{k})}\left(\theta^{(\boldsymbol{j})}(\tilde{Y})\right) = \theta^{(\boldsymbol{j})}\left(\theta^{(\boldsymbol{k})}(\tilde{Y})\right) = 0,$$

and

$$\theta^{(\boldsymbol{k})}\left(\theta^{(\boldsymbol{j})}(\tilde{Y})\right) = \theta^{(\boldsymbol{k})}\left(\tilde{A}_{\boldsymbol{j}} \cdot \tilde{Y}\right) = \theta^{(\boldsymbol{k})}(\tilde{A}_{\boldsymbol{j}})\tilde{Y}.$$

Hence, $\theta^{(\boldsymbol{k})}(\tilde{A}_{\boldsymbol{j}}) = 0$. Therefore $\tilde{A}_{\boldsymbol{j}}$ has coefficients in F_ℓ.

Since $\tilde{A} \in \mathrm{GL}_n(F_\ell[[\boldsymbol{T}^{p^\ell}]])$, R_ℓ is actually a PV-ring over F_ℓ with fundamental solution matrix $\tilde{Y}$. By taking p^ℓ-th roots, we obtain that $R_{[\ell]}$ is a PV-ring over $F_{[\ell]}$ with fundamental solution matrix $\left((\tilde{Y}_{i,j})^{p^{-\ell}}\right)_{i,j}$.

For obtaining the relation between the Galois groups, we first observe that F and R_ℓ are linearly disjoint over F_ℓ and hence $F \otimes_{F_\ell} R_\ell \cong R$, which induces a natural isomorphism of the Galois groups $\underline{\mathrm{Gal}}(R/F) \cong \underline{\mathrm{Gal}}(R_\ell/F_\ell)$.

Furthermore the p^ℓ-th power Frobenius endomorphism leads to an isomorphism

$$R_{[\ell]} \otimes_{F_{[\ell]}} R_{[\ell]} \xrightarrow{()^{p^\ell}} R_\ell \otimes_{F_\ell} R_\ell.$$

Since $\underline{\mathrm{Gal}}(R_\ell/F_\ell)$ (resp.$\underline{\mathrm{Gal}}(R_{[\ell]}/F_{[\ell]})$ is isomorphic as C-group scheme to $\mathrm{Spec}(C_{R_\ell \otimes_{F_\ell} R_\ell})$ (resp. $\mathrm{Spec}(C_{R_{[\ell]} \otimes_{F_{[\ell]}} R_{[\ell]}})$), this gives the desired property

$$(\mathbf{Frob}^\ell)^* \left(\underline{\mathrm{Gal}}(E_{[\ell]}/F_{[\ell]})\right) \cong \underline{\mathrm{Gal}}(E_\ell/F_\ell) \cong \underline{\mathrm{Gal}}(E/F). \qquad \square$$

From this theorem we obtain a criterion for $E_{[\ell]}/E$ being a PV-extension.

E_ell-is-ppv

Corollary 4.3.4. *Let E/F be a PV-extension and suppose that $F_1 = F^p$. Then the extension $E_{[\ell]}/E$ is a PV-extension, for all $\ell \in \mathbb{N}$.*

Proof. By Prop. 4.3.2, the condition $F_1 = F^p$ implies that $F_{[\ell]} = F$ for all ℓ. Hence by the previous theorem, $E_{[\ell]}/F$ is a PV-extension and therefore $E_{[\ell]}/E$ is a PV-extension. $\square$

finite-id-ext

Proposition 4.3.5. *Let E be a finite ID-extension of some ID-field F with $C_E = C$. Then there is a finite field extension L over C such that E is contained in a PV-extension of $FL = F \otimes_C L$.*

Proof. Let $e_1, \dots, e_n \in E$ be an F-basis of E. Then there are unique $A_{\boldsymbol{k}} \in F^{n\times n}$, such that $\theta_E^{(\boldsymbol{k})}(e_i) = \sum_{j=1}^n (A_{\boldsymbol{k}})_{ij} e_j$ for all $\boldsymbol{k} \in \mathbb{N}^m$ and $i = 1, \dots, n$. Since the $A_{\boldsymbol{k}}$ are unique, the property of θ_E being an iterative derivation implies that $\theta(\boldsymbol{y}) = A\boldsymbol{y}$ is an iterative differential equation, where $A = \sum_{\boldsymbol{k}\in\mathbb{N}^m} A_{\boldsymbol{k}} \boldsymbol{T}^{\boldsymbol{k}} \in \mathrm{GL}_n(F[[\boldsymbol{T}]])$. Let $U := E[X_{ij}, \det(X)^{-1}]$ be the universal solution ring for this IDE over E (i. e. $\theta_U(X) = AX$). Then the ideal $(x_{11} - e_1, x_{21} - e_2, \dots, x_{n1} - e_n) \trianglelefteq U$ is an ID-ideal and there is a maximal ID-ideal P containing $(x_{11} - e_1, \dots, x_{n1} - e_n)$. Then the field of constants $L := C_{U/P}$ of U/P is a finite field extension of C and by construction U/P is a PV-extension of FL which contains E. $\square$

thm:general-realisation

Theorem 4.3.6. *Let F be an ID-field with $C_F = C$ perfect.*
Let $\tilde{C}_\ell$ denote the maximal subalgebra of $C_{F_{[\ell]} \otimes_F F_{[\ell]}}$ which is a Hopf algebra with respect to the comultiplication induced by

$$F_{[\ell]} \otimes_F F_{[\ell]} \longrightarrow \left(F_{[\ell]} \otimes_F F_{[\ell]}\right) \otimes_{F_{[\ell]}} \left(F_{[\ell]} \otimes_F F_{[\ell]}\right), a \otimes b \mapsto (a \otimes 1) \otimes (1 \otimes b).$$

Then an infinitesimal group scheme of height $\leq \ell$ is realisable as ID-Galois group scheme over F, if and only if it is a factor group of $\mathrm{Spec}(\tilde{C}_\ell)$.

In particular, there is a PV-extension of F with Galois group scheme $\operatorname{Spec}(\tilde{C}_\ell)$*, and this is the unique maximal PV-extension which is purely inseparable of exponent* $\leq \ell$*.*

Furthermore, if $F_{[\ell]}/F$ is a PV-extension, then $\tilde{C}_\ell = C_{F_{[\ell]} \otimes_F F_{[\ell]}}$, and $\operatorname{Spec}(\tilde{C}_\ell)$ *is isomorphic to* $\underline{\mathrm{Gal}}(F_{[\ell]}/F)$*.*

Proof. The uniqueness in the second statement follows from the fact that there is only one minimal ID-extension $\tilde{F}$ of F such that $\tilde{C}_\ell$ is contained in $\tilde{F} \otimes_F \tilde{F}$. (This $\tilde{F}$ is the desired PV-extension.)

The proof of the first statement is done in two steps.

Let $\tilde{\mathcal{G}}$ be an infinitesimal group scheme of height $\leq \ell$ which is realisable as ID-Galois group scheme over F and let F'/F be a PV-extension with Galois group scheme $\tilde{\mathcal{G}}$. By Cor. 4.3.1 and Prop. 4.3.2, F' is an ID-subfield of $F_{[\ell]}$. Therefore, $C[\tilde{\mathcal{G}}] \cong C_{F' \otimes_F F'}$ is a subalgebra of $C_{F_{[\ell]} \otimes_F F_{[\ell]}}$ and is a Hopf algebra with comultiplication as given in the statement. Hence it is a sub-Hopf algebra of $\tilde{C}_\ell$ and so $\tilde{\mathcal{G}}$ is a factor group of $\operatorname{Spec}(\tilde{C}_\ell)$.

For the converse, let $\tilde{\mathcal{G}}$ be a factor group of $\operatorname{Spec}(\tilde{C}_\ell)$. We first assume that there is a PV-extension E/F such that $E \supseteq F_{[\ell]}$. Let R denote the corresponding PV-ring and $\mathcal{G} := \underline{\mathrm{Gal}}(E/F)$ the Galois group scheme. Since $F_{[\ell]}$ is an intermediate ID-field by Thm. 4.2.3, there is a subgroup $\mathcal{H} \leq \mathcal{G}$ such that $F_{[\ell]} = E^{\mathcal{H}}$. Since $F_{[\ell]}$ is a finite dimensional F-vector space, all elements in $F_{[\ell]}$ are differentially finite over F, and we obtain $F_{[\ell]} = R^{\mathcal{H}}$ by Prop. 4.1.6. Then $\tilde{C}_\ell \subseteq C_{F_{[\ell]} \otimes_F F_{[\ell]}} \subseteq C_{R \otimes_F R} \cong C[\mathcal{G}]$ is a sub-Hopf algebra, i. e. $\operatorname{Spec}(\tilde{C}_\ell)$ is a factor group of $\mathcal{G}$. Since $\tilde{\mathcal{G}}$ is a factor group of $\operatorname{Spec}(\tilde{C}_\ell)$, it also is a factor group of $\mathcal{G}$, and therefore there is a normal subgroup $\mathcal{G}' \trianglelefteq \mathcal{G}$ such that $\tilde{\mathcal{G}} \cong \mathcal{G}/\mathcal{G}'$. Then by the Galois correspondence, $\tilde{F} := E^{\mathcal{G}'}$ is a PV-extension of F with Galois group scheme $\tilde{\mathcal{G}}$.

If there is no PV-extension E/F containing $F_{[\ell]}$, then by Prop. 4.3.5, there is a finite Galois extension C' of C such that there is a PV-extension E'/FC' containing $F_{[\ell]}C'$. By the previous arguments there is a PV-field F' over FC' with Galois group $\tilde{\mathcal{G}} \times_C C'$. Since F' is a purely inseparable extension of FC', it is defined over F, i. e. there is an ID-field $\tilde{F}/F$ such that $F' = \tilde{F} \otimes_C C'$. Since $\mathrm{Gal}(C'/C)$ acts on $F' = \tilde{F}C'$ by ID-automorphisms, the constants of $\tilde{F} \otimes_F \tilde{F} \cong (F' \otimes_F \tilde{F})^{\mathrm{Gal}(C'/C)} \cong (F' \otimes_{FC'} F')^{\mathrm{Gal}(C'/C)}$ are equal to the $\mathrm{Gal}(C'/C)$-invariants of $C_{F' \otimes_{FC'} F'} \cong C'[\tilde{\mathcal{G}}]$ inside $C_{F_{[\ell]} \otimes_F F_{[\ell]}}C'$, i. e. are equal to $C[\tilde{\mathcal{G}}]$. By comparing dimensions, one obtains that the $\tilde{F}$-linear mapping $\tilde{F} \otimes_C C[\tilde{\mathcal{G}}] \to \tilde{F} \otimes_F \tilde{F}$ is in fact an isomorphism, and hence by [Mau10a], Prop. 10.12, $\tilde{F}/F$ is a PV-extension with Galois group scheme $\tilde{\mathcal{G}}$.

In the case where $F_{[\ell]}/F$ is a PV-extension, the torsor isomorphism (4.1) implies that $C[\underline{\mathrm{Gal}}(F_{[\ell]}/F)] \cong C_{F_{[\ell]} \otimes_F F_{[\ell]}}$ is a Hopf algebra. Hence, $\tilde{C}_\ell = C_{F_{[\ell]} \otimes_F F_{[\ell]}}$, and $\operatorname{Spec}(\tilde{C}_\ell) \cong \underline{\mathrm{Gal}}(F_{[\ell]}/F)$. □

special-realisation

Corollary 4.3.7. *Let E be an ID-field and suppose that E is a PV-extension of some ID-field F satisfying $F_1 = F^p$. An infinitesimal group scheme of height $\leq \ell$ is realizable as ID-Galois group scheme over E, if and only if it is a factor group of $\underline{\mathrm{Gal}}(E_{[\ell]}/E)$.*

Proof. This follows directly from Corollary 4.3.4 and Theorem 4.3.6. □

all-ids-are-ppv

Corollary 4.3.8. *Let E be an ID-field and suppose that E is a PV-extension of some ID-field F satisfying $F_1 = F^p$, and that $\underline{\mathrm{Gal}}(E/F)$ is a commutative group scheme. Then every purely inseparable ID-extension of E is a PV-extension of E.*

Proof. By Thm. 4.3.3, $\underline{\mathrm{Gal}}(E_{[\ell]}/F)$ is commutative, if $\underline{\mathrm{Gal}}(E/F))$ is. Hence $\underline{\mathrm{Gal}}(E_{[\ell]}/E)$ is commutative for all ℓ. Since every purely inseparable ID-extension of E sits inside some $E_{[\ell]}$ and every subgroup scheme of a commutative group scheme is normal, the statement follows from the Galois correspondence 4.2.3. □

The following table recalls some properties of a PV-extension E/F and the corresponding properties of the Galois group scheme $\mathcal{G} = \underline{\mathrm{Gal}}(E/F)$:

Property of $\mathcal{G}$	**Property of E/F**
finite scheme with $\dim_C(C[\mathcal{G}]) = m$	finite extension with $[E : F] = m$.
reduced scheme	separable extension
infinitesimal scheme of height n	purely inseparable extension of exponent n.

4.4 Finite separable PV-extensions

sec:sep-pv

We now consider PV-extensions with finite reduced Galois group schemes, i.e., finite separable PV-extensions. Since iterative derivations extend uniquely to finite separable field extensions (see [MvdP03],2.1,(5)), we obtain a close relationship to classical Galois extensions.

Lemma 4.4.1. *Let E be a finite (classical) Galois extension of F which is geometric over C, and let G be its Galois group. Let E be equipped with the unique iterative derivation extending the iterative derivation on F. Then the extension E/F is a PV-extension with Galois group scheme $\underline{\mathrm{Gal}}(E/F) = \mathrm{Spec}(C[G])$, the constant group scheme corresponding to G.*

Proof. Let $\{x_1, \ldots, x_n\}$ be an F-basis of E, and let $a_{ij} \in F[[T]]$ such that $\theta(x_i) = \sum_{j=1}^n a_{ij}x_j$ for all $i = 1, \ldots, n$. Furthermore, let $G = \{\sigma_1, \ldots, \sigma_n\}$, and $Y = \big(\sigma_k(x_i)\big)_{1\leq i,k\leq n} \in \mathrm{GL}_n(E)$. ($Y$ is invertible by Dedekind's lemma on the independence of automorphisms.)

By definition, one has $\theta(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, where $A = (a_{ij}) \in \mathrm{Mat}_{n\times n}(F[[T]])$. Since the extension of the iterative derivation of F to E is unique, all automorphisms are indeed ID-automorphisms, and therefore $\theta(Y) = AY$.

Therefore by Remark 4.1.4, $\theta(\boldsymbol{y}) = A\boldsymbol{y}$ is an IDE and Y is a fundamental solution matrix for this IDE. Furthermore, E is generated by the entries of Y, and $C_E = C$, since E/F is geometric. Hence, E is a PV-field for the IDE $\theta(\boldsymbol{y}) = A\boldsymbol{y}$.
Finally, $\mathrm{Spec}(C[G])$ is a subgroup scheme of $\underline{\mathrm{Gal}}(E/F)$, since G acts by ID-automorphisms, and $\dim_C(C[G]) = n = [E : F] = \dim_C(C[\underline{\mathrm{Gal}}(E/F)])$. Hence, $\mathrm{Spec}(C[G]) = \underline{\mathrm{Gal}}(E/F)$. □

Remark 4.4.2. In the case that C is algebraically closed, the statement also follows easily from [MvdP03], 4.1.: in this case, Matzat and van der Put proved that the C-rational points of $\underline{\mathrm{Gal}}(E/F)$ equal G. Since for an algebraically closed field C, a reduced group scheme is determined by its C-rational points, the claim follows.

Lemma 4.4.3. *Let E/F be a finite separable PV-extension with Galois group scheme $\mathcal{G}$. Let $E_{\bar{C}} = E \otimes_C \bar{C}$ and $F_{\bar{C}} = F \otimes_C \bar{C}$ be the extensions of constants, where $\bar{C}$ denotes an algebraic closure of C. Then $E_{\bar{C}}/F_{\bar{C}}$ is a finite (classical) Galois extension with Galois group $\mathcal{G}(\bar{C})$.*

Proof. By definition of the Galois group scheme $\mathcal{G}$, the group $\mathcal{G}(\bar{C})$ equals the group $\mathrm{Aut}^{ID}(E_{\bar{C}}/F_{\bar{C}})$. (Recall that in the finite case the PV-ring and the PV-field are equal.) Since $E_{\bar{C}}/F_{\bar{C}}$ is separable, $\mathcal{G}$ is reduced and hence, $E^{\mathcal{G}(\bar{C})} = E^{\mathcal{G}} = F$. Therefore, $(E_{\bar{C}})^{\mathcal{G}(\bar{C})} = F_{\bar{C}}$, which implies that $E_{\bar{C}}$ is Galois over $F_{\bar{C}}$ with Galois group $\mathcal{G}(\bar{C})$. □

Remark 4.4.4. The previous lemma tells us that all finite separable PV-extensions become classical Galois extensions after an algebraic extension of the constants. Actually, this extension of constants can be chosen to be finite Galois. Hence finite separable PV-extensions are *almost classical Galois extensions* in the sense of Greither and Pareigis (cf. [GP87], Def. 4.2).

4.5 Finite PV-extensions

sec:finite-pv

We finally consider the case of arbitrary finite PV-extensions, i.e., PV-extensions with finite Galois group schemes. By [DG70], Ch. II, §5, Cor. 2.4, every finite group scheme is the semi-direct product of an infinitesimal group scheme and a finite reduced group scheme, since our base field C is assumed to be perfect. Hence, the results of the previous sections also give us information in this case.

thm:finite-realisation

Theorem 4.5.1. *Let $\mathcal{G}$ be a finite group scheme over C, $\mathcal{G}^0 \trianglelefteq \mathcal{G}$ the connected component of $\mathcal{G}$ (an infinitesimal group scheme), and $\mathcal{H} \leq \mathcal{G}$ the induced reduced group scheme. Assume that there is $\ell \geq \mathrm{ht}(\mathcal{G}^0)$ such that $F_{[\ell]}/F$ is a PV-extension. Then $\mathcal{G}$ is realizable over F, if and only if $\mathcal{G} \cong \mathcal{G}^0 \times \mathcal{H}$, $\mathcal{G}^0$ is a factor group of $\underline{\mathrm{Gal}}(F_{[\ell]}/F)$ and $\mathcal{H}$ is realizable over F.*

Proof. Let $\mathcal{G} \cong \mathcal{G}^0 \times \mathcal{H}$, such that $\mathcal{G}^0$ is a factor group of $\underline{\mathrm{Gal}}(F_{[\ell]}/F)$ and $\mathcal{H}$ is realizable over F as $\mathcal{H} \cong \underline{\mathrm{Gal}}(E''/F)$. By Theorem 4.3.6, $\mathcal{G}^0$ is the Galois group scheme of some intermediate PV-field $F \leq E' \leq F_{[\ell]}$. Since E''/F is separable and E'/F is purely inseparable, E' and E'' are linearly disjoint over F, and so $E' \otimes_F E''$ is a PV-extension of F with Galois group scheme $\underline{\mathrm{Gal}}(E' \otimes_F E''/F) \cong \mathcal{G}^0 \times \mathcal{H}$. Hence, $\mathcal{G}$ is realizable over F.

On the other hand, let $\mathcal{G}$ be realized over F as $\mathcal{G} \cong \underline{\mathrm{Gal}}(E/F)$. By [DG70], Ch. II, §5, Cor. 2.4, $\mathcal{G}$ is a semi-direct product $\mathcal{G} \cong \mathcal{G}^0 \rtimes \mathcal{H}$, and therefore $\mathcal{H} \cong \mathcal{G}/\mathcal{G}^0 \cong \underline{\mathrm{Gal}}(E^{\mathcal{G}^0}/F)$, i.e., $\mathcal{H}$ is realizable over F. Furthermore, $E^{\mathcal{H}}$ is a purely inseparable ID-extension of F of height $\leq \mathrm{ht}(\mathcal{G}^0)$. By assumption, there is $\ell \geq \mathrm{ht}(\mathcal{G}^0)$ such that $F_{[\ell]}/F$ is a PV-extension and therefore $F_{[\ell]}$ is a PV-extension containing $E^{\mathcal{H}}$. As in the first part of the proof, $\tilde{E} := F_{[\ell]} \otimes_F E^{\mathcal{G}^0}$ is a PV-extension of F with Galois group $\underline{\mathrm{Gal}}(\tilde{E}/F) \cong \underline{\mathrm{Gal}}(F_{[\ell]}/F) \times \underline{\mathrm{Gal}}(E^{\mathcal{G}^0}/F) \cong \underline{\mathrm{Gal}}(F_{[\ell]}/F) \times \mathcal{H}$. Since $E^{\mathcal{H}}$ and $E^{\mathcal{G}^0}$ are subfields of $\tilde{E}$, E is also a subfield of $\tilde{E}$. Therefore, $\underline{\mathrm{Gal}}(E/F) \cong \mathcal{G}^0 \rtimes \mathcal{H}$ is a factor group of $\underline{\mathrm{Gal}}(\tilde{E}/F) \cong \underline{\mathrm{Gal}}(F_{[\ell]}/F) \times \mathcal{H}$ which implies that $\mathcal{H}$ acts also trivially on $\mathcal{G}^0$, i.e., the semi-direct product $\mathcal{G}^0 \rtimes \mathcal{H}$ is in fact a direct product. Finally, we obtain that $E^{\mathcal{H}}$ is a PV-extension of F (since $\mathcal{H} \leq \mathcal{G}$ is a normal subgroup) with Galois group $\mathcal{G}^0$, and hence $\mathcal{G}^0$ is a factor group of $\underline{\mathrm{Gal}}(F_{[\ell]}/F)$. □

cor:inverse-problem-over-pv-field

Corollary 4.5.2. *Let C be algebraically closed, and let F be a PV-extension of some function field L/C in one variable with non-degenerate univariate iterative derivation. Then the finite group schemes which occur as Galois group scheme over F are exactly the direct products $\mathcal{G}^0 \times \mathcal{H}$, where $\mathcal{H}$ is a constant group scheme (i.e., a reduced finite group scheme) and $\mathcal{G}^0$ is a factor group of some $\underline{\mathrm{Gal}}(F_{[\ell]}/F)$.*

Proof. By Corollary 4.3.4, $F_{[\ell]}$ is a PV-extension of F for all ℓ. So by Theorem 4.5.1, we only have to show that every finite reduced group scheme $\mathcal{H}$ is realizable. Since C is algebraically closed, the PV-extensions E of F with Galois group $\mathcal{H}$ are the (classical) Galois extensions with Galois group $\mathcal{H}(C)$. By [Har95], Thm. 4.4, the absolute Galois group of L, $\mathrm{Gal}(L^{\mathrm{sep}}/L)$, is a free group on infinitely many generators. Hence, there is an epimorphism $\phi : \mathrm{Gal}(L^{\mathrm{sep}}/L) \to \mathcal{H}(C) \times \mathrm{Gal}(F \cap L^{\mathrm{sep}}/L)$ such that the composition of ϕ and the projection pr_2 onto the second factor is the restriction map $\mathrm{Gal}(L^{\mathrm{sep}}/L) \to \mathrm{Gal}(F \cap L^{\mathrm{sep}}/L)$.

But this means that $\mathrm{pr}_1 \circ \phi : \mathrm{Gal}(L^{\mathrm{sep}}/L) \to \mathcal{H}(C)$ corresponds to a Galois extension $\tilde{L}$ of L with group $\mathcal{H}(C)$ which is linearly disjoint to F. Hence $\tilde{L} \otimes_L F$

is a Galois extension of F with Galois group $\mathcal{H}(C)$. $\square$

4.6 Examples

examples

In this section we consider some examples. Throughout this section C denotes a perfect field of characteristic $p > 0$ and $C((t))$ is equipped with the univariate iterative derivation θ given by $\theta(t) = t + T$.

ex1

Example 1. We start with the easiest case, namely $F = C(t)$ or F is a finite ID-extension of $C(t)$ inside $C((t))$. We have already seen in Remark 4.1.1 that $F^p \subseteq F_1$ and that $[F : F_1] = p$. Since F is a function field in one variable over the perfect field C, we also have $[F : F^p] = p$. Hence, $F_1 = F^p$, i. e. $F_{[1]} = F$, and therefore by Prop. 4.3.2, there exist no purely inseparable ID-extensions of F.

Example 2. We present an example for an ID-field F with $F_{[\ell]} \supsetneq F$ which nevertheless has no purely inseparable PV-extensions. More precisely, we show that the constants of $F_{[\ell]} \otimes_F F_{[\ell]}$ are equal to $C = C_F$ for all $\ell \in \mathbb{N}$.

Let $\alpha \in \mathbb{Z}_p \setminus \mathbb{Q}$ be a p-adic integer, and for all $k \in \mathbb{N}$, let $\alpha_k \in \{0, \ldots, p^k - 1\}$ be chosen such that $\alpha \equiv \alpha_k \mod p^k$. Then we define $r := \sum_{k=1}^{\infty} t^{\alpha_k} \in C[[t]]$. The field $F := C(t, r)$ is then an ID-subfield of $C((t))$, since for all $j \in \mathbb{N}$,

$$\begin{aligned} \theta^{(p^j)}(r) &= \sum_{k=1}^{\infty} \theta^{(p^j)}\left(t^{\alpha_k}\right) = \sum_{k=1}^{\infty} \binom{\alpha_k}{p^j} t^{\alpha_k - p^j} \\ &= \binom{\alpha_{j+1}}{p^j} t^{-p^j} \sum_{k=j+1}^{\infty} t^{\alpha_k} = \binom{\alpha_{j+1}}{p^j} t^{-p^j} \left(r - \sum_{k=1}^{j} t^{\alpha_k} \right) \in C(t, r). \end{aligned}$$

Here we used that $\binom{a}{p^j} = 0$ if $a < p^j$ and $\binom{a}{p^j} \equiv \binom{b}{p^j} \mod p$ if $a \equiv b \mod p^{j+1}$.

We will show now that r is transcendental over $C(t)$:

Let s be a solution for the 1-dimensional IDE $\theta^{(p^j)}(y) = \binom{\alpha_{j+1}}{p^j} t^{-p^j} y$ $(j \in \mathbb{N})$ in some extension field of F. Since $\alpha \notin \mathbb{Q}$, the element s is transcendental over $C(t)$ by [Mat01], Thm. 3.13. The rules for the derivatives of r and s can be written as a matrix equation

$$\theta^{(p^j)} \begin{pmatrix} s & r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \binom{\alpha_{j+1}}{p^j} t^{-p^j} & -\binom{\alpha_{j+1}}{p^j} \sum_{k=1}^{j} t^{\alpha_k - p^j} \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} s & r \\ 0 & 1 \end{pmatrix},$$

which shows that $C(t, r, s)$ is a PV-field over $C(t)$ with Galois group inside $\mathbb{G}_m \ltimes \mathbb{G}_a \cong \{ \left(\begin{smallmatrix} x & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2 \}$.

Since s is transcendental over $C(t)$, the full subgroup $\mathbb{G}_m$ is contained in the Galois group. The only subgroups of $\mathbb{G}_a$ which are stable under the $\mathbb{G}_m$-action

are the Frobenius kernels $\boldsymbol{\alpha}_{p^m}$. But all Galois groups over $C(t)$ are reduced (cf. [Mau10a], Cor. 11.7), and hence we have $\underline{\mathrm{Gal}}(C(t,r,s)/C(t)) = \mathbb{G}_m \ltimes \mathbb{G}_a$ or $= \mathbb{G}_m$. In both cases $C(t,r,s)$ contains no elements that are algebraic over $C(t)$. Since the power series of r does not become eventually periodic, $r \notin C(t)$ and so r has to be transcendental over $C(t)$.

Next we are going to calculate the constants of $F_{[\ell]} \otimes_F F_{[\ell]}$:

It is not hard to see that $F_{[\ell]} = C(t, r_{[\ell]})$, where

$$r_{[\ell]} := \left(t^{-\alpha_\ell}(r - \sum_{k=1}^{\ell} t^{\alpha_k}) \right)^{p^{-\ell}} = \sum_{k=1}^{\infty} t^{(\alpha_{k+\ell}-\alpha_\ell)p^{-\ell}} \in C[[t]],$$

and the derivatives of $r_{[\ell]}$ are given by:

$$\theta^{(p^j)}(r_{[\ell]}) = \binom{(\alpha_{j+1+\ell} - \alpha_\ell)p^{-\ell}}{p^j} t^{-p^j} \left(r_{[\ell]} - \sum_{k=1}^{j} t^{(\alpha_{k+\ell}-\alpha_\ell)p^{-\ell}} \right).$$

Hence, one obtains for all $n \in \mathbb{N}$:

$$\theta^{(n)}(r_{[\ell]}) \in \binom{(\alpha - \alpha_\ell)p^{-\ell}}{n} t^{-n} r_{[\ell]} + C(t).$$

For calculating the constants in $F_{[\ell]} \otimes_F F_{[\ell]}$, we remark that $\{r_{[\ell]}^i \otimes r_{[\ell]}^j \mid 0 \leq i, j \leq p^\ell - 1\}$ is a basis of $F_{[\ell]} \otimes_F F_{[\ell]}$ as an F-vector space. A further calculation shows that for $n \in \mathbb{N}$ and $k \in \mathbb{Z}$

$$\theta^{(n)} \left(t^k r_{[\ell]}^i \otimes r_{[\ell]}^j \right) \equiv \binom{k + (i+j)(\alpha - \alpha_\ell)p^{-\ell}}{n} t^{-n} \left(t^k r_{[\ell]}^i \otimes r_{[\ell]}^j \right)$$

modulo terms in $r_{[\ell]}^\mu \otimes r_{[\ell]}^\nu$ with $\mu + \nu < i + j$. So an element $x := \sum_{i,j} c_{i,j} r_{[\ell]}^i \otimes r_{[\ell]}^j \in F_{[\ell]} \otimes_F F_{[\ell]}$ can only be constant, if for the terms of maximal degree these binomial coefficients vanish for all n. Since α is not rational, this is only possible if $i = j = 0$ is the maximal degree and if $k = 0$, i. e. $x \in C$. So we have shown that $C_{F_{[\ell]} \otimes_F F_{[\ell]}} = C$ for all $\ell \in \mathbb{N}$, which implies by Theorem 4.3.6 that there are no purely inseparable PV-extensions over $F = C(t, r)$.

ex3

Example 3. The following example is quite contrary to the previous one. In this example all purely inseparable ID-extensions are PV-extensions.

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p$ be p-adic integers such that the set $\{1, \alpha_1, \ldots, \alpha_n\}$ is $\mathbb{Z}$-linear independent, and let $\alpha_i =: \sum_{k=0}^{\infty} a_{i,k} p^k$ $(i = 1, \ldots, n)$ be their normal series, i. e. $a_{i,k} \in \{0, \ldots, p-1\}$. For $i = 1, \ldots, n$, we then define

$$s_i := \sum_{k=0}^{\infty} a_{i,k} t^{p^k} \in C((t))$$

and consider the field $F := C(t, s_1, \ldots, s_n)$. This is an ID-subfield of $C((t))$, since $\theta^{(p^\ell)}(s_i) = a_{i,\ell}$ for all $\ell \in \mathbb{N}$ and $i = 1, \ldots, n$. Also from $\theta^{(p^\ell)}(s_i) \in C$, one obtains that the extension $F/C(t)$ is a PV-extension and its Galois group scheme is a subgroup scheme of $\mathbb{G}_a^n$. Actually, the condition on the α_i implies that the s_i are algebraically independent over $C(t)$ and hence the Galois group scheme is the full group $\mathbb{G}_a^n$. Therefore by Corollary 4.3.4, for all $\ell \in \mathbb{N}$ the extension $F_{[\ell]}/F$ is a PV-extension and $\underline{\mathrm{Gal}}(F_{[\ell]}/F) \cong (\boldsymbol{\alpha}_{p^\ell})^n$, where $\boldsymbol{\alpha}_{p^\ell}$ denotes the kernel of the p^ℓ-th power Frobenius map on $\mathbb{G}_a$. Furthermore, $(\boldsymbol{\alpha}_{p^\ell})^n$ is a commutative group scheme and so all its subgroup schemes are normal subgroup schemes. By Theorem 4.2.3, this implies that every intermediate ID-field $F \leq E \leq F_{[\ell]}$ is a PV-extension of F. So all purely inseparable ID-extensions of F are PV-extensions over F. Furthermore, by Cor. 4.3.7, an infinitesimal group scheme is realizable over F if and only if it is a factor group scheme of $(\boldsymbol{\alpha}_{p^\ell})^n$ for some ℓ, which are exactly the infinitesimal closed subgroup schemes of $\mathbb{G}_a^n$.

Example 4. Let C be an algebraically closed field of positive characteristic p. We want L/C to be a function field in one variable over C with a non-degenerate iterative derivation θ, and F to be a PV-extension of L with Galois group scheme $\mathbb{G}_m$. For example, we may take $L = C(t)$ with $\theta = \theta_t$ the iterative derivation with respect to t, given by $\theta(t) = t + T \in L[[T]]$, and $F = L(t^\alpha)$, with $\alpha \in \mathbb{Z}_p \setminus \mathbb{Q}$ and the iterative derivation given by $\theta^{(n)}(t^\alpha) = \binom{\alpha}{n} t^\alpha / t^n$.

By Theorem 4.3.6, for all $\ell \geq 0$, $F_{[\ell]}/L$ is a PV-extension with $\underline{\mathrm{Gal}}(F_{[\ell]}/L) \cong \mathbb{G}_m$, and the "restriction map" $\underline{\mathrm{Gal}}(F_{[\ell]}/L) \cong \mathbb{G}_m \to \underline{\mathrm{Gal}}(F/L) \cong \mathbb{G}_m$ is given by the Frobenius map $x \mapsto x^{p^\ell}$. Hence, $\underline{\mathrm{Gal}}(F_{[\ell]}/F) \cong \mu_{p^\ell}$, the "group of p^ℓth roots of unity". The only factor groups of μ_{p^ℓ} are μ_{p^k} where $k \leq \ell$. Hence by Theorem 4.5.1, the finite Galois group schemes over F are exactly the group schemes of the form $\mu_{p^\ell} \times H$, where $\ell \geq 0$ and H is finite reduced.

Chapter 5

Realization of Torsion group schemes

chap:real-of-torsion

This chapter contains the results of [Mau15]. We show that torsion group schemes of abelian varieties in positive characteristic occur as iterative differential Galois groups of extensions of iterative differential fields. The main part is to find computable criteria when higher derivations are iterative derivations, and furthermore when an iterative derivation on the function field of an abelian variety is compatible with the addition map. For an explicit example, we give a construction of (a family of) such iterative derivations on the function field of an elliptic curve in characteristic two.

The rough idea for getting the n-torsion scheme $A[n]$ of an abelian variety A over a perfect field C as ID-Galois group scheme is the following. Starting with the abelian variety A over C we consider the function field L of $A_{C(t)}$ (i.e. of A after base change to $C(t)$) as an extension of the rational function field $C(t)$. The field $C(t)$ comes with the standard iterative derivation with respect to t, and this iterative derivation is then extended to an iterative derivation on L. By taking care that this extension fulfills the appropriate conditions, one guarantees that the torsion group scheme $A[n]$ indeed acts on L by ID-automorphisms. Hence by Picard-Vessiot theory, one obtains $A[n]$ as the iterative differential Galois group of L over $L^{A[n]}$, the fixed field under $A[n]$. To be more precise, one should say that the group scheme acts by functorial automorphisms, i.e. D-rational points act as ID-automorphisms on the total quotient ring $\mathrm{Quot}(L \otimes_C D)$.

This chapter is structured as follows. In Section 5.1, we give the basic notation and some basic properties which will be used in the calculations later on. Furthermore, we give a short summary of the Picard-Vessiot theory used in this article. The theoretical considerations for obtaining the torsion group scheme of an abelian scheme as ID-Galois group are given in Sections 5.2 and 5.3. The main theorems are Theorem 5.2.2 giving a necessary and sufficient condition for the iterative derivation on the function field of an abelian variety to "commute" with the addition map, as well as Theorem 5.3.1 stating that the torsion group schemes are the ID-Galois group schemes over an appropriate subfield when the iterative derivation satisfies the previous conditions.

In the last two sections, we turn the conditions of Theorem 5.2.2 into explicit recursive formulas for the higher derivatives of the generators of the field L. While Section 5.4 deals with the condition that the extension to the overfield is an iterative derivation, Section 3.7 is dedicated to giving recursive formulas for constructing the iterative derivation on the function field in a way that it "commutes" with the addition map (cf. Theorem 5.5.3). As this becomes quite complicated in the general case, we restrict to the example of an elliptic curve in characteristic 2 in this last section.

5.1 Basic notation

sec:basics

All rings are assumed to be commutative with unit.

In addition to the notation on iterative derivations given in Section 3.1, we will need a more general notion, namely the notion of a *higher derivation*.
A **higher derivation** (HD for short) on a ring R is a homomorphism of rings $\theta : R \to R[[T]]$, such that $\theta(r)|_{T=0} = r$ for all $r \in R$. If there is need to emphasis the extra variable T or if we use another name for the variable, we add a subscript to θ, i.e. denote the higher derivation by θ_T (resp. θ_U if the variable is named U).

Hence, an iterative derivation on R is a higher derivation with the additional property that for all $i, j \geq 0$, $\theta^{(i)} \circ \theta^{(j)} = \binom{i+j}{i}\theta^{(i+j)}$, where as before the maps $\theta^{(i)} : R \to R$ are defined by $\theta(r) =: \sum_{i=0}^{\infty} \theta^{(i)}(r)T^i$. The pair (R, θ) is then called an **HD-ring** (resp. **ID-ring**) and $C_R := \{r \in R \mid \theta(r) = r\}$ is called the **ring of constants** of (R, θ). An HD/ID-ring which is a field is called an **HD/ID-field**. Higher derivations and iterative derivations are extended to localisations by $\theta(\frac{r}{s}) := \theta(r)\theta(s)^{-1}$ and to tensor products by

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

for all $k \geq 0$.

Given a homomorphism of rings $f : R \to S$, we often consider the T-linear extension of f to a homomorphism $R[[T]] \to S[[T]]$ of the power series rings. This map will be denoted by $f[[T]]$. Given two HD-rings (R, θ) and $(S, \tilde{\theta})$. A homomorphism of rings $f : R \to S$ is called an **HD-homomorphism** (resp. ID-homomorphism if R and S are ID-rings) if $\tilde{\theta} \circ f = f[[T]] \circ \theta$. As a special case of a homomorphism $f[[T]]$, we have the homomorphism $\theta_U[[T]] : R[[T]] \to R[[T, U]]$ induced by the higher derivation $\theta_U : R \to R[[U]]$ on R. A short calculation shows (cf. [Rös07]) that a higher derivation θ on R is an iterative derivation if and only if the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\theta_U} & R[[U]] \\ {\scriptstyle \theta_T}\downarrow & & \downarrow{\scriptstyle U \mapsto U+T} \\ R[[T]] & \xrightarrow{\theta_U[[T]]} & R[[U,T]], \end{array}$$

or in other terms $\theta_U[[T]] \circ \theta_T = \theta_{T+U}$.

ex:ID-fields

Example 5. (cf. [Mau10a])

1. For any field C and $F := C(t)$, the homomorphism of C-algebras $\theta : F \to F[[T]]$ given by $\theta(t) := t+T$ is an iterative derivation on F with field of constants C. This iterative derivation will be called the **iterative derivation with respect to** t.

2. For any ring R, there is the **trivial** iterative derivation on R given by $\theta_0 : R \to R[[T]], r \mapsto r \cdot T^0$. Obviously, the ring of constants of (R, θ_0) is R itself.

item:fin-sep-ext

3. If (F, θ) is an HD-field and $L \geq F$ is a finite separable field extension, then θ can be uniquely extended to a higher derivation on L. If the higher derivation θ is an iterative derivation, then the extension to L is also an iterative derivation.

4. Let (F, θ) be an HD-field, L/F a finitely generated separable field extension and $x_1, \ldots, x_k$ a separating transcendence basis of L over F (i.e. $F(x_1, \ldots, x_k)/F$ is purely transcendental and $L/F(x_1, \ldots, x_k)$ is finite separable). Using the previous example, it is easy to see that any choice of elements $\xi_{i,n} \in L$ ($i = 1, \ldots, k$ and $n \geq 1$) defines a unique higher derivation θ_L on L extending θ and satisfying $\theta_L(x_i) = x_i + \sum_{n=1}^{\infty} \xi_{i,n} T^n$ for all $i = 1, \ldots, k$.

We now summarize some well known formulas for higher derivations and iterative derivations in characteristic $p > 0$ which will be used later on:

lem:known-stuff

Lemma 5.1.1.

1. *$\theta^{(j)}(x^p) = 0$ if p does not divide j and $\theta^{(j)}(x^p) = \left(\theta^{(j/p)}(x)\right)^p$ if p divides j.*

2. *If $m = m_0 + m_1 p + \cdots + m_k p^k$ and $n = n_0 + n_1 p + \cdots + n_k p^k$ where $m_i, n_i \in \{0, \ldots, p-1\}$ then*

$$\binom{m}{n} \equiv \binom{m_0}{n_0} \cdot \binom{m_1}{n_1} \cdots \binom{m_k}{n_k} \mod p.$$

3. *If θ is iterative, then $(\theta^{(j)})^p = 0$ for all j.*

item:expansion

4. *Let $m = m_0 + m_1 p + \cdots + m_k p^k$ where $m_i \in \{0, \ldots, p-1\}$. If θ is iterative, then all the $\theta^{(p^i)}$ commute with each other, and*

$$\theta^{(m)} = \frac{1}{m_0! \cdot m_1! \cdots m_k!} (\theta^{(1)})^{m_0} \circ (\theta^{(p)})^{m_1} \circ \cdots \circ (\theta^{(p^k)})^{m_k}.$$

Notation *Let (L, θ) be an HD-field of characteristic $p > 0$, and $k \in \mathbb{N} \cup \{\infty\}$. We say that "for $x \in L$ the iteration rule holds up to level k" if for all $i, j \in \mathbb{N}$ satisfying $i + j \leq k$ one has*

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

or equivalently if

$$\theta_U[[T]]\big(\theta_T(x)\big) \equiv \theta_{T+U}(x) \mod (U^{k+1-j}T^j \mid 0 \leq j \leq k+1).$$

We say that "the iteration rule holds on L up to level k" if the iteration rule holds up to k for all $x \in L$.

lem:Things to show

Lemma 5.1.2. *Let (L, θ) be an HD-field of characteristic $p > 0$.*

item:subfield

1. *For $k \in \mathbb{N} \cup \{\infty\}$, the set of elements $x \in L$ for which the iteration rule holds up to level k is a subfield of L.*

item:level-extended

2. *Assume that for fixed $\ell \geq 0$ the iteration rule holds on L up to level p^ℓ, then for all $0 \leq k, m < p^\ell$ such that $k + m \geq p^\ell$, one has*

$$\theta^{(k)} \circ \theta^{(m)} = 0 = \binom{k+m}{k}\theta^{(k+m)}.$$

item:cancellation

3. *Assume that for fixed $\ell \geq 0$ the iteration rule holds on L up to level p^ℓ, and that L contains an element t satisfying $\theta(t) = t + T$. Then for all $x \in L$ and all $0 < r < p^\ell$ one has:*

$$\theta^{(r)}\left(\sum_{m=0}^{p^\ell-1} \theta^{(m)}(x)(-t)^m\right) = 0$$

Proof. (1) The set under consideration is just the equalizer of the ring homomorphisms $\theta_U[[T]] \circ \theta_T : L \to L[[T, U]/(U^{k+1-j}T^j \mid 0 \leq j \leq k+1)$ and θ_{T+U}. Hence, it is a subfield of L.

(2) As $k, m < p^\ell$ and $k + m \geq p^\ell$, the binomial coefficient $\binom{k+m}{k}$ equals 0 in characteristic p. Hence, the right hand side of the equation equals 0. For proving that the left hand side equals zero, it is sufficient to consider the case where $k = p^j$ for some $j < \ell$, as any $\theta^{(k)}$ is a composition of those up to a non-zero constant. Let $m' := m + p^j - p^\ell$. By assumption on m and p^j, we have $0 \leq m' < p^j$. As $m - m' = p^\ell - p^j$ is divisible by p^j, m' is the first part of the p-adic expansion of m up to p^{j-1} and $m - m'$ is the second part. Hence, by the previous lemma $\binom{m}{m'} = 1$ in characteristic p. As the iteration rule holds on L up to level p^ℓ, and as $k = p^j < p^\ell$ one gets

$$\theta^{(p^j)} \circ \theta^{(m)} = \theta^{(p^j)} \circ \theta^{(p^\ell - p^j)} \circ \theta^{(m')} = \binom{p^\ell}{p^j}\theta^{(p^\ell)} \circ \theta^{(m')} = 0,$$

since $\binom{p^\ell}{p^j} = 0$.

(3) This is a more complicated, but straightforward calculation:

$$\begin{aligned}
\theta^{(r)} \quad & \left(\sum_{m=0}^{p^\ell-1} \theta^{(m)}(x)(-t)^m\right) \quad = \quad \sum_{m=0}^{p^\ell-1}\sum_{k=0}^{r} \theta^{(r-k)}\left(\theta^{(m)}(x)\right)(-1)^m\theta^{(k)}(t^m) \\
\overset{\text{by(2)}}{=} \quad & \sum_{k=0}^{r}\sum_{m=k}^{p^\ell-1-(r-k)} \binom{m+r-k}{m}\theta^{(m+r-k)}(x)\cdot(-1)^m\binom{m}{k}t^{m-k} \\
= \quad & \sum_{k=0}^{r}\sum_{m'=0}^{p^\ell-1-r} \binom{m'+r}{m'+k}\binom{m'+k}{k}(-1)^{m'+k}\theta^{(m'+r)}(x)t^{m'} \\
\overset{(\star)}{=} \quad & \sum_{m'=0}^{p^\ell-1-r} \binom{m'+r}{r}\underbrace{\left(\sum_{k=0}^{r}\binom{r}{k}(-1)^k\right)}_{=0}(-1)^{m'}\theta^{(m'+r)}(x)t^{m'} \\
= \quad & 0.
\end{aligned}$$

Equation $(\star)$ holds, as both products $\binom{m'+r}{m'+k}\binom{m'+k}{k}$ and $\binom{m'+r}{r}\binom{r}{k}$ count the number of possibilities of splitting a set of cardinality $m'+r$ into three disjoint subsets of cardinalities k, m' and $r-k$ respectively. □

5.1.1 Picard-Vessiot theory

We now recall the main definitions from Picard-Vessiot theory. (F,θ) denotes some ID-field with constants C.

Definition 5.1.3. Let $A=\sum_{k=0}^{\infty}A_kT^k \in \mathrm{GL}_n(F[[T]])$ be a matrix with $A_0=\mathbb{1}_n$ and for all $k,l\in\mathbb{N}$, $\binom{k+l}{l}A_{k+l}=\sum_{i+j=l}\theta^{(i)}(A_k)\cdot A_j$. An equation

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

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

Remark 5.1.4. (cf. Rem. 4.1.4) The condition on the A_k is equivalent to the condition that $\theta^{(k)}(\theta^{(l)}(Y_{ij}))=\binom{k+l}{k}\theta^{(k+l)}(Y_{ij})$ holds for a matrix $Y=(Y_{ij})_{1\le i,j\le n}\in \mathrm{GL}_n(E)$ satisfying $\theta(Y)=AY$, where E is some ID-extension of F. (Such a Y is called a **fundamental solution matrix**) . The condition $A_0=\mathbb{1}_n$ is equivalent to $\theta^{(0)}(Y_{ij})=Y_{ij}$, and already implies that the matrix A is invertible.

Definition 5.1.5. An ID-ring $(R,\theta_R)\ge(F,\theta)$ is called a **Picard-Vessiot ring** (PV-ring) for the IDE $\theta(\boldsymbol{y})=A\boldsymbol{y}$, if the following hold:

1. R is an ID-simple ring, i.e. has no nontrivial θ_R-stable ideals.

2. There is a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$, i. e., an invertible matrix satisfying $\theta(Y) = AY$.

3. As an F-algebra, R is generated by the coefficients of Y and by $\det(Y)^{-1}$.

4. $C_R = C_F = C$.

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

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

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

where D is equipped with the trivial iterative derivation. In [Mau10a], Sect. 10, it is shown that this functor is representable by a C-algebra of finite type, and hence, is an affine group scheme of finite type over C. This group scheme is called the (iterative differential) **Galois group scheme** of the extension R over F – denoted by $\underline{\mathrm{Gal}}(R/F)$ –, or also, the Galois group scheme of the extension E over F, $\underline{\mathrm{Gal}}(E/F)$, where $E = \mathrm{Quot}(R)$ is the corresponding PV-field.

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

$$\gamma : R \otimes_F R \to R \otimes_C C[\underline{\mathrm{Gal}}(R/F)] \tag{5.1}$$

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

On the other hand, if (R, θ_R) is an ID-simple ID-ring extending (F, θ) with the same constants, and if there is an R-linear ID-isomorphism $\gamma : R \otimes_F R \to R \otimes_C C[\mathcal{G}]$ for some affine group scheme $\mathcal{G} \leq \mathrm{GL}_{n,C}$ corresponding to an action of $\mathcal{G}$, then R/F is indeed a Picard-Vessiot ring for some IDE (cf. [Mau10a], Prop. 10.12).

For later purposes, also keep in mind that for a finite Picard-Vessiot extension R/F, the PV-ring R already is a field. Hence, in that case the quotient field E coincides with the PV-ring R.

5.2 Iterative derivations compatible with addition

sec:it-der-on-ab-schemes

Let C be a field of positive characteristic p, $k = C(t)$ the rational function field with iterative derivation by t, and let A/C be a connected abelian scheme over C.

[1] The PV-rings and PV-fields defined here were called pseudo Picard-Vessiot rings (resp. pseudo Picard-Vessiot fields) in [Mau10a] and [Mau10b]. This definition, however, is the most natural generalisation of PV-rings and PV-fields to non algebraically closed fields of constants.

The addition map on A will be denoted by $\oplus : A \times A \to A$ (and the subtraction by $\ominus$).
Let K_A denote the function field of A. Let (L, θ) be the field $L = K_A(t)$ with some higher derivation θ extending the one on $k = C(t)$, and let D be the field K_A equipped with the trivial higher derivation. The higher derivations of L and D are extended to a higher derivation (also denoted by θ) on $LD := L \cdot D := \mathrm{Quot}(L \otimes_C D)$, the total ring of fractions of $L \otimes_C D$.

The map $\oplus$ induces a homomorphism of fields $K_A \to K_{A\times A} = K_A \cdot K_A$ and also a homomorphism $L \to L \cdot D$ by t-linear extension. Extending again D-linearly, we obtain an isomorphism $\rho : LD \to LD$. This isomorphism fixes exactly the elements in $D(t) \subseteq LD$, i.e. $D(t) = \{x \in LD \mid \rho(x) = x\}$. Actually ρ is nothing else than the homomorphism on the generic fibers corresponding to $A_{C(t)} \times A \to A_{C(t)} \times A, (p_1, p_2) \mapsto (p_1 \oplus p_2, p_2)$.

As the sheaf $\mathcal{O}_A$ of regular functions on A embeds into $D = K_A$, we have a generic point $\eta_D \in A(D) = \mathrm{Hom}(\mathcal{O}_A, D)$ given by that embedding. Similarly, we have a "generic point" $\eta_L \in A(L) = \mathrm{Hom}(\mathcal{O}_A, L)$ given by the inclusion $\mathcal{O}_A \subseteq K_A \to L$.

If we have a homomorphism of rings $\alpha : R_1 \to R_2$, we let $\alpha_* : A(R_1) \to A(R_2)$ denote the induced map from the R_1-points of A to its R_2-points.

lem:rho-HD-homo

Lemma 5.2.1. *With notation as above, let $\theta_* : A(L) \to A(L[[T]])$ be the map induced by $\theta : L \to L[[T]]$. Then ρ is an HD-homomorphism if and only if $\eta_L \ominus \theta_*(\eta_L) \in A(C(t)[[T]]) \subseteq A(L[[T]])$ where we consider η_L as an $L[[T]]$-point of A via the inclusion $L = L \cdot T^0 \subset L[[T]]$.*

Proof. Since in any case $\eta_L \ominus \theta_*(\eta_L) \in A(L[[T]])$, the condition is equivalent to saying that $\eta_L \ominus \theta_*(\eta_L) \in A(D(t)[[T]]) \subseteq A(LD[[T]])$.

Let η_D denote the generic point of A in $A(D)$, and $\rho_* : A(LD) \to A(LD)$ the map induced by ρ. Then by construction, one has $\rho_*(\eta_L) = \eta_L \oplus \eta_D$, and therefore, $\theta_*(\rho_*(\eta_L)) = \theta_*(\eta_L \oplus \eta_D) = \theta_*(\eta_L) \oplus \eta_D$, since θ acts trivially on D.

Hence:

$$\begin{aligned}
\eta_L \ominus \theta_*(\eta_L) \in A(D(t)[[T]]) &\Leftrightarrow (\rho[[T]])_*(\eta_L \ominus \theta_*(\eta_L)) = \eta_L \ominus \theta_*(\eta_L) \\
&\Leftrightarrow \rho_*(\eta_L) \ominus (\rho[[T]])_*(\theta_*(\eta_L)) = \eta_L \ominus \theta_*(\eta_L) \\
&\Leftrightarrow (\eta_L \oplus \eta_D) \ominus (\rho[[T]])_*(\theta_*(\eta_L)) = \eta_L \ominus \theta_*(\eta_L) \\
&\Leftrightarrow \theta_*(\eta_L) \oplus \eta_D = (\rho[[T]])_*(\theta_*(\eta_L)) \\
&\Leftrightarrow \theta_*(\rho_*(\eta_L)) = (\rho[[T]])_*(\theta_*(\eta_L))
\end{aligned}$$

Since η_L is the generic point of A, the last equality is equivalent to $\theta \circ \rho = \rho[[T]] \circ \theta$, i.e. to the condition that ρ is an HD-homomorphism. □

thm:commuting with rho

Theorem 5.2.2. *We use notation as above. Let $C(t)[[T, U]]$ be the power series ring over $C(t)$ in two variables T and U and let R denote the subring of $C(t)[[T, U]]$ of those power series $P(t, T, U)$ such that $P(t+U, T, 0) = P(t, T, U)$.*

Then θ is an iterative derivation and ρ is an ID-homomorphism if and only if $\theta_{U,*}(\eta_L) \ominus \theta_{T+U,*}(\eta_L) \in A(R)$.

As already mentioned earlier, $\theta_U : LD \to LD[[U]]$ and $\theta_{T+U} : LD \to LD[[T,U]]$ denote the maps θ with T replaced by U and $T+U$, respectively, and $\theta_{U,*} : A(LD) \to A(LD[[U]])$ as well as $\theta_{T+U,*} : A(LD) \to A(LD[[T,U]])$ the induced maps.

Proof. Let us first remark that R is nothing else than the image of $C(t)[[T]]$ under the homomorphism $\theta_U[[T]]$, since the map $\theta_U[[T]]$ on $C(t)[[T]]$ is just replacing t by $t+U$.
Now assume that θ is an iterative derivation such that ρ is an ID-homomorphism. Since θ is an iterative derivation, one has $\theta_{T+U} = \theta_U[[T]] \circ \theta_T$, and therefore $\theta_{U,*}(\eta_L) \ominus \theta_{T+U,*}(\eta_L) = (\theta_U[[T]])_* (\eta_L \ominus \theta_{T,*}(\eta_L))$. Since ρ is an ID-homomorphism, one has $\eta_L \ominus \theta_{T,*}(\eta_L) \in A(C(t)[[T]])$ by the previous lemma. Hence, we obtain $(\theta_U[[T]])_* (\eta_L \ominus \theta_{T,*}(\eta_L)) \in A(C(t)[[T,U]])$. By the characterisation of R above, the point $(\theta_U[[T]])_* (\eta_L \ominus \theta_{T,*}(\eta_L))$ is indeed R-valued.

For the converse, let $\theta_{U,*}(\eta_L) \ominus \theta_{T+U,*}(\eta_L) \in A(R)$. Applying the homomorphism $C(t)[[T,U]] \to C(t)[[T]]$ given by mapping U to 0 (or more precisely the induced map on the points of A) leads to $\eta_L \ominus \theta_{T,*}(\eta_L) \in A(C(t)[[T]])$, hence ρ is an HD-homomorphism by the previous lemma. As before, the condition that the expression is in $A(R)$ implies that we obtain the same element when mapping $U \mapsto 0$ and applying $(\theta_U[[T]])_*$. Hence

$$\begin{aligned} \theta_{U,*}(\eta_L) \ominus \theta_{T+U,*}(\eta_L) &= (\theta_U[[T]])_* (\theta_{0,*}(\eta_L) \ominus \theta_{T+0,*}(\eta_L)) \\ &= \theta_{U,*}(\eta_L) \ominus (\theta_U[[T]])_* (\theta_{T,*}(\eta_L)) \end{aligned}$$

This means $\theta_{T+U,*}(\eta_L) = (\theta_U[[T]])_* (\theta_{T,*}(\eta_L))$. Since η_L is the generic point, this implies $\theta_{T+U} = \theta_U[[T]] \circ \theta_T$, and therefore θ is iterative. □

Remark 5.2.3. So far, we didn't use commutativity of $\oplus$. Hence, all the statements made so far are also valid for non-commutative connected group schemes instead of abelian schemes.

5.3 Torsion schemes as Galois group schemes

sec:torsion-galois-groups

We use the notation of the previous section. In particular, A/C is an abelian scheme and L is the function field of $A_{C(t)}$ equipped with a higher derivation θ extending the iterative derivation with respect to t on $C(t)$.

thm:torsion as galois

Theorem 5.3.1. *Let θ be an iterative derivation on L such that ρ is an ID-homomorphism. Also assume that the constants of (L,θ) are C. For $n \in \mathbb{N}$, let $[n] : A \to A$ denote multiplication by n, $A[n] = \mathrm{Ker}([n])$ the n-torsion scheme, and $[n]^\# : L \to L$ the corresponding map on the function fields of $A_{C(t)}$. Then*

1. *the subfield $[n]^{\#}(L) \subseteq L$ is an ID-subfield of L,*

2. *the extension $L/[n]^{\#}(L)$ is a PV-extension and the iterative differential Galois group scheme is given as*

$$\underline{\mathrm{Gal}}(L/[n]^{\#}(L)) \cong A[n]$$

as affine group schemes over C.

Proof. The addition $A \times A[n] \to A$ induces a homomorphism $\bar{\rho} : \mathcal{O}_A(U) \to \mathcal{O}_A(U) \otimes_C C\big[A[n]\big]$ for an appropriate (affine) open subset $U \subseteq A$, where $C\big[A[n]\big]$ denotes the ring of regular functions on the affine scheme $A[n]$. The subring $[n]^{\#}(\mathcal{O}_A(U))$ is then the equalizer of $\bar{\rho}$ and $\mathrm{id} \otimes 1$.
Furthermore, $\bar{\rho}$ can be extended to a homomorphism $\bar{\rho} : L \to L \otimes_C C\big[A[n]\big]$ by $\bar{\rho}(t) = t \otimes 1$ and by localisation. This map $\bar{\rho}$ is actually a specialisation of the map $\rho : L \to LD$. By assumption ρ is an ID-homomorphism and therefore $\bar{\rho}$ is an ID-homomorphism when $C\big[A[n]\big]$ is equipped with the trivial iterative derivation.
This shows that the equalizer $[n]^{\#}(L) \subseteq L$ is an ID-subfield of L.

The L-linear extension of $\bar{\rho}$ leads to an ID-homomorphism $\bar{\rho}_L : L \otimes_{[n]^{\#}(L)} L \to L \otimes_C C\big[A[n]\big]$ which is a monomorphism, since $[n]^{\#}(L)$ is the equalizer of $\bar{\rho}$ and $\mathrm{id} \otimes 1$.
As the degree of the extension $L/[n]^{\#}(L)$ equals the dimension $\dim_C(C\big[A[n]\big])$, this monomorphism is indeed an ID-isomorphism.
Therefore, the second claim follows by [Mau10a], Prop. 10.12. (Here we use that the constants of L are indeed C.) □

Remark 5.3.2. In the previous theorem, there is an issue which we couldn't solve satisfactorily, namely whether a given higher derivation θ which satisfies the other conditions will also satisfy $L^{\theta} = C$. Even more, whether there exists such a θ. We will see in Proposition 5.5.4 that for the example considered in that section, there exists an iterative derivation satisfying all the assumptions above for cardinality reasons.

We are confident that a similar – but more involved – argument should also show the existence of such an iterative derivation θ as in Theorem 5.3.1 in the general case. Motivated by explicit calculations, we even think that $L^{\theta} \neq C$ only occurs in exceptional cases. In the case of elliptic curves we make this more precise in the following conjecture.

Conjecture 5.3.3. *If A is an elliptic curve, and θ an iterative derivation on L such that ρ is an ID-homomorphism, then either $L^{\theta} = C$ or $L^{\theta} = K_A \subseteq L$.*

Theorem 5.3.1 above has a consequence to the realisation of all commutative finite group schemes which was communicated to us by an anonymous referee. We state it in the following corollary.

cor:finite-group-schemes

Corollary 5.3.4. *Assume that for every abelian variety A/C, the function field L of $A_{C(t)}$ can be equipped with an iterative derivation θ satisfying the conditions in Thm. 5.3.1. Then every commutative finite group scheme G over C can be realised as ID-Galois group scheme of some PV-extension. Even more, G can be realised over some $[n]^{\#}(L)$ for such an ID-field (L, θ) and some $n \in \mathbb{N}$.*

Proof. Every commutative finite group scheme G over C can be embedded into an abelian variety over C, and hence into its subscheme of n-torsion points $A[n]$ for some n (see [**?**, Sect. 15.4]). Letting L be the function field of $A_{C(t)}$ with θ as in Thm. 5.3.1, we have $\underline{\mathrm{Gal}}(L/[n]^{\#}(L)) \cong A[n]$. By the Galois correspondence (cf. [Mau10a, Thm. 11.5]), one therefore obtains that G (now considered as a subgroup of $A[n]$) is the Galois group of L over L^G, the fixed field of L under G.

For obtaining the realisation over some $[n]^{\#}(L)$, one has to obtain G as a quotient of some $A[n]$. Then, one can again apply the Galois correspondence to this situation, and obtain that G is the ID-Galois group scheme of $L^{\mathrm{Ker}(A[n] \to G)}$ over $L^{A[n]} = [n]^{\#}(L)$.

Obtaining G as a quotient is done by first applying the embedding result to the Cartier dual $G^\vee$ of G, and possibly enlarging A (as e.g. in Zarhin's trick) so that A can be principally polarized. In this case the Cartier dual of $A[n]$ is again $A[n]$, and hence the embedding $G^\vee \to A[n]$ corresponds to a quotient map $A[n] \to G$. □

5.4 Extension of iterative derivations

sec:ID-extensions

In this section we develop criteria for a higher derivation to be iterative. This will be used in the last section. We will assume that C is a field of characteristic $p > 0$, and (F, θ) is an ID-field containing $C(t)$ such that $\theta|_{C(t)}$ is the iterative derivation with respect to t (compare Ex. 5(2)).

thm:equivalent conditions

Theorem 5.4.1. *Let L be a finitely generated separable field extension of F with a higher derivation on L extending θ on F, which will also be denoted by θ. Let $x_1, \ldots, x_k$ be a separating transcendence basis of L over F, and $\theta(x_i) =: x_i + \sum_{n=1}^{\infty} \xi_{i,n} T^n$ for all $i = 1, \ldots, k$.*
Assume that $\xi_{i,n} \in L^p F \subset L$ for all $i = 1, \ldots, k$ and all $n \geq 1$. Then for any $\ell_0 \geq 0$ the following are equivalent:

1. *The iteration rule holds on L up to level p^{ℓ_0+1}.*
2. *For all $0 \leq \ell \leq \ell_0$, one has:*
   (a) *for all $0 \leq m < p^\ell$ and $0 < a < p$: $\theta^{(m+ap^\ell)} = \frac{1}{a!} \left(\theta^{(p^\ell)}\right)^a \circ \theta^{(m)}$,*

(b) $\left(\theta^{(p^\ell)}\right)^p = 0$, *and*

(c) *for all* $0 \leq j < \ell$: $\theta^{(p^j)} \circ \theta^{(p^\ell)} = \theta^{(p^\ell)} \circ \theta^{(p^j)}$.

3. *The iteration rule holds up to level* p^{ℓ_0+1} *for all* x_i $(i = 1, \ldots, k)$.

3'. *Condition (2) holds when evaluated at all* x_i $(i = 1, \ldots, k)$.
item:explicite formula

4. *For all* $0 \leq \ell \leq \ell_0$ *and* $i = 1, \ldots k$, *one has:*

$$\xi_{i,p^\ell} + \sum_{m=1}^{p^\ell - 1} \theta^{(p^\ell)}(\xi_{i,m})(-t)^m \in \bigcap_{0 \leq j < \ell} \mathrm{Ker}\left(\theta^{(p^j)}\right) \cap \mathrm{Ker}\left(\theta^{(p^\ell(p-1))}\right),$$

for all $1 < a < p$:

$$\xi_{i,ap^\ell} = \frac{1}{a!}\left(\theta^{(p^\ell)}\right)^{a-1}(\xi_{i,p^\ell}),$$

and for all $0 < m < p^\ell$ *and* $0 < a < p$:

$$\xi_{i,m+ap^\ell} = \frac{1}{a!}\left(\theta^{(p^\ell)}\right)^{a}(\xi_{i,m}).$$

Remark 5.4.2. Condition (4) of the previous theorem, gives a recursive rule for constructing an iterative derivation on L. In more detail:

1. Choose $\xi_{i,1} \in L^pF \cap \mathrm{Ker}\left(\theta^{(p-1)}\right) = L^p\left(F \cap \mathrm{Ker}\left(\theta^{(p-1)}\right)\right)$ arbitrarily for all $i = 1, \ldots, k$.

2. Calculate $\xi_{i,a} := \frac{1}{a!}\left(\theta^{(1)}\right)^{a-1}(\xi_{i,1})$ for $1 < a < p$.

3. Proceed inductively: Assume that for $\ell > 0$, the elements $\xi_{i,m}$ for $m < p^\ell$ are already given satisfying condition (4) of the theorem. Then choose

$$\xi_{i,p^\ell} \in -\sum_{m=1}^{p^\ell - 1} \theta^{(p^\ell)}(\xi_{i,m})(-t)^m + \bigcap_{0 \leq j < \ell} \mathrm{Ker}\left(\theta^{(p^j)}\right) \cap \mathrm{Ker}\left(\theta^{(p^\ell(p-1))}\right) \cap L^pF$$

and calculate ξ_{i,ap^ℓ} for $1 < a < p$ as well as $\xi_{i,m+ap^\ell}$ for $0 < m < p^\ell$ and $0 < a < p$, by the rules above.
Since for an element $x^p \in L^p$, one has $\theta^{(p^\ell)}(x^p) = \left(\theta^{(p^{\ell-1})}(x)\right)^p$, the condition $\xi_{i,m} \in L^pF$ implies that $\theta^{(p^\ell)}(\xi_{i,m})$ is computable using only the values $\xi_{i,m}$ for $m < p^\ell$. By the same reason the set $\bigcap_{0 \leq j < \ell} \mathrm{Ker}\left(\theta^{(p^j)}\right) \cap \mathrm{Ker}\left(\theta^{(p^\ell(p-1))}\right) \cap L^pF$ is determined by the elements $\xi_{i,m}$ for $m < p^\ell$.

Proof of Thm. 5.4.1.

(1)⇔(2) All three conditions in (2) follow directly from the iteration rule for θ. On the other hand, given the conditions in (2), any $\theta^{(i)}$ with $i < p^{\ell_0+1}$ can be written as a composition of several $\theta^{(p^n)}$ as in Lemma 5.1.1(4). Then it is not hard to check that $\theta^{(i)} \circ \theta^{(j)}$ indeed equals $\theta^{(i+j)}$ whenever $i+j < p^{\ell_0+1}$. Using again this decomposition and the conditions $\left(\theta^{(p^\ell)}\right)^p = 0$, one verifies that $\theta^{(i)} \circ \theta^{(j)} = 0$ whenever $i, j > 0$ and $i + j = p^{\ell_0+1}$. Hence the iteration rule holds on L up to level p^{ℓ_0+1}.

(1)⇔(3) We only have to show that (3) implies (1). Since the set for which the iteration rule holds up to level p^{ℓ_0+1} is a subfield of L (cf. Lemma 5.1.2(1)) and since $x_1, \ldots, x_k$ generate $F(x_1, \ldots, x_k)$ over F it is immediate that the iteration rule holds up to level p^{ℓ_0+1} on $F(x_1, \ldots, x_k)$. But an extension of an iterative derivation to a finite separable field extension is unique, and again an iterative derivation. So the iteration rule holds on L up to level p^{ℓ_0+1}.

(2)⇔(3') This is shown in a similar way.

(1),(2) ⇒(4) By the iteration rule resp. condition (2)(a), one has

$$\xi_{i,m+ap^\ell} = \theta^{(m+ap^\ell)}(x_i) = \frac{1}{a!}\left(\theta^{(p^\ell)}\right)^a \circ \theta^{(m)}(x_i) = \frac{1}{a!}\left(\theta^{(p^\ell)}\right)^a (\xi_{i,m})$$

for all $0 < m \leq p^\ell$ and $0 < a < p$ s.t. $m + ap^\ell < p^{\ell+1}$. Furthermore for all $1 \leq m \leq p^\ell - 1$,

$$\begin{aligned}
\theta^{(p^\ell)}\left(\theta^{(m)}(x_i)(-t)^m\right) &= \sum_{k=0}^{p^\ell} \theta^{(k)}\theta^{(m)}(x_i)(-1)^m\theta^{(p^\ell-k)}(t^m) \\
&= \sum_{k=0}^{p^\ell} \binom{k+m}{k}\theta^{(k+m)}(x_i)(-1)^m\binom{m}{p^\ell-k}t^{m-p^\ell+k} \\
&= \theta^{(p^\ell+m)}(x_i)(-1)^m t^m = \theta^{(p^\ell)}(\xi_{i,m})(-t)^m,
\end{aligned}$$

as for $k < p^\ell - m$ the second binomial coefficient vanishes and for $p^\ell > k \geq p^\ell - m$ the first one. Hence, using condition (2)(c) and Lemma 5.1.2(3) we have

$$\theta^{(p^j)}\left(\xi_{i,p^\ell} + \sum_{m=1}^{p^\ell-1}\theta^{(p^\ell)}(\xi_{i,m})(-t)^m\right) = \theta^{(p^\ell)}\theta^{(p^j)}\left(x_i + \sum_{m=1}^{p^\ell-1}\theta^{(m)}(x_i)(-t)^m\right) = 0$$

for all $0 \leq j < \ell$ and by condition (2)(b)

$$\theta^{(p^\ell(p-1))}\left(\xi_{i,p^\ell} + \sum_{m=1}^{p^\ell-1}\theta^{(p^\ell)}(\xi_{i,m})(-t)^m\right) = \theta^{(p^\ell(p-1))}\theta^{(p^\ell)}\left(x_i + \sum_{m=1}^{p^\ell-1}\theta^{(m)}(x_i)(-t)^m\right) = 0.$$

(4)⇒(3') The formulae for ξ_{i,ap^ℓ} and $\xi_{i,m+ap^\ell}$ imply the conditions (2)(a) evaluated at x_i. Furthermore, by induction $\theta^{(p^{j-1})}\theta^{(p^{\ell-1})} = \theta^{(p^{\ell-1})}\theta^{(p^{j-1})}$ for all $j < \ell$ and hence $\theta^{(p^j)}\theta^{(p^\ell)}(x) = \theta^{(p^\ell)}\theta^{(p^j)}(x)$ for all $x \in L^pF$, in particular for $x = \theta^{(m)}(x_i)$. This implies

$$\begin{aligned}
0 &= \theta^{(p^j)}\left(\xi_{i,p^\ell} + \sum_{m=1}^{p^\ell-1} \theta^{(p^\ell)}(\xi_{i,m})(-t)^m\right) \\
&= \theta^{(p^j)}(\xi_{i,p^\ell}) - \theta^{(p^\ell)}\theta^{(p^j)}(x_i) + \theta^{(p^\ell)}\theta^{(p^j)}(x_i) + \theta^{(p^j)}\left(\sum_{m=1}^{p^\ell-1} \theta^{(p^\ell)}(\theta^{(m)}(x_i))(-t)^m\right) \\
&= \theta^{(p^j)}\theta^{(p^\ell)}(x_i) - \theta^{(p^\ell)}\theta^{(p^j)}(x_i).
\end{aligned}$$

The last step is obtained by the same calculation as above.

Similarly, one obtains

$$\begin{aligned}
0 &= \theta^{(p^\ell(p-1))}\left(\xi_{i,p^\ell} + \sum_{m=1}^{p^\ell-1} \theta^{(p^\ell)}(\xi_{i,m})(-t)^m\right) \\
&= \theta^{(p^\ell(p-1))}\theta^{(p^\ell)}(x_i) + \sum_{m=1}^{p^\ell-1} \theta^{(p^\ell)}\theta^{(p^\ell(p-1))}(\xi_{i,m})(-t)^m \\
&= \frac{1}{(p-1)!}(\theta^{(p^\ell)})^{p-1}\theta^{(p^\ell)}(x_i).
\end{aligned}$$

□

5.5 Example

sec:torsion-example

In this section, we restrict to an example for which it is even possible to give a recursive formula for constructing an iterative derivation θ which is compatible with the addition map (see Theorem 5.5.3). Indeed, it will be a sharpening of the formula in Thm. 5.4.1, Item 4. We also show that there is such an iterative derivation θ which additionally satisfies $L^\theta = C$ (see Prop. 5.5.4).

The example we consider is the elliptic curve E/C in characteristic $p = 2$ given by the equation $x^3 = z^2 + z$, the neutral element of addition being given by the point $(0, 0)$.

As before, K_E/C denotes the function field of E/C, and $L = K_E(t) = C(x, z, t)$ is the HD-field with a higher derivation θ extending the iterative derivation with respect to t on $C(t)$. The iterative derivatives of x are denoted by ξ_m, i.e. $\theta(x) =: x + \sum_{m=1}^{\infty} \xi_m T^m$, and $\eta_L := (x, z) \in E(L)$ is the generic point of E. Furthermore, $D = K_E$ denotes the ID-field with trivial iterative derivation.

Lemma 5.5.1. *For two points (x_1, z_1) and (x_2, z_2) with $z_1 \neq 1$ and $x_2 \neq \frac{x_1}{1+z_1}$, the difference $(x_d, z_d) := (x_1, z_1) \ominus (x_2, z_2)$ is given by:*

$$x_d = x_2 + \frac{x_1}{1+z_1} + \left(\frac{z_2 - \frac{z_1}{1+z_1}}{x_2 - \frac{x_1}{1+z_1}} \right)^2$$

and

$$z_d = \frac{z_2 - \frac{z_1}{1+z_1}}{x_2 - \frac{x_1}{1+z_1}} \cdot (x_d - x_2) + z_2$$

Proof. One only has to check, that the point (x_d, z_d) is the third intersection of the elliptic curve with the line passing through (x_2, z_2) and $\ominus(x_1, z_1) = (\frac{x_1}{1+z_1}, \frac{z_1}{1+z_1})$. □

Let

$$f(T) := \sum_{k=0}^{\infty} f_m T^m := \theta(x) + \frac{x}{1+z} + \left(\frac{\theta(z) - \frac{z}{1+z}}{\theta(x) - \frac{x}{1+z}} \right)^2 \in L[[T]].$$

Then by the previous lemma, $f(T)$ is the x-coordinate of $\eta_L \ominus \theta_*(\eta_L)$. For the coefficients f_m we have: $f_0 = 0$, $f_m = \xi_m$ for odd m and $f_m = \xi_m + (\widetilde{f_m})^2$ for even $m > 0$ and an appropriate element $\widetilde{f_m} \in L$, depending only on x, z and the elements ξ_k for $k \leq m/2$.

Furthermore, let $g(T)$ denote the z-coordinate of $\eta_L \ominus \theta_*(\eta_L)$, i.e. $\eta_L \ominus \theta_*(\eta_L) = (f(T), g(T))$ in these local coordinates. Since this is a point on E, one has the relation $f(T)^3 = g(T)^2 + g(T)$, and hence the coefficients g_m of $g(T) =: \sum_{k=0}^{\infty} g_m T^m$ can be expressed in terms of the f_m. In more detail, $g_0 = g_1 = g_2 = 0$ and g_m can be written as a polynomial in $f_1, \ldots, f_{m-2}$.

lem:theta-f

Lemma 5.5.2. *Assume that θ is an iterative derivation on L. Then for even $m, j \in \mathbb{N}\backslash\{0\}$ the difference $\theta^{(m)}(f_j) - \binom{m+j}{m} f_{m+j}$ is a polynomial in $\binom{(m+j)/2}{m/2} f_{(m+j)/2}$, $f_{(m+j)/2-1}, \ldots, f_1$, whereas for all other choices of $m, j \in \mathbb{N}$ this difference is 0.*

Proof. By definition, $f(T)$ is the x-coordinate of $\eta_L \ominus \theta_*(\eta_L)$, hence $\theta_U[[T]](f(T))$ is the x-coordinate of $(\theta_U[[T]])_*(\eta_L \ominus \theta_*(\eta_L))$. But

$$\begin{aligned} (\theta_U[[T]])_*(\eta_L \ominus \theta_*(\eta_L)) &= \theta_{U,*}(\eta_L) \ominus (\theta_U[[T]])_*(\theta_*(\eta_L)) \\ &= \theta_{U,*}(\eta_L) \ominus \eta_L \oplus \eta_L \ominus \theta_{U+T,*}(\eta_L) \\ &= \big(\eta_L \ominus \theta_{U+T,*}(\eta_L)\big) \ominus \big(\eta_L \ominus \theta_{U,*}(\eta_L)\big) \end{aligned}$$

Hence, $(\theta_U[[T]](f(T)), \theta_U[[T]](g(T))) = (f(U+T), g(U+T)) \ominus (f(U), g(U))$. Using the formula for the difference, we obtain

$$\theta_U[[T]](f(T)) = f(U) + \frac{f(T+U)}{1+g(T+U)} + \left(\frac{g(U) - \frac{g(T+U)}{1+g(T+U)}}{f(U) - \frac{f(T+U)}{1+g(T+U)}} \right)^2 \in L[[T, U]].$$

The coefficient of U^mT^j on the left hand side is $\theta^{(m)}(f_j)$. For the right hand side, we first remark that

$$\frac{f(T+U)}{1+g(T+U)} = f(T+U) + \big(g(T+U)/(T+U)\big)^2 \cdot \big(f(T+U)/(T+U)\big)^{-2},$$

as power series in $(T+U)$. So the right hand side is $f(U)+f(T+U)$ modulo squares. This already shows that the coefficient of U^mT^j on the right hand side is $\binom{m+j}{m} f_{m+j}$, if m or j are odd.

For the other coefficients one has to have a closer look at the equation. Therefore, we consider the remaining terms as power series in $(T+U)$ with coefficients in $L((U))$. The coefficient of U^mT^j in $\big(g(T+U)/(T+U)\big)^2 \cdot \big(f(T+U)/(T+U)\big)^{-2}$ is $\binom{m+j}{m}$ times the coefficient of $(T+U)^{m+j}$ in this expression. Since $\big(g(T+U)/(T+U)\big)$ is a multiple of $(T+U)^2$, this coefficient depends only on $f_{(m+j)/2-2}, f_{(m+j)/2-3}, \ldots, f_1$. The last term in the equality above is the square of

$$\begin{aligned}
\frac{g(U) - \frac{g(T+U)}{1+g(T+U)}}{f(U) - \frac{f(T+U)}{1+g(T+U)}} &= \frac{1}{1+g(U)} \cdot \frac{g(U) + g(U)^2 + (g(U)^2-1)g(T+U)}{f(U) + f(U)g(T+U) - f(T+U)} \\
&= \frac{1}{1+g(U)} \cdot \frac{f(U)^3 + (g(U)^2-1)g(T+U)}{f(U) + f(U)g(T+U) - f(T+U)} \\
&= \frac{1}{1+g(U)} f(U)^2 \cdot \frac{1 + \sum_{k=1}^{\infty} g_k (\frac{g(U)^2-1}{f(U)^3})(T+U)^k}{1 + \sum_{k=1}^{\infty} (g_k - \frac{f_k}{f(U)})(T+U)^k} \\
&= \big(1+g(U)\big)^{-1} f(U)^2 \cdot \left(\sum_{n=0}^{\infty} \tau_n (T+U)^n \right)
\end{aligned}$$

where τ_n is some polynomial in $f_1, \ldots, f_n$ (and $g_1, \ldots, g_n$), $g(U)$ and $\frac{1}{f(U)}$. Since the whole expression is a power series, $f(U)^2 \cdot \tau_n$ is already in $L[[U]]$. Hence, the coefficient of U^mT^j in $\left(\frac{1}{1+g(U)} f(U)^2 \cdot (\sum_{n=0}^{\infty} \tau_n (T+U)^n) \right)^2$ depends only on $f_{(m+j)/2}, f_{(m+j)/2-1}, \ldots, f_1$, and $f_{(m+j)/2}$ only occurs with the factor $\binom{(m+j)/2}{m/2}$. □

thm:strong formula

Theorem 5.5.3. *θ is an iterative derivation on L commuting with ρ if and only if for all $\ell \geq 0$ and all $0 < m < 2^\ell$ one has $\xi_{m+2^\ell} = \theta^{(2^\ell)}(\xi_m)$ and*

$$\xi_{2^\ell} \in \sum_{m=1}^{2^\ell-1} \theta^{(2^\ell)}(\xi_m) t^m + \left(\sum_{m=0}^{2^\ell-1} \theta^{(m)}(\widetilde{f}_{2^\ell}) t^m \right)^2 + C(t^{2^{\ell+1}}). \qquad (*_\ell)$$

In particular, it is possible to choose/calculate elements ξ_m recursively for $m = 1, 2, \ldots$ in order to obtain an iterative derivation on L commuting with ρ.

Proof. First let θ be an iterative derivation which commutes with ρ. Then $\xi_{m+2^\ell} = \theta^{(m)}(\xi_{2^\ell})$ for all $0 < m < 2^\ell$ by Theorem 5.4.1.
Further using the rules in Theorem 5.4.1, we obtain:

$$\xi_{2^\ell} + \sum_{m=1}^{2^\ell-1} \theta^{(2^\ell)}(\xi_m)t^m \;=\; \sum_{m=1}^{2^\ell-1} \theta^{(m)}(\xi_{2^\ell})t^m = \sum_{m=1}^{2^{\ell+1}-1} \theta^{(m)}(\xi_{2^\ell})t^m,$$

since $\theta^{(m)}(\xi_{2^\ell}) = 0$ for $2^\ell \le m < 2^{\ell+1}$, as well as

$$\begin{aligned}\left(\sum_{m=0}^{2^\ell-1} \theta^{(m)}(\widetilde{f}_{2^\ell})t^m\right)^2 &= \sum_{m=0}^{2^\ell-1} \left(\theta^{(m)}(\widetilde{f}_{2^\ell})\right)^2 t^{2m} = \sum_{m=0}^{2^\ell-1} \theta^{(2m)}\big((\widetilde{f}_{2^\ell})^2\big)t^{2m} \\ &= \sum_{m=0}^{2^{\ell+1}-1} \theta^{(m)}\big((\widetilde{f}_{2^\ell})^2\big)t^m,\end{aligned}$$

since $\theta^{(m)}\big((\widetilde{f}_{2^\ell})^2\big) = 0$ for m odd. Combining these we get:

$$\begin{aligned}&\xi_{2^\ell} + \sum_{m=1}^{2^\ell-1} \theta^{(2^\ell)}(\xi_m)t^m + \left(\sum_{m=0}^{2^\ell-1} \theta^{(m)}(\widetilde{f}_{2^\ell})t^m\right)^2 \\ &\quad= \sum_{m=0}^{2^{\ell+1}-1} \theta^{(m)}(\xi_{2^\ell})t^m + \sum_{m=0}^{2^{\ell+1}-1} \theta^{(m)}\big((\widetilde{f}_{2^\ell})^2\big)t^m = \sum_{m=0}^{2^{\ell+1}-1} \theta^{(m)}(f_{2^\ell})t^m\end{aligned}$$

This expression is in $C(t)$, since $f_{2^\ell} \in C(t)$ by Lemma 5.2.1, and it is in the intersection $\bigcap_{0\le j<\ell+1} \mathrm{Ker}(\theta^{(p^j)})$ by Lemma 5.1.2, hence in $C(t^{2^{\ell+1}})$ as desired.

On the other hand, assume that the conditions on ξ_{m+2^ℓ} and on ξ_{2^ℓ} hold. We will first show that θ is an iterative derivation by showing inductively that $\theta^{(j)} \circ \theta^{(m)} = \binom{j+m}{j}\theta^{(j+m)}$ for all $j + m \le 2^{\ell_0+1}$.

For $\ell_0 = 0$, condition $(*_{\ell_0})$ is just $\xi_1 \in C(t^2)$, which implies $\theta^{(1)}(\xi_1) = 0$. Hence by Theorem 5.4.1, the iteration rule holds for all $j + m \le 2 = 2^{0+1}$. Now, assume by induction that the iteration rule holds for all $j + m \le 2^{\ell_0}$. Then it even holds for all $j + m < 2^{\ell_0+1}$, since $\xi_{m+2^\ell} = \theta^{(2^\ell)}(\xi_m)$, and we obtain by Lemma 5.1.2 that $\theta^{(2^j)}\left(\sum_{m=0}^{2^{\ell_0}-1} \theta^{(m)}(x)t^m\right) = 0$ for all $x \in L$ and $0 \le j < \ell_0$, in particular $\theta^{(2^j)}\left(\sum_{m=0}^{2^{\ell_0}-1} \theta^{(m)}(\widetilde{f}_{2^{\ell_0}})t^m\right) = 0$ for $0 \le j < \ell_0$. Therefore using $(*_{\ell_0})$, $\xi_{2^{\ell_0}} + \sum_{m=1}^{2^{\ell_0}-1} \theta^{(2^{\ell_0})}(\xi_m)t^m \in \bigcap_{0\le j\le\ell_0} \mathrm{Ker}(\theta^{(2^j)})$. By Theorem 5.4.1, this shows that the iteration rule holds for $j + m \le 2^{\ell_0+1}$.

It remains to show that ρ is an ID-homomorphism. By Lemma 5.2.1, this is equivalent to $f_k \in C(t)$ for all $k \ge 1$. Again we use induction: The case $k = 1$ is given by condition $(*_0)$, since $f_1 = \xi_1$. Assume $f_m \in C(t)$ is already shown for

$1 \leq m \leq 2^\ell - 1$. If $k = 2^\ell + m$ for some $0 < m < 2^\ell$, then by Lemma 5.5.2, $f_{2^\ell+m}$ differs from $\theta^{(2^\ell)}(f_m)$ by a polynomial in f_j for $1 \leq j \leq 2^\ell - 1$, and hence is an element of $C(t)$ by induction. If $k = 2^\ell$, condition $(*_\ell)$ and the calculations above imply that

$$\sum_{m=0}^{2^{\ell+1}-1} \theta^{(m)}(f_{2^\ell})t^m \in C(t). \tag{$\dagger$}$$

By using Lemma 5.5.2, and $f_{2^\ell+m} \in C(t)$ as well as $f_j \in C(t)$ for $1 \leq j \leq 2^\ell - 1$, we see that $\theta^{(m)}(f_{2^\ell})$ is an element of $C(t)$ for $0 < m < 2^\ell$, and also $\theta^{(2^\ell)}(f_{2^\ell}) \in C(t)$, since $\binom{2^{\ell+1}}{2^\ell}$ and $\binom{2^\ell}{2^{\ell-1}}$ are both zero in characteristic 2. For $2^\ell < m < 2^{\ell+1}$, we have $\theta^{(m)}(f_{2^\ell}) = \theta^{(m-2^\ell)}\left(\theta^{(2^\ell)}(f_{2^\ell})\right) \in C(t)$. Therefore all the terms in ($\dagger$) different from f_{2^ℓ} are in $C(t)$ and hence $f_{2^\ell} \in C(t)$. □

prop:theta-exists

Proposition 5.5.4. *The higher derivation θ in Theorem 5.5.3 (or the ξ_i's respectively) can be chosen in such a way that $L^\theta = C$.*

Proof. If we have an iterative derivation θ on L such that $L^\theta \supsetneq C$, then L is finite over $L^\theta(t)$, since both fields have the same transcendence degree. Since all ID-extensions of $L^\theta(t)$ with same constants are separable, there is a separable irreducible polynomial $\mu[X] \in L^\theta(t)[X]$ such that $\mu(x) = 0$, and the higher derivatives ξ_i of x are uniquely determined by μ (comp. Example 5(3)). In particular, the parameter space of such iterative derivations is bounded by the countably dimensional C-vector space of polynomials with coefficients in $L \supseteq L^\theta(t)$.

On the other hand, the space of iterative derivations satisfying the conditions in Theorem 5.5.3 is parametrized by $\prod_{\ell \geq 0} C(t^{2^{\ell+1}})$ which has uncountable dimension over C. Hence, there is an iterative derivation θ as desired (and indeed uncountably many). □

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*. PhD thesis, University of Tsukuba, Tsukuba, Japan, 2005.

[Ama06] Katsutoshi Amano. On a discrepancy among picard-vessiot theories in positive characteristics. Preprint, Dezember 2006.

[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.

[BHH16] Annette Bachmayr, David Harbater, and Julia Hartmann. Differential Galois groups over Laurent series fields. *Proc. Lond. Math. Soc. (3)*, 112(3):455–476, 2016.

[BHHP17] Annette Bachmayr, David Harbater, Julia Hartmann, and Florian Pop. Large fields in differential Galois theory. Preprint available from arXiv at http://arxiv.org/abs/1710.03183, October 2017.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Bru94] Alain Bruguières. Théorie tannakienne non commutative. *Comm. Algebra*, 22(14):5817–5860, 1994.

[ByB62] A. Biał ynicki Birula. On Galois theory of fields with operators. *Amer. J. Math.*, 84:89–109, 1962.

[Car58] Pierre Cartier. Questions de rationalité des diviseurs en géométrie algébrique. *Bull. Soc. Math. France*, 86:177–251, 1958.

[CHS13] Teresa Crespo, Zbigniew Hajto, and Elżbieta Sowa. Picard-Vessiot theory for real fields. *Israel J. Math.*, 198(1):75–89, 2013.

[CHvdP16] Teresa Crespo, Zbigniew Hajto, and Marius van der Put. Real and p-adic Picard-Vessiot fields. *Math. Ann.*, 365(1-2):93–103, 2016.

[CS69] Stephen U. Chase and Moss E. Sweedler. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[Del90] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990.

[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.

[DM82] Pierre Deligne and James S. Milne. Tannakian Categories. In *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*, pages 101–228. Springer-Verlag, Berlin, 1982.

[Dyc08] Tobias Dyckerhoff. The inverse problem of differential Galois theory over the field R(z). Preprint, 2008.

[Fra63] Charles H. Franke. Picard-Vessiot theory of linear homogeneous difference equations. *Trans. Amer. Math. Soc.*, 108:491–515, 1963.

[GP87] Cornelius Greither and Bodo Pareigis. Hopf Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 1987.

[Har95] David Harbater. Fundamental groups and embedding problems in characteristic p. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 353–369. Amer. Math. Soc., Providence, RI, 1995.

[Har05] Julia Hartmann. On the inverse problem in differential Galois theory. *J. Reine Angew. Math.*, 586:21–44, 2005.

[Hei07] Florian Heiderich. Picard-Vessiot-Theorie für lineare partielle Differentialgleichungen. Master's thesis, Heidelberg University, 2007.

[Inf81] Ronald P. Infante. On the Galois theory of difference fields. *Aequationes Math.*, 22(2-3):194–207, 1981.

[Jan03] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2003.

[Kat82] Nicholas M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[Kat87] Nicholas M. Katz. On the calculation of some differential Galois groups. *Invent. Math.*, 87(1):13–61, 1987.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.

[Kol48] E. R. Kolchin. Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)*, 49:1–42, 1948.

[Kol52] E. R. Kolchin. Picard-Vessiot theory of partial differential fields. *Proc. Amer. Math. Soc.*, 3:596–603, 1952.

[Kre65a] H. F. Kreimer. An extension of differential Galois theory. *Trans. Amer. Math. Soc.*, 118:247–256, 1965.

[Kre65b] H. F. Kreimer. On an extension of the Picard-Vessiot theory. *Pacific J. Math.*, 15:191–205, 1965.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Mat01] B. Heinrich Matzat. Differential Galois theory in positive characteristic, 2001. Notes written by J. Hartmann.

[Mau10a] Andreas Maurischat. Galois theory for iterative connections and nonreduced Galois groups. *Trans. Amer. Math. Soc.*, 362(10):5411–5453, 2010.

[Mau10b] Andreas Maurischat. Infinitesimal group schemes as iterative differential Galois groups. *J. Pure Appl. Algebra*, 214(11):2092–2100, 2010.

[Mau13] Andreas Maurischat. On the finite inverse problem in iterative differential galois theory. In *Séminaires et Congrès 27, Geometric and differential Galois theories*. Société Mathématique de France, 2013.

[Mau14] Andreas Maurischat. Picard-Vessiot theory of differentially simple rings. *J. Algebra*, 409:162–181, 2014.

[Mau15] Andreas Maurischat. Torsion group schemes as iterative differential galois groups. Preprint available from arXiv at http://arxiv.org/abs/1203.6198, October 2015.

[ML65] Saunders Mac Lane. Categorical algebra. *Bull. Amer. Math. Soc.*, 71:40–106, 1965.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[MS96] C. Mitschi and M. F. Singer. Connected linear groups as differential Galois groups. *J. Algebra*, 184(1):333–361, 1996.

[MS02] Claude Mitschi and Michael F. Singer. Solvable-by-finite groups as differential Galois groups. *Ann. Fac. Sci. Toulouse Math. (6)*, 11(3):403–423, 2002.

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

[Oku63] Kôtaro Okugawa. Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory. *J. Math. Kyoto Univ.*, 2:295–322, 1962/1963.

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

[OW15] Alexey Ovchinnikov and Michael Wibmer. σ-Galois theory of linear difference equations. *Int. Math. Res. Not. IMRN*, (12):3962–4018, 2015.

[Pap08] Matthew A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Invent. Math.*, 171(1):123–174, 2008.

[Pic91] Émile Picard. *Traité d'analyse. Tome III.* Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1991. Des singularités des équations différentielles. Étude du cas où la variable reste réelle. Des courbes définies par des équations différentielles. Équations linéaires; analogies entre les équations algébriques et les équations linéaires. Intégration de certaines équations aux dérivées partielles avec des conditions aux limites, [Singularities of differential equations. Study of the case in

which the variable remains real. Curves defined by differenial equations. Linear equations; analogies between algebraic equations and linear equations. Integration of some partial differential equations with boundary conditions], Reprint of the third (1928) edition.

[Ple64] Josip Plemelj. *Problems in the sense of Riemann and Klein*. Edited and translated by J. R. M. Radok. Interscience Tracts in Pure and Applied Mathematics, No. 16. Interscience Publishers John Wiley & Sons Inc. New York-London-Sydney, 1964.

[Rös07] Andreas Röscheisen. *Iterative Connections and Abhyankar's Conjecture*. PhD thesis, Heidelberg University, Heidelberg, Germany, 2007.

[Sei56] A. Seidenberg. Contribution to the Picard-Vessiot theory of homogeneous linear differential equations. *Amer. J. Math.*, 78:808–818, 1956.

[Sin93] Michael F. Singer. Moduli of linear differential equations on the Riemann sphere with fixed Galois groups. *Pacific J. Math.*, 160(2):343–395, 1993.

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

[Tak72] Mitsuhiro Takeuchi. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.*, 7:251–270, 1972.

[Tak89] Mitsuhiro Takeuchi. A Hopf algebraic approach to the Picard-Vessiot theory. *J. Algebra*, 122(2):481–509, 1989.

[TT79] Carol Tretkoff and Marvin Tretkoff. Solution of the inverse problem of differential Galois theory in the classical case. *Amer. J. Math.*, 101(6):1327–1332, 1979.

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

[vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

[Ves92] Ernest Vessiot. Sur l'intégration des équations différentielles linéaires. *Ann. Sci. École Norm. Sup. (3)*, 9:197–280, 1892.

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.

[Wib10] Michael Wibmer. *Geometric Difference Galois Theory*. PhD thesis, Heidelberg University, Heidelberg, Germany, 2010.